Gestión de portales cautivos con daloRADIUS en Debian

Tesis profesional

(Opción I)

Que para obtener el título de:

Ingeniero en Sistemas Computacionales

Presentan:

Juan Alberto Monzón García

Roberto Salvador Vazquez Hermitaño

Asesor de la tesis:

Ing. Milton José Martil Cruz

Tapachula, Chiapas, Septiembre de 2014

Dedicatoria

Juan Alberto Monzón García

Roberto Salvador Vazquez Hermitaño

Agradecimientos

Juan Alberto Monzón García

Roberto Salvador Vazquez Hermitaño

Resumen

La finalidad de esta tesis es la gestión de portales cautivos en una red inalámbrica, para lo cual se hace uso de la aplicación daloRADIUS, con esto se puede llevar un control adecuado de los usuarios existentes en un portal cautivo, ya sea chillispot, coovachilli, y otros más.

Destacando los parámetros de evaluación como: Facilidad de instalación, facilidad de configuración, seguridad, funcionalidad e Interfaz amigable para el Administrador. El desarrollo de la aplicación se realizó sobre una distribución LINUX, debido a la estabilidad, además se ocupó FREERADIUS que garantiza la conexión para la autenticación, interoperabilidad y sobre todo seguridad.

Contenido

Índice de figuras

Índice de tablas

Introducción

Con la aparición de internet se solucionaron muchos problemas de comunicación a nivel mundial, las redes se expandieron brindando a las instituciones varias opciones para compartir y obtener información, una de estas opciones son las redes locales Wireless (WLAN).

El uso de WLAN ha crecido exponencialmente es por eso que las instituciones buscan formas de hacer más eficientes sus redes actuales, tanto en aspectos de seguridad como con el aprovechamiento de los recursos disponibles. 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 acceso a usuarios o autenticación.

En la elaboración del proyecto con el nombre: “Gestión de portales cautivos con daloRADIUS en Debian” se dan a conocer la importancia que tienen un portal cautivo, pero aún más importante la gestión de usuarios, informes gráficos, entre otras opciones dentro de la red por medio de una aplicación web llamada daloRADIUS.

DaloRADIUS, es una aplicación avanzada de gestión de un servicio RADIUS; web destinadas a la gestión de puntos de acceso y las implementaciones de proveedor de internet para fines generales. Es una interfaz web administrativa que permite configurar y administrar un servidor FreeRADIUS. Un portal cautivo (o captivo) es un programa o máquina de una red informática que vigila el tráfico http y https en los puertos TCP 80 y 443 para dirigir a un servidor web que obliga a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.

La aplicación intercepta todo el tráfico HTTP y/o HTTPS hasta que el usuario se autentica.

En un portal Cautivo el usuario tiene que introducir sus credenciales (usuario y contraseña o certificado electrónico) en su navegador para ser autorizados a utilizar la red. La estructura de este documento se encuentra conformada por cinco capítulos los cuales se detallan a continuación.

Capítulo I Marco referencial: En este capítulo se hace una descripción de las razones fundamentales para efectuar el estudio de la gestión de portales cautivos y los objetivos que se alcanzaran.

Capítulo II Fundamento teórico: En este capítulo se da una referencia teórica sobre daloRADIUS, redes inalámbricas, sus componentes, funcionamiento, amenazas contra seguridad y métodos de protección, en este capítulo también se presenta información en general de portales cautivos como su funcionamiento, tipos y componentes. También se describe la metodología utilizada así como la técnica utilizada para recopilar información y el vaciado e interpretación del mismo.

Capítulo III Metodología: En este capítulo se detallara la metodología que se propone para el desarrollo del proyecto y también la implementación de esta. Algunos otros aspectos que se abordan son: el tipo de investigación que se realizara y la técnica utilizada para la recopilación de información, así como, la interpretación de la información recolectada.

Capítulo IV: Conclusiones y recomendaciones: En este último capítulo se mencionan las conclusiones que ha dejado el proyecto para dar claridad a los conceptos desarrollados y servir de base a futuros desarrollos de la misma área, también se dan algunas recomendaciones sobre la gestión de portales cautivos.

Capítulo I Marco referencial del proyecto

1.1 Planteamiento del problema
1.2 Antecedentes
1.3 Justificación
1.4 Objetivos
1.4.1 Objetivo general
1.4.2 Objetivos específicos
1.5 Metas
1.6 Formulación de hipótesis
1.7 Programa de actividades, calendarización
1.8 Lugar donde se va desarrollar

1.1 Planteamiento del problema

Un portal cautivo necesita ser gestionado para tener el control de los usuarios que se tienen y poder generar informes gráficos por lo que se requiere de una aplicación para generar dichos informes.

1.2 Antecedentes

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

Cuando un usuario potencial se autentica por primera vez ante una red con un portal cautivo, se presenta una página Web en la cual se requieren ciertas acciones antes de proceder con el acceso.

Un portal cautivo sencillo obliga al visitante a que por lo menos mire (así no lea) y acepte las políticas de uso, pulsando un botón en la página. Supuestamente esto puede absolver al proveedor del servicio de cualquier culpa por el uso anormal y/o ilegal del servicio.

En otros portales se provee publicidad para el proveedor y/o sus patrocinadores y el usuario deberá hacer clic en la publicidad o cerrar la ventana en las cuales aparecen estos comerciales antes de continuar con el uso del servicio. En algunos casos se debe ingresar una identificación y/o clave asignada antes de acceder a Internet, con el objetivo de desalentar a quienes quieran usar estos servicios para usos no autorizados.

1.3 Justificación

Un portal cautivo es un conjunto de páginas web que emergen en cualquier petición que hagan los clientes, para identificar y tener el control sobre los usuarios.

Este proyecto surge por la necesidad de brindar seguridad y gestionar el acceso indebido a una red inalámbrica utilizando un portal cautivo.

Con la implementación de daloRADIUS podremos generar informes gráficos, además de estadísticas de un portal cautivo que utilice la autenticación de usuarios con FreeRADIUS. Esta aplicación además de generar informes también nos permite gestionar los usuarios que tenemos creados, es decir podemos crear, modificar o eliminar usuarios, también se puede tener control de los puntos de acceso que se tengan registrados.

1.4 Objetivos

1.4.1 Objetivo general

El objetivo principal es gestionar portales cautivos utilizando una solución libre, la cual nos va servir para realizar la administración de usuarios y generar informes del uso de los datos en la red. Estos datos servirán para realizar un análisis de toda la información que fluye en la red inalámbrica.

1.4.2 Objetivos específicos

- Implementación de un servidor RADIUS para la gestión de una red inalámbrica mediante servicio de autenticación
- Análisis de los datos que usa la red inalámbrica para generar históricos estadísticos
- Manejo de una Base de Datos para la creación de credenciales de usuarios

- Generar estadísticas y gráficos de los aspectos más relevantes para una mejor interpretación de los datos

1.5 Metas

- Administración de usuarios existentes en nuestra red (creación y eliminación de usuarios)
- Gestión de las actividades que realizan los usuarios en nuestra red (páginas visitadas, fecha y hora de las conexiones realizadas, número de veces que se conecta un usuario en un periodo determinado)
- Generación de gráficas de aspectos o datos que sirvan para llevar un control de usuarios u otras características

1.6 Formulación de hipótesis

La hipótesis nos indica lo que estamos buscando o tratando de probar y pueden definirse como explicaciones tentativas del fenómeno investigado, formuladas a manera de proposiciones. En una investigación podemos tener una, dos o más hipótesis, y hay ocasiones en las que no se tiene hipótesis.

Hipótesis:
"Llevar un control de una red inalámbrica nos proporciona información detallada en la toma de decisiones para brindar un mejor servicio".

1.7 Lugar donde se va desarrollar

El presente proyecto de tesis se desarrolla en el Laboratorio de Software Libre (LABSOL), ubicado en el Consejo Zacatecano de Ciencia, Tecnología e Innovación (COZCyT) en la ciudad de Zacatecas, Zacatecas México.

Capítulo II:

Fundamento Teórico

2.1 Redes Inalámbricas

2.1.1 Definición

2.1.2 Tecnologías actuales

2.2 Seguridad en redes inalámbricas

2.2.1 Métodos para garantizar seguridad en redes inalámbricas

2.2.2 Filtrado de direcciones MAC

2.2.3 WEP (Wired Equivalent Privacy)

2.3 Sistema Operativo Linux

2.3.1Caracteristicas principales

2.3.2Distriibucion Debian

2.4 Servidor HTTP

2.4.1 Servidor HTTP Apache

2.5 Protocolo AAA

2.5.1 Definición de las siglas AAA

2.5.2 Listado de protocolos AAA

2.6 NAS

2.6.1 Uso

2.7 Servidores RADIUS

2.7.1 Tipos de servidores RADIUS

2.7.2 Servidores de licencia libre

2.7.3 Servidores de tipo comerciales

2.8 Portal Cautivo

2.8.1 ¿Qué es un portal cautivo?

2.8.2 Tipos de portales cautivos

2.9 daloRADIUS

2.1 Redes Inalámbricas

2.1.1 Definición

Cuando hablamos de redes inalámbricas, nos referimos a una interconexión de dispositivos con la capacidad de compartir información entre ellos, pero sin un medio físico de transmisión. Estos dispositivos pueden ser de muy variadas formas y tecnologías[1], en la **figura 2.1** se muestran algunos de ellos:

- Computadoras de escritorio
- Teléfonos celulares
- Asistentes digitales personales (PDA)
- Access point, encargado de permitir a los dispositivos inalámbricos el acceso a la red
- Computadoras portátiles: laptop, netbook, notebook

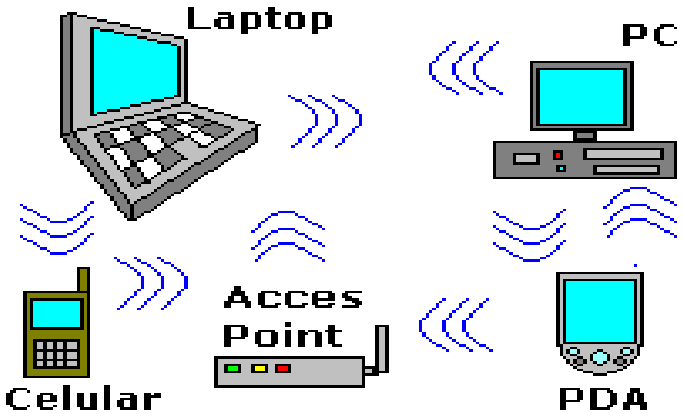


Figura 2.1 Interconexión Inalámbrica
(Fuente: http://www.informaticamoderna.com/Redes_inalam.htm)

[1] (moderna, 2014)

2.1.2 Tecnologías actuales

Las tecnologías más comunes en la actualidad para interconexión inalámbrica son:

a) Wi-Fi (Wireless Fidelity): En lenguaje español significa literalmente fidelidad sin cables. También se les denomina WLAN (Wireless Local Area Network) o redes de área local inalámbricas. Se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio con muy buena calidad de emisión para distancias cortas (hasta teóricamente 100 metros).

Este tipo de transmisión se encuentra estandarizado por la IEEE, siglas en ingles del Instituto de Ingenieros en Electricidad y Electrónica, la cal es una organización internacional que define las reglas de operación de ciertas tecnologías.

Para la transmisión es necesario el uso de antenas integradas en las tarjetas, además este tipo de ondas son capaces de traspasar obstáculos sin necesidad de estar frente a frente el emisor y el receptor.

El estándar IEEE 802.11x es un estándar internacional que define las características de una red de área local inalámbrica (WLAN), el cual se enfoca directamente con la capa física y enlace de datos del modelo OSI para todas las conexiones inalámbricas que utilizan ondas electromagnéticas. Al estándar IEEE 802.11x también se lo define como el Conjunto Básico de Servicio (BSS) que consiste en dos o más nodos inalámbricos o estaciones que se conocen una a la otra y pueden transmitir información entre ellos[2].

El estándar 802.11x ha venido presentando modificaciones con el transcurso del tiempo para cada vez optimizar más el ancho de banda. Los estándares IEEE 802.11b, IEEE 802.11g e IEEE 802.11n disfrutan de una aceptación internacional debido a que trabajan en la banda de 2.4 GHz que está disponible casi universalmente, alcanzando

[2] (Wikipedia, Estandar IEEE 802.11x, 2014)

velocidades de hasta 11 Mbit/s, 54 Mbit/s y 300 Mbit/s, respectivamente, en la **figura 2.2** se muestra la representación de tipos de estándares.

Figura 2.2 Tipo de estándares
(Fuente: http://es.wikipedia.org/wiki/IEEE_802.11)

A continuación se muestra la comparación de los estándares básicos en la ***tabla 2.1***.

Estándar.	*Año de Lanzamiento.*	*Frecuencia.*	*Tasa de Velocidad.*	*Técnica de Modulación.*
802.11b	*1999*	*2 GHz*	*11 Mbps*	*DSSS*
802.11a	*1999*	*5 GHz*	*54 Mbps*	*OFDM*
802.11g	*2003*	*2.4 GHz*	*54 Mbps*	*OFDM*
802.11n	*2007*	*2.4 GHz*	*500 Mbps*	*SDM/OFDM*

Tabla 2.1: Comparación de los estándares básicos
(Fuente: http://es.wikipedia.org/wiki/IEEE_802.11)

Para el uso de redes "Wireless" es necesario que los dispositivos dispongan de un emisor ya sea integrado o agregado para el uso de este tipo de red[3].

- **Computadoras de escritorio:** un emisor/receptor integrado en la Motherboard, una tarjeta PCI inalámbrica o un adaptador USB para red inalámbrica
- **Computadoras portátiles:** en caso de no tenerlo integrado se puede usar una tarjeta PCMCIA para red inalámbrica o un adaptador USB para red inalámbrica
- **PDA:** tiene integrada la tarjeta de red inalámbrica
- **Celular:** En la actualidad la todos los teléfonos muy especializados tienen la tarjeta de red inalámbrica integrada

[3] (Gutierrez, 2014)

b) Infrarrojo (Ir): Se trata de una tecnología de transmisión inalámbrica por medio de ondas de calor a corta distancia (hasta 1 m), capaces de traspasar cristales.

Tiene una velocidad promedio de transmisión de datos hasta de 115 Kbps (Kilobits por segundo), no utiliza ningún tipo de antena, sino un diodo emisor semejante al de los controles remoto para televisión. Funciona solamente en línea recta, debiendo tener acceso frontal el emisor y el receptor ya que no es capaz de traspasar obstáculos opacos.

Para el uso de redes infrarrojas es necesario que los dispositivos dispongan de un emisor ya sea integrado o agregado para el uso de este tipo de red.[4]

- **Computadoras de escritorio:** un adaptador infrarrojo USB o en su caso un puerto integrado al gabinete
- **Computadoras portátiles:** un adaptador infrarrojo USB
- **PDA:** tiene integrado el puerto infrarrojo
- **Celular:** algunos teléfonos tienen integrado el puerto infrarrojo

c) Bluetooth: En lenguaje español significa literalmente diente azul, ello por ser un nombre de un Rey de la antigüedad. Se trata de una tecnología de transmisión inalámbrica por medio de ondas de radio de corto alcance (1, 20 y 100 m a la redonda dependiendo la versión). Las ondas pueden incluso ser capaces de cruzar cierto tipo de materiales, incluyendo muros.

Para la transmisión de datos no es necesario el uso de antenas externas visibles, sino que pueden estar integradas dentro del mismo dispositivo. Este tipo de transmisión se encuentra estandarizado de manera independiente y permite una velocidad de transmisión de hasta 1 Mbps.

[4] (Gutierrez, 2014)

Para el uso de redes Bluetooth es necesario que los dispositivos dispongan de un emisor integrado o agregado para el uso de este tipo de red.

- **Computadoras de escritorio:** un adaptador Bluetooth USB
- **Computadoras portátiles:** un adaptador Bluetooth USB
- **PDA:** tiene integrado el emisor Bluetooth
- **Celular:** tiene integrado el emisor Bluetooth

d) Microondas: Se trata de comunicaciones a gran escala, muy caras y con poco uso doméstico. Las hay de dos tipos:

- **Satelitales:** se realizan a través de bases terrestres con antenas que envían señales al satélite, este se encarga de direccionarlas hacia la estación receptora con la onda amplificada para evitar pérdidas
- **Terrestres:** se basan en conexiones denominadas punto a punto, ya que sus antenas deben estar sin obstáculos físicos para evitar fallas en la transmisión

e) Láser: Son tecnologías de muy alta velocidad, basadas en el envío de datos en grandes regiones por medio de un haz de luz láser emitida por un diodo especial (hasta 5 Km. de distancia) y un foto-diodo que reciba las señales. Tiene la desventaja de que es necesaria una conexión punto a punto, esto es que el emisor y el receptor no cuenten con ningún tipo de obstáculo entre sí.

2.2 Seguridad en redes inalámbricas

Una de las razones por las cuales las redes inalámbricas son tan populares es el acceso sin necesidad de usar cables de red, esto a la vez es el problema más grande en cuanto a seguridad se refiere. Cualquier equipo o dispositivo que se a 100metros o menos de un punto de acceso, podría tener acceso a la red.[5]

[5] (Seguridad en redes, 2014)

En la **tabla 2.2** se muestran unas de las amenazas de seguridad más relevantes que existen en las redes inalámbricas.

Confidencialidad	• Riesgo de interferencia, usuarios no autorizados pueden obtener acceso al tráfico de datos en su red • Riesgo de arrebato de tráfico y riesgo de un ataque o tipo de intermediario
Integridad	- Riesgo de alteración de tráfico en la red.
Disponibilidad	• Riesgo de interferencia, negación de servicio (cuestionamiento) • Riesgo de no disponibilidad de ancho de banda debido a retransmisiones de radio • Riesgo de no disponibilidad de ancho de banda debido a software malicioso
Autenticación	• Riesgo de acceso no autorizado a su intranet • Riesgo de uso no autorizado

Tabla 2.2 Amenazas de seguridad más relevantes en redes inalámbricas
(Fuente: http://www.redusers.com/noticias/seguridad-en-redes-autenticacion-con-servidores-aaa/)

2.2.1 Métodos para garantizar Seguridad en redes inalámbricas

Para que una red se pueda considerar como segura, debe cumplir con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr en su totalidad, pero se pueden obtener buenos resultados empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso
- Debe existir un mecanismo de autenticación de doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva[6]

[6] (Seguridad en redes, 2014)

Existen varios métodos para lograr la configuración segura de una red inalámbrica, a continuación se mencionan algunos de ellos.

2.2.2 Filtrado de direcciones MAC

El filtrado de direcciones MAC tiene como finalidad proteger la red inalámbrica e impedir el acceso de dispositivos inalámbricos no autorizados.

Cuando se activa el filtrado de direcciones MAC, solo pueden asociarse a la puerta de enlace y transferir datos a través de una conexión inalámbrica las tarjetas de PC y los puntos de acceso cuyas direcciones MAC correspondan con las que el usuario haya programado en la puerta de enlace.[7]

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

2.2.3 WEP (Wired Equivalent Privacy)

WEP fue el primer protocolo de encriptación introducido en el primer estándar IEEE 802.11 en 1999. Está basado en el algoritmo de encriptación RC4 con una clave secreta de 40 o 104 bits, combinada con un vector de inicialización (IV) de 24 bits para encriptar el mensaje de texto.[8]

El protocolo WEP no fue creado por expertos en seguridad o criptografía, así que pronto se demostró que era vulnerable ante los problemas RC4 descritos por David

[7] (Robotic, 2014)
[8] (Seguridad WEP, 2014)

Wagner cuatro años antes. Desde entonces se ha aceptado que WEP proporciona un nivel de seguridad aceptable solo para usuarios domésticos y aplicaciones no críticas.[9]

2.3 Sistema Operativo Linux

Linux es un sistema operativo con un núcleo basado en Unix. Es uno de los principales ejemplos de software libre, está licenciado bajo la GPLv2 y está desarrollado por colaboradores de todo el mundo.

El núcleo de Linux fue concebido por el entonces estudiante de ciencias de la computación finlandés, Linus Torvalds, en 1991. Pero Torvalds decidió aprovechar el sistema GNU y completarlo con su propio núcleo, que bautizó como Linux (Linux IsNotUniX). El sistema conjunto (herramientas GNU y núcleo Linux) forma lo que llamamos GNU/Linux, y consiguió rápidamente que desarrolladores y usuarios adoptaran códigos de otros proyectos de software libre para su uso en nuevas distribuciones.[10]

El núcleo Linux ha recibido contribuciones de miles de programadores de todo el mundo. Normalmente Linux se utiliza junto a un empaquetado de software, llamado distribución Linux y servidores. Su código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL (General Public License).

2.3.1 Características principales

- **Sistema Multitarea.** Describe la habilidad de ejecutar, aparentemente al mismo tiempo, numerosos programas sin obstaculizar la ejecución de cada aplicación. Esto se conoce como multitarea preferente, porque cada programa tiene garantizada la posibilidad de correr

[9] (Schauer, 2014)
[10] (Wikipedia, sistema operativo Linux, 2014)

- **Sistema Multiusuario.** El concepto de que numerosos usuarios pudieran accesar aplicaciones o el potencial de procesamiento en una sola PC era un mero sueño hace unos cuantos años. Linux permite que más de una sola persona pueda trabajar en la misma versión de la misma aplicación de manera simultánea, desde las mismas terminales, o en terminales separadas (elinux.com.mx)
- **Programación.** Linux cuenta con un conjunto poderoso de herramientas para el desarrollo de programas: C, C++, ObjectiveC, Pascal, Fortran, BASIC, CLISP, SmallTalk, Ada, Perl, así como depuradores y bibliotecas compartidas de enlace dinámico (DLL)
- **Estabilidad.** Linux se ha distinguido por su estabilidad de operación, se han conocido y comentado muchos casos de equipo trabajando por más de un año sin tener que apagar o reiniciarlo
- **Velocidad.** Los equipos Linux también se han distinguido por su extraordinaria velocidad. El sistema operativo administra eficientemente los recursos como memoria, poder de CPU y espacio en disco
- **Portabilidad.** Una de las características más importantes de Linux es su portabilidad. En la actualidad es usado en las plataformas Intel x86, PowerPC, Macintosh, Amiga, Atari, DEC Alpha, Sun Sparc, ARM y otras más[11]

2.3.2 Distribución Debian

Debian GNU/Linux es un sistema operativo libre, desarrollado por más de mil voluntarios alrededor del mundo, que colaboran a través de Internet. La dedicación de Debian al software libre, su base de voluntarios, su naturaleza no comercial y su modelo de desarrollo abierto la distingue de otras distribuciones del sistema operativo GNU. Todos estos aspectos y más se recogen en el llamado Contrato Social de Debian.

[11] (Wikipedia, sistema operativo Linux, 2014)

Nació en el año 1993, de la mano del proyecto Debian, con la idea de crear un sistema GNU usando Linux como núcleo ya que el proyecto Debian, organización responsable de su mantenimiento en la actualidad, también desarrolla sistemas GNU basados en otros núcleos (Debian GNU/Hurd, Debian GNU/NetBSD y Debian GNU/kFreeBSD).

Uno de sus principales objetivos es separar en sus versiones el software libre del software no libre. El modelo de desarrollo es independiente a empresas, creado por los propios usuarios, sin depender de ninguna manera de necesidades comerciales.

Debian no vende directamente su software, lo pone a disposición de cualquiera en Internet, aunque sí permite a personas o empresas distribuir comercialmente este software mientras se respete su licencia.[12]

Debian Linux puede instalarse utilizando distintos mecanismos de instalación, como DVD, CD, Blu-Ray, memorias USB y diskettes, e incluso directamente desde la red.

Características

La disponibilidad en varias arquitecturas. La versión estable incluye soporte para 12 plataformas:

- i386 – x86-32
- amd64 – x86-64
- alpha – DEC Alpha
- sparc – Sun SPARC
- arm – Arquitectura ARM
- armel – Emulador de ARM Emulator
- powerpc – Arquitectura PowerPC
- ia64 – Arquitectura Intel Itanium (IA-64)

[12] (debian, 2014)

- mips, mipsel – Arquitectura MIPS (big-endian y little-endian)
- s390 – Arquitectura IBM ESA/390 y z/Architecture
- m68k – Arquitectura Motorola 68k en Amiga, Atari, Mac, y varios sistemas embebidos VME

Una amplia colección de software disponible. La versión 5.0 viene con más de 23.000 paquetes y la versión 6.0 con casi 30.000.2.

Un grupo de herramientas para facilitar el proceso de instalación y actualización del software (APT, Aptitude, Dpkg, Synaptic, Dselect, etc.) Todas ellas obtienen información de donde descargar software desde /etc/apt/sources.list, que contiene los repositorios.

Su compromiso con los principios y valores involucrados en el movimiento del Software Libre. No tiene marcado ningún entorno gráfico en especial, pudiéndose no instalar ninguno, o instalar GNOME, KDE, Xfce, LXDE, Enlightenment u otro.[13]

Requisitos mínimos para la instalación de Debian 6.

Los requisitos mínimos que nos recomiendan en la propia web de Debian, son los siguientes:

Instalación sin escritorio

- Procesador: Pentium 4 a 1Ghz
- Memoria RAM 64MB
- Disco duro: 1GB

[13] (debian, 2014)

Instalación con escritorio

- Procesador: Pentium 4 a 1Ghz
- Memoria RAM: 128MB
- Disco duro: 5GB[14]

Debian como servidor

Según las estadísticas publicadas por W3techs, Debian no solo mantiene la corona de distribución Linux más utilizada en el ámbito de los servidores desde 2012, sino que su cuota de mercado ha crecido considerablemente, posicionándola a la cabeza del pelotón con bastante holgura.

El auge del sistema operativo universal ha sido contundente, pues a principios de 2012 recuperaba el terreno perdido frente a CentOS, pero todavía se disputaban ambas la cúspide de la gráfica. Ahora, la situación es muy distinta.[15]

Por primera vez, Ubuntu supera a CentOS en servidores, lo que deja a la distribución de Canonical en un segundo puesto y otorga al binomio Debian / Ubuntu un 58,5% del pastel, que se reduce al 37,3% en el caso de CentOS / Red Hat, en tercer y cuarto lugar respectivamente.

[14] (Rodriguez, 2014)
[15] (Muy linux, 2014)

Como se puede observar en la **figura 2.3**, la tendencia, además, es realmente favorable para Ubuntu.

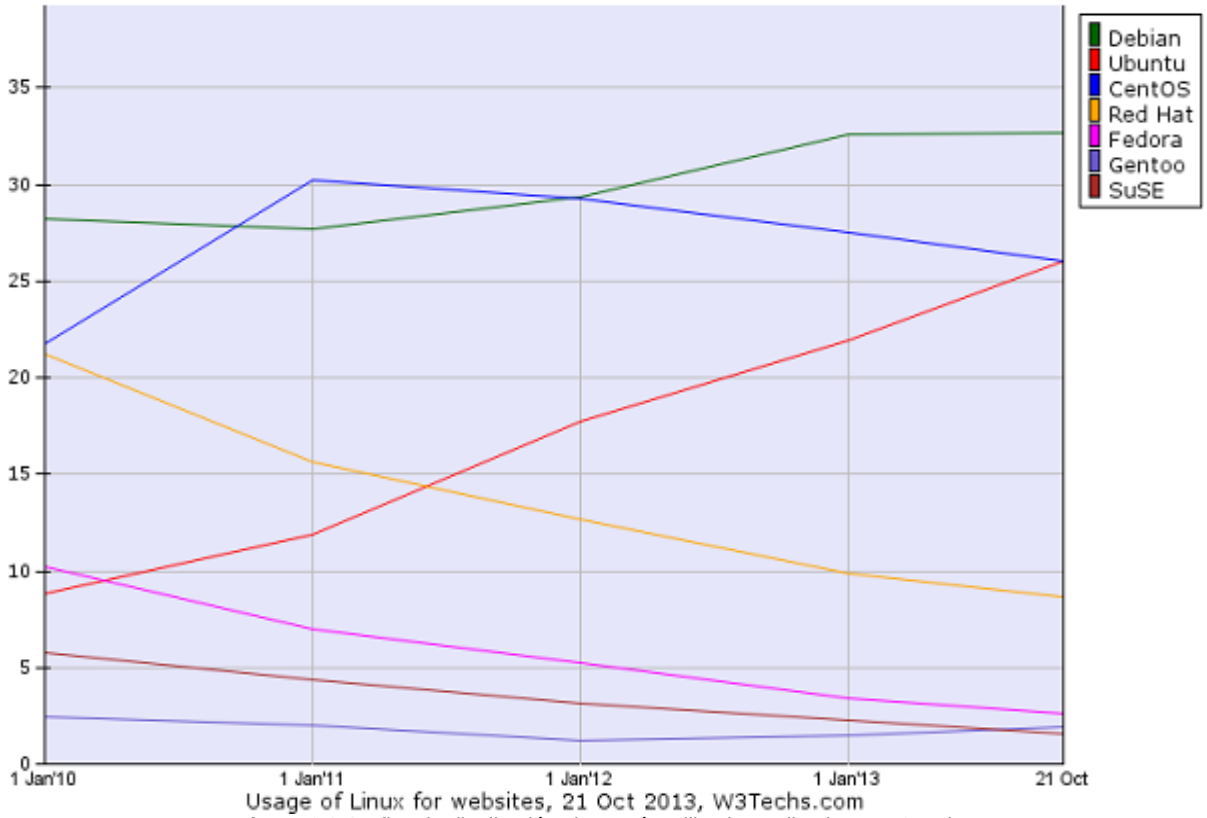


Figura 2.3 Grafica de distribución Linux más utilizada, realizado por w3Techs
(Fuente: http://www.muylinux.com/2013/10/25/debian-sigue-numero-uno-en-servidores)

2.4 Servidor HTTP

Un servidor HTTP es un programa informático que procesa una aplicación del lado del servidor realizando conexiones bidireccionales y unidireccionales y síncronas o asíncronas con el cliente generando una respuesta en cualquier lenguaje o aplicación del lado del cliente.

En la **figura 2.4** se observa el funcionamiento de un servidor http. El código recibido por el cliente suele ser compilado y ejecutado por un navegador web.

Figura 2.4 Función de un servidor HTTP
(Fuente: http://www.edu4java.com/es/web/web30.html)

Los servidores HTTP pueden disponer de intérpretes de otros lenguajes de programación que ejecutan código embebido dentro del código HTML de las páginas que contiene el sitio antes de enviar el resultado al cliente. Esto se conoce como programación de lado del servidor y utiliza lenguajes como ASP, PHP, Perl y Ajax.[16]

2.4.1 Servidor HTTP Apache.

El servidor HTTP Apache es un servidor web HTTP de código abierto, para plataformas Unix, BSD, GNU/Linux, Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3. El servidor Apache nace dentro del proyecto HTTP Server (httpd) desarrollado por la Apache Software Foundation, y está diseñado para ser un servidor web potente y flexible que puede funcionar en la más amplia variedad de plataformas y entornos.

[16] (Servidor HTTP, 2014)

Las diferentes plataformas y los diferentes entornos, hacen que a menudo sean necesarias diferentes características o funcionalidades, o que una misma característica o funcionalidad sea implementada de diferente manera para obtener una mayor eficiencia.[17]

2.4.1.1 Principales características de Apache

Entre las principales características de apache tenemos:

- **Sistema de Código Abierto.** Apache es una tecnología gratuita de código fuente abierto, esto le da una transparencia a este software de manera que si queremos ver qué es lo que estamos instalando como servidor, podemos saber, sin ningún secreto, sin ninguna puerta trasera
- **Multiplataforma.** Apache es multiplataforma, capaz de correr sobre una gran diversidad de plataformas y Sistemas Operativos.
- **Diseño Modular.** Es un servidor altamente configurable de diseño modular. Es muy sencillo ampliar las capacidades del servidor Web Apache. Actualmente existen muchos módulos para Apache que son adaptables a este, y están ahí para que los instalemos cuando los necesitemos
- **Compatibilidad con Lenguajes de Programación.** Trabaja perfectamente con lenguajes como Java, Perl, PHP y otros lenguajes de script. Pero Perl destaca en el mundo del script ya que apache utiliza con soporte CGI al mod_perl
- **Soporte Avanzado de Programas CGI (COMMON GATEWAY INTERFACE).** Ofrece características avanzadas, como variables de entorno personalizadas y soporte para depuración de dichos programas. (ocw.uniovi.es, 2010) Mejorando funcionamiento bajo threads. Esto se lo realiza a través de los módulos mod_cgi y mod_cgid
- **Soporte de FASTCGI.** Con el módulo mod_fcgi se puede crear un entorno FastCGI dentro de Apache y aumentar el rendimiento de estas aplicaciones.

[17] (Servidor web Apache, 2014)

- **Soporte para Autenticación HTTP.** Mediante módulos adicionales pueden implementarse autenticaciones que empleen bases de datos, ficheros, sentencias SQL o llamadas a programas externos sobre un mismo servido
- **Servidor Proxy Integrado.** Apache se puede convertir en un caching (forward) proxy server
    - Un forward proxy es un servidor intermedio que se sitúa entre el cliente y el servidor que tiene los contenidos al que llamaremos O
    - Para obtener los contenidos de O, el cliente envía una petición al forward proxy, especificando O como el origen del contenido que busca
    - El forward proxy entonces pide el contenido a O y lo devuelve al cliente
    - El cliente debe estar especialmente configurado para soportar esto, ya que tiene que conectarse a través de dicho proxy en lugar de usando otros medios[18]

2.4.1.2 Ventajas y Desventajas de Apache

Ventajas:

- **Código Libre.** Apache es un software de código abierto, esto significa que la programación que impulsa el software puede ser consultada y editada por cualquiera persona. Este diseño permite a cualquier programador crear una solución personalizada basada en el programa núcleo de Apache, o ampliar las funciones del software. La mayoría de programadores contribuyen constantemente con mejoras, que están disponibles para cualquier persona que use el servidor web apache[19]
- **Costo.** Otra ventaja que destacamos en apache es su costo, el servidor Web Apache es completamente gratuito y puede ser descargado por cualquier persona en el mundo que desee implementarlo. Al utilizar el código abierto Apache Web Server crea un ahorro sustancial, lo que es particularmente valioso

[18] (Servidor web Apache, 2014)
[19] (Pro y contra de Apache, 2014)

para las pequeñas empresas y medianas empresa que se encuentran lanzando nuevos programas de tecnología, y no tienen grandes presupuestos para el servidor web

- **Funcionalidades.** Apache Web Server tiene un gran conjunto de funcionalidades de gran alcance, las mismas junto con las extensiones ayudan a que la plataforma Apache sea competitiva incluso frente a rivales de alto precio

  Apache ha incorporado en su soporte una gama amplia de lenguajes de programación web, como Perl, PHP y Python. Estos lenguajes son fáciles de aprender y se pueden utilizar para crear potentes aplicaciones en línea. También incluye soporte "SSL" y "TLS", que son los protocolos para enviar datos encriptados a través de Internet, los mismos que son muy importantes en el desarrollo de aplicaciones seguras en línea
- **Soporte.** Apache Web Server cuenta con una gran comunidad de usuarios de soporte, a diferencia de muchos software el soporte técnico de Apache se extiende a lo largo de múltiples localizaciones, empresas, y foros. Esta modalidad de dar soporte permite a los usuarios obtener respuestas a preguntas técnicas casi las 24 horas al día, no importa dónde se encuentren. Al ser de código abierto, Apache está conectado a muchos usuarios que son capaces de crear parches y correcciones de errores técnicos muy rápidamente. Cuando se detecta un error o problema todos usuarios en todo el mundo comunican y aportan las soluciones posibles, dando como resultado que Apache posea un soporte muy estable y bien mantenido
- **Portabilidad.** Apache Web Server es muy portable y puede ser instalado en una amplia gama de servidores y sistemas operativos, es capaz de ejecutarse en todas las versiones del sistema operativo UNIX. Linux es compatible, así como los sistemas operativos Windows NT y MacOS

- **Apache** puede ser utilizado en cualquier servidor con procesadores de serie Intel 80x86 cuando se combina con Windows, y cuando se usa un sistema operativo Unix o Linux, casi cualquier tipo de procesador es compatible[20]

Desventajas:

- **Complejidad.** En Apache Web Server algunas veces resulta muy complejo de configurar algunas herramientas, incluso hasta para los mismos programadores que trabajan a diario con apache
- **Formatos no Estándar.** La falta de formatos no estándar dificulta un poco la automatización, y el procesamiento de la configuración al no estar basada está en formatos más soportados como el XML
- **Falta de Integración.** Apache al ser un producto multiplataforma, no aprovecha al máximo las posibilidades que le ofrece el sistema operativo sobre el que se encuentra funcionando
- **Administración.** Apache Web Server no posee una herramienta de administración, por lo que es necesario instalar herramientas adicionales para facilitar todas las tareas de administración del servidor[21]

2.5 Protocolo AAA

En seguridad informática, el protocolo AAA realiza tres funciones importantes: Autenticación, Autorización y Contabilidad (Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados anteriormente.

Adicionalmente el servicio AAA debe ser capaz de autenticar a los usuarios, dar una respuesta correcta a las solicitudes de autorización de los mismos así como de

[20] (Pro y contra de Apache, 2014)
[21] (Pro y contra de Apache, 2014)

recolectar datos que permitan una auditoría total sobre los recursos a los que se ha tenido acceso.[22]

2.5.1 Definición de las siglas AAA

2.5.1.1 Autenticación (AUTHENTICATION)

Es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente usuario, ordenador, etc.; y la segunda un servidor. La autenticación se consigue mediante la presentación de una identidad (Un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla.

Ejemplos de las Credenciales:

Las contraseñas, los Certificados Digitales, o los números de teléfono en la identificación de llamadas.
Es importante mencionar que los protocolos de autenticación digital modernos permiten la posesión de las credenciales requeridas sin necesidad de transmitirlas por la red.

2.5.1.2 Autorización (AUTHORIZATION)

Se refiere a la concesión de privilegios específicos a una entidad o usuario basándose en su identidad autenticada, los privilegios que solicita, y el estado actual del sistema.

Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio.

[22] (wikipedia, Protocolo AAA, 2014)

Ejemplos de Tipos de Servicio:

Filtrado de Direcciones IP, Asignación de Direcciones, Asignación de Rutas, Asignación de Parámetros de Calidad de Servicio, Asignación de Ancho de banda, y Cifrado.[23]

2.5.1.3 Contabilidad (ACCOUNTING)

Se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos.

La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes (Batch Accounting) consiste en la grabación de los datos de consumo para su entrega en algún momento posterior.

La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.

Principales Características

- Usualmente se desarrollan aplicaciones servidor, para el manejo de los requerimientos de AAA
- Generalmente funcionan sobre internet aunque puede ser utilizado en cualquier tipo de red
- Comúnmente utilizada para IP móviles
- Se suelen hacer Auditorias basadas en AAA

[23] (Seguridad en redes, 2014)

2.5.2 Listado de Protocolos AAA

RADIUS: Es un protocolo cliente-servidor utilizado por el estándar de seguridad del 802.1x en redes inalámbricas para la autenticación, autorización y administración de usuarios remotos para acceder a los recursos de una red. RADIUS mejora el estándar de encriptación WEP, en conjunto con otros métodos de seguridad como EAP-PEAP. Posee gran capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar si fuera el caso.[24]

Un cliente envía las credenciales de usuario y la información de los parámetros d conexión en forma de mensaje al servidor RADIUS. El servidor RADIUS comprueba las credenciales, autentica y autoriza la solicitud del cliente, indicando mediante un mensaje de respuesta si se autoriza o no a la petición de acceso del cliente. Por otro lado los mensajes RADIUS son enviados como mensajes UDP utilizando el puerto UDP 1812 para mensaje de autenticación RADIUS y, el puerto UDP 1813, es usado para mensajes de cuentas RADIUS.[25]

RADIUS también es comúnmente usado por el NAS (Network Access Server) para notificar eventos como:

- El inicio de sesión del usuario
- El final de sesión del usuario
- El total de paquetes transferidos durante la sesión
- El volumen de datos transferidos durante la sesión
- La razón para la terminación de la sesión[26]

[24] (wikipedia, Protocolo AAA, 2014)
[25] (wikipedia, Protocolo AAA, 2014)
[26] (Seguridad en redes, 2014)

Diameter: Protocolo de tipo P2P. Diseñado principalmente para aplicaciones que acceden a redes o de IP móvil.

TACACS: Protocolo para desarrollo de servidores. Usado comúnmente para servidores Unix.

TACACAS+: Basado en TACACS pero se redefinió totalmente el protocolo. Provee los servicios de AAA por separado. Basado en TCP.

PPP: El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico.

EAP: Es una autenticación Framework usada habitualmente en redes WLAN Point to-Point Protocol. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas, es más frecuentemente su uso.

LDAP: Es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también se considera una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

2.6 NAS

Un Network Access Server (NAS) es un sistema que proporciona acceso a la red. En algunos casos también se conoce como Remote Access Server (RAS) o Terminal Server. NAS es un elemento que controla el acceso a un recurso protegido, que puede ser desde un teléfono para VoIP o una impresora, hasta el acceso a una red inalámbrica o a Internet (proporcionado por un ISP).

En la **figura 2.5** se observa la estructura de un sistema NAS.

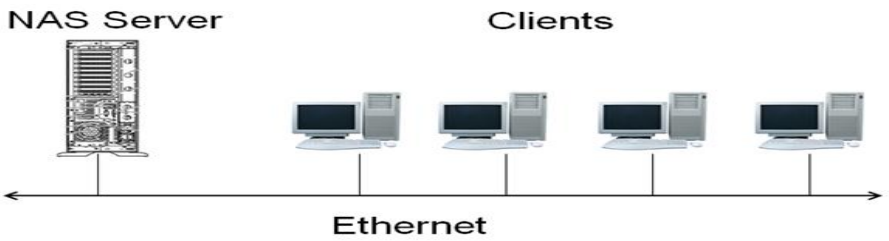


Figura 2.5 Diagrama de sistema NAS
(Fuente: http://es.over-blog.com/Que_es_un_servidor_NAS_definicion_del_experto-1228321779-art379097.html)

Cuando un cliente quiere hacer uso de uno de estos servicios se conecta a NAS, quien a su vez se conecta a un servidor de AAA (típicamente RADIUS) preguntando si los credenciales proporcionados por el cliente son válidos. Si la respuesta es afirmativa y positiva el servidor NAS dará acceso al usuario para que pueda entrar a sacar partido del recurso. En este momento termina el objetivo y la finalidad del servidor NAS, volviendo sólo a entrar en acción cuando es otro usuario el que requiere el acceso al sistema protegido.[27]

2.6.1 Uso

Este tipo de servidores en red NAS que aumentan la seguridad se aplican a diversos sectores de diferentes tecnologías y finalidades. Un buen ejemplo de su utilización se encuentra en las centralitas telefónicas de servicios especiales para clientes de servicios.

Este tipo de números, por ejemplo, servicios de atención al cliente de empresas en las que se requiere una suscripción, sólo pueden ser contactados por usuarios aprobados. En este caso, el servidor NAS recopila el número de teléfono desde el que se está llamando, lo envía a la central de comprobación, y después autentifica al usuario para terminar la llamada.

[27] (overblog, 2014)

Otro uso habitual de los servidores NAS se encuentra en conexiones y servicios de internet en los que se requiere una comprobación adicional en cuanto a nombre de usuario y contraseña para que se lleve a cabo la conexión.

En definitiva, los servidores NAS se ocupan de crear una plataforma de protección entre usuario y servicio para mantener efectivos los niveles de seguridad.[28]

2.7 Servidores RADIUS

2.7.1 Tipos de Servidores RADIUS

Existe un gran número de servidores RADIUS principalmente para entornos UNIX, cada uno de ellos comparte muchas características similares aunque cada servidor busca explotar factores tecnológicos que le den la ventaja sobre los demás. Hay servidores comerciales como también los hay con licencia libre, siendo FreeRADIUS, Radius Cistron y Radiator los servidores más populares, sin embargo se analizaran varias alternativas.[29]

2.7.2 Servidores de licencia libre

2.7.2.1 FreeRADIUS

FreeRADIUS es uno de los servidores RADIUS más modulares y ricos en características disponibles hoy en día. Ha sido escrito por un equipo de desarrolladores que tiene décadas de experiencia recolectada en implementar y desarrollar software RADIUS, en ingeniería de software, y administración de paquetes Unix.

El producto es el resultado de la sinergia entre muchos de los más reconocidos nombres en software libre basado en implementaciones RADIUS, incluyendo una gran cantidad de desarrolladores del sistema operativo Debian GNU/Linux. El servidor FreeRADIUS es distribuido bajo la licencia GNU GPL (versión 2).

[28] (overblog, 2014)
[29] (Servidores RADIUS, 2014)

El servidor FreeRADIUS está siendo usado alrededor del mundo en instalaciones a gran escala, abarcando múltiples servidores RADIUS con millares de usuarios y millones de sesiones.[30]

Características

El servidor FreeRADIUS tiene un número de característica que son comúnmente encontradas en los servidores RADIUS, y características adicionales que no son encontradas en otro servidor libre. A continuación se describe una lista de características importantes de este servidor:

- Ediciones multiplataforma y código fuente
- El servidor FreeRADIUS ha sido compilado y probado para correr en las siguientes plataformas
    - Linux (todas las Versiones)
    - FreeBSD
    - NetBSD
    - Solaris

A diferencia de varios servidores comerciales, un gran número de CPU's y arquitecturas han sido verificadas para trabajar, y son "soportadas" vía lista de usuarios. La desventaja de apoyar tantas variaciones de sistemas es que los pasos para instalar el servidor son algo más que simplemente "instalar el paquete". Es recomendable revisar si existe un paquete específico para el sistema operativo utilizado, en caso de que no exista entonces se debe construir el servidor del código.

Métodos de autorización. Los siguientes tipos de autorización son algunos de los métodos que son soportados por este servidor.

[30] (Servidores RADIUS, 2014)

- Archivos locales
- Bases de datos DB/DBM locales
- Protocolo LDAP
- Un programa de ejecución local (como los programas CGI)
- Programa Perl, Python
- Base de datos MySQL, PostgreSQL, Oracle SQLDB, IODBC SQL
- IBM's DB2[31]

Métodos de autenticación. Los siguientes son sólo algunos métodos de autenticación soportados por este servidor.

- Contraseñas en Texto simple en un archivo local de configuración (PAP)
- Contraseñas encriptadas en un archivo local de configuración
- CHAP
- MS-CHAP
- MS-CHAPv2
- Autentificación a un controlador de dominio Windows
- Proxy a otro servidor RADIUS
- Sistema de autenticación (usualmente por /etc/password)
- PAM (Modulo de autenticación conectable)
- LDAP (solo PAP)
- PAM (solo PAP)
- CRAM
- Programas Peral, Python
- SIP Diges (Cisco por cajas VOIP)
- Un programa de ejecución local (como CGI)
- Contraseñas encriptables Netscape-MTA-MD5
- Autenticación Kerberos
- Métodos EAP (incluyendo cisco LEAP)

[31] (Servidores RADIUS, 2014)

Métodos para el manejo de cuentas de usuarios.- Los siguientes métodos de cuentas están soportados

- Archivos locales de “detalle”
- Archivos locales “wtmp” y “utmp”
- Proxy a otros servidores RADIUS
- Replique a otro o más servidores RADIUS
- SQL (Oracle, MySQL, PostgreSQL, Sybase IODBC, etc.)[32]

2.7.2.2 Radius Cistron

Es un servidor de autentificación y manejo de cuentas para servidores de terminal por medio del protocolo RADIUS, este se ha convertido en uno de los servidores más usados por la comunidad de software libre.

Entre sus características más importantes están:

- Es libre (bajo la licencia GNU GPL)
- Soporta el acceso basado en huntgropus
- El archivo de usuarios se procesa en orden, es posible múltiples entradas por defecto, y todas las entradas pueden ser opcionalmente "fall throught"
- Atrapa todos los archivos de configuración en memoria, incluyendo los archivos de usuarios
- Mantiene una lista de entrada de usuarios
- Soporta el uso simultáneo de parámetros X
- Soporta atributos especificados del vendedor, incluyendo los no estandarizados USRs
- Soporta proxing
- Puede replicar datos de uso de cuentas entre servidores

[32] (Servidores RADIUS, 2014)

2.7.2.3 XtRADIUS

La diferencia más importante entre XTRADIUS y otros servidores RADIUS, es que permite ejecutar scripts que pueden ser modificados completamente para manejar autentificación y uso de cuentas. El beneficio que da esta característica, es que en lugar de usar el mismo archivo de usuarios RADIUS, o el sistema de archivo de contraseña para la autenticación, se puede llamar a una aplicación de scripts para preguntar a cualquier fuente (tal como una base de datos SQL), y revisar las condiciones válidas antes de permitir la entrada del usuario. A diferencia de otras soluciones, no requiere parche.

Este servidor está basado en el servidor Radius Cistron por lo cual incluye todas sus características, como también otras mejoras. La comunicación entre el servidor XtRadius y los scripts externos se da usando parámetros de línea de comando o por variables de ambiente.[33]

2.7.3 Servidores de tipo comerciales

2.7.3.1 Radiator

Radiator es un altamente configurable y flexible servidor RADIUS el cual soporta autenticación para cerca de 60 diferentes tipos de métodos de autenticación tales como archivos planos , archivos DBM, archivos de contraseña Unix, bases de datos SQL, servidores RADIUS remotos (proxying), programas externos, utilidades de administración de usuarios NT, directorios activos, LDAP, etc. Entre sus características más importantes tenemos:

- Soporta RadSEC – seguridad confiable del proxying RADIUS
- Radiator ahora soporta más métodos de autenticación 802.1X que cualquier otro servidor RADIUS dando una amplia gama para escoger clientes de red 802.1X

[33] (Servidores RADIUS, 2014)

- Incluye certificados privados para clientes y servidores para probar la autenticación 802.1X
- Trabaja con la mayoría de NASs, VDPN, ADSL y puntos de acceso inalámbrico
- Incluye todo el código fuente
- Radiador puede ser comprado para ser usado en un solo servidor, o como parte de alguno de los paquetes ofrecidos, para la empresa, para los profesionales para la casa, etc
- Trabaja en la mayoría de las plataformas. UNIX, Linux, Windows, Mac, VMS[34]

2.7.3.2 AXL RADIUS

AXL es un servidor RADIUS completo que puede autenticar, manejar cuentas, y Proxy. La interface del programa permite al usuario usar métodos de autenticación y de uso de cuentas mediante cualquier método por el que Java puede acceder al mundo, bases de datos, LDAP, archivos planos, URL's.
AXL no es un servidor que regresa llaves. Este es una interface de programa al servidor RADIUS. AXL puede realizar todas las funciones de un servidor RADIUS pero no puede configurarse por sí mismo usando archivos o bases de datos, no tiene conocimiento de quien se puede conectar, y no tienen control sobre asuntos de políticas.

Se debe proporcionar la programación para leer archivos de configuración o bases de datos para poblar las tablas del cliente, y configurar el servidor por sí mismo (como puertos, direcciones, y nombre del servidor). El servidor tiene métodos para aceptar esta información. Algunas características adicionales:

- Incluye integración con el cliente RADIUS
- Se pueden empezar secuencias separadas de manejo de cuentas y autenticación

[34] (Servidores RADIUS, 2014)

- Soporte para atributos de Vendedores Específicos
- Soporte completo para Proxy
- Proxy dinámico: se puede enrutar cualquier paquete en cualquier parte basándose en una política o en paquetes de atributos del RADIUS
- Trabaja con cualquier base de datos que tenga el controlador JDBC
- El código fuente está muy bien documentado

En la **tabla 2.3** se realiza una comparativa de algunos servidores RADIUS tanto de comerciales como gratuitos y de esta forma, poder comprender las características para la elección de uno que más se adapte a nuestras necesidades.

Servidor RADIUS.	Características.
FreeRADIUS.	• Licencia Libre • Multiplataforma • Métodos de Autorización: ✓ Archivos locales ✓ Bases de datos DB/DBM locales ✓ Protocolo LDAP ✓ Un programa de ejecución local (como los programas CGI) ✓ Programa Perl, Pythón ✓ Base de datos MySQL, PostgreSQL, Oracle SQLDB, IODBC SQL ✓ IBM's DB2 • Métodos de Autenticación: ✓ CHAP ✓ MS-CHAP ✓ MS-CHAPv2 ✓ Autentificación a un controlador de dominio Windows ✓ Proxy a otro servidor RADIUS ✓ Sistema de autenticación (usualmente por /etc/password) ✓ PAM (Modulo de autenticación conectable) ✓ LDAP (solo PAP) ✓ PAM (solo PAP)
Radius Cistron.	• Es libre (bajo la licencia GNU GPL) • El archivo de usuarios se procesa en orden, es posible múltiples

	• Atrapa todos los archivos de configuración en memoria, incluyendo los archivos de usuarios • Mantiene una lista de entrada de usuarios • Soporta el uso simultáneo de parámetros X
XtRADIUS.	• Basado en el servidor Radius Cistron
Radiator.	• Trabaja con la mayoría de NASs, VDPN, ADSL y puntos de acceso inalámbrico • Incluye todo el código fuente • Radiador puede ser comprado para ser usado en un solo servidor, o como parte de alguno de los paquetes ofrecidos, para la empresa, para los profesionales para la casa, etc
AXL RADIUS.	• Incluye integración con el cliente RADIUS • Se pueden empezar secuencias separadas de manejo de cuentas y autenticación • Soporte para atributos de Vendedores Específicos • Soporte completo para Proxy • Proxy dinámico: se puede enrutar cualquier paquete en cualquier parte basándose en una política o en paquetes de atributos del RADIUS • Trabaja con cualquier base de datos que tenga el controlador JDBC • El código fuente está muy bien documentado

Tabla 2.3 Características de servidores RADIUS
(Fuente: http://trabajotele08.blogspot.mx/)

Después de haber estudiado las características de los servidores se ha llegado a la conclusión de utilizar FreeRADIUS para nuestro proyecto ya que este servidor RADIUS goza de una gran aceptación entre los usuarios y administradores de red porque cuenta con un gran número de características y funciones únicas que no existen en otros servidores.[35]

Su gran popularidad ayuda a que sea usado en un mayor número de entornos de seguridad y que si llegara a encontrar fallas y limitaciones podrán ser corregidas para hacer de este uno de los servidores más robustos y eficientes que se puede encontrar, además FreeRADIUS maneja varias alternativas de almacenamiento de información de sus usuarios entre ellas está el almacenamiento en base de datos MySQL la cual usaremos en esta ocasión.

[35] (Servidores RADIUS, 2014)

2.8 Portal Cautivo

2.8.1 ¿Que es un portal cautivo?

Un portal cautivo (o captivo) es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.

El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede empezar a controlar el ancho de banda usado por cada cliente.

Se usan sobre todo en redes inalámbricas abiertas, donde interesa mostrar un mensaje de bienvenida a los usuarios y para informar de las condiciones del acceso.

Los administradores suelen hacerlo para que sean los propios usuarios quienes se responsabilicen de sus acciones, y así evitar problemas mayores. Se discute si esta delegación de responsabilidad es válida legalmente.[36]

2.8.2 Tipos de Portales Cautivos

Los portales cautivos se encuentran clasificado en 2 grupos principales que se enumeran a continuación.

2.8.2.1 Portales Cautivos por software

Son aquellos implementados mediante el uso de aplicaciones o programas cuya arquitectura fue diseñada para trabajar como portales cautivos, los mismos que van instalados y configurados desde un servidor principal dentro de la red. A continuación se listan los principales portales cautivos que pueden ser implementados mediante software:

[36] (wikipedia, Portales cautivos, 2014)

- PepperSpot (Linux)
- GRASE Hotspot (Linux)
- NoCatAuth (Linux)
- Chillispot(Linux)
- CoovaChilli (Linux)
- WifiDog (embedded Linux - OpenWRT, Linux, Windows)
- Ewrt (embedded Linux - WRT54G, Linux)
- HotSpotSystem.com (embedded Linux, WRT54GL, Mikrotik, etc)
- FirstSpot (Windows)
- m0n0wall (embedded FreeBSD)
- OpenSplash (FreeBSD)
- wicap (OpenBSD)
- Public IP (Linux)
- PfSense (FreeBSD)
- AirMarshal (Linux)
- ZeroShell (Linux)
- Easy Captive (Linux)
- Antamedia HotSpot Software (Windows)

2.8.2.2 Portales Cautivos por Hardware

Son aquellos implementados mediante dispositivos físicos, diseñados específicamente para funcionar como portales cautivos, se agregan a la red al igual que los dispositivos de Networking, y generan las mismas funcionalidades que los portales implementados mediante Software.

A continuación se listan los dispositivos que implementan un portal cautivo sin necesidad de ordenador:

- Cisco BBSM-Hotspot

- Cisco Site Selection Gateway (SSG) / Subscriber Edge Services (SESM)
- Nomadix Gateway
- Aptilo Access Gateway
- Antica PayBridge
- 3G/Wimax: Usado principalmente para prepago

2.9 daloRADIUS

daloRADIUS es una plataforma RADIUS web avanzado destinado a la gestión de zonas interactivas y los despliegues de ISP de uso general. Cuenta con rica gestión de usuarios, informes gráficos, contabilidad, y se integra con GoogleMaps para geo-localización (SIG). daloRADIUS está escrito en PHP y JavaScript, y utiliza una capa de abstracción de base de datos lo que significa que es compatible con muchos sistemas de bases de datos, entre ellos el MySQL popular, PostgreSQL, SQLite, MSSQL, y muchos otros.

Se basa en una implementación FreeRADIUS con un servidor de base de datos. Entre otras características se implementa ACLs, integración GoogleMaps para la localización de los puntos de puntos de acceso / acceso visual y muchas más características. daloRADIUS es esencialmente una aplicación web para administrar un servidor RADIUS lo que en teoría se puede gestionar cualquier servidor RADIUS y no específicamente gestiona FreeRADIUS y su estructura de base de datos. Desde la versión 0.9-3 daloRADIUS ha introducido una capa de abstracción de base de datos en toda la aplicación basada en paquete de PEAR, DB de PHP que soportan una amplia gama de servidores de bases de datos.[37]

[37] (Tal, 2014)

En la **figura 2.6** se muestran una gráfica de los leguajes de programación que utiliza daloRADIUS, en la cual se puede observar que PHP es el lenguaje más utilizado.

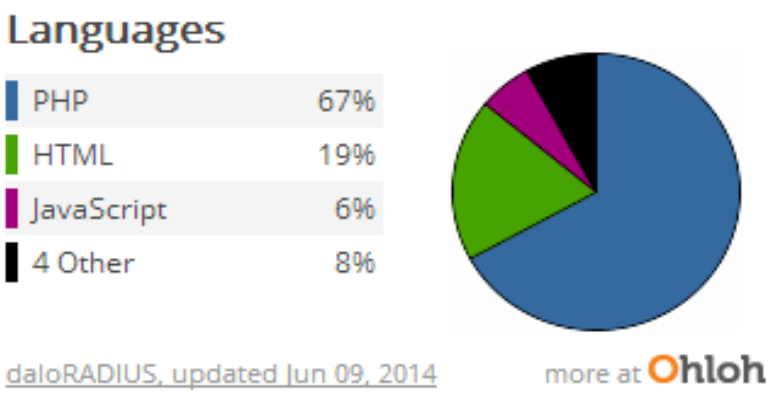


Figura 2.6 Características de daloRADIUS
(Fuente: http://www.daloradius.com/)

En la **figura 2.7** se muestran más características de daloRADIUS como lo es el lenguaje de programación principal y el número de personas que contribuyen al desarrollo del proyecto.

Figura 2.7 Lenguajes soportados por daloRADIUS
(Fuente: http://www.daloradius.com/)

daloRADIUS se ha ganado la reputación de ser un producto sólido y maduro como una plataforma de gestión de FreeRADIUS, ya sea dirigida a las soluciones de VPN, hotposts gestión wi-fi o configuraciones de ISP en toda regla. Es la comunidad de

usuarios y empresas que han contribuido al proyecto de muchas maneras ha ayudado a darle forma al producto que es hoy.[38]

En la **figura 2.8** se muestran una lista, la cual proporciona una vista de las empresas que apoyaron daloRADIUS o uso que se haga de ella.

Figura 2.8 Empresas que apoyaron daloRADIUS
(Fuente: http://www.daloradius.com/)

[38] (Tal, 2014)

Capítulo III Metodología

3.1 Metodología propuesta

Para desarrollar este proyecto fue necesario tener claro ¿A quiénes nos dirigimos?, es decir, quienes beneficiara el servicio de gestión de un portal cautivo dentro de una organización, por lo que identificamos que los principales beneficiados son: el personal administrativo de redes o en su caso, el encargado de sistemas, puesto que la gestión de un portal cautivo, nos brindara argumentos más claros para poder realizar mejoras de la red inalámbrica.

3.1.1 Requerimientos para la gestión de portales cautivos

Es necesario tener en cuenta que para poder implementar una aplicación de gestión de portales cautivos, debe existir un portal cautivo en la red inalámbrica y también debe haber un servidor de autenticación de usuarios, en caso de no contar con los servicios mencionados, es debe realizar la implementación de ambos, tomando en cuenta los costos que traen consigo.

3.1.2 Equipo y herramientas necesarias

Para realizar la implementación de una aplicación para la gestión de portales cautivos es necesario contar con los siguientes requerimientos:

- Un servidor en el cual se alojaran las aplicaciones necesarias, con dos tarjetas de red (eth0 y eth1) y con sistema operativo Linux (Debian)
- Una conexión a internet constante y de alta velocidad
- Un servidor de autenticación de usuarios (FreeRADIUS)
- Un Portal cautivo en funcionamiento (chillispot)

3.1.3 Método de investigación

Este proyecto se basa en los métodos de investigación **documental y de campo,** para su mejor comprensión, a continuación se detalla cada uno de estos métodos.

Investigación documental: Son trabajos cuyo método de investigación se concentra exclusivamente en la recopilación de datos de fuentes documentales, ya sea de libros, textos, sitios Web o cualquier otro tipo de documentos gráficos, iconográfico y electrónico. Su único propósito es obtener antecedentes documentales para profundizar en teorías, leyes, conceptos y aportaciones ya existentes y asentadas en documentos sobre el tema que es objeto de estudio, para luego complementar, refutar o derivar, en su caso, nuevos conocimientos.

Investigación de campo: Son las investigaciones cuya recopilación de información se realiza dentro del ambiente específico donde se presenta el hecho o fenómeno de estudio. En la realización de estas tesis, se utilizan los métodos de investigación específicos para la disciplina de estudios y también se diseñan ciertas técnicas e instrumentos para recabar información en el medio donde interactúa el fenómeno bajo estudio. Para la tabulación y el análisis de la información obtenida, se utilizan métodos y técnicas estadístico-matemáticos que ayudan a concentrar, interpretar y obtener conclusiones formales, científicamente comprobadas.

Como se mencionó anteriormente, en el presente proyecto se aplicaron los métodos documental y de campo puesto que con esto se pretende consolidar los datos y los resultados obtenidos.

La investigación documental nos sirve para recopilar la información necesaria sobre la teoría en que se basa todo lo concerniente a portales cautivos y la investigación de campo nos sirve para realizar un estudio más de cerca y detallado del fenómeno en estudio.

3.1.4 Enfoque del proyecto

Dentro de una investigación pueden desarrollarse muchas metodologías pero todas ellas pueden encasillarse en dos grandes grupos, la metodología de investigación cualitativa y cuantitativa.

Enfoque cuantitativo

Son las investigaciones de tesis cuyo planteamiento obedece a un enfoque objetivo de una realidad externa que se pretende describir, explicar y predecir en cuanto a la causalidad de sus hechos y fenómenos. Para ello, se requiere de un método formal de investigación de carácter cuantitativo, en el que la recolección de datos es de tipo numérico, estandarizado y cuantificable mediante los procedimientos estadísticos que usa.

Enfoque cualitativo

Estas investigaciones se fundamentan más en estudios descriptivos, interpretativos e inductivos (que van de lo particular a lo general) y se utilizan para analizar una realidad social con el propósito de explorar, entender interpretar y describir el comportamiento de la realidad en estudio, no necesariamente para comprobarla.

El enfoque de esta investigación se basó en los dos mencionados anteriormente puesto que de esta manera se logra una perspectiva más precisa del fenómeno, la cual nos ayudó a clarificar y formular mejor el planteamiento del problema.

3.1.5 Técnica implementada para la recolección de información

Para la recolección de información existen diversas técnicas como lo son la encuesta y la entrevista. En nuestro caso decidimos utilizar la encuesta como técnica para

recolectar información, la encuesta va dirigida a los encargados de sistemas de los establecimientos en los que se aplicara.

La encuesta consta de 8 preguntas cerradas, ¿Por qué cerradas?, se tomó la decisión de realizar preguntas cerradas puesto que este tipo de preguntas se le facilita más a las personas, al contario de las preguntas abiertas aquí solamente tendrán que seleccionar una de las respuestas que se le dan al encuestado y así evitamos que contesten algo incoherente o que se aburran. En la **figura 3.1** se muestra el formato de la encuesta realizada.

Encuesta Realizada para proyecto de titulación titulado: Gestión de portales cautivos con daloRADIUS en Debian

1. **¿Tiene algún problema con el servicio de internet dentro del establecimiento?**
   a) Si b) No

2. **¿Qué problemas de servicio de internet se presentan con regularidad?**
   a) No conecta a internet b) Internet lento c) Ninguno d) Otro

3. **¿Tienen algún método de autenticación de usuarios para acceder a internet?**
   a) Si b) No

4. **¿Le gustaría tener un control de los usuarios que acceden a la red de internet?**
   a) Si b) No c) En otro momento

5. **¿Tiene conocimiento acerca de portales cautivos?**
   a) Nada b) Poco c) Regular

6. **¿Tiene o han implementado algún portal cautivo?**
   a) Si b) No

7. **¿Sabía que con un portal cautivo puede mostrar ofertas o promociones acerca de su negocio?**
   a) Si b) No c) No lo creía

8. **¿Le interesaría implementar un portal cautivo y una aplicación para gestionar los usuarios de su red de internet?**
   a) Si b) No c) En otro momento

¡Gracias por su tiempo su atención!

Figura 3.1 Formato de encuesta
(Fuente: Obtenida de investigación realizada)

La aplicación de la encuesta nos permitirá recabar información necesaria para fundamentar la necesidad que se tiene para gestionar un portal cautivo o en el caso de no existir plantear la propuesta de implementar un portal cautivo, así como, también dar a conocer los beneficios que tiene llevar un control de los usuarios que se conectan a la red inalámbrica.

3.1.6 Fases de la metodología

Para el desarrollo de este proyecto se han identificado las actividades que se deben realizar, las cuales se detallan a continuación.

3.1.6.1 Análisis del problema

En esta fase se realizara una investigación de detallada de todo lo necesario para la implementación de portales cautivos, servidores de autenticación de usuarios, y aspectos teóricos que servirá para fundamentar lo que se realizara.

3.1.6.2 Identificación de las variables involucradas

Variables independientes

La variable independiente que se detectó en este proyecto fue: **Un Servidor Remoto de Autenticación de Usuarios (RADIUS)** como se menciona en este mismo capítulo en el apartado, RADIUS es un protocolo que nos permite gestionar la autenticación, autorización y registro de usuarios remotos sobre un determinado servicio. Es un una variable independiente puesto que no requiere de algún otro servicio para su funcionamiento.

Variables dependientes

Como se mencionó anteriormente, en este proyecto se identificaron dos variables dependientes.

- **Portal cautivo:** Los portales cautivos requieren de un protocolo de autenticación para que puedan funcionar, en nuestro caso se hace uso del protocolo RADIUS y para eso se implementó un servidor FreeRADIUS
- **Servidor daloRADIUS:** Para que el servidor daloRADIUS funcione es necesario que se tenga implementado un servidor RADIUS y un portal cautivo, puesto que esta herramienta nos proporciona estadísticas acerca de los usuarios que acceden a un portal cautivo

Para hacer la comprobación de este proyecto, no solo se implementara o probara con una sola aplicación de portales cautivos sino que se hará la prueba en otros más, como lo es: ChilliSpot y coovachilli.

3.1.6.3 Instalación y configuración de daloRADIUS

Una vez realizado el análisis y la identificación de las variables involucrados ya podemos realizar la instalación y configuración de daloRADIUS, en esta parte ya deberá de haber un servidor de autenticación de usuarios y un portal cautivo en funcionamiento para poder realizar las configuraciones y la relación de daloRADIUS con el servidor de autenticación.

3.1.6.4 Documentación

Otra fase importante y necesaria del proyecto es la documentación, en esta etapa se realizara la documentación de los módulos principales y más importantes de daloRADIUS, de acuerdo a las necesidades del lugar en que se implementara.

3.2 Implementación de la metodología propuesta

En esta sección se describe la ejecución de la metodología propuesta anteriormente, con sus respectivas actividades realizadas.

3.2.1 Análisis de información obtenida a través de encuestas

En este apartado se muestran las gráficas de los resultados obtenidos con la encuesta realizada, se realizaron 12 encuestas con la finalidad de detectar necesidades y problemáticas a resolver, las encuestas van dirigidas a las personas encargadas de los establecimientos en los que se puede hacer uso de un portal cativo y se puedan gestionar los clientes que se conectan a la red.

A continuación se presentan las gráficas de cada pregunta con sus respectivas interpretaciones.

Pregunta No. 1.

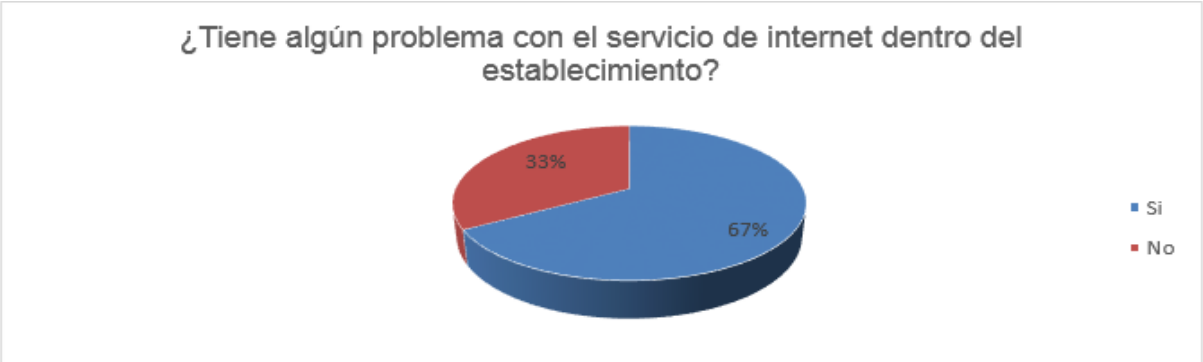


Figura 3.2 Pregunta No. 1
(Fuente: Obtenido en base a resultados de investigación)

En esta grafica se puede observar que en el 67% de los lugares donde se realizó la encuesta tienen problemas con el servicio de internet, mientras que el otro 33% de los encuestados no tienen problemas con el servicio de internet.

Pregunta No. 2.

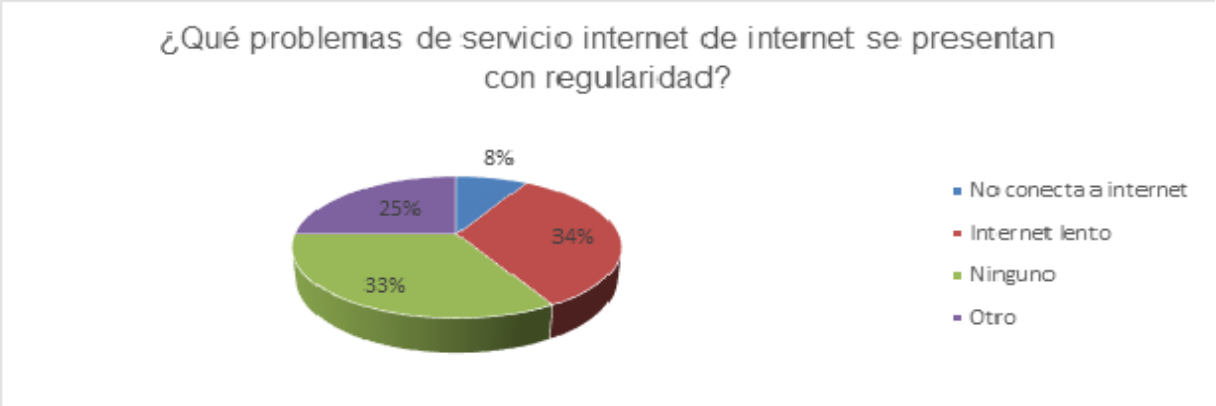


Figura 3.3 Pregunta No. 2
(Fuente: Obtenido en base a resultados de investigación)

En esta grafica se puede observar que el 34% de los lugares donde se realizó la encuesta presenta el problema de que el internet es lento, el 33 % no tienen ningún problema, en el 25% de los lugares se presentan otros problemas con el servicio de internet en su mayoría relacionado con el proveedor de internet y el otro 8% presenta el problema de que no conecta a internet.

Pregunta No. 3.

Figura 3.4 Pregunta No. 3
(Fuente: Obtenido en base a resultados de investigación)

En esta grafica se observa que el 67% de los lugares en que se realizó la encuesta no utilizan un método de autenticación de usuarios, mientras que el 33% restante si utiliza un método de autenticación de usuarios.

Pregunta No. 4.

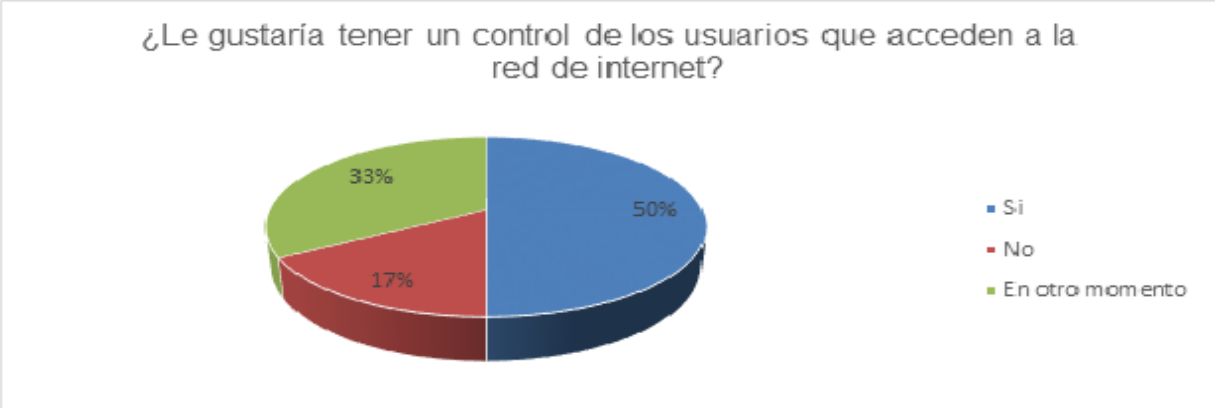


Figura 3.5 Pregunta No. 4
(Fuente: Obtenido en base a resultados de investigación)

En esta grafica se observa que al 50% de los lugares en los que se realizó la encuesta les gustaría llevar un control de los usuarios que se conectan a la red de internet, el 17% no está interesado en llevar un control de los clientes que se conectan a la red y el 33% restante contesto que en otro momento si le gustaría tener un control de los clientes que se conectan a la red.

Pregunta No. 5.

Figura 3.6 Pregunta No. 5
(Fuente: Obtenido en base a resultados de investigación)

Con respecto a la pregunta de, si tienen conocimiento de lo que es un portal cautivo el 67% de los encestados respondió que no tienen nada de conocimiento sobre el tema

de portales cautivos, el 25% dijo que tienen poco conocimiento y el 8% restante respondió que tienen conocimiento regular de los portales cautivos.

Pregunta No. 6.

Figura 3.7 Pregunta No. 6
(Fuente: Obtenido en base a resultados de investigación)

En la gráfica se observa que de todos los lugares en los que se realizó la encuesta, en el 100% no tienen o han implementado un portal cautivo.

Pregunta No. 7.

Figura 3.8 Pregunta No. 7
(Fuente: Obtenido en base a resultados de investigación)

En esta grafica se observa que el 92% de las personas que respondieron la encuesta no sabían que con un portal cautivo se pueden dar a conocer ofertas o promociones

acerca del negocio, el 8% respondió que si sabían que mediante el uso de un portal cautivo se pueden hacer promociones ofertas y nadie respondió que no creía que se pueda hacer promociones ofertas.

Pregunta No. 8

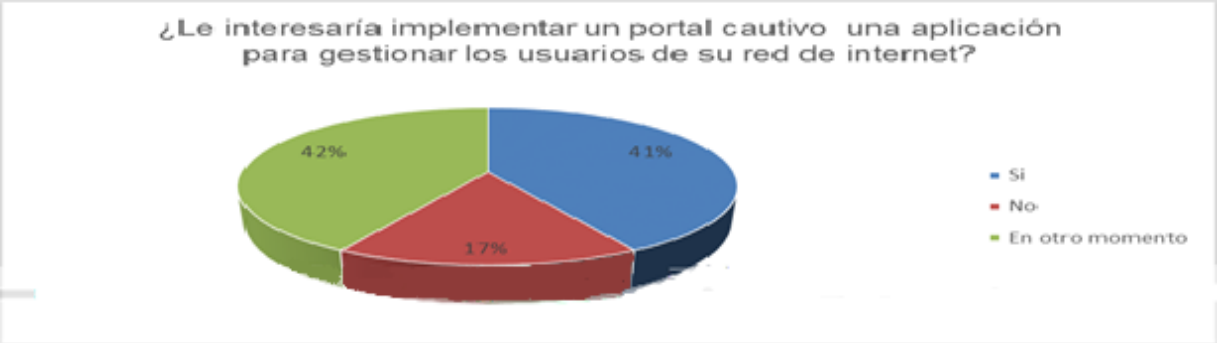


Figura 3.9 Pregunta No. 8
(Fuente: Obtenido en base a resultados de investigación)

La pregunta número 8 y última de la encuesta se refiere al interés de los encuestados en implementar un portal cautivo y una aplicación para gestionar los usuarios de la red de internet, en esta pregunta el 41% de los encuestados respondió que si le interesaría implementar estos servicios, el 17% respondió que no está interesado en el servicio, el 42% restante dijo que si le interesaría implementar un portal cautivo y una aplicación para gestionar los usuarios de la red pero en otro momento.

3.2.2 Variables involucradas

Como se mencionó en el apartado 3.1.6.2, se identificaron dos tipos de variables: dependientes e independientes.

Variables dependientes

- Portal cautivo (chillispot), para tener un mejor conocimiento de la instalación y configuración de chillispot véase el **anexo II** al final de este documento.
- Aplicación para la gestión del portal cautivo (daloRADIUS)

Variable independiente

- Servidor para autenticación de usuarios (FreeRADIUS), para su mejor comprensión véase el **anexo I** al final de este documento, en el cual se muestra la instalación y configuración de FreeRADIUS.

3.2.3 Instalación y configuración de daloRADIUS

En este apartado se realizara la instalación y configuración de daloRADIUS, para lo cual tendremos que descargar el paquete para poder instalarlo.

Para descargar el paquete de daloRADIUS se puede hacer de dos formas; la primera opción es ir a la página oficial que está en el siguiente link: http://sourceforge.net/projects/daloradius/ y dar clic en el botón verde que dice: "Download" como se muestra en la **figura 3.10**.

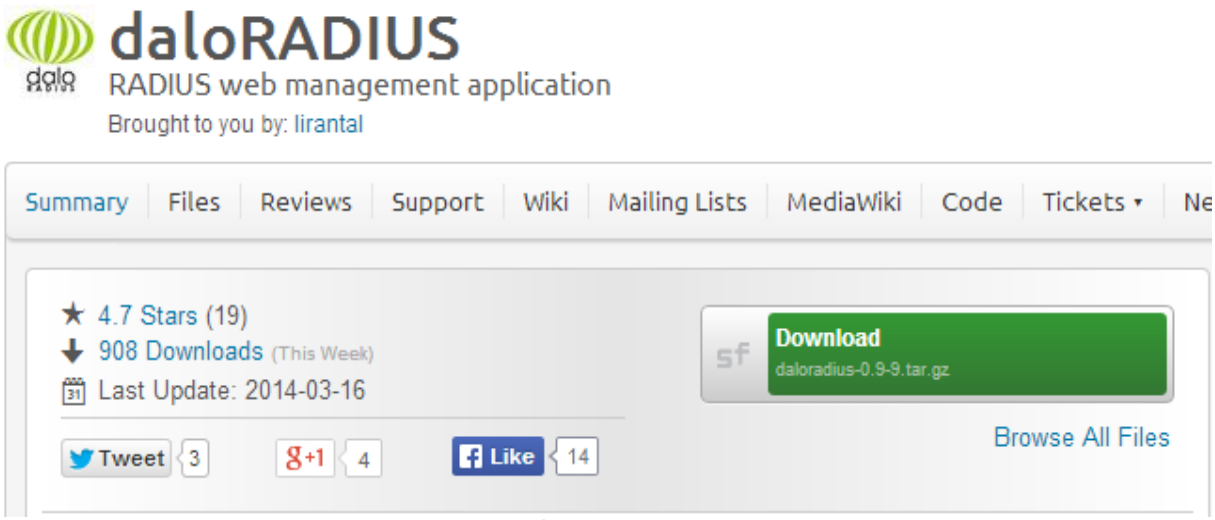


Figura 3.10 Página oficial de daloRADIUS
(Fuente: http://www.daloradius.com/)

La segunda manera para descargar el paquete es desde la terminal, primero se deberá ubicar en el directorio donde se va guardar el paquete de daloRADIUS y una vez que se ubique en el directorio procedemos a descargar el paquete con el siguiente comando (**figura 3.11**):

wget 'http://downloads.sourceforge.net/project/daloradius/daloradius/daloradius-0.9-8/daloradius-0.9-8.tar.gz'

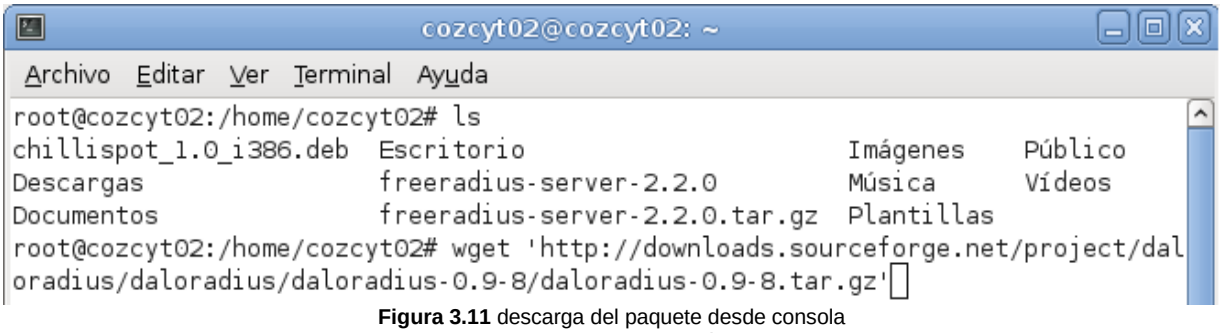


Figura 3.11 descarga del paquete desde consola
(Fuente: Obtenida de investigación realizada)

Una vez que se descargue el archivo, ubicarse en el directorio de descarga. Estando ahí desde la terminal descomprir el archivo y moverlo a la dirección "**/var/www/**" poniéndole un nuevo nombre tal y como se muestra en la **figura 3-12**.

Figura 3.12: Comando para mover el directorio
(Fuente: Obtenida de investigación realizada)

Lo que se deberá hacer a continuación es realizar el cambio del propietario del directorio "daloradius" y dar permisos con los comandos:

chown -R www-data:www-data /var/www/daloradius
chmod 644 /var/www/daloradius/library/daloradius.conf.php

Como se muestra en la **figura 3.13**

Figura 3.13 Cambio de propietario y asignacion de permisos
(Fuente: Obtenida de investigación realizada)

A continuación deberá copiar todos los directorios que se encuentren dentro de "**/var/www/dalorarius/contrib/chilli/portal2/**" a "**/var/www/**", tal y como lo muestra la **figura 3.14.**

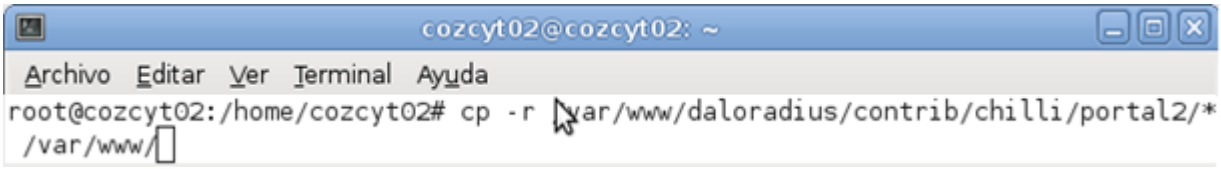


Figura 3.14: Copia de archivos a "/var/www/"
(Fuente: Obtenida de investigación realizada)

Los archivos que hemos copiado anteriormente son los directorios donde se encuentran las páginas de logeo para usuarios que no necesitan realizar ningún pago y la página de logeo para usuarios que deben realizar un pago mediante pay-pal, la opción de pago va dirigido para negocios en los que se paga por el servicio de internet.

Para continuar con la configuración de daloRADIUS deberá ubicarse en el directorio "**/var/www/daloradius/contrib/db**", en este paso deberá de tener instalado un gestor de base de datos y tener configurado FreeRADIUS para que funcione con base de datos, en nuestro caso se utilizara MySQL (para ver la configuración de FreeRADIUS con base de datos vea el **anexo III**), una vez que se tenga lo necesarios, ejecutar la siguiente sentencia para agregar todas las tablas que necesita daloRADIUS para poder trabajar como se muestra en **la figura 3.15**.

mysql -u root –p radius < mysql-daloradius.sql

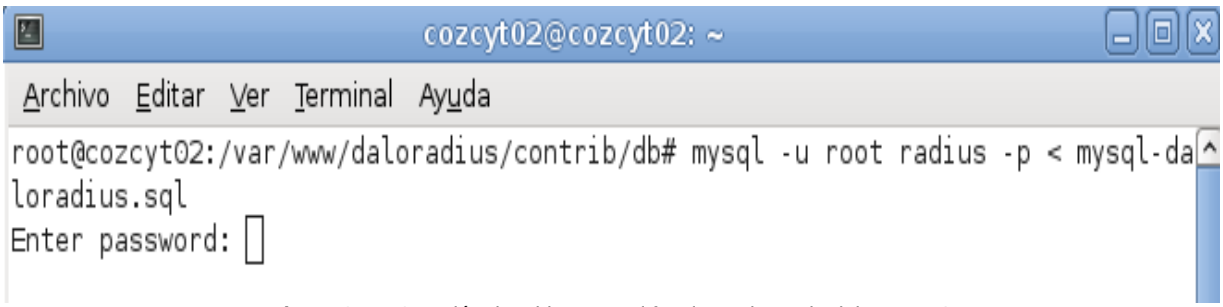


Figura 3.15: Creación de tablas para el funcionamiento de daloRADIUS
(Fuente: Obtenida de investigación realizada)

Una vez que ya estén creadas las tablas que se requieren pasaremos a configurar los archivos necesarios para la conexión de daloRADIUS con la base de datos, el primer archivo que se modificara se encuentra en el directorio:

"**/var/www/daloradius/library/daloradius.conf.php**"

En este archivo se deben configurar la contraseña, el usuario y la base de datos que se utilizara, los cuales se muestran en la **figura 3.16**.

$configValues['CONFIG_DB_PASS'] = '*******';
$configValues['CONFIG_MAINT_TEST_USER_RADIUSSECRET'] = 'testing123';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';

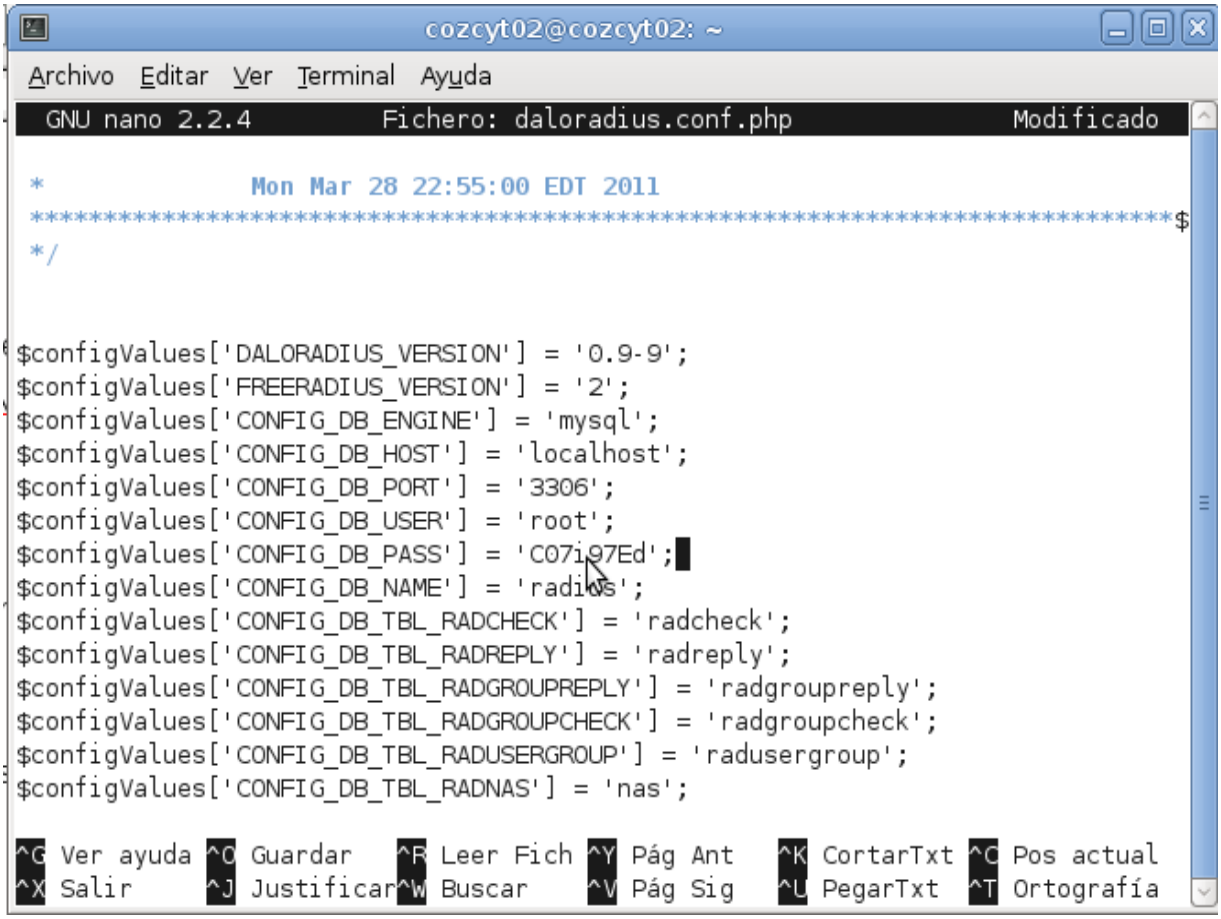


Figura 3.16: Configuración del archivo daloradius.conf.php
(Fuente: Obtenida de investigación realizada)

Los siguientes archivos que se tienen que modificar se encuentran en el directorio: "**/var/www/signup-*/library/daloradius.conf.php**"

Los parámetros que se tienen que modificar son los que se mencionan a continuación y se muestran en la **figura 3.17.**

$configValues['CONFIG_DB_PASS'] = 'xxxx';
$configValues['CONFIG_DB_NAME'] = 'radius';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';
$configValues['CONFIG_SIGNUP_SUCCESS_MSG_LOGIN_LINK'] = "
Click here".
" to return to the Login page

Figura 3.17: Configuración del archivo para dar acceso a internet
(Fuente: Obtenida de investigación realizada)

Ahora se configurara el archivo que se encuentra en el directorio "**/var/www/signup-free/index.php**" y se modificaran los parametros "**User-Password**" por "**Cleartext-Password**" y "**==**" por "**:=**".tal y como se muestra en la **figura 3.18**.

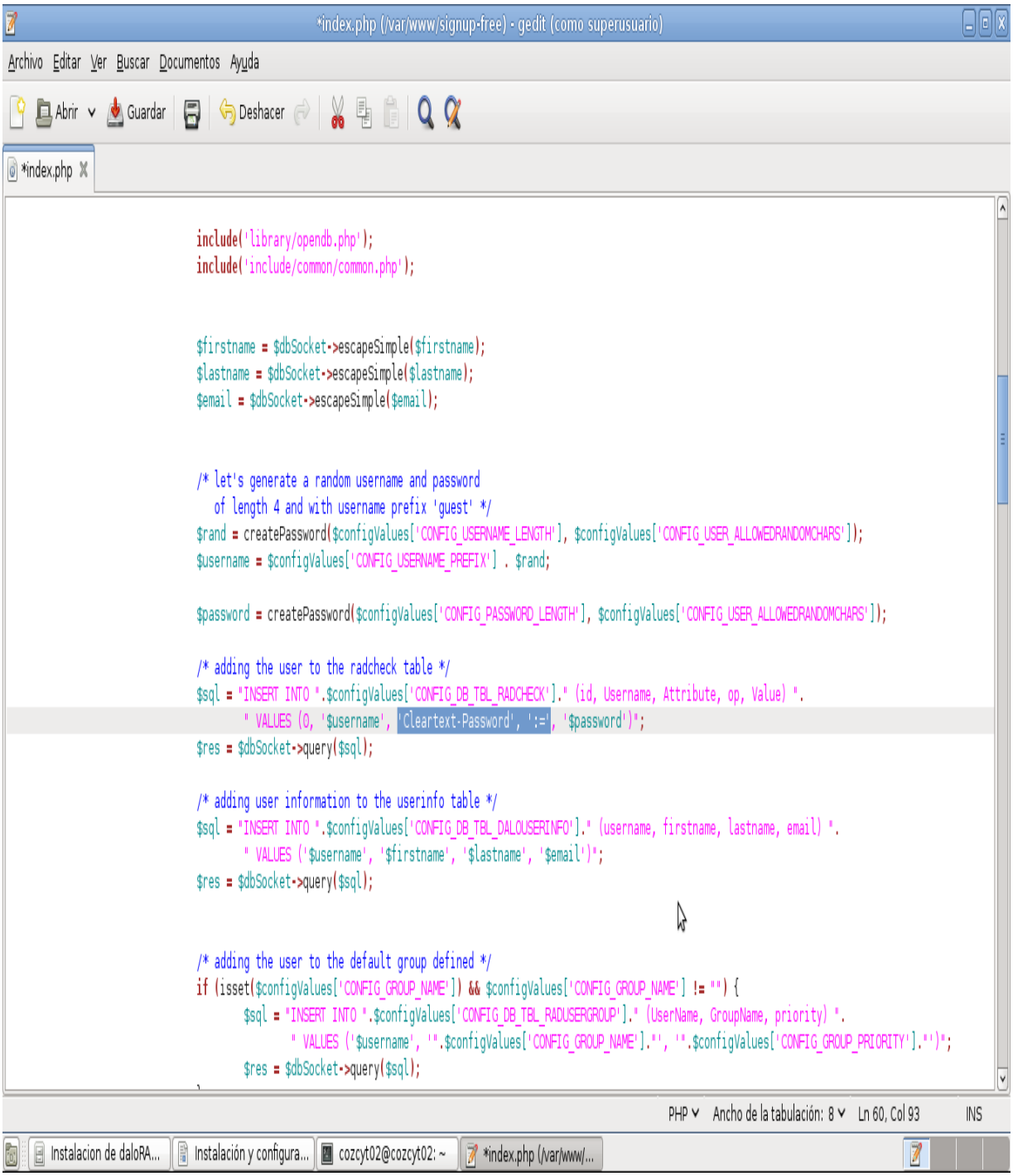


Figura 3.18 Configuración de archivo para agregar nuevos usuarios
(Fuente: Obtenida de investigación realizada)

El ultimo archivo que se tiene que configurar es el que se encuentra en el directorio "**/var/www/hotspotlogin/hotspotlogin.php**" en el cual se configuraran los parámetros $uamsecret y $userpassword quedando como se muestra en la **figura 3.19**.

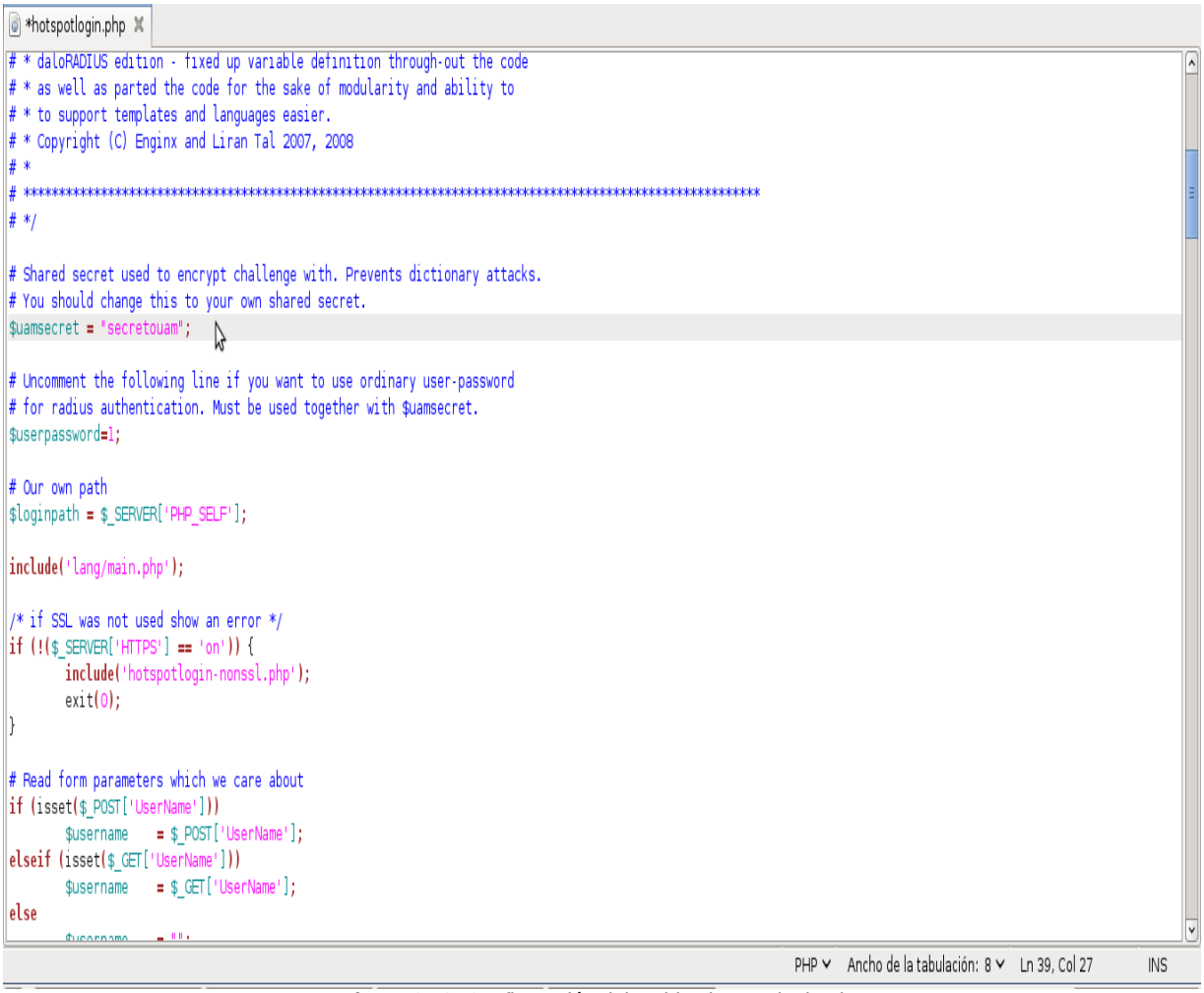


Figura 3.19: Configuración del archivo hotspotlogin.php
(Fuente: Obtenida de investigación realizada)

El archivo hotspotlogin.php es el archivo que realiza las validaciones de las credenciales que se introducen. Se puede usar el archivo php que trae consigo daloRADIUS o también se puede usar el archivo cgi que es que trae por default chillispot, aunque es un poco más complicado de poder modificar y adaptarlo a las necesidades que se tengan.

Si se siguieron todos los pasos anteriores al abrir un navegador e introducir la url "**https://ipdelservidor/daloradius**" nos aparecerá lo de la **figura 3.20**.

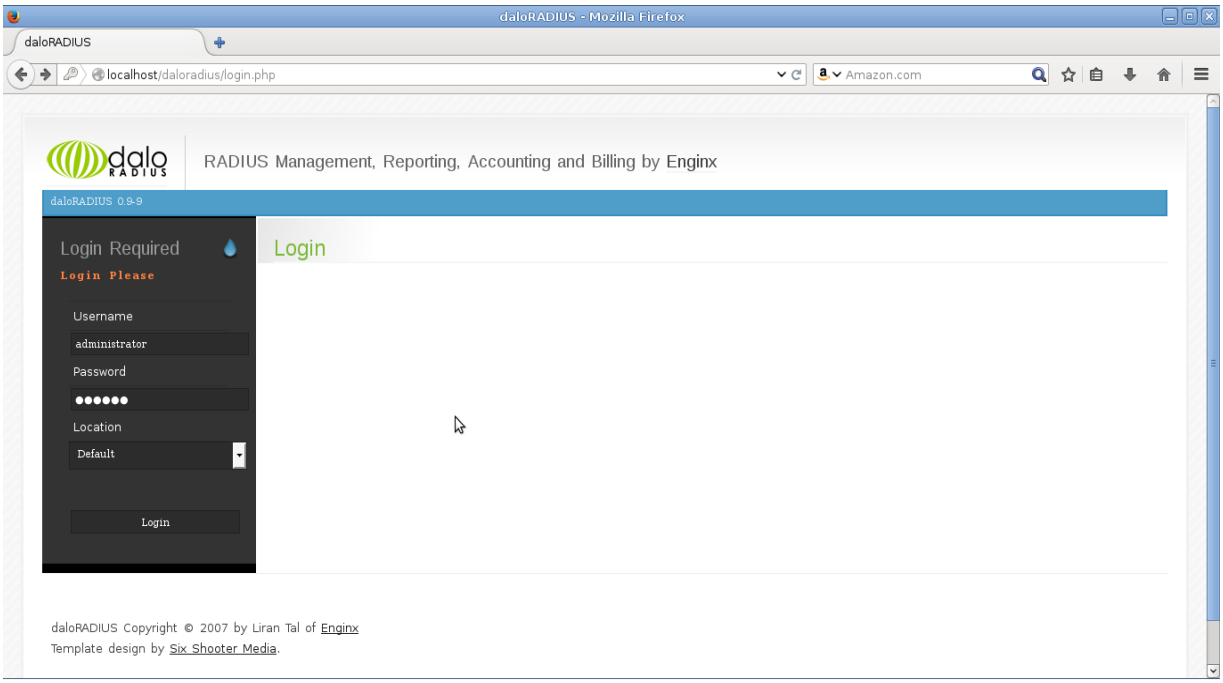


Figura 3.20: Interfaz de inicio de daloRADIUS
(Fuente: Obtenida de resultados de investigación)

3.2.4 Implementación de daloRADIUS

Una vez que ya se tenga todo lo necesario en funcionamiento, es necesario conocer el funcionamiento de daloRADIUS.

A continuación se explican los módulos más importantes de los que consta daloRADIUS. Para el buen uso de daloRADIUS y para ingresar a ella hacer lo siguiente: abrir un navegador y teclear la dirección del directorio donde se instaló daloRADIUS ("**direcciondelared/daloradius**") tal y como se muestra en la **figura 3.21**.

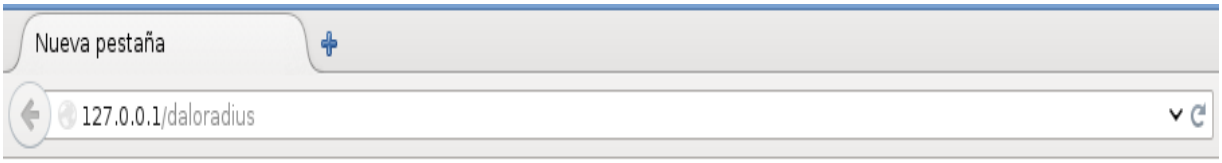


Figura 3.21 Url para acceder a daloRADIUS
(Fuente: Obtenida de investigación realizada)

Dar un ENTER y mostrara la página donde se debe de ingresar el usuario y la contraseña. Por defecto el usuario es “**administrator**” y la contraseña “**radius**” los cuales es recomendable cambiarlos después de acceder por primera vez. La **figura 3.22** muestra el aspecto de **Login.**

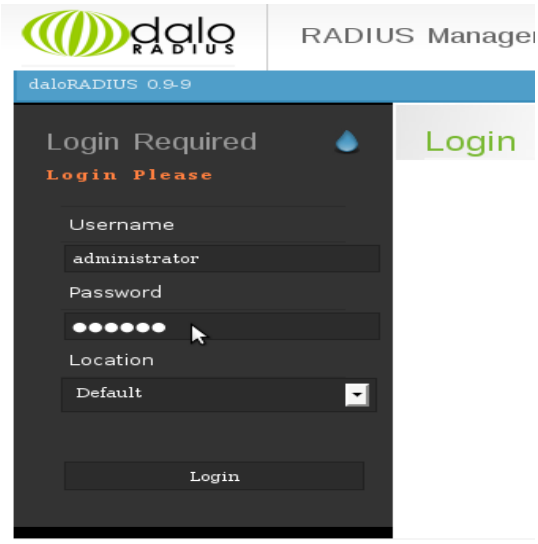


Figura 3.22 Login de daloRADIUS
(Fuente: Obtenida de resultados de investigación)

Una vez dentro de la aplicación se puede observar que estamos situados en la parte de **Home** de la aplicación por defecto y esta muestra en la parte izquierda varias opciones de las cuales vienen, desde lo que es información del estado del servidor, los servicios, entre otros. En la **figura 3.23** se puede ver la interfaz de inicio de daloRADIUS.

Figura 3.23 Interfaz de inicio de daloRADIUS
(Fuente: Obtenida de resultados de investigación)

Server Status: Como se puede observar en la **figura 3.24**, en la sección de server status se muestra información general del servidor, como el estado de memoria, espacio en disco, interfaz de la red sobre la que se proporciona el servicio, entre otros.

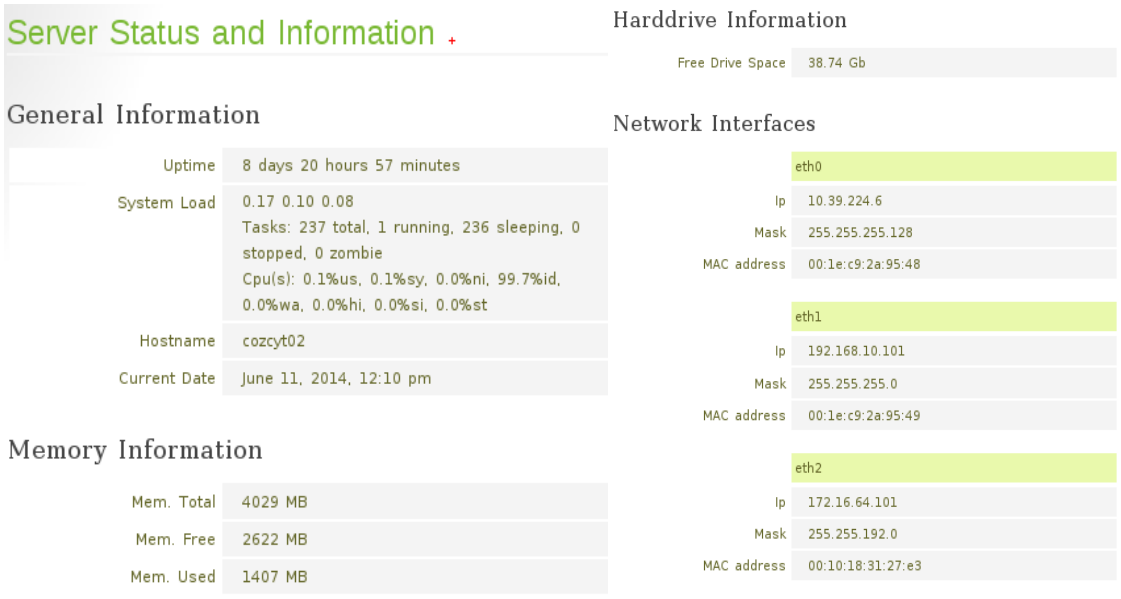


Figura 3.24 Estado del servidor
(Fuente: Obtenida de resultados de investigación)

Services Status: Muestra los servicios que se están ejecutando como se muestra en la **figura 3.25**, mínimo deben de existir dos: MySQL y Radius.

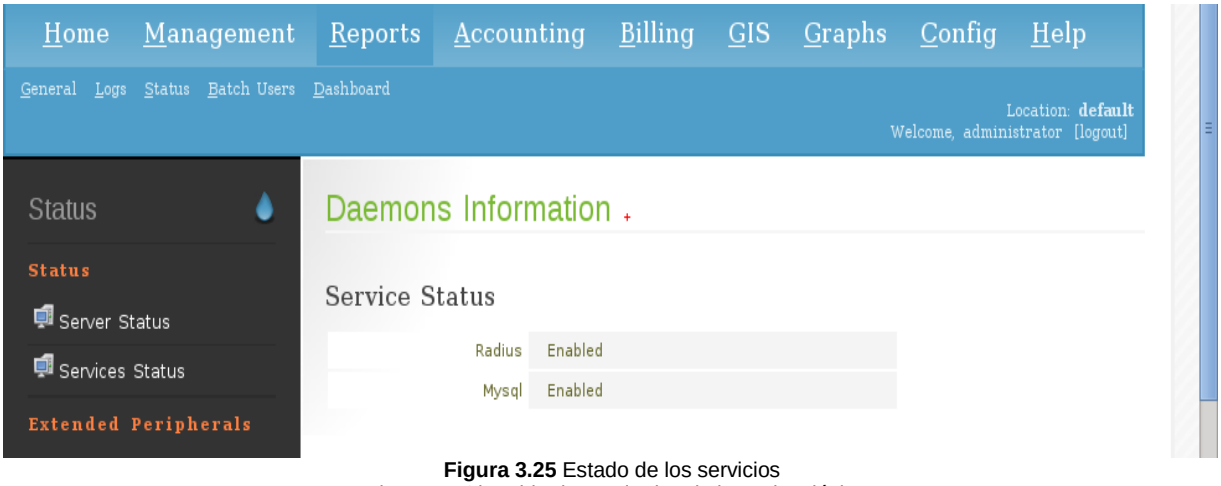
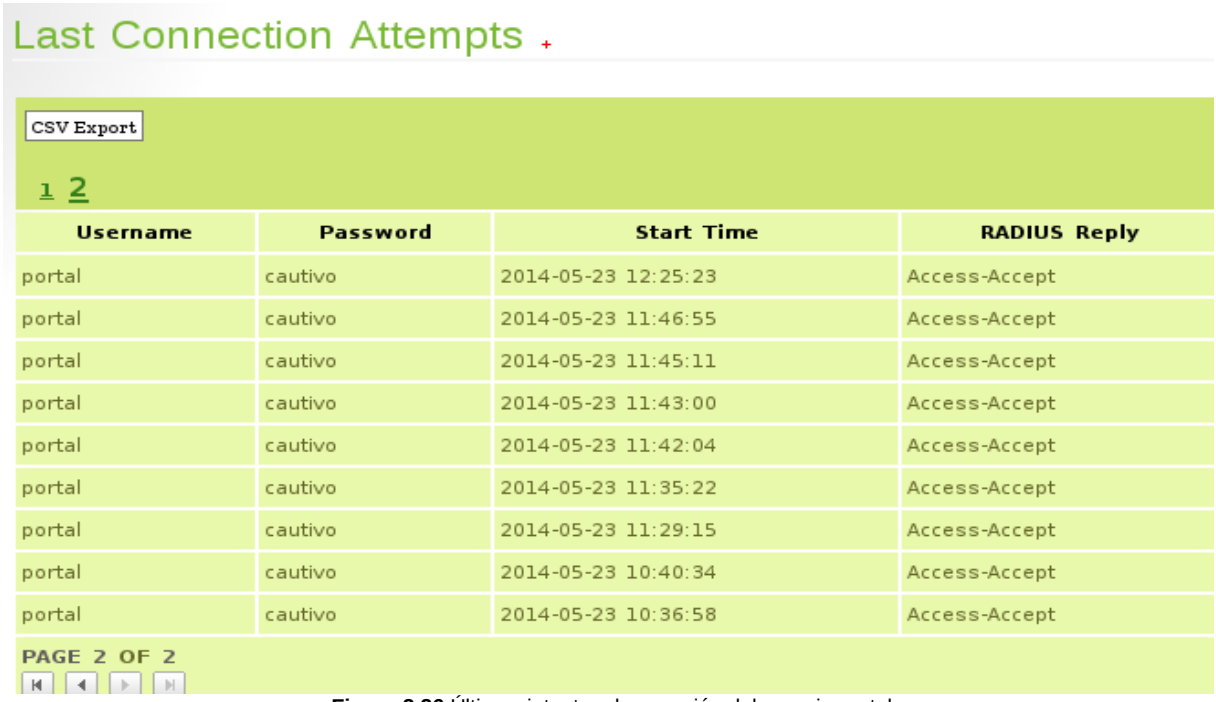


Figura 3.25 Estado de los servicios
(Fuente: Obtenida de resultados de investigación)

Last Connection Attempts: Lista todos los intentos de conexión al servidor Radius de los usuarios que nos interesen, tanto los exitosos como los inicios de sesión fallidos,

en la **figura 3.26** se observa los últimos intentos de conexión del usuario **portal**, así como también se muestra la fecha hora en que se realizó la conexión.



Last Connection Attempts

CSV Export

1 2

Username	Password	Start Time	RADIUS Reply
portal	cautivo	2014-05-23 12:25:23	Access-Accept
portal	cautivo	2014-05-23 11:46:55	Access-Accept
portal	cautivo	2014-05-23 11:45:11	Access-Accept
portal	cautivo	2014-05-23 11:43:00	Access-Accept
portal	cautivo	2014-05-23 11:42:04	Access-Accept
portal	cautivo	2014-05-23 11:35:22	Access-Accept
portal	cautivo	2014-05-23 11:29:15	Access-Accept
portal	cautivo	2014-05-23 10:40:34	Access-Accept
portal	cautivo	2014-05-23 10:36:58	Access-Accept

PAGE 2 OF 2

Figura 3.26 Últimos intentos de conexión del usuario portal
(Fuente: Obtenida de resultados de investigación)

Radius Log: Como se muestra en la **figura 3.27**, en esta parte se muestra el monitoreo de las tareas que ha realizado FreeRADIUS.

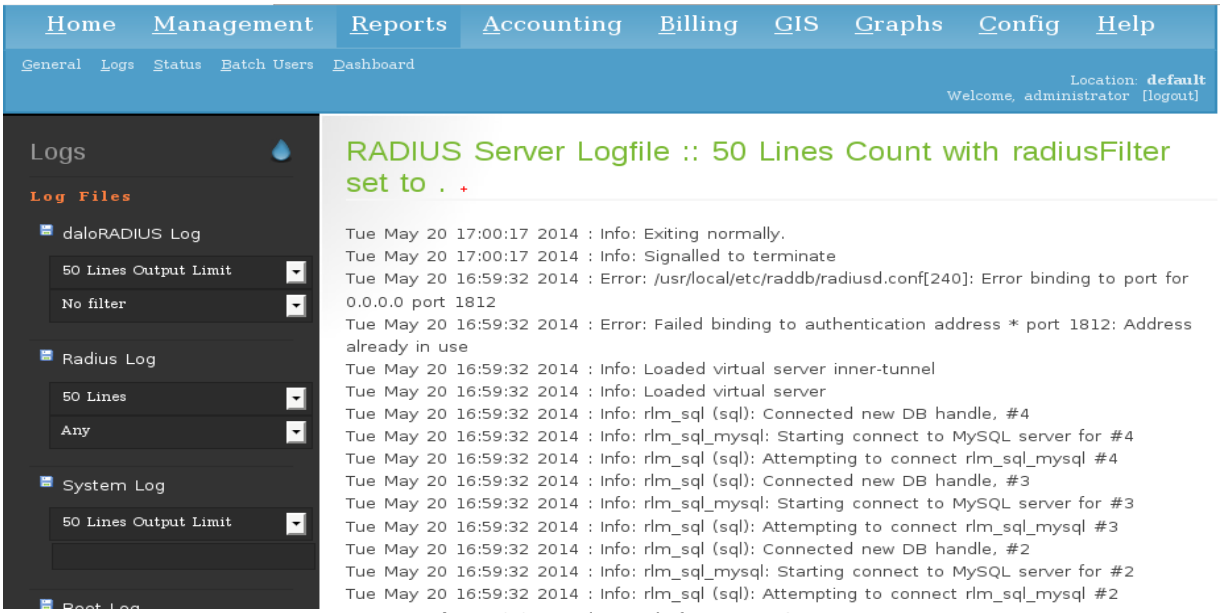


Figura 3.27 Monitoreo de freeRADIUS
(Fuente: Obtenida de resultados de investigación)

daloRADIUS Log: Al dar clic en esta opción, se muestra el archivo de registros de daloRADIUS, muestra los módulos que se han revisado, así como el nombre del operador que realizo las operaciones (ver **figura 3.28**).

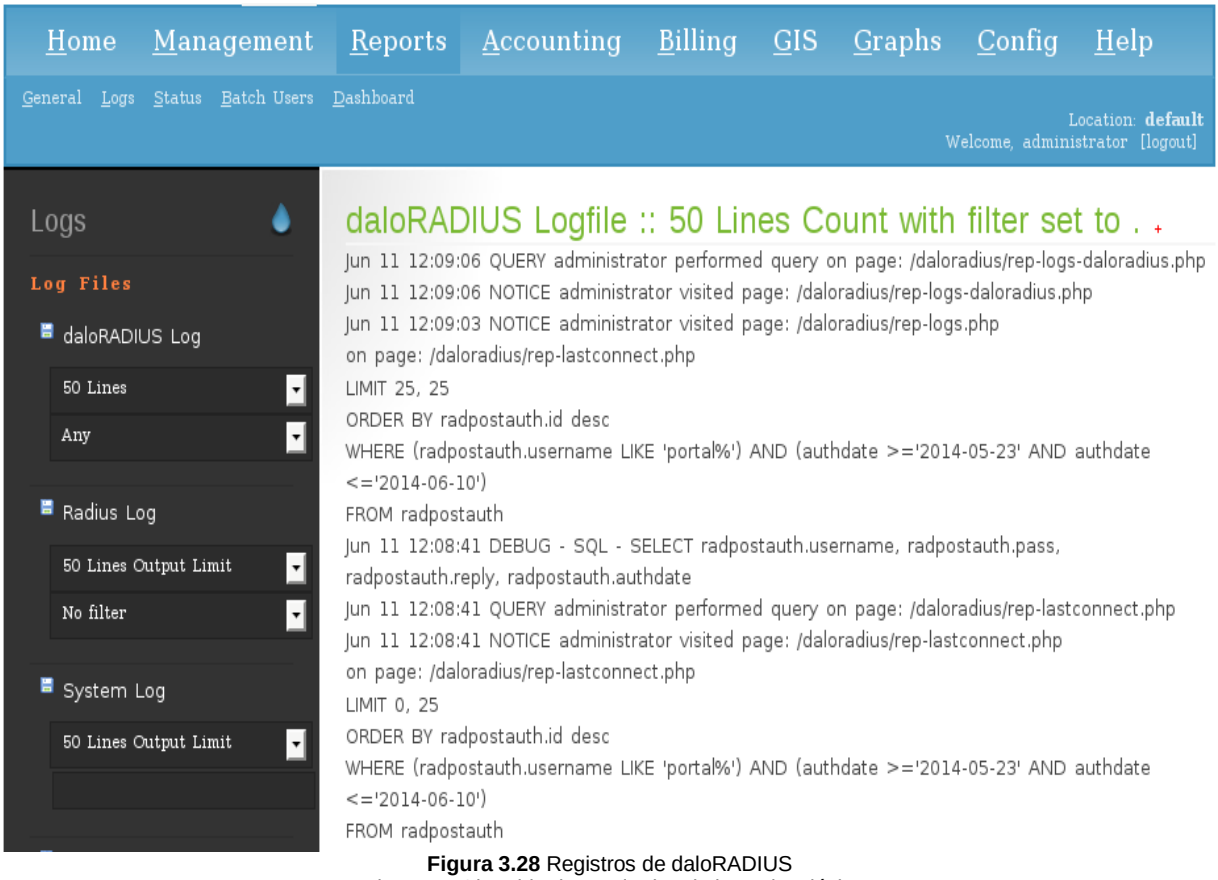


Figura 3.28 Registros de daloRADIUS
(Fuente: Obtenida de resultados de investigación)

A continuación se hablara del apartado de administración, estando situados en esta parte del menú encontrara en la parte izquierda unas opciones como lo es lista de usuarios, agregar usuarios, editar, eliminar, buscar e importar.

Esta es una de las partes importantes de la aplicación pues desde aquí se administrara a los usuarios para tener la gestión de ellos. Una vez hecho clic en la parte de **Management** se verá en la parte central una pequeña gráfica. En ella se lista el total de todos los usuarios registrado en la base de datos, pero esto no quiere decir que todos hayan sido registrados desde la aplicación.

Los usuarios registrados desde la aplicación daloRADIUS se listan al dar clic en **List Users** que se encuentra en la parte izquierda, y nos aparecerá algo similar a la **figura 3.29**.

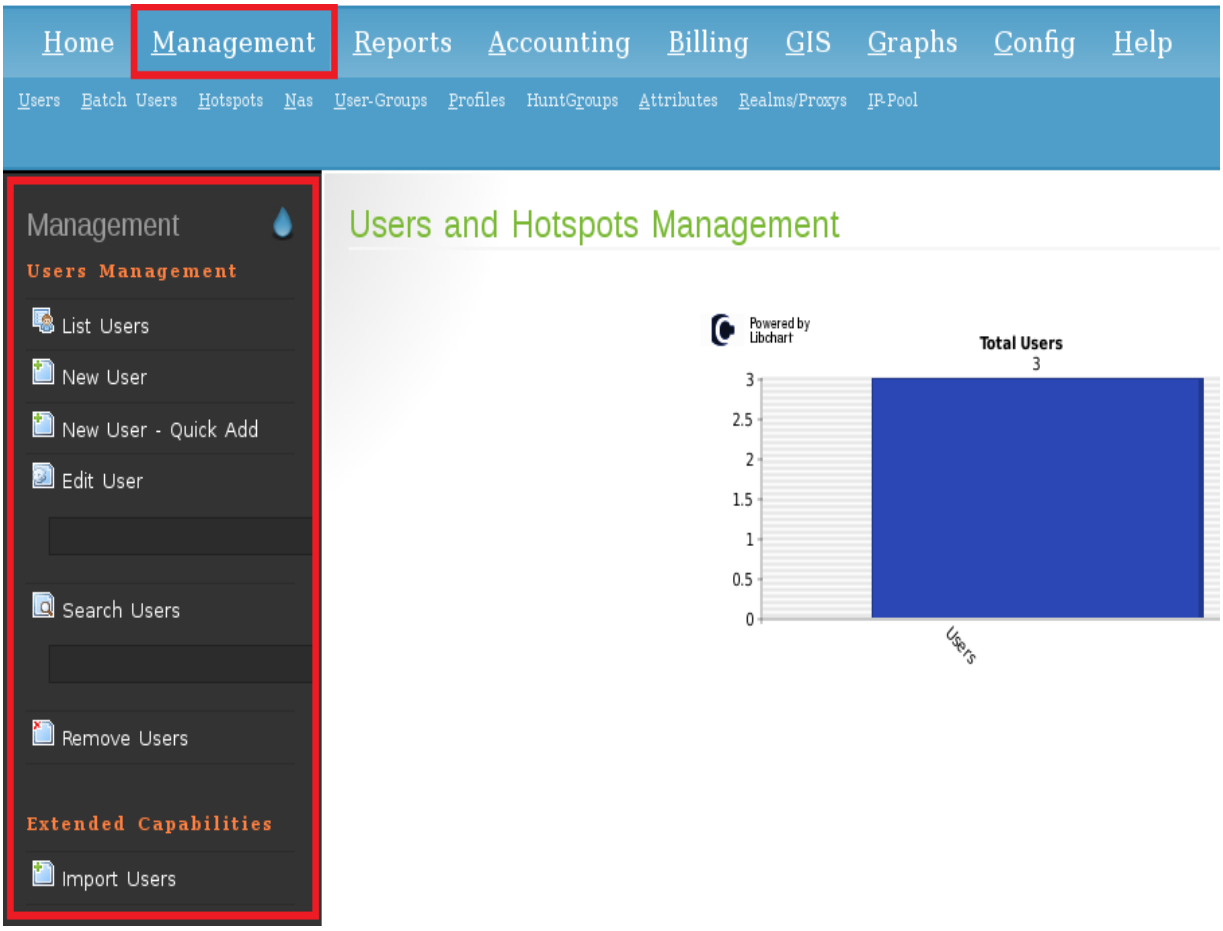


Figura 3.29 Grafica del total de usuarios existentes
(Fuente: Obtenida de resultados de investigación)

Para agregar usuarios hacer los siguientes pasos (Ver **figura 3.30**):

1. - Dar clic en **Management**
2. - Clic en **New User**
3. – Crear nuevo usuario: Para crear un nuevo usuario se puede hacer de dos formas. La primera opción es agregándolo nosotros mismos y la segunda opción es que se genere aleatoriamente, puesto que daloRADIUS nos permite crear nombres de usuarios aleatorios al dar clic en el botón random.

4. - Introducir la contraseña para dicho usuario: Al igual que los usuarios también se pueden crear contraseñas aleatorias o crearlas nosotros mismos.

5. Clic en **Apply** para guardar los cambios

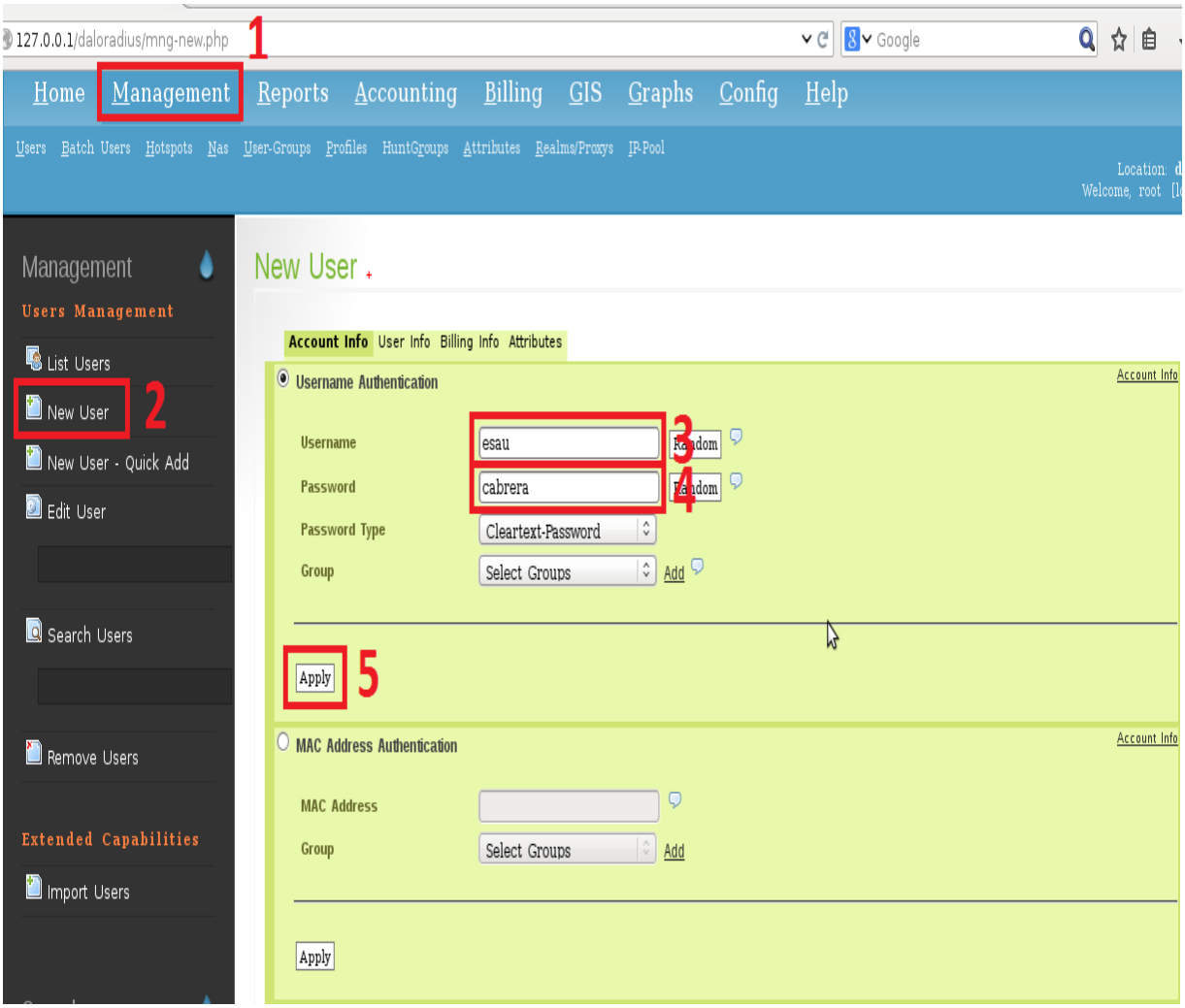


Figura 3.30 Creación de nuevo usuario
(Fuente: Obtenida de resultados de investigación)

Una vez hecho esto ya se ha agregado al usuario en la base de datos y se puede hacer la prueba de conexión al intentar conectarse con el usuario y contraseña que se halla creado o haciendo un test en la consola mientras FreeRADIUS este corriendo en modo debug.

Para verificar que el usuario ya se encuentra registrado, bastara con dar clic en **List Users** como se muestra en la **figura 3.31**, y mostrara la lista de usuarios que ya estén en la base de datos y el que se acaba de agregar desde la aplicación.

Figura 3.31 Listado de usuarios existentes
(Fuente: Obtenida de resultados de investigación)

Para eliminar a uno de los usuarios bastara con hacer los siguientes pasos:

1.- Dar clic en **List Users** para listar a todos los usuarios ya agregados.
2.- Seleccionarlo el usuario a eliminar (se pueden seleccionar varios usuarios o seleccionar todos **ALL**).
3.- Dar clic en **Delete.**

También se puede realizar una eliminación múltiple, es decir, eliminar varios o todos los usuarios que se encuentren registrados, para elimiar todos los usuarios existetes basta con dar clic en **ALL,** en la parte de **SELECT** y luego en **Delete**.

Para tener una idea más clara de lo anterior, podemos observar la **figura 3.32** en la cual se detallan visualmente los pasos para eliminar uno, varios o todos los usuarios que existan en la base de datos.

Figura 3.32 Eliminación de un usuario
(Fuente: Obtenida de resultados de investigación)

Nota:

Se pueden agregar usuarios no solo por nombre y contraseña, sino también por dirección MAC del dispositivo, esto se hace de la misa forma que agregar a un usuario normal, solo que ahora selecciona la siguiente opción (**Figura 3.33**).

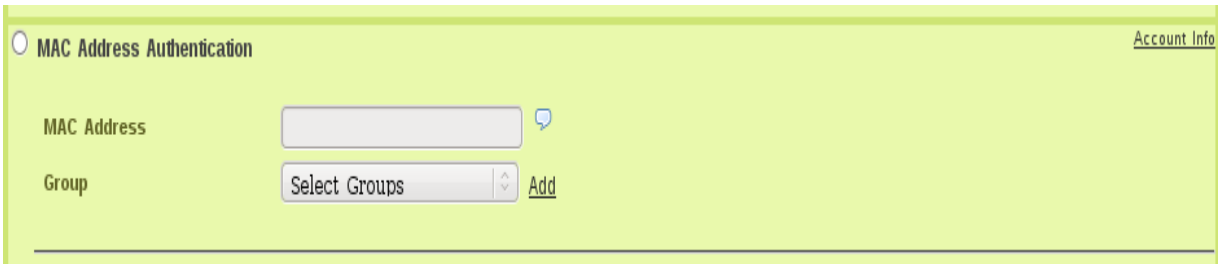


Figura 3.33 Agregar nuevo usuario por dirección MAC
(Fuente: Obtenida de resultados de investigación)

Para pasar al apartado de los reportes y ver sus usos prácticos se hace lo siguiente (Ver **figura 3.34**).

1.- Dar clic en **Reports**

2.- Por defecto en la parte izquierda se despliegan las opciones de las que se pueden hacer uso

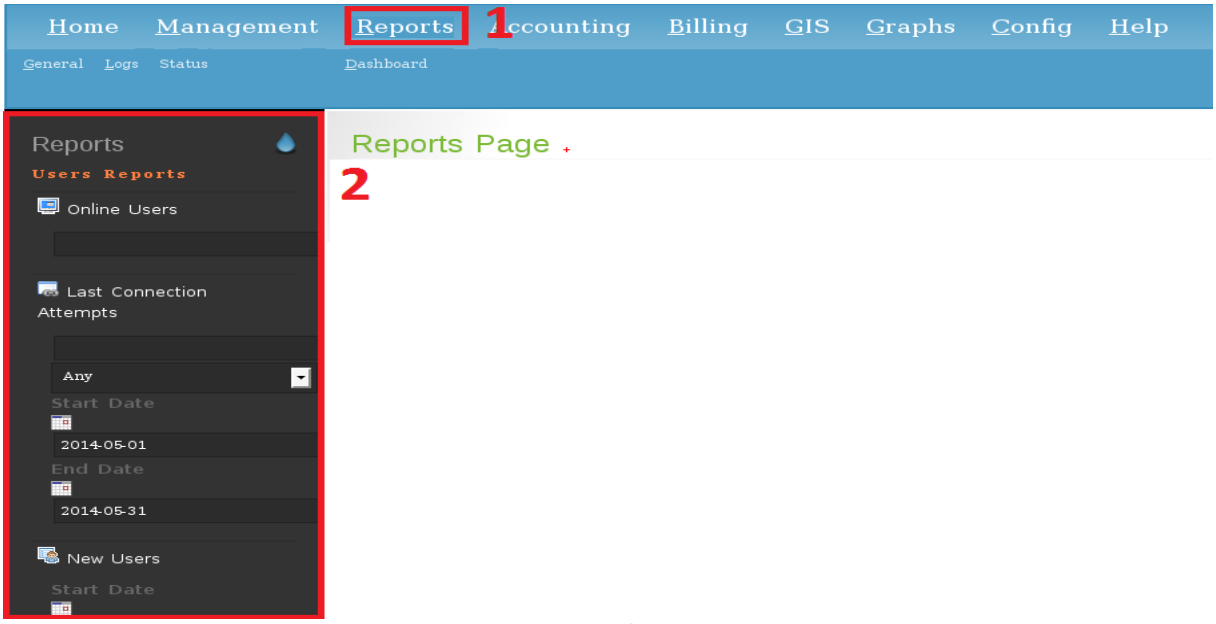


Figura 3.34 Sección de reportes
(Fuente: Obtenida de resultados de investigación)

Las opciones que se describen en el apartado son las siguientes:

Usuarios en línea: Como se muestra en la **figura 3.35**, proporciona una lista de todos los usuarios que se encuentran en línea, a través de la contabilidad en la base de datos.

SELECT: ALL NONE

Clear Sessions | CSV Export

1

Username	Name	IP Address	Start Time	Total Time	HotSpot / NAS Shortname	Total Traffic
portal		IP: 192.168.4.191 MAC: 08-9E-01-BF-74-48	2014-05-20 11:00:01	0 seconds	localhost	Upload: 0 B Download: 0 B Total Traffic:
portal		IP: 172.16.64.2 MAC: 44-87-FC-17-CD-55	2014-05-21 18:55:19	0 seconds	localhost	Upload: 0 B Download: 0 B Total Traffic:

Figura 3.35 Lista de usuarios que están en línea
(Fuente: Obtenida de resultados de investigación)

La comprobación que se realiza, es para los usuarios que no tienen tiempo de finalización (AcctStopTime). Es importante notar que estos usuarios también pueden ser de sesiones antiguas que suceden cuando el NAS por alguna razón deja de enviar los paquetes de contabilidad.

Últimos intentos de conexión: Esta opción nos proporciona una lista de todos los inicios de sesión para los usuarios, tanto los aceptados como los rechazados (Access-Accept, Access-Reject). En la **figura 3.36** se muestran los últimos intentos de conexión del usuario portal.

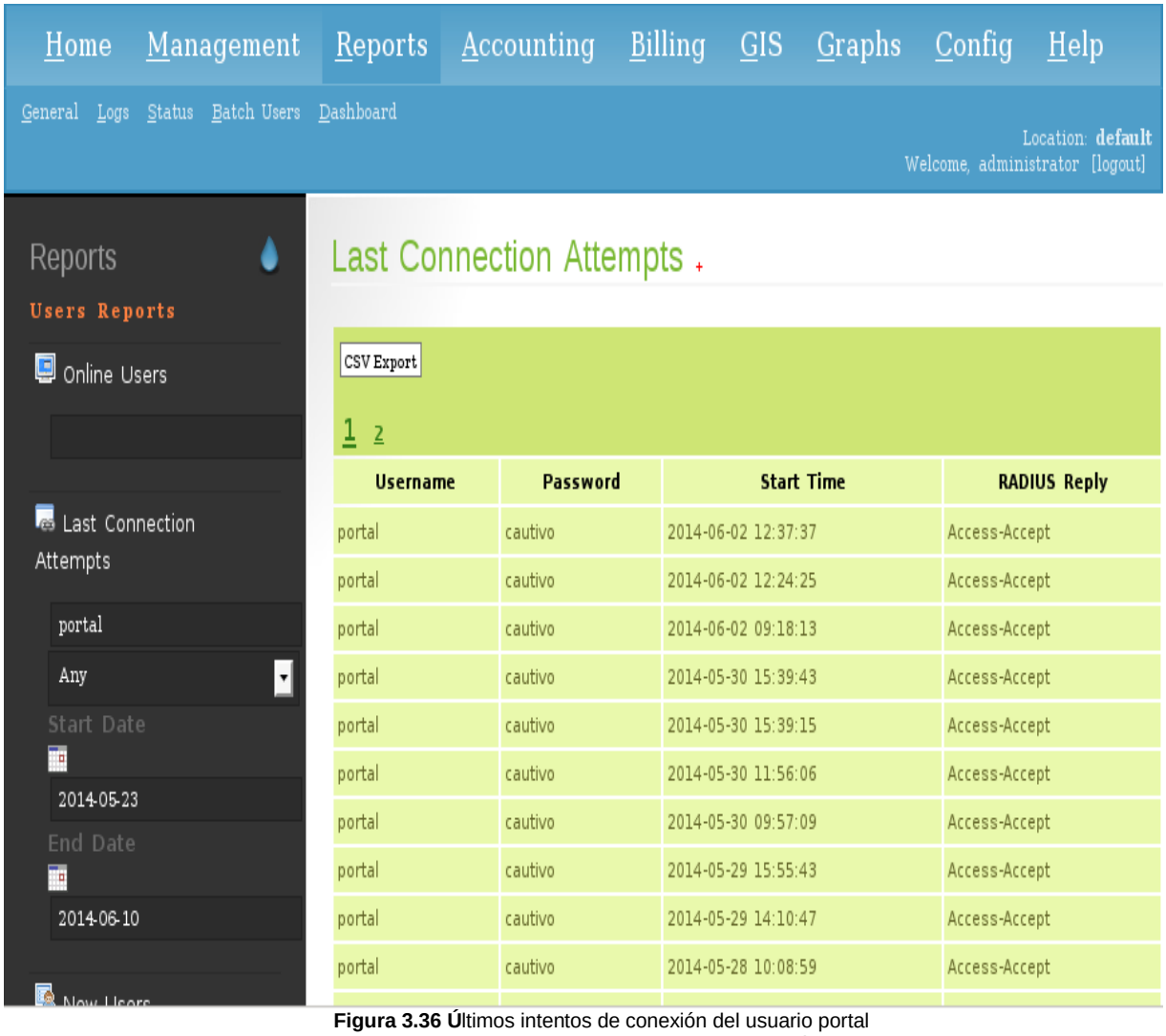


Figura 3.36 Últimos intentos de conexión del usuario portal
(Fuente: Obtenida de resultados de investigación)

Estos datos se extraen de la tabla PostAuth de la base de datos que se requiere para ser definido en el archivo de configuración de FreeRADIUS.

Dentro del menú **Reports**, en la parte de abajo, se observa un submenú que muestra opciones avanzadas, como lo es información general del servidor, información de la memoria, información del disco de almacenamiento y la interfaces de red que tiene el servidor que se esté usando (ver **figura 3.37**).

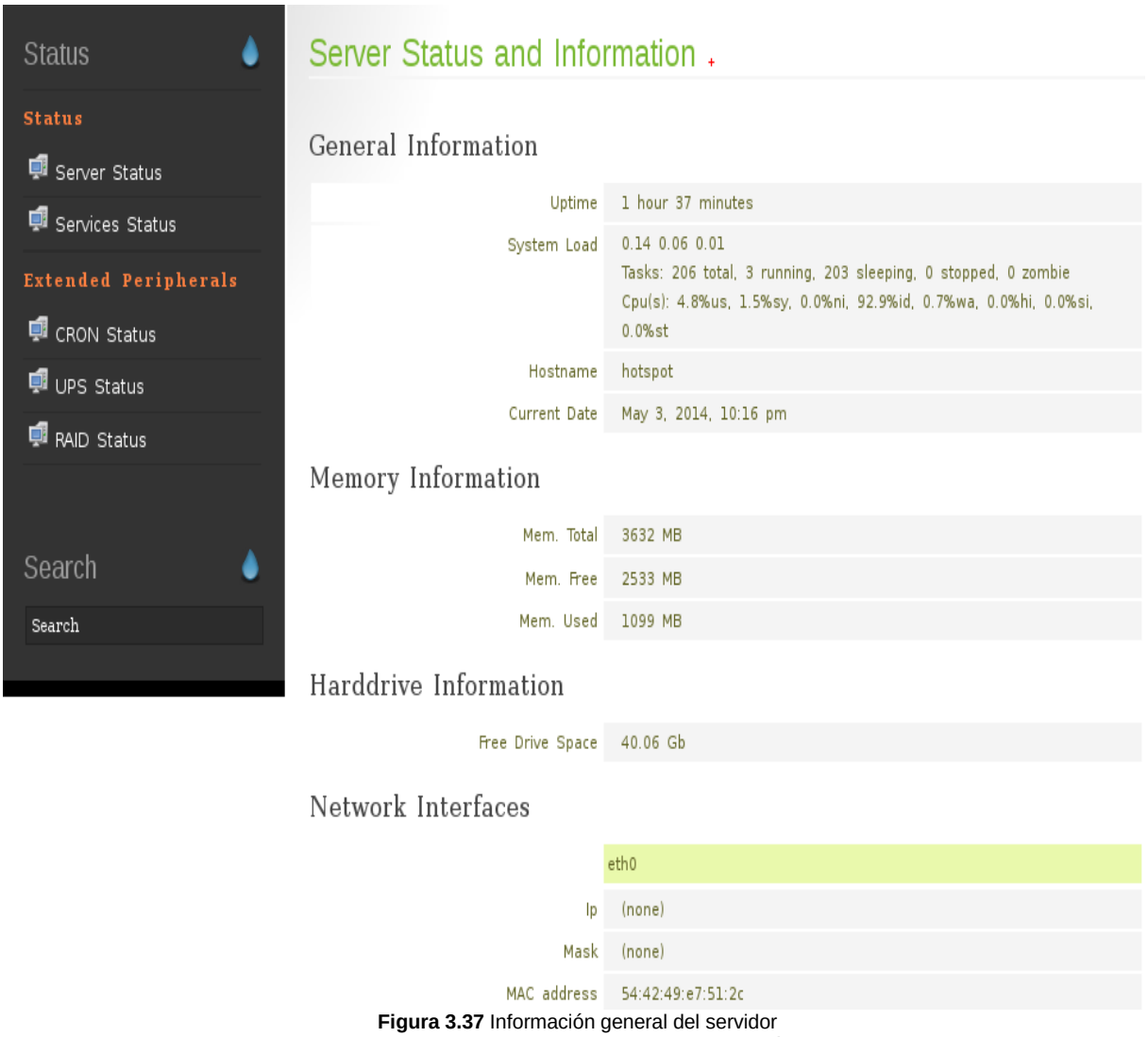


Figura 3.37 Información general del servidor
(Fuente: Obtenida de resultados de investigación)

Como se puede observar en la imagen anterior, este apartado proporciona una rica porción de opciones que se puede aprovechar para verificar el estado del servidor, el

tiempo de conexión, nombre del server, consumo en cuestión de memoria, disco duro, CPU, y ver en qué tarjeta de red se está trabajando. La misma información del apartado de **Home – Server Status.**

El siguiente apartado es contabilidad. Dar clic en **Accounting** como se muestra en la **figura 3.38**, y de la misma manera que los demás, mostrara una descripción de las opciones que contiene.

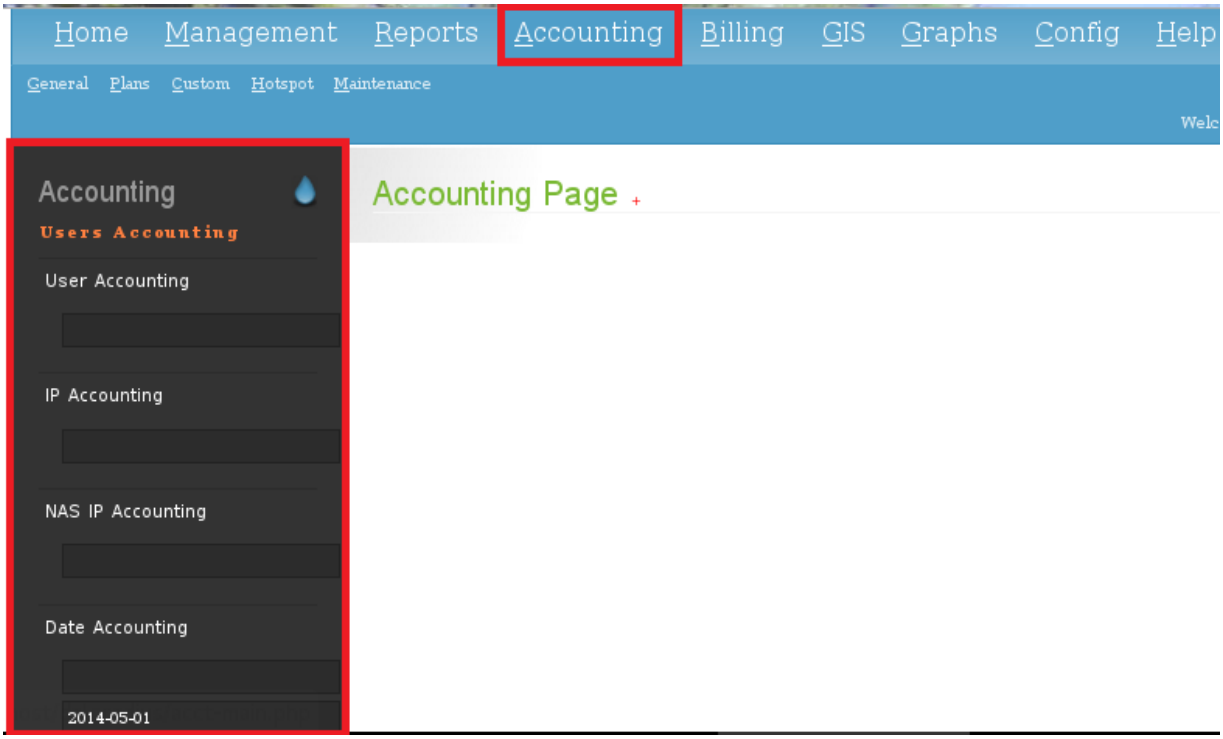
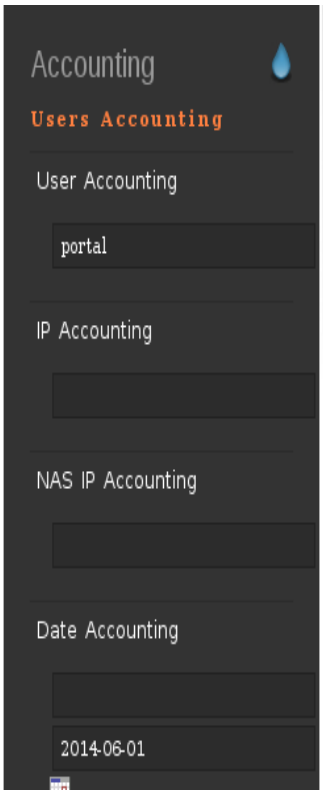


Figura 3.38 Menú Accounting
(Fuente: Obtenida de resultados de investigación)

Contabilidad de usuarios: Este módulo proporciona información contable exhaustiva para todas las sesiones en la base de datos para un usuario en particular, esta sección muestra datos del plan, análisis de la suscripción información de las sesiones del usuario.

Dicha información se puede ver en las **figuras 3.39**, **3.40** y **3.41** respectivamente.



Users Accounting

PLAN INFORMATION

Item	Allowed by plan	Used	Remainning
Session Time	0 seconds	19 days, 6 hours, 11 minutes, 8 seconds	-20 days, -7 hours, -12 minutes, -8 seconds
Session Download	unavailable B	36.48 Gb	
Session Upload	unavailable B	1.95 Gb	

Plan Name	unavailable
Plan Recurring Period	unavailable
Plan Time Type	unavailable
Plan Bandwidth Up	
Plan Bandwidth Down	

SUBSCRIPTION ANALYSIS

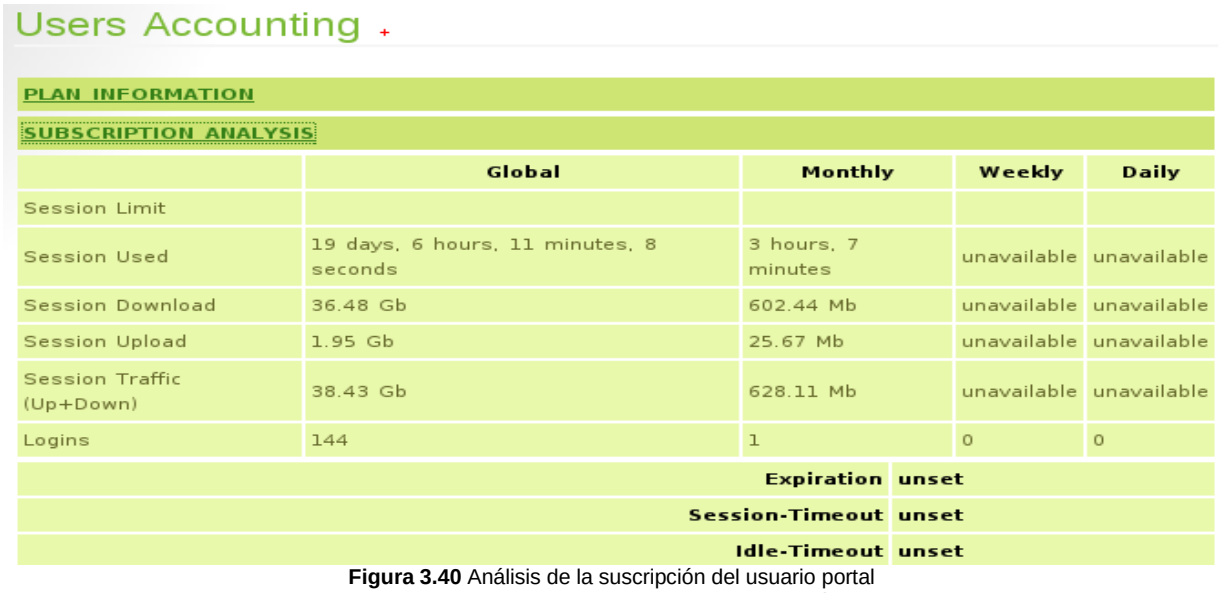
Figura 3.39 Información del plan
(Fuente: Obtenida de resultados de investigación)

La figura anterior muestra los datos de contabilidad del plan que tiene el usuario portal, como es: el tiempo que se ha usado el servicio, la cantidad en Mb del ancho de banda usado para descargas y subida de archivos.

Los datos que se muestran son:

- El tiempo total que estuvo conectado a la red
- La cantidad de datos subidos y descargados
- El total de veces que se inició sesión con el usuario especificado

En la **figura 3.40** se puede apreciar lo mencionado anteriormente con datos reales obtenidos de la implementación de la investigación.



Users Accounting

PLAN INFORMATION

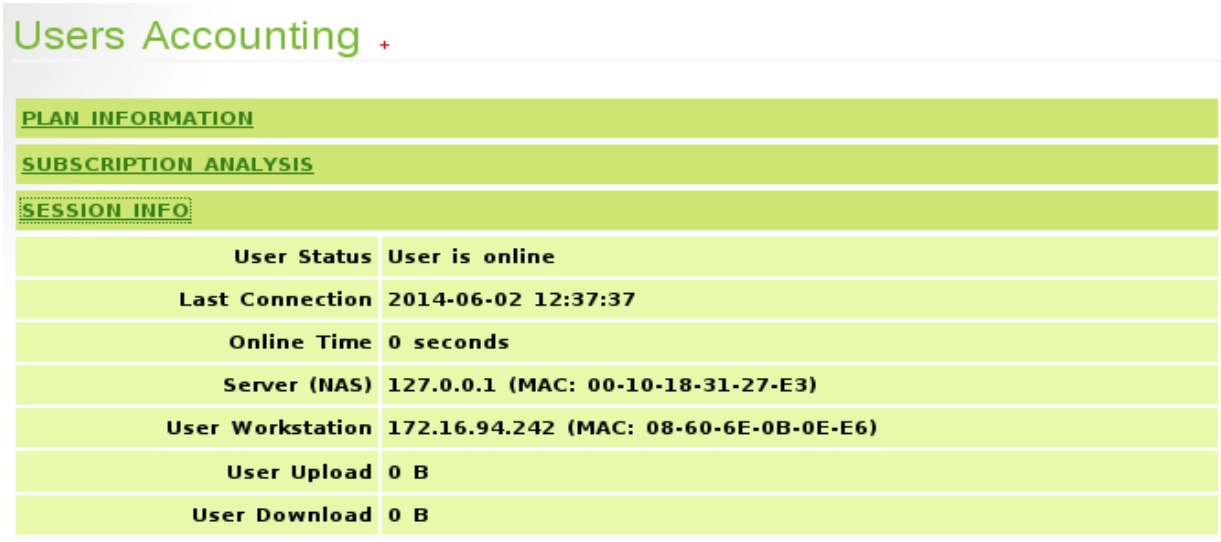
SUBSCRIPTION ANALYSIS

	Global	Monthly	Weekly	Daily
Session Limit				
Session Used	19 days, 6 hours, 11 minutes, 8 seconds	3 hours, 7 minutes	unavailable	unavailable
Session Download	36.48 Gb	602.44 Mb	unavailable	unavailable
Session Upload	1.95 Gb	25.67 Mb	unavailable	unavailable
Session Traffic (Up+Down)	38.43 Gb	628.11 Mb	unavailable	unavailable
Logins	144	1	0	0

Expiration	unset
Session-Timeout	unset
Idle-Timeout	unset

Figura 3.40 Análisis de la suscripción del usuario portal
(Fuente: Obtenida de resultados de investigación)

En la **figura 3.41** se muestra la otra sección del módulo: “users accouting”. En esta sección se muestra datos como; el estatus del usuario, última vez que realiza una conexión.



Users Accounting

PLAN INFORMATION

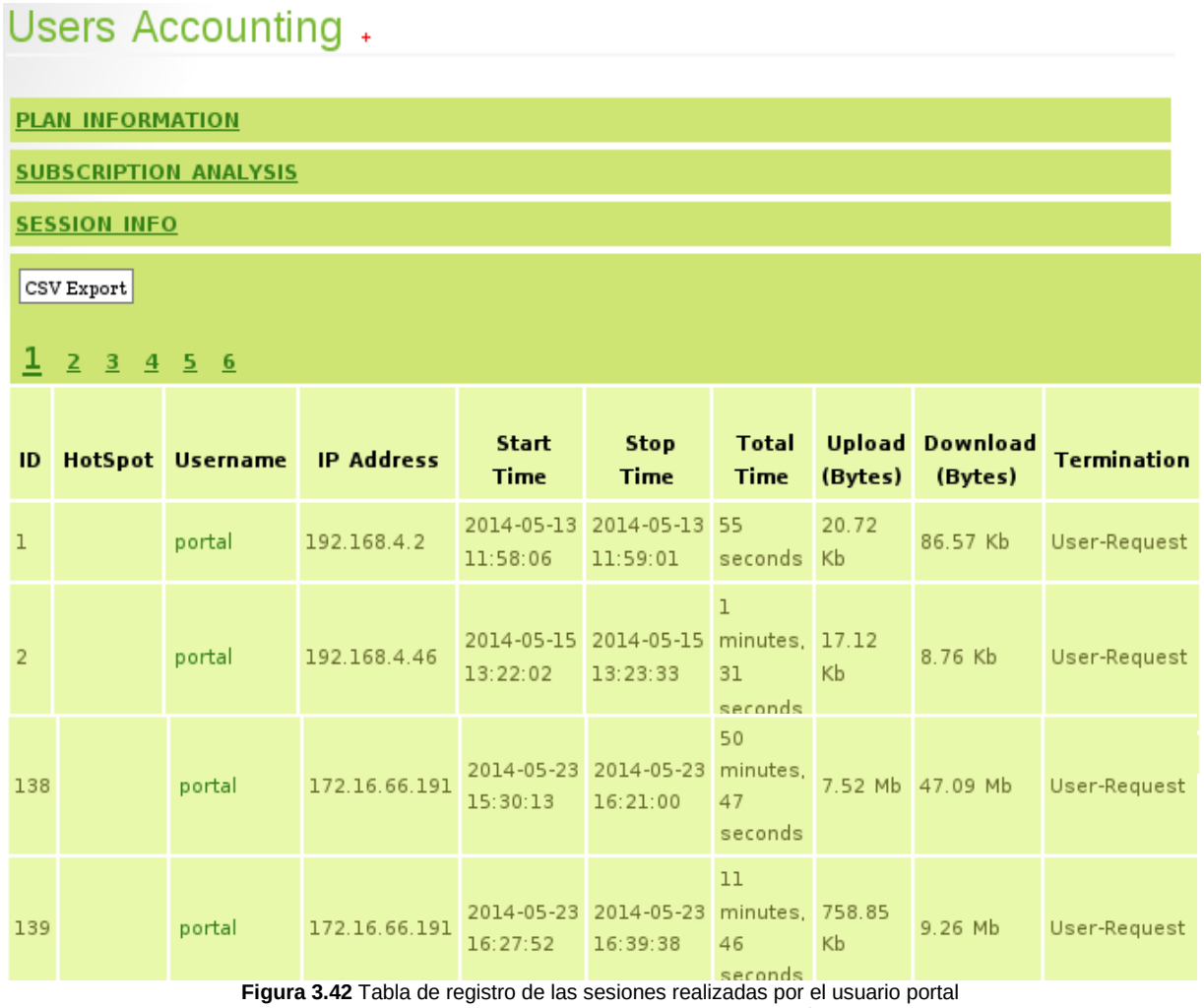
SUBSCRIPTION ANALYSIS

SESSION INFO

User Status	User is online
Last Connection	2014-06-02 12:37:37
Online Time	0 seconds
Server (NAS)	127.0.0.1 (MAC: 00-10-18-31-27-E3)
User Workstation	172.16.94.242 (MAC: 08-60-6E-0B-0E-E6)
User Upload	0 B
User Download	0 B

Figura 3.41 Información de sesión
(Fuente: Obtenida de resultados de investigación)

La **figura 3.42** muestra una tabla con los registros del usuario que nos interese saber. Se muestran datos como: las veces que se conectó, fecha de inicio de sesión y fecha de terminó de la misma, el tiempo que duro la sesión iniciada y la manera en que se terminó la sesión, es decir, si el usuario cerro sesión o la sesión fue terminada por el administrador.



Users Accounting

PLAN INFORMATION

SUBSCRIPTION ANALYSIS

SESSION INFO

CSV Export

1 2 3 4 5 6

ID	HotSpot	Username	IP Address	Start Time	Stop Time	Total Time	Upload (Bytes)	Download (Bytes)	Termination
1		portal	192.168.4.2	2014-05-13 11:58:06	2014-05-13 11:59:01	55 seconds	20.72 Kb	86.57 Kb	User-Request
2		portal	192.168.4.46	2014-05-15 13:22:02	2014-05-15 13:23:33	1 minutes, 31 seconds	17.12 Kb	8.76 Kb	User-Request
138		portal	172.16.66.191	2014-05-23 15:30:13	2014-05-23 16:21:00	50 minutes, 47 seconds	7.52 Mb	47.09 Mb	User-Request
139		portal	172.16.66.191	2014-05-23 16:27:52	2014-05-23 16:39:38	11 minutes, 46 seconds	758.85 Kb	9.26 Mb	User-Request

Figura 3.42 Tabla de registro de las sesiones realizadas por el usuario portal
(Fuente: Obtenida de resultados de investigación)

Contabilidad IP: Proporciona información contable exhaustiva para todas las sesiones que se originó con una dirección IP determinada.

Como se muestra en la **figura 3.43** en el extremo izquierdo del menú se tiene que introducir una dirección IP que queramos consultar y al dar clic en IP Accounting nos mostrara una tabla con los usuarios a los que se les haya asignado esa IP.

Esta opción muestra los mismos datos que la anterior pero en lugar de introducir el nombre de un usuario, introducimos una dirección IP valida, en caso de introducir una IP que no se encuentre dentro del rango de IP´s que proporciona el servidor, no mostrara ninguna información.

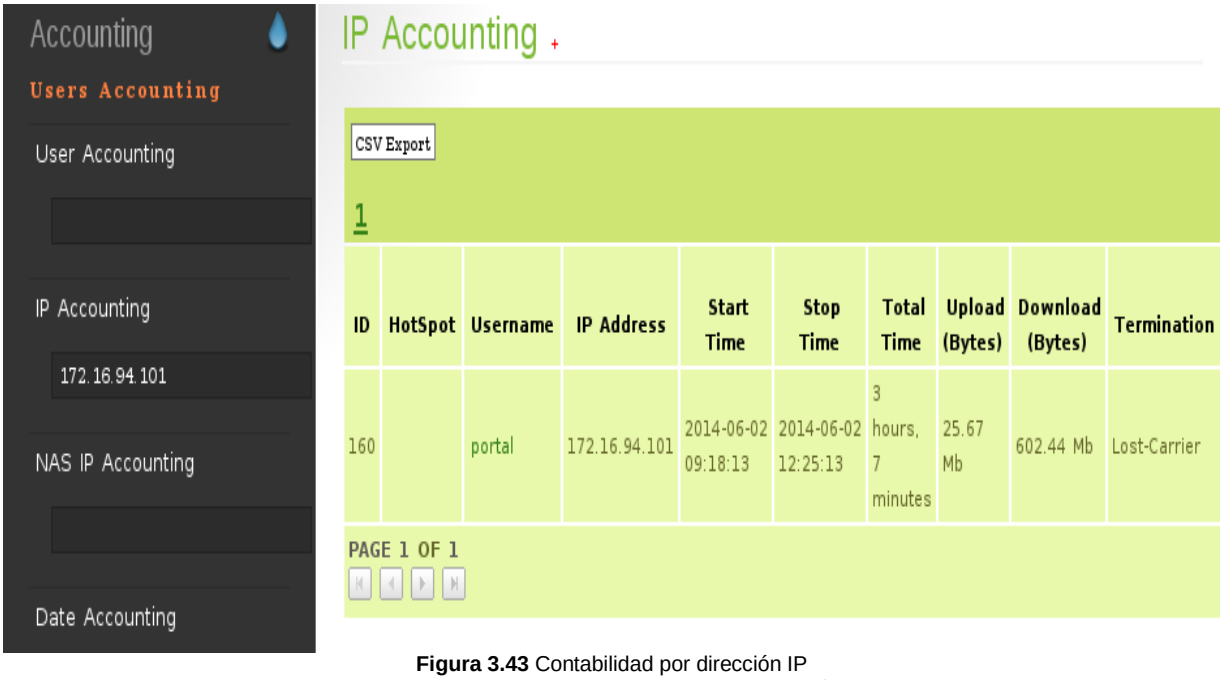
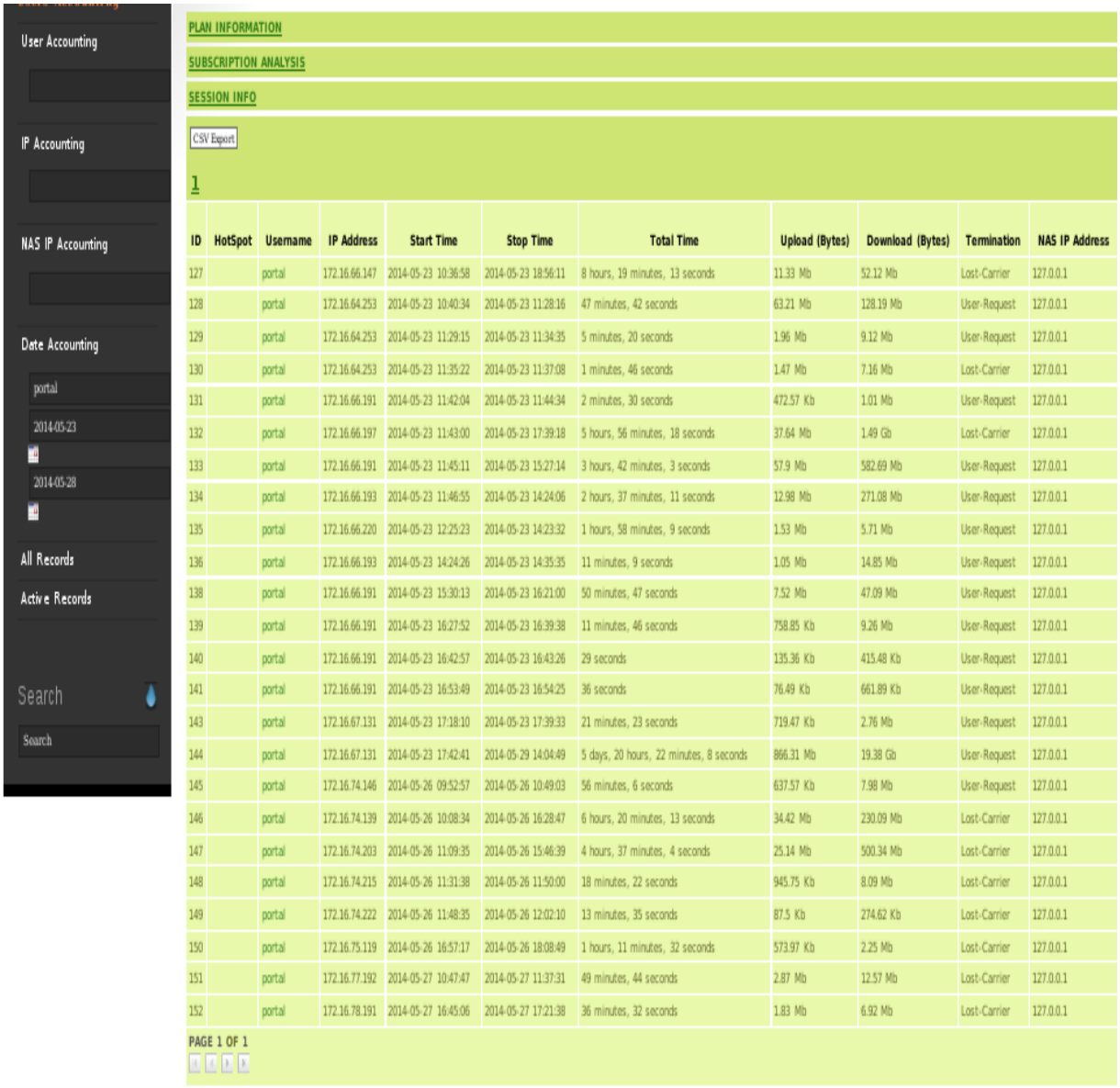


Figura 3.43 Contabilidad por dirección IP
(Fuente: Obtenida de resultados de investigación)

Contabilidad NAS: Proporciona información contable exhaustiva para todas las sesiones que la dirección IP del NAS ha manejado.

Contabilidad por fecha: Proporciona información contable exhaustiva para todas las sesiones entre los que figuran 2 fechas para un usuario en particular (**figura 3.44**).



ID	HotSpot	Username	IP Address	Start Time	Stop Time	Total Time	Upload (Bytes)	Download (Bytes)	Termination	NAS IP Address
127		portal	172.16.66.147	2014-05-23 10:36:58	2014-05-23 18:56:11	8 hours, 19 minutes, 13 seconds	11.33 Mb	52.12 Mb	Lost-Carrier	127.0.0.1
128		portal	172.16.64.253	2014-05-23 10:40:34	2014-05-23 11:28:16	47 minutes, 42 seconds	63.21 Mb	128.19 Mb	User-Request	127.0.0.1
129		portal	172.16.64.253	2014-05-23 11:29:15	2014-05-23 11:34:35	5 minutes, 20 seconds	1.96 Mb	9.12 Mb	User-Request	127.0.0.1
130		portal	172.16.64.253	2014-05-23 11:35:22	2014-05-23 11:37:08	1 minutes, 46 seconds	1.47 Mb	7.16 Mb	Lost-Carrier	127.0.0.1
131		portal	172.16.66.191	2014-05-23 11:42:04	2014-05-23 11:44:34	2 minutes, 30 seconds	472.57 Kb	1.01 Mb	User-Request	127.0.0.1
132		portal	172.16.66.197	2014-05-23 11:43:00	2014-05-23 17:39:18	5 hours, 56 minutes, 18 seconds	37.64 Mb	1.49 Gb	Lost-Carrier	127.0.0.1
133		portal	172.16.66.191	2014-05-23 11:45:11	2014-05-23 15:27:14	3 hours, 42 minutes, 3 seconds	57.9 Mb	582.69 Mb	User-Request	127.0.0.1
134		portal	172.16.66.193	2014-05-23 11:46:55	2014-05-23 14:24:06	2 hours, 37 minutes, 11 seconds	12.98 Mb	271.08 Mb	User-Request	127.0.0.1
135		portal	172.16.66.220	2014-05-23 12:25:23	2014-05-23 14:23:32	1 hours, 58 minutes, 9 seconds	1.53 Mb	5.71 Mb	User-Request	127.0.0.1
136		portal	172.16.66.193	2014-05-23 14:24:26	2014-05-23 14:35:35	11 minutes, 9 seconds	1.05 Mb	14.85 Mb	User-Request	127.0.0.1
138		portal	172.16.66.191	2014-05-23 15:30:13	2014-05-23 16:21:00	50 minutes, 47 seconds	7.52 Mb	47.09 Mb	User-Request	127.0.0.1
139		portal	172.16.66.191	2014-05-23 16:27:52	2014-05-23 16:39:38	11 minutes, 46 seconds	758.85 Kb	9.26 Mb	User-Request	127.0.0.1
140		portal	172.16.66.191	2014-05-23 16:42:57	2014-05-23 16:43:26	29 seconds	135.36 Kb	415.48 Kb	User-Request	127.0.0.1
141		portal	172.16.66.191	2014-05-23 16:53:49	2014-05-23 16:54:25	36 seconds	76.49 Kb	661.89 Kb	User-Request	127.0.0.1
143		portal	172.16.67.131	2014-05-23 17:18:10	2014-05-23 17:39:33	21 minutes, 23 seconds	719.47 Kb	2.76 Mb	User-Request	127.0.0.1
144		portal	172.16.67.131	2014-05-23 17:42:41	2014-05-29 14:04:49	5 days, 20 hours, 22 minutes, 8 seconds	866.31 Mb	19.38 Gb	User-Request	127.0.0.1
145		portal	172.16.74.146	2014-05-26 09:52:57	2014-05-26 10:49:03	56 minutes, 6 seconds	637.57 Kb	7.98 Mb	User-Request	127.0.0.1
146		portal	172.16.74.139	2014-05-26 10:08:34	2014-05-26 16:28:47	6 hours, 20 minutes, 13 seconds	34.42 Mb	230.09 Mb	Lost-Carrier	127.0.0.1
147		portal	172.16.74.203	2014-05-26 11:09:35	2014-05-26 15:46:39	4 hours, 37 minutes, 4 seconds	25.14 Mb	500.34 Mb	Lost-Carrier	127.0.0.1
148		portal	172.16.74.215	2014-05-26 11:31:38	2014-05-26 11:50:00	18 minutes, 22 seconds	945.75 Kb	8.09 Mb	Lost-Carrier	127.0.0.1
149		portal	172.16.74.222	2014-05-26 11:48:35	2014-05-26 12:02:10	13 minutes, 35 seconds	87.5 Kb	274.62 Kb	Lost-Carrier	127.0.0.1
150		portal	172.16.75.119	2014-05-26 16:57:17	2014-05-26 18:08:49	1 hours, 11 minutes, 32 seconds	573.97 Kb	2.25 Mb	Lost-Carrier	127.0.0.1
151		portal	172.16.77.192	2014-05-27 10:47:47	2014-05-27 11:37:31	49 minutes, 44 seconds	2.87 Mb	12.57 Mb	Lost-Carrier	127.0.0.1
152		portal	172.16.78.191	2014-05-27 16:45:06	2014-05-27 17:21:38	36 minutes, 32 seconds	1.83 Mb	6.92 Mb	Lost-Carrier	127.0.0.1

PAGE 1 OF 1

Figura 3.44 Contabilidad de un usuario por fecha
(Fuente: Obtenida de resultados de investigación)

En la imagen anterior se muestra un ejemplo de contabilidad del usuario portal, en el cual se tiene que introducir una fecha de inicio y una fecha final para que nos muestre los registros de ese usuario comprendidos entre las fechas que se hayan introducido.

Todos los registros de contabilidad: Proporciona información contable exhaustiva para todas las sesiones en la base de datos.

Contabilidad de Registros Activos: Proporciona información que resulte útil para el seguimiento de los usuarios activos o caducados en la base de datos en términos de usuarios que tienen un atributo de caducidad o un atributo Max-All-Session.

Para ver un ejemplo de cómo es que funciones se hacen los siguientes pasos (ver **figura 3.45**).

1.- Clic en **Accounting**

2.- Introducir el usuario del cual se requiere saber información, y luego dar clic en **User Accounting.**

3.- Se observa información muy relevante del usuario, IP, fecha de inicio, fecha fin de sesión, tiempo en conexión, descargas… y otras opciones más.

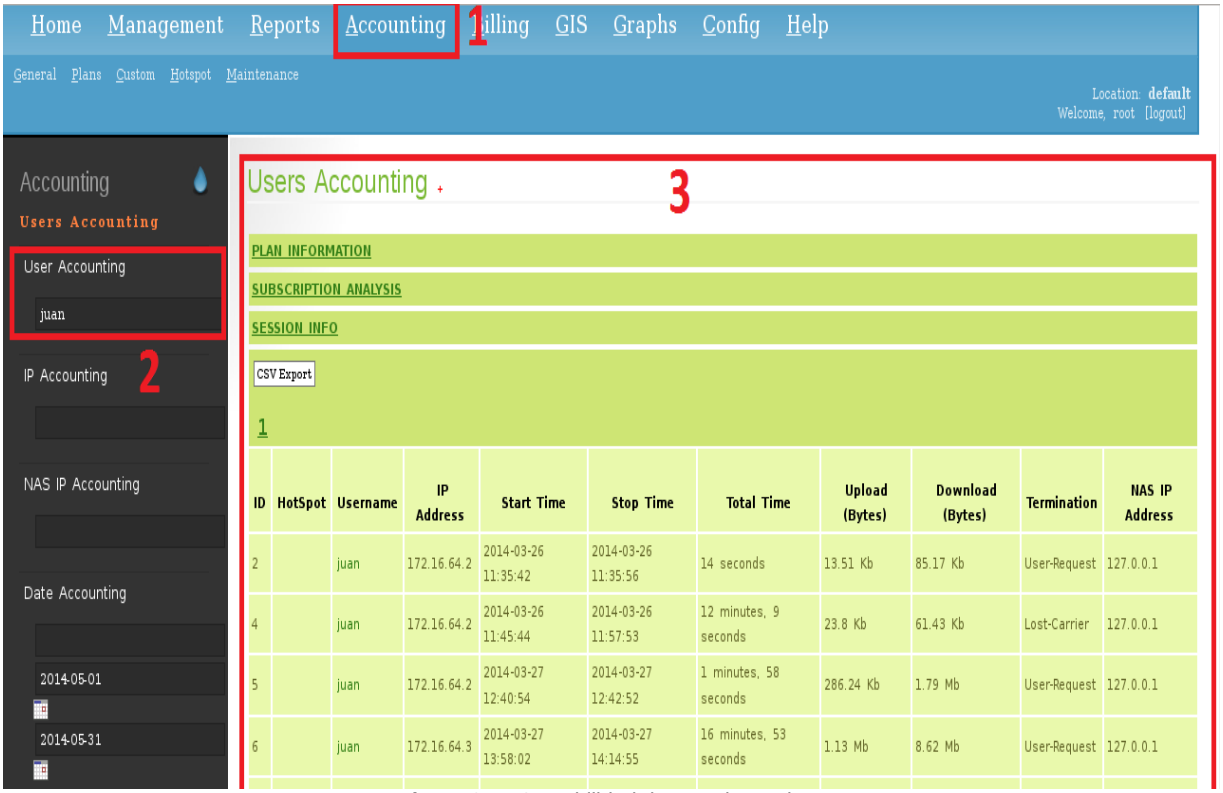


Figura 3.45 Contabilidad de usuarios activos
(Fuente: Obtenida de resultados de investigación)

El siguiente apartado es **Billing** y se muestra en la **figura 3.46**, se utiliza principalmente en lugares donde se pretende cobrar el tiempo de conexión de los usuarios, por tiempo, por consumo o por otras variables ya que daloRADIUS proporciona toda esta información.

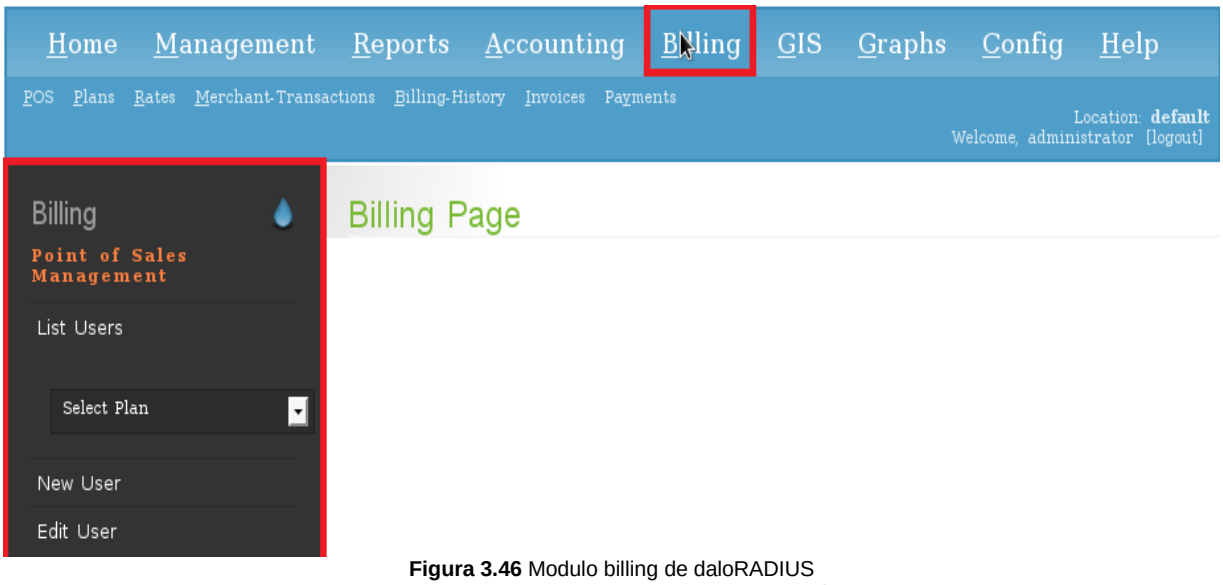


Figura 3.46 Modulo billing de daloRADIUS
(Fuente: Obtenida de resultados de investigación)

En la sección de GIS, tendremos la localización de los puntos de puntos de acceso / acceso visual y muchas más características (Siempre y cuando se agreguen dichas características (ver **figura 3.47**).

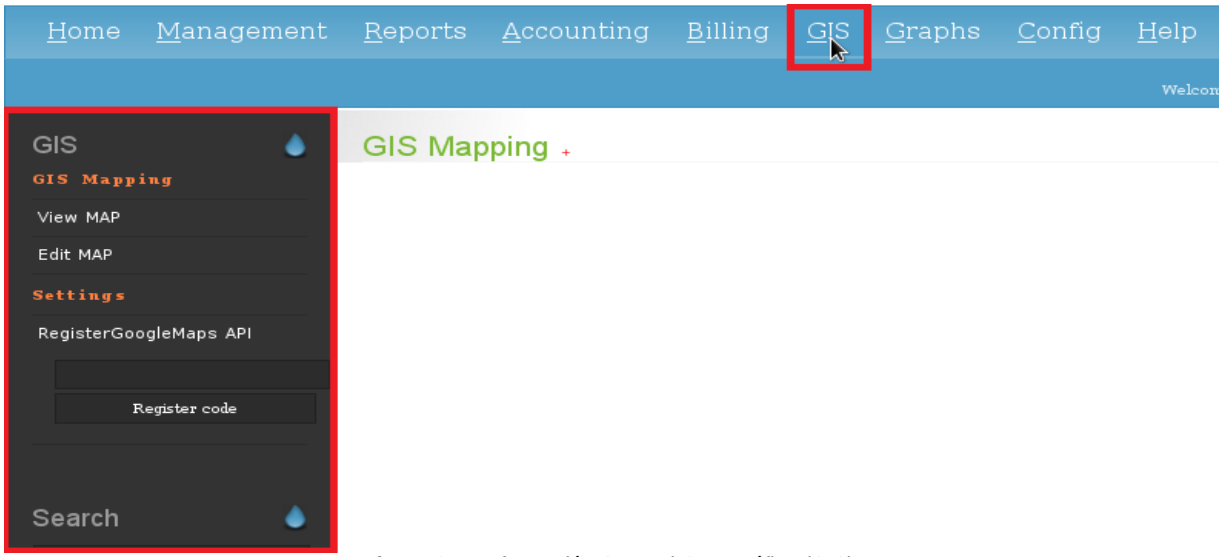


Figura 3.47 Información General Cartográfica (GIS)
(Fuente: Obtenida de resultados de investigación)

Información general Cartografía GIS proporciona asignaciones visuales del punto de conexión a través de un mapa del mundo que utiliza GoogleMaps API.

En la página de Administración son capaces de añadir nuevas entradas de zona interactiva para la base de datos, donde también hay un campo llamado Geolocalización, este es el valor numérico que la API de Google Maps utiliza con el fin de precisar la ubicación exacta de ese punto de acceso en el mapa.

En la opción de GIS hay 2 Modos de funcionamiento disponibles:

Modo Vista: esta opción nos permite la "navegación" a través del mapa del mundo y ver las ubicaciones actuales de los puntos de acceso en la base de datos.

Editar MAP - que es el modo que se puede utilizar con el fin para crear hotspot visibles simplemente haciendo clic sobre el mapa o la eliminación de entradas de punto de acceso existentes por las banderas de hotspot existentes en el botón izquierdo.

Otra cuestión importante es que cada equipo de la red requiere un código de registro único que se puede obtener de la página de Google Maps API, proporcionando la dirección web completa al directorio alojado de aplicación daloRADIUS en su servidor. Una vez que haya obtenido el código de Google, simplemente pegarlo en el cuadro de registro y haga clic en el botón "Registrar código" para escribirlo. Entonces usted puede ser capaz de utilizar los servicios de Google Maps.

Graphs es el apartado donde podremos hacer ver registros de los usuarios que nos interesen, en esta sección hay varias opciones para realizar las consultas que queremos, en estas consultas que hagamos se nos proporciona una tabla y una gráfica con la información que queremos.

En este apartado de **Graphs** se pueden hacer graficas a partir de los datos obtenidos en la sección de contabilidad sobre los usuarios para tener una información más clara, la información de las opciones las podemos observar a continuación.

Overal Logins / Hits. Proporciona una gráfica del uso de un usuario concreto por un período determinado de tiempo. La cantidad de inicios de sesión (o "hits" al NAS) se muestran en una gráfica (**figura 3.48**), así como acompañado de una lista de tabla.

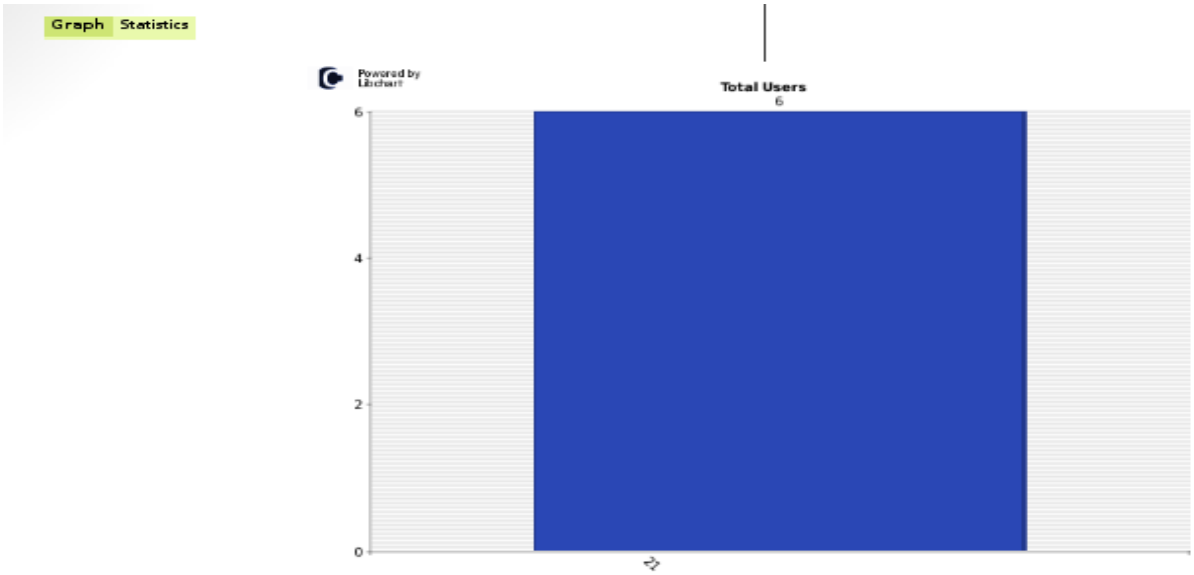


Figura 3.48 Inicios de sesión realizados por un usuario en un día especifico
(Fuente: Obtenida de resultados de investigación)

Al dar clic en la pestaña estatistics en la parte superior izquierda se nos muestra una tabla con los datos numéricos relacionados con la gráfica anterior (**figura 3.49**).

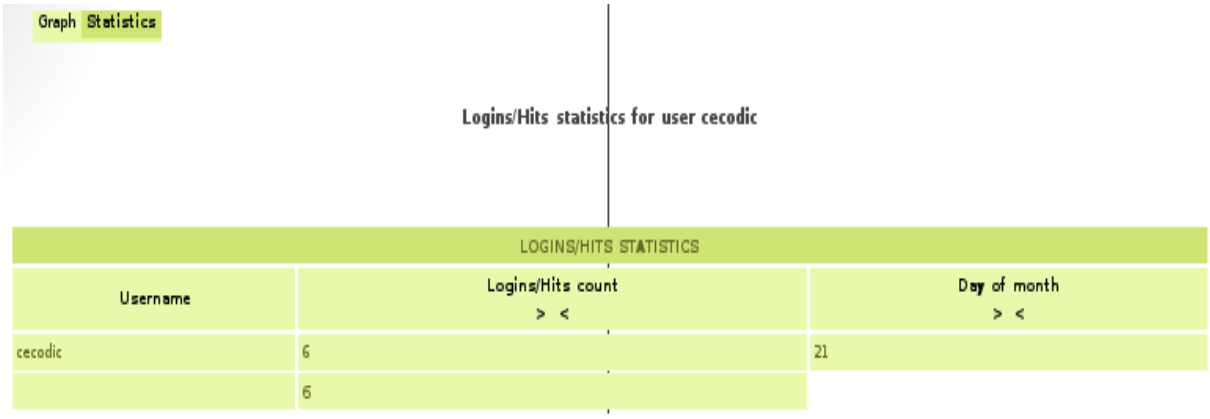


Figura 3.49 Sesiones iniciadas por el usuario cecodic el día 21
(Fuente: Obtenida de resultados de investigación)

Overal Downloads Statistics. Proporciona una gráfica del uso de un usuario concreto por un período determinado de tiempo. La cantidad de datos descargados por el cliente es el valor que se está calculando.

La gráfica está acompañada de un listado de tablas, en las **figuras 3.50** y **3.51** se muestra la gráfica y la tabla, respectivamente.

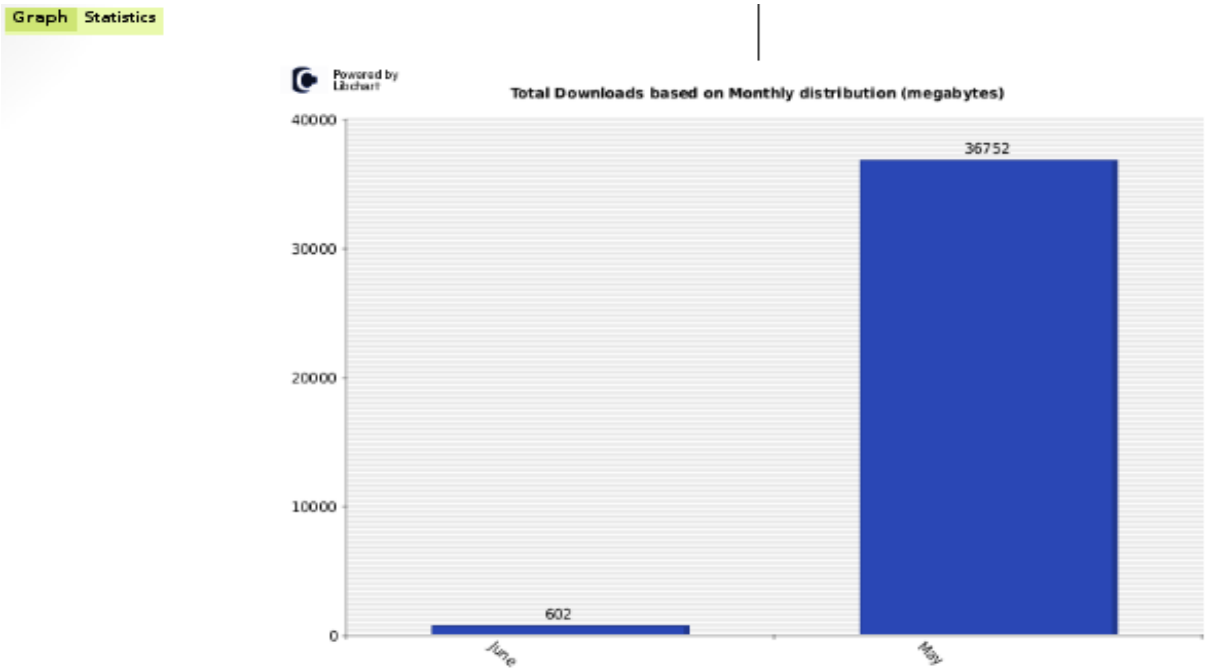


Figura 3.50 Grafica del total de datos descargados
(Fuente: Obtenida de resultados de investigación)

Graph Statistics

ALL-TIME DOWNLOAD STATISTICS

Downloads count in MB > <	Month of year > <
36752	May
602	June
37354	

Figura 3.51 Datos numéricos del total de datos descargados
(Fuente: Obtenida de resultados de investigación)

Overal Uploads Statistics. Proporciona una gráfica del uso de un usuario concreto por un período determinado de tiempo. La cantidad de carga de datos por parte del cliente es el valor que se está calculando. La gráfica está acompañado de un listado tablas, las cuales lo podemos ver en las **figuras 3.52** y **3.53**, respectivamente.

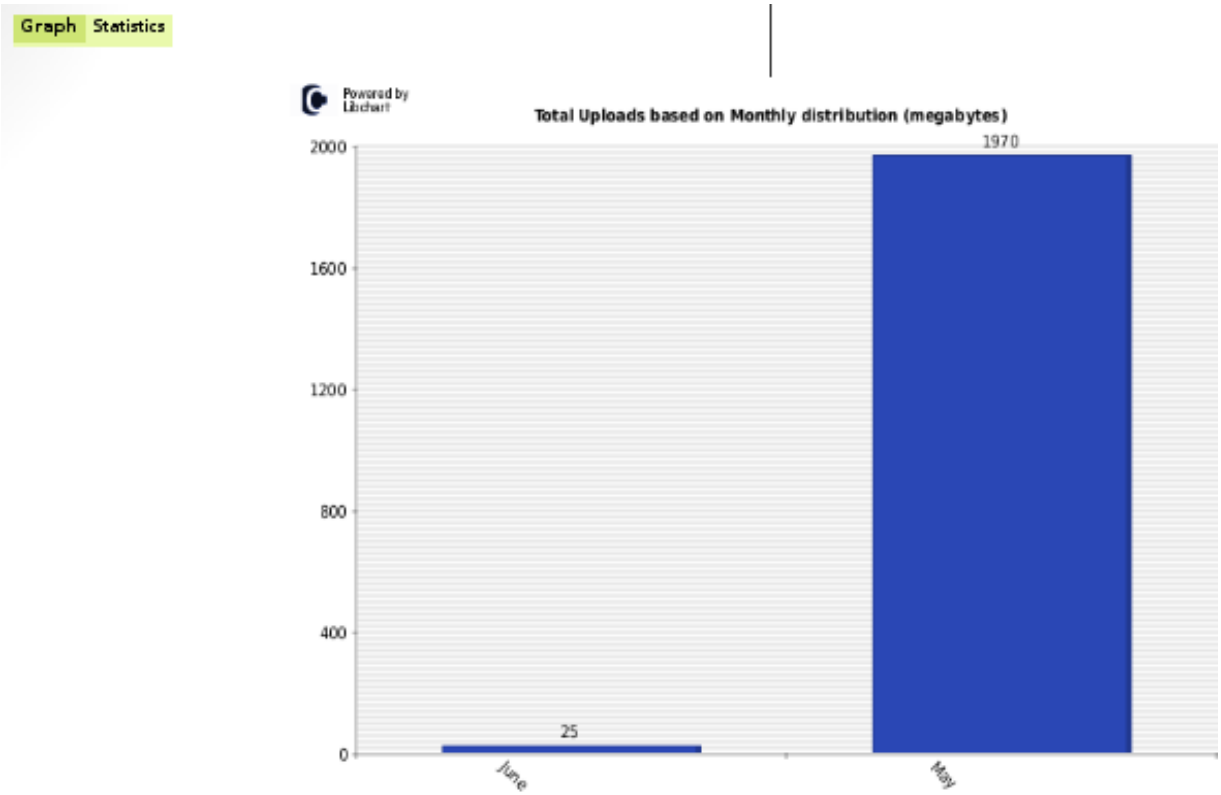


Figura 3.52 Grafica del total de datos cargados (subidos)
(Fuente: Obtenida de resultados de investigación)

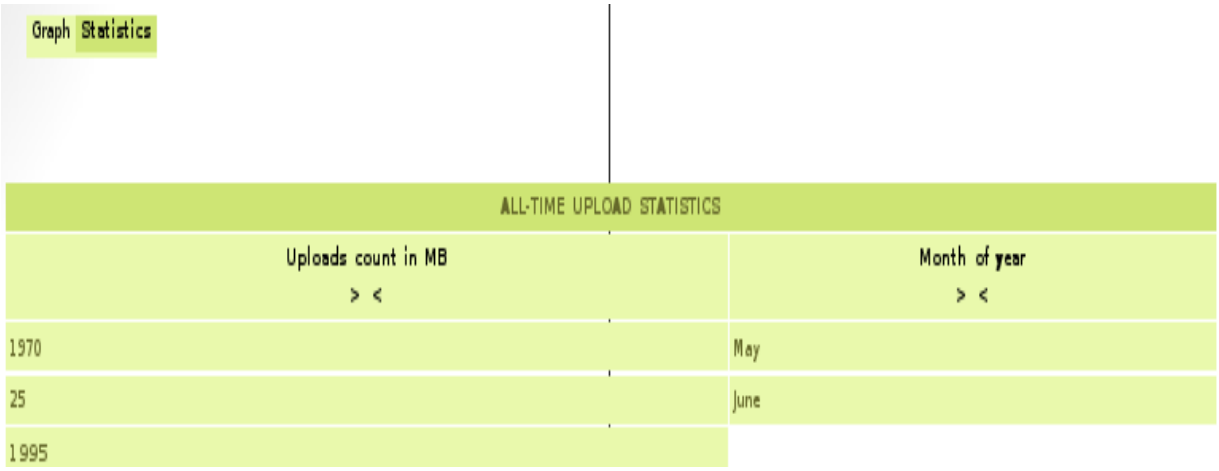


Figura 3.53 Datos numéricos del total de datos cargados (subidos).
(Fuente: Obtenida de resultados de investigación)

Alltime Logins / Hits. Proporciona una gráfica de los inicios de sesión en el servidor durante un período determinado de tiempo, en las **figuras 3.54** y **3.55** se muestra la gráfica y la tabla de los inicios de sesión distribuidos por mes.

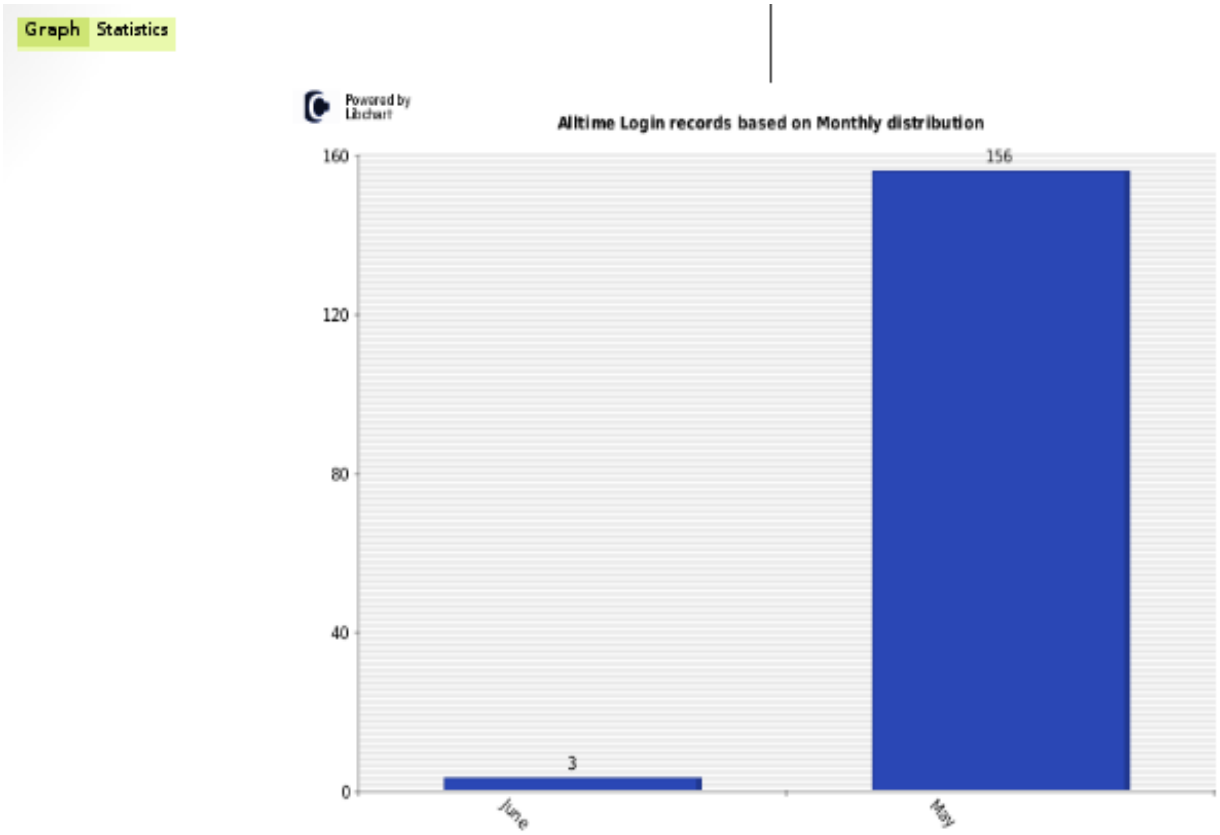


Figura 3.54 Grafica de los inicios de sesión, distribuidos por mes
(Fuente: Obtenida de resultados de investigación)

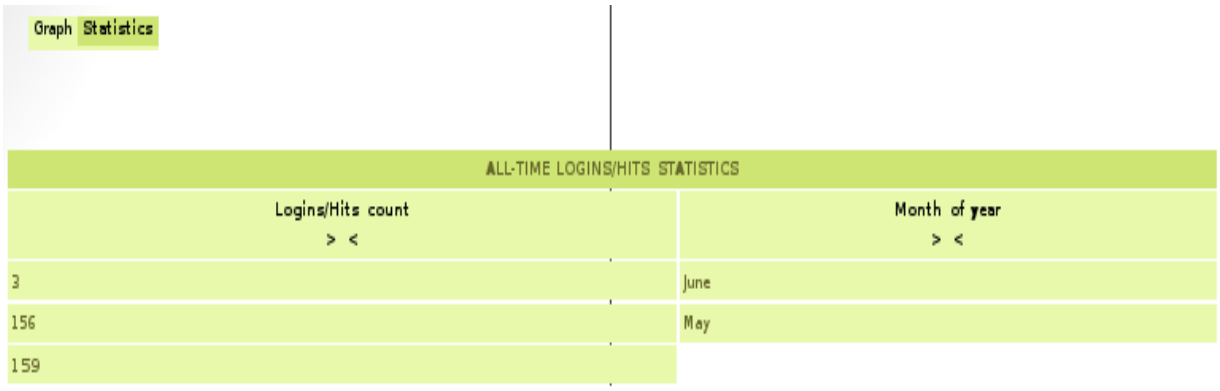


Figura 3.55 Datos numéricos de los inicios de sesión, distribuidos por mes
(Fuente: Obtenida de resultados de investigación)

Para que podamos ver un informe más detallado de los inicios de sesión realizados daloRADIUS nos da la opción de realizar la misma consulta, pero realizando una distribución por día, es decir, muestra los inicios de sesión que se realizaron en cada día del mes, en la **figura 3.56** y **3.57** se muestra esta información.

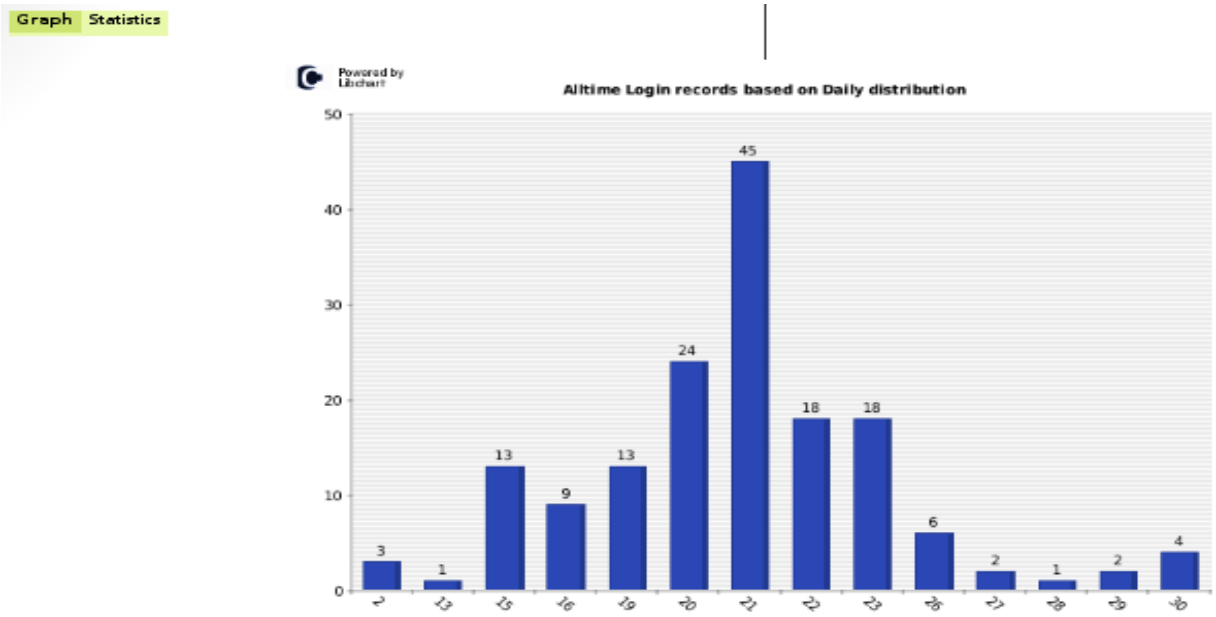


Figura 3.56 Grafica de inicios de sesión realizados, distribuidos por día
(Fuente: Obtenida de resultados de investigación)

Graph Statistics

ALL-TIME LOGINS/HITS STATISTICS	
Logins/Hits count > <	Day of month > <
1	13
1	28
2	27
2	29
3	2
4	30
6	26
9	16
13	15
13	19
18	22
18	23
24	20
45	21
159	

Figura 3.57: Datos numéricos de inicios de sesión realizados, distribuidos por día
(Fuente: Obtenida de resultados de investigación)

Alltime Traffic Comparison. Proporciona una tabla grafica de las descargas y subidas de usuarios. En las figuras **3.58** y **3.59** se muestran las gráficas de las cargas y descargas realizadas por los usuarios, distribuido por día.

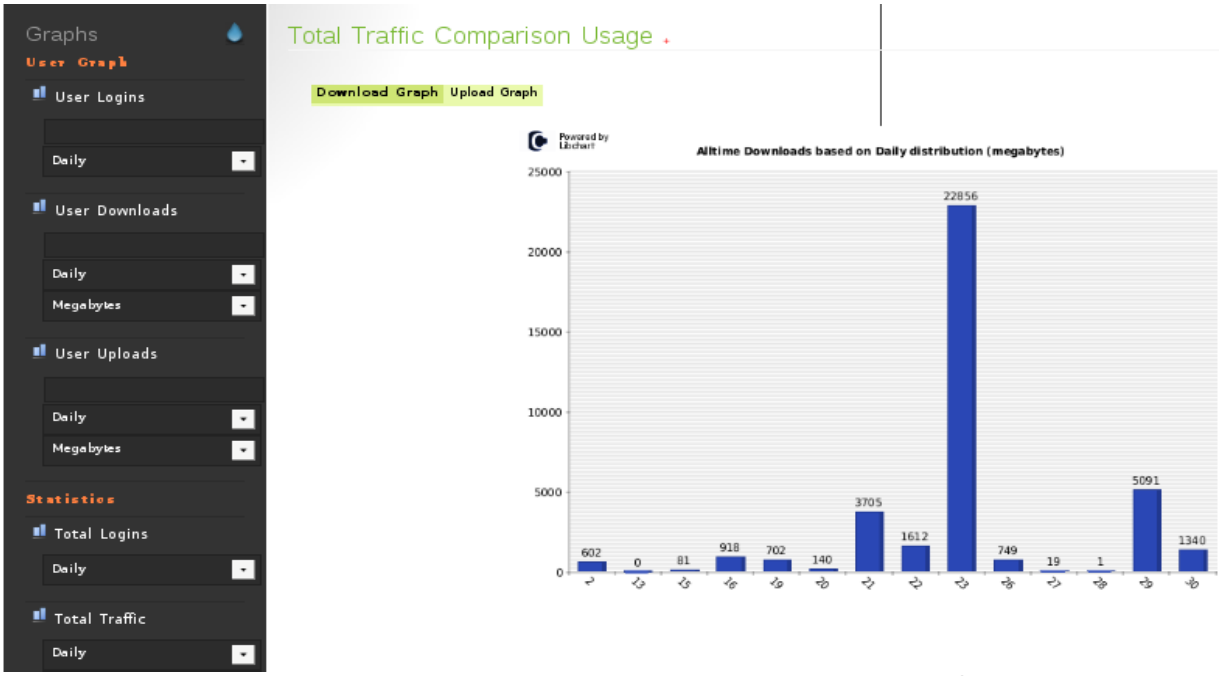


Figura 3.58 Grafica de las descargas de datos realizadas (distribuido por día)
(Fuente: Obtenida de resultados de investigación)

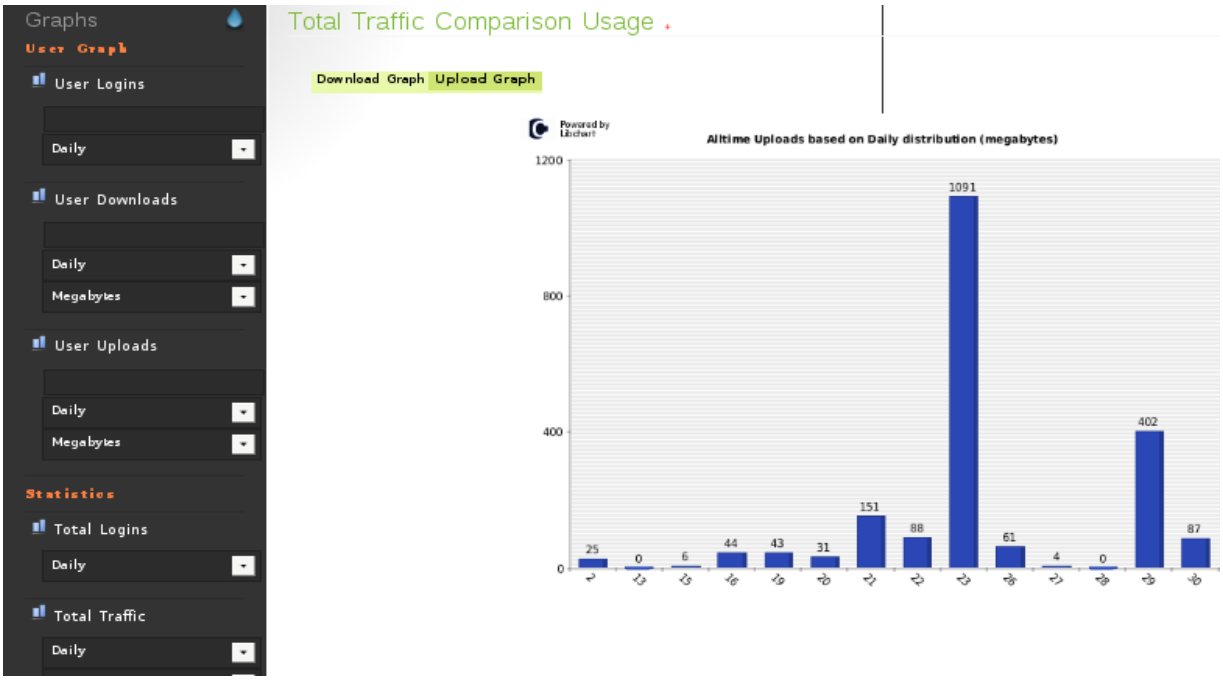


Figura 3.59: Grafica de las cargas de datos realizadas (distribuido por día)
(Fuente: Obtenida de resultados de investigación)

Las estadísticas de las cargas y descargas de datos realizados también se pueden realizar por mes, es decir, se muestra la información distribuida por mes, en las **figuras 3.60** y **3.61** se muestra el ejemplo.

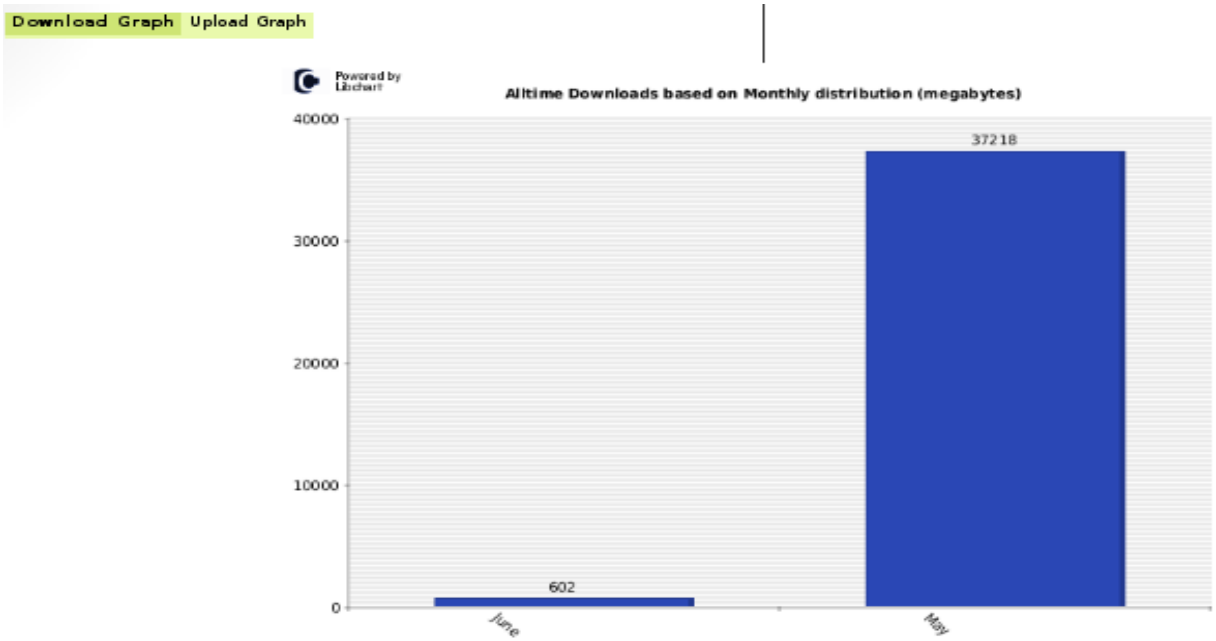


Figura 3.60 Grafica de los datos descargados por los usuarios (distribuido por mes)
(Fuente: Obtenida de resultados de investigación)

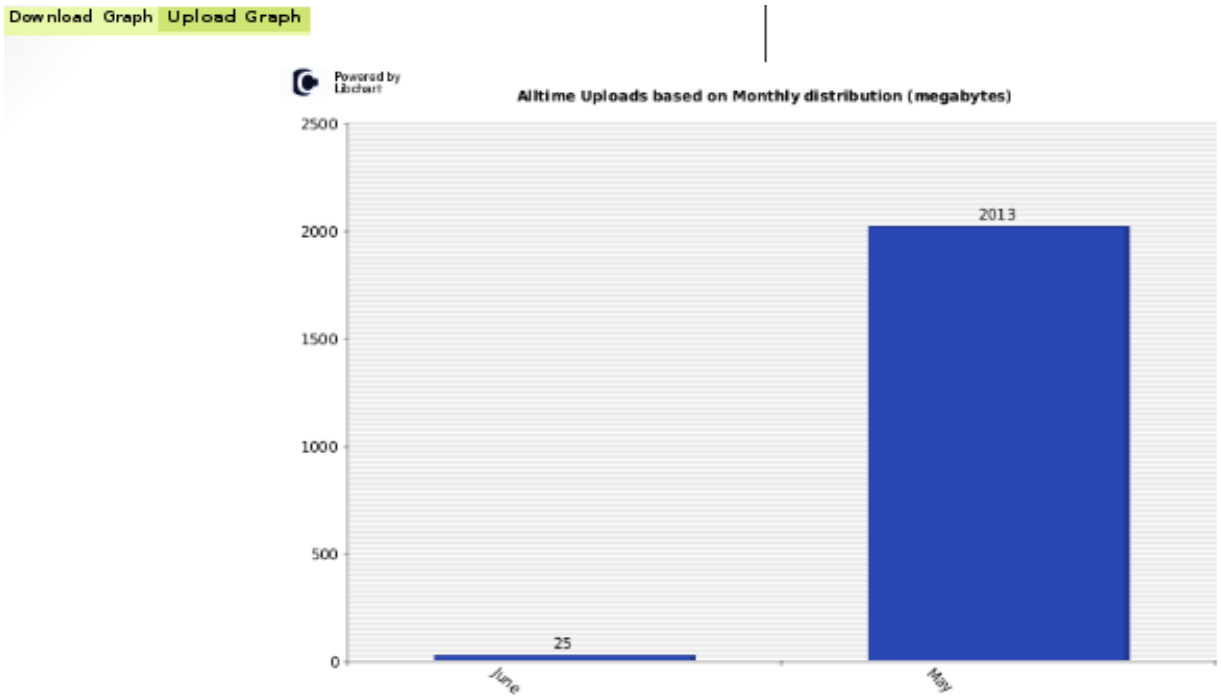


Figura 3.61 Grafica de los datos cargados por los usuarios (distribuido por mes)
(Fuente: Obtenida de resultados de investigación)

Logged Users. Proporciona una gráfica de la los usuarios registrados en el período especificado. Para realizar estas consultas se tiene que filtrar el día, mes y año; para graficar por hora o filtrar sólo por meses y años (seleccione "---" en el campo del día) para graficar los valores mínimo y máximo de los usuarios registrados en el mes seleccionado (ver **figura 3.62**).

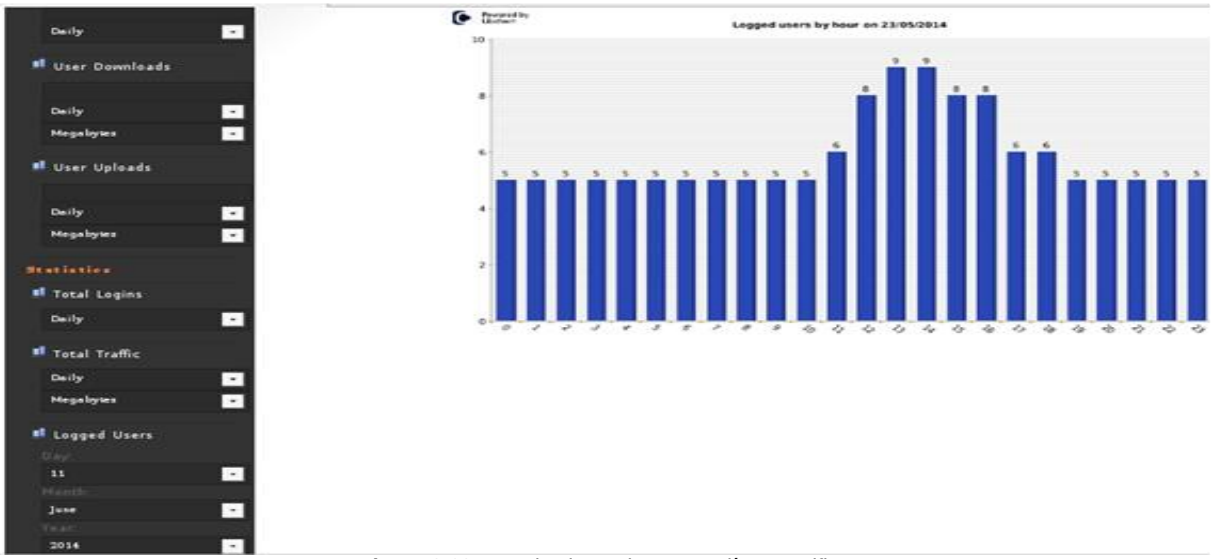


Figura 3.62 Usuarios logeados en un día especifico
(Fuente: Obtenida de resultados de investigación)

Y para finalizar en la sección **Config** se observan las opciones de configuraciones que van desde la de usuarios, la bases de datos, el lenguaje (en la actualidad español no se encuentra en su totalidad traducido al 100%), entre otras más. Es recomendable no modificar la configuración actual a menos que sepan muy bien que es lo que están haciendo.

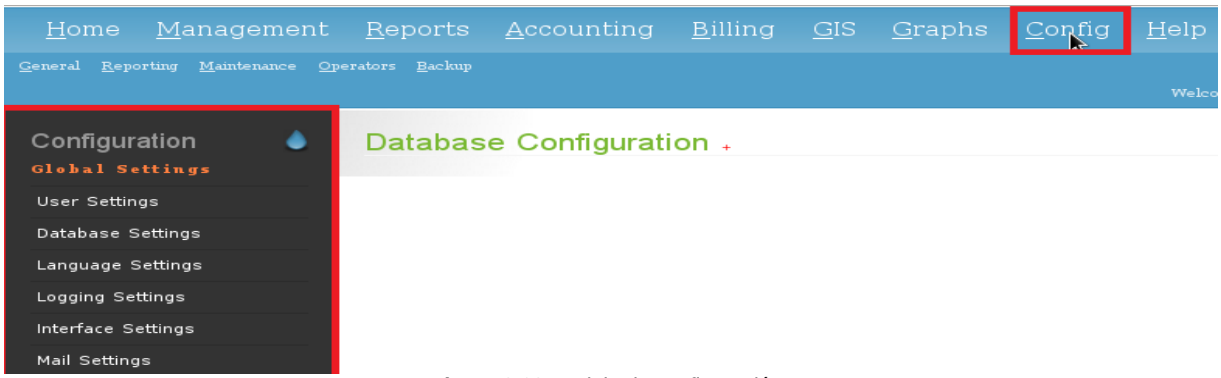


Figura 3.63 Modulo de configuración
(Fuente: Obtenida de resultados de investigación)

Configuración de la base de datos. Esta opción muestra información del motor de base de datos, en esta parte se puede configurar los ajustes de conexión, nombres de tablas si el que trae por defecto no se utilizan, y el tipo de cifrado de la contraseña en la base de datos.

Configuración de idioma. Esta opción nos permite configurar el idioma de la interfaz, pero se recomienda mantenerlo en inglés para evitar confusiones de traducción.

Configuración de acceso. En esta sección se configuran los datos que queremos que se guarden en el archivo de registros de daloRADIUS que se muestra en la figura 3.16 al inicio de este apartado, en este parte se configura si deseamos guardar las páginas visitadas por el administrador de daloRADIUS, las consultas realizadas, las acciones realizadas y también aquí se define el directorio en el que se encuentra el archivo daloradius.log.

Configuración de la interfaz. En esta sección se configuran las opciones de diseño de interfaz como lo es: si queremos ocultar los caracteres de las contraseñas, el número de líneas que queremos mostrar en las tablas y si queremos activar el autocompletado de formularios.

Operadores. En esta sección se configuran los operadores (administradores) de daloRADIUS, aquí se pueden agregar tantos administradores como queramos, así como también se pueden eliminar.

Otra utilidad de esta sección es que también aquí podemos definir los privilegios para cada administrador que tengamos, es decir podemos se pueden crear operadores que no tengan permisos para eliminar usuarios o acceder a información que que no se quiera mostrar para nadie más.

En la **figura 3.64** se muestran la información que proporciona esta consulta.

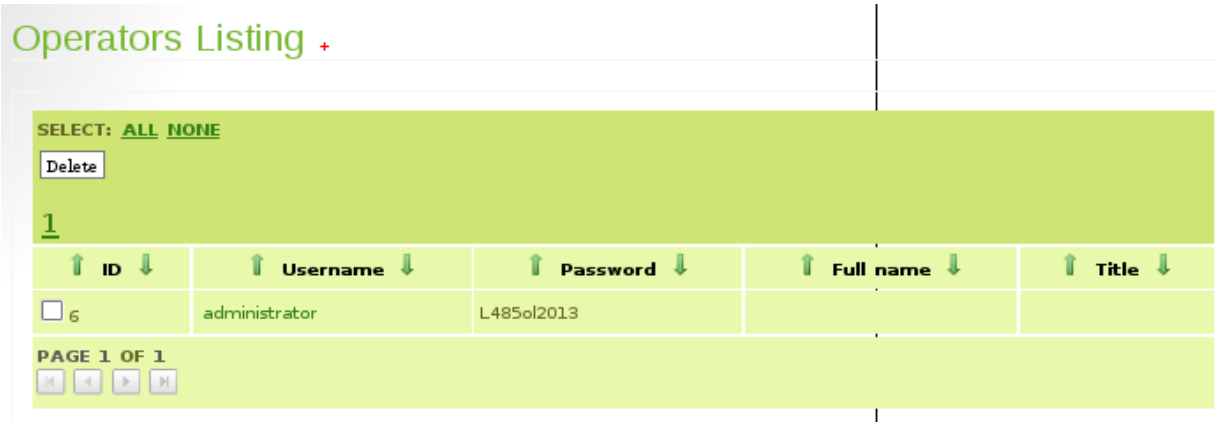


Figura 3.64 Operadores de daloRADIUS
(Fuente: Obtenida de resultados de investigación)

La última sección del módulo de configuración es la de **backup**, en esta sección se realizan respaldos de la base de datos tanto de FreeRADIUS como de daloRADIUS, podemos crear respaldos de las tablas que queramos para posteriormente poder restaurarlas, en las **figuras 3.65**, **3.66** y **3.67** se muestra lo anterior mencionado.

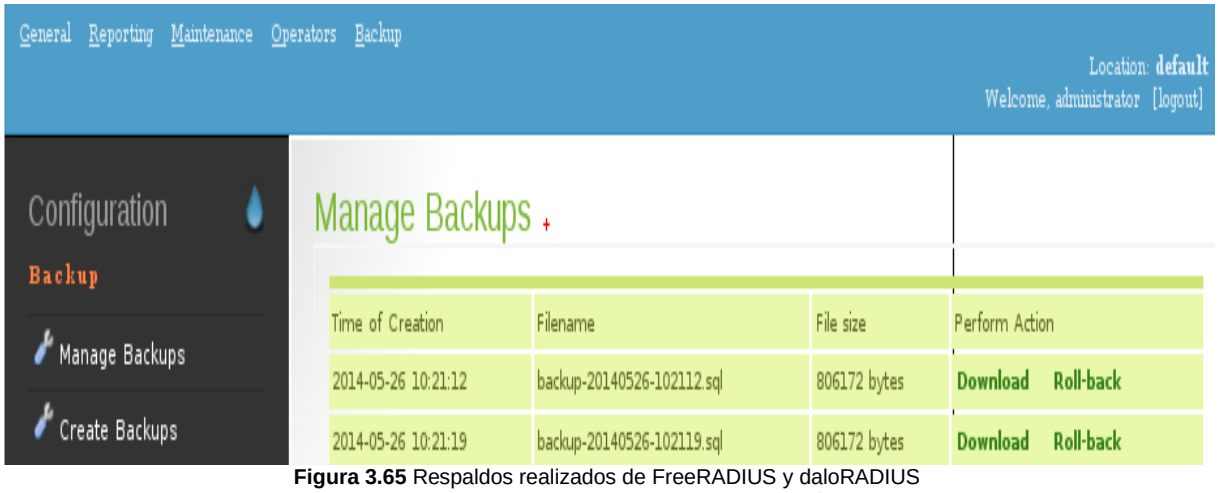


Figura 3.65 Respaldos realizados de FreeRADIUS y daloRADIUS
(Fuente: Obtenida de resultados de investigación)

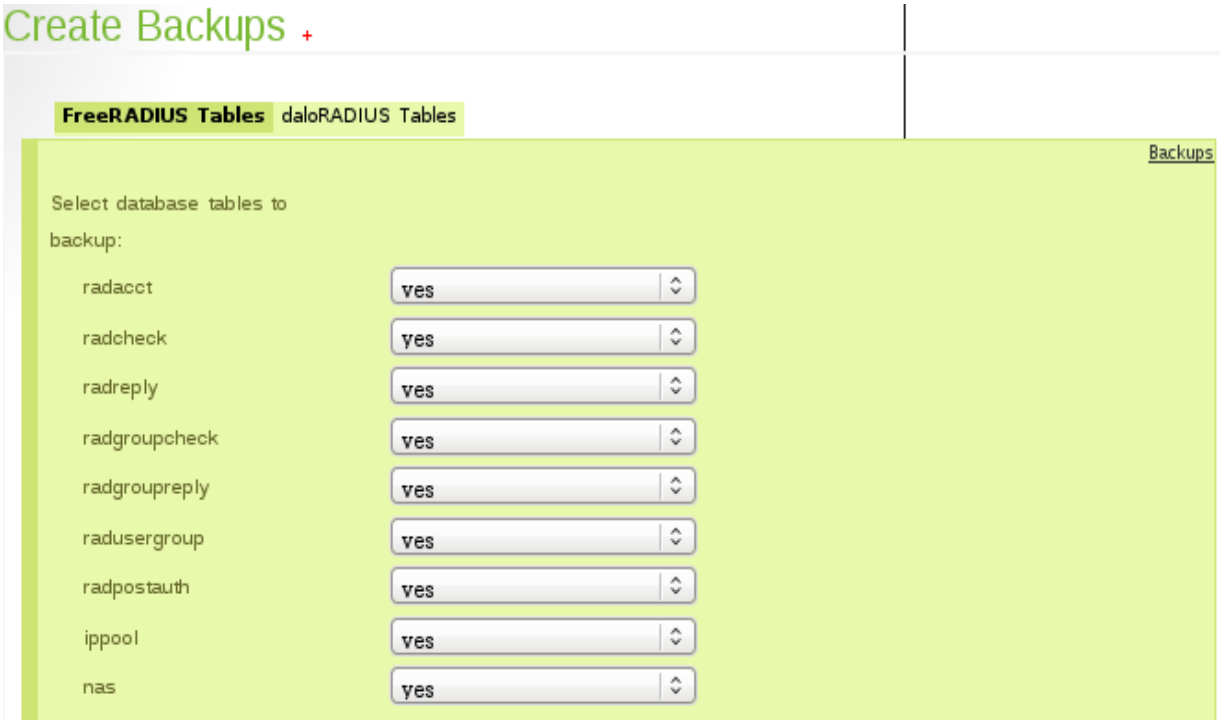


Figura 3. 66 Seccion para seleccionar tablas de freeRADIUS
(Fuente: Obtenida de resultados de investigación)

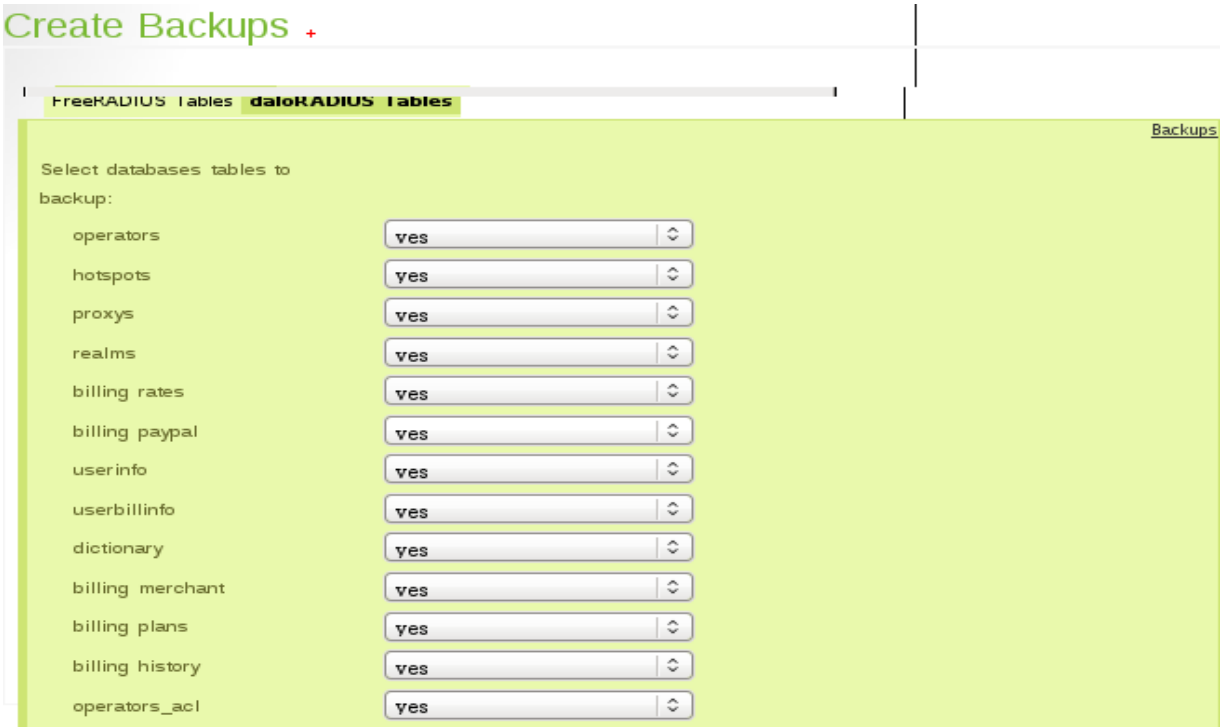


Figura 3.67 Sección para seleccionar tablas de daloRADIUS
(Fuente: Obtenida de resultados de investigación)

Capitulo IV Conclusiones y recomendaciones

4.1 conclusiones

4.2 Recomendaciones

4.1 Conclusiones

Después de realizar la implementación y gestión de este proyecto, se concluye que es importante llevar el control de los usuarios que acceden, así como de toda la información de lo que sucede en una red de cómputo inalámbrica.

Al tener conocimiento de cuantos usuarios se conectan al día y de la cantidad de datos que se cargan y descargan dentro de la red, se puede tomar la decisión de incrementar el ancho de banda de internet para proporcionar un mejor servicio, dependiendo del lugar en que se implemente la gestión de un portal cautivo.

Otro aspecto importante que se debe tomar en cuenta es que gracias al manejo de base de datos se facilita más la generación de reportes y creación de respaldos para poderlos restaurar cuando se requiera.

4.2 Recomendaciones

Para el buen funcionamiento de la aplicación para la gestión de portales cautivos se hacen las siguientes recomendaciones:

- Tener conocimiento del funcionamiento del portal cautivo con que se cuente
- Realizar los respaldos de la base de datos periódicamente
- No permitir acceso a la aplicación a cualquier persona ajena a la organización
- Cambiar credenciales de usuarios de acceso a la red periódicamente

Anexos

Anexo I: Instalación y configuración de FreeRADIUS

Anexo II: Instalación y configuración de chillispot sobre FreeRADIUS

Anexo III: Configuración de FreeRADIUS con base de datos

Anexo I: Instalación y configuración de FreeRADIUS

Para realizar la instalación de FreeRADIUS, descargar FreeRADIUS desde la web oficial http://freeradius.org.Y posteriormente se acedera a una terminal o Shell como súper-usuario.

Los paquetes que se descarga desde la página oficial son los paquetes de fuentes y tienen un formato (tar.gz), por lo cual realizaremos el procedimiento de descompresión, compilación y finalmente la instalación, para ello realizar lo siguiente:

Ir a la página oficial de FreeRADIUS, y procedemos a la descarga, seleccionando la versión 2.2.0.tar.gz que al momento es la versión actual y estable del servidor y que es la que se muestra en la **figura A1-1**:

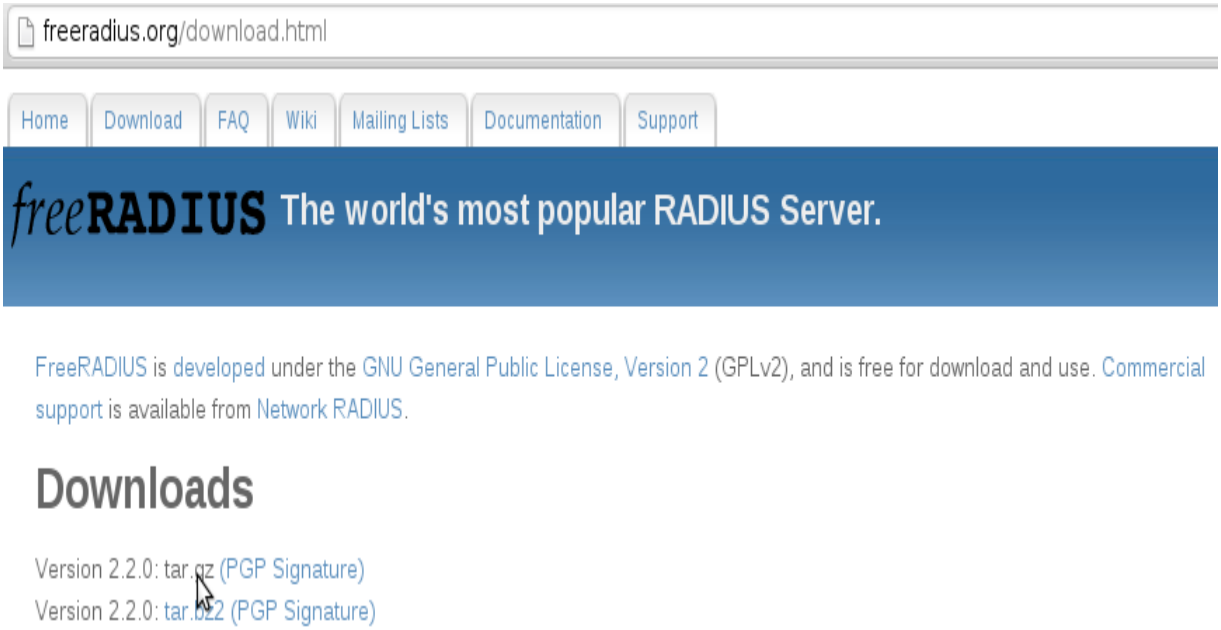


Figura A1-1 Descarga de paquete fuente de FreeRADIUS
Fuente: freeradius.org/dowload.html

Una vez descargado y con el sistema operativo actualizado instalar las dependencias (librerías) y herramientas que nos harán falta para la compilación y posterior instalación

de FreeRADIUS. Para esto, desde la terminal, como administrador (súper usuario), se realiza el siguiente procedimiento como lo indica la **figura A1-2**:

apt-get install libssl-dev

apt-get install build-essential

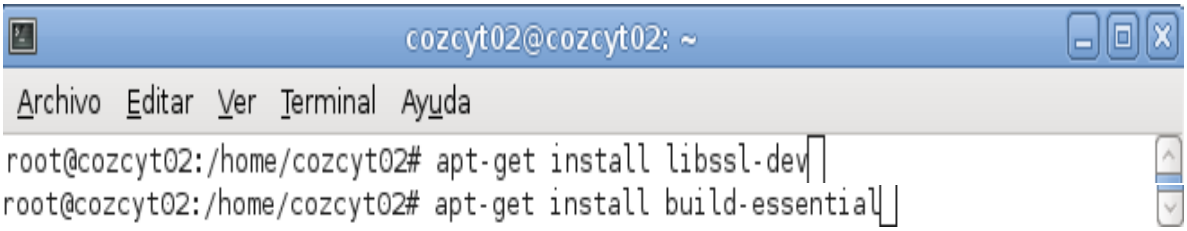


Figura A1-2 Instalación de libssl-dev y build-essential
(Fuente: Obtenida de investigación realizada)

Copiar el fichero descargado a nuestra carpeta de trabajo (/home/"usuario"), **figura A1-3** y lo descomprimimos haciendo uso de tar:

cp /tmp/freeradius….tar.gz /home/cozcyt02

cd /home/cozcyt02

tar xzvf freeradius… tar.gz

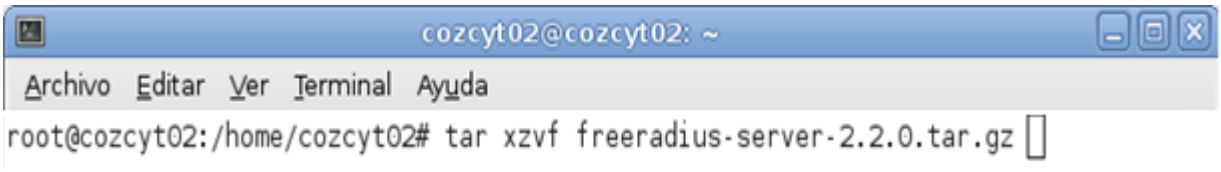


Figura A1-3 Descomprimiendo el paquete FreeRADIUS
(Fuente: Obtenida de resultados de investigación)

Copiar la carpeta correspondiente a la raíz (/).

cp -r freeradius…. /

cd /freeradius….

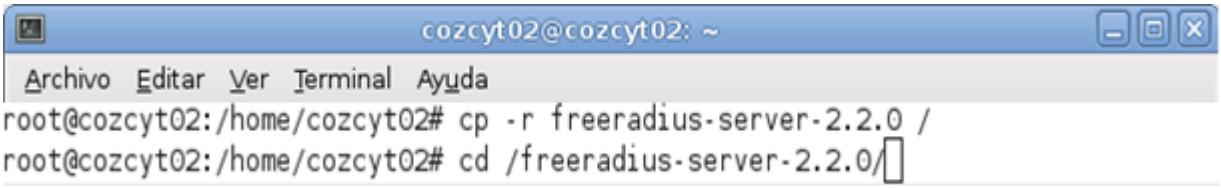


Figura A1-4 Copia de FreeRADIUS a la carpeta personal
(Fuente: Obtenida de resultados de investigación)

El siguiente paso es la configuración e instalación **figura A1-5**, **A1-6** y **A1-7**.

./configure --without-rlm_smb --without-rlm_perl --without-rlm_ldap --without-rlm_krb5

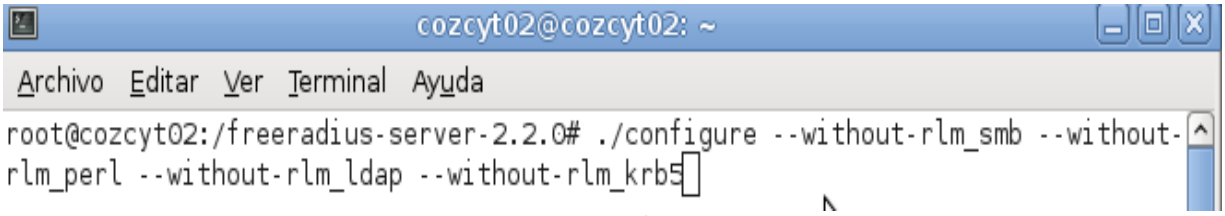


Figura A1-5 Configuración de FreeRADIUS
(Fuente: Obtenida de investigación realizada)

make

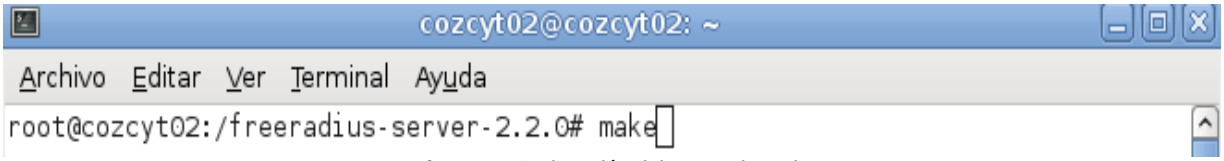


Figura A1-6 Ejecución del comando make
(Fuente: Obtenida de investigación realizada)

make Install

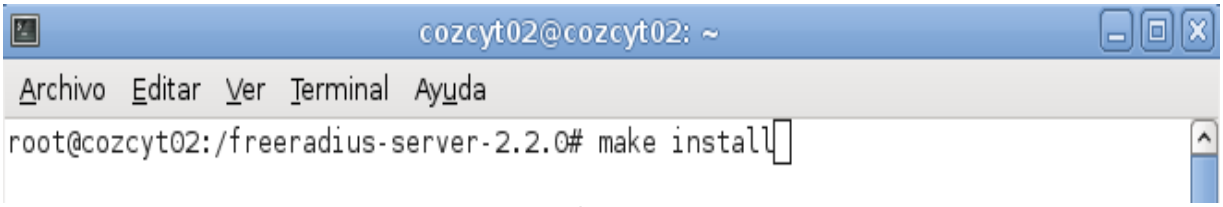


Figura A1-7 Ejecución del comando make install
(Fuente: Obtenida de investigación realizada)

De esta forma, FreeRADIUS ya está instalado en el sistema. Ahora es momento de proceder a la configuración del servidor.

Configuración de FreeRADIUS

Llegado este punto de la instalación de FreeRADIUS, se procederá a realizar la configuración de los archivos de FreeRADIUS. Los ficheros de configuración del servidor RADIUS, se encuentra en /usr/local/etc/raddb. Para configurar el servidor

modificaremos ciertos parámetros de los ficheros de configuración del servidor RADIUS:

eap.conf

Lo primero que se hará será moverse hasta el directorio donde se encuentran los ficheros de configuración (/usr/local/etc/raddb):

cd /usr/local/etc/raddb/

Una vez en el directorio adecuado, se puede realizar una copia del fichero eap.conf con el nombre de eap2.conf con el comando siguiente:

cp eap.conf eap1.conf

Posteriormente, con un editor (por ejemplo, gedit o nano), editamos el fichero (**figura A1-8**) y realizamos los cambios.

nano eap.conf

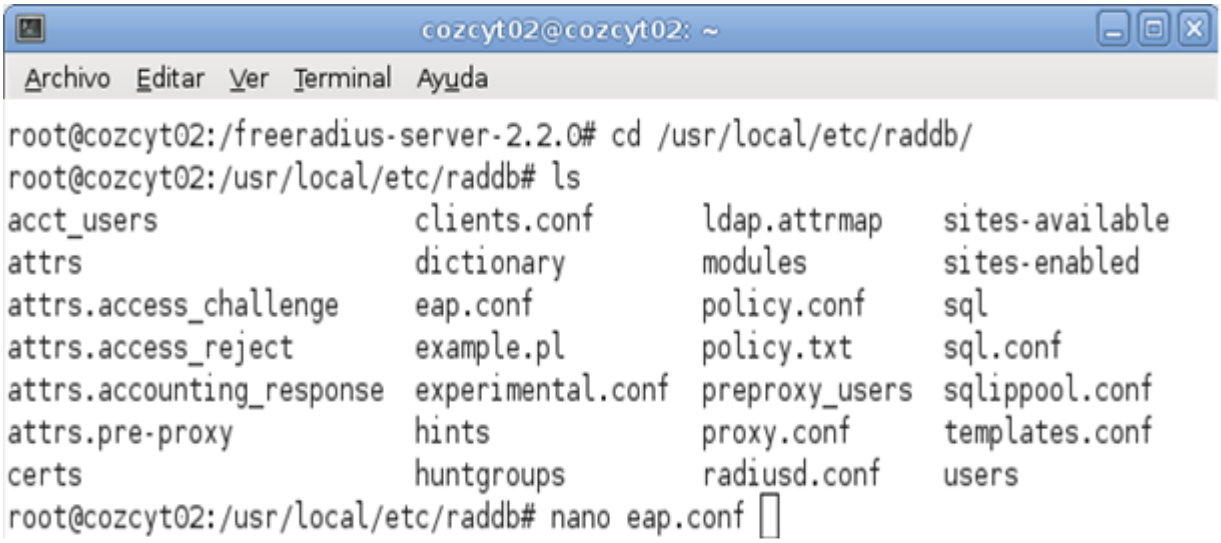


Figura A1-8 Edición del archivo eap.conf
(Fuente: Obtenida de investigación realizada)

Modificar **default_eap_type**: Cambiar el valor md5 (por defecto) a **peap** (**figura A1-9**).

```
eap {
        #  Invoke the default supported EAP type when
        #  EAP-Identity response is received.
        #
        #  The incoming EAP messages DO NOT specify which EAP
        #  type they will be using, so it MUST be set here.
        #
        #  For now, only one default EAP type may be used at a time.
        #
        #  If the EAP-Type attribute is set by another module,
        #  then that EAP type takes precedence over the
        #  default type configured here.
        #
        default_eap_type = peap
```

Figura A1-9 Modificación del archivo eap.conf
(Fuente: Obtenida de investigación realizada)

Users

Al igual que con el archivo eap.conf se pueden realizar copias de los siguientes ficheros por si en algún momento se necesitan de sus configuración original.

En este fichero daremos de alta los nombres de usuario y contraseña que podrán ser usados para autenticarse frente al servidor RADIUS. Se edita el fichero users con un editor de texto, como per ejemplo nano (**figura A1-10**):

nano users

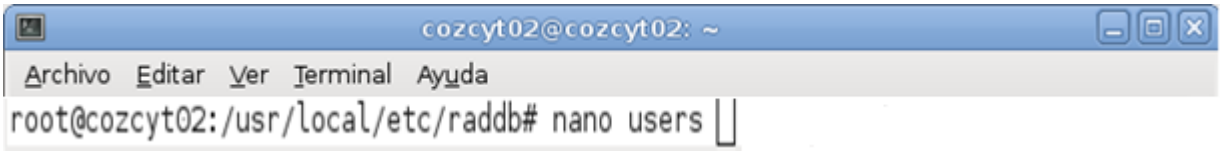


Figura A1-10 Copia y edición del archivo users
(Fuente: Obtenida de investigación realizada)

En este fichero añadir al final del mismo (**figura A1-11**), tantos usuarios como queramos, con el formato:

usuario Cleartext-Password:=”password”

Figura A1-11 Modificación del archivo users
(Fuente: Obtenida de investigación realizada)

Una vez introducidos, guardamos los cambios y cerramos el archivo.

Mschap

Modificamos el siguiente fichero de tal forma que quede igual que en la **figura A1-12**.

nano mschap

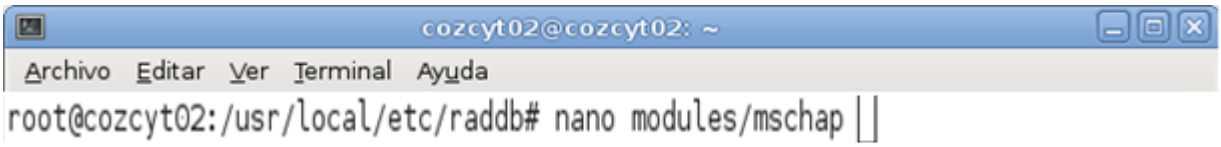


Figura A1-12 Edición del archivo mschap

Y realizar los cambios adecuados para que las distintas variables que a continuación se muestran, para que tengan los respectivos valores:

Use_mppe = yes

Require_encryption = yes

Require_strong = yes

With_ntdopmain_hack = yes

En la **figura A1-13**, se muestra la forma de cómo debe quedar el archivo anteriormente mencionado.

```
mschap {
        #
        #  If you are using /etc/smbpasswd, see the 'passwd'
        #  module for an example of how to use /etc/smbpasswd

        # if use_mppe is not set to no mschap will
        # add MS-CHAP-MPPE-Keys for MS-CHAPv1 and
        # MS-MPPE-Recv-Key/MS-MPPE-Send-Key for MS-CHAPv2
        #
        use_mppe = yes

        # if mppe is enabled require_encryption makes
        # encryption moderate
        #
        require_encryption = yes

        # require_strong always requires 128 bit key
        # encryption
        #
        require_strong = yes

        # Windows sends us a username in the form of
        # DOMAIN\user, but sends the challenge response
        # based on only the user portion.  This hack
        # corrects for that incorrect behavior.
        #
        with_ntdomain_hack = yes
```

Figura A1-13 Modificación del archivo mschap
(Fuente: Obtenida de investigación realizada)

Una vez realizados los cambios, guardar y salir. Para que los cambios realizados en la configuración sean cargados en RADIUS, se debe ejecutar el siguiente comando:

ldconfig

En este momento ya está instalado y configurado el servidor RADIUS. A continuación se realizara una prueba, y solo quedara configurar el cliente en el servidor RADIUS, y

el punto de acceso para que pida autentificación de usuarios al servidor que se configuro.

Prueba del funcionamiento del servidor RADIUS FreeRADIUS

Para realizar la prueba del funcionamiento de nuestro servidor RADIUS ejecutamos el siguiente comando.

/usr/local/sbin/radiusd –f –X

Con lo que se lanza el demonio de FreeRADIUS. El aspecto de la pantalla, de FreeRADIUS, a la espera que algún cliente se intente conectar a nuestra red Wifi, sería (**figura A1-14**):

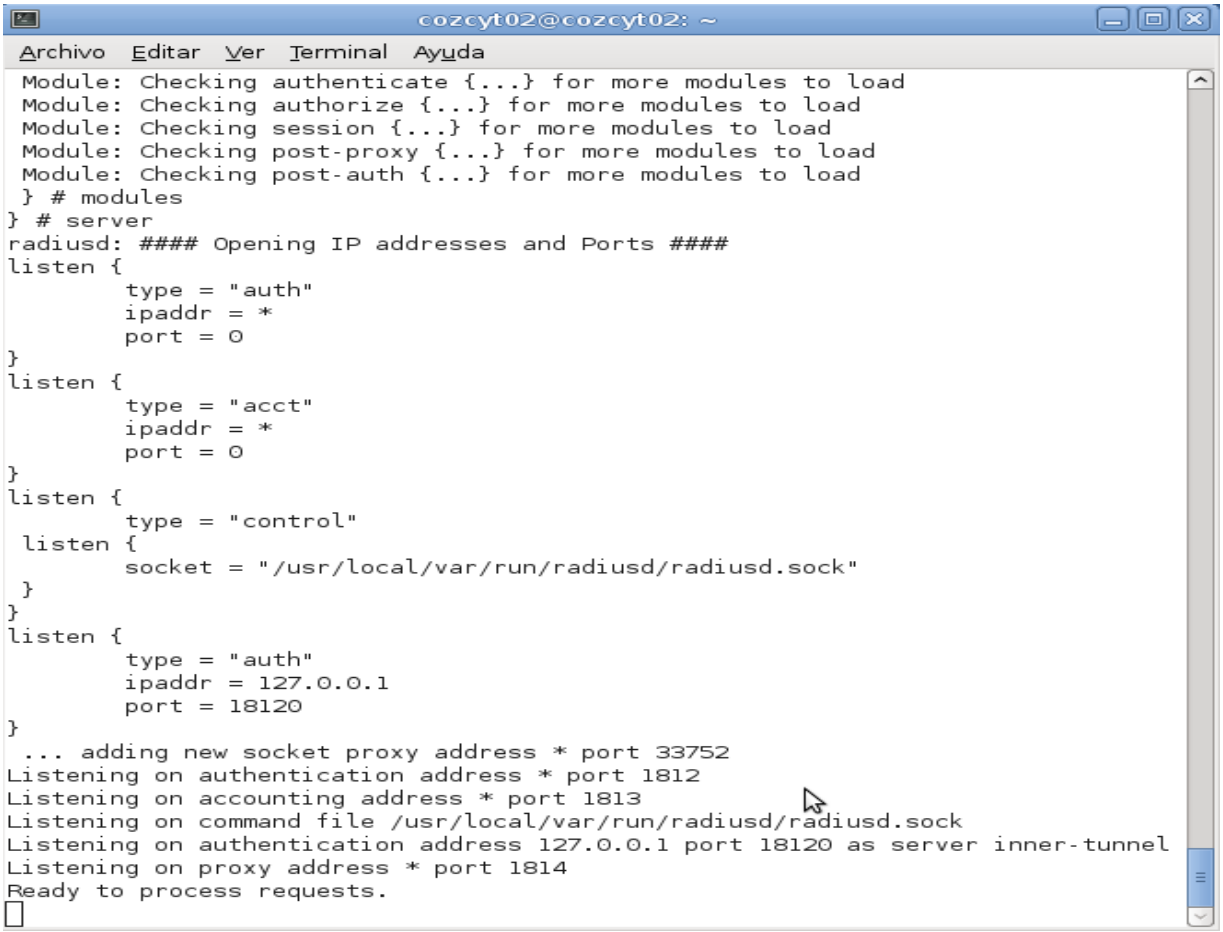


Figura A1-14 Funcionamiento del servidor RADIUS
(Fuente: Obtenida de resultados de investigación)

Configuración del cliente en nuestro servidor RADIUS FreeRADIUS.

Dado a que en nuestro caso la dirección IP del servidor RADIUS es la de loopback por estar en el mismo equipo en que se encuentra Chillispot, debemos verificar que dentro de los clientes se encuentre especificado nuestro host local y si no se encuentra agregarlo.

Si el caso fuera un servidor RADIUS remoto, deberíamos agregar la dirección IP a través de la cual es visible para RADIUS el host con Chillispot. Abrimos el fichero con gedit (**figura A1-15**):

nano clients.conf

Figura A1-15 Edición del archivo clients.conf
(Fuente: Obtenida de investigación realizada)

Para el primer caso expuesto, el archivo debe quedar como en la **figura A1-16**:

Figura A1-16 Configuración de clients.conf
(Fuente: Obtenida de investigación realizada)

Para probar el funcionamiento de que el servidor RADIUS está funcionando correctamente podemos hacer un test con el siguiente comando (**figura A1-17**).

radtest labsol L485ol2013 127.0.0.1 1812 testing123

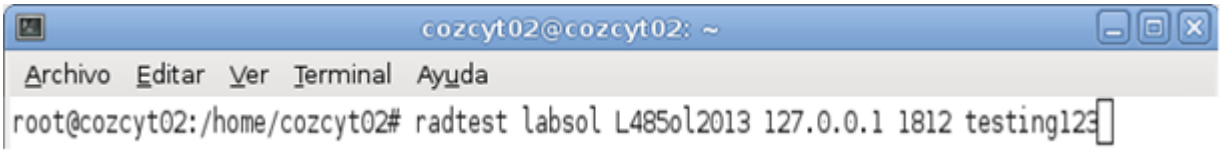


Figura A1-17 Prueba de servidor RADIUS
(Fuente: Obtenida de investigación realizada)

Si el usuario existe en el archivo de textos users, en la terminal debe aparecer el mensaje “Access Accept”, como se muestra en la **figura A1-18**.

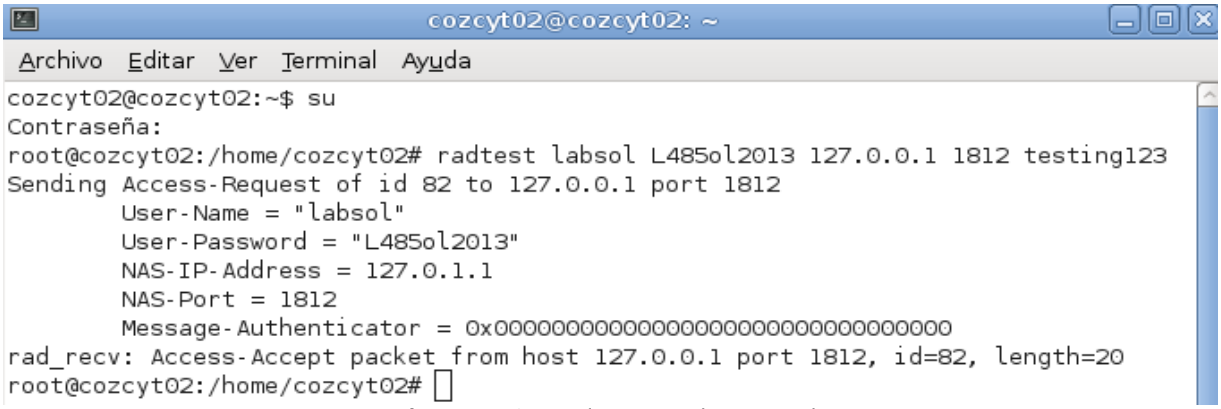


Figura A1-18 Usuario encontrado y aceptado
(Fuente: Obtenida de resultados de investigación)

Anexo II: Instalación y configuración de ChilliSpot sobre FreeRADIUS

En este apartado se realizara la Instalación y configuración de ChilliSpot en un sistema Debian. Este sistema ya deberá de tener instalado y configurado FreeRADIUS.

Para la puesta en marcha de Chillispot, deberemos de tener dos interfaces de red en nuestro sistema ya sea de manera mixta, ethernet y wifi o dos tarjetas ethernet, para efectos de esta practica utilizaremos dos tarjetas de red ethernet, las cuales llevaran la siguiente sintaxis:

- eth0: conectará con la red local(sea wifi o cableada).
- eth1: Conectará con Internet.

A continuación se muestra en la **figura A2-1** la topología de como seria nuestra red, haciendo uso de un servidor ChilliSpot:

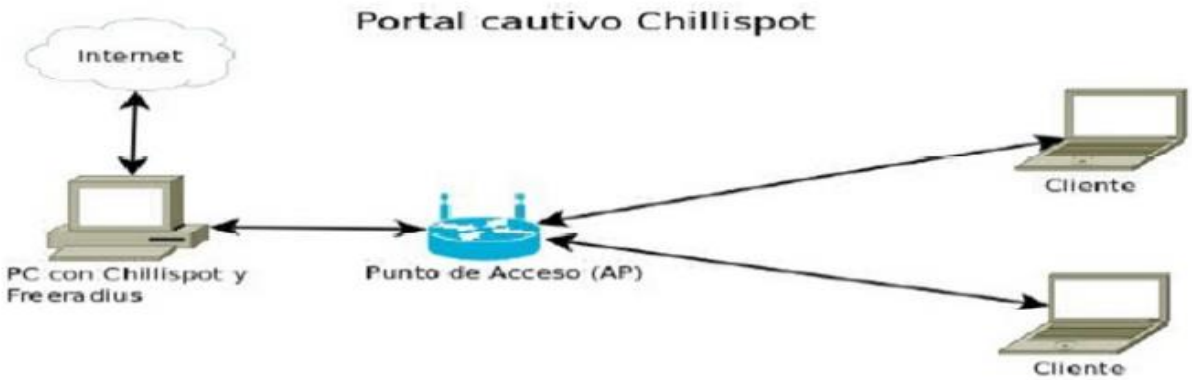


Figura A2-1 Topología de red con ChilliSpot
(Fuente: Obtenida de investigación realizada)

A lo largo de la configuración, se hace uso de un adaptador virtual TUN, el cual hará las veces de servidor de autentificación en el sistema local.

Una vez que es analizada la topología se pasa a configurar nuestro sistema. Nos logeamos desde la terminal como administrador y ejecutamos el comando ifconfig para verificar la ip que tenemos asignada y por medio del comando ping checamos si tenemos salida al exterior:

ifconfig

ping 8.8.8.8

Descarga de ChilliSpot

Una vez confirmada que verificamos que tenemos salida al exterior, nos conectamos desde un navegador, ya sea Ice Weasel, Mozilla Firefox, Google Chrome o cualquier otro navegador de nuestra preferencia a la web de Chillispot http://www.chillispot.org, y en su sección de descargas, podremos ver el enlace a los archivos fuente.

Una vez estando en la pagina ofical de chillispot, seleccionamos la version del paquete que más nos convenga, asi como tambien debe ser de extension compatible con nuestro sistema operativo.

El paquete que nos interesa es el paquete .deb, como lo muestra la **figura A2-2**.

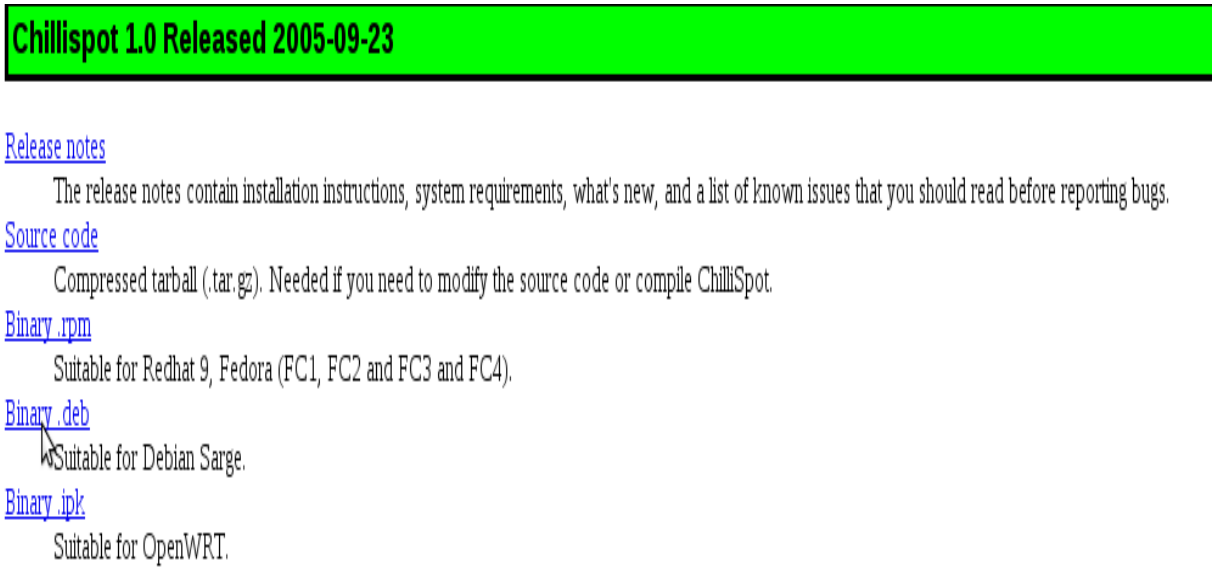


Figura A2-2 Descarga del paquete fuente de ChilliSpot
(Fuente: www.chillispot.org)

Una vez descargado el paquete lo podremos encontrar en la carpeta de descargas del usuario (/home/"usuario").

Instalación y configuración de Apache 2 + SSL

Para el funcionamiento de nuestro portal cautivo ChilliSpot necesitamos un servidor web con soporte SSL al cual redireccionará a los usuarios de la red inalámbrica cuando intenten navegar. Nosotros instalaremos Apache y los módulos respectivos para soporte SSL

Lo primero que se tiene que hacer es abrir un terminal e instalar apache con el comando:

apt-get install apache2 apache2.2-common apache2-mpm-worker apache2-utils

En la **figura A2-3** se muestra el comando para instalar apache.

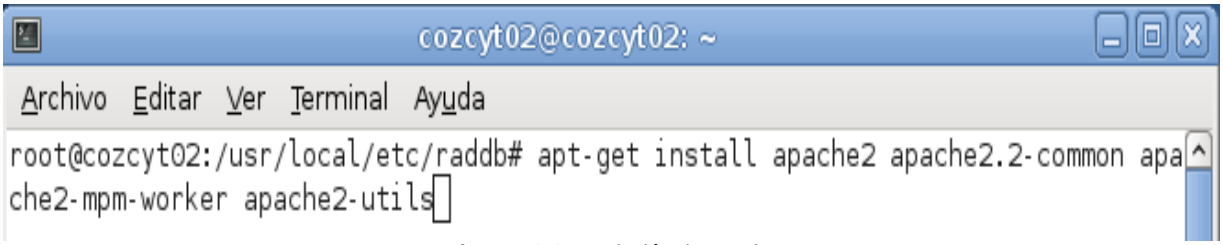


Figura A2-3 Instalación de apache
(Fuente: Obtenida de investigación realizada)

Pasamos ahora a generar el certificado SSL con el que trabajará Apache, ya que la página de autentificación, será bajo el protocolo SSL+HTTP, es decir, HTTPS. Para ello, desde un terminal, creamos la carpeta ssl (**figura A2-4**), dentro de /etc/apache2, que es la ubicación donde se depositará el certificado una vez creado.

mkdir /etc/apache2/ssl

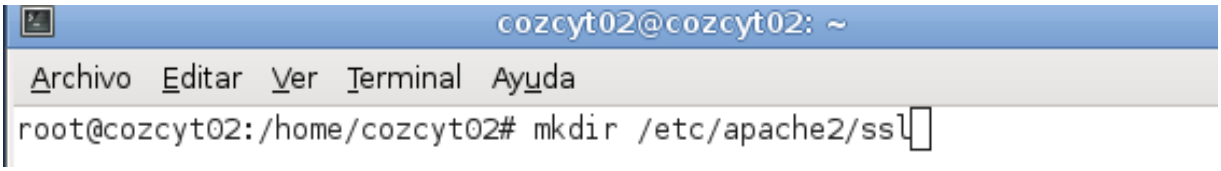


Figura A2-4 Creación del directorio para el certificado
(Fuente: Obtenida de investigación realizada)

Una vez creado el directorio ssl, pasamos a crear el certificado, por medio del comando make-ssl-cert (**figura A2-5**).

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

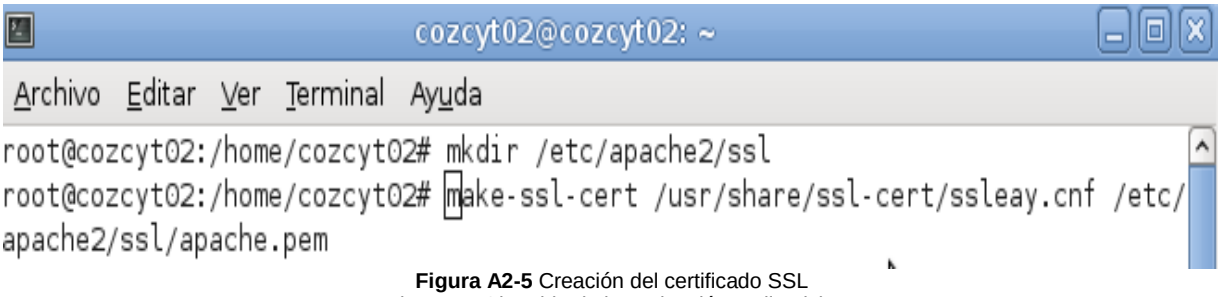


Figura A2-5 Creación del certificado SSL
(Fuente: Obtenida de investigación realizada)

Después de haber creado el certificado procedemos a llenar los datos que se nos pida según sea nuestro caso y luego habilitamos el módulo (**figura A2-6**):

a2enmod ssl

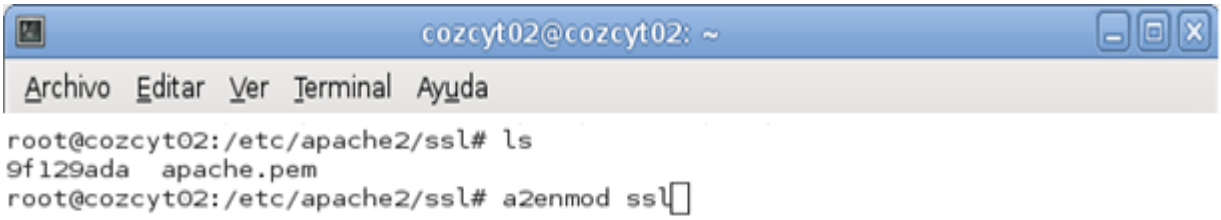


Figura A2-6 Habilitación del módulo
(Fuente: Obtenida de investigación realizada)

Una vez habilitado el modulo debemos verificar que Apache esté configurado para escuchar por el puerto 443.

Cuando se trabaja con el módulo SSL, las versiones recientes de Apache suelen ya venir configuradas de esta manera, por lo que editamos el archivo ports.conf (**figura A2-7**):

gedit /etc/apache2/ports.conf

Figura A2-7 Edición del archivo ports.conf
(Fuente: Obtenida de investigación realizada)

Una vez abierto el archivo, debe tener la forma como se muestra en la **figura A2-8**.

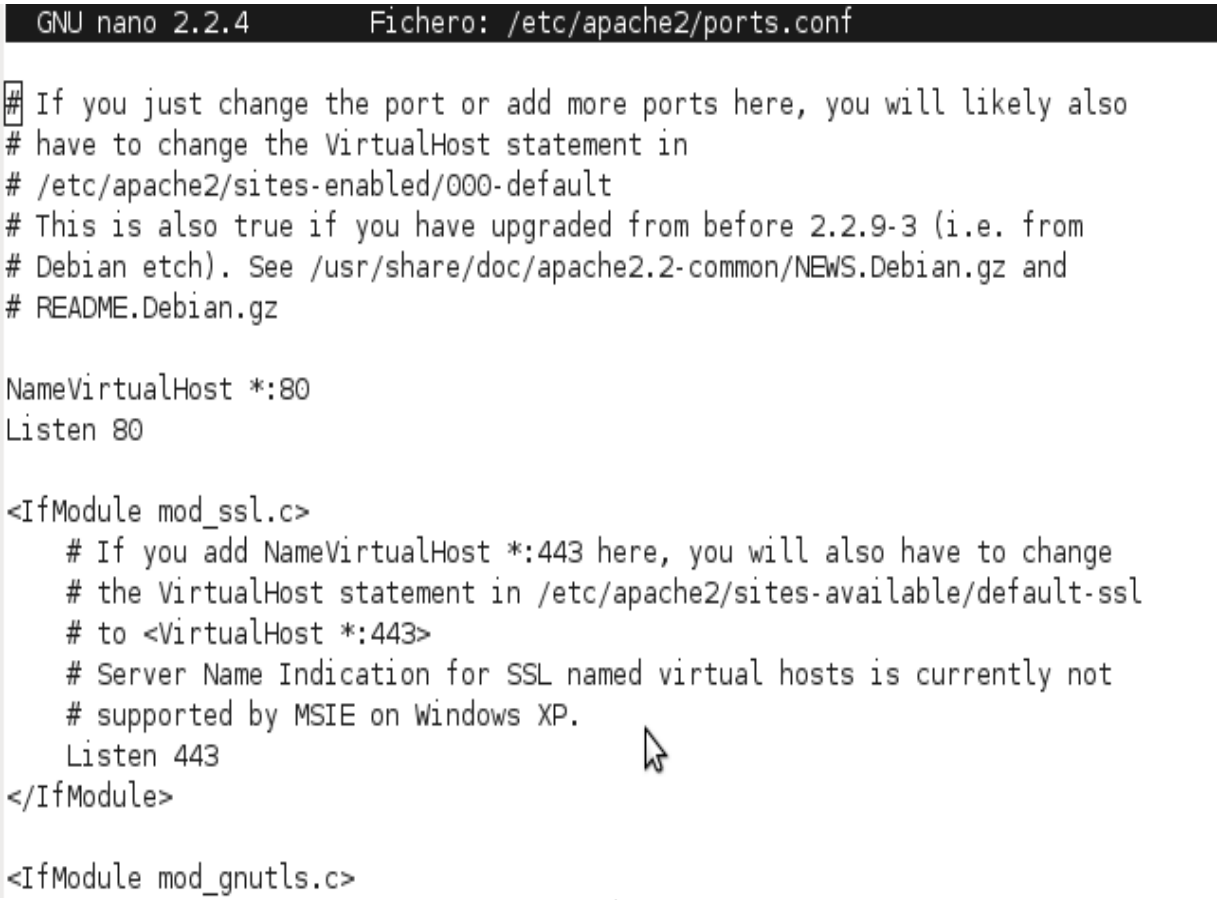


Figura A2-8 Configuración del archivo ports.conf
(Fuente: Obtenida de investigación realizada)

Ahora creamos el sitio SSL. Por defecto, Apache trae el fichero default ubicado en la carpeta /etc/apache2/sites-available/. Copiamos este archivo para luego poder modificarlo (ver **figura A2-9**):

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

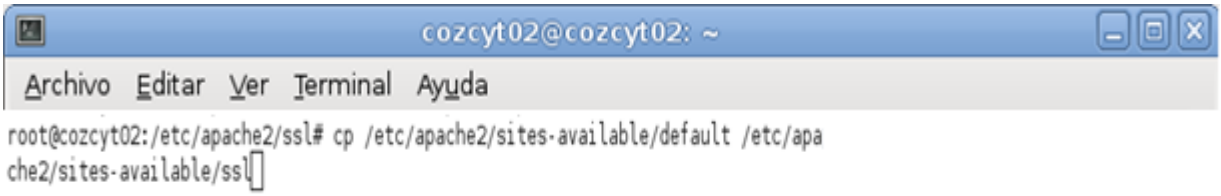


Figura A2-9 Creación del archivo ssl
(Fuente: Obtenida de investigación realizada)

Una vez creado el certificado lo modificamos para que quede como se muestra en la **figura A2-10**

nano /etc/apache2/sites-available/ssl

```
  GNU nano 2.2.4     Fichero: /etc/apache2/sites-available/ssl

NameVirtualHost *:443
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        SSLEngine On
        SSLCertificateFile /etc/apache2/ssl/apache.pem
        DocumentRoot /var/www/
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>
        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>
        ErrorLog /var/log/apache2/error.log
        LogLevel warn
        CustomLog /var/log/apache2/access.log combined
    Alias /doc/ "/usr/share/doc/"
    <Directory "/usr/share/doc/">
        Options Indexes MultiViews FollowSymLinks
        AllowOverride None
        Order deny,allow
        Deny from all
        Allow from 127.0.0.0/255.0.0.0 ::1/128
    </Directory>
</VirtualHost>
```

Figura A2-10 Estructura del certificado ssl
(Fuente: Obtenida de investigación realizada)

Para finalizar la configuración de Apache, habilitamos el nuevo sitio (**figura A2-11**):

a2ensite ssl

Figura A2-11 Habilitación del nuevo sitio
(Fuente: Obtenida de investigación realizada)

Una vez habilitado, el sitio ssl, reiniciamos el servicio apache2, tal y como se muestra en la **figura A2-12**:

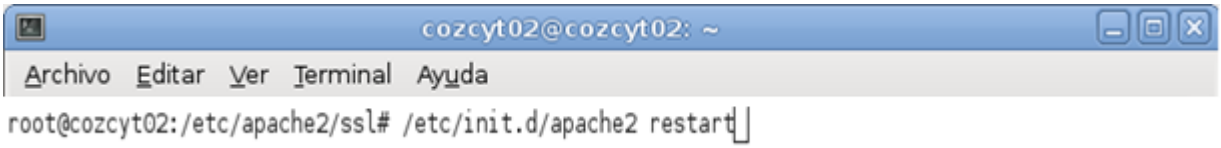


Figura A2-12 Reinicio de apache
(Fuente: Obtenida de investigación realizada)

Después de esto ya podremos acceder a nuestro sitio, tanto de forma normal (**figura A2-13**), como por acceso seguro SSL (**figura A2-14**).

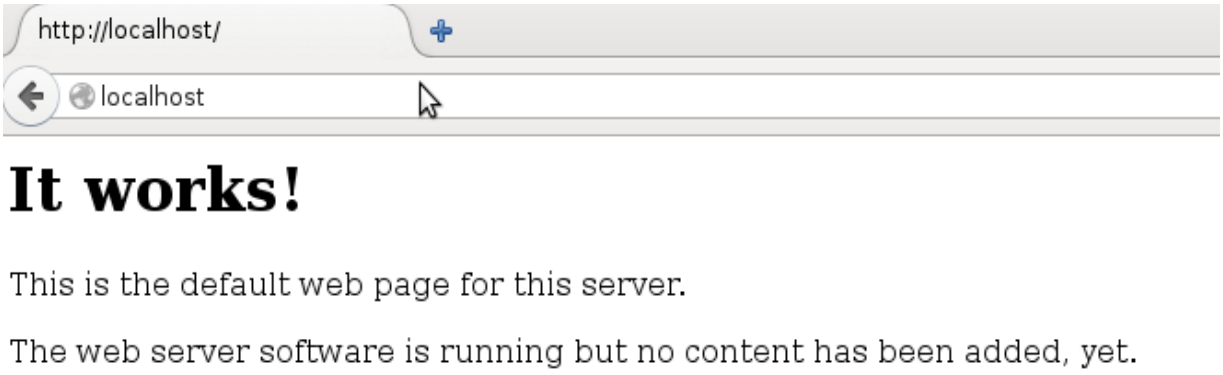


Figura A2-13 Página de nuestro sitio con http
(Fuente: Obtenida de resultados de investigación)

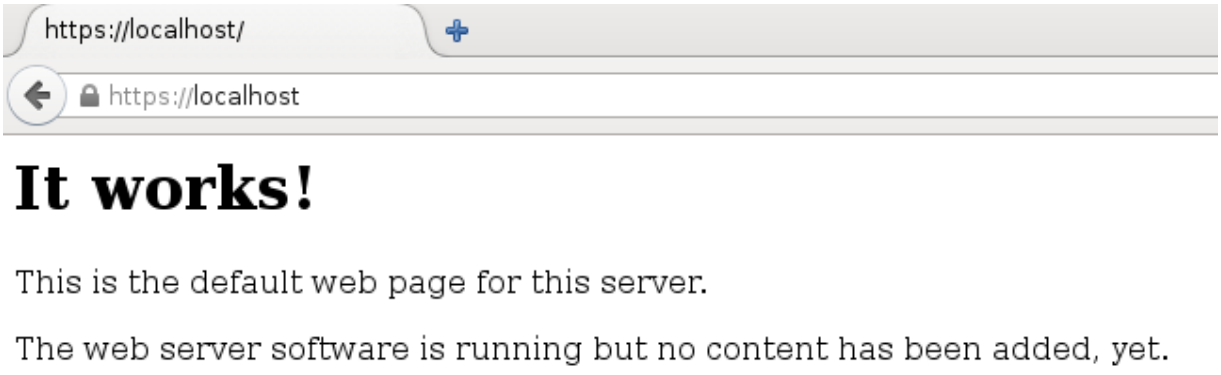


Figura A2-14 Página de nuestro sitio con https
(Fuente: Obtenida de resultados de investigación)

Soporte TUN/TAP

En primer lugar, nuestro sistema debe tener habilitado el soporte TUN/TAP para interfaces virtuales. Desde la terminal ejecutamos los siguientes comandos (**figura A2-15**):

apt-get Install modconf

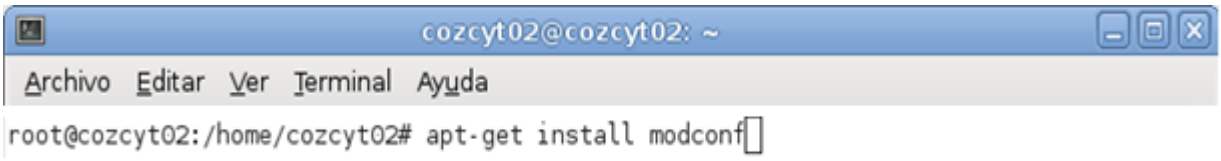


Figura A2-15 Instalación de modconf
(Fuente: Obtenida de investigación realizada)

Ahora pasamos a la configuración de TUN, por medio del comando modconf (**figura A2-16**):

modconf

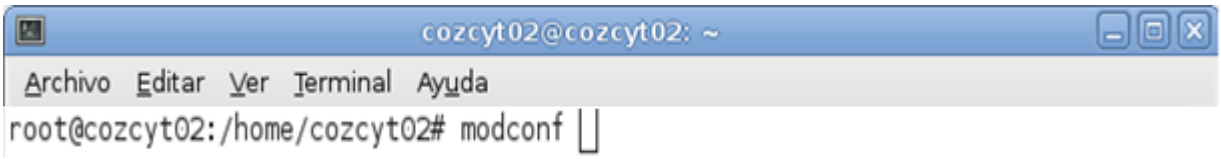


Figura A2-16 Configuración de TUN
(Fuente: Obtenida de investigación realizada)

Con esto aparecerá un recuadro que muestra las categorías de los módulos soportados por el sistema. Para nuestro caso, buscaremos sección kernel/drivers/net (**figura A2-17**):

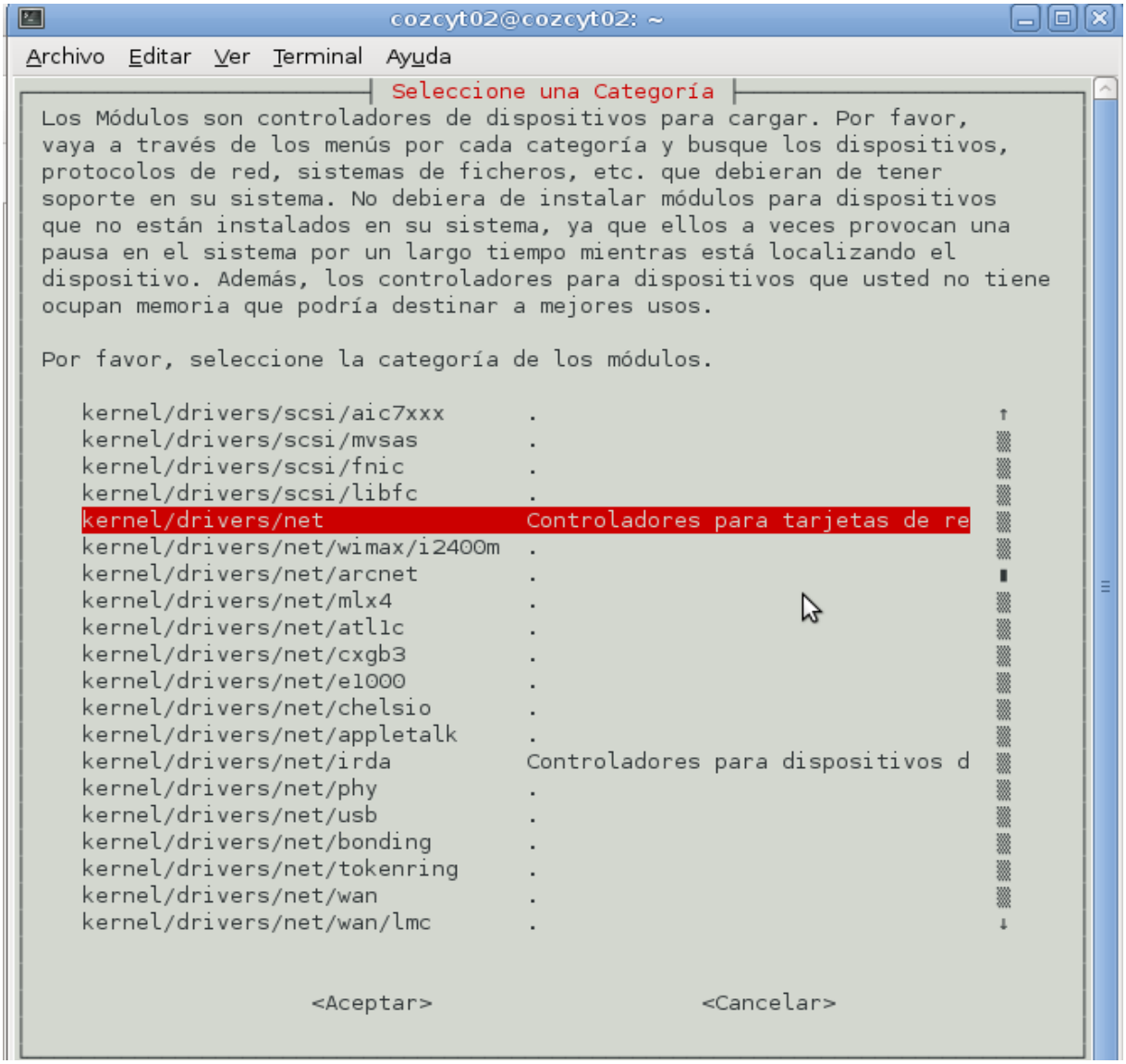


Figura A2-17 Módulos soportados por el sistema
(Fuente: Obtenida de investigación realizada)

Haciendo uso de la tecla tab, seleccionamos “Aceptar” y aparecerá un nuevo recuadro, en el que buscamos “tun” (**figura A2-18**). Si posee soporte debe aparecer con un signo “+”.

Figura A2-18 Localización de tun
(Fuente: Obtenida de investigación realizada)

De lo contrario instalarlo dando Enter sobre el modulo tun y aparecerá el siguiente cuadro (**figura A2-19**) donde daremos clic en “SI”.

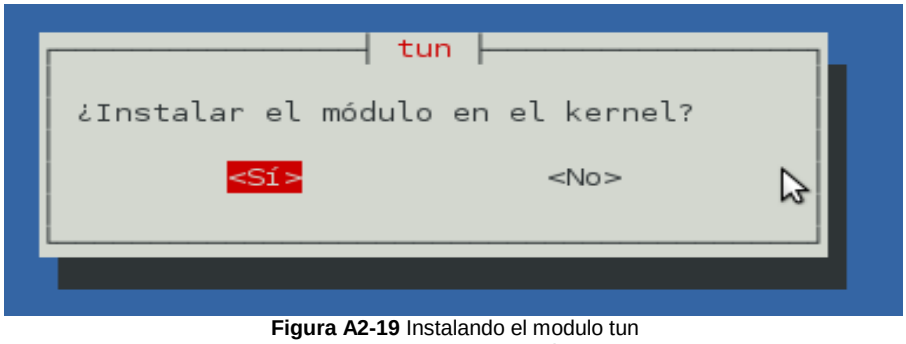


Figura A2-19 Instalando el modulo tun
(Fuente: Obtenida de investigación realizada)

Si tenemos soporte TUN/TAP nuestro sistema posee soporte para un módulo indispensable para ChilliSpot, sin embargo, aún debemos agregarlo al inicio del sistema. Desde el terminal ejecutamos el siguiente comando (**figura A2-20**):

modprobe tun

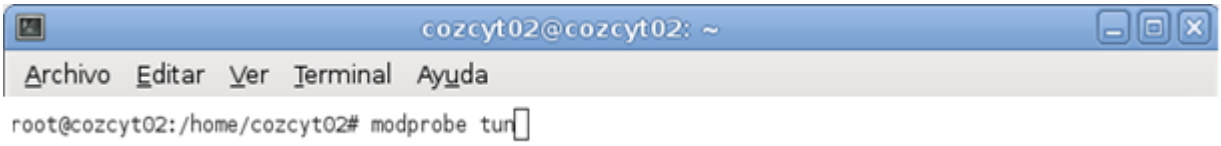


Figura A2-20 Agregación de tun al inicio del sistema
(Fuente: Obtenida de investigación realizada)

Ahora pasamos a editar el fichero /etc/modules, y en la última línea deberá de aparecer tun (**figura A2-21**). Si no fuera así lo añadiremos nosotros.

gedit /etc/modules

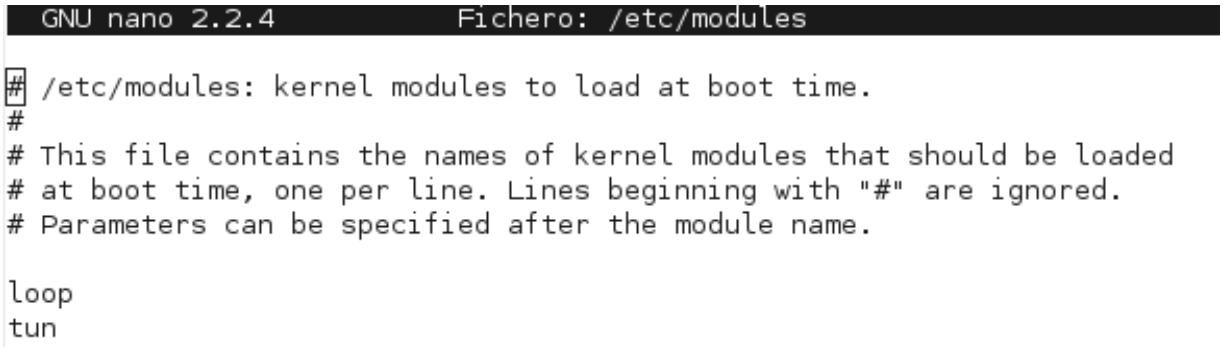


Figura A2-21 Configuración del archivo modules
(Fuente: Obtenida de investigación realizada)

Forwarding de direcciones IP

Nuestro equipo con Chillispot estará trabajando como un firewall, de hecho, sin las reglas de firewall no sería posible que Chillispot funcionara.

Al funcionar como firewall debe tener la capacidad de hacer NAT (Network Address Translation) para lo que ejecutamos el siguiente comando:

echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

En la **figura A2-22** se muestra la ejecución del comando mencionado anteriormente.

Figura A2-22 Asignación de valor para hacer NAT
(Fuente: Obtenida de investigación realizada)

Ahora editamos el archivo sysctl (**figura A2-23**):

gedit /etc/sysctl.conf

Figura A2-23 Edición del archivo sysctl
(Fuente: Obtenida de investigación realizada)

Nos aseguramos que posea la siguiente línea (si no la posee la agregamos y si se encuentra comentada con # al principio se lo quitamos):

net.ipv4.ip_forward=1(**figura A2-24**)**.**

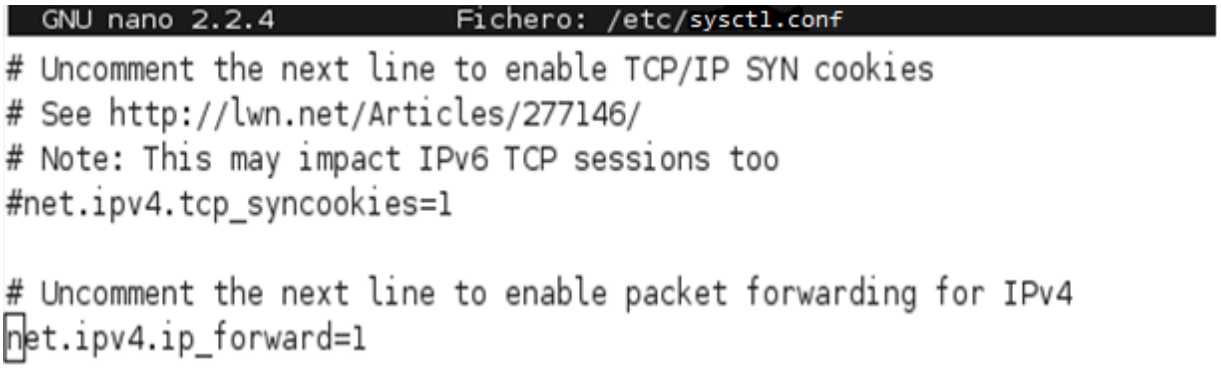


Figura A2-24 Agregación de: net.ipv4.ip_forward=1
(Fuente: Obtenida de investigación realizada)

Ahora ya tenemos configurado nuestro firewall para que sea capaz del redireccionamiento entre las interfaces interna y externa.

Instalación de ChilliSpot

Para proceder a la instalación de ChilliSpot, accederemos al directorio donde, en el punto 3.18 nos descargamos el paquete *.deb de chillispot.

Una vez en la ubicación oportuna, en nuestro caso /home/hermi/Servidor, para la instalación ejecutamos el comando (**figura A2-25**):

dpkg -i chillispot_1.0_i386.deb

Figura A2-25 Instalación de ChilliSpot
(Fuente: Obtenida de investigación realizada)

Hasta aquí ya tenemos instalado ChilliSpot con alguna configuración básica. Estas configuraciones se encuentran en /etc/chilli.conf donde podemos modificarlas y aun definir otros parámetros. Esto se hará posteriormente, entro de la documentación de ChilliSpot encontramos el archivo hotspotlogin.cgi (generalmente viene comprimido y lo encontramos como hotspotlogin.cgi.gz).

Descomprimimos el archivo y lo copiamos en la carpeta /usr/lib/cgi-bin (**figura A2-26**).

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

Figura A2-26 Descomprimir y copiar el archivo hotspotlogin.cgi
(Fuente: Obtenida de investigación realizada)

Con esto ya tenemos nuestro servidor de autenticación. Faltaría configurarlo los aspectos más relevantes.

Edición de los archivos de configuración

Básicamente los archivos de configuración a modificar son cuatro:

- /etc/chilli.conf.
- /usr/local/etc/raddb/clients.conf.
- /usr/lib/cgi-bin/hotspotlogin.cgi.
- /etc/init.d/chillispot.iptables.

Modificación de chilli.conf

Aquí es donde definimos los parámetros propios de Chillispot, los cuales explicamos a continuación.

- 'net': Es la red sobre la cual estará trabajando Chillispot, es decir la Wireless LAN. Se debe poner con el formato <dirección IP>/<mascara de subred>.
- 'radiusserver': La dirección IP de los servidores RADIUS. Es necesario indicar dos servidores, aunque en nuestro caso solamente contamos con uno. Debido a que el servicio de RADIUS se encuentra corriendo en el mismo equipo, utilizamos la dirección de loopback.
- 'radiussecret': Cadena de caracteres que indica el secreto compartido entre Chillispot y el servidor RADIUS.
- 'dns': Dirección IP del servidor DNS.
- 'dhcpif': Interfaz conectada al punto de acceso y por la que se proveerá DHCP. Dicho sea de paso que en la red sobre la que esté trabajando Chillispot no debe haber ningún servidor DHCP activado, dado que este servicio lo proporciona Chillispot mismo.

- 'uamallowed': Aquí podemos especificar direcciones IP o nombres de dominio a los que se permitirá el acceso sin autenticación. Como mínimo debemos poner la dirección IP del servidor web al que serán redireccionados los usuarios no registrados y la dirección IP del Servidor de Nombres de Dominio (DNS).
- 'uamserver': URL del servidor de autenticación.
- 'uamsecret': Secreto compartido entre Chillispot y el servidor de autenticación.

Utilizando el editor nano abrimos el archivo para poder editarlo (**figura A2-27**):

nano /etc/chilli.conf

Figura A2-27 Edición del archivo chilli.conf
(Fuente: Obtenida de investigación realizada)

El archivo completo debe quedar con la siguiente estructura (**Figura A2-28** a **Figura A2-36**):

```
# TUN parameters

# TAG: net
# IP network address of external packet data network
# Used to allocate dynamic IP addresses and set up routing.
# Normally you do not need to uncomment this tag.
net 172.16.64.0/255.255.192.0
```

Figura A2-28 Red sobre la que trabaja chillispot
(Fuente: Obtenida de investigación realizada)

```
# TAG: radiussecret
# Radius shared secret for both servers
# For all installations you should modify this tag.
radiussecret testing123
```

Figura A2-29 Cadena del secreto compartido entre Radius y Chillispot
(Fuente: Obtenida de investigación realizada)

```
# TAG: dns1
# Primary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
dns1 192.168.1.254

# TAG: dns2
# Secondary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
dns2 192.168.1.254
```

Figura A2-30 Dirección IP del servidor DNS
(Fuente: Obtenida de investigación realizada)

```
# TAG: radiusserver1
# IP address of radius server 1
# For most installations you need to modify this tag.
radiusserver1 127.0.0.1

# TAG: radiusserver2
# IP address of radius server 2
# If you have only one radius server you should set radiusserver2 to the
# same value as radiusserver1.
# For most installations you need to modify this tag.
radiusserver2 127.0.0.1
```

Figura A2-31 Dirección IP del servidor RADIUS (loopback)
(Fuente: Obtenida de investigación realizada)

```
# DHCP Parameters

# TAG: dhcpif
# Ethernet interface to listen to.
# This is the network interface which is connected to the access points.
# In a typical configuration this tag should be set to eth1.
dhcpif eth0
```

Figura A2-32 Interfaz por la que se proveerá dhcp
(Fuente: Obtenida de investigación realizada)

```
# Universal access method (UAM) parameters

# TAG: uamserver
# URL of web server handling authentication.
uamserver https://172.16.64.1/cgi-bin//hotspotlogin.cgi

# TAG: uamhomepage
# URL of welcome homepage.
# Unauthenticated users will be redirected to this URL. If not specified
# users will be redirected to the uamserver instead.
# Normally you do not need to uncomment this tag.
uamhomepage http://172.16.64.1/spot

# TAG: uamsecret
# Shared between chilli and authentication web server
uamsecret secretouam
```

Figura A2-33 Url de servidor de autenticación y secreto entre ChilliSpot y servidor de autenticación
(Fuente: Obtenida de investigación realizada)

```
# TAG: uamallowed
# Comma separated list of domain names, IP addresses or network segments
# the client can access without first authenticating.
# It is possible to specify this tag multiple times.
# Normally you do not need to uncomment this tag.
uamallowed 172.16.64.1
```

Figura A2-34 Dirección IP del sitio web
(Fuente: Obtenida de investigación realizada)

```
# TAG: radiusnasid
# Radius NAS-Identifier
# Normally you do not need to uncomment this tag.
radiusnasid nas01
```

Figura A2-35 radiusnasid
(Fuente: Obtenida de investigación realizada)

```
# TAG: radiuslisten
# IP address to listen to
# Normally you do not need to uncomment this tag.
radiuslisten 127.0.0.1
```

Figura A2-36 Dirección de loopback para redireccionar a los usuarios
(Fuente: Obtenida de investigación realizada)

Una vez, que se realizó la configuración del archivo /etc/chilli.conf, y que contenga las configuraciones denotadas en las imágenes anteriores, se procede a pasar a los siguientes ficheros de configuración.

Modificación de users en FreeRADIUS

Se ha partido de un sistema Debian, el cual ya habíamos instalado FreeRADIUS y configurado, por lo que los usuarios, los cuales se configuran en el fichero /usr/local/etc/raddb/users, ya están creados.

A modo de repaso, se puede acceder al fichero users, anterior, y confirmar los usuarios (**figura A2-37**). En el caso que nos ocupa, como se puede apreciar, el usuario es uno:

Usuario: labsol password: L485ol2013

Figura A2-37 Modificación de archivo users de FreeRADIUS
(Fuente: Obtenida de investigación realizada)

Al final del documento se pueden observar los usuarios, junto con la sintaxis (**figura A2-38**). Podríamos añadir tantos usuarios como quisiéramos.

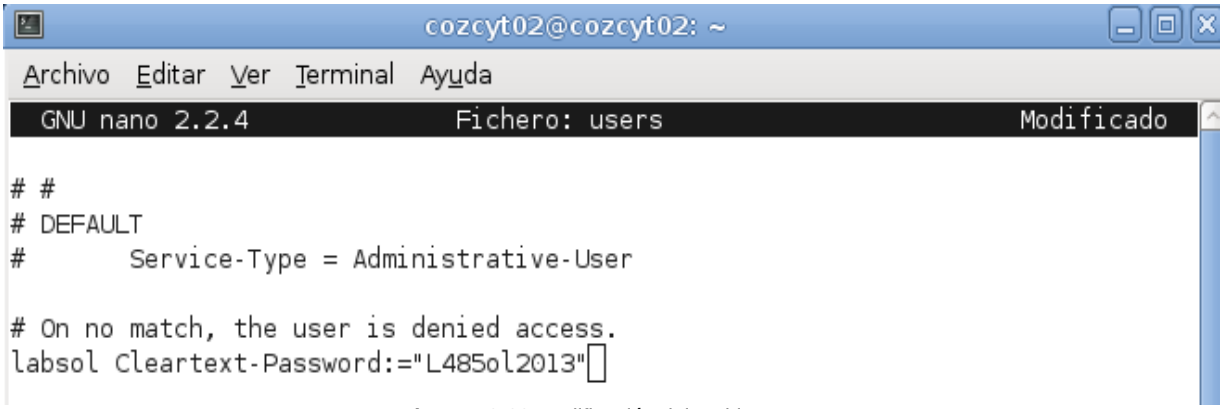


Figura A2-38 Modificación del archivo users
(Fuente: Obtenida de investigación realizada)

Configuración de clients.conf

Dado a que en nuestro caso la dirección IP del servidor RADIUS es la de loopback por estar en el mismo equipo en que se encuentra ChilliSpot, debemos verificar que dentro de los clientes se encuentre especificado nuestro host local y si no se encuentra agregarlo. Si el caso fuera un servidor RADIUS remoto, deberíamos agregar la dirección IP a través de la cual es visible para RADIUS el host con ChilliSpot. Abrimos el fichero con nano (**figura A2-39**):

nano /usr/local/etc/raddb/clients.conf

Figura A2-39 Ubicación del archivo clients.conf
(Fuente: Obtenida de investigación realizada)

Para el primer caso expuesto, el archivo debe quedar como en la **figura A2-40:**

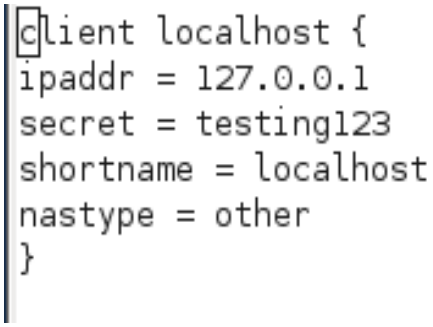


Figura A2-40 Configuración de clients.conf
(Fuente: Obtenida de investigación realizada)

Modificación de hotspotlogin.cgi

Abrimos el fichero con nano (**figura A2-41**):

nano /usr/lib/cgi-bin/hotspotlogin.cgi

Figura A2-41 Edición del archivo hotspotlogin.cgi
(Fuente: Obtenida de investigación realizada)

Lo único que debemos hacer es verificar que no se encuentre comentada la línea $uamsecret = “secretouam”; Donde secretouam es el secreto compartido entre Chillispot y el servidor de autenticación. Además, descomentamos la línea $userpassword=1, como lo indica la **figura A2-42**.

```
# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
$uamsecret = "secretouam";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1;
```

Figura A2-42 Descomentar líneas: $uamsecret=”secretouam”; y $userpassword=1;
(Fuente: Obtenida de investigación realizada)

Posteriormente, deberemos de dar permisos a los ficheros como lo indica la **figura A2-43**:

chmod 755 /usr/lib/cgi-bin/hotspotlogin.cgi

chmod 755 /usr/lib/cgi-bin

Figura A2-43 Asignación de permisos al archivo hotspotlogin.cgi
(Fuente: Obtenida de investigación realizada)

Configuración de chillispot.iptables

ChilliSpot ya incluye una configuración de iptables sugerida. La podemos encontrar dentro de su documentación con el nombre “firewall.iptables” y copiarla para hacer uso de ella, copiarla del lugar donde se encuentra al directorio “/etc/nit.d/” para que se ejecute al iniciar el sistema, al copiar el archivo podemos cambiarle nombre si así lo deseamos, lo último que se hará es cambiar los permisos como lo indica la **figura A2-44**.

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

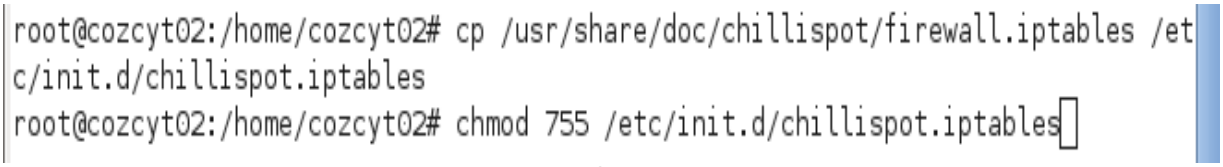


Figura A2-44 Copia y asignación de permisos a chillispot.iptables
(Fuente: Obtenida de investigación realizada)

Después de copiarla y darle permisos de ejecución abrimos el archivo con nano:

nano /etc/init.d/chillispot.iptables

Luego verificamos que los parámetros INTIF y EXTIF contengan las interfaces interna (la que va a la red inalámbrica) y externa (la que conecta a la WAN), respectivamente.

En nuestro caso queda de la siguiente manera:

EXTIF = “eth0”
INTIF = “eth1”

En la **figura A2-45** se muestra la forma del archivo chillispot.iptables en el que se configura las tarjetas de red.

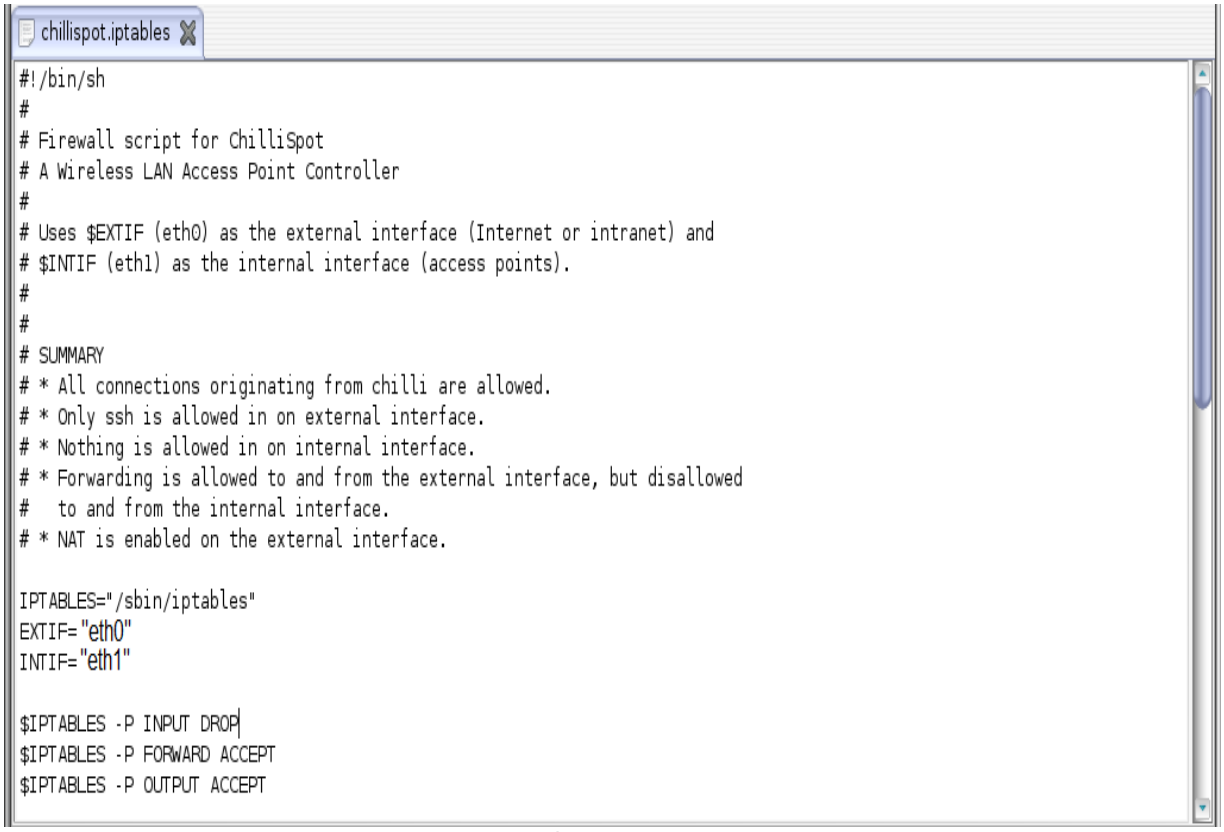


Figura A2-45 Edición del archivo chillispot.iptables
(Fuente: Obtenida de investigación realizada)

Por último agregamos las reglas al inicio del sistema (**figura A2-46**):

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

Figura A2-46 Agregación de las reglas al inicio del sistema
(Fuente: Obtenida de investigación realizada)

Creación de sitio corporativo de recepción de peticiones de conexión

Para la creación del sitio corporativo accedemos a la carpeta /var/www, y creamos un directorio donde depositaremos la página que los usuarios verán cuando se quieran conectar por primera vez. En este ejemplo, este directorio, se llamara, spot.

En su interior, con un editor, como por ejemplo nano o gedit, creamos un archivo index.html, el cual debe tener el siguiente código que hará el redireccionamiento al portal (**figura A2-47**).

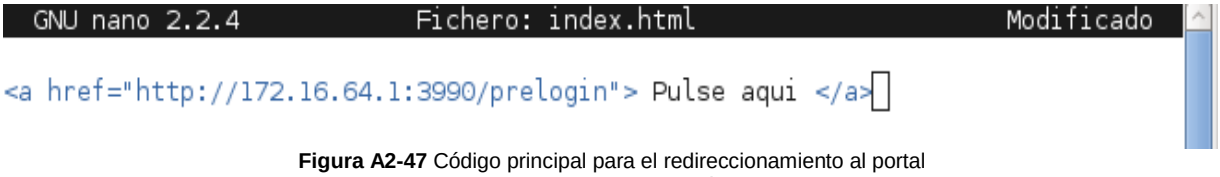


Figura A2-47 Código principal para el redireccionamiento al portal
(Fuente: Obtenida de investigación realizada)

Iniciando nuestro servidor ChilliSpot.

Ahora nuestro Servicio de portal cautivo está listo para iniciarse. Basta con ejecutar los comandos que se muestran en la **figura A2-48**.

Figura A2-48 Reinicio de todos los servicios
(Fuente: Obtenida de investigación realizada)

A la hora de inicializar FreeRADIUS, tenemos la opción de lanzarlo en un terminal independiente, y que las peticiones que reciba sean visibles, el comando seria:

radiusd -f –X

Al abrir un navegador e introducir la IP del servidor RADIUS más la dirección del sitio que se creó nos debe mostrar nuestro sitio.

E n la **figura A2-49** se muestra la página de cómo puede quedar nuestro sitio.

Figura A2-49 Sitio corporativo del portal cautivo
(Fuente: Obtenida de resultados de investigación)

Para verificar que el servidor está realizando la autenticación de los usuarios, damos clic en la imagen de invitado y tiene que aparecer el login como lo muestra la **figura A2-50**.

Figura A2-50 Página de login para accesar a la red
(Fuente: Obtenida de resultados de investigación)

Anexo III: Configuración de FreeRADIUS con base de datos

En este apartado se realizara la configuración de los archivos de FreeRADIUS para que se pueda realizar la conexión con una base de datos y de esta forma ya no se tendrá que estar editando el archivo users para poder agregar usuarios, en su caso se puede realizar una aplicación simple para agregar los usuarios o también se puede buscar e instalar una aplicación que ya exista por ejemplo daloRADIUS.

Lo primero que se tendrá que hacer es verificar que se tiene instalado un gestor de base de datos, en caso de tenerlo, se deberá instalar. Para este caso se utilizara MySQL, una vez que se tenga instalado MySQL se tendrá que identificar el usuario (puede ser root o se puede crear un usuarios diferente) y la contraseña para poder realizar la conexión de FreeRADIUS con MySQL. Una vez que se tenga el usuario y la contraseña se pasara a la configuración de los archivos **radiusd.conf**, **default** y **sql.conf**

El primer archivo que se configurara es el archivo default, en este archivo se descomentará la línea **$INCLUDE sql.conf**, este archivo se encuentra en el directorio "/usr/local/etc/raddb/", abrimos con nano como se muestra en la **figura A3-1**.

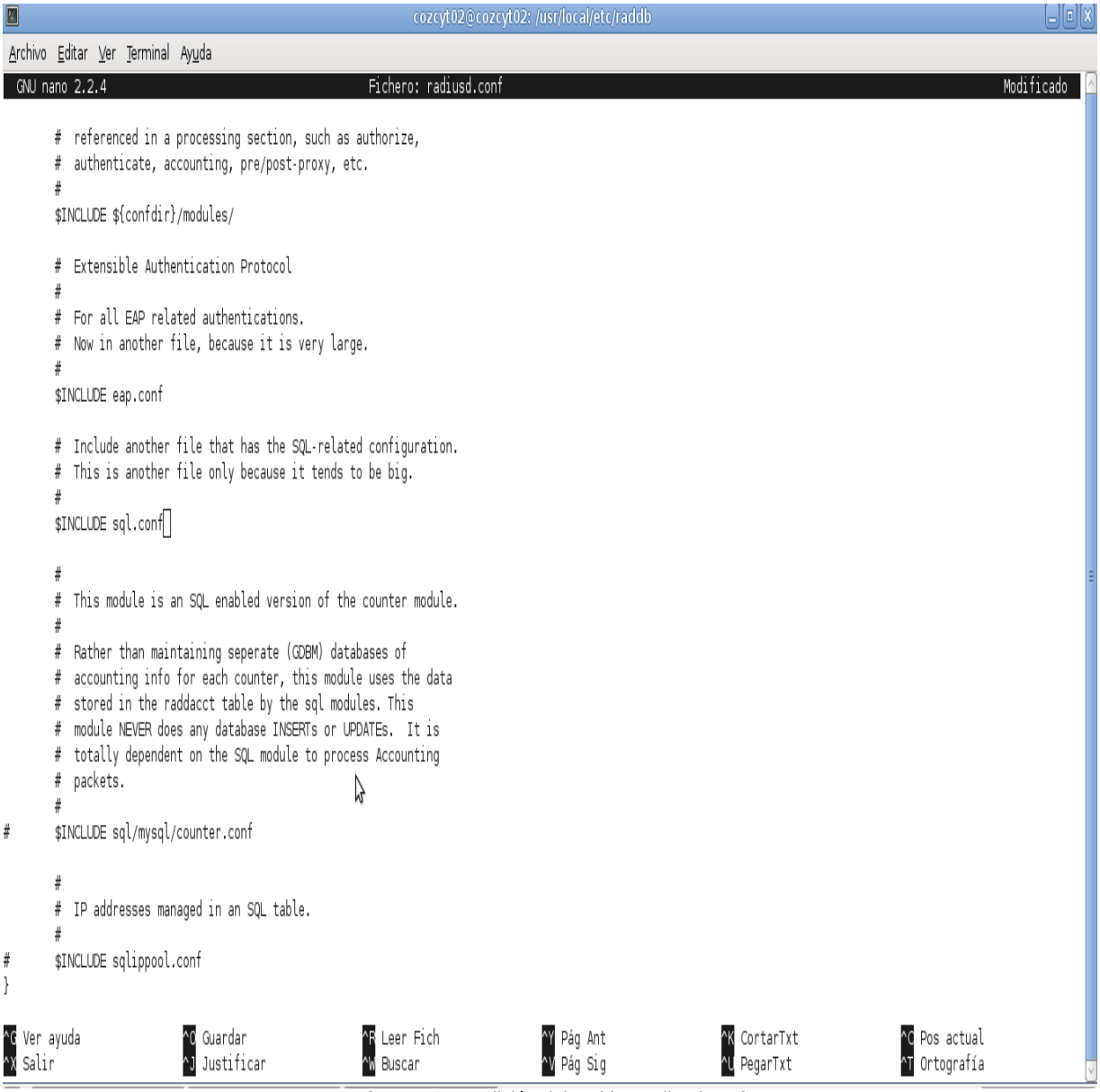


Figura A3-1: Edición del archivo radiusd.conf
(Fuente: Obtenida de investigación realizada)

El siguiente archivo que se configurara es default, el cual se encuentra en el directorio "/usr/local/et/raddb/sites-available/", en este archivo se descomentan las variables **sql** de las secciones Accouting, Sesión, Authorize y Post-Auth.

En la **figura A3-2**. Se muestra la forma como debe quedar el archivo.

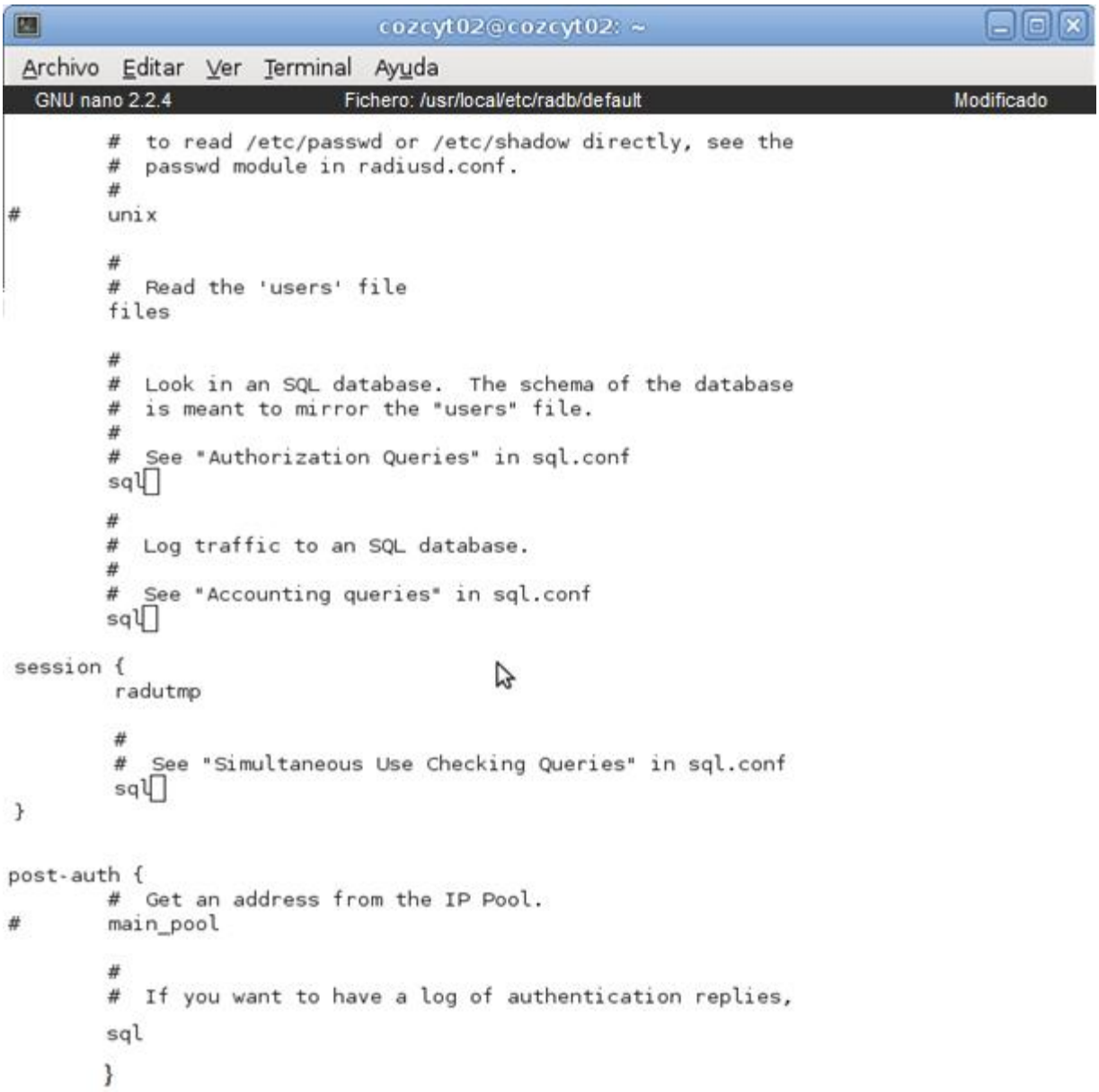


Figura A3-2: Edición del archivo default
(Fuente: Obtenida de investigación realizada)

En el archivo anterior se agregan o se descomentan las variables **sql** en las secciones indicadas puesto que esto servirá para que el servidor RADIUS reconozca sintaxis sql y se pueda llevar un control más practico y fácil de los inicios de sesión, de las cuentas y de las peticiones de autenticación reciba el servidor.

El ultimo archivo que se tiene que configurar es sql.conf, en este archivo se configura el usuario y la contraseña de la base de datos para que FreeRADIUS pueda acceder (**figura A3-3**), este archivo se encuentra en el directorio “/usr/local/etc/raddb/”.

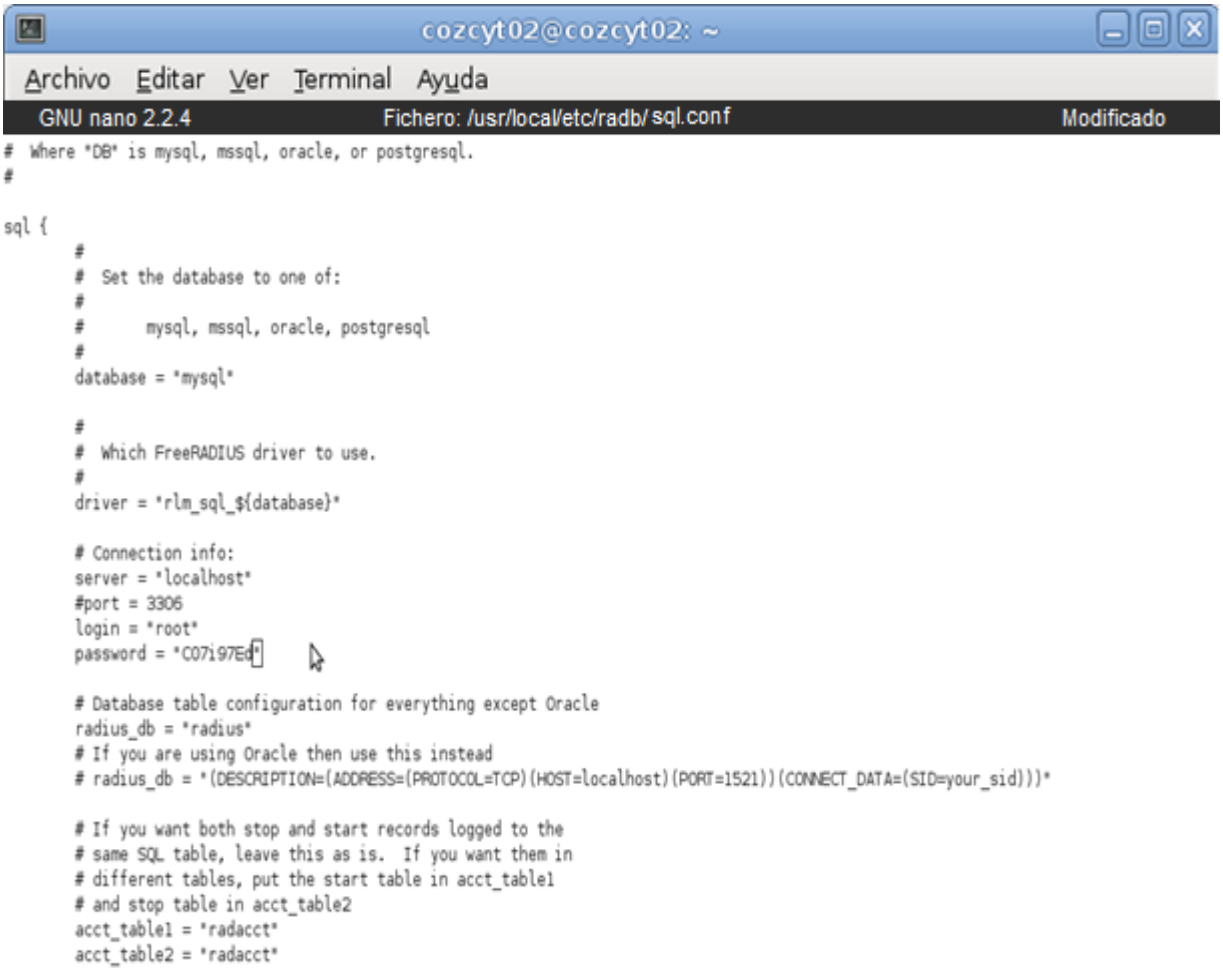


Figura A3-3: Edición del archivo sql.conf
(Fuente: Obtenida de investigación realizada)

Hasta este momento ya se tienen configurados los archivos para realizar la conexión de FreeRADIUS con MySQL, lo que falta es crear la base de datos y las tablas que utilizara FreeRADIUS, las tablas se crean a partir de unos scripts que trae FreeRADIUS los cuales se encuentran en el directorio “/usr/local/etc/raddb/sql/mysql/”, los scripts que se tienen que exportar a la base de datos para que se creen las tablas son: ippool.sql, nas.sql y schema.sql.

Para ejecutar los scripts nos ubicamos en el directorio indicado anteriormente y ejecutamos el siguiente comando (ver **figura A3-4**):

mysql -u root -p radius < xxxx.sql

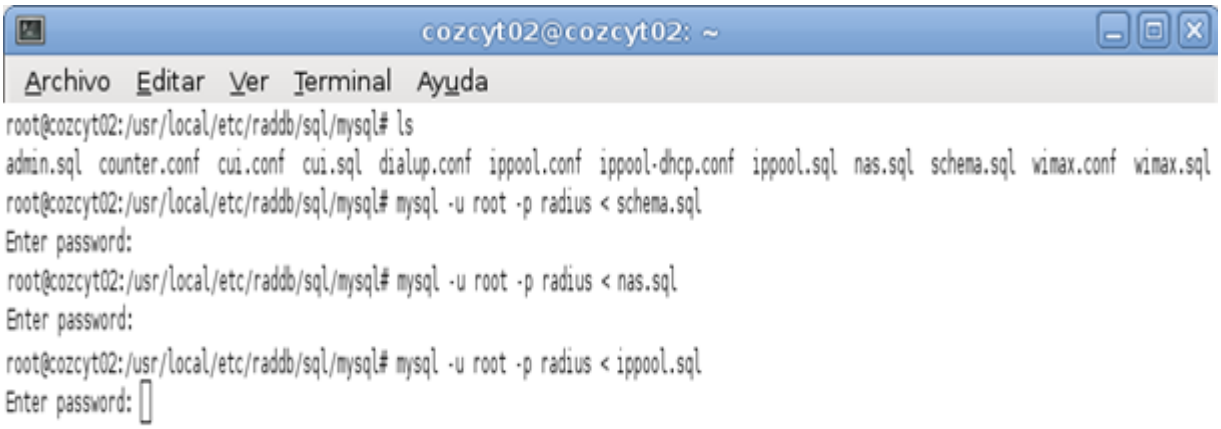


Figura A3-4: Creacion de las tablas para FreeRADIUS
(Fuente: Obtenida de investigación realizada)

Referencias

(Marzo de 2014). Obtenido de Seguridad en redes: http://www.redusers.com/noticias/seguridad-en-redes-autenticacion-con-servidores-aaa/

(Abril de 2014). Obtenido de Seguridad WEP: http://www.tech-faq.com/wep-wired-equivalent-privacy.html

(Abril de 2014). Obtenido de Servidor HTTP: http://www.edu4java.com/es/web/web30.html

(Abril de 2014). Obtenido de Servidor web Apache: http://es.opensuse.org/Apache

(Febrero de 2014). Obtenido de Servidores RADIUS: http://trabajotele08.blogspot.mx/

debian. (Abril de 2014). Obtenido de Debian: https://www.debian.org/index.es.html

Gutierrez, A. (Marzo de 2014). *Windows en español*. Obtenido de Red inalambrica, lo que necesitas saber: http://windowsespanol.about.com/od/RedesYDispositivos/a/Red-Inalambrica.htm

moderna, i. (Marzo de 2014). *Las redes inalambricas*. Obtenido de Redes inalambricas: http://www.informaticamoderna.com/Redes_inalam.htm

Muy linux. (Abril de 2014). Obtenido de Debian como servidor: http://www.muylinux.com/2013/10/25/debian-sigue-numero-uno-en-servidores

overblog. (Febrero de 2014). *Definición del experto*. Obtenido de Que es un servidor NAS: http://es.over-blog.com/Que_es_un_servidor_NAS_definicion_del_experto-1228321779-art379097.html

Pro y contra de Apache. (Febrero de 2014). Obtenido de Pro y contra de Apache: http://ldc.usb.ve/emilio/Portafolio/Software/REDES3/G5b/Presenta_Site/caracteristicas_pyc.htm

Robotic, U. S. (Abril de 2014). *Guia del usuarios de la USRobotics*. Obtenido de Filtrado de direcciones MAC: http://support.usr.com/support/9106/9106-es-ug/casestudy.html

Rodriguez, G. (Abril de 2014). *diverlandia*. Obtenido de Instalacion de Debian paso a paso: http://www.driverlandia.com/instalacion-de-debian-6-paso-a-paso/

Schauer, H. (Abril de 2014). *HSC Articles*. Obtenido de Seguridad inalámbrica: http://www.hsc.fr/ressources/articles/ hakin9_wifi/hakin9_wifi_ES.pdf

Seguridad en redes. (Febrero de 2014). Obtenido de Autenticación con servidores AAA: protocolo aaa http://www.redusers.com/noticias/seguridad-en-redes-autenticacion-con-servidores-aaa/

Tal, L. (Marzo de 2014). *daloRADIUS*. Obtenido de daloRADIUS: http://www.daloradius.com/

wikipedia. (Febrero de 2014). Obtenido de Protocolo AAA: http://es.wikipedia.org/wiki/Protocolo_AAA

wikipedia. (Febrero de 2014). Obtenido de Portales cautivos: http://es.wikipedia.org/wiki/Portal_cautivo

Wikipedia. (Abril de 2014). Obtenido de sistema operativo Linux: http://es.wikipedia.org/?title=GNU/Linux

Wikipedia. (Marzo de 2014). *Estandar IEEE 802.11x*. Obtenido de Wikipedia: http://es.wikipedia.org/wiki/IEEE_802.11