ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN

TELECOMUNICACIONES Y REDES

"ESTUDIO E IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD WPA2 PARA UN SISTEMA DE DISTRIBUCIÓN INALÁMBRICO PARA DAR COBERTURA A TRÁFICO DE VOZ SOBRE IP"

TESIS DE GRADO

Previa a la obtención del título de

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:

HELEN GABRIELA MIRANDA RUIZ

RIOBAMBA – ECUADOR

2010

Mi agradecimiento profundo a Dios, al Ing. Alberto Arellano e Ing. Daniel Haro por su apoyo en la realización del presente trabajo, a mis Abuelitos, mis tíos, mi madre y mi hermana, por ser los pilares en los que se sostiene mi vida.

Dedico todo mi esfuerzo en la realización de este trabajo a mis abuelitos Esthelita y Gonzalito quienes han formado mi persona día a día con su ejemplo y sabiduría, a mis tíos Efraín que desde el cielo me ha cuidado, Pepito y Luly por sus fuerzas y amor constante, a mi mamita adorada Mary y mi hermanita Aracely, mis dos motivos para vivir, para ser mejor cada día, mi ejemplo y orgullo, gratitud a Dios y la Virgen Inmaculada por haberme dado una familia que siempre ha estado junto a mí en los buenos y malos momentos de mi vida. A ellos está dedicado con toda mi alma el haber alcanzado esta meta. Los amo.

NOMBRE	FIRMA	FECHA
Ing. Iván Menes **DECANO FACULTAD DE INFORMATICA Y ELECTRÓNICA**	_____	_____
Ing. José Guerra **DIRECTOR DE ESCUELA INGENIERIA ELECTRÓNICA**	_____	_____
Ing. Alberto Arellano **DIRECTOR DE TESIS**	_____	_____
Ing. Daniel Haro **MIEMBRO DEL TRIBUNAL**	_____	_____
Lcdo. Carlos Rodríguez **DIR. DPTO. DOCUMENTACIÓN**	_____	_____
NOTA DE LA TESIS	_____	

"Yo, Helen Gabriela Miranda Ruiz, soy responsable de las ideas, doctrinas y resultados expuestos en esta Tesis de Grado; y, el patrimonio intelectual de la Tesis de Grado pertenece a la ESCUELA SUPERIOR POLITECNICA DEL CHIMBORAZO".

_____

Helen Gabriela Miranda Ruiz

ÍNDICE DE ABREVIATURAS

IEEE	Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos)
MADWIFI	Driver Atheros Multibanda para Aplicaciones Inalambricas
SSID	Service Set Identification
WEP	Protocolo de equivalencia con red cableada
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
TKIP	Temporal Key Integrity Protocol
NAS	Network Access Server
AAA	Authentication, Authorization and Accounting.
AP	Access Point
GNU	Gnu is Not Unix (Gnu No es Unix)
BSSID	Basic Service Set Identifier
DHCP	Protocolo de configuración Dinámica
EAP	Extensible Authentication Protocol
ESSID	Identificador del conjunto de servicio extendido.
MAC	Medium Access Control
MD5	Algoritmo de cálculo
OSI	Open System Interconnection
PCI	Version de una Red Inalambrica
PDA	Asistente Digital Personal

RADIUS Remote authentication Dial IN User Server

ROOT Nombre convencional de la cuanta de usuario.

SSID Service Set Identifier

WDS Sistema de Distribucion Inalámbrico

UDP Protocolo de Datagrama de Usuario

IBSS Independent Basic Service Set

ÍNDICE GENERAL

CAPÍTULO III
DISEÑO DE LA RED INALAMBRICA Y SISTEMA DE SEGURIDAD

CAPÍTULO IV
PRUEBAS DEL SISTEMA DE SEGURIDAD- 100 -

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPITULO I

MARCO METODOLOGICO

1.1 INTRODUCCION

En la actualidad el uso de redes inalámbricas se ha extendido por sus ventajas de movilidad, flexibilidad y productividad. Esta tendencia hacia las redes inalámbricas ha hecho que se las pueda encontrar en aeropuertos, campus universitarios, cafés y en ciudades que se están difundiendo rápidamente por lo que no es de extrañarse que las empresas vean en las WLANs una solución a sus necesidades de comunicación.

Sin embargo, junto con su funcionalidad y demás ventajas, este tipo de implementaciones trae consigo importantes riesgos de seguridad que afrontar, en su mayoría asociados a la inexistencia de delimitación física de forma clara, y otros más importantes asociados a la carencia de mecanismos de seguridad suficientemente fuertes que protejan el acceso a los recursos tecnológicos y a la información.

Entre las soluciones de seguridad más eficientes para el control de acceso a los recursos y la protección de la información en redes inalámbricas, se describe una de las más eficientes, la cual se basa en el uso de autenticación para el acceso a la red y en el uso de encriptación en las comunicaciones sobre este tipo de redes.

Ahora bien los medios inalámbricos han experimentado un gran crecimiento en el ámbito de las comunicaciones. Por lo tanto, es inevitable que las aplicaciones de Internet sean introducidas dentro de estos tipos de medio. Las principales aplicaciones se dirigen hacia medios de comunicación como voz sobre IP (VoIP) esta es una tecnología que hace posible que la señal de voz viaje a través de una red empleando un protocolo IP.

El tráfico de tiempo real, VoIP y videoconferencias, requiere de conectividad lo cual representa un reto en las comunicaciones inalámbricas debido a la movilidad de las estaciones. Existen varias maneras de solventar esta limitante, una de ellas puede ser mediante un sistema de distribución inalámbrico que permite la interconexión de puntos de acceso. Con lo que se obtiene una mayor área de cobertura, dentro de una misma red.

El contenido de esta tesis está estructurado en 4 capítulos, el **Capítulo I** se describen los objetivos del presente proyecto de tesis, en el **Capítulo II** se proporciona una introducción y nociones generales acerca de las Redes inalámbricas y la arquitectura 802.11, el **Capítulo III** muestra el diseño de la red inalámbrica y sistema de seguridad del proyecto, concluyendo con el **Capítulo IV** en donde se realizan todas las pruebas de conexión, usuarios y VoIP.

1.2 JUSTIFICACIÓN

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbrico en la misma red.

Un punto de acceso inalámbrico mal configurado se convierte en una puerta trasera que vulnera por completo la seguridad informática de la red. Debido a esto es necesario implementar técnicas que protejan de una forma más efectiva la seguridad en las redes.

Ahora bien el tráfico de tiempo real, VoIP requiere de conectividad lo cual representa que las comunicaciones inalámbricas tengan como característica principal la movilidad de las estaciones. Por lo que se implementará un sistema de distribución inalámbrico con lo que se obtiene una mayor área de cobertura, dentro de una misma red, se compondrá de dos puntos de acceso. Un primer punto de acceso el cual está conectado a la red ethernet. El segundo punto de acceso ampliará el área de cobertura del AP primario. Puntos de acceso que operarán sobre computadoras con un sistema operativo GNU/Linux. A las cuales, se les instalarán tarjetas inalámbricas que soportan el modo master.

En el entorno de seguridad que se utilizará en la implementación, se emplean mecanismos rigurosos que brinden confidencialidad en el trafico de VoIP.

El complemento de la autenticación, para lograr tener un entorno de seguridad riguroso, es el mecanismo de cifrado propuesto en este trabajo que es el que implementa todos los elementos que el estándar IEEE 802.11i establece como obligatorios (CCMP), el cual supone lo mejor en seguridad en estas fechas.

De esta forma el presente proyecto permitirá proveer una comunicación de tráfico de VoIP enmarcada en la privacidad, autenticidad e integridad de la información dentro de un sistema de distribución para poder dar roaming de señal inalámbrica en una extensión más amplia que la proporcionada por un solo punto de acceso.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Analizar e implementar mecanismos de seguridad WPA2 para un sistema de distribución inalámbrico, utilizando puntos de acceso basados en GNU/Linux, que permita dar roaming a tráfico VoIP en redes LAN inalámbricas.

1.3.2 OBJETIVOS ESPECÍFICOS

- Investigar la distribución de GNU/Linux en la que se diseñará el sistema que permita configurar un WDS con puntos de acceso que brinden roaming al servicio de VoIP.
- Analizar los métodos de seguridad más idóneos para implementación en redes inalámbricas, en un entorno Open Source.
- Implantar un WDS con puntos de acceso utilizando tarjetas inalámbricas comunes.

- Reducir costos al implementar una infraestructura de red LAN inalámbrica.

1.4 HIPÓTESIS

Con la implementación de mecanismos de seguridad WPA2 en el servicio de Voz sobre IP en una infraestructura de red inalámbrica distribuida mediante puntos de acceso que brinden el servicio de roaming basados en GNU/Linux, se proporcionará confidencialidad, seguridad, y autenticidad, en el servicio en la transmisión de tráfico en tiempo real VoIP.

CAPITULO II

REDES INALAMBRICAS

2.1 ARQUITECTURA 802.11

La forma elemental de crear un segmento de red 802.11 es el Basic Service Set (BSS), el cual consta sólo de un grupo de estaciones que se comunican unas con otras. La estación que se encuentra en un BSS puede comunicarse con las demás estaciones miembros del mismo BSS.

2.1.1 Independent Basic Service Set (IBSS)

Las estaciones que se encuentran en un IBSS se comunican directamente una con la otra. El IBSS se puede formar a partir de dos estaciones y suele estar formado por un número pequeño de estaciones. Es poco común encontrar redes 802.11 operando como IBSS y cuando se suele formar una es por un periodo de tiempo corto y para situaciones específicas. Debido a estos aspectos los IBSSs suelen ser mejor conocidos como redes ad hoc. La figura II.1 muestra el modo de operación de un IBSS.

Figura II.1 Modo de operación de un IBBS

2.1.2 Infrastructure Basic Service Set (Infrastructure BSS)

Para evitar confusiones con los Independent BSSs este tipo redes nunca es referido como IBSS. Este tipo de redes se distingue de los IBSSs por utilizar un punto de acceso para proporcionar comunicación entre las estaciones. Es decir, cuando una estación se desea comunicar con otra, la comunicación lleva a cabo dos saltos. Primero, la estación origen envía sus tramas al Punto de Acceso (AP, Access Point, por sus siglas en inglés). Después, el AP transmite dichas tramas a la estación destino. Este tipo de redes es conocido como redes de tipo infraestructura.

Algunas de las ventajas que tienen este tipo de redes son las siguientes:

- El área de cobertura de una red de tipo infraestructura es determinada por la distancia al punto de acceso. Por lo que no es existe una restricción entre la distancia de las propias estaciones, siempre cuando se encuentren dentro de la cobertura del AP.
- Se elimina la necesidad de que cada estación mantenga el estado de sus estaciones vecinas.

En las redes de tipo infraestructura las estaciones tienen que asociarse al punto de acceso para obtener los servicios de la red. La asociación es el proceso mediante el

cual una estación se une a una WLAN; es lógicamente equivalente al hecho de realizar una conexión a un puerto ethernet. Una estación puede estar asociada sólo con un punto de acceso a la vez.

El estándar 802.11 no establece un límite en la cantidad de estaciones asociadas a un punto de acceso. Sin embargo, en la práctica para obtener un buen rendimiento siempre se considera un límite en el número de estaciones. La figura II.2 muestra una semblanza de la forma de operación de una red de tipo infraestructura.

Figura II.2 Modo de operación de una red de tipo infraestructura

2.1.3 Extended Service Set (ESS)

Los BSSs brindan cobertura en entornos SOHO, pero no pueden proporcionar cobertura en áreas extensas. El 802.11 permite que las redes WLAN aumenten el área de cobertura creando el enlace de varios BSSs en un ESS (Extended Service Set). A todos los APs en un ESS se les establece un mismo SSID (Service Set Identifier), el cual sirve como un nombre de red para los usuarios. El 802.11 no especifica una tecnología particular como backbone para enlazar los BSSs. En la figura II.3, el ESS es la unión de dos BSSs.

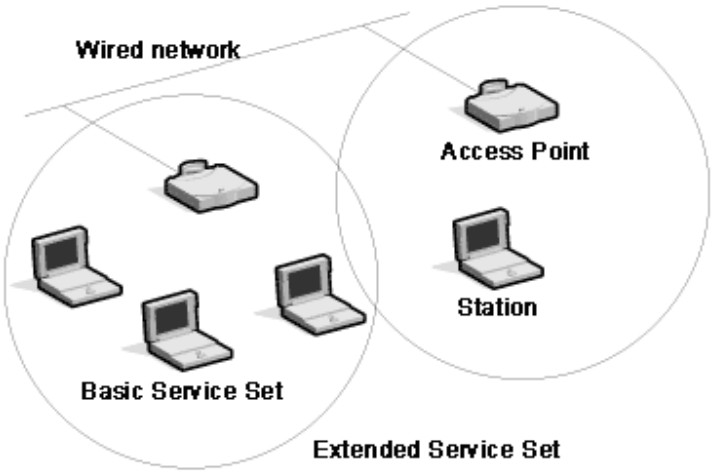


Figura II.3 Extended Service Set

Las estaciones que se encuentran en un mismo ESS pueden comunicarse unas con otras, incluso aunque las estaciones se encuentren en el área de cobertura de distintos BSSs y desplazándose entre ellos.

2.1.4 Sistemas de Distribución (DS)

Cuando muchos puntos de acceso se encuentran conectados para brindar servicios de red un área extensa de cobertura, tiene que comunicarse unos con otros para seguir proporcionando los servicios y recursos de red aunque las estaciones clientes se muevan de una ubicación a otra.

El sistema de distribución (DS) es el componente lógico de la tecnología 802.11 utilizado para enviar las tramas a sus destinos respectivos. El 802.11 no especifica ninguna tecnología en particular para el sistema de distribución.

En la mayoría de los casos el DS es implementado mediante un puente con el backbone de la red, al cual están conectados los APs, y que por lo general suele ser la conexión ethernet de la red. En la figura II.4 se muestra el DS representado como el backbone ethernet de la red.

Figura II.4 DS mediante el backbone ethernet de la red

El 802.11 describe al sistema de distribución en términos de los servicios que proporciona a las estaciones inalámbricas. El sistema de distribución proporciona movilidad mediante el enlace de puntos de acceso. El DS es el responsable de ubicar el lugar en donde la estación se encuentra físicamente (punto de acceso al cual está asociada) y entregar las tramas adecuadamente.

2.1.4.1 Comunicación Interaccess Point

Añadido a un DS es un método para administrar las asociaciones. Una estación sólo puede estar asociada con un AP a la vez. Si una estación se encuentra asociada a un punto de acceso, todos los puntos de acceso en el ESS necesitan saber información de esa estación. Para tener un sistema de distribución completo, los puntos de acceso tienen que informar a los demás puntos de acceso acerca de sus estaciones asociadas. En general muchos puntos de acceso utilizan un IAPP (InterAccess Point Protocol) sobre el backbone. Algunos fabricantes desarrollan sus propios protocolos entre APs para enviar información de las asociaciones. Un IAPP estándar es el 802.11F.

2.1.4.2 Sistema de Distribución Inalámbrico

Hasta ahora, sólo se ha dado por hecho que el sistema de distribución es la infraestructura de red ethernet. Ya que en general ese será el caso. Sin embargo, existen situaciones en las que se requiere conexión inalámbrica en sitios donde no existe un puerto cercano de conexión a la red ethernet pero existe la manera de ampliar la señal de un punto de acceso. Esta es una de las situaciones donde el sistema de distribución inalámbrico (WDS, Wireless Distribution System, por sus siglas en inglés) entra en acción, al poner a un punto de acceso a ampliar (repetir) la señal de un punto de acceso el cual si se encuentra conectado a la red ethernet que proporciona los servicios o recursos de red Un sistema de distribución inalámbrico, tal como lo muestra la figura II.5, es aquel que permite la interconexión de puntos de acceso de manera inalámbrica. Ya se mencionó que un WDS se puede utilizar para ampliar la señal de un AP conectado a la red ethernet. Sin embargo, cuando los puntos de acceso que conforman el WDS ofrecen los servicios y recursos que la red necesita, no es necesario que un AP tenga que estar conectado a la red ethernet.

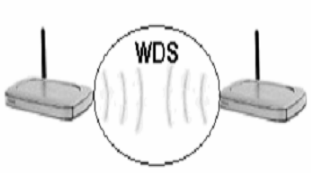


Figura II.5 Sistema de Distribución Inalámbrico

Aunque para cierto tipo de tráfico de red la perdida de conectividad no resulta alarmante, como el caso de conexiones TCP, donde la conexión puede restablecerse después de un periodo de pérdida de paquetes durante la transmisión. Esto no aplica para las aplicaciones de tiempo real, las cuales requieren de una entrega

constante de los paquetes. La retransmisión de paquetes es indeseable, por ejemplo, cuando se mantiene una transmisión de tráfico VoIP la retransmisión de paquetes perdidos provocaría una conversación desfasada.

El estándar 802.11 permite el uso del mismo medio inalámbrico como el sistema de distribución. Este es el denominado WDS y con frecuencia llamado "wireless bridge" ya que permite la conexión de redes WLAN a nivel de capa de enlace. La mayoría de los puntos de acceso en el mercado tienen el soporte para la configuración de un wireless bridge. Aunque debido a las distintas formas de implementación de los fabricantes se suelen presentar problemas de compatibilidad.

2.1.5 802.11 PHY

Tres tecnologías de capa física fueron estandarizadas en la versión inicial del 802.11, la cual fue publicada en 1997:

- Frequency-Hopping (FH) spread-spectrum radio PHY
- Direct-Sequence (DS) spread-spectrum radio PHY
- Infrared light (IR) PHY

Después, tres nuevas tecnologías basadas en ondas de radio fueron desarrolladas

- 802.11a: Ortogonal Frequency Division Multiplexing (OFDM) PHY
- 802.11b High-Rate Direct Sequence (HR/DS) PHY
- 802.11g: Extended Rate PHY (ERP)

2.1.5.1 Licencia y Regulación

En las comunicaciones mediante ondas de radio, el "ruido" es simplemente la distorsión natural que se presenta en la frecuencia. En el modelo clásico de transmisión, la eliminación de interferencia es una cuestión legal, no física. Una autoridad tiene que imponer reglas en la forma en que los espectros de RF (radiofrecuencia) son utilizados. En México el órgano encargado de estas regulaciones es la Comisión Federal de Telecomunicaciones (COFETEL). En Estados Unidos, la FCC (Federal Communications Commission) es responsable de regularizar el uso de los espectros de RF. Varias reglas de la FCC son adoptadas por otros países del continente americano.

La asignación en países Europeos está a cargo de la ERO (European Radiocommunications Office) y la ETSI (European Telecommunications Standards Institute). En Japón, el MIC (Ministry of Internal Communications) es el encargado de estas cuestiones.

Bajo los auspicios de la ITU (Internacional Telecommunications Union) se mantiene un trabajo "armónico" alrededor del mundo. Ya que varios organismos internacionales adoptan las recomendaciones de la ITU.

Para la mayoría de las ocasiones, una institución o empresa tiene que tener una licencia para transmitir en una frecuencia dada. Dicha licencia restringe las frecuencias y el poder (intensidad) de transmisión usada, así como también el área sobre la cual la señal puede ser trasmitida.

Tal como sucede con las redes de telefonía celular que tiene que solicitar licencias para el uso frecuencias que ofrecen para la comunicación de sus usuarios. Al igual como sucede con las radiodifusoras.

Cuando una señal con licencia es interferida, el dueño de la licencia puede demandar tal situación ante el organismo regulador competente para que dicho organismo resuelva el problema. La interferencia intencional puede verse como un delito.

2.1.5.2 Asignación de Frecuencia y Bandas de Frecuencia sin Licencia

El espectro de radio es asignado en bandas dedicadas para un propósito particular. Una banda define las frecuencias que una aplicación particular puede usar. Varias bandas han sido reservadas para su uso sin licencia. La FCC (y sus equivalentes en otros países) designó algunas bandas para el uso de equipo industrial, científico, y médico. Estas bandas de frecuencia son comúnmente referidas como bandas ISM (Industrial, Scientific, and Medical). La banda de los 2.4 GHz está disponible alrededor del mundo para su uso sin licencia.

Es preciso aclarar que no es lo mismo el uso sin licencia que la venta sin licencia. Elaborar, manufacturar y diseñar dispositivos 802.11 requiere una licencia. Por ejemplo, en Estados Unidos cada tarjeta vendida legalmente lleva un número de identificación asignado por la FCC.

Las bandas sin licencia han tenido una gran actividad, es decir, nuevas tecnologías han sido desarrolladas para explotar las bandas sin licencia. Los usuarios pueden pasar desapercibidos el hecho que están utilizando varios dispositivos en las bandas

ISM. Nuevos sistemas de comunicación han sido desarrollados en la banda ISM de los 2.4 GHz:

- Variantes de dispositivos 802.11 (802.11b, 802.11g)
- Dispositivos bluetooth, que utilizan un protocolo de comunicación inalámbrica de corto alcance
- Teléfonos de casa inalámbricos (cordless phones)

2.1.5.3 Otras bandas sin licencia

Espectro adicional está disponible en el rango de los 5 GHz. Estados Unidos fue el primer país en permitir el uso de dispositivos sin licencia en el rango de los 5 GHz, aunque le siguieron Japón y el continente Europeo.

2.1.5.4 Disposición de canales en la banda de 2.4GHz (802.11b/g)

Los dispositivos 802.11b y 802.11g comparten la misma banda de frecuencia. Por lo que ambos están sujetos a los mismos requerimientos de regulación, y utilizan un mapa de canales idéntico, tal como se muestra en la tabla 1. Aunque hay 14 canales, cada canal tiene sólo una amplitud de 5 MHz. Una transmisión Direct Sequence PHY es propagada a través de una banda más amplia que la asignada a su canal. Para evitar interferencia entre canales lo ideal sería establecer una separación de 33 MHz entre asignación de canales.

En la mayoría de los casos no existe un espectro de radio suficiente como para tener tres canales completamente sin que causen interferencia unos con otros. En este tipo de situaciones sólo se podría conseguir dos canales libres de interferencia, pero la mayoría de usuarios tolera un grado leve de interferencia para poder tener 3 canales con al menos 25 MHz de separación.

El conjunto de canales resultantes es 1, 6 y 11. Esto provoca una pequeña cantidad de interferencia a cada canal, pero vale la pena aceptar una pequeña reducción de rendimiento por canal para obtener tres canales.

Tabla II-1 Uso de los canales en distintos dominios de regulación

Canal	Frecuencia del canal (GHz)	Estados Unidos	ETSI	Japón
1	2.412	✓	✓	✓
2	2.417	✓	✓	✓
3	2.422	✓	✓	✓
4	2.427	✓	✓	✓
5	2.432	✓	✓	✓
6	2.437	✓	✓	✓
7	2.442	✓	✓	✓
8	2.447	✓	✓	✓
9	2.452	✓	✓	✓
10	2.457	✓	✓	✓
11	2.462	✓	✓	✓
12	2.467		✓	✓
13	2.472		✓	✓
14	2.783			✓

2.1.6 802.11 MAC

Para satisfacer los retos puestos en la capa de enlace de datos 802.11, la función de la capa MAC (Medium Access Control) tuvo que ser forzada a adoptar varias características únicas. Una de las cuales fue el uso de cuatro campos para direcciones, No toda las tramas utilizan todos los campos, y los valores asignados a los campos de dirección pueden cambiar dependiendo del tipo de trama MAC que es transmitido. En la figura II.6 se muestra una trama genérica MAC 802.11.

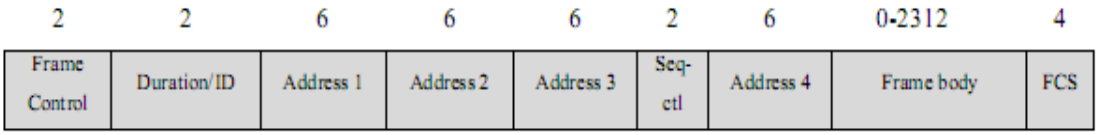


Figura II.6 Trama genérica MAC 802.11

Debido a que el entendimiento completo de las tramas MAC requiere de un estudio arduo. Para fines del presente trabajo se contemplan sólo las consideradas relevantes para el mismo. Y para poder tener un mejor conocimiento de las tramas MAC se dejan a reserva la bibliografía utilizada en este trabajo.

2.1.6.1 Tramas de datos

Este tipo de tramas lleva datos en el campo frame body de la trama para protocolos de capas superiores. Tal como muestra la figura de una trama genérica MAC 802.11. Dependiendo del tipo particular del tipo de trama de datos, algunos campos pueden ser o no utilizados.

2.1.6.2 Bits DS y campos de direcciones

El número y función de los campos de direcciones depende de los valores de los bits DS, bits que son definidos en el campo frame control de la trama MAC. La tabla 2 resume el uso de los campos de direcciones en las tramas de datos. Los cuatro campos de direcciones sólo son utilizados cuando se tienen funcionando wireless bridges.

Tabla II-2 Uso de los campos de direcciones en las tramas de datos

Función	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBBS	0	0	DA	SA	BSSID	Sin Utilizar
A un AP	1	0	BSSID	SA	DA	Sin Utilizar
De un AP	0	1	DA	BSSID	SA	Sin Utilizar
WDS (Bridge)	1	1	RA	TA	DA	SA

Para un buen entendimiento de la tabla anterior. A continuación se da la interpretación a las siglas que representan los valores de los campos:

- DA (Destination Address): Destinatario
- SA (Source Address): Remitente
- RA (Receiver Address): Receptor
- TA (Transmitter Address): Emisor
- BSSID (Basic Service Set Address): Dirección MAC de un AP

El campo Address 1 indica al receptor de la trama. En muchos casos, el receptor es el destinatario, pero no siempre.

El destinatario es la estación que procesará el paquete de capa de red contenido en la trama; el receptor es la estación que intentará decodificar las ondas de radio de una trama 802.11. El campo Address 2 es la dirección del emisor y es utilizada para envío de ACKs. El emisor no tiene que ser necesariamente el remitente. El remitente es la estación que genera el paquete del protocolo de capa de red contenido en la trama; el emisor coloca la trama en ondas de radio.

El campo Address 3 es utilizado para cuestiones de filtro por los puntos de acceso y el sistema de distribución, pero el uso de este campo depende del tipo de red usado. En el caso de un IBSS, ya que no se utilizan puntos de acceso, y no está presente ningún sistema de distribución, el emisor es el remitente y el receptor es destinatario. En un IBSS, el BSSID es creado por un generador de números aleatorios.

El 802.11 deja en claro la diferencia entre el remitente (source) y el emisor (transmitter) así como también la diferencia entre el destinatario (destination) y el receptor (receiver). El emisor envía una trama al medio inalámbrico pero no necesariamente crea la trama. Una similar diferencia mantiene para las direcciones del destinatario y el receptor, un receptor puede ser un destino intermedio, pero las tramas son procesadas por protocolos de capa superior cuando estas llegan a su destinatario.

Para dejar aún más claro estas diferencias. A continuación se muestran una serie de figuras. La figura II.7 muestra una red en modo infraestructura en la cual un cliente está conectado a un servidor a través de una red 802.11. Las tramas enviadas por el cliente al servidor utilizan el conjunto de direcciones de la segunda línea de la tabla II-2.

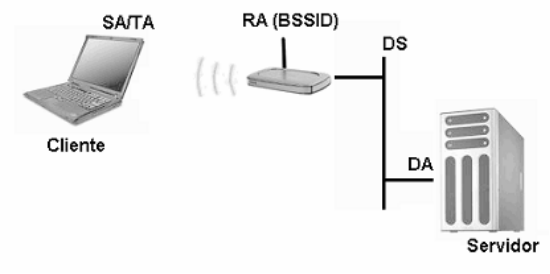


Figura II.7 Uso de los campos de direcciones en tramas MAC hacia el DS

En el caso en que las tramas están dirigidas a un destinatario en el sistema de distribución, el cliente es tanto el remitente como el emisor. El receptor de la trama 802.11 es el punto de acceso, pero ya que el AP es sólo un destino intermedio. Cuando la trama llega al AP, es enviada al DS para llegar al servidor. Por lo tanto, el AP es el receptor, y el destinatario es el servidor. En las redes de tipo infraestructura, los puntos de acceso crean BSSs asociados con la dirección de sus interfaces de red inalámbricas, es por ello que la dirección del receptor (Address 1) toma el valor del BSSID.

En el caso en que las tramas están dirigidas a un destinatario en el sistema de distribución, el cliente es tanto el remitente como el emisor. El receptor de la trama 802.11 es el punto de acceso, pero ya que el AP es sólo un destino intermedio. Cuando la trama llega al AP, es enviada al DS para llegar al servidor. Por lo tanto, el AP es el receptor, y el destinatario es el servidor.

En las redes de tipo infraestructura, los puntos de acceso crean BSSs asociados con la dirección de sus interfaces de red inalámbricas, es por ello que la dirección del receptor (Address 1) toma el valor del BSSID.

Cuando el servidor contesta al cliente, las tramas son transmitidas al cliente vía el punto de acceso, como lo muestra la figura II.8. Este escenario corresponde a la tercera línea en la tabla II-2.

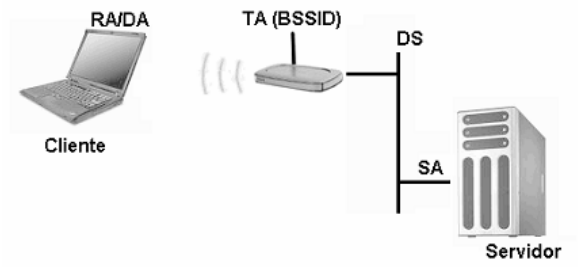


Figura II.8 Uso de los campos de direcciones en tramas MAC provenientes del DS

Las tramas son creadas por el servidor, así que la dirección MAC del servidor es la dirección origen (SA). Cuando las tramas llegan al punto de acceso, el AP utiliza dirección de su interfaz de red inalámbrica como dirección de emisor (TA). Por último las tramas son enviadas al cliente, el cual desempeña los roles de destinatario y receptor.

La cuarta línea en la tabla II-2, muestra el uso de los cuatro campos de las direcciones en un sistema de distribución inalámbrico, también denominado en ocasiones como wireless bridge. La figura II.9 muestra un escenario en la que dos redes de medios guiados (cableadas) son unidas por puntos de acceso que realizan la función de wireless bridges. Las tramas se dirigen del cliente al servidor a través del WDS 802.11. Las direcciones origen (SA) y destino (DA) de las tramas

corresponden al cliente y al servidor respectivamente. Estas tramas, además, también identifican al emisor y al receptor de la trama en el medio inalámbrico. Para las tramas dirigidas del cliente al servidor, el emisor es el punto de acceso del lado del cliente, y el receptor es el punto de acceso del lado del servidor. La separación del origen del emisor permite al AP del lado del servidor enviar ACKs 802.11 al otro AP sin ningún tipo de interferencia con la capa de enlace de la red cableada.

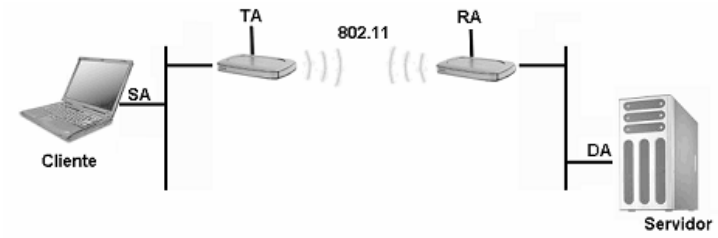


Figura II.9 Uso de los campos de direcciones en tramas MAC en un WDS

2.1.6.3 Tramas con cifrado

Las tramas protegidas por un protocolo de seguridad a nivel de capa de enlace de datos no son nuevos tipos de tramas. Cuando una trama es controlada con un mecanismo de cifrado el valor del bit Protected Frame en el campo Frame Control es puesto en 1 y el campo Frame Body comienza con el "header" apropiado de cifrado, dependiendo del protocolo de seguridad utilizado.

2.1.7 Movilidad

La disponibilidad de acceso vía inalámbrica resulta productiva debido a que los usuarios pueden acceder a recursos y servicios en donde sea conveniente hacerlo. En realidad, sin embargo, la disponibilidad sólo elimina las barreras físicas de la

conectividad. Pero no cambia la complejidad de conectarse a redes distintas en cada nueva ubicación. La movilidad, por otro lado, es un concepto más complejo: elimina más barreras, la mayoría de las cuales están basadas en la arquitectura lógica de la red. Las conexiones de red permanecen activas incluso mientras el dispositivo inalámbrico se encuentra en movimiento.

2.1.7.1 Precisando el concepto de movilidad

Sin la movilidad, el acceso vía inalámbrica no sería particularmente interesante. La movilidad significa que los recursos y servicios estén disponibles, sin importar la ubicación del dispositivo. La construcción de una infraestructura de tal magnitud que proporcione servicios independientemente de la ubicación es una tarea ardua y compleja. Aterrizar el amplio concepto de movilidad a un nivel técnico puede ser realizado de distintas maneras. Son varias las tecnologías que pueden ser utilizadas para proporcionar movilidad.

A nivel de capa de enlace de datos la movilidad requiere que la red parezca la misma sin importar la ubicación. Varios son los procesos que proporcionan movilidad a este nivel:

- Handoffs[1] transparentes entre puntos de acceso. Los usuarios tal vez necesiten realizar un proceso de configuración inicial para seleccionar una red y conectarse a ella, pero no deben estar involucrados en decisiones de handoffs.

[1] Concepto mayormente utilizado en comunicaciones móviles celulares aunque también aplicable en entornos 802.11. Consiste en transferir los servicios de una célula (cobertura de señal) a otra adyacente.

Si la señal llega a debilitarse, el software debe intentar localizar una mejor señal y realizar el cambio sin la intervención del usuario. Cada tarjeta realiza el cambio automáticamente entre puntos de acceso que son parte de la misma red. El 802.11 fue diseñado con este requerimiento:

- El desplazamiento entre puntos de acceso requiere establecer un nuevo conjunto de parámetros de seguridad para el cifrado y protección de los datos o transferir los parámetros del anterior AP al nuevo AP. Dependiendo del hardware en uso y la complejidad del sistema de seguridad, el proceso de establecer un contexto de seguridad con el nuevo AP puede tomar una cantidad de tiempo considerable.

2.2 SEGURIDAD INALÁMBRICA

Siempre que se utiliza una red para comunicarse, ya sea cableada o inalámbrica, se desea que los datos viajen de forma segura. Si no se cuenta con una red que cuente con mecanismos de seguridad, se tiene el riesgo que la información enviada por la red pueda ser interceptada por terceros u obtener algún beneficio de la red.

La vulnerabilidad inherente de las redes WLAN debido a que no se requiere de un punto de conexión física como sucede en las redes cableadas. Se refleja en lo fácil que resulta para un intruso (con los conocimientos, herramientas, equipo y tiempo necesarios) tener acceso a la red, siempre y cuando la red no cuente con mecanismos de seguridad o estos sean obsoletos.

El estándar IEEE 802.11 cuenta con un mecanismo de cifrado para asegurar los datos que son transmitidos. Este mecanismo, que tiene por nombre WEP (Wired Equivalent Privacy), es suficiente aún para redes domésticas, ya que en estas sólo se necesita un nivel ligero de seguridad. Sin embargo, utilizar WEP en redes

corporativas representa un nivel de riesgos considerable, por lo que se ha tenido que recurrir a otras tecnologías para proteger los datos.

Entre las tecnologías complementarias a WEP se encuentran VPN (Virtual Private Networking), 802.1X, EAP (Extensible Authentication Protocol) y RADIUS. Además de los mecanismos de seguridad nativos de Wi-Fi, Wi-Fi Protected Access (WPA) y Wi-Fi Protected Access 2 (WPA2).

2.2.1 Cifrado y autenticación

El cifrado consiste en disfrazar o codificar mensajes de acuerdo a una llave secreta, que sólo el emisor y el receptor conocen. La autenticación es el proceso de asegurar que los usuarios son quienes dicen ser antes de que sean autorizados de acceder a la red. Ambos deben estar presentes en una solución de seguridad, así mismo trabajar juntos uno complementándose uno al otro. La figura II.10 ilustra la forma en que se complementan la autenticación y el cifrado.

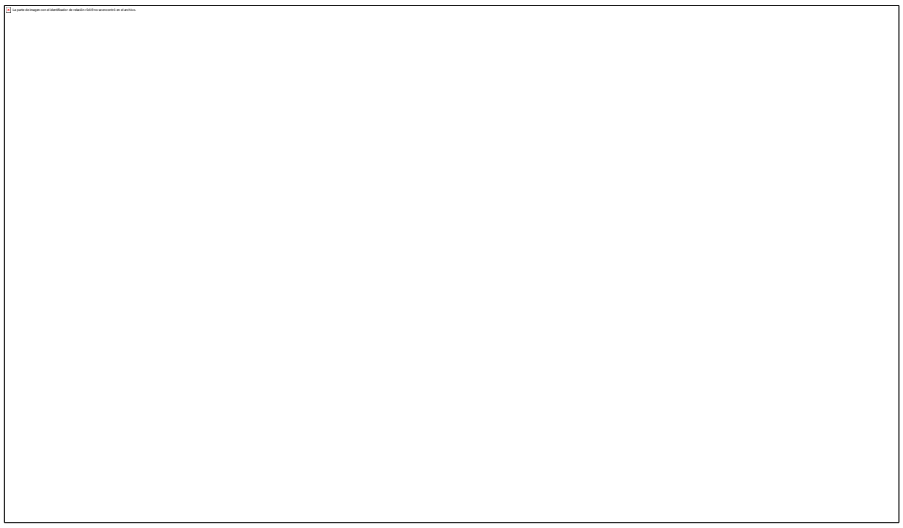


Figura II.10 Manera en que se complementan la autenticación con el cifrado

Algunos esquemas de cifrado pueden ser quebrantados si un hacker tiene el tiempo y recursos necesarios para reunir una cantidad suficiente de datos para analizar y descifrar la llave secreta. Las llaves son determinadas por algoritmos que especifican la longitud y contenido de la llave o con qué frecuencia es cambiada la llave, o ambas. La capacidad de "hackear" eventualmente un método de cifrado es la razón principal por lo que la seguridad debe estar constantemente envuelta en nuevas tecnologías.

A pesar de que los esquemas de autenticación varían ampliamente, todos proporcionan un método de verificación de credenciales, requiriendo un nombre de usuario y una contraseña, o un certificado digital. Dichas credenciales son comparadas contra un servidor de autenticación que determina su validez antes de dar acceso a la red a un usuario.

2.2.2 WEP y sus vulnerabilidades

WEP es el protocolo de seguridad del 802.11, utiliza el algoritmo de cifrado RC4 para mantener la privacidad de los datos que se transmiten en una WLAN. La llave WEP tiene una longitud de 64 bits, tal y como se muestra en la figura II.11, 24 bits corresponden al vector de inicialización (IV) y 40 a la llave secreta compartida entre los puntos de acceso y las estaciones clientes.

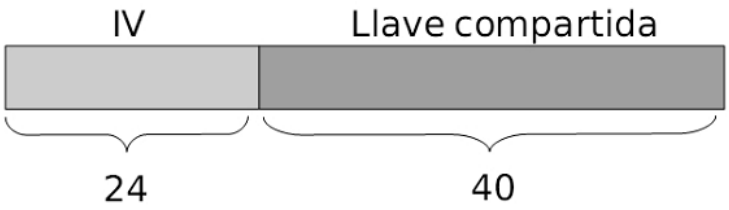


Figura II.11 Longitud y segmentación de la llave WEP

El principal problema con WEP es que no tiene especificado un esquema de determinación y distribución de llaves para el cifrado de datos. La determinación de las llaves se lleva acabo manualmente en los APs y los estaciones clientes, siendo la misma llave para ambas partes. Este sistema de distribución de llave no resulta satisfactorio para entornos empresariales.

Además, no hay un mecanismo para el cambio de llaves WEP por autenticación o por periodos de tiempo. Todos los APs y clientes utilizan la misma llave para múltiples sesiones. Con un envío vasto de datos un atacante puede capturar una cantidad suficiente, y usar una herramienta de criptoanálisis para obtener la llave WEP, y por lo tanto obtener acceso a la red. Este tipo de ataques se lleva a cabo principalmente en las redes de tipo infraestructura en las que operan un gran número de estaciones, aunque las redes ad hoc no quedan exentas de estos ataques.

Poco tiempo después de que WEP fue desarrollado, una serie de investigaciones académicas e independientes comenzaron a exponer sus debilidades criptográficas. El primer ataque práctico sobre WEP fue identificado por los investigadores Scott Fluhrer, Itsik Mantin y Adi Shamir (FMS attack).

Las principales cuestiones de seguridad con el estándar original IEEE 802.11 son las siguientes:

- Falta de soporte para la administración de llaves.
- Falta de mecanismos de autenticación por usuario.
- Falta de soporte para la identificación de falsos APs.

La solución para estas cuestiones de seguridad del estándar original IEEE 802.11 es la que proporciona el estándar IEEE 802.1X.

2.2.3 Autenticación con el estándar IEEE 802.1X

Un usuario con acceso autorizado a la red puede conectar a la red un punto de acceso en lugar del equipo de la empresa o institución. Esto implica una serie de riesgos para la red cuando dispositivos ajenos a la corporación obtienen acceso a la red. Esta situación se agrava si el dispositivo ajeno es un punto de acceso y empieza a funcionar. Aún más si el punto de acceso no cuenta con mecanismos de seguridad o dichos mecanismos sean obsoletos. Por lo que cualquier dispositivo móvil (PDA, laptop) que se encuentre dentro del área de cobertura del punto de acceso puede obtener acceso a los recursos de la red. Con lo cual se corren los siguientes riesgos (entre otros):

- Robo y/o alteración de información.
- Si el equipo está infectado con algún virus, se corre el riesgo de infectar toda la red.

El estándar IEEE 802.1X define un mecanismo para el control de acceso a red basado en puertos. Hace uso de características físicas de las infraestructuras de red 802 LAN para proporcionar autenticación y autorización a dispositivos conectados a un puerto, y prevenir el acceso en aquel puerto en el que el proceso de autenticación y autorización falla. Aunque este estándar fue diseñado en un principio para redes LAN Ethernet, ha sido adoptado en redes LAN 802.11. Los elementos del 802.1X se muestran en la figura II.12.

Figura II.12 Esquema de autenticación 802.1X

Los elementos del estándar 802.1X, está definido por los siguientes términos para la comprensión del control de acceso basado en puertos:

- Port access entity
- Authenticator
- Supplicant
- Authentication Server

2.3 AUTENTICACIÓN CON EL ESTÁNDAR IEEE 802.1X

2.3.1 Port Access Entity (PAE)

Es una entidad lógica que controla el protocolo IEEE 802.1X asociado con un puerto. Un PAE es capaz de desempeñar el rol de authenticator, supplicant o ambos.

2.3.2 Authenticator

Es un puerto LAN que hace cumplir la autenticación antes de permitir el acceso a los servicios o recursos disponibles mediante el uso de dicho puerto. En las conexiones inalámbricas, el authenticator es el puerto LAN lógico (hecho mediante la asociación) en un punto de acceso mediante el cual los clientes en redes de tipo infraestructura obtienen acceso a otros clientes y a la red cableada.

2.3.3 Supplicant

Es el puerto LAN que quiere el acceso a los servicios disponibles que mediante el authenticator se pueden obtener. En las conexiones inalámbricas, el supplicant es el puerto lógico (hecho mediante la asociación) en una NIC inalámbrica que quiere obtener acceso a otros clientes o a la red cableada.

Ya sea mediante una conexión inalámbrica o Ethernet, el supplicant y el authenticator están conectados por un segmento LAN point-to-point físico o lógico.

2.3.4 Authentication Server

Valida las credenciales del supplicant y envía una respuesta al authenticator indicando si el supplicant está autorizado para acceder a los servicios que mediante el authenticator puede obtener. El authentication server se puede encontrar en los siguientes escenarios:

- ***Como parte del punto de acceso***. En este caso, el AP tiene que estar configurado con el conjunto de credenciales de usuarios o computadoras correspondiente a los supplicants autorizados que estarán intentando conectarse.
- ***Como un host aparte***. En este caso, el AP envía las credenciales de intentos de conexión a un authentication server alojado en un lugar aparte. La mayoría de las veces, un AP utiliza el protocolo RADIUS para enviar un mensaje de solicitud de conexión a un servidor RADIUS.

2.3.5 Puertos controlados e incontrolados

El funcionamiento del control de acceso basado en puertos tiene el efecto de crear dos formas lógicas distintas de acceso, en el punto de conexión física del dispositivo, a la LAN.

- ***Puerto incontrolado:*** Permite el intercambio de paquetes del dispositivo (authenticator) a otros dispositivos en la LAN, a pesar del estado de autorización. Es utilizado durante el proceso de autenticación. Este puerto en ocasiones también es referido como puerto inautorizado.
- ***Puerto controlado:*** Permite el intercambio de paquetes sólo si el estado actual del puerto es autorizado. Antes de la autenticación, el enlace permanece truncado y no son enviadas tramas entre el cliente y los dispositivos a los que se pueden acceder mediante el authenticator. Cuando el cliente es autenticado con éxito mediante IEEE 802.1X, el enlace es establecido y las tramas pueden ser enviadas entre el cliente y los nodos alcanzables vía el authenticator.

Este puerto en ocasiones también es referido como puerto autorizado. Los puertos controlado e incontrolado son considerados como parte del mismo punto de conexión física a la LAN.

2.4 CONSIDERACIONES DE SEGURIDAD CON EL IEEE 802.1X

Las soluciones a los aspectos de seguridad que proporciona el IEEE 802.1X son las siguientes:

- Se soluciona el problema de detección de falsos APs con los protocolos de autenticación mutua como EAP-TLS. El cliente se asegura de que el AP al que se conecta en realidad forma parte del entorno de seguridad que valida el servidor RADIUS.
- La utilización del IEEE 802.1X habilita una autenticación a nivel de usuario, por medio de un servidor (RADIUS).

A pesar de que el 802.1X se encarga de algunas de las debilidades propias del estándar IEEE 802.11 original, no proporciona mecanismos que mejoren el proceso de cifrado de datos WEP. Por lo que siguen presentes hasta este punto las debilidades del mecanismo WEP.

2.5 EAP (EXTENSIBLE AUTHENTICATION PROTOCOL)

EAP es un entorno de autenticación (definido en el RFC 3748 de la IETF), no un propio mecanismo en sí. Aunque este protocolo no está limitado a WLAN y puede ser utilizado para la autenticación en redes cableadas, sí es más utilizado en entornos WLAN.

EAP proporciona algunas funciones comunes y negociación para el mecanismo de autenticación deseado. Dichos mecanismos son llamados métodos EAP, y existe una gran variedad de estos métodos. Entre los métodos incluidos en IETF RFCs se encuentran: EAP-MD5, EAP-TLS, EAP-TTLS, EAP-SIM, además de, por supuesto, métodos propietarios.

2.5.1 EAP-MD5

Es otro estándar de la IETF, pero ofrece un nivel mínimo de seguridad. La función de hash MD5 es vulnerable a ataques de diccionario, además de no soportar autenticación mutua o generación de llaves, por lo que es inadecuado para ser usado en entornos WPA/WPA2 Entreprise.

2.5.2 EAP-TLS

EAP-Transport Layer Secutity (EAP-TLS) es un método EAP que es utilizado en entornos de seguridad basados en certificados. Utiliza PKI[2] para mantener comunicaciones seguras con el authentication server.

Es el método EAP estándar para la autenticación en WLANs, es aún considerado uno de los métodos más seguros disponibles y es universalmente soportado por todos los fabricantes de hardware y software. Debido a que este método se basa en certificados, el hecho que un password se encuentre comprometido no es suficiente para quebrantar sistemas EAP-TLS debido a que se requiere un certificado del lado del cliente.

TLS proporciona autenticación mutua, por lo tanto, el authenticator válida al supplicant y el supplicant al authenticator. Con lo que se solucionan los ataques MITM[3]. Mientras se mantiene la conversación EAP entre el authenticator y el supplicant, el primero actúa como intermediario y encapsula los paquetes recibidos del supplicant para la transmisión al authentication server.

[2] Es un arreglo que ata llaves públicas con identidades respectivas de usuarios por medio de un certificado.

[3] Man In The Middle, ataque mediante el cual un intruso se posiciona entre el cliente y el AP, con su propio dispositivo, para manipular la información que se transmite entre el cliente y el AP.

2.5.3 EAP-TTLS

En algunas situaciones, el requerimiento de una infraestructura PKI es prioridad para lograr una autenticación enérgica en redes WLAN. Aunque algunas organizaciones prefieren reutilizar sus sistemas de autenticación existentes, tales como LDAP o Active Directoty. Es entonces cuando EAP-TTLS es atractivo para habilitar esos mecanismos "legacy".

El proceso de funcionamiento consiste en que primero se establece un túnel TLS. Se utilizan certificados digitales en el Authentication Server para validar que la red es confiable. Después el túnel TLS es usado para cifrar algún protocolo de autenticación existente, por lo general contraseñas, que da acceso a la red. En este método EAP aún se requieren certificados, pero sólo del lado del authentication server.

Lo cual representa una gran ventaja sobre EAP-TLS, ya que reduce el número de certificados de cientos o tal vez miles a unos cuantos para los authentication servers. EAP funciona en conjunto con 802.1X, por lo que estas tecnologías forman un framework para realizar el proceso de autenticación, la figura 13 muestra la forma de operación del framework 802.1X/EAP.

Figura II.13 Framework de autenticación 802.1X/EAP

2.6 WPA (WI-FI PROTECTED ACCESS)

Con las mejoras proporcionadas con el estándar IEEE 802.1X al proceso de autenticación en las redes WLAN, se tuvo una mejora relativa sobre la seguridad en este tipo de redes. Sin embargo permanecían las debilidades del mecanismo de cifrado WEP. En octubre del año 2003, la Wi-Fi Alliance en conjunto con el instituto de Ingenieros Eléctricos y Electrónicos (IEEE) lanzó WPA. Aunque ninguna solución de seguridad puede decirse "del todo segura", WPA representa un avance en las debilidades de seguridad conocidas de WEP. WPA es un subconjunto del estándar IEEE 802.11i. El avance en la seguridad inalámbrica respecto a WEP es un nuevo mecanismo de cifrado, así como también el mecanismo de autenticación a nivel de usuario. Cuando es correctamente instalado y configurado, proporciona a los usuarios un nivel alto en seguridad de que sus datos permanecerán protegidos y que sólo usuarios autorizados pueden acceder a la red.

Una de las principales debilidades de WEP es que utiliza una llave pequeña estática para iniciar el cifrado. La llave secreta de 40 bits es introducida manualmente en el AP y las estaciones clientes que se comunican con el AP. Lo cual convierte la administración de WEP en una labor intensiva, ya que el cambio de llave representa un cambio manual de la misma en el AP y en todas las estaciones clientes. WPA utiliza un esquema mejorado de cifrado, TKIP. De la mano con la autenticación 802.1X/EAP, TKIP emplea una jerarquía de llave que mejora la protección de los datos. También agrega un mensaje de verificación de integridad (MIC, en ocasiones llamado "Michael") para proteger la modificación de paquetes.

2.6.1 TKIP (Temporal Key Integrity Protocol)

Incrementa el tamaño de la llave de 64 a 128 bits, incrementando a su vez el IV de 24 a 48 bits, y reemplaza la llave estática de WEP por llaves que son generadas dinámicamente y distribuidas por el authentication server. TKIP utiliza una metodología de jerarquía de llave y administración de llave que elimina la predisponibilidad en la que los atacantes se basan para quebrantar la llave WEP.

Para llevarlo a cabo, TKIP echa mano del entorno (framework) 802.1X/EAP. Una vez que el authentication server acepta una credencial de usuario, utiliza el 802.1X para generar una llave "master" para esa sesión. TKIP distribuye esta llave a la estación cliente y al AP, y establece una jerarquía de llave y sistema de administración usando la llave master para generar dinámicamente llaves únicas para cifrado de datos para cada paquete de datos que es transmitido inalámbricamente durante la sesión del usuario. La jerarquía de llave que utiliza TKIP intercambia la llave estática de WEP por alrededor de 280 trillones de llaves posibles[4].

2.6.2 MIC (Message Integrity Check)

El MIC está diseñado para prevenir que un atacante capture, modifique y reenvíe paquetes de datos que son transmitidos por la WLAN. El MIC proporciona una función matemática con la que el emisor y el receptor calculan y comparan cada uno el MIC. Si no coinciden, se asume que ha habido intentos de corromper los datos y el paquete es eliminado. Debido al incremento del tamaño de las llaves, el número que llaves que son usadas, y el mecanismo de verificación de integridad, TKIP aumenta la complejidad y dificultad implicadas en el descifrado de datos en un WLAN.

[4] Wi-Fi Alliance. Deploying Wi-Fi Protected Access (WPA™) and WPA2™ in the Enterprise, 2005.

2.6.3 Autenticación

Para el proceso de autenticación WPA utiliza el 802.1X junto con uno de los métodos EAP disponibles. El 802.1X es un método de control de acceso a red basado en puertos para redes cableadas e inalámbricas. Fue adoptado como estándar por el IEEE en agosto del año 2001 y revisado en el 2004. EAP se encarga de la presentación de credenciales de usuarios en forma de certificados digitales, nombres de usuario y contraseña, smartcards.

EAP tiene una gran variedad de métodos para utilizarse, entre los que se incluyen EAP-TLS, EAP-TTLS, PEAP. Junto con EAP, el 802.1X crea un entorno en el que las estaciones clientes se autentican mutuamente con el authentication server. Con el proceso de autenticación mutua se previene que los usuarios se puedan conectar accidentalmente a un falso o inautorizado AP en la WLAN y también se asegura de que los usuarios efectivamente son quienes dicen ser.

2.7 WPA2 (WI-FI PROTECTED ACCESS 2)

Aunque el protocolo TKIP es mejor que WEP, ya que remedia algunos de los defectos de WEP. Está predestinado a ser vulnerable ya que fue diseñado a partir del funcionamiento de WEP. TKIP mantiene el uso del algoritmo de cifrado RC4, el cual es la causa de varias de las vulnerabilidades de WEP.

Una vez concluida la elaboración del estándar IEEE 802.11i, en él se especificó como obligatorio la utilización de CCMP (Counter mode with CBC-MAC Protocol), un nuevo protocolo de cifrado, el cual tiene como gran referente el nuevo algoritmo, AES (Advanced Encryption Standard). Al igual que TKIP utiliza una longitud de 128 bits para la llave, 48 para el IV y 80 para los datos cifrados.

Una ventaja de TKIP sobre CCMP es que como está basado en el algoritmo RC4, por lo que el mismo hardware de WEP puede ser utilizado para lograr el nivel de seguridad que proporciona TKIP mediante una actualización de software o firmware. Lo cual no es posible con CCMP ya que la naturaleza de AES tiene procesos complejos de cómputo, y por consecuencia requiere de actualización de hardware. Sin embargo, algunos controladores pueden realizarlo mediante software sin requerir actualización de hardware 802.11. WPA2 sigue manteniendo el framework de autenticación 802.1X/EAP tal como lo utiliza WPA.

2.7.1 Preautenticación

El 802.11i permite realizar el proceso de roaming seguro en un menor tiempo. Pero a pesar de disminuir la latencia, no es lo suficiente capaz de proporcionar latencia más baja como para permitir un roaming aceptable para conexiones donde se transmite tráfico de tiempo real, como VoIP.

Esto es el proceso que se sigue en la pre-autenticación:

- Primero la estación se asocia con un AP, realizando un proceso de autenticación normal 802.11i.
- La estación tiene que enterarse de los APs vecinos. Los cuales son normalmente APs en el mismo ESS con suficiente intensidad de señal.
- La estación inicia una conversación EAP normal con cada uno de los candidatos vía AP al cual está asociado.
- Con el paso anterior se resuelve el problema de no ser capaz de comunicarse con APs vecinos sin romper su asociación con el actual AP.

La pre autenticación hace el proceso de roaming menos tedioso ya que la autenticación se realiza antes de que sea necesaria una asociación, lo cual elimina el tiempo de autenticación al momento preciso que se lleva a cabo el roaming.

2.8 Modo Personal vs Modo Enterprise

Tanto WPA como WPA2 cuentan con dos modos de operación, Personal y Enterprise. Ambos modos utilizan los mismos protocolos para el proceso de cifrado y su diferencia radica en el protocolo de autenticación. La tabla II-3 muestra las características de los modos.

Tabla II-3 Modos de seguridad de WPA y WPA2

	WPA	**WPA2**
Modo Personal	Autenticación: 802.1X/EAP Cifrado: TKIP	Autenticación: 802.1X/EAP Cifrado: CCMP
Modo Enterprise	Autenticación: PSK Cifrado: TKIP	Autenticación: PSK Cifrado: CCMP

2.8.1 Modo Personal

Diseñado para usuarios domésticos, SOHO, los cuales en principio no cuentan con authentication servers disponibles en su infraestructura de red. Utiliza llaves precompartidas, PSK (Pre-Shared Keys), para el proceso de autenticación en lugar del framework 802.1X/EAP. La autenticación en este modo es mediante contraseñas, las cuales son introducidas manualmente en los puntos de acceso y las estaciones clientes. Se recomienda en este modo utilizar contraseñas basadas en frases, las cuales utilicen caracteres y números alternados, además de combinar el uso de mayúsculas y minúsculas.

2.8.2 Modo Enterprise

Utiliza requerimientos rigurosos de seguridad, los cuales delega al framework de autenticación 802.1X/EAP. Proporcionando autenticación mutua entre la estación cliente y el authentication server vía el punto de acceso. Este modo asigna una única llave por usuario para acceder a la WLAN, lo cual ofrece un nivel de seguridad alto.

2.9 ROAMING

Con el "boom" de Internet y el avance suficiente en tecnología celular de radiofrecuencia en los años 90, era natural la concepción de una asociación entre ambas tecnologías. De esta asociación surgió el concepto de lo que hoy se conoce como 802.11. A diferencia de los diseñadores del servicio de telefonía celular. La IEEE decidió que estas células operarían utilizando una frecuencia sin licencia para simplificar su expansión. El concepto de roaming, dentro de la tecnología 802.11, es referido como el acto de desplazarse entre puntos de acceso (APs).

2.9.1 Naturaleza del roaming en el 802.11

El roaming en la tecnología 802.11 es conocido como "break before make". Debido a que una estación tiene primero que terminar su asociación con un punto de acceso para poder asociarse a otro. Este proceso es inadecuado, debido a que existe la posibilidad de pérdida de datos en el proceso de roaming. Sin embargo, simplifica la implementación de un protocolo a nivel de capa de enlace.

2.9.2 Modo de operación de las aplicaciones

La forma de funcionamiento de las aplicaciones está directamente relacionada a su persistencia durante el proceso de roaming. Las aplicaciones orientadas a conexión,

las cuales utilizan el protocolo TCP (Transmission Control Protocol), son más tolerantes a la pérdida de paquetes involucrada en el proceso de roaming. Aunque TCP proporciona una solución sutil para aplicaciones que se ofrecen en redes WLAN, no todas las aplicaciones se basan en TCP. Algunas hacen uso de UDP (User Datagram Protocol) debido a su entorno no orientado a conexión. Aplicaciones como VoIP y video utilizan este protocolo. En estos tipos de aplicaciones la retransmisión de paquetes, que ofrece TCP, es indeseable ya que alteraría el proceso de comunicación (charlas desfasadas por ejemplo).

2.9.3 Dominio del roaming

En la tecnología ethernet se define el concepto de dominio de broadcast como aquella red que conecta dispositivos que son capaces de enviar y recibir tramas de broadcast unos a otros. Este dominio también es conocido como red de capa 2. El concepto se mantiene en la tecnología 802.11. Los puntos de acceso que se encuentran en el mismo dominio de broadcast y son figurados con el mismo SSID (Service Set Identifier) son destinados a estar en el mismo dominio de roaming. Ya que un ESS es definido como la unión de varios BSSs que se comunican vía un DS, un dominio de roaming puede también ser referido como un ESS.

Es necesario recalcar que los dispositivos 802.11 están limitados al proceso de roaming a nivel de capa de enlace de datos. Recordemos que 802.11 trabaja en una capa física y una capa de enlace datos. Sin embargo, esto de ninguna manera hace imposible el roaming a nivel de capa de red, ya que no lo es. Lo que sí significa es que el 802.11 de forma nativa soporta el roaming a nivel de capa 2, y para el proceso de roaming a nivel de capa de red se requiere de alguna otra tecnología de capas superiores.

2.9.5 Duración del roaming

La figura II.14 muestra el dominio de roaming a nivel de capa 2. Las aplicaciones mantienen conectividad siempre que mantengan su dirección de red.

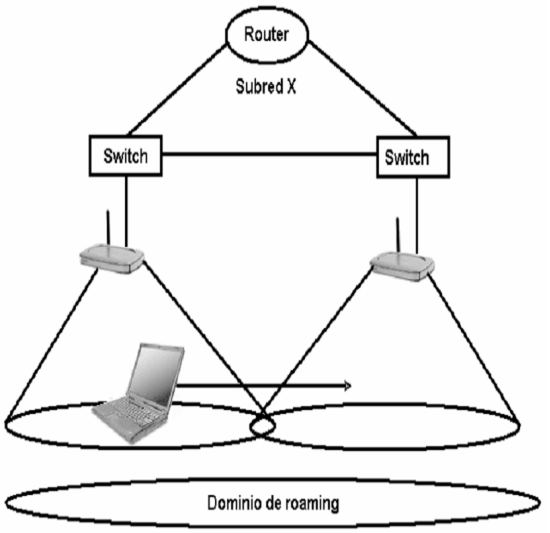


Figura II.14 Dominio de roaming a nivel de capa 2

La figura II.15 muestra una situación donde se ven involucrados varios dominios de roaming.

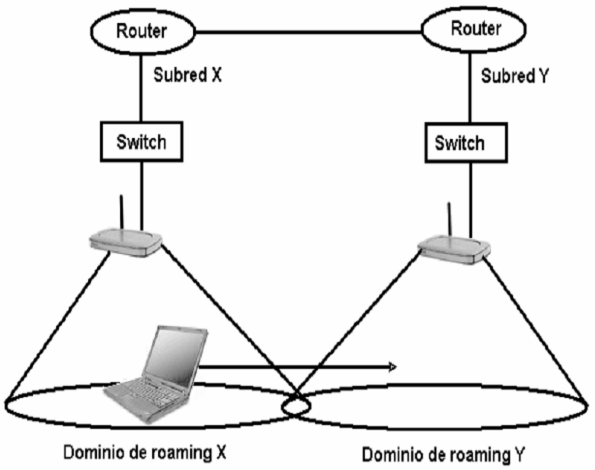


Figura II.15 Roaming entre varios dominios de roaming

La duración del roaming es el tiempo que toma realizar por completo el proceso de roaming. Esencialmente es el proceso de asociación y la duración depende de los siguientes factores:

- Proceso de autenticación
- Proceso de asociación
- Proceso de autenticación 802.1X (si es que lo hay)

La suma de los tiempos que toma cada uno de los factores es igual a la duración del roaming. Algunas aplicaciones como VoIP, son extremadamente sensibles al retardo y no pueden tolerar largos tiempos de duración del roaming.

2.9.6 Roaming a nivel de capa 2

Una perspectiva del proceso de roaming es mostrada en la secuencia de los siguientes eventos:

- ***El cliente decide cuando realizar el proceso de roaming***. Los algoritmos de roaming son específicos conforme a los fabricantes, y se basan en parámetros como la intensidad de la señal, tramas ACK (de acuse de recibo), etc.
- ***El cliente decide a dónde establecer el proceso de roaming.*** El cliente tiene que saber con cual AP tiene que realizar el roaming. Esto se realiza censando el medio en busca de APs ya sea antes de tomar la decisión de realizar el roaming o después de haber tomado la decisión.
- ***El cliente inicia el proceso de roaming.*** El cliente utiliza una trama de reasociación para asociarse al nuevo AP.

2.9.6.1 Algoritmos de roaming

El mecanismo para decidir cuándo realizar el proceso de roaming no está definido en el estándar 802.11 y por lo tanto recae en los fabricantes la implementación. Aunque esto supone un desafío de interoperabilidad.

En el hecho de cuando realizar el proceso de roaming uno esperaría que la estación se asociara con el AP que al momento tuviera una mayor intensidad en su señal. Sin embargo, esta estrategia no funciona en la práctica. La intensidad de la señal se encuentra sujeta a varios factores, incluso cuando la estación se encuentra estática. En los primeros dispositivos 802.11, la práctica más común era iniciar el roaming hasta perder la señal o cercana a un nivel de no ser usable. El hecho que la implementación quede a cargo de los fabricantes, les ofrece una oportunidad de diferenciarse entre ellos elaborando algoritmos de mejor rendimiento que sus competidores.

2.9.7 802.11r

El estándar original 802.11 incorpora funciones de roaming en una forma simple. Sin embargo, la velocidad y seguridad limitadas que proporciona el 802.11 original se refleja en lo inadecuado que resulta para mantener aplicaciones de voz seguras con conectividad. El grupo de tarea (task group) 802.11r trabaja en la forma de encontrar aspectos estandarizados que reducirán el tiempo de transición durante el proceso de roaming, referido como una BSS transition en el 802.11r. El objetivo del 802.11r es minimizar el tiempo que la estación pierde conectividad del DS. Ya que la pérdida de conectividad con el DS es igual a parar el flujo del tráfico de las aplicaciones del usuario.

El estándar 802.11r promete dar soluciones a los problemas en los aspectos que tienen que ver con los retardos en el proceso de roaming, apoyándose en estándares ya concluidos como lo es el 802.11i. Del cual toma varios aspectos, ante todo la seguridad es uno de los factores más importantes en una infraestructura de red. Al momento de realizar este proyecto de tesis, el 802.11r no se encuentra concluido aún.

2.10 REDES DE VOZ

La conversación es el proceso de comunicación elemental del ser humano. En algunas ocasiones este proceso de comunicación no puede llevarse a cabo forma física (es decir, personas hablando una frente a la otra).

Es por ello que con cada avance tecnológico que se ha ido realizando, siempre se ha ido mejorando la forma en que nos comunicamos (la mejora en los medios de comunicación). Estos avances han ido desde el telégrafo hasta el Internet, sin dejar a un lado al teléfono.

El teléfono ha sido el avance más significativo en cuanto a la comunicación a distancia entre las personas. Ya que permite la comunicación sin importar distancias, tiempo, etc.

Aunque el teléfono ha representado un gran avance en las aspectos referentes a la comunicación. De alguna forma las empresas encargadas de prestar este servicio, se han encargado de monopolizar la oferta del mismo.

Con los avances que se han logrado en las redes (LAN, WAN y WLAN) y tecnologías de red, se tiene una nueva perspectiva para el ámbito de las comunicaciones. Utilizando dichas infraestructuras de red existentes, en conjunto con herramientas de software, como plataforma para lograr una comunicación semejante a las proporcionadas por las empresas de telefonía. Logrando esto, mediante el uso de tecnologías como VoIP y herramientas de software libre como Asterisk.

2.10.1 VoIP (Voice over IP)

Voz sobre IP es una tecnología que permite que la señal de voz viaje a través de una red utilizando el protocolo IP. Consiste en convertir señales de voz en paquetes de datos. Uno de los grandes motivos por los que VoIP ha tenido y tiene un gran auge, es que fácilmente puede introducirse en una infraestructura de red ya existente.

Implementar la tecnología VoIP es una tarea compleja, debido a que se necesita cumplir con ciertos requerimientos de calidad de servicio (QoS) para poder mantener conversaciones óptimas.

2.10.2 Calidad de servicio (QoS)

La calidad de servicio respecta al trato preferencial que se le tiene que ofrecer a un tipo de tráfico. Voz sobre IP necesita de requerimientos estrictos de rendimiento. Los factores que afectan la calidad en la transmisión de datos impactan de manera distinta la calidad en la transmisión de voz. Por ejemplo, en general las transmisiones de datos no se ven afectadas por pequeños retardos. Aunque, por otro lado, la calidad en las transmisiones de voz se ve reducida si existen pequeñas cantidades de retardo durante la transmisión.

La calidad de una conversación VoIP depende de los siguientes factores de la red:

- **Latencia:** El tiempo que toma a una transmisión viajar desde su origen hasta su destino. Algunos procesos que aumentan la latencia son el paso de un firewall, cifrado de datos, negociaciones ACL.
- **Jitter:** La variación en la latencia de paquetes
- **Tasa de pérdida de paquetes:** La frecuencia con la que los paquetes no llegan a su destino.

En la ausencia de algún mecanismo que proporcione calidad de servicio, las redes operan mediante una entrega de paquetes best-effort. Lo cual significa que todo el tráfico de la red tiene una igual prioridad y por consiguiente todo el tráfico tiene la misma oportunidad de ser transmitido. Cuando la red experimenta congestiones, cualquier tipo de tráfico corre el mismo riesgo de presentar retardos o incluso ser eliminado. Cuando tráfico de voz se introduce en la red, se vuelve crítico que dicho tipo de tráfico tenga prioridad para asegurar la calidad esperada durante una conversación.

La calidad de servicio respecta al trato preferencial que se le tiene que otorgar cierto tipo de tráfico, entregado principalmente mediante el manejo de colas. Algunos ejemplos de calidad de servicio son CBWFQ (Class Based Weighted Fair Queuing), RSVP (RESERVATION Protocol–RFC 2205), MPLS, (Multi Protocol Label Switching–RFC 1117). Las redes que experimentan problemas de congestionamiento pueden proporcionar transmisiones de voz con calidad siempre y cuando utilicen una política adecuada de QoS.

2.10.3 Condicionantes para la calidad en las transmisiones

Además de los factores inevitables (latencia, jitter, pérdida de paquetes) que intervienen para que una red disminuya la calidad en sus transmisiones, existen otros factores que se deben tomar en cuenta para un óptimo funcionamiento de la red. Factores que tienen que ver con la forma en que se realice la implementación de una infraestructura VoIP.

La relación entre los parámetros de QoS con respecto a la calidad en las transmisiones de voz será determinada por factores de la implementación para proporcionar servicios de voz en una red IP, tales como:

- **Codecs de voz:** La forma en que las señales de voz son digitalizadas para su transmisión.

2.10.3.1 Codecs de voz

Los codecs (coder/decoder) son generalmente entendidos como modelos matemáticos utilizados para codificar (y comprimir) digitalmente información de audio analógico.
El propósito de la mayoría de los algoritmos de codificación de audio es establecer una relación entre eficiencia y calidad. La tabla II-4 muestra una guía de referencia de algunos los códecs más utilizados.

Tabla II-4 Guía de referencia de los codecs más utilizados

Codec	Data britate (Kbps)	¿Requiere licencia?
G.711	64 Kbps	No
G.726	16, 24, 32 o 40 Kbps	No
G.729A	8 Kbps	Si
GSM	13 Kbps	No
Speex	Varía (entre 2.15 Kbps y 22.4 Kbps)	No

- **G.711**

  Es el codec fundamental de la red de telefónica pública. Este es el codec del cual se derivan todos los demás codecs. G.711 impone un mínimo de carga al CPU. Sin embargo, la que lo hace inconveniente es el requerimiento de ancho de banda que establece. Lo cual para cierto tipo de redes es un factor importante a considerar.

- **G.726**

  Este codec ha estado presente por algún tiempo (solía ser G.721, el cual es ahora obsoleto), y es uno de los codecs comprimidos originales, también conocido como ADPCM (Adaptive Differential Pulse-Code Modulation), y puede funcionar en varios bitrates.

  Los más comunes son 16 Kbps, 24 Kbps, y 32 Kbps. Este codec ofrece una calidad casi idéntica a la proporcionada por G.711, pero sólo requiere la mitad de ancho de banda.

- **G.729A**

  Considerado como el que utiliza el menor ancho de banda, G.729A entrega un sonido con calidad impresionante. Esto lo realiza mediante el uso de CS-ACELP (Conjugate-Structure Algebraic-Code-Excited Linear Prediction). Debido a su patente, el codec G.729A no puede ser usado sin el previo pago de una licencia; sin embargo, es muy popular, y tiene soporte para distintos teléfonos y sistemas. Para alcanzar su impresionante calidad en el sonido con el menor requerimiento de ancho de banda, este codec requiere de una gran cantidad de esfuerzo por parte de la CPU.

- **GSM**

  Este codec no viene cubierto con un requerimiento de licencia como lo tiene G.729A, y ofrece un rendimiento destacado con respecto a la demanda que pone en la CPU.

  La calidad del sonido es generalmente considerado a ser sólo un poco menor al producido por G.729A. GSM opera a los 13 Kbps.

- **Speex**

  Es un codec VBR (Variable Bitrate), lo cual significa que es capaz de modificar dinámicamente su bitrate para responder a cambios de condiciones en la red. Speex es totalmente un codec libre (free codec). Más información puede ser encontrada en su sitio en Internet (http://www.speex.org). Speex puede operar de 2.15 a 22.4 Kbps, debido a su bitrate variable.

La tecnología de VoIP es muy extensa, y para propósitos del presente trabajo sólo se han tomado en cuenta aquellos aspectos que son relevantes para el mismo. Tocando sólo los puntos que se relacionan directamente con el rendimiento de la red. Para una mejor compresión de esta tecnología e incluso echar a andar un servidor VoIP (asterisk), se dejan a reserva las lecturas[5] que pueden brindar una mejor perspectiva de esta tecnología.

[5] Romero Barrientos, Mauricio Alfredo. Convergencia entre redes de voz y datos. 2007

CAPÍTULO III

DISEÑO DE LA RED INALAMBRICA Y SISTEMA DE SEGURIDAD

3.1 INTRODUCCIÓN

El diseño y la implementación del presente trabajo se realizó utilizando equipos de cómputo y herramientas de software libre. Lo cual resultó todo un éxito, tal como ha sucedido en muchos otros casos, abaratando costos de implementación.

Este capítulo se enfoca en el diseño e implementación de un escenario de red inalámbrico que se basa en un AP Primario y un AP WDS Bridge interconectados entre sí para brindar servicio de internet y video llamadas. Permitiendo a aquellas personas que dispongan de un computador portátil conectarse a la red para navegar y usar el servicio de voz sobre IP.

La implementación se desarrollará según las necesidades, presupuesto y/o requerimientos del Departamento de Sistemas y Telemática de la Escuela Superior Politécnica de Chimborazo.

3.2 DISEÑO Y UBICACIÓN DE LOS PUNTOS DE ACCESO

Para el diseño de la Red Inalámbrica se ha tomado en cuenta principalmente la estructura del edificio, el área que se desea cubrir y la velocidad las tarjetas inalámbricas que se usaran en los Servidores GNU/Linux.

En la tabla III-5 se listan los elementos requeridos para la implementación del WDS, tanto de software como de hardware. En la misma tabla se especifican algunos datos particulares, como modelos de algunos dispositivos y versiones de software, utilizados en la presente implementación.

Tabla III-5 Elementos requeridos para la implementación de los APs

HARDWARE	SOFTWARE
Dos computadoras: • AP Primario – Procesador Pentium IV a 3 GHz – 512 MB de memoria RAM • AP WDS Bridge – Procesador AMD Athlon o Celeron a 1 GHz – 256 MB de memoria RAM	Sistema Operativo GNU/Linux: • Distribución Debian 4.0 (etch) Paquetes: • wireless-tools • bridge-utils • linux-headers-`uname –r`
3 tarjetas de red inalámbricas con chip Atheros, las utilizadas en esta investigación son las siguientes: • Una D-Link DWL-G520 • Dos TP-Link TL-WN550G/ TL-WN551G	Controlador MadWifi: • madwifi-0.9.3.3 (versión utilizada en esta implementación)

El diseño de la red inalámbrica se muestra en la figura III.16 a continuación.

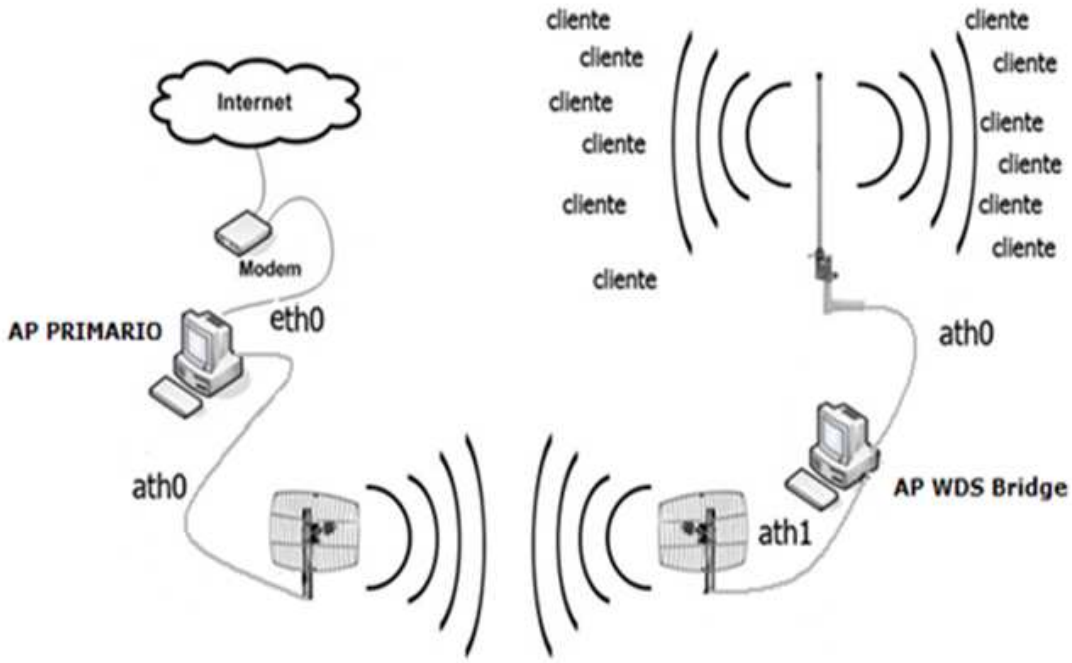


Figura III.16 Diseño de la Red Inalámbrica

3.3 ESQUEMA DE RED

3.3.1 Situaciones donde es útil un WDS

Una vez ya dejado en claro los aspectos teóricos relevantes con la tecnología 802.11. Se entra en materia en los aspectos de implementación propio del sistema de distribución inalámbrico.

Para ello se ejemplifican situaciones en las que puede ser útil el empleo de un sistema de distribución inalámbrico. Y dejar de forma precisa, las situaciones en las que sí es conveniente establecer un WDS para el enlazar redes. Ya que de ninguna manera el presente trabajo de investigación propone el uso de un WDS como backbone de la red, es decir, que los enlaces WDS sean el sistema de distribución (DS) de toda una infraestructura de red.

Algunas de las razones en las cuales se fundamenta la situación anterior son las siguientes:

- Por qué reducir el ancho de banda de nuestro DS a 54Mbps, y por ende congestionar más fácil nuestra red, cuando se puede incluso tener un DS Gigabit.

Las situaciones donde puede ser útil en enlace vía un WDS son muy particulares, dichas situaciones se pueden presentar en distintos escenarios:

- En sitios donde no es posible la instalación de una infraestructura de red de medios guiados debido a barreras físicas.
- Lugares donde no está permitido el deterioro de las instalaciones (realizar agujeros con taladros, perforar paredes con clavos), tales como sitios declarados patrimonio cultural.
- Para aquellas situaciones en las que se tiene que improvisar una infraestructura de conexión inalámbrica.

3.3.2 AP basado en GNU/Linux

Aunque en la actualidad, el aspecto financiero ya no es un impedimento para la adquisición de un punto de acceso común. Debido a los costos accesibles en los que se pueden encontrar gran cantidad de puntos de acceso comerciales.

Y que dichos puntos de acceso cuentan con asistentes de configuración "intuitivos" (Siguiente, siguiente...). Existen situaciones en las que requiere más flexibilidad de configuración que la que ofrece un simple asistente de configuración. Algunas de las ventajas que tiene la utilización de puntos de acceso implementados con herramientas de software libre son las siguientes:

- Se deja abierta la posibilidad de implementar nuevas tecnologías para redes WLAN.
- Se pueden realizar adecuaciones a requerimientos específicos.
- Puede usarse equipo no muy poderoso en cuanto a hardware.
- Flexibilidad de configuración.

Son esas razones por las que el presente trabajo realiza la implementación en puntos de acceso basados en GNU/Linux.

El elemento principal de implementación del presente trabajo son los puntos de acceso. Puntos de acceso que operan sobre computadoras con un sistema operativo GNU/Linux. A las cuales, se les instalaron tarjetas inalámbricas que soportan distintos modos de operación, entre ellos el modo punto de acceso.

Para la implementación de un punto de acceso basado en GNU/Linux, se necesitan los siguientes elementos:

- Una computadora con el sistema operativo GNU/Linux. La distribución Debian en su versión 4.0 (etch).
- El paquete wireless-tools
- Una tarjeta de red inalámbrica con chip Atheros.
- El controlador MadWifi[6] para la tarjeta inalámbrica.

La figura III.17 ilustra la forma en que el AP basado en GNU/Linux funciona para proporcionar servicios a estaciones clientes.

[6] http://madwifi.org

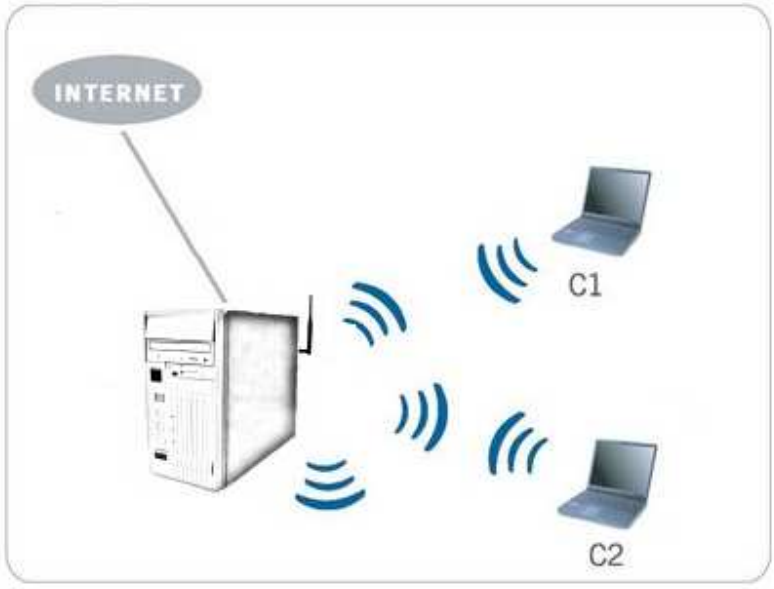


Figura III.17 Contexto inalámbrico mediante un AP basado en GNU/Linux

3.3.3 RADIUS (Remote Authentication Dial-In User Server)

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

Cuando se realiza la conexión hacia una Red Inalámbrica, se envía previamente un nombre de usuario y una contraseña hacia un dispositivo cliente NAS (punto de acceso) sobre el protocolo PPP, quien redirige la petición hacia un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba si el usuario se encuentra autorizado, utilizando métodos de autenticación como EAP. Si el usuario y su contraseña son válidos, el servidor de autenticación autorizará el acceso a la Red Inalámbrica, asignándole una dirección IP, mediante el uso de direccionamiento dinámico o DHCP, el cual se encuentra configurado en el AP GNU/Linux.

3.4 SERVIDOR DE AUTENTICACIÓN FREERADIUS

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

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

3.4.1 Autenticación

Consiste en el proceso de validar la petición de un usuario, el cual quiere hacer uso de los recursos de la red inalámbrica. El proceso de autenticación se realiza mediante la presentación de identidad y credenciales por parte del usuario.

La identidad del usuario viene a ser el nombre o alias con el cual está registrado en la base de datos del servidor de autenticación, mientras que las credenciales se implementarán mediante contraseñas, aunque también podría incluirse el uso de certificados digitales.

El protocolo de autenticación usado será EAP-MD5, este protocolo es usado entre el servidor FreeRADIUS y el Punto de Acceso para el proceso de autenticación de los usuarios.

Existen varios métodos de autenticación que son soportados por el servidor FreeRADIUS, algunos de los cuales se detallan a continuación:

- EAP-MD5
- EAP-TLS
- EAP-PEAP MSCHAPv2
- EAP-TTLS
- Kerberos

3.4.2 Autorización

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

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

3.4.3 Contabilidad

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

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

3.5 BASE DE DATOS DE USUARIOS DE LA RED

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

La plataforma FreeRADIUS puede soportar las siguientes bases de datos:

- MySQL
- Oracle
- PostgreSQL

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

3.5.1 Base de datos MySQL

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

Las tablas creadas en MySQL se detallan a continuación:

- *badusers*: Contiene la información de los usuarios que no pudieron conectarse a la red inalámbrica, por proveer una incorrecta credencial.
- *nas*: Consiste en el cliente o clientes NAS o puntos de acceso los cuales realizan la autenticación hacia el servidor FreeRADIUS.
- *radcheck*: Contiene todas las contraseñas de cada uno de los usuarios autorizados a hacer uso de la red inalámbrica.
- *radgroupcheck*: Muestra los grupos de usuarios que contienen un método de autenticación, como por ejemplo EAP-MD5.
- *radgroupreply*: Muestra todos los grupos de usuarios creados con sus protocolos y características de cada uno de ellos. Cabe mencionar que los usuarios pertenecientes a un grupo, adoptarán las características del grupo al que forman parte.
- *radpostauth*: Contiene un reporte sobre los procesos de autenticación realizados satisfactoriamente, cada proceso es almacenado en el día y la hora exacta.
- *usergroup*: Contiene la tabla de todos los usuarios, indicando los grupos a los que pertenecen.
- *userinfo*: Contiene todas las características de los usuarios, como por ejemplo: número telefónico de casa o trabajo, teléfono móvil, departamento y correo electrónico.

3.6 CLIENTES FREERADIUS

3.6.1 NAS (Network Access Server)

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

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

3.6.2 Portal Cautivo - HOTSPOT

Un portal cautivo es una página Web con la cual un usuario de una red pública y/o privada debe interactuar antes de garantizar su acceso a las funciones normales de la red. Estos portales son principalmente utilizados por centros de negocios, aeropuertos, hoteles, cafeterías, cafés Internet y otros proveedores que ofrecen hotspots de Wi-Fi para usuarios de Internet.

Cuando un usuario potencial se autentica por primera vez ante una red con un portal cautivo, una página Web se presenta en la cual se requieren ciertas acciones antes de proceder con el acceso. Un portal cautivo sencillo obliga al visitante para que por lo menos mire (así no lea) y acepte las políticas de uso, y luego acepte presionando sobre un botón en la página. Supuestamente esto puede absolver al proveedor del servicio de cualquier culpa por el uso anormal y/o ilegal del servicio.

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

3.6.3 Servidor HTTP Apache

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

3.7 DIAGRAMA DE SOLUCIÓN PARA UNA RED INALÁMBRICA SEGURA

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

El proceso de autenticación de usuarios se realiza mediante un servidor FreeRADIUS, el cual realiza las peticiones a los suplicantes, a través de los clientes NAS. El método de autenticación usado será el EAP-MD5/802.1x, el cual hace uso de la identidad del usuario y una contraseña para poder acceder a la red.

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

A su vez, se contará con una Portal Cautivo denominado "AirMarshal", el cual es de sencillo de usar, donde se podrá crear las cuentas de usuario y contraseñas directamente en la base de datos, así como poder realizar pruebas de testeo sobre el servidor de autenticación.

Este modelo sistema de seguridad se encuentra esquematizado en la figura III.18

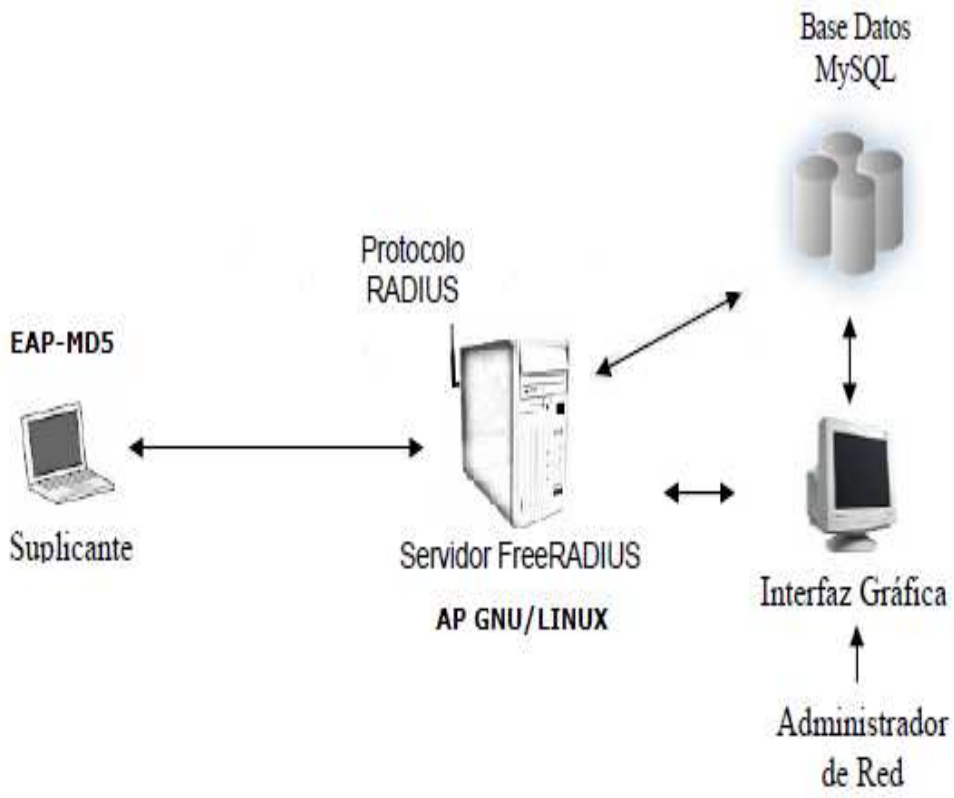


Figura III.18 Diagrama del Sistema de Seguridad

3.8 SISTEMA DE DISTRIBUCIÓN INALÁMBRICO

La implementación del sistema de distribución inalámbrico se propone para ser utilizado el situaciones muy concretas, tales como en las que no se posible establecer una conexión con medios guiados. Ver figura III.19.

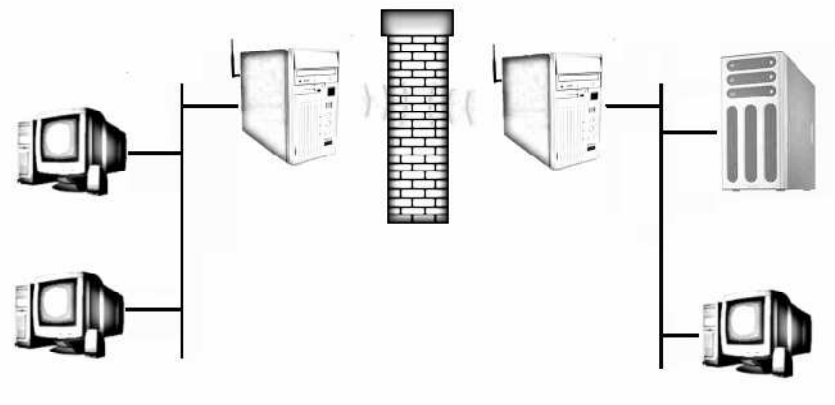


Figura III.19 Enlace WDS para conectar una red que presenta barreras físicas

O en situaciones en las que se tiene que improvisar una red que proporcione conectividad vía inalámbrica, figura III.20.

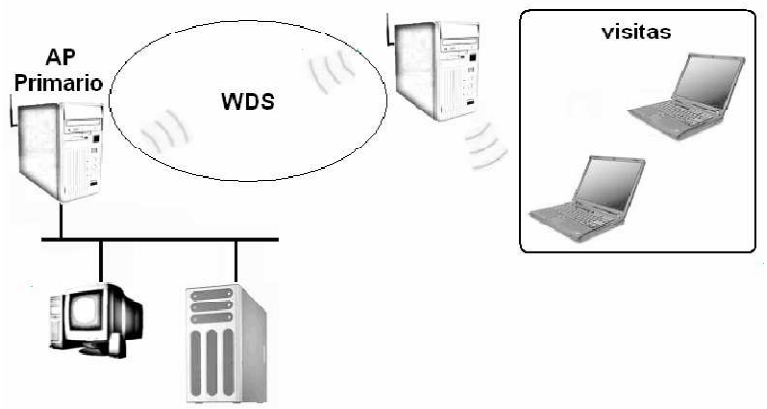


Figura III.20 Enlace WDS para dar señal a las estaciones distantes del AP primario

3.9 INSTALACIÓN Y CONFIGURACIÓN DE PAQUETES NECESARIOS

3.9.1 AP Primario

Para poder configurar un computador como Access Point (AP), es necesario de la instalación de un driver adicional llamado madwifi y que se usa generalmente con

tarjetas de red inalámbricas que posean chip Atheros. La instalación de los siguientes paquetes es necesaria para dar soporte a los controladores de madwifi:

```
#apt-get install linux-headers -`uname -r`
# apt-get install fakeroot build-essential
# apt-get install wireless-tools
# apt-get install bridge-utils
```

El driver madwifi se lo encuentra en código fuente y también en binario pero solo para la distribución Debian dentro de los mismos DVDs de instalación. En este caso se uso el controlador en código fuente en su versión 0.9.3.3:

```
# cd /usr/src
# wget http://downloads.sourceforge.net/project/
   madwifi/madwifi/0.9.3.3/madwifi-0.9.3.3.tar.gz
# tar zxvf madwifi-0.9.3.3.tar.gz
```

Una vez que se haya descargado y descomprimido el archivo, se debe ingresar en el nuevo directorio creado para poder hacer la instalación:

```
# cd madwifi-0.9.3.3.tar.gz
# make && make install
```

Ahora se procede a verificar que el controlador se haya instalado correctamente y que no se genere ningún error al momento de cargarse. Luego se verifica que una interfaz athX sea visualizada entre las interfaces de red:

```
# modprobe ath_pci  && echo "controlador funcionando"
# ifconfig
```

Para habilitar la tarjeta inalámbrica en modo Access Point siempre que el computador arranque, se debe modificar el archivo interfaces dentro del directorio /etc/network:

```
# nano /etc/network/interfaces
#configuracion de la interfaz de red  por la que se accede a
#internet.
iface eth0 inet static
       address 192.168.1.6
       netmask 255.255.255.248
       network 192.168.1.0
       broadcast 192.168.1.7
       gateway 192.168.1.1
       dns-nameservers 192.168.1.1
#configuracion de la interfaz de red (inalámbrica) que dara
#conexion a la LAN.
iface ath0 inet static
       address 10.122.10.1
       netmask 255.255.255.0
       broadcast 10.122.10.255

#El modo y canal que se utilizara.
wireless-mode master
wireless-channel 10

#El SSID que es el nombre de red en la que operaran los usuarios.
wireless-essid HELEN-AP

#Habilitar la interfaz de red inalambrica para que trabaje en modo
#master y de este modo crear el access point
pre-up ifconfig ath0 down
pre-up wlanconfig ath0 destroy
pre-up wlanconfig ath0 create wlandev wifi0 wlanmode ap
pre-up iwpriv ath0 wds 1
```

3.9.2 AP WDS Bridge

La configuración del AP WDS Bridge difiere su configuración en relación al AP Primario debido a que éste último contará con 2 tarjetas de red y su configuración será contenida por un script que se cargará al momento de iniciar el computador.

Los scripts pueden ser diferentes dependiendo de la configuración que se use de acuerdo a las necesidades, a continuación se describirán las dos opciones que se usaron y que dieron resultado exitoso.

```
wlanconfig ath0 create wlandev wifi0 wlanmode ap
wlanconfig ath1 create wlandev wifi1 wlanmode wds
iwconfig ath0 essid HELEN-AP
iwpriv ath1 wds_add 00:1B:11:1C:38:E1
iwpriv ath1 wds 1
iwpriv ath0 wds 1
ifconfig ath1 0.0.0.0 up # Esperar asociación
ifconfig ath0 0.0.0.0 up
brctl addbr br0
brctl stp br0 off
brctl addif br0 ath0
brctl addif br0 ath1
brctl setfd br0 1
ifconfig br0 10.122.10.101 netmask 255.255.255.0 up
route add default gw 10.122.10.1 br0
```

En este script se usó la dirección MAC para que el AP WDS Bridge se asocie únicamente con el AP Primario cuya dirección MAC sea 00:1B:11:1C:38:E1, sin importar que ESSID posea.

En el siguiente script se usará una configuración diferente que no necesitará de una dirección MAC y que será más simple debido a que se hará referencia al ESSID del AP Primario.

```
wlanconfig ath0 create wlandev wifi0 wlanmode ap
wlanconfig ath1 create wlandev wifi0 wlanmode sta nosbeacon
iwconfig ath0 essid HELEN-AP
iwconfig ath1 essid HELEN-AP
iwpriv ath0 wds 1
iwpriv ath1 wds 1
ifconfig ath1 up #esperar la asociación
ifconfig ath0 up
brctl addbr br0
brctl addif br0 ath0
brctl addif br0 ath1
brctl setfd br0 1
ifconfig br0 10.122.10.101 netmask 255.255.255.0 up
route add defatult gw 10.122.10.1 br0
```

3.9.3 Configuración del servidor DHCP

Es indispensable poder contar con un servidor de DHCP para poder asignar direcciones dinámicamente a los clientes que se conecten a la red inalámbrica para que puedan navegar en internet o puedan realizar video llamadas.

Hay que tomar en consideración que el servicio de direccionamiento IP con DHCP debe ser instalado y configurado exclusivamente en el AP Primario ya que el segundo AP trabajará como un puente o repetidor.

```
# apt-get  install dhcp3-server

# nano  /etc/dhcp3/dhcpd.conf
```

```
# option definitions common to all supported networks...
option domain-name "apprimario.org";
option domain-name-servers 192.168.1.1;

subnet 10.122.10.0 netmask 255.255.255.0 {
       range 10.122.10.100 10.122.10.200;
       option broadcast-address 10.122.10.255;
       option routers 10.122.10.1;
}
```

Modificar el siguiente archivo para asignar el servicio de DHCP por la interfaz ath0 en el archivo dhcp3-server dentro del directorio /etc/default:

```
# Defaults for dhcp initscript
# sourced by /etc/init.d/dhcp
# installed at /etc/default/dhcp3-server by the maintainer scripts

#
# This is a POSIX shell fragment
#

# On what interfaces should the DHCP server (dhcpd) serve DHCP
requests?
#     Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="ath0"
```

Figura III.21 Archivo /etc/default/dhcp3-server

Finalmente reiniciar el servicio:

```
# /etc/init.d/dhcp3-server restart
```

3.9.4 Servidor Freeradius

Para instalar el Servidor Freeradius con soporte para mysql, se debe ejecutar el siguiente comando:

```
# apt-get install freeradius freeradius-mysql
```

Modificar en el archivo "clients.conf" la línea secret, que será la contraseña del servidor FreeRadius.

```
# nano /etc/freeradius/clients.conf
```

```
[…]
client 10.122.10.0/24 {
       secret       = wdscliente
       shortname    = localhost
       nastype     = other # localhost isn't usually a NAS...
}
[…]
```

Modificar el archivo *radiusd.conf* ==> este archivo contiene información necesaria sobre los archivos de configuración de FreeRadius y también de la manera de conectarse a través de MySQL.

Eliminar los comentarios de todo el apartado referente al enunciado "sql_log":

```
# nano /etc/freeradius/radiusd.conf
```

```
#
#  See rlm_sql_log(5) manpage.
#
sql_log {
        path = "${radacctdir}/sql-relay"
        acct_table = "radacct"
        postauth_table = "radpostauth"
        sql_user_name = "%{%{User-Name}:-DEFAULT}"

        Start = "INSERT INTO ${acct_table} (AcctSessionId, UserName, \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '%S', '0', '0', '');"
        Stop = "INSERT INTO ${acct_table} (AcctSessionId, UserName,  \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '0', '%S', '%{Acct-Session-Time}',  \
         '%{Acct-Terminate-Cause}');"
        Alive = "INSERT INTO ${acct_table} (AcctSessionId, UserName, \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '0', '0', '%{Acct-Session-Time}','');"

        Post-Auth = "INSERT INTO ${postauth_table}                   \
         (username, pass, reply, authdate) VALUES                            \
         ('%{User-Name}', '%{User-Password:-Chap-Password}',         \
         '%{reply:Packet-Type}', '%S');"
}

#
#  Create a unique accounting session Id.  Many NASes re-use
#  or repeat values for Acct-Session-Id, causing no end of
SERT --
```

Figura III.22 Archivo /etc/freeradius/radiusd.conf

Modificar el archivo *sql.conf* para especificar el tipo de base de datos a usarse, la dirección o nombre del servidor, el nombre del usuario que tiene permisos sobre la base de datos con su contraseña y el nombre de la base de datos usada por Freeradius.

nano /etc/freeradius/sql.conf

```
sql {
        #
        #  Set the database to one of:
        #
        #       mysql, mssql, oracle, postgresql
        #
        database = "mysql"

        #
        #  Which FreeRADIUS driver to use.
        #
        driver = "rlm_sql_${database}"

        # Connection info:
        server = "localhost"
        login = "root"
        password = ""

        # Database table configuration for everything except Oracle
        radius_db = "radius"
        # If you are using Oracle then use this instead
        # radius_db = "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=localhost)(PORT=1521))(CONNECT_DATA=(SID=your_sid)))"

        # If you want both stop and start records logged to the
        # same SQL table, leave this as is.  If you want them in
        # different tables, put the start table in acct_table1
        # and stop table in acct_table2
        acct_table1 = "radacct"
        acct_table2 = "radacct"

        # Allow for storing data after authentication
        postauth_table = "radpostauth"
```

Figura III.23 Archivo /etc/freeradius/sql.conf

Modificar el archivo *radiusd.conf* y descomentar las líneas que contengan "sql" y "sql_log" en los apartados "authorize" y "accounting".

nano /etc/freeradius/radiusd.conf

```
[…]
authorize {
       preprocess
       chap
       mschap
       suffix
       eap
       sql
}
accounting {
       detail
       unix
       radutmp
       sql
       sql_log
}
[…]
```

Ejecutar los siguientes comandos para crear el archivo *schema.sql* con el contenido de todas las tablas usadas por el servidor Freeradius:

cd $HOME (para dirigirse al directorio personal del usuario)

zcat /usr/share/doc/freeradius/examples/mysql.sql.gz >> schema.sql

Los archivos *.sql deben ejecutarse en la sección de ejecutar archivos sql dentro del paquete webmin que será configurado más adelante.

Descargar el paquete webmin-1.5.20 para la distribución Debian y luego instalarlo, usando los siguientes comandos:

wget

http://prdownloads.sourceforge.net/webadmin/webmin_1.520_all.deb

dpkg –i webmin_1.520_all.deb

Luego de la instalación se podrá acceder a Webmin para administrar la mayoría de servicios y servidores del sistema vía Web. El nombre de usuario y su password son los mismos que los del administrador del sistema, en este caso sería el usuario root. Escribir en el browser o navegador, lo siguiente para ingresar a administrar el sistema con webmin:

http://localhost:10000/

Figura III.24 Ingreso de usuarios a Webmin

Luego de autenticarse, se puede ingresar a la interfaz web para configurar el sistema y se puede cambiar el idioma del webmin a español o dejar el idioma inglés por defecto.

Ahora se debe ir al apartado Servidores y ubicarse en Servidor de Base de Datos MySQL, luego de esto se mostrará una pantalla en la cual se elige crear una nueva base de datos.

Crear una base de datos llamada *radius* y no escribir nada en el resto de campos porque luego se ejecutara el archivo *schema.sql* con el código sql para crear las tablas para la base de datos.

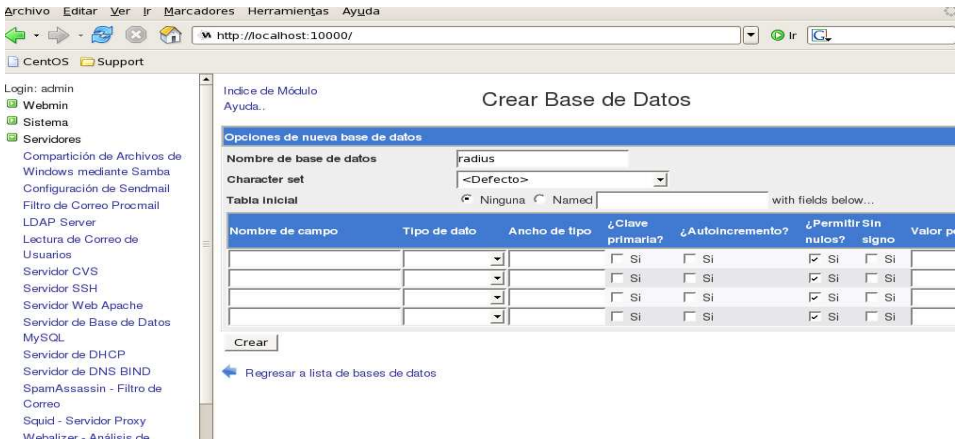


Figura III.25 Creación de la base de datos para Freeradius

Luego dar clic sobre la base de datos *radius* y dar clic en ejecutar SQL para poder ejecutar los archivos sql. Escoger la opción "Run SQL from file" y ubicar el archivo *schema.sql* que se encuentra en */root*.

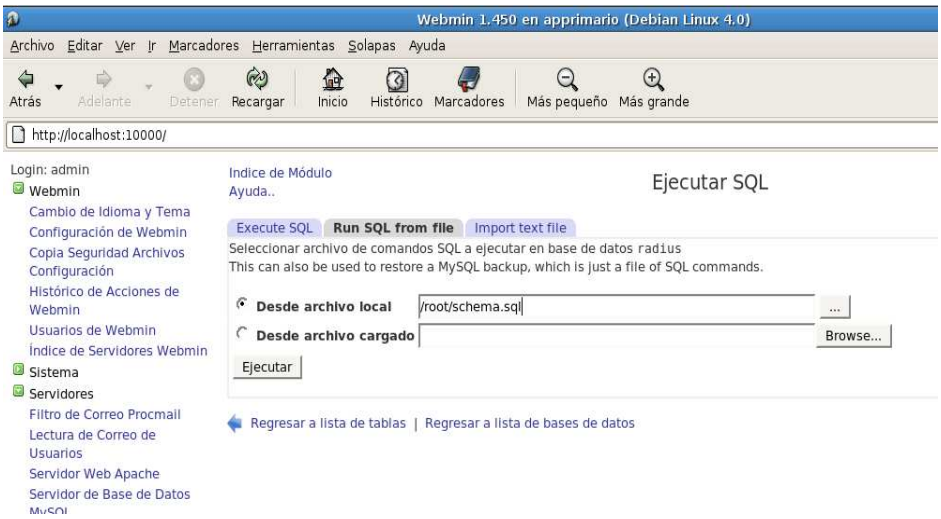


Figura III,26 Creación de las tablas para la base de datos de Freeradius

Cuando se haya ejecutado el archivo *schema.sql*, la base de datos *radius* deberá quedar de la siguiente manera, ver figura III.27

.

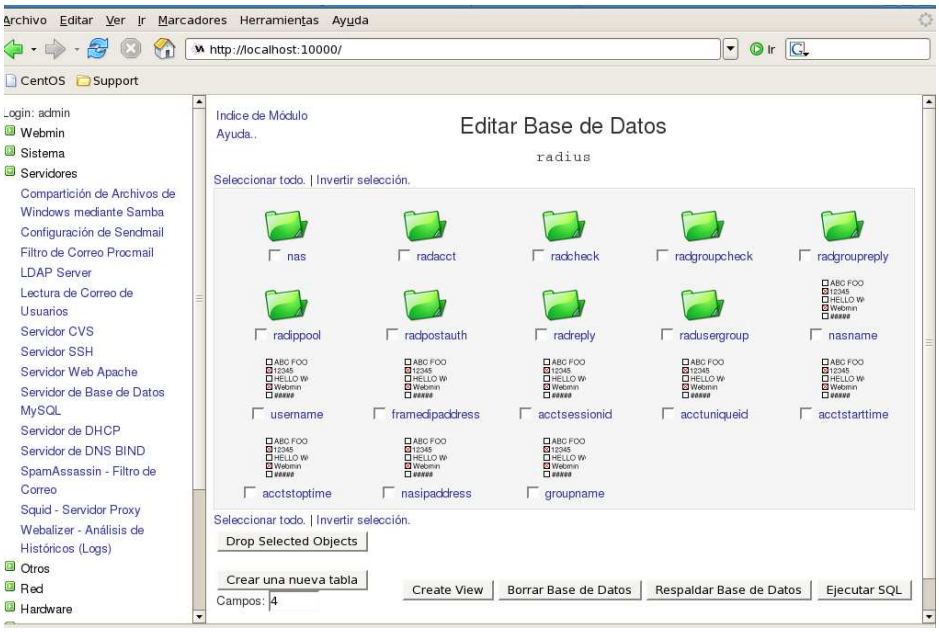


Figura III.27 Esquema de la base de datos de Freeradius

Una vez que se tenga la base de datos *radius* con las tablas correspondientes, se procede a llenar la tabla *radcheck* que es la tabla más importante ya que en esta se almacenan los usuarios con sus respectivas contraseñas.

El formato de los campos, es el siguiente:

campo	dato
id	ninguno (autoincrementado)
user	“nombre_usuario”
attribute	User-Password
op	:=
password	“password_usuario”

Al momento de dar clic en la tabla *radcheck*, se muestra una ventana como la de la figura III.28.

Figura III.28 Información sobre la tabla radchek

En la ventana anterior se muestra detalles de los campos de la tabla pero todavía no podemos ingresar datos, para eso hay que dar clic en el botón de más abajo que dice *Ver Datos* y se muestra otra ventana como en la figura III.29.

Figura III.29 Ver datos en la tabla radchek

Dar clic en el botón que dice *Añadir Fila* y en la siguiente ventana llenar los campos con información del usuario que se desea autenticar y se almacena el usuario al

hacer clic sobre el botón *Salvar*. En el campo *id* no se debe escribir nada debido a que el campo es autoincrementado.

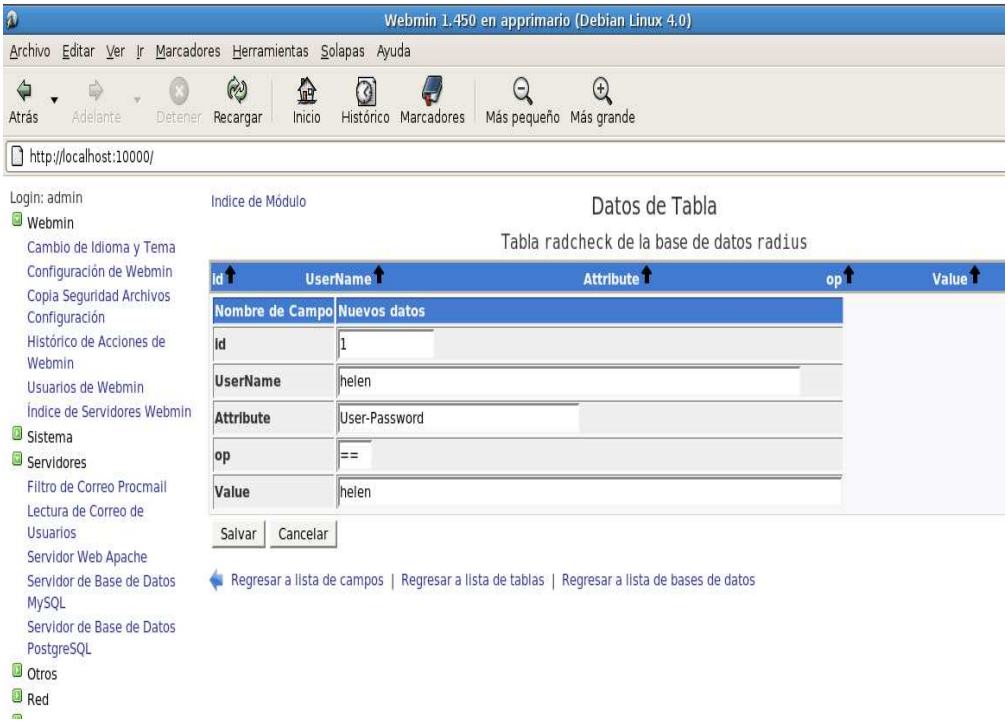


Figura III.30 Creación de usuarios

Una vez hecho esto se puede decir que ya se cuenta con al menos un usuario para ser validado en el servidor de autenticación FreeRadius.

Ahora se procede con la instalación y configuración del portal cautivo que será el encargado de presentar una pantalla de registro para la autenticación de usuarios con sus contraseñas, los cuales ya están almacenados en la base de datos llamada *radius*.

3.9.5 Portal Cautivo AirMarshal

A continuación se detalla la instalación y configuración del portal cautivo usado en esta tesis y que será de mucha utilidad para que los usuarios que quieran usar los servicios de red inalámbricos, primero sean autenticados y luego puedan acceder a los recursos brindados.

Los siguientes comandos se usaron para la instalación:

```
# cd /usr/src/
# mkdir airmarshal
# wget http://www.iea-
software.com/ftp/AirMarshalV2/linux/airmarshalv2_linux.tar.gz
# mv airmarshalv2_linux.tar.gz  airmarshal
# cd airmarshal
# tar zxvf  airmarshalv2_linux.tar.gz
# rm airmarshalv2_linux.tar.gz
# /usr/src/airmarshal
```

Ejecutar el instalador:

```
# ./install.pl
```

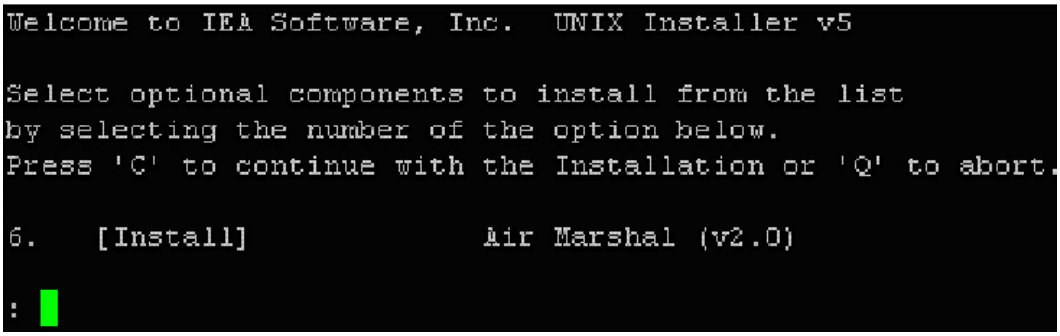


Figura III.31 Pantalla de instalación

Presionar "C" para continuar. Airmarshal está ahora instalado y configurado automáticamente para correr cuando el sistema inicie.

Ahora arrancar el servidor en modo DEBUG para poder configurarlo a nuestra conveniencia.

```
#/usr/local/portal/portald –debug
```

Usar un navegador en el que se deberá escribir la siguiente dirección http://[direccion del servidor]:81/settings, en nuestro caso:

```
http://10.122.10.1:81/settings
```

Ahora se le pedirá que cree una contraseña de administrador.

Se debe hacer clic en "Guardar" una vez que haya completado la configuración para la puesta en marcha del servidor. Después de probar que el servidor funciona correctamente, puede pulsar Ctrl-C para detener el modo de depuración y ejecutar el servidor en background, para esto:

```
# /usr/local/portal/portald
```

Se debe iniciar con la Configuración General. Ver figura III.32.

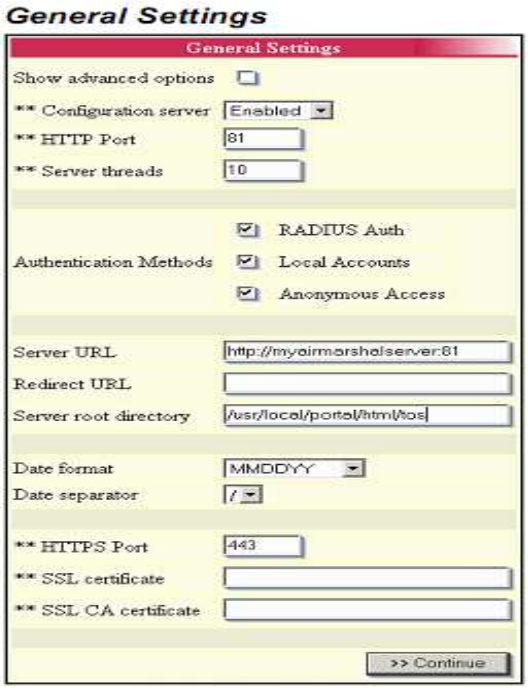


Figura III.32 Configuración General

Una vez configurado, hacer clic en "Guardar" para verificar la configuración y empezar a procesar las solicitudes del cliente. Si la validación presenta un mensaje de error para corregir los errores, vuelva a intentarlo. Una vez que la puerta de enlace muestra la barra de estado "Running", significa que AIRMARSHAL está activo y es capaz de procesar las solicitudes de red de acceso de los clientes.

Las interfaces de red y subredes controlada por la puerta de enlace de autenticación se configuran a través del menú "Opciones de red". Hay tres rutas de red disponibles las tecnologías disponibles según sus necesidades: IP Routing, Network Address Translation e IP Bridging; en nuestro caso usaremos la opción IP Bridging.

- ***IP Bridging (Capa 2)***

IP bridging implica combinar múltiples redes en la capa de Ethernet. El modo bridge interno de Airmarshal, se aplica de forma transparente y reorienta los servicios de autenticación de los datos y se desplazan a través del puente.

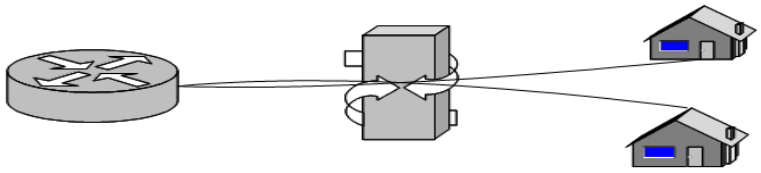


Figura III.33 Esquema IP Bridging

- ***RADIUS Auth***

La autenticación RADIUS proporciona la gestión centralizada de los clientes a través de todos los dispositivos de acceso a la red. Normalmente RADIUS se utiliza para

administrar un gran número de cuentas, que participan en redes móviles o la integración con la gestión de clientes.

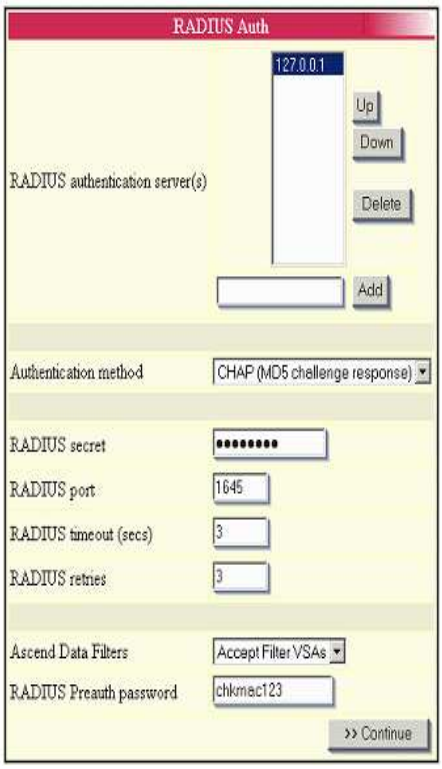


Figura III.34 RADIUS Auth

- ***RADIUS Accounting***

Tanto el inicio de sesión de clientes y registros contables de RADIUS se utilizan para almacenar información importante relacionada con los servicios proporcionados a cada cliente como el tiempo en línea, la cantidad de tráfico de datos, IP, MAC y la información de diagnóstico, como la razón de cada sesión cerrada. Estos datos son generalmente útiles para la amplia gama de tareas tales como la facturación por uso, la aplicación de los datos y los plazos, la gestión de acceso simultáneo, la capacidad de planificación, auditoría y resolución de problemas.

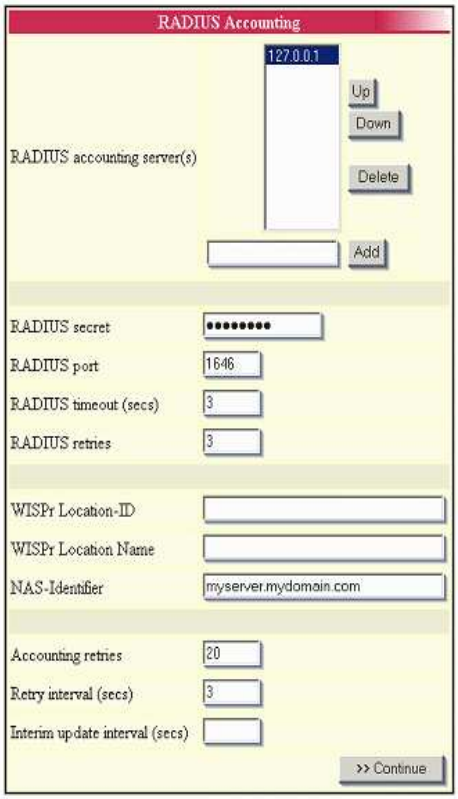


Figura III.35 RADIUS Accounting

3.10 CONSIDERACIONES

Para la implementación de un WDS se deben tomar en cuenta varios aspectos. Para poder tener un buen funcionamiento del WDS se deben tomar en cuenta los siguientes:

- El punto de acceso que se utilice para ampliar tiene que tener alcance al área de cobertura de señal del AP primario, tal como muestra lo muestra la figura III.36.
- Todos los puntos de acceso tienen que compartir el mismo ESSID.

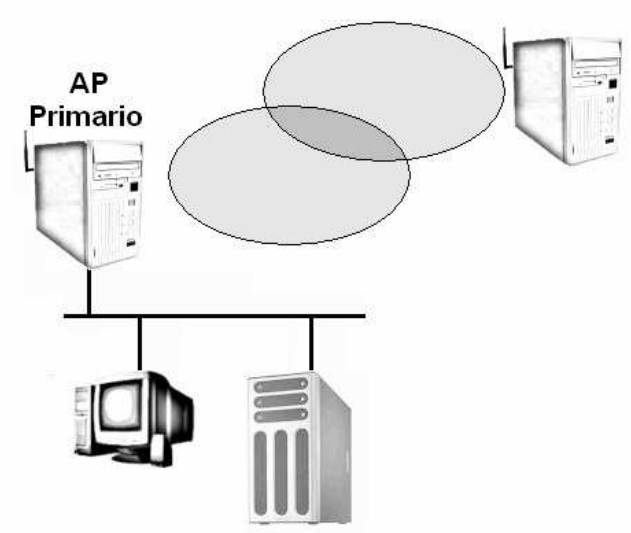


Figura III.36 Forma de ubicación de los APs en un enlace WDS

La implementación del WDS en este proyecto, consideró sólo un dominio de roaming a nivel de capa 2. Por lo que los dispositivos que se encuentren funcionando en el WDS, tienen que tener un direccionamiento dentro de la misma subred.

Aunque en el desarrollo de este trabajo sólo se creó un enlace WDS sólo entre dos puntos de acceso, no es regla que esto deba realizar así (sólo con dos puntos de acceso). Pero si se desea realizar en WDS con más de dos puntos de acceso se deben seguir tomando las siguientes consideraciones anteriormente mencionadas. Además de otra importante:

- Siempre que sea posible dar salida al tráfico de puntos de acceso por distintos APs conectados al backbone de la red (figura III.37), hacerlo de esta manera. Evitando con esto saturar de tanto procesamiento a un sólo AP, además de congestionar menos el enlace WDS de dicho AP.

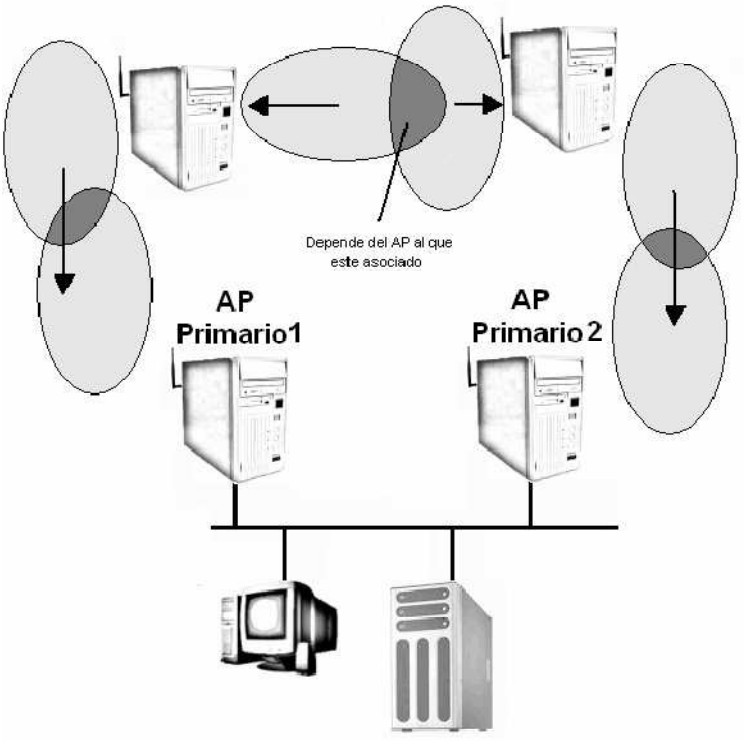


Figura III.37 Desahogo de tráfico por distintos flujos

3.11 INCONVENIENTES

Aunque el empleo de enlaces vía un WDS es valioso, también es cierto que se pueden presentar inconvenientes que mermen el uso de este tipo de enlaces.

Como lo muestra la figura III.38, debido a que los puntos de acceso obtienen los recursos mediante su enlace con el AP primario, si el AP primario llegase a fallar los puntos de acceso que dependen de él quedarían incomunicados, y por ende las estaciones que se encuentren asociadas a dichos puntos de acceso.

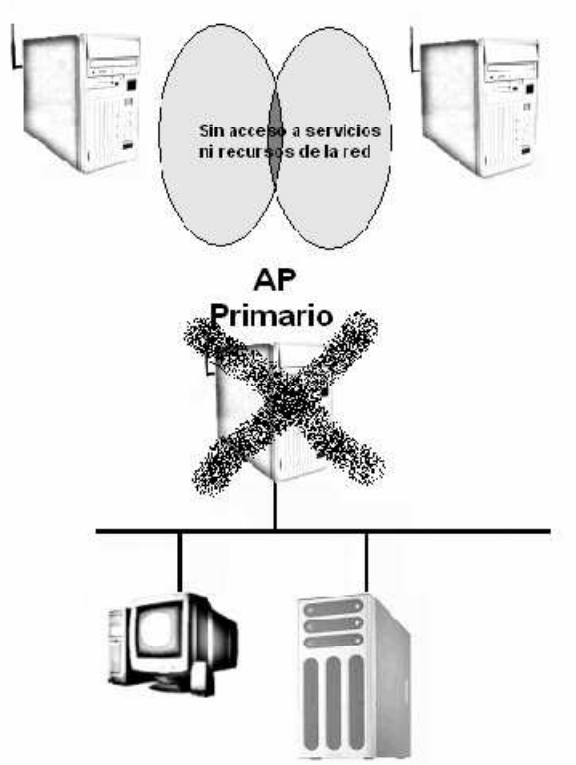


Figura III.38 WDS sin comunicación

3.12 COBERTURA PARA TRÁFICO VOIP

Para el sistema de distribución inalámbrico aplican las mismas políticas y reglas establecidas en la red. Si la red cuenta con un servidor VoIP, este servicio puede ser utilizado y correr sin ningún inconveniente por el WDS.

En el presente trabajo se configuró un sistema Asterisk para brindar el servicio de VoIP. Sin mayor problema se pudieron establecer conversaciones entre estaciones inalámbricas con portátiles conectadas indistintamente al AP Primario o al AP WDS Bridge.

Las conversaciones se realizaron mediante el uso de softphones[7] como: X-Lite, WengoPhone, Twinkle, Ekiga. Sin presentar ningún inconveniente, exceptuando aquellos casos en los que la configuración del audio no estaba correcta.

[7] Es un software que hace una simulación de teléfono convencional por computadora. Es decir, permite utilizar la computadora para hacer llamadas a otros softphones o teléfonos convencionales. Principalmente utilizados en entornos de VoIP.

CAPÍTULO IV

PRUEBAS DEL SISTEMA DE SEGURIDAD

4.1 INTRODUCCIÓN

El esquema de pruebas utilizado para la implementación en este trabajo es el que se muestra en la figura IV.39. El cual utiliza tanto estaciones inalámbricas como computadoras enlazadas con medios guiados. Dichos equipos habilitados con softphones para poder mantener conversaciones mediante VoIP.

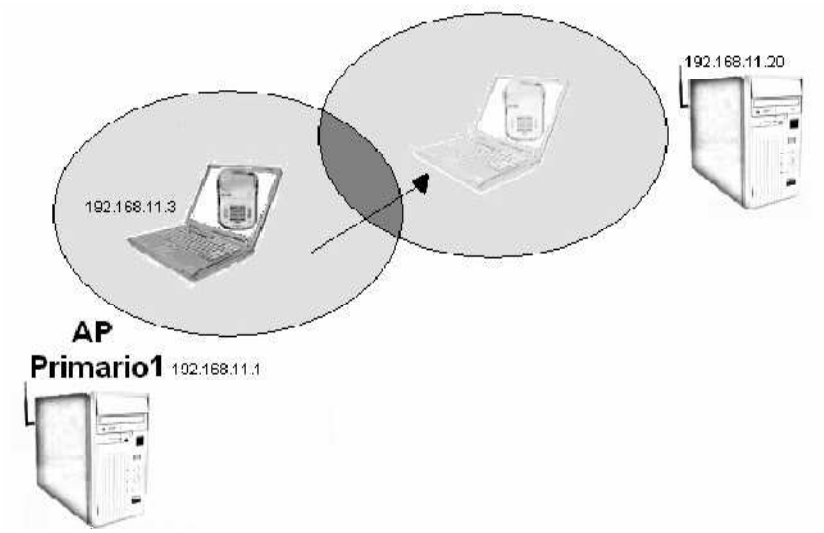


Figura IV.39 Esquema de pruebas

4.2 CONFIGURACIÓN CIFRADO WPA2

4.2.1 Configuración AP PRIMARIO

La configuración del AP Primario ya fue descrita en el capítulo anterior pero en este capítulo se explicará la razón por la cual no se pudo realizar el cifrado de la red inalámbrica usando WPA2.

Al principio se pensó utilizar un paquete adicional llamado HostAP para poder brindar un cifrado WPA2 en el AP Primario pero en las pruebas realizadas, se pudo comprobar que el WDS no soporta ningún tipo de cifrado.

La razón principal de este problema es que en el AP Primario se configuran todos los servicios y para el cifrado se usa un paquete adicional debido a que el driver madwifi no soporta ningún tipo de cifrado de manera nativa. Por esta razón el AP WDS Bridge que trabaja como un repetidor, no pudo establecer una asociación con el AP Primario.

A continuación se detalla la configuración del archivo *hostapd.conf* usado al inicio para la seguridad del WDS.

```
# nano /etc/hostapd.conf

[…]
ctrl_interface_group=0
ssid=HELEN-AP
hw_mode=g
channel=60
beacon_int=100
dtim_period=2
max_num_sta=255
rts_threshold=2347
auth_algs=3
ignore_broadcast_ssid=0
eap_server=0
```

```
own_ip_addr=10.122.10.1
wpa=2
wpa_psk=6fac17af904d6f57b1906598e0036c8776747ee995d8d24935fed5924
f1b3db9
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP CCMP
wpa_group_rekey=300
wpa_gmk_rekey=640
[…]
```

Una vez modificado el archivo *hostapd.conf*, basta con arrancar el servicio *hostapd* para que el AP Primario tenga protección mediante cifrado WPA2.

4.2.2 Configuración del AP WDS Bridge

La configuración del AP WDS Bridge es la misma que la descrita en el capítulo anterior.

4.3 PRUEBAS DE CONEXIÓN

Para comprobar que el AP WDS Bridge este asociado con el AP Primario, se ejecuta el comando siguiente:

```
# brctl showmacs br0
```

port no	mac addr	is local?	ageing timer
X	00:00:00:00:00:00	yes/no	0.00
X	00:11:00:00:00:00	yes/no	0.00
…	…	…	…

port no: Número de puerto usado para la comunicación de las interfaces de red con el AP WDS Bridge.

mac addr: Direcciones MAC de todos los equipos conectados al AP WDS Bridge.

is local?: Parámetro que especifica si el host conectado pertenece a la interfaz local del AP WDS Bridge o externo.

ageing timer: Tiempo de conexión de las interfaces de red, por lo general registra el tiempo de las interfaces de red externas.

A continuación se detallan las direcciones MAC tanto de los AP como de los clientes conectados:

- Interfaz ath0 ***AP WDS Bridge*** 00:23:cd:ff:a4:15
- Interfaz ath1 ***AP WDS Bridge*** 00:21:97:d0:cb:6f
- Interfaz ath0 ***AP Primario*** 00:1b:11:1c:38:e1
- Interfaz de cliente conectado 00:16:fe:3a:a1:9a

Ahora se procede a comprobar si el AP WDS Bridge logró asociarse con el AP Primario, ejecutando el comando *brctl* y almacenando la información en un archivo de texto de la salida de dicho comando para poder analizar los datos.

```
# brctl showmacs br0 >> salida_bridge.txt
# cat salida_bridge.txt
```

port no	mac addr	is local?	ageing timer
1	00:16:fe:3a:a1:9a	no	75.66
3	00:21:97:d0:cb:6f	Yes	0.00
1	00:23:cd:ff:a4:15	yes	0.00

Mediante la visualización del comando anterior, se puede comprobar que el AP WDS Bridge no pudo realizar la asociación con el AP Primario debido a que la dirección MAC del AP Primario no se muestra después de la ejecución del comando *brctl*.

Se realizaron múltiples pruebas para intentar la asociación del AP Primario con el AP WDS Bridge pero no se lograron resultados exitosos y la única manera de

comprobar la asociación es con el uso del comando *brctl showmacs br0* en el AP WDS Bridge.

Se ha comprobado de esta manera que la configuración no dió los resultados esperados de acuerdo al esquema inicial planteado en la hipótesis con cifrado WPA2.

En vista de que se dió de baja a la opción de usar cifrado WPA2, se utilizó un servidor de autenticación RADIUS para asegurar el WDS y restringir el uso de los servicios tanto de telefonía IP como de internet.

La solución que se dió, incluida la configuración de un servidor RADIUS para lograr tener seguridad inalámbrica compuesta por varios Access Points en un WDS, fue descrita en el Capítulo III. De esta manera tanto el AP Primario como el AP WDS Bridge quedan sin ningún tipo de cifrado para establecer la asociación entre ellos.

Para comprobar que el AP WDS Bridge este asociado con el AP Primario, se ejecuta el comando siguiente:

```
# brctl showmacs br0 >> salida_bridge.txt
# cat salida_bridge.txt
```

port no	mac addr	is local?	ageing timer
2	00:21:97:d0:cb:6f	yes	00.00
1	00:16:fe:3a:a1:9a	no	64.20
2	00:1b:11:1c:38:e1	no	94.77
1	00:23:cd:ff:a4:15	yes	0.00

Al aplicar la solución anteriormente mencionada, se puede visualizar que la dirección MAC **00:1b:11:1c:38:e1** que corresponde al AP Primario, aparece en la lista con lo cual se demuestra que la asociación se realizó satisfactoriamente.

4.4 PRUEBAS DE CONEXIÓN DE USUARIOS

Figura IV.40 Pantalla de ingreso al portal

Si el usuario ingresa correctamente su nombre y su password, se abrirá una ventana popup indicando el tiempo de conexión.

Figura IV.41 Pantalla Popup

Luego de dar clic sobre el botón "Navegar", se abrirá la página escrita en el browser del cliente y podrá usar los servicios de internet y telefonía IP. Ver figura IV.42.

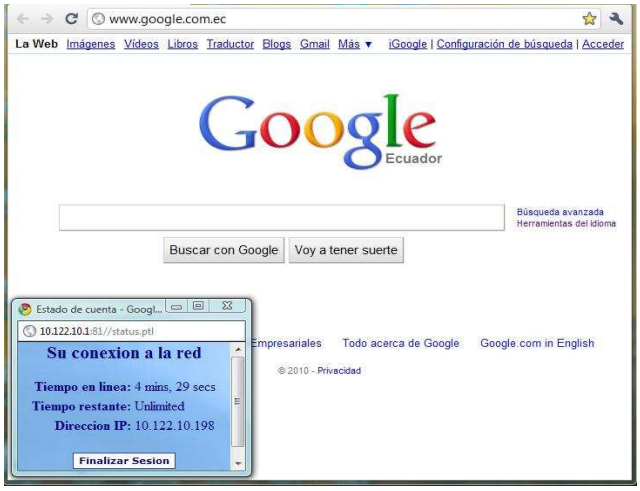


Figura IV.42 Pantalla de navegación

CONCLUSIONES

1. El desarrollo de este trabajo deja en claro que la implementación de un entorno de enlace de puntos de acceso para transmitir tráfico VoIP mediante una red 802.11 en un ambiente de software libre es una labor viable sin requerir elementos y esfuerzos adicionales en sus infraestructuras.

2. Para asegurar un sistema de distribución inalámbrico sin necesidad de disponer de ningún tipo de cifrado se requiere implementar un Portal Cautivo que permite el acceso a la red, brindando autenticación y autorización para utilizar los servicios de VoIP.

3. El auge que tiene la tecnología 802.11 ha provocado que cada vez más dispositivos móviles (teléfonos móviles, PDAs) introduzcan esta interfaz de esta tecnología en dichos dispositivos. El aspecto principal a tener en cuenta sigue siendo la seguridad.

4. Para poder seguir obteniendo resultados efectivos con el uso de herramientas de software libre tenemos que mantener una actitud adecuada y ética para seguir aprovechando sus beneficios.

5. La combinación del software libre con la tecnología 802.11 es una alternativa para la implementación de entornos de enlaces inalámbricos y de seguridad, obteniendo resultados satisfactorios.

6. El diseño de un sistema de distribución de red inalámbrico de área local es una solución versátil que permite el intercambio de información y acceso a Internet, pudiendo ser instalada en distintos lugares donde el cableado no pueda ser accesible permitiendo ampliar el área de cobertura.

7. Los precios de los productos para implementar redes inalámbricas se han estado reduciendo enormemente y continuarán bajando conforme se alcance el consumo masivo de software y hardware basados en tecnologías inalámbricas.

8. La seguridad es el factor más importante al diseñar una Red Inalámbrica, caso contrario se permitiría el acceso de personas sin autorización, exposición de nuestra información y el mal uso de los servicios.

9. Cuando se evalúa una solución inalámbrica es muy importante tener en cuenta los estándares y tecnologías de más penetración, ya que esta decisión ahorrará dinero, tiempo y problemas de incompatibilidad y brindará una comunicación rápida, eficiente, segura.

RECOMENDACIONES

1. Al diseñar una red inalámbrica, se debe tener especial cuidado con la elección del tipo de cifrado a utilizar ya que al usar herramientas de software libre, algunos estándares no pueden cumplirse.

2. Considerar el uso de GNU/Linux debido a que fue diseñado exclusivamente para servidores, brindando seguridad, estabilidad y escalabilidad.

3. Al configurar un computador como AP, se pueden expandir las posibilidades que brinda un AP comercial debido a que este no permite la instalación de módulos adicionales. El costo de implementación se ve reducido al usar GNU/Linux.

4. Utilizar en lo posible siempre un servidor de autenticación para asegurar una red inalámbrica, en este caso es altamente aconsejable el uso de un servidor Radius debido a la incompatibilidad que tiene un WDS al momento de utilizar algún tipo de cifrado.

5. Continuar incrementando funcionalidad al AP GNU/Linux ya que por el momento solo se cuenta con el servicio de proxy transparente para internet y el servicio de Voz IP.

RESUMEN

Se implementó mecanismos de seguridad de autenticación RADIUS, que permiten a usuarios autorizados hacer uso de servicios de telefonía IP e Internet en un Sistema de Distribución Inalámbrico (WDS) que brinda servicio de roaming.

El sistema operativo implementado fue Debian GNU/Linux Etch 4.0 instalado en PCs, con tarjetas de red inalámbricas con chip atheros. Se empleo un Portal Cautivo Airmarshal que permite el acceso a la red mediante métodos de autenticación de un servidor FREERADIUS, para brindar el servicio de roaming a la comunicación de VoIP se usaron métodos basados en un Sistema de Distribución Inalámbrico y Asterisk. Está basado en que los usuarios hacen una petición de conexión de red, el Portal Cautivo solicita nombre y contraseña, se transfiere al *servidor RADIUS* para la verificación y autorización, si es aceptado, el servidor permite el acceso a los recursos de red.

Se pudo comprobar que la implementación de una infraestructura de área distribuida inalámbrica (WDS) no soporta mecanismos de cifrado en este caso de estudio WPA2, por lo cual la implementación de un portal cautivo que permite el acceso mediante un servidor FRERADIUS, proporcionan con excelentes resultados confidencialidad, seguridad y autenticidad en la transmisión de tráfico en tiempo real VoIP en una área de cobertura que brinda el servicio de roaming.

SUMARY

Security mechanisms are implemented RADIUS authentication, which allows authorized users to use IP telephony and the Internet in a Wireless Distribution System (WDS) wich provides roaming service.

The operating system was implemented Debian GNU / Linux Etch 4.0 installed on PCs with wireless cards with Atheros chip. It was used Airmarshal Captive Portal that enables network access through authentication methods FreeRADIUS server, to provide roaming service to VoIP communication based methods were used in a Wireless Distribution System and Asterisk. It is based on users to make a network connection request, the request HostSpot name and password, is transferred to the RADIUS server for verification and approval, if accepted, the server allows access to network resources.

It was found that the implementation of an infrastructure for distributed area wireless (WDS) does not support encryption mechanisms in this case study WPA2, thus implementing a HostSpot provide excellent results with confidentiality, security and authenticity in the transmission of traffic real-time VoIP in a coverage area that provides the roaming service.

GLOSARIO

Access Point (AP) Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

The Wi-Fi Alliance Alianza sin ánimo de lucro formada por diversos fabricantes de redes inalámbricas en agosto de 1999 para certificar la interoperabilidad de productos WLAN basados en la especificación 802.11 así como la promoción del estándar WLAN en todos los segmentos del mercado

AAA Abreviatura de Autenticación, Autorización y Accounting, sistema en redes IP para a qué recursos informáticos tiene acceso el usuario y rastrear la actividad del usuario en la red.

Autenticación Es el proceso de identificación de un individuo, normalmente mediante un nombre de usuario y contraseña. Se basa en la idea de que cada individuo tendrá una información única que le identifique o que le distinga de otros.

Autorización	Es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito.
Accounting	Es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo conectado, servicios a los que accede, datos transferidos durante la sesión.
Bridge	Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar
Confidencialidad	Calidad de secreto, que no puede ser revelado a terceros o personas no autorizada.
EAP - Extensible Authentication Protocol	Extensión del Protocolo punto a punto (PPP). Proporciona un mecanismo estándar para aceptar métodos de autenticación adicionales junto con PPP.
HotSpot	Punto de Acceso generalmente localizado en lugares con gran tráfico de público (estaciones, aeropuertos, hoteles, etc) que proporciona servicios de red inalámbrico de banda ancha a visitantes móviles.

MD5	Algoritmo de encriptación de 128-bits del tipo EAP empleado para crear firmas digitales. Emplea funciones hash unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos. Sólo autentica el cliente frente al servidor, no el servidor frente al cliente.
802.1x	Estándar de seguridad para redes inalámbricas y cableadas. Se apoya en el protocolo EAP y establece la necesidad de autenticar y autorizar a cada usuario que se conecte a una red.
PAP - Password Authentication Protocol	El método más básico de autenticación, en el cual el nombre de usuario y la contraseña (clave) se transmiten a través de una red y se compara con una tabla de parejas nombre-clave, la no coincidencia provocará la desconexión.
RADIUS Remote Authentication	Sistema de autenticación y accounting q cuando el usuario realiza una conexión a su ISP debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que chequeará que la información es correcta y autorizará el acceso al sistema del ISP.

Roaming	En redes inalámbricas se refiere a la capacidad de moverse desde un área cubierta por un Punto de Acceso a otra sin interrumpir el servicio o pérdida de conectividad
Servidor de Autenticación	Servidores que gestionan las bases de datos de todos los usuarios de una red y sus respectivas contraseñas para acceder a determinados recursos. Permiten o deniegan el acceso en función de los derechos atribuidos.
SSID	Identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.
WPA - Wireless Protected Access	Protocolo de Seguridad para redes inalámbricas. Encripta las comunicaciones de WIFI. Se basa en el estándar 802.11i
WPA2 Wireless Protected Access	Protocolo de seguridad para redes wifi, definido en el estándar 802.11i. Reemplaza al protocolo temporal WPA. Se basa en el algoritmo AES y se debe incorporar a todos los Access Point de última generación.

WEP - Wired Equivalent Privacy	Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada.
WDS	(Wireless Distribution System) Sistema que permite la interconexión de puntos de acceso de manera inalámbrica.
Wi-Fi	Es el nombre "comercial" con que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica. En lenguaje popular: Redes wifi.
WLAN - Red de Área Local Inalámbrica	También conocida como red wireless. Permite a los usuarios comunicarse con una red local o a Internet sin estar físicamente conectado. Opera a través de ondas y sin necesidad de una toma de red (cable) o de teléfono.

ANEXOS

ANEXO A

INSTALANDO DEBIAN ETCH 4.0

A continuación se explicará los procesos que realizaron para lograr una instalación satisfactoria.

Cuando arrancamos con el cd de debian etch, escribimos “installgui” para proceder a la instalación desde el instalador en modo gráfico que facilita mucho las cosas a los más nuevos.

Elegimos la distribución del teclado:

Elegimos la interfaz de red. En el caso que no logremos activar en este momento, no pasa nada, más tarde desde modo texto se puede hacer instalando y compilando los módulos correspondientes a nuestra tarjeta de red:

Le damos a siguiente elegimos configurar la red manualmente

Asignamos el nombre del dominio y maquina.

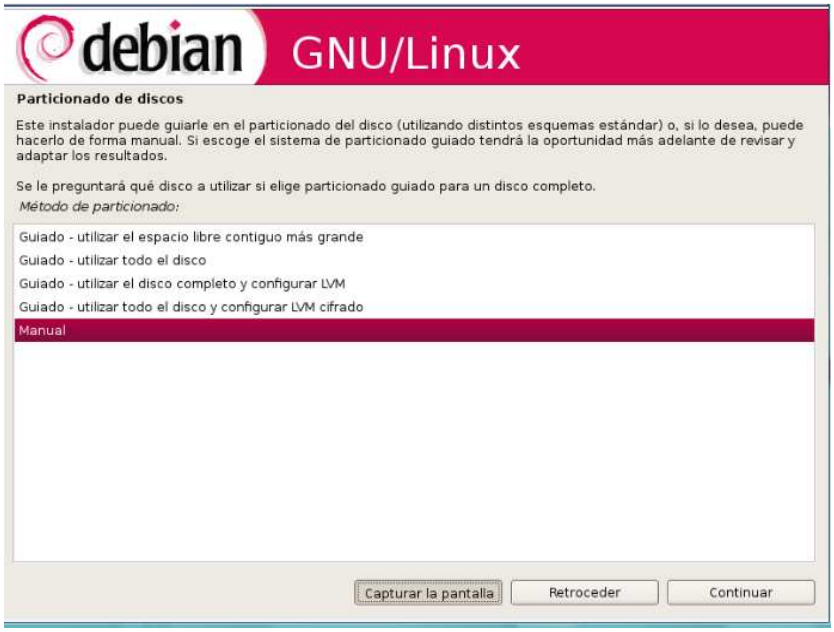
Asignamos el nombre de la maquina.

Escribimos la dirección IP de nuestro servidor.

Ingresamos la dirección del servidor de nombres:

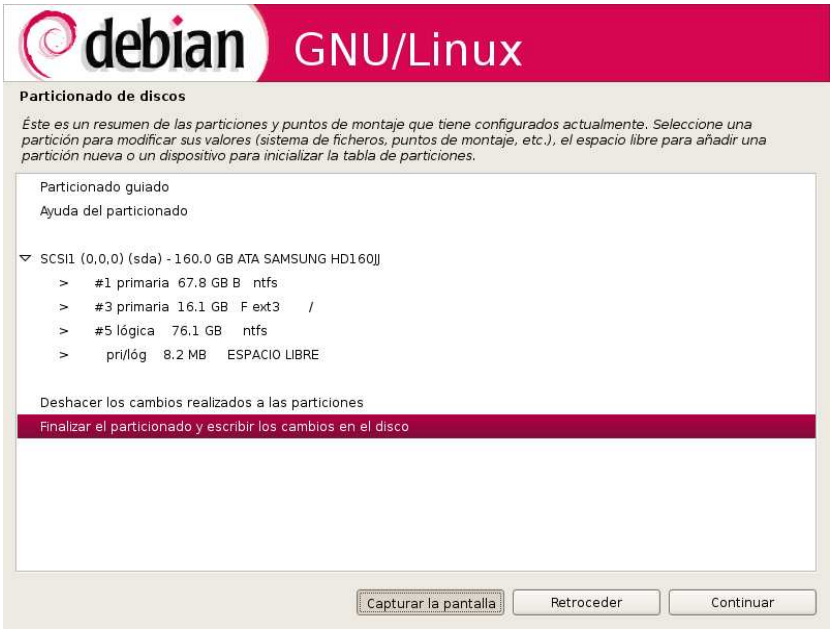
Ingresamos la máscara de red.

Ahora viene la sección en la que se particionará el disco duro. Para ello elegimos la opción manual:



Dar click sobre la partición donde queramos instalar y asignamos que tipo de formato tendrá

Al darle a finalizar el particionado nos preguntará si queremos aplicar los cambios:



Elegimos la opción si para escribir los cambios en los discos.

Seguimos con la selección de la zona horaria

Ahora se deberá escribir la clave del superusuario.

Ingresamos el nombre del nuevo usuario.

Ingresamos la contraseña del nuevo usuario.

Ahora toca establecer si queremos usar un servidor de replica para descargarnos los paquetes necesarios de un entorno gráfico. Por defecto te instala gnome como gestor de ventanas. Si por lo que sea no tenemos activada la conexión a internet o queremos sólo un sistema básico en modo texto para instalar después lo que queramos le damos a no.

Es esta sección Ud. Deberá seleccionar los programas que requeriremos según nuestras necesidades.

Terminada la instalación, sólo nos falta proceder al cargador de arranque:

ANEXO B

ARCHIVO DE CONFIGURACION INTERFACES AP PRIMARIO

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
      address 192.168.1.6
      netmask 255.255.255.248
      network 192.168.1.0
      broadcast 192.168.1.7
      gateway 192.168.1.1
      # dns-* options are implemented by the resolvconf package, if
installed
      dns-nameservers 192.168.1.1
      dns-search debian

auto ath0
iface ath0 inet static
      wireless-mode master
      wireless-channel 10
      wireless-essid HELEN-AP

      address 10.122.10.1
      netmask 255.255.255.0
      broadcast 10.122.10.255

      pre-up ifconfig ath0 down
      pre-up wlanconfig ath0 destroy
      pre-up wlanconfig ath0 create wlandev wifi0 wlanmode ap
      pre-up iwpriv ath0 wds 1
```

ANEXO C

ARCHIVO DE CONFIGURACION SIP.CONF

```
[general]
context=default
allowoverlap=no
videosupport=yes
port=5060

bindaddr=10.122.10.1
srvlookup=yes

[1000]
type=friend
username=helen
secret=1234
nat=yes
context=phones
canreinvite=no
host=dynamic
allow=ulaw

[1001]
type=friend
username=pepito
secret=1234
nat=yes
context=phones
canreinvite=no
host=dynamic
allow=ulaw

[1002]
type=friend
username=aracely
secret=1234
nat=yes
context=phones
canreinvite=no
host=dynamic
allow=ulaw
```

ANEXO D

ARCHIVO DE CONFIGURACION EXTENTIONS.CONF

```
[globals]

[general]

autofallthrough=yes

[default]
exten => s,1,Verbose(1|Unrouted call handler)
exten => s,n,Answer()
exten => s,n,Wait(1)
exten => s,n,Playback(tt-weasels)
exten => s,n,Hangup()

[incoming_calls]

[internal]
exten => 500,1,Verbose(1|Echo test application)
exten => 500,n,Echo()
exten => 500,n,Hangup()

[phones]
;include => internal
exten => 1000,1,Dial(SIP/1000)
exten => 1000,2,Hangup

exten => 1001,1,Dial(SIP/1001)
exten => 1001,2,Hangup

exten => 1002,1,Dial(SIP/1002)
exten => 1002,2,Hangup
```

BIBLIOGRAFIA

BIBLIOGRAFÍA EN INTERNET

EBOOKS

- **STALLMAN RICHARD,** Software Libre para una Sociedad Libre.

  Madrid: Traficantes de Sueños, 2004. pp. 19 - 95

  http://www.gnu.org/philosophy/fsfs/free_software.es.pdf

  (03-03-2010)

- **FRIENDLY LLC HACKER,** Redes Inalámbricas en los Países en Desarrollo.

  EE.UU Creative Commons, 2008. pp. 149 – 213

  http://wndw.net/pdf/wndw3-es/wndw3-es-ebook.pdf

  (25-05-2010)

PAGINAS WEB

GNU/LINUX

- http://wiki.debian.org/WiFi

  (03-04-2010)

- http://sites.google.com/site/urramax/comandognulinux

  (05-03-2010)

- http://d-i.alioth.debian.org/manual/es.s390/ch03s03.html

  (07-04-2010)

- http://man-es.debianchile.org/wlan.html

  (01-05-2010)

- http://debiantotal.blogspot.com/2007/02/instalacin-debian-etch-40.html

  (10-04-2010)
- http://madwifi-project.org/wiki/UserDocs/Distro/Debian/MadWifi

  (16-05-2010)
- http://madwifi.org/

  (19-05-2010)

Redes Inalámbricas

- http://www.scribd.com/doc/3321904/WiFi-Tutorial WiFi – WiFi Explained

  (01-04-2010)
- http://www.irit.fr/~Ralph.Sobek/wifi/

  (01-05-2010)
- http://linux-wless.passys.nl/query_chipset.php?chipset=Atheros

  (03-05-2010)
- http://en.wikipedia.org/wiki/802.11

  (06-06-2010)
- http://es.kioskea.net/contents/wifi/wifimodes.php3

  (07-05-2010)

Seguridad inalámbrica

- http://www.iec.csic.es/gonzalo/descargas/SeguridadWiFi.pdf

  (06-05-2010)

- http://www.saulo.net/pub/inv/SegWiFi-art.htm

  (14-06-2010)

- http://www.pdaexpertos.com/Tutoriales/Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml

  (14-06-2010)

- http://www.conocimientosweb.net/dt/article8301.html

  (16-06-2010)

VoIP

- http://comunidad.asterisk-es.org/index.php?title=Instalacion_de_Asterisk

  (29-08-2010)

- http://www.voipresource.net/VoIP-tutorial.htm

  (29-06-2010)

- http://www.voip-info.org/wiki/view/Asterisk

  (30-08-2010)

- http://www.smithonvoip.com/wireless-voip/

  (18-09-2010)

- http://www.ecualug.org/?q=2006/04/06/comos/instalar_asterisk_y_freepbx_en_debian

  (18-09-2010)