

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.



Facultad de Ingeniería en Electricidad y Computación

Maestría de Seguridad de Información Aplicada

"IMPLEMENTACIÓN DE POLÍTICA DE SEGURIDAD EN LAS
REDES WI-FI DE LAS AULAS DEL CONOCIMIENTO DE
HOGAR DE CRISTO"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del Título de:

MASTER EN SEGURIDAD DE INFORMACIÓN APLICADA

Presentado por:

Lady Mariuxi Sangacha Tapia

Guayaquil - Ecuador

2016

AGRADECIMIENTO

Al Ing. Albert Espinal Santana
Director Regional de cisco quien
impartió sus conocimientos y
experiencia a lo largo de mi carrera.
A mí querida Corporación de
Viviendas de Hogar de Cristo por
haber confiado en mí y permitido
aplicar el conocimiento aprendido.

DEDICATORIA

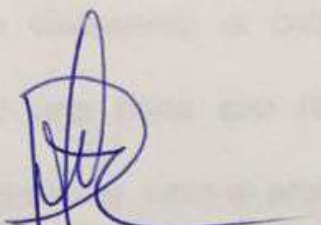
A mi Dios, porque de Él proviene la fortaleza para seguir adelante.

A mi madre, mi tía que tuve el apoyo incondicional, hicieron posible que culmine satisfactoriamente mi carrera profesional.

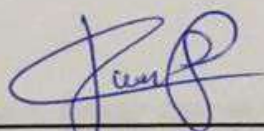
David, quien me colaboro económicamente en el año 2011, fecha que inicie mi profesión de seguridad.

Lady Songreha Espina

TRIBUNAL DE SUSTENTACIÓN



Ing. Lenin Eduardo Freire Cobos
DIRECTOR DEL MSIA o MSIG



Ing. Juan Carlos García P.
PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA



Mgs. Lenin Eduardo Freire Cobos
PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

RESUMEN

La matriz de la corporación se trasladó a la Sergio toral, comúnmente llamado al fondo de la entrada de la 8, con la intención de estar cerca de los más vulnerables del noroeste de Guayaquil, el cableado física que tiene hogar de cristo es alto, dejando una parte con red inalámbrica para el directorio y otra de manera independiente para el proyecto llamado aulas del conocimiento de hogar de cristo, son aulas con tecnología de punta, se encuentra a la vista de usuarios ya sean internos, externos o socios .

Las socias traen a sus hijos para gozar con el beneficio de la reducción de la brecha digital, existe una cantidad de equipos que se comunican por una red no física llamada tecnología WI-FI o redes inalámbricas.

Las redes inalámbricas son facilitadas por una LAN, el acceso a la red es para las estaciones que se encuentran en las Aulas. Usar esta tecnología ofrece oportunidad de productividad y servicio que no puede entregar una red física. Ha sido más fácil y rápida su instalación puesto que no habría necesidad de

pasar cables por paredes, a pesar que implementar la red no física llevo un costo alto esto como ciclo de vida puede ser significativamente inferior.

Las Wlan pueden usar equipos de fácil configuración para las estaciones de trabajo clientes, administrador y el servidor pero no con facilidad para la incorporación de nuevos usuarios a la red.

El presente tema tiene como objetivo de elaborar políticas de accesos a las redes inalámbricas puesto que se propone disminuir los riesgos de ataques de usuario de sombrero blanco, gris o negro, así mismo en completar los niveles básicos y medios de seguridad en la implementación de una red de este tipo.

Se da a conocer los pasos para mantener controlado el acceso a la red, mitigando los riesgo de usuarios no autorizados, se describen los elementos

que participan en la solución, los protocolos de red, funcionalidades, lo que describe en los capítulos.

Para conocer las generalidades, objetivos, metodología a usar se puede visualizar en el capítulo 1. Donde describen los conceptos básicos de las redes de área local inalámbricas, se explica su definición, configuración, conociendo las normas es el capítulo 2. La metodología a desarrollarse con la ayuda del levantamiento de información, identificando la vulnerabilidad, así también se define de manera global las políticas de seguridad de redes wi-fi, los tipos que hoy en día usan y que se va a usar para la gestión, es el segundo capítulo más importante en el capítulo 3. Demostración detallada el diseño de red con la ayuda de un emulador para ello, con sus direcciones de las estaciones de trabajo en el capítulo 4. En el análisis de costo y beneficio de una red inalámbrica se muestra en el capítulo 5. En el capítulo 6, el más importante donde muestra los resultados de la elaboración de políticas de seguridad, los pasos a seguir.

ÍNDICE GENERAL

AGRADECIMIENTO	II
DEDICATORIA	III
RESUMEN	V
ÍNDICE GENERAL.....	VII
ÍNDICE DE TABLAS	X
ÍNDICE DE FIGURAS.....	XI
INTRODUCCIÓN	XII
CAPÍTULO 1	1
GENERALIDADES	1
1.1 Descripción del problema.....	1
CAPÍTULO 2.....	6
MARCO TEÓRICO	6
2.1 Concepto y Generalidades.....	6
2.2 Definición	8

2.3	Configuración Wlan	8
2.4	Punto a Punto	9
2.5	Enlace entre varias WLAN	12
2.6	Normalización de IEEE para redes inalámbricas	12
CAPÍTULO 3.....		15
METODOLOGÍA DESARROLLO A LA SOLUCIÓN		15
3.1	Levantamiento de información	15
3.4	Elaboración de métodos de defensa en los equipos inalámbricos....	23
3.6	Tipos de Políticas de acceso a una red inalámbrica	26
CAPÍTULO 4.....		29
DISEÑO DE RED.....		29
4.1	Diseño inalámbrico y alámbrico	29
4.2	Tabla de direcciones	30
CAPÍTULO 5.....		32
COSTO Y BENEFICIOS DE LA IMPLEMENTACIÓN DE SEGURIDAD		32

	x
5.1 Disminución de Incidentes	32
5.2 Costo y beneficios	33
CAPÍTULO 6.....	34
CONTROL DE ACCESOS.....	34
6.1 Pasos para obtener una red inalámbrica de acceso más segura y autorizada	34
6.2 Parámetros básicos de configuración.....	37
CONCLUSIONES Y RECOMENDACIONES.....	44
BIBLIOGRAFÍA.....	46

ÍNDICE DE TABLAS

Tabla 1 La normas 802.11x	13
---------------------------------	----

	xi
Tabla 2 Lista de equipos existente.....	16
Tabla 3 Direccionamiento ips.....	30
Tabla 4 Rango de direccionamiento	30

ÍNDICE DE FIGURAS

Figura 2.1 Los Puntos de acceso al terminal cliente.....	10
--	----

Figura 2.2 El espacio externa de las aulas del conocimiento	11
Figura 2.3 Los múltiples puntos de accesos	11
Figura 3.4 Una demostración de la estación de trabajo	19
Figura 3.5 Access point	21
Figura 4.6 Esquema general de la red de aulas del conocimiento.....	30
Figura 6.7 Las guías para otorgar autorización de acceso	35
Figura 6.8 La configuración del equipo de los puntos de acceso	39
Figura 6.9 Aplicación de los 4 puntos anterior mente mencionado.....	39
Figura 6.10 Se muestra el comando para obtener la direccion mac	40
Figura 6.11 La demostración del ingreso de configuracion al equipo inalámbrico	41
Figura 6.12 ingreso de las dirección mac	41
Figura 6.13 El ingreso al adaptador de red.....	42
Figura 6.14 Ingreso de direccion ip válida	43

INTRODUCCIÓN

Se muestra la elaboración de políticas de seguridad para controlar el acceso no autorizado a una WLAN abreviaturas en inglés significa Wireless Local Area Network lo que en el lenguaje española es Red de Área Local Inalámbrico.

Lo que hoy en día está a disposición al mundo tanto para los empresarios como los usuarios de casas domésticas, como una alternativa al cableado LAN que ofrece conectividad en lugares donde resulta inconvenientes o casi imposible de brindar servicios con red física.

Existen otras tecnologías de red no física en áreas de extensión como la WPAN/WLAN Personal Área Network denominada Bluetooth ya que se considera complementaria a una red inalámbrica.

Es importante no solo considerar la tecnología sino ante todo tener un esquema, un modelo a seguir, y en caso de no tener poderlo realizar, existen ventajas extremadamente altas cuando se documenta el diseño de red,

incluso cuando se plasman las direcciones ips, Mac, modelos de equipos, ayuda a responder de manera más óptimo en el momento que se presente un apuro informativo o ataque informático.

CAPÍTULO 1

GENERALIDADES

1.1 Descripción del problema

Hogar de Cristo es una institución no gubernamental, pluralista y sin ánimo de lucro, dirigida por la Compañía de Jesús, que a comienzos de los años 70 nace con la intención de garantizar una vivienda digna a los más pobres de la costa ecuatoriana.

Sin embargo actualmente Hogar de Cristo se abre a nuevos procesos sociales aparte de vivienda social y habitad, como el del banco de materiales, Iniciativas económicas asociativas, Banca Comunal, salud, Seguridad alimentaria, Casa de acogida, macro proceso de

economía solidaria, Proyectos sociales (Aulas del Conocimiento, misión y pastoral).

Como muchos proyectos de la corporación Las Aulas del Conocimiento impulsa a la reducción de la brecha digital desde el año 2013, es muy apreciada por los habitantes de bajos recursos del sector noreste de Guayaquil (Sergio toral, nueva prosperina, monte Sinaí, bastión popular, etc.) donde se imparte conocimiento tecnológico a los mejores estudiantes niños, niñas y adolescentes más vulnerables de bajos recursos ya que no poseen en sus centros educativos un laboratorio informático.

Actualmente se está formando a 241 niños, niñas y adolescentes con la ayuda de un tutor y un coordinador tutor quienes guían al desarrollo de habilidades y conocimiento a través de las tecnologías en las Aulas del Conocimiento, en ella existe 44 equipos de último modelo, 41 estaciones clientes tipo casero, 1 estación administrador y 1 equipo de servidor, se encuentra 4 puntos de accesos de las cuales solo 3 se encuentran operativos que imparten el enlace a la internet y comunicación de red de información de manera inalámbrica.

Diariamente existe visitas de personas como visitantes, compañeros, socios, socias, ancianos, niños, niñas y adolescente que portan

equipos como Smartphone, Tablet, computador portátiles que intentan acceder a la red inalámbrica.

En ocasiones se hace préstamo de las Aulas para realización de capacitación y necesitan proyectar información de sus propios equipos y el no tener políticas, procedimientos a proceder, el personal a cargo de trabajo no sabe cómo reaccionar, preguntándose ¿Qué hacer?

Dependen de mi conocimiento para proceder con la configuración del acceso a las redes inalámbricas para el enlace a internet.

No existe un diseño de red ordenada para facilitar de manera más óptima y oportuna la configuración para el acceso al enlace a internet tanto para personas externas como para los equipos internos del proceso.

El acceso sin la utilización de redes físicas, la razón que hace tan interesante a las redes inalámbricas, pero también es el problema de seguridad más potente. Si no se toma esta medida de seguridad es fácil que exista una intrusión en la red, además de presentar afectaciones en red.

Se conoce que las redes inalámbricas los operan en un espectro de frecuencia utilizados por otro dispositivo, esto podría presentarse interferencia que afectarían a la red de forma negativa su rendimiento,

como equipos de bluetooth, los hornos microondas y algunos teléfonos DECT inalámbricos. Existen riesgos al no mantener controlado el acceso porque afecta el rendimiento de la red inalámbrica.

1.2 Solución del problema

Debido a la gran afluencia de personas, el intento de ingreso a la red para tener acceso al enlace a internet es alta, además de visitantes a las Aulas del Conocimiento, es de vital importancia que se implemente políticas de seguridad de las redes wifi, principalmente para responder con eficaz al momento de registrar un equipo nuevo sin la necesidad de un profesional que realice la respectiva configuración.

Con la elaboración de una política de control de acceso a la red inalámbrica que se encuentre desarrollado y probado para [1] mitigar los riesgos de ataques.

Por ello se propone considerar lo siguiente:

- Levantamiento de información actualizado
- Elaboración de un esquema - diseño de red
- Actualizar el control de inventario
- Actualizar la información de los equipos informáticos de las Aulas del Conocimiento de Hogar de Cristo.

- Elaboración de pasos a seguir para la configuración de un nuevo equipo.
- Elaboración de una política de acceso

1.3 Objetivo general

Elaboración de políticas de seguridad con recursos tecnológicos actuales para controlar y proteger el acceso no autorizado a las redes inalámbricas de las Aulas del conocimiento de Hogar de Cristo.

1.4 Objetivo específico

Elaborar las políticas de acceso tecnológico a las redes de área local inalámbrica para controlar y proteger la información de usuarios no autorizados.

1.5 Metodología

La metodología para el desarrollo del tema es la investigativa de la cual se escogió aplicar las teorías y prácticas aprendidas durante el transcurso de la maestría.

Me permite la construcción y desarrollo de la teoría y práctica científica profundizando los conocimientos de las seguridades de la tecnología de las redes inalámbricas. Esto también me permite manifestar el análisis,

la síntesis, la inducción, deducción que me permite aclarar más del tema.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Concepto y Generalidades

Es importante recordar el concepto de una red inalámbrica antes que se presenta a continuación:

Se utiliza en informática para designar la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica la cual la transmisión se realiza por medio de puertos.

Una vez dado el concepto de redes inalámbricas ahora se explica lo que es seguridad de redes inalámbricas, es una protección a usuarios no autorizados al acceso a los equipos la transmisión de comunicación en una red local.

Dentro de sus generalidades existe su origen, las ventajas y desventajas, podremos comenzar indicando que en un principio, las computadoras eran elementos aislados que formaba una estación de trabajo de manera independiente o de una isla informática. De tal forma que cuando alguien necesitaba imprimir debía usar el computador que tenía conectada la impresora, la comunicación era de cable. La idea de comunicarse a través de una red intangible fue posible dando ciertas ventajas como costo relativamente bajos, ofrece un máximo rendimiento posible, mayor velocidad, pero así mismo existen desventajas como el precio de la instalación, dificultad y expectativa de expansión.

La utilización de las WLAN es demandado, cuya función es permitir al usuario conectarse a la LAN empresarial sin la necesidad de una conexión física.

En la seguridad de las redes WLAN, se identifican otros protocolos a mencionar como el TKIP (Temporal Key Integrity), LEAP (Lightweight EAP), WEP (Wireless Encryption Protocol o Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), EAP (Extensible Authentication Protocol).

Son herramientas que proporciona cierta medida la seguridad, para obtener la fiabilidad que se necesita en una red inalámbrica debemos fijarnos al menos dos factores esenciales:

- La autorización del acceso a nuestra WLAN (autenticación), tener claro quién debería tenerlo.
- Eludir que los datos puedan ser leídos con facilidad por cualquier usuario que tenga la capacidad básica de acceder al canal (confidencialidad).

2.2 Definición

Las redes inalámbricas (en inglés Wireless network) son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante [7] ondas electromagnéticas.

2.3 Configuración Wlan

Las redes inalámbricas es un tema de alta complejidad y muy variable, contando con las necesidades que se deben cubrir, llevando esto una dependencia de los requerimientos para implementar las diversas configuraciones y establecerlo como políticas de seguridad en las redes inalámbricas.

A pesar que existe variedad de configuración en el mundo de la red no física, en el Proyecto de las Aulas del Conocimiento tiene implementado la conexión entre WLANS.

2.4 Punto a Punto

Las redes punto a punto es un tipo de arquitecturas que responden a un tipo canal de datos se usa para comunicar únicamente dos nodos, en otros casos a redes multipunto, puesto que los canales de datos se comunican en diversos nodos.

Dentro de las Aulas del Conocimiento utiliza su red con la ayuda de un **punto de acceso** como muestra la Figura 2.1, la máxima distancia permitida no es entre estaciones, sino entre cada estación y el punto de acceso. En la misma figura 2.1 muestra que los puntos de accesos se pueden conectar a otras redes.

Esto se lo conoce como una red como **BSS** extensiones de celdas básicas

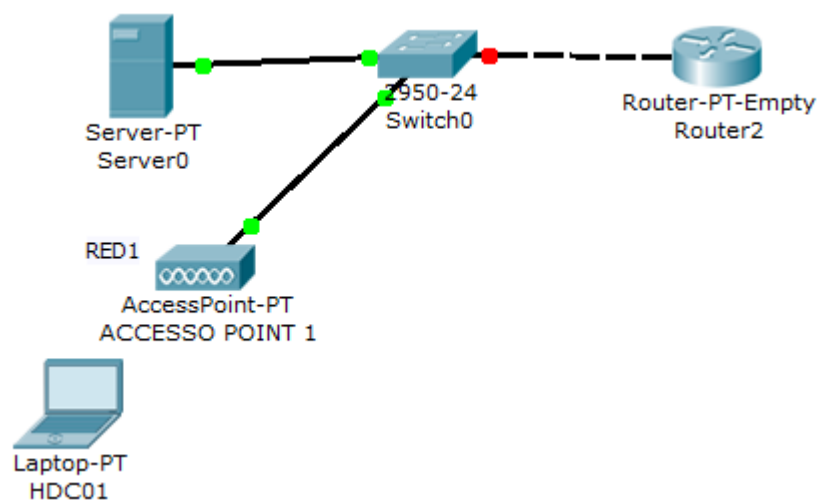


Figura 2.1 Los Puntos de acceso al terminal cliente

En teoría los puntos de acceso tienen un límite de rango, 100 m en lugares cerrados y 300 m en lugares abiertos. En el caso de las Aulas del Conocimiento es cerrado, dentro de un edificio de 105 metros cuadrados como se muestra en la Figura 2.2 y dentro de ella se utilizan 3 puntos de accesos que están operativos como muestra en la Figura 2.3.



Figura 2.2 El espacio externa de las aulas del conocimiento

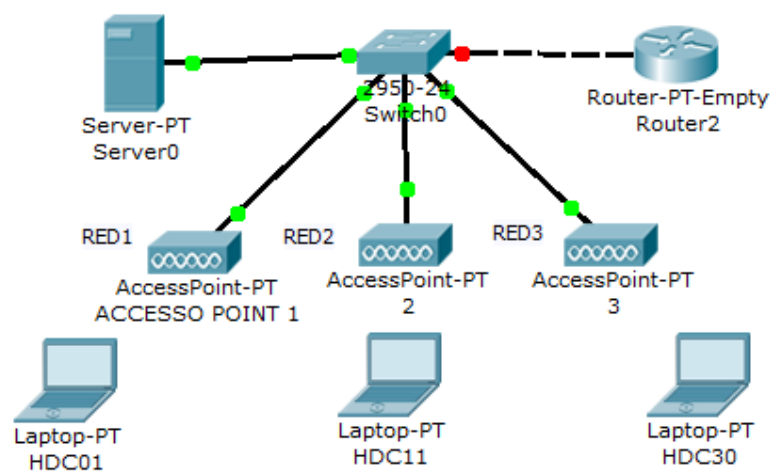


Figura 2.3 Los múltiples puntos de accesos

El uso de la red en las Aulas es de PE Punto de Extensión llamada también modo de infraestructura para aumentar el número de puntos de accesos.

2.5 Enlace entre varias WLAN

Geográficamente Aulas del conocimiento no cuenta con antenas de entre LAN, puesto que la red es totalmente independiente a la red que tiene la corporación porque el proceso se basa a un proyecto dando referencia a un corto plazo o hasta que no pueda autofinanciarse pero si cuenta con varias wlan internas.

2.6 Normalización de IEEE para redes inalámbricas

WIFI (Wireless Fidelity) [2] describe los productos WLAN basados en los estándares 802.11, modelo desarrollado por un grupo de comercio y por otras compañías como 3com, Aironet, Luncent o Nokia y responde al nombre oficial WECA (Wireless Ethernet Compatibility Alliance).

Desde el año 1997 del mes de junio se dio a conocer el estándar 802.11 y se caracteriza por ofrecer velocidades con sistema cifrado y operar en su banda de frecuencia, luego de dos años empezó aparecer las variantes de 802.11 a y 802.11b. A continuación se mostrara una tabla del detalle de la norma 802.11 que se encuentra compuesta al día de hoy por los siguientes estándares:

Tabla 1 La normas 802.11x

NORMA	DESCRIPCIÓN	MBPS
802.11 a	5,1-5,2 Ghz, 5,7-5,8 GHz) OFDM: Multiplexación por división de frecuencia ortogonal.	54 Mbps
802.11b	2,4-2,485 GHz	11 Mbps
802.11c	Define características de AP como Bridges	NI
802.11d	Múltiples dominios reguladores (restricciones de países al uso de determinadas frecuencias)	
802.11e	calidad de servicio (QoS)	
802.11f	Los protocolos de conexión entre puntos de acceso (AP), protocolo IAPP: Inter Access Point Protoco	
802.11g	2,4-2,485 GHz, OFDM, Multiplexación por división de frecuencia ortogonal, aprobado año 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b	36 o 54 Mbps
802.11h	DFS: Dinamic Frequency Selection, Esto habilita una poco de coexistencia con HiperLan y regula la potencia de difusión	
802.11 i	referente a seguridad	
802.11j	Permitiria armonización entre IEEE (802.11), ETSI (HiperLan2) y ARIB (HISWANa)	
802.11m	El Mantenimiento redes Wireless	
802.11n	La velocidad real de transmisión	Hasta los 600 Mbps
802.11p	Operan en el espectro de frecuencias de 5,90 GHz y de 6,20 GHz	
802.11r	Es el Fast Basic Service Set Transition, su particularidad principal es permitir a la red que establezca los protocolos de seguridad que identifican un dispositivo en el nuevo punto de acceso antes de que abandone el actual y se pase a él	
802.11v	La configuración remota de los dispositivos cliente	
802.11w	sirve para proteger redes WLAN contra ataques sutiles en las tramas de gestión inalámbricas (WLAN)	

A pesar que se dio a conocer las normas para las redes inalámbricas para este tema se usara tres normas que son:

- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

CAPÍTULO 3

METODOLOGÍA DESARROLLO A LA SOLUCIÓN

3.1 Levantamiento de información

En las Aulas del Conocimiento se encuentra estaciones, puntos de accesos, servidor, impresora, a continuación se muestra la tabla 1 de distribución de equipos tecnológicos existentes.

Tabla 2 Lista de equipos existente

Cantidad	Descripción	Funcionamiento
41	Estaciones clientes	operativo
1	Estaciones clientes	no operativo
1	Estación Administrador	operativo
1	servidor	operativo
3	puntos de accesos	operativo
1	puntos de accesos	no operativo
1	Switch	operativo
1	impresora	operativo
1	rack	operativo
1	ups triple de 20 k	operativo

El levantamiento de información acerca de los equipos tecnológico fue realizado por medio de la observación. Se ha obtenido el nombre de la red, la misma que existe 4 subredes para los 44 equipos más la impresora.

Los puntos acceso son equipos caseros, no adecuado para el uso de los 44 equipos sin embargo por factor económico han realizado la implementación de los equipos.

La zona se encuentra en un clima excelente para los equipos tecnológicos, con sus respectivas mesas, parte eléctrica, tienen respaldo eléctrico en caso de existir un apagón. En el capítulo 4 se mostrara el diseño de la red.

Por el momento se puede analizar que se aplicó la fase del hacking ético que es la de reconocimiento con la modalidad de hacking interno de caja blanca. Recordando que Hacker Ético o de Sombrero Blanco – Profesional que usa sus habilidades de hacking con fines preventivos.

3.2 Identificación de vulnerabilidad en las redes inalámbricas

La vulnerabilidad existe más en las redes inalámbricas que las físicas, debido al desconocimiento de las configuraciones a los equipos de puntos de accesos, además de herramientas y protocolos que ayuda a mitigar el riesgo de la seguridad en la red , corriendo el riesgo el ingreso a los archivos compartidos, informaciones de descargas etc.

También existen otros factores como la mala práctica de los estándares ya que los equipos que tienen las aulas no son ideales para la necesidad del proyecto.

Existen otros ataques a redes WLAN, que explotan algunas de las debilidades comentadas, y que pueden ser agrupados en varios niveles:

- **Vulnerabilidad en el método de autenticación:** Si un atacante logra capturar el 2do y 3er mensaje de datos administración en una autenticación mutua. El segundo posee el desafío en texto plano y el tercero contiene el mensaje criptografía con la clave compartida. Esto hace que se autentique luego al acceso
- **La Debilidad en WEP:** Es una característica lineal de CRC32 que la demostró en teoría por Nikita Borisov, Ian Goldberg y David Wagner. El ICV es el que comprueba la integridad de un mensaje. Esto presenta dos problemas, el CRC es independiente de la clave empleada y lineal.
- **Los Puntos no visuales:** En los puntos de acceso se muestran alrededor la presencia de los dispositivos donde indica la presencia del SSID sus siglas significa Service Set Identifier.
- **El nombre del SSID del dispositivo:** En los equipos de puntos de acceso se encuentra el nombre por defecto del equipo, lo cual esto evita la utilización de un nombre que pueda adivinarse con facilidad.

3.3 **Característica de los equipos**

Equipo: Desktop HP Pavilion All-in-One 20-b052la



Figura 3.4 Una demostración de la estación de trabajo

Marca: HP

Características importantes:

Pantalla LCD de alta definición de 50,80 cm (20 pulgadas)

Placa IPISB-AB (Leeds-U)

Factor de forma: HP nano-AIX - 19 cm (7,5 pulgadas) x 24 cm
(9,4 pulgadas)

Chipset: Intel H61

Sockets de memoria: 2 para DDR3

Socket del procesador: LGA 1155

Ranuras de expansión:

1 socket para mini tarjetas PCI Express de media altura (Generación 2.0)

Intel Core i3 2130

Memoria 4gb

Sistema operativo Windows 8

LAN inalámbrica 802.11 b/g/n con banda única (2,4 GHz) 1x1 :

Tipo de interfaz: Mini tarjeta PCI Express de media altura

Velocidades de transferencia de datos: Hasta 150 Mbps

Estándares de transmisión: 802.11 b/g/n

Conexiones de antena admitidas: Hasta 2 (depende del modelo)

Banda de funcionamiento única: 2,4 GHz (b/g/n)

Protocolos de seguridad admitidos en Windows:

WPA-PSK

WPA2-PSK

LAN: 10-Base-T

Tecnología: Realtek RTL8111F

Velocidades de transferencia de datos: hasta 10/100 Mb/s

Estándares de transmisión: Gigabit Ethernet 10-Base-T

Diseño compatible con Realtek RTL8175EH/RTL8105E

Disco duro de 1TB

Equipo: Router inalámbrico Zyxel NBG-419N



Figura 3.5 Access point

Marca: Zyxel

Características importantes:

Puerto

LAN: 4

Puertos WAN: 1

Puertos USB 2.0: 1

Tasa de transferencia Ethernet: 10/100

Tasa de transferencia Wi-Fi: 300 MB/s

General

Wi-Fi: Si

Estándares: IEEE 802.11b / IEEE 802.11g / IEEE 802.11n

Nivel de ganancia de antenas: 2 dB

Codificación: WEP

Modo de seguridad: WEP, WPA-PSK, WPA2PSK

Protocolos: DHCP / PPPoE / PPTP / L2TP

Soporte NAT: Si

Protección Firewall: Si

Dimensiones y Peso

Peso: 252 g

Alto: 33 mm

Ancho: 162 mm

Profundidad: 115 mm

3.4 Elaboración de métodos de defensa en los equipos inalámbricos

El primer método es la autenticación y control de acceso es el SSID (Service Set Identifier) con Contraseña WEP o el WPA2 casero, tomando en consideración de la tecnología existente.

Es un estándar 802.1X, permite un empleo de WEP para autenticación que se denominó "Dynamic WEP", se refiere un algoritmo como parte de 802.1x, de manera que sea un poco más segura que el "WEP estático", pero la alianza Wifi sin embargo hoy en día ya no se recomienda en emplear ninguno de ellos en entornos seguros.

Existe la seguridad por restricción de direccionamiento MAC, esto se basa al permitir restringir a un listado de direcciones, las que se pueden conectar y las que no, pero presenta la debilidad que el atacante podría llenar a la red con direcciones falsas.

Contraseñas no estáticas:

- Periódicas: La OTP (One Time Password) es una Contraseñas de un solo uso, conocidas como token flexibles.

El estándar 802.1x no fue presentado para la red no física, sino para el acceso seguro PPP (en tecnologías de cable). Arquitectura 802.1x está dividida en 3 partes:

- A) El Solicitante: En el mayor de los casos se trata del cliente que se conecta inalámbricamente.
- B) Los Autenticados : usualmente es el punto de Acceso
- C) El Servidor de autenticación: que intercambiará el nombre y credencial de cada usuario sin embargo Aulas del Conocimiento no cuenta con esto.

La WiFi Alliance indica 2 tipos de certificación para los productos, cuyas características para modelos de empresas (WPA: Autenticación: IEEE 802.1x/EAP y Encriptación: TKIP/MIC -WPA2: Autenticación: IEEE 802.1x/EAP y Encriptación: AES-CCMP) y el Modelo personal (SOHO/personal): que son WPA refiriéndose a Autenticación: PSK y Encriptación: TKIP/MIC y el WPA2: Autenticación: PSK y Encriptación: AES-CCMP.

Para la implementación de elaboración de políticas de seguridad es el modelo personal con encriptación AES.

Segundo Método es mejorar la seguridad física: restringe el número de direcciones MAC que pueden acceder. Las ACLs (Access List Control)

permite realizar actividad por medio de en los AP, donde se especifica (a mano) las direcciones MAC de las tarjetas que permite el acceso, no permitiendo a cualquiera que no esté registrada en el equipo. Como anteriormente se ha dicho que es muy fácil engañar con falsificación direcciones Macs.

El tercer método es disponer con el uso del internet, existen ocasiones la necesidad de parte de los compañeros de otras áreas el acceso al enlace a internet para sus actividades o capacitación.

El cuarto método es implemente la autenticación de usuario, es importante que en los puntos de acceso se pueda implementar la normas con equipos de WPA y 802.11 i sin embargo por cuestiones de recursos no es posible pero existe otras alternativas.

3.5 Conocimiento en general de las políticas en las redes inalámbricas

Antes de indicar el contenido de las políticas se debe definir que es una política en las redes inalámbricas, se basa a la protección que existe a una infraestructura o información usando estándares, protocolos, reglas, herramientas y leyes para minimizar los posibles riesgos.

Las políticas implementadas y documentadas permiten guiar al responsable del área de la corporación, la manera de actuar de manera más óptima y así mismo mitigar los riesgos a la red.

Se debe considerar que cuando se tomen decisiones se considere las políticas siguientes:

- La política de privacidad.
- La política de acceso.
- La política de autenticación.
- La política de contabilidad.
- La política de mantenimiento para la red.
- La política de divulgación de información.

Para la elaboración de este documento se enfocara a la **política de acceso**

3.6 Tipos de Políticas de acceso a una red inalámbrica

La elaboración de las políticas dependerá a la necesidad de la corporación, en este caso es dirigido al proyecto Aulas del Conocimiento. Para ello hemos definido 2 tipos que se da a conocer a continuación:

- La política de administración

- La políticas de Operación

Políticas de Administración: La responsabilidad de la realización de las configuraciones, gestión y control del equipamiento de acceso a la red, para ofrecer soporte a varios tipos de usuarios con parámetros y requisitos de seguridad diferentes, mientras la red se mantiene para reducir la mala seguridad.

Políticas de Operación: Es el uso de las configuraciones ya gestionadas, controladas de la red ya asegurada.

3.7 **Herramientas a usar**

A pesar que existen diferentes distribuidores se menciona los tipos de dispositivos inalámbricos y herramientas para la administración, la corporación en el 2013 realizo la compra de 3 puntos de accesos caseros, un switch como puente entre el dispositivo que son de marca ZYXEL [5] las características lo especifica en el tercer capítulo, 42 equipos de un espacio de 105 m², un servidor Windows server 2008, 1 equipo administrador marca hp home con sistema operativo Windows 7.

Referente a la marca ZYXEL durante más de 20 años ha seguido siendo uno de los principales proveedores mundiales de productos para diferentes necesidades de despliegue de red. Es la primera opción de

muchos de nivel uno los proveedores de servicios, que conecta a más de 400.000 empresas pequeñas y medianas, y más de 100 millones de usuarios finales en todo el mundo.

CAPÍTULO 4

DISEÑO DE RED

4.1 Diseño inalámbrico y alámbrico

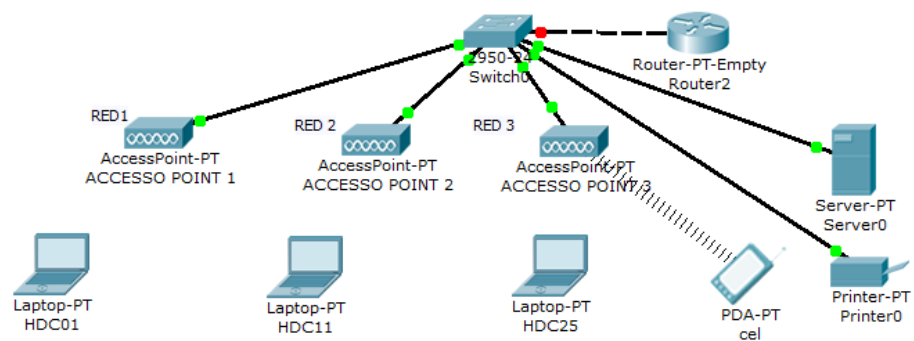


Figura 4.6 Esquema general de la red de aulas del conocimiento

4.2 Tabla de direcciones

Tabla 3 Direccionamiento ips

Broadcast	Nombre de la Red	Ips disponible a Usar
		192.168.X.1
192.X.X.31	192.X.X.32	192.168.X.33
192.X.X.63	192.X.X.64	192.168.X.65
192.X.X.95	192.X.X.96	192.168.X.97
192.X.X.127	192.X.X.128	192.168.X.129
192.X.X.159	192.X.X.160	192.168.X.161

Tabla 4 Rango de direccionamiento

AP 1	AP 2	AP 3	AP 4
-------------	-------------	-------------	-------------

Rango de direcciones	192.168.X.33	192.168.X.65	192.168.X.97	192.168.X.129
Hasta	Hasta	Hasta	Hasta	Hasta
ips para las estaciones	192.168.X.62	192.168.X.94	192.168.X.126	192.168.X.158

A continuación un diagrama de red General, por motivos de seguridad no se dará a conocer las direcciones ip real.

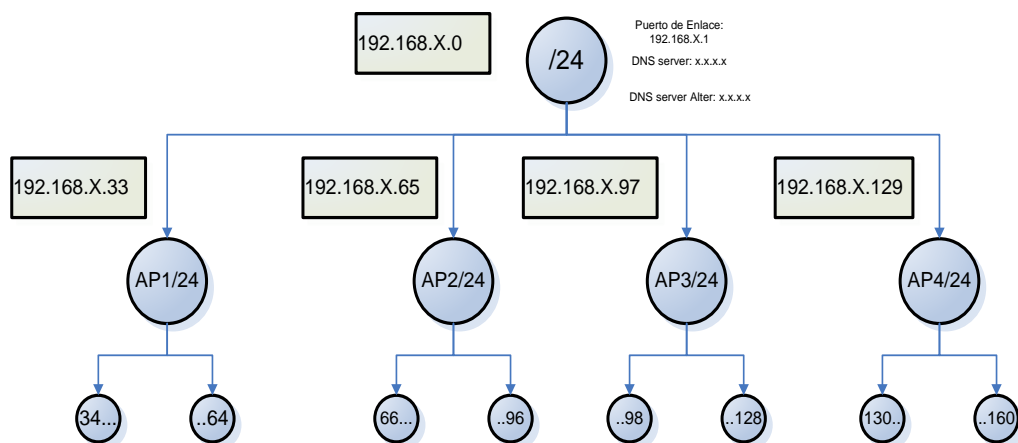


Figure 4. 1 La segmentación de red

CAPÍTULO 5

COSTO Y BENEFICIOS DE LA IMPLEMENTACIÓN DE SEGURIDAD

5.1 Disminución de Incidentes

La elaboración de [5] políticas tendrá varias ventajas que se lista a continuación:

- Se evita la replicación de dirección ip al momento de autorizar un equipo nuevo.
- Tiempo de respuesta más optimo

- No se necesita de los conocimientos profesionales para asegurar la red
- Mitigar los riesgos del intento de ingreso no autorizado
- Fortalecer la seguridad de datos.

5.1 Costo y beneficios

Se refiere a que tan beneficioso seria implementar políticas de accesos no autorizado a las WLAN, existe algunos puntos importantes:

- Asegurar la información cuando se utiliza equipos móviles.
- Ayuda a evitar al atacante descubrir con facilidad la contraseña
- Ayuda a evitar la presencia del dispositivo inalámbrico
- El uso de contraseña es optimo
- Los cambios de los nombre del SSID dependiendo de la actividad evita ser detectado
- Obtener el cifrado de datos
- La protección contra ataques de malware e internet
- Ahorro de costos de mantenimientos

CAPÍTULO 6

CONTROL DE ACCESOS

6.1 Pasos para obtener una red inalámbrica de acceso más segura y autorizada

La documentación es una guía para cumplir y mitigar los riesgos de accesos no autorizados por esa razón se da a conocer un diagrama general que el personal debe tomar en consideración al momento de autorizar al equipo acceder a la red como lo muestra en la figura 6.7

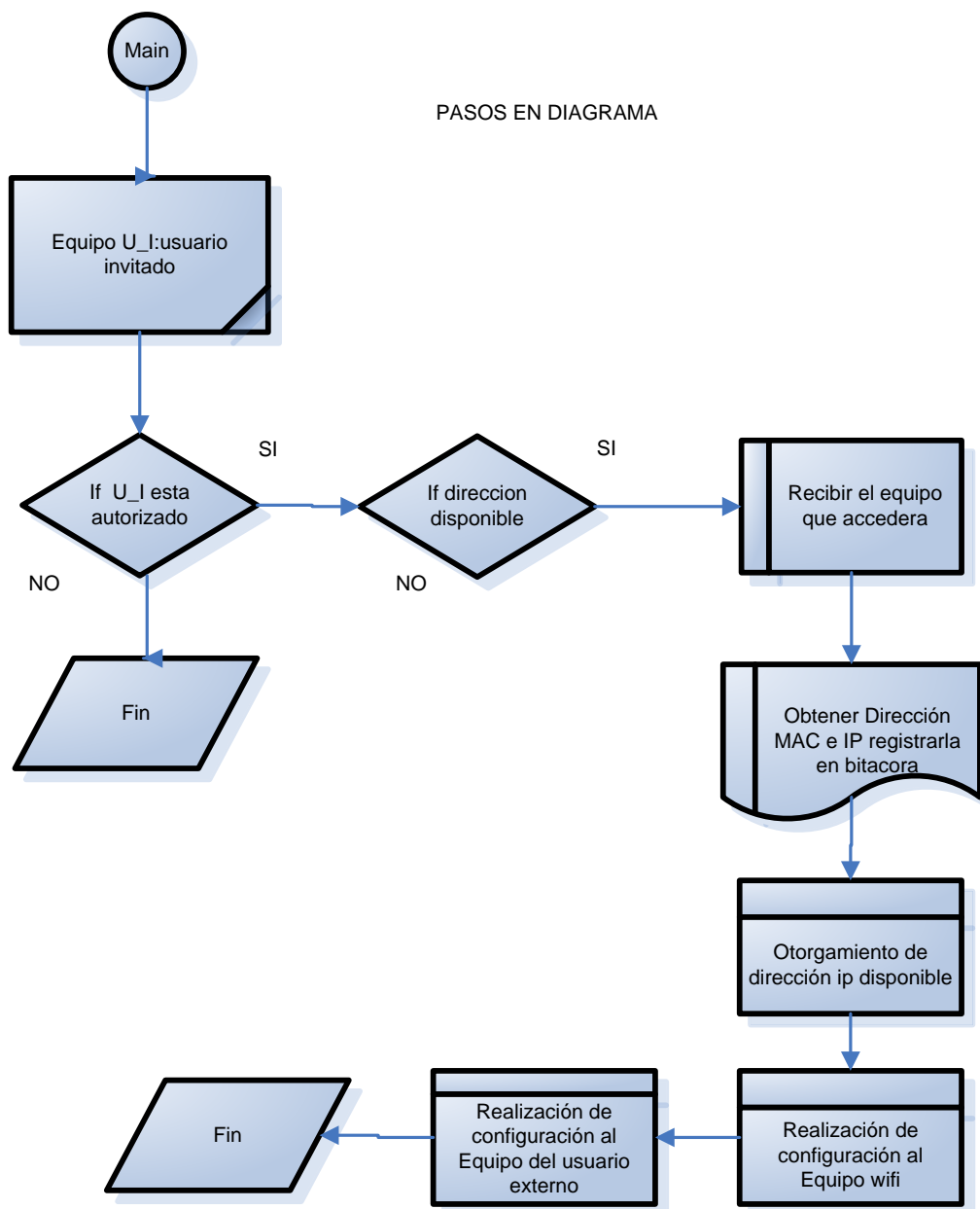


Figura 6.7 Las guías para otorgar autorización de acceso

Además se debe considerar algunos puntos que refleja las condiciones de accesos, de uso, monitoreo, control y conexión:

Condiciones de acceso

Las redes inalámbricas de acceso de dispositivo WiFi están únicamente al servicio del proyecto Aulas del Conocimiento de Hogar de Cristo, y el ingreso acceso está restringido a los compañeros de otras áreas, a los participantes del proyecto, a los representantes del participante. No se debe facilitar a usuarios ajenos la información siempre y cuando esté autorizado por el responsable del área.

Además en el caso de los equipos nuevos o de visitante se debe solicitar autorización de la persona a cargo del área, para la realización de configuración respectiva.

Las Condiciones de uso: El uso de estas redes debe limitarse a las actividades educativas es plenamente la responsabilidad del usuario no efectuar el uso ilícito con la red. No se puede emplear a la red para fines privados ni en ninguna forma que viole la creación de esta política.

El Monitoreo y control: La corporación, persona responsable de la función se reserva el derecho a monitorizar y registrar la actividad que se realice a través de estas redes.

Las conexiones de puntos de accesos: Recuerde que, por motivos de seguridad, los puntos inalámbricos de acceso WiFi deben ubicarse en lugares seguros y conectarse a la Red del Proyecto Aulas del Conocimiento. A través del técnico del área o colaboración de sistemas, a la elaboración de configuración a los puntos de acceso WIFI, que adquiera la propia área, de forma que se garantice un nivel apropiado de seguridad e interoperabilidad. No está permitido en ningún caso conectar puntos de acceso a la Red Corporativa.

6.2 Parámetros básicos de configuración

Consejos de seguridad [6] para proteger la red inalámbrica:

A continuación se incluyen varios pasos sencillos que puedes seguir para proteger tu red y los puntos de accesos (dispositivo Zyxel) inalámbricos:

- Evita la utilización de la contraseña predeterminada: Es muy fácil para un hacker pueda descubrir cuál es la contraseña predeterminada del fabricante de tu router inalámbrico y utilizarla para acceder a la red inalámbrica. Razón es conveniente que cambies la contraseña de administrador del dispositivo inalámbrico. A la hora de establecer la contraseña nueva, trata de elegir una serie compleja de números y

caracteres mayúscula, minúscula, e intenta evitar la utilización de una contraseña que pueda adivinarse fácilmente.

- Es más seguro que no se muestre la presencia de un dispositivo inalámbrico
- Desactiva la difusión del identificador de red SSID siglas (Service Set Identifier) para evitar que el dispositivo inalámbrico anuncie su presencia al mundo que te rodea.
- El cambio el nombre SSID del dispositivo
- El Cifrar datos: En la configuración de la conexión, asegúrate de que actives el cifrado. Los equipos si tiene compatibilidad para la seguridad cifrado WPA, utilízalo; en caso contrario, se puede usar utiliza el cifrado WEP.
- La Protección contra los ataques de malware e Internet: se debe mantener actualizada la protección antimalware, selecciona la opción de actualización automática en el producto. Tomando en consideración la referencia de los consejos prácticos, los pasosa seguir son:

Paso 1: El ingreso al equipo por defecto, la dirección ip es 192.168.0.1, clave admin, aquí se establecerá la dirección ip del proveedor, la dirección ip para el equipo, cambiar el nombre del SSID, la contraseña

no menor de 8 dígitos usando mayúsculas, signos especiales, y numero, selección de encriptación como muestra en la figure 6.8 y 6.9.

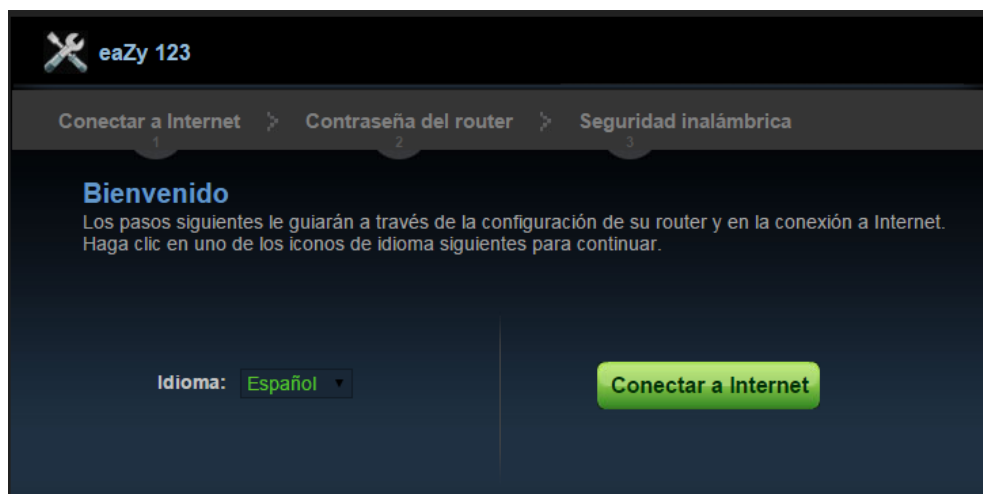


Figura 6.8 La configuración del equipo de los puntos de acceso

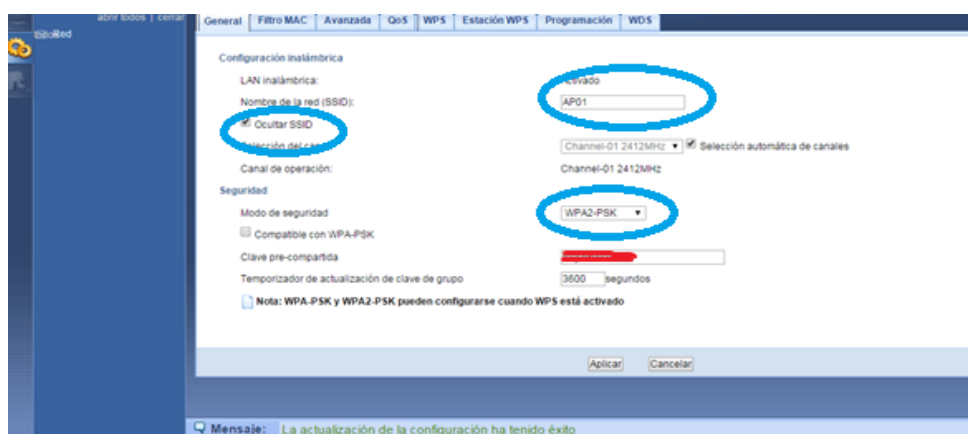


Figura 6.9 Aplicación de los 4 puntos anterior mente mencionado

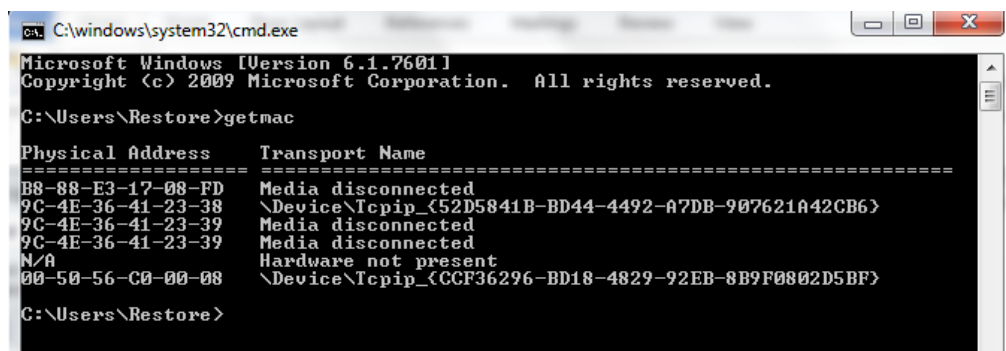
Se refleja los pasos a seguir en forma de diagrama y un pequeño manual para mantener y mitigar el riesgo de los accesos no autorizados a la red inalámbrica, esto es cuando es a un equipo externo.

Configuración al equipo ZYXEL para el acceso autorizado

Paso 1: Sobre entendiendo que existe una autorización de por medio para un equipo ya sea portátil, escritorio o celular, se procede a revisar la tabla de direccionamientos de ips disponibles.

Paso 2: Luego de verificar si existe disponibilidad se procede en obtener la dirección mac del equipo y anotarlo en bitácora.

La Mac se obtiene con el comando getmac en caso de Windows como se observa la figure 6.10



```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Restore>getmac

Physical Address      Transport Name
-----
BB-88-E3-17-08-FD    Media disconnected
9C-4E-36-41-23-38    \Device\Tcpip_{52D5841B-BD44-4492-A7DB-907621A42CB6}
9C-4E-36-41-23-39    Media disconnected
9C-4E-36-41-23-39    Media disconnected
N/A                  Hardware not present
00-50-56-C0-00-08    \Device\Tcpip_{CCF36296-BD18-4829-92EB-8B9F0802D5BF}

C:\Users\Restore>
```

Figura 6.10 Se muestra el comando para obtener la direccion mac

Paso 3: se debe ingresar al equipo de punto de acceso para ello se ha escogido el AP04

de adaptador de red y finalmente ingresar a propiedades del adaptador de red

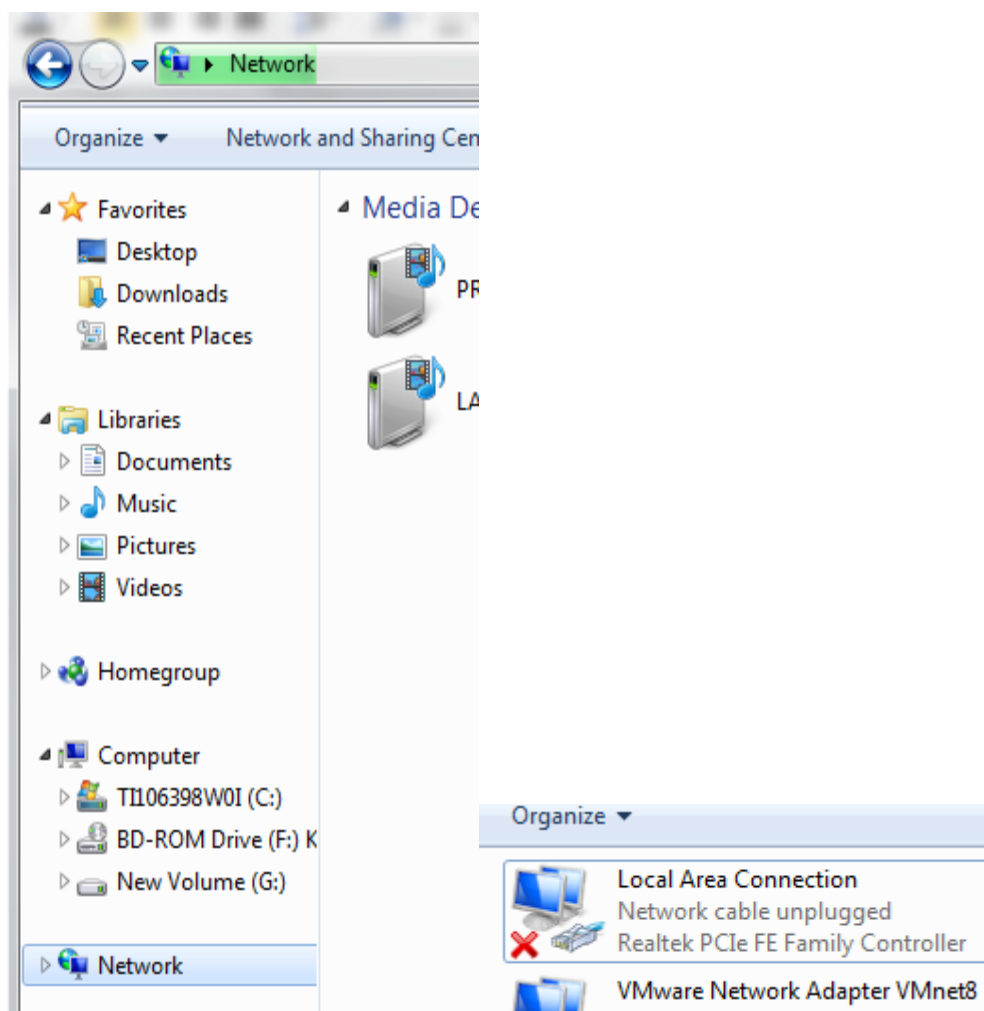


Figura 6.13 El ingreso al adaptador de red

Paso 7: Una vez ingreso a propiedades del adaptador de red, se ingresa a propiedades de la versión IPV4 para proceder a ubicar una dirección

valida y disponible al equipo, con su máscara y DNS respectivos como se observa en la figure 6.14. y listo.

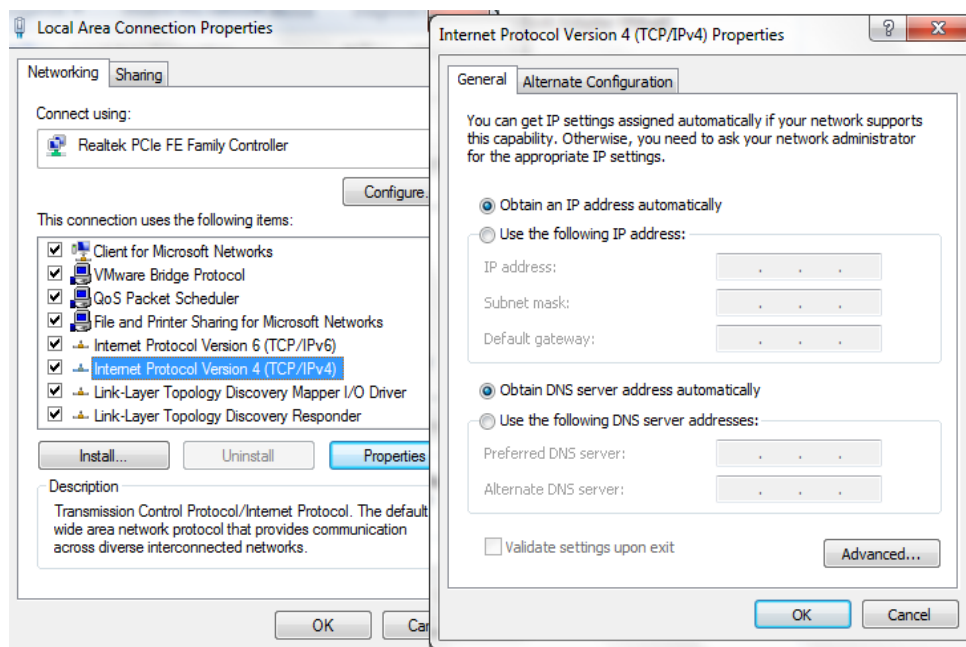


Figura 6.14 Ingreso de direccion ip válida

CONCLUSIONES Y RECOMENDACIONES

Para concluir con la elaboración del tema se consideró lo siguiente:

1. Una vez realizado la primera fase de ética hacking refiriéndose al reconocimiento para la realización de políticas de acceso a la red inalámbrica, luego se detectó la vulnerabilidad.
2. Se explicó ciertos conceptos importantes básicos, como las normas de la 802.11X, la creación de diagrama de red que ayudo mucho para tener claro la realización de procedimientos, además de las características de los equipos de los puntos de accesos, cuáles serían los beneficios al implementar lo que especifica como objetivo general.

3. Los beneficios en cuestión de costo que indica el ahorro que se tendría en mantenimiento, la parte significativos en cuanto al rendimiento y optimización de los recursos; considerando que la maximización de los beneficios que ofrece una red inalámbrica dependerán de la actividad de la corporación.
4. Haciendo referencia al desarrollo de la implementación se sugiere realizar un cambio en los equipos de los 3 puntos de accesos debido a que la transmisión de radio frecuencia es baja como resultado no permite el flujo de comunicación de forma adecuada.
5. El tener una ayuda de tener las políticas de acceso a la red inalámbrica documentada es tan beneficioso tanto para la organización como para el personal responsable que este al mando el momento que suscitase el evento de autorizaciones de accesos.

BIBLIOGRAFÍA

[1] Astudillo Karina, Hacking Ético 101 Como hackear profesionalmente en 21 días, autor-editor, año 2013.

[2] Wi-Fi Alliance, Wireless Fidelity Alliance, www.wi-fi.org , fecha de consulta mes de diciembre 2016.

[3] Astudillo Karina, Seguridad Informática, www.seguridadinformaticafacil.com, fecha de consulta diciembre del 2015

[4] MaxDev , Seguridad en Redes Inalámbricas <http://www.securitywireless.info/> , fecha de consulta mes de diciembre del 2015.

[5] Tato Lino, Adsl Ayuda Comunidad Fibra y ADSL, FTTH Movistar+ Foro Manuales, http://www.adslayuda.com/zyxel-configurar_ip_dinamica.html , Fecha de Consulta en el mes de enero del 2016

[6] AO Kaspersky Lab., Consejos Protección en las redes inalámbricas, <http://www.kaspersky.es/internet-security-center/internet-safety/protecting-wireless-networks> , fecha de consulta en el mes de enero del 2016

[7] Vega Ana, Verdoy Alberto, Redes inalámbricas, <http://myslide.es/technology/seguridad-en-redes-inalambricas-558c20cb3be41.html> , fecha de consulta mes de enero 2016

[8] Caballero Francisco, "Seguridad Informática en Redes Inalámbricas", <http://www.aslan.es/boletin/boletin32/s21sec.shtml> , fecha de consulta en el mes de enero 2016

[9] Sourangsu Banerji, On IEEE 802.11: Wireless LAN Technology, <http://arxiv.org/ftp/arxiv/papers/1307/1307.2661.pdf> , fecha de publicación 2013