



UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN TELECOMUNICACIONES MENCIÓN: GESTIÓN DE LAS TELECOMUNICACIONES

Resolución: RPC-SE-01-No.016-2020

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del trabajo:

Desarrollo de una red domótica aplicando el Internet de las Cosas con una herramienta tecnológica de simulación y verificación de conectividad

Línea de Investigación:

Telecomunicaciones y Sistemas Informáticos aplicados a la producción y la sociedad

Campo amplio de conocimiento:

Ingeniería, industria y construcción

Autor/a:

Eddie Xavier Yánez Suikouski

Tutor/a:

PhD. Fidel David Parra Balza

Quito – Ecuador

2021

APROBACIÓN DEL TUTOR



Yo, Fidel David Parra Balza con C.I: 1757469950 en mi calidad de Tutor del trabajo de investigación titulado: Diseño y simulación de una red domótica para aplicación del Internet de las cosas.

Elaborado por: Eddie Xavier Yánez Suikouski, de C.I: 1710537471, estudiante de la Maestría: en Telecomunicaciones, mención: Gestión de las Telecomunicaciones de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito, 09 de septiembre de 2021

Ph. D. Fidel David Parra Balza



TABLA DE CONTENIDOS

APROBACIÓN DEL TUTOR	ii
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE ¡Error! Marcador no definido.	
ÍNDICE DE TABLAS	iv
ÍNDICE DE FIGURAS	v
INFORMACIÓN GENERAL	1
Contextualización del tema.....	1
Pregunta Problémica.....	2
Objetivo general.....	2
Objetivos específicos.....	2
Beneficiarios directos.....	2
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO	4
1.1. Contextualización de fundamentos teóricos	4
1.2. Problema a resolver	7
1.3. Proceso de investigación.....	8
1.4. Vinculación con la sociedad	8
1.5. Indicadores de resultados	8
CAPÍTULO II: PROPUESTA.....	9
2.1. Fundamentos teóricos aplicados	9
2.2. Descripción de la propuesta.....	18
2.3. Matriz de articulación	38
CONCLUSIONES.....	39
RECOMENDACIONES.....	41
BIBLIOGRAFÍA.....	42
ANEXOS	44

ÍNDICE DE TABLAS

Tabla 1 Características de herramientas tecnológicas de simulación.....	19
Tabla 2 Fases a desarrollar de acuerdo a los objetivos específicos planteados	23
Tabla 3 Dispositivos de red y dispositivos compatibles con IoT	25
Tabla 4 Direccionamiento IPv4 de la red de Internet	27
Tabla 5 Direccionamiento IPv4 de la red de la empresa IoT.....	28
Tabla 6 Direccionamiento IPV4 de la red de proveedor de servicio de cable.....	28
Tabla 7 Direccionamiento IPV4 de la red de DSL	29
Tabla 8 Matriz de articulación.....	38

ÍNDICE DE FIGURAS

Figura 1 Componentes del objeto IoT.....	17
Figura 2. Como se construye un proyecto de domótica orientado al IoT.....	21
Figura 3. Diagrama general de las redes.....	24
Figura 4. Diagrama de la Red de redes.....	29
Figura 5. Diagrama de la Red de la empresa de servicio IoT.....	30
Figura 6. Diagrama de la Red de servicio móvil.....	31
Figura 7. Diagrama de la red del proveedor de servicios de cable.....	32
Figura 8. Diagrama de la Red de DSL.....	32
Figura 9. Topología física de la red.....	33
Figura 10. Diagrama de la Red inalámbrica donde se conectan los objetos IoT al WiFi.....	35
Figura 11. Conexión de objetos inteligentes dentro de la misma red.....	35
Figura 12. Comando remoto de los dispositivos IoT.....	36
Figura 13. Diagrama de la Red Smart Home.....	37

INFORMACIÓN GENERAL

Contextualización del tema

El trabajo de investigación que se presenta, consiste en crear diferentes redes de área extensa y local para formar una estructura global de redes como internet, proveedor de servicios, telefonía, y redes domótica, para lograr la conectividad de los objetos inteligentes, para lo cual se utilizará una aplicación como herramienta para el diseño y simulación de redes, donde se podrá verificar el funcionamiento de los dispositivos y visualizar el acceso remoto a la red domótica desde un *smartphone* que controlara las “cosas” dentro del hogar; con esto se ampliara el concepto e importancia del Internet de las Cosas y los beneficios hacia los usuarios.

En el boletín estadístico No. 2020-02 de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), menciona que Ecuador comenzaría con el desarrollo de tecnología inalámbrica de quinta generación (5G) en el año 2021, pero los tiempos tuvieron cambios por el asunto de la pandemia mundial del covid19 además, se estimaba que para el año 2023 dicha tecnología ya estaría desarrollada y se tendría más de 60 millones de conexiones de la red 5G en el 2025 en América Latina con 25 mil millones de conexiones globales, datos según la Asociación para el Sistema Global de Comunicaciones Móviles (GSMA), que es una organización que representa a los intereses de las operadoras móviles a nivel mundial.

Se pronostica que habrá un número mayor de 20 mil millones de “cosas” (objetos del mundo físico) en el Internet de las cosas o conocido también como *Internet of Things*, por sus siglas en inglés (IoT), ya para el año 2021 que puedan comunicarse entre sí. Gracias a esta conectividad entre “cosas” se pueden controlar y monitorear en forma remota e inalámbrica, entre otras cosas, la luz, calefacción, los electrodomésticos, sensores inteligentes, interruptores, etc. Además, se puede compartir datos e información entre equipos, cosas y dispositivos inteligentes. (MINTEL, 2020).

Con el avance de la tecnología, las nuevas o potenciadas aplicaciones, el crecimiento de usuarios conectados a la red del Internet, los servicios de almacenamiento en la nube; la plataforma del IoT permite que se conecten los objetos que antes no eran conectados para el beneficios de los usuarios tanto para el hogar como la industria y generan un cambio significativo en la automatización de los procesos, que está llevándose a cabo con la creación de ciudades inteligentes, casas inteligentes, accesorios inteligentes, etc.

Es así, de acuerdo a las publicaciones más recientes en la IEEE, que es el Instituto de Ingenieros Eléctricos y Electrónicos, de tesis de posgrado publicadas y revistas científicas que tienen como referencia al IoT, además se considera que es un tema de actualidad con gran

crecimiento a nivel mundial, se puede manifestar que el presente trabajo de investigación es innovador y será una fuente pedagógica sustancial por tal razón se lo debe realizar.

Pregunta Problemática

¿Qué aplicación servirá como herramienta de simulación didáctica para crear una red doméstica donde incluya dispositivos y objetos inteligentes que logren comunicarse remotamente?

Al no disponer de laboratorios que cuenten con la infraestructura adecuada y todos los insumos necesarios para prácticas de construcción de diferentes topologías de red y aplicaciones como la plataforma IoT; el presente trabajo investigativo con el uso de un software libre de construcción y simulación de redes, se realizara la configuración de los *router*, servidores y objetos inteligentes que formen parte de las diferentes redes aplicado al Internet de las cosas.

Objetivo general

Desarrollar una red doméstica aplicando el Internet de las Cosas con una herramienta tecnológica de simulación y verificación de conectividad.

Objetivos específicos

- Definir los fundamentos teóricos de la domótica para la aplicación del internet de las cosas.
- Determinar los dispositivos y equipos adecuados que permitan la simulación de la red doméstica aplicado al Internet de las cosas.
- Diseñar las redes necesarias con el software *Packet Tracer* que permita la visualización del funcionamiento de los objetos inteligentes de la red doméstica desde un teléfono *smartphone*.
- Elaborar la simulación de las redes para la conectividad de los objetos inteligentes aplicado a la domótica.
- Validar el desempeño de los componentes principales utilizados en la red doméstica mediante un análisis de conectividad para determinar su efectividad.

Beneficiarios directos

Para los estudiantes que estén cursando los últimos semestres de la Universidad Tecnológica Israel de carreras a fines que tengan interés en el IoT desde la herramienta de estudio *Packet Tracer* que es utilizado en las materias de CCNA, para los usuarios con interés en las redes de

computación y el Internet de las Cosas, que servirá de antecedentes para futuros proyectos de investigación y además se debe considerar el desarrollo de las telecomunicaciones en el país está en proceso con la próxima llegada de la tecnología inalámbrica de quinta generación que permitirá potenciar aplicaciones como el Internet de las cosas, la inmótica, la domótica y la creación de las *smart city* y *smart house*, que beneficiará en general a los usuarios en las actividades cotidianas del hogar y la industria sea esta de forma directa o indirecta.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización de fundamentos teóricos

El presente trabajo titulado “Desarrollo de una red domótica aplicando el Internet de las Cosas con una herramienta tecnológica de simulación y verificación de conectividad” se considera que tenga un enfoque metodológico y cuyo objetivo es la visualización mediante simulación de la conectividad de los objetos para ampliar el conocimiento de los beneficios que conlleva el uso de tecnologías y aplicaciones en la sociedad que permitan la recopilación, procesamiento y envío de datos, para lograr dar inteligencia a las cosas y resolver problemas relacionados o simplemente, facilitar el trabajo diario de las personas.

Por otro lado, se ha tomado a cinco fuentes teóricas de publicaciones en la IEEE, tesis a nivel de doctorado y maestría de los autores Figueroa, Tamayo, Meneghelo y otros, Hwang y otros, Swany y otros en el periodo comprendido entre el año 2017 al 2020, que tienen relación con el tema de investigación propuesto en el presente trabajo.

Donde a la simulación se la debe considerar como una herramienta de apoyo pedagógico que es un recurso viable para la investigación y desarrollo de un tema específico al usar la teoría y la práctica además de la demostración de resultados.

En el ámbito de las comunicaciones y el desarrollo de la tecnología, es importante considerar las nuevas tendencias mundiales que están en auge en países desarrollados como es el caso del Internet de las cosas, que pretende mostrar todo su potencial y aplicaciones apoyados de la llegada de la tecnología de quinta generación, que cambiara considerablemente las telecomunicaciones a nivel mundial.

Con el uso de una herramienta tecnológica con el aval de Cisco como es el *Packet Tracer* (PT), muy utilizado para la simulación de redes, que permite diseñar desde cero o sobre proyectos pre construidos, se realizará una red de redes aplicado al Internet de las Cosas.

Se puede señalar que para realizar el tema investigativo se hizo una revisión de los trabajos previos que tienen alguna relación con las variables a utilizar como son el Internet de las cosas, redes de computadoras, domótica, protocolos, dispositivos, automatización, entre los que se destaca los siguientes trabajos:

El elaborado por Figueroa (2017), que presento una tesis de doctorado sobre “Estudio de la influencia de un entorno de simulación en la enseñanza de redes de computadoras en el nivel universitario”, presentada en la Universidad Nacional de La Plata, con las siguientes variables: *Packet Tracer*, redes de computadoras, direccionamiento IP (Protocolo de Internet), apoyado en 51 fuentes de información como revistas internacionales, exposiciones de congresos, cursos, documentos como tesis y libros.

Al no ser tan factible por el aspecto económico disponer de equipos específicos para el montaje de laboratorios de redes y demás insumos para las prácticas pedagógicas de las diferentes topologías y sumando el mantenimiento y actualizaciones de los equipos de acuerdo al avance tecnológico el estudio dio como resultado los métodos de simulación para aplicaciones de redes de computadoras con el uso de diferentes softwares y la influencia que incide en los estudiantes en su aprendizaje a nivel universitario.

Las herramientas utilizadas para la simulación de redes de computación en el trabajo de investigación fueron *Packet Tracer*, GNS3 y Kiva-NS, dichos software cuentan con gran potencial para simulaciones de protocolos de comunicación muy apropiados para laboratorios de redes. La similitud con el tema planteado es el uso de la herramienta pedagógica *Packet Tracer* para la simulación de redes y la diferencia es que a partir de la versión 7.0 de PT ya dispone de dispositivos que permite utilizar objetos inteligentes para la simulación de redes aplicados al Internet de las Cosas.

El trabajo de titulación de maestría de Tamayo (2018), sobre “Estudio de factibilidad de la tecnología *connected home* a través del Internet de las Cosas IoT dentro de la ciudad de Quito (D.M)” presentado en septiembre con las variables Internet de las cosas, *connected home*, Mercado, Análisis financiero, VAN, y TIR, apoyado en 50 fuentes bibliográficas.

Obtuvo como resultado que, a pesar de existir varias marcas de dispositivos inteligentes disponibles en el mercados nacionales e internacionales, en Ecuador existe pocas empresas que brinden servicios de implementación e instalación de equipos *connected home* aplicado al IoT. Como semejanza con el tema de investigación es la factibilidad de uso de la tecnología *connected home* aplicado al IoT y como diferencia se orientará al lector en el diseño global de la red domótica aplicada al IoT de forma gráfica.

En la ciudad de Quito mediante el método de encuesta el 84.1% de la muestra tendría el interés de adquirir el servicio de instalación de los equipos inteligentes, pero existe un porcentaje mínimo que estaría en la capacidad económica de adquirirlo. Se entiende que el porcentaje a la fecha actual debe ser diferente por el avance y la comercialización de la tecnología en el país.

Mientras que Meneghello, Calore, Zucchetto, Polese, & Zanella (2019), realizaron un artículo científico “IoT: ¿Internet de las amenazas? Una encuesta de vulnerabilidades de seguridad prácticas en dispositivos IoT reales”. publicado en la IEEE el 13 de agosto, con las siguientes variables: Ataques, Dispositivos, Internet de las cosas (IoT), Seguridad, apoyado en 123 fuentes referenciales, entre artículos de revistas y libros.

Como resultado se obtuvo la adopción generalizada de soluciones de Internet de las cosas para sensores, redes, domótica, aplicaciones de salud. La importancia de la seguridad de las

comunicaciones en las redes de IoT y tiene como similitud con el tema de investigación que los dispositivos IoT se están transformando progresivamente como objetos comunes y de uso cotidiano en la sociedad, pero suele suceder que el usuario final a menudo desconoce de las seguridades con los dispositivos que forman parte en su día a día. Como diferencia es que no se abordó el tema de seguridad a pesar de ser uno de los ejes fundamentales del IoT.

Las redes inalámbricas de IoT pueden exponer la información personal y confidencial; sin la autenticación, los atacantes malintencionados pueden hacerse pasar por dispositivos legítimos e interrumpir la red de IoT, en el artículo, el *ZigBee* y BLE, brindan la factibilidad de uso sobre la seguridad sólida

Hwang y otros (2020), realizaron un artículo científico de “AUTOCON-IoT: automatizado y escalable en línea Pruebas de conformidad para aplicaciones de IoT”, motivados por el crecimiento exponencial de las aplicaciones de IoT en las ciudades e industrias inteligentes y la falta de mecanismos de pruebas de conformidad estandarizadas; dicho artículo fue publicado por la IEEE el 9 de octubre, con las siguientes variables: Pruebas de conformidad, Internet de las cosas (IoT), Interoperabilidad. Estándares M2M, Pruebas de Automatización, apoyado en 49 fuentes referenciales, entre artículos de revistas y libros.

En la investigación logran como resultado la descripción de una conformidad automatizada y escalable del mecanismo de prueba mediante la introducción de un mecanismo de activación en el estado actual del arte de las pruebas de conformidad en el IoT. El mercado actual de IoT está fragmentado debido a la ineficiencia en las pruebas de conformidad, lo que crea problemas entre múltiples aplicaciones de IoT, debido a la a gran escala de las aplicaciones de IoT, cada una de las cuales tiene docenas de funciones y es difícil realizar la conformidad manual de pruebas. El enfoque del estudio para las pruebas de conformidad automáticas ayuda a acelerar el proceso de prueba y certificación de los organismos de normalización de IoT.

La publicación más actual encontrada lo realizó Swany & Raju (2020), con el método investigativo de “Un estudio empírico sobre aspectos a nivel del sistema de Internet de las cosas (IoT)”, publicado por la IEEE el 9 de octubre, con las siguientes variables: IoT, Pilares de IoT, Aplicaciones emergentes de IoT, Requisitos de aplicaciones de IoT, Arquitectura de IoT, Protocolos de capa de aplicación de IoT, Paradigmas informáticos, Privacidad y seguridad, Plataforma para IoT; con información de 318 fuentes referenciales, entre artículos de revistas y libros.

El resultado fue la comprensión básica de Internet de las cosas, junto con las tendencias de investigación actuales en tecnologías de IoT a partir de 2020, las características y requisitos del IoT, aplicaciones emergentes de IoT, análisis de los desafíos en el diseño del sistema de IoT, tendencias de investigación en arquitecturas de IoT, problemas que son necesarios y deberían

ser abordado en el futuro. La similitud con el tema de investigación es la concordancia de los beneficios pronosticados con la llegada de la plataforma del Internet de las Cosas hacia la sociedad que mejorara considerablemente su vida cotidiana y la diferencia es que el documento incorpora programaciones y configuraciones que pueden ser aplicados a los equipos de red.

Los estándares de comunicación en IoT, junto con investigaciones futuras, los protocolos de la capa de aplicación de IoT y los requisitos más importantes como: confiabilidad, escalabilidad, adaptación, conciencia del contexto, interoperabilidad, inteligencia integrada, son temas importantes a ser considerados.

Por consiguiente, para el desarrollo de la red domótica aplicado al IoT, se utilizarán redes WAN y LAN de diferentes clases, donde incluya las redes domésticas, del proveedor de servicios, de IoT, DSL, una red de telefonía y por supuesto la red global de Internet, además los equipos y cosas que se integren en la simulación. Además, se detallará una breve descripción de los dispositivos utilizados.

Con el apoyo de la herramienta tecnológica de Cisco *Packet Tracer*, versión 7.0 o superior para Windows de 64 bits, se construirán las redes necesarias con sus respectivos *interfaces* para enlazar todas las cosas que se usen en la red domótica y establecer la conectividad entre los dispositivos para simular el funcionamiento de las objetos inteligentes para acceder de forma remota desde los dispositivos inteligentes que se encuentren fuera de las redes de área local de donde se encuentran instaladas las cosas, para de forma gráfica mostrar las virtudes de contar con un sistema automatizado e inteligente dentro de un hogar.

Para la configuración de los equipos de red se utilizará redes de clase A, B y C; además, a cada dispositivo se le asignará una dirección de protocolo de Internet versión 4 (IPv4), con su respectiva máscara de subred, sean de /16, /24 o /30; se detallarán las configuraciones de los *router* o *switch*, servidores DHCP, MCU, dispositivos inteligentes, cosas, etc. Finalmente se deberá evaluar el desempeño de la red domótica en referencia a la conectividad efectiva de los dispositivos de la red, sus inconvenientes y posibles soluciones.

1.2. Problema a resolver

Con el avance tecnológico de los países considerados como potencias mundiales, se crea una brecha tecnológica muy grande en países como el Ecuador, además del costo económico que implica disponer de laboratorios para aplicativos IoT, dispositivos de última tecnología y de un proveedor de servicios, dificulta su implementación; pero, tarde o temprano se presentará la oportunidad de comprobar los beneficios de la tecnología y dejar a un lado lo manual e introducirse en el campo de la digitalización y automatización en el hogar o la industria.

En la actualidad los fabricantes están trabajando como solventar la incompatibilidad de los equipos por sus marcas, ya muchos países están normando las tecnologías vigentes, para lograr la estandarización de equipos y sistemas. Conocer al IoT de una forma pedagógica e ilustrativa puede dar un mayor panorama de su potencial y mediante la simulación con una herramienta como *Packet Tracer* permitirá el desarrollo del tema planteado y obtener un testeado del funcionamiento de la red, para comprobar la conectividad entre los dispositivos, finalmente lograr comandar remotamente el funcionamiento de los objetos inteligentes de la red doméstica.

1.3. Proceso de investigación

Por lo antes expuesto es necesario establecer la metodología con la que se va a llevar el procedimiento para cumplir con los objetivos planteados por consiguiente es un paradigma cuantitativo de tipo documental y diseño no experimental. Mientras que la población objeto de estudio en esta investigación es el conjunto de dispositivos y equipos de red además de la herramienta de diseño, mientras que para la muestra se consideran los mismos factores del conjunto de la población.

1.4. Vinculación con la sociedad

Cada día crece la necesidad de tener el control de las cosas físicas que están alrededor de las personas, estar más conectados con el mundo, por tal razón existe grupos de la población que utilizan la tecnología como un recurso cotidiano para comunicarse y estar al día con la información, por consiguiente, la plataforma orientada a objetos, puede facilitar la interacción entre el hombre y los objetos inteligentes y lograr que la sociedad con el uso de la tecnología acceda y controle de forma remota sus objetos IoT implementados en sus hogares desde cualquier lugar del mundo, para mejorar la vida cotidiana de las personas.

1.5. Indicadores de resultados

Además de ser una fuente de información para futuros proyectos de investigación se incluye un valor práctico en donde, se pueden utilizar las configuraciones realizadas en el presente documento ubicados en el anexo A, en los equipos físicos de la marca Cisco, partiendo de los resultados efectivos de la simulación ejecutada. El levantamiento de las *interfaces* de los dispositivos con su respectiva comprobación de la latencia y que esta no sea superior a 100 ms se puede considerar como efectiva. Además, de medir los alcances o logros de la red IoT del presente trabajo de investigación con enfoque a la conectividad de los dispositivos de la red doméstica.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

A continuación, se explica los fundamentos teóricos aplicados al tema en desarrollo con la finalidad de encaminar a los conocimientos generales utilizados como la conectividad que hoy en día es parte fundamental del ser humano; se podría decir que es una necesidad para el hombre y cada vez se expande por todo el mundo incluso fuera del planeta. La evolución en las telecomunicaciones es constante y cada vez aparece tecnologías nuevas, como es el caso de la tecnología inalámbrica de quinta generación (5G), que actualmente está en proceso de implementación; pero ya se escucha de la sexta generación de la conectividad móvil conocida como 6G.

Por consiguiente, se debe estar preparados para los cambios tecnológicos y la inclusión de aplicaciones que permitan mejorar las condiciones de las personas como la domótica aplicado al internet de las cosas (IoT). En el presente trabajo investigativo con el uso de una herramienta tecnológica de libre acceso de la empresa Cisco denominado *Packet Tracer* con la versión 7.3, se pretende mostrar el alcance y virtudes que implica el IoT en el hogar o en la industria, para ello se va a construir una topología de redes WAN y LAN, donde se utilice equipos para conectar dichas redes, además de varios dispositivos con acceso de IoT.

Se realizará las configurarán de los dispositivos de redes para establecer la conectividad entre ellos y de los componentes de la red de redes, con el objetivo de comandar las “cosas” de forma remota mediante un celular inteligente, *tablet* o *laptop*, mediante una simulación.

De este modo con las configuraciones de los *router*, servidores y dispositivos, cada uno con su respectiva dirección única IP que significa protocolo de Internet, se prevé lograr la conectividad de los dispositivos que formen parte de la simulación de la red domótica para aplicación del Internet de las cosas. En este sentido es importante conocer el significado de los términos y temas como:

Internet: es un sistema de red de redes conformado con más de 100.000 redes interconectas que logran formar la red más grande a nivel mundial para permite intercambiar libremente información entre sus usuarios, así se eliminó las fronteras y se conectó a las agencias gubernamentales, clientes comerciales e individuos privados, estableciéndose como Ley en el Ecuador el acceso de los servicios del régimen general de telecomunicaciones sobre la base de cuatro servicios incluidos el acceso al internet. (MINTEL, Plan de Servicio Universal, 2018).

Con la aparición del protocolo TCP/IP se establece el concepto de internet y aparece la WWW (*World Wide Web*) que en informática se le conoce como la red informática mundial y es un

sistema de distribución que permite compartir documentos de hipertexto, en otras palabras, es un texto que contienen enlaces hacia otros textos por medio de la red y es donde aparece el protocolo HTTP (*HyperText Transfer Protocol*) que es el método para transferir datos e información en la WWW mediante la red de redes.

El Internet permite la conectividad entre las personas y los dispositivos, es un recurso fundamental para la conectividad a nivel mundial, y cada día se convierte en una parte cotidiana de las personas, gracias a esta plataforma la comunicación es inmediata y sin barreras, además, fue declarado en el año 2011 como un derecho humano fundamental por las Naciones Unidas

Interfaz: como el medio físico que permite la comunicación de dos o más sistemas que no necesariamente dispongan de un lenguaje de comunicación común o idéntico. (Velasco, Sánchez, Laureano, & Mora, 2009).

Red: y se dice que se considera al grupo de equipos, elementos y dispositivos periféricos que se comunican y comparten información entre cada uno de componentes de la red. La conexión de dos equipos que comparten datos se considera como una pequeña red. (WordPress, 2016).

TCP/IP: Que fue definido en el año 1981 e implementado en 1990 y sirve para la comunicación de los dispositivos de la red y es necesario contar con un protocolo de comunicación que se utiliza en sistemas con diferentes inter redes y este puede operar en capas de red y capa de transporte que son considerados en el modelo OSI. (Madrid, 2016).

Para las configuraciones de TCP/IP es necesario una dirección IP, la máscara de subred y la puerta de enlace; el protocolo TCP/IP en la red de internet tiene gran capacidad para conectar a las redes de diferentes tamaños y de diferentes tipos de sistemas, de donde parten las redes de clases A, B y C como las más comunes y las redes de clases D y E. Las direcciones de internet son asignadas por la organización que administra el internet.

De acuerdo al informe técnico de Evans (2011), quién para esa fecha era el director tecnológico de Cisco, publico que en febrero de 2010 ya se agotaron los protocolos de Internet **IPv4** que se asignan automáticamente cuando se registra un dominio; las direcciones IPv4 que vendrían hacer casi 4.300 millones de direcciones de direcciones IP, mientras que sus reservas se previa que se agoten en el 2020. De ahí parte la aparición y uso de la versión 6 del protocolo de Internet **IPv6** que viene a ser una actualización del protocolo IPv4 para soportar todos los dispositivos que se conecten en los próximos años para manejar con mayor eficiencia los paquetes, para optimizar el rendimiento y la seguridad.

Enrutadores: son equipos que trabaja a nivel de capa 3 del modelo OSI se los conoce también como *router* y son dispositivos de red que tienen la finalidad de realizar el enrutamiento de los

paquetes entre las diferentes redes independientes; dicho enrutamiento se ejecuta mediante una la tabla de enrutamiento, donde obedece las reglas definidas. Dichos equipos permiten la comunicación de los dispositivos con el mundo exterior por medio de los protocolos de comunicación como el *Ethernet*, RFID, WiFi, *Bluetooth*, etc.

Internet de las cosas (IoT): que se hace referencia a la infraestructura que a nivel mundial presta el servicio a la comunidad de la información que brinda mejores y avanzados servicios mediante el uso de la interconexión física y virtual de las “cosas” y ésta a su vez, con el IoT que se refiere a los objetos del mundo físico donde se consideran a las cosas físicas y también en el mundo de la información que en cambio están las cosas virtuales, para obtener la interoperabilidad de las tecnologías que involucren a la información y la comunicación. (ITU, 2012).

El IoT pretende conectar lo que no ha sido conectado al internet, para que se pueda compartir datos, información, estados, etc. La incorporación de nuevas “cosas” con inteligencia, pueden brindar mayor comodidad a las personas en el día a día, tanto en el hogar, la industria, y las ciudades, mediante el uso de aplicativos e dispositivos inteligentes como son las laptop o teléfonos móviles.

En el año de 1982 se conectó la primera máquina dispensadora de refrescos al internet y en 1990 un electrodoméstico como la tostadora se podía prender y apagar de forma remota; para el año 1999 ya se empezó a escuchar el concepto del Internet de las Cosas en el Instituto Tecnológico de Massachusetts (MIT), mencionado por Kevin Asthon que explico el potencial beneficio de la identificación por radio frecuencia (RFID) en sus trabajos; para el 2000 hubo planes por parte de LG crear un refrigerador que mediante internet se tenga el acceso al registro de las cosas almacenadas; el departamento de los EEUU en el año 2003 implementa la identificación de Radiofrecuencia para identificar contenedores y para el 2005 la Unión Internacional de Telecomunicaciones (UIT) publicó un primer informe del Internet de las Cosas.

La primera conferencia en la Unión Europea trató de la incorporación de IP en las redes de objetos inteligentes y la habilitación del Internet de las Cosas en el año 2008, un año después Cisco inicia la comercialización del IoT, al año siguiente 2010, China toma al IoT como industria clave para los planes de desarrollo a largo plazo, el año siguiente es lanzado el protocolo de internet versión 6 IPv6 y el IoT empieza a normalización por la UIT; en el 2013 la empresa Google lanza al mercado las *google glass* con visualización de realidad aumentada, un año después otra empresa como Amazon promociona el “*Echo*” para iniciar con el “*Smart Home*”.

Una plataforma fundamental para el IoT es el 5G que fue iniciado la fase de pruebas en los juegos Olímpico de invierno de Corea en el año 2018. En la actualidad se estima más de 20

millones de dispositivos con aplicativos IoT conectados. (Terrazas, Guarneros, Ponce, Esqueda, & Martínez, 2019).

En el entorno del IoT es importante conocer las capas que están interactuando con el objetivo de comunicarse para enviar información y que esta sea analizada y procesada para generar una acción, en tal virtud se tiene las siguientes capas:

1. Capa física: Se trata específicamente del hardware y constituyen todos los dispositivos físicos que puedan realizar acciones de captura, procesamiento y transmisión de información, para ello deben contar con la interfaz de usuario, módulo de comunicación, sensores y actuadores, y dispongan de tareas de cómputo y espacio de almacenamiento.
2. Capa de comunicación de red: Interactúan las diferentes tecnologías tanto físicas como de radiocomunicación que se dispone actualmente con el fin de comunicarse entre los dispositivos de la capa física con los dispositivos de las redes. Entre las tecnologías se puede mencionar a la Tecnología **RFID** (*Radio Frequency Identification*) que es un identificador automático de productos por radiofrecuencia a los objetos que porten la etiqueta, **NFC** (*Near Field Communication*) que permite la transmisión de información mediante el uso de ondas de radio de corto alcance y se basa en RFID, **Bluetooth** con el estándar de la IEEE 802.15.1 que utiliza la transmisión inalámbrica de corto alcance para la comunicación de voz y datos.

Además, se tiene las tecnologías **Zigbee** de tipo IEEE 802.15.4, que tienen un alcance mayor, que va desde los 10 a 100m y es inalámbrica con uso en la domótica e industria, **Z-Wave** basado en RF y que cubre un rango de acción de 100 a 180m, también es inalámbrica que permite controlar y monitorear aplicaciones de entorno en casas y oficinas. Como una de las más utilizadas se tiene el **WiFi** con un rango de 0 a 1000m, tecnología inalámbrica que utiliza el estándar IEEE 802.11 y que actualmente ya tienen cinco variables del estándar, otra tecnología es **EnOcean** de baja potencia para el uso de convertidores de poder miniatura, su uso en hogares y edificios inteligentes como aire acondicionado, iluminación, etc.

A Continuación, se puede mencionar a la tecnología **Lora** (*LoraWan*), estándar abierto con alcance de 5 a 30km para aplicación en la industria y ciudades inteligentes cuya arquitectura de red permite la comunicación de mensajes de los dispositivos con un servidor central, **Sigfox** con rango similar a Lora pero en la frecuencia 900Mhz y menor tasa de transmisión que no supera 1 Kbps, no licenciado

que utilizada para la comunicación M2M (*machine to machine*) de largo alcance, muy utilizado en Europa, la tecnología **Weightless** totalmente abierto, que pertenece a LPWAN (*low power wide area networks*) que significa redes de área amplia de baja potencia, con estándar abierto con rango de 2km para la comunicación bidireccional entre dispositivos, **NB-Fi** para la comunicación hombre – máquina de baja potencia en área amplia con rango de hasta 30km.

Ahora la tecnología **EC-GSM-IoT** que es una tecnología basada en redes (GSM 2G). **NB-IoT** con acceso de radio celular en base a LTE que trabaja en múltiples bandas de frecuencia como 600, 700 y 850Mhz. Con alcance menor de 15km, **LTE-M** que se usa para conexiones de móvil incorporando la voz mediante la utilización de antenas LTE, **Celular** con las tecnologías que van desde 3G hasta 5G, **WIMAX**, con el estándar IEEE 802.16 que es una tecnología inalámbrica con velocidades similares a ADSL o cable modem, con un alcance de hasta 50Km, para aplicaciones de IoT. **Satelital** que es una conexión mediante satélites geoestacionarios que utilizan las bandas C:4-8Ghz, Ku: 12-18Ghz, y Ka: 27- 40Ghz con cobertura mundial.

3. Capa de procesamiento: permite el almacenamiento y procesamiento de la información registrada por los sensores y tiene la capacidad de actuar con la capa física, además se puede hacer uso de servicio de la nube
4. Capa de almacenamiento: la información almacenada se encuentra en reposo y disponible para el uso de aplicaciones que tengan permitido el acceso a los datos, para mayores capacidades de información se utiliza cómputo en la nube para los procesos internos automatizados que estén distantes.
5. Capa de abstracción: tiene relación con la capa de almacenamiento con el objetivo de centrarse en la prestación y almacenamiento de datos, para permitir el desarrollo de aplicaciones para mejorar su rendimiento.
6. Capa de servicio, aplicación, colaboración y procesamiento: permite interpretar la información de capa de aplicación y mantener la información disponible en la capa de servicio, mientras que la capa de aplicación realiza los reportes, análisis y control de la información y finalmente la capa de procesamiento involucran los procesos de las personas y sus negocios para darle un fin específico. (Terrazas, Guarneros, Ponce, Esqueda, & Martínez, 2019).

Entre las aplicaciones que están en progreso gracias el Internet de las Cosas se pueden mencionar lo citado de acuerdo al documento de investigación de (Brea, 2018).

- *Wearables*: llamados a los dispositivos electrónicos que se pueden utilizar en alguna parte del cuerpo, enfocados en la salud y el bienestar de los usuarios, donde se podrán medir por ejemplo las calorías del cuerpo, el ritmo cardiaco y a través del sudor, la saliva, la temperatura, etc. Lograr obtener datos importantes que permitan ser analizados por un médico y determinar el estado actual de un paciente, sin que éste tenga que acudir a una unidad médica para ser valorado.
- Internet de los edificios (IoB): donde se integran otros recursos con inteligencia como el *smart grid* que hace referencia a la distribución eléctrica inteligente que son combinadas con la tecnología de la información, que intercambian paquetes de energía con el distribuidor y hacen uso de aplicaciones para interactuar con dispositivos IoT. Dichos IoB entran a formar parte de las *smart city* cuando interaccionan con objetos externos inteligentes.
- Internet del vehículo (IoV): que hace referencia al transporte inteligente con la incorporación de aplicaciones que mejoren la gestión del transporte en beneficio del usuario y por supuesto la autonomía de los vehículos eléctricos que actualmente están en usos en países pioneros de la automatización como en China y Japón, que pretende cambiar la matriz productiva reduciendo el consumo de combustibles fósiles para evitar la contaminación.
- Agricultura y ganadería inteligente: que permita mejorar la productividad de la tierra con el uso de las aplicaciones para la prevención de plagas y controlar la cantidad de insecticidas, evaluar la calidad del agua, la prevención de eventos naturales. El IoT también es utilizado en las actividades de pesca y medio ambiente.
- *Smart Home*: que es un sistema que permite el control y monitoreo de un hogar y se usa en la instalación y configuración de objetos inteligente, que permiten manejar con facilidad las acciones dentro y fuera del hogar. En cualquier caso, ofrece la posibilidad de vigilar y controlar el hogar cómodamente desde un dispositivo *smartphone* o *tablet* con la ayuda de una intuitiva aplicación.
- Ciudades Inteligentes: conocidas también como *smart city* que optimizan el desarrollo de las infraestructuras con el uso de aplicaciones tecnológicas de información y comunicación para garantizar un desarrollo sostenible,

incrementando la calidad de vida con mayor eficiencia de los recursos disponibles, en beneficio de la sociedad que permite mejorar la economía y el bienestar social, con la integración de las demás aplicaciones del Internet de las Cosas.

- **Industria inteligente:** con el uso de IoT en la manufacturación de productos y en la industria en general, en donde utiliza la computación basada en sensores, la analítica industrial y las aplicaciones inteligentes, para mejorar los procesos.

Domótica: que viene del término *domus* (casa) y de tica (automática) y se entiende al conjunto de técnicas orientadas a la automatización de las casas para brindar comunicación, seguridad, comodidad y ahorro energético a los usuarios; la domótica tiene relación con dar inteligencia a las viviendas con el uso de la red de comunicación en donde se integran la electrónica, la informática y los procesos a la infraestructura tecnológica que coexiste con la estructura del hogar, todo con el fin de satisfacer al usuario y dar mayor comodidad y confort en el hogar (Díaz, 2017).

En la actualidad existe además de la domótica que es exclusivo para el hogar y que no necesariamente está ligado con la conexión del Internet, la inmótica que está orientada a la aplicación de tecnologías que permitan dar control y automatización en edificio, pero con la diferencia que estos no sean utilizados para vivienda.

Con la domótica se obtiene funciones de control remoto por lo general in situ, además de la gestión automatizada de procesos cíclicos programados. El control dentro del hogar facilita al usuario el manejo de tareas sin tener que movilizarse y sirve de gran ayuda en personas con discapacidad o de la tercera edad, a diferencia del control remoto fuera del hogar que permite optimizar el recurso tiempo y brinda el control de tareas desde cualquier punto donde se disponga de conectividad y se pueda enlazar a la red de Internet.

Entre los elementos principales que permiten obtener información (variables físicas o químicas) y esta a su vez transformarlas en variables eléctricas y enviarlas para realizar un proceso se tiene a los sensores, por lo contrario, los elementos de respuesta que van a realizar una acción para un proceso determinado se tienen a los actuadores que convierten la energía eléctrica, neumática o hidráulica en dicha acción. Los sensores más comunes que se encuentran normalmente en el mercado son los sensores de temperatura, movimiento, magnéticos, ópticos, de distancia laser, de vibración, de luz, para la calidad del aire, de distancia ultrasónicos y larga distancia, sensores de inundación, entre otros.

Mientras que los dispositivos de respuestas como son los actuadores más comunes se tienen a los motores DC, servomotores, opto acopladores, relés, las cámaras, entre otros. Los servicios

más relevantes que brinda la domótica a los usuarios gracias a la inteligencia de los objetos se puede mencionar a:

- **Seguridad:** Al Hablar de seguridad como parte física, con la domótica se pueden incorporar varias alternativas para proteger su hogar de actos maliciosos, un ejemplo de esto sería el acoplar un sistema de simulación de presencia, esto ayuda a programar el encendido y apagado de luces con el objetivo de dar un ambiente de presencia de personas en el hogar. Así mismo, sistemas de detección de humo, gas, inundaciones, etc. Qué mediante un mensaje, luces de alerta o una alarma sonora pueda notificar al usuario o a la entidad correspondiente sobre el hecho que se está en proceso.
- **Confort:** Es un servicio que brinda comodidad al usuario dentro del hogar, donde en sus manos tiene opciones de control para comandar por ejemplo los niveles de atenuación de la iluminación, sistemas motorizados y climatización, mando del audio y video, entre otras cosas que brinda la automatización del hogar.
- **Ahorro energético:** Un aspecto a considerar es la racionalización de la energía eléctrica y ésta a su vez se transforma en ahorro económico para el hogar, con la implementación de sistemas de temporización o detección de movimiento vinculado a la iluminación, cambio de electrodomésticos a tecnología *smart frost* para controlar el nivel de enfriamiento, etc.
- **Monitorización:** Con el uso de aplicaciones para dispositivos inteligentes, pantallas táctiles o desde la web se puede tener el control remoto de los objetos inteligentes en el hogar donde se puede determinar el estado y las acciones a tomar desde cualquier parte donde se tenga acceso al Internet.

Objeto inteligente: En el mundo físico existen infinidad de objetos o cosas (que carecen de vida) a nuestra disposición, pero dichos objetos se vuelven inteligentes cuando mediante una interfaz de comunicación se logran conectar con el internet. Al hablar de los objetos del Internet de las cosas se deben considerar los componentes de acuerdo a la figura 1.



Figura 1 Componentes del objeto IoT

Fuente: (Cuzme, 2015)

Dichos componentes se integran en un solo objeto inteligente que si se parte desde la base de la gráfica se tiene al microcontrolador, que es un circuito integrado que contiene la CPU, las memorias y las I/O como unidades de entrada y salida; mientras que el *firmware*, viene a ser el programa básico que permite controlar la parte electrónica de los dispositivos. La información que recibe el objeto es a través de los sensores para que los actuadores realicen la ejecución de un proceso o instrucciones programadas, naturalmente es necesario de disponer de una fuente de alimentación para el funcionamiento de los objetos.

A Continuación, con la conectividad, que hace referencia a los protocolos de comunicación entre los dispositivos que les permitan interactuar entre ellos, mientras que la parte que permite manejar al dispositivo es el SO (sistema operativo), que utiliza un conjunto de programas con pasos lógicos al utilizar un lenguaje de programación y esta a su vez permiten la instalación de aplicaciones para mejorar la funcionalidad de los objetos inteligentes.

Packet Tracer: Es herramienta de simulación libre de la empresa *networking CISCO SYSTEMS* que permite la construcción y simulación de redes de computación, se desarrolla en un entorno gráfico y su interfaz si puede considerar sencilla para el manejo de los usuarios. El archivo de instalación se puede descargar de la página www.netacad.com, con la última versión 8.0.1 (ingles) de un tamaño de 150MB para plataformas de Windows, Ubuntu y MacOS

Packet Tracer (PT), es muy utilizado en pedagogía de redes de computación, ya que es un programa integral de enseñanza y aprendizaje al permitir ensayar con los dispositivos de

networking desde la parte teórica hasta lograr las competencias procedimentales para que los estudiantes comprendan la lógica de programación y la viabilidad de acuerdo a los componentes del hardware. Esto quiere decir que es importante considerar las condiciones físicas de los equipos y su configuración, para así lograr una estructura de conectividad de la red.

Es importante manifestar que es necesario tener una cuenta en *Cisco Netacad* para acceder a la herramienta de *Packet Tracer* para aquello basta con realizar el registro en *Cisco Networking Academy*. La versión actual de *Cisco Packet Tracer 8.0* presenta dos actualizaciones, la primera en referencia al modo físico mejorado, con el cableado de dispositivos del *rack* lo más realista posible, desde su instalación, encendido, cableado de puertos, etc. Y la segunda actualización es el controlador de red, muy similar a los controladores SDN disponibles en el mundo real, se puede realizar prácticas de gestión de red centralizadas.

2.2. Descripción de la propuesta

➤ ***Descripción general de la propuesta***

El mundo del internet de las cosas, pretende cambiar significativamente los sistemas de automatización utilizados en las grandes industrias, pero también se debe considerar a los hogares como potenciales consumidores a futuro de la domótica, es así que, para mostrar de una forma gráfica, se ha planteado realizar un sistema de control aplicado al hogar o una *smart house*, con el uso de una herramienta de simulación como es el *Packet Tracer (PT)*, muy utilizada en el aprendizaje a nivel universitario y para la certificación de *Cisco Certified Network Associate (CCNA)*. PT permite el diseño, construcción y simulación de redes mediante el software IOS.

En el presente trabajo se van a crear redes de área local (LAN) y de áreas amplias (WAN), con la finalidad de crear diferentes redes y que entre las mismas exista la conectividad; para lo cual, se formaran las redes de Internet, doméstica (donde se aplicará la domótica), del proveedor de servicios, DSL, de una empresa de telefonía móvil y la red de la empresa IoT; donde se utilizan redes de clase A, B y clase C. De este modo, lograr obtener el control de los dispositivos inteligentes instalados en la red domótica que son considerados como “cosas” en el IoT, y las mismas se puedan comandar remotamente mediante un dispositivo móvil.

Es importante dar a conocer que existen varias herramientas tecnológicas de simulación y construcción de redes de pago y libres que están disponibles y en uso para el diseño de aplicaciones en el Internet de las cosas, de las cuales se presentan en la tabla 1 donde se puede hacer una breve comparación entre dichas herramientas tecnológicas de simulación.

Tabla 1*Características de herramientas tecnológicas de simulación*

Programa	Licencia	Aprendizaje	Plataforma	Interface gráfica	Aplicación IoT
NS3	Libre	Alto	Unix y Windows	Intermedio	Si
Omnet++	Libre	Alto	Unix y Windows	Intermedio	Si
GNS3	Comercial y libre	Intermedio	Windows, Mac y Linux	Alto	Si
Tossim	Libre	Bajo	TinyOs	Alto	Si
NetSim	Comercial	Alto	Windows	Alto	Si
PTracer	Libre	Alto	Unix, Win, GNU, Macintosh	Alto	Si

Nota. Direccionamiento de IPv4 de clase A y B

NS3 es un software de código abierto que se basa en eventos, utiliza C++ como su lenguaje de programación, además puede modelar en Python con algunas tecnologías, es compatible con aplicaciones como *Wireshark*; mientras que *Omnet++*, se utiliza para simulación de redes y capaz de modelar sistemas complejos de software, multiprocesadores y hardware distribuido, maneja una gran interfaz gráfica para visualización de las topologías, simulación y análisis de resultados, muy utilizado en el ámbito del aprendizaje académico. (Hernández, López & Vilajosana, 2020).

Por otro lado, GNS3 también es un software de código abierto, muy utilizado para la certificación de *Cisco Certified Network Professional (CCNP)* y sirve para el diseño y emulación de redes, utiliza módulos *Qemu*, *Dynamips* y *VirtualBox*, con una interfaz gráfica potente para asemejarse a lo real, en cambio *Tossim* es un simulador muy potente para el desarrollo, comprobación de protocolos y aplicaciones de WSN que significa redes de sensores inalámbricos, muy utilizados en IoT, utiliza la herramienta *PowerTossim* para generar mediciones de energía. (Marelli, 2015)

Finalmente, las herramientas *Netsim* permite la simulación de protocolos, redes para modelado, construcción y desarrollo de redes, es muy utilizado para el análisis de sistemas informáticos, compatible con software de *Matlab*, *Wireshark* y *Sumo*, tiene diferentes versiones para clientes comerciales, educativos y para interactuar en vivo. Mientras que la herramienta

utilizada en el presente trabajo investigativo, puede considerarse como la más popular en el aprendizaje por su sencillez, *interfaz* gráfico y manejo para la construcción y simulación de redes interactivas, es una herramienta que tiene como objetivo el entrenamiento para la certificación de CCNA, CCNP y CCIE, ya que maneja simulación de equipos Cisco. (Calle, Tovar, Castaño, & Cuellar, 2018)

a. Estructura general

En la forma de llamada de flecha hacia abajo de la figura 2, incluye los componentes principales que son necesarios para lograr obtener un proyecto aplicado al Internet de las Cosas como son:

- Hardware: que está conformado por los sensores y actuadores
- Conectividad: con los protocolos de comunicación
- Plataforma: Que permite la recolección de la información y donde existen las aplicaciones que son orientadas al internet de las Cosas.

A los tres componentes antes descritos más la plataforma de Internet como la red de redes más grande a nivel mundial que es donde las personas tienen acceso a los servicios de la nube, almacenamiento, navegación, gestión de datos, seguridad, etc. Se obtiene lo necesario para crear un proyecto aplicado al Internet de las Cosas, mientras al IoT se integran y relacionan componentes como las personas, cosas, datos y procesos, para lograr crear la red de objetos físicos que tiene la capacidad de combinar dichos componentes con el fin de intercambiar datos entre dispositivos para realizar una acción mediante la conexión de Internet.

En definitiva, IoT es el Internet con más objetos inteligentes conectados que personas. La plataforma IoT es el escenario ideas donde la domótica como la base para la inteligencia del hogar, se puede explotar a su máximo nivel con el objetivo de brindar a los usuarios seguridad física, ocio y comodidad para lograr la comunicación efectiva con los objetos inteligentes que pueden ser controlados remotamente para optimizar los recursos energéticos y así obtener un mayor ahorro económico.

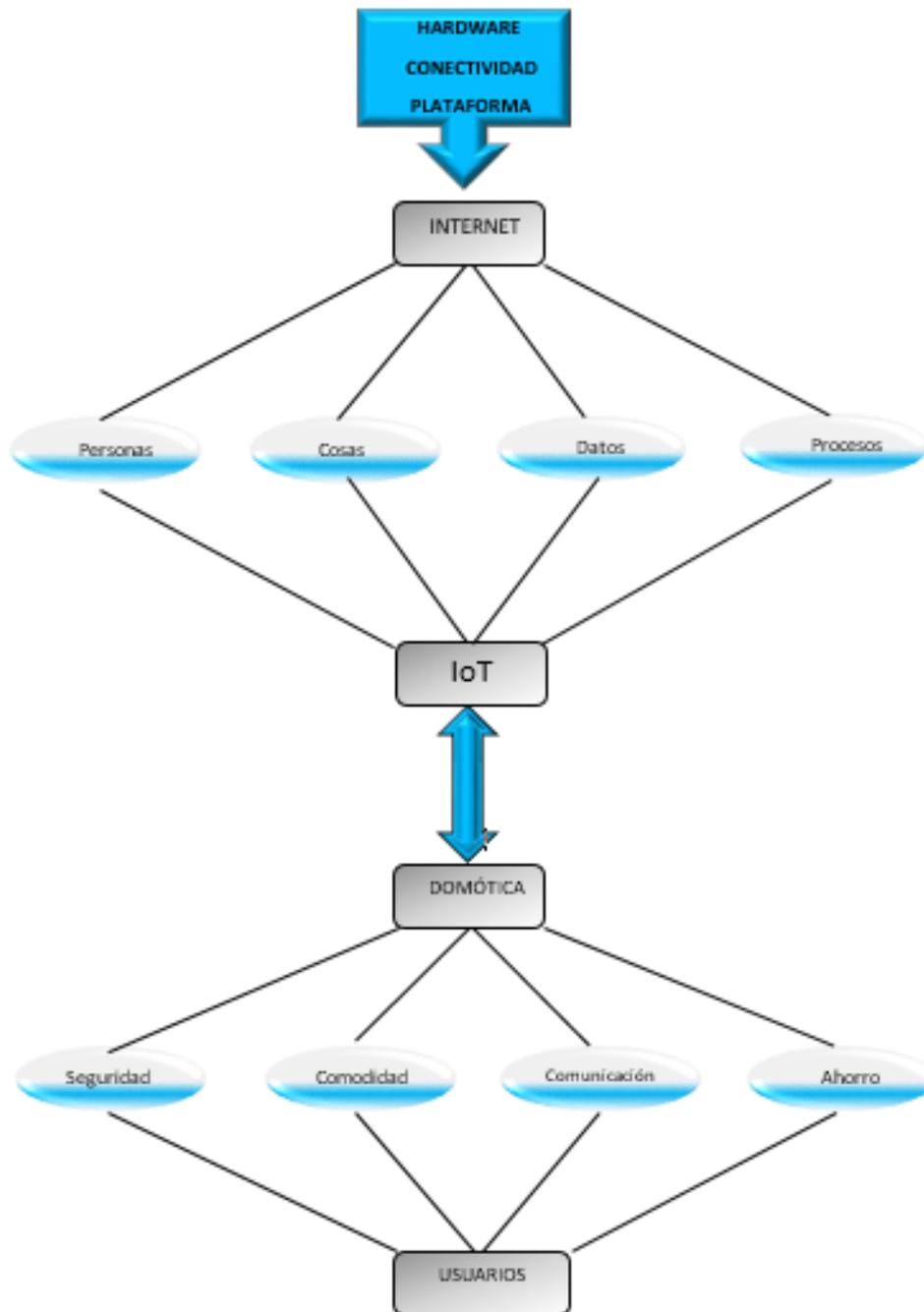


Figura 2. Como se construye un proyecto de domótica orientado al IoT

b. Explicación del aporte

Las tecnologías están evolucionando constantemente y el Internet de las Cosas es una de ellas, que va a permitir mejorar las condiciones de los usuarios desde sus hogares hasta el desarrollo de las ciudades; con el uso de la inteligencia en los dispositivos y utilización de aplicaciones, por tal razón se enumeran los siguientes aportes:

- El término IoT poco a poco seguirá dándose a conocer entre los estudiantes de carreras a fines y profesionales que estén enrolados con la automatización y quieran

tener el control remoto de los objetos inteligentes que integren las redes domóticas, en tal virtud el presente tema de investigación tratará de aportar con información relevante sobre el Internet de las cosas, sus beneficios y aplicaciones.

- Con la ayuda de la aplicación libre de *Packet Tracer* de Cisco, se pretende demostrar de forma gráfica la aplicación del IoT en el hogar y lo que será el futuro cercano de la automatización de las cosas.
- Elaborar un escenario completo con todas las redes que se necesitan para lograr obtener como resultado final el control remoto de las cosas dentro del hogar mediante la configuración de los equipos de red y sus componentes.
- Mediante la simulación en el software libre *Packet Tracer* se demostrará la conexión entre los equipos de la capa 3 como son los enrutadores y los dispositivos IoT con dos teléfonos inteligentes que comandarán remotamente a los objetos inteligentes de la red domótica
- Determinar los indicadores de conectividad de la red.

c. Estrategias y/o técnicas

Entre las principales estrategias que se va a emplear en la elaboración del diseño y simulación de una red domótica para aplicación del Internet de las cosas se tiene los siguientes puntos:

- Disponer de información relevante del Internet de las Cosas, de fuentes a nivel de posgrado, investigaciones, publicaciones en revistas reconocidas e información confiables que permita dar un rumbo adecuado y efectivo para el desarrollo del tema de investigación.
- Contar con la herramienta tecnológica de *Packet Tracer* de Cisco versión 7.3 que se utiliza como plataforma de aprendizaje en construcción y diseño de redes de comunicación en la carrera de Posgrado de la Universidad Israel, que ha permitido llevar a cabo la simulación de una red domótica aplicado al IoT y con ello, lograr entender de mejor manera que es una *smart house* y sus beneficios.
- Conocimiento de configuración y programación de equipos de red como los *router* y las “cosas” para lograr la comunicación de los elementos que integran las diferentes redes, y demostrar mediante la simulación que cualquier dispositivo inteligente puede comandar a las cosas que tienen aplicación de acceder al IoT.

- Distribución adecuada de las direcciones IPv4 en la simulación de las redes, para evitar que existan demasiadas direcciones IP que no se lleguen a utilizar.

➤ **Desarrollo de la propuesta**

Para el desarrollo de la propuesta fue necesario estructurarla con cuatro de los cinco objetivos específicos que son presentados en la tabla 2, con las descripciones de cada fase se toma como referencia los objetivos específicos planteados en el presente trabajo de investigación. El quinto objetivo específico no es considerado ya que hace referencia a la evaluación del desempeño de los componentes principales utilizados en la red doméstica y que será debidamente abordado más adelante.

Tabla 2

Fases a desarrollar de acuerdo a los objetivos específicos planteados

Fases	Descripción
Fase 1	Consiste en definir los fundamentos teóricos de la domótica que puedan ser utilizados con la aplicación del Internet de las Cosas.
Fase 2	Determinar los equipos de red y los dispositivos compatibles con el IoT que sean adecuados para la simulación de la red doméstica.
Fase 3	Diseñar varias redes WAN y LAN que incluyan las redes de Internet, doméstica, del proveedor de servicios, DSL, de la empresa de telefonía móvil y la red de la empresa IoT, que permitan visualizar el funcionamiento de las objetos inteligentes.
Fase 4	Desarrollar el diseño de la red de redes que sea aplicado al Internet de las Cosas.

Nota. El objetivo específico 5 no forma parte de las fases a desarrollar

- **Fase uno (fundamentos teóricos del IoT y la domótica)**

Una vez realizada la investigación de los documentos que tienen relación con el área de estudio se ha tomado como base el trabajo elaborado por Durán (2019), sobre “Sistema de gestión de red para Internet de las Cosas”, como trabajo de titulación de maestría en la Universidad Javeriana de Bogotá, donde se acoge los fundamentos de las variables de gestión de redes, redes IoT, dispositivos IoT, lenguajes de programación, apoyado en 28 fuentes de investigación que obtuvo como resultado la identificación y el análisis de las principales iniciativas de los sistemas de gestión para las redes del Internet de las cosas.

Y el trabajo de Rodríguez (2020), sobre “Control doméstico auto-configurable basado en Inteligencia Artificial”, como trabajo de titulación de maestría en la Universidad Nacional de

Colombia, donde se toma los fundamentos de las variables como *home automation*, automatización de casas, *smart home*, apoyado en 65 fuentes de investigación de donde obtuvo como resultado reducir la brecha entre enfoques tradicionales de predicción y reconocimiento de acciones que se utiliza en una casa inteligente.

- **Fase dos (determinación de equipos y dispositivos compatibles para IoT)**

Para la simulación con el software libre *Packet Tracer* se va a utilizar los siguientes equipos de red y los dispositivos compatibles con el Internet de las Cosas que permitan realizar la conectividad de las diferentes redes, con las redes domóticas en donde se incluye una *smart house*. Es importante aclarar que PT es un simulador que mediante una aplicación trata de reproducir el comportamiento de un programa (software IOS de Cisco) que genera una limitación en su comportamiento y no trabaja como un emulador como así lo es por ejemplo GNS3 que simula la parte física de una plataforma que emulan imágenes IOS que se pueden encontrar en Cisco, por tal razón su comportamiento se asemejará mucho a un equipo real.

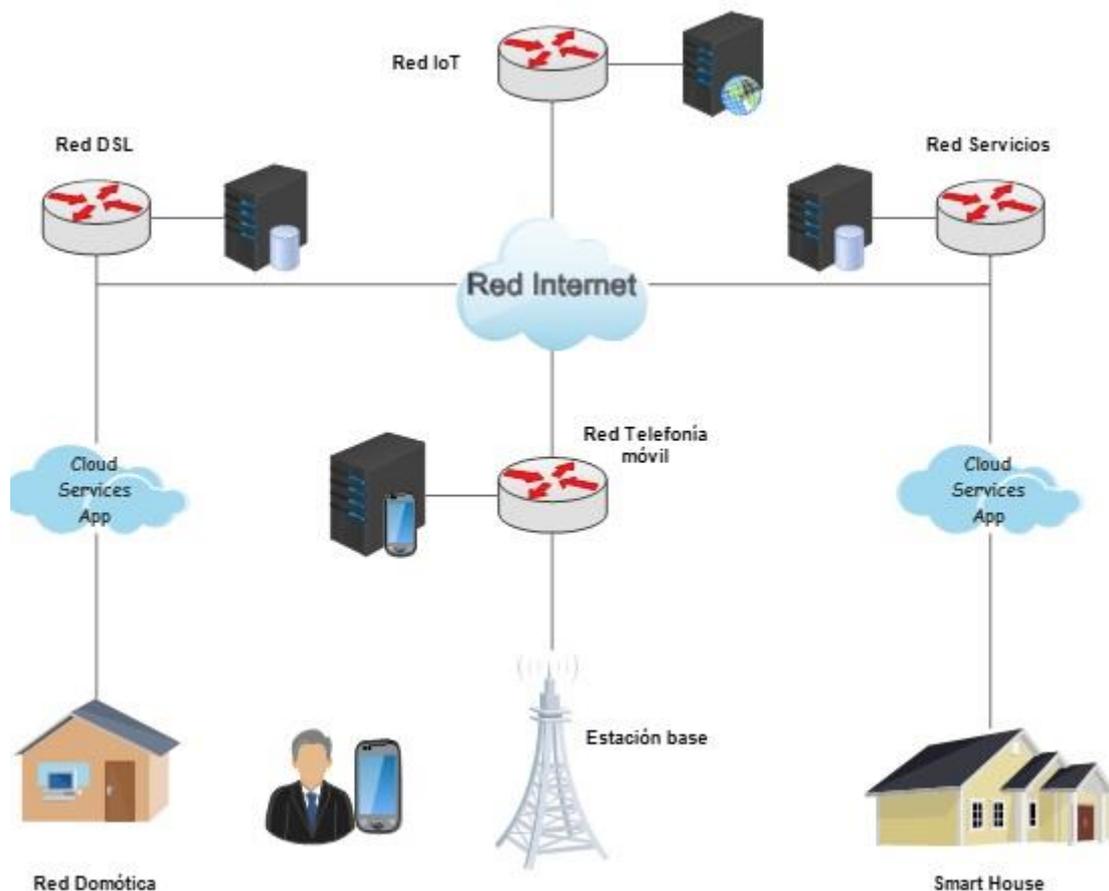


Figura 3. Diagrama general de las redes

El diagrama de la figura 3 integra las diferentes redes que van a formar parte de un conjunto de conexiones que permiten lograr la comunicación remota entre el usuario con los objetos inteligentes instalados en las redes domótica y *smart house*.

Los dispositivos que van a integrar el diagrama general de las redes se muestra en la tabla 3 que consta con la descripción del dispositivo y el modelo de acuerdo a la información obtenida de la herramienta *Packet Tracer*, mientras que las imágenes referenciales han sido tomadas desde el buscador de Internet, para tener una visión más real de los componentes que se necesitan para la ejecución del presente tema de desarrollo.

Tabla 3

Dispositivos de red y dispositivos compatibles con IoT

Dispositivo	Modelo	Imagen
Router	2811	
Router	ISR4321	
Power		
Cloud	Cloud-PT	
Servidor	PT-DHCP	
Switch	2960-24TT	

Access Point	Point-PT Tipo AC 24 puertos	
Smartphone	Smart device	
Arduino	MCU board	
Arduino	SBC board	
Modem	Modem-PT	
Laptop	Laptop-PT	
Dispositivos IoT		

Nota. Dispositivos del *Packet Tracer* e imágenes obtenidas de internet

- **Fase tres (diseño de las redes WAN y LAN aplicadas para IoT)**

Para el diseño de redes WAN y LAN que se va a utilizar en la simulación de la red doméstica aplicado al Internet de las cosas se plantea la construcción y simulación de las redes de Internet, doméstica, del proveedor de servicios, DSL, de la empresa de telefonía móvil y la red de la empresa IoT, que permitan visualizar el funcionamiento de las “cosas”

En la distribución de las direcciones únicas IP se han tomado de las redes de clases A que tiene una cobertura extremadamente grande, que consta de 126 direcciones de redes con

16.387.064 posibles direcciones de asignación para dispositivos (computadoras y servidores). Las redes de clase B con cobertura mediana a grande, que se compone de 16.384 redes individuales para asignación de 65.516 posibles direcciones y finalmente redes de clase C con cobertura local o de mediana a pequeñas empresas para un total de 2.097.152 redes compuestas máximo 255 posibles direcciones individuales o computadoras en red. (Han, 2020)

Por lo tanto, la red de redes que corresponde al Internet como la red más grande que existe se le asigna el direccionamiento IPv4 es de clase A, que puede utilizar su máscara de subred por defecto 255.0.0.0, pero para optimizar recursos de red se le va a asignar la máscara /30, como se muestra en la tabla 4.

Tabla 4

Direccionamiento IPv4 de la red de Internet

Equipo	Red	Dirección IP	Interface	Reloj
R0-A	10.10.100.0	10.10.100.1	F1/0	No
R0-A	10.10.100.4	10.10.100.5	S0/3/0	No
R0-A	10.10.100.8	10.10.100.9	S0/3/1	Si
R1-B	10.10.100.28	10.10.100.29	F1/0	No
R1-B	10.10.100.4	10.10.100.6	S0/3/0	Si
R1-B	10.10.100.12	10.10.100.13	S0/3/1	Si
R1-B	10.10.100.16	10.10.100.17	S0/1/0	No
R2-C	10.10.100.32	10.10.100.33	S0/2/0	Si
R2-C	10.10.100.16	10.10.100.18	S0/1/1	Si
R2-C	10.10.100.20	10.10.100.21	S0/1/0	Si
R3-D	10.10.100.24	10.10.100.25	S0/2/1	Si
R3-D	10.10.100.8	10.10.100.10	S0/1/1	No
R3-D	10.10.100.12	10.10.100.14	S0/2/0	No
R3-D	10.10.100.20	10.10.100.22	S0/1/0	No

Nota. Direccionamiento de IPv4 de clase A con máscara de subred /30

Para la red que representa a la empresa de servicios IoT se han utilizado direccionamiento IPv4 de clases B con máscara de subred predeterminado 255.255.0.0 que corresponde al prefijo /16 con el primer octeto de la dirección IPv4 empieza con 172 y de direccionamiento de clase A

con máscara de subred 255.255.255.252 que corresponde al prefijo /30 para hasta 4 *host*, con el objetivo de optimizar el número de *host*, como se muestra en la tabla 5.

Tabla 5

Direccionamiento IPv4 de la red de la empresa IoT

Equipo	Red	Dirección IP	Interface	Subred
R4IoT	172.10.0.0	172.10.0.1	F0/0	/16
R4IoT	10.10.100.24	10.10.100.26	S0/3/0	/30

Nota. Direccionamiento de IPv4 de clase A y B

Para la red de servicio móvil se planteó usar direccionamiento IPv4 de clases B con máscara de subred 255.255.0.0 y de direccionamiento de clase C que tiene una máscara de red predeterminada de 255.255.255.0 pero para el presente proyecto se va a asignar la máscara de subred 255.255.255.252 que corresponde al prefijo /30, como se muestra en la tabla 6.

Tabla 3

Direccionamiento IPV4 de la red de telefonía móvil e Internet

Equipo	Red	Dirección IP	Interface	Subred
R5Mov	172.20.0.0	172.20.0.1	F0/0	/16
R5Mov	10.10.100.32	10.10.100.34	S0/3/0	/30

Nota. Direccionamiento de IPv4 de clase C

Para las redes del proveedor de servicios y DSL se utilizaron direccionamiento IPv4 de clase C, con primer octeto de 192 y máscara de subred predeterminada 255.255.255.0 que corresponde al prefijo /24, como se muestran en las tablas 6 y 7 respectivamente.

Tabla 6

Direccionamiento IPV4 de la red de proveedor de servicio de cable

Equipo	Red	Dirección IP	Interface	Subred
R6Cab	192.168.50.0	192.168.50.1	F0/0	/24
R6Cab	Ip helper	172.50.0.2	F0/0	
R6Cab	172.50.0.0	172.50.0.1	F0/1	/24
R6Cab	10.10.100.0	10.10.100.2	F1/0	/30

Nota. Direccionamiento de IPv4 de clase A, B y C

Tabla 7

Direccionamiento IPv4 de la red de DSL

Equipo	Red	Dirección IP	Interface	Subred
R7DSL	192.168.60.0	192.168.60.1	F0/0	/24
R7DSL	Ip helper	172.60.0.2	F0/0	
R7DSL	172.60.0.0	172.60.0.1	F0/1	/30
R7DSL	10.10.100.28	10.10.100.30	F1/0	/30

Nota. Direccionamiento de IPv4 de clase A, B y C

Se sabe que las direcciones IPv4 tiene un número de 32 bits y que sirve para identificar de forma única a un *host* que puede ser físicamente un equipo o dispositivo dentro de una red TCP/IP es necesario identificar a que *host* se va a direccionar y es por esa razón que una dirección IP tiene dos partes, donde los tres primeros octetos se usan para el direccionamiento de la red, mientras que el cuarto octeto es la ubicación del *host*.

La máscara de subred como el segundo elemento además de la dirección IP del protocolo TCP/IP, sirve para determinar si un *host* está en la subred local o pertenece a una red remota. La red TCP/IP puede ser dividido por el administrador de red en subredes de clases A, B o C, todo dependerá, finalmente el tercer elemento es la puerta de enlace que permite comunicarse con un *host* en otra red, es así que el *router* es el dispositivo que sirve de medio de comunicación, en otras palabras, el *router* o enrutador vincula la subred del *host* con otras redes y este es el responsable de reenviar paquetes a la subred correcta.

- **Fase cuatro (desarrollo del diseño de la red IoT aplicado a la domótica)**

- **Red del Proveedor de Internet**

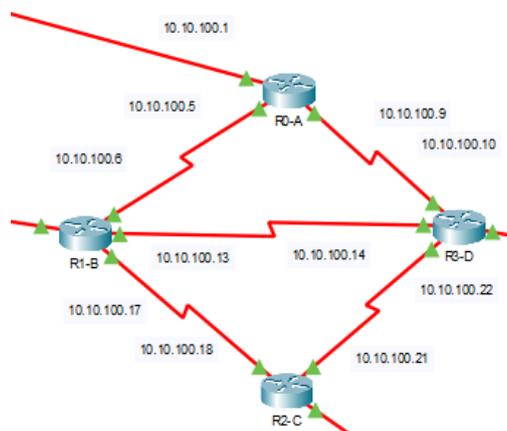


Figura 4. Diagrama de la Red de redes

En la red del Proveedor de Internet, contiene direcciones de IPv4 de clase "C", formado por cuatro *router* Cisco 2811 con la nomenclatura de R0, R1, R2 y R3, configurados en modo de enrutamiento.

No se utiliza el protocolo de enrutamiento de puerta de enlace interior mejorado EIGRP (*Enhanced Interior Gateway Routing Protocol*), que es un protocolo exclusivo de Cisco que permite enrutamiento del tipo vector distancia avanzado y esto es una condicionante a que los equipos sean de la misma marca. Razón por la cual se puede utilizar protocolos del tipo abiertos como OSPF (*Open Shortest Path First*) que es un protocolo de enrutamiento dinámico que usa algoritmos de tipo estado de enlace, que por supuesto es usado para redes IP y su base es en los algoritmos de primera vía más corta, en otras palabras, es un protocolo de pasarela interior, que se usa para distribuir la información de ruteo y permite integrar tecnologías de redes y equipos de diferentes marcas. (Suárez, 2020).

El *router* 0-A, utiliza como medio de transporte de datos el cable serial DTE para prácticas de la simulación y se enlaza con la *interface fastEthernet1/0* hacia el *router* 6 de la red del proveedor de servicio. En los *router* se van a levantar *interfaces fastEthernet* y algunos puertos seriales, para posterior proceder con la asignar del direccionamiento IPv4 de acuerdo a las tablas de enrutamiento con su respectiva máscara de subred.

- **Red de la Empresa de Servicio IoT**

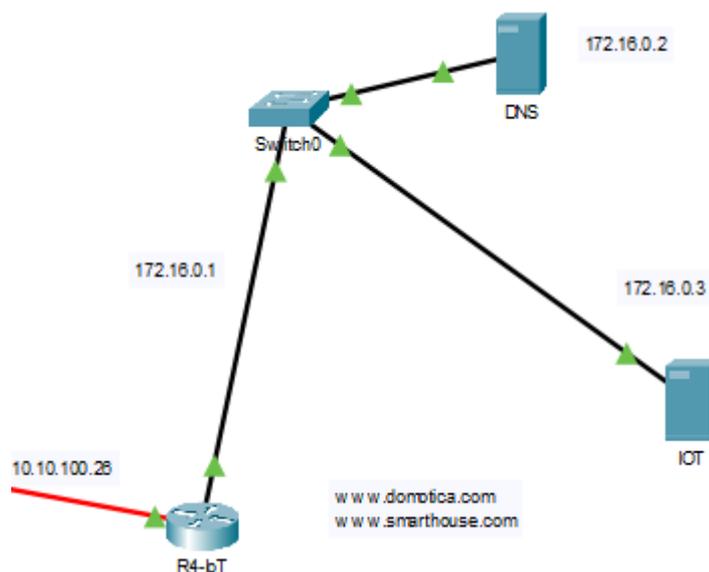


Figura 5. Diagrama de la Red de la empresa de servicio IoT

La figura 5 muestra el diagrama de la red de la empresa IoT donde se va a implementar el servidor remoto para acceder a los objetos IoT, donde el *router* 4 desde el puerto serial0/3/0 se conecta mediante cable serial al interfaz serial0/2/1 del *router* R3-D ISR4321 de la red de Internet.

- **Red de Servicio Móvil**

Para culminar con la configuración de los equipos *router*, el R5 pertenece a la red de Telefonía Móvil que brinda a las empresas y usuarios soluciones tecnológicas integrales de tecnologías de la información y comunicación móvil que sería lo que aplica a la presente simulación dotando del servicio al dispositivo móvil *smartphone* para permitir al usuario contratar datos móviles para navegar y usar el Internet y así además acceder al control remoto de los objetos inteligentes de las redes doméstica y *smart house* como se observa en la figura 6.

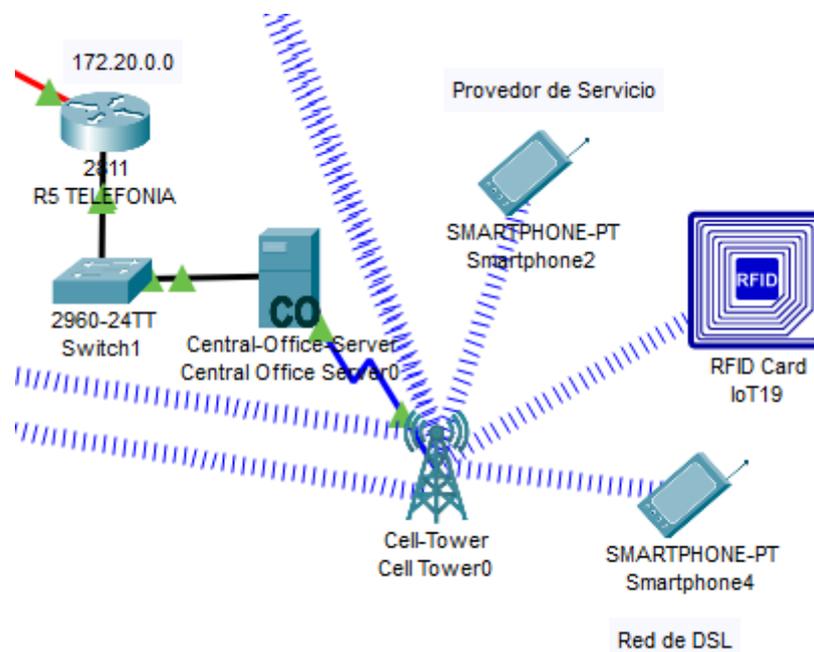


Figura 6. Diagrama de la Red de servicio móvil

- **Red del Proveedor de Servicios por cable**

El diseño de la red del Proveedor de Servicios simula la conexión con los ISP (Proveedor de servicios fijos y móviles), considerándose una red externa, que permitirá el acceso al servicio de Internet fijo en el hogar, además de facilitar la conectividad a los objetos inteligentes de la red doméstica de forma remota a cambio de un pago o contratación de servicios con el ISP. La red del proveedor de servicio de cable se conecta con la red de redes o Internet.

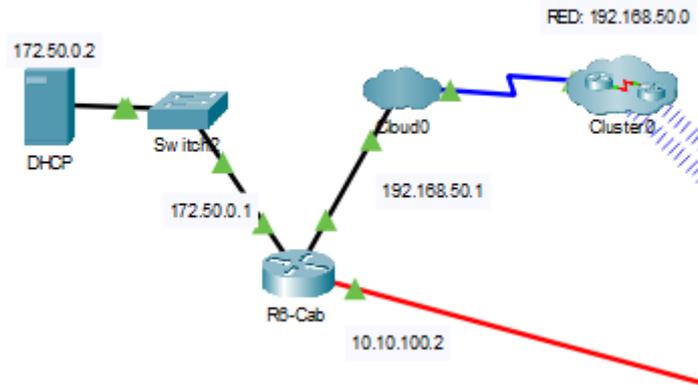


Figura 7. Diagrama de la red del proveedor de servicios de cable

En la red WAN del proveedor de servicios de cable, se debe realizar la configuración de la nube de dicho proveedor (*Cloud-PT*), habilitar el acceso al servidor DHCP, que es un protocolo de configuración dinámica de *host* y configurar su protocolo para permitir el envío y recepción de paquetes. Todo esto en el *router 6*.

Los *router* pueden enviar los paquetes de difusión solo a la red local a la que pertenecen, por tal razón para la redistribución DHCP hacia una red remota se debe utilizar el comando de redistribución "*ip helper-address*", con esto se logra publicar las direcciones IPv4 hacia una red remota. Se debe configurar la *interface fastEthernet 0/0* para que tenga acceso al *Cloud-PT* y con esto enlazar a la red remota del *Cluster 0*. Los *Cluster* en general vienen hacer la unión de varios sistemas informáticos (servidores) que comparten recursos de hardware y software

- **Red de DSL**

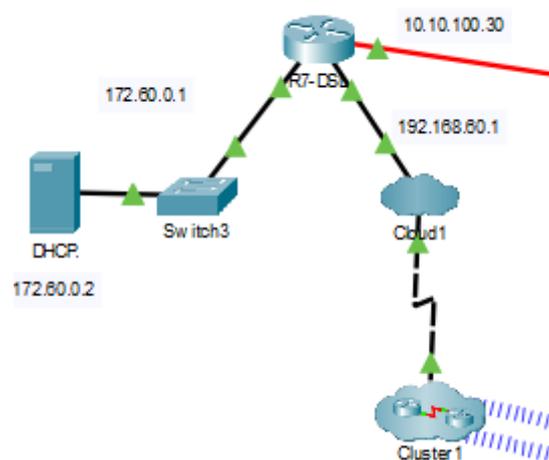


Figura 8. Diagrama de la Red de DSL

smartphone que se encuentran fuera de dichas redes, es efectiva y se tiene el acceso remoto para comandar las instrucciones de los objetos aplicados al Internet de las Cosas.

Para la conexión de los objetos IoT dentro de la red LAN que comprende la red doméstica es necesario vincularlos con el equipo *access point* (AP) mediante la tecnología inalámbrica WiFi considerado de medio alcance que tiene un rango de cobertura de 0 a 1000m, con una tasa de transmisión de 8 a 450 Mbps, en la banda de frecuencias de 900MHz, 2.4Ghz y 5GHz con estándares IEEE 802.11, 802.11b (WiFi 1), 802.11a (WiFi 2), 802.11g (WiFi 3), 802.11n, 802.11ac (WiFi 5), 802.11ax (WiFi 6) que es el último estándar con un alcance de 10Gbps de velocidad. Para la simulación presente se ha considerado el estándar 802.11b que es el más utilizado actualmente y tiene un alcance de hasta 300m con un rango de frecuencia de 2.4Ghz con tres canales de radio.

Se debe considerar adquirir un dominio del servidor WEB de IoT y contar con una IP pública que es otorgado por el proveedor a cambio de un costo, para que se tenga acceso desde cualquier punto fuera de la red doméstica. Una vez que se configure el WiFi hacerlo también con el protocolo inalámbrico de seguridad WPA2-PSK que permite cifrar los datos y evitar el acceso no autorizado.

Para que puedan tener acceso hacia el Internet, además, para el direccionamiento de la red IoT se ha considerado asignar direcciones IP de clase A; no se estableció un número exacto de puntos (dispositivos) disponibles para conectarse a la red de área local virtual o VLAN. Es importante considerar los estándares 802.11n (2009) y 802.11ac (2014) utilizados para las redes inalámbricas WAN y redes inalámbricas de área local WLAN que operan en las bandas de frecuencias de 2.4Ghz y 5Ghz y estas permiten velocidades máximas teóricas que están entre 600Mbps y 1.3 Gbps, respectivamente. En la actualidad existe el estándar 802.11x (2019).

En el Anexo B, se detalla paso a paso la configuración de los objetos inteligentes que son vinculados al *access point* (AP), con la incorporación de una *interfaz* inalámbrica en cada objeto y su respectiva configuración de acceso; así se ha logrado una efectiva comunicación. La figura 10 muestra la comunicación dentro de la red doméstica.

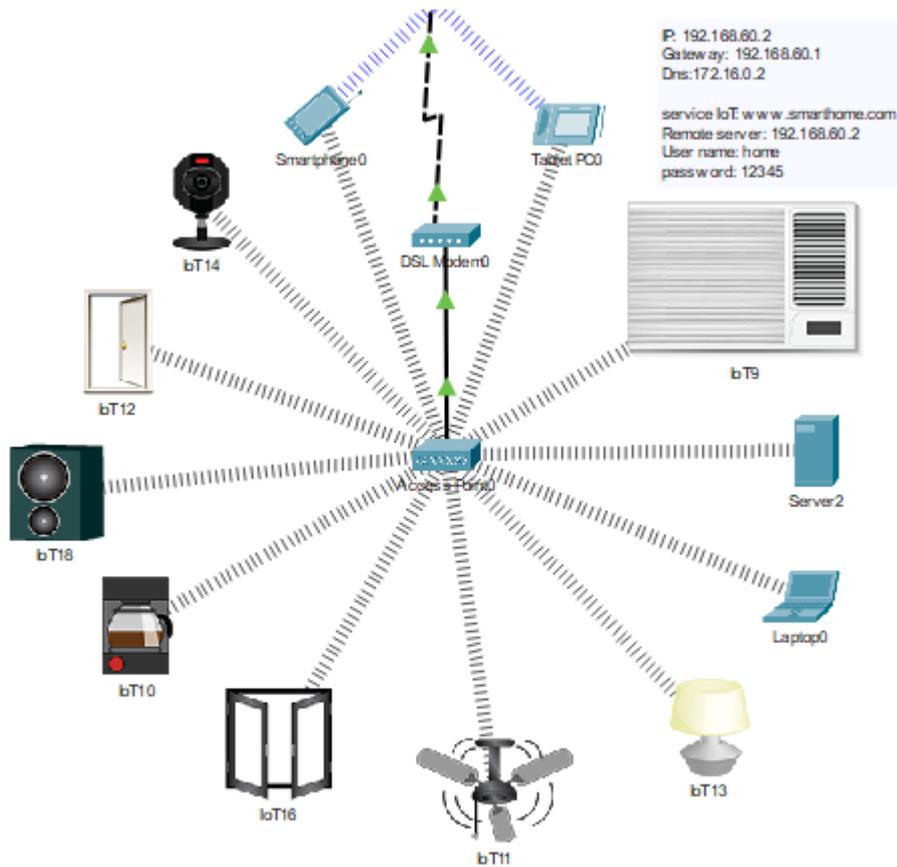


Figura 10. Diagrama de la Red inalámbrica donde se conectan los objetos IoT al WiFi

A continuación, en la figura 11 se puede observar la integración de todos los objetos inteligentes que se pueden comandar desde otro dispositivo inteligente como es una laptop que pertenece a la red local. Dichos objetos actuarán de acuerdo a las instrucciones que reciban desde el ordenador comandado por el usuario.



Figura 11. Conexión de objetos inteligentes dentro de la misma red

Desde un dispositivo inteligente como por ejemplo un *smartphone* que este fuera de la red LAN (red domótica) e incluso que pertenezca a una red WAN, gracias al servicio que se contrate, de ser en el caso real, se puede tener la opción de comandar las acciones de los dispositivos inteligentes remotamente, basta con tener acceso al Internet, ahorrándose así recursos y tiempo. En la figura 12 se observan los objetos inteligentes que pertenecen a la red domótica y pueden ser comandado desde un *smartphone* de otra red diferente, en otras palabras, se puede tener acceso remoto desde cualquier parte del mundo, gracias al Internet de las Cosas.

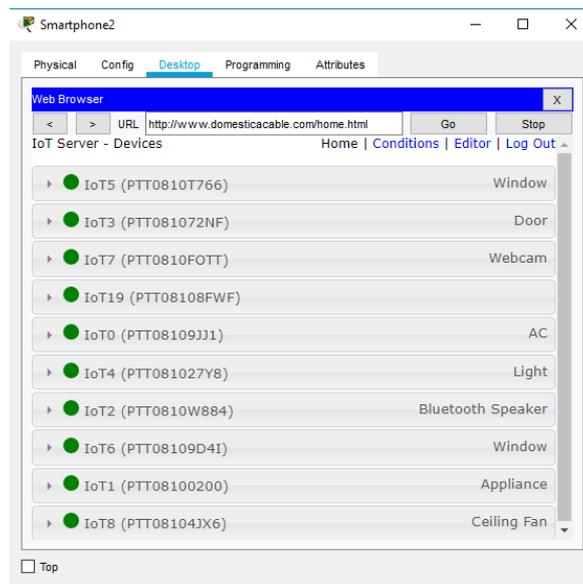


Figura 12. Comando remoto de los dispositivos IoT

La domótica viene hacer una rama clave para el Internet de las Cosas comprendiendo en primer lugar a la domótica como la infraestructura tecnológica que es parte de la estructura de una casa que permite dar una solución que implique el cableado físico para la integración de dispositivos que por lo general son comandados de una sola aplicación. Por lo tanto, se podría asemejarse a una casa inteligente.

Mientras que una *smart home* permite conectar a través del Internet los objetos, dispositivos y sistemas para generar nuevas funciones que permitan la automatización y administración de forma remota, para así lograr la simplificación de las actividades del hogar y mejorar los beneficios de las personas sustancialmente. Dicha gestión lo puede realizar un teléfono inteligente con la ayuda del asistente de voz, aplicativos, etc. Que permitirán visualizar consumos, programar horarios y generar acciones. Por tal razón, se podría decir que una *smart home* que utiliza la tecnología del Internet de las Cosas es más barata y sencilla su gestión que la domótica. En la figura 13 se observa el diagrama de cómo sería una red *smart home*.

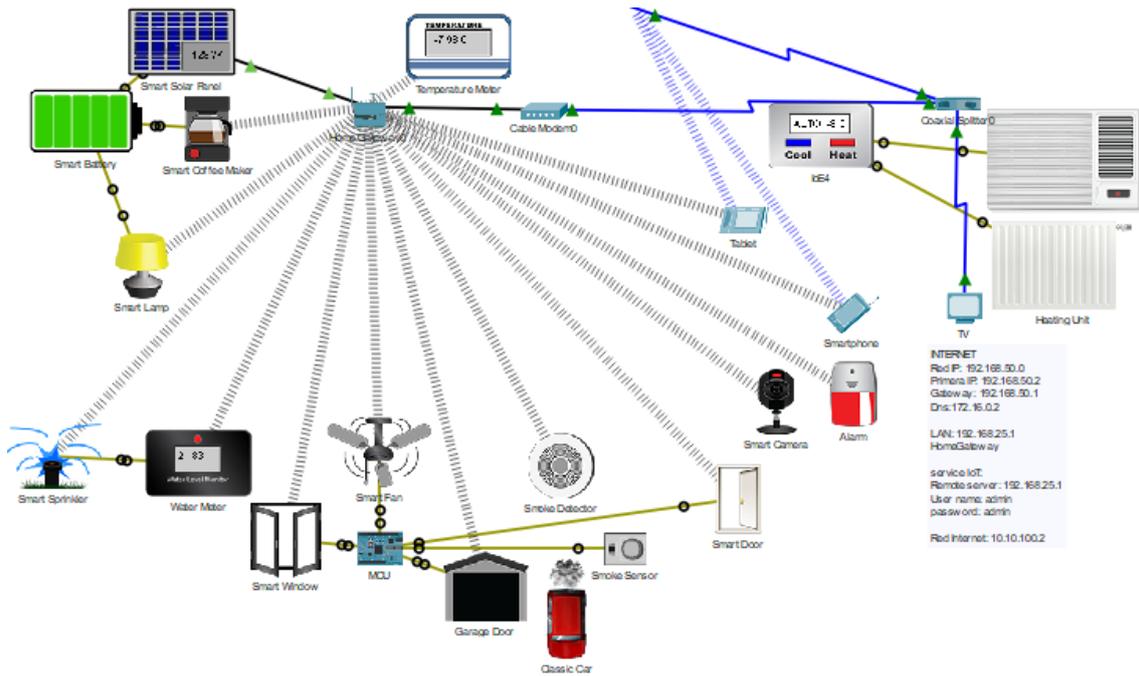


Figura 13. Diagrama de la Red Smart Home

➤ **Resultados obtenidos de la investigación**

De acuerdo a la fundamentación teórica investigada en los últimos cinco años se tomó los fundamentos más relevantes que tienen relación con el tema de investigación de acuerdo a las variables de interés como son el Internet de las Cosas, la domótica, redes de computadoras, software de simulación de Cisco entre otros. Se logró contextualizar de forma óptima en el tema de investigación propuesto, entre los que destacan los autores referidos Rodríguez (2020), Durán (2019), Terrazas (2019), Brea (2018) y López (2017).

2.3. Matriz de articulación

Tabla 8

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	CLASIFICACIÓN TIC
Internet de las cosas IoT	Se trabajó con fundamentos de Durán (2019) y Rodríguez (2020), ya que la unión de sus teorías llevan a la comunicación de redes con los dispositivos inteligentes forman la domótica aplicado al IoT	Con investigaciones bibliográfica más actuales de temas relacionados	Mostrar una fuente teórica y práctica del proceso de comunicación de dispositivos IoT. El IoT permite mejorar el día a día a las personas con el uso de la tecnología	Estado del arte y análisis del Internet de las cosas	Comunicación de redes
Simular con Packet Tracer	Se utilizó los fundamentos de López (2017) que utilizo un software libre para demostrar como se aplica IoT en beneficio de la gente, además del fundamento del uso y configuraciones en PT (Cando, 2020)	Con el uso del software <i>Packet Tracer</i> es factible realizar construcción de redes con la programación de equipos y dispositivos para lograr la conectividad	Dar al lector las configuraciones y programaciones de equipos de red y dispositivos aplicados al IoT	Conectividad de los equipos y dispositivos de la red	Configuración y programación de redes

CONCLUSIONES

Vale indicar que las conclusiones se harán con base en los resultados e insumos obtenidos en el trabajo investigativo de tema “Desarrollo de una red domótica aplicando el Internet de las Cosas con una herramienta tecnológica de simulación y verificación de conectividad” donde se utilizó la aplicación de Cisco *Packet Tracer* como herramienta para la construcción y diseño de varias redes de área extensa y local con la finalidad de simular una red global donde incluyen a la red de redes o internet, el proveedor de servicios, la red IoT, la red telefónica y las redes donde se establece la domótica y esta a su vez se van a diferenciar en dos redes una con acceso remoto hacia el control de los objetos inteligentes y otra red donde se tiene una *smart house*; para lo cual se establece las siguientes conclusiones derivados de los objetivos específicos planteados.

- De acuerdo a la fundamentación teórica investigada en los últimos cinco años, con las variables relevantes IoT, domótica, *Packet Tracer* (PT), se llegó a la conclusión que con fines pedagógicos y demostrativos es viable el uso del software libre PT para la simulación de una red que utilice la plataforma de Internet de las Cosas y esta a su vez a mediano y largo plazo con llevaría a su aplicación para brindar beneficios a la sociedad sea de forma directa o indirectamente para quienes lo utilice.
- La determinación de los dispositivos y equipos que se utilizaron en la simulación de la red domótica no es compleja elegir cuando se tienen ciertos conocimientos en redes, además que la aplicación para la simulación *Packet Tracer* a partir de la versión 7.0 está diseñada para dicho uso y cuenta con una librería importante, a diferencia de una implementación real en donde económicamente sería muy costoso por los equipos específicos de red y en el país aún no se cuenta con un catálogo amplio de objetos físicos con inteligencia para uso en la plataforma de IoT.
- Se diseñaron siete redes con direcciones IPv4 de subredes de clases A, B y C para diferenciar el tipo de red y su cobertura para dar una mejor idea al lector de la magnitud a nivel global que tiene el alcance de la plataforma IoT y además se concluye que el software *Packet Tracer* permitió cumplir a satisfacción la construcción de redes y disponer de los objetos necesarios para completar las redes domóticas.
- Con el software libre de Cisco *Packet Tracer* se logró la simulación de las redes diseñadas y se obtuvo una conectividad efectiva entre los dispositivos de capa tres

y se logró la comunicación de objetos inteligentes desde dos smartphone, los mismos que pueden comandar acciones remotamente.

- Para lograr la validación del desempeño de los componentes principales utilizados en la red domótica se utilizó comandos de verificación de envío y recepción de paquetes, el cual permitió comprobar la comunicación efectiva de los elementos simulados.

RECOMENDACIONES

- La plataforma del Internet de las cosas a futuro se estima que sea tan importante en la vida de las personas como lo es actualmente el Internet, pero es fundamental considerar las vulnerabilidades y riesgos de accesos no autorizados a las redes que utilicen el IoT, para garantizar al usuario que la información y sus datos están protegidos, por tal razón es necesario continuar con investigaciones que determinen las recomendación adecuadas y efectivas.
- Si bien es cierto que, no es tan sencillo disponer de laboratorios donde se pueda simular o hacer ejercicios prácticos con componentes reales que dispongan de interfaz y conectividad hacia el Internet, pero existe varias herramientas de simulación de pago y libres que pueden ser muy útiles para el aprendizaje y desarrollo del IoT.
- Se tiene claro que los proveedores de servicios son los encargados de manejar las grandes redes, plataformas, aplicaciones y son quienes brindan el servicio a cambio de un costo económico, pero eso no implica que por motivos investigativos o pedagógicos se pueda experimentar con topologías y diseños de redes que tengas aplicativos al IoT con el uso de aplicaciones de simulación de redes de computación.
- Actualmente existen software de pago y libres que tienen herramientas muy potentes para la construcción y simulación de redes y varias de ellas están enfocadas con el Internet de las Cosas que pueden ser útiles para tener una mayor comprensión de los alcances y beneficios que traerá el IoT, razón por la cual se recomienda explorar otras aplicaciones de simulación.
- Existen otras variables de comprobación para la validación del desempeño de redes que pueden experimentarse, donde se puedan utilizar otros software o herramientas para obtener otros parámetros de medidas y así garantizar una mayor eficiencia de la red y sus dispositivos antes que se implemente físicamente.

BIBLIOGRAFÍA

- Brea, V. (julio de 2018). *Internet de las Cosas. Horizonte 2050*. Obtenido de Instituto Español de Estudios Estratégicos (IEEE): http://www.ieee.es/Galerias/fichero/docs_investig/2018/DIEEEINV17-2018_Internet_de_las_Cosas_Horizonte_2050.pdf
- Calle, M., Tovar, J., Castaño, Y., & Cuellar, J. (diciembre de 2018). *Comparación de parámetros para una selección apropiada de herramientas de simulación de redes*. Obtenido de https://www.researchgate.net/publication/329460409_Comparacion_de_Parametros_para_una_Seleccion_Apropiada_de_Herramientas_de_Simulacion_de_Red
- Cando, D. (01 de junio de 2020). *IoT Fundamentals connecting things*. Obtenido de Universidad Tecnológica Israel: <https://www.netacad.com/courses/iot/introduction-iot>
- Cuzme, F. (abril de 2015). *El Internet de las cosas y las consideraciones de seguridad*. Obtenido de Repositorio Universidad Católica del Ecuador: <http://repositorio.puce.edu.ec/handle/22000/8492>
- Díaz, M. (2017). *Caracterización, implementación y evaluación de dispositivos domóticos para adultos mayores mediante sistemas embebidos e Internet de las Cosas*. Obtenido de Repositorio Maestría Universidad Distrital Francisco José de Caldas: <https://repository.udistrital.edu.co/bitstream/handle/11349/8025/D%C3%ADazHern%C3%A1ndezMar%C3%ADaFernanda2018.pdf?sequence=1&isAllowed=y>
- Durán Dajud, M. A. (mayo de 2019). *Sistema de gestión de red para Internet de las Cosas*. Obtenido de repositorio Pontificie Universidad Javeriana de Bogota: <https://repository.javeriana.edu.co/bitstream/handle/10554/45208/Documento.pdf?sequence=1&isAllowed=y>
- Evans, D. (Abril de 2011). *Internet de las cosas Cómo la próxima evolución de Internet lo cambia todo*. Obtenido de Cisco: https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf
- Figueroa, D. A. (mayo de 2017). *Estudio de la influencia de un entorno de simulación en la enseñanza de redes de computadoras en el nivel universitario*. Obtenido de Repositorio Institucional de la UNLP: http://sedici.unlp.edu.ar/bitstream/handle/10915/63704/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y
- Han, L. (21 de septiembre de 2020). *Comprender los conceptos básicos de direccionamiento TCP/IP y subredes*. Obtenido de Microsoft: <https://docs.microsoft.com/es-es/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting>
- Hernández Caballero, S., López Vicario, J., & Vilajosana Guillen, X. (enero de 2020). *Estudio en detalle de loRaWAN. Comparación con otras tecnologías LPWAN considerando diferentes patrones de tráfico*. Obtenido de Universitat Oberta de Catalunya: <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/106369/7/shernandezc6TFM0120memoria.pdf>
- Hwang, J., Aziz, A., Sung, N., Ahmad, A., Le Gall, F., & Song, J. (2020). AUTOCON-IoT: automatizado y escalable en línea Pruebas de conformidad para aplicaciones de IoT. *IEEE Access*.
- ITU. (15 de 06 de 2012). *International Telecommunication Union*. Obtenido de <https://www.itu.int/rec/T-REC-Y.2060-201206-I>
- López, M. (2 de diciembre de 2017). *Internet de las cosas en Packet Tracer*. Obtenido de Estudio Tecnovisual: https://www.youtube.com/watch?v=IKP_x4NOR18
- Madrid, M. (2016). *Términos técnicos de Telecomunicaciones*. Obtenido de http://bear.warrington.ufl.edu/centers/purc/DOCS/papers/sp_02.pdf
- Marelli, G. R. (Noviembre de 2015). *DEVS-Tossin: un frame DEVS para simular redes de sensores inalámbricas que utilizan el sistema operativo TinyOS*. Obtenido de Facultad de Ingeniería de Buenos Aires: <http://materias.fi.uba.ar/7500/Marelli.pdf>
- Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: ¿Internet de las amenazas? Una encuesta de vulnerabilidades de seguridad prácticas en dispositivos IoT reales. *IEEE*.
- MINTEL. (octubre de 2018). *Plan de Servicio Universal*. Obtenido de Telecomunicaciones.gob.ec: <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/11/Plan-de-Servicio-Universal.pdf>
- MINTEL. (2020). *Infraestructura y cobertura. Boletín estadístico trimestral mayo 2020*, 14.

- Rodríguez Segura, M. (15 de mayo de 2020). *Controlador domótico auto-configurable basado en inteligencia artificial*. Obtenido de Repositorio Universidad Nacional de Colombia: https://repositorio.unal.edu.co/handle/unal/77663?locale-attribute=pt_BR
- Suárez, M. (10 de agosto de 2020). *CCNA desde cero*. Obtenido de CCNA: <https://ccnadesdecero.com/cursos/ospf/>
- Swamy, N., & Raju, S. (2020). Un estudio empírico sobre aspectos a nivel del sistema de Internet de las cosas (IoT). *IEEE Access*.
- Tamayo, V. V. (septiembre de 2018). *Estudio de factibilidad de la tecnología Connected Home a través del Internet de las Cosas IoT dentro de la ciudad de Quito D.M.* Obtenido de Repositorio Dspace: <http://dspace.utpl.edu.ec/xmlui/bitstream/handle/20.500.11962/22223/Tamayo%20Vegas%2c%20Viviana%20Alejandra.pdf?sequence=1&isAllowed=y>
- Terrazas, P., Guarneros, R., Ponce, J., Esqueda, R., & Martínez, S. (2019). *Análisis exploratorio de la comercialización de servicio de conectividad para IoT*. Obtenido de Instituto Federal de Telecomunicaciones de México: <http://www.ift.org.mx/sites/default/files/contenidogeneral/estadisticas/analisisexploratorioiot.pdf>
- Velasco, P., Sánchez, L., Laureano, A., & Mora, M. (2009). Un diseño de interfaz: tomando en cuenta los estilos de aprendizaje. *XXII Congreso Nacional y VIII Congreso Internacional de Informática y Computación de la ANIE*. Baja California.
- WordPress. (Septiembre de 2016). *Sistemas de comunicación*. Obtenido de <https://sistemascomunic.wordpress.com/redes-de-telecomunicaciones/>

ANEXOS

ANEXOS A. Configuración de equipos para la interconexión de redes

- **Red de Internet**

Enrutador 0

```
Router>enable
Router#configure terminal
Router(config)#hostname R0-A
R0-A(config)#banner motd &
*****
RED DE INTERNET
EDDIE YANEZ
*****
&
R0-A(config)#enable secret iot
R0-A(config)#line console 0
R0-A(config-line)#password iot
R0-A(config-line)#login
R0-A(config-line)#exit
R0-A(config)#line vty 0 15
R0-A(config-line)#password iot
R0-A(config-line)#login
R0-A(config-line)#exit
R0-A(config)#service password-encryption
R0-A(config)#banner motd $RED INTERNET$
R0-A(config)#interface fastEthernet 1/0
R0-A(config-if)#ip address 10.10.100.1 255.255.255.252
R0-A(config-if)#no shutdown
R0-A(config-if)#exit
R0-A(config)#interface serial 0/3/0
R0-A(config-if)#ip address 10.10.100.5 255.255.255.252
R0-A(config-if)#bandwidth 128
R0-A(config-if)#no shutdown
R0-A(config-if)#exit
R0-A(config)#interface serial 0/3/1
R0-A(config-if)#ip address 10.10.100.9 255.255.255.252
R0-A(config-if)#clock rate 128000
R0-A(config-if)#bandwidth 128
R0-A(config-if)#no shutdown
R0-A(config-if)#exit
R0-A(config)#router rip
R0-A(config-router)#version 2
R0-A(config-router)#network 10.10.100.0
R0-A(config-router)#network 10.10.100.4
R0-A(config-router)#network 10.10.100.8
R0-A(config)#end
R0-A#wr
```

Enrutador 1

```
Router>enable
Router#configure terminal
Router#hostname R1-B
R1-B(config)#banner motd &
*****
RED DE INTERNET
EDDIE YANEZ
*****
&
R1-B(config)#enable secret iot
R1-B(config)#line console 0
R1-B(config-line)#password iot
R1-B(config-line)#login
R1-B(config-line)#exit
R1-B(config)#line vty 0 15
R1-B(config-line)#password iot
R1-B(config-line)#login
R1-B(config-line)#exit
R1-B(config)#service password-encryption
R1-B(config)#banner motd $RED INTERNET$
R1-B(config)#interface fastEthernet 1/0
R1-B(config-if)#ip address 10.10.100.29 255.255.255.252
R1-B(config-if)#no shutdown
R1-B(config-if)#exit
R1-B(config)#interface serial 0/3/0
R1-B(config-if)#ip address 10.10.100.6 255.255.255.252
R1-B(config-if)#clock rate 128000
R1-B(config-if)#bandwidth 128
R1-B(config-if)#no shutdown
R1-B(config-if)#exit
R1-B(config)#interface serial 0/3/1
R1-B(config-if)#ip address 10.10.100.13 255.255.255.252
R1-B(config-if)#bandwidth 128
R1-B(config-if)#no shutdown
R1-B(config-if)#exit
R1-B(config)#interface serial 0/1/0
R1-B(config-if)#ip address 10.10.100.17 255.255.255.252
R1-B(config-if)#bandwidth 128
R1-B(config-if)#no shutdown
R1-B(config-if)#exit
R1-B(config)#router rip
R1-B(config-router)#version 2
R1-B(config-router)#network 10.10.100.28
R1-B(config-router)#network 10.10.100.4
R1-B(config-router)#network 10.10.100.12
R1-B(config-router)#network 10.10.100.16
R1-B(config-router)#end
R1-B#wr
```

Enrutador 2

```
Router>enable
Router#configure terminal
Router(config)#hostname R2-C
R2-C(config)#banner motd &
*****
RED DE INTERNET
EDDIE YANEZ
*****
&
R2-C(config)#enable secret iot
R2-C(config)#line console 0
R2-C(config-line)#password iot
R2-C(config-line)#login
R2-C(config-line)#exit
R2-C(config)#line vty 0 15
R2-C(config-line)#password iot
R2-C(config-line)#login
R2-C(config-line)#exit
R2-C(config)#service password-encryption
R2-C(config)#banner motd $RED INTERNET$
R2-C(config)#interface serial 0/2/0
R2-C(config-if)#ip address 10.10.100.33 255.255.255.252
R2-C(config-if)#clock rate 128000
R2-C(config-if)#bandwidth 128
R2-C(config-if)#no shutdown
R2-C(config-if)#exit
R2-C(config)#interface serial 0/1/1
R2-C(config-if)#ip address 10.10.100.18 255.255.255.252
R2-C(config-if)#clock rate 128000
R2-C(config-if)#bandwidth 128
R2-C(config-if)#no shutdown
R2-C(config-if)#exit
R2-C(config)#interface serial 0/1/0
R2-C(config-if)#ip address 10.10.100.21 255.255.255.252
R2-C(config-if)#clock rate 128000
R2-C(config-if)#bandwidth 128
R2-C(config-if)#no shutdown
R2-C(config-if)#exit
R2-C(config)#router rip
R2-C(config-router)#version 2
R2-C(config-router)#network 10.10.100.32
R2-C(config-router)#network 10.10.100.16
R2-C(config-router)#network 10.10.100.20
R2-C(config-router)#end
R2-C#wr
```

Enrutador 3

```

Router>enable
Router#configure terminal
Router(config)#hostname R3-D
R3-D(config)#banner motd &
*****
RED DE INTERNET
EDDIE YANEZ
*****
&
R3-D(config)#enable secret iot
R3-D(config)#line console 0
R3-D(config-line)#password iot
R3-D(config-line)#login
R3-D(config-line)#exit
R3-D(config)#line vty 0 15
R3-D(config-line)#password iot
R3-D(config-line)#login
R3-D(config-line)#exit
R3-D(config)#service password-encryption
R3-D(config)#banner motd $RED INTERNET$
R3-D(config)#interface serial 0/2/1
R3-D(config-if)#ip address 10.10.100.25 255.255.255.252
R3-D(config-if)#clock rate 128000
R3-D(config-if)#bandwidth 128
R3-D(config-if)#no shutdown
R3-D(config-if)#exit
R3-D(config)#interface serial 0/1/1
R3-D(config-if)#ip address 10.10.100.10 255.255.255.252
R3-D(config-if)#bandwidth 128
R3-D(config-if)#no shutdown
R3-D(config-if)#exit
R3-D(config)#interface serial 0/2/0
R3-D(config-if)#ip address 10.10.100.14 255.255.255.252
R3-D(config-if)#bandwidth 128
R3-D(config-if)#no shutdown
R3-D(config-if)#exit
R3-D(config)#interface serial 0/1/0
R3-D(config-if)#ip address 10.10.100.22 255.255.255.252
R3-D(config-if)#bandwidth 128
R3-D(config-if)#no shutdown
R3-D(config-if)#exit
R3-D(config)#router rip
R3-D(config-router)#version 2
R3-D(config-router)#network 10.10.100.24
R3-D(config-router)#network 10.10.100.8
R3-D(config-router)#network 10.10.100.12
R3-D(config-router)#network 10.10.100.20
R3-D(config-router)#end
R3-D#wr

```

- **Red de la empresa de IoT**

Enrutador 4

```
Router>enable
Router#configure terminal
Router(config)#hostname R4-IoT
R4-IoT(config)#banner motd &
*****
RED DE EMPRESA IOT
EDDIE YANEZ
*****
&
R4-IoT(config)#service password-encryption
R4-IoT(config)#banner motd $RED INTERNET DE LAS COSAS$
R4-IoT(config)#interface serial 0/3/0
R4-IoT(config-if)#ip address 10.10.100.26 255.255.255.252
R4-IoT(config-if)#bandwidth 128
R4-IoT(config-if)#no shutdown
R4-IoT(config-if)#exit
R4-IoT(config)#interface fastEthernet 0/0
R4-IoT(config-if)#ip address 172.16.0.1 255.255.0.0
R4-IoT(config-if)#no shutdown
R4-IoT(config-if)#exit
R4-IoT(config)#router rip
R4-IoT(config-router)#version 2
R4-IoT(config-router)#network 10.10.100.24
R4-IoT(config-router)#network 172.16.0.0
R4-IoT(config-router)#no auto-summary
R4-IoT(config-router)#exit
R4-IoT(config)#do wr
```

- **Red de Telefonía móvil**

Enrutador 5

```
Router>enable
Router#configure terminal
Router(config)#hostname R5-Mov
R5-Mov(config)#banner motd &
*****
RED DE TELEFONIA MOVIL
EDDIE YANEZ
*****
&
R5-Mov(config)#service password-encryption
R5-Mov(config)#banner motd $RED TELEFONIA MOVIL$
R5-Mov(config)#interface serial 0/3/0
R5-Mov(config-if)#ip address 10.10.100.34 255.255.255.252
```

```

R5-Mov(config-if)#bandwidth 128
R5-Mov(config-if)#no shutdown
R5-Mov(config-if)#exit
R5-Mov(config)#interface fastEthernet 0/0
R5-Mov(config-if)#ip address 172.20.0.1 255.255.0.0
R5-Mov(config-if)#no shutdown
R5-Mov(config-if)#exit
R5-Mov(config)#router rip
R5-Mov(config-router)#version 2
R5-Mov(config-router)#network 10.10.100.32
R5-Mov(config-router)#network 172.20.0.0
R5-Mov(config-router)#no auto-summary
R5-Mov(config-router)#exit
R5-Mov(config)#do wr

```

- **Configuración de la red del proveedor de servicios**

Enrutador 6

```

Router>enable
Router#configure terminal
Router(config)#hostname R6-Cab
R6-Cab(config)#banner motd &
*****
RED DE PROVEEDOR SERVICIO CABLE
EDDIE YANEZ
*****
&
R6-Cab(config)#service password-encryption
R6-Cab(config)#banner motd $RED PROVEEDOR SERVICIOS$
R6-Cab(config)#interface fastEthernet 1/0
R6-Cab(config-if)#ip address 10.10.100.2 255.255.255.252
R6-Cab(config-if)#no shutdown
R6-Cab(config-if)#exit
R6-Cab(config)#interface fastEthernet 0/0
R6-Cab(config-if)#ip address 192.168.50.1 255.255.255.0
R6-Cab(config-if)#no shutdown
R6-Cab(config-if)#exit
R6-Cab(config)#interface fastEthernet 0/1
R6-Cab(config-if)#ip address 172.50.0.1 255.255.255.0
R6-Cab(config-if)#no shutdown
R6-Cab(config-if)#exit
R6-Cab(config)#interface fastEthernet 0/0
R6-Cab(config-if)#ip helper-address 172.50.0.2
R6-Cab(config-if)#exit
R6-Cab(config)#router rip
R6-Cab(config-router)#version 2
R6-Cab(config-router)#network 10.10.100.0
R6-Cab(config-router)#network 192.168.50.0
R6-Cab(config-router)#network 172.50.0.0

```

```
R6-Cab(config-router)#no auto-summary
R6-Cab(config-router)#end
R6-Cab#wr
```

- **Red de DSL**

Enrutador 7

```
Router>enable
Router#configure terminal
Router(config)#hostname R7-DSL
R7-DSL(config)#banner motd &
*****
RED DE DSL
EDDIE YANEZ
*****
&
R7-DSL(config)#service password-encryption
R7-DSL(config)#banner motd $RED DE DSL$
R7-DSL(config)#interface fastEthernet 1/0
R7-DSL(config-if)#ip address 10.10.100.30 255.255.255.252
R7-DSL(config-if)#no shutdown
R7-DSL(config-if)#exit
R7-DSL(config)#interface fastEthernet 0/0
R7-DSL(config-if)#ip address 192.168.60.1 255.255.255.0
R7-DSL(config-if)#no shutdown
R7-DSL(config-if)#exit
R7-DSL(config)#interface fastEthernet 0/1
R7-DSL(config-if)#ip address 172.60.0.1 255.255.255.0
R7-DSL(config-if)#no shutdown
R7-DSL(config-if)#exit
R7-DSL(config)#interface fastEthernet 0/0
R7-DSL(config-if)#ip helper-address 172.60.0.2
R7-DSL(config-if)#exit
R7-DSL(config)#router rip
R7-DSL(config-router)#version 2
R7-DSL(config-router)#network 10.10.100.28
R7-DSL(config-router)#network 192.168.60.0
R7-DSL(config-router)#network 172.60.0.0
R7-DSL(config-router)#no auto-summary
R7-DSL(config-router)#exit
R7-DSL(config)#do wr
```

ANEXOS B. Configuración de equipos servidores, dispositivos y objetos IoT

La tabla 1 de direccionamiento IPv4 para los servidores se muestra a continuación y debe ser una configuración estática y no dinámica mediante DHCP, además no es necesario en algunos de ellos asignar el *Domain Name System* (DNS) o en español sistema de nombres de dominio que viene hacer el conjunto de servicios y protocolos, que asocia una dirección IP con un nombre (nombre de dominio), con el objetivo de facilitar al usuario usar un nombre en vez de una IP numérica.

Tabla 1

Direccionamiento IPV4 de servidores

Equipo	Gateway	Dirección IPv4	DNS	Mascara	DHCP
ServerDHCP Cable	172.50.0.1	172.50.0.2	-	255.255.255.0	NO
ServerDNS IoT	172.16.0.1	172.16.0.2	-	255.255.0.0	NO
ServerIoT IoT	172.16.0.1	172.16.0.3	172.16.0.2	255.255.0.0	NO
COS backbone	172.19.0.1	172.19.0.2	172.16.0.2	255.255.0.0	NO
COS Celltower	-	172.18.1.1	172.16.0.2	255.255.255.0	-
ServerDHCP DSL	172.60.0.1	172.60.0.2	-	255.255.255.0	NO
Server2 Red2	192.168.60.1	192.168.60.2	172.16.0.2	255.255.255.0	NO

Nota. Direccionamiento IPv4 de clase B y C

La tabla 2 muestra el direccionamiento referencial que deben tener los dispositivos inteligentes, ya que se recomienda que las direcciones IPv4 sean automáticas mediante DHCP. Cuando existe algún inconveniente en la configuración de los equipos de red puede reflejar un error de *"DHCP failed. APIPA is being used"* y la asignación IPv4 puede arrojar por ejemplo 169.254.224.42 pero el *"Default Gateway"* o puerta de enlace no refleja información.

Tabla 2*Direccionamiento IPV4 de dispositivos inteligentes*

Equipo	Gateway	Dirección IPv4	DNS	Mascara	DHCP
Laptop1 Red1	192.168.50.1	192.168.50.21	172.16.0.2	255.255.255.0	SI
TabletPC1 Red1	192.168.50.1	192.168.50.23	172.16.0.2	255.255.255.0	SI
Smartph1 Red1	192.168.50.1	192.168.50.22	172.16.0.2	255.255.255.0	SI
Laptop0 Red2	192.168.60.1	192.168.60.17	172.16.0.2	255.255.255.0	SI
TabletPC0 Red2	192.168.60.1	192.168.60.11	172.16.0.2	255.255.255.0	SI
Smartph0 Red2	192.168.60.1	192.168.60.12	172.16.0.2	255.255.255.0	SI

Nota. Por ser direccionamiento DHCP, las direcciones IP se asigna automáticamente

El teléfono inteligente smartphone 2 debe acceder a la red www.domotica.com mientras que el teléfono smartphone 4 a la red www.smarthome.com.

Además de la configuración de ocho enrutadores se debe considerar el uso y configuración cinco servidores de acuerdo al direccionamiento de la tabla 1, que están enlazados en las diferentes redes LAN y WAN. Es indistinto el orden de configuración de dichos servidores, lo que importa es que tengan conectividad entre todos los equipos. Se empezará con el proceso de configuración del servidor DHCP instalado en la red del proveedor de servicios de cable que proporciona una interfaz de 2,4 GHz adecuada para la conexión a redes inalámbricas; por lo tanto, realizar las siguientes acciones y que además se muestra en la figura 1.

- En la ventana del escritorio “*Desktop*”, ingresar a la configuración IP.
- Seleccionar direccionamiento estático.
- Agregar una dirección IP estática (192.168.5.2) de acuerdo a la red de donde pertenece.
- Agregar una dirección en la máscara de subred (255.255.255.0).
- Agregar una dirección en la puerta de enlace (192.168.5.1).
- En “*DNS server*”, no se asigna ningún valor.

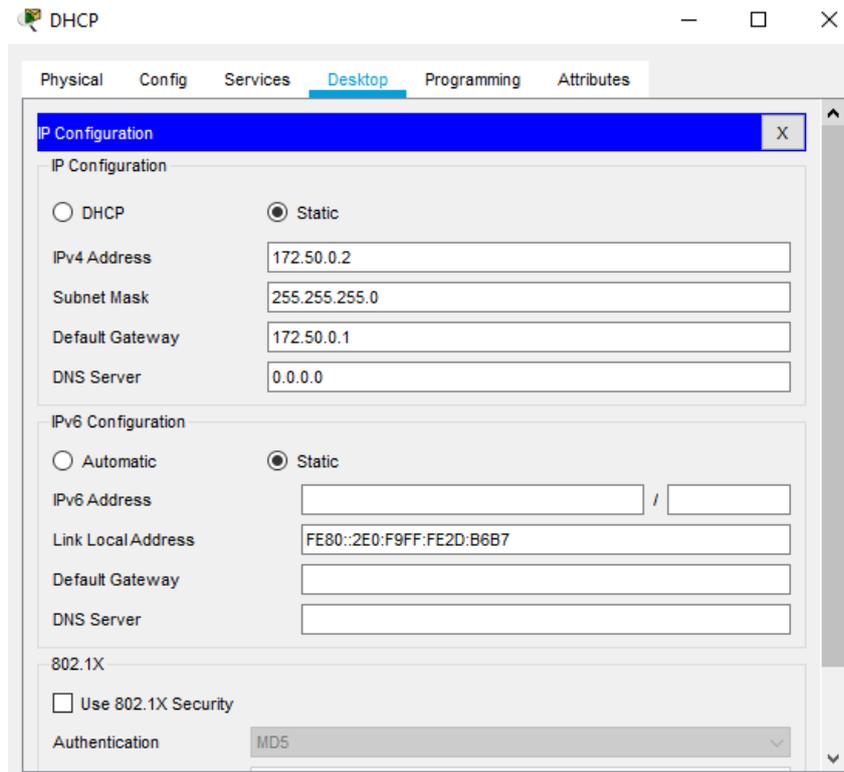


Figura 1. Configuración IP DHCP del servidor

Posteriormente en la pestaña de “Servicios”, seleccionar el servicio DHCP y en encender el servicio. Puede encontrar una configuración de DHCP por defecto; se debe incluir un nuevo servicio de DHCP, para lo cual se deben hacer las siguientes acciones:

- Cambiar el nombre del servicio “Pool name” y colocar un nombre, para la presente simulación se coloca “cable”.
- Insertar dirección IP en la puerta de enlace (192.168.50.1), dicha interfaz permite el acceso a la otra red (red doméstica 1) ya que tienen un protocolo diferente y corresponde a la dirección IP Fa0/0 asignada en el router R6-Cab.
- Insertar dirección en el servidor de DNS (172.16.0.2) del servicio que tiene como referencia a la red de la empresa de IoT
- En la dirección IP de inicio se asignación de direcciones DHCP empieza desde la siguiente IP 192.168.5.20 (tercer octeto).
- Insertar la dirección de la máscara de subred (255.255.255.0),
- Número máximo de usuarios (200) y

- Agregar.

Se recomienda crear el nuevo servicio DHCP en “off”, para posteriormente cuando se agrega el servicio proceder a encender “on”, como se muestra en la figura 2. Si el servicio no está creado o tiene alguna falla en su configuración, no se va a tener servicio DHCP en la red doméstica 1.

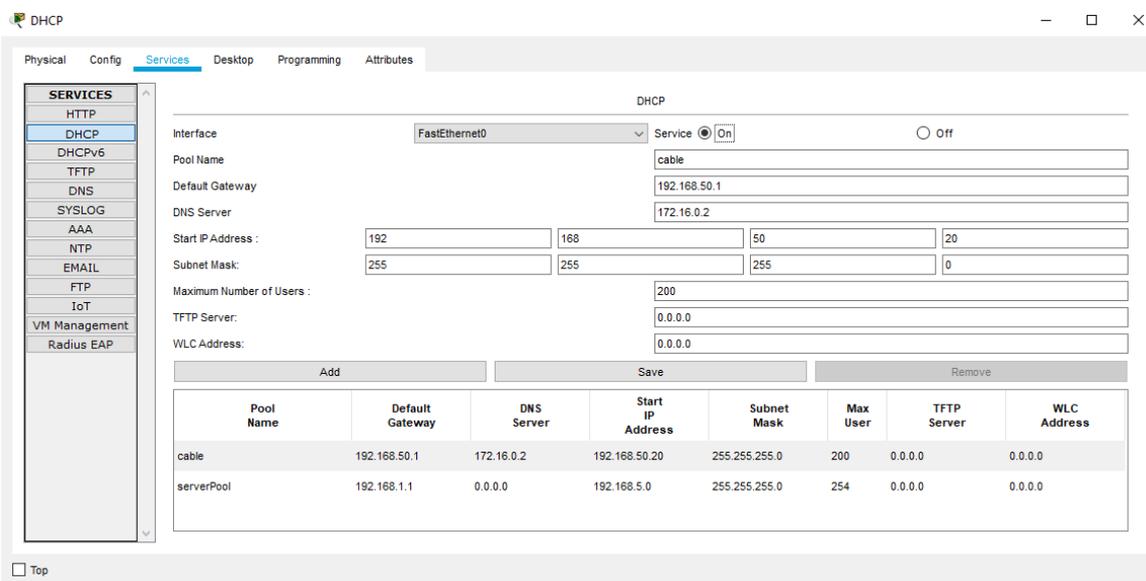


Figura 2. Crear nuevo servicio en el servidor DHCP

En la figura 3, se muestra la comunicación del servidor DHCP configurado con una IP de clase B de la red del servidor de cable con las redes de clase A que corresponde a la red del Internet y con la red de clase C que corresponde a la red doméstica, donde se tiene una latencia en el envío de paquetes de mínimo= 0ms, máximo= 1ms. Por la tanto la comunicación es efectiva.

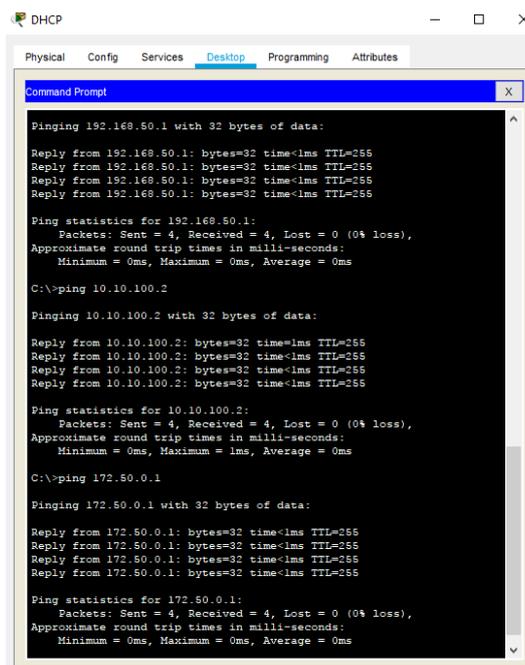


Figura 3. Ping entre servidor DHCP y las redes externas

Previo a continuar con las configuraciones es importante recomendar de ser el caso de que, en algún equipo, en el cual no se pueda acceder a la configuración y tenga como mensaje *“All tabs are in Hide mode”*, en el *software Packet Tracer*, se debe hacer los siguientes pasos:

- Ir a la “opción” y seleccionar *“preferences”*
- Escoger la pestaña de *“Hide”* y
- Desmarcar las opciones *“Hide physical tab”* y *“hide all devices config tab”*
- Ahora el equipo debe permitir acceder a la ventana de configuración.

➤ **Configuración de la nube Cloud 0 del proveedor de servicio**

Para lo cual se debe acceder a la nube y realizar la siguiente configuración o como se muestra en la figura 4.

- En la pestaña de *“Config”* en la opción *“Ethernet”* en *“Provider Network”* seleccionar *“Cable”*.
- En la opción *“Cable”* ingresar y seleccionar *“Coaxial7”* y *“Ethernet6”* y proceder a agregar.

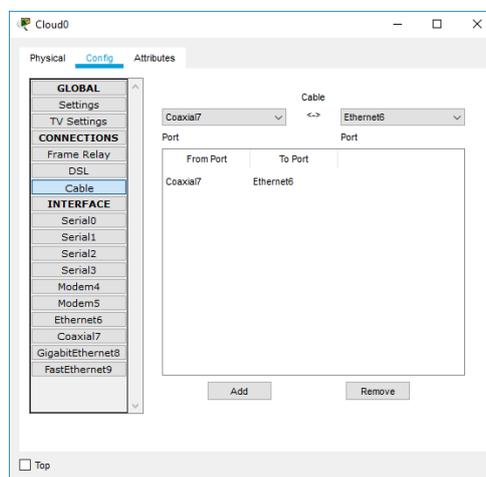


Figura 4. Configuración de Cloud

➤ **Configuración de cosas de IoT en la red domestica**

En la red doméstica 1, ingresar al *“Cluster0”*, donde se tiene varias cosas consideradas físicas incluidas en dicha red y proceder con la configuración respectiva de cada cosa u objeto físico.

Existe ciertas similitudes en las configuraciones de los objetos, para el caso; en el dispositivo laptop 1, realizar la siguiente configuración:

- Ingresar a la ventana del escritorio “Desktop”, y luego en “IP configuration”.
- Desactivar y volver a activar el protocolo DHCP.
- Aparece una dirección IP (192.168.50.21).
- Aparece una dirección de la máscara de subred (255.255.255.0).
- Aparece una dirección en la puerta de enlace (192.168.50.1), y
- Aparece una dirección del servidor DNS (172.10.0.2)

La laptop de ser necesario por alguna situación también puede ser configurado de forma manual, para lo cual se debe activar “static” y colocar una dirección IP que pertenezca a la red LAN. Para la presente simulación y por disponer de un servidor DHCP la asignación de direcciones es automático y aleatorio, como se muestra en la figura 5.

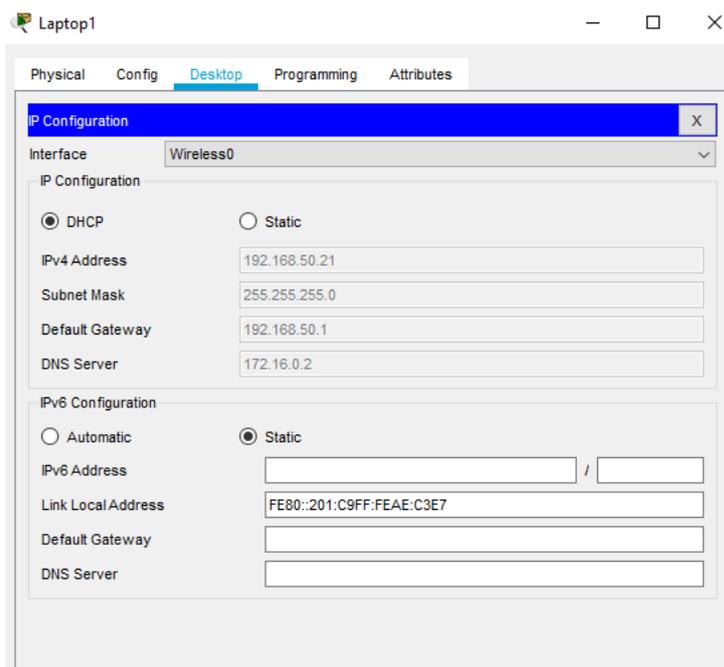


Figura 5. Configuración IP DHCP de equipo IoT

En la red doméstica, se debe configurar el “access point” para lo cual se debe ingresar al equipo y darle un nombre a la red doméstica, nombre que será replicado en todos los objetos físicos; para el presente trabajo se le denominará como “domotica”, como se muestra en la figura 6.

En el dispositivo Access point1, de ser el caso proceder a encender y continuar con la configuración. Es muy importante recordar el nombre asignado a la red, ya que se debe incluir en la configuración de las cosas. La acción a realizar es:

- Acceder a “Configuración” en el equipo “*access point*”, seleccionar “Port 1” e introducir el nombre de la red en SSID “domotica”.

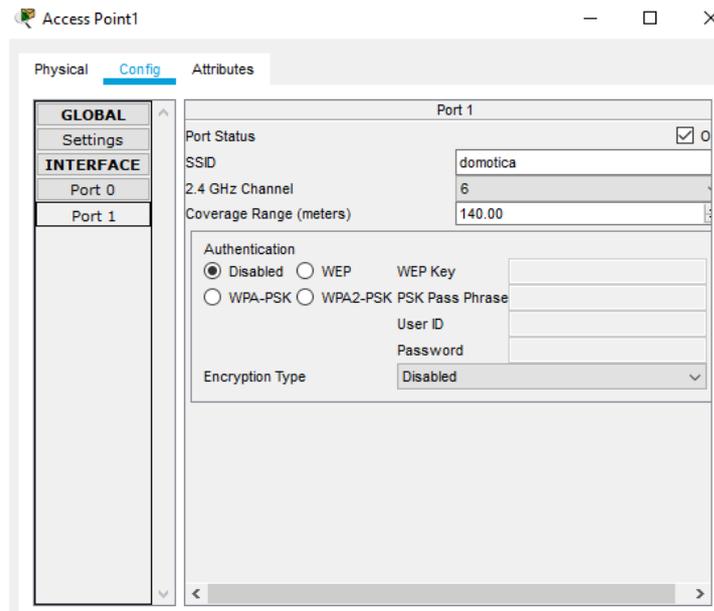


Figura 6. Configuración puerto Access Point

En el identificador de red “SSID” que viene a ser el nombre público de la red LAN inalámbrica (WLAN), éste permite diferenciar su red de las demás redes inalámbricas que estén presentes; al SSID del *access point* se le debe asignar un nombre de la red, pero esto no quiere decir que los objetos físicos se conectan automáticamente, como se muestra en la figura 7 donde además, se puede observar la conectividad del AP con el *modem* y este a su vez con el router por donde realizará el envío y recepción de paquetes desde a hacia las demás redes; pero los objetos físicos aún no están dentro de la red LAN, por tal razón se debe a la configuración de los objetos físicos.

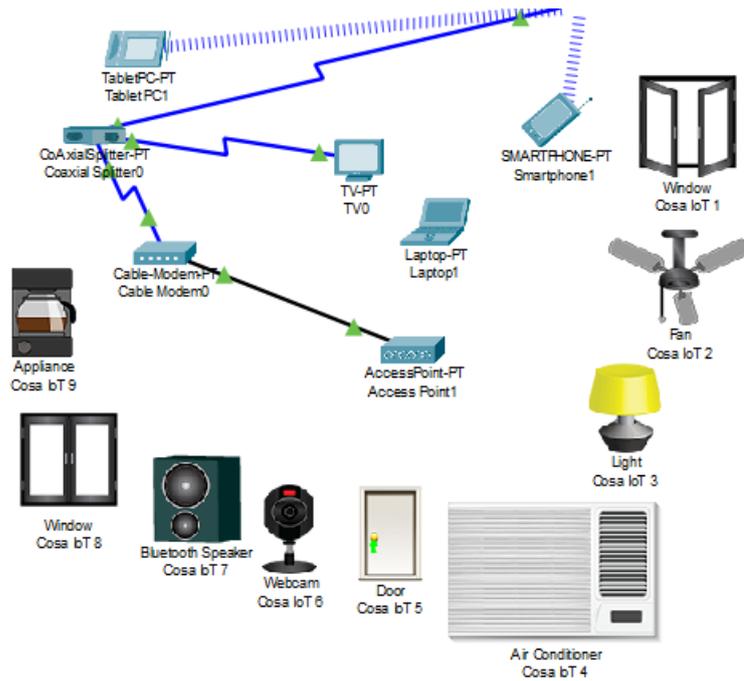


Figura 7. Esquema de objetos físicos sin comunicación

Nuevamente el orden de configuración es indiferente, para el ejemplo se va a proceder a la configuración como primer objeto a la ventana para que funcione como un dispositivo IoT y que éste se pueda controlado remotamente, por lo tanto, se debe realizar las siguientes acciones:

- Acceder a “Avanzado”, seleccionar la pestaña “I/O configuración”.
- En adaptador de red, seleccionar o agregar una *interface* inalámbrica (PT-IOT-NM-1W), que permitirá el acceso remoto, como se observa en la figura 8.

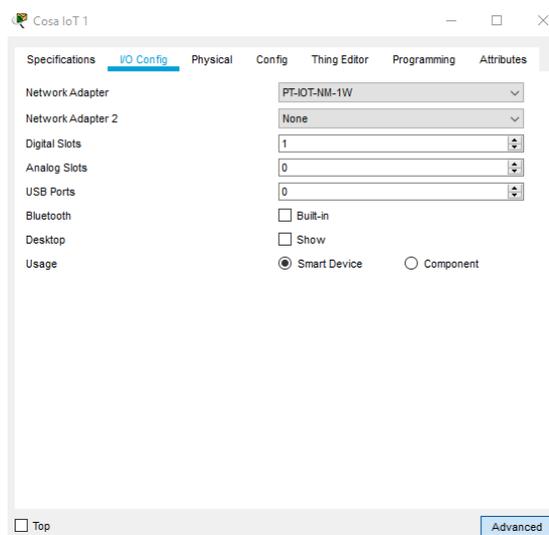


Figura 8. Configuración de interface a objetos físicos

En la pestaña “Config”, seleccionar “Interface” en el dispositivo inalámbrico “Wireles0”, asignar el nombre de la red en el campo “SSID” (domotica), de acuerdo a la configurado en el AP. En esta opción también se puede colocar contraseña de ser necesario; se logra así, que la ventana sea el primer dispositivo inteligente de la red domótica que pertenece a la red LAN, como se observa en la siguiente figura 9.

El objeto físico ahora con inteligencia que fue configurado debe reflejar conectividad Wifi con el equipo “access point”. Proceso similar se debe ejecutar con el resto de objetos físicos. Se puede observar el direccionamiento IP de cada objeto con acercar el cursor de mouse a cada dispositivo.

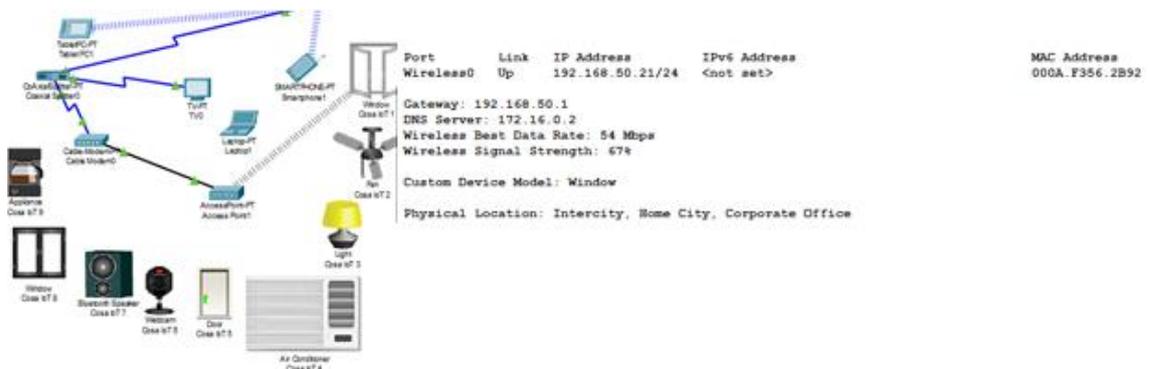


Figura 9. Conectividad de objeto inteligente en la red

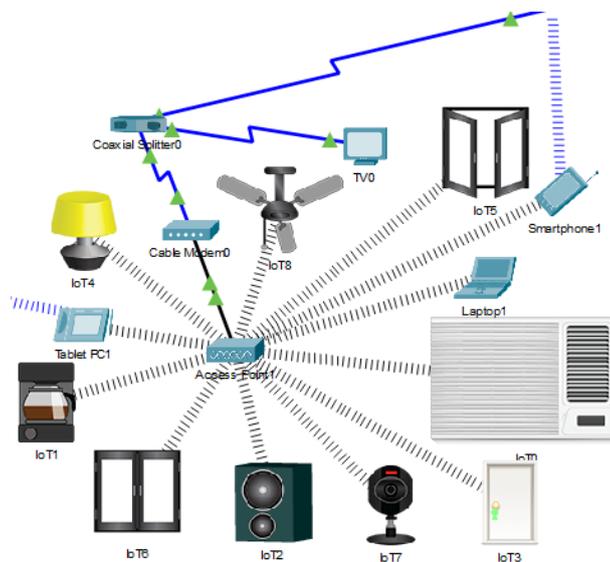


Figura 10. Conexión de los objetos IoT en la red domótica

Una vez que se hayan incluidos y configurados todos los objetos físicos en la red domótica1,

como se observa en la figura 10. Proceder con la configuración del servidor DHCP que pertenece a la red de línea de abonado digital (DSL), que puede proporcionar los equipos en la actualidad ancho de banda por medio de transmisión de alta velocidad de hasta 7.1 Mbps para la transmisión de información, todo esto por medio de la línea telefónica. La red doméstica 2 (*Cluster1*), va a hacer la base para lograr obtener una “*smart home*”; para la configuración de servidor DHCP se debe realizar las siguientes acciones:

- Acceder al servidor DHCP, seleccionar la pestaña que dice “*Desktop*” y escoger “Configuración IP”.
- Se debe asignar una dirección IPv4 estática como 172.60.0.2.
- La máscara de subred 255.255.255.0.
- *Gateway* se le asigna la IP: 172.60.0.1, como se observa en la figura 11.

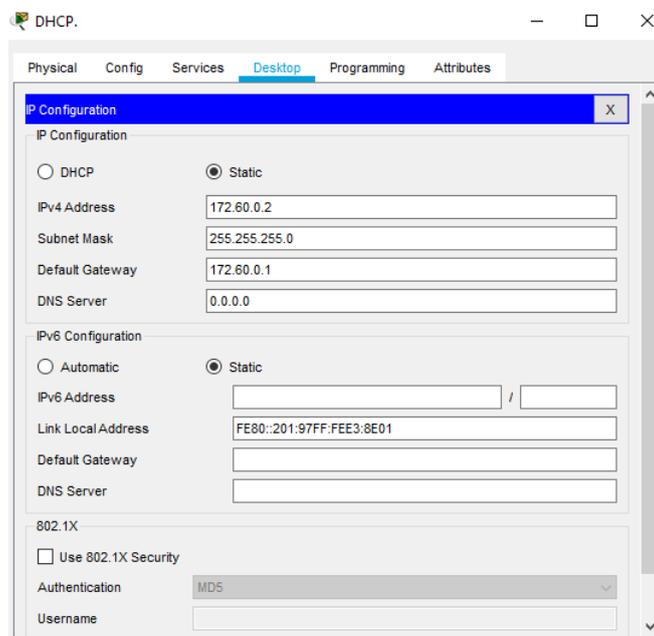


Figura 11. Configuración del servidor DHCP de la red DSL

Ahora agregar el servicio DHCP, para que puedan acceder los objetos físicos de la red doméstica 1 a un enrutamiento por DHCP, para lo cual realizar las siguientes acciones:

- Seleccionar la pestaña “*services*” y escoger “DHCP”
- Encender el servicio; se tiene la configuración de DHCP por defecto “*serverPoll*” y proceder a crear una nueva red para brindar el servicio DHCP.

- Cambiar el nombre del servicio “Pool name” y colocar “dsl” que tiene relación a la red que pertenece dicho servidor. Los nombres que se asignen pueden ser indistintos.
- Insertar dirección IP en la puerta de enlace (192.168.60.1), que corresponde a la interfaz de salida del *router* Fa0/0.
- Insertar dirección en el servidor de DNS (172.16.0.2) del servicio que tiene como referencia a la red de la empresa de IoT.
- En la dirección IP de inicio desde donde va a partir y corresponde al tercer se asigna la IP (192.168.60.10).
- Insertar la dirección de la máscara de subred (255.255.255.0)
- Número máximo de usuarios (246) y proceder a agregar, como se observa en la figura 12.

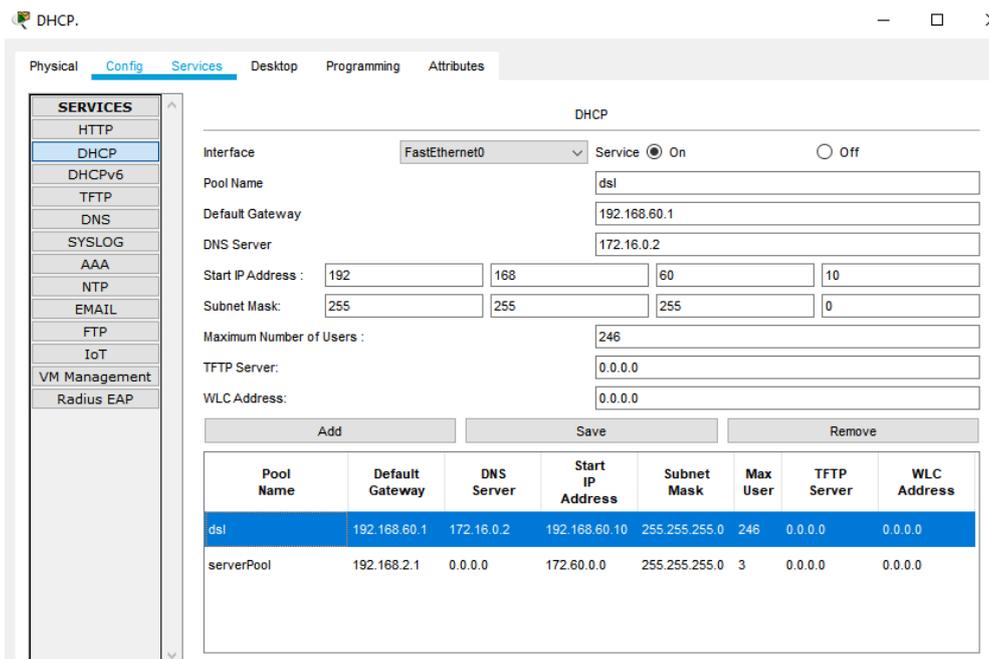


Figura 12. Crear nuevo servicio del servidor DHCP de la red DSL

Una vez configurados los equipos de red, se debe proceder a configurar los dispositivos inteligentes y los objetos físicos de la red doméstica dos, que corresponden al *Cluster1*, como recomendación se debe empezar con la configuración de la *laptop0* donde se pueda comprobar el direccionamiento DHCP, para lo cual se debe hacer las siguientes acciones:

- Acceder al equipo *laptop0*, seleccionar la pestaña “Desktop” y escoger la opción “IP configuration”

- Permitir que se asigne una dirección IP automática, para ello seleccionar “DHCP”, donde se tendrá la IP dinámica de host como podría ser la IPv4 192.168.60.17 con mascara de subred 255.255.255.0 la dirección del “Gateway” 192.168.60.1 y muy importante la dirección IP del servidor DNS 172.16.0.2 que se encuentra en otra red, como se observa en la figura 13.

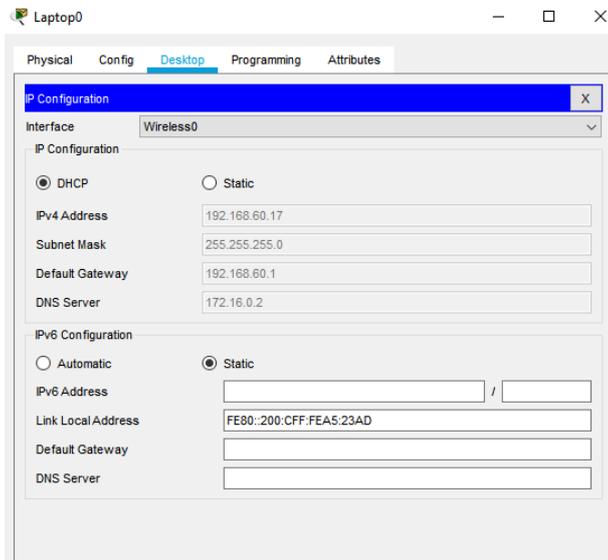


Figura 13. Configuración de dirección IP en la laptop

Se puede comprobar si existe conectividad entre la red LAN doméstica 2 con el *router* R7-DSL de la red DSL mediante un ping para medir la latencia en milisegundos, desde la laptop0, donde el resultado es satisfactorio y los valores obtenidos están en el orden de los milisegundos y además de la comprobación del servidor DHCP como se observa en la figura 14. Vale indicar que la laptop cuenta con un módulo Linksys WPC300N que proporciona una interfaz inalámbrica de 2,4 Ghz y admite protocolos de uso para *Ethernet* de acceso a redes LAN.

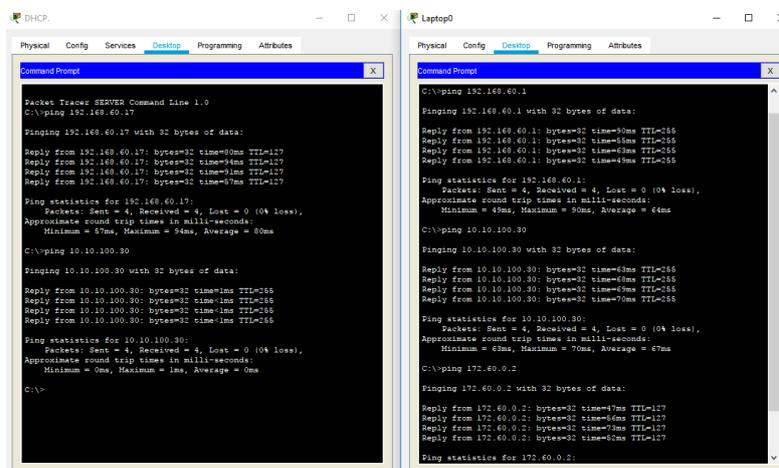


Figura 14. Comprobación de latencia de la red doméstica con la red DSL

De forma similar a lo explicado anteriormente, se debe proceder a la configuración de los objetos físicos de la red doméstica 2 que recibe el servicio DSL; para aquello asignar un nombre a la red en el “*access point*” y colocar para la simulación presente “*smarthome*”, mientras que, a los objetos físicos agregar una *interfaz* para que pueda acceder a la red inalámbrica y por ende al Internet y con ello brindar inteligencia a los objetos físicos. En la figura 15 se muestra la configuración de un objeto que pertenece a la red LAN doméstica 2.

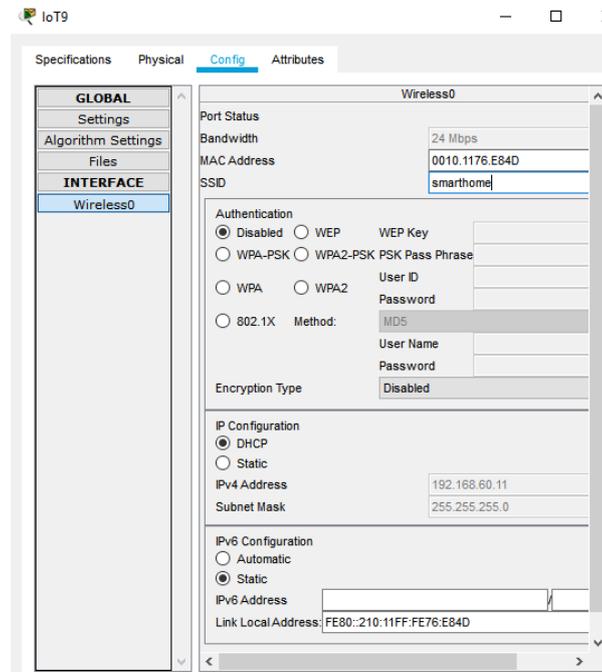


Figura 15. Configuración de la segunda red LAN

Proceder a realizar la configuración de todos los objetos físicos que pertenecen a la red doméstica dos. Una de las características de los objetos del hogar es que son compatibles con el servidor de registro para tener un control remoto y se pueden utilizar dispositivos como SBC, MCU, *Thing* si necesita una configuración personalizada para enviar escritura.

El SBC (*Single Board Computer*) es una tarjeta electrónica *Arduino* que cumple cierta semejanza con un ordenador, en la que consta de un circuito único donde incluye la memoria, I/O, microprocesador, etc. Existen varios tipos de SBC, pero uno de los más conocidos se tiene al “*Raspberry Pi*”; mientras que un MCU (Unidad de microcontrolador), viene a ser un sistema que incorpora un ordenador entero dentro de un solo chip, igualmente cuenta con un procesador, memoria, almacenamiento y algo muy interesante los pines de entrada y salida son programables. Finalmente, la placa de desarrollo conocido como *Thing* es muy útil como base para proyectos del Internet de las Cosas, que puede ser utilizado hasta para la publicación de datos con servicios web y su programación es similar que un microcontrolador.

Es importante mencionar que cada objeto IoT o equipo IoT es identificado con una dirección MAC que es única para cada dispositivo. Para configurar el teléfono inteligente (*smartphone*) y *tablet* tiene un procedimiento diferente, ya que la asignación de IPv4 por DHCP no es igual que en un computador o laptop, con esta aclaración se debe realizar las siguientes acciones:

- En la pestaña “Config”, en “Settings” cambiar la “interfaces” por defecto de “Wireless0” por “3G/4G Cell1”.
- En la opción “Wireless0”, asignar el nombre de la red en el campo “SSID” para la presente simulación se coloca “domótica”.
- Salir de “Config” e ingresar a la pestaña “Desktop”, ingresar a “IP configuration” y seleccionar “DHCP”. Automáticamente se asigna una dirección IPv4 dinámica como por ejemplo (192.168.50.22), la máscara de subred (255.255.255.0), el Gateway (192.168.50.1) y la dirección del servidor de DNS (172.16.0.2), como se observa en la figura 16.

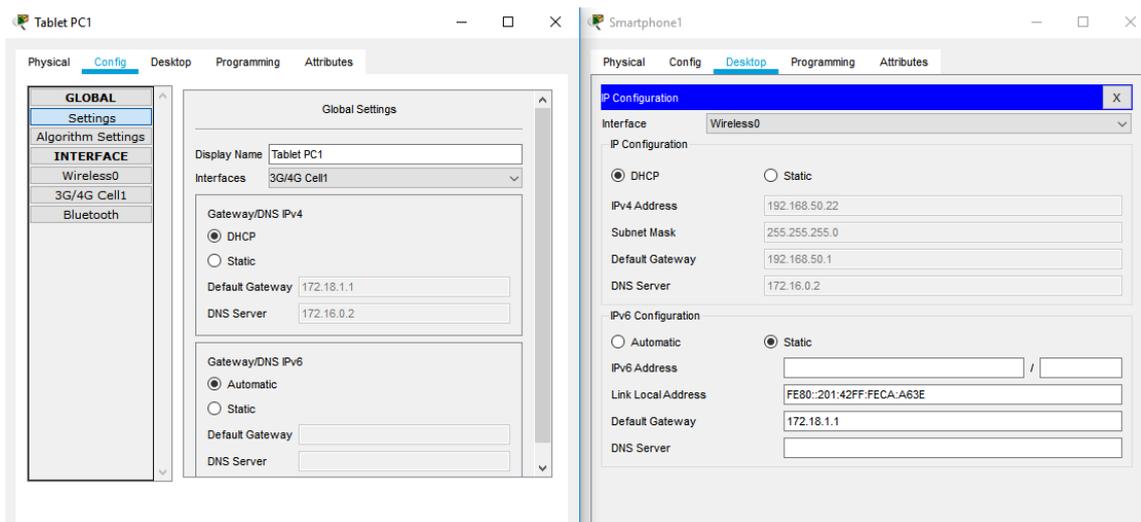


Figura 16. Configuración de dispositivos inteligentes

Como una observación la dirección IPv4 del “Default Gateway” 172.18.1.1 corresponde a la red del “Central Office Server” que conecta con la torre “Cell Tower” que brinda el servicio de celular a los usuarios que utilizan los *smartphone 2* y 4.

Seguido de la configuración de los servidores; en la red de la empresa de IoT, se tiene instalado un servidor DNS, el cual está conectado con un cable directo de cobre trenzado que usualmente se usa en redes de área local con un conector RJ-45 en cada uno de sus extremos, manteniendo la misma distribución en sus pines y está asignado con la *FastEthernet 0/0* de la red 172.16.0.0 por tanto, realizar las siguientes acciones:

- En la pestaña “Desktop” asignar una dirección IP estática, para la simulación presente se propone utiliza la dirección por defecto que se utiliza la IPv4 172.16.0.2, máscara de subnet 255.255.0.0 y un default Gateway 172.16.0.1
- Configurar servicios DNS, para ello se debe crear los “dominios” para lo cual se agrega un nombre: al primer dominio www.domotica.com, su dirección (172.16.0.3) que corresponde a la dirección IPv4 del servidor IoT y dar clic en “Add”. Recordar que antes de esta acción el “DNS service” debe estar apagado.
- A continuación, agregar el siguiente dominio www.smarthome para la administración de la red DSL que contiene a la red LAN domótica 2. La dirección que se asigne al dominio dos, debe ser la misma dirección IPv4 del servidor (server2) de la red domótica 2. Dicho servidor debe tener una configuración IP “estática”, no puede tener una dirección IP dinámica, para la presente simulación.
- Finalmente encender el servicio “DNS”.

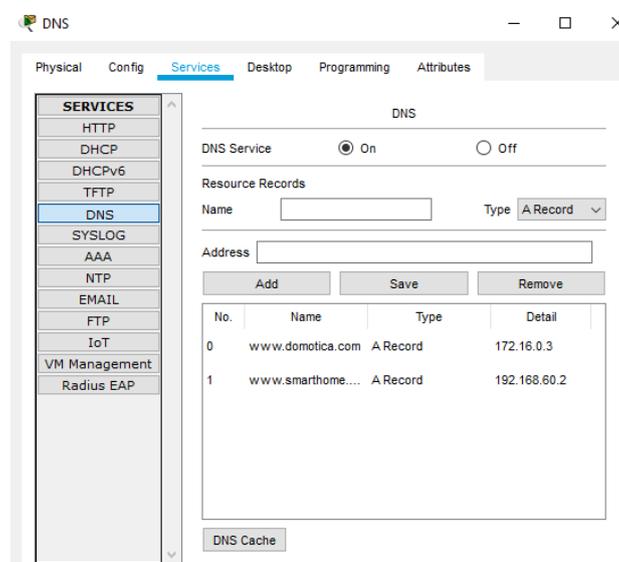


Figura 17. Configuración del servidor DNS

Ahora en el servidor IoT de la red 172.16.0.0, realizar las siguientes acciones:

- En la pestaña “Desktop” asignar una dirección IP estática IPv4 172.16.0.3, máscara de subnet 255.255.0.0, default Gateway 172.16.0.1 y se incluye la dirección del servidor DNS 172.16.0.2
- Se debe registrar el servicio IoT, para lo cual se debe ir a la pestaña de “Desktop” y escoger “IoT Monitor” y proceder a crear un usuario. En “User name” (domótica) se asigna el nombre con el cual se podrá acceder desde el dispositivo móvil desde la red domótica 1 y su correspondiente “password” (12345).
- En la pestaña “Services” debe aparecer el usuario y la clave creada. No olvidar que el servicio debe estar encendido para que pueda prestar dicho servicio.

La información creada en el servidor IoT, se debe colocar en todos los objetos IoT para que se vinculen al servicio. En la pestaña “config”, seleccionar “settings” y en “IoT server” asignar la dirección, el nombre y la clave del servidor remoto IoT. En la figura 18 se muestra las configuraciones de un objeto de la red domótica 1 respecto a la información configurada en el servidor IoT.

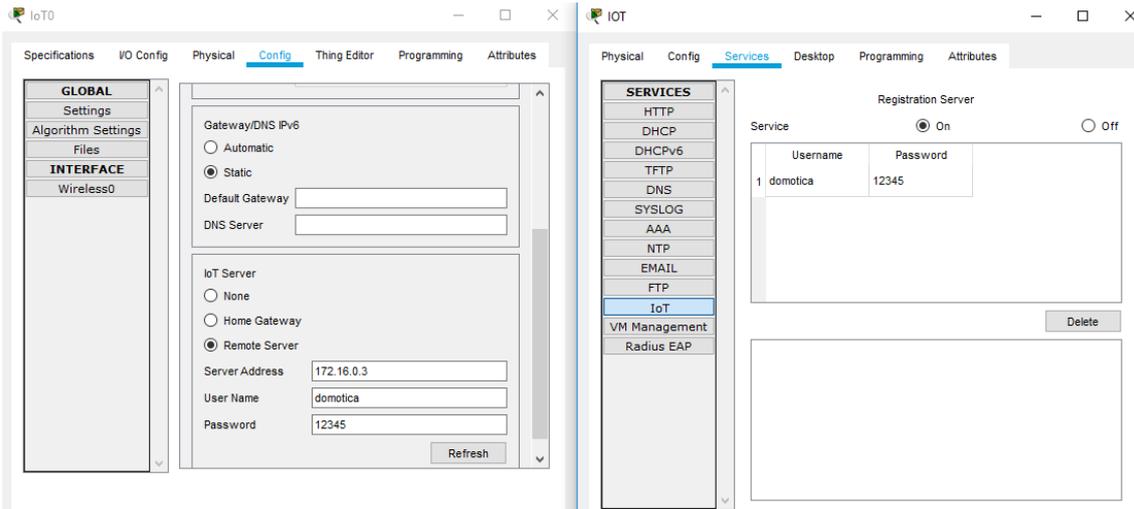


Figura 18. Registro de servicio IoT

Desde el teléfono inteligente que se encuentra dentro de la red LAN doméstica 1, ya se puede tener el control de los objetos IoT, como se muestra en la figura 19.

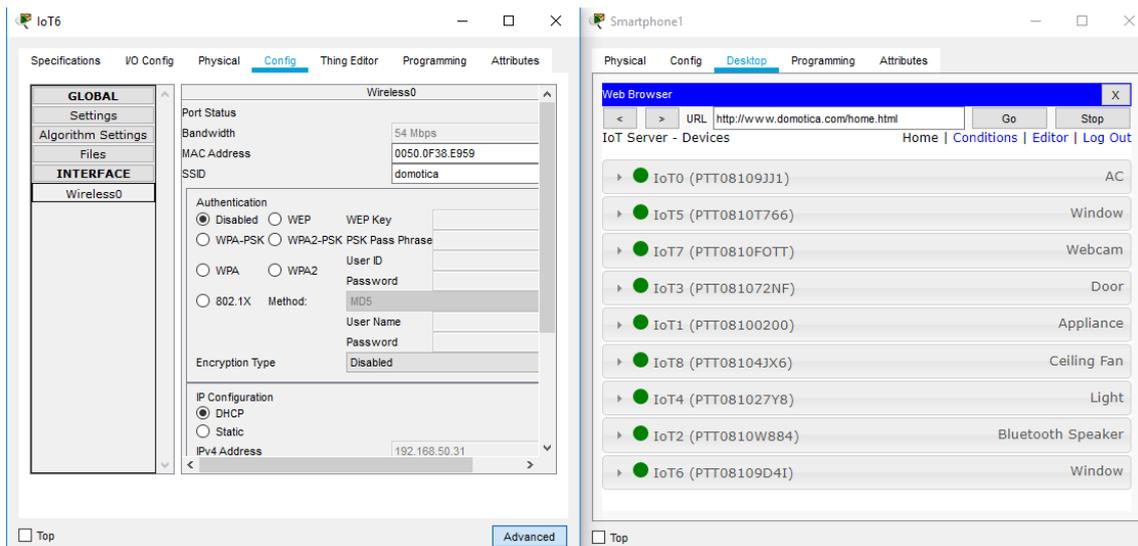


Figura 19. Control de los objetos IoT desde un smartphone

El penúltimo servidor que se va a configurar es el “server2” que pertenece a la red doméstica dos o *smart home*, pero antes es importante mencionar que lo programado hasta el momento permite que los dispositivos inteligentes como el *smartphone0* o *tablet0* tengan conexión con todos los router de las redes LAN y WAN, incluido a los servidores de DNS y IoT, como se observa en la figura 20, además se observar que a pesar que el servidor 2 tiene asignado una dirección IPv4 estática (192.168.60.2) no puede enviar ni recibir paquetes de fuera de su red; en otras palabras no tiene “ping” al *default Gateway* (192.168.60.1).

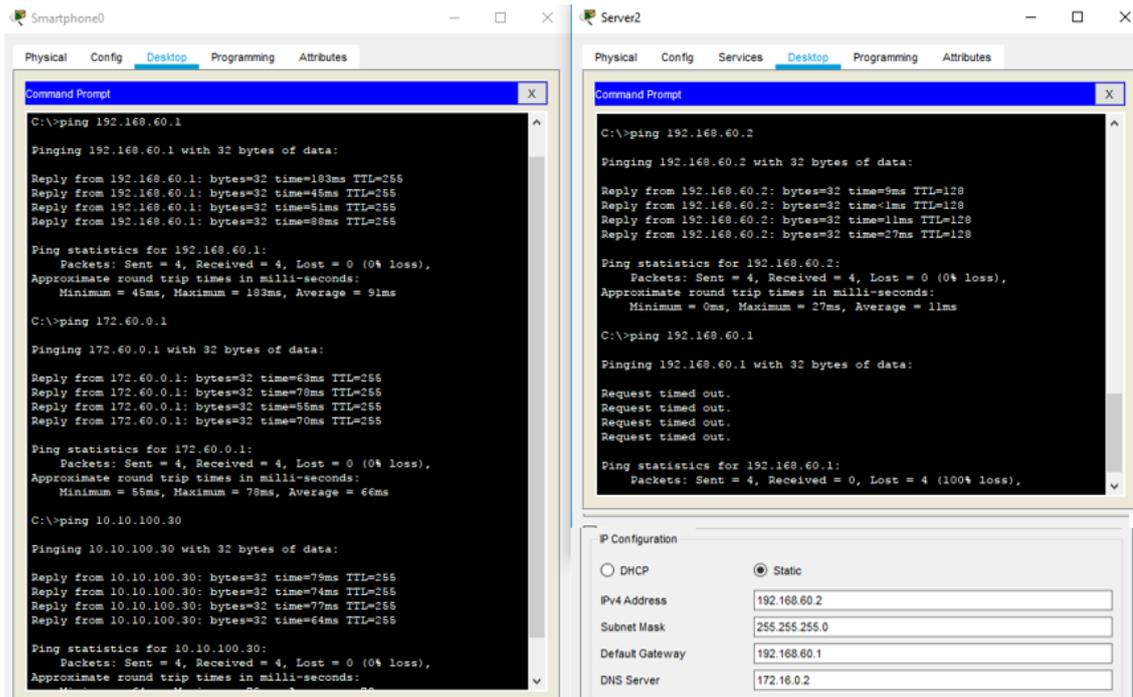


Figura 20. Dispositivos inteligentes con acceso a la red WAN

Además, los dispositivos inteligentes de la red doméstica dos, no tienen acceso a ningún objeto IoT dentro de su propia red LAN, por tal razón se va a utilizar un servidor local “server2” donde se van a realizar las siguientes acciones:

- En la pestaña “services”, dirigirse a “IoT” y proceder a encender el servidor de registro.
- En la ventana “Desktop”, Ingresar a opción “IoT monitor” y usar la dirección IPv4 del servidor proceder a ingresar en “IoT server address”, mantener el “user name” y “password” con “admin” que es por defecto, presionar “login”. Una vez que este allí proceder a crear una cuenta IoT, ya que aún no se ha registrado ninguna cuenta; escoger “Sign up now” y se debe ingresar el nombre de usuario (home) y su contraseña (12345) y “create”. Una vez registrado, aparecerá el usuario y contraseña en servicios IoT, como se observa en la figura 21.
- El servidor dos debe ser parte de la red LAN doméstica 2, para aquello en la pestaña “config” escoger “Wireless0” y asignar el nombre en SSID del access point (samarthome) y verificar si está asignado la IP estática y su máscara de red en la misma ventana de “Wireless0”.

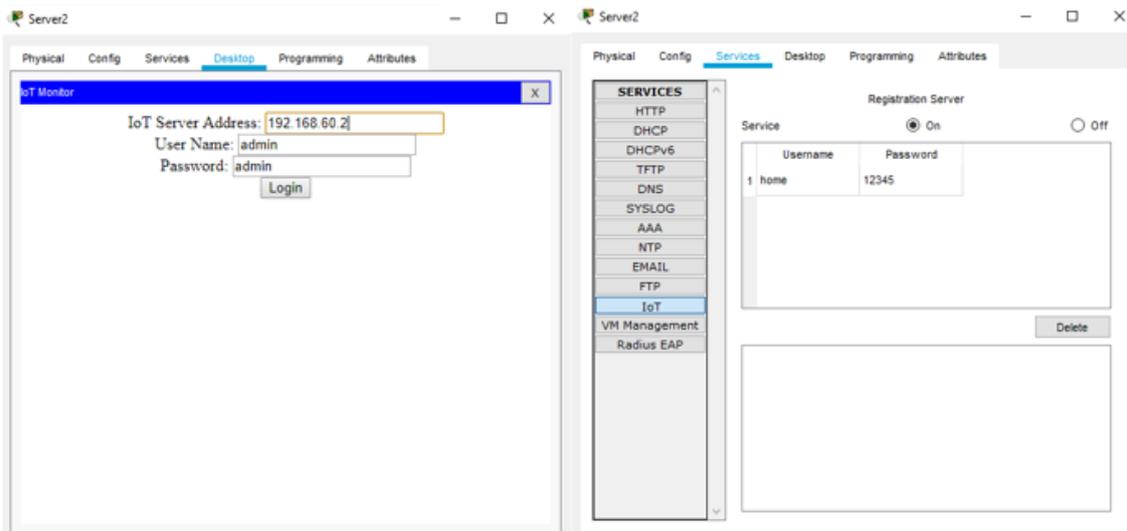


Figura 21. Registrar cuenta para servicio IoT

Finalmente, para la configuración del servidor de oficina central COS, donde se incluye al “Backbone” que viene a ser la red troncal y la “cell tower” como la torre de telecomunicaciones que pertenecen a la red de telefonía móvil. Inicialmente de debe asignar una IPv4 estática al “backbone”, ésta es la 172.20.0.2, con máscara de subred 255.255.0.0, puerta de enlace 172.20.0.1 y algo muy interesante que se da aquí es la dirección del servidor DNS, que viene a ser la dirección IPv4 del servidor IoT, como se observa en la figura 22.

Mientras el servidor central no esté debidamente configurado los teléfonos inteligentes smartphone 2 y smartphone 4 no tendrán acceso a ninguna de las redes domésticas desde del “Web Browser” que no es otra cosa más que el navegador web que permite al usuario acceder al Internet. Dicho navegador es el que interpreta el código HTML con la que está escrita la página web y ésta a su vez permite que se presente en la pantalla para que el usuario pueda interactuar con su contenido.

La configuración o no del servidor de la oficina central, no afecta de ninguna manera a los teléfonos inteligentes que están dentro de las dos redes domésticas, esto quiere decir que desde dichos dispositivos tienen el acceso completo de los objetos IoT que disponen en cada una de sus redes LAN.

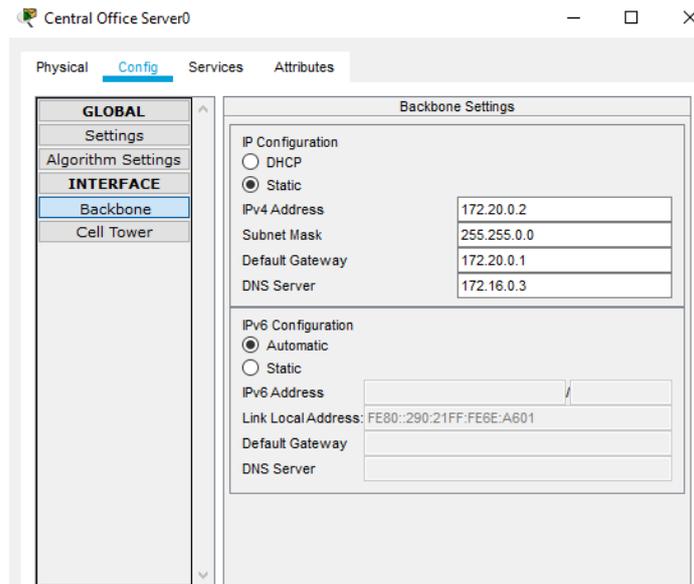


Figura 22. Configuración del Backbone

Otra parte que se debe configurar dentro del servidor de oficina central COS es la torre de telecomunicaciones donde se necesita agregar una dirección IPv4 que servirá para brindar DHCP a los usuarios de dicha red, que se refiere a los dispositivos *smartphone* 2 y 4, para ello se pueden agregar direcciones IPv4 desde 172.18.1.1 hasta 172.18.1.254, con máscara de subred 255.255.255.0, como se observa en la figura 23.

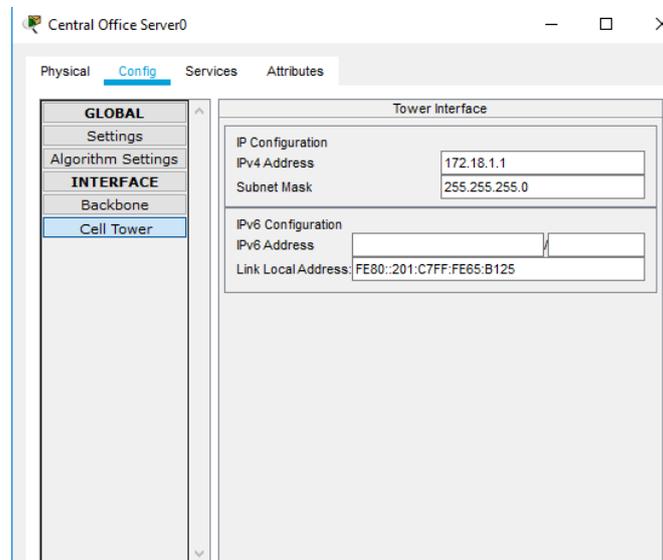


Figura 23. Configuración de la Torre de Telecomunicaciones

La torre de telecomunicaciones cuenta con una tarjeta PT-CELL-NM-1CX, con un conector coaxial que se utiliza para la conexión con el servicio de cable módem; la “cell tower” tiene casi todo listo para que se pueda acceder a las aplicaciones IoT, de ser necesario se puede configurar el rango de cobertura en metros.

Una vez configurado los equipos de la red de telefonía móvil, ya se puede gestionar el control remoto de los objetos IoT instalados en las dos redes domésticas inteligentes, como se observa en la figura 24. Cabe indicar que el acceso mediante el “*web browser*” puede ser mediante IPv4 172.16.0.3 o con www.smarthouse.com para ir a la red domótica 1 o *smart home* y con la IPv4 192.168.60.2 o con www.domotica.com para acceder a la red domótica.

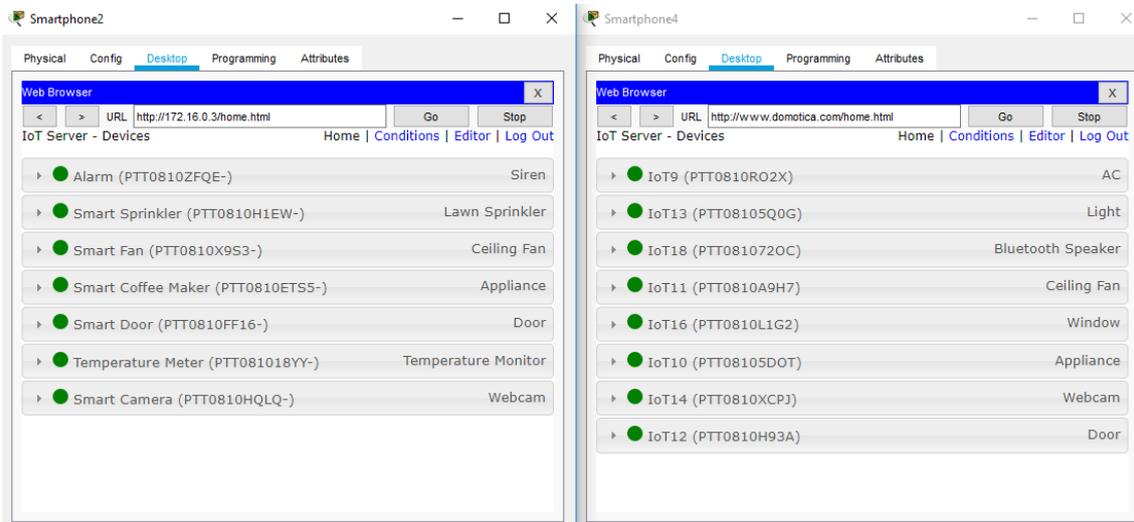


Figura24. Acceso remoto a las redes domésticas

Un dispositivo esencial y muy útil para dar inteligencia a un grupo importante de objetos es el Identificador de radio frecuencia, que justamente es muy utilizado en las tiendas de venta de ropa, que utiliza ésta etiqueta RFID, para llevar la cantidad de venta, sirve además para el rastreo de un dispositivo de baja potencia y que pueda acceder a bajas transmisiones e incluso para rastreo de personas. Para la configuración se debe realizar las siguientes acciones:

- Acceder a “*I/O Config*” y proceder a agregar la respectiva tarjeta inalámbrica, de forma similar que los objetos, pero con la diferencia que se debe agregar una conexión telefónica 3G/4G.
- En la pestaña “*Config*” asignar el acceso remoto en “*remote server*” con la dirección IPv4 correspondiente a la red donde se le vaya a incluir, como se observa en la figura 26.

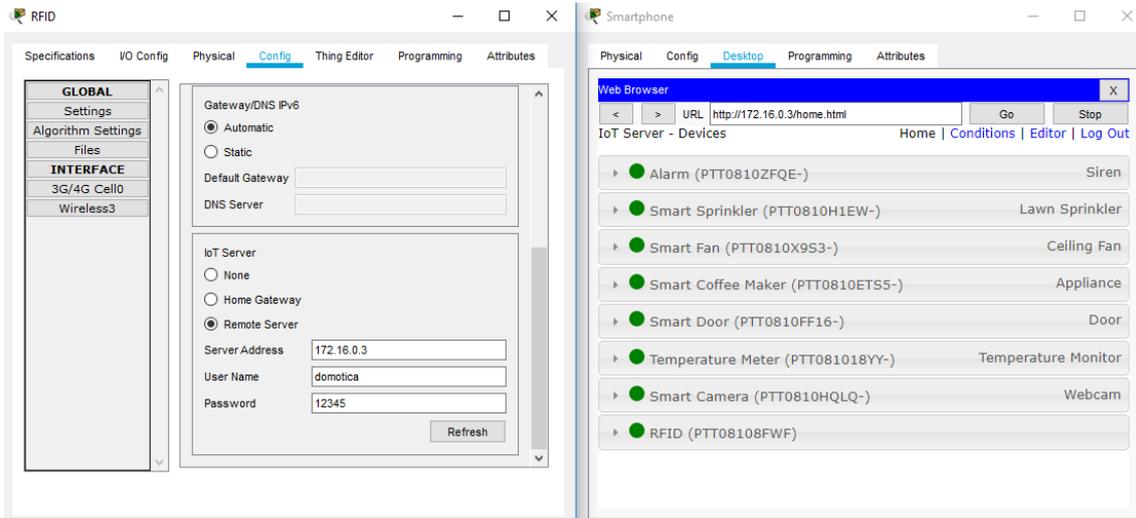


Figura 25. Configuración de etiqueta RFID

Una vez que se ha llegado a la configuración de los router, servidores y demás dispositivos inteligentes de las redes domóticas, es más fácil de implementar una red *smart home* y se lo puede realizar en cualquiera de las redes diseñadas, basta con incluir un *home Gateway* en reemplazo del *access point* y lógicamente se pueden utilizar dispositivos como SBC, MCU, *Thing* donde se pueden generar programaciones personalizadas de acuerdo a las necesidad propias de los usuarios, dando una inteligencia global en el hogar como se observa en la figura 25.

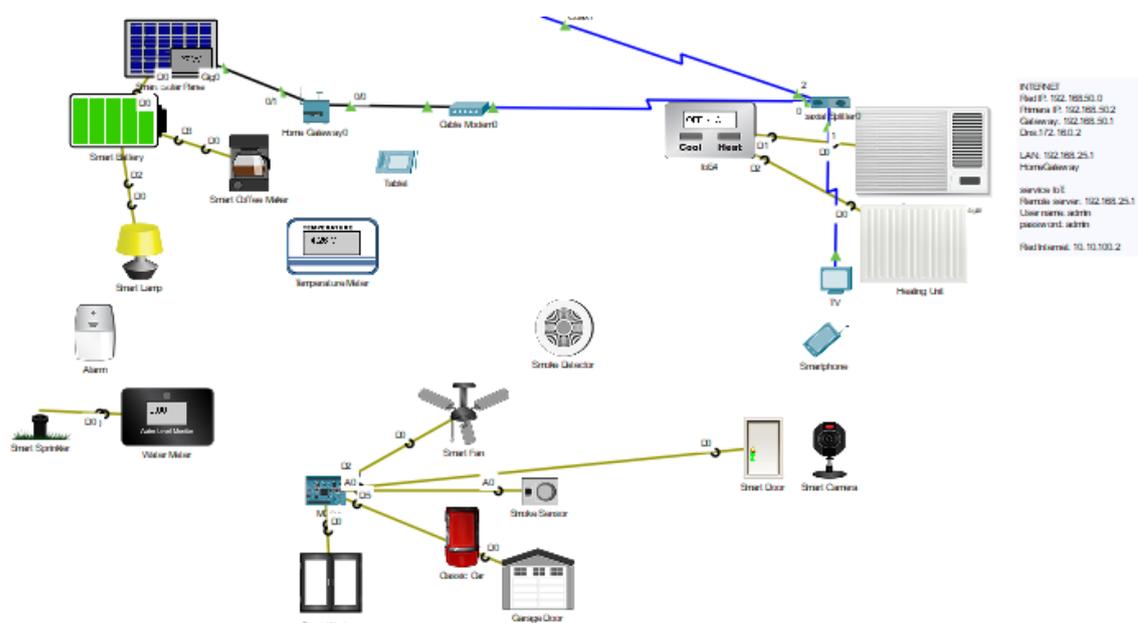


Figura 26. Red Smart Home

El Internet del IoT está en crecimiento acelerado a nivel mundial, y se debe estar preparado para cuando empiece el despliegue en Ecuador; con las herramientas tecnológicas que se disponen se puede comprender un poco más a fondo del funcionamiento, aplicaciones, virtudes y los alcances que se pueden lograr con la plataforma del Internet de las Cosas, pensando en el bienestar de la sociedad.