PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

MÁSTER EN TECNOLOGÍAS DE LA INFORMACIÓN CON MENCIÓN REDES DE COMUNICACIONES

TEMA:

"DISEÑO Y SIMULACIÓN DE UNA RED DOMÓTICA APLICANDO PROTOCOLOS DE SEGURIDAD EN LA RED DE ÁREA LOCAL"

AUTOR:

DONALD PATRICIO CÓRDOVA GARCÍA

QUITO – ECUADOR

2023

APROBACIÓN DEL TUTOR

En mi carácter de Director (a) – Tutor (a) del Trabajo de Posgrado, presentado por el maestrante DONALD PATRICIO CÓRDOVA GARCÍA, con Cédula de Identidad N.º 091923659-6, para optar al Grado de Magíster en Tecnologías de la Información mención en Redes de Comunicaciones, considero que dicho Trabajo de Investigación reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte de los Lectores – Evaluadores que se designen para tal fin por parte de las autoridades de la Facultad de Ingeniería.

En la ciudad de Quito, a los 06 días de agosto de 2023

Charles Escobar Terán

C.I. 1202812549

cescobar637@puce.edu.ec

NOTA:

Se comunica que en el servicio de análisis Turnitin, el referido trabajo de titulación alcanzó el siguiente resultado: 3 % índice de similitud con otras fuentes.

Turnitin: Incluir hoja del informe con el porcentaje

Tesis_Cordova Donald

INFORME DE ORIGINALIDAD

3%	4%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

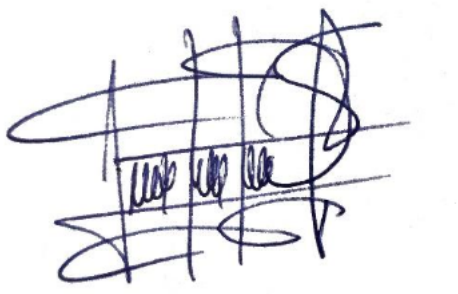
FUENTES PRIMARIAS

1	repositorio.ug.edu.ec Fuente de Internet	1%
2	Submitted to Pontificia Universidad Catolica del Ecuador - PUCE Trabajo del estudiante	1%
3	repositorio.puce.edu.ec Fuente de Internet	1%
4	repositorio.uta.edu.ec Fuente de Internet	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo, Donald Patricio Córdova García, portador de la cédula de ciudadanía número 091923659-6, bajo juramento que el presente trabajo de titulación previo a la obtención del título de MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN REDES DE COMUNICACIONES es de mi total autoría, y que se ha respetado las diferentes citas como fuentes bibliográficas que respaldan este trabajo.



Donald Patricio Córdova García

CI: 0919236596

DEDICATORIA

A mis queridos padres y hermanos, no tengo palabras suficientes para agradecerles todo lo que han hecho por mí a lo largo de los años. Su presencia ha sido mi mayor apoyo y la razón por la que siempre he seguido adelante en los momentos más difíciles. Desde el fondo de mi corazón, quiero dedicarles todo mi éxito, todo mi amor y toda mi gratitud. Han sido mi mayor inspiración, mi guía y mi fuerza. Son el motor de mi vida y siempre estaré en deuda con ustedes y su generosidad, paciencia y amor incondicional.

AGRADECIMIENTO

Deseo expresar un enorme agradecimiento a todas las personas que fueron parte de lograr este objetivo, este sueño tan significativo para mí. Agradezco sinceramente todo el apoyo, palabras de ánimo, los conocimientos compartidos y consejos brindados con dedicación.

Quiero extender mi gratitud a mi familia, en particular a mis padres, quienes con sus sabios consejos fueron el impulso inicial y mi constante motivación. Agradezco su paciencia y comprensión, y, sobre todo, el amor incondicional que me han brindado.

Quiero agradecer a la Pontíficia Universidad Católica del Ecuador, por brindarme la posibilidad de proseguir con mi educación, compartir conocimientos y experiencias que nos brindaron los docentes a lo largo de este proceso.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Los avances tecnológicos nos han permitido ver los cambios que se producen con el tiempo, así como el “Internet of Things” (Internet de las cosas), un avance que desde que comenzó se halla en contínua evolución, estando bastante próspero y aprovechado por las personas, aunque pareciera que no existe problema alguno, hay algo que por desconocimiento presenta inconvenientes y es la seguridad en las redes. Por esta razón, en este proyecto de titulación se llevará acabo un diseño y simulación de una red IoT en un entorno doméstico aplicando ciertos protocolos de seguridad en la red LAN y esto permitirá disminuir la amplia variedad de amenazas que afectan a los dispositivos que utilizan este desarrollo tecnológico y garantizar frente a posibles infiltraciones una mayor seguridad.

Palabras claves: Redes, IOT, Riesgos, Seguridad, Protocolos.

Capítulo 1

Introducción

1.1 Justificación

El diseño de una red IOT en un hogar y aplicando protocolos de seguridad, permitirá dar más control de los equipos a su usuario, evitando así sólo hacer una configuración básica predeterminada por los fabricantes quienes no demuestran preocupación por proveer una seguridad adecuada, sino sólo en funcionalidad.

Al modelar la red de IOT se puede identificar cualquier riesgo que pueda aparecer en la red antes de implementarlo en el mundo real. Esto le permite tomar medidas para prevenir futuros ataques y mejorar la seguridad de su hogar o negocio.

Un buen diseño y simulación permitirá explorar diferentes parámetros y configuraciones para maximizar el rendimiento de la red, lo que puede ayudar a reducir costos y garantizar la conectividad y la seguridad.

Una red doméstica puede recopilar información valiosa de su hogar u oficina. El uso de protocolos de seguridad de la red ayudará a proteger la privacidad de estos datos y garantizará que solo las personas autorizadas tengan acceso a ellos.

1.2 Planteamiento del Problema

La fabricación de dispositivos inteligentes se hace con una rapidez constante, limitando la seguridad y priorizando la usabilidad. Todo esto el usuario muchas veces desconoce y no sabe cómo se transmiten o usan los datos de los dispositivos que tiene en su hogar. En caso de que un atacante acceda a la red y produjera un ciberataque podría resultar en una pérdida de datos importantes almacenados en los dispositivos de la LAN, también el ataque podría interrumpir los

servicios, además la introducción de virus o programa maligno en la red LAN y dispositivos IOT esto podría extenderse a otros dispositivos afectando su funcionamiento y seguridad.

Además si logran acceder a la red se tendría una pérdida de control de los dispositivos IOT y el atacante podría tener control de ellos, también se lograría daños a la reputación de los equipos que se vean comprometidos perdiendo así la confianza de sus clientes.

El uso de cámaras conectadas a redes IoT puede causar varios problemas con la seguridad, pueden ser vulnerables a los ciberataques y utilizarse como puerta de entrada a internet, lo que permite a los atacantes acceder a otros dispositivos conectados a la red o robar información privada, incluyo se podría ver y grabar lo que visualiza la cámara en ese instante, lo que provocaría una vulnerabilidad de la privacidad a el usuario, hogar o negocio.

En muchas ocasiones no es posible conseguir de forma gratuita entornos de simulación, o vienen muy limitados para su uso.

Conocer cómo diseñar en los diferentes entornos de simulación es algo difícil, ya que algunos necesitan imágenes binarias que no son tan accesibles.

Las redes LAN de los hogares no siempre están protegidas, sólo hay configuraciones básicas y se desconoce ciertos niveles de la red que el atacante puede conocer y penetrar en la red del usuario.

1.3 Objetivos

1.3.1 Objetivo General

- Diseñar una red IOT de un entorno doméstico aplicando protocolos de seguridad para garantizar la seguridad ante posibles infiltraciones.

1.3.2 Objetivos Específicos

- Revisar la información bibliográfica para identificar los protocolos de seguridad que se deben configurar en una red IOT.
- Identificar el entorno de simulación adecuado para una red IOT a través de estudios bibliográficos.
- Diseñar una red IOT doméstica en el entorno de simulación considerando los protocolos de seguridad previamente identificados.
- Evaluar los niveles de seguridad en una red LAN para una red IOT para evitar posibles infiltraciones.

1.4 Metodología

Inicialmente se realizará una revisión bibliográfica de los protocolos de seguridad que se necesitan en una red con dispositivos IOT. Para establecer ciertos protocolos más utilizados en estos ámbitos y sus limitaciones, así como las tendencias y los desafíos actuales.

Para realizar una simulación de una red IOT, se realizará una revisión bibliográfica de los diferentes entornos de simulación y después de una comparativa y evaluación elegir el más idóneo.

En el marco teórico se revisarán referencias de documentos científicos en los cuales se encuentre información necesaria para el desarrollo del proyecto, además de la definición de conceptos esenciales dentro del presente trabajo.

Dentro de la red IOT, la experimentación que se realiza implica la simulación de diferentes escenarios y situaciones de vulnerabilidad de la red y observar cómo reacciona frente a esas situaciones, así se puede monitorear la actividad en la red, revisar los registros de acceso y uso de los dispositivos. A través de la observación se puede identificar los comportamientos

irregulares en la red y detectar las posibles vulnerabilidades que se presenten, lo que nos permitirá aumentar la confiabilidad de los resultados.

A partir de los requisitos ya previamente identificados se diseñaría el entorno IOT, esto implica la selección de los protocolos de seguridad adecuados y configurarlos de tal manera que se minimice el riesgo de las intromisiones dentro de la red y aumentar la protección de datos de los dispositivos conectados.

Finalmente se evalúa el rendimiento de la red y se identifica si hay alguna posible área para mejorar u optimizar. Se podrían hacer ajustes en la configuración o introducir nuevos elementos de seguridad para una mayor protección.

Capítulo 2

Marco Teórico y Conceptual

2.1 Antecedentes o Marco Referencial

Gélvez Luis y Santos Luz en el año 2020 hacen público el artículo “Internet de las Cosas: una revisión de vulnerabilidades, amenazas y contramedidas” en la revista Ingenio en la cual detallan “el estudio basado en una ardua investigación, recopilación de vulnerabilidades y amenazas que normalmente se podrían presentar en entornos IOT, se generaron diferentes propuestas de gestión de la información para asegurarla frente a vulnerabilidades” (Gélvez-Rodríguez & Santos-Jaimes, 2020).

Plaza Kevin en el año 2020 realizó el presente trabajo “Diseño de una red IOT doméstica aplicando protocolos de seguridad para una red LAN el cual detalla que haciendo uso de un diseño de red IOT y aplicando diferentes protocolos de seguridad permitieron minimizar los diferentes tipos de vulnerabilidades que existen en los dispositivos, logrando asegurar la red LAN y que no se vea afectada de posibles amenazas” (Plaza Vera, 2020).

Cárdenas Quintero et al., en el año 2020 realizaron la siguiente investigación "Vulnerabilidad en la seguridad del internet de las cosas en el cual se detalla que después de conocer las vulnerabilidades a las que está expuesta IOT, se buscaron metodologías que contrarresten los peligros existentes" (Cárdenas Quintero et al., 2020).

Luis Estrada Bolívar en el año 2021 realizó el presente trabajo "Confiabilidad de los sistemas de seguridad del hogar inteligente basados en IOT en el cual detalla que, con el fin de obtener información relevante sobre el tema, se realizó una búsqueda de información en diferentes fuentes bibliográficas, se analizaron las brechas técnicas y tecnológicas que se presentan a nivel de seguridad de la información en un hogar inteligente" (Estrada Bolívar, 2021).

David Patiño y Sánchez Galindo en el año 2021 realizaron la siguiente investigación "Las amenazas de seguridad a las que se enfrenta IOT y las soluciones en desarrollo su objetivo es resaltar los principales problemas de seguridad que enfrenta IOT mediante el análisis de cómo estos problemas afectan al usuario, mientras que al mismo tiempo busca soluciones diseñadas para resolver los problemas" (David Patiño & Sánchez Galindo, 2021).

Casarrubias Márquez et al., en el año 2021 publicaron la siguiente investigación "Vulnerabilidades de las redes IOT en la cual se describen las buenas prácticas que se deben considerar en redes IOT durante su implementación para mitigar las amenazas y vulnerabilidades a las que pudieran estar expuestas" (Casarrubias Márquez et al., 2021).

López Naranjo en el año 2022 realizó el presente trabajo "Análisis de amenazas IOT en un sistema domótico en el cual se detalla que el objetivo es analizar las amenazas de IOT que existen en el sistema de automatización del hogar, a través de un enfoque cualitativo y un diseño de prueba previa. Toda esta información recopilada se utiliza como base para el diseño de un

entorno domótico simulado que luego se utiliza para verificar la seguridad del dispositivo IOT y registrar todos los resultados, lo que da como resultado un manual técnico con pasos y buenas prácticas de ciberseguridad que ayudan resolver problemas de seguridad" (López Naranjo, 2022).

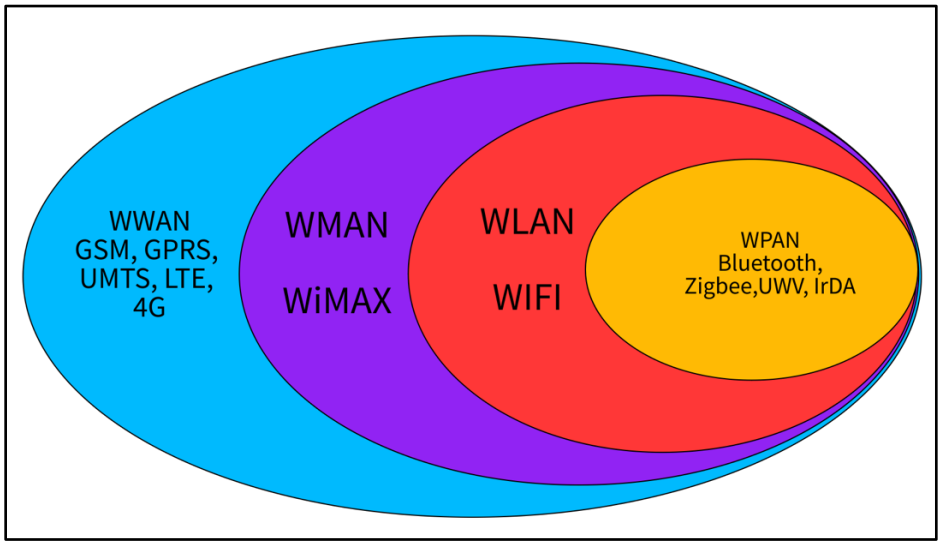
2.2 Marco Teórico

2.2.1 Redes Inalámbricas

Esta definición se utiliza muchas veces en informática con el propósito de distinguir la conexión de nodos por señales electromagnéticas sin recurrir al cableado por puertos (Pipa Huamán, 2019). Los equipos utilizan comunicaciones por radio para enviar datos entre sí. Puede comunicarse directamente con otras computadoras inalámbricas o conectarse a una red existente a través de un AP inalámbrico (Intel.la, 2021).

Figura 1

Diferentes redes inalámbricas existentes



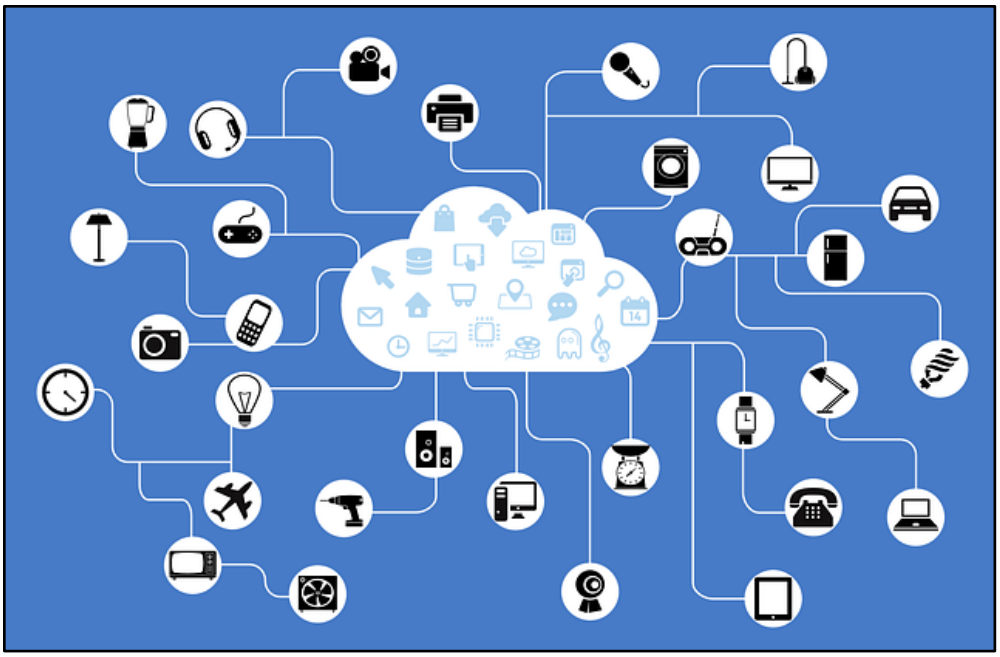
2.2.2 Internet de las Cosas (IOT)

Según Salazar & Silvestre (2017), define al IoT (Internet of things/Internet de las cosas) como una arquitectura en desarrollo que se fundamenta en la internet global, permitiendo el

intercambio de bienes y servicios entre distintas redes dentro de la cadena de suministro. Su impacto en la seguridad y privacidad de los participantes involucrados es significativo (Salazar & Silvestre, 2017).

Figura 2

Esquema del internet de las cosas



2.2.3 Seguridad en la Redes de Internet de las Cosas

Los dispositivos del Internet de las cosas (IoT) son objetos informatizados conectados a Internet, como las cámaras de seguridad en red, los frigoríficos inteligentes y los automóviles con capacidad WiFi. La seguridad del IoT es el proceso de asegurar estos dispositivos y garantizar que no introduzcan amenazas en una red (Cloudflare, 2021).

Dentro de la seguridad IOT existen dos tipos de seguridad, seguridad en la nube y dispositivo, a continuación una definición:

- **Seguridad en la nube:** La seguridad en la nube es una familia de políticas, procedimientos, herramientas y tecnologías de seguridad diseñadas para proteger a los

usuarios, los datos confidenciales, las aplicaciones y la infraestructura en entornos de computación en la nube (Zscaler, 2022).

- **Seguridad en los dispositivos:** La seguridad de los dispositivos móviles se refiere a estar libre de peligro o riesgo de pérdida de activos o datos al utilizar computadoras móviles y hardware de comunicación (IBM, 2022).

2.2.4 Conexión Física de los Dispositivos IOT

Para que la información fluya de los medios físicos a los medios virtuales, los equipos necesitan seguir un procedimiento y, no obstante existen varios ejemplos para constituir un esquema de IoT, sus objetivos son los mismos (Valencia Llerena, 2018).

- **Dispositivos:** son los elementos físicos (hardware), que permite la comunicación con el mundo digital.
- **Puntos de accesos:** facilitan la conexión de los equipos a internet, permitiendo establecer una conexión segura ante fallos.
- **Procesamiento de datos:** para un correcto manejo de un esquema de IOT, éste necesita de la recopilación de data para realizar una adecuada gestión de uso.
- **Aplicaciones:** Muestra la visualización de los datos con opción a modificar parámetros para realizar un determinado comportamiento.

2.2.5 Conexión Lógica de los Dispositivos IOT

La comunicación comienza con un mensaje o información que debe ser enviada de origen a destino regida por los protocolos que deben seguirse para que el mensaje sea entregado y entendido correctamente (Valencia Llerena, 2018).

- **Codificación de mensajes**: Proceso en el que se convierte la información para su comunicación garantizada.

- **Mensaje encapsulado**: En cada trama un mensaje se envuelve para luego proporcionarle un sentido de comienzo a fin.
- **Dimensión del mensaje:** La dimensión debe tener un rago de mínimo 64 bytes y máximo de 1518 bytes para que la comunicación sea clara cuando llegue a su destino.
- **Medición de tiempo de un mensaje**: Señala cuando la comunicación sebe ser iniciada, la velocidad de transmisión y el lapso para aguardar una respuesta.
- **Distribución del mensaje**: Existen varias opciones que pueden realizar este proceso como el broadcast, unicast y multicast.

2.2.6 Protocolos de IOT

Un protocolo para la comunicación, es un conjunto de reglas que definimos con la finalidad de que varios equipos logren intercambiar información y entenderse entre sí. Hay varias maneras de intercambio de información como la M2M (machine-to-machine). El avance que han tenido las telecomunicaciones en el campo del IoT es impresionante y existen algunos requisitos especiales en las formas de comunicación entre dispositivos que no son del todo adecuados (Llamas, 2019).

2.2.6.1 Protocolo ZiggBee. Según el análisis de vulnerabilidades de Ramo Oliveira, 2020) “realizó un estudio sobre las vulnerabilidades del protocolo y la herramienta KillerBee, utilizada para realizar ataques contra redes ZigBee. Se presentan las dificultades de integrar la herramienta con el hardware necesario para realizar los ataques, así como una nueva propuesta que tiene como objetivo estudiar los dispositivos vendidos al por menor, buscando evidencias de que los productos puedan tener problemas de seguridad. El estudio del protocolo presenta características importantes, como un completo sistema de seguridad con claves y algoritmos bien definidos para el ingreso y permanencia en la red. El protocolo está bien documentado, pero es un poco confuso y muy largo, lo que puede ser una desventaja al intentar usarlo” (Ramon De Oliveira, 2020).

2.2.6.2 Protocolo Z-Wave. Según el análisis de Francisco en el 2019 “Este protocolo se hizo popular en la carrera de la automatización de hogar rápidamente porque cubría las mismas necesidades que sus estándares competidores, como 802.15.4 (ZigBee), pero con menos problemas de interoperabilidad y menos interferencias debido a que se encuentra en la banda ISM que suele ser menos problemática que la banda de 2.4 GHz. Entre las características más destacadas de este protocolo está el bajo consumo de sus dispositivos, que pueden durar varios años alimentados por baterías, el alcance de éstos, de hasta 30 metros indoor y hasta 100 metros outdoor, la frecuencia en la que trabajan, que está en la banda ISM o SDR 860 (en Europa 868.42 MHz) y que no tiene interferencias con tecnologías como el Wi-Fi o el Bluetooth” (Francisco et al., 2019).

2.2.6.3 Protocolo Thread. Según la auditoría de seguridad e investigación de protocolos IOT de Vázquez en el 2021 “Thread es un nuevo protocolo de red diseñado para equilibrar y mejorar los estándares inalámbricos existentes en lo referente a aspectos de consumo de energía, seguridad y rentabilidad, y permite la comunicación entre múltiples dispositivos de manera fácil y segura. La pila de Thread está específicamente diseñada para hogares inteligentes y aplicaciones donde se requiere una red basada en IP en la cual se puedan utilizar varias capas de aplicación. La pila solo define la capa de red y transporte (las aplicaciones se ejecutan por encima del protocolo), basándose en el estándar IEEE 802.15.4 para la capa física y MAC” (Vázquez et al., 2021).

2.2.6.4 Protocolo WIFI (802.11). Según en la aplicación de domótica en el contexto IOT investigada por Emilio Longo y Guillermo Juan, 2019 “El estándar 802.11 proporciona una velocidad de transmisión de hasta 2 Mbps en el rango de frecuencia de 2.4 GHz. Utiliza las técnicas de reducción de interferencias conocidas como formatos de unidifusión inalámbrica de tipo FHSS o espectro ensanchado por salto de frecuencia y DSSS o espectro ensanchado por secuencia directa. El estándar 802.11a alcanza unas velocidades de hasta 54 Mbps en el rango de 5 GHz. Utiliza el formato de unidifusión inalámbrica OFDM o multiplexado por división de frecuencias ortogonales. El estándar 802.11b tiene tasas de transmisión entre 5 Mbps y 11 Mbps en la frecuencia de 2.4 GHz y el formato de unidifusión inalámbrica HR/DSSS o multiplexado por secuencia directa de alta tasa” **(Emilio Luis Longo Imedio & Del Barrio -Guillermo Botella Juan, 2019)**.

2.2.6.5 Protocolo 6LoWPAN. Según la investigación de Márquez Peña en el 2021 “El protocolo 6LoWPAN (IPv6 over Low power Wireless Personal Area Network), es una tecnología que está hecha para facilitar el envío de paquetes IPv6 en redes fundamentadas en el estándar IEEE 802.15.4. Además, está diseñada para ser incorporada en sistemas que se caracterizan por su baja tasa de transmisión y acotados recursos. Destaca por hacer una excelente compresión de encabezado, capa de fragmentación y reensamblado y autoconfiguración de direcciones” (Márquez Peña, 2021).

2.2.6.6 Protocolo BacNet. Según la investigación realizada por Meléndez Torres en el 2020 “El protocolo BACnet es un protocolo de comunicación de datos que estandariza las comunicaciones entre equipos electrónicos de automatización de edificios de diferentes fabricantes, lo que permite compartir datos y que los equipos trabajen juntos fácilmente. BACnet define los objetos de datos, sus propiedades y los servicios para la comunicación. A diferencia de otros estándares (como Modbus), este se ha escrito específicamente para sistemas de automatización de edificios, no para sistemas de automatización y control en general. Esto significa que tiene todas las definiciones y tipos de datos necesario facilitando también la documentación y análisis. Su comunicación basada en IP (BACnet/IP) se basa en UDP/IP, mientras que la mayoría de los estándares más seguros de comunicación y autenticación (como TLS y SSH) (en su forma estándar) se basan en TCP/IP” (Meléndez Torres, 2020).

2.2.6.7 Protocolo KNX. Según la investigación de Algarve en el 2021 “El protocolo KNX da la posibilidad de controlar diferentes dispositivos, como iluminación, seguridad, energía gestión, sistemas HVAC, etc. KNX es también el único estándar abierto para residencial y control de edificios y cumple con EN 50090, EN 13321-1 e ISO / IEC 14543. Con el uso de KNX, podemos excluir el uso de sensores y actuadores aislados, haciendo posible la comunicación a través de Internet con todos estos dispositivos. El protocolo tiene desde alrededor de 500 fabricantes, lo que permite una amplia gama de aplicaciones de automatización (KNX, 2020). La arquitectura distribuida del protocolo KNX donde la conexión con los dispositivos de actuación, tales como lámparas o calentadores y la detección de dispositivos, ya que la luminosidad se realiza con un cable de control en paralelo con un cable de 230V. Esto significa que la cantidad de cableado en comparación con la tecnología de instalación convencional se reduce considerablemente cuando los dispositivos de bus están dispuestos de forma descentralizada, aumenta el número de posibles funciones del sistema, y la transparencia de la mejora de la instalación” (Algarve, 2021).

2.2.6.8 Protocolo LonWorks. Según la investigación que realizaron Amaguaya et al. en el año 2019 “El protocolo LonWorks es de bajo estándar y licencia de elevado costo, basado en el modelo de referencia OSI, pertenece a la compañía Echelon. Generalmente se aplica en edificios de oficinas, hoteles e industrias en EE.UU. La raíz principal del protocolo LonWorks es el microcontrolador Neuron Chip elaborado por Motorola y Toshiba. Neuron Chip; posee tres procesadores, dos para que se dé la comunicación, y un tercero para las aplicaciones. LonTalk es el protocolo de comunicación utilizado y en cuanto al medio físico, LonWorks brinda la capacidad de utilizar los siguientes medios de comunicación: infrarrojo, cable coaxial, par trenzado cat. IV de cinco hilos, fibra Óptica, radio frecuencia, power line y RS-232” (Amaguaya Ramos Richard Xavier et al., 2019).

2.2.6.9 Protocolo ModBus. Según la investigación que realizaron Abdelouahab Pereira et al. en el año 2022 “El protocolo ModBus se popularizó mucho en el sector de la automatización industrial debido a que se trata de un protocolo libre y a que su configuración e implementación es sencilla. Actualmente se continúa utilizando en la industria y en instalaciones tanto domóticas como inmóticas con algunas adaptaciones. Modbus se sitúa en los niveles 1, 2 y 7 del Modelo OSI (ISO/IEC 7498-1). Presenta una arquitectura de tipo maestro/esclavo donde el dispositivo maestro solicita información y los dispositivos esclavos se la proporcionan a partir de sus registros. Esto significa que el esclavo no puede ofrecer la información, mientras que el maestro puede leer y escribir en los registros de los esclavos. Una red Modbus estándar tiene 1 maestro y puede tener hasta un máximo de 247 esclavos” (Abdelouahab Pereira et al., 2022).

2.2.7 Lista de Control de Acceso

En un entorno donde existe una gran cantidad de dispositivos conectados a la red, en el cual habrá una gran cantidad de tráfico de datos entrantes y salientes. Esto produce una congestión del ancho de banda, que luego afecta la transmisión de datos primordiales. Para ayudar a la red se puede aplicar políticas de "lista de control de acceso" (ACL) en los dispositivos de red para determinar la prioridad de los datos en tránsito (ManageEngine, 2021).

Se tiene dos tipos de lista de control de acceso:

- **ACL Standard:** son aquellas que efectúan el filtrado, permitiendo o denegando inspeccionando la IP de origen. Cada ACL de este tipo lo podremos numerar de un rango que podrá ir de 1-99 o 1300-1999 (Echave, 2015).
- **ACL Extend:** pueden llevar a cabo el filtrado considerando la IP de origen, la de destino, y los puertos. Los rangos para identificar estas ACLs van de 100 a 199 y de 2000 a 2699 (Echave, 2015).

2.2.8 Red de Área Local Virtual

VLAN es un segmento lógico más pequeño dentro de una gran red física cableada. Siempre que estén conectadas entre sí en la misma LAN, es posible combinarlas. No existe ningún inconveniente si la LAN abarca varios switches. Lo que importa es que el switch también sea compatible con la VLAN (IONOS, 2019).

Cuando el switch se divide en vlan, tiene dos tipos de puertos:

- **VLAN basada en puertos:** se implementa en pequeñas redes y se implementa solo en un solo conmutador, también se puede configurar en varios conmutadores. Es decir, los puertos del 1 al 3 del primer conmutador y el puerto 1 del segundo conmutador se pueden

conectar juntos en la misma VLAN. Sin embargo, esto requiere conectar los conmutadores con dos cables para tener una conexión separada para cada VLAN (IONOS, 2019).

- **VLAN etiquetada:** la asignación a las VLAN es más flexible. Se denomina de manera similar a las redes basadas en puertos como en marcos. En la tarjeta hay información sobre la VLAN que está utilizando, así un conmutador puede reconocer en qué segmento se está comunicando y reenviar el mensaje en consecuencia (IONOS, 2019).

2.2.9 Simuladores de IOT

2.2.9.1 Simulador Packet Tracer. Según el trabajo realizado de Chicaiza, 2020 “el software Packet Tracer es un simulador que permite crear redes complejas y comprobar que el diseño de la red cumple los requerimientos de la empresa, además brinda opción de simular una red IoT con microprocesadores y la configuración del servidor DHCP para que puedan ser reconocidos en el servidor IoT” (Chicaiza, 2020).

2.2.9.2 Simulador OMNET++. Según la investigación realizada por Cachago 2019 “OMNET++ es un software libre de simulación de red de eventos discretos, módulos y orientado a objetos. Proporciona una infraestructura de componentes y herramientas para simular modelos de redes, estos modelos se ensamblan en base a componentes denominados módulos y se los pueden usar de manera combinatoria como bloques Lego” (Cachago, 2019).

2.2.9.3 Simulador NS2. Según la investigación realizada por Kumar & Singh en el año 2022 “NS2 es un simulador de eventos discretos diseñado e implementado para la investigación de redes. Brinda soporte sustancial para la simulación utilizando protocolos TCP, UDP, enrutamiento y multidifusión. Cubre la comunicación por cable e inalámbrica entre los nodos de la red. Hay varios parámetros que son críticos para medir el comportamiento benigno y consistente de los nodos en una red” (Kumar & Singh, 2022).

2.2.9.4 Simulador TOSSIM.

Según la investigación realizada por Iqbal en el año 2021 ”TOSSIM es un simulador de eventos discretos para simular aplicaciones IoT/WSN desarrollado en lenguaje NesC sobre la plataforma TinyOS. TOSSIM ofrece modelos de ruido y propagación de señal basados en implementación real, proporcionando así una simulación realista de aplicaciones IoT basadas en TinyOS” (Iqbal et al., 2021).

2.3 Alcance

La profundidad del presente trabajo de titulación llegará hasta la simulación de un esquema de red IOT hogareño empleando protocolos de seguridad en la red de área local, si los resultados son los esperados, se podrá determinar que los protocolos usados pueden ser de mucha ayuda para evitar posibles infiltraciones dentro de la red local.

Para el cumpliento del objetivo específico uno, se realizará un estudio exploratorio que permitirá recolectar información de los diferentes protocolos de seguridad existentes, para esto se revisará fuentes como el internet, bibliotecas virtuales, fichas nemotécnicas y bibliográficas.

Para el cumplimiento del objetivo dos, se realizará un estudio exploratorio que me permita conocer el número de simuladores, compararlos y escoger el más adecuado para realizar la simulación, para esto se revisará fuentes de internet y las bibliotecas virtuales.

Para el cumplimiento del objetivo tres, se realizará un estudio descriptivo que permitirá conocer el número de dispositivos activos, número de conexiones entre dispositivos, número de protocolos de tráfico de la red para esto se usará una computadora portátil que tendrá el software packet tracer.

Para el cumplimiento del objetivo cuatro, se realizará un estudio explicativo que permitirá conocer el número de protocolos de seguridad a implementar, para esto se usará una computadora portátil que tendrá el software packet tracer.

Capítulo 3

Diseño de la Propuesta

3.1 Revisión Bibliográfica para Identificar los Protocolos de Seguridad que se deben Configurar en una Red IOT

3.1.1 Comparativa de protocolos IOT

De acuerdo a la revisión bibliográfica desarrollada en el marco teórico se puede identificar varios protocolos de seguridad que se deben configurar para el desarrollo de la red IOT que se revisarán en este acápite, se hará una comparativa entre diferentes protocolos y se establecerá el que posea las características más apropiadas.

Tabla 1

Análisis de protocolos IOT

Protocolo	**Licencia**	**Facilidad de implementación**	**Documentación**	**Curva de aprendizaje**	**Seguridad**	**Total**
ZiggBee	1	3	2	3	5	14
Z-Wave	1	3	3	3	5	15
Thread	1	3	3	3	4	14
WIFI (802.1)	1	2	2	2	4	11
6LoWPAN	1	3	3	3	3	13
BacNet	1	3	2	3	3	12

KNX	1	3	3	3	3	13
LonWorks	1	3	3	3	3	13
Modbus	1	3	3	3	4	14

Tipos de licencia	**Implementación, documentación, aprendizaje, seguridad**
1. No tiene	1. Sencillo
2. Privativa	2. Fácil
3. Freeware	3. Medio
4. CC	4. Difícil
5. Libre	5. Complejo

Se realizó una comparativa entre varios protocolos de seguridad para determinar cuál es el más adecuado. Como se puede observar el protocolo WIFI (802.1), ofrece una fácil implementación, hay mucha información en la red, su curva de aprendizaje es fácil y posee buena seguridad, esto hace que no sea tan complicada su usabilidad, además con las configuraciones necesarias se puede conectar de manera remota.

3.2 Entorno de simulación para una red IOT a través de estudios bibliográficos

3.2.1 Comparativa de simuladores IOT

En el presente trabajo de titulación hay que determinar qué tipo de entorno de simulación se utilizará para el desarrollo de la red IOT, para lo cuál se hizo la revisión bibliográfica que está detallada en el marco teórico y aquí se presentan los diferentes simuladores para poder establecer el que posea las características más apropiadas.

Tabla 2

Análisis de modelos virtuales para diseñar una red IOT

Simuladores	Rendimiento	Información	Facilidad de uso	Escalable	Total
TOSSIM	5	2	4	3	14
NS2	5	3	3	2	13
OMNETT++	5	2	4	3	14
Packet Tracer	5	4	2	4	15

Rendimiento, información, facilidad de uso, escalable.

1. Muy bajo
2. Bajo
3. Medio
4. Alto
5. Muy alto

Se realizó una comparativa entre varios simuladores para establecer cuál de ellos es el más adecuado. Se puede observar que Packet Tracer ofrece una gran facilidad de diseño y una interoperabilidad entre diferentes fabricantes, lo que muchos otros simuladores no permiten debido a su distribución limitada y uso de software propietario. Además, el programa ofrece suficiente información para llevar a cabo diferentes implementaciones o diseños de red, lo cual resulta en una ventaja adicional.

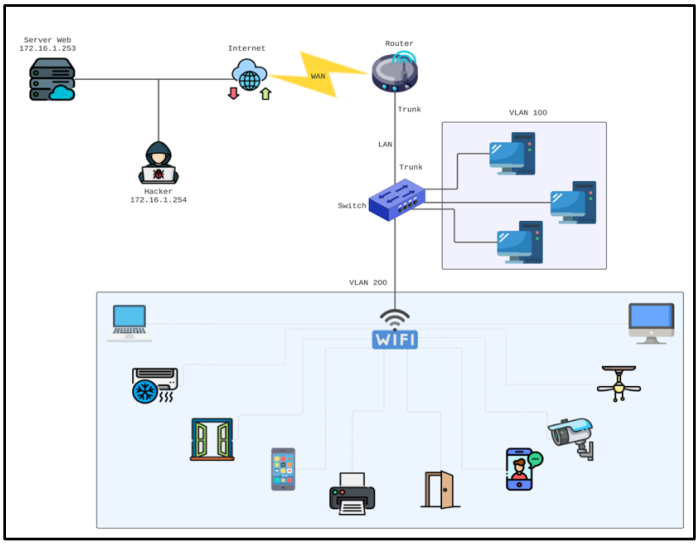
3.3 Diseñar una Red IOT Doméstica en el Entorno de Simulación Considerando los Protocolos de Seguridad Previamente Identificados

Después de haber analizado y comparado con detalle los diferentes protocolos y simuladores a utilizar para realizar el presente trabajo de titulación, se presenta el diseño IOT que estará simulado conforme a los procedimientos establecidos en redes y hacking. Para lo cual se elaboró el diseño en la aplicación web Lucidchart, debido a su facilidad en la creación de entornos de manera fácil e interactiva para luego simularlo en el software Packet Tracer. La configuración que se implementará será detallada a continuación:

- Realizar subnetting para la red Wireless.
- Realizar la segmentación de la red con vlans diferentes de hogar y visitante.
- Direccionar las vlans para un mayor control mediante un único servidor DHCP en el enrutador.
- Implementar el protocolo dot1Q en las vlan tal como se define en el estándar.
- Llevar a cabo la configuración elemental de los dispositivos.
- Usar lista de control de acceso (ACL) para definir el permiso o bloqueo de las redes al internet.
- Desactivar los protocolos que podrían ser vulnerados (CDP - LLDP).
- Usar port-security para el bloqueo de puertos específicos.

Figura 3

Diseño de red IOT en Lucidchart

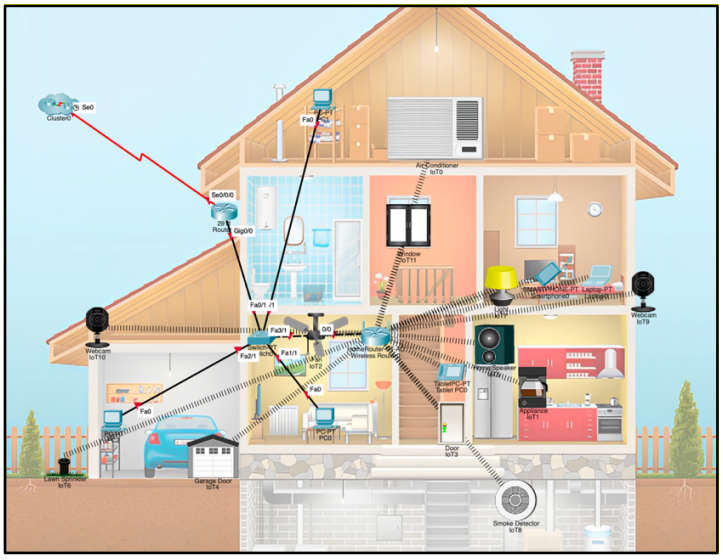


3.3.1 Diseño de la de red IOT propuesta.

Después de determinar los elementos a realizar en este proyecto de titulación y haber diseñado el diagrama físico en LucidChart, se lleva a cabo la realización del diseño en Packet Tracer del diagrama lógico de la red IOT.

Figura 4

Diseño de la red IOT en Packet Tracer



Continuando con la propuesta se hace la utilización de varias capas de seguridad definidas a nivel de redes, para de esta manera prevenir algún tipo de ataque tanto interior como exterior, lo que conlleva a ocasionar un riesgo si no posee las precauciones adecuadas en la red.

Debido a las funcionalidades que se aplican en el presente trabajo posibilitará disminuir el riesgo potencial en una red IoT doméstica.

Antes de realizar el proyecto, se necesita iniciar con una configuración básica de los equipos, lo que permite aumentar la seguridad del dispositivo para que no se vea afectado por limitaciones o problemas cotidianos. Dentro del diseño establecido anteriormente hay equipos que necesitan una configuración previa:

- **Switch**: Este componente del diseño de red se encarga de dividir los dominios de transmisión en varios vlans para evitar el ataque de "storm de transmisión". También se utiliza para la seguridad de puertos, lo que permite la conexión de equipos con parámetros determinados y la deshabilitación de protocolos los cuales pueden incitar amenazas si están encendidos, como es el caso de ARP Spoofing.
- **Router**: Este dispositivo se encarga de rutear dispositivos situados entre distintas subredes o en la web, así como el protocolo dot1Q, lo que permite la existencia de vlans diferentes y encapsuladas. También se crean direcciones fijas para la conexión a la web y se utilizan reglas de ACL para determinar qué equipos se encuentran admitidos al interior de una red, lo que causa un bloqueo de la transmisión de infomación.
- **Access Point:** El punto de acceso tiene una función en modo bridge, lo que permite transferir los datos de una vlan de acceso y utilizarlos como un puente cristalino, lo que permite que los equipos inalámbricos se dividan en diferentes dominios de transmisión.

Además, de tener protocolos de seguridad está configurado con dos bandas de frecuencias.

- **End Point:** Son dispositivos finales como computadores, tabletas, smartphones, entre otros. Que permiten la conexión a través de una configuración superior como Router y el Switch.
- **Equipos IoT:** Son dispositivos que poseen ciertos sensores, actuadores y hasta controladores para poder interactuar dentro de la red y mejorar los procesos que normalmente tardan mucho en completarse.

Después de explicar el desarrollo, se hará la configuración fundamental de un dispositivo, comenzaremos por el Switch por medio de línea de comandos y todos los cambios realizados aquí afectarán directamente al kernel y los procesos del equipo.

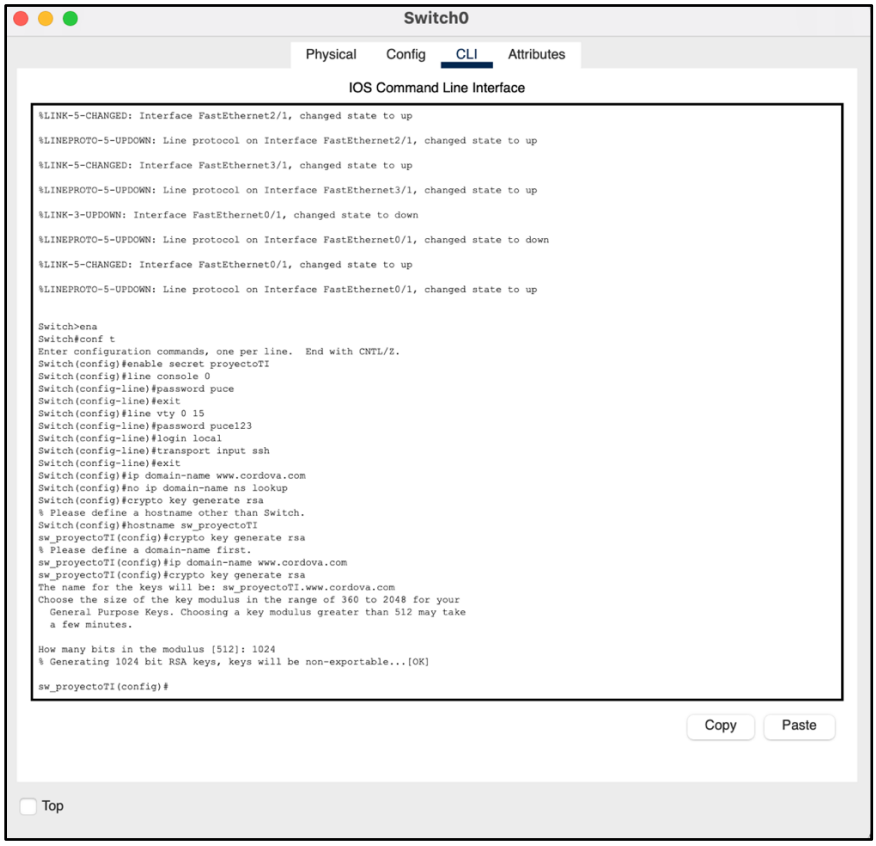
3.3.2 Acceso no autorizado

Todos los comandos empleados tienen como objetivo evitar el acceso del atacante a la red doméstica en los equipos no autorizados. Los comandos que se utilizan a continuación están de manera ascendente, a partir del más fundamental hasta el más complicado.

La instrucción “configure terminal” permite cambiar la forma de administración fundamental a una forma de configuración superior, donde cualquier cambio que se realice genera algún efecto de configuración que puede arriesgar el dispositivo, por lo que sólo alguien capacitado puede acceder. Por lo tanto, el acceso sólo es permitido a aquellos que cumplan con el reconocimiento requerido mediante sus credenciales.

Figura 5

Configuración del switch en Packet Tracer



Es fundamental destacar que hay varias maneras en las que un usuario puede acceder a la configuración y generar una afectación en la red IOT. Una de estas formas es la autenticación local, que también permite conectarse de manera remota. Si no se implementan las medidas de seguridad indispensables, el diseño de la red podría verse seriamente comprometido.

El usuario que use el puerto de consola para acceder de forma física al equipo, debe conocer la configuración de usuario y contraseña para garantizar que la persona sea la correcta. De lo contrario, la entrada será limitada y la red IoT se resguardará de cualquier intromisión causada por personas presentes en el lugar. Para lograrlo, se requieren la implementación de comandos específicos, los cuales se enumeran a continuación:

Tabla 3

Configuración del switch, para acceder al equipo

Comandos	Descripción
Line console 0	Autoriza el ingreso por consola al nivel de administración
Password	Establece una contraseña para mejorar la seguridad
Exit	Regresa al modo anterior de configuración

Para que el usuario pueda acceder de forma remota a un equipo debe configurar las condiciones de acceso mediante una VPN o por el protocolo SSH. El uso de SSH concede que todo tráfico transite a través de la red pública o privada cifrando la información, es decir, que nadie puede intervenir en estos paquetes porque se utilizan cifrados tipo asimétricos. Es esencial implementar este mecanismo de seguridad para determinar quién puede acceder a la configuración, lo que permitirá realizar modificaciones sin necesidad de estar físicamente en el hogar, haciendo de esto una gran ventaja para la administración de la red IOT, a continuación, se seguirán detallando los comandos de la imagen anterior:

Tabla 4

Comandos básicos de configuración en el switch

Comandos	Descripción
Line vty 0 15	Cuantía de enlaces remotos en la red mediante SSH
Password	Contraseña que se elija para cuando se ingrese de manera remota a la red y logre darle acceso
Transport input ssh	El usuario podrá ingresar a la administración del equipo de manera segura a través del protocolo SSH

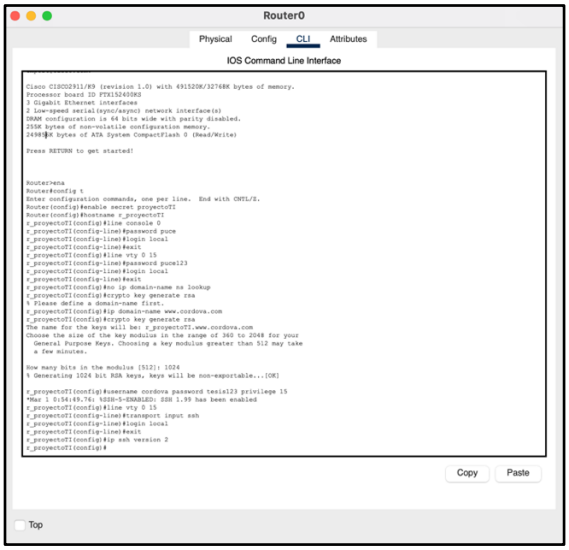
Ip domain-name www.cordova.com	Este comando define nombre un dominio predeterminado que completa nombres de host no calificados.
Hostname	Cambia el nombre del dispositivo, esto ayuda a identificar qué equipo se está conectando a internet
Crypto key generate rsa	El siguiente comando crea un cifrado asimétrico que genera dos tipos de claves: una pública y privada. El uso de este tipo de encriptación es más seguro y agrega mayor nivel de complejidad a la clave para evitar ser hackeada
Ip ssh version 2	Especifica el grado de seguridad
Username cordova password puce123 privilege 15	Para que el usuario pueda ingresar a la administración remota del equipo se debe validar un usuario con su respectiva contraseña además del nivel de privilegio donde 1 es bajo y 15 es alto

El proceso de configuración que se realizó anteriormente con el switch se debe realizar con el router, se adjunta evidencia del proceso.

De la misma manera que en el proceso anterior hay cómo establecer la cantidad de sesiones que pueden estar operativas simultáneamente y se puede acceder de manera remota y gracias a esto tener un mayor control de aseguramiento de la red IOT.

Figura 6

Configuración del router en Packet Tracer

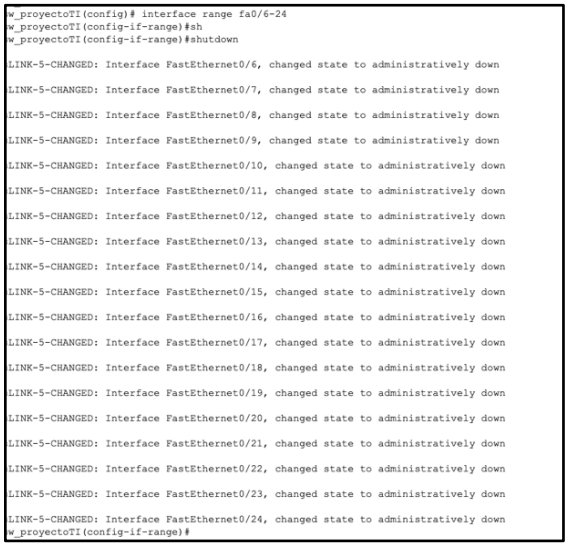


3.3.3 Desactivar interfaces que pueden ser vulnerados

La desactivación de todas las interfaces no utilizadas es otra precaución de seguridad imprescindible para el proyecto de investigación actual, lo que evita que un atacante desde la red interna se enlace a un puerto y provoque un problema, como se muestra a continuación:

Figura 7

Deshabilitar interfaces sin uso del switch en Packet Tracer



A continuación, se ha decidido desactivar algunas interfaces que no están siendo usadas del switch, esto es una buena práctica para limitar cualquier tipo de intromisión en la red interna o también externa ante un ciberataque.

La administración de los equipos cisco es la casi similar en todas las versiones por lo cual es una diferencia mínima en cuanto a la lista de comandos, es decir que lo que se haga en esta versión de Packet Tracer puede ser replicado en la interfaz de línea de comandos, haciendo una configuración estándar y nada compleja para que cualquier usuario que desee implementar seguridades dentro de la red IOT lo haga sin inconvenientes.

Cuando el proveedor del servicio de internet deja los equipos con una configuración preestablecida y lista para su uso, es importante establecer qué red o redes se van a utilizar como una aplicación de políticas básicas. El generar diferentes subredes relacionadas, ayuda a separar el tráfico y así lograr que las redes situadas en distintas locaciones para que no puedan tener comunicación a menos que encuentren cierto protocolo de enrutamiento que lo acepte. En el presente proyecto se procedió dividir el tráfico tanto de la red hogar como la red inalámbrica, todo esto con el propósito de dividir los dominios de broadcast e incrementar la cuantía de espacio de direcciones, lo cual ayuda a defender las redes de un ataque MIT (hombre en el medio) y hasta de sniffing, debido a que mientras más direccionamiento haya dentro de la red, más complejo se hace el encontrar que IP vulnerar.

Para dividir el tráfico en dos subredes se hará uso del estándar 1918 de clase C establecido por la RFC para el uso interno IOT de la red privada:

192.168.100.X - 255.255.255.0

192.168.200.X - 255.255.255.0

La conexión cableada hará uso de la primera dirección en sus dispositivos y eso trae mayor ancho de banda, para el otro direccionamiento se usarán en dispositivos inalámbricos para los IOT como otros que necesiten la conexión. Para poder hacer un buen diseño se debe tener en consideración algunos aspectos:

- El nombre de la red en la que se colocarán cada dispositivo según el tipo de conexión que manejen.
- Direcciones IP para establecer comunicación ya sea con asignación estática o dinámica.
- Establecer un broadcast que ayudará a que todos los dispositivos contesten las peticiones.

Tabla 5

División en subredes

Red	IP	Broadcast	Tipo
192.168.100.0/24	192.168.100.1 – 192.168.100.254	192.168.100.255	Cable
192.168.200.0/24	192.168.200.1 – 192.168.200.254	192.168.200.255	Inalámbrico

3.3.4 Seguridad en las Vlans y Broadcast

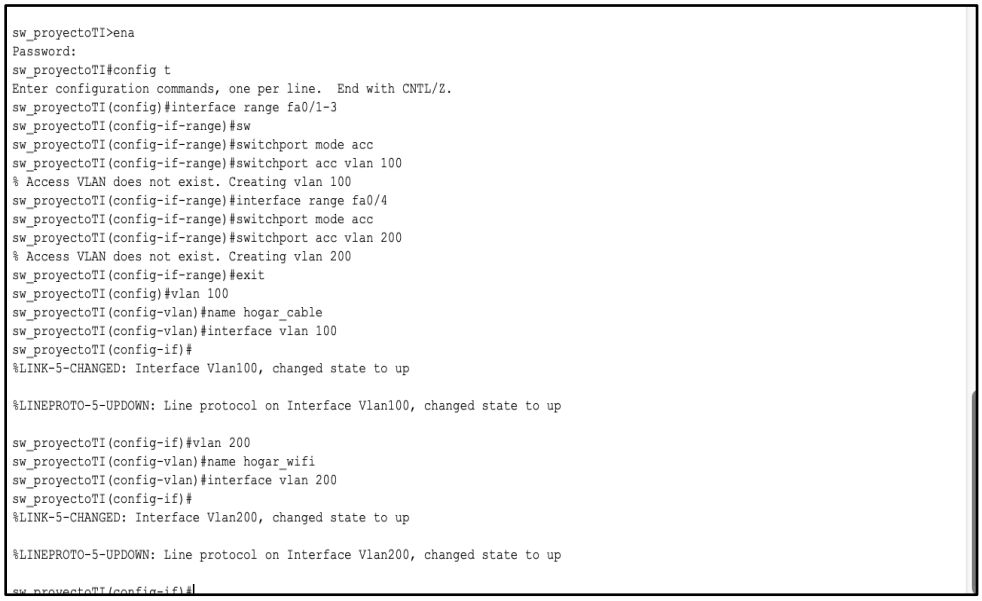
Después de generar las subredes y elegir la IP que se va utilizar, se realiza la creación de Vlans en las cuales funciona el direccionamiento IP específico, para que tenga los diferentes beneficios .

- No se necesita un router para dividir las redes.
- Ayuda con la seguridad en la red
- El broadcast se ve con menos dominios.

El uso de vlans hace que si sucede un ataque en una de ellas la otra se mantenga intacta porque no hay comunicación.

Figura 8

Configuración de las VLANs en Packet Tracer



```
sw_proyectoTI>ena
Password:
sw_proyectoTI#config t
Enter configuration commands, one per line.  End with CNTL/Z.
sw_proyectoTI(config)#interface range fa0/1-3
sw_proyectoTI(config-if-range)#sw
sw_proyectoTI(config-if-range)#switchport mode acc
sw_proyectoTI(config-if-range)#switchport acc vlan 100
% Access VLAN does not exist. Creating vlan 100
sw_proyectoTI(config-if-range)#interface range fa0/4
sw_proyectoTI(config-if-range)#switchport mode acc
sw_proyectoTI(config-if-range)#switchport acc vlan 200
% Access VLAN does not exist. Creating vlan 200
sw_proyectoTI(config-if-range)#exit
sw_proyectoTI(config)#vlan 100
sw_proyectoTI(config-vlan)#name hogar_cable
sw_proyectoTI(config-vlan)#interface vlan 100
sw_proyectoTI(config-if)#
%LINK-5-CHANGED: Interface Vlan100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, changed state to up

sw_proyectoTI(config-if)#vlan 200
sw_proyectoTI(config-vlan)#name hogar_wifi
sw_proyectoTI(config-vlan)#interface vlan 200
sw_proyectoTI(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

sw_proyectoTI(config-if)#
```

Tabla 6

Comandos usados para crear VLANs en Packet Tracer

Comandos	**Descripción**
Interface range	Establece un rango específico de puertos para configurar
Vlan xxx	Se establece un número deseado para esa vlan
Name	Se coloca un nombre a la vlan
Switchport mode acc	Configura el puerto en modo acceso, sólo se usará para conectar un dispositivo final y se le asignará una vlan.
Switchport acc vlan xxx	Este comando se utiliza para asignar un puerto específico a una VLAN particular.

La configuración que se está haciendo se debe realizar en cada Vlan que se desee crear dentro de la red, al realizar todo esto, es como que internamente se dividan en 2 redes

independientes, esto nos permite no hacer solicitudes de respuesta entre una vlan y otra, también se puede crear una vlan sólo para invitados, separándolos de las redes importantes del hogar, esto hace más segura la arquitectura de red.

3.3.5 Comunicación del Protocolo Dot1Q

Debido a que las vlans separan el tráfico y no tienen comunicación entre sí, se necesita de alguna forma para intercambiar datos, por lo cual se hace uso del protocolo Dot1Q, el cual haciendo las respectivas configuraciones puede enviar tráfico de las diferentes vlans a través de un equipo de capa 3.

Figura 9

Configuración troncal de la vlan en Packet Tracer

```
sw_proyectoTI(config)#interface gi0/1
sw_proyectoTI(config-if)#switchport mode trunk
sw_proyectoTI(config-if)#switchport trunk native vlan 99
sw_proyectoTI(config-if)#
```

Tabla 7

Comandos para configurar una Vlan troncal en Packet Tracer

Comandos	**Descripción**
Interface	Establece un rango específico de puertos para configurar
Switchport mode trunk	Con este comando se puede detallar, que a través de ese puerto circulará el tráfico de varias vlans.
Switchport trunk native vlan	Este comando puede establecer una vlan que va ser la que administre las otras.

Después de realizar lo anterior, se realizó las siguientes configuraciones dentro del router para que los procesos dentro del vlan se puedan administrar y configurar dentro de CLI, además

se crea algunas interfaces dentro de la fundamental con el objetivo de asignar una IP fija de las vlans anteriormente creadas con el fin de que los dispositivos que se encuentran en nivel de capa 2 envíe paquetes a la subinterfaz que ayudará con la comunicación e incluso con la conectividad en la red.

Figura 10

Configuración de protocolo dot1Q en Packet Tracer

```
r_proyectoTI(config)#interface gi0/0.100
r_proyectoTI(config-subif)#no sh
r_proyectoTI(config-subif)#no sh
r_proyectoTI(config-subif)#no shutdown
r_proyectoTI(config-subif)#sh
r_proyectoTI(config-subif)#shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/0.100, changed state to administratively down
r_proyectoTI(config-subif)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/0.100, changed state to down
r_proyectoTI(config-subif)#no shutdown
r_proyectoTI(config-subif)#interface gi0/0.100
r_proyectoTI(config-subif)#no shutdown
r_proyectoTI(config-subif)#encapsulation dot1q 100
r_proyectoTI(config-subif)#ip add 192.168.100.1 255.255.255.0
r_proyectoTI(config-subif)#no sh
r_proyectoTI(config-subif)#interface gi0/1.200
r_proyectoTI(config-subif)#ip add 192.168.200.1 255.255.255.0

% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vLAN.

r_proyectoTI(config-subif)#encapsulation dot1q 200
r_proyectoTI(config-subif)#ip add 192.168.200.1 255.255.255.0
r_proyectoTI(config-subif)#no sh
r_proyectoTI(config-subif)#exit
r_proyectoTI(config)#interface gi0/0.99
r_proyectoTI(config-subif)#encapsulation dot1q 99 native
r_proyectoTI(config-subif)#no sh
r_proyectoTI(config-subif)#exit
r_proyectoTI(config)#
```

Tabla 8

Comandos para configurar protocolo dot1Q

Comandos	**Descripción**
Interface gi0/0.xx	Para configurar una subinterfaz hay que primero acceder a la misma, de preferencia usar el mismo id de la vlan.
Encapsulation dot1q	Este comando determina un id de la vlan que va a ser enrutado.
Ip add net mask	Este comando ayuda a establecer una dirección ip que funcione como puerta de enlace en el grupo de vlan.
Encapsulation dot1q xx native	Establece una vlan que sirve para administrar

Después de las configuraciones realizadas, se procede a crear pool de direcciones dinámicas para ayudar a diferenciar si se conecta a la red inalámbrica y al hogar. Para esta configuración se debe establecer en el router que se hará la encapsulación a través del protocolo 802.1Q, a continuación se muestran los comandos.

Figura 11

Direccionamiento tipo pool para las dos VLANs

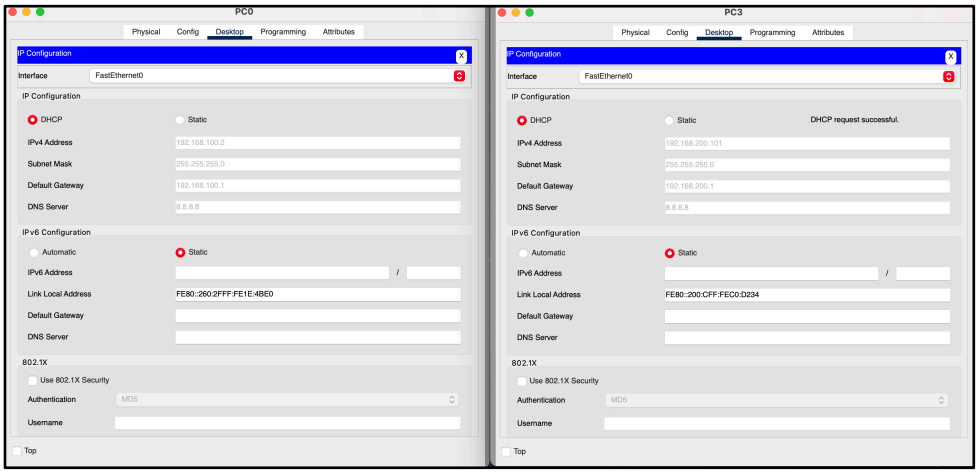
```
r_proyectoTI(config)#ip dhcp pool invitados
r_proyectoTI(dhcp-config)#net
r_proyectoTI(dhcp-config)#network 192.168.200.0 255.255.255.0
r_proyectoTI(dhcp-config)#default-router 192.168.200.1
r_proyectoTI(dhcp-config)#dns-server 8.8.8.8
r_proyectoTI(dhcp-config)#domain-name www.cordova.com
r_proyectoTI(dhcp-config)#exit
r_proyectoTI(config)#ip dhcp pool hogar
r_proyectoTI(dhcp-config)#network 192.168.100.0 255.255.255.0
r_proyectoTI(dhcp-config)#default-router 192.168.100.1
r_proyectoTI(dhcp-config)#dns-server 8.8.8.8
r_proyectoTI(dhcp-config)#domain-name www.cordova.com
r_proyectoTI(dhcp-config)#exit
r_proyectoTI(config)#
```

3.3.6 Direccionamiento IP Dinámico en las Vlans

Para realizar la asignación de direcciones ip se realiza un proceso realizado entre el servidor y un equipo que requiere la ip, para así poder conectarse y comunicarse con los otros dispositivos que estén en la red u otra subred, aquí se establece que tanto la red cableada como inalámbrica tengan una dirección dinámica.

Figura 12

Asignación DHCP en las dos VLANs



Después de comprobar que el direccionamiento funciona correctamente en cada dispositivo en las diferentes vlans, se procede aplicar protección en la red IOT para prevenir cualquier tipo de vulnerabilidad.

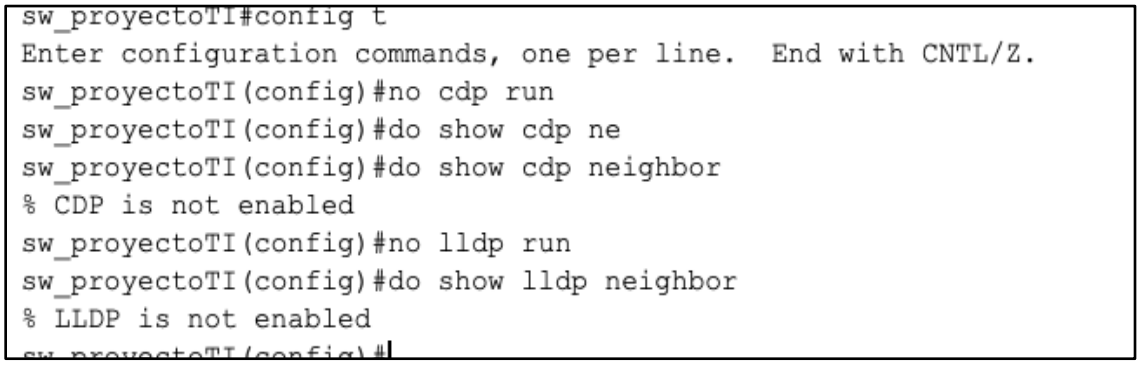
3.3.7 Deshabilitar los protocolos CDP y LLDP

Cuando se adquiere dispositivos normalmente vienen con una configuración de fábrica, que fácilmente si no se cambian las configuraciones se pueden vulnerar los equipos e ingresar a la red. Por lo tanto hay que establecer una red IOT con ciertos grado de seguridad y activar o desactivar lo que no se está utilizando dentro de la red.

En este caso el protocolo CDP y LLPD son los que ayudan hacer un rastreo de los dispositivos conectados a un router o switch, aquí se halla información importante como: direcciones mac, conexión de puertos, plataforma, version del SO del equipo.

Figura 13

Comandos usados para deshabilitar los protocolos CDP y LLDP



Como se aprecia en la figura, se acaban de desactivar los protocolos y gracias a esto el nivel de seguridad aumentó un poco, previniendo ataques que se puede realizarse a través de un software libre llamado Yersenia, ya que el mismo puede causar ataques a los protocolos mencionados haciendo que la red baje su rendimiento y hasta lo más probable que no esté disponible por completo.

3.3.8 Desactivar el protocolo DTP

El siguiente protocolo facilita la creación de enlaces troncales y además ayuda al envío de vlans en un solo enlace, esto es un beneficio en la red, pero al mismo tiempo ocasiona que cualquier puerto habilite una conexión con el switch para la creación de una troncal, tanto así que se podría analizar las tramas mediante un ataque de tipo Vlan Hopping. Para deshabilitar el siguiente protocolo se utiliza el siguiente comando que se presenta a continuación.

Figura 14

Deshabilitar el protocolo DTP

```
sw_proyectoTI(config)#interface range fa0/6-24
sw_proyectoTI(config-if-range)#sw
sw_proyectoTI(config-if-range)#switchport nonegotiate
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
sw_proyectoTI(config-if-range)#
```

3.3.9 Configuración del router inalámbrico

Los equipos inalámbricos se deben conectar de una forma correcta a la vlan 200, por lo cual se necesita de una configuración con ciertos datos a continuación:

- El router debe estar en conexión tipo Wireless AP, esto hará que funcione como si fuera un switch, donde solo pasarán datos de la vlan 200.
- Configurar las redes inalámbricas de 2.4GHz y 5GHz.
- Colocar una contraseña y tipo de cifrado, se eligió el uso de WPA2 con encriptación tipo AES, las cuales se componen de complejos algoritmos

Figura 15

Configuración del tipo de conexión a internet

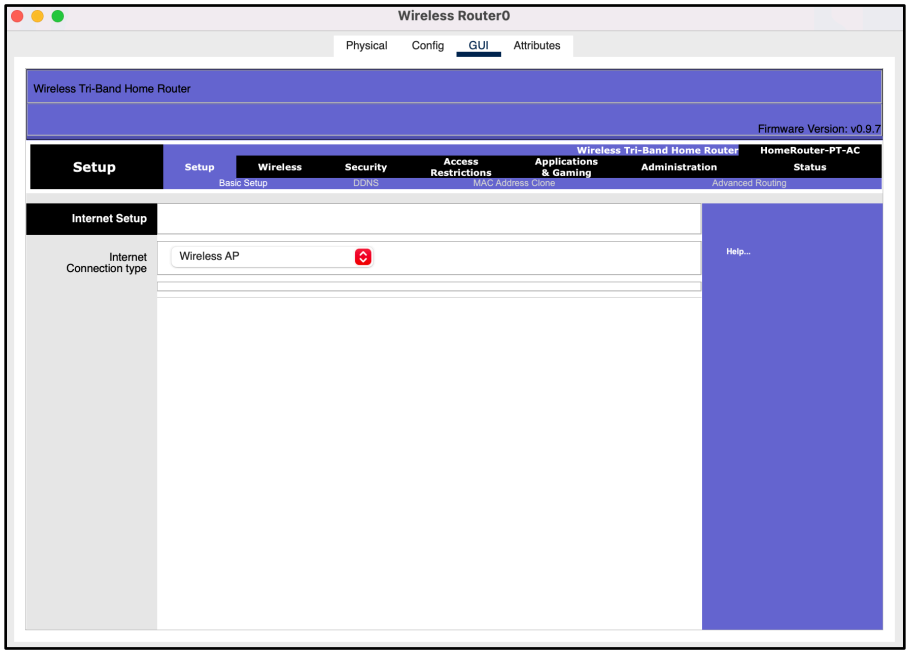


Figura 16

Configuración inalámbrica básica de seguridad

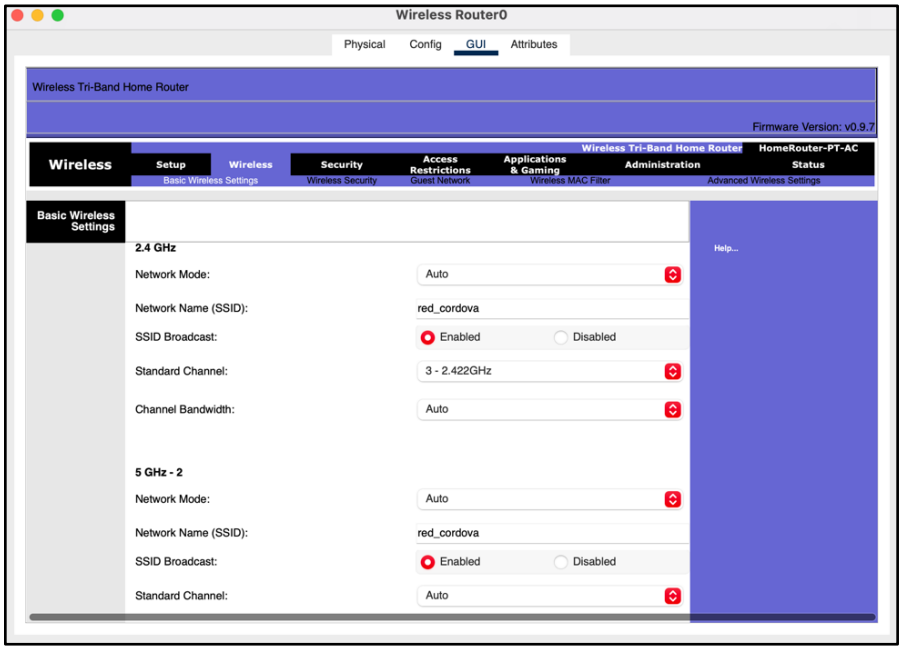
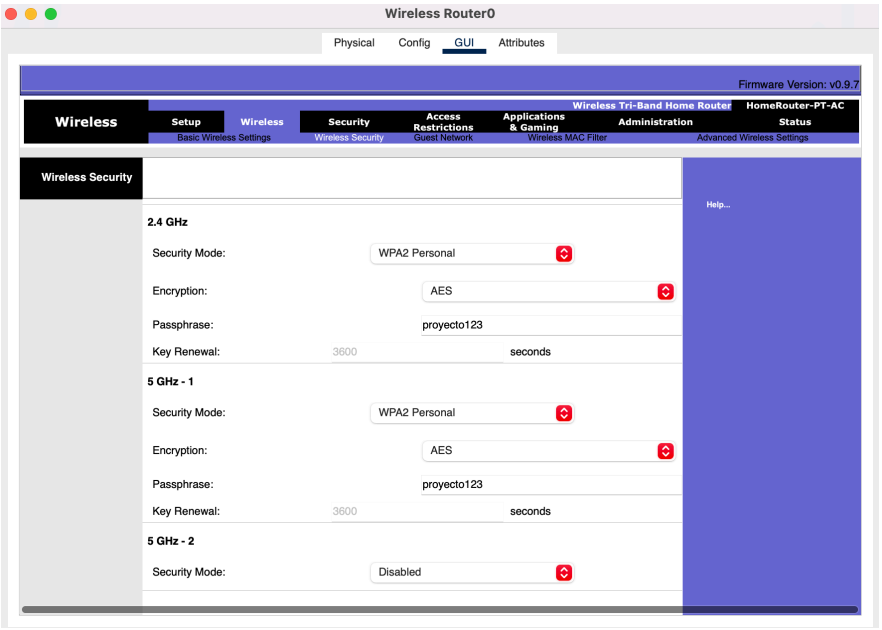


Figura 17

Configuración básica de modo de seguridad



3.3.10 Listas de Control de Acceso

Las listas de control nos ayudan a crear ciertas normas para el bloqueo de tráfico a la entrada o salida de la red, así está más seguro cuando esté navegando por internet. Estas ACL funcionan como si fuesen un firewall y a su vez puede filtrar el tráfico y aplicar medidas cautelares.

Para crear normas de ACL hay que hacerlo en el dispositivo que se encarga de la administración, toda esta configuración se debe hacer de manera global para que los cambios se generen en la memoria. Hay que establecer varios puntos antes de realizar la configuración:

- Primero hay qué establecer a que dispositivo se le va aplicar los ALC, luego colocar un número que lo identifique dentro de un rango 1-99.
- Después hay que señalar que tipo de función colocar (permit, deny, any), las cuales permiten el tráfico, lo bloquean o selecciona respectivamente.

- Luego buscar la dirección de red, establecer la máscara de bits y verificar cuantos equipos se les va colocar los ACL.
- En el CLI colocar el comando “ip access-group x x” las x se reemplazan con el número de ACL establecido con antelación y colocar si es entrada o salida (in-out).

Para realizar los pasos anteriores en el presente proyecto se establecen los siguientes puntos a considerar en tema de seguridad los cuales son:

- Dar permisos de conectividad de entrada a la ip 192.168.100.0 0.0.0.255.
- Dar autorización de conexión a toda la red inalámbrica 192.168.200.0.
- Bloqueo de cualquier otra conexión que no esté en los puntos establecidos.

Figura 18

Configuración y aplicación de los ACL

```
r_proyectoTI(config)#access-list 1 permit 192.168.100.0 0.0.0.255
r_proyectoTI(config)#access-list 1 permit 192.168.200.0 0.0.0.255
r_proyectoTI(config)#access-list 1 deny any
r_proyectoTI(config)#interface gi0/0
r_proyectoTI(config-if)#ip access-group 1 in
r_proyectoTI(config-if)#exit
r_proyectoTI(config)#do show access-list 1
Standard IP access list 1
    permit 192.168.100.0 0.0.0.255
    permit 192.168.200.0 0.0.0.255
    deny any

r_proyectoTI(config)#
```

Los comandos ingresados para configurar los ACL establece que todos los tramos que hay en la vlan 100 y vlan 200, se conectan con equipos externos de la red. Para saber si las normas ingresadas están correctas se puede realizar una consulta y verificar con el comando “show access-list 1”.

3.3.11 Bloqueo de Puertos

El bloqueo de puertos da un mayor nivel en temas de seguridad y rendimiento, esto ayuda a que no se produzcan ataques realizados por usuarios externos o internos. En el siguiente

proyecto se ha optado por hacer uso de port-security, un protocolo estándar usado por muchos fabricantes de dispositivos, su aplicación en redes es bastante eficiente en sus distintos modos de uso como son:

- El comando “protect”, el cual permite proteger una interfaz de ser desactivada si se excede del límite de direcciones MAC.
- El comando “restrict”, descarta el tráfico de red que quiera pasar por un dispositivo, pero no desactiva la interfaz.
- El comando “shutdown”, protege que ante un intento de vulneración se detenga de inmediato.

Existen ciertos puntos que se deben establecer para poder habilitar port-security y pueda trabajar de manera óptima.

Figura 19

Comandos para configurar port-security

```
sw_proyectoTI(config)#interface range fa0/1-4
sw_proyectoTI(config-if-range)#sw
sw_proyectoTI(config-if-range)#switchport port-security
sw_proyectoTI(config-if-range)#switchport port-security mac-address sticky
sw_proyectoTI(config-if-range)#switchport port-security mac-address violation shutdown
                                                                    ^
% Invalid input detected at '^' marker.

sw_proyectoTI(config-if-range)#switchport port-security violation shutdown
sw_proyectoTI(config-if-range)#switchport port-security maximum 5
sw_proyectoTI(config-if-range)#exit
sw_proyectoTI(config)#do show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        5          0                0         Shutdown
        Fa0/2        5          0                0         Shutdown
        Fa0/3        5          0                0         Shutdown
        Fa0/4        5          1                0         Shutdown
---------------------------------------------------------------------
sw_proyectoTI(config)#
```

Tabla 9

Comandos ingresados para la configuración de port-security

Comandos	**Descripción**
Switchport port-security	Este comando activa port-security.
Switchport port-security mac-address sticky	Este comando hace que el registro de las MAC sea dinámico.
Switchport port-security violation shutdown	Este comando si detecta cualquier intento de violación de seguridad el switch apagará la interfaz intervenida.
Switchport port-security maximun “X”	Este comando determina una cantidad de direcciones MAC registradas y si sobrepasa se excluyen.

3.4 Evaluar los niveles de seguridad de una red LAN para una red IOT, para evitar posibles infiltraciones.

En el diseño, dado que se tiene un enfoque hacia la seguridad, ya se consideraron algunas medidas de seguridad como:

- Bloqueo de puertos.
- Segmentación de la red.
- Deshabilitar protocolos no usados y con vulnerabilidad.
- Control de acceso.

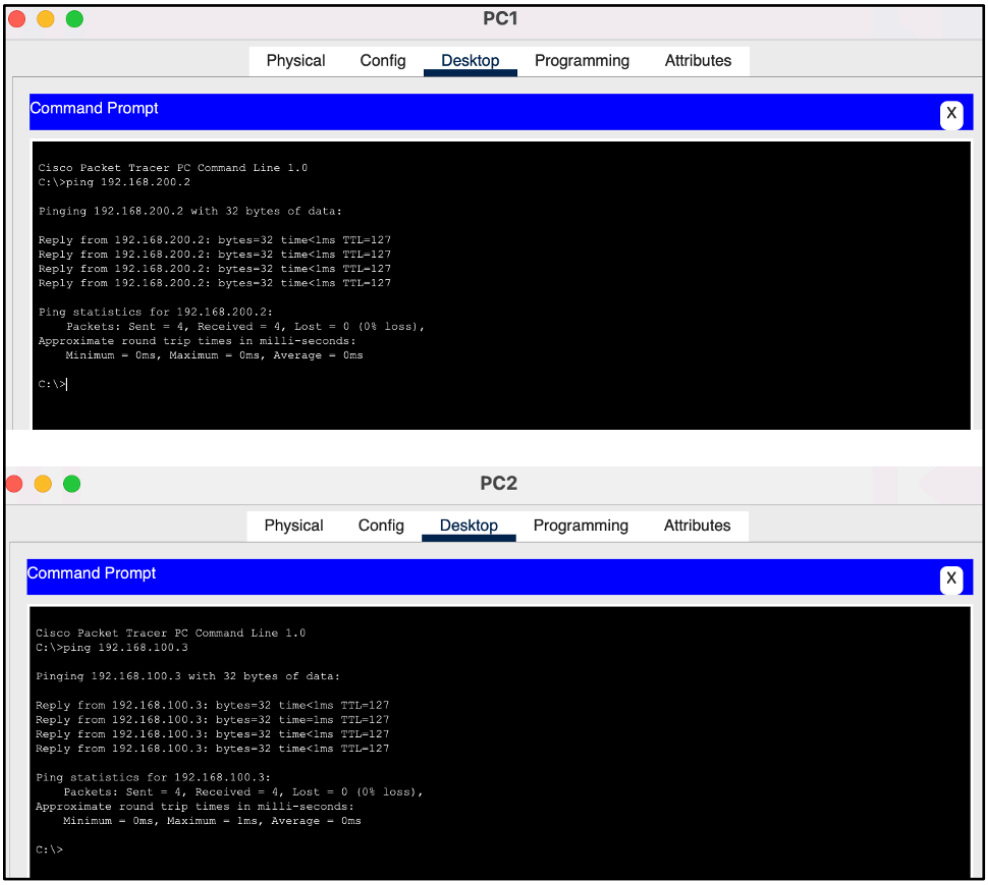
Como complemento a esto en este acápite se revisará cada punto de los antes mencionados.

3.4.1 Verificación de la red y su Conectividad

Para realizar la siguiente verificación de la red y constatar que todo funciona adecuadamente se hará uso del protocolo ICMP, este nos ayudará a verificar si la red está operativa a través de sus solicitudes como son: el echo request y el echo reply, al usar estas 2 solicitudes nos dará un ping el cual nos dice que la conexión entre vlans es la correcta.

Figura 20

Prueba de conectividad entre vlans



3.4.2 Verificar la seguridad de port-security

Para comprobar si el funcionamiento de port-security es el correcto se procede a realizar un envío de paquetes y verificación también de que cumple con la norma de sticky ingresada anteriormente.

Figura 21

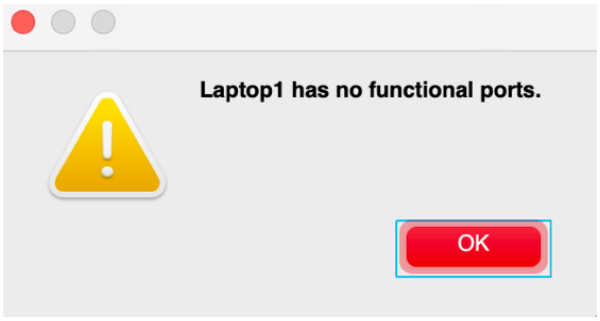
Envío de paquete exitoso

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Printer0	ICMP		0.000	N	0	(...	

Como se acaba de ver el envío del paquete fue exitoso, ahora se procederá hacer un cambio de la impresora por otro dispositivo y se verifica que el mensaje no se envía, porqué port-security está habilitado y muestra el siguiente resultado.

Figura 22

Error al enviar el mensaje



Se cambió la impresora por una laptop y cuando se quiso enviar un mensaje arrojó el siguiente mensaje el cual nos dice que ese puerto no está funcional pese a que con la impresora si funcionaba. Para que vuelva a estar operativo hay que apagar y encender la interfaz, lo que parece un poco molesto pero como se comprobó es bastante ventajoso debido a la protección que genera en la red.

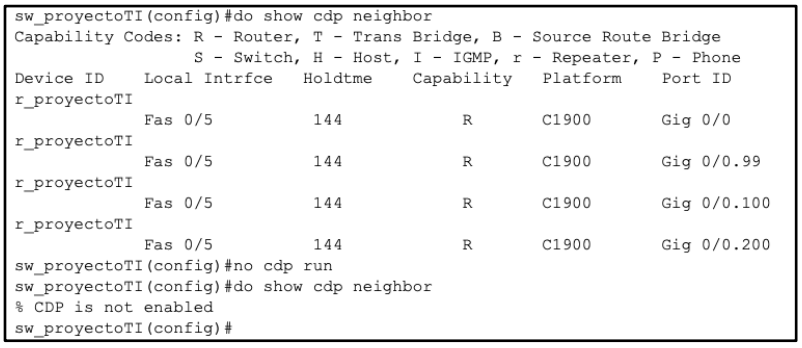
El resultado que nos da este protocolo es para ayudar y evitar que posibles usuarios quieran conectarse a la red sacando el dispositivo que estaba en un inicio y cambiarlo por otro para vulnerar la red IOT.

3.4.3 Verificar desactivación de cierto protocolos

Para realizar la siguiente verificación de ciertos protocolos que pueden ser usado para vulnerar la seguridad de la red como puede ser el protocolo CDP, este trabaja a nivel de capa 2 y permite a los dispositivos de la red descubran y obtengan información de otros equipos conectados en la misma red local, cabe recalcar que esto funciona sólo en los dispositivos de Cisco a menos que otros fabricantes también tengan este protocolo compatible.

Figura 23

Verificación del protocolo CDP

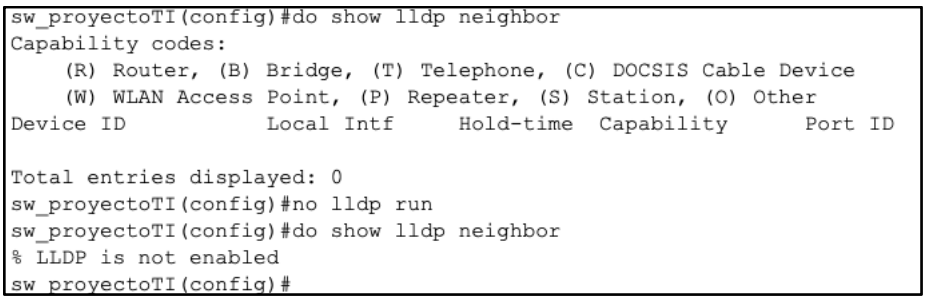


```
sw_proyectoTI(config)#do show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
r_proyectoTI
             Fas 0/5          144            R       C1900       Gig 0/0
r_proyectoTI
             Fas 0/5          144            R       C1900       Gig 0/0.99
r_proyectoTI
             Fas 0/5          144            R       C1900       Gig 0/0.100
r_proyectoTI
             Fas 0/5          144            R       C1900       Gig 0/0.200
sw_proyectoTI(config)#no cdp run
sw_proyectoTI(config)#do show cdp neighbor
% CDP is not enabled
sw_proyectoTI(config)#
```

Otro de los protocolos a verificar es el LLDP, este también trabaja a nivel de capa 2 y permite que los dispositivos compartan información como la identificación, direcciones ip, capacidad, tipo de dispositivo, entre otros. La desactivación de este protocolo y el anterior no afectaría la comunicación básica de la red ya que son independientes las operaciones capa 2 y 3.

Figura 24

Verificación del protocolo LLDP



```
sw_proyectoTI(config)#do show lldp neighbor
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID

Total entries displayed: 0
sw_proyectoTI(config)#no lldp run
sw_proyectoTI(config)#do show lldp neighbor
% LLDP is not enabled
sw_proyectoTI(config)#
```

Dentro del diseño también se requiere deshabilitar el protocolo DTP, el cual facilita la creación de enlaces troncales que permiten el transporte de vlans por un mismo cable. Si está habilitado iniciará un modo de negociación automática, para lo cual es preferible la desactivación por motivos de seguridad para que no se conecten a ninguna de las interfaces libres y así reducir el riesgo de configuraciones no deseadas y posibles ataques maliciosos.

Figura 25

Verificación del protocolo DTP

```
sw_proyectoTI(config)#interface range fa0/6-24
sw_proyectoTI(config-if-range)#sw
sw_proyectoTI(config-if-range)#switchport nonegotiate
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
sw_proyectoTI(config-if-range)#
```

3.4.4 Verificar el control de acceso

Dentro de las configuraciones realizadas también se destaca la creación de ACL, las cuales se utilizan para dejar pasar o negar el paso de paquetes basándose en criterios como son las direcciones IP, número de puertos y tipos de protocolos. Al tener unas reglas establecidas será permitido o denegado en tráfico que se tenga configurado en las listas de control de acceso.

Figura 26

Verificación de ACL ingresados correctamente

```
r_proyectoTI(config)#do show access-list
r_proyectoTI(config)#do show access-list 1
r_proyectoTI(config)#access-list 1 permit 192.168.100.0 0.0.0.255
r_proyectoTI(config)#access-list 1 permit 192.168.200.0 0.0.0.255
r_proyectoTI(config)#access-list 1 deny any
r_proyectoTI(config)#interface gi0/0
r_proyectoTI(config-if)#ip access-group 1 in
r_proyectoTI(config-if)#exit
r_proyectoTI(config)#do show access-list 1
Standard IP access list 1
    permit 192.168.100.0 0.0.0.255
    permit 192.168.200.0 0.0.0.255
    deny any

r_proyectoTI(config)#
```

A continuación se realiza una configuración con respecto a todo el tráfico que provenga del proveedor de servicio de internet 10.10.10.2, también los paquetes que vengan desde el servidor hacia la red diseñada.

Figura 27

Verificación de ACL al proveedor

```
r_proyectoTI(config)#access-list 2 permit 10.10.10.0 255.255.255.0
r_proyectoTI(config)#access-list 2 permit host 10.10.10.2
r_proyectoTI(config)#access-list 2 deny any
r_proyectoTI(config)#interface gi0/1
r_proyectoTI(config-if)#ip access-group 2 in
r_proyectoTI(config-if)#do show access-list 2
Standard IP access list 2
    permit 0.0.0.0 255.255.255.0
    permit host 10.10.10.2
    deny any

r_proyectoTI(config-if)#
```

Una vez realizado lo anterior no permitirá que si un atacante se conecta desde el exterior hacia la red interna tenga acceso. Si se requiere habilitar alguna ACL adicional se lo podría hacer.

Tabla 10

Tabla resumen con los niveles de seguridad encontrados para la red LAN e IOT y evitar posibles infiltraciones

Elemento	Nivel de seguridad	Vulnerabilidad	Acción	Grado de protección
VLAN	Bajo	Acceso no autorizado, problemas de tráfico, escalabilidad baja, confidencialidad comprometida	Se crea vlans que ayudan a la segmentación de red, esto permite mejorar la seguridad, rendimiento y la administración de la red al limitar la comunicación entre dispositivos y agruparlos según las necesidades.	Alto
Port-Security	Bajo	Suplantación de direcciones MAC, conexiones no autorizadas, congestión de tráfico, dificultades en	La activación de este comando permite aplicar medidas de seguridad a un puerto espcīfico y restringir	Alto

		el seguimiento de dispositivos.	la conexión de otros equipos a ese puerto.	
CDP y LLDP	Bajo	Divulgación de información sensible, spoofing, enumeración de dispositivos, exposición de la topología de red	La desactivación de estos protocolos brindan mayor seguridad y privaciodad, pero es importante complementar con la creación de ACL	Alto
DTP	Bajo	Configuración no deseada de enlaces troncales, vulnerabilidades de VLAN hopping, exposición de información sensible.	La desactivación del protocolo DTP brinda beneficios en términos de seguridad y estabilidad de la red, también indica que los enlaces troncales deben configurarse manualmente.	
ACL	Bajo	Ataques DoS, falta de control de accesso basado en políticas,	Se crea ACL para mejorar la seguridad, eficiencia y tener un	Alto

	violación de cumplimiento y regulaciones, acceso no autorizado.	mejor control de la red al implementar políticas de acceso y segmentación de red.

Conclusiones y Recomendaciones

4.1 Conclusiones

- Tener un conocimiento básico sobre cómo configurar los equipos correctamente aplicando protocolos de seguridad en la red IOT minimiza el riesgo a que un agente externo vulnere la red.
- Usar un simulador como Packet Tracer ayuda a diseñar y realizar prácticas en un entorno IOT, además es intuitivo de usar y hay bastante información en la web para poder aprender sobre redes, sin necesidad de comprar equipos físicos.
- Ejecutar protocolos como ACL y port-security ayudan mucho a controlar el tráfico como las interfaces, de esta manera el usuario siente mayor protección al momento de realizar su diseño de red IOT.

4.2 Recomendaciones

- El software de Packet Tracer tiene sus limitaciones en cuanto a la navegación de internet, por lo cual se recomienda realizar esta práctica en un ambiente de emulación donde permita aplicar lo propuesto.
- Se recomienda implementar un sistema de monitoreo y registro de eventos para así detectar si existe actividad sospechosa en la red IOT, esto permitirá tomar medidas preventivas.

- Desactivar servicios o funcionalidades innecesarios de los dispositivos IOT para minimizar los ataques.
- Actualizar regularmente el firmware de los dispositivos, para corregir vulnerabilidades que ya fueron descubiertas.

Bibliografía

Abdelouahab Pereira, B., Tutor, O., Ivars, P., & Francisco, Á. (2022). *Uso de tecnologías IoT y protocolos BACnet para la monitorización y control de climatización*. https://riunet.upv.es/handle/10251/187243

Algarve, U. DO. (2021). *Framework for controlling automation devices based on gestures*. https://sapientia.ualg.pt/handle/10400.1/17786

Amaguaya Ramos Richard Xavier, I., David Salazar Chacón, G., & Gabriela Torres Olmedo, J. (2019). *para la automatización de los servicios, confort y seguridad en los laboratorios de la Carrera de Ingeniería en Sistemas con el Protocolo X10 usando Arduino.* http://repositorio.ug.edu.ec/handle/redug/39769

Cachago, A. C. (2019). *Waypoint y Gauss-Markov de movilidad ipv6 para determinar la calidad de servicio (QoS) en el internet de las cosas (IoT) utilizando software de simulación omnet++.* http://bibdigital.epn.edu.ec/handle/15000/19932

Cárdenas Quintero, D., Ropero Silva, E., Puerto López, K., Sanchez Mojica, K., Castro Casadiego, S., & Ramírez Mateus, J. (2020). Vulnerabilidad en la seguridad del internet de las cosas. *Mundo Fesc*, *10*(19), 162–179.

Casarrubias Márquez, E. A., Castro Domínguez, J. F., Hernández Alarcón, R. F., & Vázquez Galarce, J. (2021). *Vulnerabilidades de las Redes IoT*.

Chicaiza, D. B. (2020). *Diseño de la red internet de las cosas (IOT) en la empresa Roger Sport*. https://dspace.ups.edu.ec/handle/123456789/18932

Cloudflare. (2021). *¿Qué es la seguridad del IoT?* Cloudflare. https://www.cloudflare.com/es-es/learning/security/glossary/iot-security/

David Patiño, D. R., & Sánchez Galindo, E. A. (2021). *Las amenazas de seguridad a las que se enfrenta IoT y las soluciones en desarrollo*.

Echave, E. (2015). *Listas de Control de Acceso (ACL)*. Enredando Con Redes. https://enredandoconredes.com/2015/01/08/acls-listas-de-control-de-acceso/

Emilio Luis Longo Imedio, J., & Del Barrio -Guillermo Botella Juan, A. A. (2019). *Aplicación de domótica en el contexto de IoT*. https://eprints.ucm.es/id/eprint/51613/

Estrada Bolívar, L. B. (2021). CONFIABILIDAD DE LOS SISTEMAS DE SEGURIDAD DEL HOGAR INTELIGENTE BASADO EN IOT. *Trabajo de Investigación Presentada Como Requisito Para Optar Por El Título de Ingeniero En Telecomunicaciones*, 1–11.

Francisco, J., Bernal, B., María, D. :, & Cano Baños, D. (2019). *El protocolo Z-Wave desde la perspectiva de la seguridad*. https://repositorio.upct.es/handle/10317/8283

Gélvez-Rodríguez, L. F., & Santos-Jaimes, L. M. (2020). *Internet de las Cosas: una revisión sobre los retos de seguridad y sus contramedidas*. Revista Ingenio. https://revistas.ufps.edu.co/index.php/ingenio/article/view/2370/2893

IBM. (2022). *¿Qué es la seguridad móvil?* IBM. https://www.ibm.com/ar-es/topics/mobile-security

Intel.la. (2021). *Descripción general de redes inalámbricas*. Información y Documentación Sobre Productos.

IONOS. (2019). *Conceptos básicos de VLAN*. Digital Guide IONOS. https://www.ionos.es/digitalguide/servidores/know-how/vlan/

Iqbal, U., Digital, A. M.-I. J. of C. and, & 2021, undefined. (2021). Efficient and dynamic access control mechanism for secure data acquisition in IoT environment. *Journal.Uob.Edu.Bh*, *10*(1), 2210–142. https://doi.org/10.12785/ijcds/100102

Kumar, A., & Singh, D. (2022). Detection of Security Attacks on Edge Computing of IoT Devices through NS2 Simulation. *Journal of Physics: Conference Series*, *2327*(1), 012016. https://doi.org/10.1088/1742-6596/2327/1/012016

Llamas, L. (2019). *Protocolos de comunicación para IoT*. Www.Luisllamas.Es. https://www.luisllamas.es/protocolos-de-comunicacion-para-iot/

López Naranjo, M. A. (2022). Análisis de amenazas IOT en un sistema domótico. *Proyecto de Investigación Previo a La Obtención Del Título de Magister En Ciberseguridad*.

ManageEngine. (2021). *Lista de control de acceso ACL*. Www.Manageengine.Com. https://www.manageengine.com/latam/network-configuration-manager/lista-de-control-de-acceso-cisco.html

Márquez Peña, R. (2021). *Implementación de una red de sensores inalambricos (WSN) para el Internet de las cosas (IoT) utilizando comunicación 6LoWPAN con nodos con microcontrolador*. https://upcommons.upc.edu/handle/2117/339712

Meléndez Torres. (2020). Asegurar sistemas de automatización y control de edificios contra ataques cibernéticos. *Prcrepository.Org*. https://prcrepository.org/handle/20.500.12475/1065

Pipa Huamán, J. (2019). Redes Inalámbricas. *Monografía*, 1–65.

Plaza Vera, K. J. (2020). Diseño de una red IOT doméstica aplicando protocolos de seguridad para una red LAN. *Trabajo de Titulación Previo a La Obtención Del Título de Ingeniero En Teleinformática*, 1–97.

Ramon De Oliveira, R. (2020). *Análise de vulnerabilidades em redes ZigBee*. https://repositorio.ufsc.br/handle/123456789/218151

Salazar, J., & Silvestre, S. (2017). Internet de las cosas. *Erasmus+*, 1–34. http://www.techpedia.eu

Valencia Llerena, C. A. (2018). *Hacking ético al IOT mediante SDR*. Universidad técnica de Ambato.

Vázquez, A., Directores, V., Purificación, :, & Amigo, C. (2021). *Auditoría de seguridad e investigación de protocolos IoT (Thread y Zigbee)*. https://nootropico.li/files/tfg/TFG_IoT_ZigbeeThread.pdf

Zscaler. (2022). *¿Qué es la seguridad en la nube?* Zscaler. https://www.zscaler.es/resources/security-terms-glossary/what-is-cloud-security

Anexos

Comandos para la Configuración de los Equipos.

Switch:

sw_proyectoTI#show run

Building configuration...

Current configuration : 1879 bytes

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname sw_proyectoTI

!

enable secret 5 1mERr$19X5nldMdxnigClpc587N.

```
!
!
!
ip ssh version 2
ip domain-name www.cordova.com
!
username cordova privilege 1 password 0 puce123 privilege 15
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 100
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 100
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 100
switchport mode access
!
```

```
interface FastEthernet0/4
switchport access vlan 200
switchport mode access
!
interface FastEthernet0/5
switchport trunk native vlan 99
switchport mode trunk
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
```

```
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
```

```
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
```

```
interface Vlan1
no ip address
shutdown
!
interface Vlan100
no ip address
!
interface Vlan200
no ip address
!
line con 0
password puce123
!
line vty 0 4
password puce123
login local
transport input ssh
line vty 5 15
password puce123
login local
transport input ssh
!
End
```

==========

Router:

r_proyectoTI#show run

Building configuration...

Current configuration : 1764 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname r_proyectoTI

!

enable secret 5 1mERr$19X5nldMdxnigClpc587N.

!

ip dhcp pool cableado

network 192.168.100.0 255.255.255.0

default-router 192.168.100.1

dns-server 8.8.8.8

domain-name www.cordova.com

ip dhcp pool inalambrico

network 192.168.200.0 255.255.255.0

default-router 192.168.200.1

```
dns-server 8.8.8.8
domain-name www.cordova.com
!
ip cef
no ipv6 cef
!
username cordova password 0 puce123 privilege 15
!
license udi pid CISCO1941/K9 sn FTX1524X313-
!
ip ssh version 2
ip domain-name www.cordova.com
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
ip access-group 1 in
duplex auto
speed auto
!
interface GigabitEthernet0/0.99
```

```
encapsulation dot1Q 99 native
no ip address
!
interface GigabitEthernet0/0.100
encapsulation dot1Q 100
ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet0/0.200
encapsulation dot1Q 200
ip address 192.168.200.1 255.255.255.0
!
interface GigabitEthernet0/1
ip address 10.10.10.1 255.255.255.252
ip access-group 2 in
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

```
!
ip flow-export version 9
!
access-list 1 permit 192.168.100.0 0.0.0.255
access-list 1 permit 192.168.200.0 0.0.0.255
access-list 1 deny any
access-list 2 permit 0.0.0.0 255.255.255.0
access-list 2 permit host 10.10.10.2
access-list 2 deny any
!
line con 0
password puce123
login local
!
line aux 0
!
line vty 0 4
password puce123
login local
transport input ssh
line vty 5 15
password puce123
login local
```

```
transport input ssh
!
end
```