PONTIFICIA **UNIVERSIDAD CATÓLICA** DEL PERÚ

PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA
Sección de Electricidad y Electrónica

DISEÑO DE UNA RED LOCAL INALÁMBRICA UTILIZANDO UN SISTEMA DE SEGURIDAD BASADO EN LOS PROTOCOLOS WPA Y 802.1X PARA UN COMPLEJO HOTELERO

Tesis para optar el título de Ingeniero Electrónico

Presentado por:
Ilich Hernán Liza Hernández

Lima - PERÚ
2007

Resumen

Las Redes Inalámbricas de Área Local pueden definirse como una red de computadoras en un área geográfica limitada que utiliza la tecnología de radiofrecuencia para transmitir datos. Este tipo de red está siendo implementada en numerosos lugares para poder ofrecer conexión hacia Internet, debido a sus numerosas ventajas entre las que se encuentran movilidad del usuario, facilidad y velocidad de desarrollo, flexibilidad, costo.

El uso del aire como medio de transmisión en lugar de cables, ha revolucionado las redes de computadoras hoy en día, principalmente en lugares donde el tendido de cables es bastante difícil o no está permitido porque no contribuye con la estética del ambiente. Por estas razones la elección de una Red Inalámbrica es mayormente preferida en Hoteles, Aeropuertos o edificios antiguos.

Las Redes Inalámbricas corresponden a una tecnología emergente y por esto no están exentos de problemas. Uno de los principales problemas que tiene que afrontar una Red Inalámbrica es la seguridad de la información que se transmite, al no contar con un medio guiado como el cable, los paquetes de información viajan libremente por el aire, por lo cual usuarios no autorizados de la red pueden obtener dicha información y también acceder a la misma para obtener los beneficios sin restricción.

El presente documento se centra en el Diseño de una Red Inalámbrica de Área Local para un Complejo Hotelero, el cual cuenta con una Red Inalámbrica ya instalada, la cual no logra brindar cobertura a todas las instalaciones del Hotel y no cuenta con ningún nivel de seguridad de red. Por lo cual se propone un diseño para la ampliación de la Red Inalámbrica y una solución segura para la red, en base de un protocolo de encriptación de información y un método de autenticación de usuarios, de esta forma solo las personas autorizadas podrán tener acceso a la Red Inalámbrica y su información se verá protegida de posibles intrusos.

El siguiente documento se encuentra dividido en 4 capítulos, donde el primero de ellos se centra en el análisis de los problemas de la red Inalámbrica en estudio y además los problemas de seguridad de las redes inalámbricas en general.

El segundo capítulo corresponde a las tecnologías de diseño para las redes inalámbricas, así como los distintos sistemas de seguridad que se pueden implementar.

El tercer capítulo consiste en el diseño propiamente dicho de la Red Inalámbrica para el Complejo Hotelero y el sistema de seguridad para la misma red.

El cuarto capítulo trata de las pruebas realizadas del sistema de seguridad propuesto en una red de laboratorio. Así también se detalla el presupuesto de la solución final a implementar.

En el final del documento se encuentran las conclusiones de todo el documento, así como también las recomendaciones para futuros proyectos.

Un agradecimiento profundo a Dios
y mis padres, a quienes dedico todo
este trabajo.

INDICE:

Desde el principio, un tema fundamental con respecto al desarrollo y progreso, ha sido la necesidad de comunicación entre unos y otros. La aplicación de la tecnología inalámbrica, viene teniendo un gran auge en velocidades de transmisión, aunque sin competir con la utilización de redes cableadas o el uso de la fibra óptica, sin embargo cubre satisfactoriamente la necesidad del movimiento de los usuarios.

Entre los tipos de tecnologías inalámbricas, se encuentran las redes de pequeño alcance (WPAN), como los que usan los dispositivos Bluetooth; redes de área local (WLAN), como las aplicaciones Wi-Fi, y redes de área metropolitana (WWAN) como la creciente tecnología WIMAX. Todos los tipos antes mencionados, comparte un mismo objetivo, el intercambio de de información y comunicación a través del aire como medio de transmisión, lo cual lo convierte en una red muy vulnerable a posibles ataques.

Las redes inalámbricas de área local se presentan hoy en día como una alternativa para la conexión a Internet y constituyen en un complemento de las redes cableadas tipo Ethernet.

El presente trabajo tiene como objetivos el diseño de una red inalámbrica de área local para un complejo hotelero, el cual deberá poseer un sistema de seguridad y autenticación de usuarios para el uso exclusivo de huéspedes del mismo.

Para lograr estos objetivos, primero se realizará un estudio de la Infraestructura del hotel, para identificar toda el área a la cual se brindará cobertura de la red inalámbrica. También se realizarán mediciones de potencia de la red inalámbrica ya implementada en el hotel, para poder identificar el problema en relación a la señal e identificar también las zonas que no se encuentran dentro de la cobertura.

Seguidamente, se pasará a realizar un estudio de las redes inalámbricas, criterios de diseño y los métodos de seguridad más conocidos; para que finalmente se pueda elaborar un diseño basado en la elección y disposición de los puntos de acceso. En base al estudio realizado se presenta el diseño de un sistema de seguridad para la misma red, el cual cuenta con protocolos de encriptación y autenticación de usuarios.

Por último se presenta las pruebas realizados del sistema de seguridad en una red implementada en laboratorio y el presupuesto final del proyecto.

CAPÍTULO 1: ANÁLISIS DE LA RED INALÁMBRICA ACTUAL Y LOS SISTEMAS DE SEGURIDAD

1.1 Estado actual de las Redes Inalámbricas

En un periodo muy corto, las Redes Inalámbricas de Área Local se han convertido en una alternativa para la conexión a Internet, tanto en lugares empresariales como en oficinas, centros de cómputo y residencias; convirtiéndose no sólo en un complemento a las redes cableadas tipo Ethernet, sino también en una alternativa para su reemplazo.

Entre las ventajas más sobresalientes de usar redes de este tipo podemos mencionar la facilidad y rapidez de su instalación, la movilidad del usuario con equipo portátil, la Red Inalámbrica puede llegar a lugares donde el cableado sea quizás inaccesible. Por estas razones, se convierte en una implementación más simple debido a que se evita el cableado; adquiere una sencillez para añadir usuarios al sistema sin necesidad de instalar un punto adicional de conexión, como es el caso de las redes cableadas.

Sin embargo se debe considerar algunas desventajas de la red inalámbrica, entre las cuales se encuentran la relativa velocidad limitada, entre 1 a 54 Mbps y la inseguridad en las redes inalámbricas.

La desventaja más saltante en las Redes Inalámbricas de Área Local hoy en día es la poca seguridad con la que se diseñan las mismas, pues es bastante sencillo como personas no autorizadas pueden acceder a Redes Inalámbricas con pocas medidas de seguridad, dando posibilidad a que estas personas accedan a nuestra información.

Pero gracias al resultado del gran esfuerzo por mejorar la seguridad e inalterabilidad de los paquetes de información, nuevos protocolos y métodos de protección han ido sucediéndose, comenzando con la restricción de direcciones MAC (Media Access Control), el protocolo WEP (Wired Equivalent Privacy), el método de autenticación LEAP usado por la marca CISCO, y por último una mezcla de estándares y protocolos que involucra encriptación, autenticación y corresponde uno de los métodos más seguros en la actualidad: WPA (Wi-Fi Protected Access) y el uso de un servidor RADIUS para autenticación de usuarios.

Es debido a las ventajas de implementación de una Red Inalámbrica que los hoteles consideran más conveniente su elección que una red cableada Ethernet, lo cual favorece también en la conservación de la estética y acabado, pues se evita el paso de canaletas y cableado innecesario; favoreciendo de esta manera a los huéspedes,

que en viajes de recreación cuentan con un equipo portátil para el uso de Internet a través de una Red Inalámbrica.

1.2 Importancia de las redes inalámbricas en la actualidad

El amplio uso de las redes inalámbricas ha ido creciendo vertiginosamente en la actualidad. Según datos estadísticos proporcionados por la compañía consultora In-Stat/MDR [5], los equipos hardware para redes inalámbricas de tipo 802.11 crecieron para el año 2006, sobrepasando los 40 millones de unidades (Ver figura 1), y su precio irá disminuyendo considerablemente en la medida de que se sigan utilizando como alternativa para implementación de redes.

Comentario [ihlh1]: SE AGREGO FUENTE BIBLIOGRAFICA Y SE MEJORO LA REDACCIÓN

Las redes inalámbricas actualmente se encuentran instaladas en distintos lugares, incluso se prefiere en compañías grandes, como complemento a sus redes tipo Ethernet. Una de las más importantes razones del crecimiento de redes inalámbricas, es el mercado sorprendente de equipos inalámbricos como “laptop”, “PDA”, tarjetas inalámbricas para computadoras, celulares con conexión wi-fi, entre muchos otros.

Figura 1: Crecimiento de las Redes Inalámbricas de Área Local

http://www.instat.com

1.3 Inseguridad en redes inalámbricas

En gran parte de los casos en implementaciones inalámbricas, el intruso no tiene mucho que hacer para poder vencer las distintas barreras para ingresar a una red inalámbrica.

En un evento internacional llamado “DefCon” [5], mostró en el año 2002 un análisis de las Redes inalámbricas, donde solo el 29.8% de 580 Puntos de Acceso tenía habilitado el protocolo WEP como seguridad, 19.3 por ciento poseía el valor predeterminado del “SSID” y un 18.6 por ciento no poseían ningún tipo de seguridad.

Muchas de las redes las cuales fueron analizadas no solo eran redes de casa, también existían redes gubernamentales o redes de grandes compañías.

Según el reciente estudio de la compañía investigadora "Computer Economics" [4] realizado el año 2006, revela cuantas organizaciones descuidan el aspecto de seguridad en sus redes inalámbricas. Como se puede apreciar en la figura 2, 39% de las compañías confía en el protocolo WEP como medida de seguridad en redes inalámbricas, un 27% se encuentra en proceso por recién colocar esta medida de seguridad e increíblemente más de la tercera parte de las redes inalámbricas no cuentan con ninguna medida de seguridad.

Del mismo modo según se aprecia en la figura 3, para el estándar de seguridad WPA, solo el 42% de las redes inalámbricas funcionan bajo este protocolo.

Comentario [ihlh2]: SE AGREGO FUENTE BIBLIOGRÁFICA Y SE AGREGO DATOS ESTADÍSTICOS

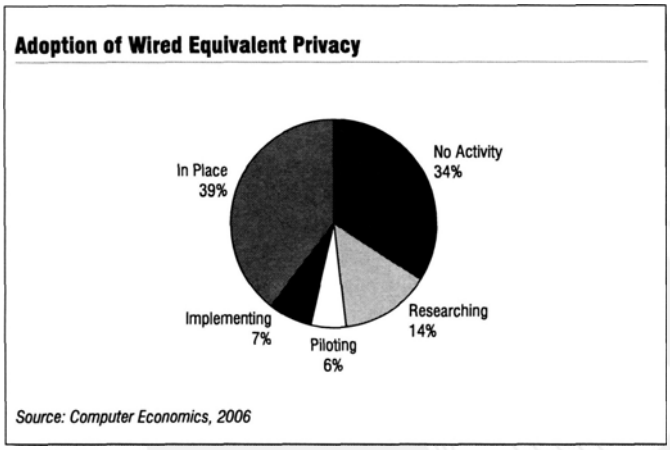

Figura 2: Cuadro estadístico del uso del protocolo WEP

Fuente: Computer Economics

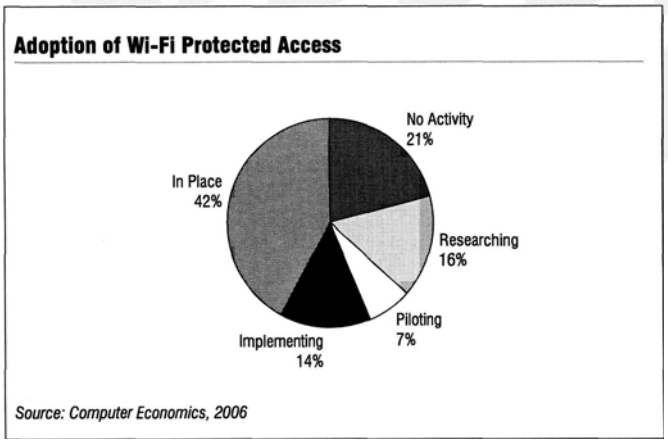

Figura 3: Cuadro estadístico del uso del protocolo WPA

Fuente: Computer Economics

1.3.1 Tres pilares de la Seguridad

Comentario [ihlh3]: NUEVO ITEM, AGREGUE ESTE NUEVO TEMA DENTRO DEL CAPITULO 1.

Uno de los mayores problemas en seguridad inalámbrica es el desconocimiento de las vulnerabilidades de la red o la aplicación de métodos ineficaces para protegerla; gran parte de las redes inalámbricas no poseen ningún nivel de seguridad, o implementan métodos inseguros como lo son el protocolo WEP, esconder el SSID, filtro de direcciones MAC.

Según lo señala Aaron E. Earle en su libro “Wireless Security HandBook” [14], cuando hablamos de seguridad en redes inalámbricas, no estamos refiriendo a tres grandes pilares: confidencialidad, disponibilidad e integridad. Entender los tres pilares de seguridad para redes inalámbricas, nos ayuda a entender que es lo que queremos proteger y porque.

Comentario [ihlh4]: SE AGREGA FUENTE BIBLIOGRÁFICA

Confidencialidad

Los ataques en la confidencialidad de información se relacionan con el hurto o la revisión sin autorización de datos. Esto se puede realizar de varias maneras, ya sea mediante la intercepción de información mientras esta se encontraba en comunicación o simplemente mediante el robo del equipo donde se encuentra la información.

Ataques a la confidencialidad en redes inalámbricas, se encuentra en el simple hecho de analizar las señales transmitidas a través del aire. El uso de encriptación combate este tipo de ataques, pues esto consiste en un lenguaje solamente entendido por el remitente y el destinatario.

Disponibilidad

Disponibilidad consiste en permitir solamente a los usuarios autorizados en poder acceder a su información, no está demás decir, luego de un proceso de autenticación de usuarios. Este proceso de autenticación de usuarios, permitirá el ingreso e intercambio de información a los usuarios autorizados a acceder a la red inalámbrica, luego de presentar ciertas credenciales digitales de su persona. De otra manera, siempre se denegará el ingreso a la red.

Integridad

Integridad involucra la modificación inautorizada de la información. Este puede significar la modificación de la información mientras se encuentra en comunicación o mientras se almacena en el dispositivo electrónico. Para proteger la integridad de la información de los usuarios, uno debe emplear un proceso de validación de paquetes de información.

1.3.2 Múltiples ataques a una red inalámbrica

Los ataques a una Red Inalámbrica son de distinto tipo, pero todos se basan en aprovechar la comunicación a través del aire de los puntos de acceso, en donde las tramas de información no solo llegan al usuario que las requiere sino a todos los usuarios que se encuentran en el área de cobertura. Esto es posible debido a que el medio de comunicación es el aire y mediante una tarjeta inalámbrica se pueden realizar distintos tipos de ataques dependiendo de las barreras que presenta la red a atacar.

Existen distintos tipos de ataques que se pueden realizar a una Red Inalámbrica, entre los cuales se tiene:

- Ataque de tipo ”Man-in-the-Middle”
- Ataque de tipo “Denial of Service“
- “Rogue AP”
- “Wireless bridge”
- “Spoofing”
- Programas “Sniffer”

Debido al amplio uso de Internet, el software especializado “Sniffer” para la captura y análisis de tramas de redes inalámbricas se encuentra al alcance de todos, generalmente este software es utilizado para gestionar la red y optimizarla, pero también es utilizado con fines maliciosos, uno de esos objetivos es poder romper llaves de protocoloes e ingresar a una red protegida por protocolo WEP por ejemplo.

Otro tipo de software muy usado son los programas “Spoofing”, los cuales sirven para cambiar la identidad del usuario, como IP, ARP, DNS o dirección física MAC; mediante este tipo de ataque, se puede ingresar a distintas redes las cuales se basen en un filtro de direcciones MAC.

1.4 Declaración del Marco Problemático

En nuestros días, la instalación de una Red Local Inalámbrica de Área Local se va haciendo cada día más común, ya sea para el sector residencial, como para el sector corporativo; debido a su facilidad de instalación y comodidad de precios (no necesita cableado UTP), es entonces que se enfrenta, ante un problemas de gran importancia: La seguridad de la información.

Las redes inalámbricas requieren nuevos conceptos de seguridad que se obvian en las redes cableadas; la razón de esto, es por la sencilla razón que para las redes inalámbricas, el medio de transmisión es distinto: es el aire. Cualquier persona que desee tener acceso a una red inalámbrica solo deberá encontrarse en la zona de cobertura del Punto de Acceso.

Ante tales problemas, múltiples protocolos y estándares han tratado de brindar los primeros intentos de seguridad; la mayoría de ellos han sido intentos fallidos; como el uso del protocolo WEP.

Además existe software dedicado y diseñado para aprovechar las debilidades de las redes inalámbricas, como por ejemplo los programas “sniffer”, entre ellos tenemos: AirSnort, AirCrack, Kismet.

Pero gracias al apoyo de la organización IEEE y la colaboración de la asociación “Wi-Fi Alliance”, por tratar de generar nuevos estándares más comprometidos con el tema de seguridad, nuevos estándares como WPA y 802.11i han surgido para poder hacer frente a uno de los mayores problemas de las redes inalámbricas.

Por lo expuesto la presenta tesis desarrolla el diseño de una Red Inalámbrica de Área Local segura para un Complejo Hotelero, quien actualmente cuenta con una Red Inalámbrica que no logra cubrir todas las instalaciones y no cuenta con ningún sistema de seguridad.

1.5 Análisis de la Estructura del Complejo Hotelero

Actualmente el Complejo Hotelero en estudio cuenta con una Red Inalámbrica de Área Local para el acceso a Internet por parte de los huéspedes, sin embargo la red mencionada no logra brindar cobertura a todas las zonas del complejo por razones de pérdida de potencia de la señal. El Complejo Hotelero se encuentra ubicado frente al mar, consta de un área administrativa y dos áreas de casas pequeñas, conocidas como “bungalows”.

El área administrativa incluye la recepción, los baños, una torre, la cocina y la sala de juego; por otro lado las habitaciones se encuentran divididas en 2 áreas, un área ubicada en el lado derecho y otra hacia el lado izquierdo del hotel; además cada área se encuentra conformada por 3 casas y cada casa cuenta con 2 habitaciones para los huéspedes. Se debe indicar que cada una de las pequeñas casas cuenta con una terraza con vista al mar, lugar donde también es requerido el acceso inalámbrico por parte de los usuarios.

El Complejo Hotelero sólo cuenta con una sola planta y la estructura tanto de la parte administrativa, como de las pequeñas cosas está conformada por paredes de aproximadamente 15 centímetros de espesor. Es importante señalar también que el resto del área del Complejo Hotelero, incluyendo las piscinas, no se encuentra techado y el Restaurante se encuentra hecho de madera y solo cuenta con techo, mas no de paredes.

En la figura 4 se muestra la estructura del Hotel.

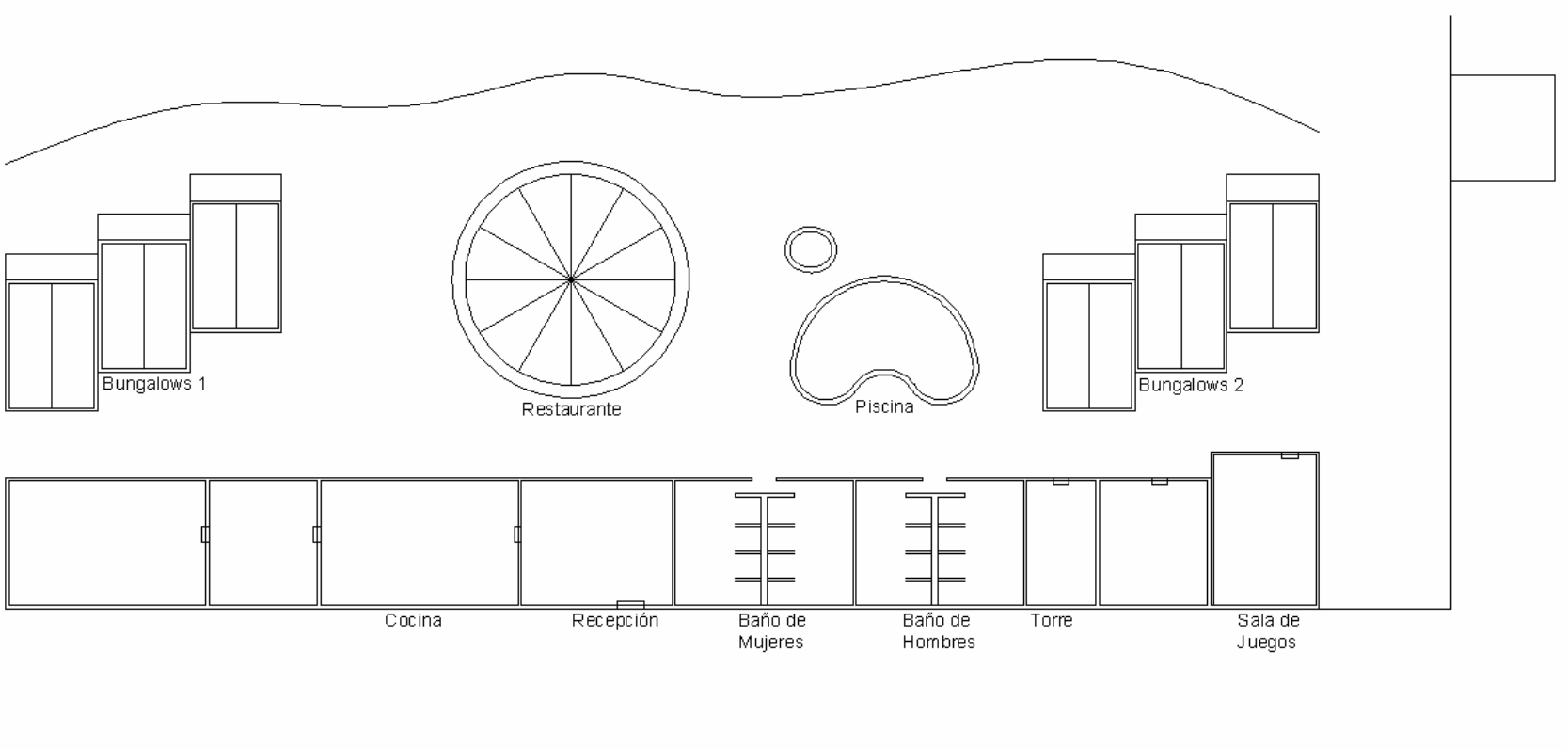

Figura 4: Estructura del Complejo Hotelero

1.6 Análisis de la Red Inalámbrica Actual

La actual Red implementada en el Complejo Hotelero está formada por un equipo de Telecomunicaciones para la conexión a Internet, consiste en un "router" de marca Zyxel, de modelo "Prestige 660HW", el cual es instalado por la compañía que provee servicio de Internet. Este router posee cuatro puertos RJ45 fastethernet 10/100 Base-T, para la implementación de una Red de Área Local cableada y un puerto RJ11 para la conexión hacia la línea telefónica para el servicio ADSL. Además este modelo de router posee una antena dipolo de 2.5 dbi de ganancia que provee la conectividad inalámbrica hacia Internet.

El router Zyxel se encuentra conectado a tres computadoras en el área de recepción del Hotel. En la figura 5 se muestra un Diagrama de la Red actual del Complejo.

Este router inalámbrico se encontró funcionando en el canal 6 de radiofrecuencia, el cual coincidía con el mismo canal de configuración de un Punto de Acceso instalado en el área vecina, lo cual generaba cierto grado de interferencia. El diagrama de Cobertura de la señal se encuentra bosquejado en la figura 6. El Punto de Acceso señalado con línea azul es con el que cuenta el Complejo Hotelero, el Punto de Acceso con línea roja es el equipo instalado en el área contigua.

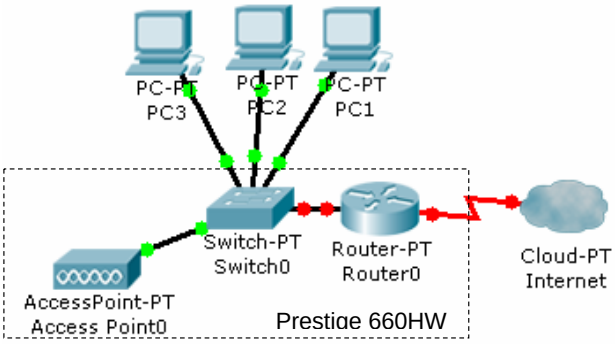

Figura 5: Diagrama de la Red Actual del Hotel

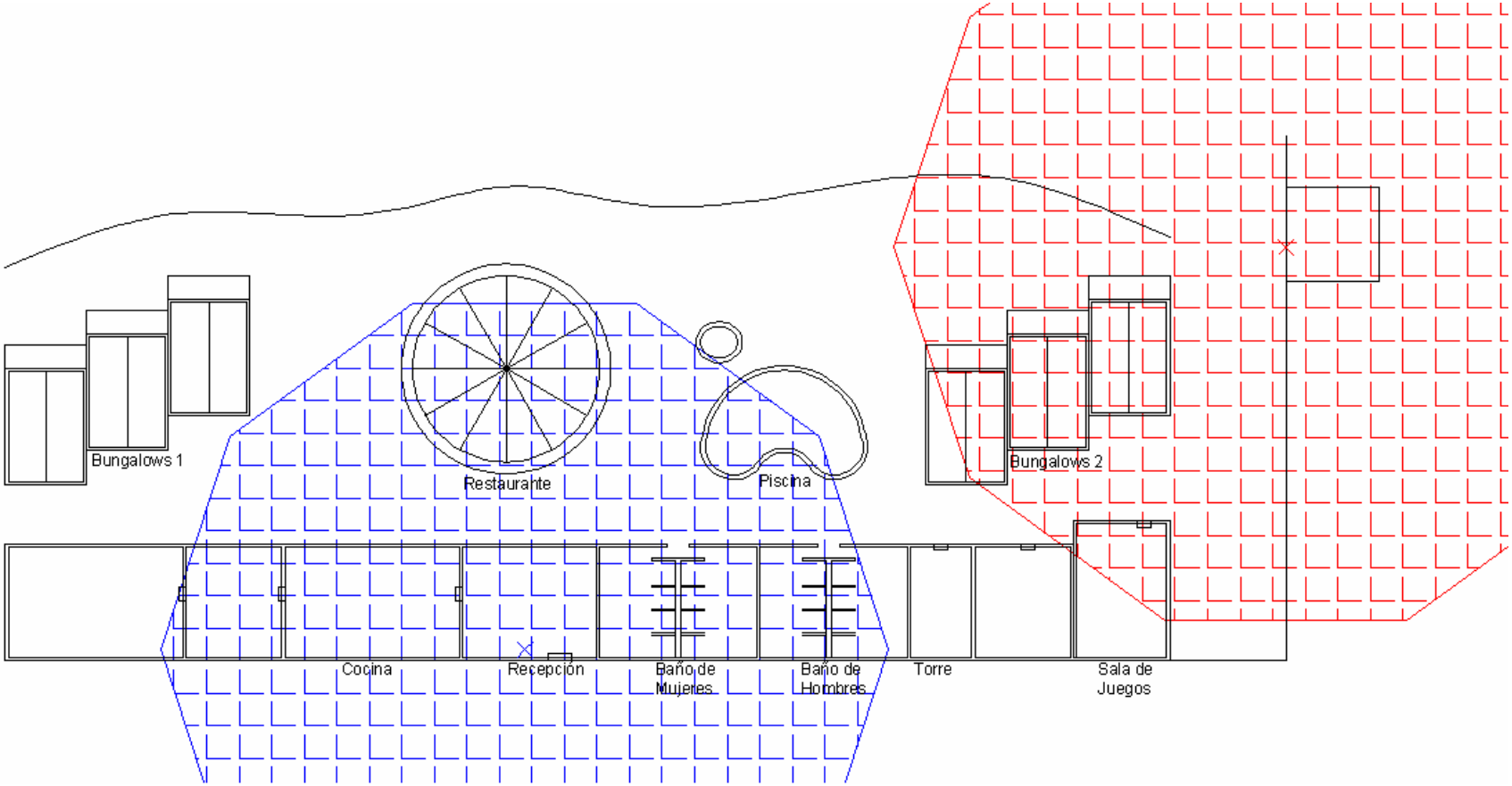

Figura 6: Cobertura de Actuales Puntos de Acceso

Comentario [ihlh5]: SE MEJORO EL GRÁFICO DE COBERTURA

1.7 Mediciones de Potencia

Para poder encontrar los actuales problemas de cobertura de la Red Inalámbrica del Complejo Hotelero se han realizado una serie de mediciones de la Señal respecto al ruido (SNR) del router inalámbrico Zyxel, en varias zonas del Complejo Hotelero. Las mediciones de potencia fueron realizadas con un software especializado denominado "Netstumbler" de versión 0.4.0, este programa puede ser instalado en un sistema operativo Windows y necesita de una tarjeta inalámbrica para poder realizar las mediciones. La tarjeta inalámbrica usada para las pruebas ha sido de marca Intel, de modelo "PRO/Wireless 3945ABG Network Connection" y el programa fue instalado en un equipo portátil. Las mediciones del programa Netstumbler son graficadas en un plano bidimensional, donde el eje Y corresponde a la potencia de la Señal respecto al Ruido, en unidades de "dBm", y en el eje X el tiempo, indicado en función de la hora en la que se realizó la prueba.

Es importante señalar que para poder realizar las pruebas, el router inalámbrico Zyxel configurado en el canal 6 inicialmente fue cambiado al canal 1 para poder disminuir la interferencia con el equipo instalado en el área vecina, el cual también estaba configurado en el canal 6.

Se realizaron 3 pruebas en todo el ambiente del Complejo Hotelero, la primera medición se hizo a 7 metros de distancia del router inalámbrico y se puede observar en la figura 7 con la línea de color rojo; la segunda medición se realizó a 37 metros de distancia del router inalámbrico y se muestra en línea azul en la misma figura. Por último se hizo una medición general en varias zonas del Hotel desde los 7 metros hasta los 37 metros de distancia, que es la zona que requiere de la cobertura de la red inalámbrica. El router inalámbrico se encuentra señalado con una "X" en la figura siguiente.

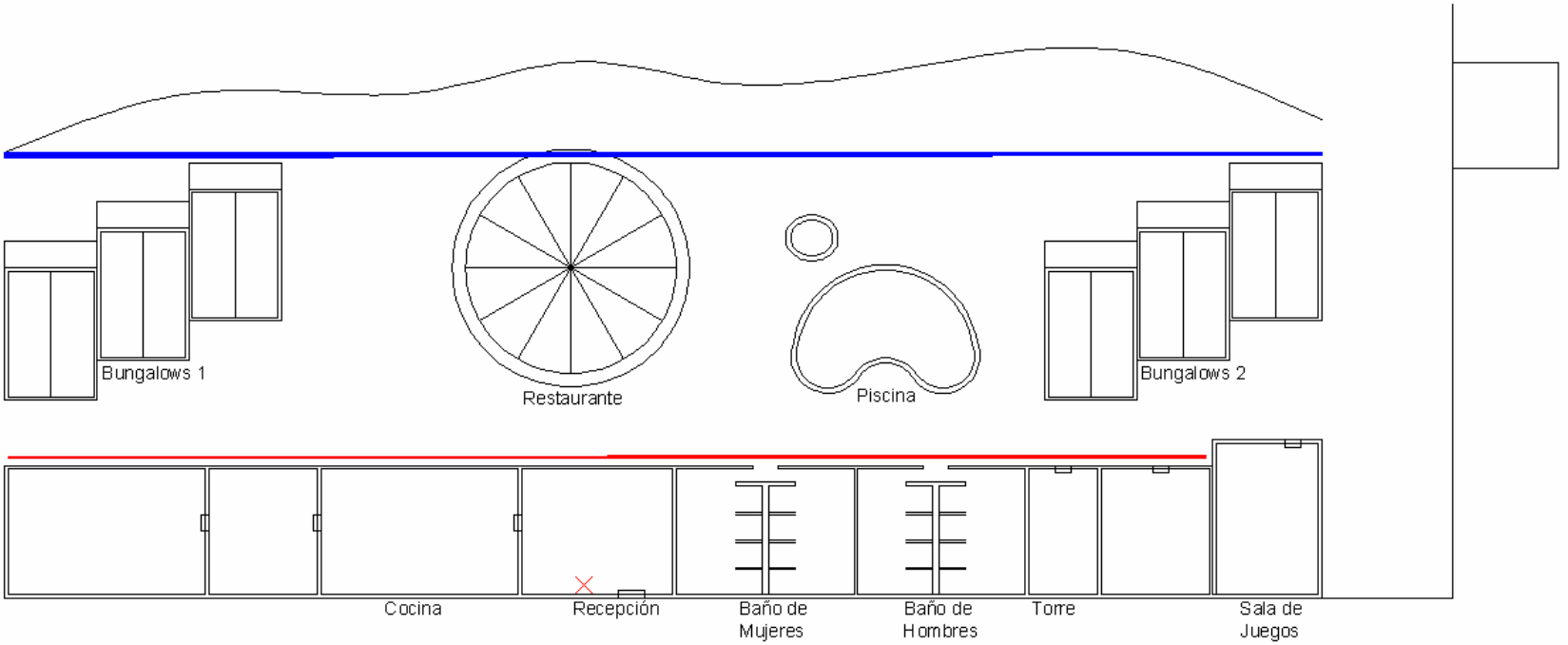

Figura 7: Lugar de Mediciones de Potencia

1.8 Resultado de las Mediciones

La medición realizada a 7 metros del router inalámbrico se muestra en la figura 8. Se puede observar que en el tiempo 11:56:30 se tiene una potencia muy baja de -90dBm y la situación donde se realizó la prueba corresponde a 50 metros a la derecha de la recepción, luego entre las horas 12:02:30 y 12:07:30 la potencia obtenida es aceptable y superior a -73dBm, en donde la zona medida fue 20 metros a la derecha y 20 metros hacia la izquierda de la recepción. En la hora 12:09:30 se tiene una baja potencia de -80dBm a una distancia de 40 metros a la izquierda del lugar de la recepción.

La segunda medición hecha a 37 metros del router inalámbrico se puede observar en la figura 9. En esta medición se puede apreciar la bajísima potencia de la señal, por ejemplo en el instante 14:05:42 la relación señal a ruido es de -93dBm, lo cual fue medido a 45 metros a la izquierda de la recepción, frente a las casas del lado izquierdo; de igual forma en el tiempo 14:12:50 se midió una potencia de -94dBm a unos 50 metros a la derecha de la recepción, lugar frente a las casas de la parte derecha del Hotel.

Por último en la tabla 1, se muestran los valores de potencia a una distancia de 7 hasta 37 metros del router inalámbrico, medidos cada 5 metros a distancias de 45 metros hacia la izquierda y 50 metros hacia la derecha de la recepción del Hotel. Estas mediciones quedan graficados en la Figura 10 para la mejor visualización del problema de potencia.

De esta manera queda demostrado el fuerte problema de pérdida de potencia por la gran cantidad de paredes que la señal de radiofrecuencia del Punto de Acceso tiene que superar.

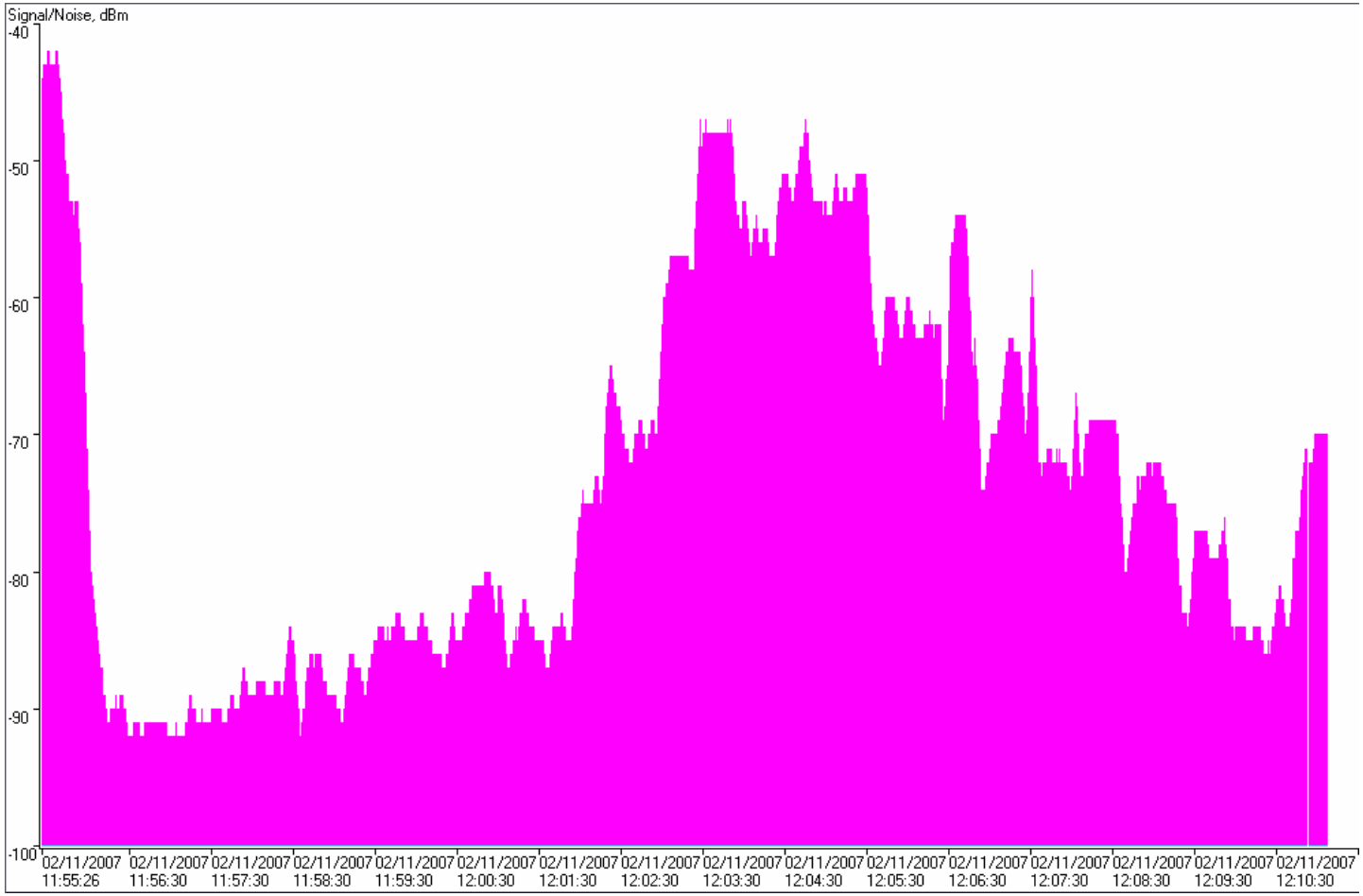

Figura 8: Medición de Señal a Ruido a 7 metros del equipo Zyxel

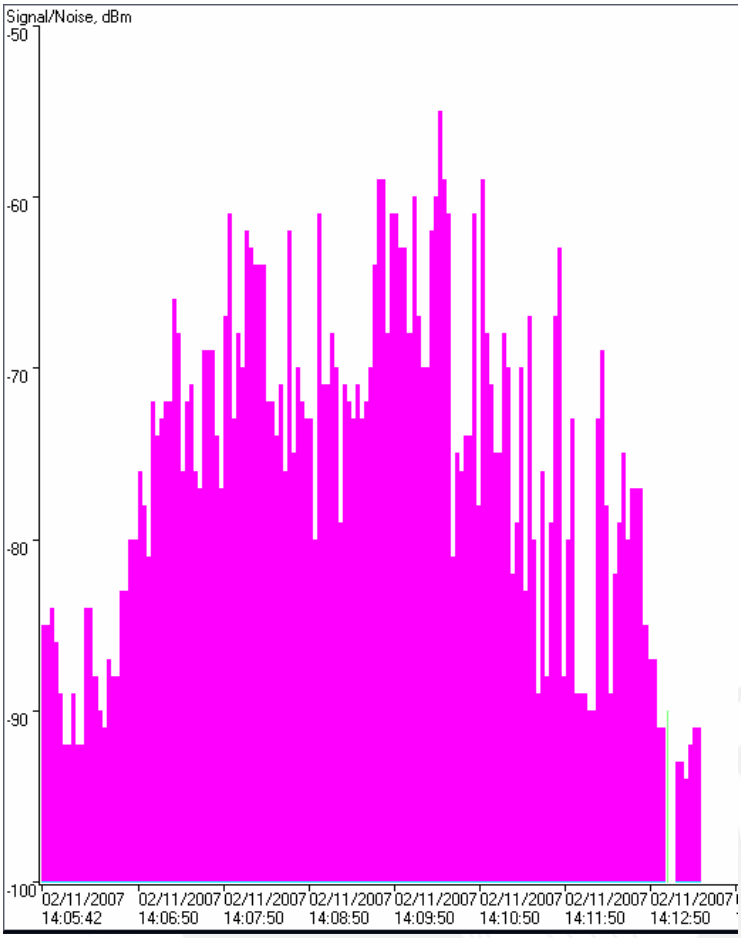

Figura 9: Medición de Señal a Ruido a 37 metros del equipo Zyxel

SNR(dBm)		Lado Derecho(m)												Lado Izquierdo(m)								
		55	50	45	40	35	30	25	20	15	10	5	0	5	10	15	20	25	30	35	40	45
Distancia	7	-92	-91	-89	-88	-85	-87	-84	-77	-70	-58	-48	-55	-53	-63	-66	-72	-72	-73	-78	-85	-85
	17	-90	-86	-84	-78	-75	-70	-68	-64	-58	-63	-70	-63	-70	-64	-68	-74	-72	-72	-75	-85	-89
	27	-85	-82	-72	-81	-80	-85	-64	-78	-73	-73	-76	-69	-74	-74	-73	-72	-72	-63	-83	-96	-95
	37	-87	-82	-77	-72	-70	-73	-75	-70	-81	-72	-81	-72	-71	-78	-81	-75	-77	-79	-84	-95	-97

Tabla 1: Medición de Señal a Ruido de 7 a 37m del equipo Zyxel

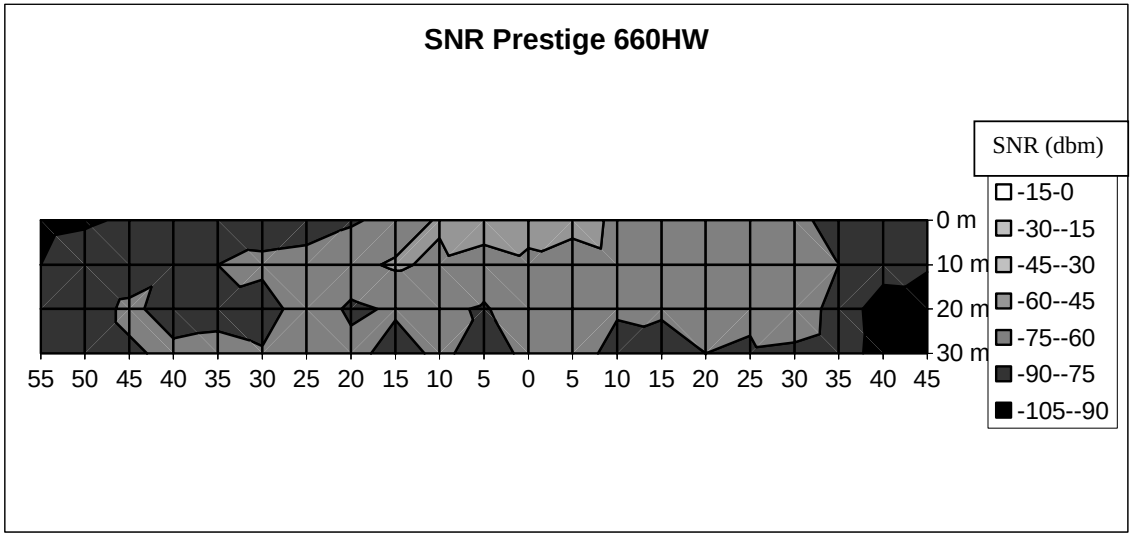

Figura 10: Medición de Señal a Ruido de 7 a 37m del equipo Zyxel

2.1 Red Inalámbrica de Área Local

Es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a las redes de área local cableadas o como extensión de éstas, utilizando tecnología de radiofrecuencia, esta tecnología está normada bajo el estándar 802.11 de la IEEE y se encuentra situada entre las tecnologías inalámbricas de mediano alcance, como se puede apreciar el en la figura 11:

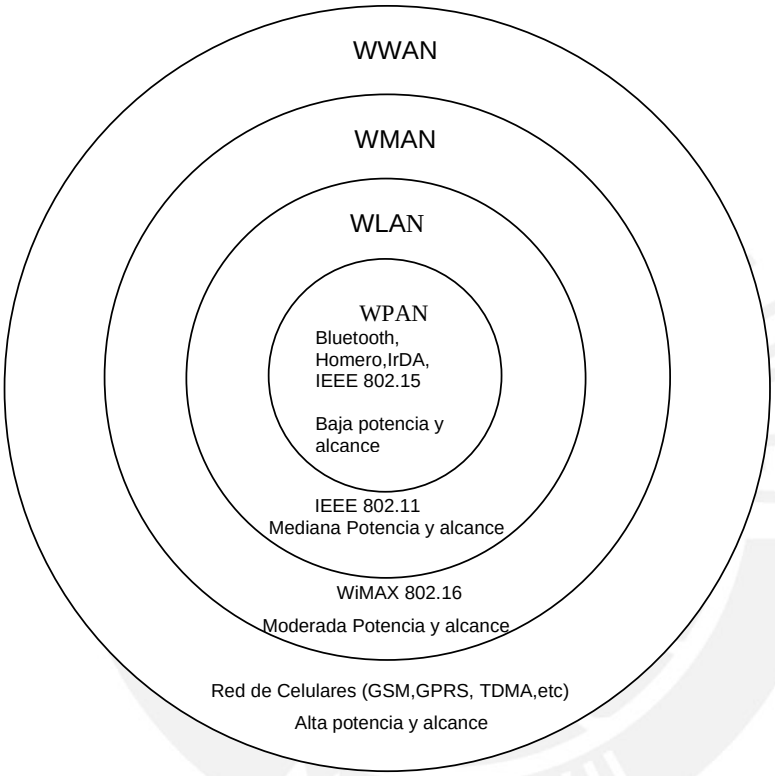

Figura 11: Tipos de Redes Inalámbricas

Entre las características más importante de las redes inalámbricas se pueden mencionar:

- Movilidad: permite transmitir información en tiempo real en cualquier lugar de la organización o empresa a cualquier usuario. Esto supone mayor productividad y posibilidades de servicio.

- Facilidad de instalación: al no usar cables, se evitan obras para tirar cable por muros y techos, mejorando así el aspecto y la estética de los locales, y reduciendo el tiempo de instalación. También permite el acceso instantáneo a usuarios temporales de la red.
- Flexibilidad: puede llegar donde el cable no puede, superando mayor número de obstáculos, llegando a atravesar paredes. Así, es útil en zonas donde el cableado no es posible o es muy costoso: parques naturales, reservas o zonas escarpadas.
- Costo de propiedad reducido: Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en hardware de una red cableada, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo, son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.
- Escalabilidad: las Redes Inalámbricas pueden ser configuradas en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

2.1.1 Los estándares en Redes Inalámbricas Locales

Existe una diversidad de estándares que surgieron para normar las comunicaciones en Redes Inalámbricas Locales, estas normas se iniciaron con el estándar 802.11, desarrollado en 1997 por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE). Este estándar base permitió la transmisión de datos hasta 2 Mbps. Poco después, dicho estándar fue ampliado, a través de extensiones las cuales son reconocidas por la incorporación de una carta al estándar 802.11 original, incluyendo el 802.11a y el 802.11b.

A continuación de mencionan los diferentes estándares para redes WLAN:

- 802.11 Estándar de Red Inalámbrica de Área Local original. Soporta de 1 Mbps a 2 Mbps.
- 802.11a Estándar de Red Inalámbrica de Área Local de alta velocidad para banda de 5 Ghz. Soporta 54 Mbps.
- 802.11b Estándar de Red Inalámbrica de Área Local para banda de 2.4 Ghz. Soporta 11 Mbps.
- 802.11e Dirige los requerimientos de calidad de servicio para todas las interfaces de radio de Red Inalámbrica de Área Local.

- 802.11g Establece una técnica de modulación adicional para banda de 2.4 Ghz. Propuesta para ofrecer velocidades hasta 54 Mbps y 108Mbps.
- 802.11i Dirige las actuales debilidades de seguridad para los protocolos de autenticación y encriptación. El estándar comprende los protocolos 802.1X, WPA-2 y AES.

2.1.1.1 Estándar 802.11

Comentario [ihlh6]: SE AGREGO LA EXPLICACIÓN DE LOS ESTÁNDARES 802.11, 802.11b Y 802.11g

El estándar 802.11 fue el primer estándar para redes inalámbricas de área local aceptado en el mercado. 802.11 define las capas física (Physical) y enlace (Media Access Control – MAC) para una red inalámbrica.

Este tipo de redes operan en dos tipos de capas de nivel físico: la primera se denomina “Direct sequence spread spectrum (DSSS)” y la segunda “Frequency hopping spread spectrum (FHSS)”. Cada una de las cuales utiliza un método distinto para transmitir señales inalámbricas a través del aire.

La capa de enlace ha sido estandarizada debido a la interferencia y la excesiva pérdida de paquetes si se le compara con Ethernet. El estándar 802.11 posee una máxima velocidad de 2Mps, razón por la cual se siguieron buscando nuevos estándares para mejorar dicha velocidad.

2.1.1.2 Estándar 802.11b

El estándar 802.11b fue creado en el año 1999, al mismo tiempo que el estándar 802.11a. 802.11b posee mayor ancho de banda su antecesor, el estándar 802.11, y además guarda compatibilidad con este, razón por la cual la migración del estándar 802.11 a 802.11b podría ser realizada de manera rápida por las compañías.

El estándar 802.11b posee una máxima velocidad de 11 Mbps, trabaja con DSSS a nivel de capa física e implementa a nivel de capa de enlace el “Acceso múltiple por detección de portadora con evitación de colisiones (CSMA/CA)”.

802.11b es uno de los estándares más ampliamente usados en redes inalámbricas hoy en día, así como el estándar 802.11g, debido a su notable mejora en velocidad.

2.1.1.3 Estándar 802.11g

En el año 2003 fue creado el estándar 802.11g. Dicho estándar usa la modulación OFDM en la capa física en la misma banda de frecuencia del estándar 802.11b (2.4 GHz). Por tanto el estándar 802.11g es compatible con el estándar 802.11g, esto significa que el estándar 802.11g puede soportar clientes del estándar 802.11. Sin embargo los puntos de acceso que soportan el estándar 802.11b necesitan una

mejora en el hardware para poder soportar el estándar 802.11g, pues corresponde a una técnica de modulación totalmente distinta.

802.11g provee de mayor ancho de banda, con una velocidad hasta de 54 Mbps. Lo cual no significa que los clientes 802.11b podrán alcanzar dicha velocidad. Si en una red inalámbrica de tipo 802.11g existe solo un cliente 802.11b, este disminuirá el ancho de banda de toda la red. El motivo por el cual el estándar 802.11g es compatible con el estándar 802.11b fue para facilitar la migración de las redes a este nuevo estándar.

2.1.2 Configuraciones de Redes Inalámbricas Locales

Existen dos tipos de configuraciones de una Red Inalámbrica de Área Local: la configuración Ad-Hoc y la configuración Infraestructura.

2.1.2.1 Red Ad-Hoc

Una Red Ad-Hoc es una Red de Área Local independiente que no está conectada a una infraestructura cableada y donde todas las estaciones se encuentran conectadas directamente unas con otras (en una topología tipo malla). La configuración de una red de área local inalámbrica en modo Ad-Hoc, se utiliza para establecer una red donde no existe la infraestructura cableada o donde no se requieran servicios avanzados de valor agregado, como por ejemplo una exposición comercial o colaboración eventual por parte de colegas en una localización remota.

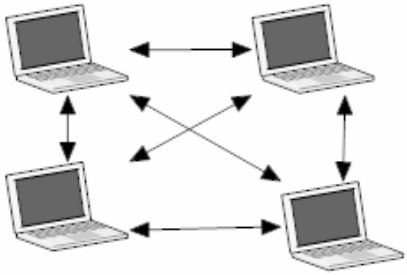

Figura 12: Configuración Inalámbrica Ad-Hoc

2.1.2.2 Red de Infraestructura

En una red de infraestructura, los clientes de una Red Inalámbrica se conectan a la red a través de un Punto de Acceso inalámbrico y luego operan tal como lo haría un cliente con cableado. La mayoría de las Redes de Área Local Inalámbricas opera en

modo de infraestructura y acceden a la red cableada para conectarse a las impresoras y servidores de archivos o para la conexión a Internet.

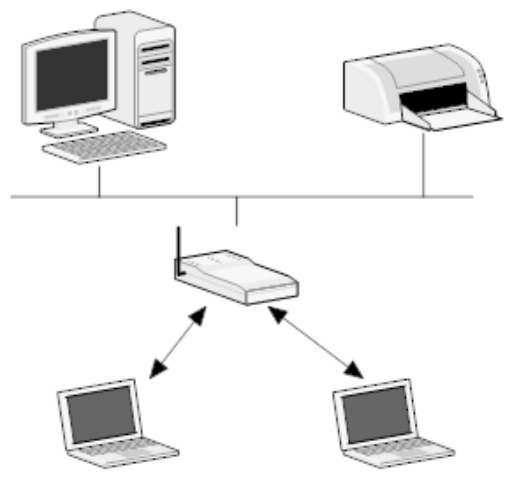

Figura 13: Configuración Inalámbrica Infraestructura

2.1.3 Espectro de Radio para las Redes Inalámbricas

Los dispositivos inalámbricos están obligados a funcionar en una determinada banda de frecuencia. Las entidades normativas controlan rigurosamente la asignación del espectro radioeléctrico a través de procesos de licencias; en el Perú el Ministerio de Transportes y Comunicaciones es la identidad que regula la asignación de bandas de frecuencia para las comunicaciones inalámbricas.

Las Redes Inalámbricas de Área Local es una tecnología inalámbrica la cual no necesita licencias para poder implementarse debido a que trabaja en la banda ISM del espectro de radio.

Bandas ISM

Las Bandas ISM (Industrial Scientific and Medical) corresponden a parte del espectro de radio destinado para aplicaciones de corte industrial, científico y médico. Las bandas ISM operan en las frecuencias de 902-928 MHz, 2.400-2.4835 GHz y 5.725-5.850 GHz (Tabla 2) y se caracterizan porque dichas bandas permiten un funcionamiento sin licencias, siempre que los dispositivos cumplan determinadas restricciones de potencia.

El estándar 802.11 funciona en las bandas ISM junto con muchos otros dispositivos como por ejemplo un horno microondas, equipos Bluetooth, entre otros. El estándar 802.11b y el 802.11g trabajan en la banda de 2.4 Ghz, mientras que el estándar 802.11a opera en la banda de 5GHz.

Banda	Rango de frecuencia
UHF ISM	902-928 MHz
Banda ISM S	2.400-2.4835 GHz
ISM Banda C	5.725-5.850 Ghz

Tabla 2: Bandas de Frecuencia ISM

2.2 Capa Física del estándar 802.11

La capa física del estándar 802.11 hace referencia a la modulación y codificación de los datos para ser enviados posteriormente por el aire.

La Comisión Federal de Comunicaciones (FCC) autorizó a los productos de redes inalámbricas a operar en las bandas ISM, mediante modulación de "esparcimiento del espectro" y con una potencia de salida de hasta 1 vatio.

2.2.1 Tecnologías de Espectro Ensanchado

La tecnología de espectro ensanchado, consiste en difundir la señal de información a lo largo del ancho de banda disponible, es decir, en vez e concentrar la energía de las señales alrededor de una señal portadora se pretende repartirla por toda la banda disponible. Este ancho de banda total se comparte entre todos los usuarios que se encuentran haciendo uso de la red inalámbrica en la misma banda de frecuencia.

Las tecnologías de espectro ensanchado más conocidas y usadas en redes de tipo WLAN son las siguientes:

FHSS: Espectro Ensanchado por Salto en Frecuencia

DSSS: Espectro Ensanchado por Secuencia Directa

OFDM: Multiplexación por División de Frecuencias Ortogonales

El estándar 802.11 utilizó la tecnología FHSS en sus inicios, luego el estándar 802.11b pasó a utilizar la tecnología DSSS, por otro lado los estándares 802.11a y 802.11g utilizan OFDM para la transmisión de datos. A continuación se detalla la tecnología DSSS y OFDM para la mejor comprensión del funcionamiento de una Red WLAN.

2.2.1.1 Tecnología DSSS

La tecnología DSSS opera en el rango de frecuencia de 2.4 GHz hasta los 2.4835 GHz, es decir, con un ancho banda total disponible de 83.5 MHz. Este ancho de banda total se divide en un total de 14 canales con un ancho de banda por canal de 5 MHz, de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras. En la Tabla 3 se presenta la asignación para los países de Norte América, Europa y Japón.

En una Red Inalámbrica con gran cobertura se pueden presentar varias celdas, ya sean solapadas o adyacentes, los canales en la que se encuentra funcionando cada celda pueden operar simultáneamente sin hacer interferencia en el sistema si la separación entre las frecuencias centrales, es como mínimo de 30 MHz. Esta independencia de canales permite aumentar la capacidad del sistema de forma lineal, colocando los puntos de acceso operando en los canales respectivos (Ver figura 14).

Los tipos de modulación utilizada por la tecnología DSSS son DBPSK – Differential Binary Phase Shift Keying y DQPSK – Differential Quadrature Phase Shift Keying, proporcionando velocidades de 1 y 2 Mbps.

Numero de Canal	Frecuencia GHz	Norte América	Europa	Japón
1	2.412	X	X	X
2	2.417	X	X	X
3	2.422	X	X	X
4	2.427	X	X	X
5	2.432	X	X	X
6	2.437	X	X	X
7	2.442	X	X	X
8	2.447	X	X	X
9	2.452	X	X	X
10	2.457	X	X	X
11	2.462	X	X	X
12	2.467		X	X
13	2.472		X	X
14	2.483			X

Tabla 3: Canales DSSS

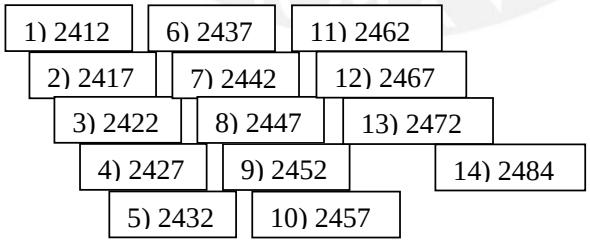

Figura 14: Distribución Canales DSSS

2.2.1.2 Tecnología OFDM

Esta tecnología es también denominada “Modulación por Multitono Discreto”, es una modulación que consiste en enviar la información modulando en QAM o en PSK un conjunto de portadoras de diferentes frecuencias. OFDM utiliza 52 portadoras de las cuales 4 se dedican a la transmisión de pilotos y el resto para datos, cada canal es de 20 MHz.

2.3 Capa Enlace del estándar 802.11

En la capa de enlace de las redes inalámbricas 802.11 se hace uso de la tecnología de Acceso múltiple por detección de portadora con evitación de colisiones: “CSMA/CA”. El Control de Acceso al medio es similar al utilizado en las redes cableadas tipo Ethernet, debido a que se aplica el concepto de “escuchar antes de transmitir”. Por otro lado la comunicación inalámbrica presentar ciertas diferencias respecto a las redes cableadas:

- El canal de radio no es un medio fiable, pues está sujeto a interferencias.
- Las estaciones no pueden monitorear fácilmente el canal cuando están transmitiendo.
- Solo una estación puede transmitir a la vez, pues si dos o más lo hacen, se producirá colisiones. Esto sucede debido a que solo se tiene un medio de transmisión que es el aire.

2.3.1 Formato Trama MAC

El estándar 802.11 define varios tipos de tramas cada una de las cuales tiene un objeto específico, por ejemplo cuando los puntos de acceso asocian estaciones, autentican clientes, o cuando la estación se encuentra en modo de bajo consumo; por lo que se puede clasificar las tramas dependiendo de la función que desempeñan. Se tienen tramas de datos, las que transportan la información de capas superiores, tramas de gestión que permiten mantener las comunicaciones y tramas de control para, como su nombre indica, controlar el medio.

La trama general del estándar 802.11 se puede apreciar en la figura 15:

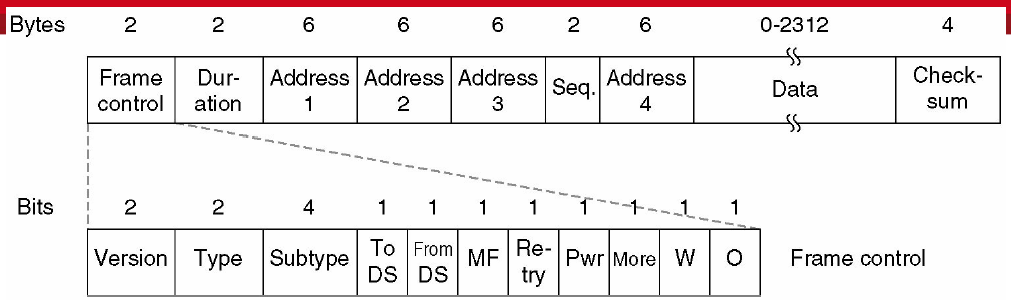

Figura 15: Formato Trama 802.11

Fuente: http://antares.itmorelia.edu.mx

El formato de la trama 802.11 contiene tramas de control: RTS, CTS, ACK, CF-End; tramas de gestión: Beacon, Probe Reques, Probe Response, Authentication, Associantion Request/Response; tramas de datos: Data, Null Data, Data+CF+Ack, entre otros.

La trama 802.11 también cuenta con banderas de 1 bit c/u: To DS, From DS, More Frag, Retry, Power Management, Wep, Orden.

2.3.2 Funcionamiento del CSMA/CA

Antes de transmitir información, una estación comprueba el medio o canal inalámbrico, para determinar su estado (libre u ocupado).

Si el medio no está ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada espaciado entre tramas (IFS)

Si luego de este intervalo temporal, o desde el principio del evento, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.

Una vez finalizado el tiempo de espera debida y el intervalo IFS, empieza el procedimiento de contención para ganar el acceso al canal, donde la estación ejecuta el denominado algoritmo de Backoff, según el cual se determina una espera adicional aleatoria. Este algoritmo nos ayuda a reducir la probabilidad de colisión, cuando por ejemplo varias estaciones se encuentran esperando el medio para poder transmitir.

Mientras se continúa esperando el tiempo del algoritmo de Backoff, se sigue escuchando el medio, de modo que si se determina libre para un tiempo igual a IFS, la estación podrá transmitir. De otro modo, si el medio no permanece libre en un tiempo igual a IFS el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición.

2.3.2.1 Mecanismo ACK

Si el paquete se recibe intacto, la estación receptora envía un paquete ACK a la estación emisora. El ciclo de transmisión termina cuando el emisor recibe este paquete.

Si el emisor no recibe un ACK, pueden darse dos opciones, el paquete de datos pudo no haber llegado o porque se perdió el ACK, se asume que se produjo una colisión y se espera un tiempo aleatorio para volver a transmitir el mismo paquete.

El Control de Acceso al Medio (capa MAC) es la encargada de asociar un cliente inalámbrico con un punto de acceso. Cuando una estación inalámbrica entra en la cobertura de uno o más puntos de acceso, se elige uno de ellos al cual se vincula, basándose en criterios de potencia de la señal recibida. Una vez vinculado a un punto de acceso, el cliente sintoniza un canal de radio en el que el punto de acceso esta configurado.

Los procesos que sigue la estación para vincularse con un punto de acceso son:

“Synchronization”

“Probe Process”

“Authentication Process”

“Association Process”

Después que la estación es autenticada y asociada con el punto de acceso, podrá utilizar los servicios y recursos de red y podrá comunicarse con el resto de equipos.

2.3.2.2 Proceso de Roaming

El proceso de Roaming consiste en la renovación del vínculo hacia un punto de acceso de mayor potencia dentro de una red inalámbrica, debido a la posible movilidad del usuario. También puede darse el caso de una renovación debido a la sobrecarga de la red sobre un punto de acceso, permitiendo el balance de carga sobre varios puntos de acceso. Esta vinculación dinámica de los puntos de acceso, permite ampliar zonas de cobertura empleando para ello una serie de celdas superpuestas.

El proceso de Roaming se realiza mediante el protocolo IAPP de la siguiente forma:

- La estación decide cuando renovar el enlace hacia otro punto de acceso, por no poseer la calidad suficiente en el actual enlace.
- La estación realiza la búsqueda para encontrar un nuevo punto de acceso.
- La estación envía una petición de reasociación hacia el nuevo punto de acceso.
- Si la petición no es aceptada el Terminal busca otro punto de acceso.

- Si el punto de acceso acepta la reasociación, el Punto de acceso notifica del proceso hacia el sistema de distribución, siendo informado el antiguo punto de acceso.

2.4 Seguridad en el estándar 802.11

2.4.1 Encriptación de paquetes

La encriptación es el proceso para que cierta información sin formato sea cifrado, de manera tal que sea ilegible para personas ajenas que no sean el transmisor o receptor, los cuales contienen los datos necesarios para su interpretación.

Esta medida de seguridad es ampliamente usada en transmisión de datos en redes cableadas tipo Ethernet, como también en redes inalámbricas. Algunos usos importantes de encriptación se encuentran en el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas de crédito, conversaciones privadas, entre otros.

La encriptación hace uso de diversos algoritmos matemáticos, para poder transformar un texto en un conjunto de caracteres sin sentido.

La encriptación se divide en dos tipos:

- Criptografía simétrica o de clave secreta (SKC): en la cual se usa una misma clave para cifrar y para descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma, el diagrama se puede observar en la Figura 16. Los estándares más usados son: Data Encryption Standard (DES), internacional Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), RSA Securities' RC4.

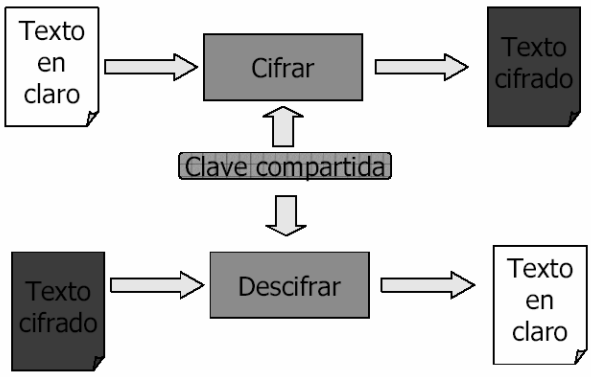

Figura 16: Criptografía Simétrica

Fuente: www.gris.det.uvigo.es/

- Criptografía asimétrica o de clave pública (PKC): en la cual se usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje. Este tipo de criptografía se inventó con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos, se puede apreciar el diagrama en la figura 17.

  Algunos estándares mas conocidos son: Rivest, Shamir and Adleman (RSA), Diffie-Hellman, Criptografía de curva elíptica.

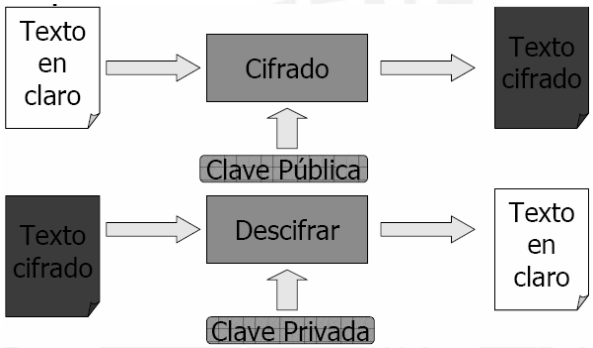

Figura 17: Criptografía Asimétrica

Fuente: www.gris.det.uvigo.es/

2.4.1.1 Protocolo Wired Equivalent Privacy (WEP)

Comentario [ihlh7]: SE CAMBIO TOTALMENTE LA EXPLICACIÓN DEL PROTOCOLO WEP.

El protocolo WEP fue creado para dar a las redes inalámbricas una seguridad similar a las redes cableadas. WEP es definido como un mecanismo de encriptación para proveer confidencialidad a los paquetes de información en redes inalámbricas.

El protocolo WEP es usado para poder encriptar los datos desde un cliente inalámbrico hasta un punto de acceso. WEP se basa en el algoritmo de cifrado simétrico RC4, el cual es aplicado a los datos de información y los bits de "IVC" o comprobación de integridad del paquete. Existen dos niveles de cifrado WEP: el primero está formado por una llave de cifrado de 40-bits y un vector de inicialización de 24-bits, esto da un total de 64 bits; el segundo nivel está formado por una llave de cifrado de 104-bits y un vector de inicialización de 24-bits, esto da un total de 128 bits.

El proceso de encriptación WEP empieza a partir del valor de una semilla, la cual debe ser introducida tanto en los puntos de acceso como en todos los usuarios miembros de la red. Este valor consiste en un número en base 16 de 26 dígitos. Además es

necesario de un vector de inicialización (IV) el cual es generado de manera aleatoria. Una vez obtenidos el IV y la llave WEP, entonces se procede a cifrar el paquete de datos mediante el algoritmo RC4. La llave WEP y el IV genera un número seudo aleatorio, el cual realiza una operación XOR con los datos y los bits de comprobación de datos "IVC", generando un paquete de datos cifrado (Ver figura 18). Luego se procede a colocar un encabezado al paquete ya cifrado y una copia exacta del vector de inicialización IV en texto claro (sin cifrar).

Posteriormente el cliente inalámbrico, una vez recibido el paquete de información cifrado, procede a recuperar el IV para realizar el algoritmo RC4 de manera inversa y recuperar el mensaje original.

En poco tiempo el protocolo WEP dejo entrever todas sus debilidades, pues radican en su propia estructura e implementación. Mediante un simple programa "Sniffer" cualquier intruso podría obtener el vector de inicialización y la llave WEP y de esta manera poder ingresar sin autorización a la red inalámbrica. Es por esta razón que el cifrado WEP no se considera un método de encriptación seguro para redes inalámbricas.

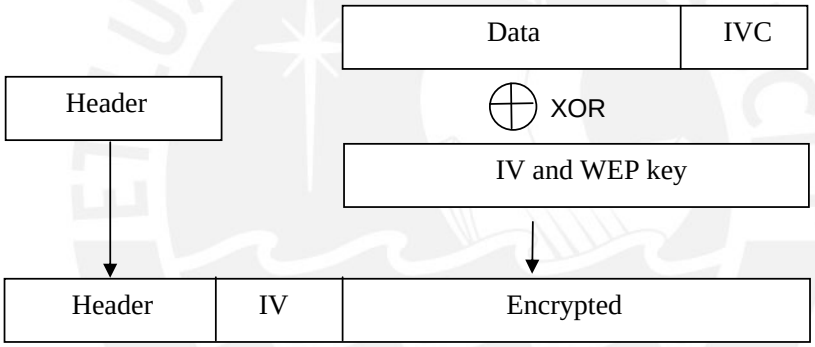

Figura 18: Proceso de encriptación WEP

Fuente: Wireless Security Handbook

Comentario [ihlh8]: NUEVA FIGURA DEL PROCESO WEP.

2.4.1.2 Estándar Wi-Fi Protected Access (WPA)

Comentario [ihlh9]: SE CAMBIO TOTALMENTE EXPLICACIÓN DEL PROTOCOLO WPA

El estándar Wi-Fi Protected Access fue creado por "Wi-Fi Alliance", como la necesidad de un estándar que mejore las deficiencias en seguridad del estándar WEP.

El estándar WPA soporta dos métodos de autenticación. El primer método consiste en la autenticación EAP en conjunto con el estándar 802.1x. Este método utiliza el protocolo EAP y 802.1x para la autenticación a través del aire del suplicante hacia el punto de acceso y el protocolo RADIUS para la autenticación del punto de acceso hacia el servidor de autenticación. Este método es el más seguro de los dos métodos de autenticación de WPA y requiere la menor cantidad de administración de usuario

final. El segundo método de autenticación de WPA consiste en el uso de llaves denominadas “preshared keys”. Esta opción requiere que la llave sea aplicada tanto a los dispositivos como a los puntos de acceso. Esto significa que todos los dispositivos tengan la misma clave ingresada, luego para combatir a posibles individuos que puedan usar la clave para obtener información transmitida por usuarios autorizados, WPA usa un método para crear una única llave por sesión para cada dispositivo. Esto se logra al tener una llave “preshared key” llamada “the group master key (GMK)” que maneja llaves temporales llamadas “pair transient key (PKT)”. Este segundo método de autenticación WPA fue creado para soluciones de casa y pequeñas oficinas (Small Office Home Office SOHO) pues es un método más sencillo de implementar que el primero.

WPA soporta el protocolo TKIP y MIC, los cuales son compatibles con los dispositivos que soportan el protocolo WEP. Asimismo WPA soporta el protocolo AES del estándar 802.11i, pero ciertamente más limitado que este.

Temporal Key Integrity Protocol (TKIP)

Comentario [ihlh10]: SE AGREGA EXPLICACIÓN DEL PROTOCOLO TKIP

El protocolo TKIP es la solución desarrollada para eliminar el problema del uso repetitivo de llaves del protocolo WEP. Este protocolo forma parte de las herramientas de los estándares WPA y 802.11i.

TKIP es un estándar que fue creado para facilitar la migración del protocolo WEP a este nuevo protocolo, pues para lograrlo no hay la necesidad de un nuevo dispositivo inalámbrico o hardware, sino basta la actualización de un pequeño programa o “firmware”.

El cifrado TKIP es un proceso de dos fases. La primera fase genera una llave por sesión de usuario, a partir de una llave temporal “temporal key”, un contador “TKIP sequence counter (TSC)” y la dirección MAC del usuario transmisor. Esta llave temporal “temporal key” es un valor de 128 bits, valor similar al de las llaves WEP. El contador TSC esta formado a partir de la dirección fuente, la dirección destino, la prioridad y los datos. Una vez terminada esta fase, un valor llamado “TKIP-mixed transmit address and key (TTAK) es creado. Este valor es usado como una llave de sesión para la segunda fase.

En la segunda fase, el valor de TTAK y el vector de inicialización (IV) son usados para producir una llave para poder encriptar todos los datos. Este cifrado se realiza mediante el algoritmo RC4, del mismo modo que WEP lo utiliza.

Es por esta razón que el protocolo TKIP es mucho más seguro que su antecesor WEP, pues no usa una misma llave para cifrar los datos, sino que esta llave varía dependiendo de que usuario se este comunicando y de que modo lo haga.

TKIP Message Integrity Check (MIC)

Comentario [ihlh11]: SE AGREGA EXPLICACIÓN DEL ALGORITMO MIC

TKIP Message Integrity Check es un protocolo creado para combatir contra los ataques de modificación de paquetes de información. El protocolo MIC o también denominado Michael, es un método mucho más seguro que el protocolo IVC usado para integridad de paquetes en WEP.

MIC utiliza un algoritmo tipo "hash" a partir de un valor semilla, la dirección MAC destino, la dirección MAC fuente, la prioridad y la carga útil; dando menos oportunidad que un intruso pueda modificar el paquete sin que el algoritmo MIC lo detecte. A su vez MIC es cifrado dentro de la porción de datos, de modo que ningún programa "Sniffer" de algún intruso pueda obtenerlo.

Para poder combatir los ataques contra modificación de paquetes, TKIP y MIC implementan un mecanismo por el cual el punto de acceso involucrado suspende todas las comunicaciones si es que se producen dos fallas MIC en menos de 60 segundos. Si es que esto logra pasar, el punto de acceso retomará actividad dentro de 60 segundos más, y requerirá que todos los usuarios vuelvan a conectarse y negocien nuevamente sus llaves de cifrado. Por otro lado para poder prevenir que este mecanismo sea inválido, debido a la modificación de paquetes por el ruido inherente a las comunicaciones RF; el algoritmo MIC se basa antes en la comprobación de los datos del paquete de información, la cual es realizada por los siguientes algoritmos: "frame check sum (FCS)", "integrity check sum (ICV)" y "TKIP sequence counter (TSC)".

2.4.2 Autenticación del estándar 802.11

El proceso de autenticación para redes inalámbricas consiste en un método de seguridad, es el proceso por el cual se verificar la identidad digital del remitente de una comunicación, como una petición para conectarse y así poder tener acceso a la red inalámbrica y sus recursos.

Normalmente las autenticaciones son hechas ante un servidor, el cual posee una base de datos, con los usuarios permitidos de acceso.

Existen diferentes tipos de autenticación de usuarios, empezando por la autenticación a través de un servidor, tal como un servidor RADIUS o un servidor OpenLDAP en Linux.

El protocolo más usado para la autenticación es: Extensible Authentication Protocol, o EAP, el cual es una estructura de soporte, cuyos métodos modernos proveen un mecanismo seguro de autenticación y negociación entre el dispositivo cliente y el servidor RADIUS. Una vez autenticado un usuario se puede abrir una sesión inalámbrica cifrada por ejemplo con el protocolo TKIP.

2.4.2.1 Estándar 802.1x

Comentario [ihlh12]: SE CAMBIO TOTALMENTE LA EXPLICACIÓN DEL ESTÁNDAR 802.1x

El estándar IEEE 802.1X es un protocolo de autenticación inicialmente desarrollado para redes cableadas como Ethernet, FDDI, token ring, y luego se adoptó en el ambiente inalámbrico, como una necesidad inherente a esta tecnología.

El estándar 802.1x no involucra ningún tipo de encriptación o cifrado, todo este proceso toma lugar fuera del protocolo. En redes inalámbricas, el protocolo EAP usa uno de varios métodos de encriptación para el proceso de autenticación tipo 802.1x. Luego que el proceso de autenticación es válido, el suplicante puede comenzar la transmisión de datos a través de cualquiera de los protocolos WEP, TKIP, AES u otro estándar de encriptación para redes inalámbricas.

El estándar 802.1x funciona en conjunto con otros estándares como lo son EAP y RADIUS. 802.1x es solo el mecanismo que deniega cualquier tipo de tráfico hacia la red, excepto paquetes de tipo EAP. Una vez que el protocolo EAP reconoce como válido a un usuario, el estándar 802.1x avisa al punto de acceso para que permita el tráfico al usuario validado.

Como muestra la figura 19, el estándar 802.1x involucra 2 protocolos, desde "Supplicant" (laptop) hacia "Authenticator" (punto de acceso) el protocolo es EAP. Desde el "Authenticator" hacia "Authentication Server" (servidor RADIUS) el protocolo es RADIUS. El protocolo 802.1x toma todas las peticiones EAP del "Supplicant" y las envía hacia el servidor RADIUS y espera por una respuesta. La respuesta deniega o permite el acceso del "Supplicant" en la red.

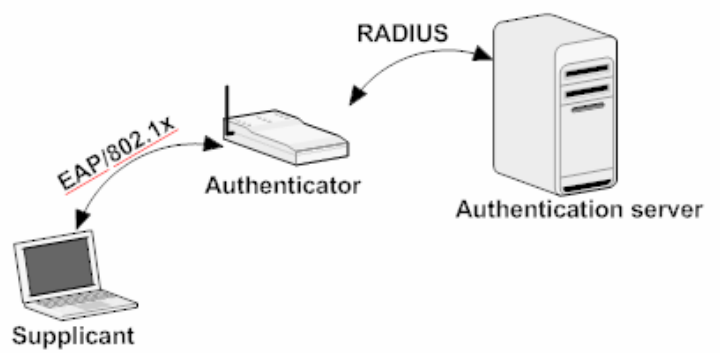

Figura 19: Autenticación 802.1x

Comentario [ihlh13]: NUEVA FIGURA, BASTANTE SIMPLE DEL ESTÁNDAR 802.1x

2.4.2.2 Remote Authentication Dial-In User Service (RADIUS)

Comentario [ihlh14]: SE CAMBIO TOTALMENTE LA EXPLICACIÓN DE RADIUS

RADIUS es el acrónimo de *Remote Authentication Dial-In User Service*, es un protocolo usado en redes para realizar autenticación, autorización y contabilidad de usuarios. RADIUS puede funcionar en distintos dispositivos de red como *switch*,

router, servidores, puntos de acceso, entre otros. La función de este protocolo es crear un túnel seguro entre el dispositivo de red y el servidor RADIUS; el cual es usado para enviar información sobre la identidad del usuario, los recursos que puede acceder y los recursos que ya accedió. Para poder crear este túnel es necesario una contraseña o *secreto compartido*, el cual debe localizarse tanto en el servidor RADIUS como también en el dispositivo de red que usa el protocolo.

Uno de los beneficios de RADIUS es el uso de una base de datos de usuarios, donde se puede almacenar los nombres de usuarios y sus respectivas contraseñas. Algunas bases de datos con las que trabaja RADIUS son Microsoft Active Directory, Novell Network Directory System, MySQL, Lightweight Directory Access Protocol (LDAP), entre muchos otros.

El protocolo RADIUS permite a los administradores de red poder localizar y administrar el acceso de usuarios y realizar el proceso de contabilidad o reporte en todos los equipos de red involucrados, así como poder realizar un acceso remoto a ellos.

Las especificaciones de este protocolo se encuentran definidas en los documentos RFC 2865 y RFC 2866 [13].

En el ambiente inalámbrico, el protocolo RADIUS funciona entre los puntos de acceso y el servidor RADIUS, siendo los puntos de acceso los negociadores de las peticiones de acceso por parte de los usuarios. De esta manera, cuando un usuario requiere el acceso a la red son los puntos de acceso quienes le proveen un tipo de autenticación; seguidamente los puntos de acceso verificarán la identidad del usuario en la base de datos del servidor RADIUS. Si las credenciales del usuario son correctas, entonces tendrá acceso permitido a la red, de lo contrario se le deniega el ingreso.

RADIUS posee cuatro tipos de paquetes para autenticación, los cuales se detallan a continuación:

- *Access-Request*: Este paquete consiste en una petición para ser atendido, dando inicio a la secuencia RADIUS.
- *Access-Accept*: Este paquete informa al cliente RADIUS (punto de acceso) que la autenticación es correcta.
- *Access-Reject*: Este paquete informa al cliente RADIUS que la autenticación es incorrecta.
- *Acces-Challenge*: Este paquete es usado para hacer un pedido de credenciales de usuario al cliente RADIUS.

Como se ha mencionado el servidor RADIUS es un tipo de servidor de clase AAA: Authentication, Authorization y Accounting, la cual es una estructura para el control de

acceso a recursos de computadora, manejo de políticas, análisis de uso de recursos y proveer la información necesaria para acceder a estos recursos. Estos procesos son considerados de vital importancia para la eficiencia y la eficacia del manejo de redes y seguridad.

Authentication

Consiste en el proceso de identificación de usuarios mediante la petición y comparación, de una serie de credenciales válidas. La autenticación es realizada en cada usuario usando el mismo criterio para obtener acceso a la red.

El servidor AAA compara la información de autenticación del usuario con la base de datos ya ingresada; si las credenciales son válidas, el usuario gana acceso a la red y sus recursos, de otra manera, el proceso de autenticación falla y el acceso es denegado.

Authorization

Es el proceso siguiente al de autenticación, y consiste en determinar si el usuario esta aprobado de usar ciertos recursos de red, tareas u operaciones que haya requerido. Usualmente el proceso de autorización se realiza junto con el de autenticación, una vez que el cliente es aprobado, este puede usar de los recursos. Un buen proceso de autorización queda determinado por una buena política de administración.

Accounting

Es el aspecto final de una estructura AAA, permite la revisión y el reporte de eventos y uso de recursos que cada usuario, también permite analizar la capacidad del sistema, o dar mantenimiento de la política de administración.

2.4.2.3 Extensible Authentication Protocol (EAP)

Comentario [ihlh15]: SE AGREGO EXPLICACIÓN DE AUTENTICACIÓN EAP

Extensible Authentication Protocol (EAP) es un protocolo desarrollado para autenticación de usuarios de una red. EAP es el resultado de mejorar anteriores intentos fallidos como lo fueron los protocolos “Password Authentication Protocol (PAP)” y “Challenge Handshake Authentication Protocol (CHAP)”. Para usar EAP, uno debe especificar dentro del campo de “Type field” que clase de autenticación se va a usar y esto es porque el protocolo EAP soporta distintas técnicas de autenticación (passwords, tarjetas inteligentes, certificados digitales) y esto lo logra sin tener que realizar cambios en su estructura.

El protocolo EAP es incluido en un paquete de tipo “Point-to-Point Protocol (PPP)”, esto permite que cualquier dispositivo que soporte PPP también soporte el protocolo

EAP. Además el protocolo EAP soporta el estándar 802.1x y esto ha sido logrado en el documento RFC 3748.

El paquete EAP está formado por 5 campos: “code”, “identifier”, “length”, “type” y “data”, como se muestra en la figura 20. Dichos campos sirven para identificar la función del paquete, relacionar múltiples usuarios, saber el tamaño del paquete, conocer el tipo de modulación usada y los datos de información que componen el paquete.

Code	Identifier	Lenght	Type	Data
8 Bytes	8 Bytes	16 Bytes	8 Bytes	Variable length

Figura 20: Formato del paquete EAP

Comentario [ihlh16]: NUEVA FIGURA DE PAQUETE EAP

Los tipos de modulación EAP conocidos son: EAP-MD5, EAP-TLS, EAP-TTLS, LEAP, PEAP y EAP-FAST. A continuación se explicará el tipo de modulación usado y porque se escogió de entre los demás.

2.4.2.4 Protocolo EAP- PEAP

Comentario [ihlh17]: SE AGREGA EXPLICACIÓN DE PROTOCOLO EAP-PEAP

Protected Extensible Authentication Protocol (PEAP) es un protocolo creado por el esfuerzo común de RAS, Microsoft y Cisco Systems, para poder manejar un método de autenticación EAP común a varias compañías.

Una de las principales ventajas de PEAP es tener un fuerte tipo de autenticación EAP que no requiere certificados digitales de los clientes. EAP-PEAP trabaja similarmente como el protocolo EAP-TLS, de modo que crea un túnel cifrado con TLS (Transport Layer Security) para poder realizar la autenticación del usuario hacia el Servidor de Autenticación.

El proceso de autenticación EAP-PEAP empieza mediante una paquete “request packet” del suplicante para ser atendido. El punto de acceso escucha la petición y responde mediante un paquete “response packet”. Esta respuesta también preguntará al suplicante por su correspondiente identidad. La identidad será el tipo de EAP, en este caso EAP-Type=PEAP, esto significa que el tipo de autenticación usada por el servidor de autenticación será PEAP. El tráfico de datos se transportará por intermedio del punto de acceso, el cual es llamado tambien “Authenticator”. Una vez que el método de autenticación PEAP es elegido, un túnel cifrado TLS es creado mediante un certificado del servidor de autenticación. Es por este túnel TLS que el proceso de autenticación del suplicante toma lugar.

El diagrama del proceso de autenticación PEAP se muestra en la figura 21.

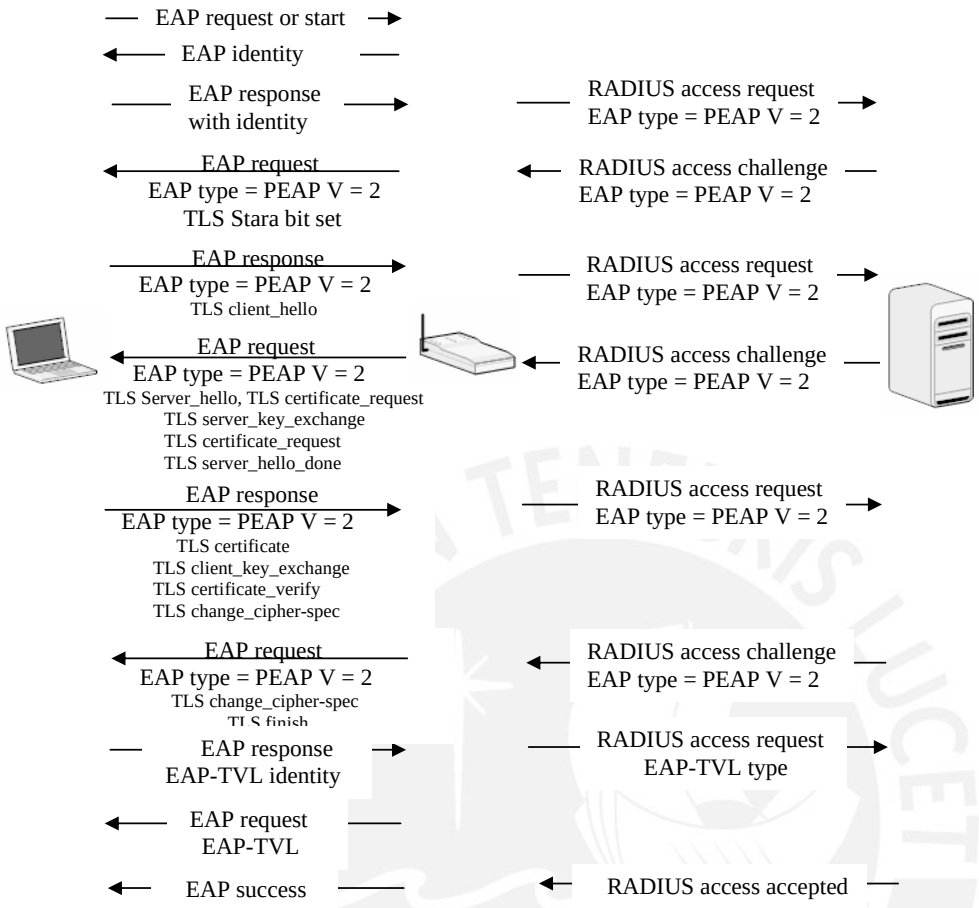

Figura 21: Proceso autenticación EAP-PEAP

Comentario [ihlh18]: NUEVA FIGURA, DE LA EXPLICACIÓN DETALLADA DEL FUNCIONAMIENTO DE EAP-PEAP

2.5 Puntos de Acceso

Un Punto de Acceso es un dispositivo que permite la conexión inalámbrica, está usualmente conectado a una red cableada ethernet y puede intercambiar tráfico entre la Red cableada con la Red Inalámbrica. Se puede disponer de varios Puntos de Acceso para poder lograr la cobertura de un área de mayor distancia, haciendo uso de un método denominado “Roaming” que consiste en la creación de celdas de alcance, en donde el usuario puede movilizarse pudiendo registrarse en los distintos Puntos de Acceso.

Para poder lograr un diseño eficaz de los Puntos de Acceso que soporten “roaming”, debe considerar una pequeña superposición de las coberturas de los access points de

tal manera que los usuarios puedan desplazarse por las instalaciones y siempre tengan cobertura.

Los Puntos de Acceso incluyen un algoritmo de decisión que decide cuando una estación debe desconectarse de un Punto de Acceso para acceder a otro más cercano. En la figura 22 se puede apreciar dicho efecto “Roaming”:

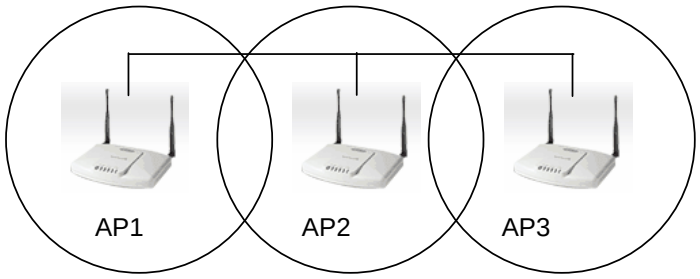

Figura 22: Proceso “roaming” formado entre tres Puntos de Acceso

2.6 Consideraciones para Diseño de Redes inalámbricas

Cobertura y Velocidad

Al diseñar una Red Inalámbrica de Área Local se debe tomar en cuenta todas las zonas que necesitan la cobertura de la Red. Luego teniendo como base el espacio total donde se va a instalar la Red Inalámbrica y la estructura de la edificación, entre esto se cuenta la cantidad de paredes que la señal de radiofrecuencia tendrá que superar, se realiza la disposición de los Puntos de Acceso para poder lograr una disposición de celdas que logren alcanzar todas las instalaciones del lugar; para ello es necesario asignar los canales de radio de manera que no exista interferencia entre celdas vecinas.

Se deberá tomar en cuenta también la velocidad requerida por la Red Inalámbrica, la cual depende de la potencia de recepción del equipo portátil, esto significa que, si la potencia recibida por el equipo es baja, la velocidad también lo será y si la potencia recibida es relativamente alta, la tasa de transferencia será más rápida.

Ahora si el requerimiento de la red son velocidades altas, pues se tendrá que diseñar una Red Inalámbrica con varios puntos de acceso, formando celdas bastante superpuestas, para que de esta manera, todas las áreas cubiertas se encuentren a una potencia considerable. Por otro lado, si solo se necesita una velocidad moderada pues se podrá diseñar la red con pocos puntos de acceso, aprovechando al máximo la potencia de la señal, la cual alcanza una distancia aproximada de 30 a 100 metros con un equipo de 32mW de potencia y una antena de 2.5dbi de ganancia.

Compatibilidad

En el diseño de una Red Inalámbrica se debe tomar en cuenta la compatibilidad con la red ya instalada y que se encuentra funcionando, la que puede ser una red cableada tipo Ethernet. Además saber que estándares en la red inalámbrica estuvieron funcionando hasta el momento. Por ejemplo si los usuarios se encontraron trabajando con el estándar 802.11a o el estándar 802.11b/g. Además se tiene que pensar no solo en respetar los estándares que se encuentran funcionando hasta el momento, sino también pensar la implementación realizada sea compatible con futuras implementaciones que se vayan a agregar, a esto se llama escalabilidad.

Interferencia y Selección de canales de radio

Las redes inalámbricas de área local trabajan en bandas ISM, junto con otros equipos electrónicos como por ejemplo los hornos microondas y los equipos de tecnología "Bluetooth", los cuales pueden causar interferencia en la Red WLAN.

Además puede existir interferencia entre 2 o más puntos de acceso de la misma red o de una red distinta, es por esto que se debe tener especial cuidado en el diseño y la elección de canales de radio para la Red Inalámbrica, para evitar la interferencia entre los puntos de acceso se deberán configurar entre los 11 canales de radiofrecuencia respectivos que no causen interferencia entre ellos. Una posibilidad es elegir los canales 1 – 6 – 11 para celdas contiguas.

2.7 Consideraciones para la Elección de los Puntos de Acceso

Para poder seleccionar un punto de acceso con el cual diseñar la Red Inalámbrica se han tomado las siguientes consideraciones:

- Estándares de trabajo. Se debe tomar en cuenta los estándares los cuales el punto de acceso soporta, en la mayoría de casos 802.11b, 802.11g ó 802.11a
- Potencia de transmisión. Un factor determinante en la elección de un punto de acceso es la potencia de transmisión del equipo, la cual garantiza una mayor zona de cobertura, no esta demás mencionar que un equipo más potente es más costoso. Los equipos actuales garantizan una potencia desde unos 18 milivatios a 200 milivatios.
- Equipo para interiores o exteriores. Se debe tener especial cuidado a la hora de seleccionar el equipo, según este sea un equipo para interior de un edificio o para exteriores y que soporte estar a la intemperie. Generalmente los equipos para exteriores son mucho más costosos que los diseñados para interiores, pero si se le provee de una caja de protección, un equipo interior podrá colocarse afueras sin inconveniente.

- Tipo de Antena. La antena para el diseño de la Red Inalámbrica puede ser de distintos tipos dependiendo el uso para el cual se aplica. Existen antenas omnidireccionales las cuales poseen un patrón de radiación uniforme en toda dirección. También se encuentra las antenas dipolos, cuyo patrón de radiación es no uniforme y de menor área de cobertura que las omnidireccionales; cabe mencionar que por lo general son las antenas que vienen con la mayoría de puntos de acceso en el mercado.
- Seguridad. Se debe tomar en cuenta los estándares de seguridad soportados por los puntos de acceso. Actualmente la mayoría de puntos de acceso soportan estándares de encriptación y autenticación como protocolos WEP, WPA, WPA-2, 802.1x, TKIP, AES, entre otros, pero son pocos los puntos de acceso que pueden soportar el emergente estándar 802.11i.
- Costo. Al diseñar la Red Inalámbrica se deberá tener presente el costo de los equipos, pues los equipos que posean mejores características tendrán un costo mayor que otros más simples.

3.1 Diseño y ubicación de los Puntos de Acceso

Para el diseño de la Red Inalámbrica se ha tomado en cuenta principalmente la estructura del edificio, el área que se desea cubrir, así como también la potencia y velocidad la cual se proporciona a la red.

Para esto se ha elegido dos puntos de acceso D-Link, de modelo DWL-2100, estos puntos de acceso soportan los estándares 802.11b y 802.11g, también cuentan con una potencia de transmisión hasta 32 milivatios y con una antena dipolo de 2dbi de ganancia. El modelo DWL-2100 soporta los estándares de seguridad 802.1x, WEP y WPA.

Comentario [ihlh19]: SE CAMBIO EL PUNTO DE ACCESO USADO.

Además se ha considerado el uso de un Conmutador o "Switch" de la marca D-Link, de modelo DES-1005D, el cual posee 5 puertos 10/100 Base-T Fastethernet, que servirán para la conexión de los puntos de acceso y el servidor de autenticación FreeRADIUS.

El diseño de la Red Inalámbrica se muestra en la figura 23.

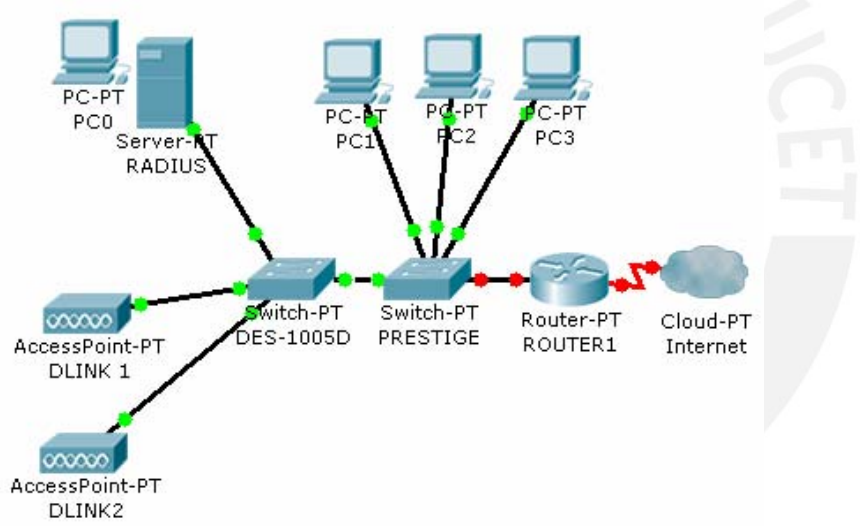

Figura 23: Diseño Red para el Complejo Hotelero

Comentario [ihlh20]: SE CAMBIO LA FIGURA. AHORA SE PUEDE VER LOS NOMBRES DE LOS EQUIPOS (DLINK, PRESTIGE O ZYXEL, DES-1005D)

La disposición de los puntos de acceso se muestra en la figura 24, los cuales se encuentran con una "X" de color azul cada uno.

Los puntos de acceso deberán configurarse en los siguientes canales:

El punto de acceso del lado izquierdo deberá configurarse en el canal 6, el router inalámbrico modelo Zyxel con el cual cuenta el Hotel deberá trabajar ahora en el canal

11 y el punto de acceso del lado derecho deberá configurarse para trabajar en el canal 1; de esta manera se reduce la posible interferencia que pueda causar el punto de acceso que se encuentra en la zona contigua del Complejo Hotelero y el cual se encuentra funcionando en el canal 6 de radiofrecuencia.

Además los puntos de acceso llevarán la siguiente configuración de direccionamiento IP estático:

Punto de acceso lado Derecho: 192.168.0.231 / 24

Punto de acceso lado Izquierdo: 192.168.0.232 / 24

Router Inalámbrico Zyxel: 192.168.0.1 / 24

El Router Inalámbrico Zyxel con el cual cuenta el Hotel y el cual provee de la conexión ADSL hacia Internet, deberá encontrarse configurado con DHCP para poder proveer de un direccionamiento dinámico a los posibles usuarios que hagan uso de la red inalámbrica.

Los puntos de acceso D-Link deberán configurarse para trabajar con encriptación WPA y cifrado TKIP, de este modo deberán autenticar a los usuarios de la red inalámbrica mediante el protocolo 802.1x gracias al uso del servidor de autenticación FreeRADIUS.

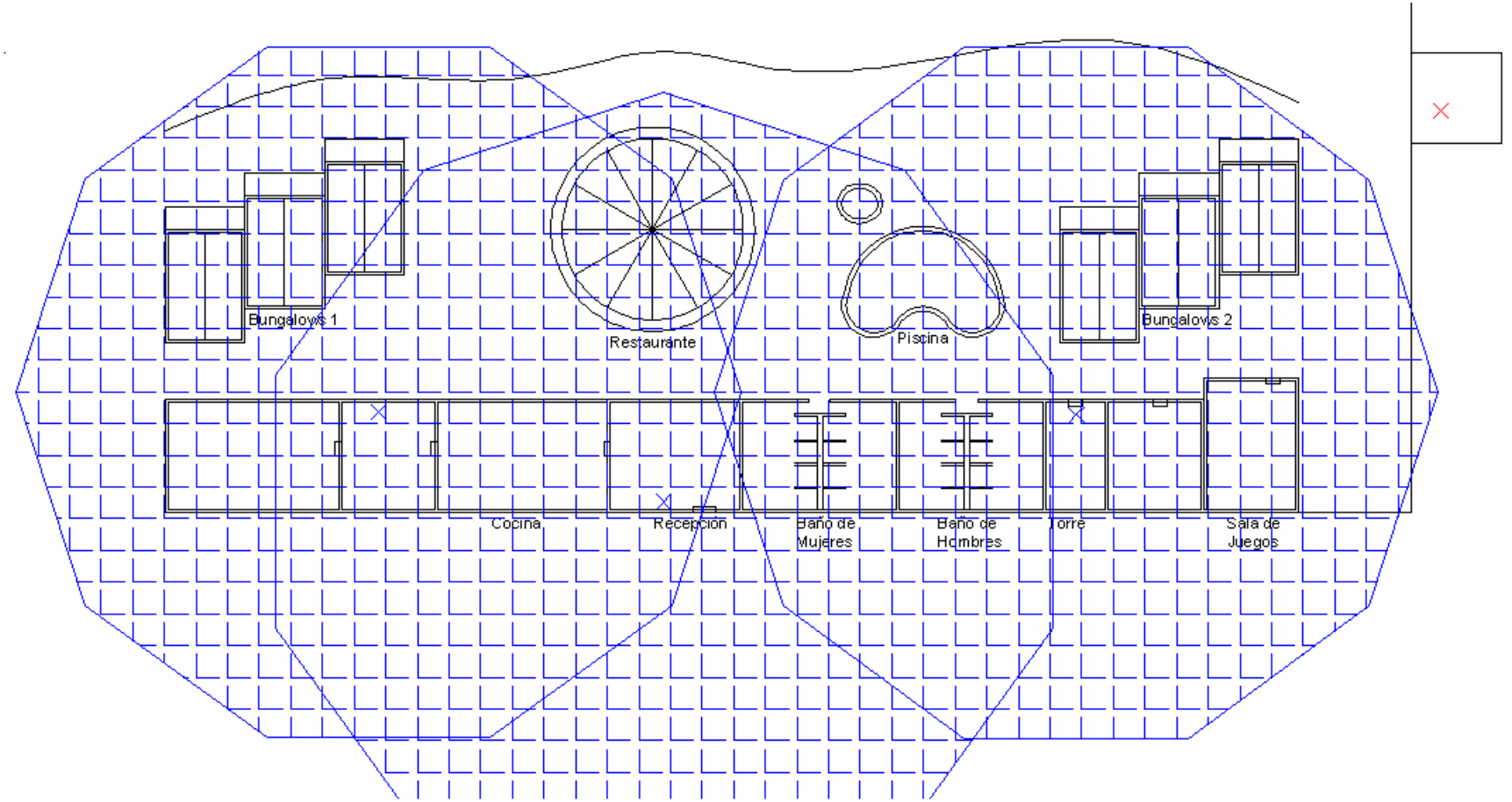

Figura 24: Disposición de los Puntos de Acceso

Comentario [ihlh21]: SE MEJORO GRÁFICA DE COBERTURA

3.2.1 Esquema de la Red

La Red actual con la cual cuenta el complejo Hotelero, está compuesta por un router inalámbrico de modelo Zyxel, el cual provee el acceso a Internet. Este dispositivo a pesar de poseer la característica de acceso inalámbrico, no logra cubrir todas las instalaciones del local. Este conmutador Zyxel posee también cuatro puertos para red cableada (fastethernet) hasta 100Mbps cada uno, tres de los puertos se encuentran ocupados por 3 computadoras y el puerto restante se usará para la conexión hacia el conmutador "switch" DES-1005D. Del conmutador DES-1005D se tendrán nuevas conexiones hacia los dos nuevos puntos de acceso D-Link DWL-2100 y hacia el servidor de autenticación FreeRADIUS.

El punto de acceso soportará los estándares 802.11b/g, utilizando el protocolo WPA para la seguridad de la red inalámbrica. El protocolo 802.1x realiza el proceso de autenticación de cada usuario que desee hacer uso de la red inalámbrica.

Se propone también hacer uso de un servidor FreeRADIUS, el cual es un software libre, que trabajará bajo el sistema operativo Linux – Ubuntu. Este servidor realiza la autenticación de usuarios que se encuentran en una base de datos de tipo MySQL, en donde también se almacenará los reportes de uso de la red inalámbrica. Para un mejor desempeño y una facilidad en uso de este servidor, se cuenta con una interfaz gráfica para poder crear cuentas de usuario y visualizar las estadísticas de uso de la red de cada uno de ellos. La interfaz gráfica corresponde también a un software libre, el cual ha sido desarrollado en el programa PHP para páginas Web y lleva por nombre "DialUp Admin".

3.2.2 Estándares y protocolos de trabajo:

3.2.2.1 Protocolo WPA - Wi-Fi Protected Access

El protocolo WPA ha sido elegido para el trabajo entre los clientes de la red inalámbrica y el Punto de Acceso, debido a que implementa un nivel de seguridad mayor que el protocolo WEP puede ofrecer; además de ser un protocolo aprobado por la institución de estandarización Alianza Wi-Fi, es un protocolo que es implementado por diversas marcas y modelos de Access Point y sistemas operativos en las computadoras clientes de la red inalámbrica.

El protocolo WPA provee una seguridad más robusta que WEP, pues corrige ciertas debilidades que presenta este último protocolo; WPA mediante el uso del protocolo

Temporary Key Integrity Protocol (TKIP), elimina la reutilización del mismo vector de inicialización de paquetes de información, además este vector se incrementa de 24 a 48 bits. TKIP hace uso de claves secretas 128 bits para la encriptación de paquetes, estas claves nunca son enviadas en texto claro en los paquetes de datos y además son claves diferentes para la comunicación entre cada cliente y el punto de acceso; estas claves de encriptación van cambiando cada diez mil paquetes de información, de esta manera se provee de una encriptación más eficiente y una mejor seguridad para la red inalámbrica.

WPA hace uso del algoritmo Message Integrity Check (MIC), llamado Michael, para la revisión de la integridad de los paquetes de información. El algoritmo MIC puede detectar posibles ataques e implementa contadores de recepción de paquetes para bloquear posibles nuevos ataques.

Sin embargo, el protocolo WPA no es infalible, el uso del método de encriptación RC4 y el protocolo TKIP, deja la posibilidad de posibles nuevas debilidades. Por esta razón, el lanzamiento del nuevo protocolo 802.11i o llamado WPA2 ha revolucionado la seguridad para las redes inalámbricas. El estándar 802.11i hace uso del concepto "Robust Security Network" (RSN), para lo cual es requerido nuevo hardware y software en los puntos de acceso. El estándar 802.11i implementa un sistema de encriptación Advanced Encryption Standard (AES) y un protocolo de seguridad Counter Mode CBC MAC Protocol (CCMP) mucho más robustos que sus antecesores RC4 y TKIP, lo que lo convierte en el método de seguridad más fuerte para redes inalámbricas de área local. Sin embargo, el estándar 802.11i no es implementado en la mayoría de puntos de acceso y en los que se encuentra implementado, su costo es mucho mayor que los puntos de acceso convencionales, además de ser incompatible con varios equipos como son las tarjetas de red inalámbricas y algunos sistemas operativos.

Por todas las razones expuestas, el protocolo WPA será implementado para la solución, pues cubre varias debilidades del protocolo WEP, y no necesita la utilización de un distinto hardware, como lo requiere el estándar 802.11i.

3.2.2.2 RADIUS - Remote Authentication Dial-In User Server

RADIUS es un protocolo de autenticación para aplicaciones de acceso a red, el cual usa el puerto 1813 UDP para establecer sus conexiones.

Cuando se realiza la conexión hacia una Red Inalámbrica, se envía previamente un nombre de usuario y una contraseña hacia un dispositivo cliente NAS (punto de acceso) sobre el protocolo PPP, quien redirige la petición hacia un servidor RADIUS

sobre el protocolo RADIUS. El servidor RADIUS comprueba si el usuario se encuentra autorizado, utilizando métodos de autenticación como EAP. Si el usuario y su contraseña son válidos, el servidor de autenticación autorizará el acceso a la Red Inalámbrica, asignándole una dirección IP, mediante el uso de direccionamiento dinámico o DHCP, el cual se encuentra configurado en el punto de acceso.

3.3 Servidor de Autenticación FreeRADIUS

FreeRADIUS es una plataforma modular, de gran potencialidad, con diversas y completas características que lo convierte en uno de los más utilizados y potentes servidores RADIUS de clase AAA. FreeRADIUS incluye servidor, clientes y desarrollo de múltiples librerías útiles para el desarrollo de un excelente servicio; puede manejar miles de cuentas de usuarios y millones de peticiones de autenticación al día.

Esta plataforma consiste en un software libre, el cual es compatible con numerosos sistemas operativos, pudiendo trabajar en conjunto con bases de datos o directorios, donde se puede almacenar la información de cada usuario miembro de la red inalámbrica.

3.3.1 Autenticación:

Consiste en el proceso de validar la petición de un usuario, el cual quiere hacer uso de los recursos de la red inalámbrica. El proceso de autenticación se realiza mediante la presentación de identidad y credenciales por parte del usuario.
La identidad del usuario viene a ser el nombre o alias con el cual esta registrado en la base de datos del servidor de autenticación, mientras que las credenciales se implementarán mediante contraseñas, aunque también podría incluirse el uso de certificados digitales.
El protocolo de autenticación usado será EAP-PEAP, este protocolo es usado entre el servidor FreeRADIUS y el Punto de Acceso para el proceso de autenticación de los usuarios.
Existen varios métodos de autenticación que son soportados por el servidor FreeRADIUS, algunos de los cuales se detallan a continuación:

- EAP-MD5
- EAP-TLS
- EAP-PEAP MSCHAPv2
- EAP-TTLS
- LEAP

- Kerberos

3.3.2 Autorización:

El proceso de autorización es el siguiente paso luego de la autenticación. Este proceso consiste en determinar si un usuario se encuentra autorizado para hacer uso de ciertas tareas, operaciones o recursos de la red. Usualmente el proceso de autorización se realiza en conjunto con el de autenticación, de esta manera una vez que el usuario es autenticado como válido, este podrá hacer uso de ciertos recursos de la red.

Asimismo, los usuarios autorizados serán registrados en la base de datos MySQL, a la cual el servidor FreeRADIUS se conecta para saber que usuarios pertenecen a la red inalámbrica

3.3.3 Contabilidad:

La contabilidad es la última característica de un servidor AAA, y consiste en el proceso de medición y almacenamiento de consumo de recursos de red. Esto permite el monitoreo y reporte de eventos y uso de la red inalámbrica para varios propósitos, entre los cuales se encuentran: tarifación de usuarios, análisis de recursos de red, capacidad de la red.

Este proceso también hace uso de la base de datos para poder registrar el comportamiento de los usuarios en la red inalámbrica

3.4 Base de Datos de Usuarios de la Red

Una base de datos es un sistema relacional que está compuesta por conjunto de datos pertenecientes a un mismo contexto, ordenados sistemáticamente para su posterior uso. Los datos son almacenados en tablas, cada tabla contiene características en común, por ejemplo tabla de nombre de usuarios, tabla de contraseñas, reporte de los usuarios, entre otros.

La plataforma FreeRADIUS puede soportar las siguientes bases de datos:

MySQL

Oracle

PostgreSQL

Para la aplicación de la red inalámbrica se utilizó MySQL como base de datos del servidor FreeRADIUS.

3.4.1 Base Datos MySQL

MySQL esta considerado un sistema de gestión de base de datos relacional, multitarea y multiusuario, que provee una solución robusta, rápida y de fácil uso. MySQL se basa en un Lenguaje de Consulta Estructurado (SQL), el cual es un lenguaje estándar de computadora para el acceso y la manipulación de base de datos.

Las tablas creadas en MySQL se detallan a continuación:

- *badusers*: Contiene la información de los usuarios que no pudieron conectarse a la red inalámbrica, por proveer una incorrecta credencial.
- *nas*: Consiste en el cliente o clientes NAS o puntos de acceso los cuales realizan la autenticación hacia el servidor FreeRADIUS,
- *radcheck*: Contiene todas las contraseñas de cada uno de los usuarios autorizados a hacer uso de la red inalámbrica.
- *radgroupcheck*: Muestra los grupos de usuarios que contienen un método de autenticación, como por ejemplo EAP-PEAP.
- *radgroupreply*: Muestra todos los grupos de usuarios creados con sus protocolos y características de cada uno de ellos. Cabe mencionar que los usuarios pertenecientes a un grupo, adoptarán las características del grupo al que forman parte.
- *radpostauth*: Contiene un reporte sobre los procesos de autenticación realizados satisfactoriamente, cada proceso es almacenado en el día y la hora exacta.
- *usergroup*: Contiene la tabla de todos los usuarios, indicando los grupos a los que pertenecen.
- *userinfo*: Contiene todas las características de los usuarios, como por ejemplo: número telefónico de casa o trabajo, teléfono móvil, departamento y correo electrónico.

3.5 Clientes FreeRADIUS

3.5.1 NAS - Network Access Server

Cuando un usuario quiere acceder a la Red Inalámbrica, lo realiza mediante los clientes del servidor FreeRADIUS, los llamados Network Access Server (NAS), los cuales realizan una petición de usuario y contraseña a cada usuario que quiera autenticarse. Los clientes NAS se comunican directamente con el servidor

FreeRADIUS a través del protocolo RADIUS, para realizar la entrega de la identificación y credenciales de cada uno de los usuarios.

En caso de que un usuario sea autenticado como autorizado, el NAS respectivo propone al usuario colocarse en el Protocolo Punto-Punto (PPP) y le asigna una dirección IP y una máscara de red para que pueda acceder a Internet a través de él.

3.5.2 Aplicación Gráfica Cliente de FreeRADIUS

Una aplicación gráfica puede trabajar como un cliente de FreeRADIUS, facilitando la creación de cuentas de usuario, así como poder realizar pruebas de autenticación de los mismos y llevar estadísticas de acceso a la red inalámbrica. El uso de una interfaz gráfica permite la administración y modificación de nuestro servidor de una manera sencilla y rápida.

La interfaz gráfica se encuentra realizada en un programa hecho en PHP4, el cual es ejecutado en un servidor Apache, especializado en páginas web.

3.5.2.1 Servidor HTTP Apache

El servidor HTTP Apache es un software libre utilizado en plataformas UNIX o Windows que soporta el protocolo HTTP y es considerado el servidor de páginas HTTP más aceptado a nivel mundial. La razón de la amplia difusión del servidor Apache es porque consiste en un software modular, de código abierto, multiplataforma, extensible, popular y gratuito.

El servidor apache puede soportar páginas web escritas en lenguaje PHP.

3.5.2.2 PHP “PHP Hypertext Pre-processor”

PHP es un acrónico recursivo que significa Personal Home Page Tools Hypertext Pre-procesor; es un lenguaje de programación utilizado para la creación de contenido dinámico de sitios Web, compatible con sistemas operativos UNIX y Windows, donde se puede programar páginas tipo html; así como la creación de aplicaciones para servidores. Este programa es de fácil uso y utiliza la programación estructurada como forma de programación, permitiendo la creación de aplicaciones complejas e interfaces gráficas para el usuario.

PHP permite la conexión a diferentes tipos de servidores de bases de datos tales como MySQL, PostgreSQL, Oracle, ODBC, DB2, entre otros; donde los primeros tres sistemas de bases de datos garantizan una compatibilidad con el servidor FreeRADIUS.

La interpretación y ejecución de las páginas web se realizan mediante la ejecución de un programa denominado “script”, el usuario sólo recibe el resultado de su ejecución en la pantalla del computador. Cuando el usuario realiza una petición al servidor para mostrar una página web, generada por un “script” PHP, el servidor Apache ejecuta el intérprete de PHP, el cual procesa el “script”, generando el contenido de manera dinámica.

3.5.2.3 Interfase de Administración “Dialup Admin”

La interfase DialUp consiste en un programa de código abierto basado en PHP4, que permite la administración del servidor FreeRADIUS vía página web. Dialup soporta las siguientes características:

- Creación de usuarios y/o grupos en base de datos mediante LDAP o SQL.
- Creación, testeo, eliminación, cambio de información personal, revisión de contabilidad para cada usuario.
- Generador de reporte de Contabilidad.
- Facilidad para ubicar usuarios con problemas para registrarse.
- Testeo del servidor RADIUS.
- Estadísticas de uso de la red inalámbrica en línea.

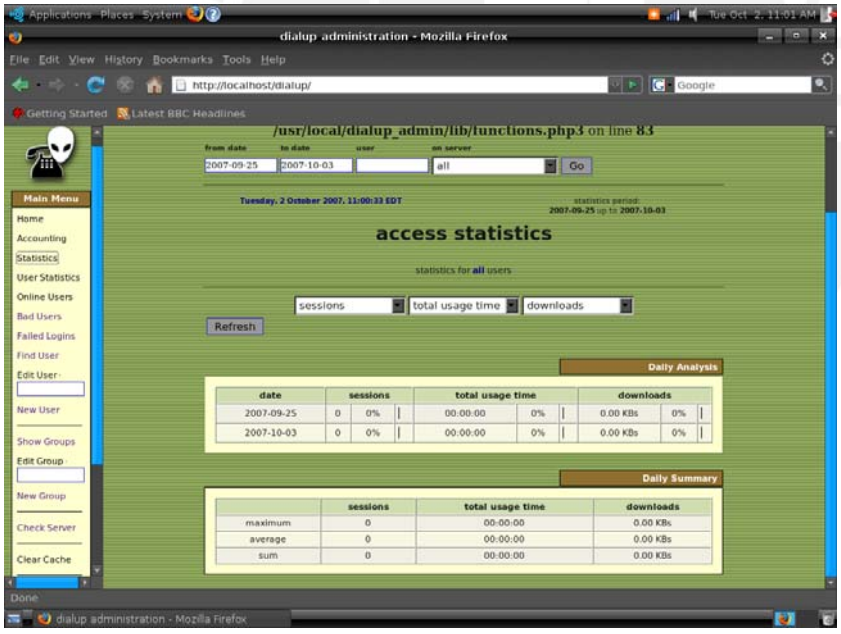

Figura 25: Interfaz Gráfica Dialup Admin

La herramienta de trabajo Dialup Admin facilita de gran manera la creación, eliminación y monitoreo de la red inalámbrica. Debido a que el servidor de autenticación FreeRADIUS se encontrará trabajando en un sistema operativo Linux, el cual no es tan sencillo de manejar a nivel de configuración de archivos.

3.6 Diagrama de Solución para una red inalámbrica segura

Una vez definido todos los protocolos y sistemas a usar, podemos presentar el modelo de trabajo a implementar. Este sistema se presenta como un método seguro para una red inalámbrica, mediante el cual sólo las personas autorizadas podrán acceder a la Red y hacer uso de sus recursos.

El proceso de autenticación de usuarios se realiza mediante un servidor FreeRADIUS, el cual realiza las peticiones a los suplicantes, a través de los clientes NAS. El método de autenticación usado será el EAP-PEAP/802.1x, el cual hace uso de la identidad del usuario y una contraseña para poder acceder a la red.

El servidor FreeRADIUS hará uso de una base de datos creada en MySQL para almacenar la información de todos los usuarios autorizados a acceder a la Red inalámbrica.

A su vez, se contará con una interfaz gráfica denominada “DialUp Admin”, la cual es de sencillo uso, donde se podrá crear las cuentas de usuario y contraseñas directamente en la base de datos, así como poder realizar pruebas de testeo sobre el servidor de autenticación.

Este modelo sistema de seguridad se encuentra esquematizado en la figura 26:

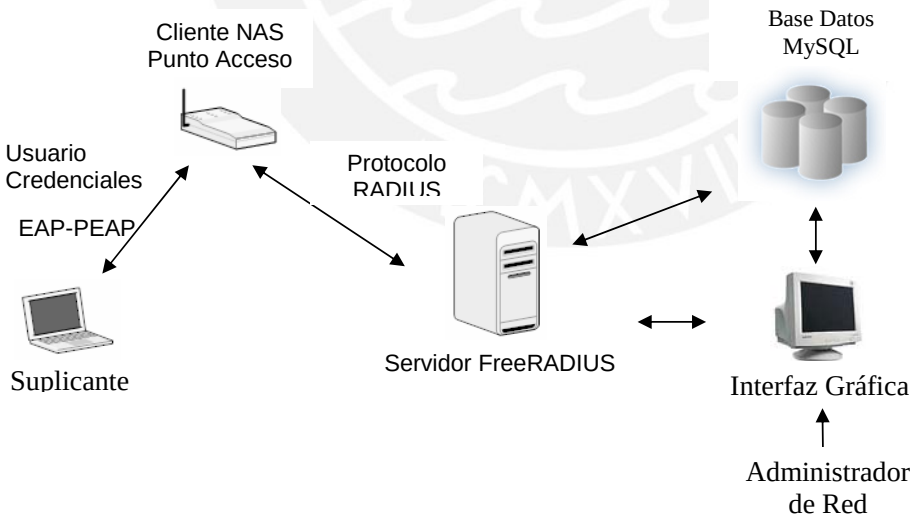

Figura 26: Diagrama del Sistema de Seguridad

Comentario [ihlh22]: SE MEJORO FIGURA DEL DIAGRAMA DE SEGURIDAD PROPUESTO

4.1 Esquema de la Red Elaborada para el Sistema de Seguridad

Las pruebas de autenticación se realizaran sobre una Red Inalámbrica modelo parecida a la red propuesta en la solución.

Para realizar las pruebas del Sistema de Seguridad basado en los protocolos WPA y 802.1x, se ha implementado la red de la figura 27. Las pruebas han sido realizadas con el Punto de Acceso de la marca D-LINK, modelo DWL-7100AP, un servidor de autenticación “FreeRADIUS” en un entorno Linux Ubuntu y una computadora portátil a autenticar con el sistema operativo “Windows XP Service Pack 2”.

La prueba consistirá en la creación de un usuario y su respectiva autenticación en la Red Inalámbrica, por medio de la presentación de su credencial o contraseña, caso contrario no podrá acceder a los recursos de la red.

A continuación se detalla la configuración de cada uno de los equipos ya mencionados.

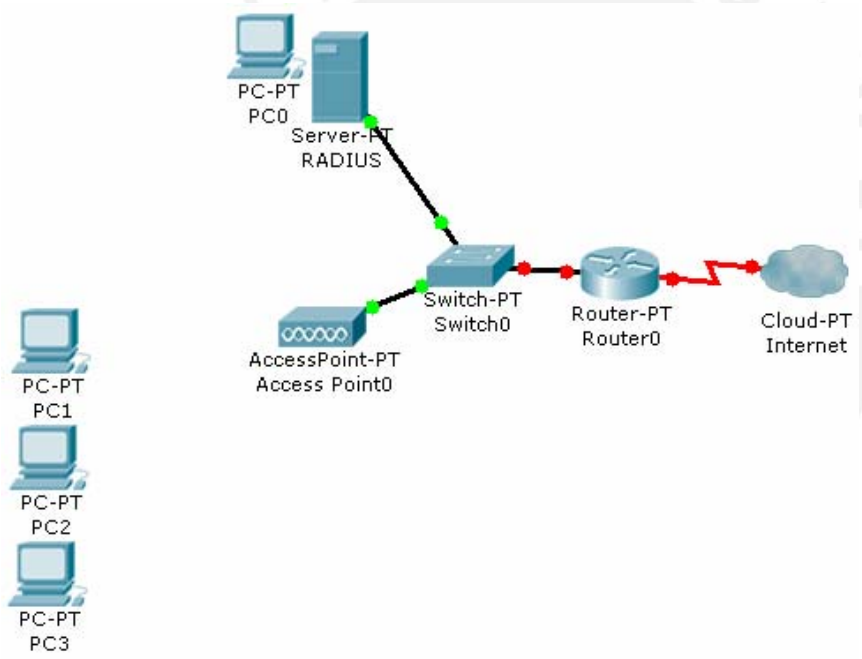

Figura 27: Red Implementada para pruebas

4.2 Configuración del Punto de Acceso

Para la realización de las prueba del Sistema de Seguridad se ha usado un Punto de Acceso de la marca D-LINK, cuyo modelo es DWL-7100AP. Este Punto de Acceso

soporta los protocolos 802.11a, 802.11b y 802.11g en Redes Inalámbricas de área local y puede ser configurado en calidad de Punto de Acceso, enlace Punto a Punto, enlace Punto Multipunto y Repetidor. Para nuestro caso, lo usaremos como Punto de Acceso.

Este modelo de Punto de Acceso incorpora también varios protocolos en Seguridad, entre los cuales se tiene: Protocolo WEP de 64 bits, 128 bits o 152 bits; Protocolo WPA con cifrado TKIP o AES; Protocolo 802.1x con autenticación EAP-MD5, PEAP, TLS, TTLS.

Cabe mencionar que este equipo posee una potencia máxima de 63 mW y cuenta con una antena dipolo de 2dbi de ganancia.

Al realizar las pruebas, el Punto de Acceso DWL-7100AP ha sido configurado con los siguientes parámetros (Ver figura 28 y 29):

SSID = dlinkprueba

IP= 192.168.0.50

Máscara de red = 255.255.255.0

Canal de propagación = 6

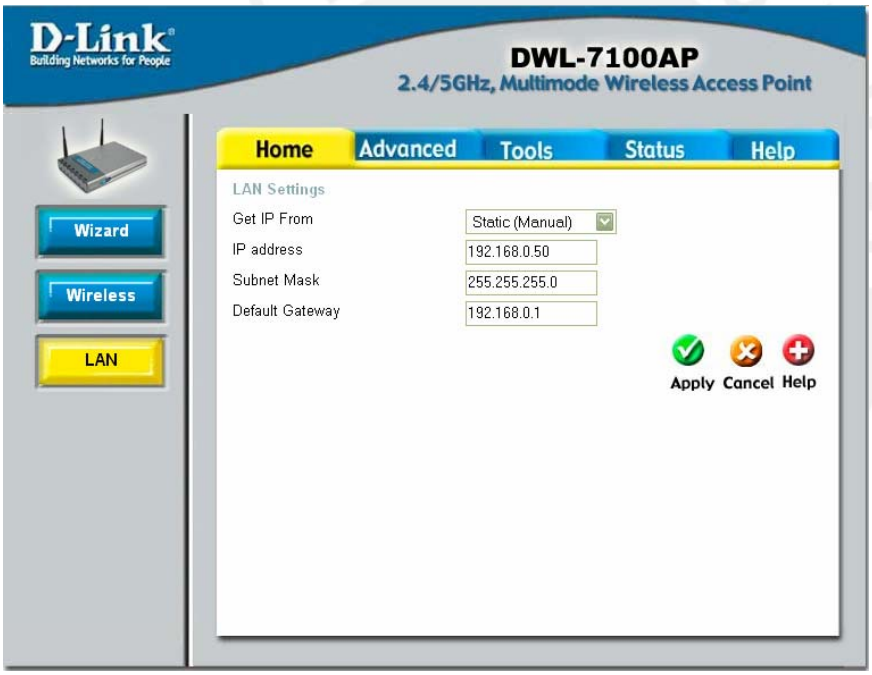

Figura 28: Parámetros de Direccionamiento en el Punto de Acceso DWL-7100

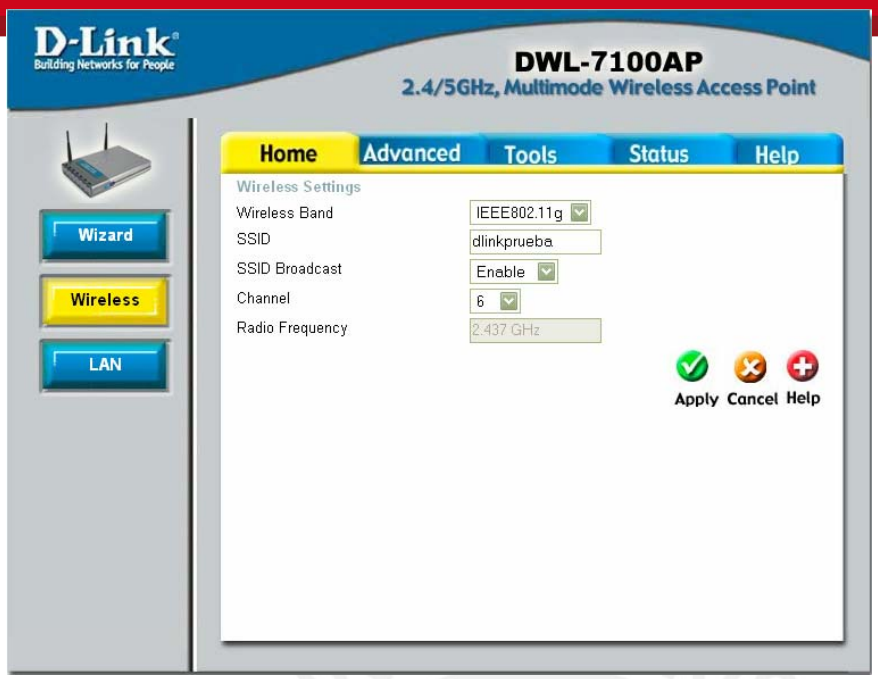

Figura 29: Parámetros de Red en el Punto de Acceso DWL-7100

Asimismo se ha configurado los parámetros de seguridad en el equipo de la siguiente manera (Ver figura 30):

Protocolo de autenticación = WPA
Tipo de Cifrado = TKIP
Dirección IP del Servidor Radius = 192.168.0.179
Puerto del Servidor Radius = 1812
Palabra Secreta del Servidor Radius = laboratorio2007

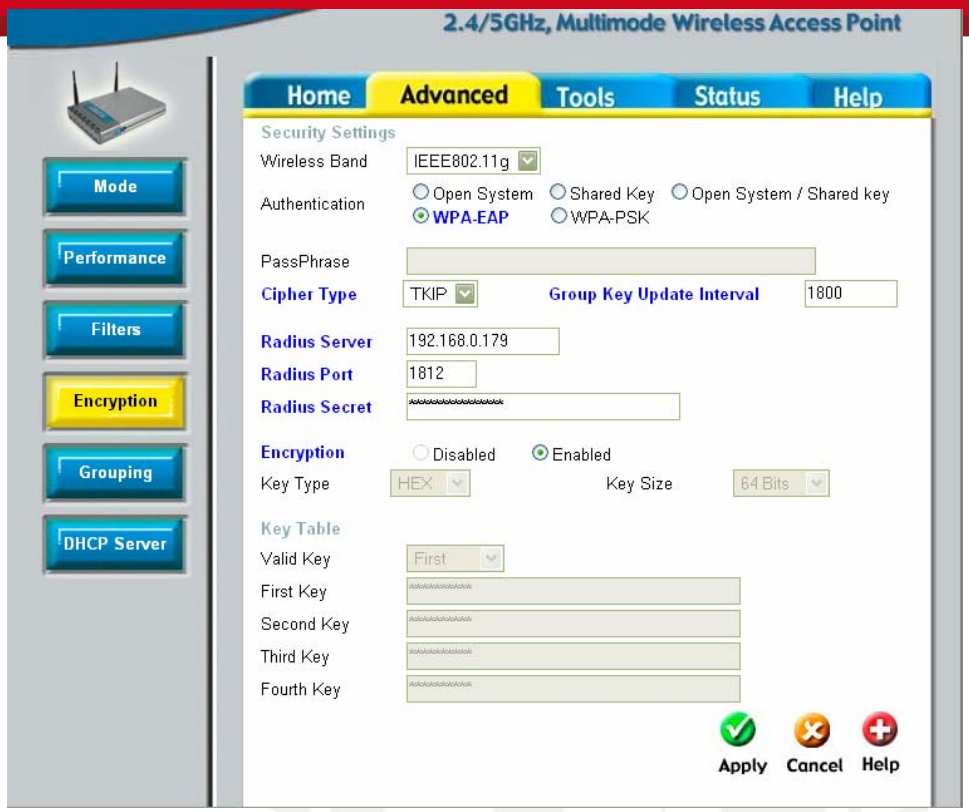

Figura 30: Parámetros de Seguridad en el Punto de Acceso DWL-7100

Cabe mencionar que la palabra secreta que configuramos en el Punto de Acceso debe ser la misma la cual configuramos en el servidor RADIUS, pues ambos se comunicarán con la misma.

4.3 Configuración del Servidor FreeRADIUS y de cuentas de usuario

El servidor FreeRADIUS versión 1.1.3 se instaló en la distribución de Linux “Ubuntu Studio 7.04” para poder realizar la autenticación de un usuario a la Red Inalámbrica.

El servidor FreeRADIUS se ha configurado para trabajar con un Punto de Acceso cliente, el cual es el DWL 7100AP. Este Punto de acceso realizará las peticiones de autenticación a todos aquellos usuarios que requieran ingresar a la red de manera inalámbrica y luego comunicará las peticiones hacia el servidor FreeRADIUS mediante el protocolo de autenticación EAP-PEAP MSCHAP v2. El servidor FreeRADIUS también ha sido configurado para poder trabajar con una base de datos de tipo MySQL, donde se almacenará los usuarios de la red inalámbrica agrupados en 2 grupos: Huéspedes y Administración. La versión instalada de la base de datos MySQL ha sido “MySQL 5.0.38”. La creación de los 2 grupos de usuarios se hizo a través de la

Interfaz Gráfica “Dialup Admin” versión 1.62; para poder trabajar con la Interfaz Gráfica se ha debido primero instalar el servidor Apache y el programa PHP para creación de páginas Web, en nuestro caso, las versiones instaladas corresponden a “Apache 2.2.3” y “PHP 5.2.1”, todos estos programas se encuentran funcionando en el mismo computador en el cual se instaló el servidor de autenticación FreeRADIUS.

La creación de grupos de usuario y usuarios de cada uno de ellos, se efectúa de manera muy sencilla a través de la página Web. Primero se debe acceder a la Interfaz, mediante la dirección “http://localhost/dialup”, luego con la opción “Show Groups” podremos visualizar los grupos de usuarios Creados (Ver Figura 31)

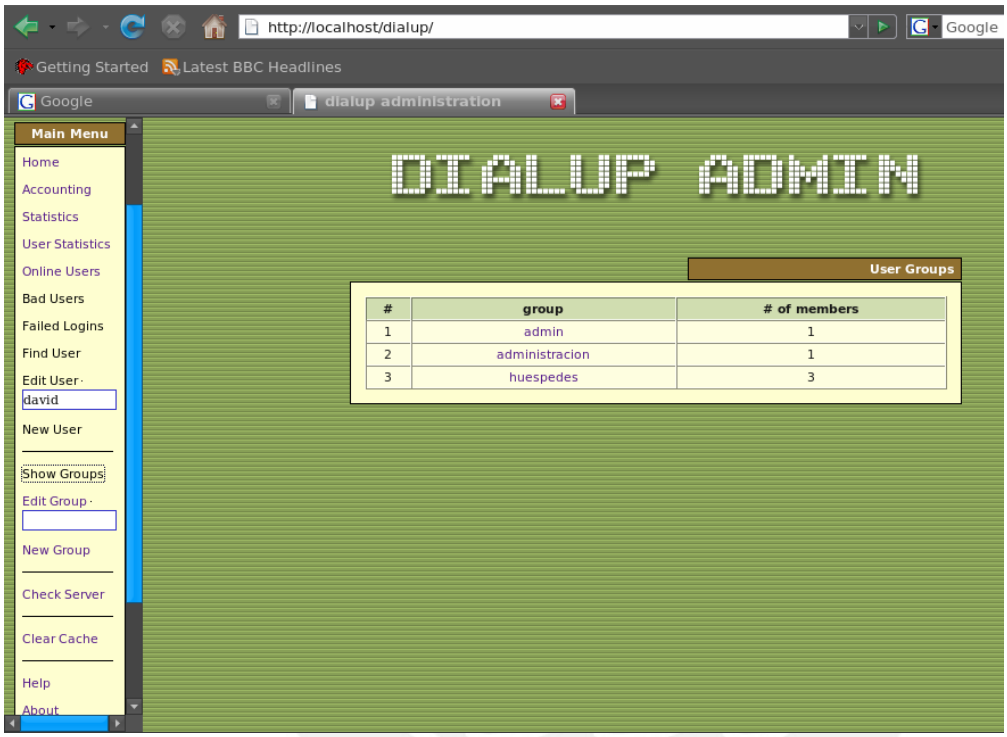

Figura 31: Grupos de Usuario Creados

De este modo, mediante la opción “New User”, podremos crear un nuevo usuario, perteneciente a alguno de los grupos de usuario ya creados (Ver figura 32); donde solo detallaremos el nombre de usuario y su respectiva contraseña; cabe indicar que todas las características podrán ser modificadas dentro de la opción “Edit User”.

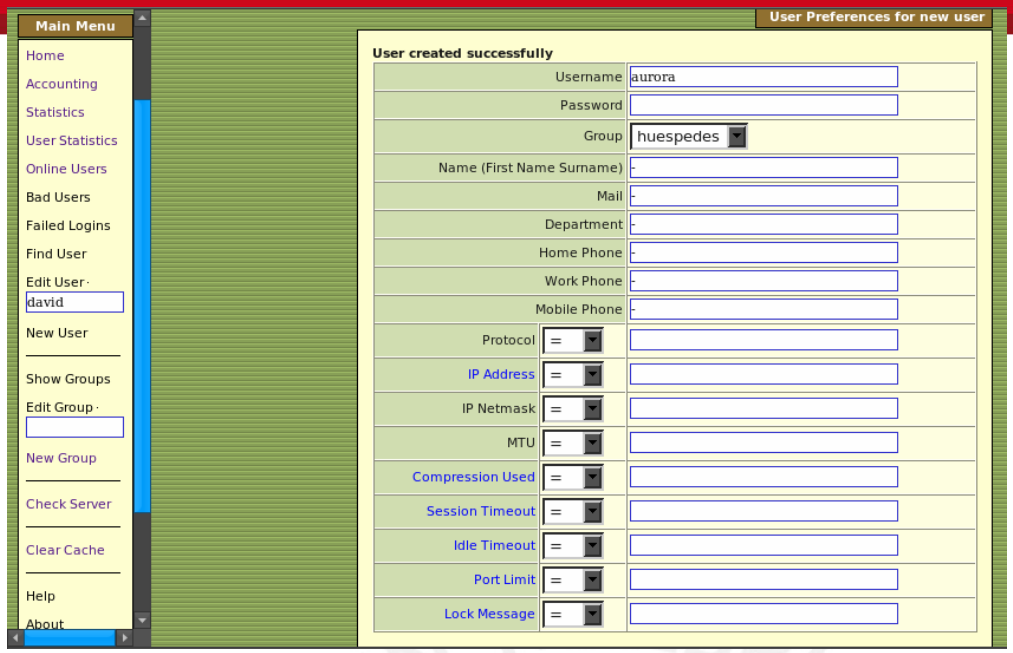

Figura 32: Creación de un Usuario

De esta manera se han configurado los siguientes usuarios:

Usuario = david Password = liza Grupo = Huéspedes
Usuario = aurora Password = hernandez Grupo = Huéspedes
Usuario = flavio Password = ramirez Grupo = Huéspedes
Usuario = susana Password = chang Grupo = Administración

También se puede mediante la Interfaz Gráfica, realizar el borrado de cuentas ya no usadas, cambio de contraseñas o realizar una pequeña prueba de autenticación hacia el servidor de manera local, en el mismo computador.

4.4 Configuración del Suplicante Inalámbrico

Para poder realizar las pruebas, se hizo uso de una computadora portátil, la cual se autenticará hacia el Servidor FreeRADIUS, para poder hacer uso de la Red Inalámbrica “dlinkprueba”. Esta computadora portátil trabaja bajo el sistema operativo “Windows XP Service Pack 2” y para poder hacer uso de los recursos de la Red Inalámbrica, se configura algunas opciones de la tarjeta inalámbrica, cuyo modelo es “Intel PRO/Gíreles 3945ABG”, la cual puede soportar los estándares 802.11a, 802.11b y 802.11g.

Se ingresa a “propiedades” de la tarjeta inalámbrica y se procede a configurar la Red Inalámbrica, accediendo a la pestaña “Redes Inalámbicas”. (Ver figura 33)

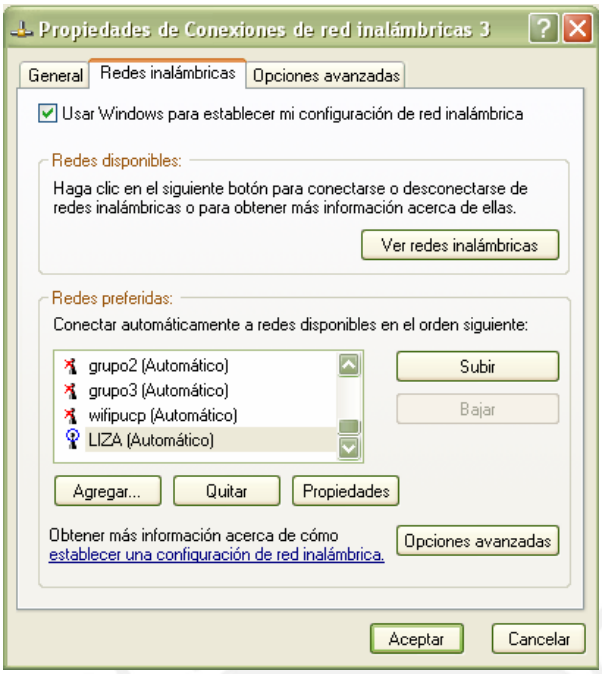

Figura 33: Propiedades de la red Inalámbrica

Se agrega luego una red, dentro de la casilla de “Redes preferidas”, colocando los siguientes parámetros para esta nueva red:

SSID = dlinkprueba
Autenticación de Red = WPA
Cifrado de datos = TKIP
Tipo de EAP = EAP protegido (PEAP)
Dentro de las propiedades de EAP-PEAP, se debe desactivar todas las opciones que aparecen por defecto, puesto que para esta prueba, no hemos hecho uso de ningún tipo de firmas digitales.
La configuración deberá quedar como aparece en las figuras 34, 35 y 36.

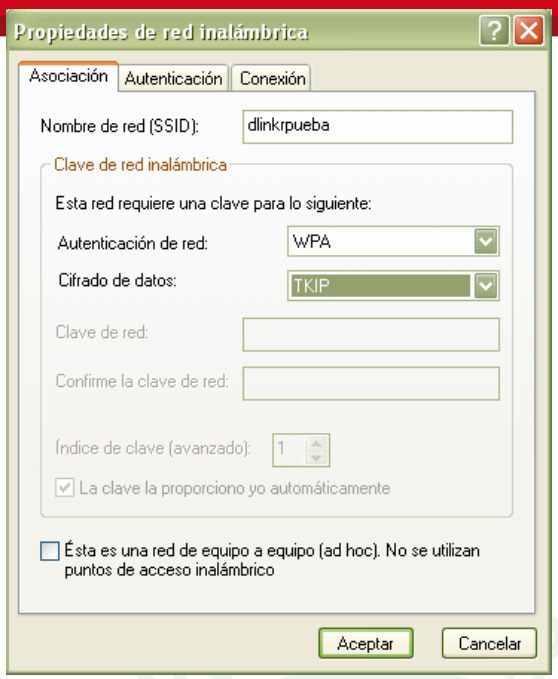

Figura 34: Propiedades de protocolo de encriptación y autenticación

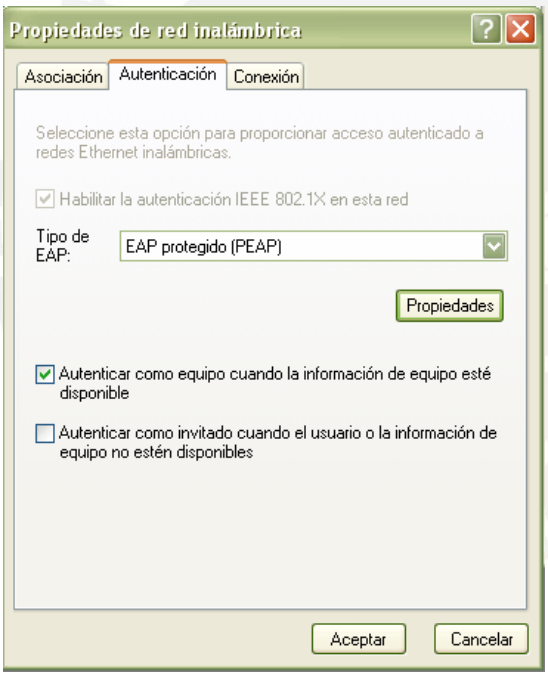

Figura 35: Propiedades de Autenticación

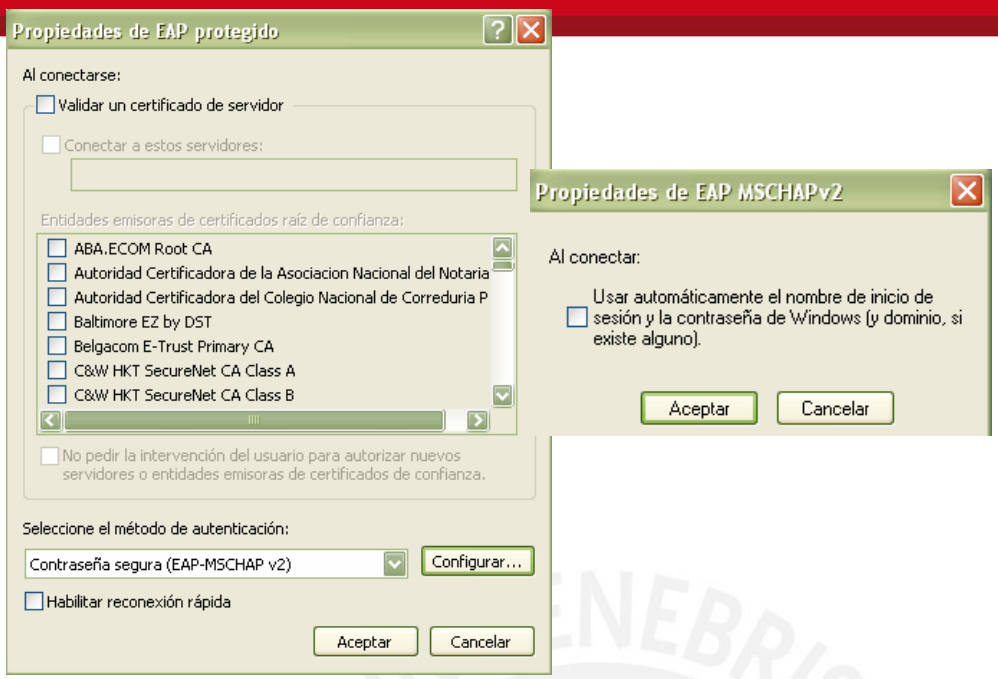

Figura 36: Propiedades del Protocolo EAP

Por último, se debe tener en cuenta que la asignación de dirección IP se realizará de manera automática, por lo que en propiedades del protocolo TCP/IP de la tarjeta inalámbrica se deberá configurar en modo DHCP.

4.5 Autenticación de usuarios al Sistema.

Se realizó una prueba de autenticación desde una computadora portátil, con las características ya mencionadas, hacia la Red Inalámbrica instalada. El usuario autenticado lleva por nombre de cuenta “david” y su respectiva contraseña es “liza”, pertenece al grupo de usuarios de “Huéspedes”. Para poder ingresar a la Red Inalámbrica “dlinkprueba”, el usuario tendrá que visualizar la red en las “Redes Inalámbricas disponibles” en el sistema operativo y luego proceder a ingresar su nombre de usuario y su credencial para acceder a la red (Ver figura 37).

Figura 37: Proceso de Autenticación de un Usuario

En el lado del Servidor FreeRadius, se necesita abrir un Terminal de Comandos e ingresar el comando "# freeradius –X –A", para poder levantar el servidor en modo "debug" y poder visualizar los resultados de las autenticaciones. Cabe mencionar que el comando "freeradius" debe ser ejecutado en modo administrador, además si toda la instalación y configuración del Servidor se encuentra correctamente hecha, se tendrá un resultado parecido al siguiente:

(...)
Module: Instantiated detail (detail)
Module: Loaded radutmp
radutmp: filename = "/var/log/freeradius/radutmp"
radutmp: username = "%{User-Name}"
radutmp: case_sensitive = yes
radutmp: check_with_nas = yes
radutmp: perm = 384
radutmp: callerid = yes
Module: Instantiated radutmp (radutmp)
Listening on authentication *:1812
Listening on accounting *:1813
Ready to process requests.

A continuación se muestra el resultado de la autenticación, frente a distintas situaciones:

- El usuario “david” ingresó correctamente su nombre y su contraseña.

Resultado del servidor:

(…)

radius_xlat: 'INSERT into radpostauth (id, user, pass, reply, date) values (", 'david', 'Chap-Password', 'Access-Accept', NOW())'

rlm_sql (sql) in sql_postauth: query is INSERT into radpostauth (id, user, pass, reply, date) values (", 'david', 'Chap-Password', 'Access-Accept', NOW())

rlm_sql (sql): Reserving sql socket id: 1

rlm_sql (sql): Released sql socket id: 1

modcall[post-auth]: module "sql" returns ok for request 8

modcall: leaving group post-auth (returns ok) for request 8

Sending Access-Accept of id 8 to 192.168.0.50 port 1142

MS-MPPE-Recv-Key = 0x5c8b5817755dfa71b8d42bfb0281a99873537e5f0a3e92bc7285e81d8359b3c9

MS-MPPE-Send-Key = 0x43c7e00ff6c88c2c5fe21e570f1715928c2b9961d8834e04918888505dbf43d8

EAP-Message = 0x03080004

Message-Authenticator = 0x00000000000000000000000000000000

User-Name = "david"

Finished request 8

Como se puede observar en el resultado obtenido, el usuario “david” fue autenticado de manera satisfactoria, al proveer un nombre de usuario y contraseña válidos.

- El usuario “david” ingresó correctamente su nombre, pero no así su contraseña.

Resultado del Servidor:

(…)

Username = 'david' ORDER BY id'

radius_xlat: 'SELECT radgroupreply.id,radgroupreply.GroupName,radgroupreply.Attribute,radgroupreply.Value,radgroupreply.op FROM radgroupreply,usergroup WHERE usergroup.Username = 'david' AND usergroup.GroupName = radgroupreply.GroupName ORDER BY radgroupreply.id'

rlm_sql (sql): Released sql socket id: 1

modcall[authorize]: module "sql" returns ok for request 32
modcall: leaving group authorize (returns updated) for request 32
rad_check_password: Found Auth-Type EAP
auth: type "EAP"
Processing the authenticate section of radiusd.conf
modcall: entering group authenticate for request 32
rlm_eap: Request found, released from the list
rlm_eap: EAP/peap
rlm_eap: processing type peap
rlm_eap_peap: Authenticate
rlm_eap_tls: processing TLS
eaptls_verify returned 7
rlm_eap_tls: Done initial handshake
eaptls_process returned 7
rlm_eap_peap: EAPTLS_OK
rlm_eap_peap: Session established. Decoding tunneled attributes.
rlm_eap_peap: Received EAP-TLV response.
rlm_eap_peap: Tunneled data is valid.
rlm_eap_peap: Had sent TLV failure. User was rejcted rejected earlier in this session.
rlm_eap: Handler failed in EAP/peap
rlm_eap: Failed in EAP select
modcall[authenticate]: module "eap" returns invalid for request 32
modcall: leaving group authenticate (returns invalid) for request 32
auth: **Failed to validate the user.**
Delaying request 32 for 1 seconds
Finished request 32

Como se puede observar en esta prueba, el usuario no pudo ingresar a la Red Inalámbrica, por proveer una incorrecta contraseña.

- La cuenta del usuario “david” fue borrada, y se procede a autenticar con usuario y contraseña válidos anteriores.

Resultado del Servidor:

usergroup.GroupName = radgroupreply.GroupName ORDER BY radgroupreply.id'

rlm_sql (sql): User david not found in radgroupcheck
rlm_sql (sql): Released sql socket id: 1
rlm_sql (sql): User not found
  modcall[authorize]: module "sql" returns notfound for request 24
modcall: leaving group authorize (returns updated) for request 24
  rad_check_password: Found Auth-Type EAP
auth: type "EAP"
  Processing the authenticate section of radiusd.conf
modcall: entering group authenticate for request 24
  rlm_eap: Request found, released from the list
  rlm_eap: EAP/peap
  rlm_eap: processing type peap
  rlm_eap_peap: Authenticate
  rlm_eap_tls: processing TLS
  eaptls_verify returned 7
  rlm_eap_tls: Done initial handshake
  eaptls_process returned 7
  rlm_eap_peap: EAPTLS_OK
  rlm_eap_peap: Session established. Decoding tunneled attributes.
  rlm_eap_peap: Received EAP-TLV response.
  rlm_eap_peap: Tunneled data is valid.
  rlm_eap_peap: Had sent TLV failure. User was rejcted rejected earlier in this session.
 rlm_eap: Handler failed in EAP/peap
  rlm_eap: Failed in EAP select
  modcall[authenticate]: module "eap" returns invalid for request 24
modcall: leaving group authenticate (returns invalid) for request 24
auth: Failed to validate the user.
Delaying request 24 for 1 seconds
Finished request 24
Going to the next request
Waking up in 6 seconds...
rad_recv: Access-Request packet from host 192.168.0.50:1146, id=7, length=243
Sending Access-Reject of id 7 to 192.168.0.50 port 1146
        EAP-Message = 0x04070004
        Message-Authenticator = 0x00000000000000000000000000000000

En el ejemplo anterior, se demuestra que ningún usuario que no se encuentre registrado en la base de datos de la Red Inalámbrica podrá acceder a usar los recursos de la red.

4.6 Presupuesto de la Solución Planteada

La Red Inalámbrica propuesta tiene como base el uso de un Punto de Acceso con una potencia mucho mayor que el que se encuentra funcionando hasta el momento. El Modelo de Punto de Acceso propuesto es el DWL-3200AP de la marca D-LINK, el cual se encontrará cableado hacia el comutador-enrutador Zyxel, mediante un cable UTP categoría 5e a la distancia de 50 metros aproximadamente. Asimismo, se detalla las características de la computadora donde se encontrará funcionando el servidor de autenticación FreeRADIUS.

Cantidad	Descripción	Precio Unitario (soles)	Precio Total (soles)
2	Punto Acceso D-LINK DWL-2100AP	210	420
1	Switch D-LinK DES-1005D	60	60
100	Cable UTP x 1 metro	1.5	150
10	Conectores RJ45	0.5	5
1	Computadora - Procesador Celeron de 2.5 Ghz - 256 MB de memoria RAM - 40 Gb de disco Duro - 32 MB de Video	900	900
		Total	1535

Tabla 4: Presupuesto de la solución planteada

- Las soluciones basadas en redes inalámbricas están disponibles hoy en día y es sólo el principio de una tendencia creciente. El estándar 802.11g prometen un gran ancho de banda para permitir un buen número de nuevas aplicaciones; aunque aún existen varios obstáculos que se tiene que vencer como la seguridad e interferencia, las Redes inalámbricas ofrecen pro lo pronto una comunicación eficiente tanto en interiores como exteriores.
- El diseño de una Red Inalámbrica de área local es una solución versátil que permite el intercambio de información y acceso a Internet, pudiendo ser instalada en distintos lugares, donde el cableado no pueda ser accesible.
- Un factor importante al realizar el diseño de una Red Inalámbrica de área local es la pérdida de potencia de la señal de radiofrecuencia al encontrar obstáculos como vidrio, ladrillo, madera, etc.
- La ubicación de uno o más Puntos de Acceso y los obstáculos que tendrá que pasar determinan la zona de cobertura de la red inalámbrica.
- El ancho de banda que posea un usuario haciendo uso de la red inalámbrica esta directamente relacionada con la cantidad de potencia que reciba del Punto de Acceso. Se podrá mejorar la potencia instalando más Puntos de Acceso, por lo cual se tendrá que hacer un balance entre velocidad y cobertura y costo.
- La seguridad es un factor importante al diseñar una Red Inalámbrica. Una Red Inalámbrica sin seguridad permitirá el acceso de personas sin autorización, exposición de nuestra información y la mal configuración de los equipos.
- Los precios de los productos para implementar Redes Inalámbricas han estado reduciendo enormemente, y continuarán bajando conforme se alcance el consumo masivo de software y hardware basados en tecnologías inalámbricas.
- Cuando se evalúa una solución inalámbrica que pueda satisfacer las necesidades de comunicación es muy importante tener en cuenta los estándares y tecnologías de más penetración. Esta decisión ahorrará dinero, tiempo y problemas de incompatibilidad y brindará una comunicación rápida, eficiente, segura y transparente.

- Al diseñar una red inalámbrica, se debe tener especial cuidado con la elección de canales de radio para la formación de celdas de cobertura, pues de ello depende la posible interferencia en la red inalámbrica.
- Para redes de mayor complejidad y que necesiten métodos de seguridad más robustos, se puede plantear la elección de puntos de acceso qu cumplan con el estándar 802,11i y el trabajo con los protocolos WPA-2 con cifrado AES
- El diseño de la red inalámbrica debe estar pensado para la posibilidad de un mejoramiento o la implementación de nuevas tecnologías, como por ejemplo la tecnología de Voz sobre IP inalámbrico.
- En aplicaciones donde se necesite una seguridad mas fuerte, el servidor de autenticación RADIUS, puede estar configurado para trabajar con certificados digitales.
- Para redes inalámbricas de mayor capacidad, por ejemplo de más de 100 usuarios, se recomienda el uso de un directorio de tipo LDAP para la organización de los distintos sectores de la entidad o empresa.
- Una posible mejora para este sistema de autenticación podría darse en la implementación de una interfaz gráfica para el sistema operativo Windows, el cual pueda acceder a la base de datos MySQL del servidor de Linux, para realizar la creación y eliminación de cuentas. De esta manera, no es necesario manejar el sistema operativo Linux para poder realizar un monitoreo sobre la red inalámbrica.

[1] American Agent & Broker
Mar 2007, “Weighing the pros and cons of wireless networks”

[2] John Kindervag
Sept/Oct 2006 “The Five Myths of Wireless Security”

[3] Principios de criptografía
www.gris.det.uvigo.es/wiki/pub/Main/PaginaRsc2/Clase6-SPT.pdf

[4] Computer Economics Report
Apr 2006, “Organizations at Risk from Lax Wi-fi Security”

[5] Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky
2004 “Wi-FOO The Secret of Wireless Hacking”

[6] SAFE: Wireless LAN Security in Depth - version 2
http://www.cisco.com/en/US/

[7] Wireless LAN Security White Paper
http://www.cisco.com/en/US/

[8] Cisco Wireless LAN Security Overview
http://www.cisco.com/en/US/

[9] Cisco_LEAP
http://www.cisco.com/en/US/

[10] In Stat/MDR, cuadro estadístico
www.isp-planet.com/research/2002/wlan_020807.html

[11] FreeRADIUS
http://www.freeradius.org

[12] Gast, Mathew S.
Redes wireless 802.11

[13] RFC2865, RFC 2866

www.ietf.org/rfc/rfc2866.txt

www.ietf.org/rfc/rfc2865.txt

[14] Earle, Aron E.

2006 Wireless Security Handbook