



**UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA DE INGENIERÍA EN TELEINFORMÁTICA**

**TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN TELEINFORMÁTICA**

**ÁREA
TECNOLOGÍA DE LOS ORDENADORES**

**TEMA
“DISEÑO DE UNA RED IOT DOMESTICA APLICANDO
PROTOCOLOS DE SEGURIDAD PARA UNA RED LAN”**

**AUTOR
PLAZA VERA KEVIN JHONNY**

**DIRECTORA DEL TRABAJO
ING. COMP. CASTILLO LEÓN ROSA ELIZABETH, MG**

GUAYAQUIL, NOVIEMBRE 2020



**ANEXO XI.- FICHA DE REGISTRO DE TRABAJO
DE TITULACIÓN
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:			
Diseño de una red IoT domestica aplicando protocolos de seguridad para una red LAN			
AUTOR(ES) (apellidos/nombres):		Plaza Vera Kevin Jhonny	
REVISOR(ES)/TUTOR(ES) (apellidos/nombres):		Ing. García Torres Ingrid Angélica, MG / Ing. Castillo León Rosa Elizabeth, MG	
INSTITUCIÓN:		Universidad de Guayaquil	
UNIDAD/FACULTAD:		Facultad de Ingeniería Industrial	
MAESTRÍA/ESPECIALIDAD:			
GRADO OBTENIDO:		Ingeniería en Teleinformática	
FECHA DE PUBLICACIÓN:		No. DE PÁGINAS:	
ÁREAS TEMÁTICAS:		Tecnología de los ordenadores	
PALABRAS CLAVES/ KEYWORDS:		IoT, Seguridad, Red, Vulnerabilidades, Amenazas. IoT, Security, Network, Vulnerabilities, Threats.	
<p>RESUMEN/ABSTRACT (150-250 palabras):</p> <p>Con el pasar del tiempo, los diferentes avances de la tecnología nos han permitido experimentar diferentes cambios a favor de la humanidad, es aquí donde entra el Internet de las Cosas o IoT, una tecnología que desde su nacimiento se encuentra en constante cambio, siendo aprovechada por el hombre en diferentes ámbitos, aunque debido a la poca preocupación en cuanto a su seguridad se han presentado diferentes inconvenientes. Por lo cual en el presente trabajo a través de la metodología experimental se realizará el diseño de una red IoT doméstica aplicando ciertos protocolos de seguridad como ACL, VLAN, Port Security, SSH, protocolo dot1Q y además la desactivación de los protocolos CDP Y LLDP que permitirán reducir los diferentes tipos de vulnerabilidades existentes en los equipos utilizados por esta tecnología, logrando que la red LAN no se vea afectada ante posibles amenazas.</p> <p>Along the time, the different advances of technology have allow us to experiment different changes as benefits for the humanity, then, is here the entrance of the Internet of the Things or IoT, a technology that is in constant change since its birth, being used in different fields by the man, however, due to the worry about its security, there have been different inconvenients. Therefore, in the present work through the experimental methodology will be done the design of a domestic IoT network, applying some security protocols like ACL, VLAN, Port Security, SSH, dot1Q protocol and also the deactivation of the CDP and LLDP protocols, that let reduce the different kinds of</p>			

vulnerabilities that exist in the equipments used by this technology, accomplishing that the LAN network does not be affected by possible threats.		
ADJUNTO PDF:	SI (X)	NO
CONTACTO CON AUTOR/ES:	Teléfono: 0980990604	E-mail: kevin.plazav@ug.edu.ec
CONTACTO CON LA INSTITUCIÓN:	Nombre: Ing. Ramón Maquilón Nicola, MG.	
	Teléfono: 593-2658128	
	E-mail: direccionTi@ug.edu.ec	



**ANEXO XII.- DECLARACIÓN DE AUTORÍA Y DE
AUTORIZACIÓN DE LICENCIA GRATUITA
INTRANSFERIBLE Y NO EXCLUSIVA PARA EL USO NO COMERCIAL DE
LA OBRA CON FINES NO ACADÉMICOS**

**FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**

LICENCIA GRATUITA INTRANSFERIBLE Y NO COMERCIAL DE LA OBRA CON
FINES NO ACADÉMICOS

Yo, **PLAZA VERA KEVIN JHONNY** con C.C. No. **2300030547**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es “**DISEÑO DE UNA RED IOT DOMESTICA APLICANDO PROTOCOLOS DE SEGURIDAD PARA UNA RED LAN**” son de mi absoluta propiedad y responsabilidad, en conformidad al Artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, autorizo la utilización de una licencia gratuita intransferible, para el uso no comercial de la presente obra a favor de la Universidad de Guayaquil.

A handwritten signature in blue ink, enclosed in a blue oval, with the text "PLAZA VERA KEVIN JHONNY" and "C.C. No. 2300030547" below it.

PLAZA VERA KEVIN JHONNY
C.C. No. 2300030547



**ANEXO VII.- CERTIFICADO PORCENTAJE DE SIMILITUD
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Habiendo sido nombrado ING. ROSA ELIZABETH CASTILLO LEÓN MG, tutor del trabajo de titulación certifico que el presente trabajo de titulación ha sido elaborado por PLAZA VERA KEVIN JHONNY, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERO EN TELEINFORMÁTICA.

Se informa que el trabajo de titulación: “DISEÑO DE UNA RED IOT DOMESTICA APLICANDO PROTOCOLOS DE SEGURIDAD PARA UNA RED LAN”, ha sido orientado durante todo el periodo de ejecución en el programa Antiplagio URKUND quedando el 1% de coincidencia.

URKUND

Document: Plaza Vera Kevin Jhonny.docx (D97004446)

Submitted: 2021-03-02 10:47 (-05:00)

Submitted by: kevin.plazav@ug.edu.ec

Receiver: rosa.castillo@ug.edu.ec

Message: Revisión de tesis [Show full message](#)

1% of this approx. 28 pages long document consists of text present in 2 sources.

Rank	Path/Filename
1	AltamiranoM_GuerreroM_GuevaraK_JimenezJ_ReveloA.pdf
2	http://www.reuter.com.ar/CCNA/CCNA1/index_todo_ccna1...

Alternative sources

Sources not used

0 Warnings | Reset | Export | Share

Como se muestra en la Figura 1:

Figura 1. Tipos de redes inalámbricas. Información tomada de Google. Elaborado por el autor.

2.2.2. Topologías de Redes Es la forma en la cual se conectan las computadoras para intercambiar información entre sí, tanto de manera física como lógica. CITATION Mar20 \l 12298 (Raffino, 2020). Los diferentes tipos de topologías se muestran en la figura 2.

Figura 2. Tipos de topologías de redes. Información tomada de Google. Elaborado por el autor.

- Topología de bus: se trata de un cable central por el cual pasa la información hacia todas las computadoras de la red.
- Topología de estrella: se basa de un host o punto central hacia los demás nodos de la red.
- Topología de malla: también conocida como topología de trama, se trata de una interconexión de nodos entre sí en donde la información puede viajar por diferentes caminos.
- Topología de anillo: es una red simple en donde las computadoras se encuentran interconectadas en

<https://secure.arkund.com/view/92584910-926934-541692>



Firmado electrónicamente por:

**ROSA
ELIZABETH
CASTILLO
LEON**

ING. ROSA ELIZABETH CASTILLO LEÓN
DOCENTE TUTOR
C.C. 0922372610
FECHA: 05 DE MARZO DE 2021



**ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR
DEL TRABAJO DE TITULACIÓN
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 05 de marzo de 2021

Sr (a).

Ing. Annabelle Lizarzaburu Mora, MG.

Director (a) de Carrera Ingeniería en Teleinformática / Telemática

FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL

Ciudad. -

De mis consideraciones:

Envío a Ud. el Informe correspondiente a la tutoría realizada al Trabajo de Titulación **“DISEÑO DE UNA RED IOT DOMESTICA APLICANDO PROTOCOLOS DE SEGURIDAD PARA UNA RED LAN”** del estudiante **PLAZA VERA KEVIN JHONNY**, indicando que ha cumplido con todos los parámetros establecidos en la normativa vigente:

- El trabajo es el resultado de una investigación.
- El estudiante demuestra conocimiento profesional integral.
- El trabajo presenta una propuesta en el área de conocimiento.
- El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se adjunta el certificado de porcentaje de similitud y la valoración del trabajo de titulación con la respectiva calificación.

Dando por concluida esta tutoría de trabajo de titulación, **CERTIFICO**, para los fines pertinentes, que el estudiante está apto para continuar con el proceso de revisión final.

Atentamente,



Firmado electrónicamente por:

**ROSA
ELIZABETH
CASTILLO
LEON**

ING. ROSA ELIZABETH CASTILLO LEÓN

TUTOR DE TRABAJO DE TITULACIÓN

C.C. 0922372610

FECHA: 05 DE MARZO DE 2021



**ANEXO VIII.- INFORME DEL DOCENTE REVISOR
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 17 de marzo de 2021.

Sr (a).

Ing. Annabelle Lizarzaburu Mora, MG.

Director (a) de Carrera Ingeniería en Teleinformática / Telemática

FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL

Ciudad. -

De mis consideraciones:

Envío a Ud. el informe correspondiente a la REVISIÓN FINAL del Trabajo de Titulación **“DISEÑO DE UNA RED IOT DOMESTICA APLICANDO PROTOCOLOS DE SEGURIDAD PARA UNA RED LAN”** del estudiante **PLAZA VERA KEVIN JHONNY**. Las gestiones realizadas me permiten indicar que el trabajo fue revisado considerando todos los parámetros establecidos en las normativas vigentes, en el cumplimiento de los siguientes aspectos:

Cumplimiento de requisitos de forma:

El título tiene un máximo de 14 palabras.

La memoria escrita se ajusta a la estructura establecida.

El documento se ajusta a las normas de escritura científica seleccionadas por la Facultad.

La investigación es pertinente con la línea y sublíneas de investigación de la carrera.

Los soportes teóricos son de máximo 5 años.

La propuesta presentada es pertinente.

Cumplimiento con el Reglamento de Régimen Académico:

El trabajo es el resultado de una investigación.

El estudiante demuestra conocimiento profesional integral.

El trabajo presenta una propuesta en el área de conocimiento.

El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se indica que fue revisado, el certificado de porcentaje de similitud, la valoración del tutor, así como de las páginas preliminares solicitadas, lo cual indica que el trabajo de investigación cumple con los requisitos exigidos.

Una vez concluida esta revisión, considero que el estudiante está apto para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente,



Firmado electrónicamente por:

**INGRID
ANGELICA
GARCIA
TORRES**

ING. INGRID ANGÉLICA GARCÍA TORRES, MG

C.C: 1308497682

FECHA: 17 DE MARZO DE 2021

Dedicatoria

Dedico el presente trabajo de titulación a mis padres, sin ellos nada hubiera sido posible, gracias por su apoyo incondicional desde el primer día y por ser los mejores padres del mundo, éste logro también es de ustedes.

Agradecimiento

Agradezco a Dios por haberme permitido alcanzar mi meta. A mis padres, hermanas y personas especiales en mi vida quienes siempre me brindaron palabras de motivación para no desmayar en el transcurso de mi carrera universitaria. A mis amigos y compañeros de carrera quienes tambien fueron parte de este proceso y a todos los docentes quienes de una u otra manera me brindaron su ayuda academica.

Índice General

N°	Descripción	Pág.
	Introducción	1

Capítulo I

El Problema

N°	Descripción	Pág.
1.1	Planteamiento del problema	3
1.2	Formulación del problema	4
1.3	Justificación	4
1.4	Objetivos	6
1.4.1	Objetivo general.	6
1.4.2	Objetivos específicos.	6
1.5	Alcance	6

Capítulo II

Marco Teórico

N°	Descripción	Pág.
2.1	Antecedentes del estudio	7
2.2	Fundamentación teorica	8
2.2.1	Redes inalámbricas	8
2.2.2	Topologías de Redes	8
2.2.3	El internet de las cosas	9
2.2.4	Arquitectura IoT	10
2.2.5	Seguridad IoT	10
2.2.6	Proceso de comunicación en dispositivos IoT: Modo físico	11
2.2.7	Proceso de comunicación en dispositivos IoT: Modo lógico	12
2.2.8	Protocolos de comunicación en el IoT	12
2.2.9	Router	13
2.2.10	Switch	13
2.2.11	Servidor	14
2.2.12	Gateway	14
2.2.13	Firewall	14
2.2.14	Subnetting	15
2.2.15	Routing	15
2.2.16	Lista de control de Acceso (ACL)	15

N°	Descripción	Pág.
2.2.16.1	Tipos de ACL	15
2.2.17	Vlan	16
2.2.17.1	Tipos de puertos	16
2.2.18	Vlan Nativa	16
2.2.19	Protocolo 802.1Q	16
2.2.20	CDP	17
2.2.21	LLDP	17
2.2.22	DTP	17
2.2.23	DCHP	17
2.2.24	WPA2	17
2.2.25	SSID	17
2.2.26	FQDN	17
2.2.27	Port Security	18
2.2.28	SSH	18
2.2.29	Packet Tracer	19
2.3	Fundamentación legal	19
2.3.1	Constitución de la Republica del Ecuador	19
2.3.2	Código Orgánico Integral Penal (COIP)	20
2.3.3	Código Orgánico de la Economía Social de los Conocimientos	21

Capítulo III

Propuesta

N°	Descripción	Pág.
3.1	Métodos de investigación	24
3.1.1	Metodología Experimental	24
3.1.2	Metodología Exploratoria	24
3.1.3	Método Descriptivo	23
3.2.	Técnica de recolección de datos	23
3.3	Elementos utilizados para el diseño de la propuesta	25
3.3.1	Simuladores	25
3.3.2	Protocolos para la intercomunicación entre vlans	26
3.3.3	Protocolos de conexión remota en una red doméstica	27
3.4	Esquema general del proyecto	29
3.5	Diseño de la propuesta	30

Nº	Descripción	Pág.
3.5.1	Prevención de acceso no autorizado	32
3.5.2	Desactivación de protocolos que pueden ser vulnerados en redes LAN	36
3.5.3	Seguridad a través de VLANs y división de los Dominios de broadcast	39
3.5.4	Aplicación del protocolo Dot1Q para comunicación Inter Vlan	40
3.5.5	Asignación de direcciones IP dinámica acorde a VLAN	44
3.5.6	Desactivación de protocolos de descubrimiento	46
3.5.7	Desactivación de DTP (Dynamic Trunking Protocol)	47
3.5.8	Configuración de AP en VLAN 200	48
3.5.9	Prueba de conectividad a la red interna	50
3.5.10	Conectividad con server externo	51
3.5.11	Creación y aplicación de ACL	53
3.5.12	Bloqueo de interfaces mediante Port-security	59
3.5.12.1	Configuración de Port-Security	59
3.6	Conclusiones y Recomendaciones	64
3.6.1	Conclusiones	64
3.6.2	Recomendaciones	65
	Anexos	66
	Bibliografía	77

Índice de Tablas

Nº	Descripción	Pág.
1	Comparativa entre simuladores	26
2	Comparativa de protocolos de encapsulación entre Vlans	27
3	Protocolos utilizados para conexión remota	28
4	Configuración de consola para acceso a equipo	34
5	Explicación de comandos para configuración básica	34
6	Separación de redes a través de subredes	38
7	Comandos para creación de Vlans	39
8	Comandos utilizados para la creación de la Vlan troncal	41
9	Comandos utilizados para la configuración Router on a Stick	42

Índice de Figuras

Nº	Descripción	Pág.
1	Tipos de redes inalámbricas	8
2	Tipos de topologías de redes	9
3	Esquema de una red IoT	10
4	Proceso de Conexión IoT en modo físico	11
5	Proceso de Conexión IoT en modo lógico	12
6	Imagen de un Router	13
7	Imagen de un switch	14
8	Imagen de un servidor	14
9	Funcionamiento de un Firewall	15
10	Funcionamiento de una Vlan	16
11	Funcionamiento del Port Security	18
12	Funcionamiento del Protocolo SSH	18
13	Esquema de Red IoT	30
14	Esquema de Red IoT en Packet Tracert	31
15	Configuración básica realizada en Switch Cisco	33
16	Configuración básica del Router	36
17	Configuración básica del Router	36
18	Desactivación de interfaces en el switch	37
19	Configuración de vlans para dividir tráfico de redes	39
20	Configuración de la vlan troncal	41
21	Configuración Router on a Stick en el Router	42
22	Configuración de la vlan nativa en proceso ROAS	42
23	Pool de direccionamiento para la vlan Wireless	43
24	Pool de direccionamiento para la vlan de Hogar	44
25	División de la red Wireless y Hogar	44
26	Asignación de IP dinámica VLAN 100 en PC	45
27	Asignación de IP dinámica VLAN 200 en PC	45
28	Protocolo CDP activado	46
29	Protocolo CDP activado	47
30	Comando para desactivación del protocolo DTP	48
31	Configuración de AP	49
32	Modo de operación de AP	49

Nº	Descripción	Pág.
33	Autenticación WPA2	50
34	Prueba de conectividad a red wifi desde LAN de hogar	51
35	Prueba de conectividad a red hogar	51
36	Ruta estática en Router principal	52
37	Acceso a servicio desde la Red IoT	53
38	Esquema en base atacante y servidor ubicados en Internet	54
39	Configuración de ACL en Router de origen	56
40	Aplicación de ACL en la Interfaz	56
41	Información de las AC	56
42	Comunicación exitosa luego de aplicar ACL	57
43	Aplicación de ACL para tráfico desde la WAN	57
44	IP del atacante ubicando fuera de la red Interna	58
45	Ping sin éxito por parte del atacante	58
46	Configuración de Port-Security	60
47	Configuración de Port-Security	60
48	Ping desde la impresora hasta el garaje	61
49	Comprobación de ping exitoso	61
50	Desactivación de interfaz debido a configuración port-security	62
51	Asignación de IP errónea	62
52	Comportamiento de la interfaz debido a port-security	63
53	Encendido de interfaz de manera manual	64
54	Funcionamiento de port-security al reiniciar la interfaz	64
55	Descarga de Cisco Packet Tracer	68
56	Aceptacion de terminos y condiciones	68
57	Ubicación de la carpeta de almacenamiento	69
58	Instalación del programa	69
59	Programa instalado y en ejecución	70
60	Interfaz gráfica de Cisco Packet Tracer	70

Índice de Anexos

Nº	Descripción	Pág.
1	Preguntas de Entrevista	67
2	Instalacion de Cisco Packet Tracer	68
3	Configuración del Switch	71
4	Configuración del Router	74



**ANEXO XIII.- RESUMEN DEL TRABAJO DE
TITULACIÓN (ESPAÑOL)
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



**“DISEÑO DE UNA RED IOT DOMESTICA APLICANDO PROTOCOLOS DE
SEGURIDAD PARA UNA RED LAN”**

Autor: Plaza Vera Kevin Jhonny

Tutor: Ing. Castillo León Rosa Elizabeth, MG.

Resumen

Con el pasar del tiempo, los diferentes avances de la tecnología nos han permitido experimentar diferentes cambios a favor de la humanidad, es aquí donde entra el Internet de las Cosas o IoT, una tecnología que desde su nacimiento se encuentra en constante cambio, siendo aprovechada por el hombre en diferentes ámbitos, aunque debido a la poca preocupación en cuanto a su seguridad se han presentado diferentes inconvenientes. Por lo cual en el presente trabajo a través de la metodología experimental se realizará el diseño de una red IoT doméstica aplicando ciertos protocolos de seguridad como ACL, VLAN, Port Security, SSH, protocolo dot1Q y además la desactivación de los protocolos CDP Y LLDP que permitirán reducir los diferentes tipos de vulnerabilidades existentes en los equipos utilizados por esta tecnología, logrando que la red LAN no se vea afectada ante posibles amenazas.

Palabras Claves: IoT, Seguridad, Red, Vulnerabilidades, Amenazas.



**ANEXO XIV.- RESUMEN DEL TRABAJO DE
TITULACIÓN (INGLÉS)
FACULTAD DE INGENIERÍA INDUSTRIAL
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



**‘DESIGN OF AN IoT DOMESTIC NETWORK APPLYING SECURITY
PROTOCOLS FOR A LAN NETWORK’**

Author: Plaza Vera Kevin Jhonny

Advisor: SE. Castillo León Rosa Elizabeth, MG

Abstract

Along the time, the different advances of technology have allow us to experiment different changes as benefits for the humanity, then, is here the entrance of the Internet of the Things or IoT, a technology that is in constant change since its birth, being used in different fields by the man, however, due to the worry about its security, there have been different inconvenients. Therefore, in the present work through the experimental methodology will be done the design of a domestic IoT network, applying some security protocols like ACL, VLAN, Port Security, SSH, dot1Q protocol and also the deactivation of the CDP and LLDP protocols, that let reduce the different kinds of vulnerabilities that exist in the equipments used by this technology, accomplishing that the LAN network does not be affected by possible threats.

Keywords: IoT, Security, Network, Vulnerabilities, Threats.

Introducción

Hablar del Internet de las cosas es referirse a escenarios en los cuales la conectividad de la red y la capacidad de cómputo se extienden a objetos, sensores y artículos de uso diario los cuales no se consideran computadoras, logrando que estos dispositivos generen, intercambien y consuman datos con una pequeña intervención humana. (Rose, Eldridge, & Chapin, 2015, pág. 5)

El internet de las cosas es una tecnología que se hace presente cada vez más entre usuarios y conforme avanza el tiempo se hace posible su uso en diferentes dispositivos. Sin embargo, algo que siempre debe estar presente es la seguridad, por lo que nuestra información puede correr peligro al igual que el funcionamiento de los sistemas.

“La mayoría de los usuarios domésticos no tienen la conciencia, el conocimiento o los medios para prevenir o manejar ataques en curso”, dice Yair Meidan, candidato al doctorado en la Universidad Ben-Gurion del Negev. Esto significa que se deben considerar siempre los parámetros de seguridad que pueden existir al momento de configurar un equipo para evitar problemas importantes en su funcionamiento.

La sociedad es testigo del avance en tecnología de dispositivos IoT, pero también son conscientes de cómo se intensifican los ataques, los ciberdelincuentes utilizan desde métodos un poco primitivos, como el adivinar la contraseña hasta realizar ataques DDos. “Es muy fácil cambiar la contraseña predeterminada, por lo que se debe exigir a todos de dar este simple paso para proteger sus dispositivos inteligentes”, dijo Dan Demeter, investigador de seguridad en Kaspersky.

El presente trabajo desarrollará un diseño de una red doméstica IoT aplicando protocolos de seguridad, el cual está dirigido a hogares que buscan mediante dispositivos inteligentes ayuda en sus tareas cotidianas, las cuales se buscará blindar de vulnerabilidades de seguridad que puedan ser aprovechadas por ciberdelincuentes. Está estructurado por capítulos de la siguiente manera:

El primer capítulo muestra cómo nace el problema a tratarse en el cual se detalla sus causas y consecuencias lo cual incentivo a buscar una solución.

El segundo capítulo hace referencia a trabajos previamente realizados que sirvieron como guía para el tema investigado y además se explicaran los conceptos básicos de lo utilizado para su desarrollo.

El tercer capítulo detalla la metodología utilizada en el presente trabajo de investigación, la técnica de recolección de datos que se utilizó, las comparativas de los diferentes elementos

a utilizar y el esquema general de la red IoT a emplearse junto con la simulación del mismo.

Capítulo I

El Problema

1.1. Planteamiento del problema

“El llamado internet de las cosas se trata de que el actual internet sale del universo en que se mueve al de los objetos, identificados y capaces de conectarse e intercambiar información”. (Delclós, 2007)

Hoy en día el internet de las cosas proporciona un gigantesco bienestar en el hogar gracias a los dispositivos inteligentes conectados a la red, los cuales permitirán organizar y realizar tareas en el hogar. Sin embargo, todos los dispositivos que realizan tareas mediante el internet de una u otra manera recopilan datos personales que si no se protegen pueden llegar a ser un eslabón débil para ciberdelincuentes.

“En la actualidad existen más de 7.000 millones de dispositivos IoT y todos ellos significan un tentador objetivo para los ciberdelincuentes por lo cual si tu hogar está conectado debes protegerlo”. (Lueth, 2018)

Al existir beneficios, también existen desafíos en el instante que un objeto pasa a formar parte de un entorno asistido e interconectado, por lo cual es necesario considerar que aquellos dispositivos han perdido seguridad física al encontrarse en entornos inhóspitos y serán accesibles al instante por personas con malas intenciones tales como interceptar, leer o modificar información que altere la funcionalidad de los sistemas.

Un eslabón débil de los dispositivos conectados en red es que no fueron diseñados pensando en su seguridad, pues la realidad es ofrecer a los consumidores un equipo que solo cumpla con su necesidad, mientras a los fabricantes más les interesa abarcar la demanda del mercado que diseñar un producto el cual no se pueda piratear o utilizar con un mal beneficio. Ejemplo, una cámara IP que el usuario la adquiere para la seguridad domésticas, pero si no se la protege puede ser utilizada para espiarlo.

“Investigaciones recientes de Avast y la Universidad de Stanford muestran que el 66 % de los hogares estadounidenses tiene al menos un dispositivo IoT, una cifra que desciende al 40 % si se tiene en cuenta todo el mundo. El número relativamente pequeño de fabricantes (100 empresas crean el 90 % de los dispositivos) sugiere la posibilidad de aprovechar vulnerabilidades similares para realizar ataques a gran escala”. (Hron, 2019)

La mayoría de los dispositivos IoT en el primer momento que se conectan a nuestra red doméstica a través del WiFi lo hacen con el fin de configurarse, por lo cual el usuario luego

de la configuración debería cambiar las claves predeterminadas para proteger su red, lo que muchas veces no se da y es aprovechado por ciberdelincuentes que ven aquella vulnerabilidad para apropiarse del dispositivo y posteriormente controlar los demás.

“Desde el 2014 los televisores de VIZIO transmiten información sobre lo que un consumidor está viendo segundo a segundo a través del software ACR el cual recopila periódicamente direcciones IP, direcciones Mac cableadas e inalámbricas, intensidad de la señal WiFi, puntos de acceso WiFi cercanos y otros elementos”. (Sterling, 2017)

El Internet de las cosas o IoT es una tecnología que aún se encuentra en una fase de constantes cambios, lo cual se ve reflejado en diferentes fallas de seguridad en los dispositivos y de conocimiento por parte del usuario que suelen dejar sus claves de acceso por defecto permitiendo vulnerabilidades aprovechadas por ciberdelincuentes para realizar sus ataques.

1.2. Formulación del problema

¿Cómo mejorar la seguridad ante riesgos potenciales por parte de ciberdelincuentes en una red de hogar inteligente?

1.3. Justificación

El internet de las cosas es un adelanto tecnológico que permitirá modificar todo objeto en “objeto inteligente”. Todo dispositivo que esté a nuestro alrededor podrá estar conectado en red transmitiendo y recibiendo información con el fin de facilitar las tareas cotidianas y volverlas más eficientes.

Según la empresa consultora y de investigación de las tecnologías de la información Gartnet Inc.” Se espera que la cantidad de dispositivos conectados a Internet alcance los 50 mil millones en 2020”. Lo cual mejoraría la calidad de vida de muchas personas, incrementaría la cantidad de riesgos de seguridad a los que los consumidores y las empresas se enfrentarán aumentando exponencialmente.

“Las vulnerabilidades que se presentan en entornos IoT son amplias y pueden llegar a presentarse o generarse en entornos como son las interfaces web no seguras, las cuales no cuentan con un sistema de bloqueo de cuentas por intentos fallidos, permitiendo a los atacantes capturar información de las interfaces en un texto plano, lo mismo pasa con las autenticaciones que son débiles o que están expuestas en las redes internas”. (Calvo del Olmo, 2018)

Uno de los más populares ciberataques que existen actualmente contra dispositivos conectados en red es el reclutamiento en botnet, el cual consiste en un enjambre de dispositivos infectados capaces de lograr grandes daños al realizar tareas en masa, apoderándose de algún dispositivo para realizar ataques DDos interrumpidamente o envío de spam.

En el internet de las cosas al detectarse vulnerabilidades de seguridad en la que un ciberdelincuente pueda llegar a controlar las cámaras de seguridad de tu casa o acceder a tu sistema de iluminación para saber si estas o no en casa, surge la necesidad e importancia de realizar una investigación para analizar las seguridades que se puedan implementar en una red doméstica IoT, la cual brinde a los usuarios el mayor nivel de seguridad posible.

Hoy por hoy la prueba de software para los dispositivos que pueden ser utilizados en una red tiene como objetivo principal que funcione y que sea fácil de configurar para el usuario, dejando a la seguridad como algo secundario, dando como resultado miles de equipos listos para ser vulnerados.

“Indudablemente, existen riesgos, pero también hay soluciones. No debemos temer a la horda de dispositivos conectados que se acerca ni el pujante surgimiento de los hogares inteligentes. Solo tenemos que mantenernos alertas al incorporarlos a la red y proteger la red: de este modo, podremos aprovechar al máximo las ventajas de la asombrosa era tecnológica en que nos encontramos”. (Empey, 2018)

La mayor parte de los dispositivos IoT requieren de una configuración durante su instalación, se puede mencionar a la identificación y autenticación como procesos fundamentales para una instalación predeterminada de un equipo, las cuales se buscan que sean lo más fáciles posibles para el usuario, pero que cumpla con requisitos mínimos de seguridad, sin embargo el limitar el acceso a la red, cifrar contraseñas y el acceso remoto pueden ser unos niveles de seguridad básicos para mantener los equipos seguros ante cualquier amenaza.

El internet de las cosas es ya una tecnología que forma parte de la vida de las personas y conforme pasa el tiempo la cantidad de dispositivos conectados va a seguir creciendo, sin embargo, ni los usuarios ni los fabricantes demuestran una preocupación por la seguridad adecuada que se les pueda brindar, fijándose únicamente en su funcionalidad y fácil configuración, lo cual es algo que debe comenzar a cambiar.

1.4. Objetivos

1.4.1 Objetivo general.

Diseñar una red IoT doméstica que garantice la seguridad ante amenazas externas aplicando protocolos de seguridad.

1.4.2 Objetivos específicos.

- Determinar mediante información teórica los posibles protocolos de seguridad ante vulnerabilidades en una red IoT.
- Identificar los diferentes entornos de simulación óptimos que representen el comportamiento real en una red IoT.
- Diseñar la red IoT doméstica.
- Establecer niveles de seguridad a nivel de redes LAN en una red IoT.

1.5. Alcance

La finalidad del presente trabajo de titulación es diseñar una red IoT doméstica en la cual se logre controlar los dispositivos conectados mediante internet utilizando protocolos de seguridad de la red tales como:

- ACL para controlar el nivel de acceso a la red.
- Port Security para evitar conexiones no deseadas a los equipos o puertos en cuestión ejecutando una acción en el momento que esta violación de seguridad ocurra.
- SSH el cual permite administración remota en la cual los usuarios controlan y modifican sus servidores remotos a través de Internet, gracias a un mecanismo de autenticación.

Los protocolos de seguridad tratarán de garantizar el mayor nivel de seguridad posible ante vulnerabilidades que puedan ser utilizados por ciberdelincuentes que quieran afectar en el funcionamiento.

Capítulo II

Marco Teórico

2.1. Antecedentes del estudio

A continuación, se describen diferentes temas como antecedentes bibliográficos que fundamentan el presente trabajo:

- Mark Stanislavc y Tod Beardsley en el año 2015 hacen público el artículo “HACKING IOT: A CASE STUDY ON BABY MONITOR EXPOSURES AND VULNERABILITIES” en la revista Rapid7, en el cual detallan las vulnerabilidades comunes a las que están expuestos los dispositivos IoT mediante Air Magnet Survey la cual es una herramienta de estudio de sitios WLAN, demostrando que los dispositivos sufren al menos un fallo crítico sea de hardware, firmware o software. Como un claro ejemplo se puntualizó las diferentes vulnerabilidades que se exponen los monitores para bebés tales como: interferencias o acceso mediante comunicaciones remotas, demostrando el bajo nivel de seguridad que brindan estos equipos. (Stanislav & Beardsley, 2015).
- Jesús Molina y Joe Gordon en la ciudad de San Francisco en el año 2016 brindaron una conferencia sobre su artículo llamado “HACKING THE IOT: WHEN GOOD DEVICES GO BAD”, en donde nos exponen sobre la nueva tecnología y nos proponen un sistema conformado por software libre el cual les permite realizar pruebas de vulnerabilidades de seguridad a los dispositivos de una red mediante GNU radio, dando como resultados bajos niveles de seguridad en los sistemas IoT. (Molina & Gordon, 2016)
- El trabajo “Cybersecurity. Introduction to Dossier” desarrollado por Carolina Sancho Hirare, el cual habla sobre la ciberseguridad el cual es un procedimiento del ciberespacio que está a disposición de los ciudadanos, organización gubernamentales y no gubernamentales en la cual se pueden efectuar relaciones sociales de una forma más rápida y económica en relación de otras formas utilizadas para intercambiar información. (Sancho, 2017)
- El trabajo “Methodology of computer security management for the internet of things” desarrollado por Ivette Mateo Washbrum, en donde argumenta sobre el crecimiento exponencial de dispositivos IoT y al no contar con estándares se

dificulta el control y gestión de seguridades informáticas en las redes de conexión de dispositivos al internet de las cosas. (Mateo, 2018)

2.2. Fundamentación teorica

2.2.1 Redes inalámbricas

Aquellas que mantienen una comunicación por medio de ondas electromagnéticas permitiendo conectar nodos sin una conexión física. Para realizar su transmisión y recepción de datos utilizan dispositivos que actúan como puertos. Al no necesitar un cableado para establecer vínculos entre computadoras y otros equipos garantizan un ahorro de dinero y una mayor comodidad en infraestructura. (Pérez Porto & Merino, 2011)

Actualmente existen varios tipos de redes inalámbricas los cuales se clasifican dependiendo de su alcance y tecnología, además de distinguirse por los estándares que manejan, tal como se muestra en la Figura 1:

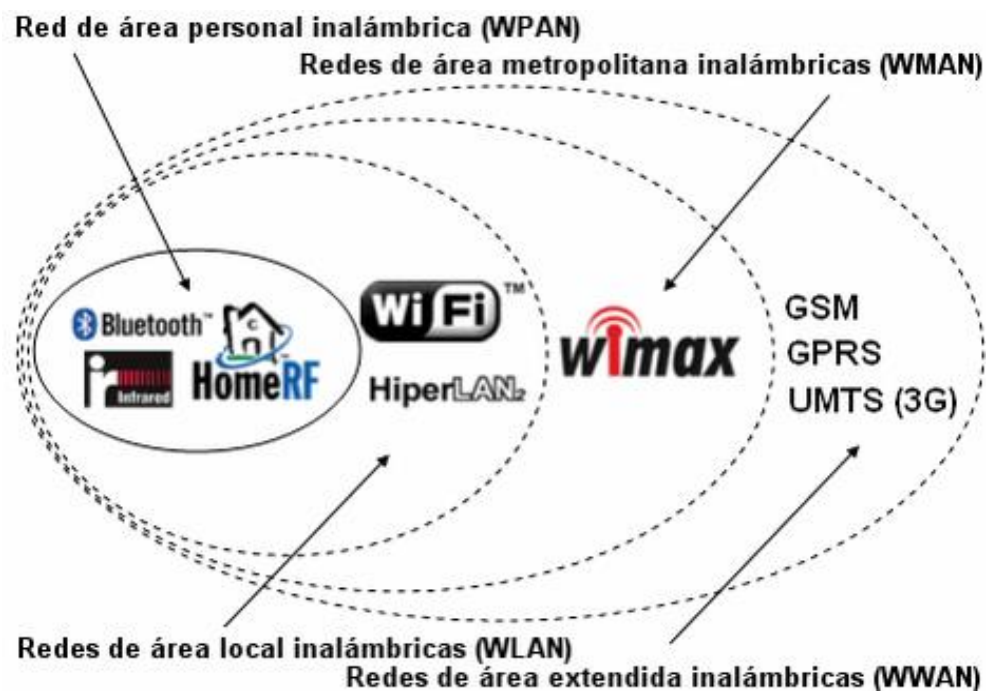


Figura 1. Tipos de redes inalámbricas. Información tomada de Google. Elaborado por el autor.

2.2.2 Topologías de Redes

Es la forma en la cual se conectan las computadoras para intercambiar información entre sí, tanto de manera física como lógica. (Raffino, 2020). Los diferentes tipos de topologías se muestran en la figura 2.

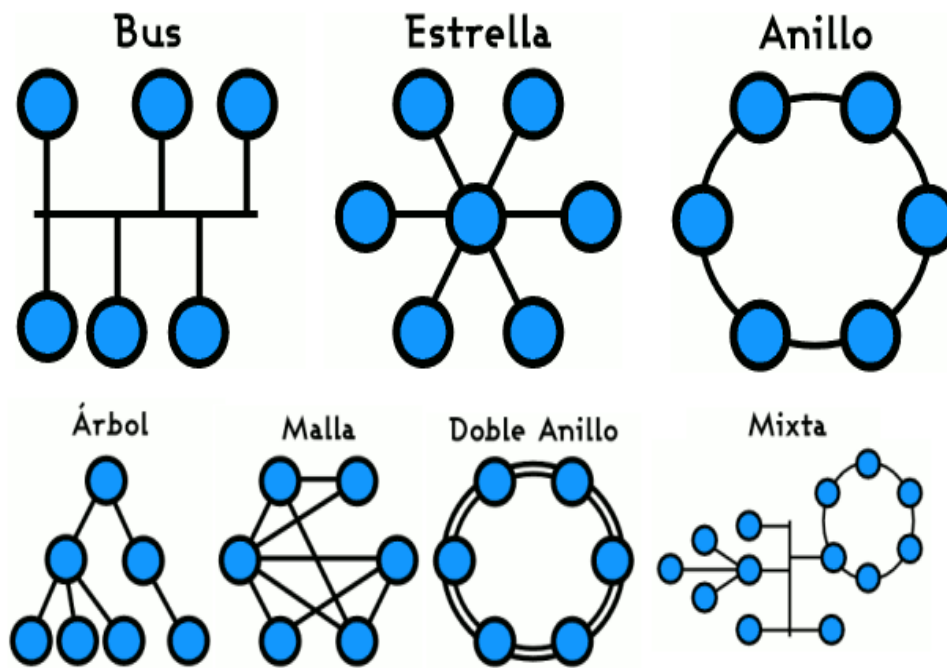


Figura 2. Tipos de topologías de redes. Información tomada de Google. Elaborado por el autor.

- **Topología de bus:** Se trata de un cable central por el cual pasa la información hacia todas las computadoras de la red.
- **Topología de estrella:** Se basa de un host o punto central hacia los demás nodos de la red.
- **Topología de malla:** También conocida como topología de trama, se trata de una interconexión de nodos entre sí en donde la información puede viajar por diferentes caminos.
- **Topología de anillo:** Es una red simple en donde las computadoras se encuentran interconectadas en forma de anillo viajando la información en un solo sentido.
- **Topología de árbol:** Es una red similar a la de estrella y bus en la cual cuenta con un cable principal llamado backbone encargado de comunicar los nodos.
- **Topología mixta o híbrida:** Para adaptar la red a las necesidades del cliente este tipo de topología es una combinación de dos o más topologías de red diferentes.

2.2.3 El internet de las cosas

Es una red capaz de conectar todo tipo de objetos físicos al internet en especial aquellos que sería imposible realizarlo, pueden variar desde objetos domésticos tales como una refrigeradora hasta dispositivos inteligentes como un teléfono celular capaces de recibir e intercambiar datos usando sensores integrados, lo cual permite que cualquier dispositivo conectado desde una ubicación remota pueda gestionar cosas cotidianas gracias a la

tecnología para mejorar la calidad de vida del usuario. (Ballard, 2016). La figura 3 muestra el funcionamiento de un esquema IoT donde todos los dispositivos conectados en red son gestionados por la nube.

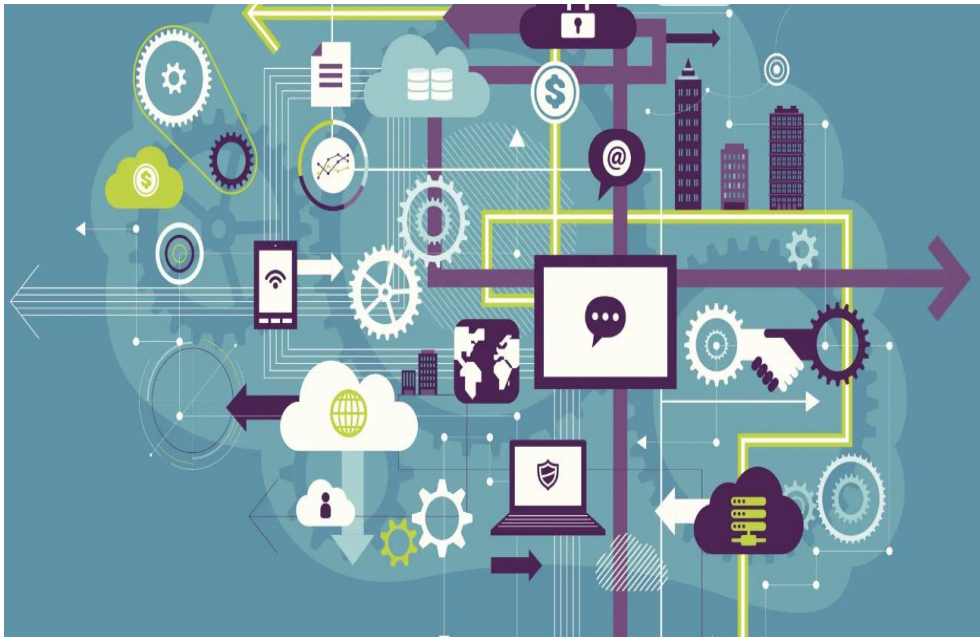


Figura 3. Esquema de una red IoT. Información tomada de hipertextual.com. Elaborado por el autor.

2.2.4 Arquitectura IoT

Se puede definir como la transmisión de datos entre los diferentes componentes de una red funcional, como equipos de transmisión, programas y protocolos de comunicación. Aunque en realidad no existe un modelo que se lo represente como fijo del IoT se debe cumplir ciertos requerimientos para que esta tecnología sea viable tales como que la tecnología sea distribuida, escalable, eficiente y segura en donde los objetos interactúen entre ellos. (Del Valle, 2015)

2.2.5 Seguridad IoT

Es uno de los aspectos más importas en IoT debido a que los dispositivos están constantemente captando información personal y por ende llevando el mundo real a internet y así viceversa. (Barberá, 2016).

La seguridad IoT se la clasifica en:

- **La seguridad de la nube:** En esta seguridad las amenazas que se deben priorizar son aquellas que vienen del entorno de la empresa o del entorno de la nube al que los dispositivos están conectados.

- **La seguridad del dispositivo:** En esta seguridad debido a los diferentes dispositivos conectados y al uso de sus aplicaciones de software junto con los datos que se comparten serán puntos de ataque para personas maliciosas.

2.2.6 Proceso de comunicación en dispositivos IoT: Modo físico

Para que la información fluya del medio físico al medio virtual los dispositivos deben seguir un proceso y aunque existan varios modelos para conformar un sistema IoT su finalidad es la misma. (Del Valle, 2015). Este proceso se divide en cuatro fases como se muestra en la figura 4.



Figura 4. Proceso de Conexión IoT en modo físico. Información tomada de programarfacil.com. Elaborado por el autor.

- **Aplicaciones:** Por lo general las aplicaciones deben ser fáciles de manejar y visualizar su información por lo que deben ser amigables para el usuario y pueden ser nativas o web.
- **Procesamiento de datos:** El buen funcionamiento de un sistema IoT dependerá de la recolección de datos y de la capacidad de gestionarlos para su uso.
- **Puntos de acceso:** Son aquellos puntos que deben garantizar una conexión segura, robusta y tolerante a fallos porque permiten la conectividad de los dispositivos al internet.
- **Cosas/objetos/dispositivos:** Se le puede considerar como el hardware de un sistema IoT que permite comunicar el mundo físico con el digital.

2.2.7 Proceso de comunicación en dispositivos IoT: Modo lógico

Al terminar la conexión física de los dispositivos en un entorno IoT no significa que es suficiente para habilitar la comunicación, pues los dispositivos deben saber cómo comunicarse entre sí. (Feijóo, 2017)



Figura 5. Proceso de Conexión IoT en modo lógico. Información tomada de bebee.com. Elaborado por el autor.

Todo comienza con un mensaje que se debe enviar desde un origen hasta un destino direccionado por protocolos que deben respetarse para realizarse con éxito la comunicación, tal como muestra la figura 5. Para que la comunicación sea exitosa se deben realizar dichos protocolos:

- **Codificación de mensajes:** Se le llama al proceso en el cual la información se transforma para la transmisión segura.
- **Formato y encapsulación del mensaje:** El mensaje se encapsula en una trama y se le proporciona dirección de destino y origen.
- **Tamaño de mensaje:** El mensaje debe estar entre 64 bytes y 1518 bytes para ser comprendida por el receptor.
- **Temporización del mensaje:** Indica cuando establecer la comunicación, la velocidad y el tiempo para esperar una respuesta.
- **Opciones de entrega de mensaje:** Se la puede realizar por Unicast, Multicast y Broadcast

2.2.8 Protocolos de comunicación en el IoT

Es una serie de normas que se define para que dos o más dispositivos puedan comunicarse, existen muchas formas de realizar una comunicación M2M, pero no todas cumplen con los requisitos especiales de un sistema IoT como escalabilidad, débil acoplamiento entre dispositivos, interoperabilidad, comunicaciones simultaneas, seguridad y acceso fácil. (LLamas, 2019)

- **MQTT:** Optimizado para comunicaciones simultaneas.

- AMQP: Asegura la confiabilidad e interoperabilidad.
- WAMP: Se ejecuta sobre WebSockets y provee aplicaciones de PubSub como rRPC
- COAP: Emplea el modelo REST de HTTP, soporte UDP, multicast y mecanismos de seguridad adicionales.
- STOMP: Emplea HTTP y mensajes de texto para buscar el máximo de interoperabilidad
- XMPP: Diseñado para aplicaciones de mensajería instantánea
- WMQ: Protocolo de cola de mensajes

2.2.9 Router

Es el dispositivo encargado de que varias redes o dispositivos se conecten entre sí y utiliza protocolos de enrutamiento para trasladar la información por la ruta más adecuada. (Bembibre, 2009)



Figura 6. Imagen de un Router. Información tomada de novicompu.com. Elaborado por el autor.

2.2.10 Switch

Es un dispositivo el cual sirve para conectar varios elementos dentro de una red y su función es servir de puente para el tráfico de paquetes de una máquina a otra mediante su MAC. (Cabrera J. , 2019)



Figura 7. Imagen de un switch. Información tomada de cisco.com. Elaborado por el autor.

2.2.11 Servidor

Es un ordenador encargado de administrar y compartir la información solicitada por los demás dispositivos conectados a la red. (García, 2018)



Figura 8. Imagen de un servidor. Información tomada de tecnozero.com. Elaborado por el autor.

2.2.12 Gateway

Conocida también como puerta de enlace, permite interconectar las redes con diferentes protocolos y arquitecturas a todos los niveles de comunicación.

2.2.13 Firewall

También conocido como cortafuego es un sistema encargado de proteger a una computadora o una red de computadoras ante amenazas de terceros filtrando los datos que están en la red. (Venturini, 2020)

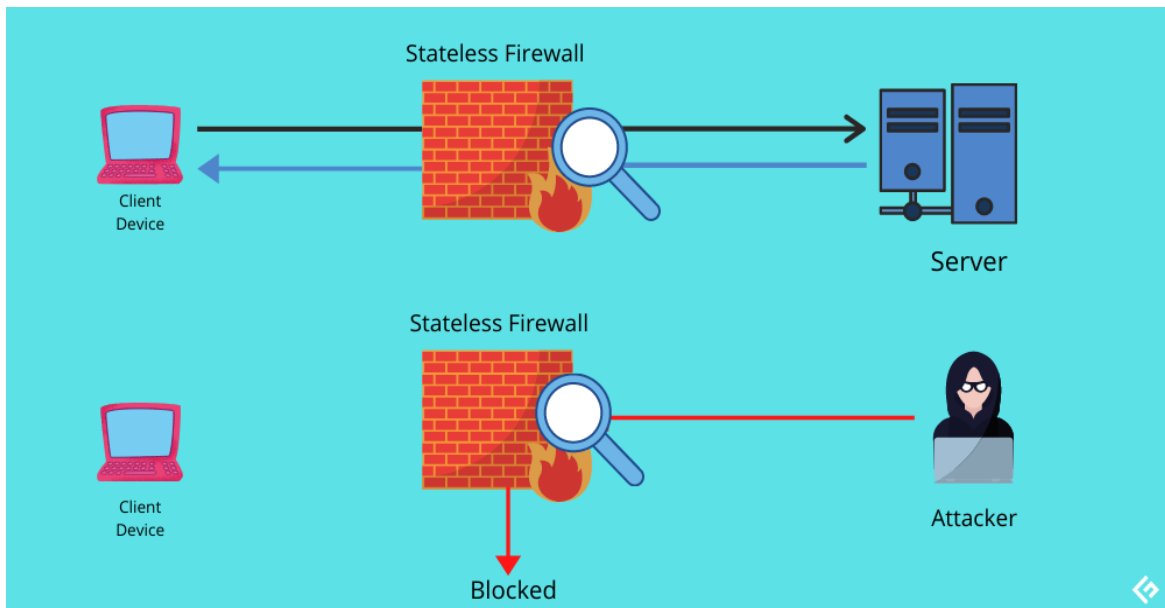


Figura 9. Funcionamiento de un Firewall. Información tomada de *geekflare.com*. Elaborado por el autor.

2.2.14 Subnetting

Es una colección de direcciones IP que permiten definir el número de redes y de host que se desean utilizar en una subred determinada.

2.2.15 Routing

Es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad.

2.2.16 Lista de control de Acceso (ACL)

Es una herramienta de seguridad que tienen los Router, la cual ayuda a controlar las amenazas internas y externas, además de controlar todo el tráfico que entra y sale de mi red. (Páramo, 2011)

2.2.16.1 Tipos de ACL

Existen dos tipos de ACL:

- **ACL estándar:** Se encarga únicamente del filtrado de paquetes de datos por medio de la verificación de dirección IP de origen.
- **ACL extendidas:** Realiza el filtrado de paquetes de datos por medio de la dirección IP de origen, dirección IP de destino, el protocolo utilizado y los números de puertos.

2.2.17 Vlan

Es un método que permite crear redes independientes, aunque estén dentro de una misma red física. De esta forma el usuario podrá disponer de varias redes estando en el mismo dispositivo. (Crespo, Redes Zone, 2016)

2.2.17.1 Tipos de puertos

Cuando un switch trabaja en función de la vlan van a existir dos tipos de puertos:

- **Puertos de acceso (Access):** Los puertos de acceso sirven para conectar equipos finales y solo transporta el tráfico de una sola vlan.
- **Puertos troncales (Trunk):** Los puertos troncales se los utiliza para conectar dos switches y pueden transportar el tráfico de varias vlans por lo que para reconocerlas es necesario etiquetar las diferentes tramas indicando a que vlan corresponden.

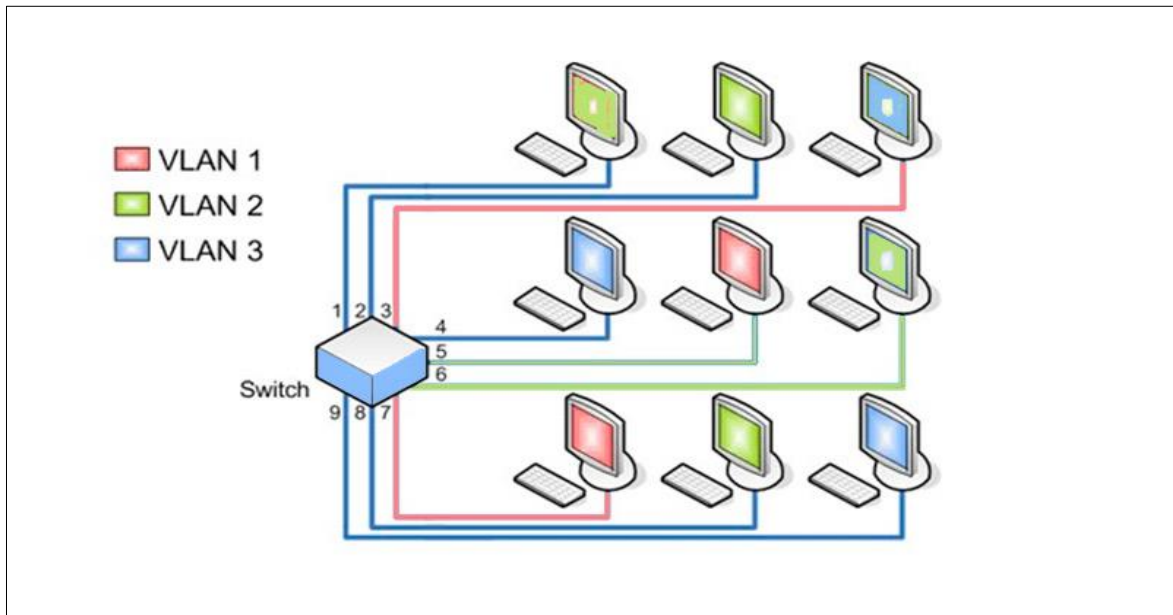


Figura 10. Funcionamiento de una Vlan. Información tomada de internetspasoapaso.com. Elaborado por el autor.

2.2.18 Vlan Nativa

Utilizada únicamente para el traslado del tráfico sin etiqueta en un enlace troncal por lo cual es recibida en un puerto configurado con el 802.1Q.

2.2.19 Protocolo 802.1Q

Es un protocolo también conocido como dot1Q creado por la IEEE a finales de los años 90, el cual permite que las vlans separadas puedan intercambiar información entre sí.

2.2.20 CDP

Es un protocolo desarrollado y utilizado únicamente en equipos cisco, el cual sirve como herramienta de recolección e intercambio de información entre dispositivos vecinos conectados directamente. (Moisa, 2019)

2.2.21 LLDP

Es un protocolo empleado por dispositivos de red para anunciar información propia a otros equipos, similar al protocolo CDP con la diferencia que no solo puede ser utilizado entre equipos cisco. (Moisa, 2019)

2.2.22 DTP

Es un protocolo exclusivo de equipos cisco, habilitado de manera automática en los switch el cual automatiza la configuración de enlaces troncales entre los switches.

2.2.23 DCHP

Es un protocolo el cual se basa en el modelo cliente-servidor que permite asignar direcciones IP de forma automática, además de puertas de enlace y otros parámetros de red en los dispositivos cliente. (González, 2021)

2.2.24 WPA2

Conocido también como IEEE 802.11i es un estándar de seguridad para redes inalámbricas el cual permite otorgar seguridad a través de contraseña.

2.2.25 SSID

También conocido como identificador de paquetes de servicio, cumple con la función de identificar una red con relación a otra, para al momento de recibir un paquete que viene acompañada de esta información, lo cual permite identificar cuál es su red de origen y a su vez identificar la red a la cual se debe enviar una respuesta. (Crespo, 2018)

2.2.26 FQDN

Se trata del nombre de dominio completo el cual permite que un equipo sea capaz de conectarse a internet.

2.2.27 Port Security

Es la seguridad a nivel de los switch la cual permite limitar un determinado número de direcciones MAC que puedan conectarse bloqueando todo el tráfico. (De luz, 2017)

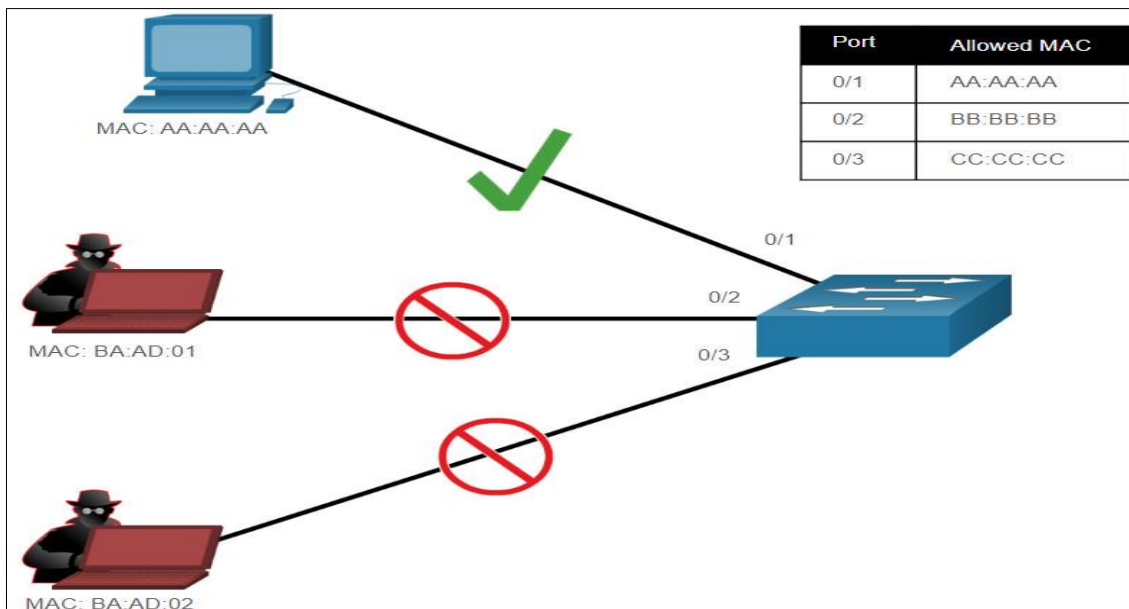


Figura 11. Funcionamiento del Port Security. Información tomada de Google. Elaborado por el autor.

2.2.28 SSH

Es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet, por medio de un mecanismo de autenticación de forma segura. (Cabrera R. , 2020)

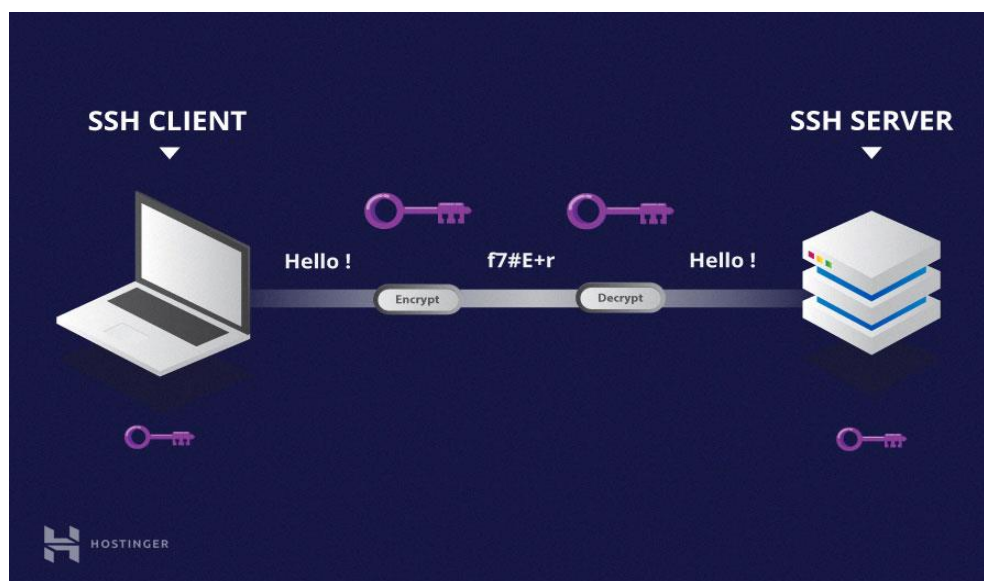


Figura 12. Funcionamiento del Protocolo SSH. Información tomada de Hostinger.es. Elaborado por el autor

2.2.29 Packet Tracer

Es un software diseñado por la empresa Cisco el cual permite realizar simulaciones de redes en un entorno virtual, como diseñar y construir una red desde cero, trabajar sobre proyectos preconstruidos, probar nuevos diseños y topologías de red, probar cambios en la red antes de aplicarlos a la misma, examinar el flujo de datos a través de una red y hacer simulaciones del internet de las cosas. (Barcia, 2018)

2.3. Fundamentación legal

Para la realización del presente proyecto de titulación se debe tener claro varios preceptos jurídicos, donde la Constitución de la Republica del Ecuador es la norma suprema originaria de nuestro país la cual faculta, permite y garantiza varios principios. Además, existen leyes o reglamentos conocidos como rangos inferiores de la constitución las cuales prohíben, permiten o sancionan.

2.3.1 Constitución de la Republica del Ecuador

- **Art. 66. Numeral 21.-** Establece “El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación”.
- **Art. 385. Numeral 1.-** Establece “Generar, adaptar y difundir conocimientos científicos y tecnológicos.”.
- **Art. 385. Numeral 3.-** Establece “Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir”.
- **Art. 387. Numeral 1.-** Establece “Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo”.
- **Art. 387. Numeral 3.-** Establece “Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumak kawsay”.

2.3.2 Código Orgánico Integral Penal (COIP)

- **Art 178.-** Establece “La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años”.

- **Art 190.-** Establece “La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años”.

- **Art. 229.-** Establece “La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años”.

- **Art 232.-** Establece “La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años”.

- **Art 234.-** Establece “La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años”.

2.3.3 Código Orgánico de la Economía Social de los Conocimientos

- **Art. 3. Numeral 2.-** Establece “Promover el desarrollo de la ciencia, la tecnología, la innovación y la creatividad para satisfacer necesidades y efectivizar el ejercicio de derechos de las personas, de los pueblos y de la naturaleza”.

Capítulo III

Propuesta

3.1. Métodos de investigación

3.1.1 Metodología Experimental

La investigación experimental está integrada por un conjunto de actividades metódicas y técnicas que se realizan para recabar la información y datos necesarios sobre el tema a investigar y el problema a resolver. (José, 2018)

La investigación experimental se presenta mediante la manipulación de una variable experimental no comprobada, en condiciones rigurosamente controladas, con el fin de describir de qué modo o por qué causa se produce una situación o acontecimiento particular. Su diferencia con los otros tipos de investigación es que el objetivo de estudio y su tratamiento dependen completamente del investigador, de las decisiones que tome para manejar su experimento. (José, 2018)

Por lo que en el presente trabajo de titulación se requirió este tipo de metodología debido al diseño a plantearse de una red IoT doméstica permitiendo analizar información y el nivel de seguridad que presentan los dispositivos.

3.1.2 Metodología Exploratoria

La investigación exploratoria consiste en proveer una referencia general de la temática, a menudo desconocida, presente en la investigación a realizar. Entre sus propósitos podemos citar la posibilidad de formular el problema de investigación, para extraer datos y términos que permitan generar las preguntas necesarias. Asimismo, proporciona la formulación de hipótesis sobre el tema a explorar, sirviendo de apoyo a la investigación descriptiva. (Morales, 2014)

Este tipo de investigación está incluida en el segundo grupo de clasificación de la investigación científica, que está orientada según el nivel de conocimientos a obtener, teniendo presente que todos los tipos de investigación se complementan. Puede ser cuantitativa, cualitativa o histórica. Se distingue de las demás investigaciones por la flexibilidad en la metodología aplicada. Dentro de sus posibilidades trata de descubrir todas las afirmaciones o pruebas existentes del fenómeno que se estudia. Como consecuencia, involucra cierto riesgo, paciencia y predisposición por parte del investigador. (Morales, 2014)

Cabe recalcar que este tipo de investigaciones no tiene como finalidad establecer las conclusiones del tema de investigación estudiado o planteado, sino que sirve como referencia a otro tipo de investigaciones para que estas definan los resultados que conlleven al planteo de las respectivas conclusiones de la investigación en cuestión. Por ende, se utilizará esta metodología porque permitirá determinar si se pueden realizar investigaciones posteriores con mayor profundidad de un tema desconocido o poco estudiado.

3.1.3 Método Descriptivo

El método descriptivo es uno de los métodos cualitativos que se utilizan en investigaciones que tienen el objetivo de evaluar algunas características de una población o situación particular. En la investigación descriptiva, tal como lo indica su nombre, el objetivo es describir el estado y/o comportamiento de una serie de variables.

El método descriptivo orienta al investigador durante el método científico en la búsqueda de las respuestas a preguntas como: quién, qué, cuándo, dónde, sin importar el por qué. (Yanez, 2019)

El objetivo de este tipo de métodos es obtener datos precisos que puedan aplicarse en promedios y cálculos estadísticos que reflejen tendencias, por ejemplo. Normalmente, este tipo de estudios es el que abre paso a otros más profundos y complejos sobre un fenómeno determinado, al ofrecer datos sobre su forma y función. (Yanez, 2019)

Por lo que el método descriptivo se lo aplicará para comprender las características de los objetos a ser utilizados en el esquema.

Una vez determinado el tipo de metodología a utilizar dentro del presente trabajo de investigación como el análisis de la entrevista se procederá a determinar el o los tipos de mecanismos necesarios para el diseño de la propuesta.

3.2. Técnica de recolección de datos

Se entrevistó a la Ing. Rosa Castillo, la cual es docente de la carrera de Ingeniería en Teleinformática, con el objetivo de tener la perspectiva de una profesional la cual se desempeña en el área de las tecnologías IoT y tener una visión de todos los escenarios posibles.

Para esta investigación se procederá a la recolección de datos mediante entrevista la cual está dirigida a una docente de la carrera de ingeniería en teleinformática de la facultad de ingeniería industrial, la misma que consta con las siguientes preguntas.

1) ¿Que es el Internet de las Cosas (IoT)?

IoT es la interconectividad de todo, una conexión avanzada de muchos dispositivos, sistemas y servicios.

Análisis: Se aprecia que el entrevistado tiene una visión clara e introductoria sobre lo que son las IoT, lo cual refleja el dominio del tema por parte del mismo, que para efectos de esta entrevista será sumamente fructífera ya que no solamente aportará con sus conocimientos, sino que también dará pautas y directrices que contribuirían al desarrollo de la red que se busca diseñar en este trabajo de titulación.

2) ¿Qué beneficios tiene el Internet de las cosas (IoT)?

Los beneficios son amplios desde la automatización en el hogar, electrodomésticos que utilizan internet para conocer el estado de los procesos, estudiar hábitos de consumidores, rastreo remoto de pacientes, hasta el control de operaciones urbanas y rurales.

Análisis: Los beneficios que puede llegar a tener el internet de las cosas es muy extenso va desde la conexión de una casa para monitorearla desde un teléfono, lo que se conoce como domótica, hasta la automatización de procesos industriales.

3) ¿Qué efecto tendrá el Internet de las Cosas (IoT) en nuestras vidas diarias?

Facilitar las actividades de las personas y en las empresas obteniendo muchos beneficios en cuanto a automatización, obtención de información, mejoramiento de procesos, etc.

Análisis: Definitivamente con la aparición del IoT se tiene un gran avance tecnológico que está en constante crecimiento y como lo menciona la ingeniera entrevistada se facilitarán muchas cosas, actividades e incluso se automatizan procesos empresariales.

4) ¿Considera que la comunicación entre dispositivos en un entorno IoT es segura?

No, debido a que IoT está en crecimiento aún no cuenta con un protocolo de seguridad en el cual se base para proteger todos los dispositivos conectados.

Análisis: Al tener un red IoT se ganan bastantes beneficios, pero a su vez eso conlleva a tener problemas de seguridad, ya sean estos filtrado de datos, robo de credenciales que dan acceso a datos sensibles de una organización, etc., y como lo menciona la ingeniera entrevistada IoT al estar en constante crecimiento no se pueden brindar facilidades en el ámbito de la seguridad ya que todavía ese tipo de redes no se cuenta con un protocolo eficaz que neutralice o elimine cual tipo de amenazas tanto a la infraestructura como a la transmisión de datos.

5) ¿Qué seguridades se deberían considerar en los dispositivos del IoT?

Dependiendo del tipo de dispositivo, se deberían considerar seguridad en red, en software y de hardware.

Análisis: Efectivamente al ser una red que interactúa entre sus dispositivos tanto a nivel de software y de hardware, los protocolos de seguridad deberán ser capaces de neutralizar cualquier tipo de ataque maliciosos para mantener la infraestructura IoT en un ambiente de red seguro.

6) ¿Cree usted que el Ecuador está listo para el uso del Internet de las cosas?

En ambientes públicos no se cuenta con la seguridad necesaria para proteger la información que se transmitirá mediante IoT, ni tampoco hay garantías de la protección de los dispositivos a utilizarse en esta interconexión.

Mientras que para ambiente empresariales privados, u hogares hay mayor viabilidad del uso del IoT.

Análisis: Actualmente el cabildo de la ciudad de guayaquil instaló puntos acceso a internet gratis alrededor de la misma, por lo que diariamente los usuarios en conectarse en ese tipo de redes abiertas públicas son bastantes, por ende el tráfico de red es enorme y al no contar con las respectivas seguridades en la red los datos de los usuarios son blanco fácil para cualquier infiltración de información, caso contrario como lo indica la entrevistada las empresas constan con una infraestructura de red más robusta lo que si le permitirá al usuario las seguridades del caso para estar en la red sin ningún inconveniente, similar escenario se tiene en los domicilios que no tienen una infraestructura de red a nivel empresarial pero brinda las seguridades básicas para que el usuario final no se vea afectado.

3.3. Elementos utilizados para el diseño de la propuesta

3.3.1 Simuladores

Dentro del presente trabajo de investigación es importante mencionar el tipo de simulador a utilizar para el desarrollo de una red IoT (Internet of Things) que cuente con los niveles de seguridad necesarios en una red LAN (Local Área Network) o red de hogar para ello se detalla a continuación los diferentes tipos de simuladores con lo que es posible hacer un diseño IoT y se determinara en base a sus características o rendimiento cual es el más idóneo.

Tabla 1.- Comparativa entre simuladores

Opciones	NS-2	NS-3	Packet Tracert	Omnet ++	Tossim
Rendimiento	Alto	Alto	Alto	Alto	Alto
Información	Media	Media	Alta	Baja	Baja
Facilidad de uso	Medio	Medio	Fácil	Complejo	Complejo
GUI	Si	Si	Si	Si	Si
Escalable	Si	Si	Si	Si	Si
Interoperabilidad con S.O.	Compleja	Compleja	Fácil	Compleja	Compleja
Actualizaciones	Si	Si	Si	Si	Si

Información tomada de google.com. Elaborada por el autor

Como se puede observar en la tabla 1 se realizó un análisis de diferentes simuladores con la finalidad de determinar cuál es el más idóneo donde a diferencia de NS-2 y NS-3, Packet Tracer permite una gran facilidad de diseño como a su vez la interoperabilidad multifabricante que gran parte de los simuladores hoy en día no cuentan debido a su distribución libre y limitación con software de tipo privado. Por otra parte, en cuanto a información el programa mencionado presenta suficiente información, un beneficio a la hora de realizar diferentes implementaciones o diseños de red.

Es necesario mencionar que para el desarrollo de red se necesitará hacer uso del simulador Packet Tracer en su versión más actualizada debido a las mejoras que presenta y actualizaciones constantes que permiten mejores funciones en cuanto a diseño de redes IoT como a su vez una mayor cantidad de equipos de simulación, permitiendo así una amplia variedad de opciones en cuando a esquema o soluciones de red mediante diseño previo.

3.3.2 Protocolos para la intercomunicación entre vlans

Se conoce como la intercomunicación entre VLANS a los protocolos a utilizar que mediante enlaces troncales son capaces de transmitir redes virtuales ubicadas en áreas diferentes con esto se logra segmentar las redes de computadoras a través de direccionamiento diferente e incluso segmentar los dominios de broadcast existente haciendo que la red sea mucho más robusta a la que se tiene como a su vez brindar mejor rendimiento en cuanto a seguridad e incluso configuración. En el presente trabajo de investigación se hace uso de un protocolo de intercomunicación para la transmisión inter vlan.

Tabla 2.- Comparativa de protocolos de encapsulación entre vlans

Opciones	ISL	802.1Q
Sobrecarga de red	Alta	Baja
Cantidad de vlans	1024	4096
Uso de vlan nativa	No	Si
Multiproveedor	No	Si
Baby giants	Si	No

Fuente tomada de investigación directa. Elaborada por el autor

Hoy en día existen 2 protocolos encargados de realizar la encapsulación entre vlans como son el 802.1Q y el protocolo ISL donde para el presente trabajo de investigación se pretende hacer uso de dot1Q debido a la menos sobrecarga que maneja como a su vez de una vlan nativa que por lo general se encarga de transmitir diferentes vlans por un solo enlace interconectando entre 2 equipos (Switch-Switch o Router-Switch) que lleva el nombre de troncal, al realizarse este proceso a través del protocolo 802.1Q permite tener mayor cantidad de registros brindando escalabilidad en los diseños de redes, otro punto a mencionar es el amplio uso de aplicación con diferentes proveedores de tecnología a diferencia del estándar ISL que es propietario de Cisco siendo una limitante. En la actualidad en el estándar de red TCP/IP se recomienda hacer uso de dot1Q debido a que es el estándar definido por IEEE que se adapta a cualquier proveedor de tecnología en lugar de ISL.

Al utilizar este protocolo se reduce ataques de red e incluso se mejora en cuanto a optimización debido a la separación de dominios de broadcast y excepciones de comunicación entre dispositivos que no son permitidos siendo de gran manera una seguridad necesaria en las redes.

Por otra parte, es importante considerar la forma en la cual los dispositivos obtienen acceso a los equipos locales a través de Internet en base a credenciales de usuario y contraseña, donde a continuación, se pretende determinar que protocolo de conexión remota brinda mayores niveles de confidencialidad en la transmisión de datos como de establecimiento seguro a los equipos.

3.3.3 Protocolos de conexión remota en una red doméstica

Permiten el acceso de forma remota al dispositivo que se encuentra relativamente lejano siempre y cuando cumpla con ciertos requisitos como:

- El equipo al que se desea acceder se encuentra funcionando en estado UP en sus interfaces
- Se requiere que al menos el equipo posea un direccionamiento IP
- Se recomienda que la forma de cifrado a utilizarse sea la más segura mediante un cifrado asimétrico
- Es necesario realizar la autenticación de forma local, aunque se recomienda usar Radius para mejor manejo mediante el estándar 802.1x

Luego de determinar los parámetros mínimos necesarios para este tipo de comunicación se procede con su respectiva comparativa y así seleccionar el protocolo que será aplicado en el diseño de red.

Tabla 3.- Protocolos utilizados para conexión remota

Opciones	SSH	Telnet
Conexión segura	Si	No
Información en texto plano	No	Si
Intercepción de mensajes	No	Si
Uso de cifrado	RSA	Ninguno

Información tomada de investigación directa. Elaborada por el autor

Como se puede observar en la tabla 3 el cifrado ssh tiene mayores facilidades de implementación como de uso a diferencia de telnet debido a la forma con la que trata los datos que son enviados a través de la red, es decir encriptados a través de un algoritmo asimétrico permitiendo que solo aquel equipo que tenga la clave pública como privada sea capaz de validar su autenticación en la red, caso contrario no habrá algún mecanismo que permita realizar esta validación. Por otra parte, es importante mencionar que tanto telnet como SSH trabajan en la misma capa de aplicación TCP/IP, pero debido al número de puerto y consideraciones realizadas por la IEEE hacen que uno tenga mayores niveles de seguridad que otro por lo ya mencionado.

Por lo general para realizar este tipo de implementación se recomienda tener parámetros básicos ya preestablecidos, permitiendo así, mejor manejo en su diseño. Por otra parte, para una mejor entrega de seguridad este tipo de soluciones se requiere la concatenación de ACL (Listas de control de acceso) logrando que solo los dispositivos o segmentos de red que el Router tenga configurado serán los que accedan a los recursos internos de la red LAN donde

para ello es relevante mencionar el uso de la ACL generado en el presente trabajo de investigación como se describe a continuación:

- Se requiere de ACL estándar que permita tráfico desde la red LAN a la Red WAN
- Se requiere descartar todo tráfico request que venga de la WAN
- Aceptar todo tráfico Replay generado de la LAN a la WAN
- Aceptar todo tráfico establecido y relacionado
- Descargar el resto

Para el uso de la ACL se debe mencionar que estas son ejecutadas de manera secuencial de mayor a menor acorde a la primera coincidencia que exista dentro de la red donde al no haber algún requerimiento por lo general la última regla descartará todo tráfico por defecto.

3.4. Esquema general del proyecto

Luego de haber realizado el análisis de la entrevista a un experto con respecto a los niveles de seguridad existentes o que deberían haber en un entorno IoT en ambientes LAN, se procede a presentar el esquema de red que será simulado acorde a los procesos de seguridad establecidos por los estándares de redes y hacking, para ello se debe tener en cuenta que el diseño elaborado será a través del software Microsoft Visio debido a su facilidad de crear entornos completos de manera sencilla y muy interactiva para posteriormente ser simulado en packet tracer, cabe detallar que la configuración a desarrollarse será descrita a continuación:

- Aplicación de subnetting para dividir la red de hogar de la red wireless
- Aplicación de vlans diferentes para la segmentación de red relacionados a las redes de subnetting para la vlan de hogar e invitados
- Asignación de direccionamiento en las VLANS de hogar y wireless para un control más centralizado del esquema a través de un solo DHCP Server en Router
- Aplicación del protocolo dot1Q para intercomunicación Inter Vlan acorde a lo definido en el estándar.
- Configuración básica de equipos para mayores criterios de seguridad
- Uso de ACL de tipo estándar que defina las redes permitidas como las bloqueadas al entrar o salir a Internet
- Uso de Port-Security para asociar direcciones MAC de los dispositivos a un puerto específico y se evite ataques

- Desactivación de protocolos que pueden ser vulnerados como CDP – LLDP

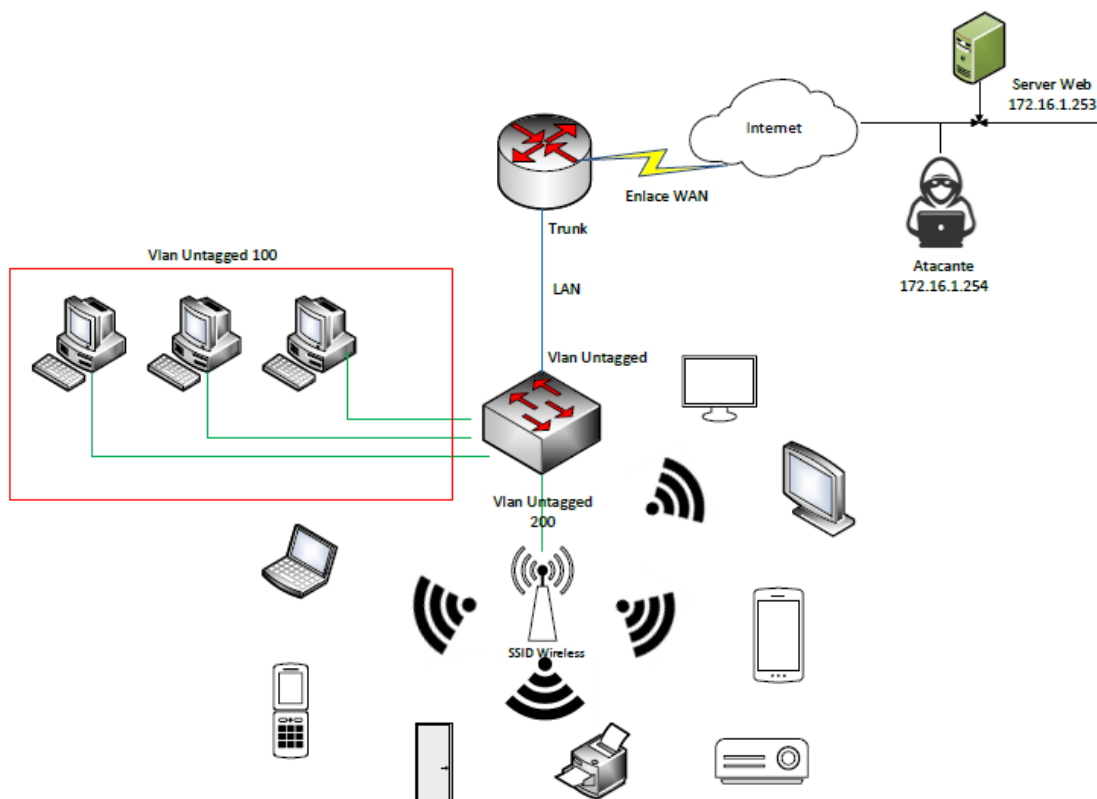


Figura 13. Esquema de Red IoT. Información tomada de Microsoft Visio. Elaborado por el autor.

3.5. Diseño de la propuesta

Una vez determinado los puntos a desarrollar en el presente trabajo investigación y haber realizado el esquema físico en Microsoft Visio se procede a diseñar el esquema lógico de la red través del software de simulación Packet Tracer con el fin de poder explicar los beneficios que este genera en un entorno IoT para redes SOHO (Small Office Home Office).

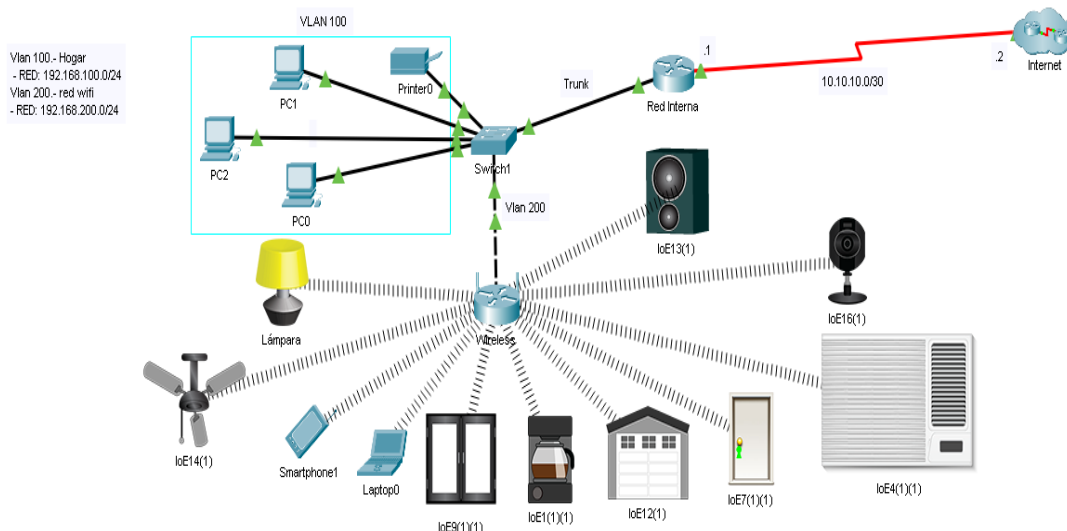


Figura 14. Esquema de Red IoT en Packet Tracer. Información tomada de Microsoft Visio. Elaborado por el autor.

Para el desarrollo de la propuesta como se mencionó con anterioridad se hace uso de diferentes niveles de seguridad como estándares establecidos a nivel de redes o seguridad informática, para así, prevenir cualquier tipo de amenaza existente tanto de manera interna como externa lo que podría generar un riesgo sino se tiene las precauciones necesarias en el entorno de red.

Cabe destacar que todo proceso a realizarse permitirá eliminar el riesgo que puede existir en una red IoT para redes SOHO e incluso en ambientes corporativos debido a las funcionalidades que se aplican que pueden ser de gran relevancia.

Como iniciativa de configuración empresas especializadas en redes mencionan que todo proyecto o diseño requiere de ciertos parámetros básicos de configuración antes de comenzar permitiendo de alguna manera u otra otorgar mayor seguridad en el equipo siendo tolerante a fallas es decir que no sea afectado por limitaciones o problemas cotidianos.

En el presente diseño se cuenta con varios equipos relevantes para la configuración los cuales son:

- **Switch:** Encargado dentro del diseño de red segmentar los dominios de broadcast a través de diferentes vlans y así evitar el ataque de broadcast storm, usado para port-security permitiendo que equipos con parámetros específicos se puedan conectar y los que no sean rechazados a través de una política, además de la desactivación de protocolos que pueden generar ataques si permanecen activados como ARP Spoofing.

- **Router:** Encargado de realizar el ruteo entre equipos ubicados en diferentes subredes o en internet como también la aplicación del protocolo dot1Q en el diseño presentado permitiendo así que vlans diferentes puedan existir a través de la encapsulación, además se

crea rutas estáticas para salida a internet y a su vez de reglas de ACL para establecer cuál de todos los dispositivos están permitidos dentro de la red como a su vez bloquear todo tráfico no establecido ni relacionado en el esquema de configuración.

- **Access Point:** Función en modo bridge a tal punto de tomar los datos de una vlan de acceso y con eso pasarlos como un puente transparente permitiendo que los dispositivos conectados de forma inalámbrica sean segmentados y divididos en dominios de broadcast diferentes, también tiene configurado 2 bandas de frecuencias con protocolos de seguridad.
- **End Point:** Equipos finales que tienen la función de permitir acceso a recursos o medios a través de los equipos de configuración avanzada como Switch y Router.
- **Dispositivos IoT:** Pequeños equipos que cuentan con un sensor, actuador y muchas veces un controlador con el fin de poder hacer que interactúen en el medio o la red y de esta manera optimizar los procesos que por lo general lleva un tiempo prolongado realizarse.

Para la configuración de los equipos se requiere en primer lugar establecer el modo de configuración y decir que va a llevar cada uno, donde es necesario establecer los escenarios de configuración básica necesaria que debe tener todo equipo administrable de red en este caso el Router y Switch debido a que tienen esa funcionalidad.

Cabe mencionar que el simulador Cisco Packet Tracer será el programa de entorno simulado a utilizar, ya que permite utilizar equipos y crear esquemas de redes IoT con los correctos protocolos y niveles de configuración esto no significa que otro software propietario no lo pueda hacer, sino que por facilidad de simulación y explicación es el más idóneo para este trabajo. Algo a mencionar es que actualmente Cisco cuenta con equipos de marca Linksys diseñados específicamente para hogares que posee una poderosa consola de comandos al igual que la corporativa pero algo más limitada, una vez detallado el proceso se realizará la configuración básica de un equipo en este caso el Switch a través de la CLI (Command Line Interface) es decir que todo cambio que se realice aquí afecta directamente al kernel y los procesos del dispositivo siendo una forma efectiva de cambios en lugar de usar una administración GUI como se presenta a continuación:

3.5.1 Prevención de acceso no autorizado

Cada comando utilizado busca prevenir el acceso a la red de usuarios no legítimos en el equipo para ello cual se detalla a continuación las líneas de comando aplicadas realizándose de forma ascendente es decir desde el más básico hasta el más complejo.

Todo cambio para que tenga algún efecto de configuración debe ser ejecutado desde el modo de configuración global para ello se requiere que se use el comando *configure terminal* permitiendo pasar de un modo de administración básica a un modo de configuración avanzado, en este modo todo cambio que se haga puede comprometer al equipo por lo cual solo el personal acreditado debe tener acceso, es por ello que se requiere que nadie pueda ingresar a menos que cumpla con la autenticación definida en el equipo siempre y cuando confirme que sus credenciales son válidas para ello se hace uso del comando *enable secret password* el cual permitirá encriptar una clave en un algoritmo de tipo MD5, la cual una vez ingresada de forma correcta dará el acceso a los datos de rutas, hora, la eliminación de archivos, líneas de comando, entre otro.

```

Switch1
Physical Config CLI Attributes
IOS Command Line Interface

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret tesis
Switch(config)#line console 0
Switch(config-line)#password tesis
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#password tesis123
Switch(config-line)#login local
Switch(config-line)#transport input ssh
Switch(config-line)#exit
Switch(config)#ip domain-name www.plaza.com
Switch(config)#no ip domain-name nslookup
Switch(config)#crypto key generate rsa
% Please define a hostname other than Switch.
Switch(config)#hostname sw_tesis
sw_tesis(config)#crypto key generate rsa
% Please define a domain-name first.
sw_tesis(config)#ip domain-name www.plaza.com
sw_tesis(config)#crypto key generate rsa
The name for the keys will be: sw_tesis.www.plaza.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Ctrl+F6 to exit CLI focus
Copy Paste

```

Figura 15. Configuración básica realizada en Switch Cisco. Elaborado por el autor

Es importante indicar que existen formas en las que un usuario puede ingresar a la configuración y así pueda afectar a la red IoT una de ellas es mediante la autenticación local como a su vez el acceso remoto remota, donde de no establecerse las medidas necesarias de

seguridad podrían afectar seriamente al diseño de red. Una solución a este tipo de problemas es:

Cuando cualquier usuario vaya a acceder de forma física al equipo mediante el puerto de consola se necesitará saber la configuración ingresada (User y Password) permitiendo así una validación de la persona que dice ser caso contrario el acceso será restringido y de esta manera se protegerá la red IoT de algún tipo de cambio o anomalía generado por personas que están presencialmente en el sitio. Para ello es necesario la ejecución de ciertos comandos los mismos que se detallan a continuación:

Tabla 4.- Configuración de consola para acceso a equipo

Comandos	Descripción
Line console 0	Permite acceder al modo de administración por consola
Password	Establece una contraseña en la línea de consola para mayor nivel de seguridad
Exit	Regresa al modo de configuración anterior

Información tomada de investigación directa. Elaborada por el autor

- Cuando un usuario quiere ingresar de forma remota a un equipo por lo general se necesita establecer criterios de permisos que son dados a través de una VPN o mediante el protocolo SSH (Secure Shell) establecido acorde a las normativas RFC para conexiones remotas de forma segura como se explicó anteriormente. Al comparar con su antecesor Telnet. SSH permite que todo tráfico se envíe a través de una red privada o pública de manera cifrada es decir que nadie pueda interceptar estos paquetes debido al uso de cifrados de tipo asimétricos. Para el presente escenario es necesario la aplicación de dicho mecanismo de seguridad debido a que con ello se podrá indicar quien tiene acceso a la configuración y así podrá realizar cambios a cientos o incluso miles de kilómetros del sitio físico siendo una gran ventaja y forma de administración, donde es necesario establecer ciertos comandos que fueron visualizados en la imagen anterior, pero serán detallados a continuación:

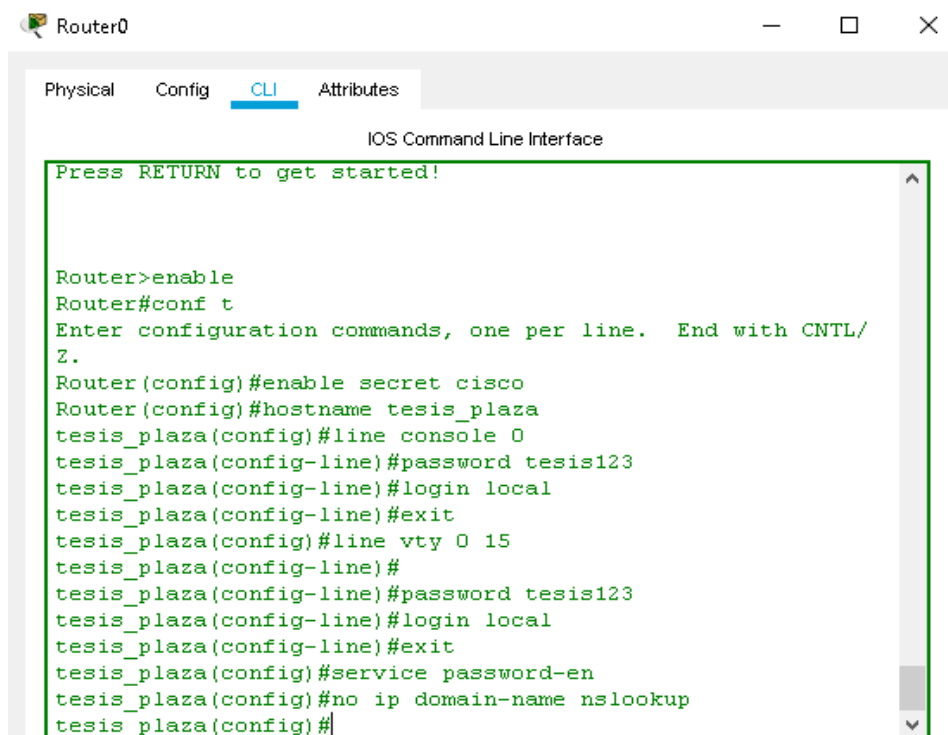
Tabla 5.- Explicación de comandos para configuración básica

Comandos	Descripción
Line vty 0 15	Son la cantidad de conexiones remotas que se pueden tener en la red SOHO mediante el protocolo SSH

Password _____	La contraseña a elegir para que cuando alguien acceda de forma remota a la red pueda ser quien dice ser acorde a la seguridad informática esto es conocido como la Autenticación
Transport input ssh	Es el medio o forma en como un usuario podrá acceder al equipo para administrarlo donde ssh es la opción más segura
Ip domain-name www.plaza.com	Permite crear un dominio en formato FQDN para ello se hace uso del dominio, el protocolo a utilizar y el Root-Server del DNS con el fin de validar que exista la conexión ssh dentro del equipo
Hostname	Cambio de nombre del equipo es requerido de forma obligatoria para saber a qué equipo se está apuntando en Internet
Crypto key generate rsa	Permite crear un cifrado de tipo asimétrico generando dos tipos de claves una privada y una publica siendo un mecanismo más seguro de autenticación donde el módulo a usar por lo general debe ser 1024 o 2048 para que haya mayor nivel de complejidad y la clave no pueda ser hackeada
Ip ssh versión 2	Usado para especificar el nivel de seguridad
Username plaza password 1234 privilege 15	Un punto necesario debido a que es la única forma de validar que el usuario existe para ello se debe crear en el equipo que va a hacer administrado remotamente los usuarios que pueden acceder con su contraseña y el nivel de privilegio es decir entre más alto mayor privilegio tiene donde 1 es bajo y 15 es todos los privilegios

Información tomada de investigación directa. Elaborada por el autor

El mismo proceso debe ser elaborado en el Router para ello se procede adjuntar las imágenes del proceso.



```

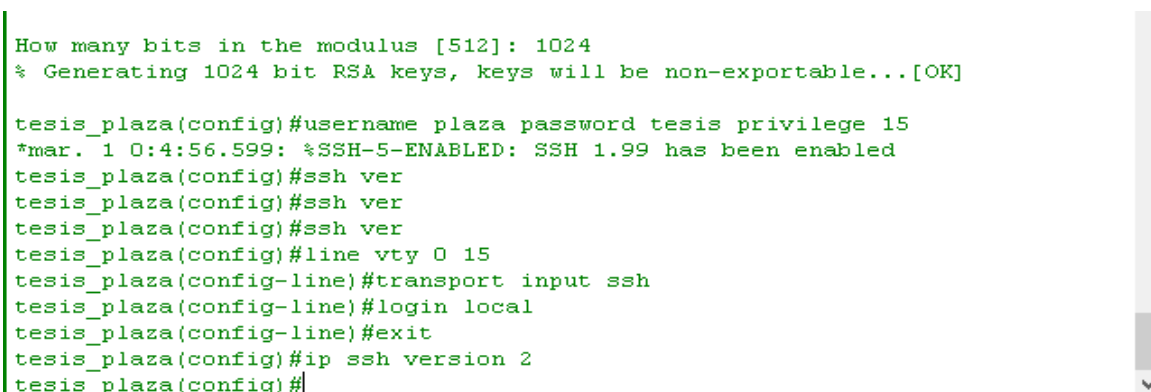
Router0
Physical Config CLI Attributes
IOS Command Line Interface
Press RETURN to get started!

Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/
Z.
Router(config)#enable secret cisco
Router(config)#hostname tesis_plaza
tesis_plaza(config)#line console 0
tesis_plaza(config-line)#password tesis123
tesis_plaza(config-line)#login local
tesis_plaza(config-line)#exit
tesis_plaza(config)#line vty 0 15
tesis_plaza(config-line)#
tesis_plaza(config-line)#password tesis123
tesis_plaza(config-line)#login local
tesis_plaza(config-line)#exit
tesis_plaza(config)#service password-en
tesis_plaza(config)#no ip domain-name nslookup
tesis_plaza(config)#

```

Figura 16. Configuración básica del Router. Elaborado por el autor

Al igual que el switch también se puede determinar la cantidad de sesiones que podrán estar activa al mismo tiempo y de manera remota accediendo así al equipo y con ello tener un control centralizado e incluso asegurar la red IoT.



```

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

tesis_plaza(config)#username plaza password tesis privilege 15
*mar. 1 0:4:56.599: %SSH-5-ENABLED: SSH 1.99 has been enabled
tesis_plaza(config)#ssh ver
tesis_plaza(config)#ssh ver
tesis_plaza(config)#ssh ver
tesis_plaza(config)#line vty 0 15
tesis_plaza(config-line)#transport input ssh
tesis_plaza(config-line)#login local
tesis_plaza(config-line)#exit
tesis_plaza(config)#ip ssh version 2
tesis_plaza(config)#

```

Figura 17. Configuración básica del Router. Elaborado por el autor

3.5.2 Desactivación de protocolos que pueden ser vulnerados en redes LAN

Otra medida de seguridad necesaria implementada en el presente trabajo de investigación es la desactivación de toda interfaz que no está siendo utilizada evitando que alguien desde la red interna se conecte a un puerto y ocasione algún tipo de problema como se presenta a continuación:

```

sw_tesis(config)#interface range fa0/6-24
sw_tesis(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

```

Figura 18. Desactivación de interfaces en el switch. Elaborado por el autor

Como se observa la figura #18 se ha optado por la desactivación de varias interfaces en el switch que no estaban siendo utilizadas en el ambiente LAN por lo cual se busca aplicar mejores prácticas y así reducir cualquier tipo de inconveniente que pudiese existir, limitando a las amenazas internas e incluso externas de cualquier renegación de ataque o acceso.

Por lo general la forma de administración en los equipos Cisco son igual casi en todas sus versiones de Firmware siendo una mínima diferencia en cuanto a comandos es decir que cualquier proceso explicado hasta ahora puede ser replicado en el Router a través de la línea de CLI del equipo permitiendo así una configuración de formato estándar y no tan difícil de manejar para cualquier usuario que desee aplicar niveles de seguridad como los explicados hasta ahora en redes IoT.

Una vez determinado los procesos de configuración que son en gran parte preestablecidos por los proveedores o empresas especialistas en redes y seguridad para todo equipo que sea puesto en producción, es necesario determinar que redes se van a usar como la aplicación de políticas básicas siendo esto un beneficio en el diseño de investigación. El uso de diferentes subredes en este caso relacionadas permite dividir el tráfico y con ello hacer que diferentes redes ubicadas en sitios diferentes no puedan comunicarse a menos que exista algún protocolo de enrutamiento que lo permita donde para el presente trabajo de investigación se procedió con la segmentación de tráfico dividiendo así la red de hogar de la red Wireless

esto con el fin de dividir los dominios de broadcast y aumentar la cantidad de espacios de direcciones permitiendo proteger a las redes de un ataque de MIT (Man in the Middle) e incluso de un sniffer debido a que entre más direccionamiento exista en la red más complicado se vuelve para el atacante descubrir a que IP deberá atacar.

Como se menciono fue necesario el uso de dos subredes que permitan dividir el tráfico donde para cada una se hará uso de una red de clase C definida en el estándar 1918 por la RFC de tipo privadas para el uso interno de la red IoT las cuales se presentan a continuación:

- 192.168.100.X/24
- 192.168.200.X/24

El primer direccionamiento es utilizado para los dispositivos que obligatoriamente necesitan de una conexión cableada y con ello un amplio ancho de banda, en cuanto al direccionamiento referente a la red 192.168.200.X/24 se usará para facilitar la comunicación Wireless tanto para dispositivos IoT que usen controladores inalámbricos como para dispositivos adicionales. De todo el espacio de direcciones utilizado se deberá de considerar lo siguiente a la hora de plantearse el diseño:

- **Network:** Nombre de red en el cual estarán cada dispositivo acorde al tipo de conexión de cada uno de ellos manejen no se puede usar esta dirección para establecer enrutamiento o comunicación entre diferentes dispositivos
- **Direcciones útiles:** Son las IPs que en el esquema podrán ser asignadas a la hora de establecer una comunicación de forma local o remota mediante asignación estática o dinámica.
- **Broadcast:** Es la dirección más gran de la red que tiene como finalidad hacer que todos los equipos respondan a su petición esto a la larga trae una desventaja debido a que si el dominio es muy grande la red puede colisionar en el caso de diseño presentado lo más optimo es tener una red de clase C con un máximo de 254 dispositivos siendo más tolerante y sucesible al dominio de broadcast que se genera.

Tabla 6.- Separación de redes a través de subredes

Red	IPs Útiles	Broadcast	Uso
192.168.100.0/24	192.168.100.1 – 192.168.100.254	192.168.100.255	Cableado
192.168.200.0/24	192.168.200.1 – 192.168.200.254	192.168.200.255	Wireless

Información tomada de investigación directa. Elaborada por el autor

3.5.3 Seguridad a través de VLANs y división de los Dominios de broadcast

Una vez determinada las direcciones IPs a utilizar como el segmento en el cual estará cada equipo se procederá con la creación de VLANs en el Switch con el fin de determinar que en una VLAN especifica solo funcione ese direccionamiento IP con la finalidad de obtener los siguientes beneficios del diseño.

- Segmentar las redes sin la necesidad de un Router
- Si una vlan se ve comprometida la otra vlan no tendrá problema debido a que no se pueden comunicar entre ellas
- Brinda niveles de seguridad
- Reduce los dominios de broadcast

Las vlans solo pueden ser creadas en solo Switches a nivel de capas 2 o Switch Layer 3 o multicapa y no en Routers ya que son funciones totalmente diferentes y el IOS no lo permiten. Una vez explicado de qué manera beneficia el uso de vlans en el entorno de red se procederá a explicar los comandos ingresados.

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

sw_tesis(config-if)#vlan 200
sw_tesis(config-vlan)#name seguridad_wifi
sw_tesis(config-vlan)#interface vlan 20
```

Figura 19. Configuración de vlans para dividir tráfico de redes. Elaborado por el autor

Tabla 7.- Comandos para creación de VLANs

Comando	Descripción
Interface range fa0/1-3	Se establece el rango o el puerto en específico que debe ser configurado para establecer una vlan
Vlan 100	Se crea una vlan en especifico

Name _____	Se establece el nombre de la vlan en específico
Switchport mode access	Proceso que especifica la forma en como un puerto va a trabajar donde para ello en el esquema de red se debe determinar su modo en formato acceso
Switchport Access vlan 100	Se indica a que vlan pertenece ese puerto o rango de puertos y con ello más adelante determinar su rango de ip de la subred 100.X/24

Información tomada de investigación directa. Elaborada por el autor

Esta configuración debe ser repetitivo para cada Vlan a crear dentro de la red en este caso la Vlan 200 correspondiente a Wireless, considerando que ahora se debe de aplicar en la interface fa0/4 debido a que ese puerto es el encargado de permitir que la vlan 200 funcione, dentro del esquema planteado permitiendo el uso del direccionamiento IP 192.168.200.X/24.

Al realizar el proceso de configuración mostrado en la figura #19 existe una división de direcciones a tal punto de que internamente es como si se separen 2 redes, esto hará que ninguna Ip dentro de la vlan 100 pueda hacer solicitudes Echo Request a equipos de la vlan 200 obteniendo tiempos de respuesta perdidos permitiendo así segmentar tráfico y crear vlans para invitados a tal punto de aislarlos de la vlan de hogar y Wireless IoT haciendo mucho más robusta la arquitectura planteada.

3.5.4 Aplicación del protocolo Dot1Q para comunicación Inter Vlan

El diseño presentado cuenta con 2 vlans que permiten separar tráfico reduciendo de esta manera los dominios de broadcast es decir que ningún pc a vlans diferentes debido a que la configuración no lo permite. Debido a la limitante existente se hace uso del protocolo 802.1Q con el objetivo de permitir que vlans separadas puedan intercambiar datos entre sí, al aplicar este tipo de configuración lo que se busca es que se pueda enviar diferente tráfico proveniente de varias vlans y que todo pueda ser ruteado a través de un equipo de capa 3 en este caso el Router, para mayor entendimiento en la creación de una interfaz troncal y su funcionamiento se detalla su configuración a continuación:

```

sw_tesis(config-if)#interface gi0/1
sw_tesis(config-if)#switchpor mode trunk
sw_tesis(config-if)#switchpor trunk native vlan 99
sw_tesis(config-if)#exit
sw_tesis(config)#

```

Figura 20. Configuración de la vlan troncal. Elaborado por el autor

Dentro del esquema de configuración hay varios puntos relevantes a tener que considerar como el tipo de interfaz en la que se deberá crear la vlan untagged que permitirá pasar las demás vlans para este escenario será el puerto GigabitEthernet 0/1 del switch donde se debe además agregar ciertos comandos que son detallados en la tabla #8 que se detalla a continuación:

Tabla 8.- Comandos utilizados para la creación de la Vlan troncal

Comando	Descripción
Interface _____	Se establece el rango o el puerto en específico que debe ser configurado para establecer una vlan troncal
Switchport mode trunk	Se debe especificar que a través de ese puerto se enviará todo el tráfico de las diferentes vlans que están configuradas en este caso vlan 100 y vlan 200
Switchport trunk native vlan ____	Se establece la vlan que va a tener la administración de las demás vlans para ello se debe identificar el número de la nueva vlan que será nativa es decir la que administre todas las demás

Información tomada de investigación directa. Elaborada por el autor

Para que Router on a Stick funcione en los procesos de Inter Vlan es necesario la aplicación en equipos de capa 2 o capa 3 y que cuenten con capacidad de administraciones, es decir puedan configurarse a través de la CLI. Dentro del estudio de investigación se segmentará las vlans acorde a la red definida anteriormente además de la creación de varias subinterfases dentro de la interfaz principal con el fin de ser asignada IP específica de la vlan 100 o vlan 200 acorde al rango de arrendamiento con el fin de que todo dispositivo a nivel de capa 2 pueda enviar paquetes a esta subinterfaz que actuara en modo Gateway y permitirá comunicación entre diferentes segmentos e incluso salida a internet como una interfaz normal.

```

tesis_plaza(config-if)#interface gi0/0/0.100
tesis_plaza(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.100, changed state to up

tesis_plaza(config-subif)#encapsulation dot1q 100
tesis_plaza(config-subif)#ip address 192.168.100.1 255.255.255.0
tesis_plaza(config-subif)#no shut
tesis_plaza(config-subif)#interface gi0/0/0.200
tesis_plaza(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.200, changed state to up

tesis_plaza(config-subif)#ip address 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.

tesis_plaza(config-subif)#encapsulation dot1q 200
tesis_plaza(config-subif)#ip address 192.168.200.1 255.255.255.0
tesis_plaza(config-subif)#no shut
tesis_plaza(config-subif)#exit
tesis_plaza(config)#

```

Figura 21. Configuración Router on a Stick en el Router. Elaborado por el autor

```

tesis_plaza#conf t
Enter configuration commands, one per line. End with CNTL/Z.
tesis_plaza(config)#interface gi0/0/0.99
tesis_plaza(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0.99, changed state to up

tesis_plaza(config-subif)#encap
tesis_plaza(config-subif)#encapsulation dot1q 99 native
tesis_plaza(config-subif)#no shut
tesis_plaza(config-subif)#exit
tesis_plaza(config)#

```

Figura 22. Configuración de la vlan nativa en proceso ROAS. Elaborado por el autor

Como se observa en la figura anterior a la hora de configurar Router on a Stick es necesario que la interfaz principal la cual se conecta a través de un cable al switch como se muestra en la figura#14 sea encendida a través del comando *shutdown* para posteriormente establecer ciertos parámetros necesarios.

Tabla 9.- Comandos utilizados para la configuración Router on a Stick

Comando	Descripción
Interface Gi0/0. ____	Para configurar una subinterfaz es necesario acceder a ella para ello es necesario determinar la interfaz en la que se está trabajando seguido del número con el que se creara la subinterfaz por lo general se recomienda que sea el mismo ID de la vlan ejemplo interface gi0/0.100

Encapsulation dot1Q ____	Activa la encapsulación en base al estándar 802.1Q donde se requiere igual determinar el ID referente a la vlan que va a hacer enrutado ejemplo encapsulation dot1Q 100
Ip address <i>network mask</i>	Se debe colocar una dirección IP que funcione como Gateway para el grupo que pertenece a la VLAN ejemplo 192.168.100.1 255.255.255.0
Encapsulation dot1Q __ native	Determina la vlan nativa que será usada para administración

Información tomada de investigación directa. Elaborada por el autor

Una vez determinada en que subinterfaces se va a trabajar es necesario mencionar que dentro del esquema de configuración se procederá a crear diferentes pool de direcciones que sean asignados de manera dinámica a los equipos conectados a la red con el fin de diferenciar el segmento al que pertenecen, es decir, que si un usuario quisiera ingresar a la red de hogar y conecta al equipo en un puerto de la vlan de hogar que ya este configurado en el switch podrá usar un direccionamiento Ip dinámico otorgado de la vlan 100 correspondiente a la red 192.168.100.X/24 permitiendo así una administración centralizada de las IP a arrendadas dentro del esquema de red, de igual manera si se conecta algún dispositivo a la red wireless se procederá con la asignación de una Ip del segmento 192.168.200.x/24.

Para que este tipo de configuración sea posible debe definirse dentro del Router que hará la encapsulación a través del protocolo 802.1Q mediante una configuración de servidor DHCP ofreciendo así arrendamientos de IP en base a la vlan en la que está configurado el puerto del switch en el que se conecta el dispositivo final como se detalla a continuación en la configuración a través del CLI.

```

tesis_plaza(dhcp-config)#domain-name www.plaza.com
tesis_plaza(dhcp-config)#exit
tesis_plaza(config)#ip dhcp pool invitados
tesis_plaza(dhcp-config)#network 192.168.200.1
% Incomplete command.
tesis_plaza(dhcp-config)#network 192.168.200.0 255.255.255.0
tesis_plaza(dhcp-config)#default-router 192.168.200.1
tesis_plaza(dhcp-config)#dns-server 8.8.8.8
      ^
% Invalid input detected at '^' marker.

tesis_plaza(dhcp-config)#dns-server 8.8.8.8
tesis_plaza(dhcp-config)#domain-name www.plaza.com
tesis_plaza(dhcp-config)#exit
tesis_plaza(config)#

```

Figura 23. Pool de direccionamiento para la vlan Wireless. Elaborado por el autor

```

Enter configuration commands, one per line. End with CNTL/Z.
tesis_plaza(config)#ip dhcp pool
tesis_plaza(config)#ip dhcp pool name
tesis_plaza(config)#ip dhcp pool name ?
  <cr>
tesis_plaza(config)#ip dhcp pool hogar
tesis_plaza(dhcp-config)#network 192.168.100.0 255.255.255.0
tesis_plaza(dhcp-config)#default-rout
tesis_plaza(dhcp-config)#default-router 192.168.100.1
tesis_plaza(dhcp-config)#dns-server 8.8.8.8
tesis_plaza(dhcp-config)#?
  default-router  Default routers
  dns-server      Set name server
  domain-name     Domain name
  exit            Exit from DHCP pool configuration mode
  network         Network number and mask
  no              Negate a command or set its defaults
  option          Raw DHCP options
tesis_plaza(dhcp-config)#domain-name www.plaza.com
tesis_plaza(dhcp-config)#

```

Figura 24. Pool de direccionamiento para la vlan de Hogar. Elaborado por el autor

3.5.5 Asignación de direcciones IP dinámica acorde a VLAN

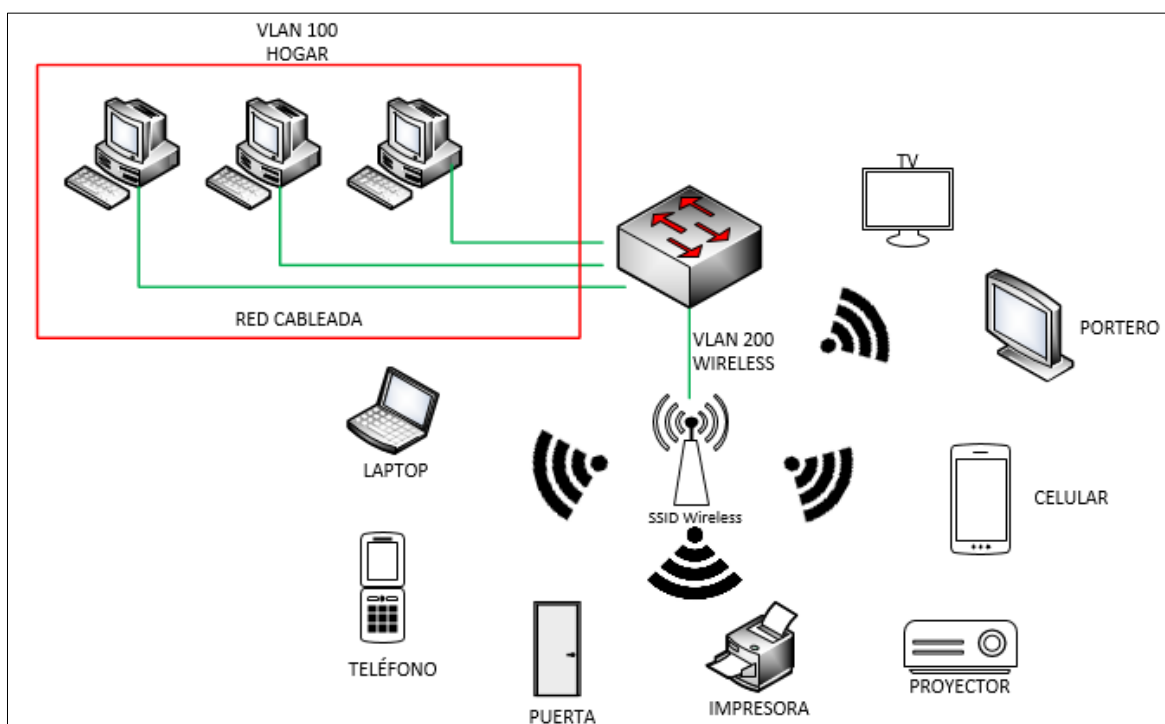


Figura 25. División de la red Wireless y Hogar. Información tomada de Microsoft Visio. Elaborado por el autor

Para verificar que la asignación de direcciones se está realizando desde el Router a los equipos ubicados en la VLAN 100 y 200 es necesario realizar el proceso conocido como DORA (Discover – Offer – Request – Acknowledgment) realizado entre un servidor DHCP y

un equipo que solicita un arrendamiento de dirección IP y así poder comunicarse con los demás dispositivos que están en la misma o diferente subred para ello se verificara que el proceso de asignación se haya completado en el escenario correspondiente y con ello verificar que tanto las PC y componentes de la Red IoT puedan tener una dirección dinámica del servidor interno creado en el Router.

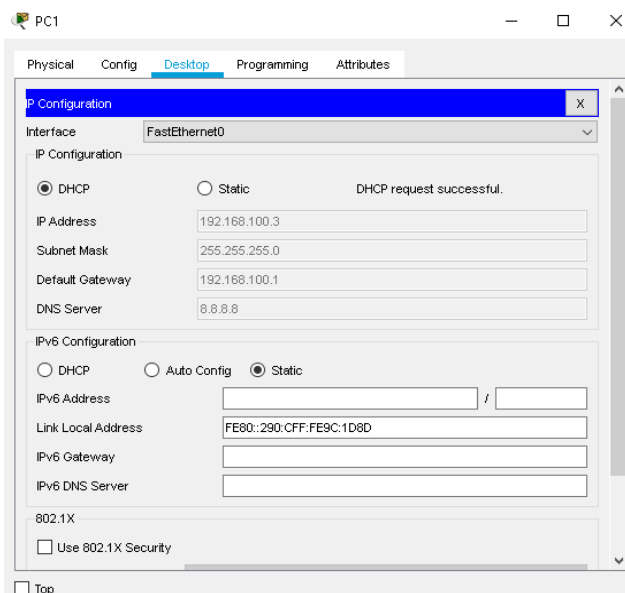


Figura 26. Asignación de IP dinámica VLAN 100 en PC. Elaborado por el autor

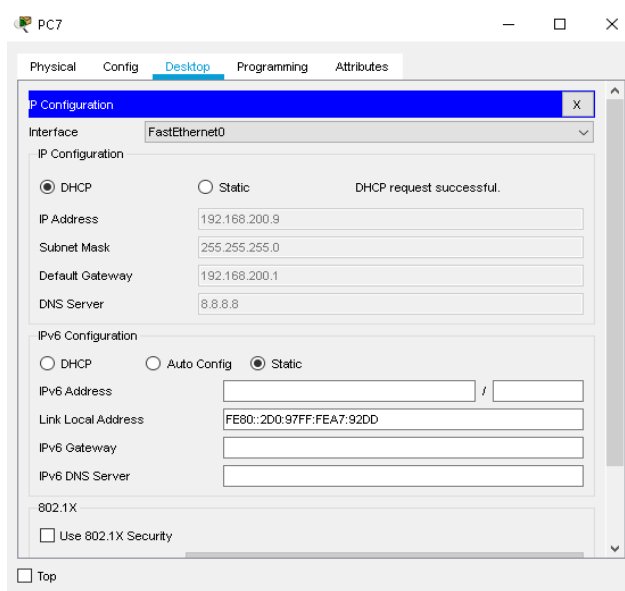


Figura 27. Asignación de IP dinámica VLAN 200 en PC. Elaborado por el autor

Una vez validado que el direccionamiento se entrega de forma correcta a cada uno de los dispositivos pertenecientes a vlans diferentes es necesario aplicar ciertos protocolos de

seguridad más avanzados a nivel de la red LAN previniendo así cualquier tipo de amenaza como a su vez la protección de la red IoT.

3.5.6 Desactivación de protocolos de descubrimiento

Un problema hoy en día muy común a nivel de redes y seguridad informática es dejar los valores que vienen por defecto en equipos de fabricantes pensando que nunca se va a tener un tipo de ataque en la red LAN.

Por lo general este tipo de problema se da por que la persona considera innecesario este proceso o en algunos casos se desconoce del protocolo utilizado y no se modifica pensando a que pueda traer repercusiones a futuro. Si se desea diseñar una red IoT con los correctos niveles de seguridad es necesario hacer uso de la desactivación de los protocolos CDP y LLDP en interfaces que no están siendo utilizadas en la topología de red.

Tanto el protocolo CDP y LLDP son protocolos que se encargan de verificar los vecinos que están en la red es decir hace un mapeo de todos los equipos que estén conectados al switch o Router y una vez eso mediante una tabla muestra información que puede ser muy delicada como puede ser:

- La versión de IOS que ejecuta el equipo
- La plataforma
- La versión
- El puerto por el cual está conectado
- La dirección MAC, entre otros

```

sw_tesis>ena
Password:
sw_tesis#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
tesis_plaza    Gig 0/1         129      R           ISR4300    Gig 0/0/0
tesis_plaza    Gig 0/1         129      R           ISR4300    Gig 0/0/0.100
tesis_plaza    Gig 0/1         129      R           ISR4300    Gig 0/0/0.200
tesis_plaza    Gig 0/1         129      R           ISR4300    Gig 0/0/0.99
sw_tesis#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 28. Protocolo CDP activado. Elaborado por el autor

Este tipo de protocolos como el presentado en la figura anterior podría causar un peligro en el entorno de red debido a que existen herramientas como Yersenia que pueden realizar ataques a este tipo de protocolo encontrando incluso vulnerabilidad en la red con solo unos cuantos clics para su ejecución haciendo que la red se vea afectada en rendimiento e incluso

en el peor de los casos que no esté disponible por prolongados periodos de tiempo. Para ello se debe considerar deshabilitar los protocolos mencionados haciendo que la red no de fallo de vulnerabilidad o que no muestre información que puede ser muy valiosa y delicada para las redes SOHO hoy en día. Cabe destacar que la mayor parte de proveedores cuentan con este tipo de protocolo de descubrimiento el cual puede generar una gran afectación si no se desactiva en interfaces que no son utilizadas.

Para deshabilitar el protocolo CDP como LLDP se debe hacer desde el cómo de configuración Global ya que es el único modo que permite los protocolos de descubrimiento de vecinos no causen alguna afectación en el diseño de la red y prevenir ataques que puedan ser causados por alguien desde adentro. El comando *no cdp run* y *no lldp run* desactivan ambos protocolos del equipo por cuestiones de seguridad.

```
sw_tesis#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw_tesis(config)#no cdp run
sw_tesis(config)#do show cdp neighbor
% CDP is not enabled
sw_tesis(config)#
```

Figura 29. Protocolo CDP activado. Elaborado por el autor

Si solo se quiere desactivar la interfaz específica se puede hacer uso de los comandos *cdp disable* y *no cdp lldp*, es importante mencionar que el proceso a realizarse en el Router va a hacer exactamente igual en cuestión de comandos y protocolos.

Al desactivar tanto CDP como LLDP se tiene mayores niveles de seguridad en la red IoT previniendo los ataques a estos protocolos a través de herramientas de software libre.

3.5.7 Desactivación de DTP (Dynamic Trunking Protocol)

Dynamic Trunking Protocol es utilizado para realizar de forma automática enlaces troncales y permitir el envío de varias vlans a través de un solo enlace esto por lo general reduce los tiempos de implementación, pero a su vez ocasiona que cualquier puerto pueda negociar con el switch y crear un troncal a tal punto de poder analizar las tramas que viajan a través de la red mediante el ataque (VLAN HOPPING ATTACK). Por lo general este tipo de ataque se da en solo equipos Cisco debido a que tienen este protocolo propietario.

Para desactivar DTP en las interfaces que no están siendo utilizadas se requiere del comando *Switchport nonegotiate* con esto el equipo atacante cuando desee establecer una

tronal con el switch va a hacer imposible debido a que su solicitud no se va a poder responder como se presenta a continuación:

[illegible]

Figura 30. Comando para desactivación del protocolo DTP. Elaborado por el autor

Este tipo de solución permite que no haya afectaciones en los dispositivos y con ello no se establezca la comunicación automática como el protocolo DTP lo determina y se explica con más detalles en el capítulo 2.

3.5.8 Configuración de AP en VLAN 200

Como se mencionó hasta ahora en el presente trabajo de investigación todos los dispositivos que se conecten de forma inalámbrica al AP deberán recibir direccionamiento dinámico del Router que funciona como DHCP de la vlan 200 a través del puerto troncalizado que va desde el switch hasta el Router y posteriormente enviado mediante la conexión que existen con el Access Point, para ello se requiere configurar el AP con ciertos parámetros explicados a continuación:

- La forma en la que debe estar trabajando el AP debe ser modo Wireless AP, esta configuración ejecutada en el equipo hará que funcione como un puente transparente trabajando en un modo parecido al switch donde solo pasara

direccionamiento de la vlan solicitada para este caso del segmento 192.168.200.X/24

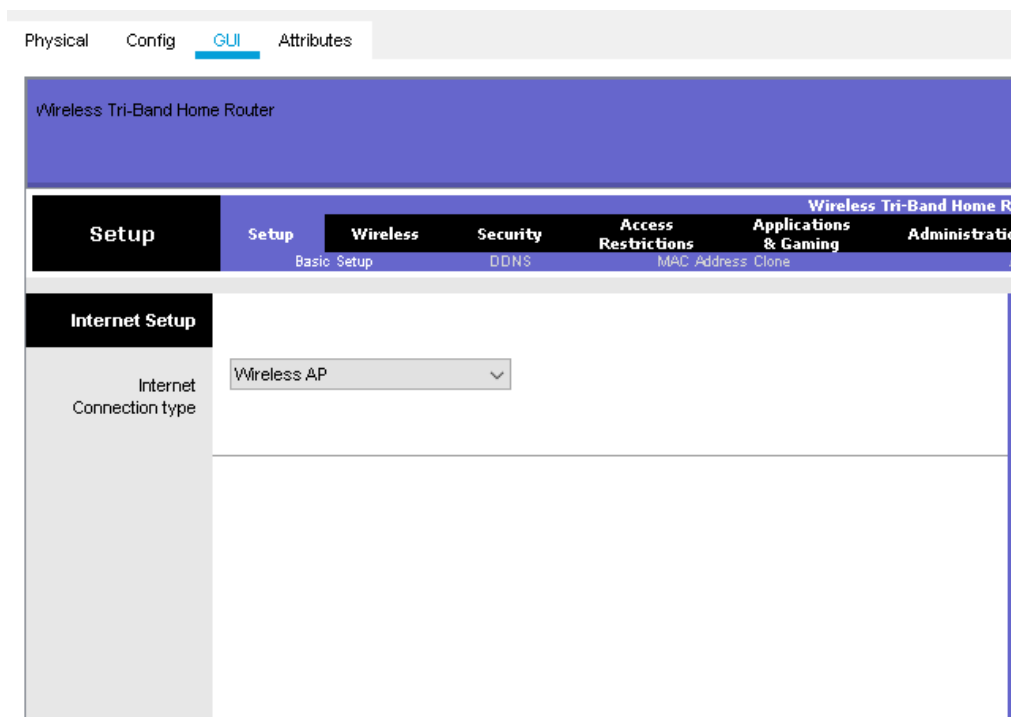


Figura 31. Configuración de AP. Elaborado por el autor

- Luego de haber definido el modo de operación del AP será necesario habilitar las redes que van a estar trabajando dentro de la red Wireless para ello se hará uso de una en la banda de 2.4GHz y otra en 5GHz

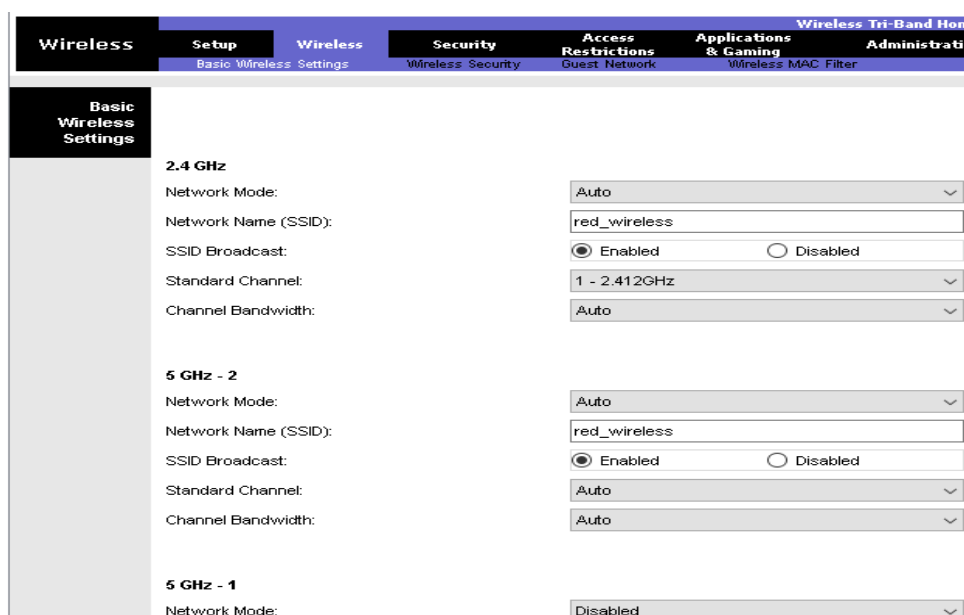


Figura 32. Modo de operación de AP. Elaborado por el autor

- Por último, a toda la conexión Wireless se le debe cifrar la contraseña para ello se requiere del protocolo de autenticación más robusto que soportan estos equipos de la línea Home WPA2. El uso de WPA2 permite trabajar con el cifrado AES como a su vez de CCMP superando al protocolo TKIP en seguridad debido a la forma de generar las claves mediante algoritmos matemáticos complejos

Band	Security Mode	Encryption	Passphrase	Key Renewal
2.4 GHz	WPA2 Personal	AES	tesis123	3600 seconds
5 GHz - 1	WPA2 Personal	AES	tesis123	3600 seconds
5 GHz - 2	Disabled			

Figura 33. Autenticación WPA2. Elaborado por el autor

3.5.9 Prueba de conectividad a la red interna

En este punto se necesita validar que la red interna esté funcionando de manera correcta y que los dispositivos ubicados en diferentes vlans se puedan comunicar en base a las configuraciones previas realizadas como a su vez los niveles de seguridad identificados y aplicados a nivel de redes LAN que pueden ser aplicados en redes IoT.

Para comprobar que la red de manera interna está funcionando se hará uso del protocolo ICMP el cual usará mensajes tipo 3 código 1 indicando que la red está operativa a través de sus mecanismos de solicitud Echo Request (enviado desde el pc que realiza la petición) hasta el Echo Reply (cliente o servidor que envía una respuesta a una solicitud echo) al usar ambas solicitudes de manera correcta se obtendrá una comunicación entre las vlans de hogar y la de red inalámbrica ubicadas en la vlan 100 y la red de la vlan 200 respectivamente.

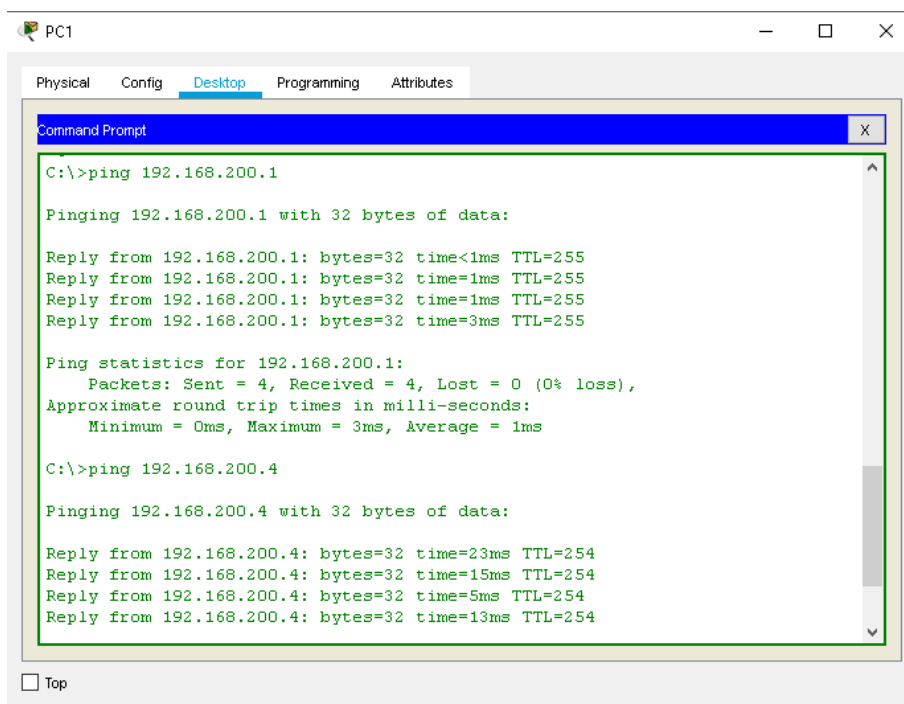


Figura 34. Prueba de conectividad a red wifi desde LAN de hogar. Elaborado por el autor

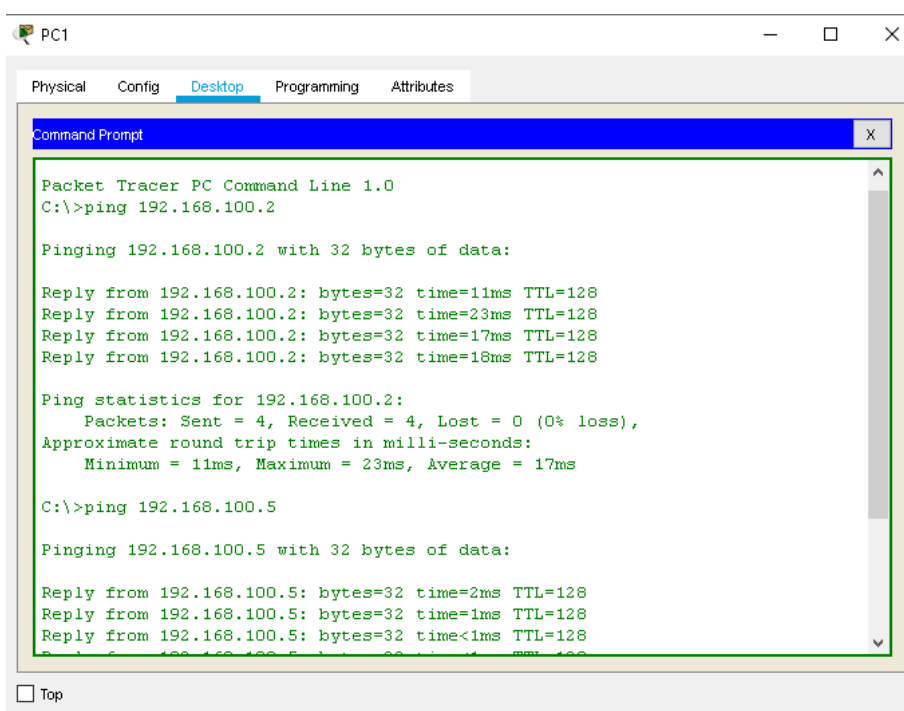


Figura 35. Prueba de conectividad a red hogar. Elaborado por el autor

3.5.10 Conectividad con server externo

Una vez comprobada que la red interna funciona y que existe comunicación entre lans que al principio se encontraban totalmente aisladas unas de otras se debe realizar la configuración de la red para que pueda tener salida a Internet y consultar cualquier servicio

como toda función que el Router realizaría, para ello se procedió a realizar una simulación de un servidor en packet tracer el cual cuenta con un servidor web de ejemplo donde para ello se necesita definir el tipo de protocolo de ruteo que generará la salida. Por lo general el tipo de asignación que se realice asigna una dirección dinámica para la salida del mismo como a su vez de una ruta estática que será utilizada para comunicarse con el Router de borde es decir que el proveedor tiene configurado del otro extremo y así el haga la resolución.

Debido a las limitantes existentes en Packet Tracer y no ser un emulador sino un simulador no se podrá hacer la prueba con una salida a Internet para una petición real, pero si se tiene configurado un esquema en el cual se presenta un servidor que resuelve el nombre de dominio de una página permitiendo así un ejemplo del funcionamiento y como la red IoT saldría a Internet

Por otra parte, es necesario hacer la demostración mediante un servidor DNS ya que una vez determinado el funcionamiento y el rol que se hará se deberá aplicar reglas de ACL o Filtrados a nivel de direcciones IP.

Para probar una conectividad dentro del simulador se procedió a realizar los siguientes procedimientos:

Ruta Estática: dentro del Router interno que tiene la red IoT se procederá a crear una ruta predeterminada o por default por lo general este tipo de direcciones permiten enviar el tráfico desconocido hacia el Router de siguiente salto por lo general el del ISP con la finalidad de que sea enviado a Internet y así obtener respuesta y poder establecer comunicación. Una ruta estática debe ser creada desde el propio Router como se muestra en la imagen:

```
tesis_plaza(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

Figura 36. Ruta estática en Router principal. Elaborado por el autor

El comando Ip route con los parámetros de dirección de Ip y mascara en 0 indican que cualquier coincidencia de paquetes que no esté dentro de la tabla de ruta sea enviada a la dirección Ip vecino es decir a la 10.10.10.2 en este proyecto será la IP del ISP ubicada del otro extremo.

Acceso a server: para cuestión de prueba se ha creado un servidor del otro extremo de la red como se detalló en la figura 13 el cual contiene una página web sencilla la cual se podrá

acceder siempre y cuando exista conectividad por parte de los equipos internos de la red IoT como se muestra a continuación:

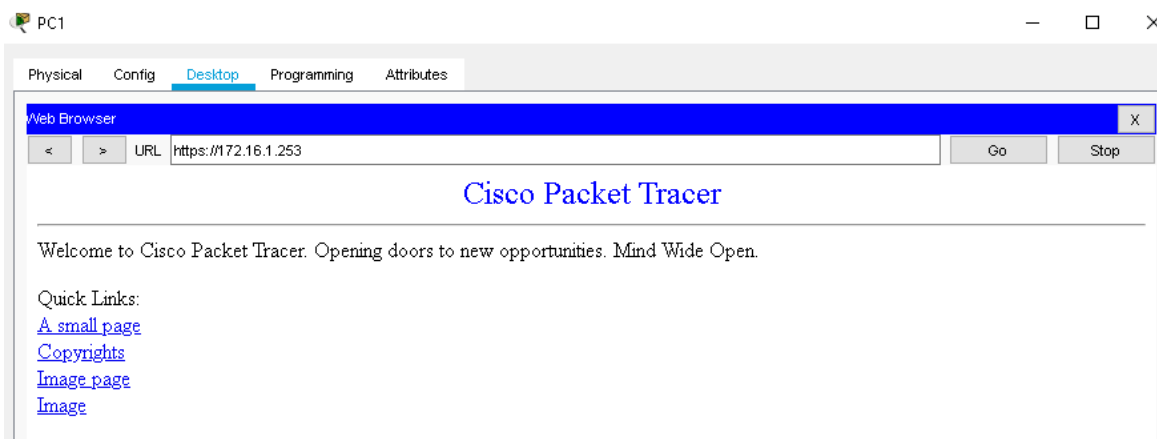


Figura 37. Acceso a servicio desde la Red IoT. Elaborado por el autor

3.5.11 Creación y aplicación de ACL

Es necesario tener ciertas reglas de bloqueo que sean aplicadas al tráfico de entrada o salida de la red en donde se está operando, esto con el fin de prevenir cualquier tipo de amenaza existente.

Hoy en día existen dispositivos de Nueva Generación conocidos como los NGFW que son Firewall que tienen funciones de bloqueo avanzada y protección ante muchos tipos de amenazas actuales debido al uso de DPI (Deep Package Inspection), Deep Learning, Web Filtering, Email Protection y un sinnúmero de características que haría que la red fuera lo más segura posible pero su costo total de operación se vería muy afectado debido a los grandes costos que se manejan.

Por otra parte, existen ciertos equipos que ya traen cierta configuración de filtrado de paquetes a nivel de capa 3 (basado en direccionamiento IP) y de capa 4 (basado en número de puerto) por lo general este tipo de solución estaba incluida en los Firewall de 2da generación, pero actualmente casi todos los Router multimarca los poseen, siendo mucho más factible en su adquisición sin elevado costo de operación como a su vez funciones esenciales a la hora de diseñar reglas de bloqueo.

Por lo general este tipo de reglas en los Router son conocidos como ACL (Listas de control de acceso) las cuales funcionan al igual que un firewall de 2da generación y pueden hacer filtrado en base a coincidencias y aplicar una acción.

Para ello se hará uso de un tipo de ACL en particular (ACL estándar) y se creará reglas en base a los requerimientos que se necesitan para tener acceso a un servicio y a su vez evitar cualquier amenaza externa.

Un factor importante a mencionar es que las ACL de tipo estándar deben aplicarse lo más cerca del origen es decir que toda configuración realizada a continuación será aplicada en el Router que conecta la red Wireless con la red de Hogar debido a que este proceso consume menos recursos como ancho de banda y procesamiento.

Como se indicó anteriormente se ha creado un servidor web ubicado en Internet con la dirección IP 172.16.1.254 al cual los usuarios podrán tener acceso desde la red interna por otra parte el diseño presentado en la figura #35 muestra un individuo en este caso un atacante que quiere ingresar desde Internet a los recursos ubicados al lado derecho pertenecientes a la VLAN 100 que es de hogar y la VLAN 200 que es Wireless donde se conectarán los dispositivos IoT para ello se procederá a realizar la aplicación de la ACL y explicar lo realizado.

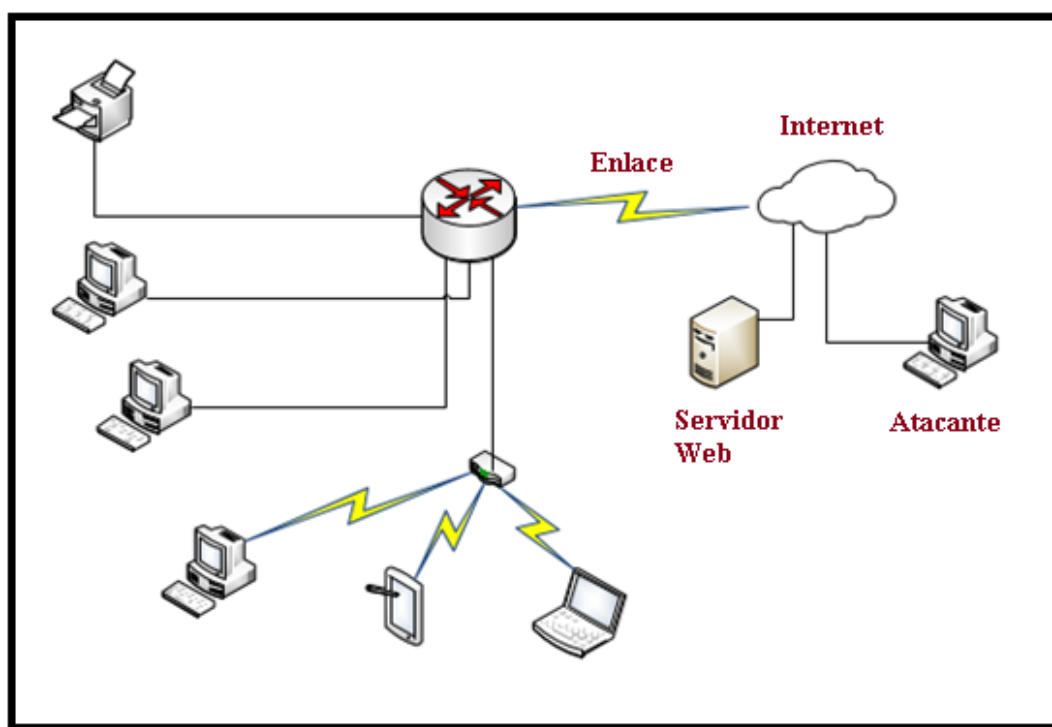


Figura 38. Esquema en base atacante y servidor ubicados en Internet. Elaborado por el autor

Como se explicó con anterioridad para crear una regla de ACL se debe aplicar al Router más cerca al origen es decir el equipo que se está administrando ya que esto reducirá problemas de latencia y rendimiento, a su vez toda configuración que se realice referente a las ACL debe aplicarse en el modo de configuración global debido a que permitirá hacer cambios a la memoria de configuración y surtirán efecto.

Toda configuración de ACL necesita definirse varios puntos antes de ser aplicada en la configuración como son:

- Determinar a que se le aplicara ACL.
- Definir el número que identifica si es una ACL estándar por lo general van desde el 1 al 99.
- Determinar cuál será la función de la ACL en base a 2 criterios permit, deny o any.
 - Permit: permite que una Ip o red tenga conectividad
 - Deny: bloquea el tráfico de una Ip o red
 - Any: selecciona todo
- Especificar la dirección de host o dirección de red a la que se le aplicara la ACL.
- Determinar la Wildcard para saber cuántos dispositivos se les aplicara la ACL.
- Ingresar a la interfaz donde se aplicará la ACL.
- Ingresar el comando ip Access-Group con el número de ACL creado con anterioridad y
- al final indicar si se analizara en la entrada o a la salida del mismo
- Guardar cambios.
- Probar conectividad.

Para realizarse la configuración del equipo es necesario determinar una serie de líneas de código como las presentada con anterioridad a través del CLI, donde ya definido el sentido de la aplicación de la ACL se procede con la configuración de los pasos anteriores en base a las buenas prácticas de seguridad donde se define que:

- Se permita que todo tráfico que venga de la red C 192.168.100.0 correspondiente a la red de hogar con comodín 0.0.0.255 tenga permisos de conectividad.
- Permitir que toda la red de clase C 192.168.200.0 perteneciente a la Wireless con comodín de máximo 255 usuarios que se les aplicara la acl tengan conectividad.
- Bloquear toda dirección que no coincida con ninguna de las anteriores.

```

tesis_plaza>enable
Password:
tesis_plaza#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
tesis_plaza(config)#access-list 1 permit 192.168.100.0 0.0.0.255
tesis_plaza(config)#access-list 1 permit 192.168.200.0 0.0.0.255
tesis_plaza(config)#access-list 1 deny any
tesis_plaza(config)#

```

Figura 39. Configuración de ACL en Router de origen. Elaborado por el autor

Luego de determinar forma de la aplicación de la ACL hacia a internet se debe colocar en una interfaz que realice el match y de coincidir aplique una acción basado en primera coincidencia para ello se procede a colocar la regla en la interfaz que se conecta a la LAN es decir el puerto Gi0/0 debido a que es el único que se conecta al Switch y como se mencionó anteriormente por ser el más cerca al origen.

```

tesis_plaza(config)#interface gi0/0
tesis_plaza(config-if)#ip access-group 1 in
tesis_plaza(config-if)#

```

Figura 40. Aplicación de ACL en la Interfaz. Elaborado por el autor

Para ver la configuración realizada referente a la ACL creada en la red se usará el comando *show Access-list 1* esto mostrará toda la información con el ID de la ACL creada en este caso la #1 con las reglas ya establecidas anteriormente.

```

tesis_plaza(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

```

Figura 41. Información de las AC. Elaborado por el autor

Esta configuración permite que todos los segmentos en las vlan 100 y vlan 200 puedan tener conexión con dispositivos externos de la red que existen por lo que si se comprueba conectividad con el servidor web se tendría conectividad como se muestra en la figura:

```

C:\>ping 172.16.1.253

Pinging 172.16.1.253 with 32 bytes of data:

Reply from 172.16.1.253: bytes=32 time=1ms TTL=126
Reply from 172.16.1.253: bytes=32 time=9ms TTL=126
Reply from 172.16.1.253: bytes=32 time=7ms TTL=126
Reply from 172.16.1.253: bytes=32 time=13ms TTL=126

Ping statistics for 172.16.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 7ms

C:\>|

```

Figura 42. Comunicación exitosa luego de aplicar ACL. Elaborado por el autor

Una vez determinadas las redes que tienen acceso o no se debe crear una regla de ACL que indique los dispositivos a los cuales se podrá acceder desde internet a nuestra red y a cuáles no esto con el fin de aumentar la seguridad en el perímetro para ello se ha establecido lo siguiente:

- Permitir todo tráfico que provenga del segmento de red donde se encuentra el proveedor de servicio hacia la red IoT
- Permitir el tráfico del 172.16.1.1 Router en el esquema ubicado en Internet
- Permitir todo paquete que venga desde el servidor web en respuesta a peticiones ICMP Request por parte de la LAN de la infraestructura diseñada
- Descartar todo tráfico que no coincida
- Ingresar a la interfaz
- Agregar si es de entrada o salida

```

tesis_plaza(config)#access-list 2 permit 10.10.10.0 0.0.0.3
tesis_plaza(config)#access-list 2 permit host 172.16.1.1
tesis_plaza(config)#access-list 2 permit host 172.16.1.253
tesis_plaza(config)#access-list 2 deny any
tesis_plaza(config)#interface s0/1/0
tesis_plaza(config-if)#ip access-group 2 in

```

Figura 43. Aplicación de ACL para tráfico desde la WAN. Elaborado por el autor

Como se mencionó anteriormente todo tráfico que no corresponda a las reglas detalladas en la parte superior será descartado esto con el fin de impedir que alguien desconocido acceda los recursos internos que se poseen en la red IoT, es decir que la IP 172.16.1.254 de la maquina ubicada a la derecha del esquema principal y ningún otro equipo podrá acceder a los recursos o tener comunicación con los equipos de la red interna de las vlan 100 y 200

debido a que la ACL filtraría todo tráfico que provenga de esas direcciones aumentando los niveles de seguridad en la red haciéndola más segura y confiable.

Al realizar solicitudes ICMP Request desde el PC que está ubicado en la WAN se observa que no tendrá acceso a los recursos internos de la red LAN creada debido a que no hay una regla que le permita por lo que es descartado por parte del filtrado aplicado en el Router.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address.....:
FE80::205:5EFF:FE33:9E24
    IP Address.....: 172.16.1.254
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 172.16.1.1

Bluetooth Connection:

    Link-local IPv6 Address.....: ::
    IP Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0
```

Figura 44. IP del atacante ubicando fuera de la red Interna. Elaborado por el autor

```
C:\>ping 192.168.100.5

Pinging 192.168.100.5 with 32 bytes of data:

Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.

Ping statistics for 192.168.100.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.200.1

Pinging 192.168.200.1 with 32 bytes of data:

Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.
Reply from 10.10.10.1: Destination host unreachable.

Ping statistics for 192.168.200.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 45. Ping sin éxito por parte del atacante. Elaborado por el autor

De requerir o permitir otro servicio se debería habilitar otra ACL que permita la entrada de tráfico por lo general todos los servicios o protocolos seguros establecidos por la IANA

tienen acceso a las peticiones que se realizan desde la red LAN es decir no se requiere crear ACL debido a que cuentan con los certificados de confianza como de algoritmos de encriptación robustos.

3.5.12 Bloqueo de interfaces mediante Port-security

El uso de port-security dentro del presente entorno de red permitirá un mejor rendimiento y protección a nivel de seguridad tanto física y así prevenir ataques a nivel lógico que pueden ser producidos por personas externas o internas de la red SOHO. Para ello se debe de considerar el formato de aplicación y a su vez el beneficio que puede presentar en la red.

Un punto a considerar es que Port-security es un protocolo estándar que puede ser aplicado desde cualquier fabricante de equipos de red permitiendo una administración más robusta y eficiente en sus diferentes modos de operación los que se detallan para mejor entendimiento a continuación:

Shutdown: comando utilizado en el presente trabajo de investigación para desactivar la interfaz siempre y cuando el dispositivo conectado al puerto que tiene configurado port-security no sea el legítimo, al hacer esto el atacante no tendrá paso a la red LAN ni a los recursos que posee impidiendo realizar su post explotación de vulnerabilidades en el sistema que se maneja en la red IoT.

Protect: se encarga de descartar todo tráfico, pero sin desactivar la interfaz ni mandando algún tipo de notificación haciendo que el proceso sea complicado de usar para el desarrollo del esquema de red en el presente trabajo debido al alto conocimiento de monitoreo y supervisión que se le debe hacer a los logs del sistema del equipo.

Restrict: proceso que permite descartar tráfico que pasar por una interfaz de un equipo que no está validado dentro de la seguridad emitiendo contadores de falla de entrega que pueden ser revisados.

3.5.12.1 Configuración de Port-Security

Para activar port-security en una interfaz y esta pueda comenzar a trabajar en el esquema de red permitiendo que tráfico pase y que no por la red se debe configurar ciertos parámetros que son presentados a continuación:

```

sw_tesis#conf t
Enter configuration commands, one per line. End with CNTL/Z.
sw_tesis(config)#interface range fa0/1-4
sw_tesis(config-if-range)#switchport port-security
sw_tesis(config-if-range)#switchport port-security mac-address sticky
sw_tesis(config-if-range)#switchport port-security violation shutdown
sw_tesis(config-if-range)#switchport port-security maximum 5

```

Figura 46. Configuración de Port-Security. Elaborado por el autor

Es necesario establecer la función de cada comando para mejor entendimiento de configuración, un punto a mencionar es que no importa el orden en cómo se esté configurando el IOS establecerá la configuración de manera correcta una vez terminado el ingreso de comandos en la CLI.

- *Switchport port-security*: Habilita el uso de port-security en la interfaz en la que se va a permitir la conexión de equipos
- *Switchport port-security mac-address sticky*: Hace que las MAC de los dispositivos se registren de manera dinámica en el switch optimizando el proceso que por lo general se aplica de manera manual
- *Switchport port-security violation shutdown*: Establece el tipo de violación a aplicarse cuando un dispositivo que no corresponde desee enviar tráfico a través de los puertos configurados con port-security
- *Switchport port-security maximum ___*: Declara la cantidad total máxima de direcciones MAC que deben ser registradas en el equipo y el resto ya serán descartadas acorde al tipo de violación definido

Para mejor entendimiento se procede a mostrar la configuración mencionada en el equipo una vez ya registrada.

```

sw_tesis#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             0             1             Shutdown

```

Figura 47. Configuración de Port-Security. Elaborado por el autor

Con la configuración ya ingresada y parámetros establecidos se procederá a crear una violación desde otro dispositivo que se conectará de forma ilícita sin ningún permiso a uno de los puertos configurados con port-security en el switch debido a que son los que están

encendidos ya que los demás puertos fueron desactivados por mejores prácticas como se explica en la figura 18.

Para validar que todo funciona se procederá a realizar el envío de paquetes desde un PC conectado en uno de los puertos que tiene port-security y se comprobará que el ping será exitoso debido a que cumple con la regla de sticky y el máximo permitido para ello como se muestra a continuación:

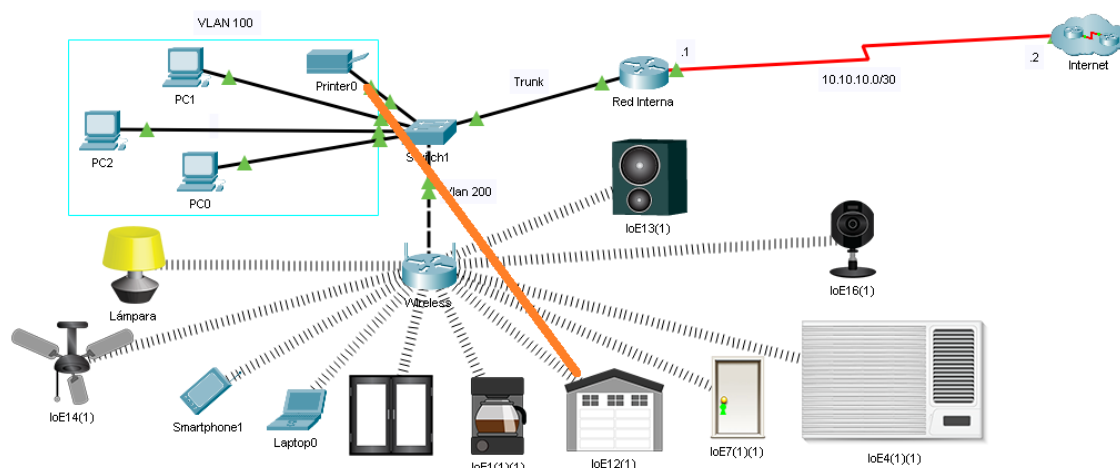


Figura 48. Ping desde la impresora hasta el garaje. Elaborado por el autor

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	E
	Successful	Printer0	IoE12(1)	ICMP		0.000	N	0	0

Figura 49. Comprobación de ping exitoso. Elaborado por el autor

Se verifica que el proceso realizado hasta ahora es exitoso por lo que se procederá a realizar el cambio de la impresora por otro equipo el cual obtendrá tratará de obtener un direccionamiento y al querer enviar un mensaje no será posible debido a que port-security está activado haciendo que la interfaz se apague como se muestra a continuación:

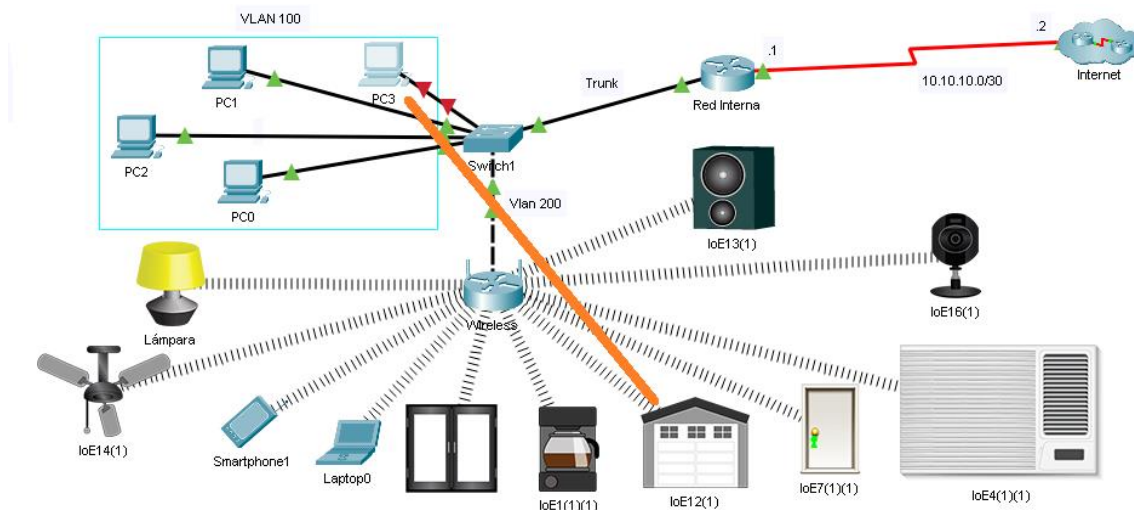


Figura 50. Desactivación de interfaz debido a configuración port-security. Elaborado por el autor

Como se observa en la figura se cambió la impresora por una PC denominada PC3 y al conectarse automáticamente el puerto se apaga debido a la función aplicada en port-security, en la cual solo 5 mac se pueden registrar y al llegar un nuevo equipo para registrarse en un puerto que ya estaba ocupado por las otras pc cableadas y el access point de la vlan 200 se procederá apagar, como dato adicional se verifica que el direccionamiento asignado a la PC3 no será ninguno.

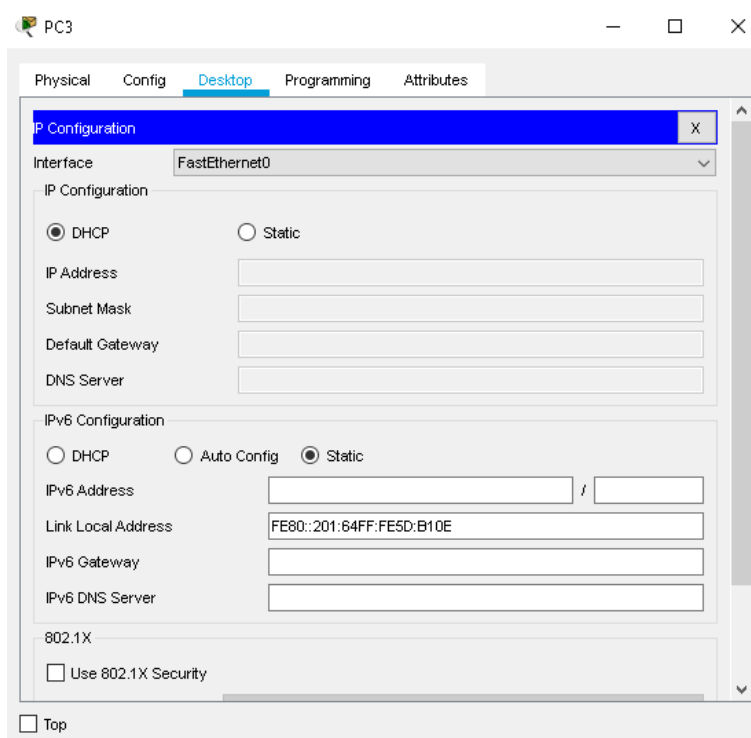


Figura 51. Asignación de IP errónea. Elaborado por el autor

Por último, para ver el comportamiento que port-security aplico en la interfaz se procederá por ingresar el comando *show port-security interface fa0/5* donde la interfaz es donde la impresora estaba conectada y ahora está el nuevo equipo es decir PC3.

```

sw_tesis#
sw_tesis#show port-security interface fa0/5
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0001.645D.B10E:100
Security Violation Count : 1

```

Figura 52. Comportamiento de la interfaz debido a port-security. Elaborado por el autor

Lo que se debe de observar dentro de la configuración son los siguientes parámetros:

- **Port Security:** indica si port-security está funcionando en la interfaz o no.
- **Port Status:** indica cual sería el estado del puerto en este caso mostrará la violación efectuada por un dispositivo por lo que mostrará el mensaje con el código de apagado junto a él.
- **Violation Mode:** indica específicamente que tipo de violación se debe de cumplir en la interfaz de haber alguien que busca acceder de forma ilícita
- **Last Source Address :Vlan :** muestra la dirección MAC del dispositivo que está efectuando la violación por lo que en efectos de auditoría esto sería de gran ayuda para identificar de que equipo proviene la amenaza si es de forma local.
- **Security Violation Count:** muestra el número de contadores que se incrementan por la violación existente por lo general en el modo shutdown solo se aumentará en 1.

Para que la interfaz vuelva a operar con el equipo que estaba anteriormente se deberá apagar y encender la interfaz de forma manual lo que a la larga toma mayor tiempo realizarse, pero su nivel de seguridad es muy útil debido a la protección de la red.

```

sw_tesis(config)#interface fa0/5
sw_tesis(config-if)#shut

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down
sw_tesis(config-if)#no shut

```

Figura 53. Encendido de interfaz de manera manual. Elaborado por el autor

Por último, se vuelve a ejecutar el comando `show port-security interface fa0/5` para ver el estado de la interfaz y los contadores de violación y el modo apagado ya no estará debido a que no habido otro intento de conexión.

```

show port-security interface fa0/5
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode                : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 1
Last Source Address:Vlan     : 0001.645D.B10E:100
Security Violation Count     : 0

```

Figura 54. Funcionamiento de port-security al reiniciar la interfaz. Elaborado por el autor

Con este tipo de soluciones lo que se busca es brindar la mayor disponibilidad posible en la red IoT reduciendo amenazas de tipo internas o externas y con ello mantener la seguridad de la información lo más segura posible en base a la TRIA donde la red IoT no se vea afectada a nivel de red LAN.

3.6. Conclusiones y Recomendaciones

3.6.1 Conclusiones

- Los protocolos de seguridad aplicados en una red IoT en entorno LAN permitió reducir los tipos de vulnerabilidades existentes debido a las malas prácticas aplicadas en las configuraciones de los equipos como Router, Switch y AP por desconocimiento.
- El simulador Packet Tracer permitió ventajas en cuanto a entornos de redes IoT a diferencia de otros simuladores debido a su facilidad de uso y la integración de nuevos componentes.

- La aplicación de vlans en el diseño de red presentado permitió reducir los dominios de broadcast como la segmentación acorde a puerto o incluso al tipo de aplicación o uso.
- El uso de ROAS y la asignación de DHCP permitió tener una administración más centralizada de la red y control de tráfico debido a la creación de diferentes subinterfaces que permitían la comunicación entre vlans
- La implementación de ACL permitió asegurar el tipo de tráfico que viaja de la LAN a la WAN y viceversa permitiendo asegurar la comunicación y limitar acceso a toda máquina desconocida desde Internet.
- La aplicación de port-security permite un estricto control de las interfaces permitiendo realizar validaciones en base a direcciones MAC de equipos con lo que el nivel de confianza en la red aumenta y detiene las amenazas existentes.

3.6.2 Recomendaciones

- Se recomienda realizar el escenario en entornos emulados donde se presente la arquitectura de seguridad que puede ser aplicada en la practica
- Hacer uso de un servidor Radius que permita la autenticación de forma centralizada en base a usuarios o equipos registrados evitando cualquier tipo de vulnerabilidad
- Tener un gestor de contraseña que permita validar el acceso a la persona indicada
- Aplicar mecanismos de pentesting sobre entorno realizado y comprobar la efectividad de la seguridad existente de la red.
- Hacer uso de Access Point actuales que permitan pasar varias vlans a través de la red permitiendo así dividir en múltiples grupos y segmentar de mejor manera la infraestructura de red
- Hacer uso de un servidor centralizado que permita entregar direccionamiento a toda la red existente evitando sobrecarga de procesos al Router principal y con ello tener mejor procesamiento en la trama de datos.

ANEXOS

Anexo 1.

Preguntas de Entrevista

- 1) ¿Que es el Internet de las Cosas (IoT)?
- 2) ¿Qué beneficios tiene el Internet de las cosas (IoT)?
- 3) ¿Qué efecto tendrá el Internet de las Cosas (IoT) en nuestras vidas diarias?
- 4) ¿Considera que la comunicación entre dispositivos en un entorno IoT es segura?
- 5) ¿Qué seguridades se deberían considerar en los dispositivos del IoT?
- 6) ¿Cree usted que el Ecuador está listo para el uso del Internet de las cosas?

Anexo 2.

Instalacion de Cisco Packet Tracer

1.- Descarga de Cisco Packet Tracer

Descargar

Elija el sistema operativo que está usando y descargue los archivos relevantes. Lea las [preguntas frecuentes](#). Vea los [tutoriales](#).

Packet Tracer requerirá autenticación con su usuario y contraseña cuando lo utilice por primera vez y para cada inicio de sesión en un SO nuevo. (1)

¿Está pensando en actualizar?

Para CCNA 7, Packet Tracer 7.3.0 es la versión mínima que admite CCNA 7.

Para CCNA 6 (y versiones anteriores), recomendamos a los instructores y alumnos que permanezcan con Packet Tracer 7.2.2.

Si está estudiando o enseñando los cursos CCNA 6 y 7, utilice Packet Tracer 7.3.0+.

Al utilizar Packet Tracer 7.3.0+ para CCNA 6, existe una pequeña posibilidad de que pueda encontrar un mensaje de advertencia.

Si es así, puede ignorar el mensaje. Es simplemente una advertencia de que los scripts en este archivo deben actualizarse para la compatibilidad con Packet Tracer 7.3.0+.

LA DESCARGA, LA INSTALACIÓN O EL USO DEL SOFTWARE CISCO PACKET TRACER CONSTITUYE LA ACEPTACIÓN DEL [ACUERDO DE LICENCIA DEL USUARIO FINAL](#) ("EULA") DE CISCO Y EL [ACUERDO COMPLEMENTARIO DE LICENCIA DEL USUARIO FINAL](#) DE CISCO PACKET TRACER ("SEULA"). SI NO ESTÁ DE ACUERDO CON TODOS LOS TÉRMINOS DEL EULA Y EL SEULA, NO DESCARGUE, INSTALE NI USE EL SOFTWARE.

Windows versión 8.0 para equipos de escritorio (en inglés)

[Descarga de 64 bits](#)

[Descarga de 32 bits](#)

Linux versión 8.0 para equipos de escritorio (en inglés)

[Descarga de 64 bits](#)

MacOS versión 8.0 (en inglés)

[Descargar](#)

Activar Windows

Ve a Configuración para activar Windows.

Figura 55. Descarga de Cisco Packet Tracer. Información tomada de netacad.com. Elaborado por el autor

2.- Aceptación de términos y condiciones

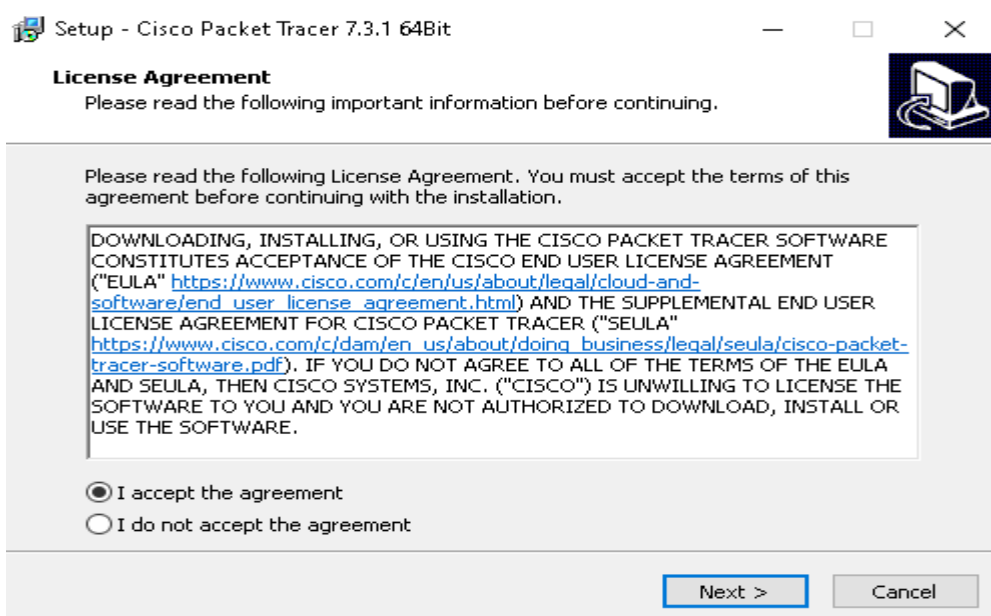


Figura 56. Aceptación de términos y condiciones. Elaborado por el autor

3.- Ubicación de la carpeta de almacenamiento

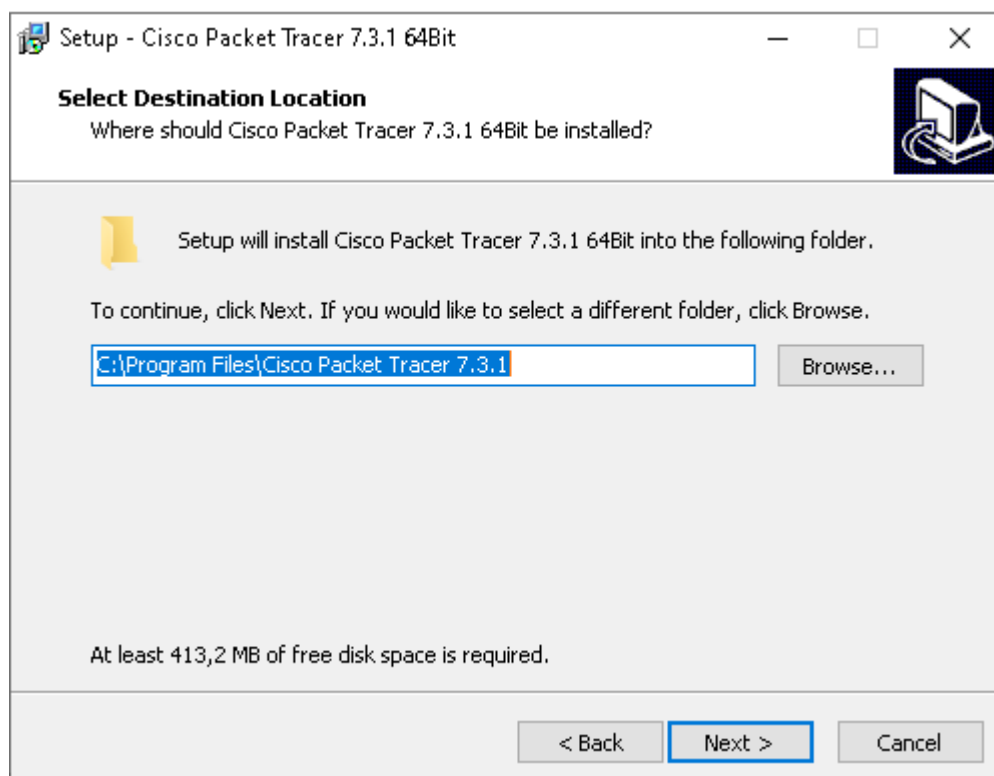


Figura 57. Ubicación de la carpeta de almacenamiento. Elaborado por el autor

4.- Instalación del programa

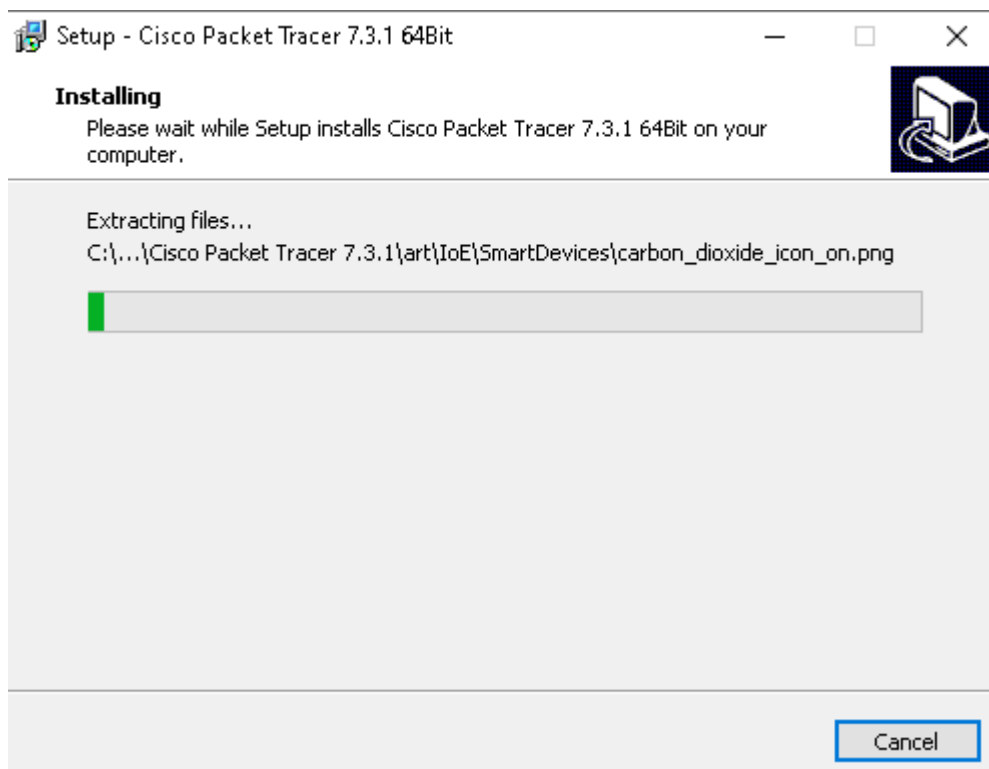


Figura 58. Instalación del programa. Elaborado por el autor

5.- Programa instalado y en ejecución

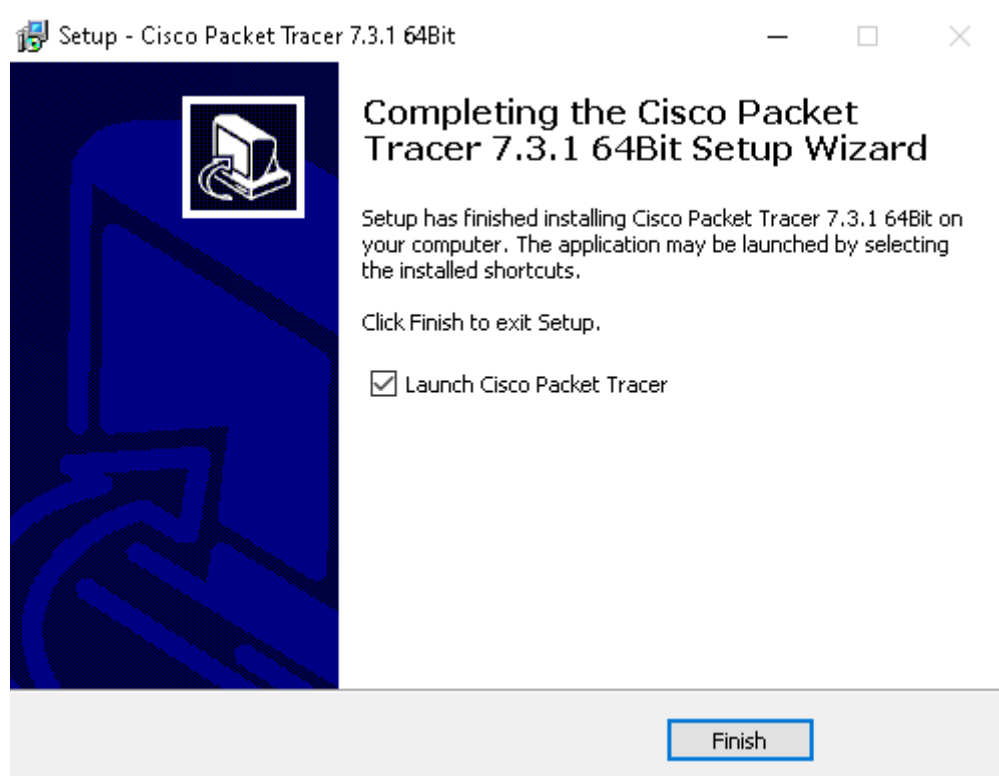


Figura 59. Programa instalado y en ejecución. Elaborado por el autor

6.- Interfaz gráfica de Cisco Packet Tracer

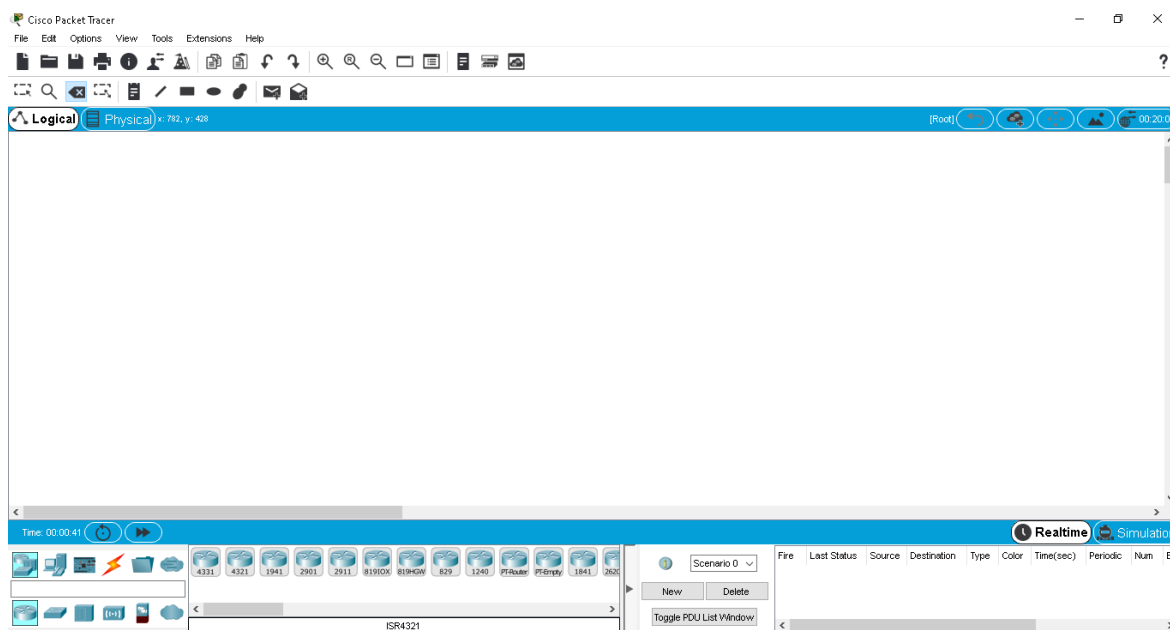


Figura 60. Interfaz gráfica de Cisco Packet Tracer. Elaborado por el autor

Anexo 3.

Configuración del Switch

```
sw_tesis# show run
Building configuration...
Current configuration: 2064 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname sw_tesis
!
enable secret 5 $1$mERr$lt3SJdThevu26qbvOq4Vi1
!
ip domain-name www.plaza.com
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
description vlan 100 usuarios
switchport access vlan 100
switchport mode access
!
interface FastEthernet0/2
description vlan 100 usuarios
switchport access vlan 100
switchport mode access
!
interface FastEthernet0/3
description vlan 100 usuarios
switchport access vlan 100
switchport mode access
!
interface FastEthernet0/4
description vlan 200 seguridad wifi
switchport access vlan 200
switchport mode access
!
interface FastEthernet0/5
description troncal con el router
switchport access vlan 100
switchport mode access
```

```
!  
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  
switchport trunk native vlan 99  
switchport mode trunk  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
no ip address  
shutdown  
!  
interface Vlan20  
mac-address 0060.7003.4401  
no ip address  
!  
interface Vlan100  
mac-address 0060.7003.4402  
no ip address  
!  
line con 0  
password tesis  
!  
line vty 0 4  
password tesis123  
login local  
transport input ssh  
line vty 5 15  
password tesis123  
login local  
transport input ssh  
!  
end
```

Anexo 4.

Configuración del Router

```
tesis_plaza#show run
Building configuration...
```

```
Current configuration: 1954 bytes
```

```
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname tesis_plaza
!
enable secret 5 $1$mERr$lt3SJdThevu26qbvOq4Vi1
!
ip dhcp pool hogar
network 192.168.100.0 255.255.255.0
default-router 192.168.100.1
dns-server 8.8.8.8
domain-name www.plaza.com
ip dhcp pool invitados
network 192.168.200.0 255.255.255.0
default-router 192.168.200.1
dns-server 8.8.8.8
domain-name www.plaza.com
!
no ip cef
no ipv6 cef
!
username plaza password 0 tesis123
!
ip ssh version 2
no ip domain-lookup
ip domain-name www.plaza.com
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
no ip address
ip access-group 1 in
duplex auto
speed auto
!
interface GigabitEthernet0/0/0.99
encapsulation dot1Q 99 native
no ip address
!
interface GigabitEthernet0/0/0.100
```

```
encapsulation dot1Q 100
ip address 192.168.100.1 255.255.255.0
!
interface GigabitEthernet0/0/0.200
encapsulation dot1Q 200
ip address 192.168.200.1 255.255.255.0
!
interface GigabitEthernet0/0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/1/0
ip address 10.10.10.1 255.255.255.0
ip access-group 2 in
clock rate 2000000
!
interface Serial0/1/1
no ip address
clock rate 2000000
!
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 10.10.10.0 0.0.0.3
access-list 2 permit host 172.16.1.1
access-list 2 permit host 172.16.1.253
access-list 2 deny any
!
line con 0
password cisco
!
line aux 0
```

```
!  
line vty 0 4  
password tesis123  
login local  
transport input ssh  
line vty 5 15  
password tesis123  
login local  
transport input ssh  
!  
End
```

Bibliografía

- Ballard, D. (10 de Mayo de 2016). *Red Hat*. Obtenido de <https://www.redhat.com/es/blog/intro-internet-things>
- Barberá, A. B. (2016). Arquitectura de referencia en el Internet of things. *SUNQU*, I(11), 11-13.
- Barcia, A. (30 de Mayo de 2018). *Conoce sobre informática*. Obtenido de <https://conocesobreinformatica.com/packetracer-redes/>
- Bembibre, V. (Enero de 2009). *Definición ABC*. Obtenido de <https://www.definicionabc.com/tecnologia/router.php>
- Cabrera, J. (27 de Diciembre de 2019). *Nobbot*. Obtenido de <https://www.nobbot.com/redes/que-es-un-switch-y-como-funciona/>
- Cabrera, R. (6 de Marzo de 2020). *Desafío hosting*. Obtenido de <https://desafiohosting.com/que-es-ssh/>
- Calvo del Olmo, Á. (31 de Diciembre de 2018). *Universidad Oberta de Catalunya*. Obtenido de <http://hdl.handle.net/10609/89625>
- Crespo, A. (29 de Noviembre de 2016). *Redes Zone*. Obtenido de <https://www.redeszone.net/2016/11/29/vlans-que-son-tipos-y-para-que-sirven/>
- Crespo, A. (24 de Abril de 2018). *RedesZone*. Obtenido de <https://www.redeszone.net/2018/04/24/ssid-red-wi-fi-modificacion/>
- De luz, S. (13 de Septiembre de 2017). *Redes zone*. Obtenido de <https://www.redeszone.net/2017/09/13/como-configurar-la-opcion-de-seguridad-port-security-en-el-switch-d-link-dxs-1100-10ts/>
- Del Valle, L. H. (22 de Enero de 2015). *Programarfacil*. Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/28812/1/Tesis_%20t1489ec.pdf
- Delclós, T. (16 de Mayo de 2007). *El País*. Obtenido de https://elpais.com/diario/2007/05/17/ciberpais/1179368665_850215.html
- Empey, C. (13 de Agosto de 2018). *avastblog*. Obtenido de <https://blog.avast.com/es/como-proteger-tu-casa-inteligente>
- Feijóo, A. (7 de Junio de 2017). *beBee*. Obtenido de <https://www.bebec.com/producer/@http-alfredo-j-feijoo-webnode-es-contacto/dispositivos-iot-la-red-de-las-cosas-protocolos-de-comunicacion>
- García, I. (5 de Febrero de 2018). *Economiasimple.net*. Obtenido de <https://www.economiasimple.net/glosario/servidor>

- González, C. (25 de Enero de 2021). *ADSLZone*. Obtenido de <https://www.adslzone.net/como-se-hace/wifi/activar-dhcp/>
- Hron, M. (30 de Septiembre de 2019). *avastblog*. Obtenido de <https://blog.avast.com/es/el-internet-de-las-cosas-c%C3%B3mo-las-vulnerabilidades-de-una-simple-cafetera-simbolizan-un-mundo-de-riesgos-avast>
- José, R. L. (2018). *Investigación experimental*. Oaxaca de Juárez, Oaxaca.
- LLamas, L. (21 de Febrero de 2019). *Luisllamas*. Obtenido de <https://www.luisllamas.es/protocolos-de-comunicacion-para-iot/>
- Lueth, K. L. (8 de Agosto de 2018). *IOT ANALYTICS*. Obtenido de <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>
- Mateo, I. (Julio de 2018). Methodology of computer security management for the internet of things. *Espirales*.
- Moisa, J. (21 de Marzo de 2019). *Cisco*. Obtenido de <https://community.cisco.com/t5/documentos-routing-y-switching/protocolo-cdp-y-lldp/ta-p/3404827>
- Molina, J., & Gordon, J. (2016). *Hacking the IoT: When Good Devices Go Bad.*, (pág. 27). San Francisco.
- Morales, N. (2014). Investigación Exploratoria: Tipos, Metodología y Ejemplos. 9.
- Páramo, H. (18 de Junio de 2011). *Neuromarketing y tecnologia*. Obtenido de <https://neuromarketingytecnologia.com/configuracion-de-acls/>
- Pérez Porto, J., & Merino, M. (2011). *definicion.de*. Obtenido de <https://definicion.de/red-inalambrica/>
- Raffino, M. E. (22 de Julio de 2020). *Concepto.de*. Obtenido de <https://concepto.de/red-lan/>
- Rose, Eldridge, & Chapin. (2015). La internet de las cosas - una breve reseña. *Internet Society*, 5.
- Sancho, H. C. (Mayo de 2017). Cybersecurity. Introduction to Dossier. *Latinoamericana de Estudios de Seguridad*(20), 8-15. Recuperado el 24 de Enero de 2021, de <https://revistas.flacsoandes.edu.ec/urvio/article/view/2859/1603>
- Stanislav, M., & Beardsley, T. (29 de Septiembre de 2015). HACKING IOT: A CASE STUDY ON BABY MONITOR EXPOSURES. *Rapid7*. Recuperado el 8 de Enero de 2021, de <https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf>

- Sterling, G. (6 de Febrero de 2017). *Marketing Land*. Obtenido de <https://marketingland.com/tv-maker-vizio-fined-2m-no-consent-tracking-consumer-viewing-habits-205810>
- Venturini, G. (16 de Julio de 2020). *Tecnología Informatica*. Obtenido de <https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/>
- Yanez, D. (2019). *lifeder*. Obtenido de <https://www.lifeder.com/metodo-descriptivo/>