PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE ACCESOS A UNA RED WI-FI UTILIZANDO SOFTWARE LIBRE

TESIS PARA OPTAR EL TÍTULO DE

INGENIERO DE LAS TELECOMUNICACIONES

PRESENTADO POR

Jorge Alonso López Mori

LIMA – PERÚ

2008

RESUMEN

El reciente aumento en la implementación de redes inalámbricas nos obliga a contemplar con más cuidado el aspecto de la seguridad en este tipo de redes. Así como en el caso de las típicas redes de datos con cables (siendo la tecnología Ethernet la más utilizada para estos casos), tiene que asegurarse que los usuarios de una red inalámbrica se encuentren conectados a ésta de una manera segura, teniendo en cuenta que ahora el medio de transmisión ya no se restringe a un cable, sino que se encuentra en todo el ambiente que lo rodea. Debe de comprobarse que el usuario sea quien dice ser (autenticación), que solo tenga acceso a los recursos que le corresponda (autorización) y también llevar a cabo un registro de las actividades que haga dentro de la red (contabilidad); realizando todo esto de una manera segura y sin que sujetos ajenos a la red puedan estar leyendo información confidencial ni mucho menos tratar de modificarla.

En esta tesis se tiene pensado explicar el diseño e implementación que se debería de llevar a cabo dentro de un escenario dado para la instalación de una red inalámbrica segura que contemple la administración de sus usuarios por medio de una plataforma de gestión Web basada en PHP, integrada a un servidor de directorios LDAP con compatibilidad hacia implementaciones libres y cerradas de dicho protocolo, un servidor de autenticación RADIUS y un servidor de base de datos MySQL. Se estudiarán los principales aspectos aplicados en redes inalámbricas Wi-Fi, poniendo especial énfasis en la seguridad de la red y de sus usuarios con mecanismos tales como: WPA2 (IEEE 802.11i), 802.1X, EAP, RADIUS, entre otros.

DEDICATORIA

A mis padres, Rosa Victoria y Jorge Alejandro,

y a mi hermana Rosa María

AGRADECIMIENTOS

A mis padres, quienes siempre me apoyaron y además brindaron todas las oportunidades para poder desarrollarme, tanto como persona como futuro profesional.

A mi asesor de tesis, Ing. Genghis Ríos Kruger, por haberme ayudado con la formación del tema de esta tesis; así como su constante apoyo en su elaboración y corrección.

A mis profesores del colegio y la universidad, quienes me brindaron de todos sus conocimientos y guiaron en mi formación, tanto académica como humanística.

A todos mis amigos de la vida, con quienes he compartido tantas alegrías y penas; y siempre estuvieron allí para brindarme sus consejos y apoyo.

Y finalmente a Ana Valeria, porque sin su apoyo y constante ánimo no hubiera sido capaz de llegar hasta donde me encuentre ahora y en el futuro.

A todos ustedes, ¡muchas gracias!

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Glosario

AES	Advanced Encryption Standard
BSSI	Basic Service Set Identifier
CTS	Clear to Send
DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ESS	Extended Service Set
FHSS	Frequency Hoping Spread Spectrum
GNU	GNU Not Unix
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ITU-T	International Telecommunication Unit – Telecommunication Standardization Sector
IV	Initialization Vector
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Medium Access Control
PHP	PHP (Personal Home Page Tools) Hypertext Pre-processor
PSK	Pre-shared Key
OSI	Open Systems Interconnection
RADIUS	Remote Authentication Dial-In User Server
RTS	Request to Send
SSID	Service Set Identity

TCP	Transport Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Introducción

Con el pasar de los últimos años se ha venido implementando cada vez en más lugares la tecnología de acceso inalámbrico a redes de área local; en las empresas principalmente para brindarles a los usuarios movilidad y mediante ello puedan aumentar su productividad y eficiencia en el trabajo del día a día, y en lugares públicos (tales como aeropuertos, cafés, parques, entre otros) para brindarles, como un servicio de valor agregado, el acceso a la Internet por esta vía.

Sin embargo, principalmente en el caso de las empresas que implementen redes inalámbricas en sus ambientes, suele descuidarse el aspecto de la seguridad, abriendo así una grieta por la cual sujetos ajenos a la empresa puedan acceder a la red, leer, escribir y hasta destruir uno de los activos más importantes que puede tener: la información (desde los proyectos que la empresa pretende llevar a cabo en un futuro cercano hasta las base de

datos en la que puede mantener información confidencial sobre sus empleados y clientes más importantes).

Esta tesis pretende estudiar, analizar y presentar un modelo de implementación a llevar a cabo en un escenario típico de una empresa u organización, bajo el cual se garantice como primer objetivo un acceso seguro a la red inalámbrica utilizando mecanismos de seguridad y siguiendo los consejos que dentro de la industria denominan como "*best practices*" o "mejores prácticas" para la implementación de una red inalámbrica segura y bajo total control por el administrador de dicha red.

Empezando por brindar de un acceso seguro en redes inalámbricas es que se combinan dos tecnologías: *Wi-Fi Protected Access 2* (WPA2) y el estándar IEEE 802.1X (*Port Based Network Access Control*), las cuales integraremos con los protocolos estándares RADIUS (*Remote Authentication Dial In User Service*) y LDAP (*Lightweight Directory Access Protocol*) para brindar los accesos en base a una relación predefinida de usuarios con sus respectivas contraseñas. Así, será posible llevar a cabo un registro de las actividades que hagan estos usuarios e incluso pudiendo llegar a tomar medidas de restricción de recursos por usuario por medio de la implementación de una plataforma Web basada en PHP (PHP Hypertext Preprocessor) que se encargue de realizar la gestión de todo este sistema. Cabe mencionar que toda la implementación será realizada teniendo en cuenta un análisis de costo-beneficio para la empresa u organización; llegando a estudiar distintas posibilidades de implementación de acuerdo a varias marcas de equipos de *access points* (las funciones que soportaría

cada uno) con los que se pueda probar y el costo que cada tipo de solución implicaría.

En la sección de servidores se tiene pensado utilizar herramientas de *software* libre que trabajen bajo la plataforma GNU/Linux; tales como OpenLDAP, FreeRADIUS, MySQL, entre otros; para los cuales los costos frente a otras implementaciones cerradas se reducirían considerablemente.

Capítulo 1: Marco Teórico

1.1. Antecedentes

Las primeras redes inalámbricas IEEE 802.11 aparecieron a finales de la década de los noventa. Su aparición se debía principalmente al propósito de brindar un acceso inalámbrico a muchas computadoras ubicadas juntas en un ambiente cerrado; de tal forma se prescindirían de los actuales cables UTP para la conexión de los usuarios a la red. Si bien las velocidades de estas redes cuando aparecieron no les permitía competir contra las redes con cables de ese entonces (donde la tecnología Ethernet empezaría su reinado), poco a poco fueron éstas mejorando hasta llegar en la actualidad a velocidades lo suficientemente rápidas (25 a 30 Mbps de *throughput* real en el mejor de los casos para redes Wi-Fi basadas en el estándar IEEE 802.11g) como para brindar un acceso satisfactorio a los usuarios de la red.

Sin embargo, un aspecto que no se había tenido en cuenta debidamente desde los inicios de las redes inalámbricas era el de la seguridad. Con un

esquema de seguridad tan débil como la no emisión (*broadcast)* del identificador de la red o el mecanismo de autenticación y cifrado WEP (*Wired Equivalent Privacy*), basado en algoritmos de cifrado muy fáciles de romper en la actualidad con la potencia de procesamiento de una computadora común y corriente (y teniendo en cuenta que actualmente en la Internet es posible encontrar artículos en los que se indiquen todos los pasos a seguir para romper la seguridad de una red inalámbrica basada en WEP en menos de 5 minutos), es que se dejaba abierta una puerta para la entrada de intrusos en nuestra red y así comprometer la seguridad de toda una empresa u organización.

De esta forma, es que se encontró necesario el desarrollo de manera urgente de protocolos que mejoren la seguridad en estas redes inalámbricas. Así fue como fueron apareciendo mecanismos tales como WPA, WPA2 (estandarizado luego por la IEEE como 802.11i), 802.1X, entre otros.

1.2. Objetivos y alcances

La presente tesis tiene los siguientes objetivos:

- Estudiar la tecnología Wi-Fi (IEEE 802.11), enfocándonos en el análisis de los aspectos de seguridad que en ella se contemplan.
- Diseñar e implementar una red inalámbrica considerando los más altos grados de seguridad: con autenticaciones y comunicaciones seguras.
- Implementar una plataforma de gestión y contabilidad de los usuarios para el acceso de la red inalámbrica.

- Llevar a cabo un análisis de costo-beneficio entre los distintos equipos disponibles en el medio para la implementación de la red inalámbrica segura.

En el estudio de la tecnología IEEE 802.11 se engloba también la investigación en temas referidos a *networking* (como por ejemplo Ethernet y TCP/IP), los cuales no se incluirán en los contenidos de esta tesis debido al espacio que esto contraería y para no desviarnos del tema central, las redes inalámbricas.

La implementación de la plataforma de gestión y contabilidad será llevada a cabo en una distribución de GNU/Linux (Ubuntu 6.06 LTS), por tratarse de un sistema operativo de libre distribución, que además se caracteriza por contar con una gran estabilidad, seguridad, performance y compatibilidad a diferencia de otras distribuciones libres de GNU/Linux. Así mismo, esta versión del sistema operativo Ubuntu cuenta con el grado LTS (*Long Term Support*), el cual significa que la organización que la implementó se compromete a brindar soporte a largo plazo (hasta junio del 2011).

Los alcances de la tesis son los que se indican a continuación:

- La implementación de la red inalámbrica contemplará altos mecanismos de seguridad; para los cuales no permitirá que un posible intruso pueda ser capaz de leer la información confidencial de los usuarios ni de permitirle si quiera acceso a la red.
- La plataforma será capaz de gestionar el acceso de los usuarios a la red inalámbrica y llevar a cabo la contabilidad de las actividades que éstos hagan, siempre que se encuentren conectados en una red IP.

- La elaboración de una guía de conexión para el usuario en distintas versiones (de acuerdo al sistema operativo que éste pueda utilizar).
- La plataforma final que se plantea en esta tesis será implementada a manera de un prototipo (piloto) puramente operativo.

1.3. Redes inalámbricas 802.11

No es la intención de esta tesis realizar un estudio exhaustivo sobre la operación del estándar 802.11, ni tampoco llegar a analizarlo hasta el nivel físico (propagación como onda de radio, modulación ni estudio de campos); pero sí se cree necesario presentar una breve introducción a las redes inalámbricas 802.11, conceptos generales, que tipos existen en la actualidad, y un conciso resumen de su funcionamiento.

1.3.1. Aspectos generales en redes 802.11

Las redes inalámbricas se caracterizan por no requerir de un medio guiado (cable) para interconectar a los equipos; sino que hace uso del aire para poder transmitir y recibir los datos. Como es de suponerse, el envío y recepción de las señales se realiza por medio de ondas electromagnéticas, las cuales se propagan por cualquier medio, teniendo al aire como principal y mejor medio aunque también pueden propagarse penetrando por obstáculos (paredes, puertas, ventanas, etc.) sufriendo una atenuación considerable y provocando que la señal se pierda como ruido.

Las redes inalámbricas 802.11, desarrolladas por el grupo de trabajo IEEE 802.11 (formado en 1990) y dadas a conocer comercialmente como Wi-Fi por la *Wireless Fidelity Alliance* (organización conformada por las distintas compañías que desarrollan hardware para esta tecnología y cuya principal misión es el de promover su uso en el hogar y en ambientes empresariales), operan en las dos capas inferiores del modelo de referencia OSI, tal y como se puede apreciar en la figura 1.1 [BAN2003].

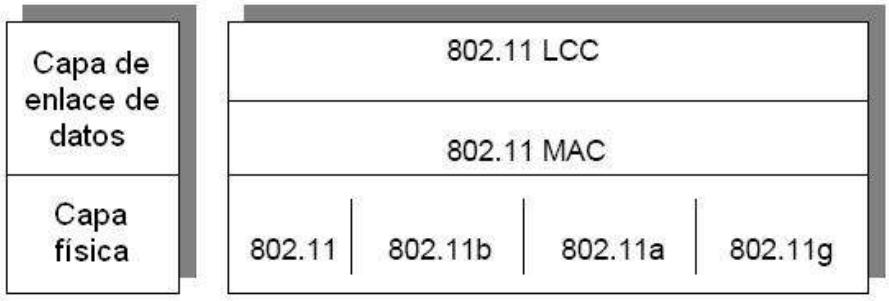

Figura 1.1 – Ubicación del estándar 802.11 dentro del modelo de referencia OSI.

La primera versión de este estándar apareció en el año 1997 y obtuvo el nombre del grupo que trabajó en él: IEEE 802.11 (ahora conocido también como 802.11Legacy). Utilizaba infrarrojos para la comunicación (por lo que requería de línea de vista) y operaba a dos tasas de transferencia (1 y 2 Mbps). A lo largo de los años fueron apareciendo otras versiones y mejoras del estándar 802.11. Así, el primero en aparecer fue el IEEE 802.11b (el mayor desplegado en la actualidad). Utilizaba como tecnología de acceso al medio el FHSS (*Frequency Hoping Spread Spectrum*) en la banda ISM de 2.4 GHz y operaba además en dos tasas mayores (5.5 y 11 Mbps). Luego

apareció el IEEE 802.11a, utilizando OFDM (*Orthogonal Frequency Division Multiplexing*) en la banda ISM de 5 GHz (lo cual lo hacía incompatible con las versiones anteriores) y logrando una tasa máxima de 54 Mbps (teóricos). Después apareció el IEEE 802.11g, utilizando DSSS (*Direct Sequence Spread Spectrum*) en la banda ISM de 2.4 GHz (lo cual lo hacía compatible con la versión b) y alcanzaba igualmente una tasa máxima de 54 Mbps (teóricos). En la actualidad se ha venido desarrollando una nueva versión del estándar llamada IEEE 802.11n, la cual promete alcanzar tanto tasas de transmisión como coberturas mucho mayores a las actuales. Se planea que esté concluida totalmente para finales del 2008.

A continuación, se presenta una tabla con un resumen de las versiones del 802.11 [1]:

Protocolo	**Fecha de aparición**	**Frecuencia de operación**	**Throughput (Típico)**	**Tasa de tx (Máx)**	**Radio de cobertura (interiores)** **Depende de # y tipo paredes**	**Rango (exteriores)** **Atenuación por una pared incluida**
802.11 *Legacy*	1997	2.4-2.5 GHz	1 Mbps	2 Mbps	~20 Metros	~100 Metros
802.11a	1999	5.15-5.25/5.25-5.35/5.49-5.725/5.725-5.85 GHz	25 Mbps	54 Mbps	~35 Metros	~120 Metros
802.11b	1999	2.4-2.5 GHz	6.5 Mbps	11 Mbps	~38 Metros	~140 Metros
802.11g	2003	2.4-2.5 GHz	20 Mbps	54 Mbps	~38 Metros	~140 Metros
802.11n	Noviembre 2008 (estimado, actualmente en *draft* 2.0)	2.4 GHz y/o 5 GHz	74 Mbps	248 Mbps = 2x2 ant	~70 Metros	~250 Metros

Tabla 1.1 – Resumen de los estándares IEEE 802.11

La banda de frecuencias ISM 2.4 GHz (utilizada por los estándares b y g) se subdivide en 14 canales, cada uno ocupando un espectro de 22 MHz y depende de la región en la que se ubique para poder utilizar canales específicos. En la tabla que se muestra a continuación, se puede apreciar las frecuencias centrales por canal, así como si está permitido su uso o no en dicha región [2]:

Identificador de Canal	Frecuencia en MHz	Dominios Reguladores				
		América (-A)	EMEA (-E)	Israel (-I)	China (-C)	Japón (-J)
1	2412	×	×	—	×	×
2	2417	×	×	—	×	×
3	2422	×	×	×	×	×
4	2427	×	×	×	×	×
5	2432	×	×	×	×	×
6	2437	×	×	×	×	×
7	2442	×	×	×	×	×
8	2447	×	×	×	×	×
9	2452	×	×	×	×	×
10	2457	×	×	—	×	×
11	2462	×	×	—	×	×
12	2467	—	×	—	—	×
13	2472	—	×	—	—	×
14	2484	—	—	—	—	×

Tabla 1.2 – Canales en la banda ISM 2.4 GHz usados por región

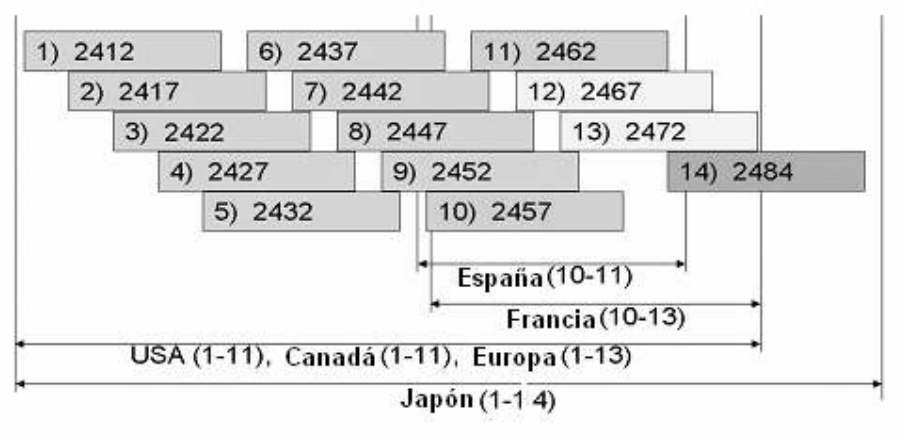

Figura 1.2 – Canales en la banda ISM 2.4 GHz para IEEE 802.11b [CHA2007]

Como podrá observarse, solo 03 canales para la región de América no se interfieren; por lo que es posible utilizar los tres canales simultáneamente en una misma área sin que esto perjudique el desempeño de la red. Para el caso de utilizar canales que ocupen parcialmente un mismo intervalo de frecuencias, se generarán interferencias y se verá afectado el desempeño de la red (registrándose velocidades muy por debajo de lo normal).

Antes de poder pasar a ver la arquitectura de una red inalámbrica 802.11 es necesario que definamos ciertos términos a manera de conceptos generales:

- *Station* o estación: Dispositivo final que se conectará a la red inalámbrica (por ejemplo: una computadora, un PDA, una impresora, etc.).
- *Basic Service Set* (BSS) o conjunto de servicio básico: Nombre que recibe a la red inalámbrica propiamente dicha. Si está conformada solo por estaciones inalámbricas recibe el nombre de IBSS (*Independent BSS*) y se dice que forma una topología *Ad-hoc*; mientras que si existe un punto de acceso a una red cableada se dice

que tiene una topología Infraestructura. Un BSS (sea IBSS o BSS) se identifica con una cadena alfanumérica de 1 a 32 bytes llamada SSID (*Service Set Identifier*) o también llamado ESSID. A su vez, cada BSS se identifica con un BSSID y un IBSS con un IBSSID, el cual consiste en un identificador de 48 bits que se utilizan para identificar a que BSS pertenece la comunicación.

- *Distribution System* (DS) o sistema de distribución: Nombre que recibe a la red cableada tradicional que se utilice para interconectar dos o más BSS.
- *Access Point* (AP) o punto de acceso: Dispositivo intermediario entre la red inalámbrica y la red cableada.
- *Extended Service Set* (ESS) o conjunto de servicio extendido: Es el conjunto de varios BSS por medio de al menos un DS.

Así, pasamos a ver los dos principales modos de arquitectura que se tienen en una red inalámbrica 802.11:

- Red *Ad-hoc:* Aquella en la que no existe ningún dispositivo que controle las comunicaciones entre las estaciones de la red ni que permite interconectarlos con un DS. Son redes aisladas, fáciles de implementar, de uso temporal, corto alcance y reducido número de estaciones.

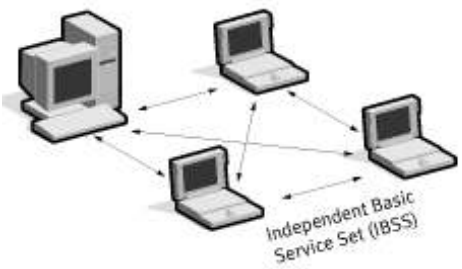

Figura 1.3 – Red inalámbrica en modo *Ad-hoc* [BAN2003]

❖ Red Infraestructura: Aquella en la que sí existe al menos un dispositivo (AP) que controle las comunicaciones entre las estaciones y les permite además interconectarlos con un DS, logrando que puedan conectarse con otras BSS y formar así un ESS.

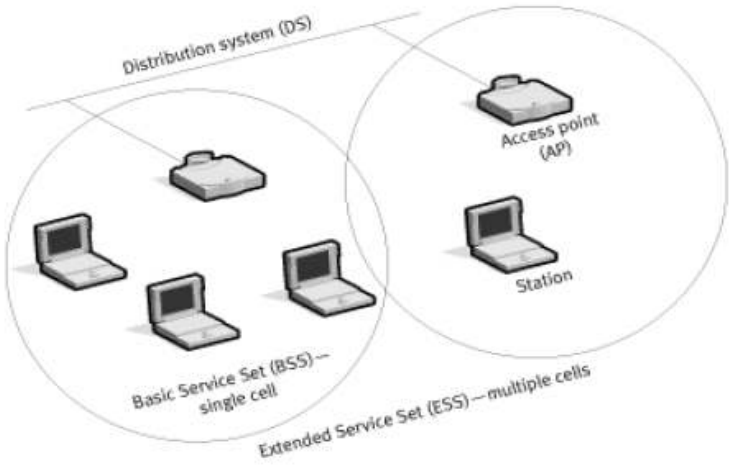

Figura 1.4 – Red inalámbrica en modo Infraestructura [BAN2003]

Para el modo infraestructura, el estándar IEEE 802.11 establece una serie de servicios que el DS debe de soportar. Estos servicios pueden dividirse en dos grupos:

1. *Station Services* (SS) o servicios de estación
    a. Autenticación
    b. Desautenticación
    c. Privacidad
    d. Reparto de MSDU (*MAC Service Data Unit*)
2. *Distribution System Services* (DSS) o servicios del sistema de distribución
    a. Asociación
    b. Reasociación

c. Desasociación

d. Distribución

e. Integración

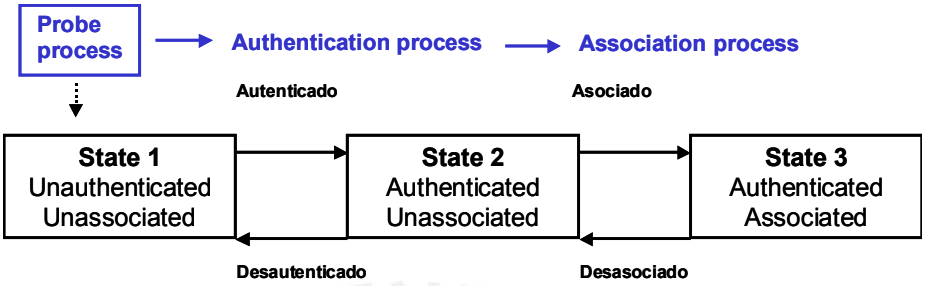

Figura 1.5 – Estados durante el proceso de asociación [BAN2003]

1.3.2. Seguridad en redes 802.11

Junto con la aparición del estándar IEEE 802.11, aparece también el primer mecanismo de seguridad mediante el cual era posible cifrar la información transmitida al medio y no enviarla como texto plano (*plaintext*). Este mecanismo fue llamado WEP (*Wired Equivalent Privacy*).

WEP

WEP, acrónimo de *Wired Equivalent Privacy*, 1999 - es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes *wireless* que permite cifrar la información que se transmite. Proporciona cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV).

El protocolo WEP se basa en dos componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

RC4 es un algoritmo de cifrado de flujo; es decir, funciona expandiendo una semilla (*seed* en inglés) para generar una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado. Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma semilla para cifrar dos mensajes diferentes, ya que obtener la clave sería trivial a partir de los dos textos cifrados resultantes. Para evitar esto, WEP especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña (a través de esta concatenación se genera la semilla que sirve de entrada al algoritmo.

El principal problema con la implementación de dicho algoritmo es el tamaño de los vectores de iniciación. A pesar de que se pueden generar muchos vectores, la cantidad de tramas que pasan a través de un punto de acceso es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo vector de iniciación, y por lo tanto sea fácil hacerse con la clave. Por lo tanto es inseguro debido a su implementación. Aumentar los tamaños de las claves de cifrado sólo aumenta el tiempo necesario para romperlo. [5]

Para atacar una red Wi-Fi se suelen utilizar los llamados *packet sniffers* y los WEP c*rackers*. Para llevar a cabo este ataque, se captura una cantidad de paquetes necesaria (dependerá del número de bits de cifrado) mediante la

utilización de un *packet sniffer* y luego mediante un WEP *cracker* o *key cracker* se trata de "romper" el cifrado de la red. Un *key cracker* es un programa basado generalmente en ingeniería inversa que procesa los paquetes capturados para descifrar la clave WEP. Romper una llave más larga requiere la interceptación de más paquetes, pero hay ataques activos que estimulan el tráfico necesario.

A pesar de existir otros protocolos de cifrado mucho menos vulnerables y más eficaces -como pueden ser el WPA o el WPA2- el protocolo WEP sigue siendo muy popular y posiblemente el más utilizado. Esto es debido a que WEP es fácil de configurar y cualquier sistema con el estándar 802.11 lo soporta. Sin embargo no ocurre lo mismo con otros protocolos como WPA, que no es soportado por mucho hardware antiguo. El hardware moderno pasa entonces a utilizar el modelo de seguridad WEP para poder interactuar con este hardware antiguo.

Concluimos diciendo que actualmente hay sistemas de cifrado mejor para redes Wi-Fi, como el WPA o WPA2, surgidos para solucionar los problemas de seguridad mencionados del WEP.

WPA/WPA2 (IEEE 802.11i)

WPA (*Wi-Fi Protected Access* - 1995 - Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas Wi-Fi; creado para corregir las deficiencias del sistema previo WEP. Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del

estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance". [6]

WPA fue diseñado para utilizarse con un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1X); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK - *Pre-Shared Key*) para usuarios de casa o pequeña oficina. La información es cifrada utilizando el algoritmo RC4 (debido a que WPA no elimina el proceso de cifrado WEP, sólo lo fortalece), con una clave de 128 bits y un vector de inicialización de 48 bits.

Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - *Temporal Key Integrity Protocol*), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización mucho más grande, evita los ataques de recuperación de claves (ataques estadísticos) a los que es susceptible WEP.

Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. El chequeo de redundancia cíclica (CRC - *Cyclic Redundancy Check*) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - *Message Integrity Code*), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (*replay attacks*), ya que incluye un contador de tramas.

Al incrementar el tamaño de las claves, el número de llaves en uso, y al agregar un sistema de verificación de mensajes, WPA hace que la entrada no autorizada a redes inalámbricas sea mucho más difícil. El algoritmo Michael fue el más fuerte que los diseñadores de WPA pudieron crear, bajo la premisa de que debía funcionar en las tarjetas de red inalámbricas más viejas; sin embargo es susceptible a ataques. Para limitar este riesgo, WPA define que se desconecte durante 60 segundos al detectar dos intentos de ataque durante 01 minuto.

WPA2

WPA2 está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i (ratificado en Junio de 2004).

La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1X/EAP como WPA-Enterprise y WPA2-Enterprise.

Los fabricantes comenzaron a producir la nueva generación de AP apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (*Advanced Encryption Standard*). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI (Tecnologías de la Información) la seguridad que la tecnología cumple con estándares de interoperatividad" declaró el Director de la Wi-Fi Alliance.

Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i (siempre y cuando se utilice una clave los suficientemente larga y compleja como para no ser comprometida por ataques de diccionario y/o de fuerza bruta).

Filtrado de direcciones

Existe un mecanismo adicional que si bien no es considerado del todo seguro por sí mismo, aporta una capa más en la seguridad de una red inalámbrica 802.11. Este mecanismo es conocido como filtrado de direcciones MAC (*MAC filtering*), en el cual se configura en cada AP las direcciones MAC de los clientes que tienen autorizado el acceso a la red inalámbrica; por lo que al detectar las tramas provenientes de usuarios cuyas direcciones MAC no se encuentren en dicha lista, sencillamente son descartadas y no se les brinda acceso a la red.

Hay que resaltar que esto representa solo un nivel más de la seguridad en una red inalámbrica; ya que es posible falsear (*spoofing*) una dirección MAC en un cliente y bastaría con conocer alguna dirección MAC de un cliente autorizado al acceso a la red (bastaría con mantenerse un tiempo escuchando con un *sniffer* cercano a un AP hasta capturar alguna trama enviada por un cliente autorizado). Así mismo, no se recomienda el uso de este mecanismo en redes inalámbricas grandes con muchos usuarios, al volverse un gran problema el llevar a cabo la administración de dicha red por requerir la configuración de cada AP por cada usuario en la red.

802.1X

El IEEE 802.1X (*Port-based Network Access Control*) es un estándar de la IEEE para Control de Admisión de Red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Con la aparición de las redes inalámbricas Wi-Fi, también es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en protocolo de autenticación extensible (EAP– RFC 2284). El RFC 2284 ha sido declarado obsoleto en favor del RFC 3748.

802.1X está disponible en ciertos conmutadores de red y puntos de acceso, y puede configurarse para autenticar nodos que están equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos.

Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo fallas de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor de RADIUS. Esto permite la autenticación solo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

1.4. Otras tecnologías a utilizar

En el desarrollo de la presente tesis se tiene planeado utilizar distintas tecnologías aplicadas en general en las redes de datos IP.

1.4.1. EAP/ 802.1X / RADIUS

EAP

EAP o Extensible Authentication Protocol (Protocolo de Autenticación Extensible), es una estructura de soporte (*framework*) frecuentemente usada en redes inalámbricas y conexiones punto-a-punto. Es definida en el RFC 3748. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas, es más frecuentemente usado en redes inalámbricas. Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación.

EAP es una estructura de soporte, no un mecanismo específico de autenticación. El EAP provee algunas funciones comunes y negociaciones para el o los mecanismos de autenticación escogidos. Estos mecanismos son llamados métodos EAP, de los cuales se conocen actualmente unos 40. Además de algunos específicos de proveedores comerciales, los definidos por RFC de la IETF incluyen EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, y EAP-AKA. Los métodos modernos capaces de operar en ambientes inalámbricos incluyen EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP y EAP-TTLS. Los requerimientos para métodos EAP usados en LAN inalámbricas son descritos en la RFC 4017.

Cuando EAP es invocada por un dispositivo NAS (Network Access Server) capacitado para 802.1X, como por ejemplo un punto de acceso 802.11 a/b/g, los métodos modernos de EAP proveen un mecanismo seguro de autenticación y negocian un PMK (Pair-wise Master Key) entre el dispositivo cliente y el NAS. En esas circunstancias, la PMK puede ser usada para abrir una sesión inalámbrica cifrada que usa cifrado TKIP o AES.

802.1X

Para poder utilizar el sistema EAP en conexiones inalámbricas es necesario utilizar un protocolo que permita encapsular el tráfico desde la conexión inalámbrica al Servidor de Autenticación. En un entorno común tendremos un Servidor de Autenticación, que tendrá configurada la política de qué Suplicantes pueden o no conectarse a la organización, y que se encontrará dentro de una zona protegida de nuestra red. El AP tendrá conexión directa al Servidor de Autenticación y es el que demandará un proceso de Autenticación para un determinado Suplicante. 802.1X nace como forma de poder permitir a cualquier elemento de la red (switches, AP, etc.) pedir un proceso de autenticación para una conexión que se acaba de producir. 802.1X utiliza EAPOL (EAP Over Lan) porque lo que va a realizar es una encapsulación del protocolo EAP sobre la red privada para llegar al Servidor de Autenticación. Así, como se ve en el gráfico, el proceso sería el siguiente:

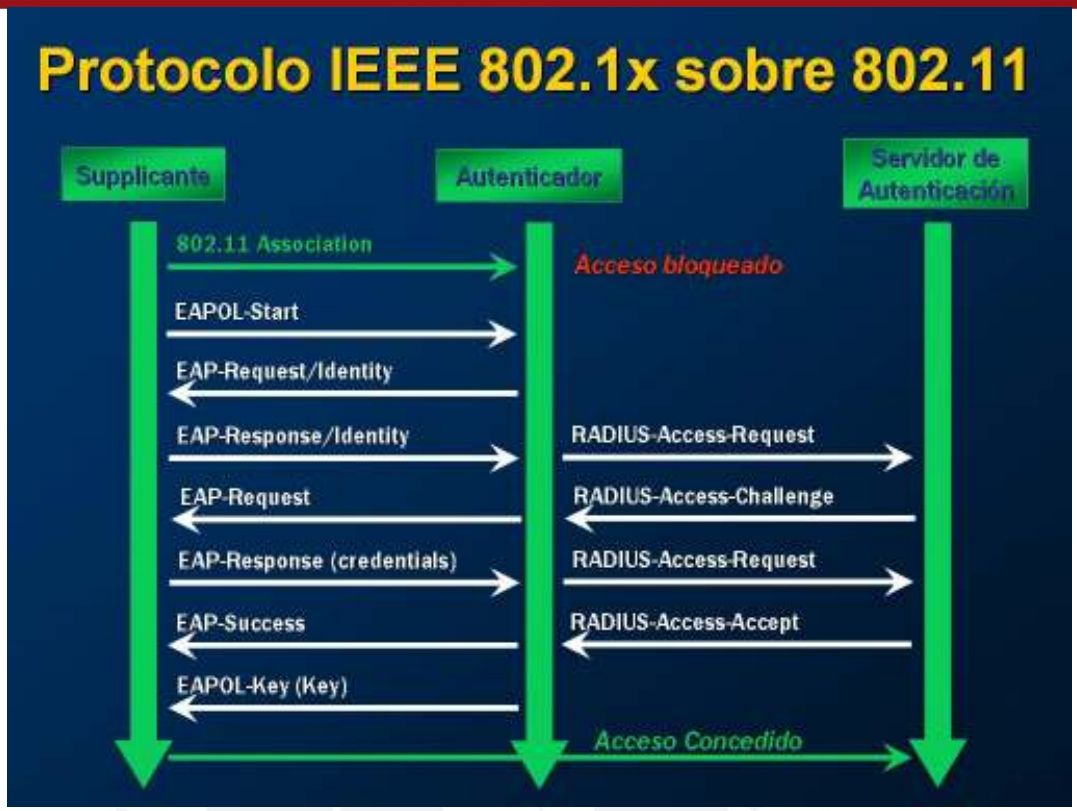

Figura 1.6 – Autenticación EAPOL [ALC2006]

Paso 1: Un cliente se asocia al AP utilizando el protocolo 802.11

Paso 2: El Suplicante inicia el proceso de autenticación 802.1X porque el AP no le concede acceso a la red y se elige el EAP-Method.

Paso 3: El Autenticador requiere la Identidad al Suplicante

Paso 4: El Suplicante le entrega la Identidad al Autenticador que retransmitirá al Servidor de Autenticación. Como se puede ver, el Servidor de Autenticación es un servidor RADIUS que pedirá las credenciales para esa identidad al Autenticador. Las credenciales pueden ser desde el par usuario/contraseña hasta el uso de certificados de seguridad X.509.

Paso 5: El Autenticador pide las Credenciales al Suplicante.

Paso 6: Suplicante entrega las Credenciales al Autenticador que se retransmiten al Servidor de Autenticación (Servidor RADIUS en este caso).

Paso 7: Servidor RADIUS valida las credenciales y acepta la conexión.

Paso 6: El Autenticador entrega tras aceptar la conexión la EAPOL-Key que no es más que una secuencia de bits que utilizaremos como Clave Maestra en el proceso de cifrado del algoritmo de cifrado elegido (TKIP o AES). Así, cada vez que tenemos un proceso de autenticación o re-autenticación se genera una nueva Clave Maestra.

RADIUS

RADIUS (acrónimo en inglés de *Remote Authentication Dial-In User Server*). Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza los puertos 1812 y 1813 UDP para establecer sus conexiones (para autenticar/autorizar y contabilizar, respectivamente).

Por ejemplo, cuando se realiza la conexión con un ISP mediante un módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (*Network Access Server* o Servidor de Acceso a la Red) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos también se pueden utilizar con propósitos estadísticos.

RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores NAS, más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio. Los servidores *Proxy* RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes).

RADIUS es extensible; la mayoría de fabricantes de software y hardware RADIUS implementan sus propios dialectos.

1.4.2. LDAP

LDAP (*Lightweight Directory Access Protocol*) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas.

Habitualmente, almacena la información de *login* o acceso a un sistema (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red. Existen diversas implementaciones y aplicaciones reales del protocolo LDAP:

Active Directory

Active Directory es el nombre utilizado por Microsoft (desde Windows 2000) como almacén centralizado de información de uno de sus dominios de administración.

Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAP versión 3 lo que permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc..

Novell Directory Services

También conocido como eDirectory es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Básicamente está compuesto por una base de datos jerárquica y orientada a objetos, que representa cada servidor, computadora, impresora, servicio, personas, etc. entre los cuales se crean permisos para el control de acceso, por medio de herencia. La ventaja de esta implementación es que

corre en diversas plataformas, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo.

OpenLDAP

Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP.

Tiene su propia licencia, la OpenLDAP Public License. Al ser un protocolo independiente de la plataforma, varias distribuciones Linux y BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS.

OpenLDAP tiene cuatro componentes principales:

* slapd - demonio LDAP autónomo.
* slurpd - demonio de replicación de actualizaciones LDAP autónomo.
* Rutinas de biblioteca de soporte del protocolo LDAP.
* Utilidades, herramientas y clientes.

Red Hat Directory Server

Directory Server es un servidor basado en LDAP que centraliza configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas así como información de control de acceso dentro de un sistema operativo independiente de la plataforma.

Forma un repositorio central para la infraestructura de manejo de identidad, Red Hat Directory Server simplifica el manejo de usuarios, eliminando la redundancia de datos y automatizando su mantenimiento.

1.4.3. Lenguaje PHP

PHP es un lenguaje de programación usado frecuentemente para la creación de contenido para sitios Web dinámicos con los cuales se puede programar las páginas HTML y los códigos fuente. PHP es un acrónimo recursivo que significa "*PHP Hypertext Pre-processor*" (inicialmente PHP *Tools*, o, *Personal Home Page Tools*), y se trata de un lenguaje interpretado usado para la creación de aplicaciones para servidores, o creación de contenido dinámico para sitios Web. Últimamente también para la creación de otro tipo de programas incluyendo aplicaciones con interfaz gráfica usando las librerías Qt o GTK+.

El fácil uso y la similitud con los lenguajes más comunes de programación estructurada, como C y *Perl*, permiten a la mayoría de los programadores experimentados crear aplicaciones complejas con una curva de aprendizaje muy suave. También les permite involucrarse con aplicaciones de contenido dinámico sin tener que aprender todo un nuevo grupo de funciones y prácticas.

Debido al diseño de PHP, también es posible crear aplicaciones con una interfaz gráfica para el usuario (también llamada GUI), utilizando la extensión PHP-Qt o PHP-GTK. También puede ser usado desde la línea de órdenes, de la misma manera como *Perl* o *Python* pueden hacerlo, esta versión de PHP se llama PHP CLI (*Command Line Interface*).

Su interpretación y ejecución se da en el servidor Web, en el cual se encuentra almacenado el *script*, y el cliente sólo recibe el resultado de la

ejecución. Cuando el cliente hace una petición al servidor para que le envíe una página Web, generada por un *script* PHP, el servidor ejecuta el intérprete de PHP, el cual procesa el *script* solicitado que generará el contenido de manera dinámica, pudiendo modificar el contenido a enviar, y regresa el resultado al servidor, el cual se encarga de regresárselo al cliente. Además es posible utilizar PHP para generar archivos PDF, Flash, así como imágenes en diferentes formatos, entre otras cosas.

Permite la conexión a diferentes tipos de servidores de bases de datos tales como MySQL, Postgres, Oracle, ODBC, DB2, Microsoft SQL Server, Firebird y SQLite; lo cual permite la creación de Aplicaciones Web muy robustas.

PHP también tiene la capacidad de ser ejecutado en la mayoría de los sistemas operativos tales como UNIX (y de ese tipo, como Linux o Mac OS X) y Windows, y puede interactuar con los servidores Web más populares ya que existe en versión CGI, módulo para Apache, e ISAPI.

El modelo PHP puede ser visto como una alternativa al sistema de Microsoft que utiliza ASP.NET/C#/VB.NET, a ColdFusion de la compañía Adobe (antes Macromedia), a JSP/Java de Sun Microsystems, y al famoso CGI/Perl. Aunque su creación y desarrollo se da en el ámbito de los sistemas libres, bajo la licencia GNU, existe además un IDE (entorno integrado de desarrollo) comercial llamado Zend Optimizer. Recientemente, CodeGear (la división de lenguajes de programación de Borland) ha sacado al mercado un entorno integrado de programación para PHP, denominado Delphi for PHP.

Los principales usos del PHP son los siguientes:

- Programación de páginas Web dinámicas, habitualmente en combinación con el motor de base datos MySQL, aunque cuenta con soporte nativo para otros motores, incluyendo el estándar ODBC, lo que amplía en gran medida sus posibilidades de conexión.
- Programación en consola, al estilo de *Perl* o *Shell scripting*.
- Creación de aplicaciones gráficas independientes del navegador, por medio de la combinación de PHP y Qt/GTK+, lo que permite desarrollar aplicaciones de escritorio en los sistemas operativos en los que está soportado.

Las principales características del PHP son las siguientes:

- Es un lenguaje multiplataforma.
- Capacidad de conexión con la mayoría de los manejadores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL.
- Leer y manipular datos desde diversas fuentes, incluyendo datos que pueden ingresar los usuarios desde formularios HTML.
- Capacidad de expandir su potencial utilizando la enorme cantidad de módulos (llamados ext's o extensiones).
- Posee una amplia documentación en su página oficial, entre la cual se destaca que todas las funciones del sistema están explicadas y ejemplificadas en un único archivo de ayuda.
- Es libre, por lo que se presenta como una alternativa de fácil acceso.
- Permite las técnicas de Programación Orientada a Objetos (POO).
- Permite crear los formularios para la Web.
- Biblioteca nativa de funciones sumamente amplia e incluida.

- No requiere definición de tipos de variables ni manejo detallado del bajo nivel.

1.4.4. GNU Linux

Para la implementación de la plataforma (toda la etapa de programación) se ha decidido utilizar Ubuntu 6.06 LTS, una distribución de GNU/Linux, como sistema operativo en el cual se pasará a trabajar. Para ello, será necesario revisar el funcionamiento de este sistema operativo, la evolución de su kernel y las herramientas libres que nos ofrece para nuestro desarrollo. En la figura que se muestra a continuación se puede apreciar como es que se han ido ramificando los sistemas operativos a partir del padre de todos estos: Unix.

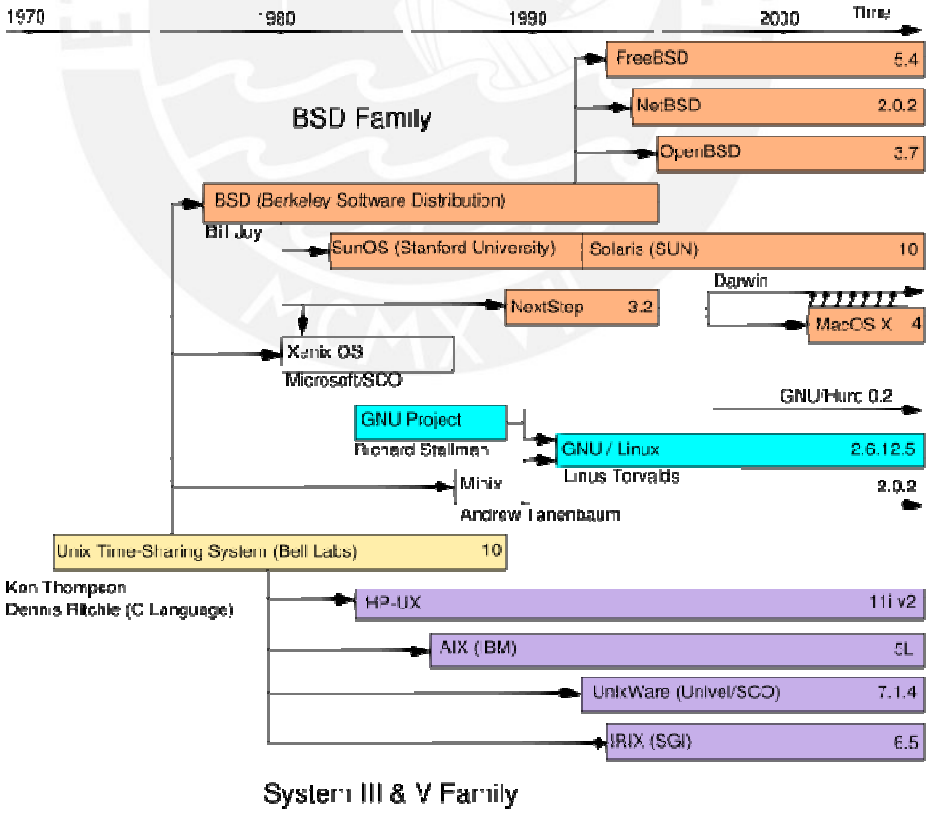

Figura 1.7 – Jerarquía histórica de los sistemas de la familia UNIX [3]

1.4.4.1. FreeRADIUS

FreeRADIUS es una implementación en software libre de RADIUS y se caracteriza por soportar múltiples mecanismos de autenticación, tales como PAP, CHAP, MD5, EAP (TLS, PEAP y TTLS), entre otros.

Provee ser una alternativa frente a otras implementaciones de servidores RADIUS comerciales, tales como el Cisco ACS o el Microsoft IAS (incluido con el MS Windows 2003 Server). Se dice que es uno de los servidores RADIUS más utilizados a nivel mundial, utilizado en todo tipo de entornos, desde pequeñas redes SOHO hasta grandes redes de ISP.

Su gran soporte por múltiples protocolos de autenticación, fácil configuración, gran soporte por parte de la comunidad, junto con su gran aceptación y divulgación, lo colocan a FreeRADIUS como una de las mejores opciones a implementar tanto dentro de un entorno LAN como WLAN.

1.4.4.2. OpenLDAP

OpenLDAP es una implementación en software libre del protocolo LDAP (*Lightweight Directory Access Protocol*), utilizado, en la mayoría de ocasiones, para la administración de usuarios en una red IP mediante servicios de directorio. En ella se puede guardar información básica que va desde el par usuario/contraseña utilizado para poder brindar accesos a los usuarios de una red, hasta información básica de dichos usuarios que

pueden ser guardados dentro de este servidor a manera de una pequeña base de datos.

OpenLDAP ha demostrado ser un servidor con una respuesta mucho más veloz que cualquier otra base de datos al encontrarse éstos ubicados de manera estructurada. Así mismo, al no haber referencias internamente se facilita las operaciones de búsqueda, brindando una respuesta veloz. Sin embargo, su simplicidad juega en contra suya cuando se desea implementar servicios más complejos o elaborados, volviéndose así en una desventaja frente a bases de datos referenciales que soportan mejor dichos desarrollos. Para nuestro caso, un servidor OpenLDAP demostrará ser una implementación que se adapta mejor al escenario propuesto debido principalmente a dos factores:

- La capacidad de integrarse con otros servidores basados en la misma tecnología LDAP, tales como un servidor MS Active Directory, Novell e-Directory Server, etc.; con los cuales podrá trabajar en armonía y de esta manera centralizar toda la información de los usuarios en una sola plataforma.
- La capacidad de responder rápidamente a consultas sencillas. En comparación de las bases de datos, para las cuales se genera toda una sesión o socket para cada una de las consultas que se realice, teniendo un tiempo de demora muy por encima de una en OpenLDAP, y a su vez tarda más tiempo en cerrarla y liberar el recurso en comparación con la propuesta.

1.4.4.3. MySQL

MySQL es un gestor de base de datos sencillo de usar y rápido. También es uno de los motores de base de datos más usados en Internet, la principal razón de esto es que es gratuito para aplicaciones no comerciales.

Las características principales de MySQL son:

- Es un gestor de base de datos. Una base de datos es un conjunto de datos y un gestor de base de datos es una aplicación capaz de manejar este conjunto de datos de manera eficiente y cómoda.
- Es una base de datos relacional. Una base de datos relacional es un conjunto de datos que están almacenados en tablas entre las cuales se establecen unas relaciones para manejar los datos de una forma eficiente y segura. Para usar y gestionar una base de datos relacional se usa el lenguaje estándar de programación SQL.
- Es de código abierto. El código fuente de MySQL se puede descargar y está accesible a cualquiera, por otra parte, usa la licencia GPL para aplicaciones no comerciales.
- Es una base de datos muy rápida, segura y fácil de usar. Gracias a la colaboración de muchos usuarios, la base de datos se ha ido mejorando, optimizándose en velocidad. Por eso es una de las bases de datos más usadas en Internet.
- Existe una gran cantidad de software que la usa.

1.4.4.4. Apache Web Server

El servidor HTTP Apache es un software libre que implementa un servidor HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Windows, Macintosh, entre otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual.

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache tiene amplia aceptación en la red: desde 1996, Apache, es el servidor HTTP más usado. Alcanzó su máxima cota de mercado en 2005 siendo el servidor empleado en el 70% de los sitios web en el mundo, sin embargo ha sufrido un descenso en su cuota de mercado en los últimos años (frente a otras soluciones como el Microsoft Internet Information Services o IIS).

Capítulo 2: Análisis de la solución

2.1. Definición del problema a resolver

El problema a resolver es el siguiente:

Una organización cuenta con una red LAN en su oficina principal. Inicialmente, esta organización cuenta con toda su red LAN cableada, siendo esto una gran traba para sus usuarios móviles que cuentan con computadoras portátiles (*notebooks*) y se encuentran en constante movimiento dentro de dicho local; ya que requieren ubicar un punto de red cercano a donde se encuentren para poder descargar sus correos o buscar alguna información en la Internet, lo que trae consigo incomodidad y una disminución en el desempeño de dicha persona al perder tiempo realizando este proceso; tiempo que se traduce en una disminución de su productividad.

Como segundo problema se tiene que el estado actual de la red no es el óptimo. Debido a un simple pero inadecuado direccionamiento IP de la red,

así como una mala distribución del equipamiento de red, ha ocasionado que se presenten síntomas de lentitud y una respuesta tardía ante los requerimientos de sus usuarios, incluso para simples usos como descargar correos o navegar por la Internet. El administrador de la red ya ha pensado en la idea de implementar una red inalámbrica para los usuarios con *notebooks*; pero aún no cuenta con los conocimientos necesarios para implementarla de manera adecuada, entendiendo por esto que no se encuentra al tanto de que tecnologías utilizar para que la nueva red inalámbrica sea segura y no represente un agujero en la seguridad del sistema, y así mismo poder llevar a cabo un control sobre los accesos de los usuarios, pudiendo tener una gestión sobre estos.

2.1.1. Ubicación del problema en un escenario inicial

El escenario inicial propuesto se trata de una empresa que cuenta con una oficinal principal ubicada en la ciudad de Lima, en donde se encuentra ubicado su infraestructura principal (servidores de correo, base de datos, Web, entre otros), así como las oficinas de los principales ejecutivos de la empresa (gerente general y gerentes de áreas), jefes de áreas, ejecutivos de ventas, ingenieros, técnicos, personal de administración y logística, entre otros.

La oficina principal tiene una salida a la Internet por medio de un *router gateway*, el cual le brinda una velocidad a la Internet de hasta 2 Mbps mediante acceso por ADSL con una dirección IP pública fija (estática).

En el ***anexo #1*** se puede observar un diagrama físico (como se encuentra distribuido el equipamiento de red) y lógico (como se ha realizado el direccionamiento IP) para el estado inicial de esta red.

2.1.2. Análisis del problema

Debido a un direccionamiento IP plano (todos los equipos se están colocando dentro de la misma subred) se ha podido detectar como la principal causa del segundo problema: una respuesta tardía por parte de la red a los requerimientos de sus usuarios. Para la cantidad de usuarios que está soportando la red se ve necesario implementar mecanismos de segmentación lógica de la red aplicando metodologías de *subnetting* (dividir la red en subredes) para así poder manejar el tráfico de *broadcasts* (mensajes enviados por un equipo dirigidos a todos los equipos dentro de su misma subred). Así mismo, sería recomendable aplicar metodologías de VLAN (Redes LAN Virtuales) para poder segmentar la red de la manera más óptima y segura a la vez. En la siguiente sección se pasará a explicar detalladamente la solución propuesta para aliviar este problema.

Con respecto al problema principal de los usuarios móviles, se ve necesario aprovechar la capacidad con la que cuentan sus computadoras portátiles para conectarse a redes inalámbricas; ya que éstas han venido de fábrica con su tarjeta de red inalámbrica incorporada. Así, se pasará a detallar cual debería de ser el óptimo diseño que se deberá de tener para esta red inalámbrica, teniendo en cuenta los factores de seguridad para este tipo de red explicados en el primer capítulo de esta tesis, para así no comprometer

la confidencialidad de los datos de los usuarios de esta red inalámbrica ni la seguridad de toda la red empresarial.

2.2. Planteamiento de una solución al problema

Una vez definido el problema y ubicado en un escenario inicial pasamos a plantear una solución teniendo en cuenta el marco teórico contemplado en un inicio. Se ve necesario establecer un procedimiento para plantear una adecuada solución al problema. Este procedimiento estará comprendido por 4 etapas: en la primera etapa se procederá con el levantamiento de información relevante al problema, en la segunda etapa se listarán los requerimientos necesarios para la solución, en la tercera etapa se definirán los alcances y limitaciones propios de la solución planteada y por último se definirá la arquitectura de la solución. Luego de realizado todo este análisis se pasará a ver el diseño propio de la solución y finalmente su implementación y sometimiento a pruebas.

2.2.1. Levantamiento de información

Para iniciar el planteamiento de una solución se requiere en primer lugar obtener la mayor cantidad de información relevante al problema en cuestión. Así, si bien ya se ha mencionado algunas características de los dos problemas en mención, procederemos a describir todo el estado actual de la red que tenga relación al problema en discusión.

En primer lugar se tiene el direccionamiento IP plano implementado en la red actualmente. Este tipo de direccionamiento IP se caracteriza por ser bastante sencillo y útil en redes pequeñas (no mayores a 16 o 20 usuarios y no cuenten con servicios de red avanzados tales como servidores Web, base de datos, etc.) por su simple, rápida y fácil implementación. Sin embargo, en un entorno como el de una empresa con más de 100 personas que acceden a los servicios de la red y la respuesta de estos servicios repercute en su desempeño dentro de la oficina, con más de un equipo por el cual pueden acceder a la red, puede concluirse que es inapropiado mantener un esquema de direccionamiento IP plano. Se requiere implementar mecanismos de *subnetting* para poder dividir a toda la gran red en redes pequeñas pero manejables y que solo se puedan comunicar los usuarios entre estas redes en los momentos necesarios y no todo el tiempo (evitando así el malgasto de los recursos de la red).

Con respecto al equipamiento de red con el que cuenta actualmente la empresa se sabe que cuenta con 6 *switches* de borde *Fast Ethernet*, de los cuales tres son de 24 puertos y tres son de 16 puertos. Todos estos *switches* son simples conmutadores Fast Ethernet 10/100 capaces únicamente de operar en la modalidad *store and forward* y no cuentan con consola de administración.

Con respecto a la red inalámbrica, se cuenta con un estudio previo de *site survey*, por el cual se ha podido conocer el número de APs requeridos y la ubicación de éstos dentro de la red principal (uno por piso, siendo así necesario tres AP's para cubrir adecuadamente las zonas de interés).

En el siguiente cuadro se resumen toda la información levantada con respecto a este escenario inicial planteado y a continuación pasaremos a listar los requerimientos que serían necesarios para poder proponer una solución a estos problemas:

Característica actual de la red	Descripción
Direccionamiento IP plano	Todos los equipos de la red se encuentran configurados para operar dentro de la misma subred.
Un solo servidor DHCP, ubicado en el *router gateway*	Se sobrecarga al router gateway con las múltiples solicitudes DHCP de los usuarios de la red.
Switches de capa 2	Los actuales switches que se tienen realizan solo la conmutación requerida para interconectar los equipos de la red; más no ofrecen ningún tipo de segmentación de redes y/o seguridad.
Access Points	Por medio de un site Surrey previamente realizado se conoce que serán necesarios 3 APs en total: colocando un AP por cada piso del edificio de tres pisos de la empresa.

Tabla 2.1 – Resumen del levantamiento de información

2.2.2. Lista de requerimientos para la solución

Luego de tener una visión más detallada del estado actual de la red al levantar la información concerniente, podemos ser capaces de realizar un listado con todos los requerimientos que serán necesarios para la solución propuesta. Así, se plantean los siguientes requerimientos:

- *Access Points*: Para solucionar el primer problema será necesario la adquisición de 03 APs, los cuales deberán de soportar los mecanismos de autenticación de usuarios por 802.1X (con EAP-PEAP, EAP-TLS o EAP-TTLS) y mecanismos de seguridad basados en el estándar 802.11i (WPA2): cifrado AES. Se considera como opcional los mecanismos de filtrado de direcciones MAC y la no emisión *broadcast* del SSID de la red inalámbrica.
- *Servidores RADIUS, LDAP y Base de datos*: Para la implementación de la red inalámbrica segura se requerirá la adquisición de nuevos servidores para poder brindar allí el servicio de autenticación de usuarios por medio del servidor de autenticación FreeRADIUS y el servidor de directorios OpenLDAP. Así mismo, para poder llevar a cabo la contabilidad de los accesos de cada usuario se requerirá de un servidor para la implementación de la base de datos MySQL.
- *Redireccionamiento IP*: Se requiere cambiar por completo el direccionamiento IP de toda la red; asignando así a cada área de la empresa una subred distinta. De la misma forma, la red inalámbrica que se implementará se encontrará en una subred distinta de la de las computadoras ya existentes. Además, la recomendación adicional que se haría sería la de implementar un esquema de VLANs (*Virtual*

Local Area Network) dentro de toda esta red; siendo necesario la adquisición de un *Switch Core* capaz de administrar VLANs y también de poder realizar el enrutamiento entre éstas. En el último capítulo de esta tesis se presentará un estudio costo-beneficio en el cual se analizará bajo cuales condiciones se vuelve necesario la implementación de VLANs y hasta que momento es que podemos prescindir de éstas.

2.2.3. Definición de los alcances y limitaciones de la solución

Después de haber levantado la información y haber listado los requerimientos para plantear una solución, se ve necesario definir cuales serán los alcances y limitaciones de la solución propuesta.

Así, los alcances de la solución propuesta serán los siguientes:

- La red inalámbrica se basará en los más óptimos mecanismos de seguridad explicados dentro del marco teórico de la presente tesis; por lo cual no se permitirá que un intruso pueda ser capaz de comprender la información de los usuarios de la red inalámbrica al viajar ésta de manera cifrada en el medio compartido que es el aire. Así tampoco le será posible tener acceso a la red inalámbrica sin un par usuario/contraseña que haya sido previamente añadido por medio del sistema de gestión Web que implementa la solución.

- La solución contemplará la gestión de los accesos de los usuarios a la red inalámbrica, llevando así la contabilidad de dichos accesos, tanto a la red inalámbrica como los accesos a la Internet.
- Debido a que el acceso seguro a la red inalámbrica requerirá de una configuración previa en los equipos (*notebooks*) de dicha red, se realizará la elaboración de una guía de conexión detallada para que el usuario pueda configurar su propio equipo y así poder conectarse sin mayores complicaciones y de manera segura a la red inalámbrica. Solamente para los casos extremos en los que los usuarios no sean capaces de llevar a cabo dicha guía es que el mismo administrador de la red tendrá que realizar dicha configuración. Es por esto que la guía ha implementar contemplará ser lo más sencilla y fácil de llevar a cabo posible; como para que un simple usuario de oficina pueda ser capaz de seguir las instrucciones allí descritas y así prescindir del administrador de red para que pueda enfocar su trabajo en otras tareas más importantes dentro de la red de la empresa.
- La plataforma final que se plantea será implementada a manera de un prototipo piloto puramente operativo; es decir, no se contemplará que la solución cuente con un acabado estilizado y/o comercial.

De igual formar, definimos las limitaciones de la solución propuesta como las siguientes:

- La solución planteada no contemplará ningún mecanismo de redundancia en caso de fallas. Cada servidor será implementado en la manera *standalone*, por lo que no contarán con otro equipo que

responda cuando alguno de éstos se encuentre fuera de servicio. La implementación de *clusters* para estos servidores sería una posible solución para estos casos, planteándolo para propuestas de trabajos a futuro que continúen esta tesis.

- La implementación de esta solución no se orientará a la eficiencia desde el código; dado que, como ya se ha mencionado anteriormente, la implementación se hará bajo un esquema operativo bajo el cual se comprobarán las funcionalidades de seguridad y gestión de accesos a usuarios antes mencionados; y no de cual sea la manera más óptima y eficiente de llevar esto a cabo.

2.2.4. Arquitectura a utilizar en la solución

Por último, señalaremos la arquitectura que se utilizará en la solución planteada, describiendo cada uno de sus elementos así como la operación de todos estos dentro del sistema.

La arquitectura de la solución estará basada en 05 elementos principales: el autenticador (*access point*), el servidor de autenticación FreeRADIUS, el servidor de directorio de usuarios OpenLDAP, el servidor de base de datos MySQL y el servidor de gestión Web del sistema.

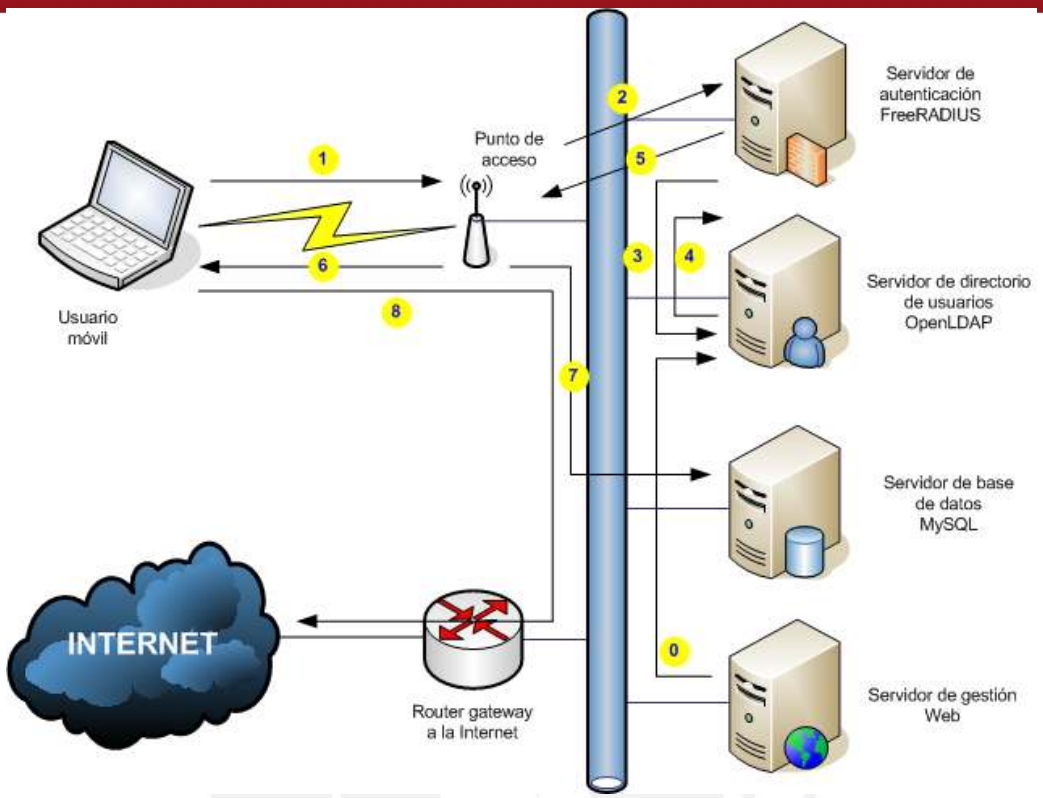

Figura 2.1 – Arquitectura de la solución

A continuación pasaremos a describir las funciones que realizará cada uno de los elementos de la arquitectura propuesta en la solución:

- *Access Point* (punto de acceso inalámbrico): Para los propósitos de esta tesis, el AP además de brindar la cobertura necesaria para que los usuarios móviles puedan conectarse a la red, actuará como el autenticador de ésta. Así, el AP se encargará de recibir las solicitudes de conexión a la red inalámbrica por parte de los usuarios y de retransmitirla al servidor de autenticación, el cual de acuerdo a como haya sido configurado, validará si es que dicho usuario cuenta con el permiso necesario para poder acceder a la red. De ser así, se lo notificará al autenticador para que inicie una sesión con el usuario

móvil, le brinde acceso cifrando la información con el mecanismo de cifrado que se haya configurado en él y por último iniciará a tomar la estadística por parte de dicho usuario; llevando la cuenta de cuantos paquetes ha descargado, cuantos ha enviado, la fecha y hora en la que inició y finalizó su sesión, el tiempo que estuvo conectado a la red, la dirección MAC del usuario móvil y la suya propia. Toda esta información se la enviará al servidor de autenticación, el cual bajo la configuración que se le haya aplicado, la guardará en el lugar correspondiente. Para esta tesis se ha decidido que sea en una base de datos desde la cual se podrá acceder desde el servidor de gestión Web para poder visualizar las estadísticas del sistema por cada usuario.

- Servidor de autenticación: Es el cerebro de toda la solución. Por medio de él se gestiona la autenticación, autorización y contabilidad del sistema; ya que él es quien recibe las solicitudes reenviadas de los puntos de acceso por parte de los usuarios móviles y le solicita al servidor de directorio de usuarios la información correspondiente para poder validar si es que dicho usuario cuenta con los permisos necesarios para acceder a la red (es decir, que la información de usuario/contraseña que ha enviado sea válida). De encontrar que es correcta le envía un mensaje al AP de “acceso autorizado” para que éste tome el control del acceso al usuario y continúe con el resto de la comunicación. Luego, recibirá periódicamente la información suministrada por el AP correspondiente a las estadísticas respecto al usuario móvil y las reenviará a una base de datos, donde serán

almacenadas para su posterior análisis; pudiendo ser visualizadas desde la consola de administración Web que se contempla dentro de toda la arquitectura.

- Servidor de directorio de usuarios: En él se registrarán a todos los usuarios que cuenten con el permiso de acceder al sistema. Se guardará información básica por cada usuario; teniendo desde su nombre de usuario, contraseña, nombres y apellidos y dirección de correo electrónico. Así mismo, es posible poder ampliar estos datos para poder almacenar datos adicionales tales como su edad, fecha de nacimiento, dirección postal, ciudad/país de residencia, área a la que pertenece dentro de la empresa, cargo que desempeña, etc.; ya que todos estos datos se encuentran contemplado dentro de los estándares de la familia X.500 en los cuales se definen las características de los servicios de directorio.
- Servidor de base de datos: Llevará a cabo la contabilidad del sistema. Es decir, dentro de él se almacenarán todos los datos suficientes para poder obtener las estadísticas del sistema por cada usuario; pudiendo conocer cuanto tiempo se ha encontrado conectado, que día y a que hora se conectó, cuando terminó su sesión, el punto de acceso desde el cual se conectó, entre otros datos ya mencionados anteriormente. Así, por medio de este servidor se podrán conocer los hábitos de conexión a la red inalámbrica por cada usuario; pudiendo así tomar las acciones correspondientes. Adicionalmente, se podría realizar la tarificación por cada usuario por haber hecho uso del sistema; orientando así la solución para mercados comerciales. El desarrollo

de este módulo se propone al final de esta tesis dentro de las recomendaciones de trabajos a futuro.

- Servidor de gestión Web: Este servidor ofrecerá al administrador de la red una interfaz Web de fácil uso con la que podrá llevar a cabo la administración de todo el sistema; pudiendo por medio de ella agregar nuevos usuarios al sistema, editar la información básica correspondiente a cada usuario, reestablecer su contraseña, mostrar una lista con todos los usuarios del sistema así como las estadísticas por cada uno de éstos.
- Usuario móvil: Para propósitos de este trabajo, puede considerarse al usuario móvil como un sexto elemento de la arquitectura de la solución. Aunque no forme parte exclusiva de ésta, el usuario móvil es el propósito de toda esta tesis, ya que a éste es a quien se le debe de suministrar de un acceso seguro para así no comprometer la confidencialidad de su información. Se encargará de iniciar la comunicación con el punto de acceso y requerirá contar con una configuración previa para poder acceder al sistema (como es el mecanismo de autenticación que se utilizará para conectarse a la red: WPA2 Enterprise; especificando que deberá suministrar un par de usuario/contraseña para ello bajo un túnel TLS con mecanismo PEAP).

Así mismo, a continuación procedemos a explicar la secuencia del procedimiento por el cual un usuario se conecta a la red inalámbrica, contemplando la arquitectura de la solución mostrada en la figura 2.1:

1. Un usuario móvil ingresa al área de cobertura del AP, inicia una sesión y envía sus credenciales (par usuario y contraseña).
2. El punto de acceso recibe las credenciales del usuario móvil y las reenvía al servidor de autenticación (FreeRADIUS) para que le indique si éstos son válidos y de ser así, le brinde acceso a la red inalámbrica. Caso contrario, impide su acceso y le envía un mensaje de falla de autenticación.
3. El servidor de autenticación recibe la solicitud por parte del AP, verifica que se encuentre registrado como un NAS (*Network Access Server*) autorizado para brindar accesos a la red (mediante una llave compartida entre el AP y el servidor) y de ser estos correctos, inicia una sesión con el servidor de directorio de usuarios (OpenLDAP) para enviarle los datos correspondientes al usuario y éste le indique si son correctos de acuerdo a sus registros.
4. El servidor de directorio de usuarios revisa si es que se encuentra registrado el usuario en su sistema y de ser así, procede a verificar si la contraseña ingresada es correcta. En caso que el usuario no se encuentre registrado, envía un mensaje de *Access-Rejected* (acceso rechazado). De ser correcto, devuelve un mensaje de *Access-Accepted* (acceso aceptado); por medio del cual se concede el acceso al usuario.
5. El servidor de autenticación recibe la autorización por parte del servidor de directorio de usuarios y envía un mensaje al AP para que le brinde acceso a la red al usuario.

6. El AP recibe la autorización para el usuario móvil e inicia una sesión WPA2 de intercambio dinámico de llaves, por medio del cual se procederá a utilizar el algoritmo AES para cifrar la comunicación de datos entre el usuario móvil y el AP.
7. Al momento de recibir la autorización, el AP inicia a registrar todas las actividades de tráfico del usuario y las envía al servidor de base de datos MySQL. En este servidor se registra el momento exacto en el que el usuario inicia su acceso a la red y se registrará el tiempo que estuvo conectado, el momento en el que se desconecta, así como otras estadísticas (número de *bytes* enviados, número de *bytes* recibidos, entre otros).
8. Una vez que el usuario cuenta con acceso a la red inalámbrica (y con ello, a la red Ethernet cableada), iniciará una sesión DHCP para obtener dinámicamente una dirección IP por parte del *router gateway* y así con estos datos poder salir a la Internet.

Adicionalmente, en el ***anexo #09*** se podrá encontrar una captura de tramas realizada con el analizador de protocolos Wireshark [9], en la cual se ha logrado capturar el intercambio de tramas entre el AP, el servidor de autenticación y el servidor de directorio de usuarios en el momento en el cual un usuario solicita conectarse a la red inalámbrica.

Capítulo 3: Diseño de la solución

3.1. Diagrama de flujo del sistema

En el anexo #2 se presentan los diagramas de flujo para los dos principales procesos que se realizará en la solución planteada. A continuación pasaremos a explicar cada paso para ambos procesos.

En el primer proceso, denominado “Conexión de un usuario móvil a la red inalámbrica” se explica el flujo de operaciones que se realizan desde el momento en el que un cliente intenta acceder a la red inalámbrica hasta el acceso concedido a dicho usuario. Para ello, se inicia con la aparición del cliente inalámbrico dentro del área de cobertura de la red inalámbrica (pudiendo el AP ser capaz de reconocerlo y empezar a intercambiar información). Luego, el cliente identifica a la red inalámbrica como una posible red a la que puede acceder e intenta conectarse a ella. Para ello, el equipo de dicho usuario se comunica con el AP y lo primero que realiza es la asociación a dicho punto de acceso. Una vez realizado esto, se inicia la

sesión 802.1X con el cliente, solicitándole su nombre de usuario y contraseña. El cliente ingresa estos datos y éstos viajan por el aire (cabe señalar que si bien el nombre de usuario viaja sin protección, la contraseña en cambio es cifrada por las llaves anteriormente intercambiadas entre estos equipos). El AP recibe esta información y la reenvía al servidor de autenticación RADIUS para el cual haya sido configurado. El servidor de autenticación RADIUS recibe esta información y la valida con el servidor de directorio de usuario LDAP para el que haya sido configurado. En el servidor LDAP se tiene una relación de todos los usuarios a los cuales se les tiene permitido el acceso a la red, así como sus respectivas contraseñas (todas éstas se encuentran almacenadas cifradas dentro de este servidor). El servidor LDAP verifica si la información es válida o no y le brinda una respuesta al servidor de autenticación. De ser válida, el servidor de autenticación envía un mensaje al AP concediendo el acceso al nuevo usuario a la red y éste inicia una conversación con el AP para establecer el cifrado con el que se haya configurado usar el WPA2 (siendo AES el cifrado recomendando al ser más fuerte y difícil de romper). Así mismo, el punto de acceso iniciará a recolectar los datos de la sesión correspondientes para dicho usuario y enviará dicha información al servidor de autenticación, el cual la reenviará al servidor de base de datos para ser almacenada. De ser inválida la información, el servidor de autenticación informa al AP que dicho usuario no está autorizado a acceder a la red y éste envía un mensaje de error al cliente.

En el segundo proceso, denominado “Acceso de un cliente a la Internet” se explica el flujo de operaciones que se realizaría de contar con un servidor

Web *Proxy* como fue mencionado anteriormente. Desde el momento en el que un cliente intenta acceder a la Internet hasta el acceso concedido a dicho usuario. Para ello, se inicia con la ejecución de algún explorador Web (*Web browser*) desde el equipo del cliente. La solicitud llega al servidor Web *proxy*, el cual solicita al cliente que ingrese su nombre de usuario y contraseña correspondiente. El servidor recibe esta información y la valida de igual forma que hacía el servidor RADIUS en el proceso anterior, conectándose con el servidor LDAP. Luego de verificar que la información suministrada es correcta, el servidor Web *Proxy* identifica el ancho de banda disponible para dicho usuario y reenvía la petición a la Internet. Luego, el servidor recibe la respuesta a la solicitud enviada y la reenvía al cliente. Desde este momento, el servidor Web *proxy* gestionará el ancho de banda de dicho usuario hacia la Internet; procurando así que un usuario no sature todo el enlace de acceso a la Web, dejando a los demás usuarios de la red sin recursos. En el caso de que la información suministrada sea incorrecta, el servidor Web *proxy* enviará un mensaje de error al cliente y le denegará el acceso a la Web.

3.2. Diseño de la arquitectura de la solución

Procederemos a describir el diseño de la arquitectura de la solución propuesta mediante el gráfico que se muestra a continuación:

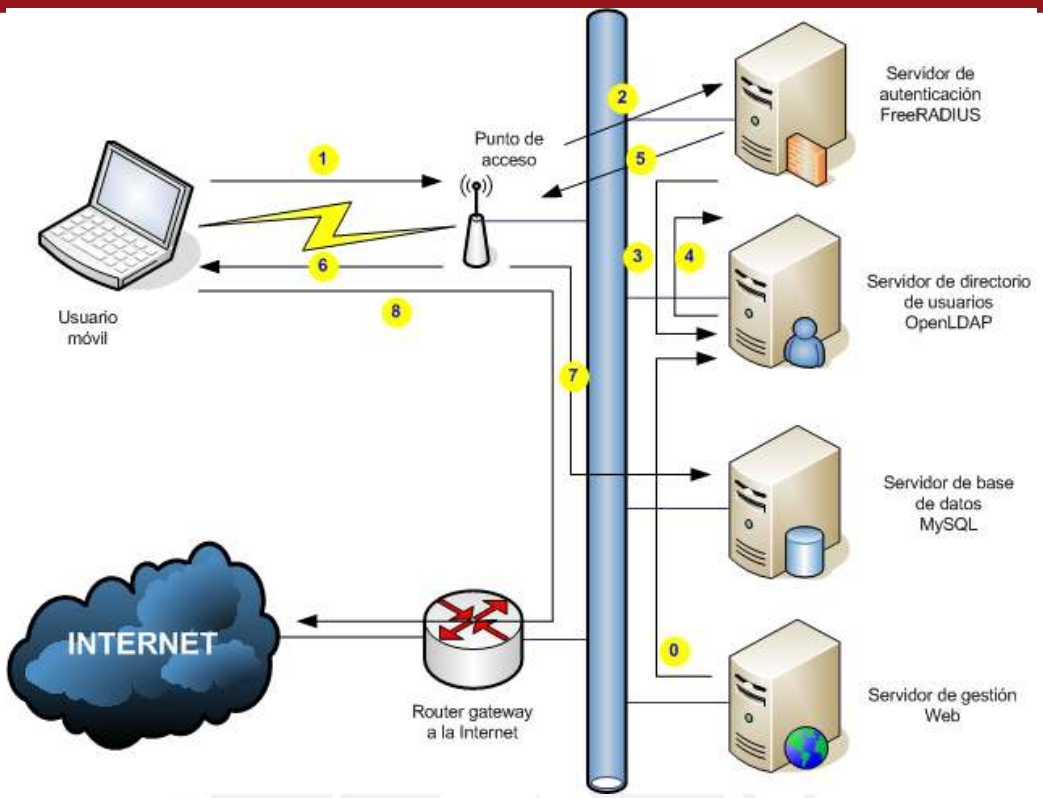

Figura 3.1 – Arquitectura de la solución

Para el diseño de la arquitectura de la solución propuesta se ha tenido en cuenta las consideraciones vistas dentro del marco teórico de esta tesis, asegurando así un óptimo grado de seguridad en la comunicación entre el cliente móvil y el punto de acceso; dado que este lugar es el más vulnerable de toda la solución al poder estar siendo vigilado por posibles intrusos al sistema. Así, se brinda un acceso seguro, tanto para los clientes móviles que se conecten a la red como para la red misma; ya que se impide que usuarios ajenos al sistema puedan interpretar la información que envían los clientes móviles, así como impedir que éstos puedan acceder a la red y por ello acceder a los recursos privados de ésta.

Capítulo 4: Implementación de la solución

Para la implementación de la solución se debe de recordar que se realizará a manera prototipo (piloto) como se ha mencionado anteriormente y se contempla dentro de los alcances de la tesis; buscando que dicho prototipo cumpla con las metas propuestas a lo largo de esta tesis a manera funcional; es decir, que cumpla con realizar las funciones u operaciones planteadas sin buscar necesariamente presentar un acabado final.

Teniendo en cuenta lo anterior, pasaremos a explicar detalladamente la implementación de la solución propuesta.

4.1. Implementación de un prototipo

La implementación de un prototipo de la solución planteada contempla el diseño descrito en el capítulo anterior. De tal forma, podemos dividir la implementación del prototipo en 06 etapas:

- Primera etapa: Implementación del servidor FreeRADIUS
- Segunda etapa: Implementación del servidor OpenLDAP
- Tercera etapa: Implementación del servidor MySQL
- Cuarta etapa: Implementación del servidor de gestión Web
- Quinta etapa: Configuración de los puntos de acceso
- Sexta etapa: Configuración de los usuarios móviles

Cabe recordar que la implementación del prototipo se basará sobre soluciones libres (*software* libre); para el cual una de sus grandes ventajas es que nos permite poder acceder al código para poder modificarlo de acuerdo a nuestras necesidades y así ser capaces de amoldarlo a la solución más óptima posible. Para este caso, se ha decidido utilizar como plataforma al sistema operativo Ubuntu para servidores, en su versión 6.06 LTS al contar éste con soporte por parte del fabricante hasta el año 2011 (por ello las siglas LTS que en inglés significan Long Term Support o Soporte a Largo Plazo).

Así, pasaremos a explicar la manera en la que se realizó la implementación de cada etapa.

4.1.1. Implementación del servidor FreeRADIUS

FreeRADIUS es una implementación en software libre de RADIUS y se caracteriza por soportar múltiples mecanismos de autenticación, tales como PAP, CHAP, MD5, EAP, etc. Para la implementación se ha elegido el mecanismo de autenticación PEAP. La autenticación PEAP viene instalada

en los equipos que cuenten con el sistema operativo MS Windows XP SP2. Al tratarse de una empresa en la que todos los *notebooks* de los usuarios móviles cuentan con dicho sistema operativo, se elige la autenticación PEAP como una opción segura y rápida de implementar (al no requerir la instalación de programas adicionales en los equipos como se hubiese requerido si es que se hubiera utilizado otros mecanismos de autenticación tales como EAP-TLS, EAP-TTLS, EAP-MD5, etc.).

Lo primero a analizar es la manera de instalación del servidor FreeRADIUS. Al tratarse de una plataforma como la de Ubuntu, nos permite realizarlo de dos maneras: o bien descargando el archivo precompilado e instalarlo (opción utilizando al comando *apt-get* con el parámetro *install*, por ejemplo: #apt-get install freeradius) o descargar el código fuente (por ejemplo: con el comando wget: #wget ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.0.3.tar.bz2), modificarlo de acuerdo a las funcionalidades que deseamos tener, prepararlo (#./configure), compilarlo y por último instalarlo (#make y #make install). Se ha elegido la segunda opción porque requerimos realizar una modificación en el código fuente para poder habilitar la funcionalidad del FreeRADIUS para que trabaje con los servidores OpenLDAP y MySQL para realizar la autenticación de los usuarios y llevar a cabo la contabilidad del sistema, respectivamente.

En el anexo #3 se muestran todas los scripts que implican la implementación de todos estos procesos.

Luego, se procede con modificar los archivos de configuración de FreeRADIUS. Estos son principalmente 04 archivos, todos ubicados en la carpeta /etc/freeradius:

- radiusd.conf
- eap.conf
- clients.conf
- sql.conf
- ldap.attrmap

La configuración final de estos archivos se muestra igualmente en el anexo #3.

Una vez realizado todos estos pasos procedemos a poner en marcha el servicio de FreeRADIUS dentro del servidor utilizando el siguiente comando:

```
#service freeradius start
```

En el caso en que se desee iniciar el proceso en modo de depuración (*debug*), puede utilizarse el siguiente comando:

```
#/usr/sbin/freeradius -x -f
```

4.1.2. Implementación del servidor OpenLDAP

OpenLDAP es una implementación en software libre del protocolo LDAP (*Lightweight Directory Access Protocol*), utilizado muchas veces para la administración de usuarios en una red IP mediante servicios de directorio.

De igual forma que con el servidor FreeRADIUS, podemos instalar OpenLDAP de dos maneras: mediante el archivo precompilado o descargando el código fuente. Sin embargo, podemos instalarlo mediante el archivo precompilado, ya que no requerimos realizar ninguna modificación especial.

Luego de haber instalado OpenLDAP se procede con instalar una aplicación que ayudará en su gestión: phpldapadmin. Mediante dicha aplicación será posible gestionar por una sencilla interfaz Web todo lo referente al servidor OpenLDAP; desde la creación del dominio hasta la creación y configuración de los usuarios. Esto simplificará la configuración del servidor; especialmente con el único archivo de configuración con el que se trabajará: slapd.conf.

Una vez concluida la instalación de estas dos aplicaciones, se requiere la instalación de un servidor Samba integrado al servidor OpenLDAP. Este servidor permitirá la comunicación entre los clientes de dominio de Windows y el servidor OpenLDAP al momento de realizar la autenticación del cliente móvil.

En el anexo #4 se pueden encontrar los detalles de la implementación y configuración de estos dos servicios; indicando los comandos utilizados y las respectivas capturas de pantalla al momento de realizar todo esto.

4.1.3. Implementación del servidor MySQL

De igual forma que con los anteriores servidores, podemos instalar MySQL de dos maneras: mediante el archivo precompilado o descargando el código fuente. Sin embargo, podemos instalarlo mediante el archivo precompilado, ya que no requerimos realizar ninguna modificación especial.

Una vez instalado el servicio, procederemos a crear una tabla en la que llevaremos a cabo todo el registro de accesos de los usuarios de la red inalámbrica. Para ello, crearemos antes el esquema de trabajo “radius” y

dentro de este esquema crearemos la tabla “radacct” con los siguientes campos:

- AcctSessionId
- AcctUniqueId
- UserName
- Realm
- NASIPAddress
- NASPortId
- NASPortType
- AcctStartTime
- AcctStopTime
- AcctSessionTime
- AcctAuthentic
- ConnectInfo_start
- ConnectInfo_stop
- AcctInputOctets
- AcctOutputOctets
- CalledStationId
- CallingStationId
- AcctTerminateCause
- ServiceType
- FramedProtocol
- FramedIPAddress
- AcctStartDelay

- AcctStopDelay
- XAscendSessionSvrKey

De todos estos campos, pasaremos a explicar a continuación los que se utilizarán para almacenar información del usuario:

- AcctUniqueId: Identificador único por cada sesión iniciada de accounting entre el servidor de autenticación y el de base de datos.
- UserName: El nombre de usuario registrado por el sistema y que ha hecho acceso a la red inalámbrica.
- NASIPAddress: Dirección IP del punto de acceso inalámbrico desde el cual el usuario ha accedido a la red.
- AcctStartTime: Fecha y hora en la que el usuario ha iniciado su acceso a la red. El formato de la fecha es el siguiente: aaaa-mm-dd; teniendo por aaaa el año, mm el mes y dd el día. Mientras que el formato de la hora es el siguiente: hh:mm:ss, teniendo por hh la hora, mm el minuto y ss el segundo.
- AcctStopTime: Fecha y hora en la que el usuario ha finalizado su acceso a la red. Los formatos de la fecha y hora son los mismos que los de AcctStartTime.
- AcctSessionTime: Campo en el que se registra el tiempo que estuvo conectado el cliente a la red. Se contabiliza en segundos.
- AcctInputOctets: Número de octetos (bytes) que el usuario ha enviado hacia el punto de acceso, o también conocido como el tráfico de subida del usuario.

- AcctOutputOctets: Número de octetos (bytes) que el usuario ha recibido del punto de acceso, o también conocido como el tráfico de bajada o descargado del usuario.
- CalledStationId: La dirección MAC y el SSID registrados en el punto de acceso por el cual el usuario ha accedido a la red. El formato en el que se guarda la información es el siguiente: aa-bb-cc-dd-ee-ff:ssid, para el cual el primer parámetro representa la dirección MAC del AP y el segundo el identificador (essid) de la red inalámbrica a la que accedió el usuario.
- CallingStationId: La dirección MAC del equipo desde el cual el usuario ha accedido a la red. El formato es el mismo al anteriormente descrito.
- AcctTerminateCause: La causa por la cual se finalizó de contabilizar y se terminó la conexión del usuario a la red inalámbrica. Se pueden tener dos posibles causas: NAS-Request (a solicitud del AP), o Lost-Carrier. El primer caso se suele dar cuando el usuario ha terminado la conexión, ya sea cerrándola manualmente o apagando su equipo; mientras que el segundo caso se da cuando el usuario ha dejado el área de cobertura del AP.
- AcctStartDelay: Registra si es que ocurrió algún retraso en atender un inicio de contabilizar una sesión. El tiempo que retraso que hubo se almacena en segundos.
- AcctStopDelay: Registra si es que ocurrió algún retraso en atender un fin de contabilizar una sesión. El tiempo que retraso que hubo se almacena en segundos.

En el anexo #5 se puede encontrar información más detallada de la implementación del servidor MySQL como los scripts utilizados para ello y la configuración final.

4.1.4. Implementación del servidor de gestión Web

Para el servidor de gestión Web se contempla la implementación de dos servicios: el servidor Web Apache y el complemento para procesar páginas PHP por parte de dicho servidor.

De igual forma que con los anteriores servidores, podemos instalar el servidor de gestión Web de dos maneras: mediante el archivo precompilado o descargando el código fuente. Sin embargo, podemos instalarlo mediante el archivo precompilado, ya que no requerimos realizar ninguna modificación especial.

Dentro del servidor de gestión Web, luego de haber instalado los servicios correspondientes, se crearon 15 páginas Web PHP por medio de las cuales se puede realizar la gestión del sistema. A continuación indicamos los nombres de dichas páginas Web PHP y su función correspondiente:

- agregar.php: Contiene el algoritmo para crear un nuevo usuario en el sistema. Obtiene de la sesión los datos necesarios para ello. De ser válida la acción la realiza y le muestra un mensaje de aceptación al administrador. De ser inválida la acción, no la realiza y muestra un mensaje de error al administrador.

- agregar_form.php: Página Web que contiene el formulario en el que se le solicita al administrador los datos necesarios para crear un nuevo usuario en el sistema, los sube a la sesión e invoca a agregar.php para que continúe con la tarea.
- consulta.php: En ella se muestran todos los datos contenidos en la base de datos correspondientes a la información que se ha registrado de los usuarios que han accedido al sistema; pudiendo apreciar toda esa información vía Web.
- eliminar.php: Contiene el algoritmo para eliminar un usuario del sistema. Obtiene de la sesión los datos necesarios para ello (nombre del usuario a eliminar). De ser válida la acción la realiza y le muestra un mensaje de aceptación al administrador. De ser inválida la acción, no la realiza y muestra un mensaje de error al administrador.
- eliminar_form.php: Página Web que contiene el formulario en el que se le solicita al administrador los datos necesarios para eliminar un usuario en el sistema (solo se solicita el nombre identificador de dicho usuario), los sube a la sesión e invoca a eliminar.php para que continúe con la tarea.
- index.php: Página de bienvenida para el administrador del sistema en la que encontrará los enlaces para realizar todas las tareas que le permite el sistema (agregar, modificar y eliminar usuarios, ver los accesos realizados, etc.). A esta página Web (así como a todas las aquí mencionadas) pueden ser accedidas solamente si es que el usuario se ha autenticado previamente en la página de ingreso al

sistema (login.php); de lo contrario le aparecerá que no lo ha hecho y se le negará el acceso.

- invalido.php: Página Web que aparecerá al usuario que no haya sido validado por el sistema al momento de registrarse por login.php y/o haya incurrido en algún error general del sistema.
- login.php: Página Web que sirve para autenticar al administrador del sistema y le sirve para poder ingresar al resto de páginas Web para realizar las tareas de gestión del mismo. Toma la información suministrada en el formulario de esta página Web (usuario y contraseña) y la sube a la sesión para que pueda ser validada luego por el algoritmo desarrollado en valida.php y tome las medidas correspondientes.
- modificar.php: Contiene el algoritmo para modificar los datos de un usuario del sistema. Obtiene de la sesión los datos necesarios para ello (nombre de identificador del usuario, nombres, apellidos, correo electrónico del usuario, etc.). De ser válida la acción la realiza y le muestra un mensaje de aceptación al administrador. De ser inválida la acción, no la realiza y muestra un mensaje de error al administrador.
- modificar_form.php: Página Web que contiene el formulario en el que se le solicita al administrador la información necesaria para modificar los datos de un usuario del sistema, los sube a la sesión e invoca a modificar.php para que continúe con la tarea.
- reestablecer.php: Contiene el algoritmo para reestablecer la contraseña de un usuario del sistema. Obtiene de la sesión los datos necesarios para ello (nombre de identificador del usuario y nueva

contraseña del usuario). De ser válida la acción la realiza y le muestra un mensaje de aceptación al administrador. De ser inválida la acción, no la realiza y muestra un mensaje de error al administrador.

- reestablecer_form.php: Página Web que contiene el formulario en el que se le solicita al administrador la información necesaria para reestablecer la contraseña de un usuario del sistema, los sube a la sesión e invoca a reestablecer.php para que continúe con la tarea.
- valida.php: Página Web que realiza una validación mediante el nombre de usuario y contraseña suministrados a la sesión por parte de login.php y verifica que éstos sean los del administrador del sistema. De ser así, le brinda la bienvenida y le permite el acceso al resto de páginas Web del sistema de gestión. De lo contrario, le niega el acceso y le indica que los datos no son válidos.
- ver_registro.php: Página Web que muestra todas las estadísticas de accesos al sistema por parte de lo usuarios. Se muestran todos los campos válidos de la base de datos MySQL mencionados en la implementación de ésta, en una página Web de fácil visualización.
- ver_usuarios.php: Página Web que muestra la relación de usuarios registrados en el sistema, así como la información básica proporcionada al momento de registrarlos.

En el ***anexo #6*** se puede encontrar mayor información sobre la implementación del servidor de gestión Web; como la instalación de los servicios de apache y php, así como el contenido de las páginas Web en PHP.

4.1.5. Configuración de los puntos de acceso

Para esta sección se ha utilizado como puntos de acceso de pruebas al Linksys WRT54g y al Zyxel Prestige 660HW-T1. En el anexo #7 se podrán encontrar las capturas de pantalla correspondiente a la configuración de dichos equipos (ya que la administración de estos es vía Web) para que opere de acuerdo a la arquitectura de la solución presentada.

4.1.6. Configuración de los usuarios móviles

La configuración de los clientes móviles se muestra en el anexo #8, mediante la implementación de un “Manual de configuración para usuarios móviles”. En este manual los usuarios encontrarán todos los pasos que deberán de realizar en sus *notebooks* para configurarlas y poder conectarse de manera segura a la red inalámbrica.

Capítulo 5: Análisis costo-beneficio de la solución

La intención de realizar un análisis costo-beneficio dentro de esta tesis trae consigo el poder identificar cuales características traen consigo los distintos equipos (puntos de acceso) y de acuerdo a estas características poder reconocer cuales de éstas aportan un beneficio significativo para la solución y cuanto sería la diferencia en costos con respecto a la que no lo tenga.

Así, podemos encontrar varios equipos Wi-Fi en el mercado; para los cuales hemos tenido la oportunidad de analizar hasta 03 diferentes equipos: Zyxel Prestige 660HW-T1, Linksys WRT54G, D-Link DWL-3200AP.

A continuación, pasaremos a detallar el análisis costo-beneficio que se realizó con estos tres equipos, mostrando primero una tabla de comparaciones de acuerdo a sus especificaciones técnicas y luego pasando a presentar una explicación en la que se indicará para cuales escenarios cada uno de los equipos se ubicaría mejor.

Característica	Zyxel Prestige 660HW-T1	Linksys WRT54G	D-Link DWL-3200AP
Precio local (US$)	30-45	80-120	160-210
Estándares	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b	IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b	IEEE 802.3, IEEE 802.3u, IEEE 802.3af, IEEE 802.11g, IEEE 802.11b
Número de puertos Fast Ethernet	4	4+1	1
Máxima potencia de transmisión (dBm)	16	18	21
Ganancia de antena (dBi)	2	2	5
Máximo EIRP (dBm)	18	20	26
Seguridad Inalámbrica	WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise WEP Lista de control de acceso por direcciones MAC Cifrado WEP de 64/128/256 bits	WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise Cifrado WEP de 64/128 bits Lista de control de acceso por direcciones MAC	WPA-Personal WPA-Enterprise WPA2-Personal WPA2-Enterprise 64/128/152-bit WEP Deshabilitación de broadcast de SSID Detección de Rogue AP Lista de control de acceso por direcciones MAC Configuración de seguridad aislada para cada SSID
Capacidades de RADIUS	Autenticación y Accounting	Autenticación	Autenticación y Accounting
Modos de operación	AP ADSL Router	AP Router Firewall (DMZ)	AP WDS con AP WDS/Bridge
Soporta VLAN	No	No	Sí
Máximo número de usuarios simultáneos	6 - 8	12 - 14	16 - 18
Administración	Interfaz Web HTTP Telnet	Interfaz Web HTTP Secure HTTP (HTTPS) UPnP	Interfaz Web HTTP Secure HTTP (HTTPS) AP Manager II Soporta SNMPv3 D-View Module Private MIB Interfaz por línea de comandos Telnet Secure (SSH) Telnet
Garantía (años)	N.E.	3	1

Tabla 5.1 – Resumen comparativo entre distintos equipos inalámbricos

5.1. Zyxel Prestige 660HW-T1

El Zyxel Prestige 660HW-T1 es un ADSL Router con funcionalidades de AP que le permite aparecer como el más económico de los tres equipos analizados. Suele ser configurado principalmente para brindar de acceso vía ADSL a la Internet por los proveedores de Internet a manera de CPE (*Customer Premises Equipment*). Permite ser configurado de dos maneras: vía Web (solo HTTP, no HTTPS) o vía Telnet y ofrece todos los modos de WPA y WPA2 (PSK y Enterprise para ambos casos).

Si bien este equipo es bastante económico, se recomienda su uso solamente para redes muy pequeñas, tanto de cobertura como de número de usuarios a soportar; ya que este equipo presenta una potencia de transmisión muy baja (apenas 16 dBm) y su antena fija con 2dBi de ganancia no le permite ofrecer un área de cobertura muy grande en interiores (solo le permite atravesar una pared, a la segunda pared ya la señal llega muy débil y la conexión se vuelve errática). Así también, no soporta más que 6 a 8 usuarios conectados en simultáneo al equipo y que todos se encuentren generando tráfico constante. Sin embargo, a pesar de sus limitaciones, permite trabajar con un servidor RADIUs tanto para realizar la autenticación de usuarios como el *accounting* (contabilidad) de éstos.

5.2. Linksys WRT54G

El Linksys WRT54G es un *wireless router* con capacidad de *firewall* (soporte de SPI o *Stateful Packet Inspection*). Cuenta con una mayor potencia de transmisión que el equipo anterior, logrando poder atravesar más obstáculos

y brindar así un área de cobertura mayor. Si bien este equipo cuesta poco más del doble que el equipo anterior, su capacidad de poder manejar un mayor número de usuarios simultáneos y brindar una mayor cobertura lo hacen una buena opción para redes medianas. Sin embargo, su incapacidad de reportar la contabilidad de los accesos hacia un servidor RADIUS hace que se tome como una gran desventaja que juega en su contra. Lamentablemente, el *firmware* con el que viene de fábrica no le permite realizar dicha tarea.

Adicionalmente, el acceso vía Web con HTTPS es una característica adicional que aporta una capa de seguridad en la administración del sistema,

5.2.1. DD-WRT v24

Se mencionó anteriormente que una de las limitaciones del equipo resultaba ser el *firmware* que trae de fábrica. El equipo ofrece la capacidad de poder actualizar su *firmware* por otros que saque la compañía que lo realizó. Sin embargo, el trabajo arduo de una comunidad denominada DD-WRT permitió obtener un *firmware* válido para poder cambiar por el de fábrica. Dicho *firmware* se encuentra basado en Linux y con ello le permite al equipo poder habilitar muchos de los servicios de red que se pueden obtener con Linux; logrando así contar con un equipo mucho más robusto y con muchas más funcionalidades que el original. A continuación se presentan algunos de los servicios que integra el uso de este *firmware*:

- Access Restrictions
- Afterburner (AKA Speedbooster)

- Chillispot hotspot
- Client Mode Wireless
- CRON
- DDNS
- DNSMasq as DHCP server
- Firewall
- Firewall Builder
- HotSpot HTTP Redirect
- NoCatSplash
- Obtaining an Unknown Router IP Address
- OpenDNS
- Port Blocking
- Port Forwarding
- Quality of Service (QoS)
- Samba Filesystem
- SNMP
- Spanning Tree Protocol
- SSH access from internet
- Static DHCP
- Telnet/SSH and the Command Line
- Configuration settings for UMA enabled phones
- URL - Keyword blocking (Access Restrictions)
- USB Support (USB)
- Use switched ports outside the router
- Useful Scripts

- VLAN Configuration
- Wake On Lan (WOL)
- Wireless Access Point
- Repeater Bridge
- Wireless Bridge
- WL command help
- WMM Support

De esta manera, podemos concluir que, si bien el equipo WRT54G por sí solo es un equipo que ofrece ciertas características que mejoran por muy poco al equipo visto anteriormente, con el cambio de firmware se vuelve una poderosa herramienta capaz de ser comparado con equipos de mucho mayor costo al contar con mucho más funcionalidades. Sin embargo, algo que no podrá modificarse será la potencia máxima de transmisión que ofrece el equipo, limitación del *hardware* de éste.

5.3. D-Link DWL-3200AP

El D-Link DWL-3200AP es el equipo con mayor potencia de transmisión que se ha podido probar para los propósitos de esta tesis. Con sus 21 dBm de potencia de transmisión y sus 5 dBi de ganancia en sus antenas duales reemplazables (utilizan conectores BNC) le permiten aparecer como el equipo de más alto rango de los tres que se han analizado. Logra una amplia cobertura en interiores, llegando incluso a brindar cobertura hasta en dos pisos y soportando una gran cantidad de usuarios simultáneos. Además, las funcionalidades con las que cuenta como el soporte de VLAN, detección de

rogue APs y soporte de gestión vía SNMPv3 representan una gran ventaja frente a las demás opciones. Así mismo, cuenta con soporte para autenticación y contabilidad con RADIUS. Este equipo resulta de gran ventaja para redes grandes y con una gran cantidad de usuarios.

Conclusiones

Tras haber logrado la implementación de un prototipo para la solución planteada, se ha podido llegar a las siguientes conclusiones:

- Es posible la integración de todas las herramientas de software libre utilizadas en la presente tesis (FreeRADIUS, OpenLDAP, SAMBA, MySQL) con un dominio desarrollado con Microsoft Windows. Es decir, en el caso de que se le desee implementar en una red ya existente y que utilice herramientas comerciales (tales como MS Windows 2003 Server y/o MS Active Directory) bastaría con modificar algunos parámetros en los archivos de configuración de las herramientas de software libre utilizadas para poder lograr la integración y trabajo entre todos estos.
- La implementación de este prototipo no contempla mecanismos de seguridad que aseguren ataques provenientes desde el interior de la red (la red cableada). Lo que se plantea aquí es garantizar un medio de acceso seguro entre el cliente móvil y el punto de acceso a la red (AP); más no entre éste y los elementos de la red interna (tales como servidores de correo, Web, archivos, entre otros).
- La implementación se ha optimizado para los clientes móviles que cuenten con una *notebook* con sistema operativo MS Windows XP SP2 o MS Windows Vista; ya que de acuerdo al escenario inicial planteado todos los clientes de esta organización cuentan con dicho sistema operativo. Sin embargo, también hubiese sido posible brindar soporte para clientes con otros sistemas operativos, tales como

distribuciones libres de GNU Linux (Ubuntu 6.06 Desktop Edition, CentOS, etc.). Sin embargo, lo que no se hubiese soportado es a aquellos clientes móviles con otros tipos de equipo portátiles (tales como PDAs, Pocket PC, smartphones, etc.) que no contaran con soporte de WPA2 Enterprise (como es el caso de las PDA de la marca Palm, a excepción del modelo T|X que cuenta con un *upgrade* para poder soportar esto).

Observaciones, recomendaciones y trabajos a futuro

- Durante la implementación del servidor OpenLDAP se pudo encontrar que se requería de un elemento adicional para que pueda 'conversar' éste con los clientes móviles (*notebooks* con sistema operativo MS Windows XP o Windows Vista). Fue así que, tras luego de haber investigado, se ubicó al servicio de SAMBA como una solución ideal para este problema. Integrando el servidor OpenLDAP con el servicio SAMBA pudo implementarse un dominio de usuarios para los cuales aparecería transparente y sin mayores inconvenientes para el momento de registrarse y contar con acceso a la red.

- Para una implementación final de la solución planteada se recomienda que los servidores de FreeRADIUS, OpenLDAP y Squid se ubiquen en máquinas distintas; es decir, en distinto hardware; ya que estos servidores (sobretodo el OpenLDAP y el Squid) se encontrarán en constante actividad solicitando y registrando datos. Para el caso del servidor FreeRADIUS puede observarse que no se requiere de un hardware de gama alta al ser un servidor que relega el trabajo principalmente al servidor OpenLDAP. Todo lo contrario sucede con el servidor Squid ya que mediante éste se contará con el acceso a la Internet por parte de toda la red; por lo que mientras más usuarios tenga esta red, requerirá un servidor más potente (sobretodo con una mayor cantidad de memoria RAM; recomendando que sea no

menor a 1 GB hasta para 20 usuarios, no menor a 2 GB hasta para 40 y no menor a 4 GB para un mayor número de usuarios; ya que este servidor utiliza la memoria RAM para almacenar la caché y como un punto de rápido acceso).

De acuerdo a los desarrolladores de Squid [10], una regla que debería de mantenerse siempre es la de reservar el doble de la siguiente cantidad para Squid: 10 MB de memoria RAM física por cada GB de espacio utilizado en disco por el archivo cache_dirs, más el parámetro cache_mem que se le haya asignado en el archivo de configuración squid.conf. El parámetro cache_mem suele ser aproximadamente el 12.5% del total de memoria física que se tenga. Así, si se contase con 128 MB de memoria física, entonces el parámetro cache_mem podría ser de 16 MB. Sin embargo, hay que mencionar que este parámetro depende mucho de los hábitos de los usuarios de la red (muchas páginas Web frecuentemente utilizadas).

- Como se había comentado anteriormente, un trabajo a futuro inmediato puede ser el desarrollo de un módulo de facturación (*billing*) para esta implementación. De tal manera, la solución planteado podría orientarse hacia sectores comerciales tales como aeropuertos, cafés, restaurantes, hoteles, entre otros; en los cuales se pueda ofrecer el acceso a la Internet como un servicio de valor agregado a sus clientes. Debe de observarse que el módulo de facturación debe de trabajar de la mano con el servidores de directorio LDAP y de base de datos MySQL que aquí se proponen, ya que allí es donde se

almacena toda la información de los usuarios de la red; ya sea permitiéndoles el acceso a la red (LDAP) o registrando el tiempo o consumo de descargas que hagan (MySQL).

BIBLIOGRAFÍA

[ALC2006] Alonso C., 2006, "Proteger una red Wireless", PC World Profesional Noviembre 2006, IDG, Madrid, España

[BAN2003] Baghaei N., 2003, "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients", Honours Project Report,University of Canterbury, Christchurch, New Zealand

[CHA2007] Chávez A., *"Redes de área local inalámbricas (WLAN)"*, Material del curso Ingeniería Inalámbrica, PUCP, ciclo 2007-1, Lima, Perú

[CIS2004] Cisco Systems Inc., 2004, *"Academia de Networking de Cisco Systems: Guía del segundo año. CCNA® 1 y 2 "*, Ed. Pearson Educación S.A., Madrid, España

[GAM2005] Gast M., "*802.11 Wireless Networks: The Definitive Guide*", O'Reilly 2nd Edition, 2005, California, USA

[IEE1999] IEEE Std. 802.11, "*Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*", Reaffirmed 12 June 2003, 1999, New Jersey, USA

[1] *"IEEE 802.11 – Wikipedia, the free encyclopedia"*, http://en.wikipedia.org/wiki/802.11

[2] *" IEEE 802.11 – Wikipedia, la enciclopedia libre"*, http://es.wikipedia.org/wiki/IEEE_802.11

[3] *"Unix"*, http://en.wikipedia.org/wiki/Image:Unix.svg

[4] *"Capítulo 3: Arquitectura de la solución de LAN inalámbrica segura"*, http://www.microsoft.com/latam/technet/articulos/wireless/pgch03.mspx

[5] *"Wired Equivalent Privacy"*, http://es.wikipedia.org/wiki/WEP

[6] *"The Wi-Fi Alliance"*, http://www.wi-fi.org

[7] *"Conceptos básicos, manual de MySQL"*, http://www.webestilo.com/mysql/intro.phtml

[8] *"Servidor HTTP Apache"*, http://es.wikipedia.org/wiki/Apache_http_server

[9] *"Wireshark"*, http://www.wireshark.org

[10] *"SquidFaq/SquidMemory"*, http://wiki.squid-cache.org/SquidFaq/SquidMemory

ANEXOS

Anexo 01: Diagramas físico y lógico de la solución

Anexo 02: Diagrama de flujo para una conexión de un cliente inalámbrico a la red

Diagrama de flujo para un acceso de un cliente a la Internet

Anexo 03: Archivos de configuración del servidor FreeRADIUS

Anexo 04: Archivos de configuración del servidor OpenLDAP

Anexo 05: Archivos de configuración del servidor MySQL

Anexo 06: Archivos de configuración del servidor de gestión Web y pantallas del sistema Web

Anexo 07: Configuración Web de los puntos de acceso

Anexo 08: Configuración de los usuarios móviles

Anexo 09: Captura de tramas con Wireshark

Anexo 10: Comparativa de throughputs