UNIVERSIDAD CENTRAL DE VENEZUELA
Facultad De Ciencias
Escuela De Computación
Laboratorio de Comunicación y Redes

Implementación de un Sistema de Seguridad para Redes Inalámbricas basado en la Integración del Protocolo RADIUS y el Protocolo LDAP

Trabajo Especial de Grado
presentado ante la Ilustre
Universidad Central de Venezuela
por el Bachiller:

Carlos Moreno
C.I.: 16.034.278
E-mail: carlos.a.moreno.c@gmail.com

para optar al título de Licenciado en Computación

Tutor: Prof. María Elena Villapol
Tutor: Prof. David Pérez

Caracas, Abril de 2009

Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Laboratorio de Comunicación y Redes

ACTA DEL VEREDICTO

Quienes suscriben, Miembros del Jurado designado por el Consejo de la Escuela de Computación para examinar el Trabajo Especial de Grado, presentado por el Bachiller Carlos Arturo Moreno Castillo C.I.: V-16.034.278, con el título "Implementación de un Sistema de Seguridad para Redes Inalámbricas basado en la Integración del Protocolo RADIUS y el Protocolo LDAP", a los fines de cumplir con el requisito legal para optar al título de Licenciado en Computación, dejan constancia de lo siguiente:

Leído el trabajo por cada uno de los Miembros del Jurado, se fijó el día 28 de abril de 2009, a las 6:00 p.m, para que sus autor lo defendiera en forma pública, en el centro de computación, lo cual este realizó mediante una exposición oral de su contenido, y luego respondió satisfactoriamente a las preguntas que le fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en la Ley de Universidades y demás normativas vigentes de la Universidad Central de Venezuela. Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió aprobarlo.

En fe de lo cual se levanta la presente acta, en Caracas el 28 de abril de 2009, dejándose también constancia de que actuó como Coordinador del Jurado el Profesor Tutor David Pérez.

Prof. David Pérez
(Tutor)

Prof. Robinson Rivas
(Jurado Principal)

Prof. Daniel Villavicencio
(Jurado Principal)

Dedicatoria

A mi familia por enseñarme que la paciencia y la perseverancia son virtudes que conllevan al éxito.

A mi madre por quererme y creer ciegamente en el fruto de su trabajo como guía, compañera y excelente amiga durante toda mi vida.

Especialmente a mi abuelo, por ser el mejor ejemplo de un trabajador constante y espero que desde donde esté pueda ver mis logros y se sienta orgulloso de ellos.

Agradecimientos

Quiero aprovechar estas líneas para agradecer a todos los que han aportado un grano de arena a lo largo del camino, el cual culmina con este trabajo especial de grado.

A Dios por haberme ayudado en todo momento y brindarme la oportunidad de rodearme siempre de personas muy valiosas, las cuales me prestaron su colaboración de una u otra forma.

A mis tías por ser las mejores segundas madres que cualquiera pueda tener, y siempre interesarse en mi trabajo y hacer un pequeño aporte con buen consejo.

A mi madre por darme siempre un apoyo incondicional y tratar de hacerme mejor hombre cada día.

A mi abuela por todo el amor brindado, por guiarme y preocuparse en todo momento por mi trabajo.

A mi novia y amiga, gracias por darme tantos momentos de alegría y servirme de apoyo durante todo este tiempo, por darme la confianza y saber aguantarme.

A los mejores amigos que cualquiera pudo conseguir en la universidad, JC "Baba" Rodríguez, Gabriel "G" Rodriguez, Christiano, el chino Say, gracias por todos los momentos compartidos hasta ahora, y por ser los mejores entes de distracción en los momentos de ocio. Igualmente a los panas de matemática por ser los mejores compañeros en las innumerables partidas de dominó, especialmente a Luigi, Adrian, "Juliano" y Rafael, porque siempre es un buen momento para "echar las piedras".

A José Terán por creer en mí y darme la oportunidad de trabajar a su lado, lo cual significó un aporte enorme para la realización de este trabajo.

A mi amigo y jefe Gustavo Colmenares, por todo lo enseñado durante 5 años; a "Super" Wendel por todo este tiempo compartido y todas las ayudas brindadas. Igualmente a Rosiris y Carla Díaz por ser un gran apoyo, excelentes amigas y personas, por escucharme, aconsejarme y siempre sacarme una sonrisa en los momentos más necesitados.

A Nelson Vicuña por interesarse en mi trabajo, y brindarme los mejores consejos en los momentos que más los necesite; los cuales ayudaron a la culminación del mismo.

A mi tutores Maria Elena Villapol y David Pérez, por brindarme la oportunidad de realizar este trabajo, y darme su apoyo durante la realización del mismo. Así como también a Daniel Villavicencio por toda la ayuda y la colaboración brindada.

Gracias.
Carlos Moreno

RESUMEN

Título:

Implementación de un Sistema de Seguridad para Redes Inalámbricas basado en la Integración del Protocolo RADIUS y el Protocolo LDAP

.

Autor:
Carlos Moreno

Tutor:
Prof. David Pérez

En la actualidad, la Facultad de Ciencias ofrece el servicio de conexión a la red interna, así como también acceso a internet, esto se hace mediante el uso de una red inalámbrica la cual carece de un mecanismo de seguridad que permita conocer quienes ingresan a la red y llevar un control de las actividades en la misma.
Tomando en cuenta lo anteriormente planteado, se implementó un sistema de control de acceso inalámbrico el cual representa una alternativa de seguridad como solución a la problemática de la red inalámbrica de la Facultad de Ciencias. Dicha solución está basada en el uso de los protocolos RADIUS y LDAP, de manera tal que se pueda realizar un proceso de autenticación al momento de ingresar a la red; dicho proceso es realizado por el servidor RADIUS el cual consultará la información contenida en el servidor LDAP y la comparará con la suministrada por los usuarios. Además, el servidor RADIUS se encarga también de mantener un registro de las conexiones que se hayan realizado diariamente y de esta manera poder llevar un control de quienes han ingresado a la red, desde que equipo se realizó dicha conexión, así como también la fecha y hora de la misma.
Por otra parte, para simplificar el proceso de autenticación a los usuarios se configuró un portal cautivo, el cual permite realizar dicho proceso mediante una página Web la cual se mostrará a los usuarios una vez se hayan conectado a la red inalámbrica.

Palabras Claves: Red Inalámbrica, Autenticación, RADIUS, LDAP, Portal Cautivo.

Tabla de Contenido

Índice de Figuras. iv
Capitulo 1: Introducción. 5
1.1 Planteamiento del Problema 5
1.2 Objetivo General 5
1.3 Objetivos Específicos 6
1.4 Justificación 6
1.5 Distribución del Documento 7
Capítulo 2: Redes Inalámbricas. 8
2.1 Definición. 8
2.2 Topología Ad Hoc. 9
2.3 Topología de Infraestructura. 9
2.4 Arquitectura de 802.11. 10
2.5 Servicios de 802.11. 11
2.6 Seguridad en Redes Inalámbricas. 12
2.6.1 Tipos de Amenazas. 12
2.6.2 Riesgos Inherentes a las Redes Inalámbricas. 13
2.6.3 Medidas de Seguridad Preventivas. 13
Capitulo 3: RADIUS 16
3.1 Tipos de Paquetes RADIUS. 17
3.2 Secretos compartidos. 18
3.3 Métodos de autenticación. 18
3.3.1 Protocolo de autenticación de contraseñas PAP. 18
3.3.2 CHAP. 19
3.4 Manejo de cuentas en RADIUS. 20
3.5 Aplicaciones de RADIUS. 21
3.5.1 Usando RADIUS con el servicio de directorio LDAP. 21
Capítulo 4: LDAP 22
4.1 Definición de Directorio. 22
4.2 Servicio de Directorio. 22
4.3 LDAP. 23
4.3.1 Modelos del Protocolo LDAP. 24
4.3.2 Modelo de Información. 24
4.3.3 Modelo de Nombramiento. 25
4.3.4 Modelo Funcional. 26
4.3.5 Modelo de Seguridad. 30
Capítulo 5: Portal Cautivo 33

5.1 Portal Cautivo. 33
5.2 Chillispot. 33
5.2.1 Métodos de Autenticación 34
Capítulo 6: Descripción y Análisis para el Control de Acceso Inalámbrico. 35
6.1 Requerimientos de la Solución. 35
6.2 Análisis 36
Capítulo 7: Configuración de la Solución de Control de Acceso Inalámbrico 37
7.1 Herramientas 37
7.1.1 Herramientas de Hardware 37
7.1.2 Herramientas de Software 38
7.2 Proceso de Configuración 38
7.2.1 Servidor LDAP. 39
7.2.2 Servidor RADIUS. 42
7.2.3 Servidor Chillispot (Portal Cautivo). 48
Capítulo 8: Pruebas y Resultados de la Solución de Control de Acceso Inalámbrico. 52
8.1 Escenario de Pruebas 52
8.2 Pruebas Realizadas 53
Capítulo 9: Conclusiones y Trabajos Futuros 58
9.1 Recomendaciones y Trabajos Futuros. 58
Capítulo 10: Glosario de Términos. 59
Capítulo 11: Fuentes Consultadas. 65
Capítulo 12: Anexos. 66
12.1 Manual de Instalación. 66

Índice de Figuras.

Figura 2.1 Topología de red ad hoc. 9
Figura 2.2 Topología de red con infraestructura. 10
Figura 2.3 Arquitectura 802.11 11
Figura 3.1 Proceso de autenticación con CHAP 19
Figura 3.2 Operación básica del manejo de cuentas en RADIUS. 20
Figura 4.1 Comparación de los protocolos X.500 y LDAP. 23
Figura 4.2 ID de mensajes de respuestas 24
Figura 4.3 Muestra de Directorio. 25
Figura 4.4 Muestra de un DIT 26
Figura 4.5 Sesión de LDAP usando TLS. 32
Figura 7.1 Archivo de configuración slapd.conf. 40
Figura 7.2 Muestra del archivo tree.ldif. 41
Figura 7.3 Muestra del archivo users.ldif. 41
Figura 7.4 Configuración del módulo LDAP. 43
Figura 7.5 Configuración del módulo MSCHAP. 44
Figura 7.6 Directivas de configuración para EAP-TLS. 45
Figura 7.7 Directivas de configuración para EAP-PEAP y EAP-TTLS. 45
Figura 7.8 Sección authorize del archivo radiusd.conf 46
Figura 7.9 Sección autentícate del archivo radiusd.conf. 47
Figura 7.10 Configuración del archivo clients.conf. 47
Figura 7.11 Archivo de configuración chilli.conf 49
Figura 7.12 Configuración del sitio ssl 50
Figura 8.1 Escenario de Pruebas 52
Figura 8.2 Asignación de Dirección IP. 53
Figura 8.3 Pantalla de bienvenida 54
Figura 8.4 Pantalla mostrada al realizar la autenticación. 55
Figura 8.5 Pantalla mostrada al fallar la autenticación. 55
Figura 8.6 Configuración del atributo radiusSessionTimeout en LDAP 56
Figura 8.7 Pantalla con el tiempo restante de la conexión 56
Figura 8.8 Configuración del atributo radiusIdleTimeout en LDAP 57

Capitulo 1: Introducción.

En los últimos años las redes inalámbricas han sido un gran apoyo para ampliar las redes cableadas, con la finalidad de poder compartir los recursos existentes en ellas sin necesitar realizar un trabajo de cableado o modificar infraestructura alguna. En la Facultad de Ciencias se ha hecho uso de estas redes inalámbricas como medio de extensión de la red cableada existente, y de esta manera poder ofrecer a la comunidad servicios como, conexión a Internet, acceso a sitios Web o FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos), y recursos que se encuentren disponibles dentro de la red de la facultad.

Debido a esto es necesario tomar algunas medidas de seguridad para poder resguardar la información que se maneja en la red de la facultad, estas medidas van un poco más allá de los esquemas de cifrado de datos, ya que se conoce bien que las redes inalámbricas son vulnerables a ataques [11], y estos pueden ser originados por algún intruso fuera de la red o peor aún por un usuario malintencionado dentro de la propia red.

1.1 Planteamiento del Problema

Actualmente la Facultad de Ciencias provee acceso público a ciertos recursos dentro de la red por medios inalámbricos, como lo son servidores Web o FTP, pero carece de algún mecanismo de seguridad para proteger estos recursos, igualmente es imposible llevar un control de la identidad de los usuarios que acceden a la red, ya que no se requiere de autenticación alguna para acceder a ella. El problema existente es claro, la seguridad informática se encuentra amenazada pues no se cuenta con un sistema de seguridad para la red inalámbrica.

1.2 Objetivo General

El objetivo de este trabajo es implementar un mecanismo de seguridad para realizar la autenticación, autorización y el manejo de usuarios que utilicen la red inalámbrica de la facultad de ciencias, usando para ello los protocolos RADIUS y LDAP.

1.3 Objetivos Específicos

A continuación se describen los objetivos específicos de la propuesta de tesis.

- Crear una estructura de directorio en LDAP, para el manejo de la información referente a los usuarios, en donde se especifique información como el nombre, contraseña, tipo de usuario, entre otros.
- Instalar y configurar un servidor RADIUS, para realizar el proceso de autenticación, autorización y manejo de cuentas de los usuarios que soliciten conexión a la red inalámbrica de la facultad de ciencias.
- Realizar la integración entre los protocolos RADIUS y LDAP, para poder llevar a cabo el proceso de autenticación de los usuarios en el servidor RADIUS.
- Realizar la configuración del router para poder realizar el proceso de autenticación de usuarios mediante el servidor RADIUS y que este valide la información suministrada con la que suministre la consulta del directorio LDAP.
- Diseñar e implementar una política de seguridad adecuada para el centro de computación, en donde se incluya la utilización de los servidores RADIUS y LDAP.
- Realizar pruebas una vez implementada la solución, las cuales se basarán en el correcto funcionamiento de la misma.

1.4 Justificación

La Facultad de Ciencias pensando en el beneficio de la comunidad, ha instalado una red inalámbrica para facilitar el acceso de la información tanto de la Intranet como de Internet. Por otra parte las redes inalámbricas son bastante vulnerables debida a su naturaleza, y son muchos los daños que puede ocasionar un ataque, desde un simple espionaje del tráfico hasta perdidas de información.

Actualmente la red inalámbrica de la Facultad de Ciencias, carece de algún sistema de seguridad, por lo que surge la imperiosa necesidad de implementar un sistema de control de acceso, que permita llevar un control de los usuarios que acceden a la red y así restringir el acceso de usuarios ajenos a la comunidad de la Facultad.

1.5 Distribución del Documento

El documento a continuación se encuentra estructurado en cinco (5) capítulos en donde el primero de ellos trata darle una breve introducción al lector, acerca de los tópicos que se trataran en el documento.

El segundo capítulo trata acerca de las redes inalámbricas, su clasificación en topologías en donde se detallan cada una de ellas, además se detalla el estándar 802.11 y los servicios que este ofrece por cada una de sus subcapas.

En el tercer capítulo se encuentra explicado en detalle el protocolo RADIUS, como está formada su trama, donde se explican cada uno de los campos que la conforman, además se mencionan los métodos de autenticación usados en él, así como también algunas vulnerabilidades y las implementaciones del mismo.

El cuarto capítulo trata sobre el protocolo LDAP, en este se explican las definiciones de directorio y servicio de directorio, también se realizan comparaciones entre un servicio de directorio y algunas tecnologías disponibles actualmente, y finalmente se explica con mayor profundidad el protocolo y los modelos que se usan en este.

El quinto capítulo trata acerca de una aplicación de un portal cautivo, específicamente la implementación Chillispot, en este se explica brevemente la definición de un portal cautivo, y se detalla un poco esta aplicación incluyendo sus métodos de autenticación.

Capítulo 2: Redes Inalámbricas.

En este capítulo se abordará el tema de las redes inalámbricas con la finalidad de dar una breve definición de las mismas, y al mismo tiempo se detallará un poco el estándar más significativo de estas, definido por el comité 802.11 de la IEEE.

2.1 Definición.

Una red de área local inalámbrica (WLAN - Wireless Local Area Network) como su nombre indica es una red LAN que hace uso de un medio de transmisión no guiado para recibir y enviar datos punto a punto entre todos los nodos que la conforman.

Las redes inalámbricas tienen los mismos requerimientos de una red LAN típica incluyendo alta capacidad, habilidad para cubrir cortas distancias, ofrecer full conectividad entre las estaciones, y tener la capacidad de broadcast. Además de esto también existen otros requerimientos que deben cubrir donde algunos de los más importantes son:

- **Rendimiento:** el protocolo de control de acceso al medio debe hacer lo más eficiente posible la utilización del medio para aprovechar al máximo la capacidad del mismo.

- **Número de nodos:** las redes inalámbricas pueden necesitar soportar cientos de nodos a través de múltiples celdas.

- **Conexión al backbone LAN:** en la mayoría de los casos se requiere la interconexión con estaciones en la red cableada.

- **Área de servicio:** el área típica de cobertura para las redes inalámbricas tiene un diámetro de 100 a 300 mts.

- **Robustez y seguridad en la transmisión:** el diseño de la red inalámbrica debe permitir transmisiones fiables y debe proveer algún nivel de seguridad contra espías.

- **Handoff y roaming:** el protocolo MAC usado en las redes inalámbricas debe permitir la movilidad de las estaciones de una celda a otra.

- **Configuración dinámica:** el direccionamiento MAC y los aspectos de la administración de la red, deben permitir dinámica y automáticamente la agregación, eliminación y relocalización de sistemas finales sin que esto ocasione interrupción en otros usuarios.

Las redes inalámbricas pueden clasificarse en dos grupos según la topología de ellas, redes Ad Hoc o redes con infraestructura.

2.2 Topología Ad Hoc.

Una red ad hoc es una red punto a punto donde no hay un servidor centralizado, configurada temporalmente para cubrir algunas necesidades inmediatas, como por ejemplo una sala de reuniones donde un grupo de empleados pueden interconectar sus dispositivos tales como una laptop, o una Palm, mientras dure la reunión.

En la Figura 2.1 se muestra un ejemplo de una red ad hoc en donde los dispositivos que pertenecen a la misma se interconectan sin necesidad de tener un punto central.

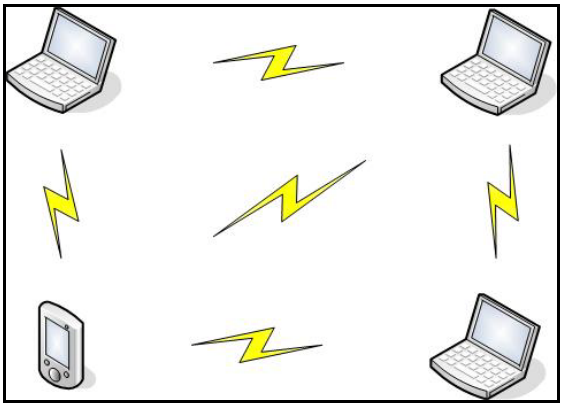

Figura 2.1 Topología de red ad hoc

2.3 Topología de Infraestructura.

Este tipo de redes inalámbricas generalmente son utilizadas para servir como una extensión de la red cableada existente. En las redes con infraestructura hay un módulo central que actúa como interfaz entre la red cableada y la red inalámbrica, estos módulos centrales pueden ser routers o puntos de acceso (AP - access point) y son los encargados de regular el acceso de las estaciones o sistemas finales.

En la Figura 2.2 se muestra un entorno donde se interconectan varias WLAN mediante la red cableada [7].

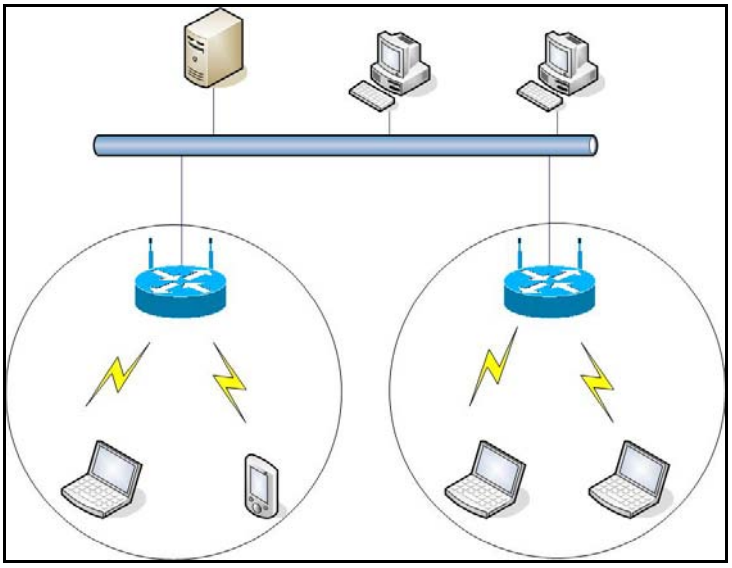

Figura 2.2 Topología de red con infraestructura

2.4 Arquitectura de 802.11.

Una red inalámbrica 802.11 está basada en una arquitectura celular, donde el sistema se divide en celdas. El bloque de red inalámbrica más pequeño se conoce con el nombre de conjunto de servicios básico BSS (BSS – Basic Service Set) el cual consiste en algunas estaciones ejecutando el mismo protocolo MAC y compitiendo por el acceso al mismo medio inalámbrico compartido. Un BSS puede estar aislado o puede conectarse a un sistema de distribución DS (DS – Distribution System) mediante un punto de acceso AP (AP – Access Point). Los AP funcionan como puentes. El protocolo MAC puede ser distribuido o puede estar controlado por una función de coordinación central ubicada en el AP. El DS puede ser un switch o una red, bien cableada o inalámbrica.

La configuración más simple de una red inalámbrica se muestra a continuación en la Figura 2.3, en donde cada estación pertenece a un solo BSS, es decir, cada estación sólo está dentro del rango inalámbrico de otras estaciones dentro del mismo BSS. Esto también es posible para dos BSS que se solapan geográficamente y que una estación podría participar en más de un BSS.

Un conjunto de servicios extendido ESS (ESS – Extended Service Set) consiste de dos o más BSS interconectados por un DS. Normalmente, los DS son un backbone a la red cableada, pero pueden ser cualquier comunicación de red.

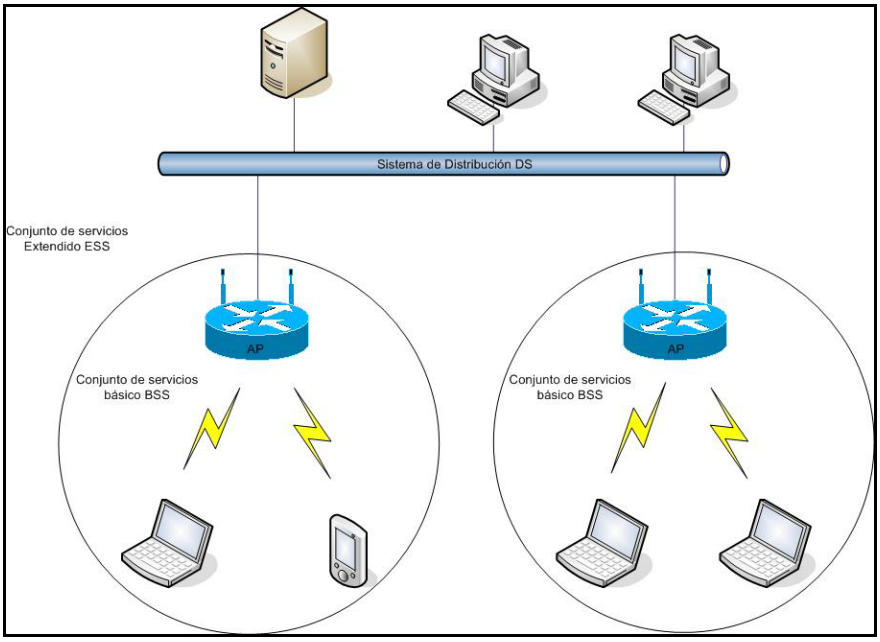

Figura 2.3 Arquitectura 802.11

2.5 Servicios de 802.11.

El estándar 802.11 establece que cada red inalámbrica debe proveer nueve servicios, los cuales se dividen en dos categorías: cinco de ellos son servicios de distribución y los otros cuatro restantes, son servicios de la estación. Los servicios de distribución se refieren a la administración de los miembros de la celda y la interacción con las estaciones fuera de ella. A diferencia de estos, los servicios de la estación se refieren a la actividad en una sola celda. Los cinco servicios de distribución son provistos por la estación base y tratan con la movilidad de la estación cuando entran y salen de la celda, adjuntándose y separándose de la estación base.
En cuanto a los servicios de distribución se tienen los siguientes:

- Asociación
- Desasociación
- Reasociación
- Distribución
- Integración

Los cuatro servicios restantes se refieren a acciones en una sola celda, estos son usados luego de haberse llevado a cabo una asociación, a continuación se listan cada uno de ellos:

- Autenticación
- Desautenticación
- Privacidad
- Entrega de Datos [8].

2.6 Seguridad en Redes Inalámbricas.

En las redes convencionales existe una seguridad que es inherente a la red, debido a su naturaleza cableada, lo que dificulta que un intruso pueda entrar en ella y realizar algún tipo de espionaje, ya que para ello es necesario realizar un cableado adicional al ya existente, el cual permita al atacante entrar en la red.

A diferencia de esto, las redes inalámbricas ofrecen a sus usuarios la ventaja de tener estaciones de trabajo móviles, pero al mismo tiempo esta ventaja recae directamente sobre la seguridad de la red, haciéndola bastante atractiva para un atacante, quien sólo necesita escanear las redes disponibles y poder ejecutar algún tipo de ataque.

2.6.1 Tipos de Amenazas.

Los ataques relacionados con la seguridad de la información, pueden clasificarse en 4 categorías: intercepción, interrupción, alteración y fabricación.

- **Intercepción:** son considerados ataques pasivos, ya que simplemente constan en analizar y capturar información que se esté transfiriendo en la red en un determinado momento. Para esto el atacante sólo necesita un software de análisis de tráfico conocido como “sniffer”, el cual permite realizar capturas del tráfico de paquetes en la red para su posterior análisis.

- **Interrupción:** son considerados ataques activos, como su nombre lo indica tratan de inhabilitar el funcionamiento de un servicio en particular, bien sea una página Web, un servidor de correo, entre otros. Por lo general en estos ataques se intenta colapsar una interfaz de red

con una gran cantidad de peticiones, para de esta manera lograr que el servicio que se esté prestando deje de hacerlo.

- **Alteración:** son considerados ataques activos, en estos se captura un mensaje, el cual es modificado y enviado nuevamente a su destino original para alterar de algún modo el resultado que se espera. Entre estos ataques se pueden encontrar varios ejemplos como modificaciones a sitios Web sin la debida autorización de los administradores del sitio, fraudes a cuentas bancarias, entre otros.

- **Fabricación:** son considerados como ataques activos, en estos se incluyen todos aquellos en donde se fabrica o crea información falsa, con el fin de engañar y estafar a las personas, entre estos ataques se encuentran los ataques de phishing, en donde se crea una página Web muy similar a la página de un banco, de manera tal que el usuario al entrar en la ella no note ninguna diferencia e introduzca sus datos en ella.

2.6.2 Riesgos Inherentes a las Redes Inalámbricas.

Entre los riesgos más comunes que corren las redes inalámbricas se pueden nombrar los ataques de sniffing, en donde se realiza la captura de información valiosa como nombres de usuarios y contraseñas, mediante el uso de sniffers, lo que origina a su vez secuestros de sesiones de usuarios, también se pueden realizar ataques de negación de servicio, en donde se introduce un dispositivo en el BSS, el cual emite ondas de radio a la frecuencia utilizada por la red lo que origina interferencias.

Igualmente es posible realizar ataques de fuerza bruta contra el AP o Router, con la finalidad de modificar la configuración del mismo. Otro riesgo existente son los puntos de acceso abusivos no autorizados, por medio del cual un atacante podría obtener el acceso a la red.

2.6.3 Medidas de Seguridad Preventivas.

La seguridad es un aspecto de especial relevancia en las WLAN, por lo que es imprescindible contar con mecanismos y protocolos que garanticen la protección de la información y que restrinjan el acceso a usuarios no autorizados.

En las redes inalámbricas existen en principio dos esquemas de seguridad para restringir el acceso de los usuarios, el primero de ellos se conoce como un sistema de autenticación abierta, en donde los usuarios sólo necesitan conocer el SSID (Service Set Identifier – Identificador del conjunto de servicios) de la red para conectarse, este esquema es bastante inseguro ya que no usa ningún tipo clave de acceso, así como tampoco utiliza algún tipo de cifrado de datos, de tal manera que lo hace vulnerable a los ataques de sniffing.

El segundo esquema se conoce como un esquema de clave compartida, en donde el usuario necesita conocer la clave para poder acceder a la red, la desventaja de este mecanismo, radica en la cantidad de usuarios que se maneje en la red, ya que la clave debe compartirse entre todos los usuarios que accedan a esta, lo que origina que la probabilidad de que la clave caiga en manos mal intencionadas se vaya incrementando mientras el número de usuarios sea mayor.

El estándar 802.11 especifica el uso de un esquema de cifrado, el cual es usado durante el transporte de los datos. Dicho esquema es el de clave compartida WEP, basado en el algoritmo de cifrado RC4. En este esquema el usuario recibe un desafío el cual viaja en texto plano, y el mismo debe ser respondido con el texto cifrado, para lo cual se usa la clave la clave compartida. Esto representa una de las principales debilidades de este esquema, ya que un atacante que se encuentre capturando los mensajes en la red, puede conocer la clave compartida fácilmente, conociendo el texto plano y el texto cifrado.

Por otra parte el algoritmo de cifrado RC4, fue vulnerado en 1994 y las debilidades del mismo ya se han hecho públicas. Por tal motivo el método de clave compartida WEP es bastante inseguro e ineficaz. Debido a esto existen otros métodos de cifrado de datos, los cuales se pueden usar en lugar de WEP, como es el mecanismo de filtrado por direcciones MAC, en donde se verifica la dirección MAC del usuario, si esta coincide con la indicada en el router se le da acceso. El problema con este método está en que no es recomendable cuando se tienen muchos usuarios, ya que dificulta la administración de la red, además actualmente existen herramientas que permiten la falsificación de las direcciones MAC, lo que permite a un atacante obtener igualmente el acceso a la red.

Por tal motivo la IEEE en conjunto con Wi-Fi, decidieron publicar en el estándar 802.11i el mecanismo de seguridad WPA. En este mecanismo se solventan las deficiencias de WEP, ya que se utiliza una clave única por cada paquete

enviado, además puede utilizar el protocolo EAP (Extensible Authentication Protocol – Protocolo de Autenticación Extensible) para llevar a cabo las tareas de Autenticación, Autorización y el manejo de cuenta de los usuarios.

De igual manera se puede usar este mecanismo en conjunto con un servidor RADIUS, configurado para llevar a cabo las tareas de autenticación, autorización y el manejo de cuentas de usuarios. Por supuesto este modo es más robusto que el anterior y su principal inconveniente es que requiere de un servidor RADIUS funcionando en la red. Este método es conocido como WPA Empresarial. [11]

Capitulo 3: RADIUS

RADIUS (Servicio de autenticación de usuarios remotos a la red - Remote Authentication Dial-In Service) es un protocolo cliente – servidor que permite realizar la autenticación, autorización y manejo de cuentas de usuarios remotos los cuales desean acceder al sistema o a algún servicio de la red. Originalmente fue desarrollado por Livingston Enterprise, y se encuentra basado en el comúnmente usado método de desafío y respuesta [9].

El término cliente en RADIUS se refiere a la entidad la cual actúa como cliente RADIUS, transmitiendo mensajes a través del protocolo, como por ejemplo un servidor de acceso a la red (NAS – Network Access Server), y no al usuario final o dispositivo que se esté autenticando a la red mediante el NAS [10].

El modelo AAA se enfoca en tres aspectos principales del control de acceso de los usuarios: la autenticación, la autorización y finalmente el manejo de cuentas, a continuación se explican brevemente estos aspectos:

- **Autenticación:** Es el proceso de verificación de una persona o máquina, que haya declarado su identidad. Por lo general el método más común es mediante la combinación de un identificador de usuario y una contraseña, en donde el hecho de conocer la contraseña es considerado como una demostración de que el usuario es autentico. Por otra parte la distribución de contraseñas, destruye este método de autenticación, lo que ha impulsado a requerir de mecanismos más fuertes y confiables de autenticación como por ejemplo los certificados digitales.

- **Autorización:** La autorización implica la utilización de un conjunto de normas u otras plantillas para decidir lo que un usuario previamente autenticado puede hacer dentro del sistema.

- **Manejo de cuenta:** El manejo de cuenta permite medir y documentar los recursos que un usuario puede aprovechar durante el acceso. Esto puede incluir el tiempo de duración de la sesión, así como también la cantidad de datos enviados y/o recibidos por un usuario. Toda esta información puede ser usada con fines estadísticos para el control de autorización, efectuar cobros por servicios, llevar un control sobre la utilización de recursos, etc. [9]

3.1 Tipos de Paquetes RADIUS.

En RADIUS existen cuatro paquetes que son relevantes en las fases de autenticación y autorización en una transacción, los cuales son:

- **Access Request:** Es usado por el consumidor del servicio, para solicitar un servicio particular de una red. El cliente envía un paquete de solicitud al servidor RADIUS con una lista de los servicios solicitados.

- **Access Accept:** Es enviado por el servidor RADIUS al cliente para indicarle que la solicitud hecha ha sido aceptada. Si todo el contenido de la carga útil del paquete es aceptable, el servidor debe de configurar el campo código del paquete de respuesta en 2. El cliente al recibir el paquete de aceptado, lo compara con el paquete de respuesta usando el campo identificador. Los paquetes que no sigan el estándar son descartados.

- **Access Reject:** El servidor RADIUS debe de enviar un paquete de Access Reject de regreso al cliente si debe denegar alguno de los servicios solicitados en el paquete Access Request. La denegación puede estar basada en políticas del sistema, privilegios insuficientes o algún otro criterio. El Access Request puede ser enviado en cualquier momento durante una sesión. Sin embargo no todos los equipos soportan la recepción de Access Reject durante una conexión preestablecida.

- **Access Challenge:** Si un servidor recibe información contradictoria de un usuario, requiere más información o simplemente desea reducir el riesgo de una autenticación fraudulenta, este puede emitir un paquete Access Challenge al cliente. El cliente al recibir este paquete debe emitir un nuevo access request donde se incluya la información adecuada.

  Cabe señalar que algunos clientes no soportan el proceso de desafío/respuesta, en ese caso, el cliente trata el paquete como un paquete de Access Reject. Algunos clientes si soportan el desafío, y en ese punto se puede enviar un mensaje al usuario en el cliente solicitando información adicional sobre la autenticación.

3.2 Secretos compartidos.

Para fortalecer la seguridad e incrementar la integridad transaccional, el protocolo RADIUS usa el concepto de secretos compartidos. Los secretos compartidos son valores generados aleatoriamente y son conocidos entre el cliente y el servidor RADIUS. El secreto compartido es usado con todas las operaciones que requieren ocultamiento de datos y valores. La única limitación técnica es que la longitud del secreto compartido debe ser mayor a 0, pero la RFC 2865 - Remote Authentication Dial In User Service (RADIUS) recomienda que el secreto compartido sea de al menos 16 octetos, lo que lo haría virtualmente imposible de craquear por un ataque de fuerza bruta.

3.3 Métodos de autenticación.

RADIUS apoya una variedad de protocolos para transmitir al usuario datos específicos hacia y desde el servidor de autenticación. Los dos más comunes son el protocolo de autenticación de contraseñas PAP (PAP – Passwords Authentication Protocol) y CHAP.

3.3.1 Protocolo de autenticación de contraseñas PAP.

El atributo user password en un paquete de solicitud le indica al servidor RADIUS que el protocolo PAP será usado para esa transacción. Es importante notar que el único campo obligatorio en este caso es el campo user password. El campo nombre de usuario no tiene que ser incluido en el paquete de solicitud.

El algoritmo usado para ocultar la contraseña de usuario original está compuesto de varios elementos, primero el cliente detecta el identificador y el secreto compartido para la solicitud original y calcula la secuencia MD5. El password original del cliente es pasado por un proceso de XOR y el resultado viene dado de estas dos secuencias y es puesto en el campo del password de usuario. El servidor RADIUS al recibir esto revierte el proceso para determinar si autoriza la conexión. La propia naturaleza del mecanismo para ocultar la contraseña, evita que un usuario pueda determinar si cuando la autenticación falla, es debido a una contraseña incorrecta o a un secreto inválido. La mayoría de los servidores RADIUS comerciales, sin embargo, incluyen la lógica que ve una serie de paquetes transmitidos previamente desde el mismo cliente. En caso de que un número de paquetes hayan sido pasados por la conexión

correctamente, lo más probable es que los pocos paquetes que hayan fallado en el envío, se deba a un password incorrecto [9].

3.3.2 CHAP.

CHAP (Challenge Handshake Authentication Protocol) está basado en la premisa de que el password nunca debe ser enviado en ningún paquete a través de la red. El proceso de autenticación con CHAP es mostrado en la Figura 3.1 y se describe en los siguientes pasos:

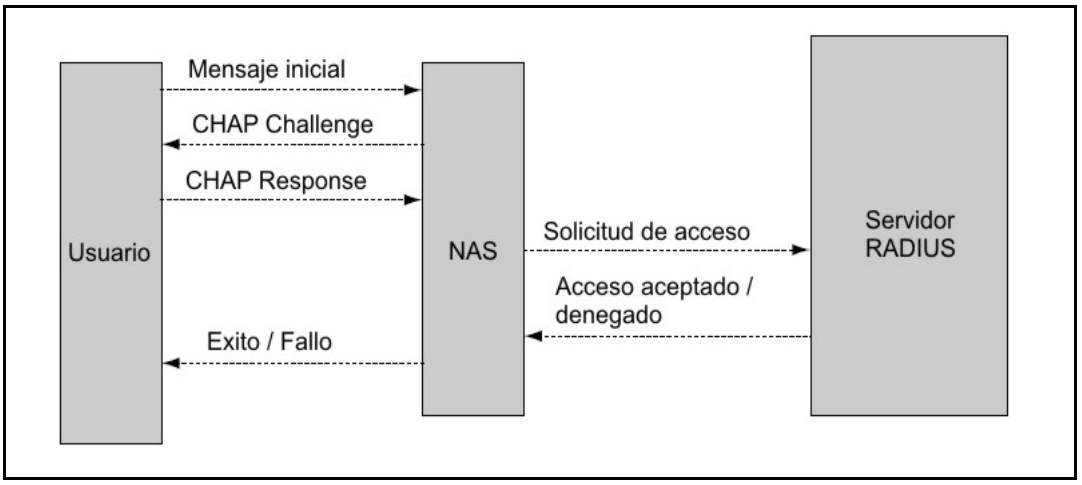

Figura 3.1 Proceso de autenticación con CHAP

- Un usuario solicita al NAS conectarse a la red.
- El NAS crea un desafío de 16 octetos y lo envía al usuario a través de un mensaje CHAP Challenge. Este mensaje también incluye un CHAP ID.
- El usuario responde al desafío usando un mensaje de respuesta en el que se incluye el mismo CHAP ID enviado en el mensaje anterior, un nombre de usuario CHAP y su respuesta al desafío. La respuesta es calculada usando una clave MD5, junto con el secreto compartido entre el usuario y el servidor RADIUS.
- El NAS entonces crea una solicitud de acceso, donde se insertan el nombre de usuario CHAP del usuario en el atributo nombre de usuario, y el CHAP ID y el CHAP Password en el atributo password de usuario, y envía estos atributos en la solicitud de acceso al servidor RADIUS.
- El servidor RADIUS toma el password basado en el nombre de usuario y calcula un hash en el mismo sentido que el usuario lo hizo. Sin embargo si el atributo CHAP Challenge no está presente en el mensaje, el servidor usa el valor en el campo autenticador de solicitud de la solicitud de acceso enviada por el cliente. El servidor compara el resultado del hash

con el valor incluido en el CHAP Password, si ellos coinciden, el servidor envía de regreso un mensaje indicando al NAS que el acceso está concedido, en caso contrario se envía un mensaje al NAS de acceso denegado.

3.4 Manejo de cuentas en RADIUS.

El manejo de cuentas en RADIUS se encuentra definido en la RFC 2866 – RADIUS Accounting, este procedimiento también está basado en el modelo cliente – servidor, donde el cliente (NAS) pasa la información de las cuentas de usuario al servidor RADIUS, quien se encarga del manejo de las cuentas. El manejo de cuentas en RADIUS utiliza dos tipos de mensajes: Accounting Request y Accounting Response. El mensaje Accounting Request es siempre enviado por el cliente RADIUS hacia el servidor, en cambio el Accounting Response es generado por el servidor RADIUS al recibir y procesar el mensaje Accounting Request. Sin embargo, en escenarios donde existan servidores Proxy, estos pueden tener algún intercambio Accounting Request-Response.

Una operación básica de este proceso es mostrada en la Figura 3.2. Un NAS genera un Accounting Request "Start", al inicio de operación y lo envía al servidor RADIUS que se encarga del manejo de las cuentas. Este paquete específica entre otras cosas, el tipo de servicio que está siendo entregado, y el usuario a quien se le está entregando. Al recibir un Accounting Request válido, el servidor agrega una entrada de la cuenta a su registro y reconoce la solicitud generando un Accounting Response para indicar que el paquete ha sido recibido.

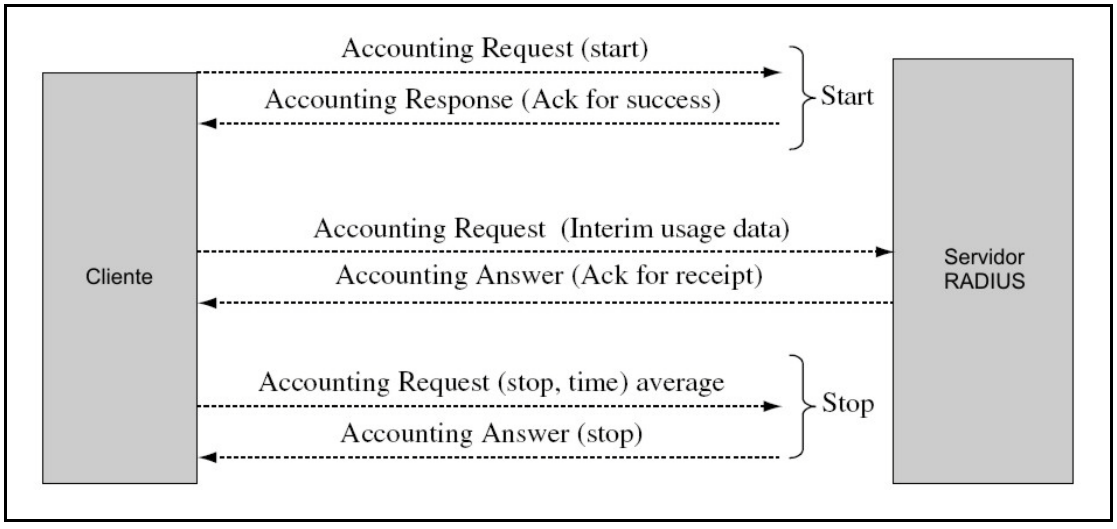

Figura 3.2 Operación básica del manejo de cuentas en RADIUS.

Al finalizar la entrega del servicio el cliente genera un paquete Accounting Request, describiendo el tipo de servicio que fue entregado y algunas estadísticas opcionales, la duración de la sesión actual, el motivo de la desconexión, o la cantidad de octetos de entrada y de salida. Todo esto es enviado al servidor RADIUS, el cual enviará de regreso un reconocimiento de que el paquete ha sido recibido, en caso de no recibir el paquete satisfactoriamente, el mensaje de reconocimiento no es enviado de regreso al cliente.

3.5 Aplicaciones de RADIUS.

En los puntos anteriores se ha tratado de describir el protocolo RADIUS con la finalidad de explicar su funcionamiento como protocolo de autenticación, autorización y el manejo de cuentas, sin embargo, en este punto se verán algunas aplicaciones del protocolo RADIUS aparte de la ya mencionada anteriormente, entre estas otras aplicaciones del protocolo se puede mencionar el trabajo en conjunto de RADIUS con el servicio de directorio LDAP.

3.5.1 Usando RADIUS con el servicio de directorio LDAP.

Los administradores de sistemas siempre denuncian la falta de eficiencia existente, al tener que tratar con varias bases de datos a través de distintas plataformas, por ejemplo el simple hecho de cambiar un password de usuario se ve multiplicado por el número de sistemas en los cuales se encuentre almacenado este usuario.

Afortunadamente, existe una solución a este problema, la cual está basada en el estándar LDAP, el cual es explicado con mayor detalle en el próximo capítulo. LDAP es el protocolo de acceso ligero a directorio, es un directorio apoyado en una base de datos de información acerca de los usuarios de una red en particular. LDAP es un protocolo que usa consultas estándar, parecidas a SQL, para hablar con un proceso compatible. Usando LDAP permite que las aplicaciones que lo soportan se comuniquen con una base de datos centralizada y usen esta información en sus operaciones internas. FreeRADIUS es una de las implementaciones del protocolo RADIUS, la cual es de código abierto y tiene completo soporte para LDAP.

Capítulo 4: LDAP.

En este capítulo se verán algunas definiciones que se consideran necesarias para poder comprender a fondo el protocolo ligero de acceso a directorio LDAP, entre algunas de estas definiciones se puede mencionar el significado de un directorio, algunas comparaciones entre un directorio y otras tecnologías y finalmente se detallará el funcionamiento del protocolo como tal y algunas implementaciones del mismo.

4.1 Definición de Directorio.

Un directorio funciona muy similar a un directorio telefónico o de direcciones, en el que se puede acceder a la información a manera de consulta y del mismo modo esta puede ser modificada [2].

En el mundo informático también existen directorios los cuales son muy similares a los de la vida diaria, pero con algunas diferencias relevantes, ya que son dinámicos desde el punto de vista en que son actualizados con mayor frecuencia de lo que puede ser por ejemplo un directorio telefónico, son flexibles, debido al tipo de información que estos almacenan y a los métodos de búsqueda que se pueden emplear en ellos, la información contenida en ellos puede ser asegurada mediante un sistema centralizado en el que se controle quien accede a la información mediante un simple método de autenticación [1].

4.2 Servicio de Directorio.

Un servicio de directorio se puede entender como una base de datos especializada diseñada específicamente para búsqueda y consulta de datos, quizás la mejor definición y al mismo tiempo la más simple es la que lo describe como una base de datos optimizada para el acceso de lectura [4].

Los directorios tienden a contener atributos descriptivos, basados en información, generalmente no soportan transacciones complicadas o esquemas de rollback, los cuales se encuentran en los sistemas manejadores de bases de datos, especializados para el manejo de gran cantidad de actualizaciones complejas. En cambio las actualizaciones de los directorios en caso de estar permitidas son típicamente simples donde todo o nada cambia [3].

4.3 LDAP.

El Protocolo de Acceso Ligero a Directorio, LDAP (LDAP – Lightweight Directory Access Protocol), es un protocolo a nivel de aplicación según el modelo de referencia OSI, que permite el acceso a un servicio de directorio ordenado y distribuido para buscar información. Está basado en el estándar X.500, pero significativamente más simple y más realmente adaptado para satisfacer las necesidades del usuario. A diferencia de X.500, LDAP soporta TCP/IP, que es necesario para el acceso a Internet [5].

En la Figura 4.1 se puede apreciar una gráfica del protocolo X.500 sobre el modelo OSI versus el protocolo LDAP sobre la pila del protocolo TCP / IP.

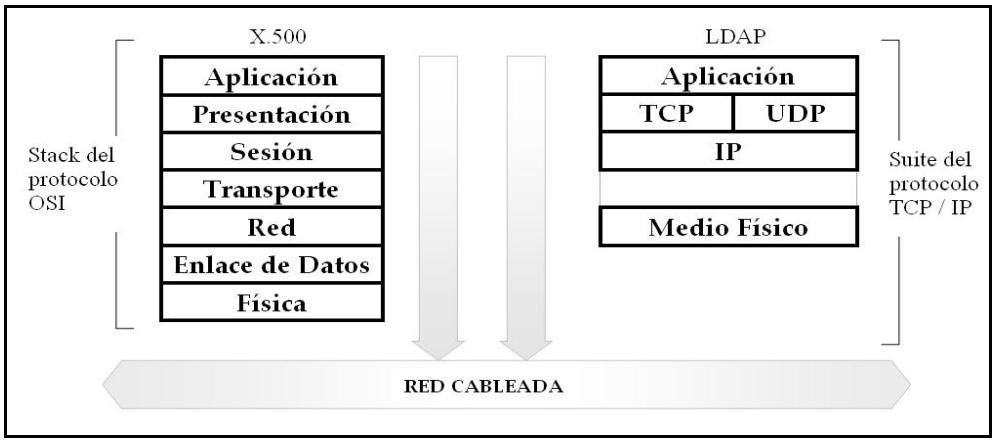

Figura 4.1 Comparación de los protocolos X.500 y LDAP

Es importante entender que el protocolo LDAP es un protocolo orientado a mensajes, donde el cliente construye un mensaje LDAP conteniendo en este una solicitud y lo envía al servidor, el servidor por su parte procesa la solicitud y envía los resultados de vuelta al cliente como una serie de uno o más mensajes LDAP.

Debido a que el protocolo está basado en mensajes también permite a un cliente emitir varias solicitudes simultáneamente. Para esto el cliente genera un ID de mensaje único para cada solicitud, los resultados para una solicitud en específico son marcados con el mismo ID del mensaje de la solicitud, de esta manera el cliente puede ordenar varias respuestas de diferentes solicitudes que hayan llegado desordenadas o al mismo tiempo. En la Figura 4.2 se muestra un ejemplo de ésta situación.

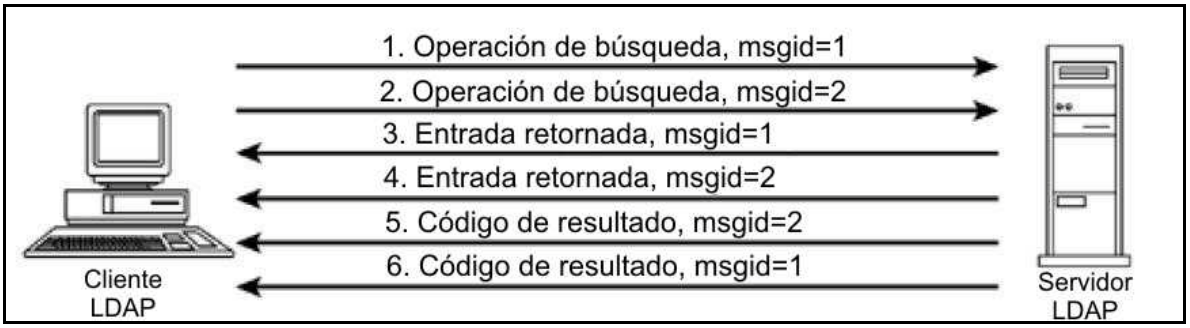

Figura 4.2 ID de mensajes de respuestas

4.3.1 Modelos del Protocolo LDAP.

El protocolo LDAP define un conjunto de cuatro modelos los cuales sirven de guía en el uso de directorios:

- **Modelo de información:** provee las estructuras y los tipos de datos necesarios para construir árbol de directorio LDAP [3].
- **Modelo de nombramiento:** describe como se puede organizar y hacer referencia a los datos almacenados en el directorio.
- **Modelo funcional:** describe que se puede hacer con la data almacenada en el directorio.
- **Modelo de seguridad:** describe como se puede proteger la data almacenada en el directorio de accesos no autorizados.

A continuación se detallaran cada uno de estos modelos en mayor profundidad.

4.3.2 Modelo de Información.

El modelo de información define los tipos de datos y las unidades básicas de información que se pueden almacenar en un directorio.

La unidad básica de información en los directorios es la entrada, la cual es una colección de información acerca de un objeto. En un directorio típico se pueden encontrar miles de entradas que corresponden a personas, departamentos, y otros objetos del mundo real [1]. A continuación se muestra un gráfico de un directorio típico con algunos objetos del mundo real en la organización.

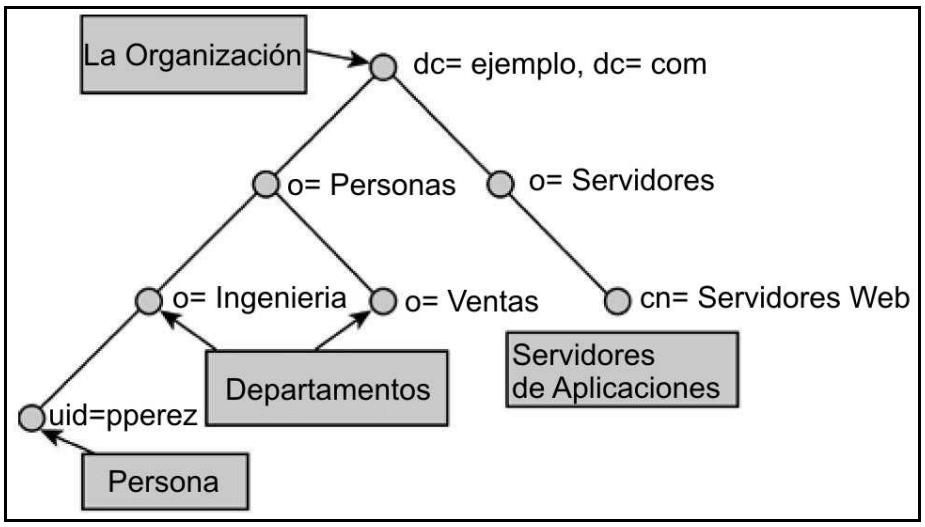

Figura 4.3 Muestra de Directorio

Cada entrada tiene un nombre distinguido (DN – Distinguished Name), por ejemplo en la Figura 4.3 el nombre distinguido para la entrada en el tope del árbol es ***dc=ejemplo, dc=com***. Una entrada se compone de un conjunto de atributos, cada uno de los cuales describe un rasgo en particular del objeto. Cada atributo tiene un ***tipo*** y uno o más valores. Los ***tipos*** describen el tipo de información contenida en los atributos y el valor contenido en los datos actuales. Los tipos de atributos también tienen asociado una sintaxis y un conjunto de reglas de congruencia. La sintaxis de un atributo especifica la forma de la data que puede estar presente en un atributo de este tipo. Por ejemplo la sintaxis ***entero*** permite que sólo estén presentes dígitos en un determinado valor [1].

4.3.3 Modelo de Nombramiento.

El modelo de nombramiento define como las entradas son identificadas y organizadas. Como se mencionó anteriormente las entradas son organizadas en una estructura tipo árbol llamada árbol de información del directorio (DIT). Las entradas son arregladas en el DIT según sus nombres distinguidos DN, los cuales son nombres únicos e identifican unívocamente a una sola entrada. Los DN están compuestos de una secuencia de nombres relativamente distinguidos (RDN – Relative Distinguished Name), los cuales representan cada uno de ellos a una rama en el DIT, que va desde la raíz del árbol a la entrada del directorio [6]. En otras palabras, cada una de las entradas tiene un atributo único entre todos los hermanos de un mismo padre. Este atributo único es el RDN [3].

Un ejemplo de un DIT es mostrado a continuación en la Figura 4.4, en el mismo cada cuadro representa una entrada en el directorio. La entrada directorio raíz es conceptual pero realmente no existe. Los atributos son listados dentro de cada entrada, éstas a su vez son identificadas de acuerdo a su posición en el DIT, por ejemplo la entrada más baja de la esquina derecha tiene el DN cn= Pedro Pérez, o= IBM, p=Venezuela. Como se puede ver en el ejemplo, los DN son leídos desde las hojas hacia la raíz del árbol, en contraste con las rutas en los sistemas de archivos, las cuales son leídas desde la raíz hacia la hoja [6].

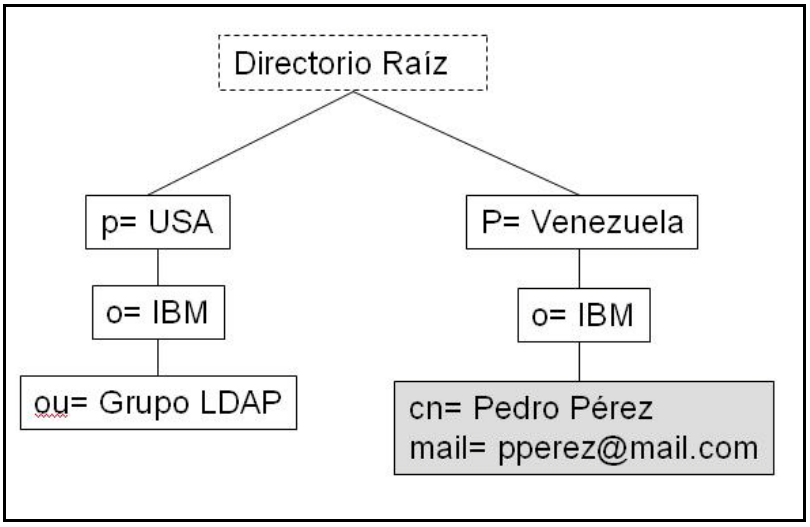

Figura 4.4 Muestra de un DIT

4.3.4 Modelo Funcional.

El modelo funcional de LDAP consiste en un conjunto de operaciones, las cuales se pueden dividir en tres grupos:

- **Las operaciones de consulta** permiten buscar en el directorio y recuperar datos del mismo.

- **Las operaciones de actualización** permiten agregar, eliminar, renombrar y modificar entradas en el directorio.

- **Las operaciones autenticación y control** permiten a los clientes identificarse en el directorio y controlar ciertos aspectos de una sesión.

Las dos operaciones de consulta permiten a los clientes LDAP buscar y recuperar datos en el directorio. La operación ***search*** permite a un cliente

encontrar entradas en el directorio, y la operación ***compare*** permite a un cliente probar si un entrada contiene un valor de atributo en particular [1].

La operación ***search*** permite a un cliente solicitarle al servidor LDAP la búsqueda a través de una parte del DIT para recaudar información, para esto el usuario especifica los criterios para leer y listar los resultados. Las operaciones de leer y listar no se encuentran separadas, ambas están incorporadas en la función de búsqueda. La operación ***search*** puede ser muy general o muy específica, ya que esta permite especificar el punto de comienzo de la búsqueda en el DIT, la profundidad de la misma y cuales atributos en una entrada deben de coincidir para retornar la entrada [6].

La segunda operación de consulta es la operación ***compare***, es usada para verificar si una entrada contiene un valor de atributo en particular. El cliente al realizar la solicitud para la comparación le suministra al servidor un DN, un nombre de atributo y un valor. El servidor devolverá una respuesta afirmativa en caso de que la entrada identificada por el DN contenga el atributo con el valor dado, de lo contrario la respuesta será negativa.

El comportamiento de la operación ***compare*** puede ser sustituido por una simple búsqueda aplicando los criterios necesarios para realizarla, mas no ha sido sustituida ya que su origen viene desde X.500 y además hay un sólo caso en el que el comportamiento de ambas operaciones difiere, y es cuando se intenta hacer la búsqueda sobre una entrada pero el atributo no se encuentra en la misma, la operación ***compare*** en este caso particular envía un mensaje al cliente indicándole que el atributo con el valor especificado no existe, a diferencia de la operación de búsqueda que no devolvería la entrada, lo que significa que la entrada no posee el atributo, por tal motivo con la operación ***compare*** es posible diferenciar entre "el atributo existe con un valor distinto al indicado" y "el atributo indicado no existe en la entrada". Por otra parte con la operación compare se intercambian menos bytes entre el cliente y el servidor [1].

En cuanto a las operaciones de actualización, se tienen cuatro operaciones las cuales se detallan a continuación.

La operación ***add*** permite agregar una nueva entrada en el directorio, esta tiene dos parámetros los cuales son el DN de la nueva entrada y un conjunto de atributos y valores los cuales constituirán la nueva entrada. Para agregar satisfactoriamente una nueva entrada deben cumplirse las siguientes cuatro condiciones:

- El padre de la nueva entrada debe de existir previamente en el directorio.
- El nombre de la nueva entrada no puede existir en alguna otra entrada en el directorio.
- La nueva entrada debe estar conforme al esquema que se encuentre en el directorio.
- El control de acceso debe permitir la operación.

La operación ***delete*** permite eliminar una entrada en el directorio, esta operación tiene un sólo parámetro que es el DN de la entrada que se desea eliminar. Para llevar a cabo esta operación satisfactoriamente se deben cumplir tres condiciones:

- La entrada que se desea eliminar debe existir previamente en el directorio.
- La entrada a eliminar no debe tener hijos.
- El control de acceso debe permitir la operación [1].

La operación ***rename***, permite renombrar y/o mover una entrada en el directorio, esta operación tiene cuatro parámetros los cuales son el DN de la entrada que se desea modificar, el nuevo RDN para la entrada, un argumento opcional que permite asignarle un nuevo padre a la entrada y la bandera para eliminar el RDN anterior. Para modificar una entrada satisfactoriamente deben cumplirse tres condiciones:

- La entrada que se quiere modificar debe existir previamente en el directorio.
- El nuevo nombre de la entrada, no debe estar usándose por alguna otra entrada.
- El control de acceso debe permitir la operación.

En caso de que la entrada que se renombre mantenga el mismo padre, el argumento del nuevo padre se debe dejar en blanco. Por otro lado el argumento del nuevo padre es un DN que identifica el contenedor hacia donde la entrada será movida. La bandera para eliminar el RDN anterior es un valor lógico que indica si el RDN anterior de la entrada será retenido como un atributo o si será eliminado.

La operación ***modify*** permite actualizar una entrada existente en el directorio, utiliza dos parámetros el primero es el DN de la entrada que se desea modificar y el segundo parámetro es el conjunto de modificaciones que se desean aplicar. Estas modificaciones pueden especificar un nuevo atributo – valor para ser agregado a la entrada, o cual atributo – valor se desea eliminar de la entrada, o si todos los atributos – valores serán reemplazados por un nuevo conjunto de atributos – valores. La solicitud de modificación puede incluir tantas modificaciones de atributos como sean necesarias.

Las operaciones de autenticación y control son tres, de las cuales dos son de autenticación que son ***bind*** y ***unbind*** y la de control es ***abandon***.

La operación ***bind*** es usada por un cliente para autenticarse en un directorio proporcionando un DN y un conjunto de credenciales, el servidor se encarga de verificar que las credenciales sean correctas y de ser así, el cliente quedará autenticado en el directorio identificado por el DN mientras se mantenga la conexión abierta o hasta que el cliente se reautentique. El servidor puede asignar privilegios al cliente basándose en las credenciales suministradas.

La operación ***bind*** simplemente envía la contraseña por la red al servidor en texto claro. Sin embargo esta puede ser protegida de espías que se encuentren interceptando contraseñas, codificando la conexión mediante SSL o TLS. En LDAPv3 se incluyen nuevos tipos de operaciones ***bind***, como por ejemplo SASL bind, la cual permite al cliente especificar el tipo de protocolo de autenticación que desea usar. SASL es un protocolo extensible independiente del framework para desarrollar autenticación y negociaciones de parámetros de seguridad.

La operación ***unbind*** no tiene parámetros, cuando un cliente emite esta operación el servidor de autenticación descarta cualquier información que se tenga asociada a la conexión del cliente, pone fin a las operaciones de LDAP que se encuentren pendientes y cierra las conexiones TCP, por lo tanto desconecta al cliente.

La operación ***abandon*** únicamente tiene como parámetro el ID de la operación que se desea abandonar, un cliente emite esta operación cuando ya no está interesado en obtener resultados de alguna operación previamente iniciada, la cual corresponde con el ID suministrado por el usuario. Esta operación es utilizada por lo general para detener búsquedas demasiado largas [1].

4.3.5 Modelo de Seguridad.

El propósito del modelo de seguridad es el de proveer un framework para proteger la información contenida en el directorio de accesos no autorizados.

El modelo de seguridad depende del hecho de que LDAP es un protocolo orientado a conexión, ya que un cliente abre una conexión con el servidor LDAP y realiza diversas operaciones del protocolo en la misma conexión. Un cliente LDAP puede autenticarse en el servidor de directorio en algún punto durante el tiempo de vida de la conexión y en ese punto se le pueden conceder privilegios adicionales.

El proceso de autenticación consiste en que el cliente le provee al servidor un DN y una contraseña enviados en texto claro, el servidor por su parte localiza la entrada que corresponde al DN provisto por el cliente y verifica si la contraseña dada por el cliente coincide con la que se encuentra almacenada en el atributo userPassword de la entrada, de ser así el cliente es autenticado de lo contrario el proceso de autenticación falla y el servidor le envía un mensaje de error al cliente.

Este proceso de autenticación en el servidor se conoce como ***binding***. Una identidad es ligada a la conexión cuando la operación ***bind*** alcanza una autenticación exitosa. En caso de que un cliente no se autentique o lo haga sin proveer alguna credencial, es catalogado como anónimo y se le conceden el conjunto de privilegios por defecto usualmente este conjunto contiene una mínima cantidad de privilegios y es completamente restrictivo.

Conociendo la necesidad de soportar diferentes métodos de autenticación en LDAPv3 se adopta el Framework SASL, el cual provee una manera estándar para soportar múltiples protocolos de autenticación. Cada tipo de sistema de autenticación corresponde a un mecanismo particular de SASL. Uno de los mecanismos de SASL es un identificador que describe el tipo de protocolo de autenticación que está siendo soportado.

Durante el desarrollo de LDAPv3 se detectó la necesidad de definir un conjunto mínimo de métodos de autenticación que deben estar soportados en los servidores LDAPv3. Para esto el grupo de trabajo de LDAP define métodos de autenticación cuya implementación es obligatoria según el RFC 2829 – Lightweight Directory Access Protocol (v3): Technical, en este documento los

servidores LDAP se desglosan en tres grupos diferentes con requerimientos separados para cada uno:

- Los servidores de directorio públicos de sólo lectura pueden permitir la autenticación anónima, la cual no requiere de contraseña alguna.
- Los servidores que soportan la autenticación basada en contraseña deben soportar el mecanismo SASL Digest- MD5, el cual se encuentra documentado en el RFC 2831 - Using Digest Authentication as a SASL Mechanism.
- Los servidores que requieren sesiones protegidas bajo encriptación y autenticación, deben implementar la operación extendida StartTLS definida en el RFC 2830 – Lightweight Directory Access Protocol (v3): Extension. Esta operación permite a un cliente LDAP solicitar encriptación de toda la información entre este y el servidor, lo que permite al cliente y el servidor autenticarse mutuamente usando certificados de clave pública [1].

La capa de transporte de seguridad (TLS – Transport Layer Security) es una tecnología de seguridad que apoya la privacidad, la integridad de la información, y la encriptación para los protocolos orientados a conexión como TCP. Los clientes que utilizan TLS para comunicarse con un servidor:

- Pueden estar seguros que la comunicación será inmune a espías.
- Pueden estar seguros que la comunicación será inmune a manipulaciones, como por ejemplo ataques de "hombre en el medio".
- Pueden autenticarse al servidor usando certificados de clave pública.
- Pueden verificar la autenticidad del servidor al cual están conectados verificando el certificado de clave pública del mismo.

TLS permite a un cliente establecer la comunicación sin encriptación, y negociar la encriptación y la autenticación después de establecer la conexión. Esto significa que en un servidor LDAP donde se soporte TLS, se pueden tener ambos tipos de clientes, los seguros y los no seguros en el mismo puerto TCP, a diferencia del uso de LDAP sobre SSL, conocido como LDAPS donde los servidores LDAPS deben proveer este servicio en diferentes puertos TCP, por lo general estos servidores escuchan por el puerto TCP 389 para las conexiones LDAP y por el puerto 636 para las conexiones LDAPS.

En la Figura 4.5 se muestra un ejemplo de cómo TLS permite asegurar la transmisión de la data del directorio sobre Internet.

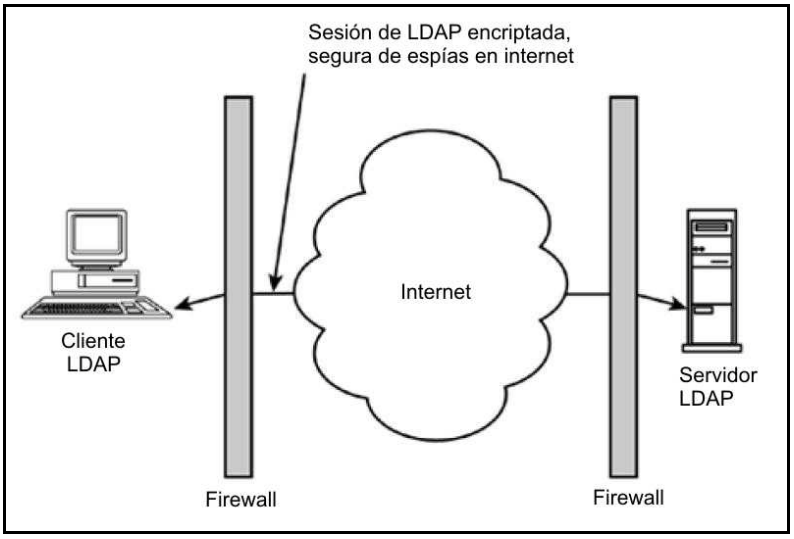

Figura 4.5 Sesión de LDAP usando TLS

La operación extendida StartTLS, es el medio por el cual un cliente le indica a un servidor LDAP cual TLS debe utilizarse en alguna conexión LDAP existente. Después que un cliente LDAP inicia TLS, este puede conectarse a través del uso del mecanismo SASL externo. El servidor típicamente mapea el certificado provisto por el cliente a la entrada del directorio usando un método de implementación específico. Un cliente LDAP normalmente ejecuta los siguientes pasos para establecer una conexión segura, autenticada a un servidor de directorio:

- Abre una conexión TCP al servidor.
- Envía una operación extendida StartTLS, y los protocolos de capas inferiores negocian la encriptación y la autenticación de acuerdo a las especificaciones del TLS.
- Se conectan usando el mecanismo SASL externo en caso de que algún certificado sea provisto durante la negociación del TLS, o utilizando otro mecanismo SASL, como por ejemplo Digest-MD5.

Capítulo 5: Portal Cautivo

En este capítulo se explicará un poco el concepto de un portal cautivo y en particular se explicará brevemente el funcionamiento de la implementación Chillispot, la cual fue la utilizada para este proyecto.

5.1 Portal Cautivo.

Un portal cautivo es una técnica en donde se fuerza a un cliente HTTP (Hypertext Transfer Protocol – Protocolo de Transferencia de Hipertexto) a ver una página Web en especial, la cual generalmente es utilizada para poder realizar el proceso de autenticación de dicho cliente. Una vez que el cliente haya sido autenticado satisfactoriamente, este puede usar el servicio de forma normal [12].

Para lograr este comportamiento es necesario interceptar todos los paquetes, independientemente del destino de los mismos, negando así la conectividad al cliente. Una vez que este abra algún navegador para consultar un sitio Web, será redirigido a una página Web donde se pueden presentar diferentes mensajes, desde la aceptación de un conjunto de políticas de uso hasta la solicitud de alguna autenticación.

5.2 Chillispot.

Chillispot es una implementación software libre de un portal cautivo, la cual es usada generalmente como controlador de los puntos de acceso de una red inalámbrica. Generalmente es utilizado como intermediario en el proceso de autenticación de usuarios en una red inalámbrica.

Algunas de sus principales características son:

- Permite realizar la autenticación a través de un servidor RADIUS, usando dos métodos, UAM (Universal Access Method – Método de Acceso Universal) que es el método tradicional de los portales cautivos; adicionalmente se permite el uso del método WPA a través del AP.
- Permite el uso de atributos RADIUS definidos previamente por la WIFI Alliance, los cuales permiten controlar el ancho de banda y la cantidad máxima de tráfico utilizable por cada cliente.
- Posee servicio de DHCP.

- Puede actuar como Proxy-RADIUS para otros métodos de autenticación.
- No exige el uso específico de algún AP en particular.
- Requiere de un servidor Web con soporte de HTTPS (Hypertext Transfer Protocol Secure – Protocolo Seguro de Transferencia de Hipertexto), para realizar el proceso de autenticación de los usuarios al servidor RADIUS.

Chillispot tiene dos componentes principales:

- Una aplicación en el espacio de usuario denominada chilli, la cual es el portal cautivo en sí mismo, y cumple con las funciones de servidor DHCP, Cliente RADIUS, Proxy RADIUS y Redirector.
- Un archivo CGI que se ubica en el servidor Web denominado Hotspotlogin.cgi; el cual es un script programado en Perl, encargado de enviar los datos de autenticación a la aplicación chilli. Este script genera un desafío CHAP para validar el usuario y la clave de acceso que ha recibido del cliente, a través del servidor Web cifrado con HTTPS, y envía el mismo a chilli [12].

5.2.1 Métodos de Autenticación.

Como se mencionó anteriormente, Chillispot permite dos métodos de autenticación, los cuales son UAM y WPA. Cuando se utiliza el método UAM, el cliente recibe una dirección IP a través del protocolo DHCP, pero cuando este intenta accesar a Internet, todo el trafico es redirigido hacia el servidor Web, donde se ubica una página de bienvenida, en la cual es posible realizar el proceso de autenticación del cliente. Una vez que el cliente ha ingresado sus datos de usuario, un script en el servidor Web, cifra la contraseña y la envía al programa chilli, el cual realiza la autenticación contra el servidor RADIUS. Luego de realizada la autenticación satisfactoriamente, se permite el tráfico normalmente.

En caso de usar el método WPA, el AP es el encargado de realizar el proceso de autenticación, en donde el cliente establece una sesión a través del protocolo EAP con el punto de acceso, el cual tiene configurado como servidor RADIUS a Chillispot. En este caso Chillispot oficia como Proxy RADIUS, reenviando la solicitud de acceso al servidor RADIUS, quien ejecuta el proceso de autenticación. En caso que la autenticación sea satisfactoria, Chillispot debe recibir un mensaje de acceso aceptado para posteriormente asignar al cliente una dirección IP mediante el protocolo DHCP [12].

Capítulo 6: Descripción y Análisis para el Control de Acceso Inalámbrico.

Para la realización del sistema de autenticación planteado en el presente trabajo, fue necesario conocer previamente los requerimientos que se debían cumplir con este sistema.

6.1 Requerimientos de la Solución.

Actualmente la red inalámbrica de la Facultad de Ciencias, carece de cualquier método de seguridad, y no se lleva ningún registro de los usuarios que se conectan a la red. Por tanto se plantea solventar estas deficiencias para mejorar así la seguridad en dicha red.

A continuación se listan los requerimientos que se deben cumplir con la solución:

1. El sistema debe realizar la autenticación de los usuarios que deseen acceder a la red inalámbrica, previo a su ingreso.

2. Debe existir una base de datos centralizada con toda la información de los usuarios pertenecientes a la red.

3. El proceso de autenticación de autenticación de los usuarios debe hacerse mediante una interfaz Web sencilla, para así facilitar el proceso a los usuarios.

4. El sistema debe funcionar correctamente sin importar el navegador que se utilice en los equipos de los clientes.

5. El sistema debe funcionar correctamente con cualquier Punto de Acceso, y no limitarse a un modelo en particular.

6. Se debe llevar un registro con la información de los usuarios que han accedido a la red.

6.2 Análisis

Para cumplir con los requerimientos planteados en el punto anterior se instaló un sistema de autenticación, basado en un servidor RADIUS, ya que este protocolo permite no sólo realizar el proceso de autenticación, sino que también permite llevar un registro de los usuarios que han accedido al sistema. Con esto se estaría cubriendo con los requerimientos 1 y 6 de los planteados en el punto anterior.

En cuanto a la manera en que se realiza el proceso de autenticación, es posible hacer uso de un portal cautivo, con el cual se realice este proceso vía Web, y se garantiza que el usuario no podrá realizar ninguna otra acción hasta tanto no se haya autenticado correctamente. Al hacer esto se estaría cumpliendo con los requerimientos 1, 3 y 4 de los planteados en el punto anterior.

Para el manejo de la información de usuarios, es posible hacer uso de un servidor LDAP, el cual permite manejar la información de los usuarios de manera eficiente y existen varias implementaciones de este protocolo, las cuales funcionan perfectamente en conjunto con los servidores RADIUS. De esta manera se estaría cumpliendo con el requerimiento 2, de los planteados anteriormente.

En cuanto al requerimiento 5, es bastante simple ya que existen varias implementaciones de un portal cautivo, las cuales no exigen el uso de un punto de acceso en específico. Por tanto se estarían cumpliendo así con todos los requerimientos planteados anteriormente.

Capítulo 7: Configuración de la Solución de Control de Acceso Inalámbrico

En este capítulo se especificarán las herramientas necesarias para la puesta en marcha del Sistema de Control de Acceso Inalámbrico, así como también se explicará detalladamente todo el proceso de instalación y configuración del mismo.

7.1 Herramientas

Para la instalación y configuración del Sistema de Control de Acceso de la red Inalámbrica, fue necesario contar con un conjunto de herramientas tanto de Hardware como de Software. A continuación se detallan cada una de ellas.

7.1.1 Herramientas de Hardware

En cuanto a los dispositivos de hardware necesarios se encuentran:

- Una computadora la cual servirá como servidor de autenticación RADIUS.
- Una computadora, la cual almacenará la información de los usuarios al funcionar como servidor LDAP.
- Una computadora, con dos (2) interfaces de red, para funcionar como servidor del portal cautivo Chillispot.
- Un Punto de Acceso Inalámbrico, el cual es indispensable pero no específico a un modelo de algún fabricante en particular.

Cada una de las computadoras usadas para los servidores, tenía la siguiente configuración de hardware:

- Procesador equivalente a Pentium 4, no mayor de 2 Ghz.
- 512 MB de memoria
- Disco duro de 40 GB
- Una interfaz de red

7.1.2 Herramientas de Software

En cuanto a las herramientas de software necesarias se encuentran:

- En cada computadora que funcione como servidor, es necesario instalar como sistema operativo, el sistema Linux ya que cada una de las aplicaciones involucradas en el Sistema de Control de Acceso, se ejecutan bajo ambiente Linux. Lo cual convierte al Sistema de Control de Acceso en una solución de software libre, completamente aplicable en cualquier escenario donde se presente este mismo problema y sin necesidad de generar costo por su utilización.
- En el servidor RADIUS, es necesario instalar la aplicación FreeRADIUS, la cual es una implementación en software libre del protocolo RADIUS, y la misma contiene módulos que brindan total compatibilidad con LDAP.
- En el servidor LDAP, es necesario instalar la aplicación OpenLDAP, la cual es una implementación en software libre de dicho protocolo, y funciona perfectamente en conjunto con FreeRADIUS. Además también es necesario instalar la aplicación PhpLDAPAdmin, la cual permite llevar la administración del servidor LDAP, mediante una interfaz gráfica vía Web.
- En la computadora que funcionará como servidor del portal cautivo, es necesario instalar la aplicación Chillispot, la cual permite realizar la autenticación de los usuarios mediante una interfaz Web. Igualmente es necesario instalar un servidor Web con soporte SSL, el cual permitirá establecer una conexión segura durante el proceso de autenticación.

Las versiones utilizadas de cada uno de los programas, se mencionan más adelante al igual que la configuración hecha a los mismos.

7.2 Proceso de Configuración

Para la configuración del sistema de control de acceso, fue necesario realizar la instalación de los siguientes paquetes, dicha instalación se realizó en el orden en que se mencionan cada uno:

- **Servidor LDAP:** Servidor encargado del manejo de la información de los usuarios que tendrán acceso a la red.
- **PhpLDAPAdmin:** Aplicación que permite realizar la administración del servidor LDAP a través de una interfaz web.
- **Servidor RADIUS:** Servidor encargado de realizar el proceso de autenticación, autorización y manejo de cuentas de los usuarios.
- **Chillispot:** Aplicación encargada de asignar la dirección IP a los usuarios de la red, y redirigirlos a una página web para iniciar el proceso de autenticación.

A continuación se explicará con mayor detalle el proceso de instalación y configuración de cada una de las aplicaciones antes mencionadas. Cabe destacar que todas estas aplicaciones fueron instaladas en el mismo equipo, ya que de esta manera se centraliza el proceso de administración del sistema, y se reducen los posibles puntos críticos en el mismo. Dicho equipo funcionaba con el sistema operativo Linux Debian Etch.

7.2.1 Servidor LDAP.

El servidor LDAP es el encargado de almacenar toda la información de los usuarios que tendrán acceso a la red inalámbrica. Para realizar la instalación de este servidor, fue necesaria la instalación de los siguientes paquetes:

- Slapd v.2.3.30: Paquete de instalación de la implementación del servidor OpenLDAP
- ldap-utils v.2.3.30 : Paquete de utilidades del servidor OpenLDAP
- db4.2-util v.4.2.52: Utilidades para el uso de la base de datos Berkeley en OpenLDAP

Una vez instalados los paquetes anteriores se procedió a la configuración del servidor. En primer lugar se editó el archivo slapd.conf, el cual contiene la configuración del servidor. Los cambios realizados a este archivo fueron los siguientes:

1. Se añadieron los schemas “samba.schema” y “openldap.schema”, los cuales son necesarios para la configuración de los atributos de los usuarios, que se utilizaran durante el proceso de autenticación en conjunto con el servidor

RADIUS.

2. Se especificó el nivel de profundidad del archivo log del servidor LDAP, para que guardara todas las operaciones realizadas y los resultados de las mismas.
3. Se indica el tipo de base de datos a utilizar, la cual es la base de datos Berkeley.
4. Se indica la ruta en el árbol de directorio del comienzo del árbol, a partir de este punto se realizarán las consultas en el mismo.
5. Se especifica la ruta del usuario administrador en el árbol de directorio.

A continuación en la Figura 7.1 se muestran los cambios realizados en este archivo.

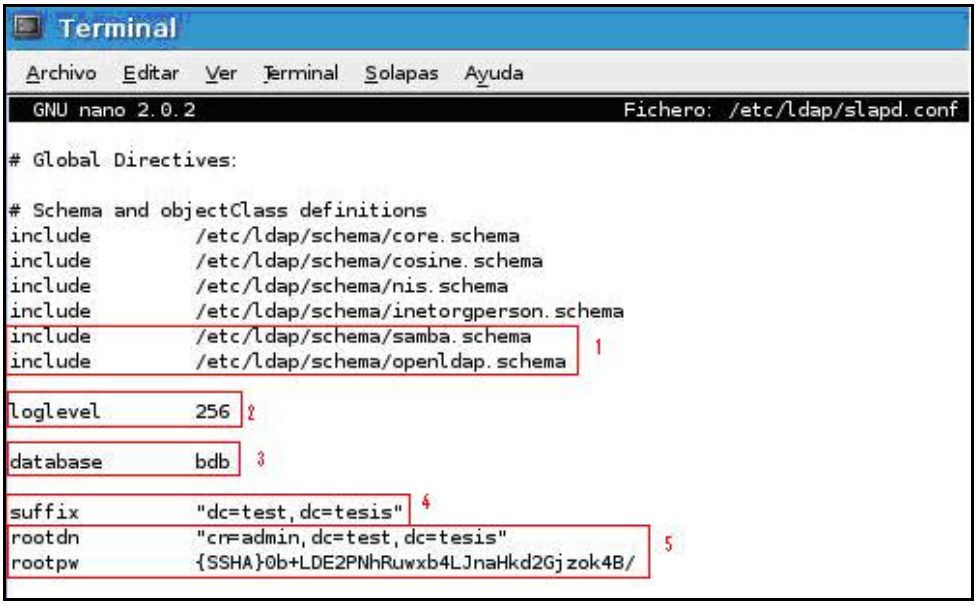

Figura 7.1 Archivo de configuración slapd.conf.

Una vez culminada la configuración del servidor, se procedió a la carga de la información con la estructura del árbol de directorio, así como también la información de los usuarios al directorio. Todos estos datos se encuentran contenidos en los archivos tree.ldif y users.ldif, respectivamente. A continuación se muestra la Figura 7.2, en donde se aprecia la estructura del DIT.

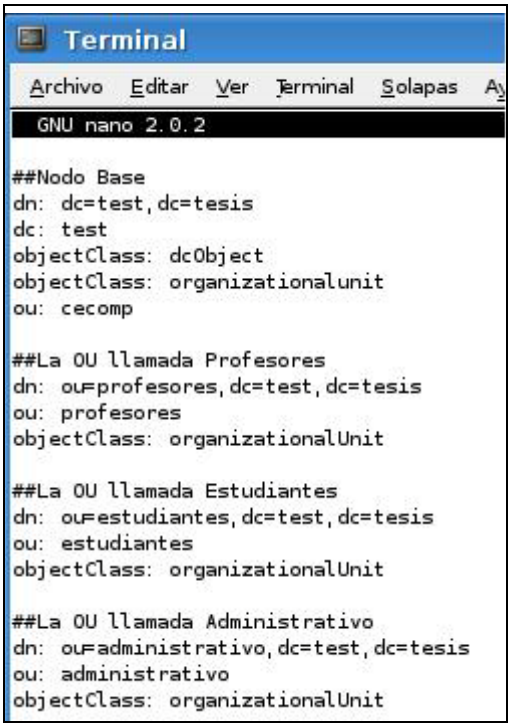

Figura 7.2 Muestra del archivo tree.ldif.

A continuación se muestra la Figura 7.3, donde se aprecia un extracto del archivo users.ldif en donde se contiene la información referente a los usuarios del directorio.

Figura 7.3 Muestra del archivo users.ldif.

Luego de cargar la información dentro del árbol de directorio y tener en funcionamiento el servidor LDAP, se instaló la aplicación PhpLDAPAdmin v.0.9.8.3-8, la cual permitirá llevar la administración del servidor mediante una interfaz Web de manera más simple y amena. Una vez finalizada la instalación, es

posible realizar la conexión con el servidor mediante la siguiente URL: http://localhost/phpldapadmin/

Para almacenar los datos de configuración pertenecientes a un perfil de usuario se creó la unidad organizativa Perfiles (ou=Perfiles), cada uno de los objetos dentro de esta unidad representa una política de conectividad específica para un grupo de usuarios. Los objetos que representan un perfil de usuario pertenecen a las siguientes clases:

- **RadiusObjectProfile:** Es una clase de objeto contenedor que se utiliza para crear objetos radiusprofile.
- **Radiusprofile:** Es una clase de objeto que posee los atributos necesarios para definir un perfil estándar de RADIUS.

Para almacenar los datos referentes a los permisos de cada perfil se hace uso del atributo Description, ya que este atributo soporta valores múltiples y soporta una longitud máxima de 1024 caracteres. Los valores de los permisos se almacenan en forma de reglas, definiendo una regla para cada valor de atributo. Dichas reglas deben usar el formato de la sintaxis del comando iptables de netfilter.

La vinculación de un usuario con un perfil de usuario se realiza mediante el atributo RadiusProfileDn en el objeto del usuario, el mismo debe contener el dn del perfil del usuario. El atributo dialupAccess es un atributo especial específicamente definido en la clase radiusprofile para usarse con soporte LDAP, la existencia de este atributo en un usuario con valor yes, significa que dicho usuario tiene autorización para conectarse. En caso de que el atributo no exista o posea el valor FALSE, indica que el usuario tiene denegado el acceso y el servidor RADIUS no continúa con el proceso de autenticación.

7.2.2 Servidor RADIUS.

Para la instalación de este servidor se utilizó la aplicación freeradius 1.1.3-3, la cual es una implementación del servidor RADIUS en software libre, que posee un amplio soporte con LDAP, para realizar el almacenamiento de la información.

El paquete freeradius disponible en los repositorios de la distribución Debian, por defecto viene sin soporte para el protocolo EAP. Por tal motivo fue necesario descargar los archivos fuentes para dicho paquete para su posterior compilación. Todo el proceso de compilación e instalación se encuentra explicado

detalladamente en el manual de instalación anexo al presente trabajo.

La configuración del servidor se encuentra conformada por varios archivos. Las directivas principales de configuración se encuentran en el archivo /etc/freeradius/radiusd.conf. Para permitir que el servidor RADIUS realice consultas en el directorio LDAP previamente configurado, se editó el módulo LDAP dentro de este archivo, en la Figura 7.4 se puede observar la configuración de este módulo.

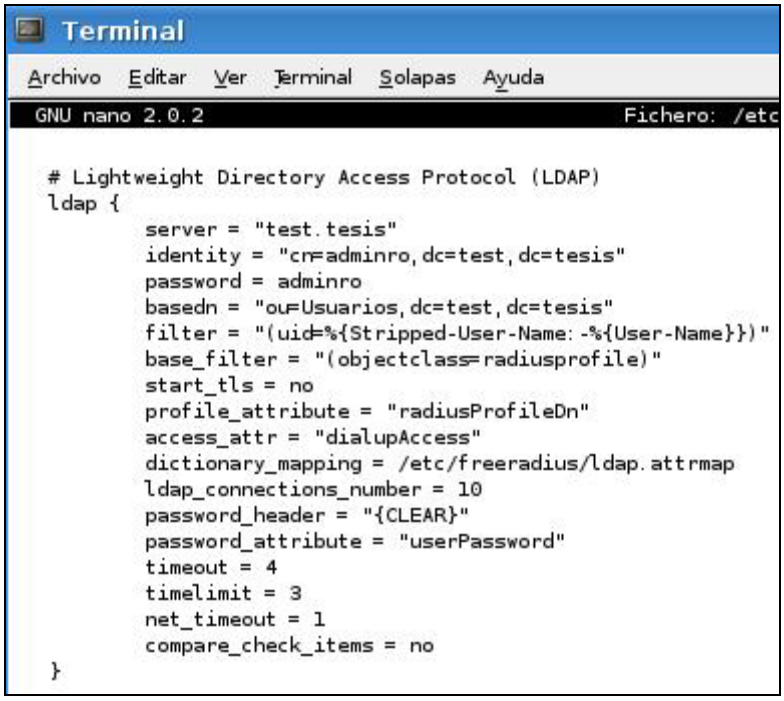

Figura 7.4 Configuración del módulo LDAP.

El módulo MSCHAP soporta la autenticación MS-CHAP y MS-CHAPv2, y es utilizado por el método de acceso EAP-PEAP. En la Figura 7.5 se muestra la configuración requerida para este módulo.

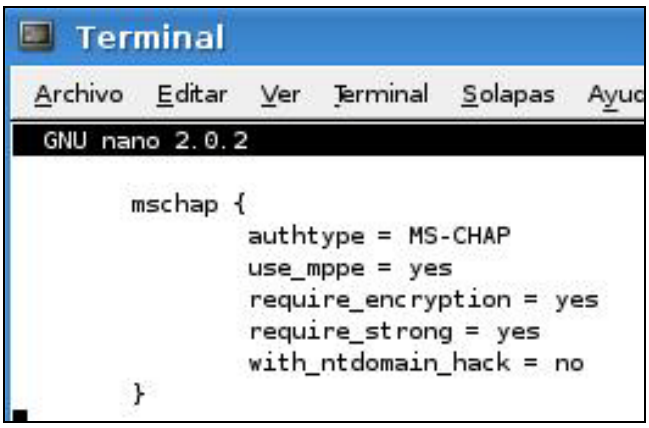

Figura 7.5 Configuración del módulo MSCHAP.

La sección de configuración EAP se encuentra en el archivo eap.conf, aquí se colocaron todas las directivas de configuración para las variantes soportadas de dicho protocolo. En este caso, que se ha elegido usar EAP-PEAP, será necesario configurar también la sección de EAP-TLS, ya que este protocolo realiza el intercambio de paquetes dentro de un túnel TLS y requiere certificado sólo por parte del servidor.

La sección de directivas de configuración del módulo EAP se divide en una sección de configuración común y diferentes subsecciones para cada una de las configuraciones específicas del protocolo EAP. Para realizar la configuración de EAP-TLS, es necesario crear previamente una Autoridad Certificadora (CA) y generar las claves y certificados para el servidor. El proceso para la creación de la CA y generar las claves y certificados del servidor, se describe detalladamente en el manual de instalación anexo al presente trabajo.

A continuación se muestra la Figura 7.6, donde se observa la sección de EAP-TLS del archivo eap.conf con la configuración realizada:

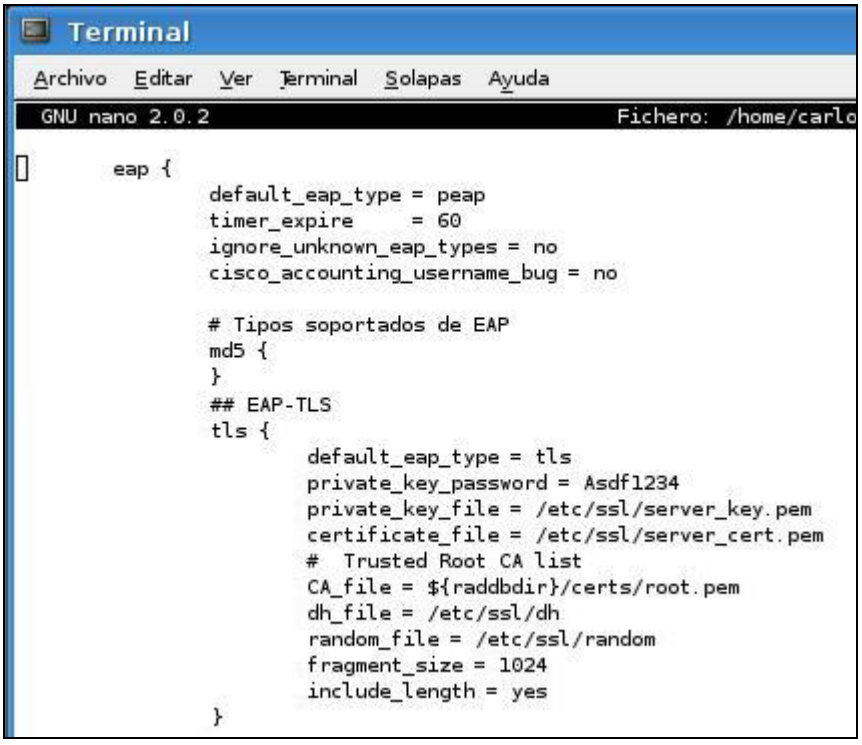

Figura 7.6 Directivas de configuración para EAP-TLS

De igual manera se configuraron las directivas para los tipos EAP-PEAP y EAP-TTLS, como se muestra en la Figura 7.7.

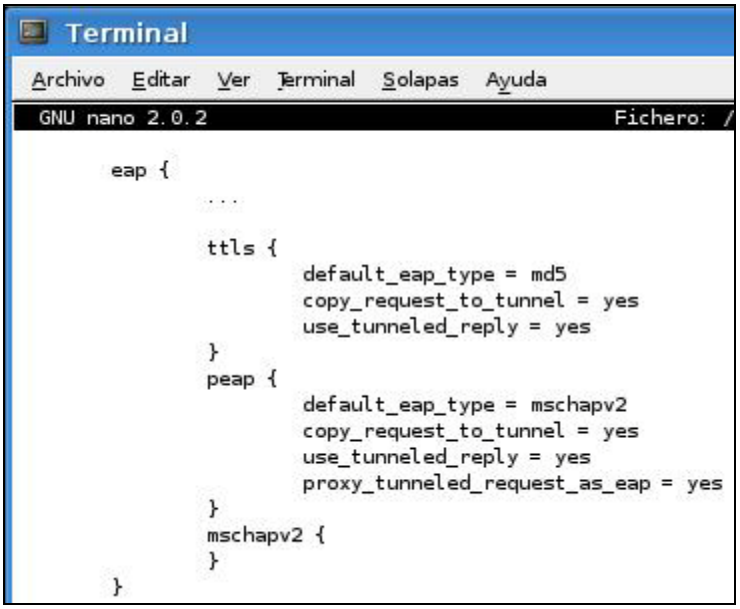

Figura 7.7 Directivas de configuración para EAP-PEAP y EAP-TTLS.

El registro de accounting se realiza mediante el uso del módulo radutmp, donde se registra los inicios de sesión y las terminaciones de sesión. Los archivos con los registros se encuentran almacenados en el directorio /var/log/freeradius/radacct, dentro de este directorio se crea un directorio cuyo nombre es la dirección IP con la que el servidor RADIUS acepta solicitudes, en este directorio se crea un archivo diariamente, en donde queda registrado todas las conexiones que se hayan realizado en ese día. En estos registros se guardan la fecha y hora, el nombre del usuario, y la dirección IP desde donde se realizó la conexión.

La sección authorize del archivo radiusd.conf, también es necesario configurarla colocando los nombres de los módulos definidos en las secciones anteriores. Es importante el orden en que se colocan los módulos. El módulo eap debe ser el primer módulo de autorización, luego de los módulos preprocess y auth_log que son los encargados de realizar los procesos para evitar ambigüedades en los nombres de usuario y el registro de pedidos de autorización. En la Figura 7.8 se puede apreciar la configuración realizada para esta sección.

Figura 7.8 Sección authorize del archivo radiusd.conf

La sección autentícate se debe configurar listando los módulos disponibles para realizar el proceso de autenticación. Dicho proceso no intenta autenticar probando con cada uno de los módulos aquí listados, sino que el módulo usado en la sección authorize agrega un atributo de configuración denominado Auth –Type. Ese tipo de autenticación se utiliza para elegir el módulo apropiado de la lista definida. En la Figura 7.9 se muestra la configuración realizada a este módulo.

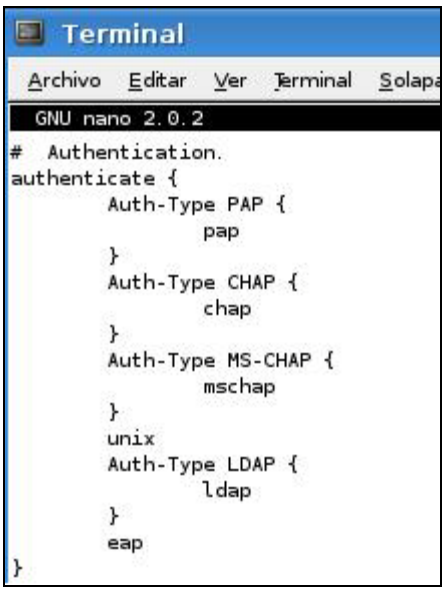

Figura 7.9 Sección autentícate del archivo radiusd.conf.

Una vez configurada esta última sección se termina la configuración principal del servidor RADIUS, sólo queda por modificar el archivo clients.conf donde se definen los NAS que pueden comunicarse con el servidor. En este archivo se debe colocar desde donde se permite el acceso al servidor RADIUS y con que contraseña. A continuación se muestra la Figura 7.10 con la configuración realizada en el mismo.

Figura 7.10 Configuración del archivo clients.conf.

7.2.3 Servidor Chillispot (Portal Cautivo).

La implementación del portal cautivo que se eligió se llama Chillispot, esta posee una implementación sencilla y depende de muy pocos servicios externos para funcionar. Algunas características de Chillispot son las siguientes:

- Soporta dos métodos de autenticación UAM (Universal Access Method – Método de Acceso Universal) y WPA/RSN (Wireless Protectes Access – Acceso Inalámbrico Protegido).
- Permite realizar los procesos de Autenticación, Autorización y Registro contra un servidor RADIUS.
- Posee un servidor DHCP propio para ambos métodos de autenticación.
- La autenticación con UAM soporta SSL.
- No exige la utilización de algún AP en particular.
- Funciona utilizando NAT o Routing.

Para este sistema se eligió la autenticación UAM, en donde se entrega una dirección IP a través del protocolo DHCP, pero cuando el cliente intenta conectarse, este es redirigido hacia una página de bienvenida en donde debe realizar el proceso de autenticación. Una vez que el usuario sea autenticado correctamente se deja de redireccionar el tráfico.

Para el correcto funcionamiento del servidor Chillispot se debe cumplir con los siguientes requerimientos:

- Un punto de acceso inalámbrico, el cual es indispensable pero no es sujeto a un modelo específico.
- El equipo donde funcionará el servidor Chillispot, debe tener dos interfaces de red.
- Se debe disponer de un Servidor RADIUS.
- Es necesario un servidor Web con soporte SSL.

Una vez instalado la aplicación Chillispot, se editó el archivo /etc/chilli.conf, el cual guarda la configuración principal del servidor. La configuración realizada en el mismo se muestra en la Figura 7.11.

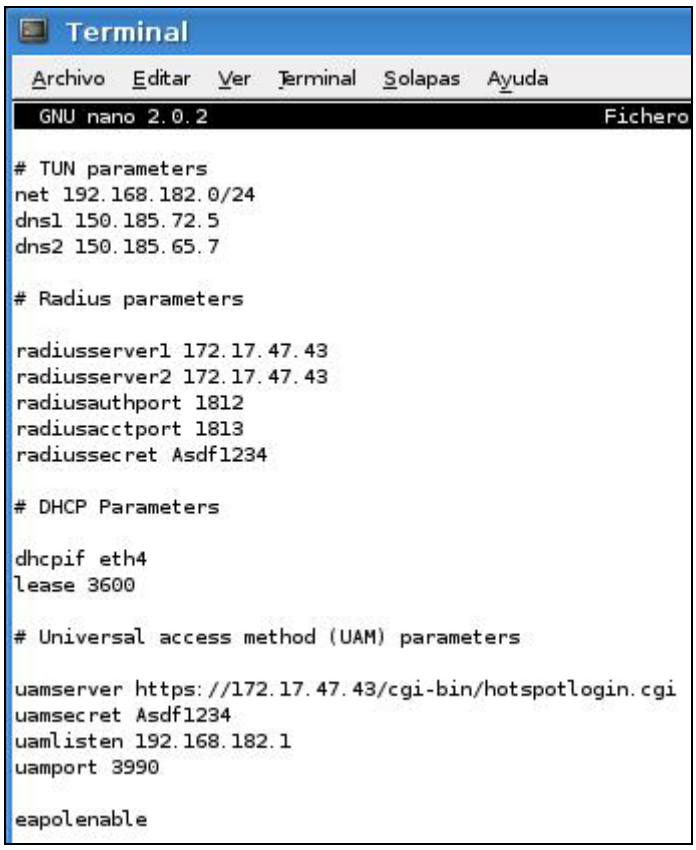

Figura 7.11 Archivo de configuración chilli.conf

Una vez configurado este archivo, es necesario copiar en el servidor web el script encargado de realizar el proceso de autenticación. Para hacer esto se ejecutan en consola los siguientes comandos:

```
#gunzip   /usr/share/doc/chillispot/hotspotlogin.cgi.gz
#cp /usr/share/doc/chillispot/hotspotlogin.cgi   /usr/lib/cgi-bin/
```

Para realizar la instalación del servidor web con soporte SSL, se ejecutó el siguiente comando:

```
#apt-get   install   apache2   apache2.2-common   apache2-utils
```

Para generar el certificado SSL con el que trabajará el servidor web Apache, se ejecutaron los siguientes comandos:

```
#make-ssl-cert   /usr/share/ssl-cert/ssleay.cnf   /etc/apache2/ssl/apache.pem
```

Luego de llenar los datos solicitados en el paso anterior, se debe habilitar el módulo con el comando: "a2enmod ssl".

Una vez habilitado el módulo, se debe crear el sitio SSL. Por defecto apache trae un archivo default, ubicado en el directorio /etc/apache2/sites-available/. Se debe realizar una copia de este archivo para poder modificarlo. La configuración de este archivo nuevo archivo se muestra a continuación en la Figura 7.12.

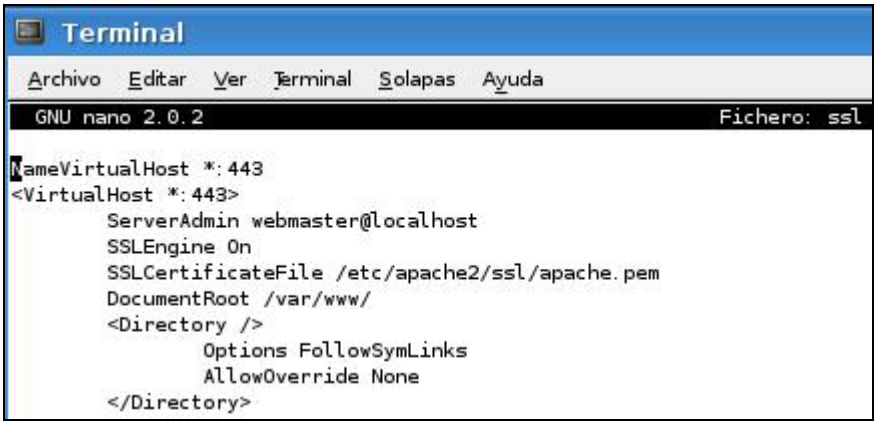

Figura 7.12 Configuración del sitio ssl

Para finalizar la configuración del servidor web apache, se debe habilitar el sitio ssl con el siguiente comando: "a2ensite ssl".

Una vez finalizada la configuración del servidor web, sólo resta por editar dos archivos, el primero de ellos es el que contiene la configuración de las reglas de iptables que usa el servidor chillispot; cabe destacar que este archivo debe tener los permisos necesarios para ser accedido por cualquier usuario que inicie sesión en el equipo. Para realizar esto se ejecutan los siguientes comandos:

```
#cp   /usr/share/doc/chillispot/firewall.iptables   /etc/init.d/chillispot.iptables
#chmod   755   /etc/init.d/chillispot.iptables
```

Con los comandos anteriores se garantiza el correcto funcionamiento del servidor Chillispot, cada vez que se reinicie el equipo. Luego se debe verificar que los parámetros INTIF y EXTIF contengan los valores correspondientes a las interfaces

de la red interna y la red externa respectivamente. Cabe destacar que la interfaz de la red interna, es la misma interfaz utilizada en la red inalámbrica. Luego de realizar estos cambios se debe agregar las reglas al inicio del sistema, mediante el siguiente comando:

```
#ln  -s  /etc/init.d/chillispot.iptables  /etc/rcS.d/S40chillispot.iptables
```

Por último se debe modificar el archivo /usr/lib/cgi-bin/hotspotlogin.cgi, el cual corresponde al script usado por chillispot durante el proceso de autenticación. En este archivo se debe verificar que el parametro "$uamsecret", contenga el mismo valor especificado en el archivo de configuración chilli.conf. Igualmente se debe descomentar la línea "$userpassword=1;" para permitir el uso del atributo user-password durante la autenticación contra el servidor RADIUS.

Este mismo archivo contiene el código HTML de las páginas que se muestran en el proceso de autenticación, si se desea estas pueden ser modificadas.

Capítulo 8: Pruebas y Resultados de la Solución de Control de Acceso Inalámbrico.

En este capítulo se detallaran como fue el escenario para la realización de pruebas, y se mostraran todas las pruebas realizadas al sistema de control de acceso inalámbrico, con sus respectivos resultados.

8.1 Escenario de Pruebas

Las pruebas realizadas al sistema de control de acceso inalámbrico se hicieron sobre el escenario mostrado a continuación en la Figura 8.1.

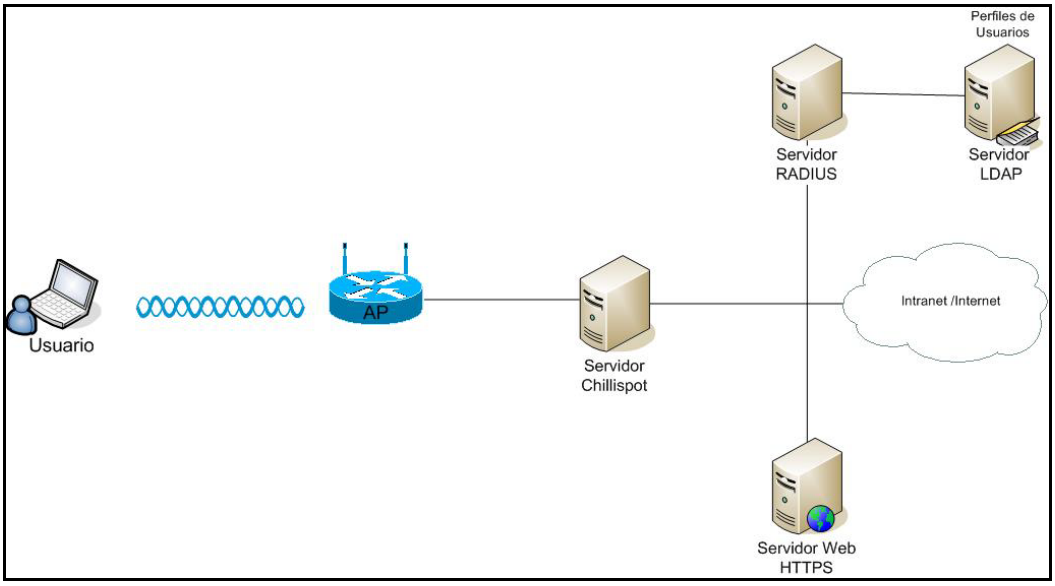

Figura 8.1 Escenario de Pruebas

Bajo este escenario el funcionamiento del sistema de control de acceso inalámbrico es el siguiente:

- El usuario solicita acceso a la red inalámbrica, la cual es difundida por el Punto de Acceso.
- El servidor Chillispot asigna una dirección IP al usuario.
- El usuario al abrir un navegador será redirigido a la página de inicio ubicada en el servidor Web con soporte SSL, en donde se le solicitarán sus datos de usuario.
- Los datos suministrados por el usuario son enviados por el servidor Chillispot al servidor RADIUS, para poder realizar el proceso de autenticación.

- El servidor RADIUS compara los datos suministrados con los que se encuentran almacenados en el servidor LDAP.
- En caso de ser un usuario inválido el servidor RADIUS deniega la solicitud de acceso y el servidor Chillispot le indica al usuario que sus datos son inválidos y por tanto el proceso de autenticación ha sido fallido, manteniendo al usuario en el sitio de inicio hasta tanto no se autentique satisfactoriamente. Por otra parte, en caso de ser un usuario válido, el servidor RADIUS permite la conexión y el usuario deja de ser redirigido al portal cautivo.

8.2 Pruebas Realizadas

Para verificar el desempeño y la buena funcionalidad del sistema, se realizaron las siguientes pruebas:

En primer lugar se verificó que al momento de realizar la conexión con la red inalámbrica, no hubiese problemas con la asignación de la dirección IP al cliente, como se muestra a continuación en la Figura 8.2.

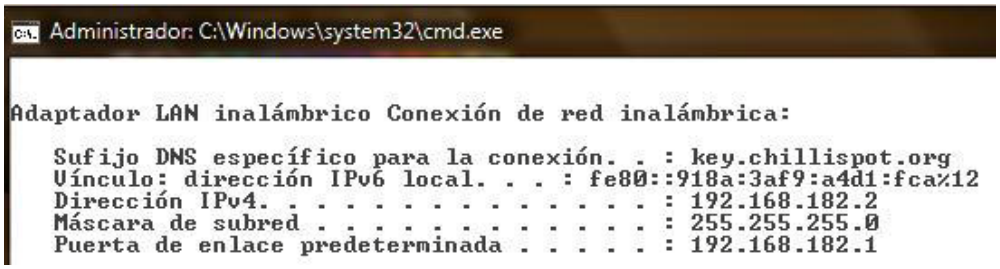

Figura 8.2 Asignación de Dirección IP.

Una vez asignada la dirección IP, se procedió con la verificación del proceso de autenticación como se muestra a continuación en la Figura 8.3. Para esta prueba se verificó también que se obtuviese el mismo resultado sin importar el tipo de navegador que se utilice o el sistema operativo que se tenga en el cliente.

Figura 8.3 Pantalla de bienvenida

En la Figura 8.3 se puede apreciar también que los datos de usuarios enviados en esta página, viajaran cifrados hacia el servidor de autenticación, ya que la conexión se realiza mediante el protocolo https. Igualmente se muestra la dirección IP correspondiente al servidor RADIUS, el cual será el encargado de verificar sí los datos enviados corresponden a un usuario válido o no.

Una vez realizado el proceso de autenticación del usuario, si el servidor RADIUS permite realizar la conexión se mostrará al usuario una pantalla en donde se le indica que la autenticación ha sido exitosa y se muestra un contador del tiempo de duración de la conexión. A continuación en la Figura 8.4 se muestra una imagen de esta pantalla.

Figura 8.4 Pantalla mostrada al realizar la autenticación.

En caso de que los datos enviados durante proceso de autenticación, no correspondan a un usuario válido o simplemente exista alguna inconsistencia entre los datos enviados y los que se encuentren almacenados en el servidor LDAP, originando así una autenticación fallida, se le mostrará al usuario una pantalla indicándole que el proceso de autenticación no ha sido exitoso, esta pantalla puede verse a continuación en la Figura 8.5

Figura 8.5 Pantalla mostrada al fallar la autenticación.

También existe la posibilidad de asignar un tiempo fijo de conexión a los usuarios según su identidad. Para lograr esto se define un atributo dentro del directorio LDAP, el cual permite especificar un tiempo fijo de conexión, es decir, una vez finalizado este lapso de tiempo, el usuario deberá autenticarse nuevamente para continuar navegando. A continuación en la Figura 8.6 se muestra el directorio LDAP perteneciente a un usuario en donde se define el atributo "radiusSessionTimeout" con un valor de prueba de 60 segundos.

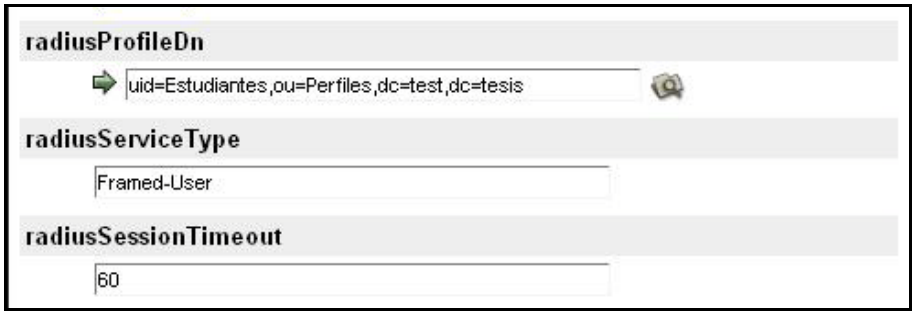

Figura 8.6 Configuración del atributo radiusSessionTimeout en LDAP

Al configurar este atributo, cuando el usuario se autentique satisfactoriamente, la pantalla mostrada cambiará, de manera tal que en lugar de contar el tiempo transcurrido durante la conexión, se mostrará el tiempo restante de la conexión antes de que sea necesario volver a autenticarse. Esta nueva pantalla es mostrada a continuación en la Figura 8.7.

Figura 8.7 Pantalla con el tiempo restante de la conexión

Del mismo modo es posible configurar un atributo en el directorio LDAP, para que la sesión finalice por inactividad, lo que evitaría que un usuario sea suplantado al dejar su sesión abierta. Para esto es necesario configurar el atributo "radiusIdleTimeout" en el directorio LDAP. Una vez configurado este atributo cuando transcurra ese tiempo sin actividad alguna en la computadora del usuario, se cerrará la sesión y el usuario deberá autenticarse nuevamente en el sistema. A continuación en la Figura 8.8 se muestra la configuración de este atributo en el directorio LDAP.

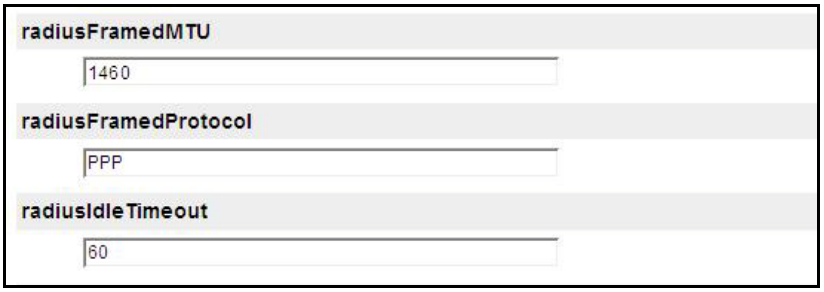

Figura 8.8 Configuración del atributo radiusIdleTimeout en LDAP

Igualmente se realizaron pruebas del lado del servidor de autenticación para verificar que verdaderamente se pudiese llevar un registro de las conexiones realizadas a la red inalámbrica, y comprobar que tan eficaces pueden ser estos registros. A continuación se muestra el contenido del registro de conexiones en el servidor RADIUS.

```
Usuario válido

Packet-Type = Access-Request
Thu Feb 26 14:56:47 2009
        User-Name = "carlos.moreno"
        User-Password = "cmoreno"
        NAS-IP-Address = 0.0.0.0
        Service-Type = Login-User
        Framed-IP-Address = 192.168.182.2
        Calling-Station-Id = "00-21-00-12-51-5B"
        Called-Station-Id = "00-0C-29-72-CA-ED"
        NAS-Identifier = "nas01"
        Acct-Session-Id = "49a6ec4f0000005c"
        NAS-Port-Type = Wireless-802.11
        NAS-Port = 92
        Message-Authenticator = 0x088c5e619e20312e605ea5fe6a84e443
        WISPr-Logoff-URL = "http://192.168.182.1:3990/logoff"
        Client-IP-Address = 172.17.47.43
```

Capítulo 9: Conclusiones y Trabajos Futuros

En el presente trabajo especial de grado se implementó un sistema de control de acceso para la red inalámbrica de la Facultad de Ciencias, para ello se usaron varias tecnologías, las cuales fueron explicadas a lo largo de este documento. De este modo se logro cumplir con el objetivo de implementar un mecanismo de seguridad para realizar la autenticación, autorización y el manejo de usuarios que utilicen la red inalámbrica de la facultad de ciencias, usando para ello los protocolos RADIUS y LDAP.

Cabe destacar que la sistema de control de acceso planteado en este trabajo, no sólo es confiable en cuanto al proceso de autenticación de los usuarios y en lo que se refiere a mantener registros de las actividades realizadas, sino que también se tomó en cuenta la usabilidad de la misma, ya que los usuarios podrán realizar el proceso de autenticación de una manera sencilla e intuitiva, mediante el uso de una página Web de bienvenida la cual es mostrada al abrir un navegador.

9.1 Recomendaciones y Trabajos Futuros.

Una vez finalizado el proceso de instalación y configuración de los servidores implicados en el sistema de control de acceso, así como también la realización de pruebas al mismo, es necesario hacer algunas recomendaciones para futuras implementaciones. Entre estas se encuentra, la creación de un mecanismo automatizado, que permita la creación e instalación de Certificados Digitales por una autoridad certificadora reconocida, de esta manera el sistema de control de acceso puede ser accesible a más usuarios y los sistemas operativos lo reconocerían como un sistema de seguridad confiable.

El sistema puede ser adaptado para realizar una integración completa con otros mecanismos de seguridad y aplicaciones, de tal manera de obtener una solución de seguridad única para toda la red y facilitando así el trabajo de los administradores.

Se sugiere realizar adaptaciones a la solución planteada, para que trabaje con los dispositivos cableados de la red de la Facultad, centralizando aun más la administración de la red y prestando así un mayor nivel de seguridad para la misma.

Capítulo 10: Glosario de Términos.

- **AP:** Es un dispositivo usado para interconectar dispositivos de comunicación inalámbrica para formar una red inalámbrica, normalmente también pueden conectarse a una red cableada, y de esta manera se puede transmitir datos entre los dispositivos de la red cableada y los dispositivos inalámbricos.

- **ASCII:** El código ASCII es el acrónimo de American Standard Code for Information Interchange – Código Estadounidense Estándar para el Intercambio de Información, es un código de caracteres basado en el alfabeto latino tal como se usa en el inglés moderno y en otras lenguas occidentales. Fue creado por el Comité Estadounidense de Estándares ASA en 1963 conocido desde 1969 como el Instituto Estadounidense de Estándares Nacionales ANSI, como una evolución del conjunto de códigos utilizados en telegrafía.

- **DIT:** Término utilizado para identificar el Árbol de Información del Directorio en LDAP.

- **DN:** Nombre distinguido, término usado en el modelo de nombramiento en el protocolo LDAP, el cual es utilizado para asignar un nombre único a cada una de las entradas.

- **DNS:** Es un sistema de nombres que permite traducir de nombre de dominio a dirección IP y viceversa.

- **EAP:** Es el protocolo de autenticación extensible, usado frecuentemente en las redes inalámbricas, y las conexiones Punto a Punto. Está definido en el RFC 3748 - Extensible Authentication Protocol (EAP), y es el mecanismo oficial de autenticación para el estándar WPA.

- **FTP:** Es un protocolo de transferencia de archivos entre sistemas interconectados mediante una red, basado en la arquitectura cliente servidor.

- **HDLC:** Es un protocolo de comunicación de datos punto a punto entre dos nodos basado en el ISO 3309. Forma parte de la base de las redes de comunicaciones X25. Es un protocolo que opera a nivel de enlace de datos y

ofrece una comunicación confiable entre el transmisor y el receptor, pues proporciona recuperación de errores.

- **IEEE:** Corresponde a las siglas en inglés del Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías.

- **IP:** Se refiere a las siglas en inglés del Protocolo de Internet, el cual es un protocolo no orientado a conexión y es usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

  Las cabeceras de este protocolo contienen entre otras cosas las direcciones de las máquinas origen y destino, estas direcciones son usadas por los switches y por los enrutadores para decidir el tramo de red por el que reenviarán los paquetes. Estas direcciones se denominan direcciones IP.

- **ISP:** Es el acrónimo de un proveedor de servicios de Internet, es una empresa dedicada a conectar a Internet a los usuarios o las distintas redes que tengan, también ofrecen servicios relacionados, como alojamiento web o registro de dominios entre otros.

- **LAN:** Es la abreviación de una red de área local – Local Area Network, es la interconexión de varios equipos, su extensión está limitada físicamente a un edificio o a un entorno de hasta 100 metros. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

- **LDAP:** Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

- **MAC:** El control de acceso al medio es el conjunto de mecanismos y protocolos por los que varios dispositivos en una red se ponen de acuerdo para compartir un medio de transmisión común.

- **MD5:** Es el acrónimo de Message Digest Algorithm 5 – Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128

bits ampliamente usado. Fue diseñado por el profesor Ronal Rivest del MIT en 1991 como reemplazo del algoritmo MD4.

- **NAS:** Se refiere al Servidor de Acceso a la Red – Network Access Server, el cual actúa como puerta de enlace a un recurso de la red cuyo acceso se encuentra protegido.

  El cliente se conecta al NAS, entonces el NAS se conecta al recurso de red consultando si el cliente que hace la solicitud del recurso es válido, depende de la respuesta el NAS permite o no el acceso al recurso protegido.

- **OSI:** Se refiere al modelo de referencia de Interconexión de Sistemas Abiertos – Open System Interconnection, lanzado en 1984, fue el modelo de red descriptivo creado por la ISO, el mismo representa un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

- **Phishing:** Es un tipo de ataque, en donde se crea un página Web, muy similar a la de alguna entidad bancaria, con la finalidad de obtener las claves de accesos de los usuarios, para de esta manera poder realizar futuras estafas.

- **RADIUS:** Es el Servicio de autenticación de usuarios remotos a la red - Remote Authentication Dial-In Service, es un protocolo cliente – servidor que permite realizar la autenticación, autorización y manejo de cuentas de usuarios remotos los cuales desean acceder al sistema o a algún servicio de la red.

- **RC4:** Es un sistema de cifrado de flujo diseñado por Ronald Rivest, es utilizado en WEP para añadir seguridad en las redes inalámbricas.

- **RDN:** Nombre relativamente distinguido, es un identificador único para las entradas en un subárbol dentro del directorio, la unión de los RDN desde una hoja hacia la raíz del árbol forman un DN.

- **ROLLBACK:** Es un término muy usado en las tecnologías de Bases de Datos y se refiere a la operación que devuelve a la base de datos a algún estado previo. Estas operaciones son importantes para mantener la integridad de la base de datos, ya que permiten restaurar la misma a una copia limpia incluso después de que se han realizado operaciones erróneas.

- **SASL:** Son las siglas en inglés de Simple Authentication and Security Layer – Capa de Seguridad y Autenticación Simple, es un Framework para autenticación y autorización en protocolos de Internet. Separa los mecanismos de autenticación de los protocolos de la aplicación permitiendo, en teoría, a cualquier protocolo de aplicación que use SASL, usar cualquier mecanismo de autenticación soportado por SASL.

- **Sniffer:** Son los programas usados para realizar la captura de paquetes de datos que viajan en una red, con la finalidad de hacer un análisis posterior de los mismos.

- **Sniffing:** Es el nombre que se le da al proceso de capturar paquetes de datos en una red, mediante el uso de un sniffer.

- **SSID:** Es un código incluido en las tramas de gestión probe response y beacon de una red inalámbrica, para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

- **SSL:** Son las siglas de Secure Socket Layer, es una tecnología estándar de seguridad para establecer un enlace cifrado entre un servidor web y un navegador. Este enlace asegura que toda la información transmitida entre el servidor web y el navegador es privada e integra.

- **TCP:** Es el protocolo de control de transmisión, es un protocolo de comunicación orientado a conexión y fiable, se ubica en el nivel de transporte, según el modelo de referencia OSI.

- **TCP/IP:** Es un modelo de referencia que consta de cinco capas, similar al modelo OSI, es catalogado como la base de Internet, fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

- **TLS:** Son las siglas de Transport Layer Security – Seguridad de la Capa de Transporte, es el sucesor de SSL. Ambos protocolos sirven para proporcionar comunicaciones seguras en Internet, usando un modelo de autenticación y privacidad de la información entre extremos sobre Internet

mediante criptografía. Esto es fundamental para mantener la seguridad en el comercio por Internet.

- **UDP:** Es un protocolo ubicado en la capa de transporte según el modelo OSI, basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama contiene suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción.

  Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

- **VPN:** Corresponde a las siglas en inglés de Virtual Private Network – Red Privada Virtual, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

- **WEP:** Son las siglas de Wired Equivalent Privacy – Privacidad Equivalente a la Cableada, es el sistema de cifrado incluido en el estándar IEEE 802.11, el cual permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2. Está basado en el algoritmo de cifrado RC4, y utiliza claves de 64 o 128 bits.

- **Wi-Fi:** Es una organización sin fines de lucro creada en 1999 por varias empresas líderes en el mercado, con el objetivo de conducir la adopción de un único estándar aceptado por todo el mundo para las redes inalámbricas de alta velocidad.

- **WLAN:** Son las siglas de Wireless Local Area Network – Red de Area Local Inalámbrica, es un sistema de comunicación de datos inalámbrico, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas.

- **WPA:** Es un sistema de seguridad para las redes inalámbricas, creado para solventar las deficiencias que presentaba WEP. Fue creado en conjunto por Wi-Fi y la IEEE.

- **X.500:** Es un conjunto de estándares de redes de computadoras, creado por la ITU-T sobre servicios de directorios, entendidos estos como bases de datos de direcciones electrónicas. El estándar se desarrolló conjuntamente con la ISO como parte del Modelo de interconexión de sistemas abiertos, para usarlo como soporte del correo electrónico X.400.

Capítulo 11: Fuentes Consultadas.

1 Timothy Howes, Mark Smith, "Understanding and Deploying LDAP Directory Services" 2da Edición Editorial Addison Wesley, 2003.

2 Matt Butcher, "Mastering Open LDAP" Editorial PACKT Publishing.

3 Gerlad Carter "LDAP System Administration" Editorial O'REILLY.

4 OpenLDAP Foundation "OpenLDAP" Disponible en: http://www.openldap.org/doc/admin24/intro.html , consulta realizada marzo 2008.

5 Michael Donnelly "Una introducción a LDAP" Disponible en: http://ldapman.org/articles/sp_intro.html , consulta realizada: marzo 2008.

6 Heinz Johner, Larry Brown. "Understanding LDAP IBM Redbook" Editorial IBM Corporation 1998.

7 William Stallings, "Wireless Communications and networks" Editorial Prentice Hall, 2002.

8 Andrew S. Tanenbaum, "Redes de Computadoras" Editorial Prentice Hall 4ta Edición 2003.

9 Jonathan Hassell, "RADIUS" Editorial O´REILLY

10 Madjid Nakhjiri, Mahsa Nakhjiri, "AAA and Network Security for Mobile Access: Radius, Diameter, EAP, PKI and IP Mobility" Editorial Wiley 2005.

11 Vicenzo Mendillo, "Seguridad en Informática y Comunicaciones" CD-ROM#1, Abril 2007.

12 Chillispot Disponible en: http://www.chillispot.info/, consulta realizada en Enero de 2009.

Capítulo 12: Anexos.

En este capítulo se incluye un manual de instalación, en el cual se explica de manera detallada todos los pasos que se deben seguir para la instalación y configuración del sistema de control de acceso.

12.1 Manual de Instalación.

Para la realización del sistema de autenticación planteado en el presente trabajo, fue necesaria la instalación y configuración de un conjunto de aplicaciones con las cuales este queda conformado en su totalidad. Dichas aplicaciones son:

- **Servidor LDAP:** Servidor encargado del manejo de la información de los usuarios que tendrán acceso a la red.
- **PhpLDAPAdmin:** Aplicación que permite realizar la administración del servidor LDAP a través de una interfaz web.
- **Servidor RADIUS:** Servidor encargado de realizar el proceso de autenticación, autorización y manejo de cuentas de los usuarios.
- **Chillispot:** Aplicación encargada de asignar la dirección IP a los usuarios de la red, y redirigirlos a una página web para iniciar el proceso de autenticación.

A continuación se explicará con mayor detalle el proceso de instalación y configuración de cada una de las aplicaciones antes mencionadas. Cabe destacar que todas estas aplicaciones fueron instaladas en el mismo equipo, ya que de esta manera se centraliza el proceso de administración del sistema, y se reducen los posibles puntos críticos en el mismo. Dicho equipo funcionaba con el sistema operativo Linux Debian.

Servidor LDAP.

El servidor LDAP es el encargado de almacenar toda la información de los usuarios que tendrán acceso a la red inalámbrica. Para realizar la instalación de este servidor, fue necesaria la instalación de los siguientes paquetes:

- Slapd v.2.3.30: Paquete de instalación de la implementación del servidor OpenLDAP
- ldap-utils v.2.3.30 : Paquete de utilidades del servidor OpenLDAP

- db4.2-util v.4.2.52: Utilidades para el uso de la base de datos Berkeley en OpenLDAP

Una vez instalados los paquetes anteriores se procedió a la configuración del servidor. En primer lugar se editó el archivo slapd.conf, el cual contiene la configuración del servidor. Los cambios realizados a este archivo fueron los siguientes:

1. Se añadieron los schemas "samba.schema" y "openldap.schema", los cuales son necesarios para la configuración de los atributos de los usuarios, que se utilizaran durante el proceso de autenticación en conjunto con el servidor RADIUS.
2. Se especificó el nivel de profundidad del archivo log del servidor LDAP, para que guardara todas las operaciones realizadas y los resultados de las mismas.
3. Se indica el tipo de base de datos a utilizar, la cual es la base de datos Berkeley.
4. Se indica la ruta en el árbol de directorio del comienzo del árbol, a partir de este punto se realizarán las consultas en el mismo.
5. Se especifica la ruta del usuario administrador en el árbol de directorio.

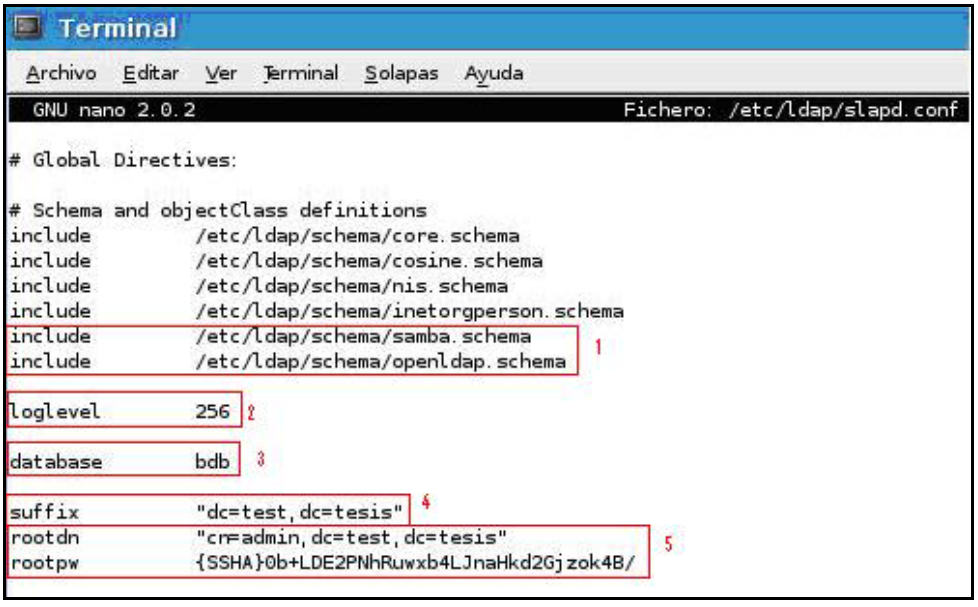

Figura 12.1 Archivo de configuración slapd.conf.

Como se puede apreciar en este archivo fueron incluidos dos nuevos esquemas a los schemas incluidos en la configuración inicial, los cuales son los schemas samba.schema y openldap.schema:

- **samba.schema:** Provee el atributo SambaNTPassword necesario para poder realizar la autenticación vía MSCHAPv2.
- **openldap.schema:** Provee los atributos necesarios para el funcionamiento con el servidor RADIUS, este esquema se obtiene a través del paquete de freeradius-1.1.3-3.

Luego se encuentra el nivel de profundidad que se utilizará en el archivo log, el cual se le asigna el valor 256 con la finalidad de registrar todas las operaciones de conexión, operaciones de consulta y resultados de las mismas. Seguidamente se especifican la base de datos que se utilizará, el inicio del árbol de directorio y el nombre y contraseña del usuario con permisos de root dentro del directorio. La contraseña de este usuario fue creada mediante el siguiente comando:

slappasswd –h {SSHA}

Una vez realizada la configuración de este archivo, se editó el archivo /etc/ldap/ldap.conf, para indicar donde se encuentra la raíz del árbol de directorio, modificando la línea

BASE dc=test,dc=tesis

Una vez culminada la configuración del servidor, se procedió a la carga de la información con la estructura del árbol de directorio, así como también la información de los usuarios al directorio. Todos estos datos se encuentran contenidos en los archivos tree.ldif y users.ldif, respectivamente. A continuación se muestra la Figura12.2, en donde se aprecia la estructura del DIT.

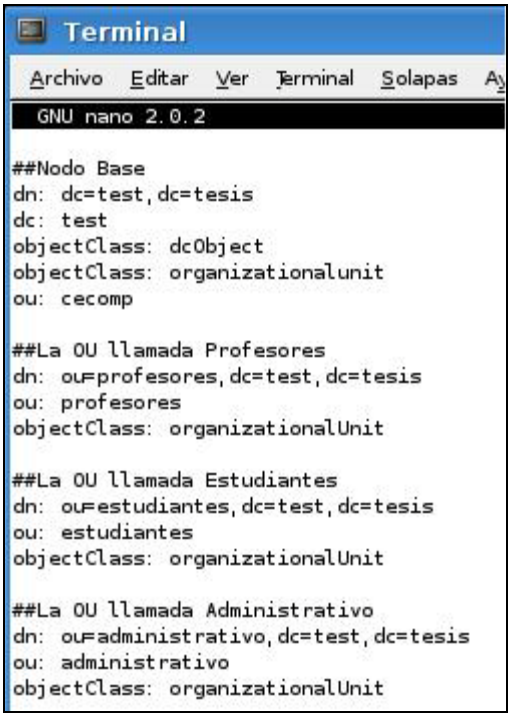

Figura 12.2 Muestra del archivo tree.ldif.

A continuación se muestra la Figura 12.3, donde se aprecia un extracto del archivo users.ldif en donde se contiene la información referente a los usuarios del directorio.

Figura 12.3 Muestra del archivo users.ldif.

Para realizar la carga de la información del directorio fue necesario detener el servidor y posteriormente levantar de nuevo el servicio, ya que se utilizó el siguiente comando:

slapadd -v -l <nombre del archivo>.ldif

Luego de cargar la información dentro del árbol de directorio y tener en funcionamiento el servidor LDAP, se instaló la aplicación PhpLDAPAdmin la cual permitirá llevar la administración del servidor mediante una interfaz Web de manera más simple y amena. Una vez finalizada la instalación, es posible realizar la conexión con el servidor mediante la siguiente URL: http://localhost/phpldapadmin/

Para contener los datos de un perfil de usuario se creó la unidad organizativa Perfiles (ou=Perfiles), cada uno de los objetos dentro de esta unidad representa una política de conectividad específica para un grupo de usuarios. Los objetos que representan un perfil de usuario pertenecen a las siguientes clases:

- **RadiusObjectProfile:** Es una clase de objeto contenedor que se utiliza para crear objetos radiusprofile.
- **Radiusprofile:** Es una clase de objeto que posee los atributos necesarios para definir un perfil estándar de RADIUS.

Para almacenar los datos referentes a los permisos de cada perfil se hace uso del atributo Description, ya que este atributo soporta valores múltiples y soporta una longitud máxima de 1024 caracteres. Los valores de los permisos se almacenan en forma de reglas, definiendo una regla para cada valor de atributo. Dichas reglas deben usar el formato de la sintaxis del comando iptables de netfilter.

La vinculación de un usuario con un perfil de usuario se realiza mediante el atributo RadiusProfileDn en el objeto del usuario, el mismo debe contener el dn del perfil del usuario. El atributo dialupAccess es un atributo especial específicamente definido en la clase radiusprofile para usarse con soporte LDAP, la existencia de este atributo en un usuario con valor yes, significa que dicho usuario tiene autorización para conectarse. En caso de que el atributo no exista o posea el valor FALSE, indica que el usuario tiene denegado el acceso y el servidor RADIUS no continúa con el proceso de autenticación.

Servidor RADIUS.

Para la instalación de este servidor se utilizó la aplicación freeradius 1.1.3-3, la cual es una implementación del servidor RADIUS en software libre, que posee un

amplio soporte con LDAP, para realizar el almacenamiento de la información.

El paquete freeradius disponible en los repositorios de la distribución Debian, por defecto viene sin soporte para el protocolo EAP. Por tal motivo fue necesario descargar los archivos fuentes para dicho paquete para su posterior compilación. Para poder realizar dicha compilación fue necesario instalar los siguientes paquetes:

```
#apt-get   install   build-essential
….
#apt-get   install   apt-src
#apt-src   update
```

Una vez instalados los paquetes, se creó el directorio en donde instaló el paquete con las fuentes de freeradius, como se observa en el siguiente fragmento de código:

```
#mkdir   /build_freeradius
#cd   /build_freeradius
#apt-src   install   freeradius
```

Luego se editó el archivo /build_freeradius/freeradius-1.1.3/debian/rules como se muestra a continuación en la Figura 12.4:

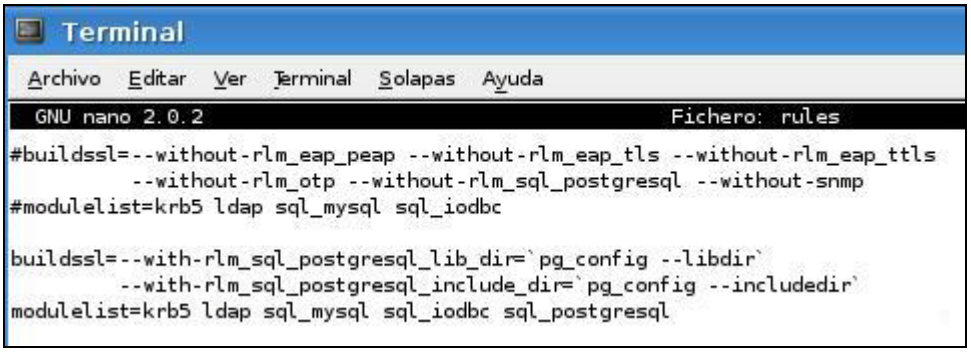

Figura 12.4 Fragmento del archivo rules

De igual manera fue necesario editar el archivo control, ubicado en el mismo

directorio, tal como se muestra a continuación en la Figura 12.5:

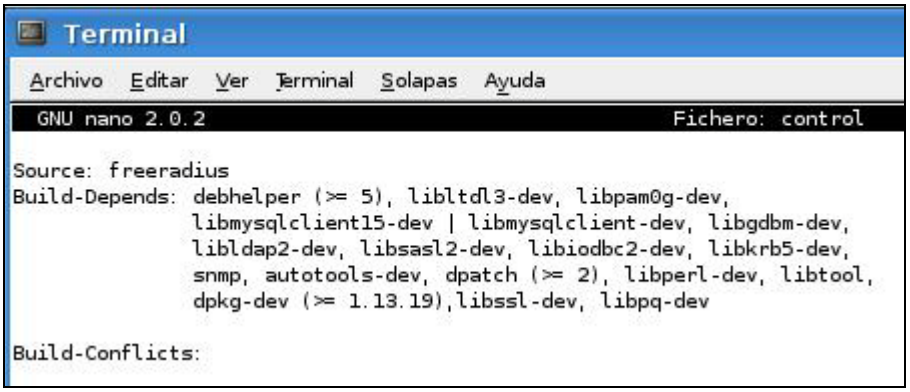

Figura 12.5 Fragmento del archivo control

Al terminar de editar los archivos anteriores se ejecutaron los siguientes comandos:

```
#cd   /build_freeradius/freeradius-1.1.3/debian
#cat   control.postgresql >> control
#apt-get   install   libssl-dev   libpq-dev
```

Una vez culminada la instalación de los paquetes anteriores se procedió a construir los paquetes deb, para su posterior instalación tal como se muestra a continuación:

```
#cd   /build_freeradius
#apt-src   build   freeradius
….
#dpkg   -i   freeradius_1.1.3-3_i386.deb    freeradius_ldap_1.1.3-3_i386.deb
```

En cuanto a la compatibilidad con LDAP, freeradius provee un esquema para LDAPv3 denominado openldap.schema y un módulo denominado rlm_ldap, que es el encargado de realizar las tareas de autorización y autenticación contra el directorio LDAP.

En freeradius existe el archivo /etc/freeradius/ldap.attrmap, el cual es un “mapa” de las correspondencias entre los atributos del diccionario RADIUS y los atributos del directorio LDAP, permitiendo así redefinir el significado de algunos atributos del directorio LDAP. Para la implementación de este sistema de autenticación fue

necesario añadir la línea donde se define la correspondencia con el atributo User-Password como puede observarse en la Figura 12.6.

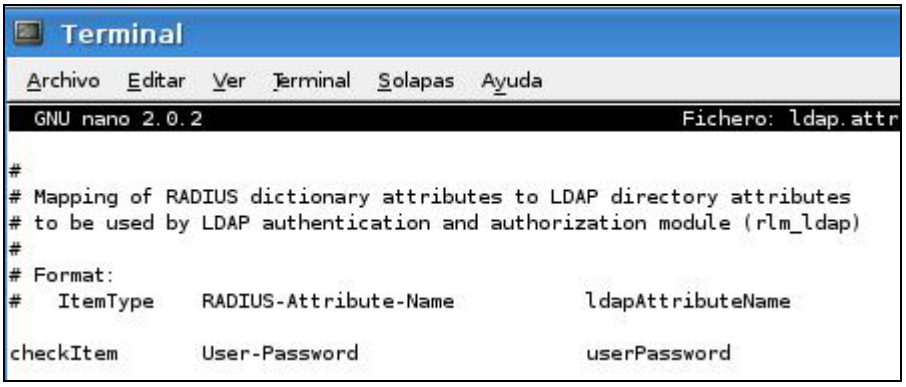

Figura 12.6 Muestra del archivo ldap.attrmap.

La configuración del servidor se ubica en el directorio /etc/freeradius, y esta se encuentra conformada por varios archivos. Las directivas principales de configuración se encuentran en el archivo /etc/freeradius/radiusd.conf. Para permitir que el servidor RADIUS realice consultas en el directorio LDAP previamente configurado, se editó el módulo LDAP dentro de este archivo, en la Figura 12.7 se puede observar la configuración de este módulo.

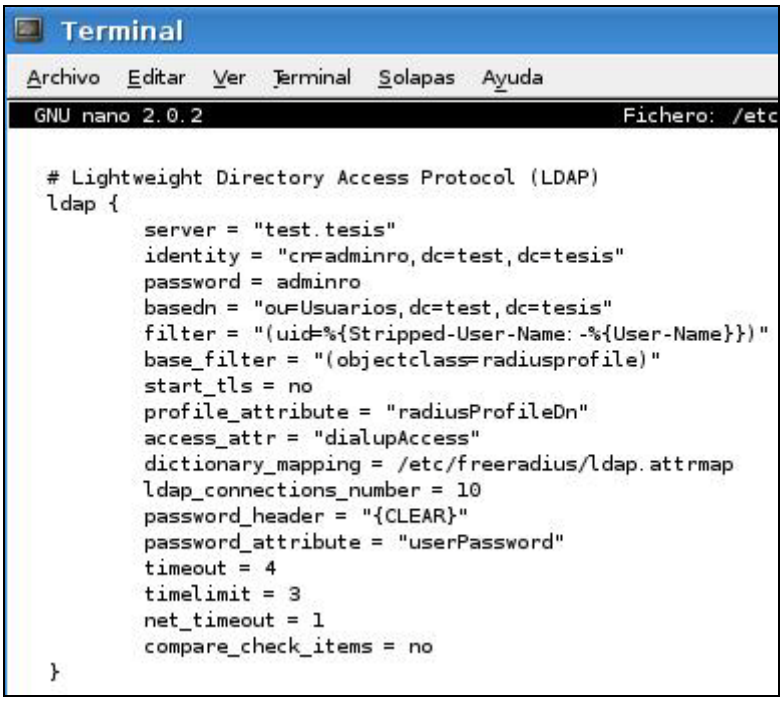

Figura 12.7 Configuración del módulo LDAP.

A continuación se muestra la Tabla 1, donde se explican las directivas de configuración que se especifican en este módulo:

Nombre	Significado
Server, identity y password	Estos son los datos de conexión necesarios para acceder al directorio LDAP.
Basedn	Ámbito a partir del cual se realizarán las búsquedas en el directorio LDAP.
Filter	Filtro de búsqueda LDAP, para localizar un objeto de usuario utilizando el nombre suministrado por el cliente durante la autenticación RADIUS.
Base_filter	Filtro de búsqueda LDAP usado como ámbito de búsqueda básico.
Start_tls	Cuando el valor de esta opción es yes, se inicia una conexión cifrada con TLS al directorio LDAP. Requiere de la configuración adicional de parámetros de claves y certificados.
Profile_attribute	El valor de profile_attribute define el nombre del atributo en el objeto de usuario que contiene el DN de un objeto radiusprofile que contiene el perfil al que pertenece dicho usuario.
Access_attr	El valor de access_attr es usado para permitir el acceso: • Si no existe o el valor es FALSE, no permite el acceso remoto • Si el valor es yes (o cualquier otro distinto de FALSE), permite el acceso remoto
Dictionary_mapping	Referencia al archivo que contiene las correspondencias entre los atributos LDAP y los atributos RADIUS. Por defecto el valor es ${raddbdir}/ldap.attrmap.
Password_header y password_attribute	Estos valores definen el atributo LDAP que contiene la contraseña del usuario por defecto y cual es el cifrado del mismo, esto se utiliza para validar por CHAP.
Timeout, timelimit, net_timeout y ldap_conections_number	Estos valores determinan los tiempos de espera para el servidor LDAP, los tiempos límite que se puede demorar en procesar un pedido y el número de conexiones abiertas contra el directorio LDAP. Estos parámetros han de establecerse en función de la carga de procesos que tiene una implementación en particular.

Tabla 1 Parámetros de configuración del módulo LDAP.

El módulo MSCHAP soporta la autenticación MS-CHAP y MS-CHAPv2, y es utilizado por el método de acceso EAP-PEAP. En la Figura 12.8 se muestra la configuración requerida para este módulo.

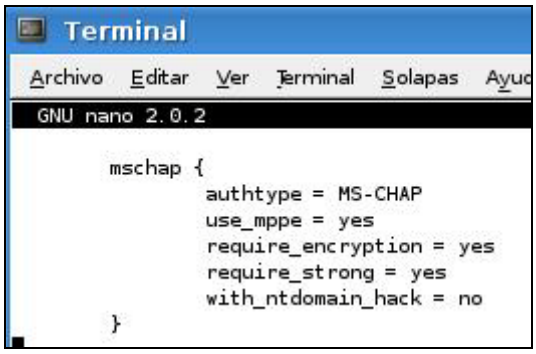

Figura 12.8 Configuración del módulo MSCHAP.

En la Tabla 2 se muestran las directivas de configuración de este módulo:

Nombre	Significado
Use_mppe	Permite la utilización de MPPE, en la autenticación.
Require_encryption	Si use_mppe tiene por valor yes, realiza un cifrado moderado.
Require_strong	Si use_mppe tiene por valor yes, siempre requiere claves de 128 bits.
With_ntdomain_hack	Si este parametro tiene valor yes, en caso de que un cliente MS Windows se conecte enviando el usuario en la forma Dominio/nombre_de_usuario y el desafío tomando la porción del nombre del usuario solamente, corrige el comportamiento incorrecto.

Tabla 2 Parámetros de configuración del módulo MSCHAP.

La sección de configuración EAP se encuentra en el archivo eap.conf, aquí se colocarán todas las directivas de configuración para las variantes soportadas de dicho protocolo. En este caso, que se ha elegido usar EAP-PEAP, será necesario configurar también la sección de EAP-TLS, ya que este protocolo realiza el intercambio de paquetes dentro de un túnel TLS y requiere certificado sólo por parte del servidor. El protocolo EAP-PEAP se usa junto con MSCHAPv2, en el método de acceso WPA para autenticar usuarios.

La sección de directivas de configuración del módulo EAP se divide en una sección de configuración común y diferentes subsecciones para cada una de las configuraciones específicas del protocolo EAP. Para realizar la configuración de EAP-TLS, es necesario crear previamente una Autoridad Certificadora (CA) y generar las claves y certificados para el servidor.

El proceso para la creación de la CA y generar las claves y certificados del servidor, se describe a continuación:

En primer lugar es necesario instalar la aplicación OpenSSL, la cual brinda las herramientas necesarias para realizar estas tareas. Luego de instalar la aplicación, en el directorio /etc/ssl, se ejecutan los siguientes comandos:

```
#opensll req –x509 –newkey rsa -keyout cakey.pem -days 3650 -out cacert.pem
….
```

Con el comando anterior se crea la CA para crear certificados X509 con algoritmos de cifrado rsa de 2048 bits. Después de ingresar una contraseña para la CA se generan una clave privada, la cual se guarda en el archivo cakey.pem y una clave pública que se guarda en el archivo cacert.pem, ambos con una duración de 10 años (3650 días).

Una vez creada la CA, se procede a la creación de un certificado. Para esto primero se genera la clave privada del mismo, con el siguiente comando:

```
#openssl genrsa -des3 -out Server_key.pem -passout pass: Asdf1234 2048
```

Con el comando anterior se genera la clave privada, con el algoritmo de cifrado triple des (des3) de 2048 bits y se guarda en el archivo de salida Server_key.pem, y con el comando –passout pass: se indica la contraseña para la clave privada, donde "Asdf1234" es la contraseña utilizada en el paso anterior. A continuación se genera la petición del certificado con el comando:

```
#openssl req -new -subj "/DC=test.tesis" -key Server_key.pem -passin pass:
Asdf1234 -out petic-certificado-serv.pem
```

En el comando anterior se indica en el parámetro –subj, a quien pertenece el certificado, en este caso se colocó el nombre del servidor. Del mismo modo con el parámetro –key, se indica que se usará la clave privada generada en el paso anterior. Finalmente se genera un archivo de salida, el cual contiene la petición del certificado. En este punto ya se puede emitir el certificado, para definir las características del certificado, se creó el archivo flags.conf que contiene lo siguiente:

```
basicConstraints = critical,CA: FALSE
extendedKeyUsage = serverAuth
```

La primera línea del archivo flags.conf, se coloca para cumplir con el estándar X509v3 y con la RFC3280. La segunda línea es para indicar que el certificado será utilizado para un servidor. A continuación se procede a la creación del certificado con el siguiente comando:

```
#openssl x509 –CA cacert.pem -CAkey cakey.pem -req -in petic-certificado-serv.pem -days 3650 -extfile flags.conf -sha1 -CAcreateserial -out Server_cert.pem
```

En este último paso se indica que se genere un certificado x509 cuya CA está definida en el archivo "cacert.pem", y usa la clave privada "cakey.pem". Las especificaciones del certificado se encuentran definidas en el archivo "petic-certificado-serv.pem", la validez del certificado tiene una duración de 10 años. Igualmente se indica que el certificado es para un servidor, por lo que se coloca el parámetro –extfile con el nombre del archivo "flags.conf" y se utiliza el algoritmo de cifrado sha1.

Luego se solicita que el certificado sea enumerado con el atributo –Cacreateserial, y finalmente se indica el nombre del archivo de salida el cual guarda el certificado.

A continuación se muestra la Figura 12.9, donde se observa la sección de EAP-TLS del archivo eap.conf con la configuración realizada:

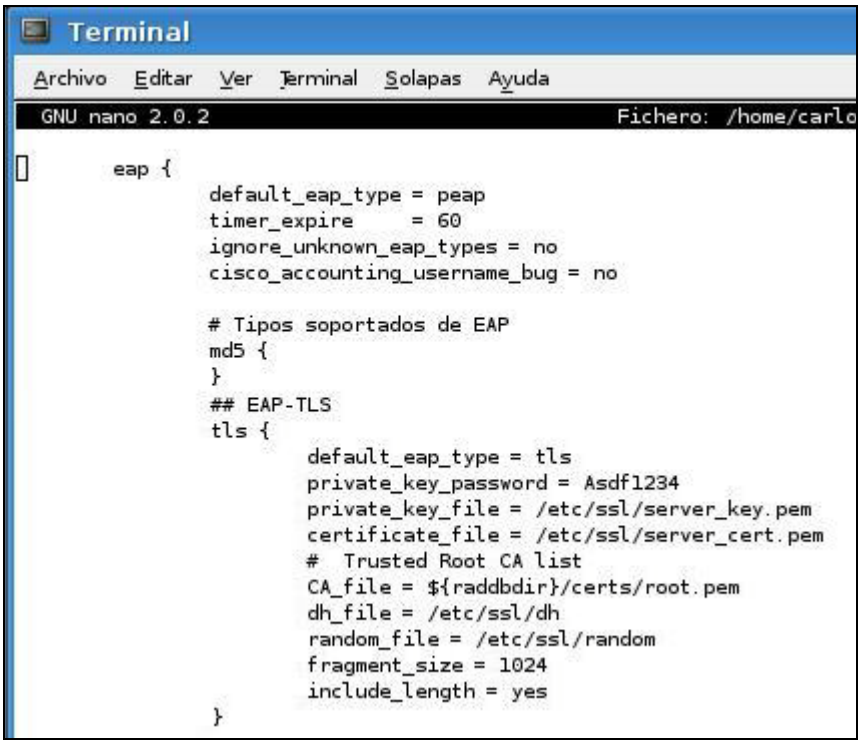

Figura 12.9 Directivas de configuración para EAP-TLS

A continuación se muestra la Tabla 3 en donde se explican las directivas mostradas en la Figura 12.9:

Nombre	Significado
Subsección General EAP	
default_eap_type	Este valor se usa para determinar el tipo EAP que se utilizará para realizar la autenticación.
timer_expire	El servidor mantiene una lista que relaciona los paquetes EAP-Request/Response. Este valor determina el tiempo que se debe esperar para borrar una entrada de la lista.
Ignore_unknown_eap_types	Dado que el servidor tiene soporte para una cantidad limitada de variantes del protocolo EAP, si recibe un tipo que no soporta, deniega el acceso. Si esta directiva tiene por valor yes y se ha definido otro módulo con un Proxy que soporte el tipo, se reenvía la petición al Proxy.
Cisco_accounting_username_bug	Soluciona el bug de Cisco AP1230B fw.12.2(13)JA1, que agrega un byte más al atributo user-name en la aceptación a la petición de acceso.
Subsección EAP-TLS	
default_eap_type	Este valor fija el tipo EAP a EAP-TLS.
private_key_password	Este valor es la contraseña de la clave privada del servidor.
private_key_file	Este valor es la ubicación del archivo con la clave privada del servidor.
certificate_file	Este valor es la ubicación del archivo del certificado del servidor.
CA_file	Este valor es la ubicación del archivo del certificado de la Autoridad Certificadora, que firma los certificados emitidos.
dh_file	Este valor es la ubicación del archivo de clave Diffie-Hellman, denominado dh.
random_file	Este valor es la ubicación de un archivo con valores aleatorios denominado random.
fragment_size	Este valor no debe exceder los 4096 bytes de un paquete RADIUS, en la mayoría de los AP la longitud máxima de un paquete es de 1500 – 1600 bytes, por lo que el tamaño de un fragmento debería ser de 1024 bytes o menor.
incluye_length	Si esta directiva tiene por valor yes, se incluye en cada paquete el tamaño total del mensaje (valor por defecto). Si el valor es no, sólo se incluye el tamaño total del mensaje en el primer paquete.

Tabla 3 Parámetros de configuración del archivo eap.conf.

De igual manera se configuraron las directivas para los tipos EAP-PEAP y EAP-TTLS, como se muestra en la Figura 12.10.

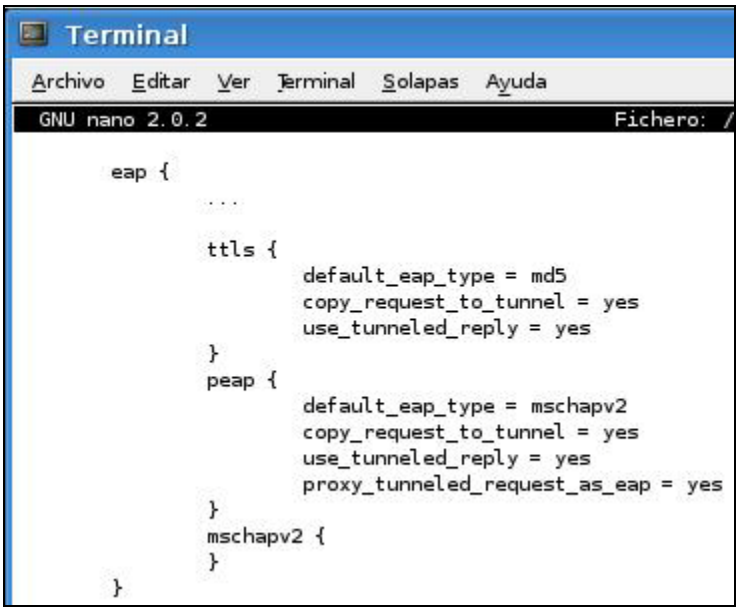

Figura 12.10 Directivas de configuración para EAP-PEAP y EAP-TTLS.

El registro de accounting se realiza mediante el uso del módulo radutmp, donde se registra los inicios de sesión y las terminaciones de sesión. Los archivos con los registros se encuentran almacenados en el directorio /var/log/freeradius/radacct, dentro de este directorio se crea un directorio cuyo nombre es la dirección IP con la que el servidor RADIUS acepta solicitudes, en este directorio se crea un archivo diariamente, en donde queda registrado todas las conexiones que se hayan realizado en ese día. En estos registros se guardan la fecha y hora, el nombre del usuario, y la dirección IP desde donde se realizó la conexión.

La sección authorize del archivo radiusd.conf, también es necesario configurarla colocando los nombres de los módulos definidos en las secciones anteriores. Es importante el orden en que se colocan los módulos. El módulo eap debe ser el primer módulo de autorización, luego de los módulos preprocess y auth_log que son los encargados de realizar los procesos para evitar ambigüedades en los nombres de usuario y el registro de pedidos de autorización. En la Figura 12.11 se puede apreciar la configuración realizada para esta sección.

Figura 12.11 Sección authorize del archivo radiusd.conf

La sección autentícate se debe configurar listando los módulos disponibles para realizar el proceso de autenticación. Dicho proceso no intenta autenticar probando con cada uno de los módulos aquí listados, sino que el módulo usado en la sección authorize agrega un atributo de configuración denominado Auth –Type. Ese tipo de autenticación se utiliza para elegir el módulo apropiado de la lista definida. En la Figura 12.12 se muestra la configuración realizada a este módulo.

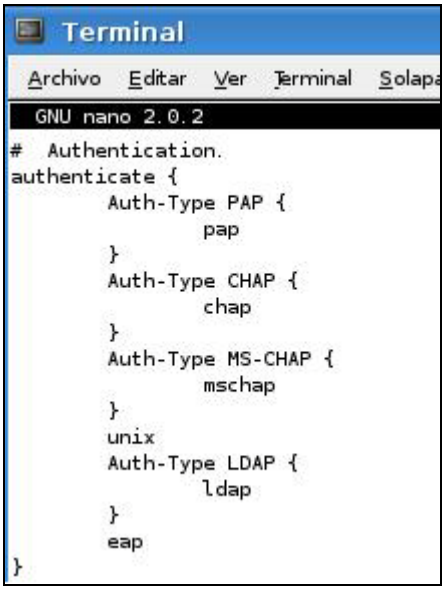

Figura 12.12 Sección autentícate del archivo radiusd.conf.

Una vez configurada esta última sección se termina la configuración principal del servidor RADIUS, sólo queda por modificar el archivo clients.conf donde se definen los NAS que pueden comunicarse con el servidor. En este archivo se debe colocar desde donde se permite el acceso al servidor RADIUS y con que contraseña. A continuación se muestra la Figura 12.13 con la configuración realizada en el mismo.

Figura 12.13 Configuración del archivo clients.conf.

Servidor Chillispot (Portal Captivo).

La implementación del portal cautivo que se eligió se llama chillispot, esta posee una implementación sencilla y depende de muy pocos servicios externos para funcionar. Algunas características de chillispot son las siguientes:

- Soporta dos métodos de autenticación UAM (Universal Access Method – Método de Acceso Universal) y WPA/RSN (Wireless Protectes Access – Acceso Inalámbrico Protegido).
- Permite realizar los procesos de Autenticación, Autorización y Registro contra un servidor RADIUS.
- Posee un servidor DHCP propio para ambos métodos de autenticación.
- La autenticación con UAM soporta SSL.
- No exige la utilización de algún AP en particular.
- Funciona utilizando NAT o Routing.

Para este sistema se eligió la autenticación UAM, en donde se entrega una dirección IP a través del protocolo DHCP, pero cuando el cliente intenta conectarse, este es redirigido hacia una página de bienvenida en donde debe realizar el proceso de autenticación. Una vez que el usuario sea autenticado correctamente se deja de redireccionar el tráfico.

Para el correcto funcionamiento del servidor chillispot se debe cumplir con los siguientes requerimientos:

- Un punto de acceso inalámbrico, el cual es indispensable pero no es sujeto a un modelo específico.
- El equipo donde funcionará el servidor Chillispot, debe tener dos interfaces de red.
- Se debe disponer de un Servidor RADIUS.
- Es necesario un servidor Web con soporte SSL.

Antes de realizar la instalación del servidor chillispot es necesario realizar los siguientes pasos:

En primer lugar se debe habilitar el soporte para interfaces virtuales, y así poder levantar la interfaz tun0, la cual es utilizada por el servidor chillispot. Para esto se ejecutan en una consola los siguientes comandos:

```
#mkdir   /dev/net
#mknod   /dev/net/tun   10   200
```

Con estas dos instrucciones se crea el dispositivo virtual tun0. Luego de esto es necesario editar el archivo /etc/modules.conf para añadirle al final del mismo, la siguiente línea:

```
alias   char-major-10-200   tun
```

Luego de esto es necesario editar el archivo /etc/modules y agregar la palabra "tun" al final del mismo, con la finalidad de que dicho modulo se cargue al inicio del sistema. Luego de editados ambos archivos se debe ejecutar el siguiente comando: "depmod –a".

Debido a que el servidor estará funcionando como un firewall, este debe tener la capacidad de hacer NAT. Para esto se edita el archivo /proc/sys/net/ipv4/ip_forward, y se modifica el valor de 0 a 1. Igualmente debe editarse el archivo /etc/sysctl.conf, para verificar que se encuentre la línea:

"net.ipv4.conf.default.ip_forward=1".

Finalmente una vez configurado el equipo se procede a instalar el servidor chillispot. Para esto se descargó el archivo "chillispot_1.0_i386.deb", de la página web: http://www.chillispot.info y se procedió con la instalación mediante el siguiente comando:

"dpkg –i ./chillispot_1.0_i386.deb".

Una vez instalado se edito el archivo /etc/chilli.conf, el cual guarda la configuración principal del servidor. La configuración realizada en el mismo se muestra en la Figura 12.14.

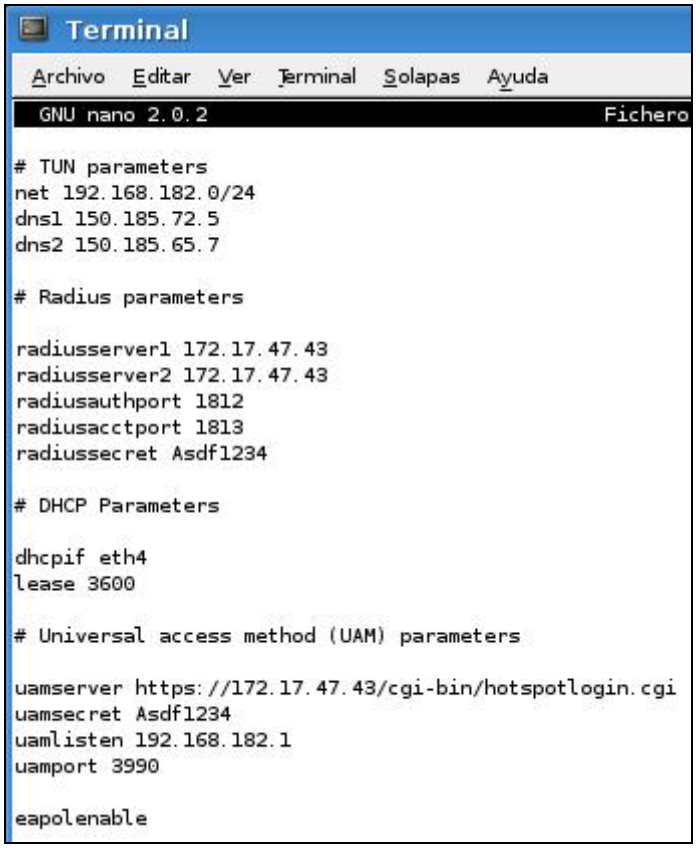

Figura 12.14 Archivo de configuración chilli.conf

Las directivas de configuración mostradas en la Figura 12.14, se describen a continuación en la Tabla 4.

Nombre	Significado
net	Es la dirección de red asignada a la interfaz de la red interna, esta red es a la que chillispot brinda servicio.
dns1 y dns2	Es usado para informar a los clientes sobre las direcciones de los servidores DNS, para hacer la resolución de nombres.
radiusserver1 y radiusserver2	Es la dirección IP del servidor RADIUS
radiusauthport	Es el número del puerto UDP en donde el servidor RADIUS acepta las solicitudes de autenticación.
radiusacctport	Es el número del puerto UDP en donde el servidor RADIUS acepta las solicitudes de accounting.
radiussecret	Es el secreto compartido entre el servidor RADIUS y sus clientes.
dhcpif	Es el nombre de la interfaz usada por chillispot para la asignación de direcciones DHCP. Esta interfaz debe configurarse sin dirección IP.
lease	Tiempo en segundos para liberar una dirección IP.
uamserver	Es el URL del servidor web que se encargará de realizar el proceso de autenticación de usuarios.
uamsecret	Es el secreto compartido entre el servidor web y el servidor chillispot.
uamlisten	Es la dirección IP en donde el servidor chillispot escuchará para realizar la autenticación de los clientes.
uamport	Es el puerto asignado para escuchar durante el proceso de autenticación de los clientes.
eapolenable	Le indica al servidor chillispot que se aceptan solicitudes EAP.

Tabla 4 Directivas de configuración del archivo chilli.conf.

Una vez configurado este archivo, es necesario copiar en el servidor web el script encargado de realizar el proceso de autenticación. Para hacer esto se ejecutan en consola los siguientes comandos:

```
#gunzip   /usr/share/doc/chillispot/hotspotlogin.cgi.gz
#cp /usr/share/doc/chillispot/hotspotlogin.cgi   /usr/lib/cgi-bin/
```

Para realizar la instalación del servidor web con soporte SSL, se ejecutó el siguiente comando:

```
#apt-get install apache2 apache2.2-common apache2-utils
```

Para generar el certificado SSL con el que trabajará el servidor web Apache, se ejecutaron los siguientes comandos:

```
#make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/apache2/ssl/apache.pem
```

Luego de llenar los datos solicitados en el paso anterior, se debe habilitar el módulo con el comando: "a2enmod ssl".

Una vez habilitado el módulo, se debe crear el sitio SSL. Por defecto apache trae un archivo default, ubicado en el directorio /etc/apache2/sites-available/. Se debe realizar una copia de este archivo para poder modificarlo, esto se realiza con los siguientes comandos:

```
#cp /etc/apache2/sites-available/default /etc/apache2/sites-available/ssl
```

La configuración de este archivo nuevo archivo se muestra a continuación en la Figura 12.15.

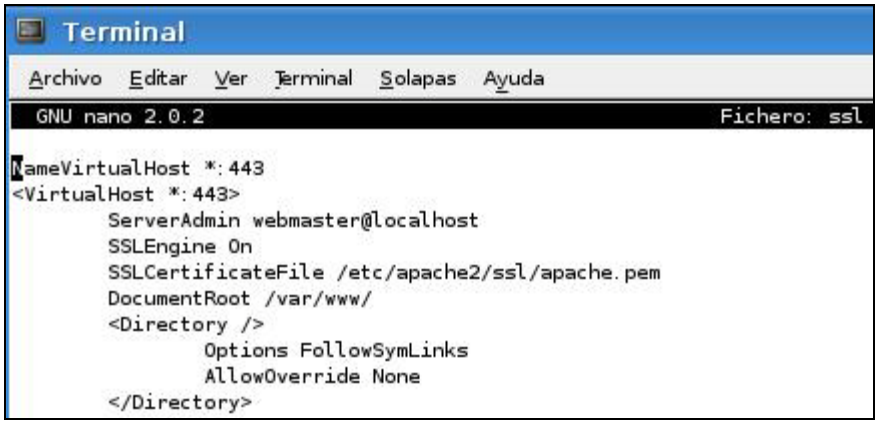

Figura 12.15 Configuración del sitio ssl

Para finalizar la configuración del servidor web apache, se debe habilitar el sitio ssl con el siguiente comando: "a2ensite ssl".

Una vez finalizada la configuración del servidor web, sólo resta por editar dos archivos, el primero de ellos es el que contiene la configuración de las reglas de iptables que usa el servidor chillispot. Para realizar esto se ejecutan los siguientes

comandos:

```
#cp   /usr/share/doc/chillispot/firewall.iptables   /etc/init.d/chillispot.iptables
#chmod   755   /etc/init.d/chillispot.iptables
```

Luego se debe verificar que los parámetros INTIF y EXTIF contengan los valores correspondientes a las interfaces de la red interna y la red externa respectivamente. Cabe destacar que la interfaz de la red interna, es la misma interfaz utilizada en la red inalámbrica. Luego de realizar estos cambios se debe agregar las reglas al inicio del sistema, mediante el siguiente comando:

```
#ln  -s  /etc/init.d/chillispot.iptables  /etc/rcS.d/S40chillispot.iptables
```

Por ultimo se debe modificar el archivo /usr/lib/cgi-bin/hotspotlogin.cgi, el cual corresponde al script usado por chillispot durante el proceso de autenticación. En este archivo se debe verificar que el parametro "$uamsecret", contenga el mismo valor especificado en el archivo de configuración chilli.conf. Igualmente se debe descomentar la línea "$userpassword=1;".

Este mismo archivo contiene el código HTML de las páginas que se muestran en el proceso de autenticación, si se desea estas pueden ser modificadas.

Con esto se concluye con la instalación del sistema de autenticación, sólo queda iniciar el servicio del servidor chillispot junto con los demás servicios asociados.