ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA

DISEÑO E IMPLEMENTACIÓN DE UN CLIENTE RADIUS EN LINUX

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

CÉSAR IVÁN CEPEDA CARVAJAL
PABLO ARTURO PROAÑO SÁNCHEZ

DIRECTORA: MSc. SORAYA SINCHE

Quito, Septiembre 2007

DECLARACIÓN

Nosotros, César Iván Cepeda Carvajal y Pablo Arturo Proaño Sánchez, declaramos que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional, puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____	_____
César Iván Cepeda Carvajal	Pablo Arturo Proaño Sánchez

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por César Iván Cepeda Carvajal y Pablo Arturo Proaño Sánchez, bajo mi supervisión.

MSc SORAYA SINCHE
DIRECTORA DEL PROYECTO

Dedicatoria

Dedico este trabajo en primer lugar a Dios quien siempre estuvo guiando mis pasos, en segundo lugar lo dedico a mi padre César Cepeda Proaño y a mi madre Rosa Carvajal Cadena, quienes supieron ser mi guía, mi apoyo y mi ejemplo durante toda mi formación personal, intelectual y profesional, Dios los bendiga padres queridos.

Dedico este trabajo a mi esposa Heydi Haro y a mi hijo Sebastián Cepeda quienes siempre estuvieron a mi lado apoyándome y dándome su cariño, siendo un incentivo durante mi culminación profesional.

Y por último dedico este trabajo a todas aquellas personas que siempre me apoyaron de forma silenciosa y que siempre confiaron en mi, gracias por su apoyo queridas hermanas, abuelitos y tíos los llevo en mi corazón.

César Iván Cepeda Carvajal

Dedicatoria

A mis padres María Sánchez y Jaime Proaño, por todo su apoyo y sacrificio durante el transcurso de mi vida académica.

A mis hermanos, Jaime, María, Mariana, Javier, gracias por estar ahí cuando los necesite.

A las personas, que de alguna manera colaboraron para que este proyecto se lleve a cabo.

Pablo A. Proaño Sánchez

Agradecimiento

Agradecemos a la empresa "LA COMPETENCIA S.A." por permitirnos realizar las pruebas de funcionamiento de nuestra implementación en sus instalaciones.

Nuestro más sincero agradecimiento a cuantas personas han hecho posible la realización de este trabajo especialmente a la Msc. Soraya Sinche directora del presente proyecto, porque con su guía pedagógica, supo despertar nuestro espíritu de superación.

De igual manera agradecemos a la Escuela Politécnica Nacional, institución que supo acogernos durante gran parte de nuestra formación personal, intelectual, moral y profesional.

César Iván Cepeda Carvajal

Pablo Arturo Proaño Sánchez

PRESENTACIÓN

Actualmente las comunicaciones juegan un papel muy importante en la actividad diaria de las empresas, ya que la utilización de la transmisión de datos en *Intranets* y a través de Internet se ha vuelto un requerimiento necesario en el desarrollo de los negocios a nivel mundial.

La seguridad de la información es otro aspecto a considerarse dentro de las organizaciones, que si bien es cierto al encontrarse dentro de la empresa se pensaría que la misma esta protegida, esto no es tan cierto pues al ser información almacenada y transmitida de forma digital conlleva consideraciones adicionales de seguridad.

Es por esta razón que, en lugar de invertir cada vez más en recursos para expandir la capacidad de sus redes, las organizaciones buscan formas de hacer más eficientes sus redes actuales, tanto en aspectos de seguridad como en el correcto aprovechamiento de los recursos disponibles.

Por lo anteriormente mencionado se vuelve un requisito necesario disponer de mecanismos que permitan controlar y registrar de forma adecuada el acceso a redes de datos, lográndose como resultado un correcto uso de los recursos de red disponibles.

El presente proyecto consiste en implementar un sistema que realiza un control registrado del acceso de cada usuario a los servicios de red. Así como también permite controlar el ancho de banda asignado a cada usuario y llevar un registro del tiempo de utilización del sistema o de los *bytes* consumidos por cada usuario.

El proyecto se ha desarrollado en su totalidad empleando software de libre distribución (LINUX). Al ser una implementación realizada en un ambiente de programación abierto, puede ser adecuada a las necesidades del usuario o pueden agregarse nuevas funcionalidades, siendo una alternativa de solución económica, escalable y modular.

Considerando que existe en el mercado soluciones de *software* y *hardware* que permiten realizar implementaciones similares pero con características restringidas. El proyecto se desarrolló con el propósito de ser una solución que reúna la mayor cantidad de características de estas soluciones.

La solución podrá ser empleada en un ISP o en una red privada, para controlar el acceso hacia Internet. Dando como resultado un servicio que permita un nivel de seguridad adecuado, el correcto aprovechamiento del ancho de banda disponible y que permita tener un control de la utilización que cada usuario da al sistema. Además con el uso de esta implementación será posible llevar a cabo la tarifación por el uso de los servicios.

RESUMEN

El presente proyecto de titulación busca ser una alternativa de solución ante el escaso o nulo control de acceso de usuarios hacia las redes de datos públicas (Internet) dentro de redes privadas, en términos de controlar a qué servicios de red pueden acceder, y registrar cuando lo hicieron y por cuanto tiempo.

Se plantea el desarrollar una aplicación de *software* que permita controlar y registrar el acceso de los usuarios a los servicios de la red, para lo cual se emplea el sistema operativo LINUX Fedora Core 3, los usuarios podrán acceder a la aplicación empleando la red cableada, la red inalámbrica y conexiones *dial-up*.

El cliente RADIUS posee una interfaz de administración que permite configurar los perfiles de acceso al sistema, el servidor DHCP, y contabilizar el uso del sistema tanto en tiempo como en *bytes* para efectos de facturación.

En el Capítulo I, se presenta como marco teórico un estudio de los aspectos más relevantes de seguridad en redes de información, tales como: confidencialidad, integridad y disponibilidad de la información y Autenticación, Autorización y Contabilidad de usuarios (AAA).

Se analiza el protocolo RADIUS y se describen los protocolos de seguridad IPSec, HTTPS y SSH, empleados para el aseguramiento de los segmentos de red, tanto de usuarios como de servidores. Además se analiza los diferentes mecanismos de control de ancho de banda que pueden ser implementados sobre el sistema operativo Linux.

En el Capítulo II, luego de describir la problemática que se va a solucionar, se definen las políticas de seguridad a implementar, se analizan los requerimientos de *hardware* de los servidores y se procede con la implementación del cliente RADIUS en base a las políticas de seguridad planteadas.

Se presenta una descripción de las herramientas empleadas durante el proceso de implementación del Cliente RADIUS y su interfaz de administración.

Para usuarios remotos se plantea el uso de un Servidor *dial-up*, el cual se lo implementa en *Windows* XP. Se describe el mecanismo empleado para el aseguramiento de los usuarios del segmento de red inalámbrico.

Se realiza una comparación del Cliente RADIUS con soluciones comerciales similares, tanto desde el punto de vista económico como funcional.

En el Capitulo III, se presentan las pruebas de funcionamiento realizadas en el ambiente de pruebas y en el ambiente real, y se analizan los resultados obtenidos.

Finalmente en el Capítulo IV, se han colocado las conclusiones y recomendaciones, resultado de la realización del presente proyecto.

ÍNDICE DE CONTENIDO

CAPÍTULO I

SEGURIDAD EN REDES DE INFORMACIÓN Y CONTROL DE ANCHO DE BANDA

1.1 INTRODUCCIÓN 1

1.2 GENERALIDADES DE SEGURIDAD EN REDES DE INFORMACIÓN 2

1.2.1 CONTROLES DE SEGURIDAD (FÍSICA, TÉCNICA Y ADMINISTRATIVA) 3

1.2.1.1 Seguridad Física y Técnica 4

1.2.1.2 Seguridad administrativa 5

1.2.2 CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN 6

1.2.2.1 Confidencialidad 6

1.2.2.2 Integridad 6

1.2.2.3 Disponibilidad 6

1.2.3 AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD DE USUARIOS 7

1.2.3.1 Autenticación 7

1.2.3.2 Autorización 7

1.2.3.3 Contabilidad 8

1.2.4 ATAQUES Y VULNERABILIDADES 8

1.2.4.1 Amenazas Humanas 8

1.2.4.2 Amenazas naturales 9

1.2.4.3 Ataques 10

1.2.5 COMPARACIÓN Y DEFINICIÓN DE LOS DIFERENTES MÉTODOS DE AUTENTICACIÓN 10

1.2.5.1 Autenticación basada en contraseñas 11

1.2.5.2 Autenticación mediante *tokens* 13

1.2.5.3 Firmas digitales 13

1.2.5.4 Certificados digitales 15

1.2.5.5 Un solo ingreso (*Single Sign-O*n) 17

1.2.5.6 Protocolo de Autentificación por Contraseña (PAP) 18

1.2.5.7 Protocolo de Autentificación por Reto (CHAP) 20

1.2.5.8 Sistemas biométricos 23

1.2.5.9 Comparación entre los métodos de autenticación 24

1.3 DESCRIPCIÓN DE LOS PROTOCOLOS UTILIZADOS Y SU RELACIÓN CON LA IMPLEMENTACIÓN 24

1.3.1 PROTOCOLO RADIUS 24
1.3.1.1 Operación del protocolo 25
1.3.1.2 Interacción con PAP y CHAP 27
1.3.1.3 Formato del paquete RADIUS 27
1.3.2 IPSEC 30
1.3.3 HTTPS (*Secure Socket Layer*) 31
1.3.4 SSH (*Secure Shell*) 32
1.3.5 802.1X 33

1.4 CONTROL DE ANCHO DE BANDA 38

1.4.1 DISCIPLINAS DE COLAS SIMPLES 39
1.4.1.1 *Pfifo-fast* (FIFO) 40
1.4.1.2 *Token Bucket Filter* (TBF) 40
1.4.1.3 *Stochastic Fairness Queueing* (SFQ) 41
1.4.2 DISCIPLINAS DE COLAS CON CLASES 41
1.4.2.1 FUNCIONAMIENTO DE LAS DISCIPLINAS DE COLAS CON CLASES 41
1.4.2.2 DISCIPLINA DE COLAS PRIO 43
1.4.2.3 DISCIPLINA DE COLA CBQ *(Class Based Queueing)* 43
1.4.2.4 DISCIPLINA DE COLAS HTB (*Hierarchical Token Bucket*) 43

CAPÍTULO II

CONFIGURACIÓN DEL SERVIDOR RADIUS E IMPLEMENTACIÓN DEL CLIENTE RADIUS

2.1 DESCRIPCIÓN DE LA PROBLEMÁTICA EXISTENTE 46

2.2 ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD A SER IMPLEMENTADAS 47

2.2.1 POLÍTICAS A SER IMPLEMENTADAS 48
2.2.1.1 Condiciones del cuarto de equipos 49
2.2.1.2 Sistema de respaldo de energía eléctrica 49
2.2.1.3 Sistema de control de incendios 49
2.2.1.4 Control de acceso mediante dirección MAC en el cliente RADIUS 49
2.2.1.5 Filtros de direcciones MAC en puntos de acceso inalámbricos 50
2.2.1.6 Autorización de acceso a usuarios con dirección IP configurada de forma estática 50
2.2.1.7 Empleo de nombre de usuario y clave de acceso segura para la autenticación de usuarios 51
2.2.1.8 Definir diferentes perfiles de acceso para los usuarios 53
2.2.1.9 Protección de la información que viaja por el segmento de red inalámbrico 55
2.2.1.10 Protección de la información de autenticación que el usuario envía al cliente RADIUS ... 55
2.2.1.11 Protección de la información de autenticación que el cliente RADIUS, envía al servidor RADIUS 55

2.2.1.12 Registro del tiempo de conexión y el consumo medido en *bytes* que realice el usuario 56

2.3 REQUERIMIENTOS DE HARDWARE 56

2.3.1 SERVIDOR RADIUS 57

2.3.2 CLIENTE RADIUS 58

2.3.3 SERVIDOR DIAL-UP 58

2.4 CONFIGURACIÓN Y PUESTA EN MARCHA DEL SERVIDOR DE AUTENTICACIÓN FreeRADIUS EN LINUX 60

2.4.1 CARACTERÍSTICAS DEL SERVIDOR FreeRADIUS VERSIÓN 1.0 61

2.4.1.1 Características de Plataforma 61

2.4.1.2 Soporte de RFCs y Atributos VSA (*Vendor Specific Attributes*) 61

2.4.1.3 Atributos de configuración adicionales del servidor 62

2.4.2 INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR FreeRADIUS 62

2.4.2.1 Ejecutando el servidor 63

2.4.2.2 Configuración de MySQL 65

2.4.2.3 Creación y configuración de la base de datos para el servidor RADIUS 65

2.4.2.4 Configuración del servidor RADIUS para usar la base de datos de MySQL 66

2.4.2.5 Instalación de Dialup Admin 67

2.5 IMPLEMENTACIÓN DEL CLIENTE RADIUS EN LINUX 71

2.5.1 PROCEDIMIENTO DE IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD 71

2.5.1.1 Control de acceso mediante dirección MAC 72

2.5.1.2 Filtros de direcciones MAC en puntos de acceso inalámbricos 72

2.5.1.3 Autorización de acceso a usuarios con dirección IP configurada de forma estática 73

2.5.1.4 Empleo de nombre de usuario y clave de acceso segura para la autenticación de usuarios 73

2.5.1.5 Definir diferentes perfiles de acceso para los usuarios 73

2.5.1.6 Protección de la información que viaja por el segmento de red inalámbrico 74

2.5.1.7 Protección de la información de autenticación que el usuario envía al cliente RADIUS ... 74

2.5.1.8 Protección de la información de autenticación que el cliente RADIUS, envía al servidor RADIUS 74

2.5.1.9 Registro del tiempo de conexión y el consumo medido en bytes que realice el usuario 75

2.5.2 DESCRIPCIÓN DE LAS HERRAMIENTAS DE SOFTWARE EMPLEADAS PARA LA IMPLEMENTACIÓN 75

2.5.2.1 Servidor Apache 76

2.5.2.2 PHP Hypertext Preprocessor 77

2.5.2.3 MySQL 78

2.5.2.4 Iptables 80

2.5.3 PROGRAMACIÓN DEL CLIENTE RADIUS 87

2.5.3.1 Organización de la información en la base de datos del cliente RADIUS 87

2.5.3.2 Programación de scripts PHP 91

2.5.4 PROGRAMACIÓN DE LA INTERFAZ DE ADMINISTRACIÓN 95
2.5.4.1 Menú Ver Perfiles 97
2.5.4.2 Menú Nuevo Perfil 97
2.5.4.3 Menú Ver Servicios 98
2.5.4.4 Menú de configuración Nuevo Servicio 98
2.5.4.5 Menú de configuración Ver MAC Address 99
2.5.4.6 Menú de configuración de Nueva MAC 100
2.5.4.7 Menú Servidor DHCP 100
2.5.4.8 Menú Tarifación por MAC 101
2.5.4.9 Menú Configuración Tarifación 102
2.5.4.10 Estructura de archivos 102
2.5.4.11 Servidor DHCP 103
2.5.5 PROGRAMACIÓN DE LOS PERFILES DE USUARIO 104
2.6 ASIGNACIÓN DE ANCHO DE BANDA 105
2.7 IMPLEMENTACIÓN DEL SISTEMA DE TARIFACIÓN 106
2.8 IMPLEMENTACIÓN DEL SERVIDOR *DIAL-UP* 107
2.9 CONFIGURACIÓN E IMPLEMENTACIÓN DE SEGURIDAD EN LOS SEGMENTOS DE RED 108
2.9.1 CONFIGURACIÓN DEL PUNTO DE ACCESO Y DE LOS CLIENTES INALÁMBRICOS 109
2.9.2 SEGURIDAD EN EL ACCESO PARA ADMINISTRACIÓN DE SERVIDORES 110
2.9.3 SEGURIDAD ENTRE SERVIDOR Y EL CLIENTE RADIUS 112
2.9.3.1 Implementación IPSec de computador a computador 112
2.9.4 SEGURIDAD ENTRE LOS USUARIOS Y EL CLIENTE RADIUS 113
2.10 COMPARACIÓN CON SOLUCIONES SIMILARES Y ANÁLISIS DE COSTOS DE LA SOLUCIÓN 114
2.10.1 SOLUCIONES COMERCIALES SIMILARES 114
2.10.1.1 Solución FirstSpot de PatronSoft 114
2.10.1.2 Solución Air Marshal de *IEA Software*, inc 116
2.10.2 ANÁLISIS DE COSTOS 117
2.10.2.1 Costos de implementación empleando FirstSpot TM 118
2.10.2.2 Costos de implementación empleando Air Marshal de IEA software, Inc. 120
2.10.2.3 Costo de implementación de la solución cliente RADIUS en linux 122
2.10.2.4 Comparación de costos de implementación de los tres sistemas planteados anteriormente 124
2.10.3 Comparación con soluciones comerciales similares 125

CAPÍTULO III

PRUEBAS DE FUNCIONAMIENTO Y ANÁLISIS DE RESULTADOS

3.1 DESCRIPCIÓN DEL ESCENARIO DE PRUEBAS 127

3.1.1 Segmento de red INTERNET 128

3.1.2 Segmento de red RADIUS 128

3.1.3 Segmento de red LOCAL 128

3.2 IMPLEMENTACIÓN DEL ESCENARIO DE PRUEBAS 129

3.2.1 CONFIGURACIÓN DE USUARIOS 129

3.2.2 CONFIGURACIÓN Y PUESTA EN MARCHA DEL SERVIDOR DHCP ESTÁTICO 131

3.2.3 CONFIGURACIÓN DEL SERVIDOR HTTP, HTTPS. FTP, MAIL, TELNET Y SSH 132

3.3 VERIFICACIÓN DE FUNCIONAMIENTO DEL SERVIDOR DIAL-UP 133

3.4 VERIFICACIÓN DEL ESTABLECIMIENTO DEL TÚNEL IPSEC ENTRE EL CLIENTE RADIUS Y EL SERVIDOR RADIUS 134

3.5 VERIFICACIÓN DEL ESTABLECIMIENTO DE LA SESIÓN HTTPS ENTRE EL USUARIO Y EL CLIENTE RADIUS PARA PROTEGER LA INFORMACIÓN DE AUTENTICACIÓN QUE EL USUARIO ENTREGA AL CLIENTE RADIUS 136

3.6 VERIFICACIÓN DE LA SEGURIDAD DE LAS SESIONES ESTABLECIDAS CON EL CLIENTE RADIUS PARA SU ADMINISTRACIÓN 137

3.6.1 Verificación del establecimiento de la sesión SSH 137

3.6.2 Verificación del establecimiento de la sesión HTTPS 139

3.7 COMPROBACIÓN DE SEGURIDAD EN EL SEGMENTO DE RED INALÁMBRICO 141

3.8 VERIFICAR EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD ESTABLECIDAS 142

3.8.1 CONTROL DE ACCESO MEDIANTE DIRECCIÓN MAC 143

3.8.2 FILTROS DE DIRECCIONES MAC EN PUNTOS DE ACCESO 143

3.8.3 AUTORIZACIÓN DE ACCESO A USUARIOS CON DIRECCIÓN IP CONFIGURADA DE FORMA ESTÁTICA 144

3.8.4 EMPLEO DE NOMBRE DE USUARIO Y CLAVE DE ACCESO SEGURA PARA LA AUTENTICACIÓN DE USUARIOS 145

3.8.5 DEFINIR DIFERENTES PERFILES DE ACCESO PARA LOS USUARIOS 148

3.8.6 REGISTRO DEL TIEMPO DE CONEXIÓN Y EL CONSUMO MEDIDO EN BYTES QUE REALICE EL USUARIO 150

3.9 ANÁLISIS DE LOS RESULTADOS OBTENIDOS EN EL AMBIENTE DE

PRUEBA 153

3.10 ANÁLISIS DE LOS RESULTADOS OBTENIDOS EN EL AMBIENTE REAL 158

3.10.1 TOPOLOGÍA DE LA RED DE PRUEBA 159

3.10.2 CREACIÓN DE LOS USUARIOS 160

3.10.3 CREACIÓN DE LOS SERVICIOS PARA CADA PERFIL 161

3.10.4 ADHESIÓN DE DIRECCIONES MAC AL CLIENTE RADIUS 166

3.10.5 ADHESIÓN DE DIRECCIONES MAC VALIDAS DE USUARIOS DEL SEGMENTO INALÁMBRICO 166

3.10.6 SERVIDOR DE ACCESO TELEFÓNICO 167

3.10.7 ADOPCIÓN DE SOLUCIÓN POR PARTE DE LOS USUARIOS 168

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES 171

4.2 RECOMENDACIONES 176

BIBLIOGRAFÍA 178

ABREVIATURAS 180

ANEXOS 182

ANEXO A A-1

ANEXO B B-1

ANEXO C C-1

ANEXO D D-1

ANEXO E E-1

ANEXO F F-1

ANEXO G G-1

ANEXO H H-1

ANEXO I I-1

ANEXO J J-1

ANEXO K K-1

ANEXO L L-1

ANEXO M M-1

ÍNDICE DE FIGURAS

Figura 1.1 Passwords de una sola vez 12
Figura 1.2 Presentación de Certificado Digital en una página WEB Bancaria 16
Figura 1.3 Formato de la trama PAP 19
Figura 1.4 Autenticación CHAP para acceso remoto 21
Figura 1.5 Formato de la trama CHAP 21
Figura 1.6 Señalización Protocolo RADIUS 25
Figura 1.7 Formato del paquete RADIUS 27
Figura 1.8 Proceso de autenticación con RADIUS 34
Figura 1.9 Estructura de Autenticación 802.1X/EAP 35
Figura 1.10 Disciplinas de colas con clases 42
Figura 2.1 Diagrama de Flujo de la trayectoria de un paquete en el kernel 86
Figura 2.2 Tabla relacional de la estructura de la base de datos 88
Figura 2.3 Ventana presentada al usuario antes de autenticarse 93
Figura 2.4 Ventana de autenticación de usuarios 94
Figura 2.5 Ventana presentada al usuario una vez autenticado 95
Figura 2.6 Interfaz de Administración del Cliente RADIUS 96
Figura 2.7 Menú de configuración de perfiles 97
Figura 2.8 Menú de configuración para crear un nuevo perfil 97
Figura 2.9 Menú de configuración de servicios 98
Figura 2.10 Menú de configuración para añadir un nuevo servicio 99
Figura 2.11 Menú de configuración de usuario por dirección MAC 99
Figura 2.12 Menú de configuración para añadir una nueva dirección MAC al sistema 100
Figura 2.13 Menú de configuración del servicio DHCP 101
Figura 2.14 Menú que permite seleccionar el dispositivo para realizar la tarifación 101
Figura 2.15 Menú que permite seleccionar el dispositivo para realizar la tarifación 102
Figura 2.16 Reporte de tarifación por consumo de tiempo 106
Figura 2.17 Diagrama de esquema de seguridad de servidores empleado 108
Figura 2.18 Pantalla de página web de configuración del Access Point 109
Figura 2.19 Sesión de shell no segura, empleo de telnet 110
Figura 2.20 Sesión de shell segura, empleo de SSH 111
Figura 3.1 Diagrama de red del escenario de pruebas 127
Figura 3.2 Configuración de seguridad de la tarjeta de red del usuario 131
Figura 3.3 Captura de tráfico entre el cliente y el servidor RADIUS sin emplear IPSec. 134
Figura 3.4 Captura de tráfico entre el servidor RADIUS y el cliente empleando IPSec. 135
Figura 3.5 Captura del trafico HTTPS entre el cliente RADIUS y un usuario. 136
Figura 3.6 Tráfico SSH hacia el cliente RADIUS 138

Figura 3.7 Trafico de una sesión TELNET hacia el Cliente RADIUS 139
Figura 3.8 Pantalla de inicio para configuración del cliente RADIUS vía interfaz WEB 140
Figura 3.9 Trafico HTTPS intercambiado en el proceso de autenticación del usuario 140
Figura 3.10 Captura del tráfico generado en el proceso de autenticación del cliente inalámbrico 142
Figura 3.11 Configuración de Control de Acceso de filtrado por dirección MAC en el Punto de Acceso Inalámbrico. 144
Figura 3.12 Página de autenticación de usuarios 145
Figura 3.13 Ventana presentada a usuarios autenticados 146
Figura 3.14 Regla de iptables generada para un usuario 146
Figura 3.15 Ventana presentada ante una autenticación fallida 147
Figura 3.16 Reglas de iptables, no se ha creado ninguna regla adicional 147
Figura 3.17 Interfaz de administración - Servicios configurados para el perfil Premium 148
Figura 3.18 Interfaz de administración - Servicios configurados para el perfil Gold 149
Figura 3.19 Reglas de iptables para el usuario con IP: 192.168.3.200 perfil Premium 150
Figura 3.20 Reglas de iptables para el usuario con IP: 192.168.3.201 Perfil Gold 150
Figura 3.21 Tarifación por usuario en base a su dirección MAC 151
Figura 3.22 Configuración del tipo de tarifación 151
Figura 3.23 Tarifación de utilización por consumo de tiempo 152
Figura 3.24 Tarifación de utilización por consumo de bytes 152
Figura 3.25 Captura de tráfico de autenticación de usuarios remotos 153
Figura 3.26 Captura de tráfico IPSec intercambiado entre el Servidor y el Cliente 155
Figura 3.27 Administración Gráfica del cliente RADIUS 157
Figura 3.28 Topología de red del ambiente real 159
Figura 3.29 Pantallas del estado y detalles de la conexión. 168

ÍNDICE DE TABLAS

Tabla 1.1 Comparación de los diferentes métodos de autenticación revisados 23
Tabla 2.1 Trayectoria de un paquete destinado a la máquina local 84
Tabla 2.2 Trayectoria de un paquete originado en la maquina local 84
Tabla 2.3 Trayectoria de un paquete destinado a una máquina en otra red 85
Tabla 2.4 Tabla de estructura de archivos y sus respectivas funciones 103
Tabla 2.5 Precios de lista de FisrtSpot 118
Tabla 2.6 Costos Implementación FirstSpot 120
Tabla 2.7 Precios de software Air Marshal 120
Tabla 2.8 Valor de los contratos de mantenimiento para Air Marshal 121
Tabla 2.9 Costos de Implementación Air Marshal 122
Tabla 2.10 Costos involucrados al implementar el Sistema Cliente RADIUS en LINUX 123
Tabla 2.11 Costos totales de las diferentes implementaciones 125
Tabla 2.12 Tabla comparativa de características de los programas de control de acceso 126
Tabla 3.1 Direccionamiento IP de los segmentos de red del escenario de pruebas 128
Tabla 3.2 Configuración de la cuenta de correo electrónico de prueba 132
Tabla 3.3 Detalle de usuarios de prueba Red LCSA 160
Tabla 3.4 Perfiles de usuarios creados 162
Tabla 3.5 Servicios configurados previamente 163
Tabla 3.6 Servicios del perfil Networking 164
Tabla 3.7 Servicios del perfil ventas 165

CAPÍTULO I

SEGURIDAD EN REDES DE INFORMACIÓN Y CONTROL DE ANCHO DE BANDA

CAPÍTULO I

SEGURIDAD EN REDES DE INFORMACIÓN Y CONTROL DE ANCHO DE BANDA

1.1 INTRODUCCIÓN

La aparición de Internet y la búsqueda de comunicación global han modificado la forma de las comunicaciones en el mundo y en las empresas, por lo que hoy en día es muy importante para las empresas encontrar mecanismos que faciliten las comunicaciones. La tendencia es que esta demanda continúe aumentando en los años subsiguientes con el objetivo de alcanzar comunicaciones permanentes y seguras.

El protocolo IP se ha ubicado como líder en el campo de la transmisión de todo tipo de información, no sólo porque ofrece comunicaciones confiables, estables y flexibles, sino también porque brinda soluciones convergentes; integrando servicios de voz, datos y video, a través de redes privadas virtuales (VPN). Y es por esta razón que para lograr una óptima funcionalidad algunas de éstas aplicaciones requieren de mayor ancho de banda, mientras que otras requieren de una entrega garantizada de los paquetes de información en tiempo y forma (Voz sobre IP, video conferencia, etc.).

En el campo de los negocios de hoy, el uso de Internet está creciendo exponencialmente. A medida que proveedores, socios y clientes migran sus operaciones comerciales a plataformas basadas en la Web, las organizaciones necesitan integrar estrechamente sus prácticas de negocios a Internet. El problema es que a medida que se incrementa el uso de Internet, también aumentan los costos asociados. Es por esta razón que, a cambio de invertir cada vez más en recursos para expandir la capacidad de sus redes, las organizaciones buscan formas de hacer más eficientes sus redes actuales, tanto en aspectos de seguridad como con el aprovechamiento de los recursos disponibles.

El cambio experimentado por las redes de comunicaciones para converger en redes capaces de integrar servicios de voz, datos y video dentro de una misma infraestructura, ha llevado a que el modelo original de servicio bajo el mejor esfuerzo no sea suficiente para poder asegurar un servicio oportuno. Dentro de este contexto, se vuelve necesario emplear mecanismos para administrar de forma eficiente el recurso de red disponible para el correcto funcionamiento de los diferentes servicios dentro de la red, como el empleo de mecanismos de control de ancho de banda, que será implementado como parte del presente proyecto de titulación.

Todos los aspectos mencionados anteriormente son muy importantes de considerar, pues hacen prever que la comunicación será un requerimiento mundial, pero no se debe olvidar el hecho de que el servicio a prestarse tiene un costo asociado y este debe ser facturado; por lo cual se deben implementar mecanismos que ayuden a controlar el acceso a la red, y así mismo definir ciertos niveles de acceso para los diferentes grupos de usuarios que harán uso del sistema en base a perfiles predefinidos. Además de un control de ancho de banda por usuario.

Dando como resultado un servicio que permita un nivel de seguridad adecuado, el correcto aprovechamiento del ancho de banda disponible y que permita tener un control de la utilización que el usuario le da al sistema por parte de quien provea este servicio.

1.2 GENERALIDADES DE SEGURIDAD EN REDES DE INFORMACIÓN

“Seguridad es una necesidad básica. Estando interesada con la preservación de la vida y las posesiones, es tan antigua como la vida.”[1]

[1] "SEGURIDAD: UNA INTRODUCCIÓN" Dr. Giovanni Manunta Consultor y profesor de seguridad de Cranfield University http://www.seguridadcorporativa.org

El gran desarrollo de la tecnología informática está ofreciendo un nuevo y amplio campo de acción a comportamientos antisociales y delictivos, presentadas de formas anteriormente no imaginadas, permitiendo la realización de delitos tradicionales de formas no tradicionales.

La mayoría del mundo informático desconoce la magnitud de la problemática a enfrentar, por lo que generalmente no invierten en recursos humanos y económicos para prevenir daños y pérdidas de información.

Al tratar de proteger la información, hay que identificar todos los elementos que participan en su manipulación, como son aplicaciones de *software*, medios de transmisión y medios de almacenamiento, y tratar de protegerlos de ataques o manipulaciones maliciosas.

Teniendo esto claro, es lógico suponer que el empleo de mecanismos de seguridad tradicionales como una cerradura o candado no serán suficientes para proteger la información, pues por su naturaleza ésta puede ser vulnerada por otro medio (Ej. medios de transmisión), lo que indica que para proteger la información, se deben considerar tanto los elementos físicos como lógicos que intervienen en este sistema con el objetivo de dar una solución de seguridad adecuada y acorde con el sistema que se desea proteger.

1.2.1 CONTROLES DE SEGURIDAD (FÍSICA, TÉCNICA Y ADMINISTRATIVA)

La seguridad de la información dentro de las redes de datos debe considerar tres aspectos fundamentales, seguridad *física*, *técnica* y *administrativa*; pues de nada serviría el instalar un sistema de seguridad como un antivirus o un *firewall*, cuando por otro lado no se ha pensado en proteger dicho sistema contra incendios o inundaciones, de igual manera de que serviría proteger un sistema contra incendios o inundaciones cuando a este puede acceder cualquier intruso, es aquí donde toma cuerpo la importancia que tiene el considerar controles de seguridad que involucren estos tres aspectos.

1.2.1.1 Seguridad Física y Técnica

Se podría definir a la seguridad física como la aplicación de barreras físicas y mecanismos de control como medidas de precaución ante amenazas a los recursos e información confidencial. Es decir controles y mecanismos de seguridad para precautelar la integridad física del *hardware* y medios de almacenamiento, que se encuentran dentro y alrededor del cuarto de operaciones, así como los medios de acceso remoto al y desde el mismo.

A continuación se lista las amenazas a ser consideradas dentro de la seguridad física t técnica:

- Desastres naturales
- Incendios accidentales
- Tormentas e inundaciones
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos.

Se espera que todo sistema de seguridad sea infalible, pero esto en la realidad no es posible, por lo que ante amenazas existentes se deberá tomar medidas que permitan reducir el riesgo de interrupciones de sistemas, robos, o daños. Se presenta a continuación una lista de prácticas que ayudarán a prevenir y sobrellevar los problemas de seguridad:

- Disposición de un plan de contingencia (esquemas redundantes, respaldos verificado su efectividad ante contingentes).
- Disponer de mecanismos de control de incendios (mecanismos adecuados diseñados para controlar incendios en cuartos de comunicaciones).
- Definición de políticas internas de las organizaciones para controlar el uso inadecuado de la tecnología.
- Controles de acceso a los cuartos de equipos (guardianía, detectores de metales, sistemas biométricos, verificación automática de firmas, seguridad con animales, seguridad electrónica).

1.2.1.2 Seguridad administrativa

La seguridad administrativa establece mecanismos y estrategias a seguir con el objetivo de proteger la información de una forma adecuada.

La seguridad administrativa, consiste en la aplicación de barreras y el establecimiento de procedimientos que resguarden el acceso a los datos, permitiendo el acceso solo a personal autorizado para hacerlo.

A continuación se presentan las siguientes consideraciones para realizar una administración correcta de la seguridad de la información:

- Restringir el acceso a determinados archivos y programas.

- Garantizar que los operadores puedan trabajar sin problema y sin causar daño alguno al sistema, sin supervisión, es decir, verificar que en los procesos de operación habitual no se pueda modificar un archivo o programa crítico del sistema.

- Garantizar que los datos, archivos y programas sean utilizados en procedimientos correctos y por los procedimientos correctos.

- Asegurar que la información enviada sea entregada y recibida únicamente por su destinatario autorizado.

- Disponer de un mecanismo para mantener la integridad de la información transmitida.

- La existencia de sistemas de transmisión redundantes.

1.2.2 CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN

Como el objetivo es proteger la información, se debe considerar tres aspectos muy importantes en la preservación de la misma, los cuales son la confidencialidad, integridad y disponibilidad.

1.2.2.1 Confidencialidad

El objetivo de la confidencialidad, es permitir que la información sea únicamente vista por las personas a quienes está destinada, es decir se refiere a la privacidad de la información. Es aquí donde juega un papel muy importante la encripción de los datos.

En la actualidad la tecnología de encripción ha avanzado notablemente, pero estudios de este tipo se realizan y muchos consideran que se lo hace de forma secreta.

1.2.2.2 Integridad

La integridad hace referencia a la habilidad de proteger la información, los datos o las transmisiones de alteraciones no autorizadas, no controladas o accidentales. Asegurar la consistencia de la información y que atributos como el tiempo y la totalidad de la información sean consistentes con los requerimientos.

Mecanismos empleados para este propósito son algoritmos de *hash*.

1.2.2.3 Disponibilidad

Hace referencia a que la red, *hardware* y *software* sean confiables, es decir se puedan recuperar rápido y completamente ante eventos de una interrupción.

Para poder lograr este objetivo se emplean generalmente mecanismos de

redundancia de enlaces, *hardware* y *software*, con el fin de que en caso de que un evento interrumpa el funcionamiento de uno de estos elementos del sistema, el respaldo redundante solucione el problema lo más rápido posible.

1.2.3 AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD DE USUARIOS

Los niveles de confidencialidad, integridad y disponibilidad de la información deben estar complementados con niveles adecuados de autenticación, con mecanismos de control de acceso, definición de niveles de acceso a servicios o perfiles y controles de auditoria de qué realizaron los usuarios después de acceder. La autenticación, autorización y contabilidad, es conocida como AAA.

1.2.3.1 Autenticación

Garantiza que una identidad sea válida y corresponda a su propietario.

Cada usuario que intente acceder a una red de datos o un servicio de la misma, posee un distintivo único que es su identidad, por lo que para poder acceder a los servicios de red deberá autenticarse. Un ejemplo de autenticación será el empleo de una huella digital o una firma, pues a través de las mismas se puede definir si el usuario cuya identidad se quiere verificar es quien dice ser.

1.2.3.2 Autorización

La autorización es un control adicional, que permite tener un control de acceso por usuario después de la autenticación.

Permite realizar un control de acceso de un usuario a determinados servicios de la red, en función de un perfil preestablecido, el cual será aplicado en base a la identidad del usuario que fue autenticada, pudiendo haber empleado una autenticación a través de nombre de usuario y contraseña por mencionar uno.

1.2.3.3 Contabilidad

La contabilidad hace referencia a poder llevar un registro de toda la actividad realizada por un usuario en el momento que accedió a un sistema, es decir, permite llevar un control de uso de un sistema en base a la identidad de quién accedió, a que accedió y por cuanto tiempo permaneció dentro del sistema.

Este tipo de control adicional, será de mucha ayuda en el momento de realizar una auditoria del uso de los sistemas, o en el caso que un servicio sea facturado, facilitando su tarifación.

1.2.4 ATAQUES Y VULNERABILIDADES

Un ataque es una técnica empleada para explotar una vulnerabilidad, por ejemplo una amenaza podría ser el ataque de negación de servicio, siendo la vulnerabilidad el empleo de un sistema diseñado sin considerar esta amenaza.

Se puede decir que una amenaza es toda posible interrupción de operación, integridad, disponibilidad de la red o sistema, pudiendo ser la misma de origen natural, por negligencia o por mal intención de alguien.

Una vulnerabilidad es una debilidad propia de los sistemas, causados por un error en el diseño, configuración o implementación de las redes o sistemas.

El ataque es la acción misma, pero previo a esta acción existió una amenaza, por lo que se considera a la amenaza como el paso previo a la ejecución de un ataque. Por tal razón lo importante será encontrar las posibles amenazas con el objetivo de identificar vulnerabilidades y prevenir posibles ataques.

1.2.4.1 Amenazas Humanas

Al tratarse de sistemas que están al servicio de humanos, es lógico suponer que la inquietud y sed de conocimiento puede ser el motivo para que se genere una

amenaza humana.

Personal interno, ataques generados por personal interno de la misma organización, que pueden darse por ignorancia en el manejo de los sistemas, intencionalmente o por inexistencia de normas básicas de seguridad. A este tipo de amenaza no se suele prestar la adecuada atención, ya que se piensa que ataques desde el interior de las organizaciones no se dan, pero esto no es así.

Ex-empleados, personal que abandonó la empresa en malos términos o fueron despedidos, pueden convertirse en este tipo de amenaza. Se trata de personas que tienen resentimiento con la empresa y que tienen conocimiento suficiente para ejecutar un ataque, pueden dejar puertas traseras abiertas, o pueden intentar realizar un ataque de bomba lógica.

Terroristas, ataques ocasionados por individuos u organizaciones que buscan a toda costa realizar un daño en la integridad de los sistemas o de los datos. Un ejemplo de esto puede ser el tratar de robar o modificar la información entre empresas competidoras. Algo adicional es que este tipo de ataques al momento ya son comercializados y generalmente empleados entre competidores de empresas para robar o destruir información de su contraparte.

1.2.4.2 Amenazas naturales

Son todas aquellas amenazas de origen natural, el efecto de las mismas puede ser aplacado considerando el daño que pueden causar en el proceso de diseño de los sistemas.

Este tipo de amenazas pueden ser sobrellevadas, pero no evitadas, se puede considerar como amenazas naturales a los terremotos, inundaciones, por mencionar algunas. Para reducir el efecto cuando una amenaza de este tipo se hace efectiva, es tener un plan de contingencias eficiente, es decir que haya sido probado de forma fehaciente.

1.2.4.3 Ataques

Como se mencionó anteriormente un ataque es la acción misma que busca causar daño a los sistemas computacionales, robar información o alterarla. Como se esta hablando de información y de mecanismo de comunicación, es posible clasificar los ataques en función del modo como se abusa de los canales de comunicación, esta clasificación es la siguiente:

- Fisgar, que es la acción de copiar información sin autorización del propietario de la misma

- Suplantar, es enviar o generar mensajes haciéndose pasar por otro individuo, es decir es el hecho de suplantar la identidad de un individuo y hacer uso de esta identidad falsificada para cometer alguna fechoría.

- Alterar mensajes, consiste en tomar un mensaje y alterarlo antes de entregarlo a su destino.

- Reenviar, consiste en capturar mensajes y reenviarlos más tarde, este ataque puede ser efectivo aun con mensajes encriptados.

- Denegación de servicio, consiste en inundar un canal o recurso con peticiones o mensajes falsos con el objetivo de que los usuarios que realmente requieren el canal o recurso no puedan hacer uso del mismo.

1.2.5 COMPARACIÓN Y DEFINICIÓN DE LOS DIFERENTES MÉTODOS DE AUTENTICACIÓN

Dentro del contexto de transmisión de datos y sistemas de comunicación electrónicos, se puede mencionar los siguientes métodos de autenticación:

- Autenticación basada en *passwords*
- Autenticación mediante *tokens*

- Firmas digitales
- Certificados digitales
- Un solo ingreso *(Single Sign-On)*
- Protocolo de autenticación por contraseña (PAP)
- Protocolo de autenticación por reto (CHAP)
- Sistemas biométricos.

Como se puede observar, los métodos empleados para verificación de identidad, pueden emplear algo que el usuario conoce, algo que el usuario posee y algo que el usuario es.

El empleo de una combinación de diferentes métodos de verificación dará un nivel de seguridad mayor, haciendo del sistema menos vulnerable, más no imposible de vulnerar.

1.2.5.1 Autenticación basada en contraseñas

Este tipo de autenticación hace uso de algo que conoce el usuario, siendo la más empleada en las organizaciones. Presenta inconvenientes, por un lado la elaboración de claves seguras resulta en claves muy difíciles de memorizar, haciendo que los usuarios escriban sus contraseñas en lugares donde puedan ser tomadas por persona maliciosas.

El hecho de que alguien administre estas claves, y considerando que se trata de un humano, añade un riesgo adicional como que pueda ser sobornado, o que en momento de dejar su puesto en la organización, el conocimiento adquirido acerca de los sistemas computacionales de la organización, conviertan a este ex-empleado en una amenaza.

Algo adicional a considerar en el caso que las contraseñas sean transmitidas en forma de texto plano, es que un intruso con un *sniffer* podría apoderarse de dicha contraseña. Por esta razón, para evitar este inconveniente, se emplea métodos de cifrado de contraseñas o el uso de *(One Time Passwords)*

Todos estos inconvenientes pueden ser solucionados en cierta forma a través de la definición y aplicación de políticas de generación y administración de contraseñas.

Las contraseñas de una sola vez trabajan de la siguiente manera, primero el servidor envía un requerimiento al cliente, el mismo que contiene una semilla aleatoria y un número de secuencia de *password*. El cliente que va ha generar el OTP, ingresa el valor aleatorio recibido y el *passphrase* en una función *hash*.

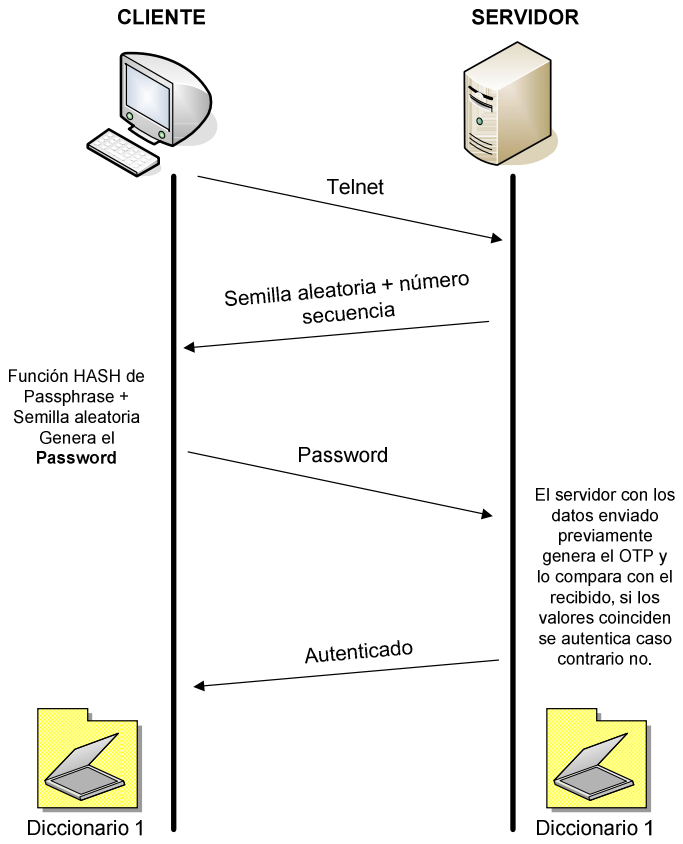

Figura 1.1 *Passwords* de una sola vez [2]

El OTP es enviado al servidor, pues el servidor compara el OTP generado por el usuario con el que generó el servidor con su función *hash*, si los valores coinciden se ha logrado autenticar el usuario o el dispositivo.

[2] Materia Seguridad en Redes, Capitulo 6 AUTENTICACIÓN Manejo de *Passwords*

Por consiguiente empleando este tipo de autenticación, un intruso aunque tenga el número aleatorio y un *password* de una sesión anterior no podrá encontrar la *passphrase*, logrando el objetivo de emplear un *password* una sola vez. En la Figura 1.1 se muestra el funcionamiento de este tipo de autenticación.

1.2.5.2 Autenticación mediante *tokens*

Este tipo de autenticación es utilizado por sistemas de autenticación a través de tarjetas inteligentes, emplea para su operación dos números, un número de PIN o *passphrase* y un número mostrado por el *token*.

El *token*, es un dispositivo generador de *paswords* basado en microprocesadores que se sincroniza con un sistema de Encripción de Control de Acceso (ACE).

Para entender mejor el funcionamiento de este mecanismo se hará referencia al funcionamiento de la tarjeta SecurID *token*.

"La tarjeta SecurID *token* genera un número único de seis dígitos cada seis segundos. Cuando se intenta ingresar con el *token*, se le solicita el *passcode*. El mismo que consiste de 4 a 8 dígitos del número de identificación personal (PIN) que registró previamente, más 6 dígitos que es el número desplegado en el SecurID *token*. Por ejemplo, si un PIN es registrado como "1234567" y el *token* desplegado es "900933," el *passcode* será "1234567900933" y se tendrá que ingresar para conexión exitosa. El SecurID *token* no tiene que ser insertada en ninguna ranura." [3]

1.2.5.3 Firmas digitales

Está técnica consiste en el empleo de algoritmos y cálculos matemáticos, para poder solucionar el problema de confidencialidad y autenticación de la información. El conjunto de técnicas empleadas para este objetivo es la encripción

[3] http://www.pnl.gov/webmailhelp/secureid.htm

de llave pública.

La técnica funciona de la siguiente manera, al ser enviada la información es cifrada con una llave, solo quien posea la llave correspondiente para poder descifrar la información lo hará, caso contrario la información no podrá ser descifrada.

Una llave consiste en un par de números matemáticamente relacionados, los mismos que son obtenidos mediante el uso de un programa de cómputo. Una llave es un número de gran tamaño, que se lo puede ver como un mensaje digital, un archivo binario, o como una cadena de *bits* o *bytes*.

En el proceso de autenticación se emplean llaves privadas y públicas, su generación es siempre en parejas y su correspondencia es unívoca. La idea es que cada individuo genere un par de llaves pública y privada.

El individuo debe mantener en secreto su llave privada, mientras que la llave pública la puede dar a conocer a los demás.

El procedimiento se realiza de la siguiente manera, empleando un programa de cómputo, se ingresa el documento digital y la llave privada, generando un documento que es la firma digital. El documento y la firma digital corresponden al documento firmado.

La firma digital será diferente para cada documento, es decir documentos diferentes generarán firmas diferentes.

Para autenticar el documento firmado, en un programa de computo se ingresa el documento firmado y la llave pública del presunto firmante, el programa se encarga de indicar si el documento digital es auténtico o no.

Si el documento firmado es modificado, por más pequeña que sea esta modificación, el documento no será validado como auténtico.

1.2.5.4 Certificados digitales

En el caso de firmas digitales se tiene un inconveniente, considerando el caso de un sujeto que autentique documentos firmados por 10 individuos deberá contar con 10 archivos o con una base de datos conteniendo las 10 llaves públicas de los posibles firmantes y si este número se aumenta a 100, 1 000 o a 1 000 000, el problema crece considerablemente. Una solución a este problema de manejo de llaves se basa en el concepto conocido como Certificado Digital.

El Certificado Digital es un documento firmado digitalmente por una persona o entidad denominada Autoridad Certificadora, dicho documento establece un nexo entre un sujeto y su llave pública. En el certificado digital constarán los datos del propietario y las condiciones de vigencia del certificado.

La idea es que cualquiera que conozca la llave pública de la AC puede autenticar un Certificado Digital de la misma forma que se autentica cualquier otro documento firmado.

Si el Certificado es auténtico y se confía en la AC, entonces, se puede confiar en que el sujeto identificado en el Certificado Digital posee la llave pública que se señala en dicho certificado.

Por varias razones es conveniente que los Certificados Digitales tengan un periodo de validez, este parece ser un principio básico en la emisión de cualquier tipo de identificación. Por razones técnicas es conveniente que el usuario renueve sus llaves, cada vez aumentando ligeramente el tamaño.

El estándar, internacionalmente aceptado, para Certificados Digitales, es el denominado X.509 de la ITU-T *(International Telecommunication Union-Telecommunication Standarization Sector)*.

Los campos básicos del certificado X.509 se listan a continuación:

- Identificación del sujeto: consiste del individuo, organización o entidad dueña de la llave pública
- Datos de validez del certificado: fecha de inicio, de vencimiento y si el certificado es válido aun para la fecha actual.
- Número de serie del certificado
- Identidad de la autoridad certificadora: nombre de quien emite el certificado
- Llave pública del sujeto.
- Firma digital de la autoridad certificadora

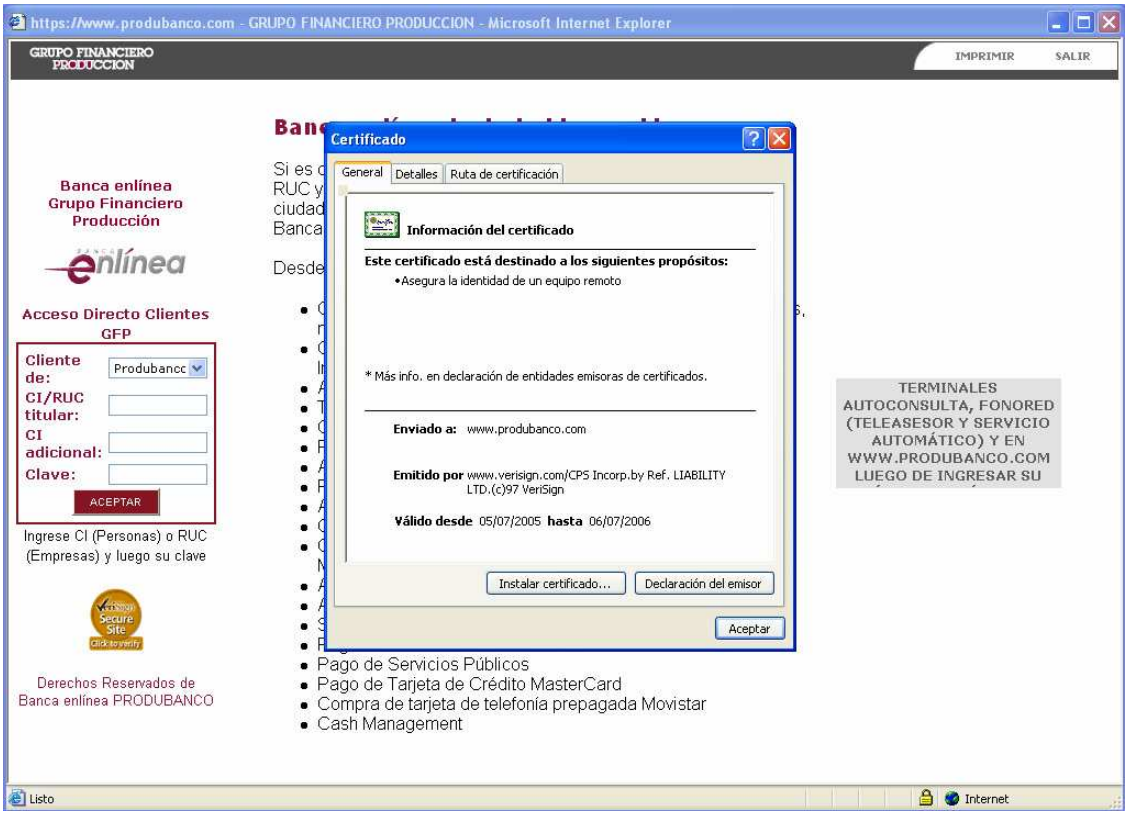

Figura 1.2 Presentación de Certificado Digital en una página WEB Bancaria [4]

La autoridad certificadora emite certificados digitales que ratifican la información de las personas o entidades a quienes se les entrega el certificado, empleando

[4] http://www.produbanco.com

una infraestructura de llave pública (PKI). En la Figura 1.2 se observa el certificado digital de la página web de PRODUBANCO.

La Infraestructura de llave pública (PKI) es la encargada de autentificar certificados digitales y Autoridades Certificadoras. Es una jerarquía de autoridades certificadoras, es decir una autoridad raíz certifica autoridades subordinadas.

Las Autoridades subordinadas confían en la jerarquía, no necesariamente entre ellas, aunque se apunta a crear relaciones de confianza entre autoridades certificadoras de misma o diferente jerarquía.

La dificultad radica en el desarrollo de estándares e infraestructura para certificar firmas digitales y certificados entre organizaciones que usan diferentes esquemas.

1.2.5.5 Un solo ingreso *(Single Sign-On)*

Single Sign-On (SSO) hace referencia al acceso a múltiples recursos por medio de un único proceso de ingreso.

El objetivo de un sistema que implemente *Single Sign-On* es transferir la funcionalidad y complejidad de todos los componentes de seguridad a un solo servicio de *Single Sign-On.*

En un sistema empleando SSO, todos los mecanismos de seguridad se encuentran concentrados en el SSO, siendo éste el único punto de autenticación y registro en el sistema.

En un sistema SSO, los usuarios deben hacer el proceso de ingreso una sola vez, a pesar de que continúan interactuando con múltiples componentes de seguridad en el sistema.

Un inconveniente se puede presentar en este tipo de soluciones, considerando

que todas las aplicaciones o servicios utilizan un mismo *password*, se corre el riesgo de que si un intruso logra conseguir el *password* de una de las aplicaciones o servicios, inmediatamente tendrá acceso a todas ellas.

En una implementación real de SSO, deberá contar con un agente SSO que es el encargado de almacenar en una base de datos o directorio protegido los *passwords* que le permiten al usuario acceder a cada una de las aplicaciones o servicios.

Si bien es cierto, a pesar de que en una verdadera implementación existe un *password* que permite el acceso a todas las aplicaciones o servicios, ésta aparente debilidad se soluciona sometiendo al usuario a un proceso de autenticación fuerte en el momento de acceder, haciendo que la arquitectura SSO aumente el nivel de seguridad del sistema completo, en lugar de disminuirlo.

Se considera como una autenticación fuerte, al proceso de autenticación en sistemas, en los cuales se emplea varios parámetros para realizar la identificación del usuario, los cuales utilizan tecnología avanzada como contraseñas dinámicas (OTP) o certificados digitales. Por mencionar uno, la tarjeta de débito es un ejemplo de autenticación con múltiples factores, ya que para autenticar un usuario, ésta requiere algo que el usuario tiene (la tarjeta) y algo que el usuario conoce (su clave); con solamente una de las dos, el usuario no logrará autenticarse.

1.2.5.6 Protocolo de Autentificación por Contraseña (PAP)

PAP es un protocolo de autenticación que requiere que los usuarios ingresen un nombre de usuario y *password* antes de tener acceso al sistema seguro, los mismos que son enviados a través de la red a un servidor, donde se comparan con una base de datos de las cuentas, es decir nombres y *passwords* de los usuarios.

El protocolo PAP es un método sencillo empleado para confirmar la identidad de

los participantes de una comunicación punto a punto, para lo cual emplea una negociación en dos sentidos, que es realizada en el establecimiento inicial del enlace.

Se envía un *ID/password* por cada uno de los participantes, esperando respuesta del otro participante, caso contrario la comunicación termina.

En éste método de autenticación, debido a que los *passwords* son enviados en forma de texto plano sin ninguna encripción, le añade una vulnerabilidad al poder robarlas y reproducirlas fácilmente, por lo que este método no es un método que proporcione un nivel de seguridad adecuado, y se deberá considerar lo anteriormente mencionado cuando se vaya a emplear PAP.

En la Figura 1.3 se presenta el formato de la trama PAP.

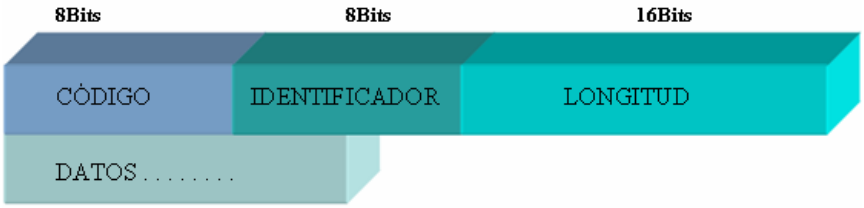

Figura 1.3 Formato de la trama PAP [5]

El campo Código, de 8 bits, indica el tipo de paquete PAP, pudiendo ser:

- *Authenticate-Request*, empleado para empezar el protocolo de autenticación de *password*.
- *Authenticate-Ack*, si el *Peer-ID/Password* recibido en el requerimiento de autenticación es reconocido o es aceptado, el autenticador enviará un paquete ACK.
- *Authenticate-Nak*, si el *Peer-ID/Password* recibido en el requerimiento de autenticación no se reconoce o no es aceptable, el autenticador enviará un

[5] http://www.faqs.org/rfcs/rfc1334.html

paquete NAK y el enlace terminará.

El campo Identificador, de 8 bits, ayuda a emparejar los requerimientos con las respuestas.

El campo Longitud, de 16 bits, indica la longitud total del paquete PAP, tanto de los campos código, identificador, longitud y campo de datos.

El campo Datos, puede tener de cero a varios octetos, su formato está dado por el campo código, es decir la estructura de este campo dependerá del tipo de parámetro del campo código.

1.2.5.7 Protocolo de Autentificación por Reto (CHAP)

El protocolo CHAP, definido en el RFC 1994, es empleado para verificar la identidad de los participantes de una comunicación punto a punto, empleando una negociación de tres vías, usualmente es empleado embebido en el protocolo PPP, como conexiones a un ISP a través de un módem.

En la Figura 1.4 se muestra el intercambio de información en el proceso de autenticación CHAP.

Este protocolo trabaja de la siguiente manera, después que la fase de establecimiento del enlace termina, el autenticador envía un reto al participante par. El participante, responde con un valor calculado empleando una función *hash* de una vía.

El autenticador revisa la respuesta comparándola con el valor calculado por el mismo empleando la misma función *hash*, si el valor coincide el autenticador responde con un *ack*, caso contrario la conexión es terminada. El reto es cambiado constantemente después de un tiempo aleatorio.

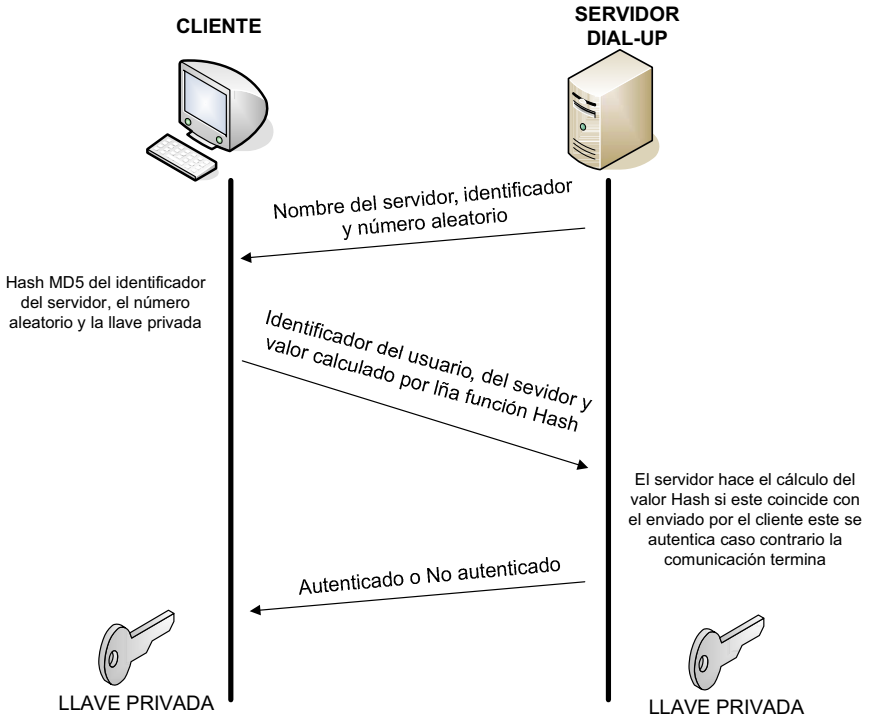

Figura 1.4 Autenticación CHAP para acceso remoto [6]

Una ventaja que se tiene con este tipo de autenticación es que las contraseñas no pueden ser grabadas y robadas para ser empleadas para un acceso posterior, pues el reto cambia constantemente el valor *hash* con el que se compara.

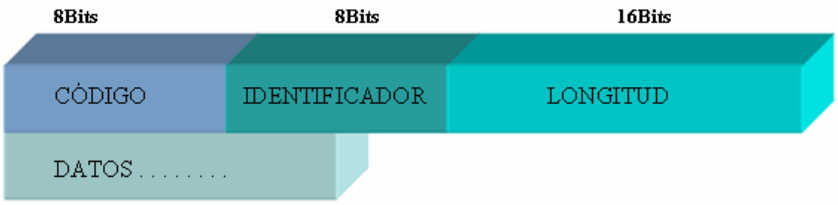

Figura 1.5 Formato de la trama CHAP [7]

En la Figura 1.5 se presenta el formato de la trama CHAP.

Otra ventaja es que el secreto solo lo conocen los extremos, éste no se

[6] Materia Seguridad en Redes, Capitulo 6 AUTENTICACIÓN Manejo de *Passwords*

[7] http://www.faqs.org/rfcs/rfc1334.html

intercambia en la autenticación.

Un problema que puede presentar este tipo de autenticación es que el secreto no se guarda en una base de datos encriptada.

El campo Código, de 8 bits, indica el tipo de paquete CHAP, pudiendo ser este campo:

- *Challenge*, empleado para empezar el protocolo de autenticación de *password*.

- *Response*, si el *Peer-ID/Password* recibido en el requerimiento de autenticación se reconocido o es aceptado, el autenticador enviará un paquete ACK.

- *Succes*, si el *Peer-ID/Password* recibido en el requerimiento de autenticación no se reconoce o no es aceptable, el autenticador enviará un paquete NAK y el enlace terminará.

- *Failure*, cuyo formato está dado por el campo código.

El campo Identificador, de 8 bits, ayuda a emparejar los requerimientos con las respuestas.

El campo Longitud, de 16 bits, indica la longitud total del paquete PAP, tanto de los campos código, identificador, longitud y campo de datos.

El campo Datos, puede tener de cero a varios octetos, su formato está dado por el campo código, es decir la estructura de este campo dependerá del tipo de parámetro del campo código.

1.2.5.8 Sistemas biométricos

Como se mencionó en el punto "1.2.1.3.2 Empleo de sistemas biométricos", los sistemas biométricos pueden ser empleados como mecanismos de autenticación, ya que el ser humano posee características que lo hacen único, como las huellas dactilares, la voz, el rostro, iris del ojo, por lo cual se puede decir que cada individuo lleva su propia palabra clave, tarjeta o número PIN.

MÉTODO DE AUTENTICACIÓN	ENVÍA *PASSWORDS*	*PASSWORDS* ENCRIPTADAS	INFORMACIÓN ENCRIPTADA	VALIDES CONTRASEÑA	REQUIEREN	VULNERABILIDAD
Autenticación basada en *passwords*	SI	SI	NO	Limitada	Algo que se conoce	Robo de contraseñas. Empleo de un humano para la administración de contraseñas
Autenticación mediante *tokens*	SI	NO	NO	Limitada	Algo que se conoce y algo que se tiene	Vulnerable solo a quien posea la tarjeta y el número secreto
Firmas digitales	NO	NO	SI	Limitada	Algo que se conoce (acuerdo entre partes)	Vulnerable al conocerse la llave pública y privada junto con el algoritmo *hash* de generación.
Certificados digitales	NO	NO	SI	Limitada	Algo que se conoce (acuerdo autoridad certificadora)	Suplantación de la autoridad certificadora
Un solo ingreso *(Single Sign-On)*	SI	SI	NO	Limitada	Algo que conoce, adicional algo que posee y algo que es	Empleo de una misma contraseña para acceder a varios servicio y aplicaciones
Protocolo de Autentificación por Contraseña (PAP)	SI	NO	NO	NO	Algo que sabe	Intercambio de contraseñas en texto plano fáciles de robar y de reproducir
Protocolo de Autentificación por Reto (CHAP).	NO	SI	NO	Limitada	Algo que conocen los extremos secreto y función *hash*	El secreto no se guardada en una base de datos encriptada
Sistemas biométricos	NO	NO	NO	Permanente	Algo que se posee	Solo vulnerable teniendo el biométrico o al portador del mismo

Tabla 1.1 Comparación de los diferentes métodos de autenticación revisados

1.2.5.9 Comparación entre los métodos de autenticación

Se ha mencionado los principales métodos de autenticación empleados en el control de acceso de usuarios hacia sistemas computacionales o sistemas electrónicos, por lo que en la Tabla 1.1 se hace una comparación de las principales ventajas y deficiencias entre los diferentes métodos.

Del cuadro comparativo se puede ver que no existe ningún método cien por ciento seguro, por lo que se debe procurar emplear en implementaciones reales métodos de autenticación fuertes, es decir que empleen una combinación de varios métodos de autenticación, lográndose de esta manera un nivel de seguridad adecuado para proteger los sistemas de comunicaciones y dificulten el acceso a intrusos maliciosos.

1.3 DESCRIPCIÓN DE LOS PROTOCOLOS UTILIZADOS Y SU RELACIÓN CON LA IMPLEMENTACIÓN

El objetivo de este trabajo es proporcionar una aplicación considerando las posibles amenazas a las que puede estar expuesto y las vulnerabilidades que el mismo pudiera presentar. Dentro del desarrollo de este trabajo se emplearán diferentes protocolos de seguridad para tratar de preservar la integridad de la información y acceso solo a usuarios autorizados a dicha información.

A continuación se realiza un estudio de los protocolos de seguridad que serán empleados dentro de la implementación.

1.3.1 PROTOCOLO RADIUS

RADIUS *(Remote Authentication Dial In User Service)* es un protocolo de control de accesos desarrollado por *Livingston Enterprises* y que la IETF ha recogido en los RFCs 2865 y 2866, diseñado y empleado para autenticar usuarios, hace uso de una arquitectura cliente/servidor.

Emplea un servidor de acceso de red *(*NAS *Network Acces Server)* como cliente RADIUS, el cliente RADIUS es el encargado de recibir las peticiones de autenticación de los usuarios y pasar esta información al servidor de autenticación, el mismo que en base a la información de usuario que reciba, indicará que servicios y configuración deberá ser aplicada a ese usuario.

El intercambio de información entre el cliente RADIUS y el servidor de autenticación RADIUS es encriptada empleando secretos compartidos, de tal manera que los secretos compartidos no son enviados sobre la red. Algo adicional que se puede emplear es encripción de las claves intercambiadas añadiendo mayor seguridad a la autenticación.

El servidor de autenticación puede soportar diferentes mecanismos de autenticación como PAP o CHAP en el caso de empleo de nombre de usuario y contraseña.

Este es un protocolo extensible, pues permite agregar nuevos valores de atributo sin perturbar aplicaciones existentes del protocolo.

1.3.1.1 Operación del protocolo

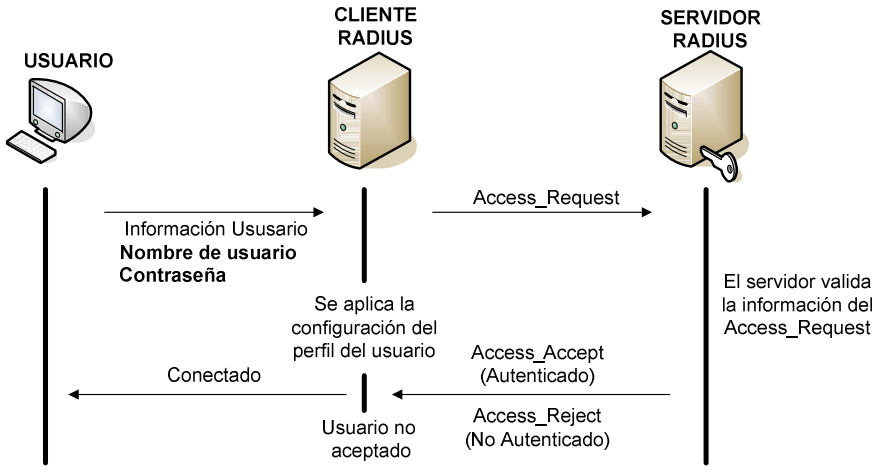

Figura 1.6 Señalización Protocolo RADIUS [8]

[8] Presentación CISCO *"Self Defending Networks"*

Cuando se tiene la configuración mencionada anteriormente, un usuario del cliente, presenta su información de autenticación al cliente, la misma que puede ser ingresada a través de una ventana de autenticación personalizada, donde el usuario debe ingresar el nombre de usuario y contraseña.

Ingresada la información, el cliente puede autenticar al usuario empleando un servidor RADIUS. El cliente crea un requerimiento de acceso *(Access-Request)* el cual contienen información como nombre de usuario, la contraseña, el identificador del cliente y el puerto al cual el cliente está accediendo. En caso que la contraseña se presente, esta es protegida empleando un método basado en RSA *Message Digest Algorithm MD5*.

Este requerimiento es enviado al servidor RADIUS, una vez que el mismo es recibido, se valida al cliente, en este caso el servidor RADIUS busca en su base de datos de nombres el usuario cuyo nombre empareja con el requerimiento. La entrada del usuario en la base de datos contiene una lista de requisitos que deben reunirse para permitir el acceso al usuario. Esto siempre incluye comprobación de la contraseña, pero también puede especificar el cliente o puerto al que el usuario tiene acceso.

Si una condición no es reunida por el usuario, el servidor RADIUS enviará un rechazo al acceso del mismo *(Acces-Reject)*, caso contrario enviará una aceptación de acceso al mismo *(Acces-Accept)* conteniendo la información necesaria requerida para brindar el servicio solicitado por el usuario.

Adicionalmente se puede emplear una autenticación reto-respuesta, esto funciona de la siguiente manera, primero al usuario se le da un número no predecible y es obligado a encriptarlo y regresar el resultado. Adicionalmente con este tipo de autenticación, los usuarios pueden emplear dispositivos o *software* que les ayude a calcular el valor que deben retornar.

Algo adicional que permite el protocolo es que se puede tener al servidor de autenticación ubicado en un lugar remoto.

1.3.1.2 Interacción con PAP y CHAP

En el caso de autenticación PAP, el NAS envía un *Acces-Request* conteniendo el identificador PAP (nombre de usuario) y la contraseña, adicionalmente el NAS puede enviar atributos adicionales que indiquen que se espera el servicio PPP.

En el caso de CHAP, el NAS genera un valor aleatorio que se envía al usuario, el cual debe retornar una respuesta CHAP conteniendo el identificador CHAP y el nombre de usuario CHAP. El NAS entonces envía un *Acces-Request* conteniendo el nombre de usuario CHAP, su identificador y la respuesta como una contraseña CHAP, adicionalmente el NAS puede enviar atributos adicionales como en PAP, que indiquen que se espera el servicio PPP.

Para validar el usuario CHAP, el servidor RADIUS busca la contraseña basado en el nombre de usuario, encripta el reto que envió al usuario con MD5 y compara el resultado con la contraseña CHAP, si los resultados son concordantes el usuario se autentica y un *Acces-Accept* es enviado, caso contrario se envía un *Acces-Reject* al cliente RADIUS.

1.3.1.3 Formato del paquete RADIUS

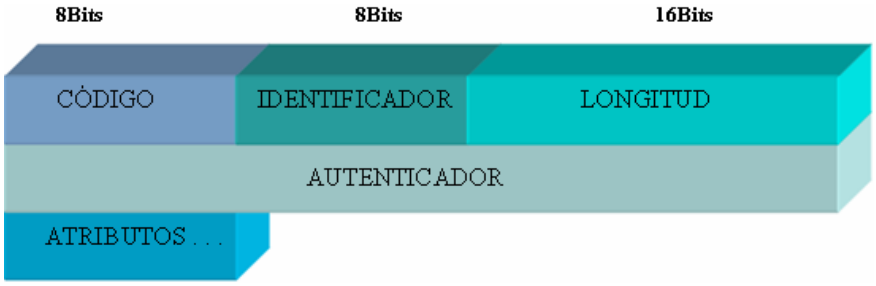

Figura 1.7 Formato del paquete RADIUS [9]

El paquete RADIUS es encapsulado dentro del campo de datos de un paquete UDP, donde el campo de puerto de destino indica 1812. Una parte del formato de

[9] http://www.untruth.org/~josh/security/radius/radius-auth.html *"An Analysis of the RADIUS Authentication Protocol"*

dicho paquete se muestra en la Figura 1.7.

El campo Código, indica el tipo de paquete RADIUS, pude tomar los siguientes valores:

- *Access-Request*, paquete enviado al servidor RADIUS que contiene información de si un usuario es permitido acceder a un NAS, y a algún servicio específico. Todo usuario que desee autenticarse deberá enviar un paquete de este tipo, es decir con el campo código en 1.

- *Access-Accept*, paquete enviado por el servidor RADIUS, y contienen la información de la configuración para que el usuario pueda hacer uso del servicio, es decir este paquete será enviado como una respuesta a un paquete "*Acces-Request*" cuyos atributos sean aceptables, el valor del campo código será 2.

- *Access-Reject*, este paquete es enviado en caso de que uno de los atributos no sea aceptado, este mensaje podrá incluir uno o varios mensajes que el NAS puede presentar al usuario, en el atributo "*Reply-Message*", el valor del campo código será 3.

- *Accounting-Request*, paquete enviado desde un cliente RADIUS a un servidor de contabilidad RADIUS, conteniendo información usada para proporcionar contabilidad de un servicio dado a un cliente, el valor del campo código será 4.

- *Accounting-Response*, paquete enviado por el servidor de contabilidad RADIUS al cliente, cuando el paquete "*Acces-Request*" ha sido recibido y copiado bien, el valor del campo código será 5.

- *Access-Challenge*, un paquete de este tipo es enviado por el servidor RADIUS cuando se desea que el usuario conteste a un reto, siendo este paquete la respuesta a un paquete "*Acces-Request*", el valor del campo

código será 11.

- *Status-Server* (experimental), el valor del campo código será 12.

- *Status-Client* (experimental), el valor del campo código será 13.

- *Reserved*, el valor del campo código será 255.

El campo Identificador, ayuda en el emparejamiento de peticiones y respuestas.

El campo Longitud, indica la longitud del paquete incluyendo los campos código, identificador, longitud, autenticador y campos de atributos. Los octetos adicionales al límite indicado por el campo longitud, son considerados como relleno y en recepción son ignorados, en caso de que el paquete sea más corto que el indicado por campo longitud, este será descartado, siendo la longitud mínima de 20 y la máxima de 4096 bytes.

El campo Autenticador, se emplea para autenticar la respuesta desde el servidor RADIUS, y es empleado en el algoritmo para ocultar las contraseñas.

- Autenticador de requerimiento, el NAS y el servidor RADIUS comparten un secreto, esa clave compartida seguida por el autenticador de requerimiento, son pasados por una función *hash* MD5 de una vía, generando un valor el cual se hace la función XOR con la contraseña ingresada por el usuario, siendo este resultado colocado en el atributo *"User-Password"* del paquete *"Access-Request"*.

- Autenticador de respuesta, el valor del campo autenticador en los paquetes *"Access-Accept"*, *"Access-Reject"* y *"Access-Challenge"* es considerado como respuesta, el mismo que es generada al aplicar una función *hash* MD5 sobre los campos código, identificador, longitud, autenticador del paquete *"Access-Request"*, atributos y el secreto compartido.

El campo Atributos, es un campo que contienen información del tipo de autenticación a emplearse, autorización, detalles de información y configuración en respuestas o requerimientos, a continuación se presenta los atributos de este protocolo con su valor numérico dentro de la trama.

En el ANEXO A se lista los atributos RADIUS.

1.3.2 IPSEC

Una Red Privada Virtual transporta de forma segura los datos por Internet a través de un túnel establecido entre dos puntos que negocian un esquema de encriptación y autentificación para el transporte, permitiendo el acceso remoto a servicios de red de forma transparente y segura, a través de un medio no seguro.

Los protocolos empleados en el establecimiento de VPNs, son *Point-to-Point Tunneling Protocol* (PPTP), *Layer Two Tunneling Protocol* (L2TP) *e Internet Protocol Security* (IPsec).

IPSec se ha convertido en el estándar criptográfico para los servicio en la capa IP, ofreciendo confidencialidad, integridad y autenticación de los extremos. IPSec esta diseñado para proporcionar interoperabilidad y seguridad basada en criptografía para IPV4 e IPv6.

IPsec puede ser empleado para proteger uno o más caminos entre un par de *hosts* o entre *routers* intermedios que implementen IPSec. Por lo que en el presente proyecto de titulación será empleado en el aseguramiento de los enlaces punto a punto entre servidores.

El concepto fundamental manejado por IPSec es la Asociación de Seguridad (SA), que es una conexión lógica unidireccional entre dos entidades IPSec y que ofrece servicios de seguridad al tráfico mantenido entre ellas.

Los servicios de seguridad son proporcionados por dos cabeceras añadidas al

nivel de IP, la *Authentication Header* (AH) y la *Encapsulation Security Payload* (ESP).

La AH ofrece integridad de las conexiones, autenticación del origen y opcionalmente servicio para contrarrestar el reenvío.

La ESP ofrece un servicio más completo, pues a parte de los servicios ofrecidos por la AH, ofrece confidencialidad.

Las cabeceras AH y ESP son medios de control de acceso, que están basados en la distribución de llaves criptográficas y la administración del tráfico intercambiado entre los *host* extremos.

Los mecanismos de seguridad IPSec se basan en que los *host* participantes tienen que hacer una negociación, para ponerse de acuerdo en el algoritmo criptográfico a emplearse y en que claves utilizar. La negociación no se realiza a nivel de capa dos, por lo que se emplea el estándar *Internet Key Exchange* (IKE) conocido también como *Internet Security Association and Key Management Protocolo* (ISAKMP/Oakley), el cual se basa primero en establecer una SA ISAKMP con la cual los extremos realizan la negociación y autenticación, y segundo se establece un SA que será empleada para la autenticación entre los extremos.

1.3.3 HTTPS (*Secure Socket Layer*)

Una de las aplicaciones más importantes para la encripción de la información en ambientes Web es *Secure Socket Layer* (SSL), que fue iniciativa y desarrollado por Netscape.

SSL proporciona seguridad en conexiones TCP, es empleado para establecer sesiones seguras entre el cliente (*browser*) y el servidor, siendo la aplicación usualmente HTTP sobre SSL o lo que es lo mismo HTTPS, SSL emplea el puerto 443.

HTTPS funciona creando un túnel seguro entre el *browser* y el servidor, la integridad de la información es mantenida empleando algoritmos *hash* y la confidencialidad de la misma empleando encripción.

La manera como se establece una sesión HTTPS es la siguiente:

- La sesión HTTPS empieza con encripción asimétrica.
- Las dos partes emplean el protocolo *Hello*, es decir intercambian números aleatorios.
- El servidor envía su llave pública junto con el certificado digital, firmado por una Autoridad Certificadora, adicionalmente el servidor también envía un identificador de sesión.
- El *browser* del cliente crea una clave secreta maestra previa.
- La clave secreta maestra previa es encriptada por el cliente, haciendo uso de la llave pública del servidor y la envía.
- Las dos partes en este momento generan la llave de sesión, empleando la clave secreta maestra previa y los números aleatorios.
- La sesión es establecida, se mantiene con encripción simétrica, ya que ésta consume menor cantidad de recursos, es decir menor *overhead*, *throughput* y uso de CPU.

1.3.4 SSH (*Secure Shell*)

Secure Shell es un programa para ingresar en un computador a través de una red, para poder ejecutar comandos desde otro computador de forma remota y poder mover archivos desde o hacia el computador remoto, siendo esta

comunicación de forma segura empleando mecanismos de autenticación a través de una red insegura.

Emplea mecanismos de encripción para proteger la integridad de la información, permitiendo redireccionar los puertos TCP/IP sobre un canal encriptado. A diferencia de rlogin o telnet, SSH encripta la sesión de registro imposibilitando que alguien pueda obtener una contraseña de texto.

No servirán de nada los intentos de falsificar la identidad de cualquiera de los dos lados de la comunicación, ya que cada paquete está cifrado por medio de una clave conocida sólo por el sistema local y el remoto.

Los clientes autentican al servidor el momento de establecer la comunicación, permitiendo controlar ataques de hombre en la mitad y de igual manera el servidor autentica al usuario antes de permitir la conexión.

La idea de emplear SSH es que sea fácil de emplear para un usuario convencional y permita crear conexiones seguras entre dos sistemas. Los problemas puntuales que soluciona SSH son, intercepción de la comunicación entre dos sistemas y personificación de un determinado *host*

Considerando las ventajas que brinda este protocolo y la seguridad que emplea tanto en el establecimiento de las comunicaciones como en el intercambio de datos en una conexión ya establecida, se consideró conveniente emplear este protocolo para la administración remota de los servidores, pues como la implementación se realiza sobre el sistema operativo LINUX, el mismo permite establecer sesiones SSH.

1.3.5 802.1X

El estándar 802.1X es un estándar IEEE para control de acceso de red basado en puerto, es decir permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o evitando el acceso por ese

puerto si la autenticación falla.

IEEE 802.1X permite implementar un acceso seguro, empleando medios de comunicación como *Ethernet*, *Token Ring* y LANs inalámbricas 802.11. Hay que tener claro que el empleo de RADIUS es opcional dentro de IEEE 802.1X, pues se espera que varios autenticadores IEEE 802.1X funcionen como un cliente y servidor de autenticación a la vez.

802.1X trabaja en capa dos del modelo OSI, para autenticación y autorización de dispositivos en *switches* LAN y puntos de acceso inalámbrico (*Wireless Access Point* WAP). Se asume un modelo punto a punto, esto indica que no es realmente proyectado para situaciones como conexiones múltiples de PCs conectadas a un *switch* vía un *hub* o un solo *switch*. Como ejemplo se puede mencionar puertos en los cuales el uso de autenticación puede ser requerida incluyendo puertos en base a su dirección MAC, y asociaciones entre estaciones y el punto de acceso en redes inalámbrica IEEE 802.11.

Cuando un nodo inalámbrico requiere tener acceso a otro recurso de una red LAN, el punto de acceso pregunta la identidad de dicho nodo, el tráfico permitido entre el nodo y el punto de acceso es EAP hasta que el nodo sea autenticado.

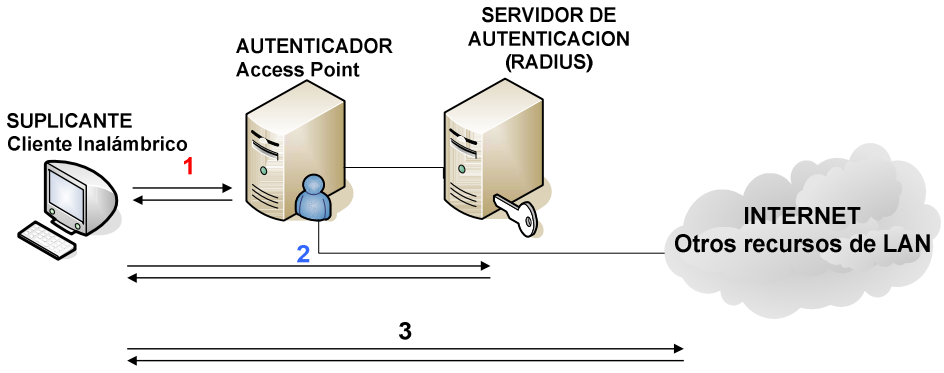

Figura 1.8 Proceso de autenticación con RADIUS [10]

El estándar 802.1X se une con el protocolo de seguridad EAP (*Extensible*

[10] http://tldp.org/HOWTO/html_single/8021X-HOWTO/#AAA *"802.1X Port-Based Authentication*

Authentication Protocol) empleado tanto en redes cableadas como inalámbricas. EAP al ser un protocolo de autenticación genérico, puede trabajar con muchos tipos de mecanismos de autenticación, por ejemplo, EAP puede autenticar un usuario basado en un nombre y contraseña, empleando certificado digital, empleando *ticket* kerberos o la información contenida en un impreso SIM (*Subscriber Identity Module*).

En redes inalámbricas, EAP ha reemplazado otros mecanismos de autenticación de capa dos, como PAP y CHAP. Las estaciones empleando 802.1X/EAP deberán autenticarse y asociarse al punto de acceso previo realizar la autenticación y asociación con 802.1X/EAP.

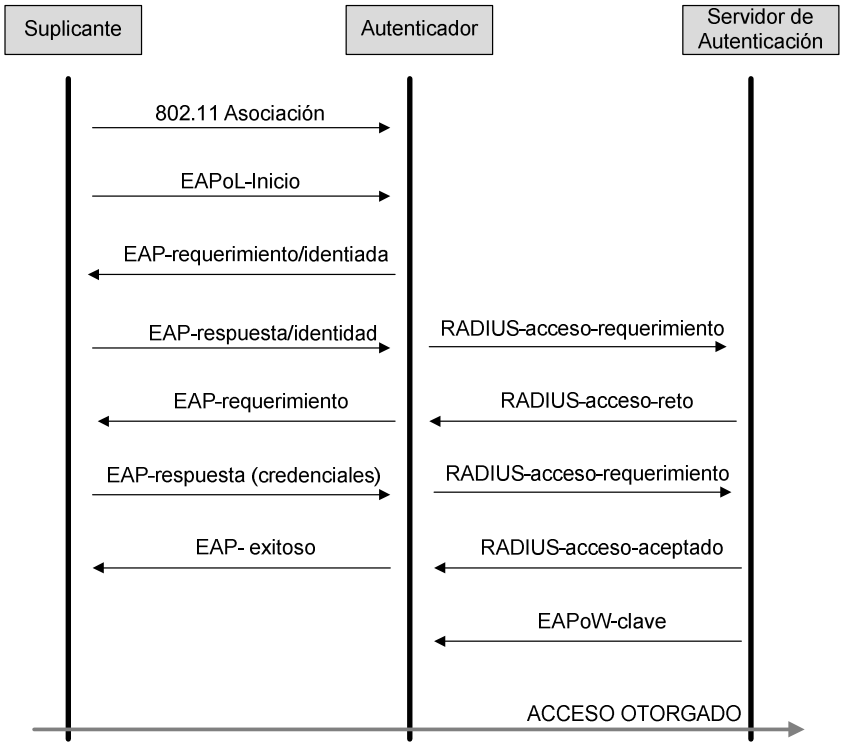

Figura 1.9 Estructura de Autenticación 802.1X/EAP[11]

El proceso de autenticación 802.1X/EAP, consiste de tres piezas importantes, un suplicante, un autenticador y un servidor de autenticación. El suplicante es el

[11] CWNA Official Study Guide Third Edition "802.1X/EAP Framework"

dispositivo que solicita acceso a la red generalmente el usuario. El autenticador es un dispositivo intermediario que pasa las tramas desde el usuario al servidor de autenticación, generalmente el punto de acceso inalámbrico. El autenticador que es el dispositivo que actualmente autentica el usuario, generalmente el servidor RADIUS. La Figura 1.9 presenta el proceso de autenticación de forma detallada.

Primero el suplicante indica que desea realizar una autenticación EAP enviando una trama EAPoL-Inicio hacia el autenticador. El autenticador envía una trama EAP-requerimiento/identidad, solicitando al suplicante que provea algunos campos de información de identidad. La información específica depende del tipo de EAP que está siendo usado, por mencionar algunos, en EAP-MD5 será el nombre de usuario, mientras que en EAP-TLS la información requerida será un certificado digital.

El siguiente paso es que una serie de tramas sean intercambiadas entre el suplicante y el servidor de autenticación, en este punto el autenticador solo actúa como un reenviador de tramas entre estos dos. Las tramas realizan el proceso de autenticación del usuario, y los datos llevados son específicos al tipo de EAP que está siendo usado.

Si la autenticación es exitosa, una trama EAP-exitoso es enviada al suplicante. En caso de que el tipo de EAP soporte asignación de llaves de encripción dinámica, el siguiente paso para el suplicante y el servidor de autenticación es deducir la llave de encripción. Ellos realizan esta tarea en base a la información intercambiada en el proceso de autenticación, o basada en la información que es preconfigurada en las dos estaciones. Posterior a esto el suplicante y el servidor de autenticación conocen la llave de encripción que el suplicante usará, pero el autenticador no la conoce.

El punto de acceso solo conocerá la llave de encripción del usuario ya que con esta enviará mensajes al usuario. El servidor de autenticación entregará la llave de encripción al autenticador en un campo atributo de la trama RADIUS, el cual se encripta usando la clave secreta que es conocida por el servidor RADIUS y el

punto de acceso. En este momento la llave de encripción es conocida por las tres piezas del modelo 802.1X/EAP y la comunicación puede comenzar.

WPA (*Wi-Fi Protected Access*) es un estándar de seguridad de redes inalámbricas que incluye TKIP (*Temporal Key Integrity Protocol*) y 802.1X con autenticación EAP. El estándar WPA define dos tipos de autenticación y administración de claves, ambos tipos emplean 802.1X/EAP para autenticar la estación, pero el primer tipo conocido como WPA requiere el uso de un servidor RADIUS, mientras que el segundo WPA-PSK (*Pre-Shared Key*) no requiere de RADIUS.

En el caso de WPA empleando RADIUS la autenticación se realiza exactamente igual que 802.1X/EAP.

En el caso de WPA-PSK, una cadena ASCII es configurada en todos los puntos de acceso y estaciones, y esta cadena es usada para autenticar las estaciones. La PSK no es empleada en la encripción de las tramas, esta es empleada en la negociación para establecer la clave WEP dinámicamente a cada estación.

WPA-PSK no es tan segura como WPA empleando RADIUS, pero si es más segura que WEP.

A continuación se presenta algunos mecanismos de autenticación EAP, con una breve descripción de cada uno.

- EAP-MD5, *MD5-Challenge* requiere nombre de usuario y contraseña, es equivalente a CHAP, poco empleado en autenticación en ambientes inalámbricos.

- *Lightweight* EAP (LEAP), envía un nombre de usuario y contraseña al servidor de autenticación, es protocolo propietario desarrollado por CISCO y es considerado no seguro por lo que se esta dejando fuera LEAP para emplear PEAP.

- EAP-TLS (*EAP – Transport Level Security*), crea una sesión TLS dentro de EAP, entre el suplicante y el servidor de autenticación, siendo necesario en el servidor y el cliente un certificado digital y una infraestructura PKI, esta autenticación es bidireccional. Asumiendo que se empleen procedimientos adecuados de mantenimiento de los certificados, EAP-TLS es una de las formas más seguras de EAP, pero también es la que conlleva mayores requerimientos de mantenimiento.

  Hay que considerar que en ambientes donde se va ha realizar cambios constantes en la red inalámbrica no sería aplicable este método pues hay que instalar certificados tanto en el cliente como en el servidor para poder ser autenticado.

- EAP-TTLS (*EAP Tunneled TLS*), se establece un túnel encriptado TLS para transporte de datos de autenticación, dentro de este túnel TLS otros métodos de autenticación se pueden emplear.

- *Protected* EAP (PEAP), emplea como EAP-TLS un túnel encriptado TLS, los certificados de suplicante para EAP-TTLS y EAP-PEAP son opcionales, pero los certificados del servidor de autenticación son necesarios.

- EAP-MSCHAPv2, requiere un nombre de usuario y contraseña, y en resumen es encapsulamiento EAP de MS-CHAP-v2.

1.4 CONTROL DE ANCHO DE BANDA

En los últimos años la gran evolución de las redes de información considerando tanto los usuarios conectados a ellas, los tipos de aplicaciones y los servicios que en ellas se emplean; ha traído consigo problemáticas en el rendimiento de las mismas.

Para remediar estas problemáticas se ha introducido el concepto de Calidad de

Servicio (*QoS*), mediante el empleo de métodos y tecnologías que permitan un mejor aprovechamiento de los recursos finitos de las redes, como el empleo de mecanismos de encolamiento en los equipos de comunicaciones.

Mediante el empleo de mecanismos de encolamiento se determina la manera en que se van ha enviar los datos, ya que los datos que pueden ser modelados en una cola son solo aquellos que se transmiten.

Considerando el siguiente ejemplo:

Si se tiene un *router* y se desea evitar que ciertos computadores dentro de la red descarguen información rápidamente, es necesario realizar un control del ancho de banda en la interfaz interna del *router*, desde la cual se envía los datos a los computadores. Si el *router* dispone de dos interfaces con diferentes velocidades, generándose un cuello de botella, se debe asegurar que no se envía más datos de los que el *router* puede manejar; el *router* será el encargado de controlar el enlace y ajustar el ancho de banda disponible.

En este caso se hace necesario el empleo de un mecanismo de encolamiento que modele la información que esta siendo enviada por el *router.*

A continuación se describe el funcionamiento de algunos de los diferentes tipos de encolamiento que se puede encontrar en el sistema operativo LINUX:

1.4.1 DISCIPLINAS DE COLAS SIMPLES

El objetivo de una disciplina de cola es cambiar el modo en que se envían los datos. Las disciplinas de cola sin clases son aquellas que aceptan datos y se limitan a reordenarlos, retrasarlos, o descartarlos.

A continuación se revisará las disciplinas de colas simples más empleadas:

1.4.1.1 Pfifo-fast (FIFO)

Maneja el algoritmo *FIFO First In, First Out* (el primero que entra es el primero que sale) e indica que ningún paquete recibe un tratamiento especial; esta compuesta por 3 bandas, dentro de cada banda, se aplican las reglas FIFO.

Cada banda tiene distinta prioridad siendo la banda 0 la de mayor prioridad y la banda 2 la de menor prioridad, es decir, los paquetes son decolados primero en la banda 0 luego la 1 y finalmente en la banda 2.

Para determinar la banda a la que será enviado un paquete, es decir, su prioridad esta disciplina de encolamiento se basa en el campo ToS (*Type of Service*) del paquete IP.

1.4.1.2 *Token Bucket Filter* (TBF)

Es una disciplina de cola sencilla que se limita a dejar pasar paquetes que lleguen a una tasa que no exceda un valor impuesto administrativamente, pero con la posibilidad de permitir ráfagas cortas que excedan esta tasa.

TBF consiste en un búfer (el *bucket* o balde), que se llena constantemente con piezas de información denominadas *tokens*, a una velocidad específica (*token rate*). El parámetro más importante del *bucket* es su tamaño, que es el número de *tokens* que puede almacenar.

Cada *token* que llega toma un paquete de datos entrante de la cola de datos y se elimina del *bucket*. Asociar este algoritmo con los dos flujos (*tokens* y *datos*), da tres posibles situaciones:

1. Los datos llegan a TBF a una tasa que es igual a la de *tokens* entrantes. Cada paquete entrante tiene su *token* correspondiente y pasa a la cola sin retrasos.

2. Los datos llegan al TBF a una tasa menor a la de los *token*, por lo que sólo una parte de los *tokens* se borran con la salida de cada paquete que se envía fuera de la cola, acumulándose los *tokens*, hasta llenar el *bucket*. Los *tokens* sin emplear podrán ser usados para enviar datos a velocidades mayores de la tasa de *tokens*, produciéndose en cuyo caso una corta ráfaga de datos.

3. Los datos llegan al TBF a una tasa mayor a la de los *tokens*. Esto significa que el *bucket* se quedará pronto sin *tokens*, causando que TBF se acelere a sí mismo por un intervalo de tiempo.

La acumulación de *token*s permite ráfagas cortas de datos, mientras que cualquier sobrecarga causará que los paquetes se vayan retrasando constantemente, y al final sean descartados.

1.4.1.3 *Stochastic Fairness Queueing* (SFQ)

En este tipo de cola, el tráfico se divide en un número bastante grande de colas *FIFO*, una por cada conversación, enviando el tráfico de una manera parecida a *round robin* dando a cada sesión por turnos la oportunidad de enviar datos.

Su comportamiento es bastante equitativo y evita que una única conversación ahogue a las demás. *SFQ* sólo es útil en caso de que la interfaz real de salida esté realmente saturada.

1.4.2 DISCIPLINAS DE COLAS CON CLASES

Este tipo de colas se emplea cuando se tienen diferentes tipos de tráfico a los que se requiere dar un tratamiento separado.

1.4.2.1 FUNCIONAMIENTO DE LAS DISCIPLINAS DE COLAS CON CLASES

Las disciplinas de colas clasifican el tráfico que ingresa a una clase en particular

de la disciplina de colas, para lo cual emplean un mecanismo de clasificación, el cual consiste en emplear filtros que son llamados desde la disciplina de colas, para determinar a que clase se debe enviar los paquetes, esta clase a su vez, puede emplear filtros adicionales para generar subclases.

Las disciplinas de colas con clases emplean manipuladores (*handle*), para poder identificar el trayecto a seguir por el paquete, por ejemplo, en la Figura 1.10 tenemos varios niveles jerárquicos, con los cuales se establece el camino a seguir.

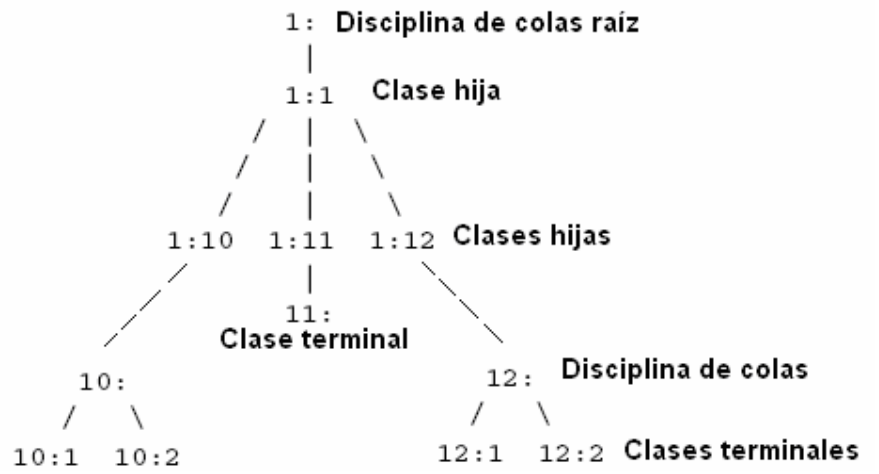

Figura 1.10 Disciplinas de colas con clases [12]

Los paquetes pueden clasificarse en una cadena como ésta:

1: ---------- 1:1 ------- 1:12 --------- 12: --------- 12:2

En este ejemplo el paquete reside en una cola de una disciplina de colas asociada a la clase 12:2, empleándose un filtro en cada nodo del árbol, y cada cual escoge qué rama se toma en su paso.

Otra alternativa es el disponer de algo como lo siguiente:

1: --------- 12:2

[12] Fuente: http://lartc.org/

Esto será posible hacer, pues se empleará un filtro que decida enviar el paquete directo a 12:2

A continuación se revisará las disciplinas de colas con clases generalmente utilizadas.

1.4.2.2 DISCIPLINA DE COLAS PRIO

Este tipo de cola lo que hace es subdividir el tráfico en función de cómo se hayan configurado los filtros. Cuando se encola un paquete a la disciplina de colas PRIO, se escoge una clase basándose en las órdenes de filtrado que haya dado. Por defecto, se crean tres clases, las mimas que contienen disciplinas de colas FIFO sin estructura interna, pero se las puede sustituir por cualquier otra disciplina de colas disponible.

1.4.2.3 DISCIPLINA DE COLA CBQ *(Class Based Queueing)*

Empleada en aplicaciones donde existe diferentes tipos de tráficos a los cuales se les quiere dar un tratamiento diferente, es la disciplina de colas más compleja, y probablemente la más difícil de configurar correctamente.

Sus aplicaciones y uso son muy similares a HTB, pero desde su aparición CBQ es muy poco utilizada, ya que conlleva una gran complejidad de implementación hasta en las configuraciones más sencillas. HTB es más fácil de configurar y mas eficiente, por lo que CBQ no será empleada para la implementación del cliente RADIUS.

1.4.2.4 DISCIPLINA DE COLAS HTB (*Hierarchical Token Bucket*)

La disciplina de encolamiento HTB reemplaza a la *qdisc* CBQ que es muy compleja y no es la más recomendable para muchas situaciones. La *qdisc* HTB es empleada para configuraciones donde se requiere dividir un ancho de banda fijo

para diferentes propósitos, o para diferentes usuarios, dando a cada propósito o usuario un ancho de banda especifico, y adicionalmente determinar cuanto ancho de banda pude tomar prestado (*borrow*).

Para su configuración HTB tienen muy pocos parámetros y para situaciones complejas, la configuración escala bien, a diferencia de CBQ que incluso para los casos más simples su configuración es compleja.

Para la implementación del cliente RADIUS se utilizará esta disciplina de colas, por ser la que mas se ajusta al propósito que es el subdividir el ancho de banda disponible del enlace en un ancho de banda fijo para cada uno de los perfiles de usuario. Además por lo sencilla que resulta su configuración.

A continuación se presenta una descripción los parámetros de HTB:

- ***rate*****,** parámetro que fija la mínima velocidad a la cual se limita la transmisión del tráfico en una clase. Puede ser considerado como un valor equivalente al *CIR* (*Committed Information Rate* - Tasa de Información Comprometida) de *Frame Relay* o como el ancho de banda garantizado para una clase hija.

- ***ceil*****,** argumento que especifica el máximo ancho de banda que la clase puede usar. Limita el ancho de banda que puede pedir prestado a otra clase, por defecto tiene el mismo valor de *rate*.

  Este parámetro puede ser útil al emplearse por ejemplo en un ISP (*Internet Service Provider*) cuando se requiera limitar el ancho de banda del que puede disponer un cliente cuando otros no lo estén utilizando, de esta forma el cliente no usara un ancho de banda por el que no este pagando.

  Una clase *root* no puede pedir prestado (*borrow*), por los cual para esta no es necesario indicar el parámetro *ceil*.

Nota: El parámetro *ceil* para una clase debe ser siempre mayor al parámetro *rate*, También el parámetro *ceil* para un clase deberá siempre ser mayor al *ceil* de cualquiera de sus clases hijas.

- ***burst*,** parámetro que permite a la clase enviar por un pequeño período, tantos paquetes como permita el enlace. Esto puede ser útil por ejemplo para una clase que manipule tráfico http. Si se tiene una clase de 10 kbps y un *burst* de 50kb, cargara pequeñas páginas web muy rápido, después de 50kb, el *burst* es utilizado y la tasa volverá a 10 kbps.

- **default**, clase por defecto empleada cuando el paquete no fue clasificado por ninguno de los filtros, Si se utiliza XX:0 como clase por defecto, todos los paquetes sin clasificar irán directamente a esta clase, lo que significa que no existe limite para la tasa de los paquetes no clasificados.

- **prio**, indica la prioridad de una clase determinando a que paquetes se debe atender primero. Por defecto toma el valor de 0 que define máxima prioridad.

El objetivo de este proyecto es conseguir un uso eficiente del ancho de banda de acuerdo a los requerimientos de los usuarios, limitando el uso del ancho de banda existente por perfil de usuarios.

La disciplina de colas que más se ajusta al propósito de este proyecto es *Hierarchical Token Bucket* (HTB) por las siguientes razones:

- La sencillez que ofrece la configuración de sus parámetros.
- La eficiencia que ofrece este mecanismo al poderlo configurar con unas pocas líneas de código, empleando menos recursos de hardware.
- Permite crear un número de clases hijas para distribuir el ancho de banda según se requiera.

CAPÍTULO II

CONFIGURACIÓN DEL SERVIDOR RADIUS E IMPLEMENTACIÓN DEL CLIENTE RADIUS

CAPÍTULO II

CONFIGURACIÓN DEL SERVIDOR RADIUS E IMPLEMENTACIÓN DEL CLIENTE RADIUS

2.1 DESCRIPCIÓN DE LA PROBLEMÁTICA EXISTENTE

En la actualidad la comunicación es una herramienta muy importante en el mundo empresarial y comercial, pues a través de ella se ha podido tener acceso a recursos ubicados remotamente, sean estos recursos de hardware o información.

Bajo esta perspectiva es importante incluir controles de acceso de que recursos son permitidos y que individuo tendrá los privilegios suficientes para emplearlos. Como ejemplo se puede mencionar la comunicación telefónica IP dentro de un ambiente corporativo, donde solo las gerencias podrán disponer del permiso de acceder a llamadas a lugares remotos a través de un enlace WAN, es decir solo la o las personas que dispongan de los privilegios suficientes podrán hacer uso del recurso enlace WAN y podrán emplear la infraestructura telefónica para poder establecer una comunicación con el lugar remoto, por lo cual se vuelve una necesidad establecer políticas de uso y mecanismos de restricción para que se cumpla lo anteriormente mencionado.

De igual manera se puede tener un registro de la ocupación de los sistemas de comunicación que involucran recursos de la red (*hardware*, *software* o información), ya que en la actualidad las empresas han ido tomando conciencia que la protección de la información y el empleo ordenado y moderado de sus recursos de red, les representarán un gran ahorro a mediano o largo plazo.

La problemática identificada es tratar de disponer de sistemas que permitan realizar un acceso controlado de forma segura hacia los recursos de un sistema de comunicaciones IP, y que a su vez permitan realizar una auditoria de la utilización del sistema. Algo importante a considerar es que se debe disponer de

sistemas modulares, es decir que permitan realizar cambios sin que esto represente una reestructuración de todo el sistema.

El presente proyecto de titulación trata de suplir los requerimientos anteriormente mencionados dentro de un ambiente corporativo o comercial. Se trata de crear una aplicación de *software* que se encargue de realizar un control de acceso de forma segura de los recursos de red, que lleve un registro de la ocupación del sistema, que sea una solución modular y permita controlar la utilización de ancho de banda.

El *software* tendrá la capacidad de realizar un control de acceso al servicio Internet a través del empleo de una página de autenticación, posterior a lo cual se podrá realizar la asignación de un perfil en función del usuario que se haya autenticado, con la finalidad de asignar una ancho de banda controlado a dicho usuario; con todo esto se logra un ahorro del recurso ancho de banda. Adicionalmente se dispone de información, como la ocupación del sistema que será registrada para llevar un control organizado y saber de forma real como los usuarios están empleando el sistema.

2.2 ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD A SER IMPLEMENTADAS

Se definirá un grupo de políticas de seguridad para la implementación del cliente RADIUS, las mismas que brindarán protección a la información considerada confidencial, como son las claves de los usuarios que serán intercambiadas entre el usuario y el cliente RADIUS y posteriormente entre el cliente RADIUS y el servidor RADIUS.

También se implementarán políticas para que cada usuario emplee adecuadamente el sistema; se proporcionarán mecanismos de control de ancho de banda y se crearán perfiles en los cuales se definirá a que el usuario tiene

permiso de acceder, de esta manera se busca mitigar el riesgo de accesos no autorizados a los recursos de red.

Se definirán políticas para la generación y utilización de las claves empleadas en los procesos de autenticación.

Se definirán políticas de los requisitos mínimos que deben cumplir el sitio en el cual se instale el sistema de control de acceso.

2.2.1 POLÍTICAS A SER IMPLEMENTADAS

Se ha considerado establecer las siguientes políticas de seguridad que permitirán un uso apropiado del sistema; estas políticas serán aplicables a todos los usuarios y equipos que requieran utilizar el sistema.

1. Condiciones del cuarto de equipos.
2. Sistemas de respaldo de energía eléctrica.
3. Sistemas de control de incendios.
4. Control de acceso mediante dirección MAC en el cliente RADIUS.
5. Filtros de direcciones MAC en puntos de acceso inalámbricos.
6. Autorización de acceso a usuarios con dirección IP configurada de forma estática.
7. Empleo de nombre de usuario y clave de acceso segura para la autenticación de usuarios.
8. Definir diferentes perfiles de acceso para los usuarios.
9. Protección de la información que viaja por el segmento de red inalámbrico.
10. Protección de la información de autenticación que el usuario envía al cliente RADIUS.
11. Protección de la información de autenticación que el cliente RADIUS, envía al servidor RADIUS.
12. Registro del tiempo de conexión y el consumo medido en *bytes* que realice el usuario.

A continuación se describe en detalle cada una de las políticas de seguridad a implementarse:

2.2.1.1 Condiciones del cuarto de equipos

El cuarto de equipos deberá proporcionar las condiciones adecuadas para la instalación de los equipos, es decir proporcionar sistemas de control de temperatura como sistemas de aire acondicionado, una adecuada instalación eléctrica y seguridad física adecuada para el acceso hacia el cuarto de equipos.

2.2.1.2 Sistema de respaldo de energía eléctrica

Se deberá proporcionar sistemas de respaldo de energía eléctrica de tal manera que si se suscitara un corte de energía se pueda apagar de forma adecuada los sistemas de comunicaciones, evitando daños por cortes eléctricos abruptos.

2.2.1.3 Sistema de control de incendios

El sistema de control de incendios a ser implementado, deberá emplear elementos químicos que no afecten los sistemas de comunicaciones.

Deberá proporcionar de señales tanto visuales como sonoras de algún evento de combustión detectado.

Deberá proporcionar sistemas de evacuación de emergencia y mecanismos de retardo en la expulsión de los químicos, en caso de que algún operario quede atrapado en el cuarto de equipos.

2.2.1.4 Control de acceso mediante dirección MAC en el cliente RADIUS

El usuario para acceder a cualquier servicio de la red (Internet) debe tener asignada una dirección IP válida, la cual será otorgada por el servidor DHCP

configurado en el cliente RADIUS, para ello el usuario debe configurar su computador como cliente DHCP.

Para evitar accesos no autorizado a la red, el servidor DHCP estará configurado para otorgar una dirección IP únicamente a los usuarios cuya dirección MAC haya sido previamente registrada en un listado de direcciones MAC autorizadas. Se podrá registrar, modificar y eliminar la dirección MAC de los usuarios en el listado mediante el uso de la interfaz de administración.

Al momento de registrar las direcciones MAC será posible también indicar una dirección IP fija para cada dirección MAC; si no se indica ninguna, el sistema asignará al usuario una dirección IP disponible del rango que se haya definido en la configuración del servidor DHCP.

2.2.1.5 Filtros de direcciones MAC en puntos de acceso inalámbricos

Con el propósito de evitar que usuarios no autorizados hagan uso indebido del sistema, se va ha configurar en los puntos de acceso inalámbricos (AP) un filtro de direcciones MAC de tal forma que únicamente lo usuarios autorizados puedan hacer uso del segmento de red inalámbrico.

Para conseguir esto se requiere que el equipo a emplearse sea compatible con esta funcionalidad.

2.2.1.6 Autorización de acceso a usuarios con dirección IP configurada de forma estática

Una vulnerabilidad identificada durante el proceso de implementación fue que cuando se configuraba una dirección IP perteneciente al segmento de red de los usuarios, de forma estática en un computador, era posible el acceso a la página de autenticación del cliente RADIUS.

Para evitar que esto suceda fue necesario, permitir el acceso a usuarios que hayan configurado su dirección IP de forma estática, únicamente si su dirección MAC fue previamente registrada en el sistema.

2.2.1.7 Empleo de nombre de usuario y clave de acceso segura para la autenticación de usuarios

Una vez que el usuario disponga de una dirección IP, podrá acceder al sistema de autenticación.

El sistema de autenticación solicitará que se ingresen un “nombre de usuario” y una “clave”, a estos dos parámetros estará asociado un perfil que será asignado de acuerdo a los requerimientos y/o necesidades del usuario.

El nombre de usuario será asignado por el administrador del sistema; una vez que el usuario haya solicitado el servicio.

Para la creación del nombre de usuario se considerará utilizar la primera letra del primer nombre del usuario seguido de su apellido, en caso de no encontrarse disponible este nombre de usuario se deja a consideración del administrador alguna otra combinación (p.e. emplear la primera letra de los dos nombres seguidas del apellido).

Para garantizar que la clave de acceso de usuario sea segura, ésta deberá ser de al menos ocho caracteres alfanuméricos, de los cuales al menos tres y no más de cinco serán números.

Para la creación de la cuenta y asignación de un “nombre de usuario” y “clave”, el usuario deberá indicar la siguiente información que será empleada para la creación de la cuenta de usuario en el servidor RADIUS:

Primeramente la información general del usuario que se lista a continuación:

- Nombre de usuarios (*Username*)
- Clave (*Password*)
- Grupo (*Group*)
- Nombre compuesto por el nombre y seudónimo [*Name* (*First Name Surname*)]
- Correo (*Mail*)
- Departamento (*Department*)
- Teléfono de casa (*Home Phone*)
- Teléfono del trabajo (*Work Phone*)
- Teléfono móvil (*Mobile Phone*)

Además se debe configurar la información que será intercambiada en el *Access-Accept*, enviado por el servidor RADIUS, misma que se lista a continuación.

- Protocolo (*Protocol*), que puede ser PPP, L2TP o IP; este campo no se empleará en la implementación.
- Dirección IP (IP *Address*), corresponde al campo de la dirección IP del usuario.
- Máscara de red de la dirección IP (IP *Netmask*), corresponde a la máscara de red empleada para el usuario.
- Tramado MTU (*Framed*-MTU), corresponde al tamaño de la trama el valor por defecto empleado en el campo es de 1500
- Compresión usada (*Compression Used*), el valor por defecto es *Van-Jacobson-TCP-IP*, este campo no se lo emplea en la implementación.
- Tipo de servicio (*Service Type*), campo que se empleará para enviar la información de perfil.
- Duración de la sesión (*Session Timeout*), campo empleado para indicar el tiempo máximo de duración de una sesión del usuario.
- Tiempo máximo de inactividad (*Idle Timeout*), campo empleado para indicar el período de tiempo en el cual se considerará un usuario como inactivo.
- Número máximo de sesiones (*Port Limit*), por política de utilización el número máximo de sesiones por usuario será de una sesión.

- Mensaje presentado (*Lock Message*), campo opcional de tipo descriptivo.

Por defecto si el usuario no se ha autenticado y desea acceder a una dirección web externa a la red a través de su navegador, en lugar de la dirección solicitada se le mostrará una página de autenticación alojada en el cliente RADIUS, en esta página se le solicitará ingresar el "nombre de usuario" y la "clave" que le fueron asignados. Una vez ingresada esta información se enviará una petición de *Access-Request* al servidor RADIUS, y dependiendo del resultado que el servidor RADIUS envié en respuesta a esta petición el usuario será aceptado o rechazado.

Si la respuesta es un *Access-Reject* se le mostrará al usuario una página de error y se le solicitará ingresar nuevamente el "nombre de usuario" y la "clave".

Si la respuesta del servidor RADIUS es un *Access-Accept* en el cliente RADIUS se crearán las reglas apropiadas que permitirán al usuario utilizar al cliente como *gateway* para el acceso a Internet y se ejecutarán un conjunto de comandos dependiendo del perfil asociado al usuario, los cuales permitirán el acceso hacia el Internet según su perfil; restringiendo y/o permitiéndole acceso a los servicios y controlando el uso del ancho de banda.

El sistema se ha diseñado para permitir una sola sesión simultanea por usuario, por lo cual si otro usuario intenta hacer uso del sistema con un "nombre de usuario" y "clave" que en ese momento estén siendo empleados, se le presentará un error indicando la dirección IP y la dirección MAC del usuario que se encuentra empleando las credenciales ingresadas y solicitando que se envíe esta información al administrador de red.

2.2.1.8 Definir diferentes perfiles de acceso para los usuarios

En el sistema se establecerán distintas categorías de usuarios en función de las actividades que el usuario realizará.

A cada perfil estará asociado un conjunto de reglas que permitirán al usuario realizar únicamente peticiones a ciertos puertos, dependiendo del perfil asignado a cada usuario del sistema se le asignarán los permisos correspondientes.

Todos los perfiles tendrán acceso al puerto http (80) y https (443) del cliente RADIUS, ya que el sistema empleará estos dos puertos para realizar la negociación de intercambio de credenciales, entre el usuario y el cliente RADIUS, credenciales que posteriormente serán enviadas al servidor RADIUS.

Por defecto se definirán tres perfiles, según el perfil asociado el usuario podrá acceder únicamente a cierto tipo de protocolos y/o aplicaciones como se describe a continuación:

- Acceso Total: Podrá utilizar todos los servicios disponibles en la red.
- Acceso Restringido: Se le permitirá acceso http, smtp, pop3 y ftp.
- Invitado: Solo tendrá acceso http.

Para el caso de usuarios que no pertenezcan a ninguno de los perfiles no tendrán acceso a ninguno de los servicios de la red.

El administrador del sistema podrá hacer uso de la interfaz de administración del cliente RADIUS para la creación y/o modificación de los perfiles de usuario existentes; esta interfaz permitirá asignar un nivel de acceso a la red diferente a cada grupo de usuarios pertenecientes a un determinado perfil, así como también limitar el uso del ancho de banda disponible.

El paso de trafico DNS hacia el Internet estará permitido para todos los usuarios, de esta forma se permitirá al usuario emplear el servidor DNS de su elección, en caso que no desee emplear el servidor DNS que se configura vía DHCP.

2.2.1.9 Protección de la información que viaja por el segmento de red inalámbrico

La información de los usuarios que se conecten por medio inalámbrico viajará encriptada, para prevenir cualquier tipo de ataque que se pueda dar en este segmento de la red.

Para proteger la confidencialidad de la información, se podrá emplear mecanismos de encripción de información utilizados en comunicación inalámbrica como por ejemplo: WEP, TKIP, 802.1X/EAP, WPA y WPA2/802.11i. El mecanismo de encripción empleado en la implementación se lo detalla en la sección “2.9”.

2.2.1.10 Protección de la información de autenticación que el usuario envía al cliente RADIUS

Será un requisito obligatorio el emplear un mecanismo de encripción en el intercambio de información confidencial como son nombres de usuario y clave. Por lo cual en la implementación se considerará emplear https con el objetivo de proteger la confidencialidad de la información importante intercambiada con el sistema de autenticación del cliente RADIUS. Es decir, la información que envíe el usuario viajará encriptada mediante el uso de Certificados Digitales.

El sistema de autenticación deberá presentar de forma automática la página de autenticación empleando https, de tal manera que para el usuario sea transparente la utilización de encripción.

2.2.1.11 Protección de la información de autenticación que el cliente RADIUS, envía al servidor RADIUS

La información intercambiada entre el cliente RADIUS y el servidor RADIUS deberá ser ecriptada, ya que esta información corresponde a datos confidenciales de los usuarios.

Con el objetivo de encriptar la información que se intercambia entre el cliente y el servidor RADIUS, se ha decidido levantar un túnel IPSec entre esos dos servidores, de tal manera que la información intercambiada sea únicamente comprendida entre estos dos participantes.

2.2.1.12 Registro del tiempo de conexión y el consumo medido en *bytes* que realice el usuario

El tiempo de conexión en segundos y la cantidad de información que el usuario intercambie en *bytes* serán registrados en una base de datos, para poder tarifar la utilización del sistema.

Con el fin de registrar la utilización del sistema se definió un mecanismo automático, que permita ir actualizando el tiempo de conexión y los *bytes* consumidos en la base de datos.

El sistema debe determinar de forma automática, si un usuario se encuentra o no en actividad, esto se lo realiza mediante la comparación del consumo acumulado medido cinco segundos antes con el consumo acumulado hasta ese instante; en caso que no se registre consumo del usuario por un tiempo mayor al tiempo máximo de inactividad configurado (*Idle Timeout*), el sistema finalizara la sesión actual del usuario y procederá a aplicar las restricciones de acceso correspondientes.

2.3 REQUERIMIENTOS DE HARDWARE

Para determinar los requerimientos de *hardware* tanto del cliente como del servidor RADIUS se han considerado las características de *hardware* para la instalación del S.O Linux Fedora Core 3, adicionalmente se ha considerado las aplicaciones que se van a ejecutar en cada uno de los equipos para determinar características adicionales para los mismos.

A continuación se indica los requerimientos del sistema operativo Fedora Core 3 que fueron tomados de las especificaciones técnicas de la referencia[1]:

Procesador

Mínimo: Procesador Intel tipo Pentium, superiores o compatibles
Recomendado para modo texto: Pentium 200 MHz o superior
Recomendado para modo gráfico: Pentium II 400 MHz o superior

Espacio en disco duro

NOTA: Considere espacio adicional para sus archivos personales
Instalación Personalizada (Mínima): 520MB
Servidor: 870MB
Escritorio Personal: 1.9GB
Estación de Trabajo: 2.4GB
Instalación Personalizada (Todo): 5.3GB

Memoria

Mínima para modo Texto: 64MB
Mínima para modo Gráfico: 192MB, recomendada: 256MB

2.3.1 SERVIDOR RADIUS

Con los requerimientos recomendados para el S.O. en cuanto a Procesador y Memoria será suficiente para este servidor, puesto que no es necesario levantar la interfaz gráfica, y su administración se puede realizar desde la línea de comandos y desde la interfaz web que proporciona el servidor RADIUS que se va a instalar.

Se debe considerar que en este servidor tendrá almacenada la información de autenticación de los usuarios del sistema, por lo que debe tener espacio en disco suficiente para la base de datos.

[1] http://docs.fedoraproject.org/fedora-install-guide-en/fc4/sn-before-begin.html

2.3.2 CLIENTE RADIUS

Adicionales a las características necesarias para la instalación de sistema operativo para este equipo se deben considerar lo siguiente:

Como se verá más adelante, el *kernel* de Linux es el encargado de realizar la clasificación y filtrado de paquetes (esta característica será empleada para el control de ancho de banda), y esto requiere una gran capacidad de procesamiento, por lo cual se ha considerado emplear como mínimo un procesador Pentium IV para este equipo.

Para tener una rápida respuesta del servidor Apache que será empleado para la autenticación de usuarios y para la administración de cliente RADIUS, se ha considerado para este servidor emplear mínimo 256 MB de memoria.

Este equipo debe también almacenar en la base de datos, la información de su configuración y la información que se vaya generando con el uso del sistema para la tarifación, por lo cual se debe considerar espacio adicional en el disco para almacenar toda esta información.

Adicionalmente este equipo debe tener al menos dos interfaces de red una para el segmento LAN y la otra para conectarse al Internet y al servidor RADIUS.

2.3.3 SERVIDOR *DIAL-UP*

En este servidor se ha instalado el sistema operativo *Windows* XP, y se ha activado la característica de permitir conexiones entrantes a través del MODEM, por lo cual con las características de *hardware* mínimas de instalación para este sistema operativo serán suficientes para este equipo.

A continuación se listan las características para la instalación de sistema operativo *Windows* XP[2].

- Microprocesador Pentium de 233 MHz o superior (o equivalente).
- Se recomienda 128 megabytes (MB). 64 MB de RAM es el mínimo y 4 gigabytes (GB) de RAM el máximo
- 1,5 GB de espacio libre en el disco duro
- Monitor VGA
- Teclado
- Microsoft Mouse o compatible
- Unidad de CD-ROM o DVD

Si bien es cierto las características anteriormente indicadas, corresponden a equipos desactualizados por lo que el tratar de realizar la implementación en uno de estos equipos no seria práctico, ya que al ser equipos que no se encuentran en el mercado su costo es mayor al de un equipo actualizado.

Por otro lado es recomendable emplear equipos actualizados, que permitan al menos un tiempo de vida útil de tres años y que tengan soporte del fabricante. Por tal razón la sugerencia de los equipos a ser usados seria la siguiente:

Servidor RADIUS:

Procesador:	Dual Core 1.6 GHz
Espacio en disco duro:	160 GB
Memoria:	1 GB

Cliente RADIUS:

Procesador:	Dual Core 1.6 GHz
Espacio en disco duro:	160 GB
Memoria:	1 GB

[2] http://support.microsoft.com/kb/306824/es

Servidor *dial-up*:

Procesador:	Dual Core 1.6 GHz
Espacio en disco duro:	160 GB
Memoria:	1 GB

2.4 CONFIGURACIÓN Y PUESTA EN MARCHA DEL SERVIDOR DE AUTENTICACIÓN FreeRADIUS EN LINUX

FreeRadius es un servidor RADIUS de código abierto, rápido, flexible, configurable y con soporte de protocolos de autenticación. Este servidor fue liberado bajo GNU *General Public License (GPL),* lo que quiere decir que este *software* es libre de ser descargado e instalado por cualquier persona.

FreeRadius es un demonio de autenticación de Internet, el cual implementa el protocolo RADIUS según los RFCs 2865 y 2866. Este servidor permite a los Servidores de Acceso Remoto (NAS) realizar la autenticación para usuarios *dial-up*. También existen clientes RADIUS para servidores web, *firewalls*, UNIX *logins*, por mencionar algunos.

El empleo de un servidor RADIUS permite que la autenticación y autorización para una red sean centralizadas y minimiza la cantidad de reconfiguraciones que deben ser hechas cuando se añaden o borran usuarios.

FreeRadius es más que un servidor RADIUS, pues incluye módulos de autenticación PAM (*Pluggable Authentication Modules*) y un módulo de autenticación para *Apache* 1.3 y 2.0. El servidor viene con una herramienta de administración de usuarios llamada *Dialup Admin* escrita en PHP (*Hypertext Preprocessor*). FreeRadius tiene todas las características de un servidor RADIUS distribuido de forma comercial, sin la asociación de costos involucrada.

2.4.1 CARACTERÍSTICAS DEL SERVIDOR FreeRADIUS VERSIÓN 1.0

FreeRadius viene con soporte para bases de datos LDAP, MySQL, PostgreSQL y Oracle. Y soporte de protocolos de autenticación como EAP, EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, y Cisco LEAP.

FreeRadius dispone de muchas características de los servidores de autenticación RADIUS, a continuación se redactan las más relevantes.

2.4.1.1 Características de Plataforma

FreeRadius ha sido compilado y se ha probado su funcionalidad en las siguientes plataformas:

- Linux (todas las versiones)
- FreeBSD
- NetBSD
- Solaris

Plataformas en las que es soportado pero no ha sido completamente probado

- HP/UX
- AIX
- MINGW32, CygWin (*Unix-style environment under Windows NT*)
- SFU (*or Interix, for Windows XP*)

2.4.1.2 Soporte de RFCs y Atributos VSA (*Vendor Specific Attributes*)

El servidor viene con soporte completo para los RFCs 2865 y 2866 y con VSA para alrededor de cincuenta vendedores incluyendo *Ascend*, *Microsoft*, *Shiva*, *USR/3Com, Cisco, Livingston, Versanet, Acc/Newbrid*ge, por mencionar algunos.

2.4.1.3 Atributos de configuración adicionales del servidor

El servidor RADIUS tiene un número de atributos de configuración, estos atributos permiten controlar casi cualquiera de los requerimientos RADIUS entrantes. Se puede emplear estos atributos de la siguiente manera:

- Ligar atributos a requerimientos.
- Reescribir algún atributo del requerimiento.
- Replicación de requerimientos a otro servidor RADIUS.
- Poder escoger el método de autenticación ha ser usado con cada cliente.
- Administrar a los usuarios por grupos.
- Implementar restricciones de acceso por hora del día.
- Ejecutar un programa local.
- Limitar el número de sesiones simultáneas por el usuario.

Todos los atributos anteriormente mencionados pueden ser usados en solicitudes de autenticación (*Authenticate-Request*) o solicitudes de auditoria RADIUS (*Accounting-Request*). Siendo ésta una ventaja del servidor frente a otros que generalmente permiten manejar estos atributos solo en el requerimiento de autenticación.

2.4.2 INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR FreeRADIUS

El primer paso es obtener la distribución de RADIUS que se desea instalar, misma que puede ser descargada desde la siguiente dirección http://www.freeradius.org. FreeRadius incluye la interfaz gráfica de administración web *Dialup Admin*. Para la instalación se procede de la siguiente manera:

Descomprimir el archivo freeradius-1.0.1.tar.gz

```
# tar -zxvf freeradius-1.0.1.tar.gz
# cd freeradius-1.0.1
```

Ejecutar el comando *configure* con los parámetros adecuados para indicar que los archivos binarios se instalen en /usr/local/{bin,sbin}, páginas de ayuda en /usr/local/man, archivos de configuración en /etc/raddb, y archivos de log en /var/log y /var/log/radacct.

```
# ./configure --localstatedir=/var --sysconfdir=/etc
```

Escribir el comando *make* para que los archivos binarios sean compilados

```
# make
```

Una vez compilados los archivos binarios, se procede a instalarlos, junto con las páginas de ayuda y los archivos de configuración. Si es la primera vez que se instala RADIUS, serán instalados los archivos de configuración para FreeRadius. Para instalar los binarios se escribe el siguiente comando.

```
# make install
```

Es de mucha utilidad leer las salidas generadas en pantalla por los comandos *make* y *make install*. Si algún módulo que se debía instalar no es instalado, la salida generada ayudará a saber el motivo de por qué no se instaló el módulo.

2.4.2.1 Ejecutando el servidor

Si el servidor se instala, pero no corre adecuadamente se puede emplear el modo depuración (*debug*) para tratar de identificar el problema y corregirlo.

Al iniciar el servidor en modo depuración, en pantalla se irán presentando los mensajes de ejecución, mediante los cuales se puede identificar posibles problemas durante la ejecución del servicio.

Para iniciar el servidor en modo depuración en la consola de ejecución, se debe escribir el siguiente comando

```
# radiusd -X
```

Después de la ejecución de este comando se observará un poco de texto impreso en la pantalla. Si se observa algún tipo de error, lo más recomendable es acudir a la página de Respuestas a Preguntas Frecuentes (*FAQ Frequently Asked Questions*), que se la puede encontrar en: http://www.freeradius.org/faq

Si en la pantalla de depuración del servidor aparece "*Ready to process requests*", esto indica que está corriendo adecuadamente, para verificar su funcionamiento se puede emplear el programa *radtest*[3] y escribir el siguiente comando de prueba al servidor RADIUS:

```
# radtest test test localhost 0 testing123
```

Se presentará en la pantalla del servidor de autenticación más mensajes indicando los requerimientos que recibe y las repuestas dadas a los mismos.

El programa *radtest* debería recibir la respuesta en unos pocos segundos, no importa si la respuesta es de aceptación o rechazo lo que interesa es que el servidor responda.

En este momento el servidor RADIUS está listo y el paso siguiente será editar los archivos de configuración de acuerdo a los requerimientos, es decir en función de las claves empleadas, dirección IP empleada, tipo de autenticación, puertos en los que trabaje el servidor, etc.

---

[3] ***radtest*** provee una forma simple y conveniente para enviar requerimientos a un servidor RADIUS y analizar las respuestas a estos requerimientos.

Es recomendable leer completamente los archivos de configuración ya que las opciones de configuración están documentadas únicamente en estos archivos.

En el ANEXO B se muestra el archivo de configuración /etc/raddb/clients.conf en el cual se deben configurar los clientes RADIUS.

2.4.2.2 Configuración de MySQL

El paquete MySQL viene junto con la distribución de Linux Fedora Core 3 por lo cual para disponer de este servicio únicamente es necesario seleccionarlo al momento de la instalación del Sistema Operativo, y configurarlo para su uso.

Las bases de datos están creadas en el directorio /var/lib/mysql. Se puede identificar a cada una como un subdirectorio. El subdirectorio *mysql* contiene la base de datos *mysql* donde se almacena la configuración de MySQL, como usuarios y sus claves.

Durante el proceso de instalación, para la administración del servidor MySQL se creo automáticamente la cuenta ***root*** con clave "*mysql*", por razones de seguridad es necesario cambiar esto, para hacerlo se debe ejecutar los siguientes comandos:

```
# mysql –u root –p mysql
> set password for root = password("nueva_clave");
> quit
```

2.4.2.3 Creación y configuración de la base de datos para el servidor RADIUS

Se debe crear una base de datos para almacenar la información de cuentas de usuario del servidor RADIUS en MySQL con un usuario con los permisos apropiados para poder acceder a la base de datos; los comandos a ejecutar son:

```
# mysql –u root –p yourrootpassword
> create database radius;
> grant all privileges on radius.* to
'dialupadmin'@localhost identified by
'adminpassword' with grant option;
```

El esquema de la base de datos de FreeRADIUS se encuentra en el archivo /usr/share/doc/freeradius-1.0.1/db_mysql.sql, el cual se lo debe emplear para la creación de las tablas en la base datos. Para ejecutar el *script* se debe ejecutar el siguiente comando:

```
mysql –u root –p rootpass radius < db_mysql.sql
```

Este *script* creará las siguientes tablas:

```
+------------------+
| Tables_in_radius |
+------------------+
| nas              |
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radpostauth      |
| radreply         |
| usergroup        |
+------------------+
```

La información de cuentas de usuario se la deberá agregar con la herramienta de administración de FreeRADIUS *Dialup Admin*.

2.4.2.4 Configuración del servidor RADIUS para usar la base de datos de MySQL

En el archivo /etc/raddb/sql.conf se debe ingresar el usuario y clave que usará el servidor FreeRADIUS para conectarse a la base de datos. El nombre de la base

de datos y estructura de las tablas no serán modificados ya que se empleará la estructura definida por defecto en el servidor FreeRADIUS.

```
#Connect info
server = "localhost"
login = "dialupadmin"
password = "administrador"
```

En el archivo /etc/raddb/radiusd.conf en la sección *authorize{ }*, se debe comentar la línea *files* y descomentar la línea *sql*, con lo que se indica que no se va ha emplear el archivo *users*, sino la base de datos de MySQL para almacenar la información de las cuentas de usuario. De igual manera en el archivo /etc/raddb/radiusd.conf, se deberá descomentar la línea *sql* en la sección *accounting{ }*.

2.4.2.5 Instalación de *Dialup Admin*

Dialup Admin, es una herramienta de administración del servidor RADIUS que permite administrar de forma gráfica el servidor a través de una interfaz web. A continuación se presenta el procedimiento realizado para su instalación y utilización.

Es necesario que la herramienta *Dialup Admin* sea copiada desde donde fue descomprimido FreeRADIUS a /usr/local; se debe configurar el servidor web Apache con cierto nivel de seguridad.

A continuación se presentan los comandos empleados para la instalación de *Dialup Admin*:

Copiar dialup_admin a /user/local

```
# cp –a dialup_admin /usr/local
```

El paso siguiente es establecer un enlace simbólico desde el directorio Apache hacia el directorio /usr/local/dialup_admin, como se muestra a continuación.

```
# ln –s /usr/local/dialup_admin/htdocs
/var/www/html/dialup
```

Con el objetivo de añadir seguridad en el acceso al servidor http, se hará uso del archivo .htaccess para lo que se usará el utilitario *htpasswd* de Apache, como se muestra a continuación:

```
htpasswd –cm /var/www/.htaccess [usuario]
```

En el comando anterior la opción –c se la emplea únicamente la primera vez para la creación del archivo ".htaccess", para añadir nuevos usuarios se emplea únicamente la opción –m de la siguiente forma.

```
htpasswd –m /var/www/.htaccess [nuevo_usuario]
```

Por ultimo se debe añadir en el archivo httpd.conf ubicado en /etc/httpd/conf, el contenido que se muestra a continuación:

```
### MyDialupAdmin
<Directory /var/www/html/dialup>
    AuthName "Restricted Area"
    AuthType Basic
    AuthUserFile /var/www/.htaccess
    require valid-user
</Directory>
```

Para que los cambio en la configuración tengan efecto se debe reiniciar el servidor Apache mediante el comando:

```
[root@gateway2 httpd] # service httpd restart
```

Se debe configurar el archivo *admin.conf* que es el archivo de configuración de *Dialup Admin*, que se encuentra en el directorio /usr/local/dialup_admin/conf.

Se definen los siguientes parámetros tal que pueda conectarse a RADIUS y MySQL:

```
#Indica tipo de base de datos a emplear
sql_type:mysql

#Indica que la base de datos a la que se debe conectar
#esta en la misma maquina
sql_server: localhost

#El puerto en el que se está ejecutando mysql
sql_port:3306

#nombre de usuario de la cuenta de MySQL
sql_username: dialupadmin

#la clave del usuario de la cuenta de MySQL
sql_password: administrador

#indica que la password no se guardará encriptada
general_encryption_method: clear
```

En el archivo /etc/httpd/conf.d/php.conf hay que añadir la siguiente línea que es necesaria ya que los *scripts* php de *Dialup Admin* tienen la extensión php3

```
 AddType application/x-http-php php3
```

Luego de esto, se podrá probar el funcionamiento de *Dialup Admin* con un explorador de Internet, colocando la dirección a la que se desea acceder http://ip_del_servidor_radius/dialup se presentará una ventana de inicio de sesión en la cual se solicita el nombre de usuario y clave, una vez que se proporcione

esta información de forma correcta se permitirá el acceso a la página de administración del servidor RADIUS (*Dialup Admin*).

En la base de datos radius se deberá crear varias tablas adicionales, necesarias para el funcionamiento de *Dialup Admin*. Estas tablas adicionales están definidas en los siguientes archivos:

- /usr/local/dialup_admin/sql/badusers.sql
- /usr/local/dialup_admin/sql/mtotacct.sql
- /usr/local/dialup_admin/sql/totacct.sql
- /usr/local/dialup_admin/sql/userinfo.sql

Se deben ejecutar los siguientes comandos:

```
# mysql -u dialupadmin -p radius < badusers.sql
# mysql -u dialupadmin -p radius < mtotacct.sql
# mysql -u dialupadmin -p radius < totacct.sql
# mysql -u dialupadmin -p radius < userinfo.sql
```

De tal forma que la tabla quedará como se muestra a continuación:

```
+------------------+
| Tables_in_radius |
+------------------+
| badusers         |
| mtotacct         |
| nas              |
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radpostauth      |
| radreply         |
| totacct          |
| usergroup        |
| userinfo         |
+------------------+
```

En el ANEXO B se muestran los archivos de configuración del servidor RADIUS, del servidor MySQL y de la interfaz de administración *Dialup Admin*.

2.5 IMPLEMENTACIÓN DEL CLIENTE RADIUS EN LINUX

En esta sección se procede a describir paso a paso el proceso de implementación del cliente RADIUS, para lo cual se ha divido este tema de la siguiente manera:

- Implementación de las políticas de seguridad planteadas.
- Descripción de las herramientas empleadas para la implementación.
- Programación de la interfaz de administración del cliente RADIUS.

2.5.1 PROCEDIMIENTO DE IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Las políticas de seguridad en las que se hace referencia a la infraestructura del cuarto de equipos y el empleo de equipos adicionales para ser cumplidas, se las tomará en cuenta como recomendación ya que el cumplimiento de este tipo de políticas depende del administrador del cuarto de equipos. Las políticas de seguridad que se listan a continuación corresponden a políticas de seguridad relacionadas con la infraestructura:

1. Condiciones del cuarto de equipos.
2. Sistemas de respaldo de energía eléctrica.
3. Sistemas de control de incendios.
4. Mecanismo de respuesta ante fallos.

El procedimiento de implementación de las políticas de seguridad realizables dentro del alcance de este proyecto, se describe a continuación:

2.5.1.1 Control de acceso mediante dirección MAC

Para conseguir implementar esta política es necesario configurar un servidor DHCP en el cliente RADIUS, de tal forma que el mismo se encargue de otorgar únicamente dirección IP a usuarios cuya dirección MAC este registrada en el sistema.

En el archivo de configuración de servidor DHCP, es posible denegar las peticiones de DHCP solicitadas por usuarios con direcciones MAC desconocidas mediante la opción:

```
deny unknown-clients;
```

Por lo cual cada usuario válido deberá ser declarado como *host* en el archivo de configuración dhcpd.conf; de la siguiente forma:

```
host nombre_host
{
     hardware ethernet 00:0a:e4:af:fb:b5;
}
```

Esta tarea la realizará automáticamente la interfaz de administración del cliente RADIUS una vez que se haya ingresado la dirección MAC en la base de datos.

2.5.1.2 Filtros de direcciones MAC en puntos de acceso inalámbricos

Para la implementación de esta política de seguridad, se procederá a configurar dentro del punto de acceso inalámbrico un listado con las direcciones MAC de los dispositivos que serán permitidos acceder a la red. Esta configuración será realizada empleando la interfaz web para la configuración del punto de acceso inalámbrico.

2.5.1.3 Autorización de acceso a usuarios con dirección IP configurada de forma estática

Para cumplir con esta política el cliente RADIUS mediante una comparación de la dirección MAC del usuario que intente acceder y la dirección almacenada en la base de datos permitirá o no el acceso al sistema.

Esta comparación se realizará no únicamente para usuarios que tengan una dirección IP estática sino para todos los usuarios que accedan al sistema al momento en que envíen su nombre de usuario y clave al cliente RADIUS.

2.5.1.4 Empleo de nombre de usuario y clave de acceso segura para la autenticación de usuarios

Una vez que el usuario tiene acceso a la red y se le ha asignado una dirección IP, las credenciales que debe conocer son su nombre de usuario y su clave, esta información se validará con el servidor RADIUS, y si es correcta el mismo generará una respuesta *Access-Accept* para que el cliente RADIUS genere en ese momento las reglas necesarias y el usuario tenga acceso a Internet en función de su perfil.

2.5.1.5 Definir diferentes perfiles de acceso para los usuarios

Lo que se desea es disponer de un mecanismo de control de utilización de los recursos dentro de la red de datos (permisos de acceso a información o aplicaciones y asignación de ancho de banda) definiendo varios perfiles con distintos niveles de acceso

Cada uno de los perfiles creados dispondrá de un conjunto de servicios específicos a los cuales puede acceder y un porcentaje del ancho de banda del que podrá hacer uso.

2.5.1.6 Protección de la información que viaja por el segmento de red inalámbrico

Con el fin de proteger la información que viaja a través del segmento de red, se procederá a emplear un punto de acceso marca 3Com modelo 3CRGPOE1007, en el que se configurará 802.1X/EAP y el tipo de EAP empleado será TLS.

Para la generación de los certificados digitales que serán empleados por los usuarios, se utilizará como autoridad certificadora al servidor de autenticación RADIUS, los *scripts* empleados en la generación de los certificados digitales se muestran en el ANEXO I.

2.5.1.7 Protección de la información de autenticación que el usuario envía al cliente RADIUS

La información que es intercambiada entre el usuario y el cliente RADIUS, durante el proceso de autenticación deberá ser protegida, por lo que se empleará mecanismos de encripción.

Para encriptar la información, en el sistema de autenticación del cliente RADIUS, se forzará al usuario a que cada vez que se autentique en el sistema tenga que emplear una página de autenticación https, de esta manera la información intercambiada en el proceso de autenticación estará encriptada.

Se procedió a configurar un redireccionamiento de las peticiones http en el cliente RADIUS, de tal manera que la petición sea redireccionada a una página https siempre y cuando el usuario no se encuentre autenticado en el sistema.

2.5.1.8 Protección de la información de autenticación que el cliente RADIUS, envía al servidor RADIUS

Se procederá ha levantar un túnel IPSec entre el servidor RADIUS y el cliente RADIUS de tal manera que la información intercambiada sea únicamente vista por sus destinatarios.

2.5.1.9 Registro del tiempo de conexión y el consumo medido en *bytes* que realice el usuario

Lo que se desea es disponer de un mecanismo que permita contabilizar la cantidad de información en *bytes* enviada y recibida por el usuario, su tiempo de permanencia dentro del sistema, es decir llevar una bitácora de comportamiento del usuario dentro de la red de datos, información que será indispensable al momento de realizar la tarifación por el uso del sistema.

Se procedió a generar un *script* que se encontrará corriendo en un segundo plano y su función será la de realizar una comparación cada cinco segundos del tiempo y consumo anterior con el consumo y tiempo actual, de tal manera que en base al resultado obtenido en esta comparación podrá definir si hubo consumo o no y actualizar la información en la base de datos.

2.5.2 DESCRIPCIÓN DE LAS HERRAMIENTAS DE *SOFTWARE* EMPLEADAS PARA LA IMPLEMENTACIÓN

Para la implementación del cliente RADIUS se hace uso de las siguientes herramientas de *software* de libre distribución:

- Apache + OpenSSL
- PHP
- MySQL
- *iptables*

Apache será el servidor web que se empleará en el cliente RADIUS; en este residirán páginas html y *scripts* php que serán empleados para la autenticación de usuarios, y la administración del cliente RADIUS, por lo que deberá ser configurado para soportar PHP y SSL.

PHP será el lenguaje empleado para la elaboración de la página de autenticación de usuarios, los *srcipts* que serán los encargados de ejecutar las reglas que

permitan el acceso de los usuarios a los servicios, y para la implementación de la interfaz de administración del cliente RADIUS.

MySQL será empleado para almacenar la información de los perfiles de usuario, para llevar un registro de la utilización del sistema y para guardar la configuración del servidor DHCP.

Con *iptables* se dará los permisos de acceso a cada usuario autenticado, dependiendo del perfil con el que esté configurado, es decir mediante el uso de *iptables* se podrá permitir, limitar o denegar el acceso a los diferentes servicios de la red.

2.5.2.1 Servidor Apache

Apache es un programa servidor http gratuito, con características como gran fiabilidad y extensibilidad que lo convierten en una herramienta potente y fácilmente configurable.

Apache puede ser implementado en gran cantidad de Sistemas Operativos, lo que lo hace prácticamente universal. Actualmente existen muchos módulos para Apache que son adaptables, y están listos para ser instalados cuando se requieran.

Apache trabaja con gran cantidad de lenguajes como Perl, PHP y otros lenguajes de *script*. También trabaja con Java y páginas jsp. Teniendo todo el soporte que se necesita para páginas dinámicas.

Apache permite personalizar la respuesta ante los posibles errores que se puedan dar en el servidor. Es posible configurar Apache para que ejecute un determinado *script* cuando ocurra un error.

Es sencilla la configuración para la creación y gestión de *logs*, ya que permite la creación de ficheros de *log* a medida del administrador, de este modo se puede tener un mayor control sobre lo que sucede en el servidor.

2.5.2.2 PHP *Hypertext Preprocessor*

PHP (PHP *Hypertext Preprocessor*) es un lenguaje de código abierto interpretado, de alto nivel, embebido en páginas HTML y ejecutado en el servidor.

Lo que distingue a PHP de tecnologías como *Javascript*, es que *Javscript* se ejecuta en la máquina cliente y el código PHP se ejecuta directamente en el servidor. El cliente solamente recibe el resultado de la ejecución de los *scripts* PHP existentes en el servidor, sin ninguna posibilidad de determinar qué código ha producido el resultado recibido. El servidor web puede ser incluso configurado para que procese todos los archivos HTML con PHP.

PHP permite hacer cualquier cosa que se pueda hacer con un *script* CGI (*Common Gateway Interfaz*), como procesar la información de formularios, generar páginas con contenidos dinámicos, o enviar y recibir *cookies*.

El CGI es utilizado comúnmente para contadores, bases de datos, motores de búsqueda, formularios, foros de discusión, *chats*, comercio electrónico y mapas de imágenes. Esta tecnología tiene la ventaja de correr en el servidor cuando el usuario lo solicita por lo que es dependiente del servidor y no de la computadora del usuario.

Existen tres ambientes en los cuales se pueden emplear *script* PHP:

- El primer ambiente consiste de *scripts* del lado del servidor. Este es el campo más tradicional y el principal foco de trabajo. Para su funcionamiento se necesitan: el intérprete PHP (CGI ó módulo), un servidor web y un navegador. Es necesario correr el servidor web con PHP instalado. El resultado del programa PHP se puede obtener a través del

navegador, conectándose con el servidor web. Este ambiente es el que se va a emplear para la implementación.

- El segundo ambiente consiste de *scripts* en la línea de comandos. Puede crear un *script* PHP y correrlo sin ningún servidor web o navegador. Solamente necesita el intérprete PHP para usarlo de esta manera.

- Y por último el tercer ambiente consiste en escribir aplicaciones de interfaz gráfica. Probablemente PHP no es el lenguaje más apropiado para escribir aplicaciones gráficas

PHP puede ser utilizado en sistemas operativos como Linux, Unix y sus variantes (incluyendo HP-UX, Solaris y OpenBSD), *Microsoft Windows*, Mac OS X, RISC OS, por mencionar algunos.

PHP es soportado con servidores web como Apache, *Microsoft Internet Information Server*, *Personal Web Server*, *Netscape* e iPlanet, Oreilly *Website Pro server*, por mencionar algunos.

Quizás la característica más potente y destacable de PHP es su soporte para una gran cantidad de bases de datos. Escribir un interfaz vía web para una base de datos es una tarea simple con PHP.

También consta con una extensión DBX de abstracción de base de datos que permite usar de forma transparente cualquier base de datos soportada por la extensión. Adicionalmente, PHP soporta ODBC (el Estándar Abierto de Conexión con Bases de Datos), así que puede conectarse a cualquier base de datos que soporte tal estándar.

2.5.2.3 MySQL

MySQL es un sistema gestor de bases de datos (SQL *Structured Query Language*), desarrollado bajo la filosofía de código abierto.

MySQL es un sistema de administración relacional de bases de datos. Una base de datos relacional archiva datos en tablas separadas en vez de colocar todos los datos en un gran archivo. Permitiendo de esta manera que el sistema sea más rápido y flexible. Las tablas están conectadas por relaciones definidas que hacen posible combinar datos de diferentes tablas sobre pedido.

En base a lo mencionado anteriormente el principal objetivo de MySQL es velocidad y robustez.

Un beneficio de la forma como fue concebido es que tenga la característica de multiproceso, es decir puede usar varias CPU si están disponibles.

Puede trabajar en distintas plataformas y sistemas operativos, sean estos de distribución libre o de distribución comercial.

El sistema de contraseñas y privilegios es flexible y seguro, es decir permite mecanismos de control de acceso a la información a través de la utilización de un nombre de usuario y una clave.

.

La base de datos maneja un esquema de encripción de la información que viaja en el momento de autenticarse, es decir las claves viajan encriptadas en la red. Los registros de la base de datos pueden ser de longitud fija y/o variable.

Los clientes usan TCP o UNIX s*ocket* para conectarse al servidor.

El servidor soporta mensajes de error en distintos lenguajes de programación y todos los comandos tienen las opciones *-help o -?,* para las ayudas.

Se puede utilizar para los datos que se desee almacenar diversos tipos de columnas como: enteros de 1, 2, 3, 4, y 8 *bytes*; coma flotante; doble precisión; carácter; fechas; enumerados; etc.

2.5.2.4 Iptables

Es un sistema de *firewall* que viene integrado con el *kernel* en las versiones de Linux con *kernel* superior al 2.4, es parte del sistema operativo.

El *firewall* viene ha ser un punto en el cual se controla el tráfico que se intercambia entre dos redes y en función de las políticas de seguridad definidas para cada una de las redes, se podrá establecer o no conexiones hacia los servicios de red entre las redes involucradas.

En la actualidad existen equipos con sistema operativo o un IOS (*Internetwork Operative System*) que es el encargado de filtrar el tráfico IP, y es el que decide si un paquete pasa, se modifica o se descarta.

El comando *iptables* que permite manipular (crear, modificar, borrar) las reglas de filtrado de paquetes; por lo que, el *firewall* de *iptables* es un *script shell* que contiene las reglas de *firewall*. Estas reglas permiten indicar al *kernel*, que hacer con un paquete cuando este llega o atraviesa la maquina local.

Los términos y expresiones empleados en la creación de un filtro IP se presentan en el ANEXO C.

2.5.2.4.1 Implementación de un filtro IP

Primero se debe considerar la ubicación del filtro IP dentro de la red y con qué objetivo se lo está colocando. En este caso el filtro IP hará la función de *firewall* y será implementado como *gateway* hacia el Internet, pues las reglas se aplicarán en términos de los servicios de Internet que los usuarios puedan tener acceso en función de su perfil, mismo que será definido en el cliente RADIUS.

Se deberá definir el comportamiento del *firewall* por defecto, por mencionar algo, si las reglas de *firewall* no se cumplen, que se debería hacer con los paquetes: aceptarlos o descartarlos.

Se puede implementar el filtro empleando una de las siguientes dos políticas: descartar todos los paquetes excepto los que se ha especificado que no se descarten, o aceptar todo excepto lo que se indique que deba ser descartado.

Generalmente se empleará las políticas de descartar todos los paquetes y especificar los paquetes que deban ser aceptados, lo cual significa que el *firewall* es más seguro por defecto, pero esto puede significar que se tenga un mayor trabajo en el momento de especificar que se va ha permitir. De hecho el *firewall* a ser implementado por defecto bloquea todo y permite el tráfico que se le indique.

Se debe escoger que tipo de *firewall* se va ha emplear y qué tipo de aplicación se desea proteger; hay que tener claro que las aplicaciones que realizan una asignación dinámica de puertos en su ejecución, no podrán ser filtrados por un *firewall* empleando *iptables*.

Para la implementación de los filtros se emplearán las diferentes tablas *mangle, nat y filter* de *iptables*, para lo cual se deberá tener un conocimiento claro de que se realiza en cada tabla.

2.5.2.4.2 Tabla Mangle

Esta tabla es empleada para modificar el contenido de los paquetes, por ejemplo, cambiar el campo ToS (*Type of Service)*.

La tabla *mangle* no debe ser empleada para filtrar paquetes, es decir no se debe emplear para ninguna tarea de NAT o tareas de enmascaramiento.

Los siguientes campos: ToS, TTL (*Time To Live*), y MARK son empleados únicamente en la tabla *mangle*.

El campo ToS, podrá ser empleado para establecer políticas en la red de cómo un paquete deberá se enrutado, hay que tener claro que este campo no es muy empleado en Internet ya que algunos *routers* no lo soportan.

El campo TTL, indica que los paquetes tendrán un específico tiempo de vida en la red, en base a un contador que se decrementa con cada salto realizado por el paquete.

El campo MARK es empleado para establecer valores de marcas específicas a un paquete. Estas marcas pueden ser empleadas posteriormente p. e. para realizar tareas de enrutamiento de acuerdo a la marca que tenga cada paquete.

Este campo posteriormente será empleado para realizar el control de Ancho de Banda colocando una marca en el paquete de acuerdo a su dirección IP de origen, y con el uso de un filtro se podrá identificar cada paquete y colocarlo en una disciplina de encolamiento diferente.

2.5.2.4.3 Tabla NAT

Esta tabla realiza la función de NAT (*Network Address Translation*) sobre los paquetes, se la emplea para la traducción de los campos: IP origen e IP destino del paquete; según el campo que se desea cambiar se emplean las siguientes opciones: DNAT, SNAT y MASQUERADE.

DNAT *(Destination Network Address Translation)* se emplea en casos donde se tiene una dirección IP pública y se desea redireccionar el acceso al *firewall* a otros computadores, en un segmento de red denominado DMZ *Demilitarized Zone* (segmento de red pública con una seguridad limitada). En otras palabras lo que hace DNAT es cambiar la dirección destino del paquete para reenrutarlo, un ejemplo de DNAT es publicar el servicio de un servidor web interno en la dirección IP pública de acceso a Internet.

SNAT *(Source Network Address Translation)* es empleado para cambiar la dirección origen del paquete, puede ser útil para ocultar las direcciones de la red local o DMZ, un ejemplo del empleo de SNAT es proporcionar acceso a un grupo

de direcciones IP privadas a Internet a través de una dirección IP pública permitiendo que todo el grupo de direcciones IP se traduzcan como la IP pública.

MASQUERADE es empleado en forma similar que SNAT, solo que en este caso se revisará siempre la dirección IP que le llega, no solo aquellas seleccionadas como es el caso de SNAT.

2.5.2.4.4 Tabla filter

La tabla *filter* es la encargada de filtrar los paquetes. Se puede buscar emparejamiento de los paquetes con condiciones y en función del resultado realizar acciones como descartar el paquete o aceptarlo. Los paquetes pueden ser tratados como se necesite ya que esta tabla toma decisiones en función del contenido del paquete.

2.5.2.4.5 Funcionamiento de iptables

El paquete llega al *firewall*, donde es recibido por el controlador del dispositivo en el *kernel*, una vez que el paquete es recibido por el dispositivo, pasa por una serie de pasos en el *kernel* antes de ser enviado a una aplicación local o a una dirección IP externa.

En las Tablas 2.1, 2.2, y 2.3 se muestra el trayecto que sigue un paquete para las tres situaciones posibles: un paquete destinado a la maquina local, un paquete originado en la máquina local y un paquete con destino a otra red, respectivamente.

	TABLA	CADENA	ACCION
1	-	-	Llega el paquete hacia la interfaz, p. e. eth0.
2	mangle	PREROUTING	Normalmente se modifica el paquete, p. e. cambiar el campo ToS.
3	nat	PREROUTING	Se emplea principalmente para traducción de direcciones.
4	-	-	Decisión de enrutamiento p. e. si el paquete está destinado para el computador local o para ser reenviado.
5	mangle	INPUT	Se usa para cambiar los paquetes después que se ha tomado la decisión de enrutamiento.
6	filter	INPUT	Se realiza un filtraje del tráfico entrante destinado para la máquina local, todos los paquetes destinados a este computador pasan por esta cadena.
7	-	-	Por último se llega al proceso de la aplicación local, p. e. un servidor http.

Tabla 2.1 Trayectoria de un paquete destinado a la máquina local

	TABLA	CADENA	ACCION
1	-	-	Decisión de eruntamiento. Se identifica cual es la dirección fuente y cual es la interfaz de salida que se va ha utilizar.
2	mangle	OUTPUT	Se pueden modificar los paquetes.
3	nat	OUTPUT	Puede ser usada para hacer NAT de paquetes que salen desde la maquina local.
4	filter	OUTPUT	Es posible filtrar los paquetes que salen desde la máquina local.
5	mangle	POSTROUTING	Se la emplea cuando se desea realizar modificación de los paquetes antes de que estos dejen la máquina local, pero después de la decisión de enrutamiento.
6	nat	POSTROUTING	Se realiza el proceso de NAT, posterior a la decisión de enrutamiento.
7	-	-	El paquete es sacado a la interfaz y enviado a través del medio de transmisión.

Tabla 2.2 Trayectoria de un paquete originado en la maquina local

	TABLA	CADENA	ACCION
1	-	-	El paquete ingresa a la interfaz desde el medio de transmisión, p. e. eth0.
2	mangle	PREROUTING	Se realiza cambios en el contenido de los paquetes.
3	nat	PREROUTING	Se realiza la función de NAT previo envío del paquete.
4	-	-	Decisión de enrutamiento, por ejemplo si el destino del paquete es la máquina local o si va ha ser reenviado y hacia donde.
5	mangle	FORWARD	Esta tabla es empleada para modificar el paquete una vez que la decisión inicial de enrutamiento ha sido tomada, pero antes de la última decisión de enrutamiento misma que es hecha antes de que el paquete sea enviado.
6	filter	FORWARD	Los paquetes son enrutados, únicamente los paquetes reenviados atravesarán esta cadena.
7	mangle	POSTROUTING	Se la emplea para realizar modificaciones de los paquetes las cuales se desea que se realicen después de que todas las decisiones de enrutamiento hayan sido tomadas.
8	nat	POSTROUTING	Se realiza el enmascaramiento.
9	-	-	El paquete se envía a la interfaz y finalmente es inyectado en el medio de transmisión.

Tabla 2.3 Trayectoria de un paquete destinado a una máquina en otra red

En la Figura 2.1 se muestra un diagrama de Fuljo en el que se puede observar la trayectoria de los paquetes anteriormente descrita:

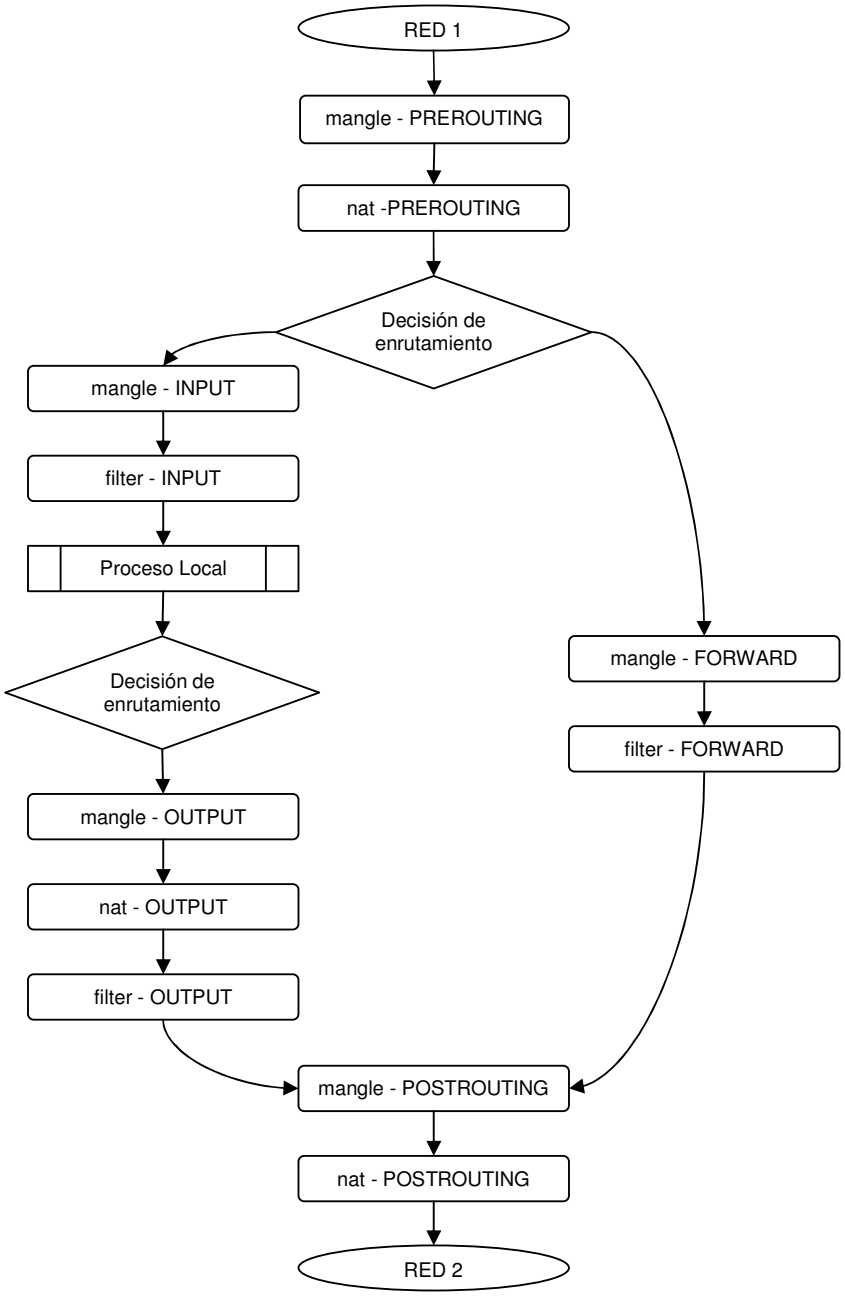

Figura 2.1 Diagrama de Flujo de la trayectoria de un paquete en el *kernel*[4]

[4] http://iptables-tutorial.frozentux.net/spanish/chunkyhtml/c392.html

2.5.3 PROGRAMACIÓN DEL CLIENTE RADIUS

El servidor RADIUS será el encargado de proporcionar la información del tiempo por el cual una sesión de usuario permaneció establecida, esta información será de utilidad para realizar una auditoria, control y tarifación de la utilización del sistema. La creación de los usuarios y sus credenciales se las hará directamente en el servidor RADIUS a través de la interfaz gráfica *Dialup Admin*.

Los datos de perfil de usuario y la información de auditoria de utilización del sistema por cada usuario se almacenarán directamente en la base de datos del cliente RADIUS.

La interfaz de administración del cliente RADIUS está realizada en leguaje PHP.

2.5.3.1 Organización de la información en la base de datos del cliente RADIUS

Para la implementación del cliente RADIUS, la información con la que trabajará la aplicación será almacenada en una base de datos MySQL, la misma que estará alojada en el computador que hará las veces de cliente RADIUS. La base de datos creada para este fin se llama “gateway” y para la creación y administración de la misma se empleará la herramienta “PHP MyAdmin”.

Dentro de la base de datos *gateway*, se han creado cinco tablas: accounting, perfiles, servicios, dhcp y pc_validos; con el fin de almacenar toda la información necesaria para el funcionamiento del cliente RADIUS. Fue necesaria la creación de una tabla adicional: per_serv; con la finalidad de crear las relaciones entre los datos de las tablas perfiles y servicios.

En la Figura 2.2 se muestra la estructura de la base de datos “gateway”, que se empleo para la implementación del cliente RADIUS.

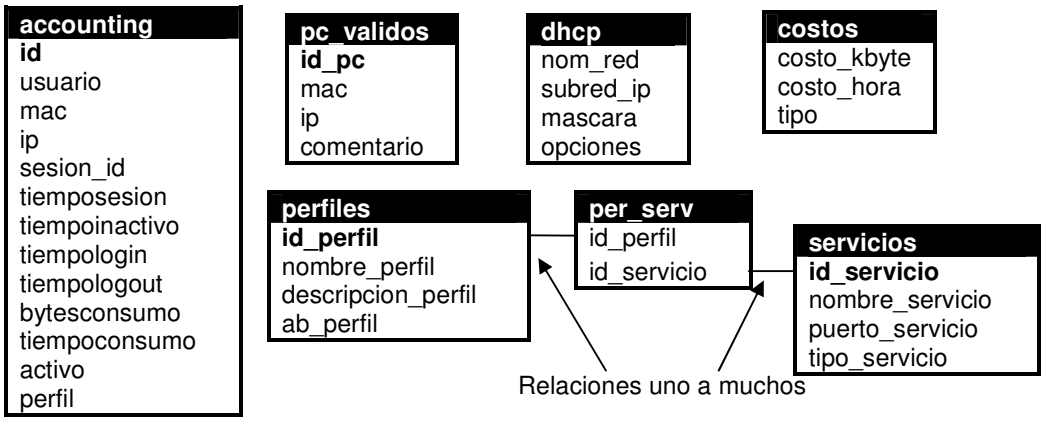

Figura 2.2 Tabla relacional de la estructura de la base de datos

A continuación se describe cada una de las tablas que forman parte de la Base de Datos:

2.5.3.1.1 Tabla Accounting

Contiene la información correspondiente a cada usuario y la información necesaria para llevar una auditoria de utilización del sistema. A continuación se listan los campos que contiene esta tabla con una descripción de cada uno:

- **id**: corresponde a un identificador de cada usuario.
- **usuario:** corresponde al nombre del usuario.
- **mac**: corresponde a la dirección MAC del adaptador de red del usuario.
- **ip**: corresponde a la dirección IP del usuario.
- **sesion_id**: es un identificador de la sesión establecida.
- **tiemposesion**: tiempo que una sesión permanecerá establecida antes que se la finalice automáticamente en el sistema.
- **tiempoinactivo**: corresponde al tiempo durante el cual no existió actividad.
- **tiempologin**: tiempo en el cual se estableció el inicio de la sesión.
- **tiempologout**: tiempo en el cual finalizó la sesión.
- **bytesconsumo**: cantidad de *bytes* transmitidos en un determinado intervalo de tiempo.

- **tiempoconsumido**: suma de todos los tiempos de los períodos en los cuales una sesión permaneció activa.
- **activo**: indica si la sesión se encuentra activa o no.

2.5.3.1.2 Tabla perfiles

Lleva la información correspondiente a un determinado perfil, a continuación se muestra los campos de esta tabla con una descripción de los mismos:

- **id_perfil**: Es un número que identifica de manera única a cada uno de los perfiles, este mismo número debe ser empleado al momento de crear el usuario en el servidor RADIUS para asociarlo con el perfil correspondiente.
- **nombre_perfil**: Un nombre que describa cada perfil.
- **descripción_perfil**: Una breve descripción del uso que se le dará a cada perfil.
- **ab_perfil**: Este campo almacenará la información del porcentaje del ancho de banda disponible que le corresponde a cada perfil.

2.5.3.1.3 Tabla servicios

Contiene la información asociada a los servicios, a continuación se muestra los campos y la información que contienen los mismos:

- **id_servicio**: Identificador de un determinado servicio.
- **nombre_servicio**: Nombre asociado a cada servicio.
- **puerto_servicio**: Puerto que emplee dicho servicio.
- **tipo_servicio**: Si el servicio es orientado o no a conexión, TCP o UDP.

2.5.3.1.4 Tabla per_serv

Se emplea para guardar la información de los servicios asociados con cada uno de los perfiles existentes; en esta tabla se encuentran definidas dos relaciones de uno a muchos una con la tabla perfiles y la otra con la tabla servicios:

- Cada perfil puede contener muchos servicios.
- Cada servicio puede pertenecer a muchos perfiles.

Contiene dos campos, los cuales se listan a continuación:

- **id_perfil**: Identificador del perfil.
- **id_servicio**: Identificador del servicio.

2.5.3.1.5 Tabla dhcp

Almacena los parámetros de configuración del servidor DHCP, con estos parámetros se generará de forma dinámica el archivo de configuración dhcpd.conf.

Los campos que contiene esta tabla son:

- **nom_red**: Nombre descriptivo de la red o subred.
- **subred_ip**: Dirección de red/subred que definirá el rango de direcciones para asignar mediante DHCP.
- **mascara**: Mascara de red/subred.
- **opciones**: Opciones de configuración del servidor DHCP tales como DNS, ruta por defecto.

2.5.3.1.6 Tabla pc_validos

Contiene las direcciones MAC de los usuarios a quienes el servidor DHCP asignará una dirección IP, esta tabla se la utiliza también para la creación del archivo dhcpd.conf.

Los campos de la tabla se describen a continuación:

- **id_pc**: Identificador único de cada PC.

- **mac**: Dirección MAC a la que se asignará una dirección IP mediante DHCP.
- **ip**: Este campo es opcional, indica la dirección IP que se le asignará a la dirección MAC, si esta en blanco se asignara una dirección IP del rango.
- **comentario**: Es opcional se recomienda colocar cualquier comentario que sea de utilidad para el administrador.

2.5.3.1.7 Tabla costos

Almacena la información del tipo de tarifación a realizarse y el valor asignado al costo por *kbyte* consumido o por hora de utilización.

Los campos de la tabla se describen a continuación:

- **costo_kbyte**: valor del costo por *byte* consumido.
- **costo_hora**: valor por hora de utilización del sistema.
- **tipo**: tipo de tarifación (por hora o por *kbyte)*

2.5.3.2 Programación de *scripts* PHP

Como un parámetro de seguridad previo a la autenticación de los usuarios se proporcionará el servicio de DHCP únicamente a usuarios cuya dirección MAC se haya registrado previamente en el cliente RADIUS, es decir la dirección MAC del usuario debe constar en el archivo de configuración del servidor DHCP (dhcpd.conf).

El código para realizar la consulta a la base de datos que extrae la información para generar el archivo de configuración del servidor DHCP (dhcpd.conf), se encuentra en el archivo in_dhcp.php.

La configuración inicial de las reglas de *firewall* del cliente RADIUS se encuentra en el archivo iptables.txt y se lo ejecutara de forma automática al momento de iniciar el sistema, en este archivo se realiza un redireccionamiento de las

peticiones http y https hacia la dirección IP del cliente RADIUS, se inicializan las tablas del *firewall*, se crea una cadena personalizada que será empleada para organizar las reglas de cada usuario que accede al sistema, se colocan los permisos iniciales de los usuarios y la seguridad propia del cliente RADIUS.

Luego de que el usuario haya solicitado cualquier página web sin haber iniciado una sesión en el Cliente RADIUS), *iptables* realiza el cambio de la dirección de destino por la dirección del Cliente RADIUS, p. e. si se solicito el URL:

http://www.psicobyte.com/html/taller/errores.html

Será substituido por:

http://192.168.1.203/html/taller/errores.html

Dando como resultado el error "**ERROR 404:** Página No encontrada", debido a que en el cliente RADIUS no existe la carpeta /html/taller/errores.html. Por lo que fue necesario realizar la personalización del error 404, añadiendo el archivo de configuración de Apache .htaccess en el directorio /opt/lamp/htdocs, con la línea:

```
ErrorDocument 404 /index.php
```

Lo que hace que, cuado se presente el error 404 se muestre la página index.php, que es la pagina de inicio del Cliente RADIUS.

Una vez que se realiza la redirección la petición del usuario es atendida en el archivo index.php, mismo que presenta una breve bienvenida y realiza un direccionamiento hacia la página login.php, forzando que ésta se presente empleando el protocolo https y se realiza la captura del URL solicitado por el usuario. En la Figura 2.3 se muestra la ventana que se presenta al usuario.

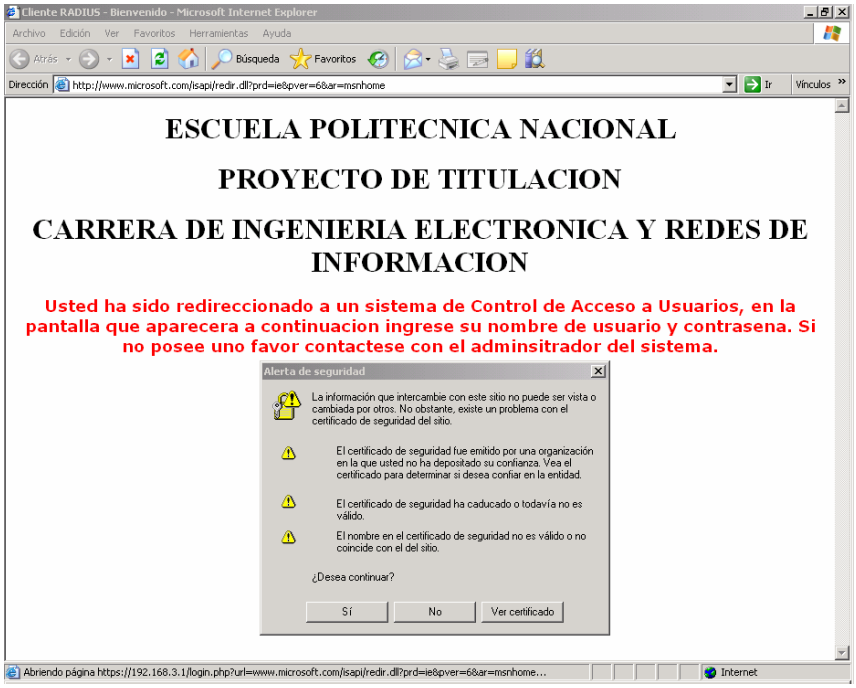

Figura 2.3 Ventana presentada al usuario antes de autenticarse

La página login.php presenta un formulario en el cual se solicita las credenciales del usuario: nombre de usuario y clave; estos datos en conjunto con el URL previamente capturado, son enviados al cliente RADIUS, luego de presionar el botón continuar. La Figura 2.4 presenta la ventana de autenticación de usuarios.

Una vez ingresados los datos el sistema llama al archivo inicio.php, en el que se han cargado previamente los módulos necesarios para interactuar con el servidor RADIUS, se recuperan las variables provenientes del formulario de autenticación y se captura la dirección IP del cliente que ingresó los datos.

En la base de datos local del cliente RADIUS, se procede a verificar si el usuario ha iniciado sesión, si es el caso se presenta un mensaje de error y si no, se procede ha enviar los datos al servidor RADIUS.

Una vez validados los datos, si se recibe un *Access_Accept* desde el servidor RADIUS, se procede a generar las reglas que permitirán al usuario acceder a los servicios de la red, y se inicializan los datos del usuario en la base de datos para

realizar el *accounting. T*ambién se almacena el URL solicitado por el usuario que será empleado en el archivo redireccionar.php.

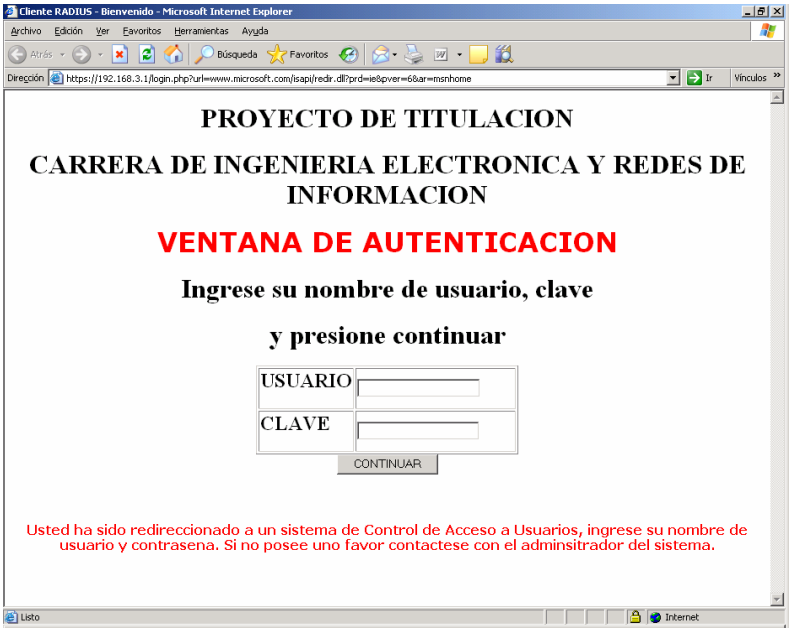

Figura 2.4 Ventana de autenticación de usuarios

A continuación se llama al archivo redireccionar.php, que es el encargado de realizar la redirección hacia la página que el usuario solicito antes de ingresar en el sistema de autenticación. Este archivo lanzará una ventana *pop-up* que contiene un botón DESCONECTAR, al hacer *click* en este botón el usuario podrá voluntariamente finalizar su sesión. En la Figura 2.5 se muestra la ventana con el mensaje que se presenta una vez autenticado el usuario y la ventana *pop-up* de desconexión voluntaria.

Una vez que el usuario se haya autenticado y registrado en el sistema, es necesario actualizar constantemente la información de la utilización del sistema en la base de datos, ya que se podrá finalizar la sesión del usuario en función de un tiempo de inactividad, en base al tiempo total que el usuario disponga o voluntariamente al hacer *click* en la ventana de desconexión.

Para realizar el control de la actividad del usuario se emplea una regla de *iptables* la cual permite ir cuantificando el tráfico del usuario, que está cursando por el cliente RADIUS.

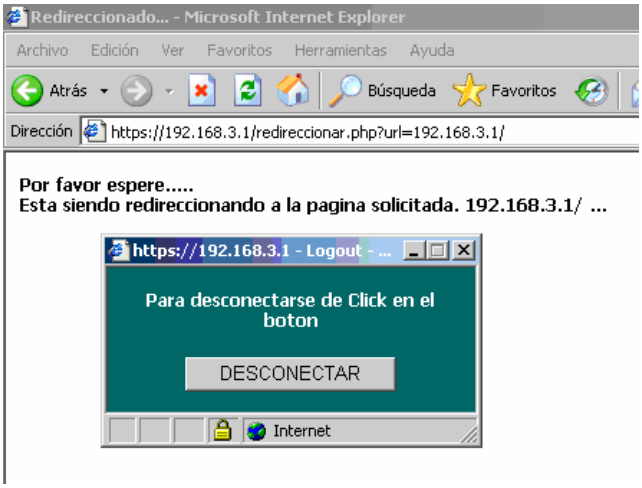

Figura 2.5 Ventana presentada al usuario una vez autenticado

En el ANEXO D se adjunta todo el diagrama de flujo del programa junto con los archivos empleados para la ejecución del sistema de autenticación.

Tanto para ejecutar los *scripts* PHP de autenticación y mostrarlos al usuario, así como también para publicar las páginas de la interfaz de administración del cliente RADIUS, se emplea el servidor web Apache con soporte para PHP.

2.5.4 PROGRAMACIÓN DE LA INTERFAZ DE ADMINISTRACIÓN

La interfaz de administración del cliente RADIUS está realizada en su totalidad en PHP, esta permite que el administrador del cliente RADIUS, pueda realizar las siguientes tareas:

- Crear, modificar y eliminar perfiles.
- Configurar y modificar el ancho de banda por perfil.
- Crear, modificar y eliminar servicios para configurarlos en cada perfil.
- Configurar el servidor DHCP.
- Mostrar la utilización del sistema por dirección MAC del usuario.

- Definir esquemas de tarifación.

En la Figura 2.6 se presenta la página correspondiente a la interfaz de administración del cliente RADIUS.

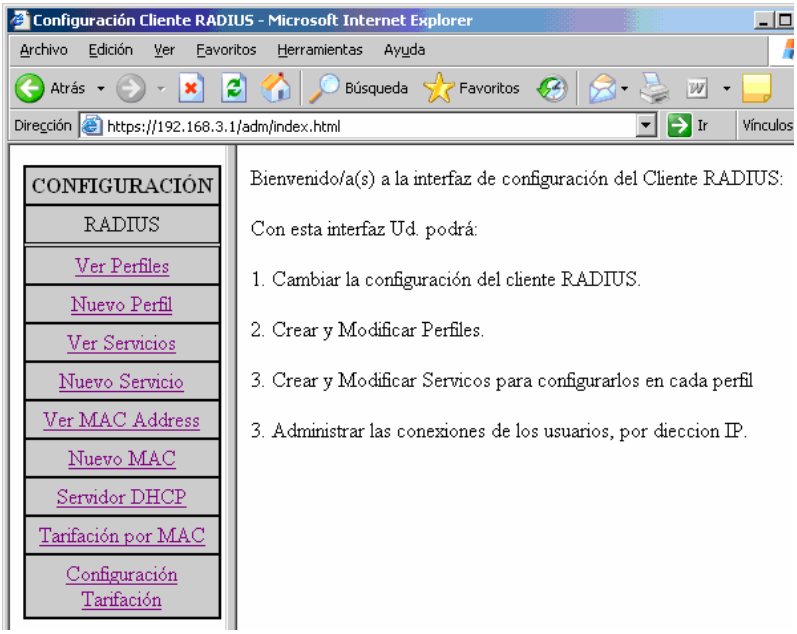

Figura 2.6 Interfaz de Administración del Cliente RADIUS

Los archivos con código PHP, que interactúan para mostrar la interfaz de administración se encuentran en la ruta /opt/lampp/htdocs/adm, dentro de esta ruta se encuentran cinco directorios (cdg, cfg, dhcp, fnc, frm) y dos archivos (index.htm y menu.htm). El archivo index.htm contiene un índice con diferentes hipervínculos hacia los formularos que manejan cada una de las funciones listadas en este archivo, mientras el archivo menu.htm es únicamente una descripción de lo que se puede realizar dentro de la interfaz de administración.

A continuación se presenta una descripción de lo que cada uno de los menús permite realizar dentro del cliente RADIUS.

2.5.4.1 Menú Ver Perfiles

En la Figura 2.7 se muestra el menú Ver Perfiles en el que se observan todos los perfiles de usuario existentes, se puede ver los servicios asociados a cada perfil, modificar los perfiles y eliminarlos.

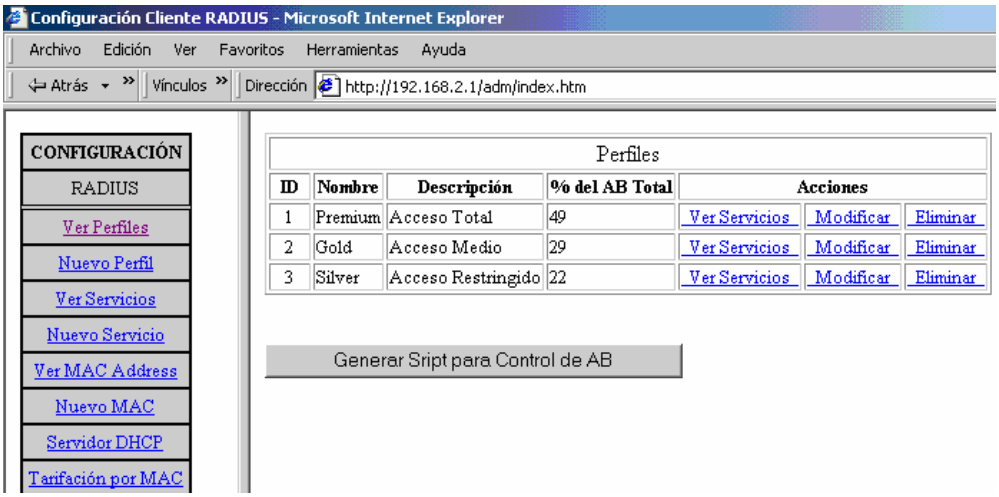

Figura 2.7 Menú de configuración de perfiles

2.5.4.2 Menú Nuevo Perfil

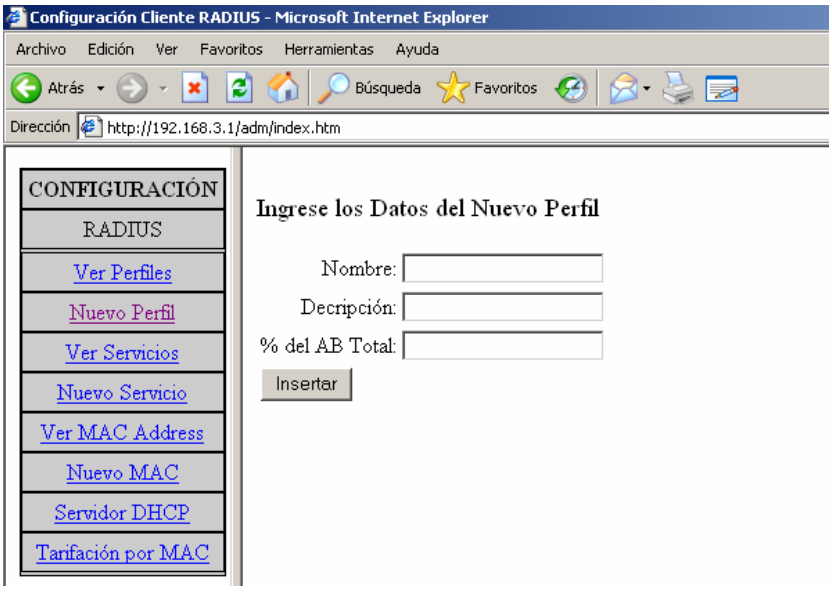

Figura 2.8 Menú de configuración para crear un nuevo perfil

La Figura 2.8 muestra el menú de creación de un nuevo perfil. Para crear un perfil se deben ingresar, el Nombre del perfil, una Descripción y el porcentaje del ancho de banda para ese perfil, cabe mencionar que se realizará una verificación para comprobar que el porcentaje que se indique más la suma del configurado en los perfiles existentes no supere el 100%.

2.5.4.3 Menú Ver Servicios

Este menú se muestra en la Figura 2.9, en el cual se observa cada uno de los servicios que se encuentran configurados y que existen en la base de datos. A través de esta página se puede eliminar un determinado servicio o modificar un servicio ya existente.

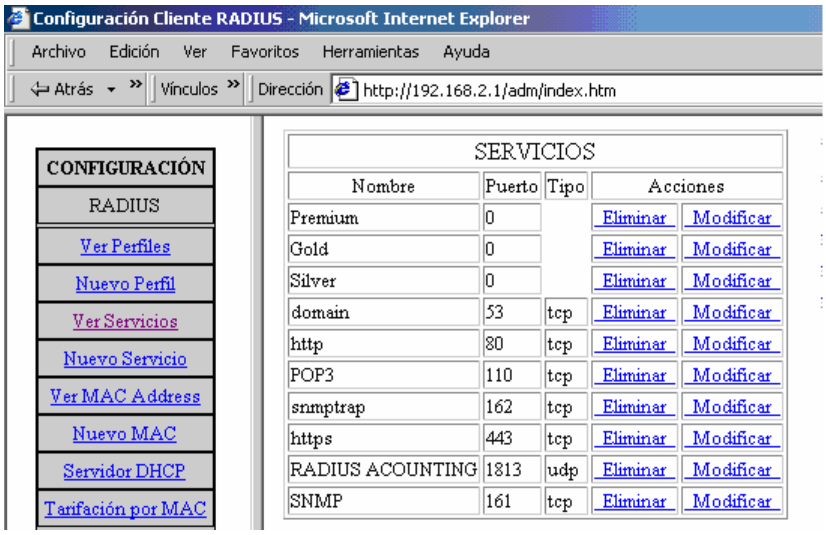

Figura 2.9 Menú de configuración de servicios

2.5.4.4 Menú de configuración Nuevo Servicio

En este menú de configuración se puede ingresar los datos de un nuevo servicio, como son: Nombre, Puerto y Tipo de servicio. En la Figura 2.10 se muestra la pantalla del menú Nuevo Servicio.

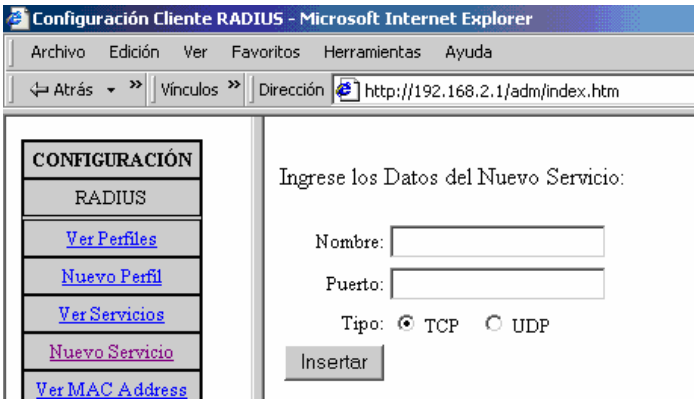

Figura 2.10 Menú de configuración para añadir un nuevo servicio

2.5.4.5 Menú de configuración Ver MAC Address

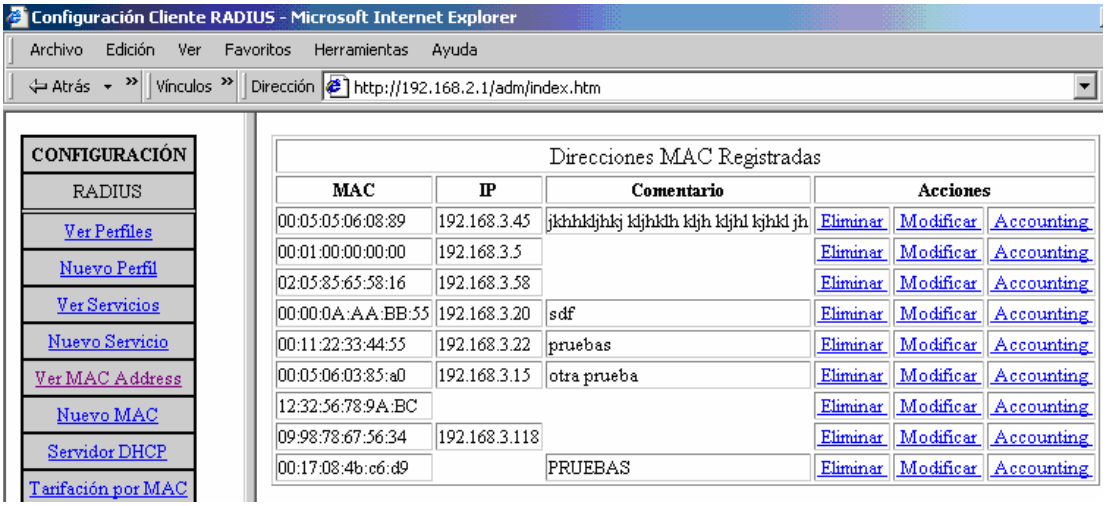

Figura 2.11 Menú de configuración de usuario por dirección MAC

En este menú se lista todas las direcciones MAC y sus correspondientes direcciones IP que se encuentran en el sistema. Permite eliminar al dispositivo, modificar los parámetros de dirección MAC, dirección IP y comentario y a su vez permite realizar una auditoria de utilización por fechas en función de la configuración inicial del cliente RADIUS, es decir poder auditar en términos de utilización del sistema por tiempo o por *bytes* consumidos. En la Figura 2.11 se muestra la pantalla del menú.

2.5.4.6 Menú de configuración de Nueva MAC

En este menú permite realizar un ingreso de un nuevo dispositivo con su respectiva dirección IP a ser asignada por DHCP y a su vez permite ingresar un comentario. En la Figura 2.11 se muestra el contenido de este menú.

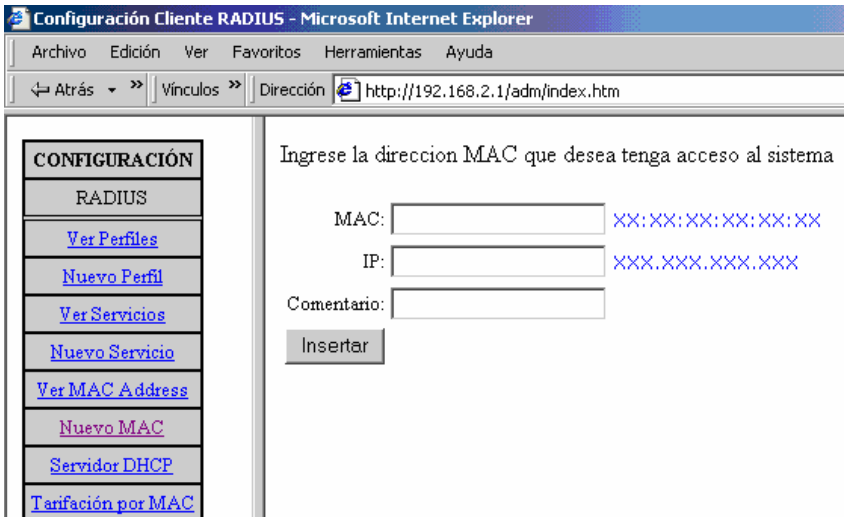

Figura 2.12 Menú de configuración para añadir una nueva dirección MAC al sistema

2.5.4.7 Menú Servidor DHCP

En este menú se lista las direcciones MAC y su correspondiente dirección IP que se encuentran en la base de datos, adicionalmente permite eliminar dispositivos o modificar los ya existentes en la base de datos.

En la parte inferior de la ventana se encuentra un enlace que genera el archivo de configuración del servidor DHCP y a su vez reinicia el servicio con los últimos cambios realizados, (el reiniciar el servidor DHCP no afecta a los usuarios que se encuentren conectados). El contenido del menú Servidor DHCP se muestra en la Figura 2.13.

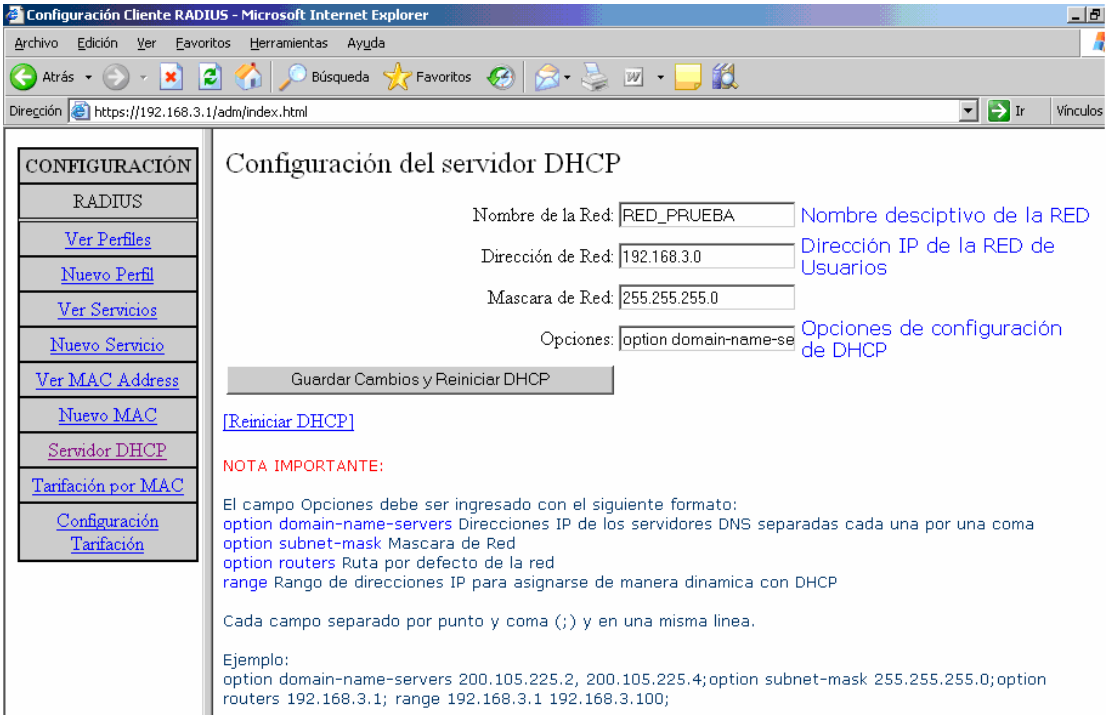

Figura 2.13 Menú de configuración del servicio DHCP

2.5.4.8 Menú Tarifación por MAC

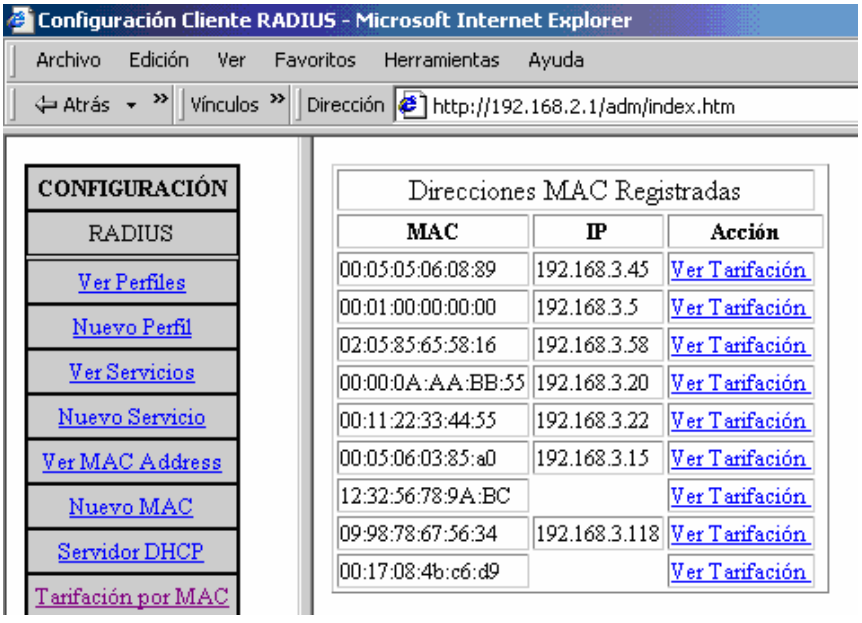

Figura 2.14 Menú que permite seleccionar el dispositivo para realizar la tarifación

En este menú se puede escoger uno de los dispositivos y realizar una tarifación de la ocupación del sistema. En la Figura 2.13 se muestran las opciones de este menú.

2.5.4.9 Menú Configuración Tarifación

En este menú se configuran los valores del costo de la ocupación ya sea por tiempo o por *byte* y se define el tipo de tarifación a realizarse (por *byte* o por tiempo). En la Figura 2.15, se presenta el Menú de Configuración Tarifación.

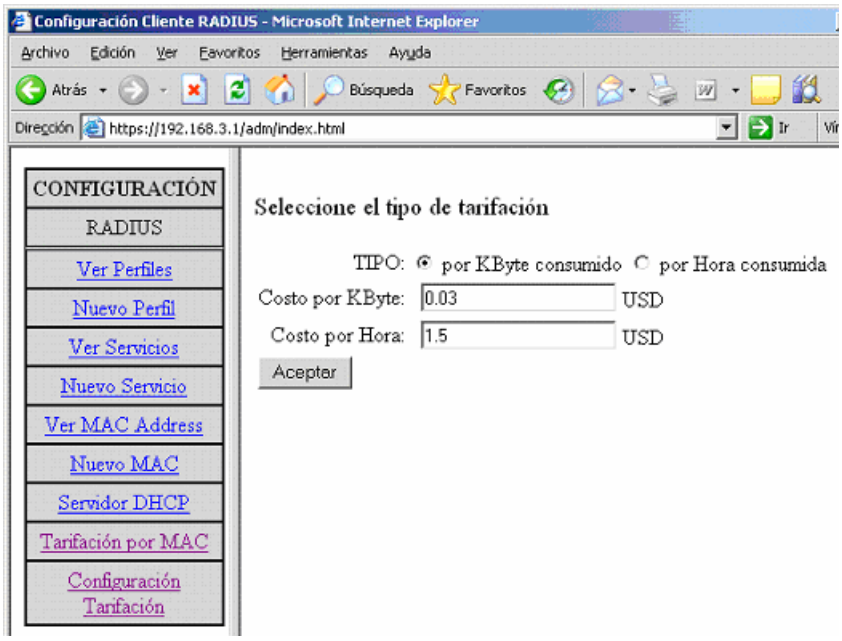

Figura 2.15 Menú que permite seleccionar el dispositivo para realizar la tarifación

2.5.4.10 Estructura de archivos

Dentro de la estructura de archivos se tiene primero; la carpeta de formularios que contiene los archivos empleados como interfaz de usuario que son los que invocan al código, en la carpeta código se encuentran los archivos que ejecutan las diferentes funciones, estas funciones se encuentran en archivos que están almacenados en la carpeta fnc, y adicionalmente se tiene una carpeta de nombre dhcp que contiene archivos de configuración y de funciones del servidor DHCP.

En el Anexo E se muestran los nombres y una descripción de los formularios que se encuentran en el directorio frm.

En la tabla 2.4 se presenta la interacción de los diferentes archivos dentro de la interfaz de administración.

FORMULARIOS	CODIGO	CONFIGURACION	DHCP	FUNCIONES
Carpeta frm	Carpeta cdg	Carpeta cfg	Carpeta d.C.	Carpeta fnc
				sql.php
bor_mac.php	bor_mac.php			bor_mac_sql($id_pc)
bor_perfil.php	bor_perfil.php			bor_perfil_sql($id_perfil)
bor_serper.php	bor_serper.php			bor_serper_sql($id_perfil, $id_servicio)
bor_servicio.php	bor_servicio.php			bor_servicio_sql($id_servicio)
in_dhcp.php		dhcpd.conf	crear_dhcpconf($link)	conectar()
				funciones.php
ins_ipmac.php	Ins_ipmac.php			validar_mac($mac)
				sql.php
				ins_mac_sql($mac, $ip, $comentario)
ins_perfil.php	Ins_perfil.php			ins_perfil($nombre, $descripcion)
ins_servicio.php	Ins_servicio,php			ins_servicio($nombre, $puerto,$tipo)
				fundiones.php
mod_ipmac.php	mod_ipmac.php			valida_mac($mac), ip_valida($ip)
				sql.php
				mod_mac_sql(&id_pc, $mac, $ip, $comentario)
mod_servicio.php				Datos_servicio_sql($id_servicio)
mos_acc.php	costos.php			mac_id_sql($id_pc)
				consumomac_sql($id_pc)
mos_ipmac.php				mos_ipmac_sql()
mos_mactar.php				mos_ipmac_sql()
mos_perfil.php	genera_htb.php	htb_gw.txt		mos_perfil()
mos_serper.php				mos_serper_sql($id_perfil)
mos_servicio.php				mos_servicio_sql()
cfg_tar.php	cfg_tar.php			datos_costos_sql()
				actualiza_tar()

Tabla 2.4 Tabla de estructura de archivos y sus respectivas funciones

2.5.4.11 Servidor DHCP

Para generar el archivo de configuración del servidor DHCP se emplea la función crear_dhcp() ubicada en el archivo /opt/lampp/htdocs/adm/dhcp/fnc_dhcp.php; la

información para crear el archivo se la toma de la base de datos *gateway;* de las tablas: dhcp donde se encuentran la configuración de servidor DHCP, y pc_validos donde se encuentran las direcciones MAC e IP de los usuarios registrados (el detalle los campos de las dos tablas se describe en “2.5.3.1.6” y “2.5.3.1.5” respectivamente).

El archivo dhcpd.conf se crea de tal manera que únicamente los dispositivos cuyas direcciones MAC han sido colocadas como válidas, podrán recibir una dirección IP de forma dinámica desde el servidor DHCP colocado en el segmento de red de los usuarios.

El archivo de configuración se crea en la carpeta /opt/lampp/htdocs/adm/dhcp/ por lo que fue necesario crear el enlace simbólico: /etc/dhcpd.conf que apunte a este archivo. A continuación se presenta el comando a ejecutar para la creación de este enlace simbólico:

```
# ln –s /opt/lampp/htdocs/adm/dhcp/dhcpd.conf /etc/dhcpd.conf
```

2.5.5 PROGRAMACIÓN DE LOS PERFILES DE USUARIO

En la base de datos se crean los perfiles de usuario, en el caso del presente proyecto de titulación serán tres como se describió en la política de seguridad correspondiente; cada perfil posee un conjunto de servicios y un determinado ancho de banda.

Mediante la interfaz de administración se ingresa toda la información necesaria dentro de la base de datos, para que se creen dinámicamente las reglas de *iptables* una vez que se registre con éxito algún usuario en el sistema.

En el archivo inicio.php se encuentra el código necesario que permite validar la información de autenticación proporcionada por el usuario y con la ayuda de la información almacenada en las tablas: per_serv, servicios y perfiles, se generan

de forma automática cada una de las reglas que serán aplicadas a los usuarios que se ha registrado con éxito en el sistema, el conjunto de reglas que se apliquen será diferente de acuerdo al perfil que le corresponda a cada usuario.

Los perfiles de usuario pueden ser modificados acorde la necesidad mediante el uso de la interfaz de administración, la manipulación de los perfiles es una tarea muy intuitiva.

2.6 ASIGNACIÓN DE ANCHO DE BANDA

En cada uno de los perfiles creados existe la posibilidad de asignar una cantidad de ancho de banda diferente.

La cantidad de ancho de banda asignado estará referido en valor a un porcentaje del ancho de banda total disponible, es decir no se podrá tener en ningún caso un valor mayor al cien por ciento. De igual forma no se podrá asignar un porcentaje que al ser sumado con los porcentajes de los perfiles ya existentes supere el valor del cien por ciento.

Para implementar el control de ancho de banda por perfil se empleó la disciplina de colas HTB. En la creación del *script* para la asignación del ancho de banda se emplea la información ingresada en la base de datos mediante la interfaz de administración; además el ancho de banda total disponible debe ser configurado en el archivo /opt/lampp/htdocs/adm/cfg/cfg.php.

El archivo htb_gw.php se encarga de generar y ejecutar el *script* (htb_gw.txt) de configuración para realizar el control de ancho de banda por perfil.

Un ejemplo del *script* de configuración para control de ancho de banda se muestra en el ANEXO F.

2.7 IMPLEMENTACIÓN DEL SISTEMA DE TARIFACIÓN

El sistema de tarifación funciona de la siguiente manera: cuando se llama desde el menú de administración a Tarifación por MAC, se invoca el archivo mos_mactar.php y en la pantalla se muestra una tabla con el listado de todas las direcciones MAC registradas, en la tabla se encuentran los campos MAC, IP y Acción.

En el campo Acción se tiene la opción: Ver Tarifación que permite invocar al archivo mos_acc.php el cual muestra el reporte de tarifación, ya sea por *kbytes*, o por tiempo. La selección de tarifación por *kbyte* o por hora y el correspondiente costo se los configura en el menú Configuración Tarifación.

En el reporte de tarifación se muestra: que usuario se autenticó, la hora de inicio de la sesión (Tiempo *Login*), la hora a la que se finalizo la sesión (Tiempo *Logout*), un detalle de los consumos realizados por sesión sea en *bytes* o tiempo, el valor total de lo consumido y el valor total en dólares de acuerdo con el costo configurado.

La Figura 2.16 presenta un reporte de tarifación de un usuario del sistema cuya dirección MAC es 00:17:08:4b:c6:d9 y en este caso la tarifación se está realizando en función de tiempo de consumo y no por *byte* consumido.

Consumo registrado de la MAC: 00:17:08:4b:c6:d9

Usuario	Tiempo Login	Tiempo Logout	Consumo de Tiempo
pablo	2007-02-25 12:32:55	2007-02-25 12:35:55	0 Dia(s) 00:03:00
cesar	2007-02-25 12:38:51	2007-02-25 12:41:05	0 Dia(s) 00:02:14
pablo	2007-02-25 12:41:52	2007-02-25 12:42:55	0 Dia(s) 00:01:03
pablo	2007-02-25 12:53:19	2007-02-25 12:53:49	0 Dia(s) 00:00:30
pablo	2007-02-25 12:54:18	2007-02-25 13:02:48	0 Dia(s) 00:08:30
CONSUMO TOTAL [tiempo]			0 Dia(s) 00:15:17
Costo Por Hora [USD]			0.000694444444444
COSTO TOTAL [USD]			0.636805555556

Figura 2.16 Reporte de tarifación por consumo de tiempo

En el ANEXO G, se presentan los archivos de configuración empleados en la implementación de la interfaz de administración.

2.8 IMPLEMENTACIÓN DEL SERVIDOR *DIAL-UP*

El servidor *dial-up* se lo implementará empleando un computador con sistema operativo *Windows XP*, el cual se ha configurado para permitir conexiones entrantes a través del MODEM, este servidor permitirá el acceso a la red local una vez que el usuario se autentique con un nombre de usuario y clave configurados en este servidor.

El usuario que desee acceder a la red empleando este servidor debe configurar en su computador una "Conexión de acceso telefónico" con los datos de nombre de usuario, clave, y el número telefónico de la línea a la que esta conectado el MODEM del servidor *dial-up;* cuando el servidor reciba la llamada desde el equipo remoto contestará automáticamente y se encargará de establecer la conexión, si la información proporciona del nombre de usuario y clave es correcta.

Una vez que se encuentre establecida la comunicación remota el usuario tendrá acceso hacia la red LAN, y deberá autentificarse en el sistema de autenticación local (Cliente RADIUS), para tener acceso a los servicios de red.

En este punto el usuario será tratado como un usuario de la red local y para realizar el registro de los consumos se empleará la dirección IP y la dirección MAC que el servidor *dial-up* tenga en la red local. Se podrá realizar un mayor control de acceso al emplear un servidor *dial-up* que permita colocar diferentes direcciones IP por cada uno de sus MODEMs. En el ANEXO H se presenta el procedimiento de la implementación del servidor de acceso remoto, con sus pantallas de configuración correspondientes.

2.9 CONFIGURACIÓN E IMPLEMENTACIÓN DE SEGURIDAD EN LOS SEGMENTOS DE RED

En la Figura 2.17 se presenta un diagrama lógico de la red en la cual el sistema será implementado, se muestran los protocolos a emplear entre los servidores, entre los usuarios y el cliente RADIUS, entre el punto de acceso y los usuarios inalámbricos, entre el servidor *dial-up* y el usuario remoto; y la ubicación del administrador de red y los protocolos que empleará para administrar el sistema ya sea de forma local o de forma remota.

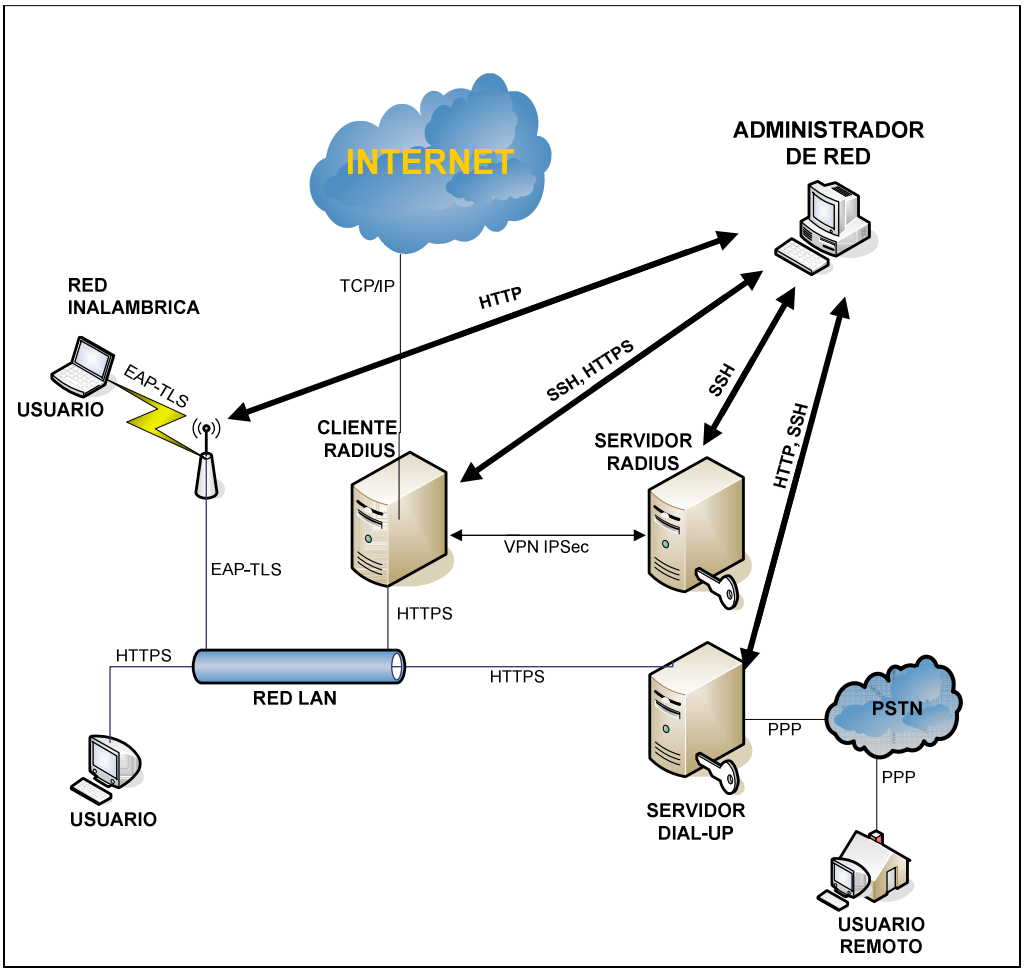

Figura 2.17 Diagrama de esquema de seguridad de servidores empleado

También se muestran dos nubes que representan a la red de Internet y a la PSTN (*Public Switching Telephone Network)*. La red de Internet en este caso será la red a la cual se controlará el acceso desde la red LAN, y la red PSTN será la red empleada para las conexiones de los usuarios remotos empleando MODEMs telefónicos.

2.9.1 CONFIGURACIÓN DEL PUNTO DE ACCESO Y DE LOS CLIENTES INALÁMBRICOS

En la implementación del segmento de red inalámbrico, para proteger la información intercambiada en el medio inalámbrico se empleará WPA con 802.1X (802.1X/EAP y el tipo de EAP será TLS).

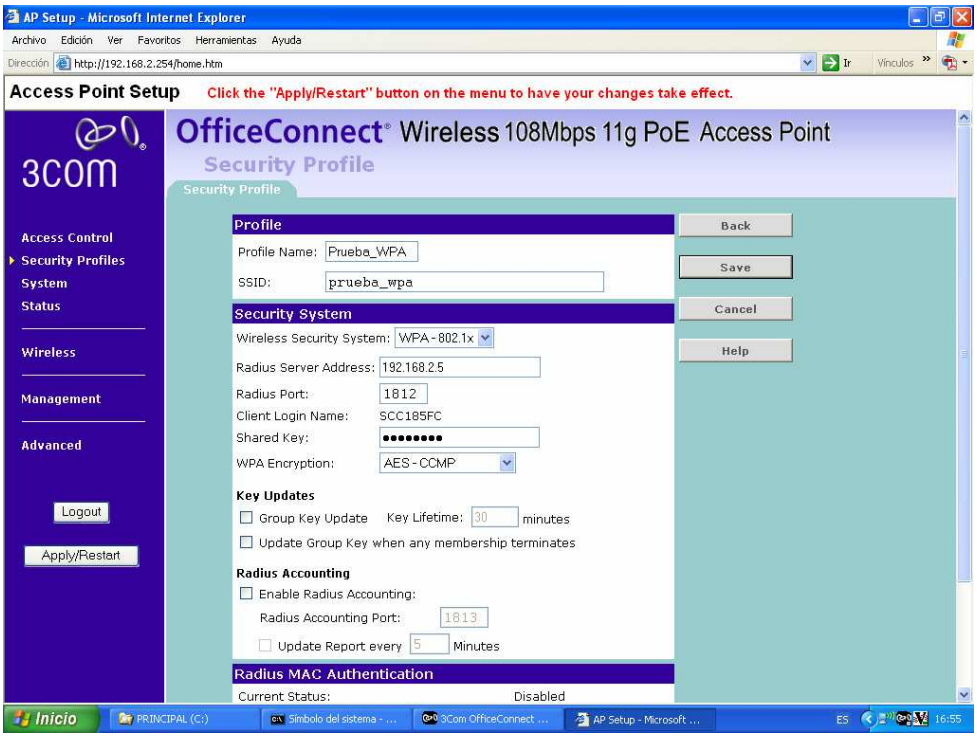

Figura 2.18 Pantalla de página web de configuración del *Access Point*

El equipo utilizado para la implementación es el punto de acceso inalámbrico 3Com modelo Office Connect 108Mbps 11g PoE (en el ANEXO K se muestra las características del punto de acceso 3Com) el cual fue configurado de la siguiente manera:

Se creo un perfil Prueba_WPA, con SSID prueba_wpa, en la seguridad del sistema se escogió la opción WPA-802.1x y se completo los campos solicitados con relación al servidor RADIUS, como se muestra en la Figura 2.18.

Para la configuración en el lado de los clientes, es necesario instalar el certificado raíz de la autoridad certificadora y un certificado para el cliente. Se procedió a crear dichos certificados con el paquete OpenSSL 0.9.7 de Linux, haciendo uso de los *scripts* que se presentan en el ANEXO I empleados para la creación de los certificados digitales necesarios para la autenticación entre los usuarios, el punto de acceso y el servidor RADIUS. Adicionalmente se presenta el procedimiento de instalación de los certificados en los clientes y en el servidor RADIUS.

2.9.2 SEGURIDAD EN EL ACCESO PARA ADMINISTRACIÓN DE SERVIDORES

Existe un par de formas de acceder al *shell* de LINUX/UNIX de forma remota, una de las formas es empleando el establecimiento de una sesión telnet hacia el equipo al cual se quiere establecer la conexión al *shell*. El acceder a una cuenta de *shell* a través de telnet posee una vulnerabilidad y riesgo, ya que al establecer este tipo de sesión, se está intercambiando claves en texto plano y cualquier intruso malicioso dentro de la red pude interceptar estos datos y utilizarlo de una forma dañina. Por esta razón es necesario emplear un programa más sofisticado que permita conectarse a *hosts* remotos de forma segura.

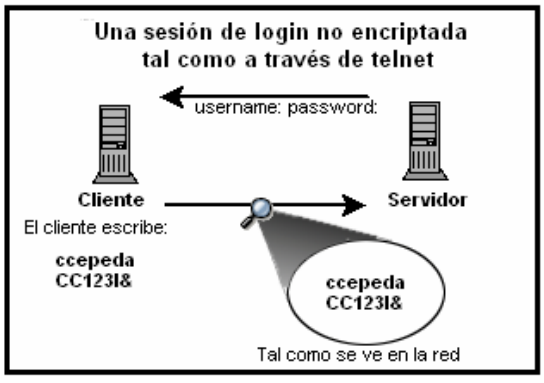

Figura 2.19 Sesión de shell no segura, empleo de telnet

La Figura 2.19 presenta el empleo de telnet para acceso a un *host* remoto:

SSH (*Secure Shell*), es un protocolo seguro y un conjunto de herramientas para reemplazar otras más comunes (inseguras). Fue diseñado desde el principio para ofrecer un máximo de seguridad y permitir el acceso remoto a servidores de forma segura. SSH se puede utilizar para asegurar cualquier tráfico basado en red. Puede emplear diferentes formas de rangos de encripción desde 512 bits hasta 32768 bits, e incluye encripción como AES (*Advanced Encryption Scheme*), Triple DES, *Blowfish*, CAST128 o Arcfour.

Por defecto ssh trae un fichero de configuración, /etc/sshd/sshd_config, en el cual se puede restringir con facilidad a quién se le permite el acceso, qué *hosts*, y qué tipo de autenticación está permitido utilizar. Se puede conseguir un mayor detalle de lo que se puede realizar con el archivo de configuración empleando la ayuda de LINUX “man”.

La Figura 2.20 presenta el empleo de ssh para acceso a un *host* remoto.

Figura 2.20 Sesión de shell segura, empleo de SSH

El servicio viene ya instalado en las distribuciones de Linux y listo para usar, por lo que no se realizó ningún procedimiento adicional para levantar esta característica en los servidores.

2.9.3 SEGURIDAD ENTRE SERVIDOR Y EL CLIENTE RADIUS

Las VPNs transmiten sobre IP usando datagramas (UDP) en la capa de transporte, creando un canal seguro a través de Internet hasta la dirección destino. La mayoría de las implementaciones de *software* libre de VPN incorporan estándares abiertos y encriptación para enmascarar aún más el tránsito de datos.

Cuando un paquete es transmitido a un cliente, lo envía a través del *router* o *gateway*, el cual posteriormente añade información de cabecera para el enrutamiento y autenticación llamado cabecera de autenticación (AH). Los datos son encriptados y encapsulados con instrucciones de cifrado y manejo llamado *Encapsulating Security Payload* (ESP). El *router* VPN receptor extrae la información y la enruta a su destino, sea este una estación de trabajo o un nodo en la red. Usando una conexión de red a red, el nodo receptor en la red local recibe los paquetes descifrados y listos para ser procesados. El proceso de encripción/descifrado en una conexión VPN de red a red es transparente al nodo local.

2.9.3.1 Implementación IPSec de computador a computador

IPSec se puede configurar para conectar un escritorio o estación de trabajo a otro a través de una conexión computador a computador. Este tipo de conexión utiliza la red a la cual están conectados los computadores para crear un túnel seguro entre ellos.

Los requerimientos de una conexión computador a computador son mínimos, como lo es la configuración de IPSec en cada computador. Los computadores necesitan de una conexión dedicada entre ellos pudiendo ser una LAN, WAN o Internet.

El primer paso en la creación de una conexión es reunir la información del sistema y de la red de cada estación de trabajo. Para una conexión computador a computador, necesita la información siguiente:

- La dirección IP para ambas computadoras a intervenir en el túnel.
- Un nombre único para identificar la conexión IPSec y distinguirla de los otros dispositivos o conexiones.
- Una llave encriptada fija o una generada automáticamente.
- Una llave compartida, que se utiliza para iniciar la conexión e intercambiar las llaves de encriptación durante la sesión.

Para asegurar el segmento de red entre el servidor de autenticación y el cliente RADIUS, se debe realizar la implementación de un túnel IPSec, haciendo uso del paquete ipsec-tools versión 0.5-2.

Se empleará el *script* ipsec.conf, en las dos computadoras que establecerán el túnel IPSec, y para ejecución del mismo, en línea de comandos se debe escribir el siguiente comando:

```
# setkey –f /etc/ipsec.conf
```

El contenido del *script* ipsec.conf se presenta el ANEXO J.

2.9.4 SEGURIDAD ENTRE LOS USUARIOS Y EL CLIENTE RADIUS

Se creó una página de autenticación de usuarios, la misma que está implementada en lenguaje PHP. Para añadir seguridad al intercambio de credenciales entre el usuario y el cliente RADIUS, esta página de ingreso de datos se presenta al usuario empleando el protocolo https. Las credenciales presentadas son el nombre de usuario y la clave.

El protocolo https es la versión segura del protocolo http. El sistema https utiliza un cifrado basado en *Secure Socket Layer* (SSL) para crear un canal cifrado para el tráfico de información sensible que emplea el protocolo http.
Cabe mencionar que el uso del protocolo https no impide que se pueda utilizar http. Es utilizado principalmente por entidades bancarias, tiendas en línea, y

cualquier tipo de servicio que requiera el envío de datos personales o contraseñas a través de formularios por Internet. El puerto estándar para este protocolo es el 443.

2.10 COMPARACIÓN CON SOLUCIONES SIMILARES Y ANÁLISIS DE COSTOS DE LA SOLUCIÓN

Se empleó como referencia las siguientes aplicaciones de *software* PatronSoft FirstSpotTM *software* desarrollado para plataforma *Windows* y Air Marshal de IEA *Software*, este último desarrollado para plataforma Linux y Sun.

Las soluciones comerciales mencionadas se emplearán para realizar tanto una comparación de costos involucrados en el proceso de implementación de cada una de estas soluciones y para realizar un análisis comparativo de las ventajas, beneficios y limitaciones de cada una de ellas, en comparación con el desarrollo planteado en el presente tema de titulación.

2.10.1 SOLUCIONES COMERCIALES SIMILARES

A continuación se va ha realizar una breve descripción de dos soluciones de *software* que permiten realizar funciones similares que las del cliente RADIUS razón de este proyecto de titulación.

2.10.1.1 Solución FirstSpot de PatronSoft

PatronSoft FirstSpotTM es un producto basado en *Windows* para tecnologías WLAN, dedicado a la gestión y monitorización de redes *Wireless*. FirstSpot™ es un *software* de fácil instalación y mantenimiento, capaz de limitar el acceso de los usuarios a la red mediante un robusto sistema de autenticación, así como también el tiempo de uso y el ancho de banda que van a usar. Este *software* permite al administrador de la red tener una seguridad excelente sobre su red y sobre sus usuarios, de una forma cómoda y sencilla.

FirstSpot™ es también un sistema totalmente escalable y adaptable a todo tipo de redes WLAN o HotSpots ya que no está sujeto a ningún hardware ni topología jerárquica, con lo que la posibilidad de emplearlo es alta.

La versión 4 incorpora las siguientes funcionalidades:

- **Control de Acceso:** Bloquea rangos de IP (Útil para bloquear Intranet), el bloqueo se realizará a nivel de dirección IP.
- **Filtrador de puertos:** El administrador puede activarlo, para limitar el acceso a ciertas aplicaciones (por ejemplo solo el puerto 80, http), el filtro se realizará a nivel de servicio que se solicita puerto TCP o UDP.
- **El servidor DHCP:** soporta la combinación de IP estática a mapeo de MAC y asignación automática de IP.
- **Accesos múltiples al sistema:** permite compartir una misma cuenta de modo anónimo, es decir que los participantes no se enteren que su cuenta esta siendo empleada por otro usuario.
- **Soporte de tarjetas de prepago:** permite añadir usuarios con un simple *click*.
- **Rastreo de URL:** recupera la dirección URL solicitada inicialmente por el usuario y una vez que se autentica el usuario lo regresa a esa URL.

Mejoras para el usuario:

- Se ha añadido el soporte de tarjetas de crédito Authorize.net
- Uso de la MAC como nombre de usuario, los usuarios únicamente ingresarán una contraseña. También soporta accesos pasivos, de manera que el usuario no ingresará ni el nombre de usuario ni la contraseña.
- Añadido el soporte para imprimir a través de *PrinterOn* en *Hotspots*.
- Ofrece Calidad de Servicio (QoS) para ciertas aplicaciones (por ejemplo VoIP).
- Ofrece *Roaming* de SMTP, de manera que los usuarios no tienen que modificar su configuración en el Outlook para realizar los envíos de mails.

- Ofrece la asignación dinámica selección de lenguaje: Firstspot se presenta en los usuarios finales en un lenguaje u otro en función de los parámetros de idioma establecidos en el PC del usuario.

Como fortalezas de la presente aplicación de *software* se puede mencionar que permite realizar un control ancho de banda por usuario, no se requiere de aplicaciones de *software* adicionales en el lado del cliente, es basado en *Windows*, soporta autenticación por RADIUS y puede trabajar WiFi y *Ethernet*.

2.10.1.2 Solución Air Marshal de IEA *Software*, inc

Software desarrollado para plataformas Linux y Sun. Air Marshal proporciona a los usuarios la habilidad de ganar acceso a una red *Ethernet* cableada o inalámbrica empleando su explorador de Internet.

Todo el tráfico es redireccionado a una página de autenticación donde los usuarios deberán ingresar su nombre de usuario y contraseña para acceder a la red.

Air Marshal emplea RADIUS para autenticar los clientes, autorizar acceso y cuantificar el uso de red. Se integra suavemente con todos los servidores RADIUS y sistema de tarifación que soportan RADIUS. Esto permite al portal tomar ventajas de las características avanzadas tales como *roaming*, control de concurrencia, y explotar la amplia variedad de datos disponibles y características de tarifación.

Características y beneficios

- RADIUS autenticación y auditoria, compatible con autenticación existente y sistemas de tarifación.
- Soporta gran variedad de servidores RADIUS.
- Autenticación CHAP basada *Java Script*, seguridad adicional a SSL.
- Aseguramiento de intercambio de datos empleando SSL.
- Configurable a través de una Interfaz HTML.

- Presenta el estado de los usuarios, estadísticas de utilización, como tiempo usado y tiempo restante.
- Interfaz de administración integrada, basada en web, mira quien está en línea, uso de ancho de banda en tiempo real.
- Permite Configurar diferentes niveles de acceso en función del usuario y la clave ingresada, al interactuar con el *firewall* estándar de Linux y herramientas de ancho de banda.

Lleva un registro de la utilización del sistema por cada usuario en base a su dirección MAC, evitando de esta manera que hagan un mal uso de la infraestructura de comunicaciones. Adicionalmente permite ver cuando un usuario está activo dentro del sistema.

2.10.2 ANÁLISIS DE COSTOS

A continuación se presenta un análisis de costos del proceso de implementación de las soluciones anteriormente mencionadas y del desarrollo propuesto en el presente tema de titulación.

Para cada caso se considerará el *hardware* a ser empleado por cada aplicación de *software*, ya que cada una de las aplicaciones tiene sus propios requerimientos mínimos necesarios.

Una consideración general que se hará es que todas las soluciones emplearán el mismo servidor de autenticación RADIUS. Por lo que un costo adicional a ser considerado en cada caso es el costo correspondiente al servidor RADIUS, se considera únicamente el costo del *hardware* ya que en la parte de *software* se emplea el servidor FreeRADIUS instalado sobre el sistema operativo LINUX Fedora Core 3, ambos de libre distribución.

Se considera en los costos el valor de la mano de obra especializada que se emplea, ya que para poder implementar una solución de este tipo al menos se debe tener un conocimiento básico de sistemas y de comunicaciones.

Como precio por hora de la mano de obra se definió 50 USD, valor promedio en base a los costos de mano de obra por hora aplicados por empresas integradoras de tecnología como La Competencia SA, Uniplex y DOS Compuequip.

En el caso del costo de capacitación se ha definido el valor por hora de 70 USD, este valor fue tomado en referencia a los valores por hora de capacitación cobrados por las empresas de comunicaciones anteriormente mencionadas

Para el caso FirstSpot y AirMarshall, como requerimiento de hardware lo único que se requiere es un computador con dos interfaces de red, por lo que se considerará esto en los costos asociados.

En el caso del servidor RADIUS se ha considerado el valor del servidor más dos horas de mano de obra para la instalación de sistema operativo y para la instalación del servidor RADIUS.

En el caso de FirstSport, se deberá considerar un valor adicional correspondiente al sistema operativo *Windows.*

2.10.2.1 Costos de implementación empleando FirstSpot TM

FirstSpot Price List (per server)				
	New License			
◉	FirstSpot Advanced Edition 4.x with 1-year maintenance contract [see #1]	Price : 1,343 USD	4ADV-LM	
○	FirstSpot Standard Edition 4.x with 1-year maintenance contract	Price : 593 USD	4STD-LM	
○	FirstSpot Advanced Edition 4.x	Price : 895 USD	4ADV-L	
○	FirstSpot Standard Edition 4.x [see #2]	Price : 395 USD	4STD-L	
	Trade-Up to Advanced Edition [see #3]			
○	Trade-up from Standard Edition 4.x to Advanced Edition 4.x	Price : 632 USD	4STDADV-T	
○	Trade-up from FirstSpot Standard Edition 4.x to Advanced Edition 4.x (with a valid maintenance contract) [see #4]	Price : 948 USD	4STDADVM-T	
	To upgrade from previous version (3.x) of FirstSpot, please click here.			
	To purchase maintenance contract separately, please click here.			

Tabla 2.5 Precios de lista de FisrtSpot[5]

[5] Referencia para costo de FirstSpot http://www.patronsoft.com/firstspot/buy_now.html 26/04/2007

En la Tabla 2.5 se presenta la lista de precios correspondiente a los costos involucrados, con respecto a la solución FirstSpot.

2.10.2.1.1 Contrato de Mantenimiento

El contrato de mantenimiento consiste en un soporte y mantenimiento necesario para poder implementar la solución exitosamente y FirstSpot. El contrato incluye lo siguiente:

- Soporte por un año vía *email* (support@patronsoft.com), o a través de un soporte de acceso remoto hacia el computador que tenga instalado el *software* vía VNC o Escritorio Remoto, siempre y cuando el usuario haya otorgado la respectiva autorización.
- Actualizaciones de versiones durante el período de contrato.
- Servicio de corrección de errores en las versiones
- Acceso a versiones de prueba

Para realizar el análisis de costo, se considera la versión de *software* más avanzada, ya que la misma proporciona funcionalidades interesantes, como controles de acceso con filtros por dirección MAC, control de ancho de banda por usuario, monitoreo en tiempo real de usuarios, asignación de direcciones IP de forma dinámica, accesos múltiples con una sola contraseña y retorno a la página web inicialmente solicitada por el usuario una vez que se autentica.

El período de garantía se considera de un año a partir de la fecha de entrega de la implementación probada y funcionando de forma adecuada.

Con las premisas anteriormente mencionadas, en al Tabla 2.6 se presentan los costos asociados en la implementación de esta solución.

FistSpot			
Producto	**Costo Unitario**	**Cantidad**	**Costo**
Servidor RADIUS Inspiron 530s[6] Intel®Pentium® dual-core processor E2140 (1.60GHz) 1GB Dual Channel6 DDR SDRAM 160GB Serial ATA Hard Drive (7200RPM)	$ 800,00	1	$ 800,00
Ingeniería de preparación de Servidor RADIUS	$ 100,00	1	$ 100,00
Sistema Operativo Windows XP Profesional	$ 200,00	1	$ 200,00
Inspiron 530s Intel®Pentium® dual-core processor E2140 (1.60GHz) 1GB Dual Channel6 DDR SDRAM 160GB Serial ATA Hard Drive (7200RPM)	$ 800,00	1	$ 800,00
FirstSpot Advanced Edition 4.x with 1-year maintenance contract	$ 1.343,00	1	$ 1.343,00
Ingeniería en la implementación (Mano de obra) 50USD/Hora	$ 50,00	8	$ 400,00
Capacitación Administrador 70USD/Hora, 50 dólares por persona adicional[7]	$ 70,00	8	$ 560,00
		Costo Total	$ 4.203,00
		IVA 12%	$ 504,36
		Total	$ 4.707.36

Tabla 2.6 Costos Implementación FirstSpot[8]

2.10.2.2 Costos de implementación empleando Air Marshal de IEA *software*, Inc.

El la Tabla 2.7 se presenta la lista de precios de los costos del *software* AIR MARSHAL DE IEA *SOFTWARE*, INC.

Concurrent Sessions	Cost per Server (USD)
50	$595.00
Unlimited	$895.00

Tabla 2.7 Precios de *software* Air Marshal [9]

Air Marshal es un *software* licenciado por servidor. El número de sesiones concurrentes corresponde al número máximo de usuarios que pueden estar

[6] http://www.dell.com

[7] Valor establecido de un promedio de costos por hora de capacitaciones de empresas integradoras de servicios (La competencia SA, Uniplex y DOS Compuequip) para cuatro personas.

[8] Tablas 2.5

[9] Referencia a costos involucrados en la adquisición del software AIR MARSHAL http://www.iea-software.com/products/pricing.cfm?product=airmarshal#airmarshal 26/04/2007

registrados al mismo tiempo. Para el análisis de costos se considera la licencia para sesiones concurrentes ilimitada.

Con respecto al valor adicional relacionado al mantenimiento, en la Tabla 2.8 se presenta los valores correspondientes a los contratos de mantenimiento del *software*.

Offering	Email Support	Telephone Support	Major Upgrades	Cost (USD)
Yearly Email Support	Yes	No	No	$695/year
Yearly Basic Support	Yes	9-5 PST	No	$1,695/year
Yearly Extended Support	Yes	9-5 PST and Emergency 24x7	Included	$2,695/year
Quickstart Program	4 hour training session over two days covering Installation/configuration and daily use of the system by accounting and CSR staff.			$495 (one-time)

Tabla 2.8 Valor de los contratos de mantenimiento para Air Marshal [10]

Los usuarios nuevos pueden hacer uso del soporte de sesenta días gratuitos, contados a partir del día de adquisición del *software*. El soporte adquirido consiste de soporte por un solo sitio, esto quiere decir que si el *software* se encuentra instalado para una misma organización en varias dependencias se deberá adquirir un contrato por cada sitio.

Para realizar la comparación en lo referente a costos se considera emplear la versión de usuarios concurrentes ilimitados; que se adquirirá un soporte con actualizaciones y que se invertirá en un curso de capacitación para el personal, con estas condiciones el costo involucrado en el análisis de costos es el que se muestra en la Tabla 2.9.

[10] Referencia a costos involucrados en la adquisición de soporte del software AIR MARSHAL http://www.iea-software.com/products/pricing.cfm?product=airmarshal#airmarshal
26/04/2007

Air Marshal			
Producto	**Costo Unitario**	**Cantidad**	**Costo**
Servidor RADIUS Inspiron 530s[11] Intel®Pentium® dual-core processor E2140 (1.60GHz) 1GB Dual Channel6 DDR SDRAM 160GB Serial ATA Hard Drive (7200RPM)	$ 800,00	1	$ 800,00
Ingeniería de preparación del servidor RADIUS	$ 100,00	1	$ 100,00
Inspiron 530s Intel®Pentium® dual-core processor E2140 (1.60GHz) 1GB Dual Channel6 DDR SDRAM 160GB Serial ATA Hard Drive (7200RPM)	$ 800,00	1	$ 800,00
Air Marshal v1 para Linux con sesiones concurrentes ilimitadas	$ 895,00	1	$ 895,00
Soporte extendido anualmente	$ 2.695,00	1	$ 2.695,00
4 horas de sesiones de entrenamiento en el transcurso de dos días cubriendo temas de instalación, configuración y administración del sistema.	$ 495,00	1	$ 495,00
Ingeniería en la implementación (Mano de obra) 50USD/Hora	$ 50,00	8	$ 400,00
		Costo Total	$ 6.189,00
		IVA 12%	$ 742,2
		Total	$ 6931,2

Tabla 2.9 Costos de Implementación Air Marshal[12]

2.10.2.3 Costo de implementación de la solución cliente RADIUS en linux

En esta sección se presentará los criterios considerados para poder definir los valores dados a cada uno de los servicios de la Tabla 2.10.

El valor asignado al desarrollo de la aplicación es de 1600 USD, ya que el tiempo invertido en la realización del presente proyecto fue en promedio 2 horas por día considerando una semana laboral durante el período de seis meses. El presente desarrollo busca ser una alternativa de solución más económica, modular y escalable de forma sencilla.

En el valor de ingeniería de implementación se ha manejado el mismo valor por hora de 50 USD y en este caso se ha definido que un tiempo adecuado en el cual se puede dejar la solución implementada y operativa es 8 horas.

[11] http://www.dell.com

[12] Tabla 2.8, Tabla 2.7 y valores definidos en la sección 2.10.2 ANÁLISIS DE COSTOS

Se ha considerado que el período de tiempo de capacitación de 4 horas es un tiempo adecuado para la capacitación de utilización y administración básica del sistema.

La Tabla 2.10 muestra los costos involucrados en la implementación del Cliente RADIUS.

Cliente RADIUS			
Producto	**Costo Unitario**	**Cantidad**	**Costo**
Servidor RADIUS Inspiron 530s[13] Intel®Pentium® dual-core processor E2140 (1.60GHz) 1GB Dual Channel6 DDR SDRAM 160GB Serial ATA Hard Drive (7200RPM)	$ 800,00	1	$ 800,00
Ingeniería de preparación del servidor RADIUS	$ 100,00	1	$ 100,00
Inspiron 530s Intel®Pentium® dual-core processor E2140 (1.60GHz) 1GB Dual Channel6 DDR SDRAM 160GB Serial ATA Hard Drive (7200RPM)	$ 800,00	1	$ 800,00
Implementación de desarrollo con soporte por un año	$ 1.600,00	1	$ 1.600,00
Ingeniería en la implemtación (Mano de obra) 50USD/Hora	$ 50,00	8	$ 400,00
Capacitación de administrador 70USD/Hora, 50UDS por persona adicional	$ 70,00	4	$ 280,00
		Costo Total	$ 3.980,00
		IVA 12%	$ 477,60
		Total	$ 4.457,60

Tabla 2.10 Costos involucrados al implementar el Sistema Cliente RADIUS en LINUX

En el caso del *hardware* empleado, si bien es cierto, la implementación fue probada con un equipo de menores capacidades, la implementación funcionó de forma adecuada. Por lo que se consideró emplear un equipo con las características presentadas en la Tabla 2.10, que es un equipo actual y con características modernas.

El tratar de considerar equipos con características similares a las empleadas en la implementación original, no es práctico pues actualmente equipos con este tipo de características no se encuentran en el mercado.

[13] http://www.dell.com

De igual manera lo que si se mantuvo es el emplear un equipo que supere las características mínimas necesarias en términos de capacidad de procesamiento, memoria y capacidad de almacenamiento.

Algo importante a considerar es que en ningún caso las organizaciones, clientes de este tipo de soluciones estarían de acuerdo en emplear un computador con características menores a las que actualmente se encuentren en el mercado.

El soporte por un año consistirá de un soporte telefónico, en caso de requerir realizar una revisión adicional en el *software* del sistema se lo hará accediendo de forma remota a través de un VPN, escritorio remoto o directamente si el equipo posee una dirección IP pública. El soporte se lo hará en el sentido de soporte de configuración y buen funcionamiento del sistema o como correctivo de algún *bug* del *software*.

El costo de implementación y capacitación son costos estándar que actualmente manejan las empresas de comunicaciones por hora de implementación y de capacitación.

En caso de que en un soporte se detecte impericia del usuario en la administración del sistema, que ocasione daño al funcionamiento del *software* o pérdida del servicio temporal y esto implique una reimplementación del sistema, se realizará un cobro por las horas técnicas involucradas en la reimplementación del sistema con un valor de 40USD + IVA la hora, el soporte cubrirá netamente problemas de configuración y/o *bugs* de sistema en ningún caso manipulación inapropiada.

2.10.2.4 Comparación de costos de implementación de los tres sistemas planteados anteriormente

A continuación se presenta una comparación de costos de implementación de las diferentes soluciones analizadas anteriormente, el criterio de costos ha sido

considerado teniendo similares escenarios en todos los casos. Los valores mostrados en la Tabla 2.11 incluyen el valor del IVA.

Solución	Costo Total
FistSpot	$ 4.707.36
Air Marshal	$ 6.931,2
Cliente RADIUS	$ 4.457,60

Tabla 2.11 Costos totales de las diferentes implementaciones

En la Tabla 2.11 se puede observar claramente que la solución Cliente RADIUS en Linux es una alternativa más barata y como se verá posteriormente cubre un mayor rango de características que las otras soluciones.

2.10.3 Comparación con soluciones comerciales similares

En la Tabla 2.12 se presenta una comparación de las características que ofrece cada uno de los programas analizados.

Revisando cada una de las características listadas, se observa que la solución planteada en el presente proyecto de titulación, proporciona gran parte de las funcionalidades de dos programas diferentes que son soluciones comerciales actuales. El presente proyecto es una alternativa bastante interesante de control de acceso de usuarios, autorización de accesos y adicionalmente al ser implementado con un criterio de modularidad podrá ser ajustado a las necesidades del usuario final.

CARACTERÍSTICA	FIRST SPOT DE PATRON SOFT	MARSHAL DE IEA *SOFTWARE*, INC.	CLIENTE LINUX
Control de acceso, bloqueo de rangos de IP	SI	NO	SI
Filtrado de puertos	SI	NO	SI
DHCP con asignación estática de IP un dispositivo en particular	SI	NO	SI
Accesos múltiples de usuarios	SI	NO	SI
Empleo de tarjetas prepago	SI	NO	NO
Rastreo de url originadota	SI	NO	SI
Acceso pasivo	SI	NO	SI
QoS	SI	NO	SI
Roaming SMTP	SI	NO	NO
Asignación de selección de lenguaje para administración	SI	NO	NO
RADIUS autenticación y auditoria, compatible con autenticación existente y sistemas de tarifación	NO	SI	SI
Soporte de varios servidores RADIUS	NO	SI	SI
Autenticación CHAP basada Java *script*, seguridad adicional a SSL	NO	SI	Autenticación PAP y CHAP estándar
SSL aseguramiento de intercambio de los datos.	NO	SI	SI
Configurable a través de una Interfase HTML	SI	SI	SI
Presenta el estado de los usuarios, estadísticas de registros, como tiempo usado y tiempo restante.	NO	SI	SI
Interfaz de administración integrada, basada en web, mira quien está en línea, consumo de bytes.	NO	SI	SI
Configurables diferente niveles de acceso en función del usuario y la clave ingresada, al interactuar con el *firewall* estándar de Linux y herramientas de ancho de banda.	NO	SI	SI
Monitoreo de sesiones en base a su dirección MAC, evitando abusos de uso, determinando cuanto los usuarios están activos, mayor control de tiempo por sesión.	NO	SI	SI
Control de cantidad de bytes consumidos	NO	SI	SI

Tabla 2.12 Tabla comparativa de características de los programas de control de acceso

CAPÍTULO III

PRUEBAS DE FUNCIONAMIENTO Y ANÁLISIS DE RESULTADOS

CAPÍTULO III

PRUEBAS DE FUNCIONAMIENTO Y ANÁLISIS DE RESULTADOS

3.1 DESCRIPCIÓN DEL ESCENARIO DE PRUEBAS

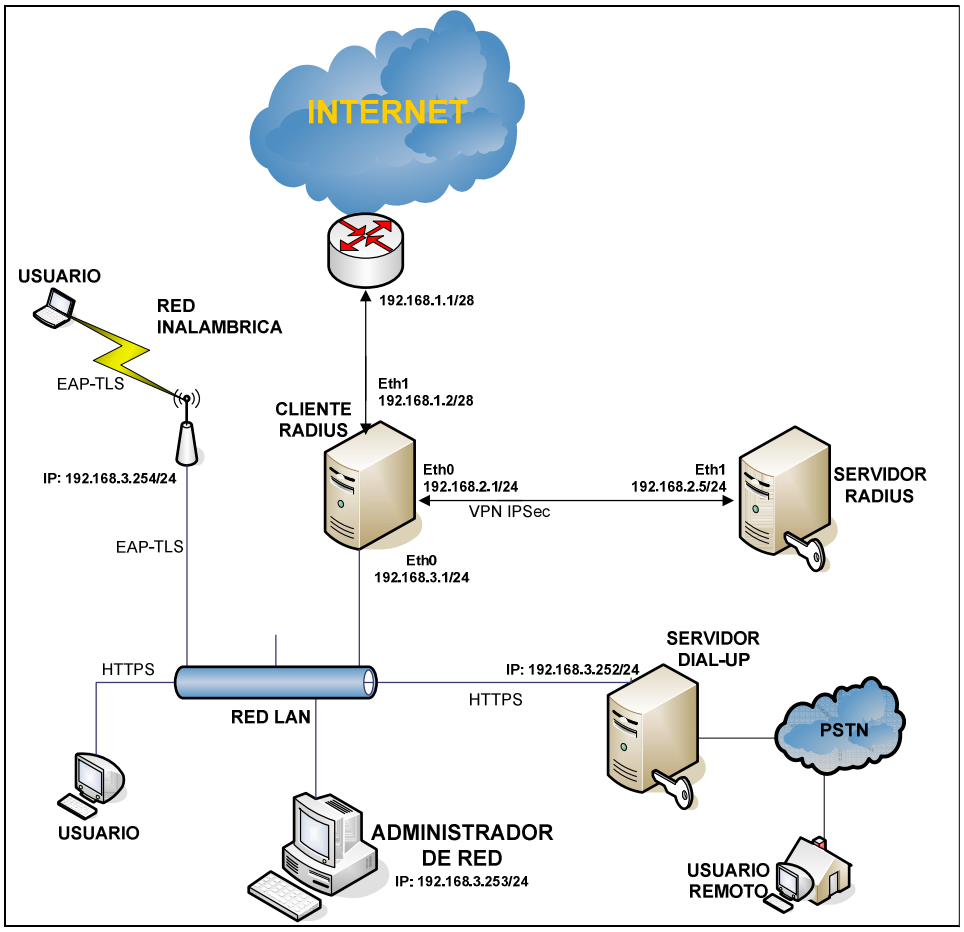

Figura 3.1 Diagrama de red del escenario de pruebas

Para realizar las pruebas de funcionamiento del cliente RADIUS se ha implementado una pequeña LAN dividida en tres segmentos de red: INTERNET, RADIUS y LOCAL; a cada uno de los cuales se conecta una interfaz del cliente RADIUS que viene a ser el elemento central de la implementación. Figura 3.1

El direccionamiento IP de los segmentos de red empleados para el escenario de

pruebas se muestra en la Tabla 3.1

Dirección de red	Máscara	Nombre del segmento de red
192.168.1.0	255.255.255.240	INTERNET
192.168.2.0	255.255.255.0	RADIUS
192.168.3.0	255.255.255.0	LOCAL

Tabla 3.1 Direccionamiento IP de los segmentos de red del escenario de pruebas

A continuación se presenta una descripción de los segmentos de red y los elementos que irán ubicados en los mismos.

3.1.1 Segmento de red INTERNET

En este segmento de red se encuentra configurado el acceso a Internet del Cliente RADIUS, el cual se lo realiza a través de un enlace por MODEM xDSL, la capacidad de este enlace es de 128 Kbps

El *router* que brinda el acceso a Internet se encuentra configurado con la dirección IP 192.168.1.1/128 y el cliente RADIUS tiene configurado en a interfaz que se conecta a este segmento la dirección IP 192.168.2.1/28 y como ruta por defecto la dirección IP del *router*.

3.1.2 Segmento de red RADIUS

En este segmento de red se encuentran configurados, el servidor RADIUS con dirección IP 192.168.2.5/24, y la interfaz del cliente RADIUS que se conecta a este segmento de la red tiene la dirección IP 192.168.2.1/24

En este segmento será levantado el túnel IPSEC para proteger la información que es intercambiada entre el cliente y el servidor RADIUS.

3.1.3 Segmento de red LOCAL

La interfaz del cliente RADIUS que se conecta a este segmento tiene la dirección

IP 192.168.3.1/24 que a su vez es la ruta por defecto de este segmento de la red.

En este segmento de la red se encuentran configurados el Punto de Acceso Inalámbrico el cual fue configurado para trabajar con EAP-TLS como se describió en el capitulo II; para tareas de administración a este equipo se lo configuró con la dirección IP 192.168.3.254/24

En este segmento se encuentra el servidor de acceso remoto con la dirección IP 192.168.3.252/24, el cual posee un MODEM de acceso telefónico que se encuentra conectado a una línea telefónica convencional, para permitir el acceso a la red vía *dial-up*.

Adicionalmente desde este segmento se realizaran las pruebas de seguridad en la administración del servidor RADIUS, para lo cual se configuró un computador con dirección IP 192.168.3.253/24 el cual servirá para realizar las tareas de administración del cliente RADIUS de forma remota.

En este segmento de red se ubicaran tres usuarios de prueba un usuario conectado de forma inalámbrica, uno que se conecte mediante un cable de red al HUB y otro que accederá mediante una conexión *dial-up* al Servidor *dial-up*.

3.2 IMPLEMENTACIÓN DEL ESCENARIO DE PRUEBAS

Una vez que se ha implementado la topología de red descrita, se procederá a realizar las configuraciones y pruebas correspondientes de funcionamiento de la implementación.

3.2.1 CONFIGURACIÓN DE USUARIOS

Se ha considerado emplear tres usuarios para realizar las pruebas de funcionamiento de la implementación: dos usuarios locales uno de los cuales se conectará mediante un cable de red al HUB y el otro accederá a través del Punto

de Acceso inalámbrico, y un usuario *dial-up* que accederá mediante el Servidor *dial-up*.

Se configuró en el cliente RADIUS las direcciones MAC de los dos usuarios de prueba locales, y del Servidor *dial-up* para el acceso del usuario *dial-up,* como direcciones MAC validas, de forma que puedan obtener una dirección IP del servidor DHCP configurado en el cliente RADIUS.

El usuario que se conecta directamente al HUB mediante el cable de red únicamente deberá configurar su tarjeta de red como cliente DHCP para que obtenga su dirección IP de forma dinámica del servidor DHCP.

El usuario inalámbrico debe realizar una autenticación empleando WPA con RADIUS, para lo cual se procedió a crear e instalar el correspondiente certificado digital tal como se mostró en el Anexo F; además debe estar configurado como cliente DHCP.

En la Figura 3.2 se presenta la pantalla correspondiente a la configuración realizada para el usuario de prueba inalámbrico; se ha empleado en el computador del usuario una tarjeta USB Wireless 3Com con su correspondiente utilitario de configuración.

El tercer usuario de prueba es un usuario *dial-up* en el cual se configuró una conexión de acceso telefónico a redes en una PC con sistema operativo *Windows* XP.

Para el acceso de este usuario remoto a la red se creó un usuario en el servidor *dial-up*, con su respectiva clave, de tal forma que este usuario que acceda de forma remota a la red, para hacer uso del Internet debe primero autenticarse en el Servidor *dial-up* y posteriormente en el cliente RADIUS.

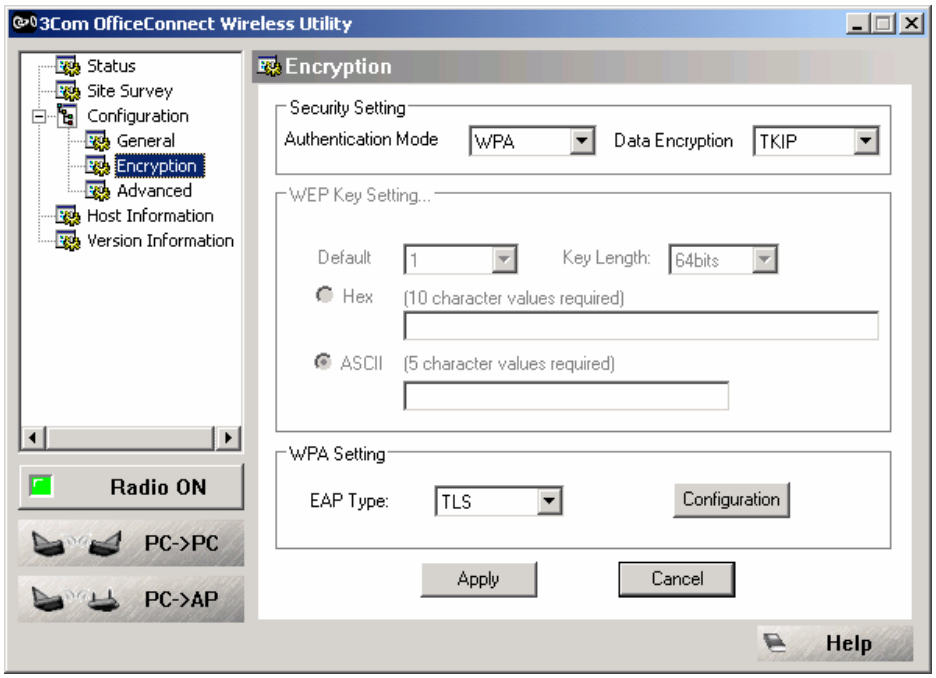

Figura 3.2 Configuración de seguridad de la tarjeta de red del usuario

3.2.2 CONFIGURACIÓN Y PUESTA EN MARCHA DEL SERVIDOR DHCP ESTÁTICO

Se procedió a realizar la implementación del servidor DHCP, con ciertas restricciones como se mostró en el Capítulo II; de tal forma que el servidor DHCP asignará direcciones IP únicamente a usuarios cuya dirección MAC haya sido registrada como valida en la base de datos del cliente RADIUS.

Este servidor se encuentra configurado en el mismo equipo que hace las veces de cliente RADIUS y su administración se encuentra embebida en el interfaz de administración del cliente RADIUS, a través del cual se puede registrar, borrar o modificar las direcciones MAC de los usuarios, así como también se puede poner en marcha o detener el servicio DHCP. En el ANEXO L se muestra el archivo de configuración del servidor de DHCP.

Se ha configurado el servidor DHCP para que otorgue direcciones IP a los usuarios en el rango comprendido entre las direcciones IP: 192.168.3.10 hasta 192.168.3.40 y que no otorgue dirección IP a usuarios cuya MAC no se haya

registrado en la configuración.

3.2.3 CONFIGURACIÓN DEL SERVIDOR HTTP, HTTPS. FTP, MAIL, TELNET Y SSH

Para efectos de pruebas de acceso a diferentes servicios de red se procedió a instalar en un computador con sistema operativo LINUX Fedora Core 3; los servicios HTTP, HTTPS, FTP, TELNET y SSH.

En el sistema operativo LINUX Fedora Core 3 por defecto vienen activados los servicios de HTTPS, HTTP y SSH, por lo cual se precedió a utilizar directamente estos servicios para realizar las pruebas.

Para realizar las pruebas de acceso a correo electrónico, se empleó una cuenta de correo electrónico gratuito de *yahoo*; la cual se configuró en el cliente de correo *Outlook Express* con los parámetros que se muestran en la Tabla 3.2.

Servidor de correo entrante (POP3):	pop.mail.yahoo.com (emplear SSL, puerto: 995)
Servidor de correo saliente (SMTP):	Smtp.mail.yahoo.com (Usar SSL, puerto: 465, con autenticación)
Nombre de cuenta	Nombre de usuario de Yahoo!
Dirección de correo:	pabartur@yahoo.com
Contraseña:	********

Tabla 3.2 Configuración de la cuenta de correo electrónico de prueba

Con esta cuenta de correo electrónico se realizaron pruebas de envío y recepción de correo, empleando esta misma cuenta para dos usuarios con diferentes perfiles; en el primero se permitía el tráfico de correo electrónico hacia (envió) y desde (recepción) el Internet y el segundo se denegaba el mismo.

Para las pruebas con el servicio de TELNET fue necesario iniciarlo previamente ya que por seguridad este servicio no viene iniciado por defecto en la distribución de LINUX Fedora Core 3 (FC3), a continuación se presenta los comandos empleados para la activación del servicio.

```
#chkconfig telnet on (para iniciar el servicio)
#chkconfig telnet off (para detener el servicio)
#chkconfig –list | grep telnet (indica el estado del servicio)
```

Cualquier usuario configurado en el servidor LINUX podrá acceder a través del servicio TELNET hacia el equipo, a excepción del usuario root.

Igualmente fue necesario configurar el servicio de FTP en el servidor de pruebas ya que el mismo no viene iniciado ni configurado en FC3, para implementarlo se hizo uso de la aplicación XAMPP que viene con los servicios de HTTP (PHP y PERL), MySQL y ProFTPD, siendo necesario el procedimiento de instalación que se muestra en el ANEXO M.

3.3 VERIFICACIÓN DE FUNCIONAMIENTO DEL SERVIDOR DIAL-UP

Se procedió a configurar una conexión de acceso telefónico a redes en el computador del usuario remoto con el usuario y clave creado en el Servidor *dial-up*.

Para probar el funcionamiento del acceso remoto a la red se realizó una llamada con la conexión configurada; hacia el Servidor *dial-up*, pudiéndose observar que el usuario se autenticaba con el Servidor *dial-up* y una vez autenticado, se pudo confirmar que el usuario puede acceder al sistema de autenticación del cliente RADIUS ya que todas las peticiones que se realizaban hacia el Internet eran redireccionadas a la página de autenticación, finalmente se ingreso un usuario y clave válidos y se pudo observar que era posible acceder a los servicios configurados para este usuario.

3.4 VERIFICACIÓN DEL ESTABLECIMIENTO DEL TÚNEL IPSEC ENTRE EL CLIENTE RADIUS Y EL SERVIDOR RADIUS

Para verificar que efectivamente se encuentra protegida la información al emplear el túnel IPSec, se procedió a realizar dos capturas del tráfico intercambiado entre el cliente y el servidor RADIUS, la primera sin el túnel establecido y la segunda con el túnel IPSec establecido.

Mediante la realización de esta prueba se verificó que la confidencialidad de los datos se encuentra protegida al emplear el túnel IPSec.

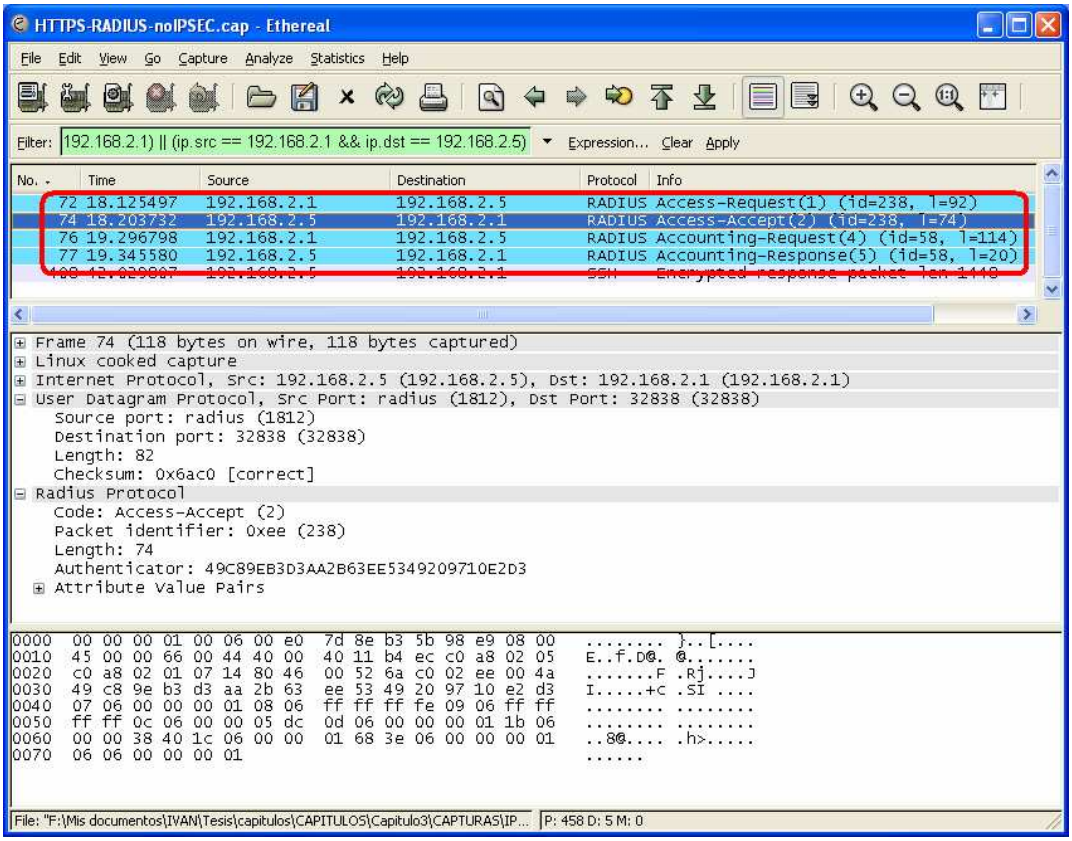

Figura 3.3 Captura de tráfico entre el cliente y el servidor RADIUS sin emplear IPSec.

Para establecer el túnel IPSec entre los dos computadores se empleo el siguiente comando tanto en el servidor como el cliente.

```
#setkey -f /etc/ipsec.conf (Para establecer el túnel IPSEc)
```

En la Figura 3.3 se presenta la captura correspondiente al tráfico intercambiado entre el cliente RADIUS y el servidor RADIUS sin haberse establecido el túnel IPSec; en ésta se puede observar claramente que la información intercambiada entre ellos no viaja cifrada; por lo que se puede distinguir el tipo de protocolo y la información que cada uno de los campos del paquete IP contiene.

Por consiguiente si estos paquetes son interceptados por alguna incursión maliciosa, la información que contienen podría ser observada fácilmente.

En la Figura 3.4 se presenta otra captura de tráfico entre el cliente y el servidor RADIUS; pero esta vez se ha levantado un túnel IPSec entre los dos equipos, se puede observar que esta vez la información que están intercambiando se encuentra cifrada; de esta forma si llegara a ser interceptada el atacante difícilmente podría obtener la información original.

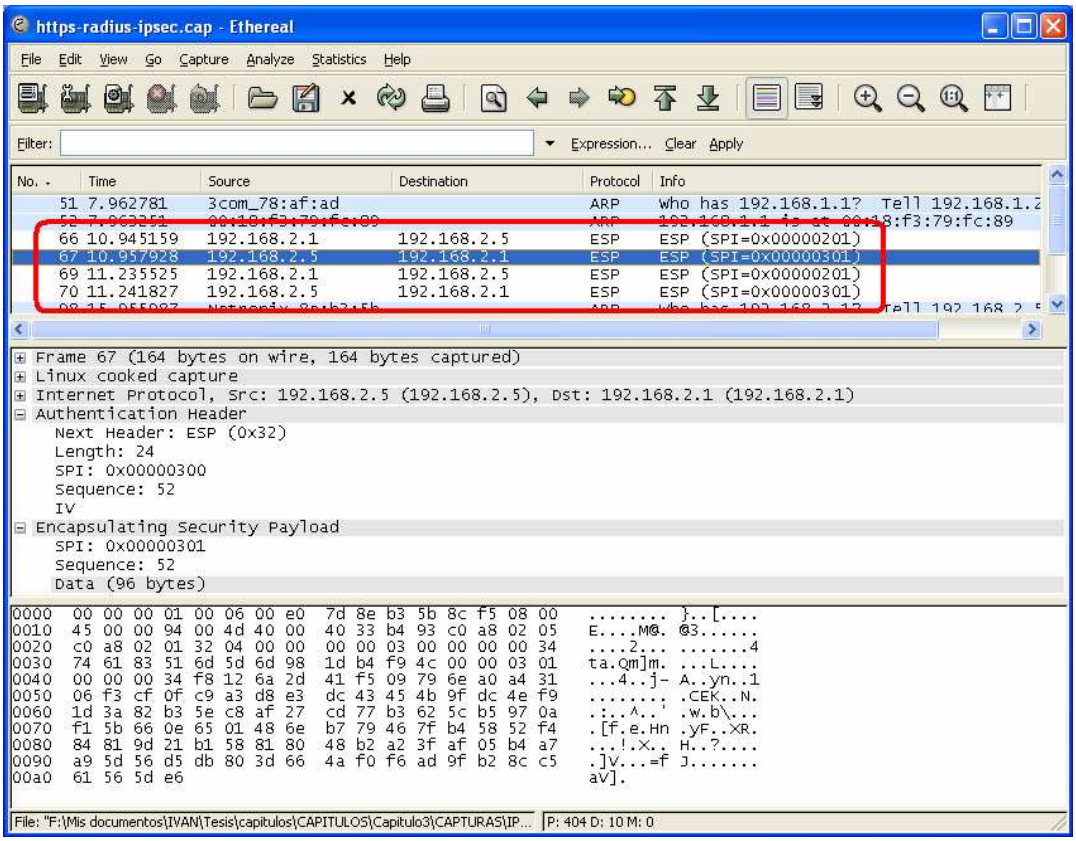

Figura 3.4 Captura de tráfico entre el servidor RADIUS y el cliente empleando IPSec.

Al encontrarse protegida la información que intercambian el cliente y el servidor RADIUS se cumple con la política de seguridad “Protección de la información de autenticación que el Cliente RADIUS, envía al servidor RADIUS”; ya que todo el tráfico que sea intercambiado por estos dos equipos se encuentra protegido por el túnel IPSec.

3.5 VERIFICACIÓN DEL ESTABLECIMIENTO DE LA SESIÓN HTTPS ENTRE EL USUARIO Y EL CLIENTE RADIUS PARA PROTEGER LA INFORMACIÓN DE AUTENTICACIÓN QUE EL USUARIO ENTREGA AL CLIENTE RADIUS

Cuando un usuario ingresa al sistema de autenticación; el sistema como tal le obliga a emplear HTTPS para el intercambio de la información de autenticación.

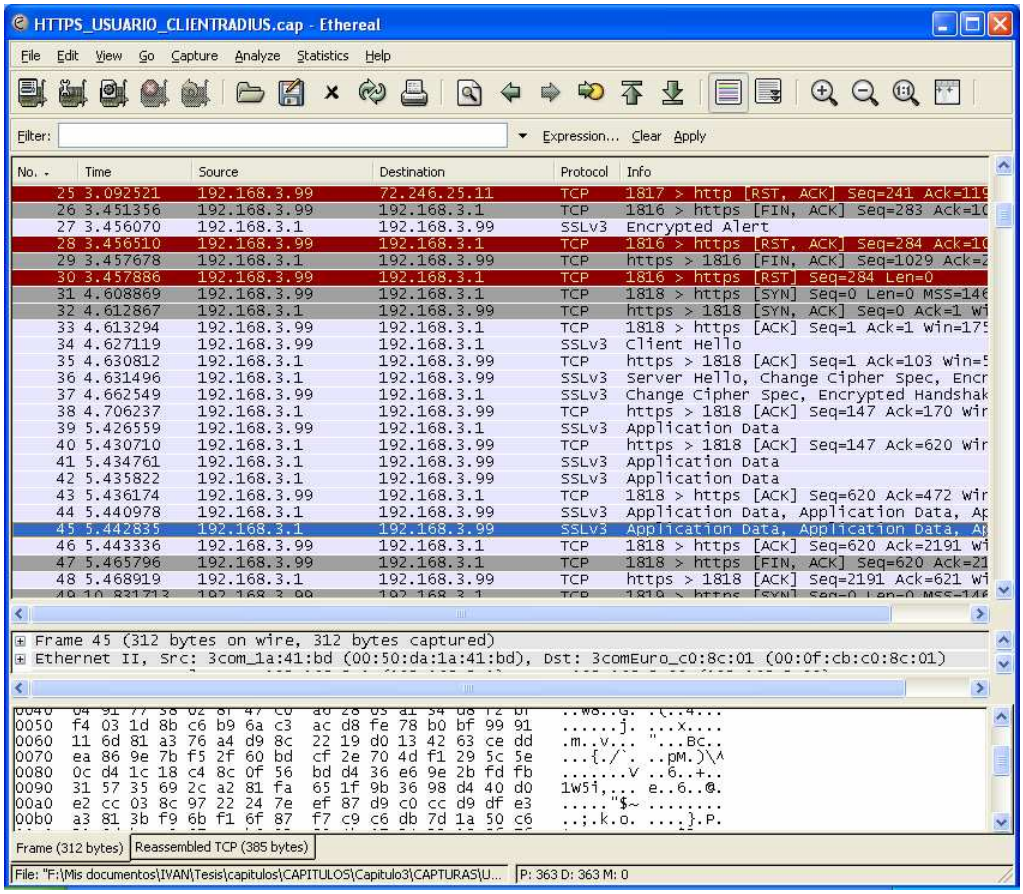

Figura 3.5 Captura del trafico HTTPS entre el cliente RADIUS y un usuario.

Para verificar que el tráfico intercambiado durante el proceso de autenticación se lo realiza empleando el protocolo HTTPS, se procede a realizar la captura del tráfico empleando un *sniffer*; en la Figura 3.5 se muestra el resultado de la captura correspondiente al establecimiento de la sesión HTTPS entre el usuario y el cliente RADIUS. Se puede observar claramente que el tráfico intercambiado es del tipo SSLv3, lo que nos indica que la información contenida en estos paquetes se encuentra cifrada.

Con lo realizado en este literal se verifica también el cumplimiento de la política de seguridad "Protección de la información de autenticación que el usuario envía al Cliente RADIUS"**.**

3.6 VERIFICACIÓN DE LA SEGURIDAD DE LAS SESIONES ESTABLECIDAS CON EL CLIENTE RADIUS PARA SU ADMINISTRACIÓN

La pruebas para verificar la seguridad en la administración remota del cliente RADIUS se realizaron desde un computador definido para este objetivo configurado con la dirección IP 192.168.3.253; esta dirección IP debe ser definida en el *script* de configuración inicial de *iptables*, de tal forma que este sea el único equipo del segmento de red LOCAL que acceda al cliente RADIUS para su administración.

Para la administración del cliente RADIUS se emplearán los protocolos SSH para acceso a línea de comandos y HTTPS para el acceso a la interfaz de administración WEB, de esta forma se consigue que la información que se intercambia con el cliente RADIUS para su administración se encuentre cifrada.

3.6.1 Verificación del establecimiento de la sesión SSH

Para realizar esta verificación se empleó la herramienta "putty.exe" que permite establecer una sesión SSH desde un equipo con Sistema Operativo *Windows*,

hacia el cliente RADIUS.

La Figura 3.6 muestra el tráfico generado durante la sesión SSH desde la dirección IP 192.168.3.253 del computador definido para la administración del cliente RADIUS y el cliente RADIUS con dirección IP 192.168.3.1

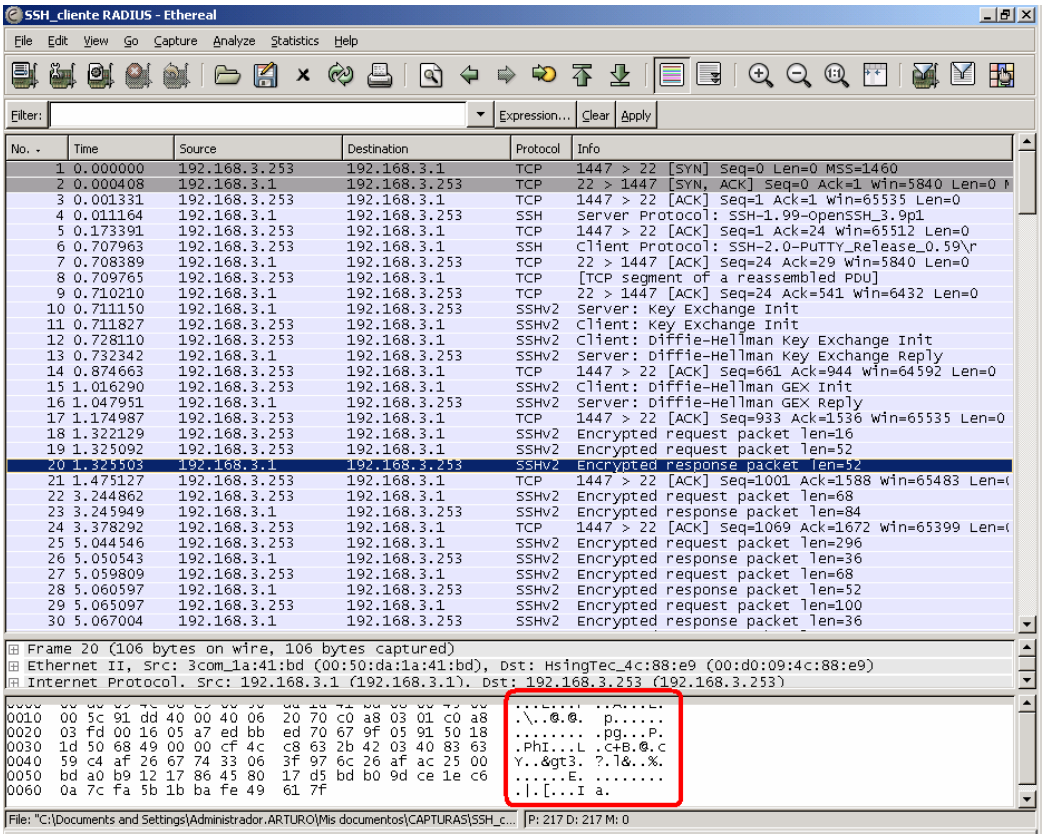

Figura 3.6 Tráfico SSH hacia el cliente RADIUS

En la Figura 3.7 se muestra una captura del trafico TELNET entre los mismos equipos, en esta se puede apreciar claramente que a diferencia de una sesión SSH la información no viaja cifrada.

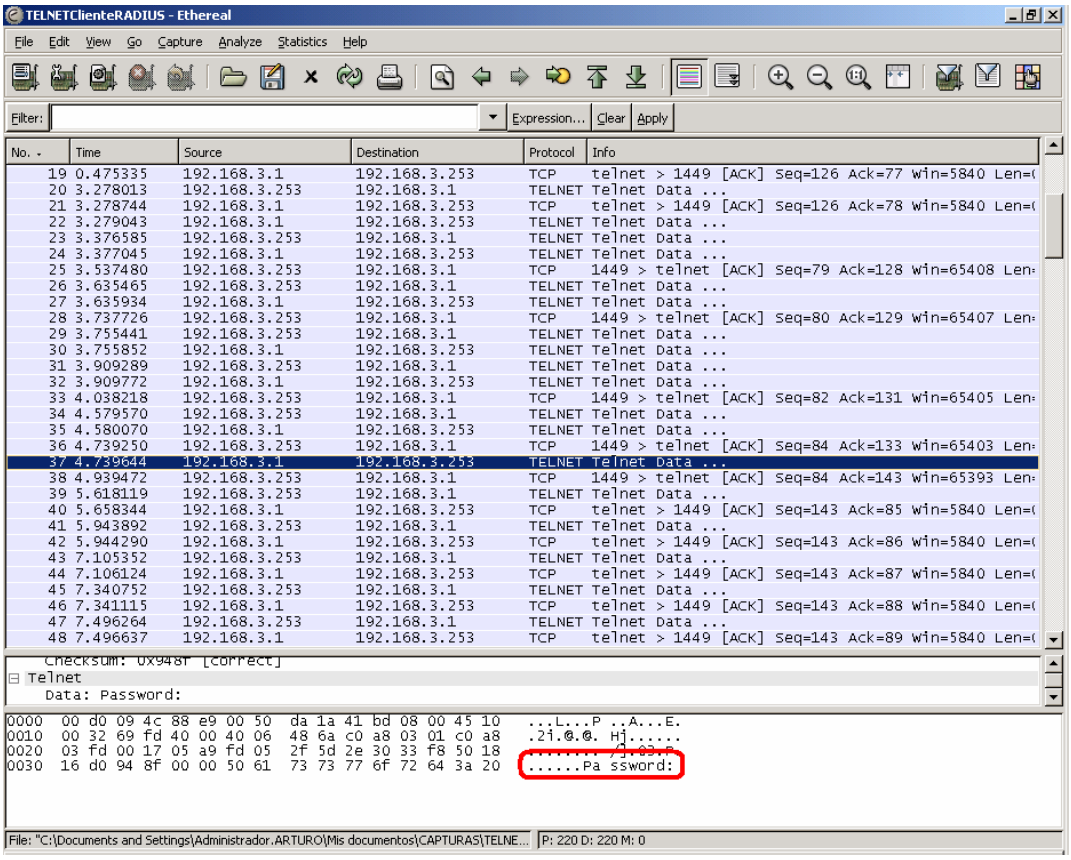

Figura 3.7 Trafico de una sesión TELNET hacia el Cliente RADIUS

3.6.2 Verificación del establecimiento de la sesión HTTPS

Para la verificación del establecimiento de la sesión HTTPS se ha empleado el navegador WEB Internet Explorer 6.0.

El URL de acceso para la administración del cliente RADIUS es el siguiente:

https://192.168.3.1/adm/index.htm

Al ingresar a la interfaz de administración del cliente RADIUS en el navegador WEB aparecerá la página que se muestra en la Figura 3.8.

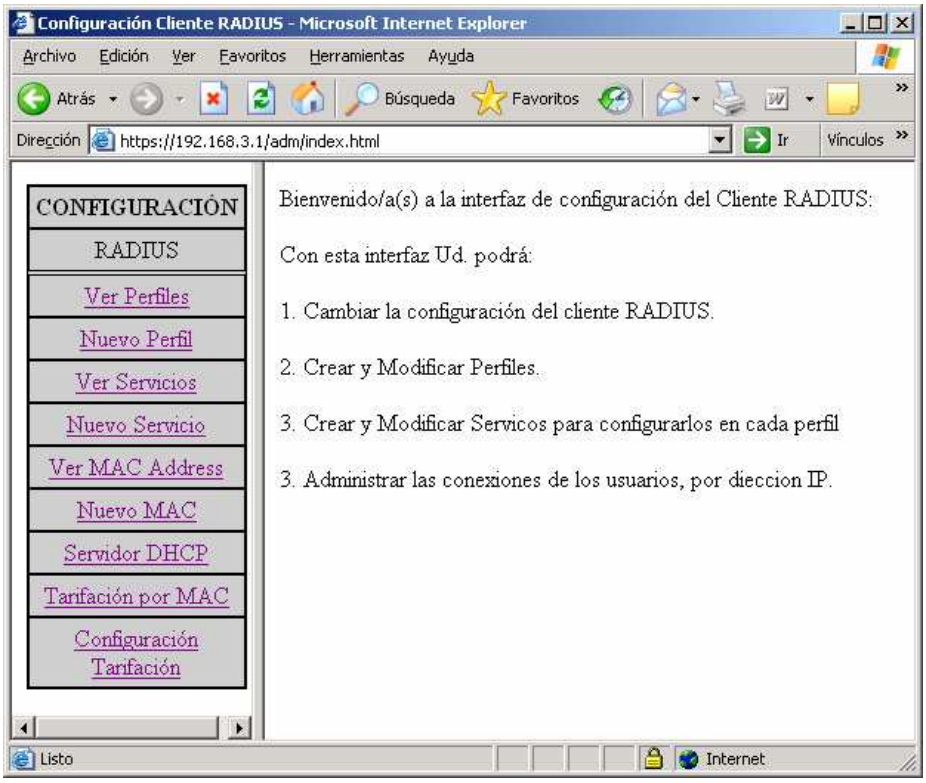

Figura 3.8 Pantalla de inicio para configuración del cliente RADIUS vía interfaz WEB

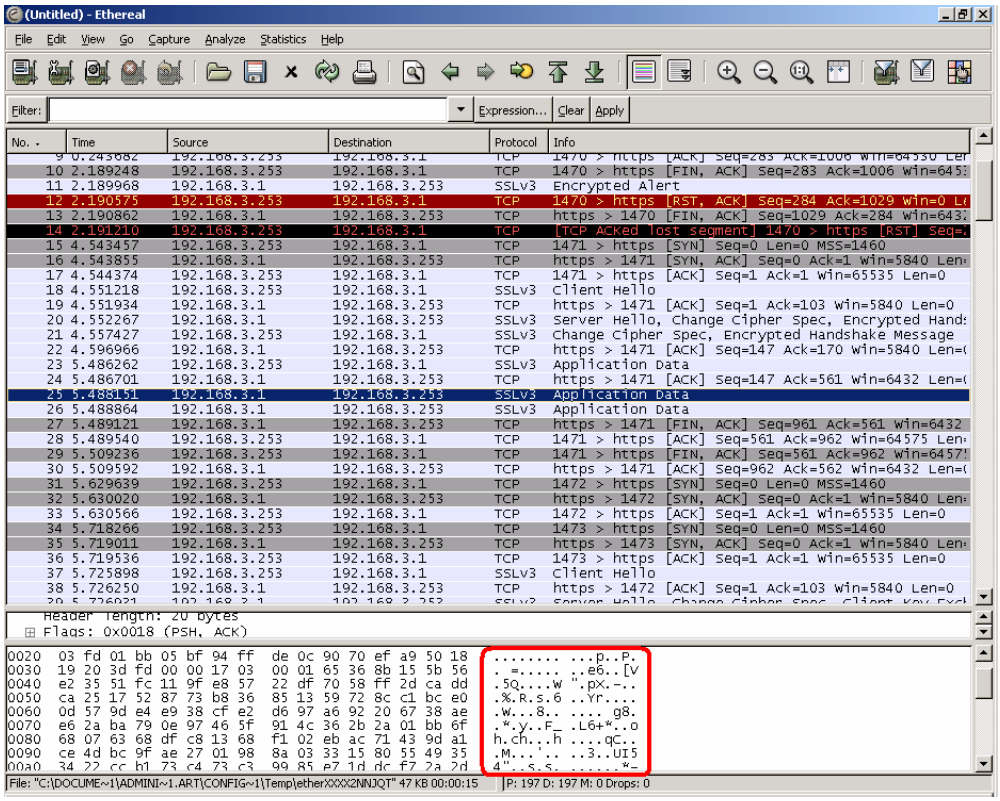

Figura 3.9 Trafico HTTPS intercambiado en el proceso de autenticación del usuario

En la Figura 3.9 se muestra el tráfico de una sesión HTTPS entre el equipo definido para la administración remota del cliente RADIUS con dirección IP 192.168.1.253 y el cliente RADIUS.

Se puede apreciar en la captura de paquetes que todo el tráfico intercambiado es del tipo HTTPS y que la información se muestra cifrada.

3.7 COMPROBACIÓN DE SEGURIDAD EN EL SEGMENTO DE RED INALÁMBRICO

Para realizar el control de acceso de usuarios de la red inalámbrica, se ha configurado en el Punto de Acceso Inalámbrico un filtro de direcciones MAC, la autenticación a través de WPA con RADIUS y en el computador del usuario se ha cargado el certificado digital correspondiente.

Una vez que la dirección MAC del usuario es validada por el punto de acceso inalámbrico, el usuario se autentica empleando RADIUS, si la autenticación es exitosa, el usuario podrá obtener una dirección IP del servidor DHCP o caso contrario no podrá obtener dirección IP de forma dinámica.

Cuando el usuario disponga de una dirección IP, podrá ya acceder al sistema de autenticación que será el último mecanismo de seguridad para que el equipo tenga acceso a los servicios de red que su perfil le permita.

En la Figura 3.10 se presenta la captura del tráfico de la autenticación del usuario empleando RADIUS.

Con respecto a esta captura, el filtro por dirección MAC configurado en el Punto de Acceso inalámbrico lo único que hace es permitir o no el acceso a la red en función de la dirección MAC de la tarjeta de red del usuario, por lo que en este caso no existirá ningún tráfico generado por este control de acceso.

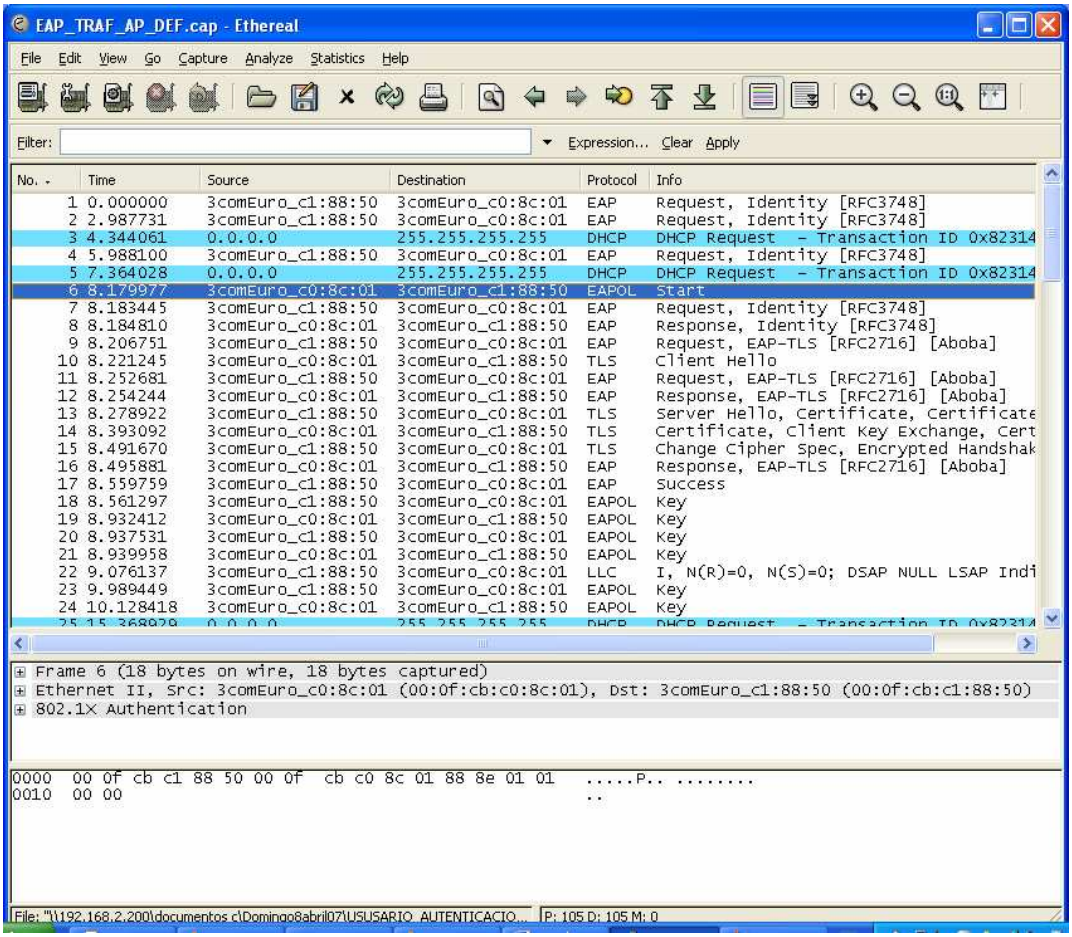

Figura 3.10 Captura del tráfico generado en el proceso de autenticación del cliente inalámbrico

Con lo realizado en este literal se verifica también el cumplimiento de la política de seguridad “Protección de la información que viaja por el segmento de red inalámbrico”.

3.8 VERIFICAR EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD ESTABLECIDAS

A continuación se describe el procedimiento empleado para verificar cada una de las políticas de seguridad implementadas en el presente proyecto de titulación.

Se excluyen de la verificación que se realiza las siguientes políticas: protección de la información de autenticación que el cliente RADIUS, envía al servidor RADIUS; protección de la información de autenticación que el usuario envía al cliente

RADIUS y protección de la información que viaja por el segmento de red inalámbrico; ya que fueron consideradas en los literales 3.4, 3.5 y 3.7 respectivamente.

3.8.1 CONTROL DE ACCESO MEDIANTE DIRECCIÓN MAC

Para realizar esta comprobación se ingresó en la red un equipo cuya dirección MAC no se encontraba registrada el la base de datos de direcciones MAC autorizadas; se comprobó en primera instancia al estar el equipo configurado como cliente DHCP y conectado mediante un cable de red al HUB, no le fue asignada una dirección IP del segmento de red LOCAL.

Posteriormente se ejecutó en la línea de comandos del sistema operativo el comando: `C:\>ipconfig /renew`

Mediante el cual se le indica al computador que solicite una dirección IP a cualquier servidor DHCP disponible, luego de varios segundos se observo que el sistema no asigno ninguna dirección IP valida para acceder a los servicio de la red.

Por lo cual queda comprobada la correcta aplicación de la política de seguridad; permitiendo únicamente que los computadores cuyas direcciones MAC hayan sido registradas previamente obtengan una dirección IP válida para el acceso a la página de autenticación del cliente RADIUS.

3.8.2 FILTROS DE DIRECCIONES MAC EN PUNTOS DE ACCESO

Para el cumplimiento de esta política de seguridad se hizo uso de la funcionalidad del Punto de Acceso Inalámbrico que permite dar acceso únicamente a usuarios cuyas direcciones MAC hayan sido previamente registradas; en la Figura 3.11 se muestra la interfaz de administración del Punto de Acceso Inalámbrico en la cual se puede observar una dirección MAC ingresada en el filtro de control de acceso.

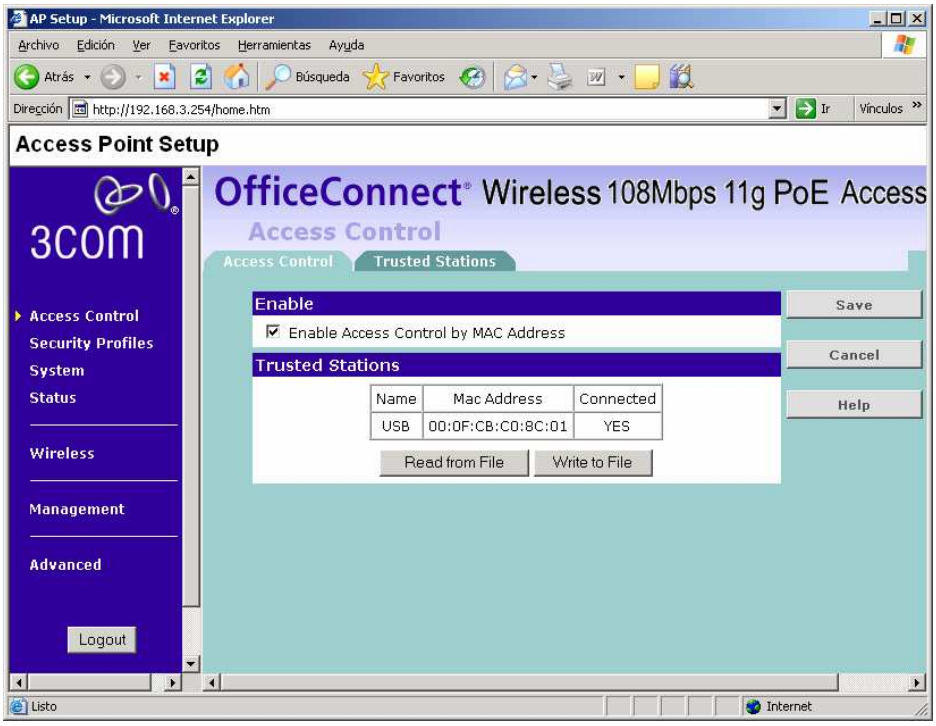

Figura 3.11 Configuración de Control de Acceso de filtrado por dirección MAC en el Punto de Acceso Inalámbrico.

3.8.3 AUTORIZACIÓN DE ACCESO A USUARIOS CON DIRECCIÓN IP CONFIGURADA DE FORMA ESTÁTICA

Se realizó las pruebas de acceso empleando para este fin la dirección IP 192.168.3.44 configurada de forma estática en el computador del usuario que intentará acceder a los servicios de red.

Para que el computador del usuario pueda acceder al sistema de autenticación el cliente RADIUS verifica que la dirección MAC del usuario sea una dirección válida, es decir, que se encuentre registrada en la base de datos de usuarios válidos.

Si algún usuario con su dirección IP configurada de forma estática, tratase de acceder al sistema, pese a que este usuario tenga configurada una dirección IP válida del segmento de red LOCAL, el sistema no le permitirá ingresar a la página

de autenticación, a menos que su dirección MAC haya sido registrada en la base de datos.

En esta circunstancia, al usuario que intente acceder al sistema en lugar de la página de autenticación se le presentará una página indicando que no esta autorizado a utilizar el sistema.

3.8.4 EMPLEO DE NOMBRE DE USUARIO Y CLAVE DE ACCESO SEGURA PARA LA AUTENTICACIÓN DE USUARIOS

Se verificó el funcionamiento del sistema de autenticación, empleando para las pruebas nombres de usuarios y contraseñas válidos, verificando que el sistema permitía el acceso de estos usuarios.

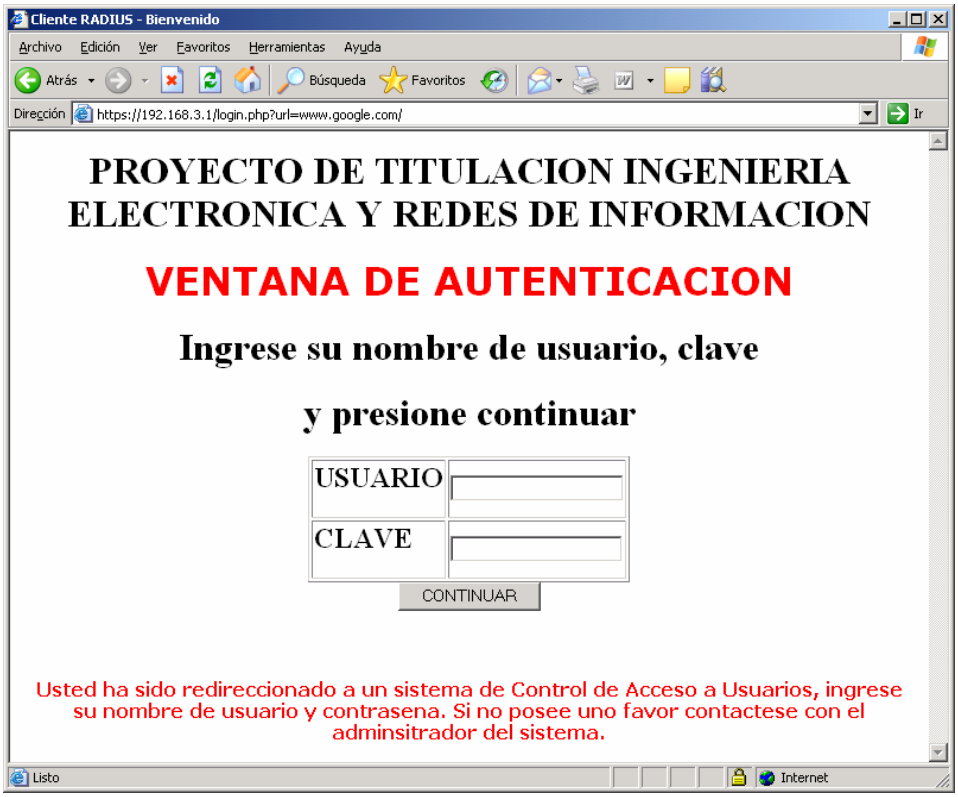

Figura 3.12 Página de autenticación de usuarios

La Figura 3.12 presenta la página de autenticación de usuarios; la Figura 3.13 presenta la página que se muestra una vez que el usuario se haya autenticado con un nombre de usuario y clave válidos.

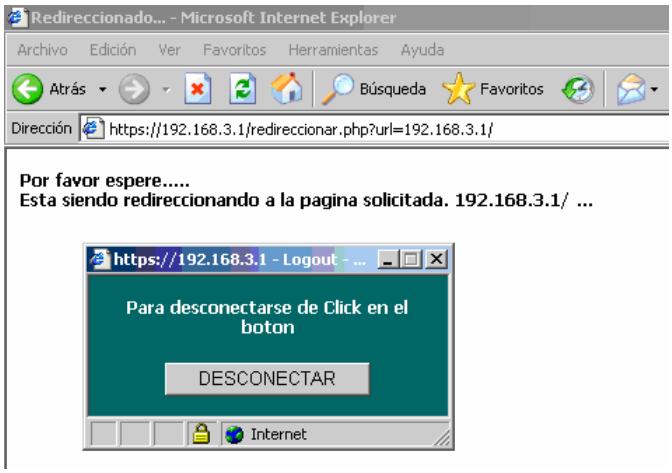

Figura 3.13 Ventana presentada a usuarios autenticados

En la Figura 3.14 se muestran las reglas de *iptables* que se crean en el cliente RADIUS para permitir el acceso a un usuario que se ha autenticado de forma exitosa en el sistema; la cantidad de reglas que se creen dependerán del perfil que posea el usuario autenticado.

```
[root@gateway iptables]# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
USUARIOPERMITIDO  all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  192.168.3.254        192.168.2.5         udp dpt:1812
ACCEPT     udp  --  192.168.3.254        192.168.2.5         udp dpt:1813
DNAT       tcp  --  192.168.3.0/24       0.0.0.0/0           tcp dpt:80 to:192.168.3.1
DNAT       tcp  --  192.168.3.0/24       0.0.0.0/0           tcp dpt:443 to:192.168.3.1
DNAT       icmp --  192.168.3.0/24       0.0.0.0/0           to:192.168.3.1
TRAFICOPERMITIDO  all  --  0.0.0.0/0            0.0.0.0/0
DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.3.254        0.0.0.0/0
SNAT       all  --  192.168.3.0/24       0.0.0.0/0           to:192.168.1.2
DROP       all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain TRAFICOPERMITIDO (1 references)
target     prot opt source               destination
ACCEPT     udp  --  192.168.3.0/24       0.0.0.0/0           udp dpt:53
ACCEPT     udp  --  192.168.3.0/24       0.0.0.0/0           udp dpt:67
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain USUARIOPERMITIDO (1 references)
target     prot opt source               destination
ACCEPT     icmp --  192.168.3.100        0.0.0.0/0
ACCEPT     tcp  --  192.168.3.100        0.0.0.0/0           tcp dpt:161
ACCEPT     udp  --  192.168.3.100        0.0.0.0/0           udp dpt:1813
ACCEPT     tcp  --  192.168.3.100        0.0.0.0/0           tcp dpt:443
ACCEPT     tcp  --  192.168.3.100        0.0.0.0/0           tcp dpt:162
ACCEPT     tcp  --  192.168.3.100        0.0.0.0/0           tcp dpt:110
ACCEPT     tcp  --  192.168.3.100        0.0.0.0/0           tcp dpt:80
ACCEPT     tcp  --  192.168.3.100        0.0.0.0/0           tcp dpt:53
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Figura 3.14 Regla de *iptables* generada para un usuario

De igual forma al emplear usuarios no válidos, se pudo verificar que los mismos no podían obtener acceso a ningún servicio de red y únicamente se obtenía un mensaje indicando un error de autenticación.

El mensaje de error que se presenta al usuario se muestra en la Figura 3.15, en este caso el usuario permanecerá sin tener acceso a ninguno de los servicios de la red por lo que las reglas de *iptables* permanecerán sin modificación alguna.

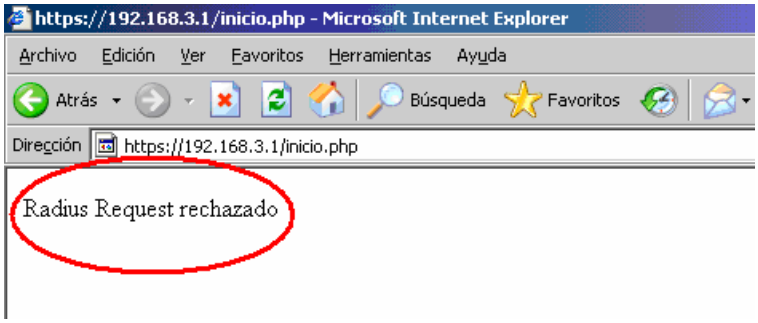

Figura 3.15 Ventana presentada ante una autenticación fallida

Adicionalmente observando la información de las reglas en *iptables*, se pudo verificar que los permisos de acceso para el usuario que no se autenticó nunca fueron creados, lo cual se muestra en la Figura 3.16

```
[root@gateway iptables]# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
USUARIOPERMITIDO  all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  192.168.3.254        192.168.2.5         udp dpt:1812
ACCEPT     udp  --  192.168.3.254        192.168.2.5         udp dpt:1813
DNAT       tcp  --  192.168.3.0/24       0.0.0.0/0           tcp dpt:80 to:192.168.3.1
DNAT       tcp  --  192.168.3.0/24       0.0.0.0/0           tcp dpt:443 to:192.168.3.1
DNAT       icmp --  192.168.3.0/24       0.0.0.0/0           to:192.168.3.1
TRAFICOPERMITIDO  all  --  0.0.0.0/0            0.0.0.0/0
DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  192.168.3.254        0.0.0.0/0
SNAT       all  --  192.168.3.0/24       0.0.0.0/0           to:192.168.1.2
DROP       all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain TRAFICOPERMITIDO (1 references)
target     prot opt source               destination
ACCEPT     udp  --  192.168.3.0/24       0.0.0.0/0           udp dpt:53
ACCEPT     udp  --  192.168.3.0/24       0.0.0.0/0           udp dpt:67
RETURN     all  --  0.0.0.0/0            0.0.0.0/0

Chain USUARIOPERMITIDO (1 references)
target     prot opt source               destination
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Figura 3.16 Reglas de *iptables*, no se ha creado ninguna regla adicional

Será responsabilidad del administrador del sistema, generar claves lo suficientemente seguras, que cumplan con un esquema de seguridad adecuado y eficiente. Por ejemplo crear nombres de usuarios de forma estándar y contraseñas que contengan al menos ocho caracteres alfanuméricos y que no sean palabras conocidas.

3.8.5 DEFINIR DIFERENTES PERFILES DE ACCESO PARA LOS USUARIOS

Para verificar que los permisos de cada uno de los perfiles están siendo asignados de forma adecuada, se procedió a crear dos perfiles en el cliente RADIUS perfil *Premium* y perfil *Gold*, configurando cada uno de los perfiles con diferentes servicios; en las Figuras 3.17 y 3.18 se puede observar los servicios configurados para cada uno de los perfiles.

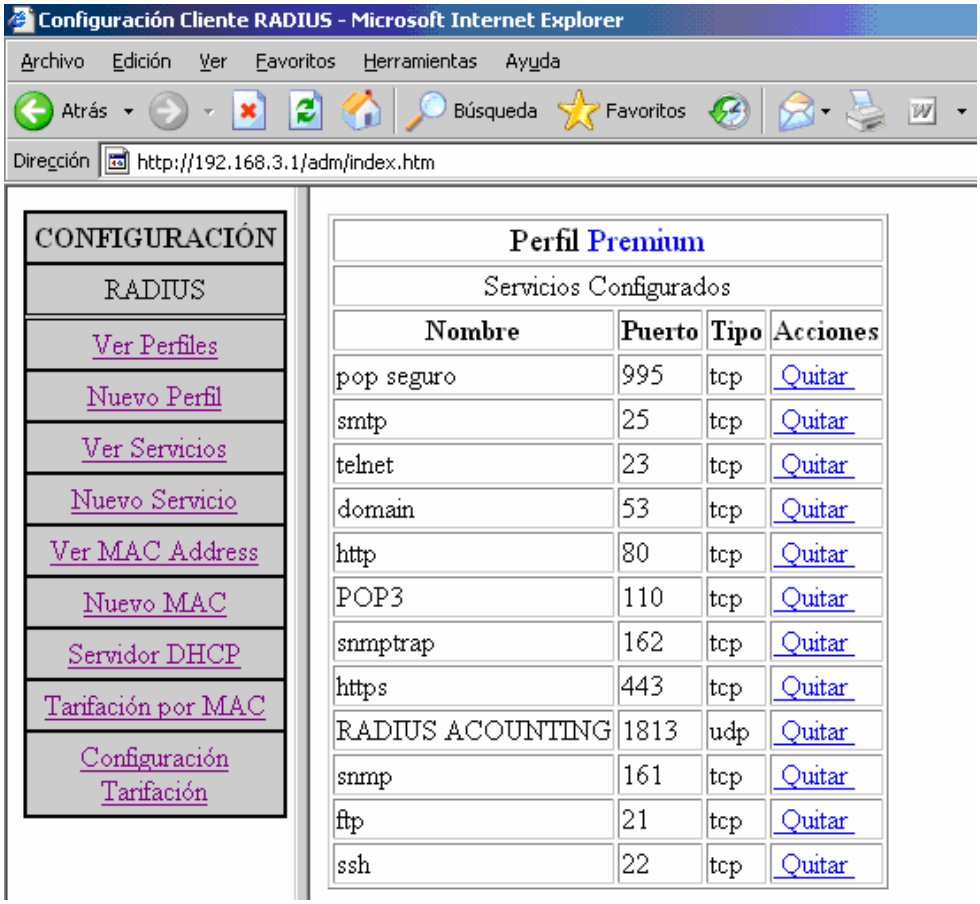

Figura 3.17 Interfaz de administración - Servicios configurados para el perfil *Premium*

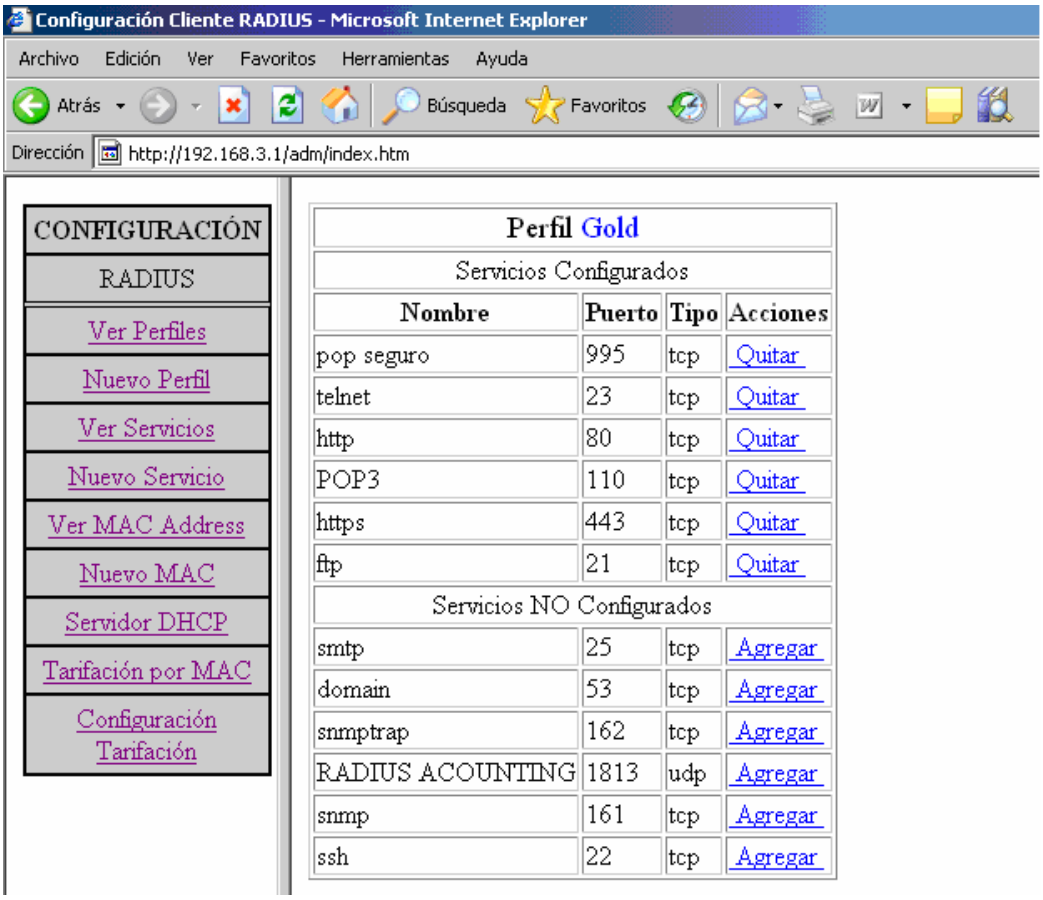

Figura 3.18 Interfaz de administración - Servicios configurados para el perfil *Gold*

Una vez creados los perfiles se añadieron dos usuarios de prueba en el servidor RADIUS, uno configurado para acceder con perfil *Premium* y el otro con perfil *Gold*.

Desde dos computadores configurados como usuarios del cliente RADIUS, se procedió a ingresar el nombre de usuario y contraseña de los dos usuarios de prueba.

Para comprobar que se asignado de forma correcta los permisos de acceso al los servicios de cada perfil se observó el listado de las reglas de *iptables* creadas en el cliente RADIUS; los cuales se muestran en las Figuras 3.19 para el perfil *Premium* y 3.20 para el perfil *Gold*.

```
Chain USUARIOPERMITIDO (1 references)
target     prot opt source               destination
ACCEPT     icmp --  192.168.3.200        0.0.0.0/0
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:21
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:161
ACCEPT     udp  --  192.168.3.200        0.0.0.0/0           udp dpt:1813
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:443
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:162
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:110
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:80
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:53
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:23
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:25
ACCEPT     tcp  --  192.168.3.200        0.0.0.0/0           tcp dpt:995
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Figura 3.19 Reglas de *iptables* para el usuario con IP: 192.168.3.200 perfil *Premium*

```
Chain USUARIOPERMITIDO (1 references)
target     prot opt source               destination
ACCEPT     icmp --  192.168.3.201        0.0.0.0/0
ACCEPT     tcp  --  192.168.3.201        0.0.0.0/0           tcp dpt:21
ACCEPT     tcp  --  192.168.3.201        0.0.0.0/0           tcp dpt:443
ACCEPT     tcp  --  192.168.3.201        0.0.0.0/0           tcp dpt:110
ACCEPT     tcp  --  192.168.3.201        0.0.0.0/0           tcp dpt:80
ACCEPT     tcp  --  192.168.3.201        0.0.0.0/0           tcp dpt:23
ACCEPT     tcp  --  192.168.3.201        0.0.0.0/0           tcp dpt:995
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Figura 3.20 Reglas de *iptables* para el usuario con IP: 192.168.3.201 Perfil *Gold*

Además, desde el computador de cada usuario se realizaron pruebas de conexión a los servicios configurados en cada perfil, comprobando que únicamente se podía acceder a los servicios que se encontraban definidos en el perfil y el acceso a otros servicios se encontraba bloqueado.

3.8.6 REGISTRO DEL TIEMPO DE CONEXIÓN Y EL CONSUMO MEDIDO EN *BYTES* QUE REALICE EL USUARIO

El tiempo y *bytes* consumidos por cada uno de los usuarios registrados en el sistema, se lo podrá obtener desde la interfaz de administración en el menú Tarifación por MAC -> Ver Tarifación, como se muestra en la Figura 3.21.

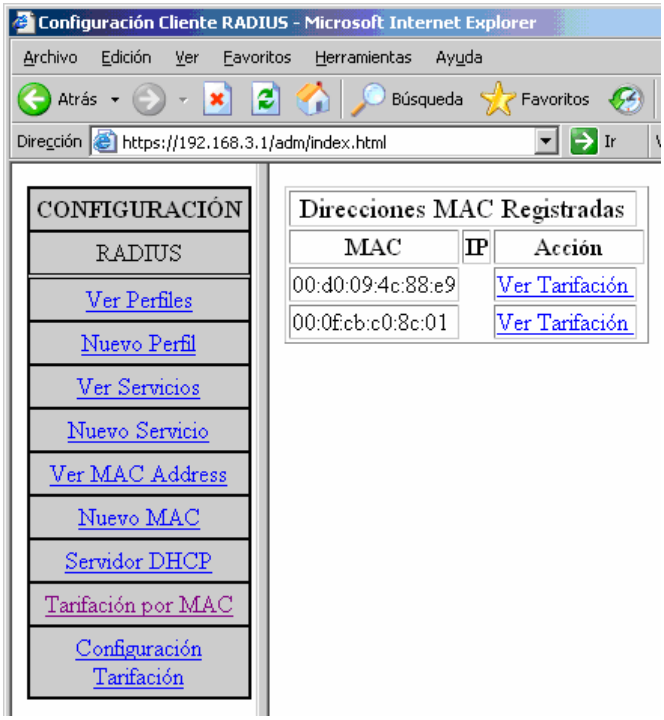

Figura 3.21 Tarifación por usuario en base a su dirección MAC

La selección para realizar la tarifación por consumo de *bytes* o de tiempo se lo realiza en la interfaz de administración del Cliente RADIUS en el menú Configuración Tarifación. Como se muestra en la Figura 3.22.

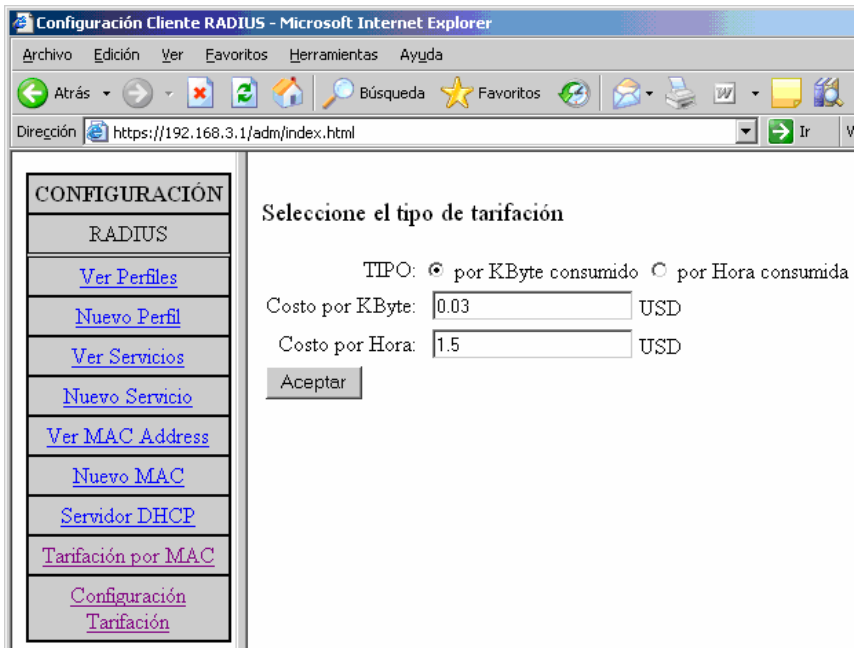

Figura 3.22 Configuración del tipo de tarifación

En la Figura 3.23 se presenta un ejemplo de tarifación por tiempo consumido.

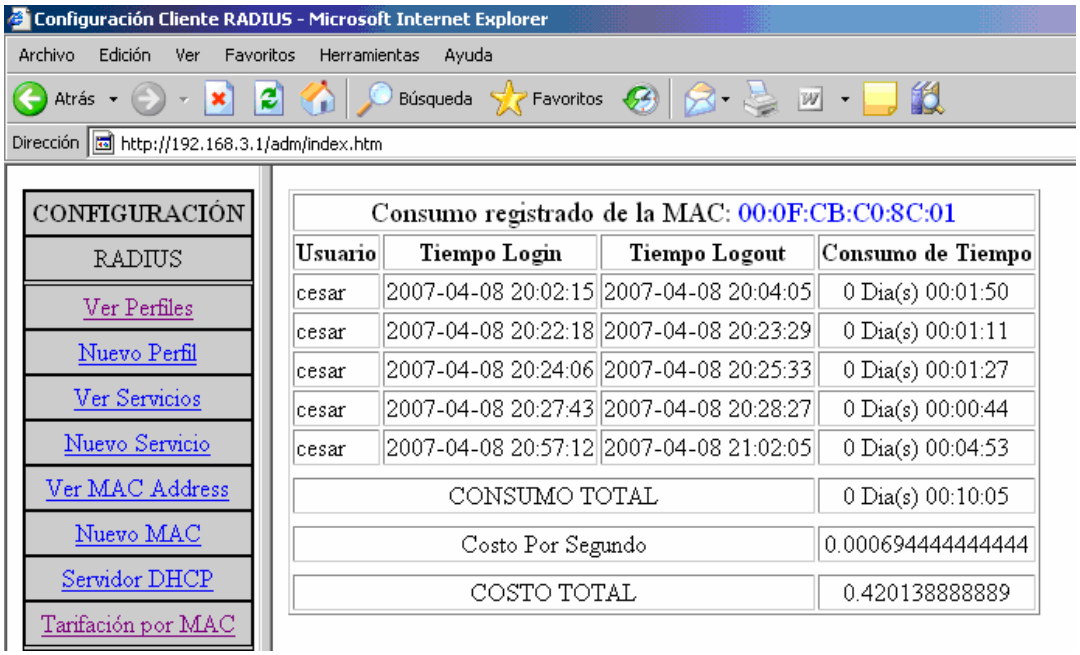

Figura 3.23 Tarifación de utilización por consumo de tiempo

En la Figura 3.24 se presenta un ejemplo de tarifación por *bytes* consumidos.

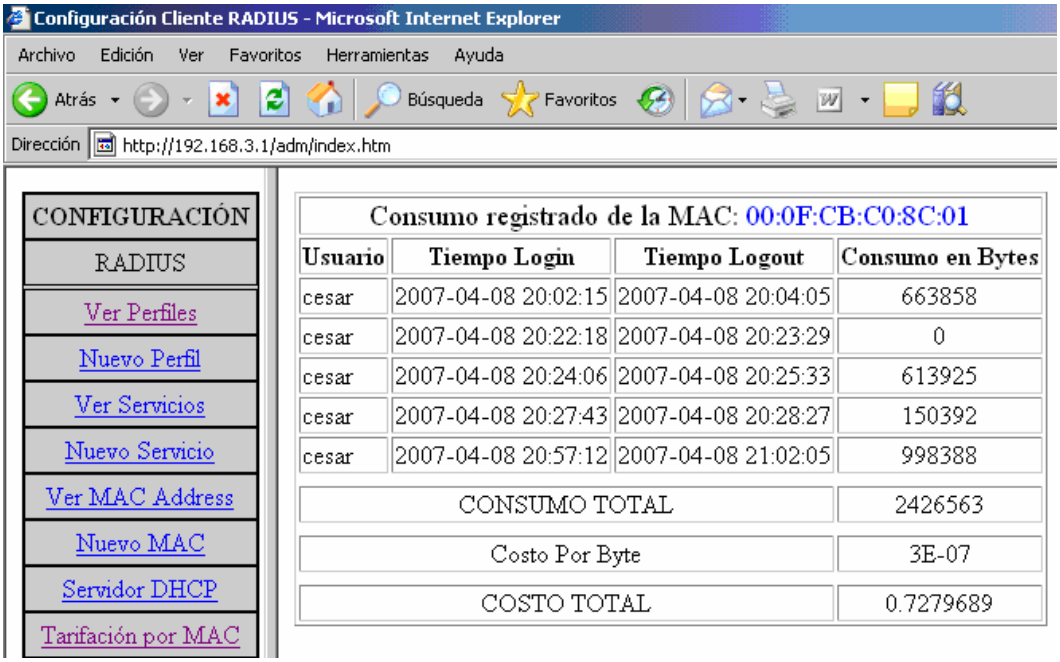

Figura 3.24 Tarifación de utilización por consumo de *bytes*

3.9 ANÁLISIS DE LOS RESULTADOS OBTENIDOS EN EL AMBIENTE DE PRUEBA

En virtud a que todos los parámetros técnicos se han revisado y verificado, el análisis de resultados se hará desde el punto de vista de cumplimiento funcional de la solución.

Se procederá a realizar un análisis de cada una de las pruebas y que implicación tiene el resultado de la misma en la funcionalidad del sistema.

El servidor *dial-up*, permitirá tener acceso a usuarios remotos hacia la red local a través de la red de telefonía pública, por lo que se empleó como servidor de acceso remoto un computador con sistema operativo *Windows* XP.

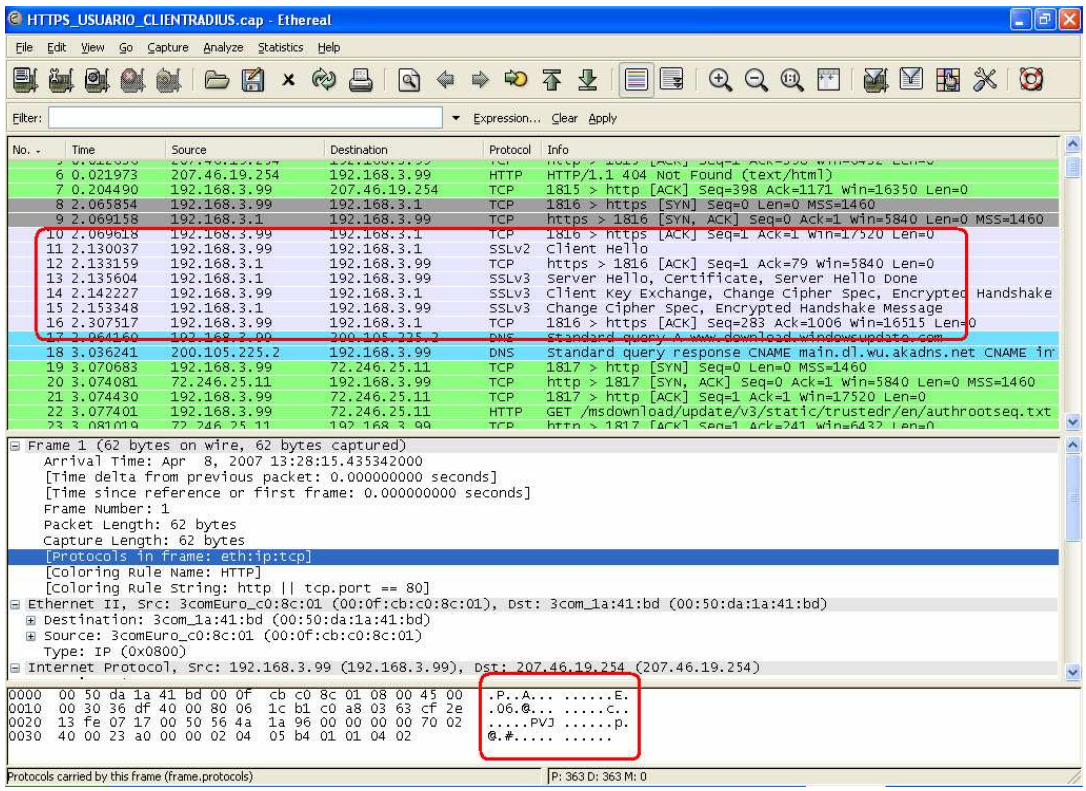

Figura 3.25 Captura de tráfico de autenticación de usuarios remotos

En base a las pruebas realizadas, se encuentra que una vez que el usuario se ha

autenticado con el servidor de *dial-up* es tratado como un usuario de la red local, y se lo puede verificar en las capturas de tráfico realizadas en el proceso de autenticación del usuario remoto Figura 3.25.

En el caso de los usuarios remotos, si el usuario desea tener acceso a los servicios de la red local deberá primeramente validarse en el servidor de acceso remoto y una vez validado deberá autenticarse con el cliente RADIUS.

La configuración del usuario remoto *dial up* es un proceso bastante sencillo y se lo realiza empleando el asistente de configuración de nuevas conexiones de *Windows*.

Revisando las capturas de *Ethereal* del intercambio de información entre el cliente RADIUS y el servidor RADIUS, se puede ver claramente que el empleo de IPSec entre estos dos computadores, efectivamente protege la información intercambiada entre los mismos sin causar un impacto representativo en la operación habitual del usuario, es decir, el hecho de que el túnel IPSec este levantado entre los dos computadores es transparente al usuario.

Durante el proceso de implementación de la solución, se contempló que para el intercambio de la información de autenticación del usuario se emplee el protocolo HTTPS, siendo esto verificado durante un proceso completo de autenticación Figura 3.26, ya que al momento que el usuario abre un explorador de Internet y realiza una petición de alguna dirección web, el sistema lo redirecciona hacia la página de autenticación que se presenta empleando HTTPS en el explorador del usuario. Este comportamiento del sistema garantiza que la confidencialidad de información de autenticación que viaja entre el cliente y el usuario se encuentra protegida.

El cliente RADIUS puede ser administrado a través del establecimiento de una sesión segura SSH, empleando línea de comandos, siendo esta administración no muy amigable al usuario final. Por otra parte y considerando reducir la complejidad de administración del sistema se diseñó una interfaz gráfica web que

permite realizar tareas de administración de una forma más sencilla e intuitiva.

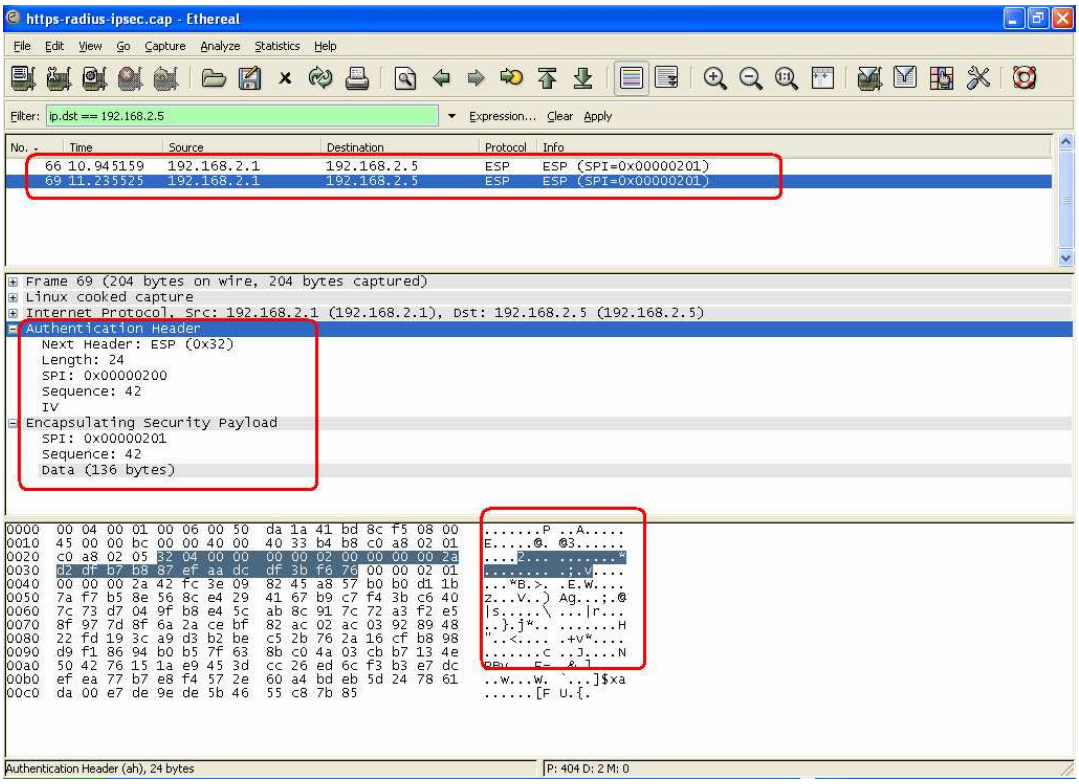

Figura 3.26 Captura de tráfico IPSec intercambiado entre el Servidor y el Cliente

Las tareas de administración del cliente RADIUS que emplearán línea de comandos serán el levantamiento del *script* de control de tiempo y el establecimiento de las reglas de *iptables* iniciales.

El momento de realizar las pruebas del segmento de red inalámbrico se observó de forma clara como se protege el segmento, al emplear WPA con 802.1X.

En la implementación del aseguramiento del segmento fue necesario instalar un certificado digital en el computador del usuario. Se pudo verificar que si un usuario no dispone del correspondiente certificado no habrá manera que pueda ser autenticado en la red inalámbrica y lograr acceso a la red y por ende a sus servicios.

Aun cuando el implementar este tipo de seguridad conlleva de tiempo, el nivel de

seguridad logrado es adecuado. De igual manera la administración de los certificados digitales, implicaría una carga adicional al administrador del sistema, pero esto es un costo aceptable por disponer de seguridad óptima dentro de la infraestructura de red inalámbrica.

En caso de implementarse este tipo de solución para proveer del servicio de Internet a usuarios (hoteles, restaurantes, aeropuertos), será necesario en todo caso emplear mecanismos de aseguramiento como filtros por MAC en el punto de acceso inalámbrico y dejar que la autenticación del usuario para acceso a los servicios lo haga a través del sistema del cliente RADIUS.

Se pudo verificar que a través de un control por dirección MAC el servidor DHCP asignaba dirección IP únicamente al dispositivo cuya dirección MAC fue registrada previamente en el sistema.

Al asignar de forma estática una dirección IP del segmento de red de usuarios, se encontró que se puede acceder al sistema de autenticación, aun cuando el dispositivo en el cual se configuró la dirección IP de forma estática no era un equipo registrado en el sistema, identificándose una vulnerabilidad del sistema.

Para mitigar la vulnerabilidad encontrada se procedió a realizar una verificación entre la dirección MAC del usuario y la base de datos de las direcciones MAC registradas en el sistema, si la validación es exitosa se permitirá que dicho usuario acceda al sistema de autenticación caso contrario no.

Una vez que el usuario ha logrado obtener dirección IP en el caso de ser un usuario que emplee DHCP o es un usuario con MAC registrada, éste podrá validarse en el sistema del cliente RADIUS.

El administrador del sistema será el encargado de generar las cuentas de usuario y las correspondientes contraseñas. Se recomienda que se maneje un estándar de generación de cuentas, por ejemplo emplear la primera letra del nombre de usuario seguida de su apellido para el nombre de usuario y una clave de por lo

menos ocho caracteres alfanuméricos.

Se verificó claramente que a través de la interfaz de administración (Figura 3.27) se puede manipular los perfiles (ver, crear nuevos), los servicios asociados a cada perfil (crear, asociar servicios a perfiles), añadir MAC válidas al sistema, configurar el servicio de DHCP, configuración de los parámetros de ancho de banda asignados a cada perfil y generar reportes de utilización del sistema con su respectiva tarifación.

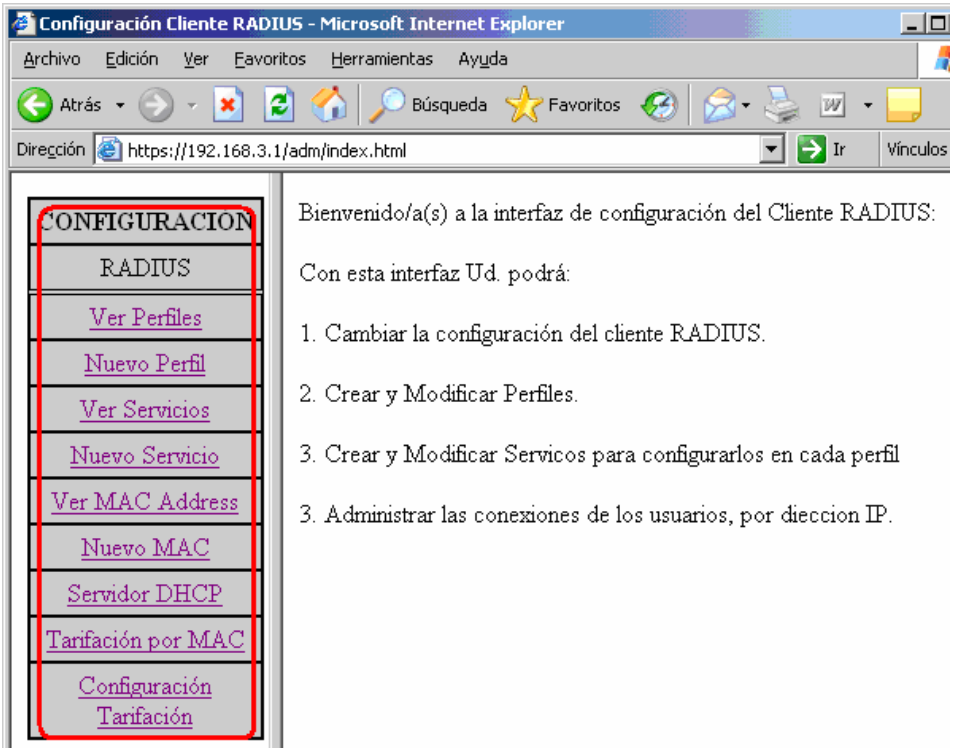

Figura 3.27 Administración Gráfica del cliente RADIUS

Se comprobó que el *script* de control de tiempo, permite actualizar la información de tiempo cada cinco segundos, cada vez que hubo actividad del usuario caso contrario después de un determinado tiempo se lo considerará como inactivo y se lo desasociará del sistema. Esto se verificó en línea de comandos que el *script* actualiza la información de consumo y se lo revisó posteriormente en el reporte de utilización que permite generar la interfaz gráfica.

En base al análisis realizado se puede concluir que el presente proyecto cumple lo planteado en el alcance, en términos de las políticas de seguridad, facilidad de configuración y funcionalidad.

3.10 ANÁLISIS DE LOS RESULTADOS OBTENIDOS EN EL AMBIENTE REAL

El objetivo de las pruebas en un ambiente real es determinar como la utilización del sistema afecta a los usuarios y su funcionamiento en un ambiente de red real, en este caso las pruebas se realizaron en la red LAN de la empresa La Competencia SA, por razones de seguridad operacional de la empresa, la Gerencia General autorizó únicamente implementar el ambiente de pruebas en un segmento de red, cuyos usuarios no manejen aplicaciones críticas de la operación organizacional (departamento financiero, usuarios gerenciales) y por otro lado que el número de usuarios que empleen el servicio sean un número reducido.

Gerencia General encargó al Jefe de Sistemas quien es el administrador de red y administrador de las aplicaciones de la red de datos de La Competencia SA, la coordinación de las pruebas y la asignación de los usuarios que participarían en las pruebas del sistema de autenticación.

Se autorizan a cinco usuarios para ser empleados en las pruebas del sistema, distribuidos de la siguiente forma, dos usuarios inalámbricos, tres usuarios cableados y las pruebas de acceso a través de *dial-up* se las realizaría de forma remota con un usuario generado para verificación de esta característica del sistema.

Para evaluar la aceptación del sistema se estableció usuarios que manejan tecnología (usuarios del departamento de sistemas y networking) y usuarios convencionales (departamento de ventas).

Se empleó en la prueba dos usuarios del departamento de ventas, dos usuarios

del departamento de *networking* y un usuario del departamento de sistemas. El objetivo de emplear usuarios de diferentes áreas fue con el fin de tener diferentes criterios en la evaluación de la aplicación implementada. Se consideró los usuarios del departamento de *networking* y sistemas para disponer de un criterio técnico de evaluación de la solución.

En la siguiente sección se presenta una descripción del ambiente de prueba real, como se lo implementó y un análisis de los resultados obtenidos en cada una de las etapas de implementación.

3.10.1 TOPOLOGÍA DE LA RED DE PRUEBA

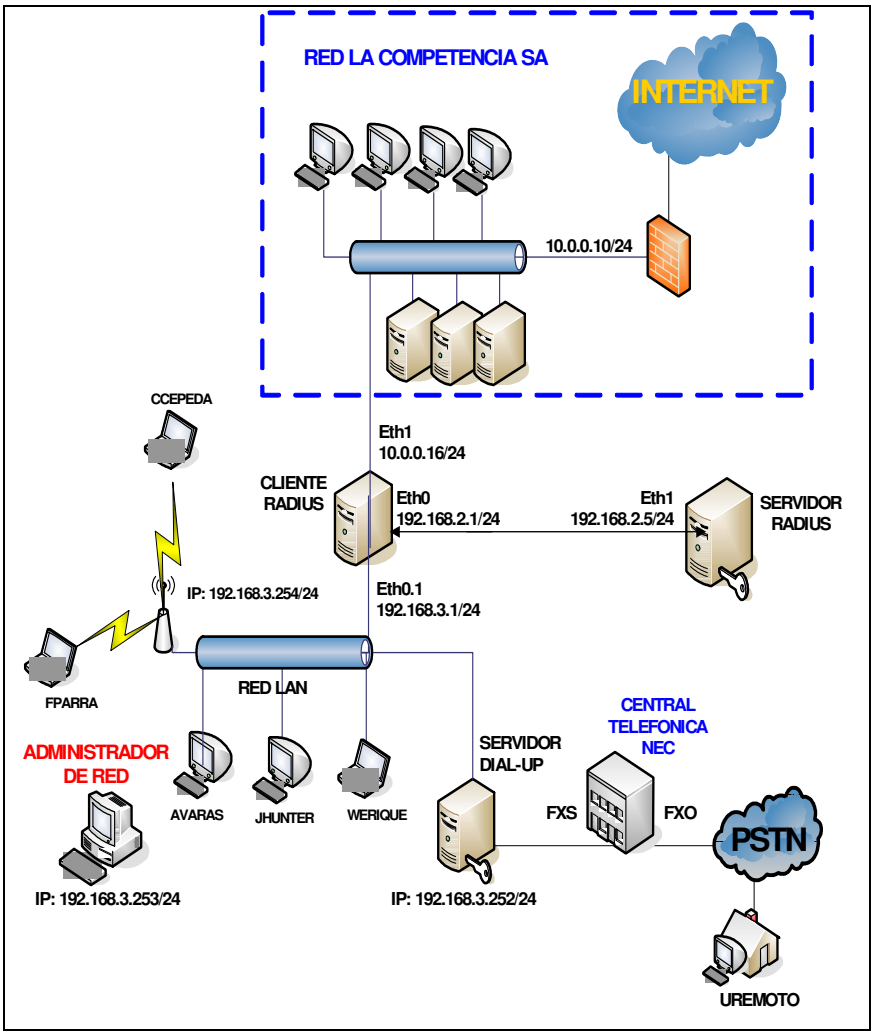

Figura 3.28 Topología de red del ambiente real

Se implementó la infraestructura de comunicaciones, colocándose todos los usuarios de prueba en la interfaz LAN del cliente RADIUS y la interfaz WAN del cliente RADIUS hacia la red local.

Se configuró el servidor DHCP, de tal manera que cuando los usuarios soliciten dirección IP, se les otorgue una dirección de la red clase C 192.168.3.0/24 y como direcciones de DNS, las direcciones IP de los servidores de Dominio de La Competencia SA.

En la Figura 3.28 se presenta la topología de red implementada en el ambiente real.

3.10.2 CREACIÓN DE LOS USUARIOS

Una vez que el sistema empezó a funcionar de forma adecuada fue necesario definir los usuarios que participarían en la prueba. De la coordinación realizada con el Jefe de Sistemas de La Competencia SA, se definieron los usuarios que se presentan en la Tabla 3.3.

Departamento	Nombre de Usuario	USUARIO	CLAVE	Tipo de usuario	Tipo de LAN
Ventas	Andres Varas	avaras	********	Convencional	Cableado
Ventas	Jhony Hunter	jhunter	********	Convencional	Cableado
Networking	César Cepeda	ccepeda	********	Técnico	Inalámbrico
Networking	Wilson Erique	werique	********	Técnico	Cableado
Sistemas	Felix Parra	fparra	********	Técnico	Inalámbrico
Networking	Usuario Remoto	uremoto	********	Técnico	Remoto

Tabla 3.3 Detalle de usuarios de prueba Red LCSA

Los usuarios convencionales fueron seleccionados del departamento de ventas, ya que los usuarios de este departamento no conllevan aplicaciones críticas en la operación diaria de la empresa como lo son las gerencias, departamento financiero y bodega, por mencionar algunos de los que fueron indicados.

Todos los usuarios tendrán un tiempo máximo de conexión al sistema por sesión

de 8 horas y un tiempo de desconexión del sistema por inactividad de 10 minutos.

Los perfiles creados fueron implementados en función del departamento al cual cada usuario pertenece, siendo el perfil que más requerimientos tenía el perfil sistemas, ya que debía tener acceso tanto a los aplicativos de la red interna de la red de La Competencia SA sin restricción alguna y acceso hacia aplicativos, cuya administración se realiza de forma remota

En la sección siguiente se analizará el criterio con el cual se han asignado los servicios y privilegios de ancho de banda por perfil de cada usuario.

3.10.3 CREACIÓN DE LOS SERVICIOS PARA CADA PERFIL

Se crearon tres perfiles de usuario en función de los departamentos a los cuales pertenecían los usuarios, es decir un perfil *networking*, uno ventas y uno sistemas.

Para realizar esta configuración fue necesario consultar la operación de cada uno de los departamentos, en el sentido de revisar a qué servicios de red debe acceder cada usuario (puerto TCP o UDP), esta información fue proporcionada por el departamento de sistemas de La Competencia SA.

El sistema permite asignar el ancho de banda para cada perfil, en función de un porcentaje ancho de banda, la suma de los porcentajes de todos los perfiles en ningún caso excederá de 100%.

En el caso del perfil sistemas por las actividades que realizan y considerando que deben realizar descargas de *software*, que deben acceder de forma remota a ciertos aplicativos y que deben acceder a administrar los usuarios y servidores de la red interna se le asignó un ancho de banda de 50%.

En el caso del perfil *networking*, considerando que esta clase de usuario accederá hacia Internet, al sistema de inventario de equipos y a correo electrónico, se le ha asignado un ancho de banda de 30%.

En le caso del perfil ventas, esta clase de usuario requiere acceder a la lista de precios internos, inventarios, acceso a Internet y correo electrónico no siendo necesario un gran ancho de banda de salida hacia el Internet, por lo que se le asignó un ancho de banda del 20%.

Se ha asignado un porcentaje de ancho de banda al perfil *networking* mayor que el perfil ventas, ya que el personal de *networking* requiere un privilegio mayor para acceder a Internet a revisar información de equipo de comunicaciones e información de cursos en línea.

En la Tabla 3.4 se presenta los perfiles creados y se puede observar adicionalmente el ancho de banda asignado a cada perfil.

Perfiles						
ID	**Nombre**	**Descripción**	**% del AB Total**	**Acciones**		
1	Sistemas	Acceso Total	50	Ver Servicios	Modificar	Eliminar
2	Networking	Acceso Medio	30	Ver Servicios	Modificar	Eliminar
3	Ventas	Acceso Restringido	20	Ver Servicios	Modificar	Eliminar

Tabla 3.4 Perfiles de usuarios creados

Para poder configurar los servicios de cada perfil es necesario primero ingresar en el sistema el listado de servicios que se va a configurar en cada perfil, para lo cual se deberá ingresar cada uno de los servicios mediante la interfaz de administración.

Se procedió a ingresar un listado de servicios, en el cual consta el nombre del servicio, el número de puerto y el tipo de puerto. La información para generar el listado fue tomada del archivo de texto plano “etc/services” del sistema de archivos de LINUX.

En la Tabla 3.5 se presenta todos los servicios ingresados; para ser configurados en los perfiles.

SERVICIOS				
Nombre	Puerto	Tipo	Acciones	
ftp-data	20	tcp	Eliminar	Modificar
ftp	21	tcp	Eliminar	Modificar
ssh	22	tcp	Eliminar	Modificar
telnet	23	tcp	Eliminar	Modificar
smtp	25	tcp	Eliminar	Modificar
tftp	69	tcp	Eliminar	Modificar
http	80	tcp	Eliminar	Modificar
netbios-ns	137	tcp	Eliminar	Modificar
netbios-dgm	138	tcp	Eliminar	Modificar
netbios-ssn	139	tcp	Eliminar	Modificar
imap	143	tcp	Eliminar	Modificar
snmp	161	tcp	Eliminar	Modificar
snmptrap	162	udp	Eliminar	Modificar
https	443	tcp	Eliminar	Modificar
ldaps	636	tcp	Eliminar	Modificar
ldaps	636	udp	Eliminar	Modificar
pop3s	995	tcp	Eliminar	Modificar
ms-sql-s	1433	tcp	Eliminar	Modificar
ms-sql-m	1434	tcp	Eliminar	Modificar
ms-sql-m	1434	udp	Eliminar	Modificar
radius	1812	tcp	Eliminar	Modificar
radius-acct	1813	tcp	Eliminar	Modificar
telefonia-ip	1000	udp	Eliminar	Modificar

Tabla 3.5 Servicios configurados previamente

Una vez que se ha configurado los diferentes servicios dentro del sistema, se procede a asignar los servicios correspondientes a cada uno de los perfiles.

Para el caso del perfil “sistemas” se procedió a añadir todos los servicios listados en la Tabla 3.5, ya que este perfil de usuario requiere de un acceso total a una gran cantidad de servicios tanto de monitoreo, de administración de la red y servicios puntuales de la operación de la organización.

En el caso del perfil “sistemas” fue necesario añadir los puertos de acceso hacia la base de datos SQL, añadir el acceso hacia el puerto 1000 UDP de servicio de

telefonía IP requerido para registro de teléfonos de software y el puerto IMAP para recoger los correos de voz en el buzón del correo electrónico.

En el caso del perfil "*networking"*, se procedió a añadir los servicios de correo electrónico (SMTP, POP3), acceso a Internet (HTTP, HTTPs), protocolos de acceso remoto a servidores de archivos (FTP, TFTP), así como también protocolos de comunicación para administración de dispositivos de red (SNMP, TELNET) y el protocolo que emplea para recoger los correos de voz en el buzón del correo electrónico (IMAP).

En la Tabla 3.6, se muestra el listado de los servicios que se añadieron al perfil *networking*.

Perfil Networking			
Servicios Configurados			
Nombre	**Puerto**	**Tipo**	**Acciones**
ftp-data	20	tcp	Quitar
ftp	21	tcp	Quitar
telnet	23	tcp	Quitar
smtp	25	tcp	Quitar
tftp	69	tcp	Quitar
http	80	tcp	Quitar
netbios-ns	137	tcp	Quitar
netbios-dgm	138	tcp	Quitar
netbios-ssn	139	tcp	Quitar
https	443	tcp	Quitar
pop3s	995	tcp	Quitar
ms-sql-s	1433	tcp	Quitar
telefonia-ip	1000	udp	Quitar

Tabla 3.6 Servicios del perfil *Networking*.

Fue necesario añadir todos los puertos empleados en el servicio SQL, ya que esto era necesario para poder acceder a la base de datos que almacena el inventario de equipos de comunicaciones y poder realizar egresos e ingresos de los equipos a bodega.

Los puertos empleados por Netbios, fue necesario añadirlos debido a que la aplicación interna que interactúa como interfaz de las consultas a la base de datos requería de este protocolo para poder funcionar de forma adecuada dentro de la infraestructura de red.

El perfil “ventas” consta de usuarios convencionales que no poseen ningún conocimiento técnico, y ayudarán a tener una evaluación adecuada de la solución implementada, ya que solo se les proporcionó su clave de acceso y las instrucciones de uso.

En el caso de estos usuarios se consideró que deben tener acceso hacia el correo electrónico (SMTP, POP3), acceso hacia Internet (HTTP, HTTPS), acceso al aplicativo de consultas de inventarios de equipos (MS-SQL, Netbios) y acceso a los correos de voz empleando correo electrónico (IMAP).

En la Tabla 3.7 se presenta la lista de los servicios configurados en el perfil ventas.

Perfil Ventas			
Servicios Configurados			
Nombre	**Puerto**	**Tipo**	**Acciones**
smtp	25	tcp	Quitar
http	80	tcp	Quitar
netbios-ns	137	tcp	Quitar
netbios-dgm	138	tcp	Quitar
netbios-ssn	139	tcp	Quitar
imap	143	tcp	Quitar
https	443	tcp	Quitar
pop3s	995	tcp	Quitar
ms-sql-s	1433	tcp	Quitar

Tabla 3.7 Servicios del perfil ventas

En todos los caso se verificó el correcto funcionamiento de cada uno de los usuarios participantes en al prueba.

3.10.4 ADHESIÓN DE DIRECCIONES MAC AL CLIENTE RADIUS

Para que cada uno de los usuarios pueda acceder al sistema de autenticación del cliente RADIUS, primeramente deberán obtener una dirección IP misma que es proporcionada a través de DHCP.

Para que un usuario pueda obtener una dirección IP de forma dinámica, su dirección MAC deberá ser registrada previamente en el cliente RADIUS.

Se verificó que únicamente los usuarios con dirección MAC registrada en el cliente RADIUS, eran capaces de obtener una dirección IP de forma dinámica y posteriormente acceder al sistema de autenticación. Este aspecto fue importante ya que al añadir un sistema adicional a una red en producción se debía mantener la seguridad de la misma.

Para el usuario es transparente todas las verificaciones que realiza el sistema y lo único que deberá configurar es su tarjeta de red para obtener una dirección IP de forma dinámica.

3.10.5 ADHESIÓN DE DIRECCIONES MAC VALIDAS DE USUARIOS DEL SEGMENTO INALÁMBRICO

En el caso de un usuario del segmento inalámbrico, se deberá ingresar la dirección MAC del usuario en el sistema del Cliente RADIUS y en la configuración del filtro por MAC del punto de acceso inalámbrico. Se puede indicar que en este caso se tiene un doble control por MAC.

Considerando que una dirección MAC puede ser robada y asignada a un usuario de forma falsa empleando herramientas de software, adicional a los controles por MAC se empleará WPA con 802.1X.

WPA con 802.1X emplea certificados digitales para la autenticación de usuarios, siendo necesario crear los certificados digitales para los dos usuarios

inalámbricos y posteriormente instalarlos en cada uno de los computadores.

El empleo de esta combinación de mecanismos de seguridad en el segmento inalámbrico, garantiza que accedan a la red interna solamente usuarios autorizados y que no se añada una vulnerabilidad a la seguridad de la red interna.

3.10.6 SERVIDOR DE ACCESO TELEFÓNICO

El servidor de acceso telefónico se lo colocó en el mismo segmento de red que a los usuarios cableados y con el MODEM conectado hacia el puerto de voz FXS de una extensión de la central telefónica NEC Modelo IPS.

Para comprobar que el servidor funcionaba de forma adecuada se configuró una conexión de acceso *dial-up*, en la configuración del teléfono a ser marcado se procedió a colocar el número de destino, seguido de unas cinco comas que emulan pausas de tiempo, de tal manera que la operadora automática conteste y se pueda ingresar los dígitos correspondientes a la extensión asignada al MODEM del servidor.

En la central NEC se asignó una extensión analógica (puerto FXS), para poder asignar esta extensión al servidor de acceso remoto.

La prueba del acceso remoto se realizó por una par de veces ya que de los usuarios disponibles para hacer pruebas, solo se designó uno para este tipo de acceso y adicionalmente el servidor de acceso remoto solo disponía de un MODEM.

En la Figura 3.29, se presenta la pantalla de la conexión de acceso remoto *dial-up*, capturas realizadas desde el computador del usuario remoto.

De hecho mediante la prueba indicada anteriormente se logró comprobar que una vez que el usuario logra autenticarse con el servidor de acceso remoto, podrá acceder al sistema de autenticación y de esta forma poder acceder a los servicios

que su perfil lo permita, en este caso el perfil utilizado para este usuario fue sistemas, y una vez autenticado en el Cliente Radius se realizó pruebas de acceso de los diferentes protocolo hacia la red interna de La Competencia SA y hacia Internet.

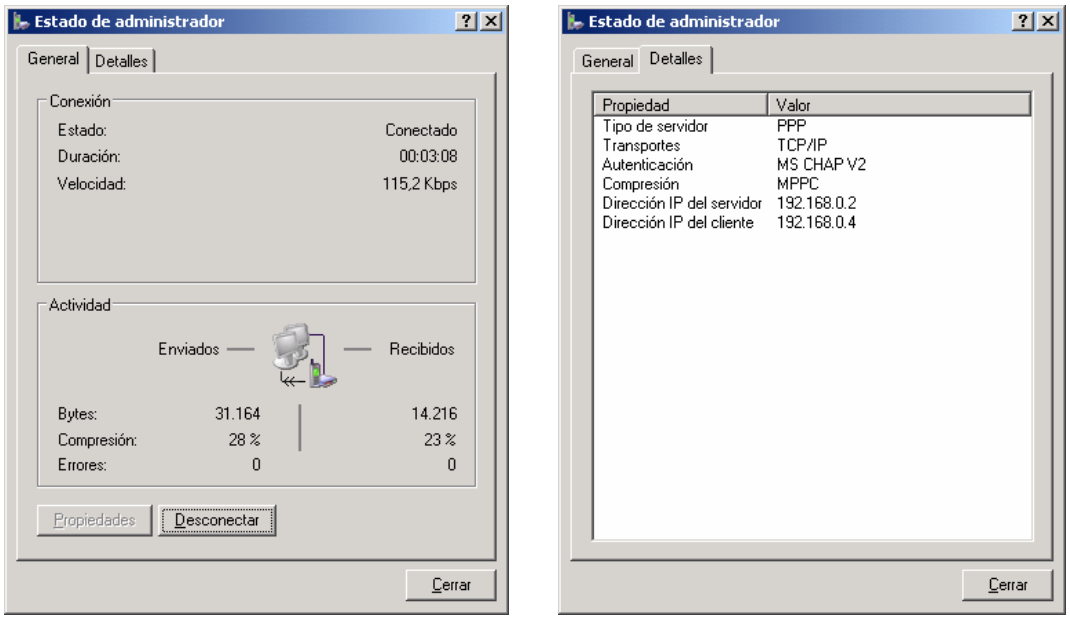

Figura 3.29 Pantallas del estado y detalles de la conexión.

3.10.7 ADOPCIÓN DE SOLUCIÓN POR PARTE DE LOS USUARIOS

Revisando el desempeño de la aplicación durante el período de prueba en ambiente real, se pudo observar que la implementación es bastante estable ya que el sistema no presentó ningún inconveniente o corte de servicio.

Cada uno de los usuarios en el período de prueba no presentaron inconveniente alguno de funcionamiento, esto fue favorable en la adopción de la solución ya que la única variación en la forma habitual de trabajo de los usuarios fue que debían autenticarse adicionalmente vía el sistema del Cliente RADIUS.

Con respecto a los usuarios del área *networking* y sistemas no fue un problema la adopción de esta nueva forma de acceso a los servicios de red, al tener que realizar previamente una autenticación, el sistema fue aceptado de buena

manera, esto debido a que no conlleva un cambio representativo en el comportamiento de los usuarios.

En el caso de los usuarios del área de ventas la adopción de la solución presentó un ligero malestar, ya que por inactividad el sistema automáticamente desconectaba al usuario del sistema cada 10 minutos, siendo necesario que se autentique nuevamente para poder acceder a los servicios de red.

Una alternativa de solución para que no se tenga este inconveniente es aumentar el valor *idle time out*, de tal manera que la desconexión por inactividad se realice de forma automática después de nueve horas, que corresponden a las horas laborables de un día de trabajo.

En el caso de los usuarios inalámbricos, el mecanismo empleado para la autenticación de los usuarios en la red fue muy atractivo a ser implementado en la organización, pues presentaba un nivel de seguridad adicional, eficiente y bastante confiable.

La adopción del sistema de autenticación del Cliente RADIUS, es una buena alternativa, ya que permite tener funcionalidades como control de ancho de banda por usuario, registro de la actividad de cada usuario, definir períodos de utilización, permite la difusión de mensajes o publicidad en la página de autenticación y es una solución implementada en su totalidad con *software* de libre distribución.

Aun cuando La Competencia SA dispone de un servidor de *Active Directory*, para el control de acceso de los usuarios a los servicios de red, la solución Cliente RADIUS en LINUX le proporciona de funcionalidades bastante útiles dentro de la infraestructura de red y lo que es mejor a un costo beneficio bastante aceptable.

Algo importante a mencionar es que al tratarse de una solución implementada en su totalidad con *software* de libre distribución, permite que la solución sea flexible en términos de poderse ajustar a las necesidades de los clientes.

El implementar esta solución no conlleva de un cambio representativo dentro de la infraestructura de red de las organizaciones ya que el equipo se lo coloca como un intermediario entre los usuarios y los servicios que se desean controlar.

El sistema podrá ser empelado en organizaciones que proporcionan el servicio de Internet como son hoteles, aeropuertos, restaurantes, colegios, universidades, por mencionar algunos. Y de igual manera será una alternativa bastante buena cuando se considere el asegurar los segmentos de red inalámbrica.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El sistema planteado reúne los requisitos de ser un sistema de uso simple desde el punto de vista del usuario, pero reúne la complejidad suficiente dentro de sus procesos internos, para ser una solución lo suficientemente segura. Todos los procesos adicionales que se realizarán dentro del sistema de seguridad, son totalmente transparentes para el usuario, es decir el usuario no se percatará que dentro del sistema se realizan verificaciones adicionales de seguridad.

- Se comprobó que el sistema realiza un control de utilización de los recursos de la red, ya que no únicamente permite tener un control de acceso por aplicación, sino que también permite realizar un control de utilización del ancho de banda de la red, a través de una asignación de un porcentaje del ancho de banda total por perfil de usuario.

- El sistema permite obtener un historial de todas las sesiones y consumo que el usuario realice por tiempo o por *kbyte*. Esta información podrá obtenerse de la base de datos del cliente RADIUS y podrá ser observada por medio de la interfaz de administración del sistema o por medio de herramienta gráfica de administración de base de datos "*PhpMyAdmin*".

- *Iptables* es una herramienta flexible, aun cuando su entendimiento conlleva algo de complejidad; una vez comprendida su filosofía de funcionamiento, la herramienta se vuelve muy versátil y permite realizar implementaciones modulares. La complejidad de utilización de *iptables* se reduce sustancialmente ya que en el sistema implementa una interfaz de

administración vía web que encapsula la complejidad de *iptables* para la generación de las reglas de control de acceso hacia aplicaciones.

- El proporcionar al usuario una interfaz de administración gráfica en implementaciones que tradicionalmente emplean archivos de configuración de texto plano y por línea de comandos, ayuda en la adopción de estas soluciones y las hace más atractivas para el usuario.

- Para personalizar los mensajes de error que presenta Apache y los mismos se presenten de forma adecuada a usuarios que empleen Internet Explorer, se debe considerar que el tamaño de la página que contiene el mensaje debe ser mayor a 512 caracteres.

- Es necesario habilitar los módulos que permiten manejar el control de tráfico FTP en el *kernel* de LINUX, para habilitar el filtro de tráfico FTP. El no habilitar los módulos ocasiona que las reglas de *firewall* correspondientes al manejo de permiso del tráfico FTP tanto pasivo como activo no funcionen bien, es decir el tráfico se bloquea de forma permanente y este tipo de tráfico no puede ser administrado de forma modular.

- Como la interfaz de administración en su totalidad esta implementada en PHP y desde la misma se realiza configuraciones que conllevan el ejecutar comandos, fue necesario permitir el acceso desde páginas PHP a los comandos *iptables* y *service*. Este tipo de permiso se lo realizó en virtud a que se requería poder ejecutar determinadas tareas que involucraban línea de comandos desde las páginas PHP. El parámetro de seguridad, con el cual se realizó este cambio, es con el criterio que la administración de los privilegios de usuarios, únicamente es asignada por el administrador del sistema central.

- Es importante leer minuciosamente las salidas generadas cada vez que se instala un nuevo programa en LINUX, pues esta información es de ayuda

cuando se solicita soporte a través de foros, información igualmente importante es saber de forma consistente cual es el error que se presenta conjuntamente con un resumen de todo el entorno en el cual se esta instalando el archivo que presenta problema.

- Emplear SSH para acceder de forma remoto a la administración a través de línea de comandos de un equipo, evita ataques del tipo "*man in the middle*", ya que el único tráfico que podría capturase sería tráfico encriptado, que no será de utilidad para un atacante.

- Para establecer sesiones de tipo SSH en ambientes *Windows,* es necesario emplear una herramienta de *software* adicional (p.e putty.exe) que permita establecer sesiones de este tipo, ya que el sistema operativo por defecto no tiene integrada una herramienta propia que le permita establecer sesiones SSH hacia otros equipos,

- Se dispondrá de mayor seguridad al emplear herramientas de *software* abierto y de libre acceso, ya que al haber más personas que lo utilizan y lo revisan, ayudarán a encontrar posibles errores o fallas de seguridad que podrían afectar el funcionamiento del sistema.

- La filosofía de distribución de código libre, busca que el conocimiento del desarrollo de las aplicaciones, sea libre para quien quiera emplearlas, de esta forma si el usuario llegase a encontrar algún problema de seguridad o de otra índole en la aplicación, podrá editar directamente el código fuente o informar al desarrollador de la aplicación, para que en una futura versión se corrija el problema.

- Al retirar una tarjeta del servidor RADIUS sin deshabilitarla anteriormente, la información correspondiente a este dispositivo permanece almacenada en el sistema LINUX, ocasionando problemas de *hardware*. Por lo que será necesario instalarla nuevamente, deshabilitarla y borrarla a través de *software*, para posteriormente retirarla. Con el procedimiento mencionado

se logra que el error desaparezca y el sistema pueda entrar en funcionamiento nuevamente.

- Se emplea el archivo rc.local ubicado en directorio /etc, para poder ejecutar *scripts* o comandos que se desee se inicien el momento que se inicializa el LINUX. Característica de utilidad en el sistema implementado, ya que el mismo interactúa con otros *scripts* de programas para funcionar adecuadamente, y los mismos deben ser inicializados cada vez que el sistema es apagado.

- El archivo .htaccess es empleado para realizar una autenticación local en el servidor http, de tal manera que una vez ingresados lo datos de usuario y clave correctos, la página se desplegará. Este mecanismo de autenticación fue de mucha utilidad en la protección de la interfaz de administración del cliente RADIUS.

- Mientras más mecanismos de seguridad se empleen en sistemas de control de acceso, el sistema será más seguro, aun cuando un sistema con seguridad absoluta no exista, el hecho de implementar un mayor número de mecanismos de control ayudará a que el sistema sea menos vulnerable.

- El mecanismo empleado para la autenticación de los usuarios inalámbricos en la red es bastante seguro y eficiente, pero conlleva de un procedimiento de instalación adicional en cada usuario, que debe ser considerado en los tiempos de implementación.

- El método de autenticación empleado con los usuarios inalámbricos, es un mecanismo bastante seguro, pero si se lo desea emplear en un ambiente en el cual se realizan cambios constantes de los usuarios inalámbricos, no sería una alternativa muy viable, en este caso lo que se puede emplear es el habilitar filtros por dirección MAC en el punto de acceso y emplear el sistema de autenticación de cliente RADIUS, para que este último se encargue del control de acceso hacia los servicios de red.

- La implementación presentada es un claro ejemplo de la gran cantidad de posibilidades que se tiene para implementar soluciones de seguridad en redes de comunicaciones con herramientas de código abierto, como por ejemplo el uso de *iptables* para la implementación de FIREWALLs, Apache para la implementación de servidores Web, entre otros, y no únicamente para el sistema operativo Linux ya que existen versiones de *software* libre que también pueden ser empleadas en otros sistemas operativos.

- El *software* de código abierto tiene una gran aceptación y está ganando cada vez mas espacio como una alternativa para quien no tiene posibilidad de pagar altos costos por *software* propietario.

- El ejecutar el servidor RADIUS en modo depuración permite observar toda la información que el Cliente RADIUS envía al servidor y la información con la cual el servidor responde a estas peticiones. Gracias a esto se pueden ubicar de forma inmediata problemas que se estén dando con algún usuario, por ejemplo que no se este asignando un perfil en el cliente RADIUS debido a que no se configuró el campo "*service type*".

- La identificación de cada uno de los procesos y las tareas asociadas a cada organización, permitirán que se pueda realizar una implementación, reduciendo los riesgos de interrupciones de la organización y ayudando en una más rápida adopción de la nueva tecnología.

- El Cliente RADIUS podrá ser implementado en cualquier ambiente que se lo pueda aplicar, realizando pequeñas modificaciones, siendo la principal idea que el presente sistema provea de una fácil implementación.

4.2 RECOMENDACIONES

- Si se emplea mecanismos de autenticación con nombres de usuario y clave, es necesario concientizar a los usuarios de la importancia de mantener sus claves seguras con normas básicas como que no deben anotarlas en ningún lugar como recordatorio o que no deben facilitárselas a otras personas.

- En el presente proyecto al estar basado en una infraestructura que emplea como elementos principales servidores, es recomendable establecer políticas de respaldo de la información, de los equipos más críticos, en este caso del cliente RADIUS y del servidor RADIUS, así como también de una política de respaldo continua de la información de base de datos y configuraciones de los equipos.

- El lugar de instalación de los equipos debe poseer una apropiada instalación eléctrica, con puesta a tierra, así como también debe poseer elementos de respaldo como fuentes de alimentación ininterrumpida de por lo menos una hora de abastecimiento de energía.

- La seguridad física de los servidores es un aspecto muy importante, para prevenir posibles accesos por parte de personas no autorizadas a los mismos, los servidores deberán colocarse en un área donde el acceso lo tengan únicamente las personas que administren estos equipos.

- Se debe seguir normas básicas de programación para la implementación de sistemas de este tipo, ya que como se pudo comprobar durante la programación de la interfaz de autenticación para los usuarios y de la interfaz de administración del sistema, fue de mucha utilidad el mantener un orden claro de cada uno de los archivos involucrados en la ejecución de las diferentes funcionalidades del sistema, al momento de realizar modificaciones o correcciones al código ya programado.

- Se recomienda en el proceso de adopción de una nueva solución de tecnología de comunicaciones, realizar un seguimiento del proyecto a través de un esquema, que permite en primer lugar levantar los requerimientos del usuario tanto técnicos como de negocios, para que una vez identificados estos requerimientos poder definir como cumplir con los requerimientos de usuario, que elementos emplear, como implementar dichos elementos, como van ha ser adoptados dichos elementos, el proceso de implementación y el proceso de administración de estos nuevos elementos en la red.

- Es importante para la óptima operación del sistema, que el administrador mantenga un estricto cumplimiento de las políticas de seguridad descritas e implementadas como parte de la solución presentada, ya que el incumplimiento de alguna de las mismas puede dar lugar a un incremento de la vulnerabilidad del sistema y este puede ser un blanco fácil para que usuarios mal intencionados hagan un mal uso de este.

- Para la configuración del Ancho de banda de cada uno de los perfiles que se creen en el Cliente RADIUS, se debe considerar que la suma del ancho de banda asignado de todos los perfiles no debe superar el 100%, ya que de ser así la interfaz de administración cuenta con un mecanismo de control que impide crear nuevos perfiles si el ancho de banda de los ya creados sumado al ancho de banda del nuevo perfil supera el 100%.

- Es muy importante luego de la instalación del servidor de base de datos mysql configurar la contraseña para el usuario “root”; ya que luego del proceso de instalación el sistema asigna una clave por defecto a este usuario; lo que podría ocasionar un problema de seguridad; en el sentido en que algún usuario mal intencionado logre el acceso a este servidor y pueda alterar o eliminar la información contenida en el mismo.

BIBLIOGRAFÍA

1. Bauer, Kirk, Automating UNIX and Linux Administration, ISBN: 1590592123, Apress © 2003, 2003.
2. Biometric Recognition: Security and Privacy Concerns, 1540-7993/03/$17.00 © 2003 IEEE, IEEE SECURITY & PRIVACY.
3. Bistic, Ivan, Apache Security, O'Reilly, Marzo 2005, ISBN: 0-596-00724-8.
4. Certified Wireless Network Administrator Official Study Guide (Exam PW0-100), Planet 3, 3ª Edición, McGraw-Hill/Osborne, California 2005, ISBN 0-07-225538-2.
5. Dimitrios , Paraskevaídis, Traffic Policing Subsystem, Diciembre 2003
6. Haller N., Metz C., A One-Time Password System, RFC 1938, Mayo 1996.
7. Kent S., Atkinson, R., Security Architecture for the Internet Protocol, RFC 2401, Noviembre 1998.
8. Lloyd, B., Simpson W., PPP Authentication Protocols, RFC 1334, Octubre 1992.
9. Lucena López, Manuel José, Criptografía y Seguridad en Computadores, Tercera Edición (Versión 2.01). Marzo de 2003.
10. Mira Alfaro, Emilio José, RADIUS en Linux y Cisco, Agosto 2001.
11. Red Hat Linux Security Guide, 2003, Rad Hat. Inc.
12. Red Hat Reference Guide, 2003, Red Hat. Inc.
13. Rigney, C., RADIUS Accounting, RFC 2866, Junio 2000.
14. Rigney, C., Rubens, A., Simpson, W. y Willens, S., Remote Authentication Dial In User Service (RADIUS), RFC 2865, Junio 2000.
15. Simpson, W., PPP Challenge Handshake Authentication Protocol (CHAP), RFC 1994, Agosto 1996.
16. Simpson, W., The Point-to-Point Protocol (PPP), RFC 1661, Julio 1994
17. Stefan Raab, Madhavi W. Chandra, Kent Leung, Fred Baker , Mobile IP Technology and Applications, Publisher: Cisco Press, Mayo 2005, ISBN: 158705132X.
18. TANENBAUM, Andrew, Redes de Computadoras, 4ta. Edición, Ed. Pearson, México, 2003.

19. http://docs.fedoraproject.org, Página Web oficial de la documentación del Proyecto Fedora Core.
20. http://luxik.cdi.cz/~devik/qos/htb/manual/theory.htm, Hierachical token bucket theory.
21. http://www.3com.com, Página Web oficial de equipos 3COM.
22. http://www.criptored.upm.es/guiateoria/gt_m142j.htm, Consideraciones para implementar una arquitectura single sign-on.
23. http://www.freeradius.org, Página Web oficial de freeRADIUS.
24. http://www.iea-software.com, Página Web oficial del Software AirMarshal.
25. http://www.patronsoft.com/firstspot, Página Web oficial del Software FistSpot.
26. http://www.php.net/manual/es/index.php, Pagina Web oficial del Manual de PHP.
27. http://www.pnl.gov/webmailhelp/secureid.htm, SecurID Token (Smartcard)

ABREVIATURAS

3DES	*Triple Data Encryption Standard*
AAA	*Authentication, authorization, and accounting*
AC	Autoridad Certificadora
AES	*Advanced Encryption Standard*
AH	*Authentication Header*
AH	*Authentication Header*
CBQ	*Class Based Queueing*
CGI	*Common Gateway Interface*
CHAP	Protocolo de Autentificación por Reto
DES	*Data Encryption Standard*
EAP	*Extensible Authentication Protocol*
EAPOL	*EAP Encapsulation Over LAN*
ESP	*Encapsulation Security Payload*
ESP	*Encapsulating Secure Payload*
FAQ	*Frequently Asked Questions*
FIFO	*First In, First Out*
GPL	*General Public License*
HTB	*Hierarchical Token Bucket*
HTTP	*Hyper Text Transfer Protocol*
IETF	*Internet Engineering Task Force*
IKE	*Internet Key Exchange*
IOS	*Internetworking Operative System*
ISAKMP	*Internet Security Association and Key Management Protocol*
ISP	*Internet Service Provider*
ITU-T	*International Telecommunication Union-Telecommunication Standarization Sector*
LAN	*Local Area network*
LEAP	*Lightweight EAP*
NAS	*Network Access Servers*
NAT	*Network Address Translation*
ODBC	*Open Data Base Connexion*
OTP	*One Time Passwords*
PAM	*Pluggable Authentication Modules*
PAP	Protocolo de Autentificación por Contraseña
PEAP	*Protected EAP*
PHP	*Hypertext Preprocessor*
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
PoE	*Power over Ethernet*
PPP	*Point to Point Protocol*
RSA	*Ramis Shamir y ALdeman*
RFC	*Request For Comment*
RFID	*Radio Frequency Identification*
SA	*Security Association*

SFQ	*Stochastic Fairness Queueing*
SIM	*Subscriber Identity Module*
SP	*Security Policy*
SQL	*Structured Query Language*
SSID	*Service Set Identifier*
SSO	*Single Sign-On*
TBF	*Token Bucket Filter*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TKI	*Temporal Key Integrity Protocol*
TOS	*Type Of Service*
TTL	*Time To Live*
VAF	Verificación automática de firmas
VNC	*Virtual Network Computing*
VPN	*Virtual Private Network*
VSA	*Vendor Specific Attributes*
WEP	*Wireless Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WPA	*Wi-Fi Protected Access*
WPA-PSK	*WPA Pre-Shared Key*