UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA: INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del título de: INGENIERO DE SISTEMAS

TEMA:
ANÁLISIS, DISEÑO Y PROPUESTA DE IMPLEMENTACIÓN DE UN PORTAL CAUTIVO PARA LA RED INALÁMBRICA DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE QUITO CAMPUS SUR

AUTORES:
DIEGO XAVIER MENA FLORES
JONATHAN JAVIER JARA LLUMIGUSÍN

DIRECTOR:
JORGE LÓPEZ LOGACHO

Quito, octubre de 2013

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO

Nosotros Diego Xavier Mena Flores y Jonathan Javier Jara Llumigusín autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

.....	.....
Diego Xavier Mena Flores	**Jonathan Javier Jara Llumigusín**
C.I. 1724004781	**C.I.** 1722589999

DEDICATORIA

Este proyecto lo dedico a Dios, por sus bendiciones lo que ha permitido llegar a la culminación de mi formación profesional. A mi madre, ser tan maravilloso que con paciencia, confianza, y cariño incondicional me ha acompañado durante todo mi ciclo de estudios y vida, a mi padre quien con sus consejos ha sabido guiarme por el camino correcto para culminar mi carrera, y en especial a mi abuelita por todo su esfuerzo, comprensión, dulzura y ser un pilar muy importante en mi vida y en mi corazón.

Jonathan Javier Jara Llumigusín

Dedico este trabajo principalmente a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional. A mi madre, por apoyarme en todo momento de mi vida y darme las fuerzas para nunca rendirme ante las dificultades. A mi padre, porque gracias a todos sus sacrificios hoy puedo terminar esta etapa de mi vida. A mis hermanas Gabriela y Daniela, por ayudarme en el momento que más las necesitaba de ellas. A mi familia en general, porque me han brindado su apoyo incondicional y por compartir conmigo buenos y malos momento. Finalmente a mi compañero Jonathan, ya que gracias a su esfuerzo y dedicación hemos podido lograr esta meta juntos.

Diego Xavier Mena Flores

AGRADECIMIENTO

Agradezco de manera especial a la empresa en la que laboró CONSPECCIME CIA. LTDA. por darme las facilidades físicas, tecnológicas y el tiempo para la elaboración del presente Proyecto de Tesis.

Jonathan Javier Jara Llumigusín

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El proyecto de tesis describe una propuesta de implementación de un portal cautivo para red inalámbrica de la Universidad Politécnica Salesiana campus Sur, ya que la misma presta servicios a estudiantes, docentes y cuerpo administrativo, por lo que la seguridad de la red debe ser controlada rigurosamente para evitar el uso inadecuado del servicio de internet por terceras personas o ajenas a la Universidad, por lo cual existen diversos métodos seguridad y control de acceso.

El avance de la tecnología hoy en día está generando que la mayoría de dispositivos electrónicos ya incorporen tecnología Wireless o conectividad inalámbrica, permitiéndoles de esta manera acceder a cualquier red inalámbrica que se encuentre dentro su alcance.

Por lo que un método de seguridad será la implementación de un portal cautivo, el mismo que estará instalado en un sistema operativo Linux y configurado con componentes de libre licenciamiento. El portal estará gestionado principalmente por el software Chillispot, que es un tipo de portal cautivo y este a su vez se comunicará internamente con un servidor RADIUS el mismo que será el encargado de la autenticación de los usuarios antes de dar paso a la navegación web a través de un "Nombre de Usuario y Password", estos datos serán consultados desde una base de datos especifica llamada radius creada en MySQL, la cual adicionalmente almacenará todos los registros de los usuarios en cuanto a información de identificación y utilización del portal cautivo.

Adicionalmente el portal contará con software de administración gráfica como son: PHPMYADMIN y DALORADIUS, los mismos que facilitaran de manera significativa la administración, control y gestión de usuarios dentro del portal cautivo, ya que en un sistema Linux todos los procesos se los realiza mediante consola de comandos o terminal.

ABSTRACT

This thesis describes a proposal to implement a captive portal for wireless network Salesian University South Campus, since it serves students, teachers and administrative body, so that the security of the network must be controlled carefully to avoid misuse of the Internet service by third parties or outside the University, for which there are various methods and access control security.
The advancement of technology today is generating most electronic devices now incorporate Wireless or wireless technology, this enabling access to any wireless network that is within reaches.

As a security method will be to implement a captive portal, the same will be installed on a Linux operating system and configured with free licensing components. The portal will be managed primarily by Chillispot software, which is a type of captive portal and this in turn will communicate with RADIUS server internally the same as will be responsible for authentication of users before giving way to web browsing through a "User Name and Password", this data will be viewed from a specified database created in MySQL called radius, which additionally store all user records information about identifying and using captive portal.

Additionally, the portal provides graphical management software including: PHPMYADMIN and DALORADIUS, the same that significantly facilitated the administration, control and management within the captive portal users, since in a Linux system all processes are performed by console command or terminal.

INTRODUCCIÓN

La Universidad Politécnica Salesiana sede Quito Campus Sur posee una infraestructura de red WLAN muy organizada la cual proporciona varios servicios a los usuarios entre ellos el servicio de internet, pero se la considera como poco segura por lo que se ofrece una solución mediante el trabajo de investigación.

A continuación se presenta una propuesta para la implementación de un portal cautivo ya que el mismo que permitirá una mejor administración y control de acceso de usuarios al servicio internet de la Universidad Politécnica Salesiana sede Quito Campus Sur, además el portal estará enfocado a reforzar la seguridad ya existente en la infraestructura de red actual, mediante el uso de software de licenciamiento libre y el protocolo AAA permitiendo la autenticación de todos los usuarios que deseen tener acceso al servicio de internet inalámbrica.

CAPÍTULO 1
MARCO REFERENCIAL

1.1. Introducción

El internet hoy por hoy es una herramienta esencial en la actualidad ya que permite la comunicación como también la capacidad de compartir información, sin importar el lugar o la distancia.

Inicialmente las redes eran en su mayoría cableadas lo que limitaba la movilidad de los usuarios, pero con la evolución de la tecnología este paradigma ha cambiado hasta permitir que los usuarios puedan utilizar redes sin la necesidad de conectarse a cables o inclusive mientras se trasladan de un lugar a otro, a este tipo de redes se las denomina redes Wireless o WLAN.

Las WLAN son cada vez más utilizadas tanto en redes de oficina como hogar, pero por las características de las redes WLAN y su medio de transmisión se deben tomar medidas de precaución para mantener la confiabilidad, integridad, seguridad y el rendimiento de la red. Dentro de este contexto, será necesario emplear mecanismos para la administración y el control del acceso a usuarios mediante la autentificación de los mismos.

Este documento presenta una propuesta para la implementación de un portal cautivo ya que este permite un método de control de acceso a usuarios de internet de la Universidad Politécnica Salesiana sede Quito Campus Sur, la cual estará enfocada a reforzar la seguridad ya existente en la red actual mediante el uso de herramientas de libre licenciamiento que permitan la autenticación de los usuarios para tener acceso al servicio de internet.

1.2. Justificación

Un portal cautivo es un medio de seguridad en red que fuerza a un cliente HTTP a ver una página web inicial, que usualmente se usa para autenticar a dicho cliente.

Una vez que el cliente se ha autenticado correctamente, puede usar el servicio web de forma normal.

Este proyecto surge por la necesidad de poder brindar seguridad al restringir el acceso a usuarios no autorizados al recurso de internet en la red Inalámbrica utilizando Portales Cautivos. En la cual se utilizará software libre de Linux, ya que cualquier dispositivo que tenga las capacidades de conexión inalámbrica puede conectarse a la red de la Universidad Politécnica Salesiana, por lo cual se necesita primordialmente una clave de acceso y adicionalmente un control más riguroso sobre los usuarios que acceden a la misma es ahí donde los portales cautivos cobran un especial interés.

Por ello, una de las principales metas de los Portales Cautivos es restringir el acceso al servicio de internet en redes WLAN, a los usuarios que no pertenecen a la red lo que permitirá que el ancho de banda sea administrado adecuadamente para obtener calidad de servicio. Esto permitirá que la red sea más segura y el acceso de los usuarios sea más ordenado y eficiente lo que beneficiará al administrador de la red puesto que es una forma de seguridad que permite decidir quién tiene acceso al servicio de internet, como también permite obtener registros de quien ha utilizado el servicio.

El beneficio principal que obtendrá la Universidad será el tener una línea de seguridad enfocada a su red Inalámbrica, como el bloqueo de usuarios no autorizados a acceder a la red lo que mejora el rendimiento y la calidad de servicio de la misma.
La mayor aportación del portal cautivo es que podrá ser implementada sobre otras redes inalámbricas de otros campus de la Universidad con algunos estudios y modificaciones a la configuración para que se adapte a la estructura donde vaya a ser implementada. Este proyecto se podrá aplicarse a futuras redes inalámbricas que vayan a ser implementadas en el recinto de la Universidad.

1.3. Formulación del Problema

Las tendencias tecnológicas actuales se enfocan cada vez más en la utilización de redes inalámbricas por sus beneficios de movilidad, flexibilidad, escalabilidad y

costo, aunque también presentan algunas desventajas especialmente en la seguridad, ya que el medio en el que se trasmiten las redes inalámbricas es de ondas electromagnéticas, lo cual las vuelve más vulnerables al acceso de usuarios no autorizados que pueden ingresar de manera sencilla a las redes inalámbricas, lo que resulta complejo o dificultoso de detectar a los usuarios no autorizados que ingresan para el administrador de red, puesto que no puede tener un control exacto de quienes entran a la red.

La seguridad de la WLAN de la universidad debe ser controlada rigurosamente para evitar el uso inadecuado de los recursos, para lo que existen diversos métodos de control y seguridad como WEP, OSA, ACL, CNAC, Portales Cautivos, IDS entre otros, cada uno con distinta manera de brindar seguridad al acceso inalámbrico.

Uno de los principales problemas que posee la red inalámbrica de la Universidad Politécnica Salesiana Sede Quito Campus Sur, es la seguridad para el evitar los posibles ataques de acceso a la misma y por ende al servicio de internet de manera no autorizada, puesto que el password de ingreso a la misma, se encuentra publicado a vista de estudiantes y público en general, lo que genera que usuarios propios y ajenos a la universidad puedan ingresar sin ningún tipo de control de acceso.

Por otra parte la falta de un registro de todos los usuarios que ingresan a la red inalámbrica de la Universidad, lo que evita detectar si se presentaron accesos no autorizados o posibles ataques a la red. Por lo que se elige la solución del portal cautivo para evitar el uso inapropiado del internet, como también para evitar posibles problemas como un alto congestionamiento la red por usuarios no vinculados a la Universidad Politécnica Salesiana.

1.4. Objetivos

1.4.1. Objetivo General:

- Analizar, diseñar y generar una propuesta de implementación de un portal cautivo para la red Inalámbrica de la Universidad Politécnica Salesiana Sede Quito Campus Sur.

1.4.2. Objetivos Específicos:

- Analizar el estado actual de las redes inalámbricas que posee la Universidad Politécnica Salesiana campus Sur mediante el levantamiento inicial de la red.

- Investigar las funcionalidades, características, arquitectura de un portal cautivo, y requerimientos necesarios para su implementación.

- Diseñar un escenario de prueba que permita mostrar las funcionalidades principales del portal cautivo tomando como referencia a la estructura inalámbrica de la Universidad.

- Realizar la factibilidad técnica en base a las configuraciones y equipos requeridos para el funcionamiento de portal cautivo, y la factibilidad económica mediante el costo de inversión que generará la propuesta planteada para Universidad.

- Generar la propuesta de implementación del portal cautivo mediante la documentación obtenida de las configuraciones y las pruebas efectuadas para el funcionamiento del portal cautivo.

1.5. Metodología

El tipo de investigación aplicada a este proyecto se basa en el método científico, que se compone de 5 elementos que son: observación, planteamiento del problema, hipótesis, experimentación que puede ser llevado a cabo en un laboratorio o en la vida real para obtener resultados más precisos en la investigación efectuada.

En el proyecto de investigación las ideas, conceptos, y teorías que se expondrán, serán obtenidos de la recopilación de información de la infraestructura de red, permitiendo así que la propuesta del portal cautivo pueda ser aplicada en la Universidad Politécnica Salesiana Campus Sur, como también en redes inalámbricas de otros campus con las respectivas modificaciones.

Mediante el análisis, diseño de un portal cautivo, requerimientos actuales de la red y conocimientos sobre protocolos de seguridad tales como el protocolo AAA que es utilizado para manejar políticas de seguridad, controlar recursos, administrar y rastrear usuarios, se podría llegar a generar una propuesta de implementación de un portal cautivo para la red inalámbrica, lo que permitirá tener un nuevo filtro que mejorará la seguridad y prohibir el acceso a usuarios no autorizados al recurso de internet de la red inalámbrica de Campus Sur.

Además se utilizará las técnicas que se detallan a continuación:

- Revisión Bibliográfica
- Pruebas de Acceso al recurso de Internet
- Recopilación de información

1.6. Alcance

Dentro del alcance del presente proyecto en un inicio se obtendrá la información sobre la situación actual de las redes inalámbricas que posee la Universidad Politécnica Salesiana Campus Sur, como también los servicios que presta mediante internet.

Un portal cautivo puede ser aplicado mediante software como hardware, en este proyecto de investigación se lo realizará utilizando software de libre licenciamiento, para ser más específicos será Chillispot el portal cautivo a usar, esto quiere decir que no se necesitará de ningún dispositivo físico dedicado a dar esta función, únicamente se necesitará un equipo que corra bajo sistema operativo Linux, el software que realizará el portal cautivo y las configuraciones correspondientes para su funcionamiento, lo que no involucra gran inversión para la Universidad, si se llegará a implementar en un futuro.

Adicionalmente se necesitará obtener información sobre:

- Servidor Radius
- Portales Cautivos basados en Linux

- Servidor HTTP
- Protocolo AAA o (Authentication, Authorization and Accounting)
- Sistema Operativo Linux

En lo que respecta a hardware se necesitará conocer los equipos o dispositivos que posean las características necesarias para soportar la implementación de un ambiente que utilice el portal cautivo.
Con la información obtenida del levantamiento inicial de la red y los requerimientos físicos y lógicos para implementar un portal cautivo, se diseñará un esquema de una red de prueba en la cual se ponga en funcionamiento del portal cautivo.

Se implementará un ambiente de pruebas basado en la topología física y lógica de acuerdo al esquema antes realizado, cabe indicar que el ambiente de pruebas será únicamente utilizando equipos físicos, ya que en este caso al usar simulaciones no hace posible demostrar en detalle el desempeño de portal cautivo por el asunto que se manejan redes y dispositivos inalámbricos por eso físicamente es la forma más práctica de demostrar el funcionamiento del portal cautivo.

Se harán las configuraciones necesarias tanto de los servicios como de los protocolos antes mencionados para el correcto funcionamiento del portal cautivo y las pruebas respectivas de comportamiento de la red con y sin el portal cautivo, se analizarán los datos obtenidos, y se procederá a generar la documentación respectiva de la implementación.

Finalmente se realizará la factibilidad tanto técnica como económica en base a toda la información obtenida de todo el levantamiento de estado inicial de la red que posee la Universidad actualmente.

CAPÍTULO 2
MARCO TEÓRICO

2.1. Introducción a las Redes Inalámbricas

"En los últimos años la tecnología ha avanzado de una manera muy vertiginosa, lo que ha generado nuevas formas de comunicación y trasmisión de la información, que cada vez se enfoca más en lo inalámbrico". (Fernandokatz, 2010)

> Las redes inalámbricas son aquellas que realizan una comunicación por un medio de transmisión no guiado, es decir sin la necesidad de cables, para lo cual se utilizan ondas electromagnéticas, por lo que para la transmisión y recepción de la información se lo hacen mediante antenas. (redesjeaneth.blogspot.com, 2013)

Las redes inalámbricas permiten a sus usuarios conectarse a una red, acceder a información específica y recursos de la red, todo esto sin la necesidad de permanecer físicamente conectado a un determinado lugar. Este tipo de redes funciona de la misma manera que una red cableada ya que permite a los usuarios conectarse a la red, acceder y trabajar con los recursos de la misma, pero ofrece ciertas ventajas importantes como son:

- Rápida instalación
- Movilidad
- Bajo costo de implementación

Inicialmente las redes inalámbricas estaban enfocadas al uso empresarial, pero con el crecimiento de usuarios móviles, estas redes se expandieron a su utilización en lugares públicos y áreas metropolitanas, como medio para acceder a servicios orientados a internet.

Existen 2 categorías de Redes inalámbricas

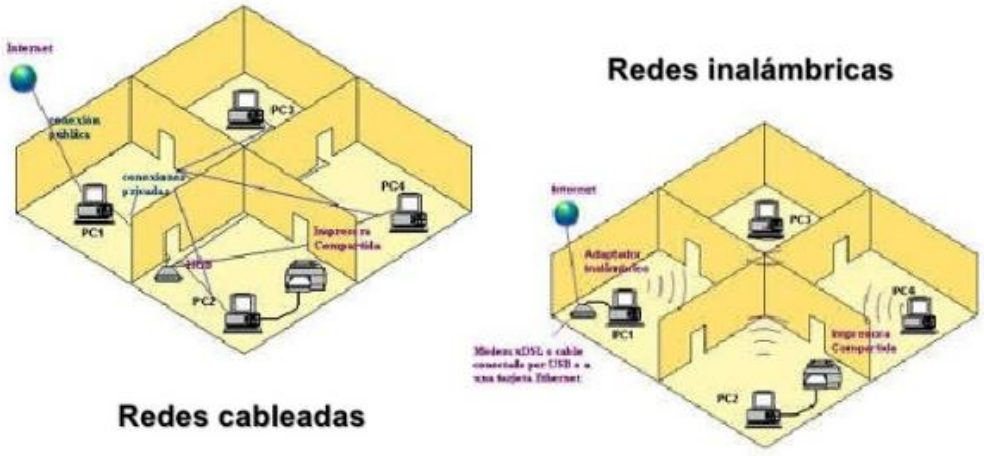
- **De Larga Distancia.-** se utilizan para la transmisión de información en áreas geográficas de gran distancia como son ciudades o entre países vecinos, y la velocidad de transmisión a la cual trabaja es de 4.8 a19.2 Kbps

- **De Corta Distancia.-** se utilizan para la transmisión de información en áreas pequeñas frecuentemente en redes corporativas que abarcan edificios que no son muy alejados entre sí, con velocidades de transmisión desde los 280 Kbps hasta los 2 Mbps

2.1.1. Características de las Redes Inalámbricas

Las redes inalámbricas se han vuelto una tecnología predominante dentro de los usuarios corporativos como también de los usuarios finales ya que presentan las siguientes características:

Figura 1. Redes Cableadas y Redes Inalámbricas



Elaborado por: Jonathan Jara y Diego Mena

Movilidad: Usuarios puedan trabajar desde cualquier lugar de la empresa sin la necesidad de estar en un espacio físico fijo, lo me mejora la productividad.

Simplicidad y Facilidad de Instalación: La instalación de una red inalámbrica elimina la necesidad de realizar cableado a través de paredes y techos, ahorrando

espacio, evitando dañar la estética del lugar y permitiendo así reducir los tiempos de instalación.

Flexibilidad de la Instalación: Las redes inalámbricas permiten conectividad a los usuarios en espacios donde es muy difícil llegar con cable.

Cobertura: Las redes inalámbricas permiten dar servicios donde con cable sería muy difícil llegar.

Bajo costo de implementación: La inversión inicial requerida para una red inalámbrica puede ser más costosa que la de una red LAN, pero los beneficios a largo plazo son superiores. Este tipo de redes son altamente recomendados en ambientes dinámicos que requieran acciones y movimientos frecuentes.

Escalabilidad: Este tipo de redes puede ser implementado con diferentes topologías dependiendo las necesidades de los usuarios. La incorporación de nuevos usuarios a la red no necesita grandes cambios dentro de la red inalámbrica.

2.1.2. Componentes de una Red Inalámbrica

- **Sistema de Distribución:**

El sistema de distribución es el componente lógico de 802.11 que se utiliza para reenviar los marcos a su destino. Si bien 802.11 no especifica ninguna tecnología en particular para implementar el sistema de distribución generalmente solo se denomina **Red de Backbone**, y está formado por las conexiones Ethernet que unen los distintos AP. (Solano & Oña, 2009, pág. 21)

- **Medio de Transmisión Inalámbrico:**

Es el medio de transmisión utilizado por las estaciones para enviar y recibir marcos. Si bien 802.11 define varias capas físicas diferentes, las capas basadas en radio frecuencia (RF) han sido mucho más populares que las capas basadas en transmisión Infrarroja (IR). El hecho de que las señales no están circunscriptas a un medio físico, como por ejemplo un cable, tiene como consecuencia que los límites geográficos de la red son difusos. (Solano & Oña, 2009, pág. 21)

- **AP (Access Point / Punto de Acceso):**

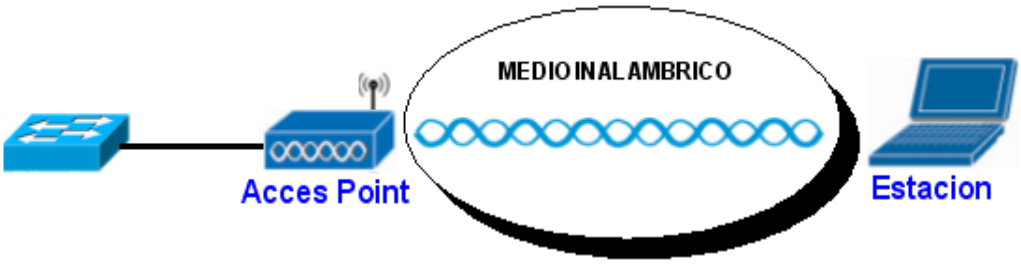
Este dispositivo es el punto de acceso inalámbrico a la red de PCs (LAN) cableada. Es decir, es la interfaz necesaria entre una red cableada y una red inalámbrica, es el traductor entre las comunicaciones de datos inalámbricas y las comunicaciones de datos cableadas. (Solano & Oña, 2009, pág. 21)

- **Estaciones:**

Las estaciones son equipos o dispositivos que poseen una interfaz de red inalámbrica. Estos equipos pueden ser: Celulares inteligentes, Tablets, Notebooks etc. O también pueden ser computadores normales que utilizan algún dispositivo que les permita trabajar dentro de la red inalámbrica. (Solano & Oña, 2009, págs. 21-22)

Actualmente varios fabricantes de dispositivos electrónicos como por ejemplo: en refrigeradoras que están implementando el estándar 802.11 para que puedan comunicarse a través de la red para dar información al usuario.

Figura 2. Componentes de Infraestructura Inalámbrica



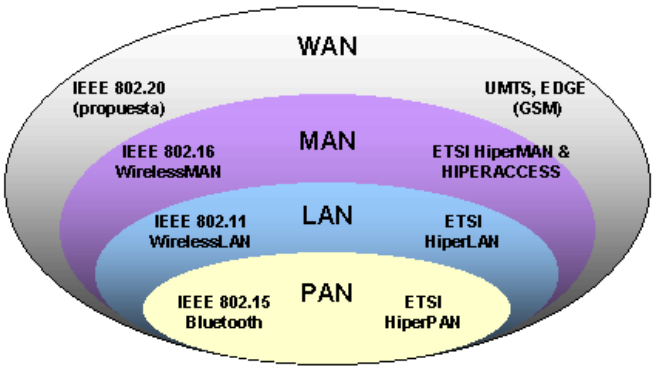
Elaborado por: Jonathan Jara y Diego Mena

2.1.3. Tipos de Redes Inalámbricas

Los sistemas inalámbricos de comunicaciones, sí se clasifican dependiendo el área geográfica que cubren, son los siguientes:

- **WPAN** (Red Wireless de Área Personal)
- **WLAN** (Red Wireless de Área Local)
- **WMAN** (Red Wireless de Área Metropolitana)
- **WWAN** (Red Wireless de Área Extendida)

Figura 3. Tipos de Redes Inalámbricas



Fuente: (upload.wikimedia.org, 2011)

2.1.3.1. Redes Inalámbricas de Área Personal (WPAN)

> Son redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Este tipo de red se usa generalmente para conectar dispositivos periféricos (por ejemplo, impresoras, teléfonos móviles y electrodomésticos) o un asistente personal digital (PDA) a un ordenador sin conexión por cables. También se pueden conectar de forma inalámbrica dos ordenadores cercanos. (Redolfi, 2010)

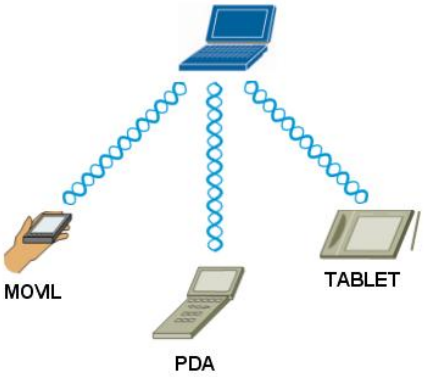
Se usan varios tipos de tecnología para las WPAN:

- **Bluetooth** que ofrece una velocidad máxima de 1 Mbps con un alcance máximo de unos treinta metros.
- **HomeRF** (Home Radio Frequency) que ofrece una velocidad máxima de 10 Mbps con un alcance de 50 a 100 metros sin amplificador.
- **La Tecnología Zigbee** (también conocida como IEEE 802.15.4) también se puede utilizar para conectar dispositivos en forma inalámbrica a un coste muy bajo y con bajo consumo de energía.
- **Conexiones infrarrojas** se pueden utilizar para crear conexiones inalámbricas en un radio de unos pocos metros, con velocidades que puedan alcanzar unos pocos megabits por segundo.

> El alcance típico de este tipo de redes es de unos cuantos metros, alrededor de los 10 metros máximo. La finalidad de estas redes es comunicar cualquier dispositivo personal (ordenador, terminal móvil, tablet, etc.) con sus

periféricos, así como permitir una comunicación directa a corta distancia entre estos dispositivos. (kioskea.net, 2013)

Figura 4. Esquema de una Red WPAN



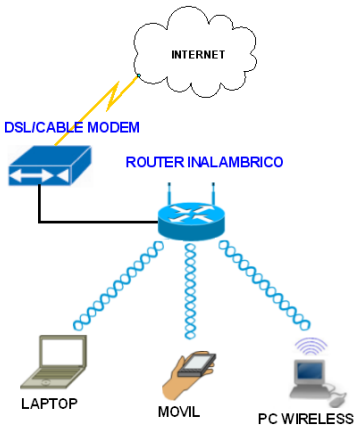
Elaborado por: Jonathan Jara y Diego Mena

2.1.3.2. Redes Inalámbricas de Área Local (WLAN)

"Es un sistema de comunicación inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas en la actualidad" (Duchi & Guerrero, 2011)

proporcionan un alto desempeño y son comúnmente utilizadas en lugares como: Universidades, Hospitales, Aeropuertos, Empresas, Hoteles y Hogares para proveer conectividad a los usuarios, que generalmente poseen laptops o dispositivos móviles, permitiendo de esta manera la interacción entre ellos y el acceso a los servicios. (Ingeniatic, 2011)

Figura 5. Esquema de una Red WLAN

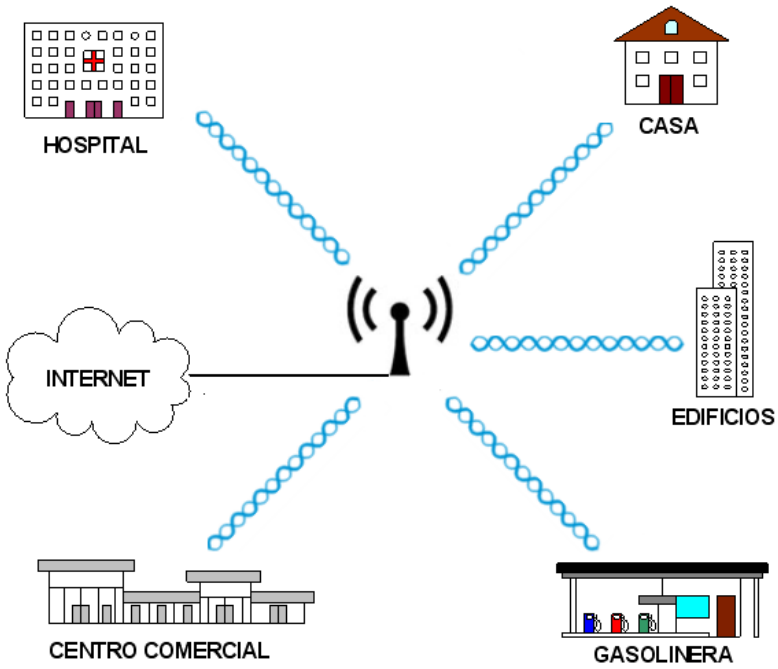


Elaborado por: Jonathan Jara y Diego Mena

2.1.3.3. Redes Inalámbricas de Área Metropolitana (WMAN)

Es un tipo de red de alta velocidad, se conocen como bucle local inalámbrico (WLL, Wireless Local Loop), dan cobertura en un área geográfica extensa, por ejemplo, entre varios edificios de oficinas de una ciudad o en un campus universitario), además ofrecen una velocidad total efectiva de 1 a 10 Mbps, y poseen un alcance de 4 a 10 kilómetros. (Machines, 2011)

Figura 6. Esquema de una Red WMAN



Elaborado por: Jonathan Jara y Diego Mena

La aplicación más común involucra a empresas que buscan conectividad entre sus agencias que geográficamente se encuentran alejadas, otra aplicación la encontramos en la implementación de Proveedores de Servicios de Internet Inalámbricos (WISP), esta solución es ideal para situaciones en las cuales no se cuenta con las facilidades físicas para la instalación de cables debido a la falta de infraestructura.

Las redes de área metropolitana se encuentran basadas en la tecnología **WiMAX** (Worldwide Interoperability for Microwave Access)**,** es decir Interoperabilidad Mundial para Acceso con Microondas, un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un

protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. (Cworld-System, 2012)

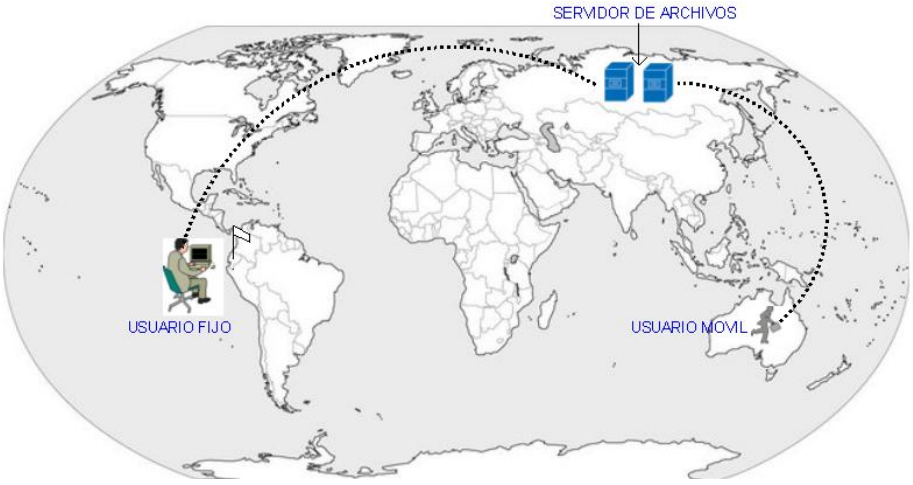
El desempeño de una WMAN depende directamente de la distancia y los componentes que se utilicen. En la actualidad existen muchas soluciones propietarias para este tipo de redes, pero la industria está tratando de normalizar la utilización del estándar 802.11 para satisfacer las necesidades de las WMAN; para lograr tal propósito se utilizan antenas directivas que permitan mayor alcance.

2.1.3.4. Redes Inalámbricas de Área amplia (WWAN)

"Las redes inalámbricas de área amplia cubren generalmente países o continentes, estas aplicaciones son considerablemente costosas debido a la infraestructura que usan, por lo que comúnmente los gastos son compartidos por muchos usuarios". (Novoa & Reyes, 2007, pág. 18)

Una WWAN permite la movilidad a sus usuarios dentro de un área extensa sin que los mismos pierdan la conectividad de sus aplicaciones. Unos ejemplos claro de una WWAN, son los enlaces satelitales o el servicio de telefonía celular, el cual interconecta diferentes redes de varias empresas proveedoras del servicio utilizando Itinerancia **(Roaming).**

Figura 7. Esquema de una Red WWAN



Fuente: (lacasainfantil.com, 2010)

Elaborado por: Jonathan Jara y Diego Mena

> El desempeño de la WWAN es relativamente bajo en rangos que van desde los 56Kbps hasta los 170Kbps, siendo este rango suficiente para el uso de aplicaciones que requiere una red de área extensa, que son ejecutados en dispositivos como teléfonos celulares y tabletas, los mismos que poseen procesadores de bajo rendimiento y pantallas pequeñas que no necesitan trasmitir muchos datos para que la información pueda ser visualizada. (Novoa & Reyes, 2007, p. 18)

2.2. Estándares Inalámbricos IEEE

Los estándares IEEE son normas internacionales que definen la forma en que deben trabajar y desarrollarse toda la tecnología actual, ya que sin las mismas cada fabricante desarrollaría su tecnología con sus propias normas y se sería un caos comunicar unas con otras.

> En 1980 la IEEE inició el proyecto internacional denominado estándar IEEE 802.11 que define las características de una red de área local inalámbrica, especificando sus normas de funcionamiento en una (WLAN), además se encuentra basado en un modelo que permite la intercomunicación de dispositivos y ordenadores para la mayoría de los fabricantes. (docente.ucol.mx, 2013)

Para ello se enunciaron una serie de normalizaciones que con el tiempo han sido adaptadas como normas internacionales por la ISO.
El protocolo 802 está dividido según las funciones necesarias para el funcionamiento de las LAN.

- **IEEE 802.1** Protocolos superiores de redes de área local.
- **IEEE 802.2** Control de enlace lógico.
- **IEEE 802.3** Ethernet.
- **IEEE 802.4** Método de acceso y nivel físico. Bus con paso de testigo token bus.
- **IEEE 802.5** Token Ring.
- **IEEE 802.6** Red de área metropolitana
- **IEEE 802.7** Grupo de Asesoría Técnica sobre Banda ancha.

- **IEEE 802.8** Grupo de Asesoría Técnica sobre Fibra óptica.
- **IEEE 802.9** RAL o LAN de servicios integrados.
- **IEEE 802.10** Seguridad ínter operable en RAL o LAN.
- **IEEE 802.11** Red local inalámbrica, también conocido como Wi-Fi.
- **IEEE 802.12** Prioridad de demanda.
- **IEEE 802.14** Cable módems, es decir módems para televisión por cable.
- **IEEE 802.15** Red de área personal inalámbrica, que viene a ser Bluetooth.
- **IEEE 802.16** Acceso inalámbrico de Banda Ancha, también llamada WiMAX, para acceso inalámbrico desde casa.
- I**EEE 802.17** Anillos de paquetes con recuperación, se supone que esto es aplicable a cualquier tamaño de red, y está bastante orientado a anillos de fibra óptica.
- **IEEE 802.18** Grupo de Asesoría Técnica sobre Normativas de Radio.
- **IEEE 802.19** Grupo de Asesoría Técnica sobre Coexistencia.
- **IEEE 802.20** Mobile Broadband Wireless Access.
- **IEEE 802.21** Media Independent Hand-Off. (Colemanres, 2008)

2.2.1. Estándar IEEE 802.11x

"El estándar IEEE 802.11 es un estándar internacional que define las características de una red de área local inalámbrica (WLAN)", (Kisokea, 2013)

> 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 802.11 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. (Jara & Nazar, 2010, p. 3)

2.2.2. Principales Estándares IEEE 802.11x

El estándar 802.11 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 velocidades de hasta 11 Mbit/s , 54 Mbit/s y 300 Mbit/s, respectivamente. (Kisokea, 2013)

Figura 8. Estándares Inalámbricos IEEE 802.11x

Fuente: (Bestofmedia, 2012)

2.2.2.1. Estándar IEEE 802.11b:

El estándar 802.11b no es más que una modificación de la Norma IEEE 802.11 que amplía la tasa de transferencia hasta los 11Mbit/s y usa la misma banda de 2.4GHz. El alcance aproximado para este estándar es de aproximadamente 300 metros en espacios abiertos. Es el más utilizado puesto que fue el primero en imponerse y existe una gran cantidad de equipos y dispositivos como teléfonos, portátiles, altavoces inalámbricos, dispositivos de seguridad, hornos de microondas, y el Bluetooth de corto alcance que manejan esta tecnología.

Se emplea CSMA/CA como técnica para el acceso al medio y utiliza la técnica de **Espectro Ensanchado por Secuencia Directa (DSSS)**, para la modulación de la señal, enviando bits de redundancia que evitan retransmisiones corrigiendo los errores en la trama, y aunque 802.11b soporta una velocidad máxima de 11Mbps, la velocidad varía según la distancia. (Villagas, 2009)

Por lo general la mayoría de hardware 802.11b está diseñado para funcionará cuatro velocidades, usando uno de los cuatro métodos de codificación de datos, en función de la gama de velocidades:

- **11Mb/s:** Modulación por desplazamiento de fase
- **5.5Mb/s:** Modulación por desplazamiento de fase **(QPSK/ CCK).**
- **2.0Mb/s:** Modulación por desplazamiento de fase **(DQPSK)**.
- **1.0Mb/s:** Utiliza binario diferencial modulación por desplazamiento de fase **(DBPSK)**. (Bestofmedia, 2012)

Ventaja: Bajo costo, rango de señal muy bueno y difícil de obstruir.

Inconveniente: Baja velocidad máxima, soporte de un número bajo de usuarios a la vez y produce interferencias en la banda de 2.4GHz.

Tabla 1. Características del Estándar IEEE 802.11b

ESTÁNDAR 802.11b	
FRECUENCIA LONGITUD DE ONDA	2.4GHz (2.400-2.4835)
ANCHO DE BANDA DE DATOS	11Mbps, 5Mbps, 2Mpbs, 1Mbps
MEDIDAS DE SEGURIDAD	WEP- (Wireless Equivalency Protocol) en combinación con espectro de dispersión directa
RANGO DE OPERACIÓN ÓPTIMA	50 metros dentro, 100 metros afuera
ADAPTADO PARA UN PROPÓSITO ESPECÍFICO O PARA UN TIPO DE DISPOSITIVO	Ordenadores portátiles, ordenadores de sobremesa donde cablear entraña dificultades, tablets

Fuente: (laserwifi.com, 2012)

2.2.2.2. Estándar IEEE 802.11a:

El Estándar 802.11a es un superior al 802.11b puesto que se obtiene velocidades teóricas máximas de hasta 54 Mbps, apoyándose en la banda de los 5GHz, lo que limita las interferencias generadas por otros dispositivos.

Trabaja con 12 canales que no se superponen, 8 dedicados a interiores y 4 a punto a punto. No es interoperable con 802.11b/g, salvo que se utilice un equipo que implemente ambos estándares. Además utiliza OFDM

(Orthogonal Frequency Division Multiplexing), lo cual produce una capacidad alcanzable neta real de aproximadamente 25Mbps. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 y luego a 6 Mbps si se requiere. (Byffalo, 2013)

Ventaja: Permite más usuarios simultáneos y trabaja en la frecuencia de 5GHz, limitando de esta manera las interferencias de otros dispositivos.

Inconveniente: "Opera en una banda diferente que el estándar 802.11b, lo que genera que los productos de dichas tecnologías no sean compatibles entre sí." (Navarrete, 2009)

2.2.2.3. Estándar IEEE 802.11g:

El estándar 802.11g trabaja a una velocidad de transmisión máxima de 54Mbps y utiliza las mismas bandas de frecuencias que el estándar 802.11b. Sin embargo al mezclar los 2 estándares en una misma red, generan interferencia y conflictos con los equipos, puesto que las más altas están más expuestas a sufrir pérdidas y reducir significativamente la velocidad de transmisión.

Emplea las técnicas de modulación OFDM y DSSS con potencias de hasta medio vatio y antenas parabólicas apropiadas, y puede alcanzar comunicaciones de hasta 50 km en larga distancia. Posee una característica adicional denominada SuperG, lo que hace posible duplicar la señal, pero ocasiona conflictos con otros equipos, provocando que no sea compatible en muchos casos. (Villagas, 2009)

Ventaja: Velocidad máxima alta, soporte de muchos usuarios a la vez, rango de señal muy bueno y difícil de obstruir.

Inconveniente: Alto costo y produce interferencias en la banda de 2.4GHz.

Tabla 2. Características del Estándar IEEE 802.11g

ESTÁNDAR 802.11g	
FRECUENCIA LONGITUD DE ONDA	2.4GHz
ANCHO DE BANDA DE DATOS	54 Mbps
MEDIDAS DE SEGURIDAD	WEP, OFDM
RANGO DE OPERACIÓN ÓPTIMA	50 metros dentro, 100 metros afuera
ADAPTADO PARA UN PROPÓSITO ESPECÍFICO O PARA UN TIPO DE DISPOSITIVO	Ordenadores portátiles, ordenadores de sobremesa donde cablear entraña dificultades, PDAs. Compatible hacia atrás con las redes 802.11b

Fuente: (laserwifi.com, 2012)

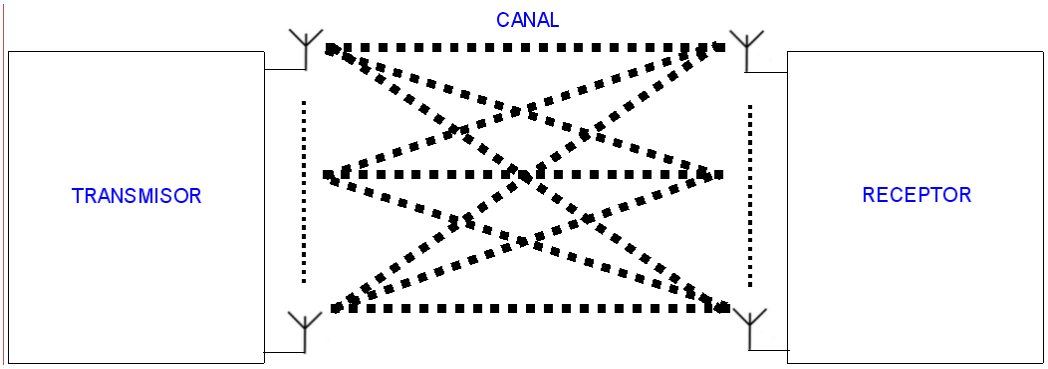
2.2.2.4. Estándar IEEE 802.11n:

El proyecto de desarrollar del estándar IEEE 802.11n se da por la gran demanda que tienen las redes inalámbricas hoy en día. Pero existen algunos puntos que se tomaron en cuenta para el desarrollo de éste estándar como son los siguientes:

- La velocidad de transmisión
- La sobrecarga **(Acuses de Recibo, Ventanas de Contención, Espaciado entre tramas).**
- Aumentar la Velocidad de Transmisión
- La Capacidad de Transmisión
- La Porción de datos acarreados se encoge mientras la sobrecarga permanece fija.

El estándar 802.11n utiliza algunas nuevas tecnologías y toma algunas características de otras ya existentes para dotarse de mayor velocidad y alcance, entre las más destacable tenemos la MIMO **(Multiple Input, Multiple Output**).

Figura 9. Estructura de Transmisión Estándar 802.11n



Elaborado por: Jonathan Jara y Diego Mena

"Esta tecnología se basa en la utilización de varias antenas para transportar múltiples corrientes de datos de un lugar a otro lo que genera mayor transmisión datos en el mismo período de tiempo", (Vitaloni, 2008) dando como resultado un aumento de velocidad de transmisión.

El estándar 802.11n tendrá una velocidad de transmisión minina de 100 Mbps y podría llegar a alcanzar los 600 Mbps, una características importante de esta versión es que puede trabajar en dos bandas de frecuencias 2,4 GHz y 5Ghz, motivo por el cual es compatible con dispositivos basados en todas las ediciones anteriores.

Tabla 3. Comparación de los Estándares Inalámbricos

ESTÁNDAR	AÑO LAZAMIENTO	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

Elaborado por: Jonathan Jara y Diego Mena

"Actualmente la mayor parte de los fabricantes ya incorpora a sus líneas de producción equipos inalámbricos 802.11n, y se conoce que el futuro estándar sustituto de 802.11n será 802.11ac con tasas de transferencia superiores a 1Gb/s." (laserwifi.com, 2012)

2.3. Seguridades Inalámbricas

La seguridad en redes inalámbricas reviste de importancia, debido a la forma de trasmisión de las WLAN en donde la información puede ser receptada por cualquier equipo que este dentro del alcance o área de cobertura, permitiendo de esta forma el acceso a las mismas pudiendo generar algún tipo de violación, ataque, o peor aun la sustracción y manipulación de la información perteneciente a dicha red la misma que puede pertenecer a una persona, empresa o institución con el fin de llevar a cabo un delito informático o demostrar las vulnerabilidades de la red.

"La utilización de las redes inalámbricas libera de ataduras físicas en cuanto a conexión se refiere," (Maldonado, 2012) pero la principal desventaja de utilizar una red inalámbrica es la seguridad, existen amenazas y ataques a las que están expuestas:

- **Amenazas No Estructuradas:** son generadas por personas sin experiencia que poseen herramientas de hacker o crackeadores de passwords en la mayoría de los casos.
- **Amenazas Estructuradas:** son generadas por personas con conocimientos técnicos, gente que conoce las debilidades de las WLAN's en profundidad, pudiendo desarrollar programas o scripts para efectuar la amenaza.

- **Amenazas Externas:** son personas que son ajenas a la red y que no tienen acceso autorizado a ella. Generalmente actúan en los alrededores de la red víctima de la amenaza.

- **Amenazas Internas:** son personas autorizadas con una cuenta en un servidor o acceso físico. Cubren la mayor parte de los incidentes y pueden exponer a la red a ataques externos.

Entre los métodos de ataques a las redes inalámbricas tenemos los siguientes:

- **Reconocimiento:** es el descubrimiento de vulnerabilidades en los sistemas para un posible ingreso a los mismos, este tipo de ataque consiste en reunir información a través de analizadores de paquetes y protocolos.

- **Ataque de Acceso:** este tipo de ataque se da cuando una persona no autorizada ingresa a los sistemas sin poseer cuentas ni contraseñas de ingreso, descubriendo passwords débiles o no existentes.

- **Negación de Servicio:** este tipo de ataque se da cuando se desactivan o se afectan los sistemas o servicios inalámbricos, negando el servicio a los usuarios autorizados.

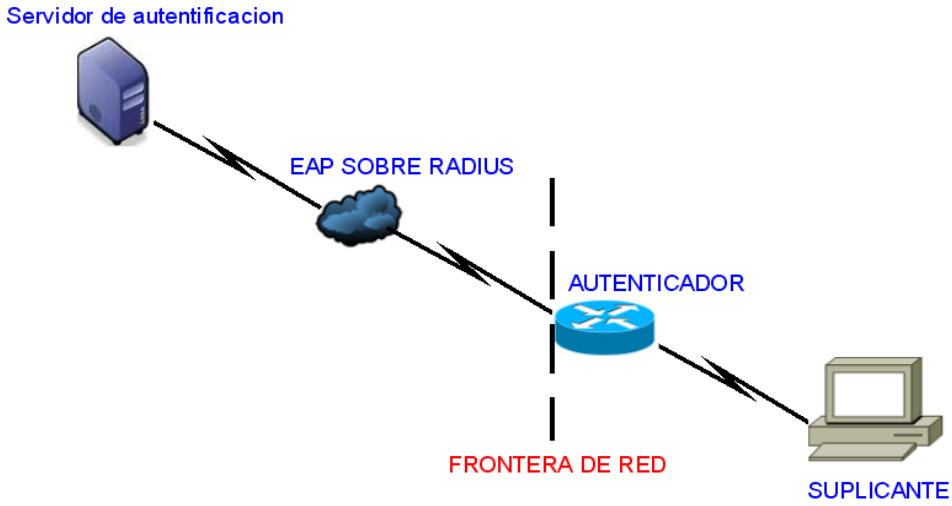
Teniendo en cuenta todas las vulnerabilidades y amenazas de seguridad que afectan a las redes inalámbricas, se han desarrollado algunos métodos con los cuales se pueda ofrecer más protección y confiabilidad de la información al momento de acceder a una red inalámbrica.

Entre los tipos de seguridad más utilizados están los cifrados (WEP, WPA), basados en controles de acceso mediante claves de red, pero se han demostrado que poseen algunas falencias en su implementación. Por otro lado se puede utilizar medidas de protección como: Filtrados de direcciones MAC y métodos de seguridad del estándar 802.1x, los cuales son mucho más robustos y confiables, ya que están basados en métodos de autenticación, autorización y contabilidad siendo el protocolo EAP (Extensible Authentication Protocol*)* y el protocolo AAA (Authentication, Authorization, Accounting).

2.3.1. Portales Cautivos

Un portal cautivo es un medio de seguridad aplicado únicamente en redes inalámbricas, que se muestra como una página web con la cual un usuario de una red pública o privada debe interactuar antes de garantizar su acceso a las funciones normales de la red inalámbrica.

Figura 10. Estructura de un Portal Cautivo



Elaborado por: Jonathan Jara y Diego Mena

Cuando un usuario potencial se autentica por primera vez ante una red con un portal cautivo, se requieren ciertas acciones antes de proceder con el acceso como por ejemplo que acepte las políticas de uso.

Los portales cautivos son muy utilizados por centros de negocios, aeropuertos, hoteles, cafeterías, cafés Internet y otros proveedores que ofrecen HotSpot de Wi-Fi para usuarios de Internet.

2.3.1.1. Tipos de Portales Cautivos

Los portales cautivos se encuentran clasificados en 2 grupos principales que se enumeran a continuación:

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:

- **PepperSpot** (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. 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.

Figura 11. Portales Cautivos por Hardware

Fuente: (channelprosmb.com, 2013)

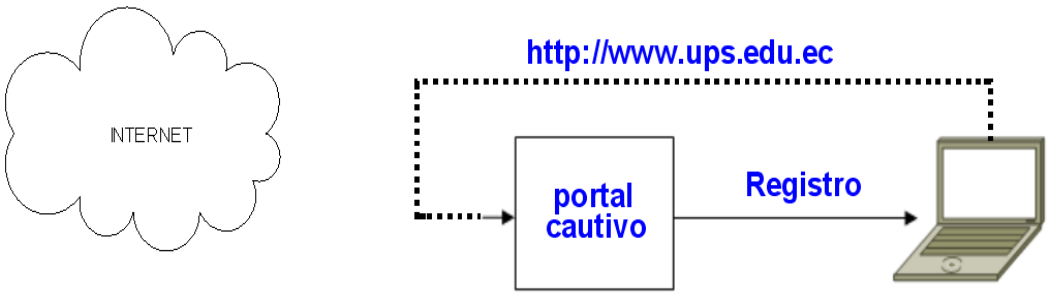
2.3.1.2. Funcionamiento de los Portales Cautivos

Los portales cautivos trabajan mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan prácticamente todas las computadoras portátiles y sistemas operativos, se usan sobre todo en redes inalámbricas abiertas, es importante tener un control de acceso de usuarios a la red y por ende a la navegación web. (Fierro & Gonzales, 2011)

- El usuario busca la red Wireless a la que desea conectarse con la ayuda de su SSID de entre todas las redes detectadas, después se conectará a la misma y seguidamente le solicitará la contraseña de acceso para validar el ingreso a la misma.

- Una vez que el usuario tiene acceso a la red inalámbrica, y al intentar usar algún servicio web, se verá imposibilitado ya que toda petición de navegación será redirigida al portal cautivo o portal de autenticación hasta que se ingresen las credenciales de acceso.

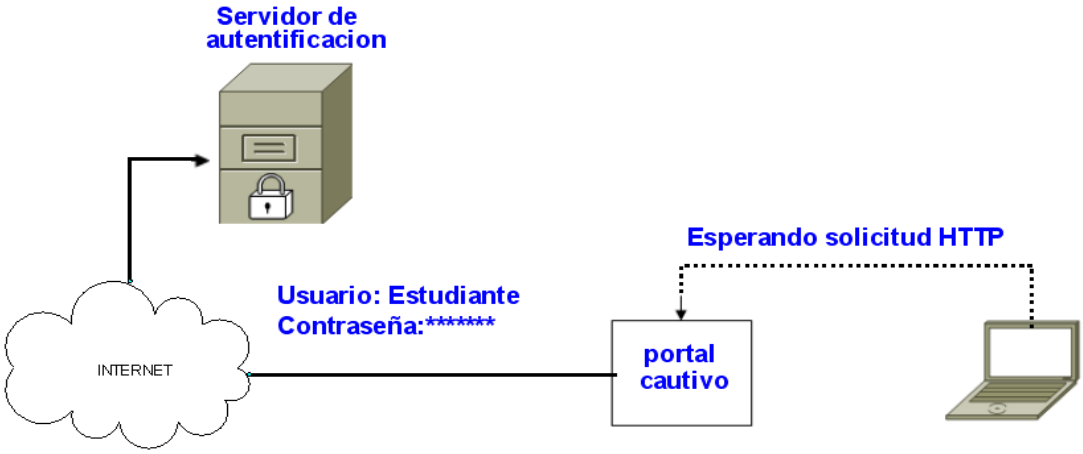
Figura 12. Solicitud de página web y es redireccionado.



Elaborado por: Jonathan Jara y Diego Mena

- Se verifican las credenciales ingresadas por el usuario, y cualquier intento erróneo de las mismas será bloqueada por el portal hasta que se verifiquen las credenciales validas para el acceso al mismo.

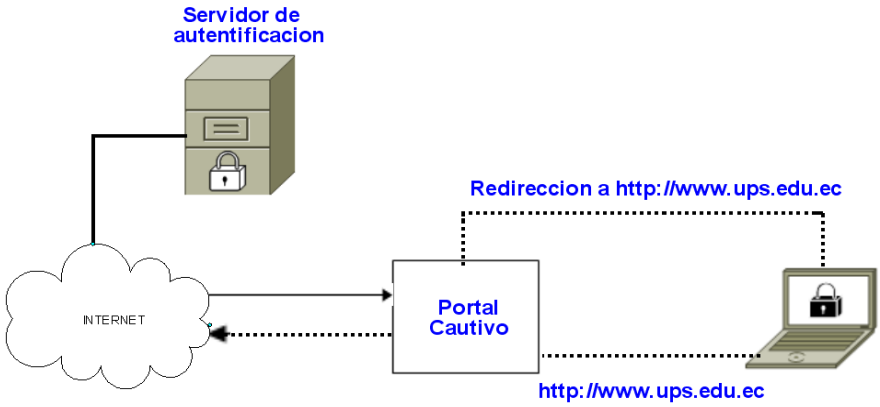
Figura 13. Verificación de Credenciales



Elaborado por: Jonathan Jara y Diego Mena

- Una vez que el usuario ha sido autenticado exitosamente por el portal cautivo, es redireccionado a la página principal que haya sido configurada por el administrador, y se le permitirá el acceso exclusivamente a los servicios vinculados con el internet.

Figura 14. Se concede el acceso a la Navegación Web



Elaborado por: Jonathan Jara y Diego Mena

2.3.1.3. Ventajas y Desventajas de los Portales Cautivos

Ventajas:

Entre las principales ventajas de usar Portales Cautivos como método de Seguridad en nuestra red inalámbrica destacamos las siguientes:

- Pueden utilizar Autenticación Centralizada.
- Permite aplicar políticas por usuario.
- Soluciones Comerciales y libres
- Seguridad Basada en Identidades
- Estadísticas de Uso por usuario.
- Mejor despliegue que VPN: no necesita cliente, solo es necesario un navegador.
- Más rápidos: No existe latencia por cifrado.

Desventajas:

Entre las potenciales desventajas de los portales Cautivos podemos mencionar las siguientes:

- Si el dispositivo no posee un navegador instalado no será posible autenticarse
- No se cifra el tráfico (depende de los protocolos de aplicación: **(https, ssh, etc.)**
- Vulnerables a Spoofing de MAC e IP.

- Los clientes asociados al AP tienen visibilidad entre ellos aunque no estén autenticados. (Pérez, 2011)

2.3.2. Protocolos AAA

"En seguridad informática, el protocolo AAA realiza tres funciones importantes: Autenticación, Autorización y Traceabilidad **(Authentication, Authorization and Accounting)**." (Garcia, Proyecto Entorno AAA, 2008) 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 recolectar datos que permitan una auditoría total sobre los recursos a los que se ha tenido acceso.

- **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". (Ramirez, 2010) 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, ó 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.

- **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." (Pestrebol, 2013)

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.

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.

- **Contabilización (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." (Pestrebol, 2013)

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." (cyclopaedia.net, 2013)

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.

Listado de Protocolos AAA

- **RADIUS**

- **DIAMETER**
- **TACACS**
- **TACACS+**

"Radius: Protocolo para aplicaciones de tipo Cliente - Servidor. Diseñado principalmente para aplicaciones que acceden a redes o de IP móvil. Basado en UDP." (QualDev, 2012)

"Diameter: Protocolo de tipo P2P. Diseñado principalmente para aplicaciones que acceden a redes o de IP móvil." (QualDev, 2012)

"TACACS: Protocolo para desarrollo de servidores. Usado comúnmente para servidores Unix." (QualDev, 2012)

"TACACAS+: Basado en TACACS pero se redefinió totalmente el protocolo. Provee los servicios de AAA por separado. Basado en TCP. Otros protocolos utilizados en combinación con los protocolos AAA." (QualDev, 2012)

- **PPP**
- **EAP**
- **LDAP**

"PPP.- El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras." (Diaz, 2013) 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." (abanet.net, 2013) Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación.

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. (Garcia, Proyecto Entorno AAA, 2008)

2.3.2.1. Protocolo Radius

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.

Un cliente envía las credenciales de usuario y la información de los parámetros de 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.

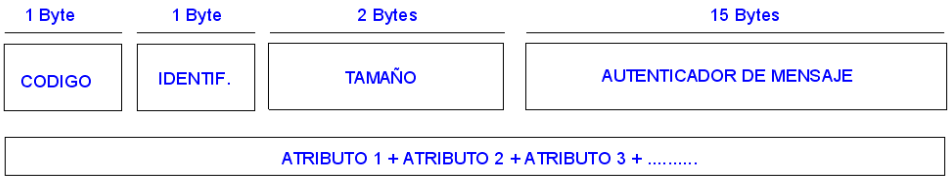
RADIUS también es comúnmente usado por el NAS (Network Access Server) para notificar eventos como:

- 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

Formato de los Mensajes Radius

El intercambio de datos que se realiza entre el cliente y el servidor RADIUS se hace a través de paquetes RADIUS, a continuación se presenta la estructura de cada uno de los campos que lo forman:

Figura 15. Estructura del Paquete Radius



Elaborado por: Jonathan Jara y Diego Mena

- **Campo Código**

"El campo de código es de longitud de 1 byte e indica el tipo de mensaje RADIUS. Se descarta un mensaje con un campo de código que no es válido". (technet.microsoft, 2013)

Los valores definidos para el campo código de RADIUS se muestran en la tabla siguiente:

Tabla 4. Códigos de Paquete RADIUS

CÓDIGOS (DECIMAL)	PAQUETES
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server
13	Status-Client
255	Reserved

Elaborado por: Jonathan Jara y Diego Mena

Mensajes Radius:

- **Access-Request:** es enviado por un cliente RADIUS al servidor RADIUS para solicitar autenticación y autorización para conectarse a la red. Debe contener el usuario y contraseña (ya sea de usuario o CHAP); además el puerto NAS, si es necesario, si este paquete es enviado el campo código tendrá el valor de 1.

- **Access-Accept:** es un paquete enviado por el servidor RADIUS en respuesta a un paquete "Access-Request" y contienen la información de la configuración para que el usuario pueda hacer uso del servicio, informa que la conexión está autenticada y autorizada, si este paquete es enviado el valor del campo código será 2.

- **Access-Reject:** es un paquete enviado por el servidor RADIUS en respuesta a un paquete "Access-Request", en caso de que uno de los atributos no sea aceptado. Un servidor RADIUS envía este mensaje ya sea porque las credenciales no son auténticas o por que el intento de conexión no está autorizado, el valor del campo código será 3.

- **Accounting-Request:** es un paquete enviado por el cliente RADIUS para especificar información de la cuenta para la conexión que fue aceptado. El valor del campo código en el paquete será de 4.

- **Accounting-Response:** es un paquete enviado por un servidor RADIUS en respuesta a un mensaje Accounting-Request. Este mensaje reconoce el procesamiento y recepción exitosa de un mensaje de Accouting-Response. El valor del campo código en el paquete será de 5.

- **Access-Challenge:** es un paquete enviado por un servidor RADIUS en respuesta a un mensaje "Access-Request". Este mensaje es enviado cuando se desea que el usuario conteste a un reto. Si este tipo de paquete es soportado, el servidor pide al cliente que vuelva a enviar un paquete Access-Request para hacer la autenticación. Otros de los valores que puede tomar el campo código son:

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

- **Status-Client**, el valor del campo código será 13.
- **Reserved**, el valor del campo código será 255.

- **Campo de Identificador**

El campo de identificador es la longitud de 1 byte y se utiliza para asociar una solicitud con su correspondiente respuesta.

- **Campo de Longitud**

El campo Longitud dos octetos indica y toda la longitud del mensaje RADIUS, incluidos los campos de código, identificador, longitud y el autenticador y los atributos RADIUS. El campo longitud puede variar de 20 a 4.096 bytes.

- **Campo Autenticador**

El campo autenticador es 16 octetos largas y contiene la información que el cliente RADIUS y el servidor que se utilizan para comprobar que el mensaje procede de un equipo que está configurado con un secreto compartido común.

- **Sección de Atributos**

“La sección atributos de mensaje RADIUS contiene uno o más atributos RADIUS, que contienen los detalles específicos de autenticación, autorización, información y configuración para los mensajes RADIUS.” (Microsoft, 2013)

Funcionamiento del Servidor Radius

El proceso de RADIUS empieza cuando un usuario intenta acceder al Access Server usando RADIUS:

- Se solicita al usuario que envié su Username y Password.
- El Username y el Password son encriptados con una llave secreta y enviada a un Access-Request al servidor RADIUS.

- El cliente ahora envía un mensaje de Accounting-Request con la información correspondiente a su cuenta y para indicar que el usuario está reconocido dentro de la red.
- El Servidor responderá con un Accounting-Response, cuando la información de la cuenta es almacenada.
- El usuario recibirá cualquiera de siguientes respuestas por parte del servidor RADIUS:

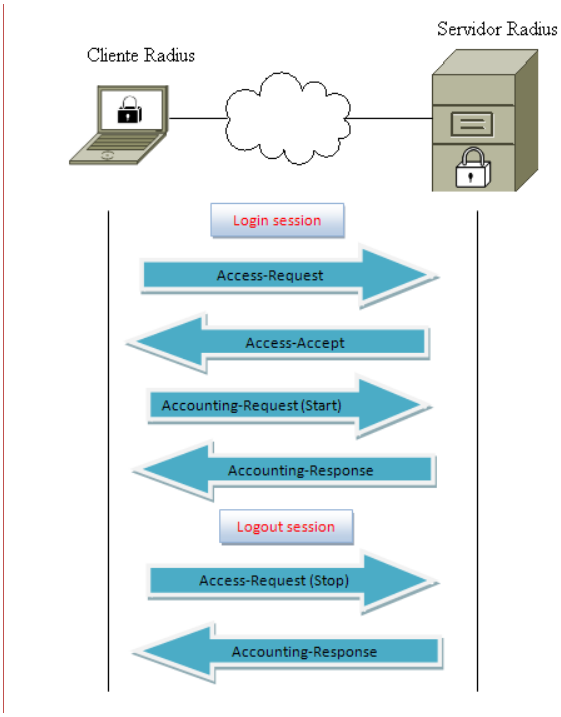
    - **Aceptado:** El usuario es autenticado.
    - **Rechazado:** El usuario no es autenticado por el servidor RADIUS, se solicita que reingrese sus datos para acceder o denegar el ingreso.
    - **Cambios de Password:** El servidor RADIUS solicita al usuario que seleccione una nueva contraseña.

- Una vez que el usuario ha sido identificado puede hacer uso de los servicios proporcionados por la red.
- Cuando el usuario desea desconectarse envía un mensaje Accounting-Request (Stop) con la siguiente información:

    - **Delay Time:** Tiempo que el cliente lleva tratando de enviar el mensaje.
    - **Input Octets:** Número de octetos recibido por el usuario.
    - **Output Octets:** Número de octetos enviados por el usuario.
    - **Session Time:** Número de segundos que el usuario ha estado conectado.
    - **Input Packets:** Cantidad de paquetes recibidos por el usuario.
    - **Output Packets:** Cantidad de paquetes enviados por el usuario.
    - **Reason:** Razón por la que el usuario se desconecta de la red.

- Finalmente, el servidor RADIUS responde con un mensaje Accounting Response cuando la información de la cuenta es almacenada.

Figura 16. Secuencia Protocolo RADIUS



Elaborado por: Jonathan Jara y Diego Mena

2.4. 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." (tecnoteresiano.wikispaces.co, 2013)

> 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 desarrolladores y usuarios que adoptaron códigos de otros proyectos de software libre para su uso en nuevas distribuciones. (slideshare.net, Evolucion del linux, 2012)
>
> 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).** (Linux, 2013)

2.4.1. 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." (elinux.com.mx)

- **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)." (Eagle, 1999)

- **"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." (elinux.com.mx)

- **"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." (elinux.com.mx)

- **"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." (elinux.com.mx)

2.4.2. Distribución Centos

CentOS (Community ENTerprise Operating System) es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux **RHEL**, compilado a partir del código fuente liberado por Red Hat.

Red Hat Enterprise está compuesto por software libre y código abierto, pero se publica en formato binario. Red Hat libera todo su código fuente del producto de forma pública bajo los términos de la Licencia pública general de GNU y otras licencias. Los desarrolladores de CentOS usan ese código fuente para crear un producto final que es muy similar al Red Hat Enterprise y se encuentra disponible para ser bajado y usado por el público, cabe recalcar que no es mantenido ni asistido por Red Hat Enterprise. (Medina, 2012)

2.4.2.1. Características Principales

- "Fácil Mantenimiento
- Idoneidad para el uso a largo plazo en entornos de producción
- Entorno favorable para los usuarios y mantenedores de paquetes
- Desarrollo activo
- La infraestructura de la comunidad
- Modelos de Negocio Abierto." (centos-55.blogspot.com, 2011)

2.4.2.2. Requisitos de Instalación de Centos

El Hardware recomendado para instalar Centos es:

-Memoria RAM: 64 MB (Mínimo).
-Espacio en Disco Duro: 2 GB (Recomendado).
-CentOS soporta casi las mismas arquitecturas que Red Hat Enterprise Linux:

- Intel x86-compatible (32 bit) Intel Pentium I/II/III/IV/Celeron/Xeon,
- AMD K6/K7/K8, AMD Duron, Athlon/XP/MP.
- AMD64(Athlon 64, etc) e Intel EM64T (64 bit).

-Las versiones 3.x y 4.x (pero no la 5.0 y posteriores) además soportaron:
Intel Itanium (64 bit).

- PowerPC/32 (Apple Macintosh PowerMac corriendo sobre procesadores G3 o G4 PowerPC).
- IBM Mainframe (eServer zSeries y S/390).

-También se tuvo soporte para dos arquitecturas no soportadas por Red Hat Enterprise Linux.

- Alpha procesador (DEC Alpha) (sólo en CentOS 4).
- SPARC (beta en CentOS 4).

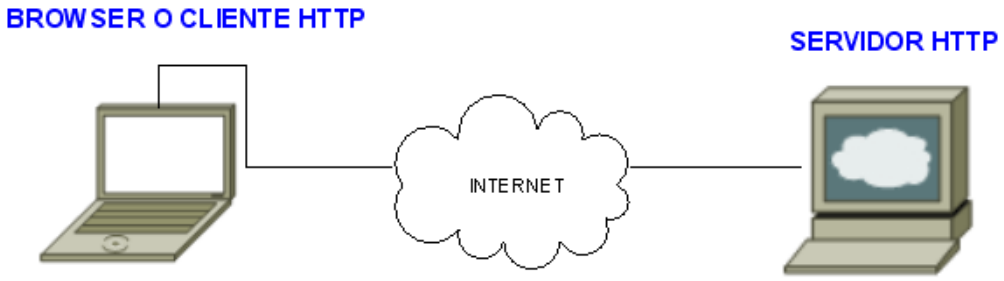
2.4.2.3. Servidores Centos

Centos es la distribución de Linux más utilizada para la instalación de servidores por ser de licenciamiento libre, por su mayor rendimiento y accesibilidad, por tener disponible actualizaciones en los repositorios de manera libre y gratuita sin la necesidad de pagar el costoso soporte anual que representaría un servidor Red Hat.

2.5. Servicio HTTP

Es un protocolo que permite a los usuarios acceder a todo tipo de información remota (Texto, audio video, etc.) de una forma sencilla e intuitiva, a estos documentos se los denomina páginas webs. El servicio de HTTP sigue el esquema petición-respuesta entre un cliente y un servidor.

Figura 17. Esquema del funcionamiento del Servicio HTTP



Elaborado por: Jonathan Jara

Al cliente que efectúa la petición (**Un navegador web**) se lo conoce como (**Agente del usuario**). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos **(URL).** Los recursos pueden ser

archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

HTTP es un protocolo sin estado, eso quiere decir que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado. (Esquivel, 2013)

2.6. Servidores 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. El código recibido por el cliente suele ser compilado y ejecutado por un navegador web. (Ramírez, 2012)

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**. (slideshare.net, 2013)

2.6.1. 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.

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.

2.6.1.1. 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 que es lo que estamos instalando como servidor, podemos saber, sin ningún secreto, sin ninguna puerta trasera." (Ciberaula, 2010)

- **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.

- **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. (Ciberaula, 2010)

2.6.1.2. Principales 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.

- **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 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. (Aries, 2013)

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 esta 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.

2.6.1.3. Módulos de APACHE

Apache se ha adaptado siempre a una gran variedad de entornos a través de su diseño modular. Este diseño permite a los administradores de sitios web elegir qué características van a ser incluidas en el servidor seleccionando que módulos se van a cargar, ya sea al compilar o al ejecutar el servidor. En Centos ya se incluye el Servidor Apache HTTP versión 2.0 por defecto dentro de servicios ya preinstalados. A continuación se listan algunos de estos módulos más importantes:

- **Mod_Ssl**

Este módulo proporciona SSL v2/v3 y TLS v1 para el Apache HTTP Server. Se basa en OpenSSL para proporcionar el motor de la criptografía. Puede ser configurado para proporcionar varios elementos de información **SSL** como variables de entorno adicionales a la SSI y CGI espacio de nombres.

- **Mod_Rewrite**

Este módulo utiliza un motor de reescritura basado en reglas (se basa en un analizador de expresiones regulares) para reescribir direcciones URL solicitado sobre la marcha. Soporta un número ilimitado de reglas y un número ilimitado de las condiciones adjuntas para cada regla, para proporcionar un mecanismo muy flexible y potente manipulación URL.

- **Mod_Dav**

Este módulo proporciona la clase 1 y clase 2 ('Web Distributed Authoring y control de versiones') la funcionalidad de Apache. Esta extensión del protocolo HTTP permite crear, mover, copiar y eliminar recursos y colecciones en un servidor web remoto.

- **Mod_Deflate**

El módulo mod_deflate proporciona el filtro de salida **DEFLATE** que permite la salida de su servidor sea comprimida antes de ser enviada al cliente a través de la red.

- **Mod_Auth_ldap**

Este módulo permite tener autentificación de usuarios contra un servidor **LDAP**.

- **Mod_Perl**

  El módulo mod_perl le da un intérprete de Perl persistente incrustado en su servidor web. Evita la sobrecarga de iniciar un intérprete externo que le da contenido dinámico súper rápido.

  Un servidor web Apache con ayuda de este módulo creará sesiones con estado, sistemas de autenticación de usuario personalizada, proxies inteligentes entre otras. (Apache, 2013)

- **Mod_Cband**

Este módulo permitirá un control de tráfico y limitador de ancho de banda.

- **Mod_Security**

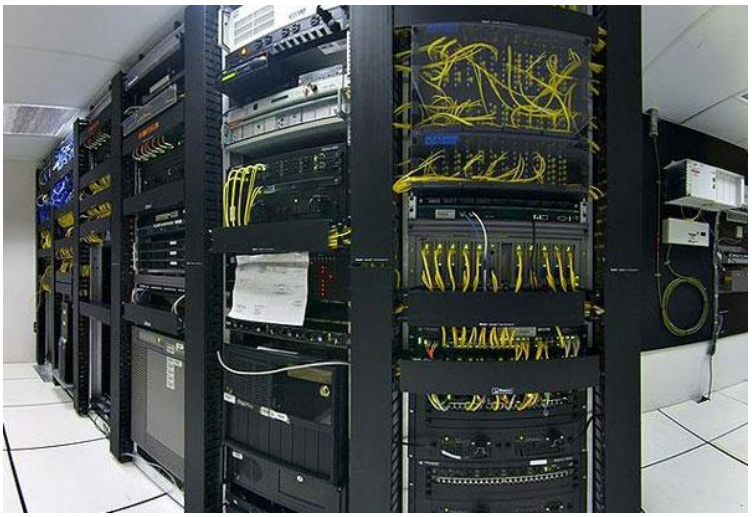
"Firewall que se ejecuta como módulo dentro del servidor web Apache, provee protección contra diversos ataques hacia aplicaciones Web y monitorizar tráfico HTTP, así como realizar análisis en tiempo real sin necesidad de hacer cambios a la infraestructura existente." (Domínguez, 2013)

2.7. Infraestructura

La infraestructura es un conjunto de elementos de hardware servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc., software sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración, etc., que en conjunto dan soporte a los sistemas informáticos de una empresa o entidad.

Por este motivo es crucial conocer todos sus componentes o elementos a nivel de software y de hardware. Una infraestructura sólida permite a un software operar de manera eficiente y eficaz durante el tiempo previsto con niveles altos de servicios y prestaciones. (Uruguay, 2013)

Figura 18. Infraestructura de Redes



Fuente: (tuexpertoit.com, 2009)

2.7.1. Routers

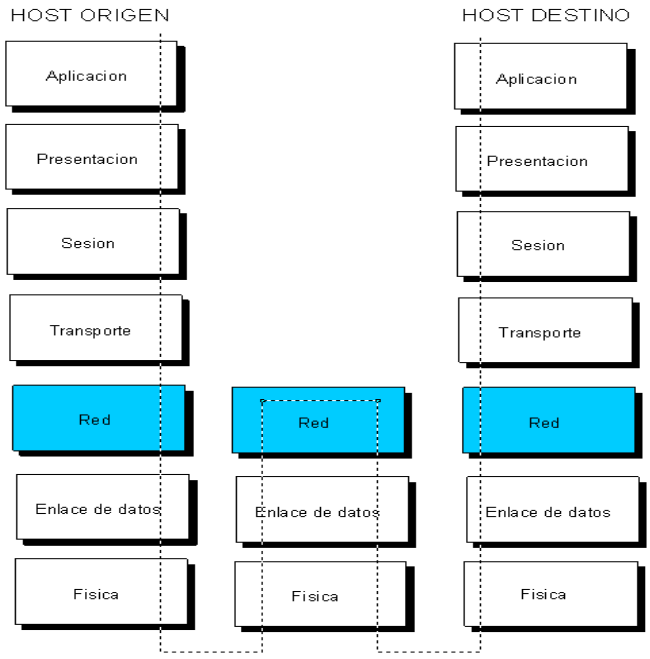
Enrutador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI.

Figura 19. Router o Enrutador

Fuente: (guayaquil.olx.com.ec, 2012)

Su función principal es enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, realiza toma decisiones en base a diversos parámetros con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados y solicitados.

Figura 20. Esquema de Funcionamiento del Router



Elaborado por: Jonathan Jara y Diego Mena

"Además se asegura que la información enviada por el emisor no vaya a un lugar innecesario, y en segundo lugar se preocupa de que la información llegue específicamente al destinatario." (Dukee, 2011)

Para ejecutar correctamente esta labor, el Router une las redes del emisor y del receptor de una información determinada a través de los protocolos de enrutamiento que utilizan los **Routers** para comunicarse entre sí, y de esta forma permitir el compartimiento de la información, tomando por ende la decisión de cuál es la ruta más adecuada en cada momento que se envié un paquete.

2.7.1.1. Funcionamiento

El funcionamiento de un Router consiste en almacenar un paquete y reenviarlo a otro Router o al host final.

Cada Router se encarga de decidir el siguiente salto en función de su tabla de encaminamiento. Por ser elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- **“Reenvío de Paquetes (Forwarding):** Cuando un paquete llega al enlace de entrada de un Router, éste tiene que pasar el paquete al enlace de salida apropiado.” (websolut, 2013)

- **“Encaminamiento de Paquetes (Routing):** Mediante el uso de algoritmos de encaminamiento es capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.” (websolut, 2013)

- **Traducción de Dirección de Red (NAT):** Permite a un Router, actuar como un agente entre Internet (red pública) y una red local (red privada). Esto significa que solo hace falta una única dirección IP para representar a un grupo entero de ordenadores. El NAT lo que hace es variar el puerto asociado a esa dirección IP, por lo que es válido asociar una sola IP a todo un grupo de ordenadores. (Eegle, 2010)

2.7.1.2. Protocolos de Enrutamiento

Los protocolos de enrutamiento permiten el intercambio de información dentro de un sistema autónomo. Tenemos los siguientes protocolos:

- **“Estado de Enlace**: se basa en la calidad y el rendimiento del medio de comunicación que los separa. De este modo cada Router puede construir una tabla del estado de la red para utilizar la mejor ruta: **OSPF.”** (Dyllan, 2009)

- **“Vector distancia**: cada Router indica a los otros Routers la distancia que los separa. Estos elaboran una cartografía de sus vecinos en la red: **RIP.”** (Dyllan, 2009)

- **Hibrido**: combina aspecto de los dos anteriores, como **EIGRP.** Los protocolos comúnmente utilizados son:

    - Routing Information Protocol (RIP)
    - Open Shortest Path First (OSPF)
    - Enhanced Interior Gateway Routing Protocol (EIGRP). (Dyllan, 2009)

2.7.1.3. Tipos de Routers

A continuación se listan los principales tipos de Routers:

“Básico: es aquel que tiene como función el comprobar si los paquetes de información que se manejan tiene como destino otro ordenador de la red o bien el exterior.” (WordPress, 2008)

Gama Baja: esta clase de Routers es el que se utiliza más frecuentemente en el ámbito doméstico pues cubre a la perfección las necesidades que puede tener el usuario en cualquier momento. Sus señales de identidad principales son que tienen capacidad para manejar multitud de información y que protegen muy bien del exterior a la red doméstica. (WordPress, 2008)

“Gama Alta: en empresas y entidades de gran calado es donde se apuesta por emplear este tipo de Routers ya que no sólo tiene capacidad para manejar millones de datos en un solo segundo sino también para optimizar el tráfico.” (WordPress, 2008)

“Inalámbricos: funcionan como una interfaz entre las redes fijas y las redes móviles como (**WiFi**, **WiMAX y otras**). Los Routers inalámbricos comparten similitudes con los Routers tradicionales, aunque admiten la conexión sin cables a la red en cuestión.” (WordPress, 2008)

2.7.2. Wireless LAN CONTROLLER

Un Wireless LAN Controller o (Controlador inalámbrico LAN) se utiliza en combinación con el Protocolo ligero de acceso a Punto (LWAPP) para gestionar ligeros puntos de acceso en grandes cantidades por el administrador de red o centro de operaciones de red .

Wireless LAN Controller forma parte del plano de datos en el modelo Wireless de Cisco. El Controlador WLAN maneja automáticamente la configuración de cualquier lugar desde 6 hasta 500 inalámbricos de acceso a los puntos, en función del modelo.

Características Principales:

• **Interferencia de Detección y Evitación:** potencia de RF y la asignación de canal se ajusta a la prevista.

• **Equilibrio de Carga:** desactivado de forma predeterminada, de alta velocidad de equilibrado de carga se puede utilizar para conectar un usuario a múltiples puntos de acceso para una mejor cobertura y las velocidades.

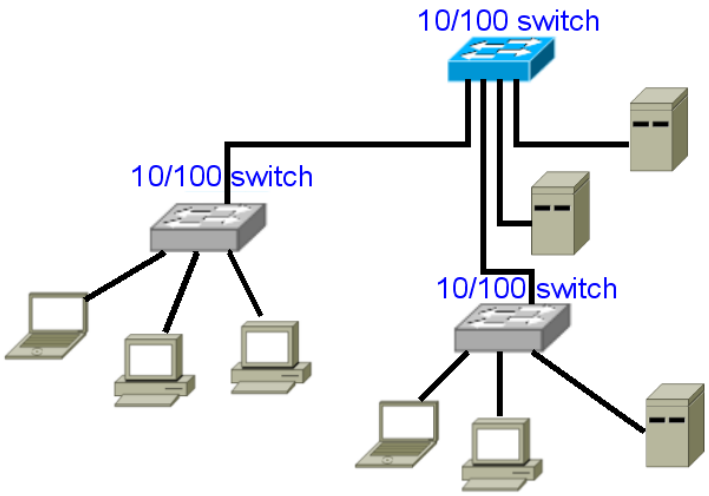
• **Detección y Corrección Agujero Cobertura:** parte de la gestión de RF es la capacidad de manejar niveles de potencia. La energía se puede aumentar para cubrir los agujeros o reducirse a proteger contra células superpuestas. El controlador de WLAN también viene con diversas formas de autenticación tales como:

- **Protected Extensible Authentication Protocol (PEAP)**
- **LEAP**
- **EAP-TLS**
- **Wi-Fi Protected Access(WPA)**
- **802.11i (WPA2)**
- **Layer 2 Tunneling Protocol (L2TP)**

2.7.3. Switch

Un Switch o conmutador un dispositivo de interconexión de redes de computadoras que trabaja directamente en la capa de enlace de datos del modelo OSI. Su función principal es interconectar dos o más segmentos de red y pequeños dominios de colisiones obteniendo un alto porcentaje de ancho de banda para cada estación final, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Figura 21. Segmentación de Dominios de Broadcast



Elaborado por: Jonathan Jara y Diego Mena

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor, mejorando el rendimiento y la seguridad de la red de área local. Actualmente se combinan con la tecnología Router para actuar como filtros y evitar el paso de tramas de datos dañadas.

2.7.3.1. Funcionamiento

El funcionamiento de un Switch radica en la capacidad que tiene de aprender y almacenar direcciones de red de dispositivos alcanzables a través de sus puertos. A diferencia de lo que ocurre con un hub o concentrador, el Switch hace que la información dirigida a un dispositivo vaya desde un puerto origen a otro puerto destino.

Los Switches tienen la capacidad de conservar las direcciones MAC de los equipos a los que puede llegar desde cada uno de sus puertos. De este modo, la información viaja de forma directa desde el puerto origen hasta el puerto de destino. (Definicionabc, 2013)

Ventajas:

- "Incremento de velocidad de la red
- Segmentación real **(**Ancho de banda completo para cada segmento**)**

- Conexión a backplanes de mayor velocidad
- Construcción de backbones
- Acelera la salida de paquetes
- Reduce tiempo de espera y baja el costo por puerto.” (Autónoma, 2000)

2.7.3.2. Tipos de Switch

Se tiene una gran variedad de Switches con distintas características y funciones, por ello se los clasifican en 2 grupos principales:

-Método de Direccionamiento de las Tramas:

- **Store-and-forward**: guarda los paquetes de datos en un buffer antes de enviarlo al puerto de salida. Si bien asegura el envío de datos sin error y aumenta la confianza de red, este tipo de Switch requiere de más tiempo por paquete de datos.

- **Cut-through:** reduce la demora del modelo anterior, ya que lee sólo los primeros 6 bytes de datos y luego lo encamina al puerto de salida.
  El problema de este tipo de Switch es que no detecta tramas corruptas causadas por colisiones (conocidos como runts), ni errores de CRC. Cuanto mayor sea el número de colisiones en la red, mayor será el ancho de banda que consume al encaminar tramas corruptas.

- **Adaptative Cut-through**: soportan operaciones de los dos modelos anteriores y son más utilizados en pequeños grupos de trabajo y pequeños departamentos. En esas aplicaciones es necesario un buen volumen de trabajo o throughput, ya que los errores potenciales de red quedan en el nivel del segmento.

-Segmentación de las Subredes

- **Switch Layer 2:** su principal finalidad es dividir una LAN en múltiples dominios de colisión, o en los casos de las redes en anillo, segmentar la LAN en diversos

anillos. Basan su decisión de envío en la dirección MAC destino que contiene cada trama.

Los Switches de capa 2posibilitan múltiples transmisiones simultáneas sin interferir en otras subredes. Pero no consiguen filtrar difusiones o broadcasts, multicasts ni tramas cuyo destino aún no haya sido incluido en la tabla de direccionamiento.

- **Switch Layer 3:** incorporan funciones de enrutamiento o routing, validación de la integridad del cableado de la capa 3 por checksum y soporte a los protocolos de routing tradicionales (RIP, OSPF, etc.).

  Además los Switches de capa 3 soportan también la definición de redes virtuales (VLAN), y según modelos posibilitan la comunicación entre las diversas VLAN sin la necesidad de utilizar un Router externo. Los Switches de capa 3 son particularmente recomendados para la segmentación de redes LAN muy grandes, donde la utilización de Switches de capa 2 provocaría una pérdida de rendimiento y eficiencia de la LAN.

- **Switch Layer 4:** básicamente incorporan a las funcionalidades de un conmutador de la capa 3; la habilidad de implementar la políticas y filtros a partir de informaciones de la capa 4 o superiores, como puertos TCP/UDP, SNMP, FTP, etc. Los Switches de capa 4 proporcionan encaminamiento adicional encima de la capa 3 mediante el uso de los números de puerto que se encuentran en el encabezado de capa de transporte para tomar decisiones de enrutamiento. Estos números de puerto se encuentran en RFC 1700 y hacen referencia al protocolo de capa superior, programa o aplicación.

  El mayor beneficio que prestan los Switches de capa 4 es que el administrador de la red puede configurar un Switch de capa 4 para priorizar el tráfico de datos por la aplicación, lo que significa una calidad de servicio puede ser definida para cada usuario.

  Esta clase de Switch está en el mercado hace poco tiempo y son llamados de también Layer 3+ **(Layer 3 Plus)**. (Tecnomagnific, 2011)

2.7.4. Servidores

Un servidores un equipo informático que forma parte de una red equipo dedicado a ejecutar uno o más servicios en beneficio de otros equipos denominados clientes dentro de la red.

> Un servidor puede ser desde un ordenador de última generación de grandes proporciones hasta un ordenador de menores características, todo depende del uso que se le dé al servidor, pero cabe recalcar que existe ordenadores diseñados específicamente para desempeñar funciones de servidor dotados de grandes prestaciones y soporte de multitarea. (Cyberprimo, 2010)

2.7.4.1. Tipos de Servidores

Existen gran cantidad de tipos de servidores o roles que estos pueden desempeñar, a continuación enumeramos algunos de los más comunes:

- **Servidores FTP:** File Transfer Protocol o (Protocolo de Transferencia de Archivos) traslada uno o más archivos entre distintos ordenadores proporcionando seguridad y organización de los archivos así como control de la transferencia.

- **Servidor de Directorio Activo/Dominio:** mantiene la información sobre los usuarios, equipos y grupos de una red.

- **Servidor de Telefonía IP**: realiza funciones relacionadas con la telefonía como un sistema interactivo para la respuesta de la voz, almacenamiento de los mensajes de voz, encaminamiento de las llamadas, un ejemplo claro de esto es la voz sobre IP (VoIP).

- **Servidor Proxy**: proporciona servicios de seguridad, o sea, incluye un cortafuegos. Además administra el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.

- **Servidor Web**: almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos, y distribuye este contenido a clientes en la red.

- **Servidor DNS:** establece la relación entre los nombres de dominio y las direcciones IP de los equipos de una red.

- **Servidor DHCP:** dispone de una rango de direcciones con el cual, asigna automáticamente los parámetros de configuración de red IP a las maquinas cliente cuando las mismas realizan una solicitudes.

- **Servidor de Base de Datos**: provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. Los Servidores de Bases de Datos surgen de la necesidad de las empresas de manejar grandes y complejos volúmenes de datos, al tiempo de requerir compartir la información con un conjunto de clientes.

- **Servidor de Seguridad**: tiene software especializado para detener intrusiones maliciosas, normalmente tienen antivirus, antispyware, antimalware, además de contar con cortafuegos redundantes de diversos niveles y/o capas para evitar ataques.

2.7.5. Access Point (AP)

"Un punto de acceso inalámbrico o AP, en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica." (slideshare.net, 2010)
Se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada para cualquier dispositivo que solicite acceder.

Figura 22. Access Point Cisco 1040

Fuente: (barcodesinc.com, 2010)

“Por otro lado un AP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos AP's pueden conectarse entre sí para formar una red aún mayor.” (todo-redes.com)

2.7.5.1. Principales Características:

- “Permiten la conexión de dispositivos inalámbricos a la WLAN, como: teléfonos celulares modernos, Notebook, Tablet, Netbook e inclusive otros Access Point para ampliar las redes.” (slideshare.net, 2010)

- “El Access Point puede tener otros servicios integrados como expansor de rango y ampliar la cobertura de la red.” (slideshare.net, 2010)

- “La tecnología de comunicación con que cuentan es a base de ondas de radio, capaces de traspasar muros, sin embargo entre cada obstáculo esta señal pierde fuerza y se reduce su cobertura.” (slideshare.net, 2010)

- “Cuenta con un alcance máximo de cobertura dependiendo el modelo, este puede estar desde 30 m hasta más de 100m.” (slideshare.net, 2010)

2.7.5.2. Modos de Operación del Access Point

"Modo Root: es el modo más común donde múltiples usuarios acceden al punto de acceso al mismo tiempo. En modo maestro, usuarios con portátiles y Tabletas pueden acceder a Internet a través de un solo Access Point compartiendo la conexión." (ordenadores-y-portatiles.com, 2013)

Modo Repetidor: se utiliza cuando quieres extender tu señal más allá de los límites actuales. Necesitas emplazar el punto de acceso en modo repetidor dentro del área de un punto de acceso en modo Root. Con esto la señal del AP maestro se extenderá con igual fuerza por medio de este AP repetidor mejorando el alcance. (ordenadores-y-portatiles.com, 2013)

Modo Bridge: como especifica el nombre, hacemos un puente inalámbrico entre dispositivos. Dos puntos de acceso en modo "bridge" solo hablarán entre ellos. Este tipo de conexión es útil cuando estás conectando dos edificios o localizaciones separadas donde instalar cableado no resulta fácil o económicamente viable. (ordenadores-y-portatiles.com, 2013)

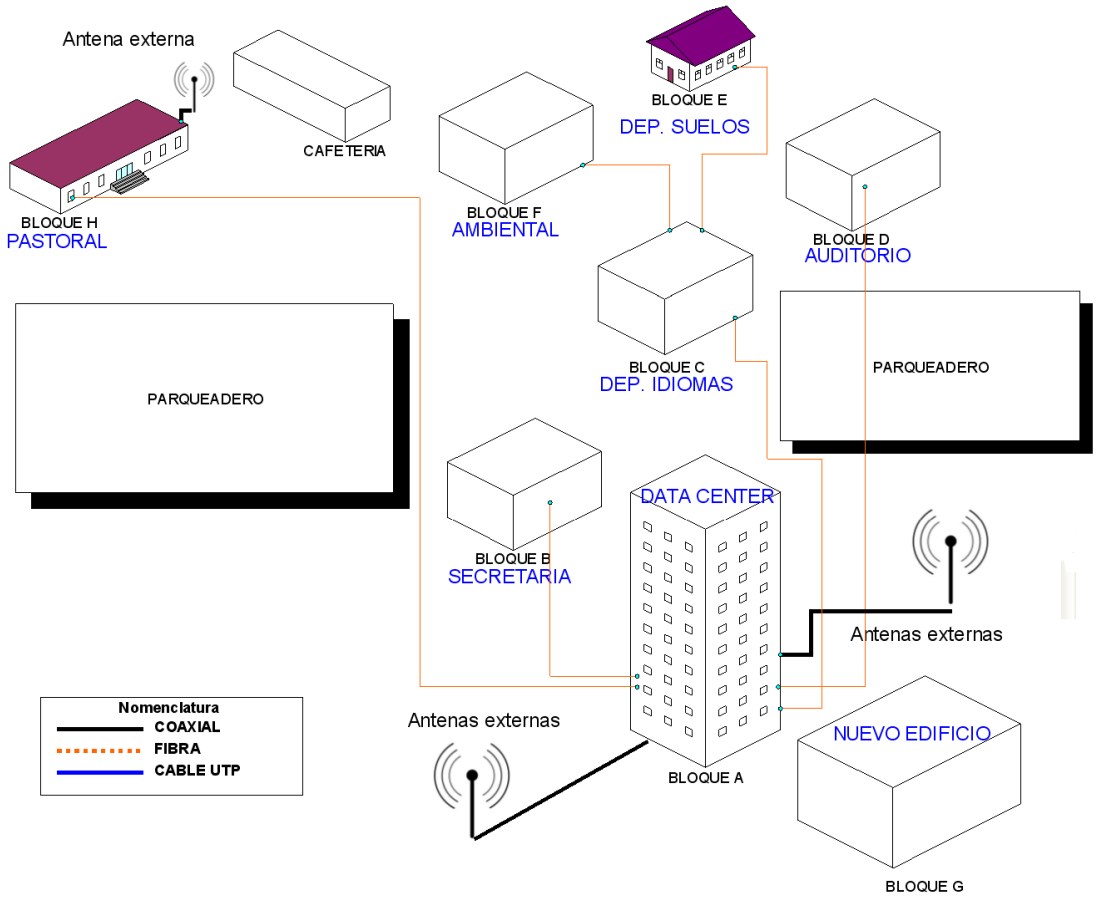
CAPÍTULO 3
ESTUDIO Y DESARROLLO

3.1. Estudio de la Situación Inicial de la Red de la Universidad Politécnica Salesiana Campus Sur

Se realiza un estudio de la situación actual de la red de la Universidad Politécnica Salesiana Campus Sur en cuanto a su topología física y lógica.

El Campus Sur se encuentra dividido en 8 bloques en total como se puede observar en la Figura 23, los cuales se listan a continuación:

Figura 23. Diagrama General de Campus Sur



Elaborado por: Jonathan Jara y Diego Mena

- Edificio Principal **(Bloque A)**

Aquí se encuentran localizadas 4 áreas de trabajo internas adicionales, a diferencia de los demás bloques:

- Recepción **(Primer Piso)**
- Biblioteca **(Primer Piso)**
- Cecasis **(Quinto Piso)**
- Data Center **(Sexto Piso)**

- Secretaria **(Bloque B)**
- Departamento de Idiomas y Laboratorios **(Bloque C)**
- Auditorio **(Bloque D)**
- Laboratorio de Suelos **(Bloque E)**
- Ambiental **(Bloque F)**
- Pastoral **(Bloque G)**
- Nuevo edificio **(Bloque H)**

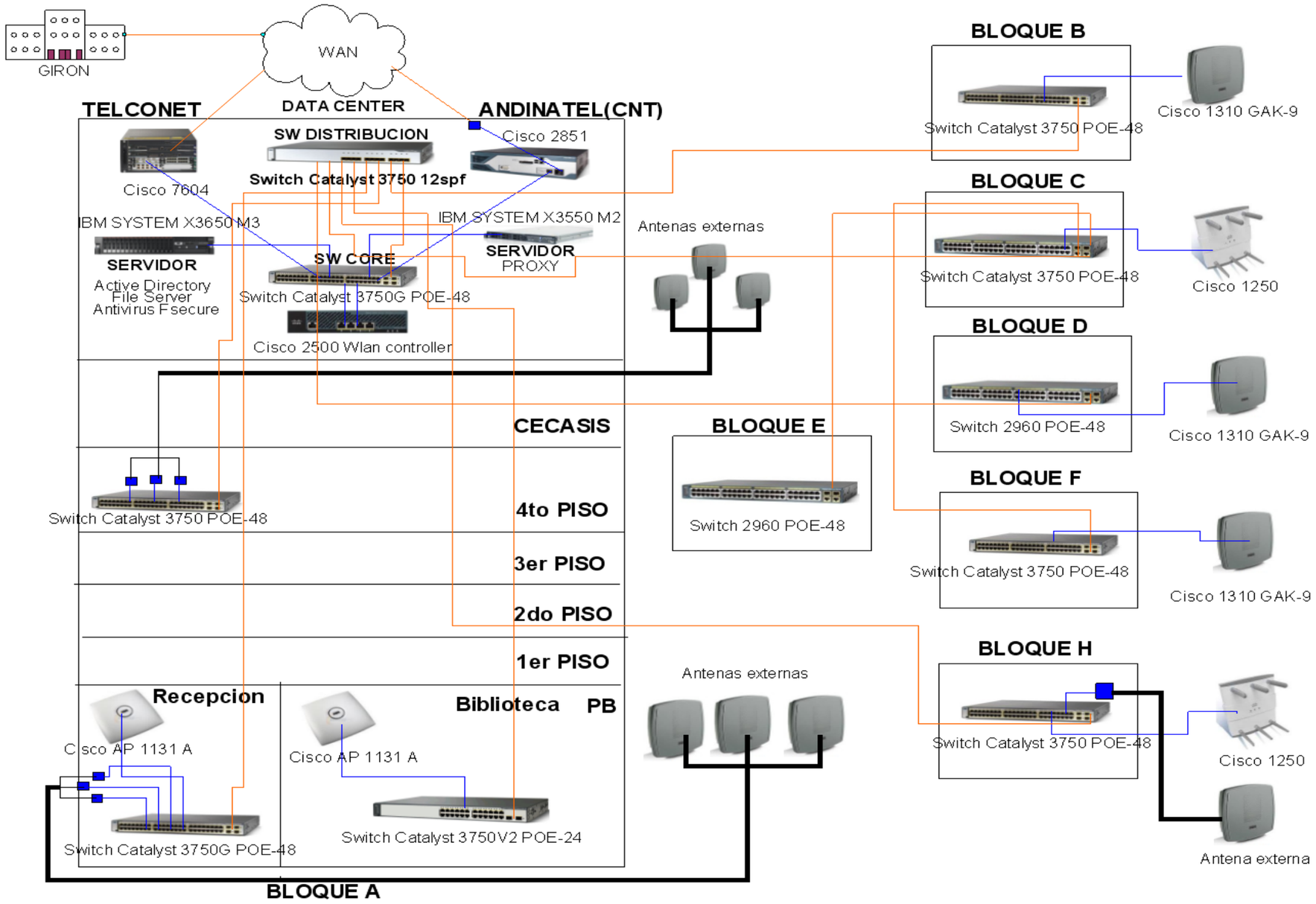
El Nuevo edificio no será tomando en este estudio, ya que este todavía se encuentra en construcción, en lo que respecta a la infraestructura de red todavía no cuenta con ningún dispositivo Wireless para ser tomado en cuenta en el presente levantamiento.

3.1.1. Esquema de Red Físico

La Infraestructura de la red física de la Universidad Politécnica Salesiana Campus Sur, esta implementada en su totalidad con equipos de la marca Cisco, posee una distribución de tipo centralizada, lo genera que las áreas de trabajo anteriormente mencionadas se encuentran directamente conectadas a un punto central, que este caso es **Data Center.**

1. Diagrama de Topología Física

Figura 24. Diagrama de la Topología Física



Elaborado por: Jonathan Jara y Diego Mena

3.1.1.1. Infraestructura Física

1. Data Center

En el Data Center se encuentra ubicado en el sexto piso del Edificio Principal de la Universidad (Bloque A), aquí se encuentran múltiples equipos de Networking más robustos y fundamentales para el funcionamiento de la red de la Universidad como son:

- Routers de Core **(Proveedores)**
- Switch de Core
- Switch de Distribución
- Servidores Blade y HP
- Wlan Controller

Para la conexión a la WAN, la Universidad dispone de enlaces redundantes que se observan en la Figura 24, con los cuales se conectan directamente al Campus el Girón, los mismos que permiten la salida a Internet y la transmisión de datos y voz. Estos servicios están provistos por las Empresas TELCONET y CNT.

- **Equipo de Telconet**

Utiliza un equipo Cisco 7604, el cual provee a la Universidad el servicio de Internet, Datos y voz mediante fibra óptica.

Figura 25. Router Cisco 7604

Fuente: (viasatelital.com, 2010)

- **Equipo de CNT**

Utiliza un transformador de fibra a cable UTP para conectarse con el equipo Cisco 2851 el cual provee únicamente servicios de datos.

Figura 26. Router Cisco 2851

Fuente: (world-point.ch, 2011)

- **Switch de Core**

El Switch de Core en marca Cisco Catalyst 3750G POE de 48 puertos y 4 interfaces ópticas o SPF extras. Es un dispositivo fundamental en la comunicación de toda la red ya que a este equipo se conectan los 2 Routers de los proveedores, el grupo de servidores, el Switch de distribución y el Wlan Controller.

Figura 27. Switch Cisco Catalyst 3750G POE-48P

Fuente: (mountakhab.net, 2010)

Adicionalmente para mejorar aun más la administración de la red de la Universidad, se han creado VLAN´s que segmentan el tráfico de la red según las áreas de trabajo de la siguiente manera:

- VLAN ADMINISTRATIVA
- VLAN CECASIS
- VLAN CISCO
- VLAN SUN
- VLAN SALAPROF
- VLAN SALA-INTERNET

- VLAN SALA-CECACIS
- VLANVIDEO
- VLANHP
- VLAN ELECTRONICA
- VLAN-TELCONET
- VLAN-IPCAM-CECASIS
- VLAN-WLAN-IPCAM-ELECTRONICA

- **Switch de Distribución**

El Switch de distribución en el data center es un Switch de fibra óptica modelo Cisco Catalyst 3750G 12-SPF, el cual permite la comunicación entre el Switch de Core y todos los Switch de acceso localizados en los diferentes bloques del Campus.

Figura 28. Switch Cisco Catalyst 3750G 12-SPF

Fuente: (tynex.com, 2012)

2. Wlan Controller

En lo que respecta a el control y administración de los Access Points y Antenas Externas de la universidad, se utiliza un equipo denominado WLAN CONTROLLER modelo Cisco 2500, el cual está conectado mediante un enlace redundante de cable UTP a el Switch de Core en Data Center.

Figura 29. Cisco 2500 Series Wlan Controller

Fuente: (tape4backup.com, 2012)

3. Switches de Acceso

Los Switches de acceso son modelos Cisco Catalyst 3750G POE-24/48P y se encuentran ubicados en las diferentes áreas de trabajo del Campus, que a continuación se listan:

- Departamento administrativo
- Biblioteca
- Cecasis
- Secretaria
- Idiomas y laboratorios de Electrónica
- Auditorio
- Laboratorio de suelos
- Ambiental
- Pastoral

Figura 30. Switch Cisco Catalyst 3750G POE 24/48P

Fuente: (Computrad, 2012)

- **Departamento Administrativo:** en esta área de trabajo es destinada para actividades por parte del personal Administrativo y CIMA de la Universidad, se encuentra localizada en la planta baja del bloque A, en la parte izquierda del edificio.

  Poseen un switch de acceso Cisco Catalyst 3750 POE-48P, al cual se interconecta la red LAN de toda el área Administrativa, el Access Point Cisco 1131-A para el servicio inalámbrico de toda esa área y las 3 antenas externas Cisco 1310 GAK-9

ubicadas en la entrada principal de la Universidad y dan el servicio de internet inalámbrico a los primeros pisos y alrededores del Edificio Principal.

- **Biblioteca:** esta área de trabajo es utilizada por los estudiantes de la Universidad, se encuentra localizada en la planta baja del bloque A, en la parte derecha del edificio.

  El Switch de acceso modelo Cisco Catalyst 3750V2 POE-24P se encuentra ubicado dentro de la oficina del personal encargado de la biblioteca. Este interconecta la red LAN del área de biblioteca y el Access Point Cisco 1131-A ubicado en biblioteca para dar el servicio de internet inalámbrico a toda esta área y por ende a las PC de biblioteca, ubicadas al lado izquierdo de la entrada, las mismas que son utilizadas para brindar servicio de internet y consultas de libros y tesis de grado en la base de datos de Universidad.

- **Cecasis:** esta área de trabajo es utilizada tanto por los estudiantes como por docentes, se encuentra ubicada en el quinto piso del bloque A. El Switch de acceso modelo Cisco Catalyst 3750G POE-48P, se encuentra en cuarto de control en el cuarto piso del Bloque. A este Switch se le interconecta toda la red LAN del área de CECASIS y adicionalmente las 3 antenas externas modelos Cisco 1310 GAK-9, ubicadas en la parte de atrás del Edificio Principal, y dan el servicio de internet inalámbrico a los pisos inferiores del CECASIS.

- **Secretaria:** esta área de trabajo es utilizada por Docentes y Personal Administrativo, y se encuentra ubicada en el primer piso del Bloque B. Su Switch de acceso modelo Cisco Catalyst 3750G POE-48P, se encuentra ubicado en el segundo piso del Bloque dentro de la Sala de Profesores.

  A este Switch se le interconecta la red LAN del área de trabajo de secretaria y el Access Point modelo Cisco 1310 GAK-9 que da el servicio de internet inalámbrico a las áreas de Docentes, Sala de Profesores y Secretaria.

- **Departamento de Idiomas y Lab. Electrónica:** esta área de trabajo se encuentra localizada en Bloque C, y es utilizada por Docentes y Alumnos, el Switch de

acceso es un modelo Cisco Catalyst 3750G POE-48P, se encuentra ubicado en el segundo piso del Bloque C en el interior del departamento de Idiomas.

Este Switch interconecta la red LAN para el área de trabajo de idiomas, los diferentes laboratorios electrónicos y el Access Point Cisco 1250, el cual da servicio de internet inalámbrico a todo el Bloque C. Además sirve de puente de comunicación entre el Data Center y los Bloques E y F.

- **Auditorio:** esta área de trabajo se encuentra en el Bloque D, es utilizada por Docentes y Alumnos, el Switch de acceso es un Cisco Catalyst 3750G POE-48P, se encuentra en ubicado en una aula de la Academia Cisco.

  Este Switch interconecta la red LAN para el área de trabajo de los laboratorios CISCO y SUN, como también el Access Point Cisco 1131-A el cual da servicio de internet inalámbrico a todo el Auditorio de la Universidad.

- **Laboratorio de Suelos:** esta área de trabajo se encuentra en el Bloque E, la es utilizada por estudiantes y docentes, el Switch de acceso es un Cisco Catalyst 3750G POE-48P, y se encuentra ubicado en el interior de la oficina principal de laboratorio de Suelos o Bloque E. Es importante resaltar que este Switch de acceso no tiene conexión directa hacia Data Center, se comunica mediante el Switch de acceso del Bloque C.

  Este Switch interconecta toda la red LAN del laboratorio de suelos, pero cabe mencionar que en esta área no se ha instalado ningún Access Point por lo que no cuenta con servicio de internet inalámbrico.

- **Ambiental:** esta área de trabajo se encuentra en el Bloque F, la cual es utilizada por Docentes y Estudiantes, el Switch de acceso es un Cisco Catalyst 3750G POE-48P, y se encuentra ubicado en el segundo piso del Bloque F. Este Switch interconecta la red LAN para el área de trabajo de ambiental y el Access Point Cisco 1310 GAK-9 para dar el servicio de internet inalámbrico a toda el área de ambiental.

  El Switch de acceso de esta área no tiene conexión directa hacia Data Center y al igual que el Switch de acceso del Bloque E, se comunica mediante el Switch de acceso del Bloque C.

- **Pastoral:** esta área de trabajo se encuentra el Bloque H, la cual es utilizada por Estudiantes y los Docentes del área de pastoral. El Switch de acceso es un Cisco Catalyst 3750G POE-48P, y se encuentra ubicado en el departamento de Pastoral.

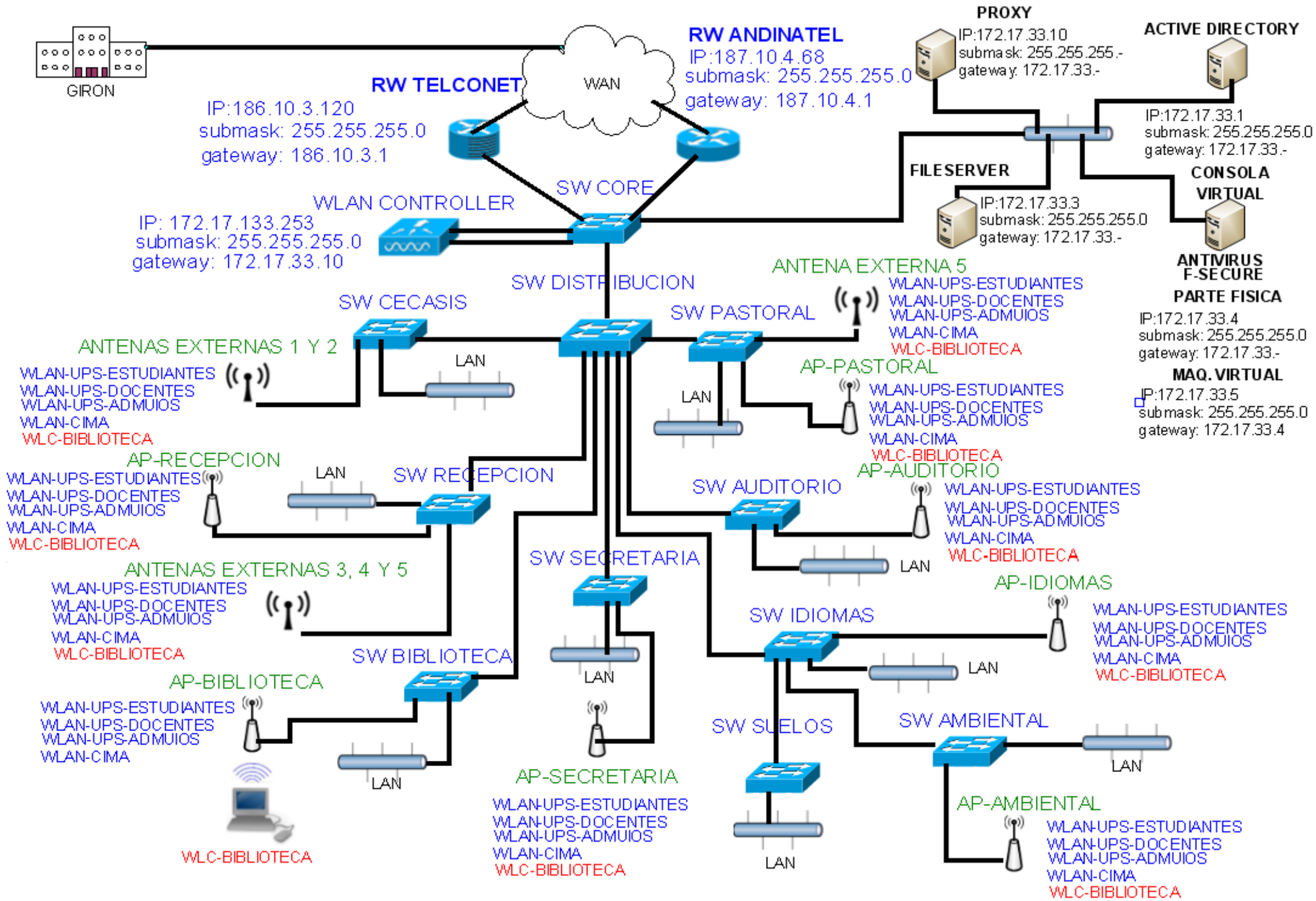
  A este Switch se le interconecta la red LAN del área de pastoral, el Access Point Cisco 1131-A, el cual da servicio de internet inalámbrico al área interna de pastoral y las antenas externas Cisco 1310 GAK-9, las cuales proveen del servicio de internet inalámbrico a los exteriores de pastoral, parte de los parqueaderos y parte de la cafetería.

3.1.2. Esquema de Red Lógica

En lo que respecta a la estudio de la red lógica de la Universidad Politécnica Salesiana Campus Sur, estará enfocado solamente a las redes inalámbricas de la Universidad. Por lo que la red LAN no será tomada en cuenta en dentro del presente análisis, ya que el portal cautivo es aplicado únicamente al ámbito de redes inalámbricas.

1. Diagrama de Topología Lógica

Figura 31. Diagrama de la Topología Lógica



Elaborado por: Jonathan Jara y Diego Mena

La topología lógica de la Universidad tiene la forma de estrella extendida como se puede observar en la Figura 31, lo que quiere decir que todos los Switches de acceso a la red de la Universidad están conectados a un Switch principal o Switch de core, el cual permite la comunicación de todos los bloques del campus sur y al mismo tiempo permite el acceso a los servicios prestados por la Universidad.

3.1.2.1. Direccionamiento Lógico

1. Routers

El Router de la Compañía TELCONET tiene la Dirección IP 186.10.3.120, utiliza una Submascara: 255.255.255.0 y su Puerta de Enlace o Gateway es la Dirección IP: 186.10.3.1/24.

El Router de la Compañía CNT tiene una Dirección IP: 187.10.4.68, utiliza una Submascara: 255.255.255.0 y su Puerta de Enlace o Gateway es la Dirección IP: 187.10.4.1/24

2. Servidores

La Universidad únicamente provee 4 servicios al campus sur, los cuales son los siguientes:

- **Servidor Proxy:** Este servicio está instalado en el equipo **IBM SYSTEM X335 M2**, el cual tiene la Dirección IP: 172.17.33.10, con una Submascara: 255.255.255.0 y su Puerta de Enlace o Gateway es la Dirección IP: 186.10.3.120
- **Active Directory:** Este servicio está instalado en el equipo **IBM SYSTEM X3650 M3**, el cual tiene la Dirección IP: 172.17.33.1, con una Submascara: 255.255.255.0 y su Puerta de Enlace o Gateway es la dirección IP: 172.17.33.10
- **Servidor de Archivos:** Este servicio está instalado en el equipo **IBM SYSTEM X3650 M3**, el cual tiene la Dirección IP: 172.17.33.3, con una Submascara: 255.255.255.0 y su Puerta de Enlace o Gateway es la Dirección IP: 172.17.33.10.

- **Servidor de F-Secure (Virtual**): Este servicio está instalado dentro de una maquina virtual en el equipo **IBM SYSTEM X3650 M3**. En lo que respecta a la parte física utiliza la Dirección IP: 172.17.33.4, con una Submascara: 255.255.255.0 y su puerta de enlace o Gateway la Dirección IP: 172.17.33.10. La máquina virtual con la consola del antivirus tiene la Dirección IP: 172.17.33.5, con una Submascara: 255.255.255.0 y su puerta de enlace la Dirección IP: 72.17.33.4.

3. WLAN CONTROLLER

Este dispositivo posee la tecnología para controlar todos los Access Point y las antenas externas instaladas en todo el Campus Sur de la Universidad. Este equipo tiene asignada la Dirección IP: 172.17.133.253 con una submascara: 255.255.255.0 y su puerta de enlace la Dirección IP: 186.10.3.1. Las antenas externas como los Access Point por el hecho de estar conectados al Wlan Controller trabajan como repetidores y reciben todas las configuraciones y las redes Inalámbricas múltiples establecidas en el Wlan Controller. A continuación listamos las redes inalámbricas que son administradas desde el Wireless Controller:

- **WLAN-UPS-ESTUDIANTES:** Es la Wireless LAN utilizada por los estudiante, el rango de direcciones IP es: 172.17.49.0 con una submascara 255.255.254.0 y su puerta de enlace es la dirección IP 172.17.49.254
- **WLAN-UPS-DOCENTES:** Es la Wireless LAN utilizada por los docentes, el rango de direcciones IP es: 172.17.131.0 con una submascara 255.255.254.0 y su puerta de enlace es la dirección IP: 172.17.131.254.
- **WLAN-UPS-ADMUIOS:** Es la Wireless LAN utilizada por el sector administrativo de la UPS, el rango de direcciones IP es: 172.17.34.0 con una submascara 255.255.255.0 y su puerta de enlace es la dirección IP 172.17.34.254
- **WLC –BIBLIOTECA:** Es una Wireless LAN enfocada únicamente a ser utilizada por las máquinas de alquiler utilizadas en la biblioteca, por lo que mediante una configuración en el Wlan Controller su SSID se encuentra oculto. El rango de direcciones IP utilizado es 172.17.41.0 con una

Submascara 255.255.255.192 y su puerta de enlace es la dirección IP 172.17.41.126.

- **WLAN-CIMA:** Es la Wireless LAN utilizada por el **Centro de Investigación en Modelamiento Ambiental (CIMA)** del Campus Sur. El rango de direcciones IP utilizado es 172.17.128.0 con una Submascara 255.255.255.192 y su puerta de enlace es la dirección IP 172.17.128.62, como se observa en la Tabla 5.

Tabla 5. Direccionamiento de la Redes Inalámbricas

NOMBRE DE RED (SSID)	RANGO DE DIRECCIONES IP	SUBMASCARA	GATEWAY	PROXY
WLAN –UPS-ESTUDIANTES	172.17.49.0	255.255.254.0	172.17.49.254	172.17.33.10
WLAN –UPS-DOCENTES	172.17.131.0	255.255.254.0	172.17.131.254	172.17.33.10
WLAN –UPS-ADMUIOS	172.17.34.0	255.255.255.0	172.17.34.254	172.17.33.10
WLAN –CIMA	172.17.128.0	255.255.255.192	172.17.128.62	172.17.33.10
WLAN –BIBLIOTECA	172.17.41.0	255.255.255.192	172.17.41.126	172.17.33.10

Elaborado por: Jonathan Jara y Diego Mensa

3.2. Servicios Web de la Universidad

Las aplicaciones y servicios usados por la Universidad Politécnica Salesiana Campus Sur son los que se listan a continuación:

- **Correo Electrónico**

La Universidad Politécnica Salesiana maneja el servicio de correo electrónico institucional, mediante un Microsoft Exchange Server. Cabe mencionar que este servicio utiliza el canal de datos proporcionado por la empresa CNT.

- **Pagina Web de la Universidad (www.ups.edu.ec)**

Este servicio es administrado desde la Sede Cuenca, proporciona información general de la Universidad, ambientes virtuales, matriculación online, correo

institucional en otros. Además contiene módulos que son utilizados tanto por alumnos para revisión de sus notas, como por docentes los cuales pueden ingresar las notas al sistema mediante el aula virtual. Este servicio utiliza el enlace proporcionado por TELCONET.

- **Antivirus F-SECURE**

Este servicio es el único que se encuentra implementado en una máquina virtual, se distribuye a dentro de la infraestructura del Campus Sur. El servidor necesita de una conexión continua al enlace de internet para bajar sus actualizaciones para después distribuirlas a los demás equipos clientes.

- **Sistemas Financieros y de Matriculación**

La Universidad Politécnica Salesiana utiliza aplicaciones basadas en Oracle, para los sistemas de administración, financieros, matriculación entre otros, los cuales se encuentran centralizados en la sede Cuenca y mencionamos a continuación:

- **SNA:** Es el sistema nacional Académico, el cual se registra toda la información y record académico de los estudiantes. Es utilizado por el personal administrativo y los docentes.
- **SIGAC:** Es el sistema contable donde se registra todos los pagos o depósitos de estudiantes, docentes y personal administrativo. Es utilizado únicamente por el personal administrativo.
- **SQUAD:** Es el sistema para la Gestión de talento humano, el cual registra toda la información personal de docentes y administrativos que laboran dentro de la universidad. Este sistema es utilizado únicamente por la parte administrativa encargada de la gestión de talento humano.
- **AVAC:** Es el sistema de Aulas virtuales, donde se consulta y se sube tareas a los estudiantes. En lo que respecta a los docentes, ellos pueden subir notificaciones sobre tareas o trabajos para que sean realizados por los alumnos y calificar los mismos. Este sistema es utilizado por docentes y alumnos.

Para la comunicación de estas aplicaciones, el Campus Sur se comunica con los servidores del Campus Girón, los cuales son un puente para comunicarse con la sede de Cuenca. Estas aplicaciones administrativas utilizan el enlace de CNT.

- **Internet**

Este servicio utiliza el canal de TELCONET, el Internet es distribuido por medio de un Proxy que se encuentra en el Campus Girón, y se lo administra por medio de conexión SSH en el Campus Sur. En general la mayoría de los servicios y aplicaciones son administrados directamente desde el Campus el Girón. A continuación en la Tabla 6 se presenta un resumen de todos los servicios.

Tabla 6. Servicios de la Universidad Salesiana

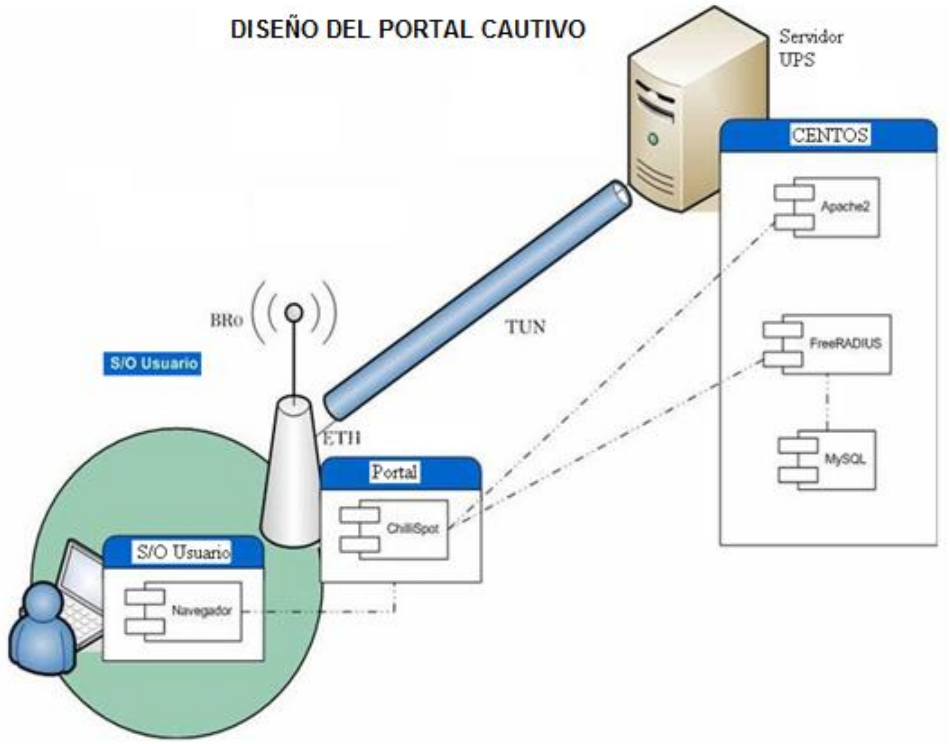
SERVICIOS	DESCRIPCIÓN	USUARIOS POR SERVICIO
CORREO ELECTRÓNICO	Correo Electrónico institucional mediante Microsoft Exchange	Estudiantes, Docentes, Administrativos y CIMA
PÁGINA WEB DE LA UNIVERDAD	Proporciona información general de la Universidad, permite acceso a otros servicios como el correo institucional, AVAC, etc.	Estudiantes, Docentes, Administrativos y CIMA
ANTIVIRUS F-SECURE	Servicio de antivirus el cual utiliza internet para tener actualizaciones de las bases de datos de virus	Docentes Administrativos CIMA
SNA	Registra la información y Record Académico de los estudiantes	Docentes Administrativos
SIGAC	Sistema Contable que registra todos los pagos o depósitos	Administrativos
SQUAD	Ingresa la información del personal de docentes y administrativos que laboran dentro de la universidad	Administrativos
AVAC	Sistema de Aulas virtuales	Estudiantes Docentes
INTERNET	Servicio de Navegación Web y VoIP	Estudiantes, Docentes, Administrativos y CIMA

Elaborado por: Jonathan Jara y Diego Mena

3.3. Diseño del Portal Cautivo

A continuación se presenta el esquema de diseño para el funcionamiento que tendrá el portal cautivo propuesto en la presente investigación:

Figura 32. Diseño de Funcionamiento del Portal Cautivo



Elaborado por: Jonathan Jara y Diego Mena

Descripción del proceso de funcionamiento del portal cautivo

1. Un usuario se conecta a la red inalámbrica.
2. El usuario ingresa a un navegador web.
3. Inmediatamente se ejecuta el portal cautivo como método de seguridad, en este caso Chillispot, y envía una página web al navegador del usuario con el fin de que el mismo sea autentificado.
4. El usuario envía sus datos para autenticarse y acceder al servicio de internet
5. El portal cautivo recibe los datos, y los envía al servidor radius para que los mismos sean verificados.
6. El servidor radius verifica si las credenciales enviadas por el usuario concuerdan con la información ingresada dentro de la base de datos del servidor
7. Si los datos enviados por el usuario concuerdan con la base de datos. El usuario será autenticado exitosamente y podrá acceder al servicio de internet.
8. En el caso, si las credenciales presentadas por el usuario no concuerdan con la base de datos, el servidor radius denegará el acceso al servicio de internet.

3.4. Implementación y Configuración del Portal Cautivo

Este capítulo consiste en la instalación y configuración de todas las herramientas de software y hardware que trabajaran en conjunto para dar como resultado un método de seguridad inalámbrico muy confiable.
Para la implementación del portal cautivo se iniciará primero por describir la instalación de cada uno de los programas informáticos a necesarios y seguidamente las configuraciones necesarias para el correcto funcionamiento.

3.3.1. Servidor Centos 6.2

Como primer punto para la implementación del portal cautivo será realizar la instalación del sistema operativo Centos 6.2, el cual será la base en donde se desarrollará el portal cautivo.
Guía de instalación descrita en la siguiente pagina de referencia. (Gonzalez, 2011)

3.3.2. Requisitos Previos a la Instalación del Portal Cautivo

Como pasos previos a la instalación del portal cautivo, se debe tener en que la versión de Centos instalada no viene con ningún aplicativo porque se debe tomar cuenta lo siguiente:

- Acceder como usuario **ROOT o súper-usuario** para evitar inconvenientes de permisos ya que durante la instalación será necesario la modificación de archivos del sistema.

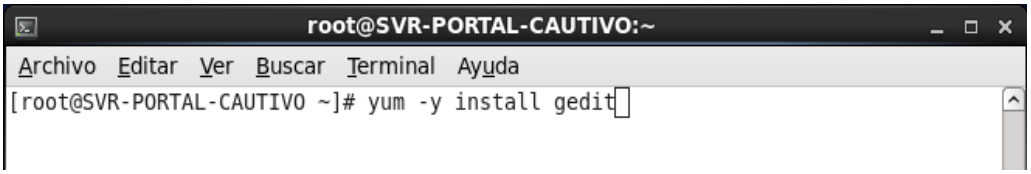
- Tener una conexión a internet estable ya que todas las herramientas y paquetes necesarios en la instalación se descargarán mediante internet.

- Instalar todas las actualizaciones disponibles de los repositorios a las versiones más actuales, cabe mencionar que este proceso puede tomar algunos minutos, mediante la línea de comandos:
  yum update

- Instalar el paquete **Gedit** que es utilizado para la edición de los archivos de configuración durante el proceso de instalación del portal cautivo, mediante la línea de comandos:

  yum -y install gedit

  Figura 33. Instalación de aplicación de edición gedit



  Elaborado por: Jonathan Jara y Diego Mena

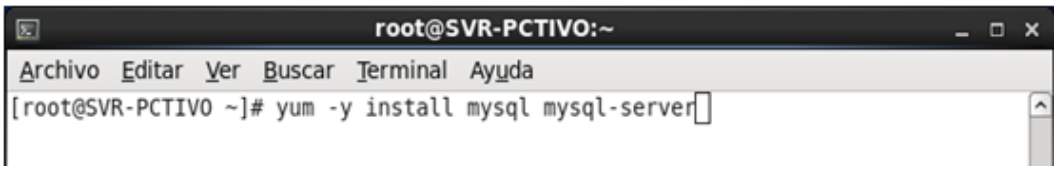
3.3.3. Servidor de Base de Datos

Un requisito fundamental para un portal cautivo que será implementado para una gran cantidad de usuarios es tener instalado un gestor de base de datos, en este caso utilizaremos **MYSQL-SERVER** para instalación del portal cautivo.

1. Se descargará e instalará el paquete de **MySQL,** mediante la siguiente línea de comandos:

   yum -y install mysql mysql-server

   Figura 34. Instalación de MySQL-Server



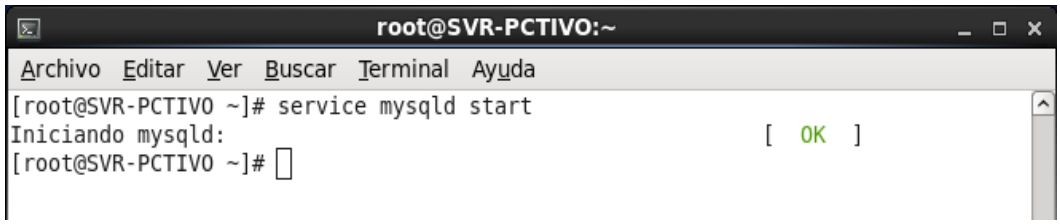
   Elaborado por: Jonathan Jara y Diego Mena

2. Se esperará a que complete toda la instalación.

3. Después, se iniciará el servicio de MySQL para verificar que se encuentre funcionando correctamente, mediante la línea de comandos:

   service mysqld start

Figura 35. Ejecución del Servicio Mysqld



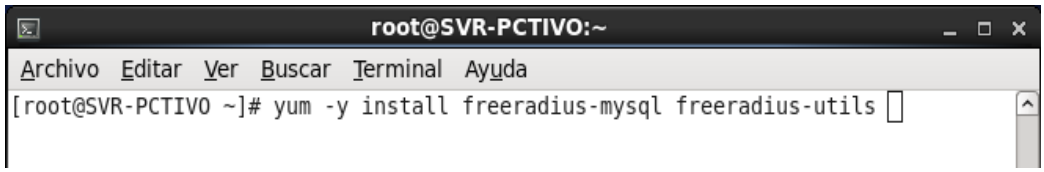
Elaborado por: Jonathan Jara y Diego Mena

3.3.4. Servidor Radius

Para la instalación de protocolo Radius utilizaremos el programa **FREERADIUS** que es el servidor Radius de código abierto más popular y utilizado en sistemas de seguridad.

1. Se descargará e instalará el paquete de **FREERADIUS** y sus herramientas adicionales para Centos 6.2, mediante la siguiente línea de comandos:
   yum -y install freeradius freeradius-mysql freeradius-utils

   Figura 36. Instalación de Freeradius



   Elaborado por: Jonathan Jara y Diego Mena

   Nota:

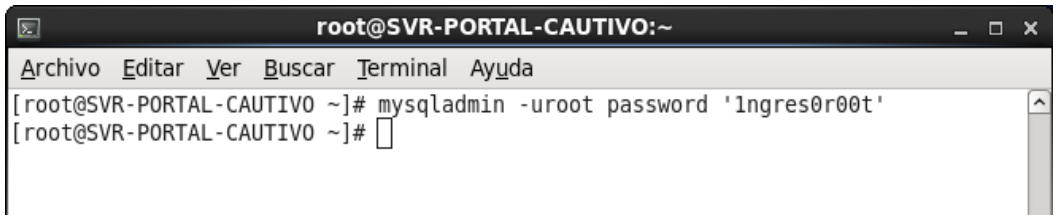
   En el caso que se desee instalar FREERADIUS en Centos 5, la línea de comandos va de la siguiente manera:

   yum -y install freeradius2 freeradius2-mysql freeradius2-utils

Creación de la Base de datos Radius en MySQL

1. Se asignará una clave de acceso al usuario root de MySQL, mediante la siguiente línea de comandos:
   mysqladmin -uroot password '1ngres0r00t'

Figura 37. Asignación de clave para usuario root en MySQL

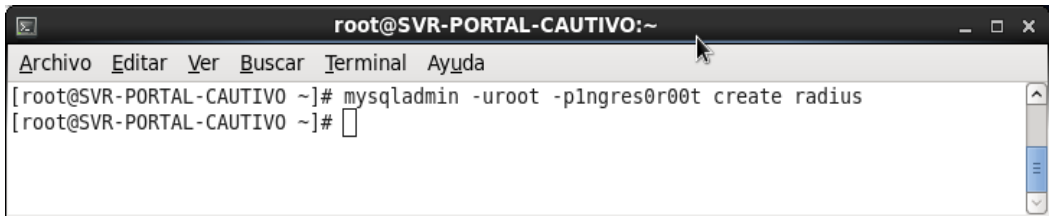


Elaborado por: Jonathan Jara y Diego Mena

2. A continuación, se creará la base de datos radius, la misma que trabajará con el Servidor Radius en la autenticación de usuarios, mediante la siguiente línea de comandos:

   mysqladmin -uroot –p1ngres0r00t create radius

Figura 38. Creación de la base de datos Radius

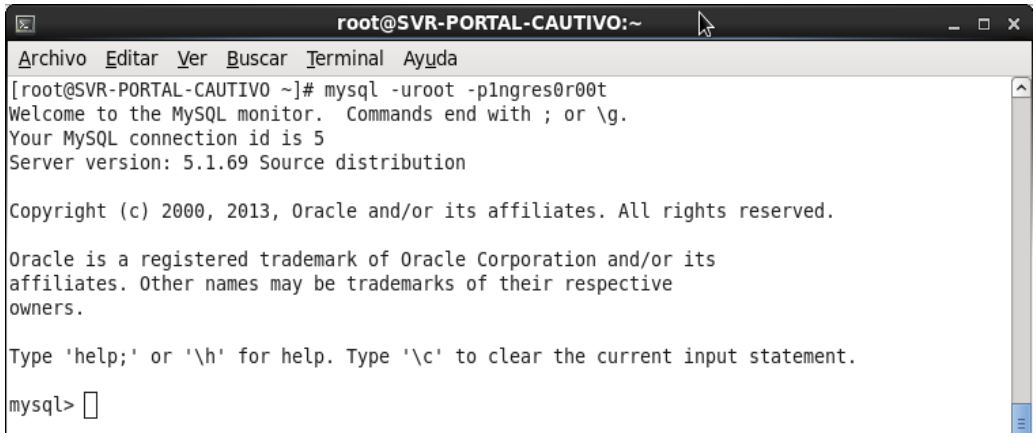


Elaborado por: Jonathan Jara y Diego Mena

3. Después se accederá a la consola de MySQL, como usuario root para no tener problemas de permiso, mediante la siguiente línea de comandos:

   mysql -uroot -p1ngres0r00t

Figura 39. Acceso a la Consola de MySQL



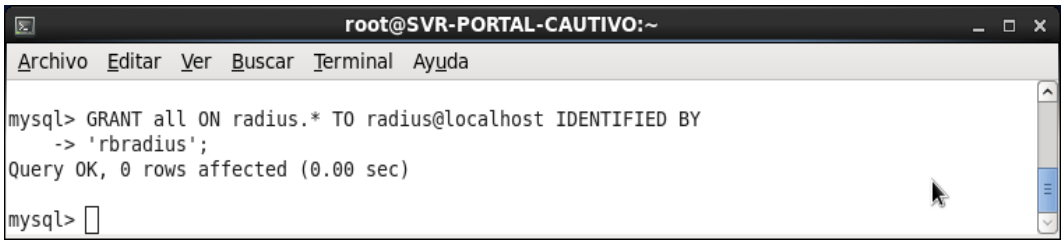
Elaborado por: Jonathan Jara y Diego Mena

4. Se designará los permisos al usuario radius que se creó al momento de instalar el freeradius y se le asignará una contraseña, mediante la siguiente línea de comandos:

   - **Usuario:** radius
   - **Contraseña: sucontraseña**

   GRANT all ON radius.* TO radius@localhost IDENTIFIED BY 'sucontraseña';

   Figura 40. Asignación de permiso a la Base de datos radius



   Elaborado por: Jonathan Jara y Diego Mena

5. Y a continuación se saldrá de la consola de MySQL mediante el comando **exit.**

   Figura 41. Comando para salir de consola de MySQL

   Elaborado por: Jonathan Jara y Diego Mena

6. Ahora, se utilizará el usuario radius y la base de datos radius anteriormente creadas para importar las tablas necesarias para el funcionamiento de freeradius.

   - **uradius:** Usuario radius
   - **prbradius:** Password del usuario radius
   - **radius:** Es la base de datos anteriormente creada

   mysql -uradius - prbradius radius < /etc/raddb/sql/mysql/cui.sql

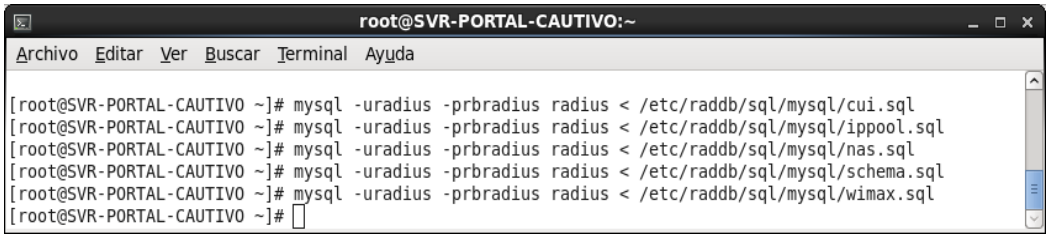
   mysql -uradius - prbradius radius < /etc/raddb/sql/mysql/ippool.sql

   mysql -uradius - prbradius radius < /etc/raddb/sql/mysql/nas.sql

   mysql -uradius - prbradius radius < /etc/raddb/sql/mysql/schema.sql

   mysql -uradius - prbradius radius < /etc/raddb/sql/mysql/wimax.sql

Figura 42. Importación de tablas radius a MySQL

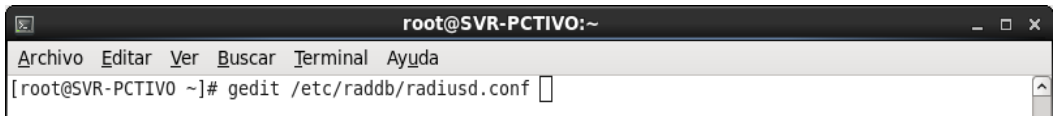


Elaborado por: Jonathan Jara y Diego Mena

7. Después, se editará el archivo **/etc/raddb/radiusd.conf,** mediante la siguiente línea de comandos:

   gedit /etc/raddb/radiusd.conf

Figura 43. Edición de Archivo de Configuración Radius.conf

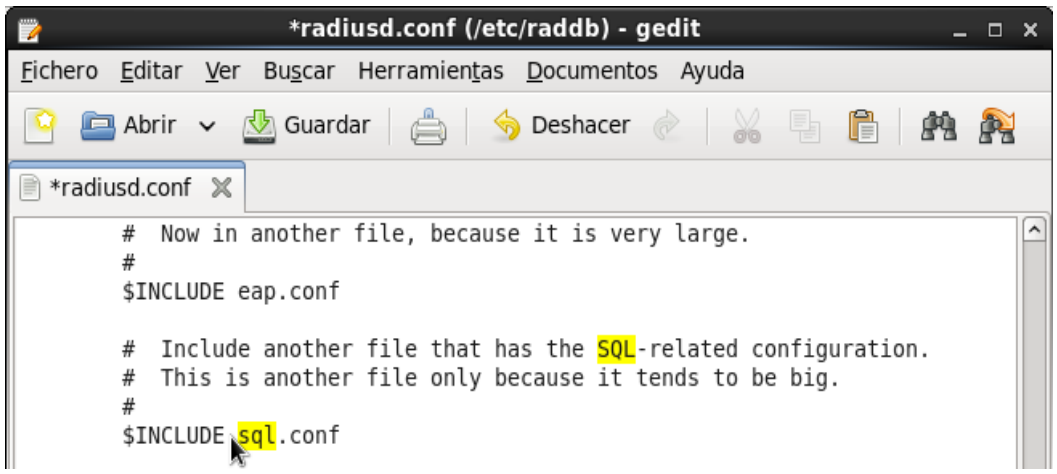


Elaborado por: Jonathan Jara y Diego Mena

8. Se descomentará la línea que dice **$INCLUDE sql.conf**, borrando el signo numeral **(#)** como se muestra en la Figura 3.35, quedando únicamente:

   $INCLUDE sql.conf

Figura 44. Descomentar $INCLUDE.conf en radius.conf

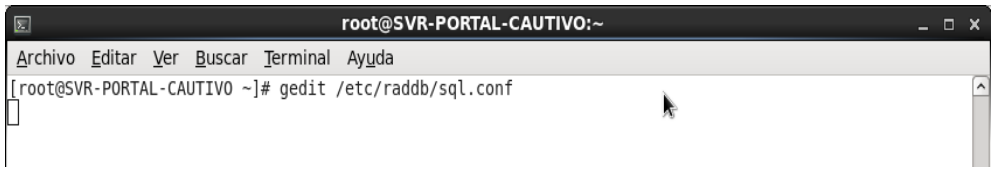


Elaborado por: Jonathan Jara y Diego Mena

9. Después, se tendrá que editar el archivo **/etc/raddb/sql.conf**, mediante la siguiente línea de comandos:

gedit /etc/raddb/sql.conf

Figura 45. Edición de Archivo de Configuración chilli.conf



Elaborado por: Jonathan Jara y Diego Mena

10. Después, se definirá los valores para la conexión a la base de datos, se modificará

 # Connection info:

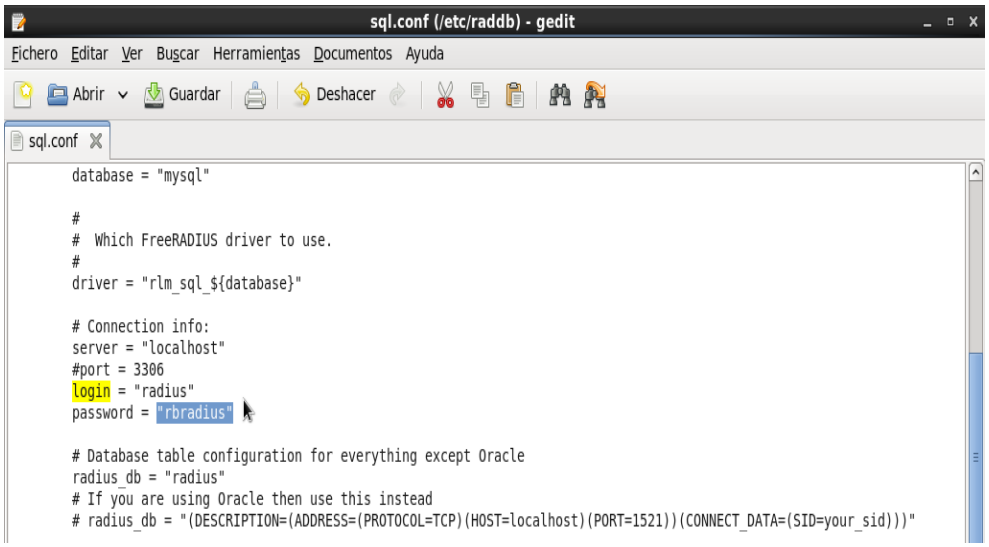
server = "localhost"

#port = 3306

login = "radius"

password = "sucontraseña"

Figura 46. Configuración de la Base de datos utilizada por Radius

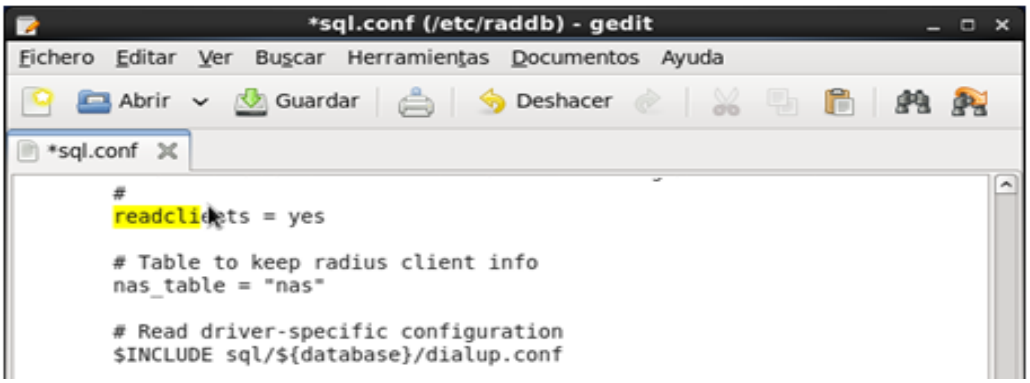


Elaborado por: Jonathan Jara y Diego Mena

11. También, se descomentará la línea **readclients** con el valor igual **yes**, lo cual permitirá que los clientes de las bases de datos estén activos al mismo tiempo que arranque el servidor, el cual se localiza en el mismo archivo **sql.conf,** debe quedar de la siguiente manera:

readclients = yes

Figura 47. Inicialización de clientes al arrancar MySQL

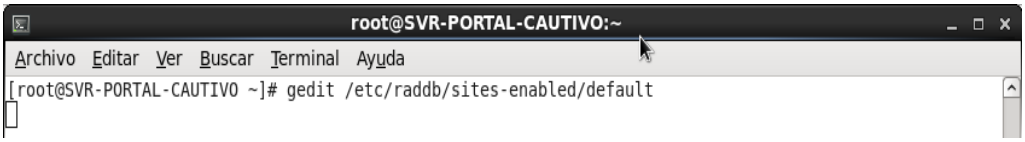


Elaborado por: Jonathan Jara y Diego Mena

12. Después, se editará el archivo **/etc/raddb/sites-enabled/default,** mediante la siguiente línea de comandos:

gedit /etc/raddb/sites-enabled/default

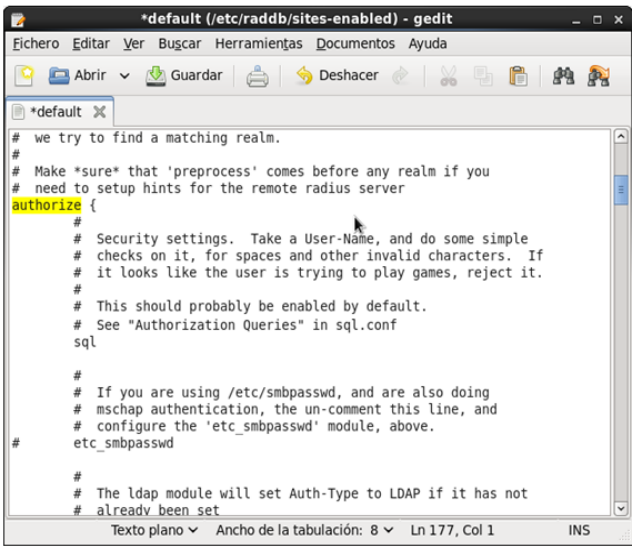
Figura 48. Edición del Archivo default



Elaborado por: Jonathan Jara y Diego Mena

13. A continuación en el archivo **default** se descomentará borrando el numeral **(#)**, en la sección **authorize** al inicio de la línea donde este **sql.**

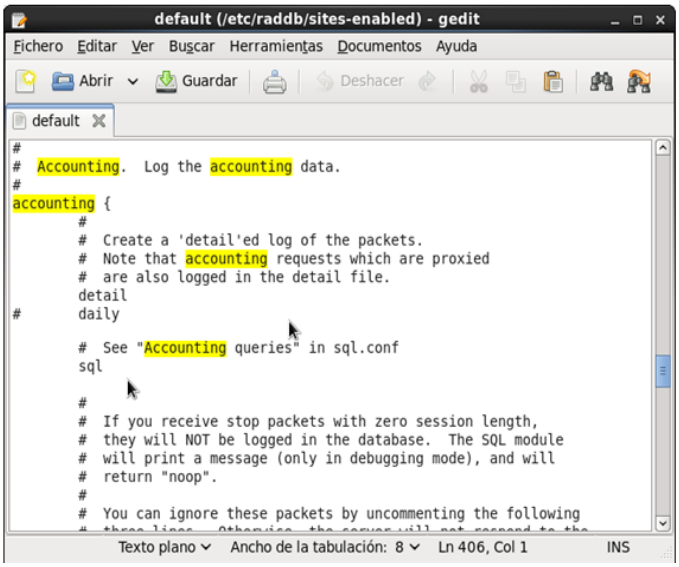
Figura 49. Sección Authorize del archivo default



Elaborado por: Jonathan Jara y Diego Mena

14. En el mismo archivo se descomentará el numeral **(#)** en la sección **accounting** al inicio de la línea donde este **sql.**

Figura 50. Sección Accounting del archivo default

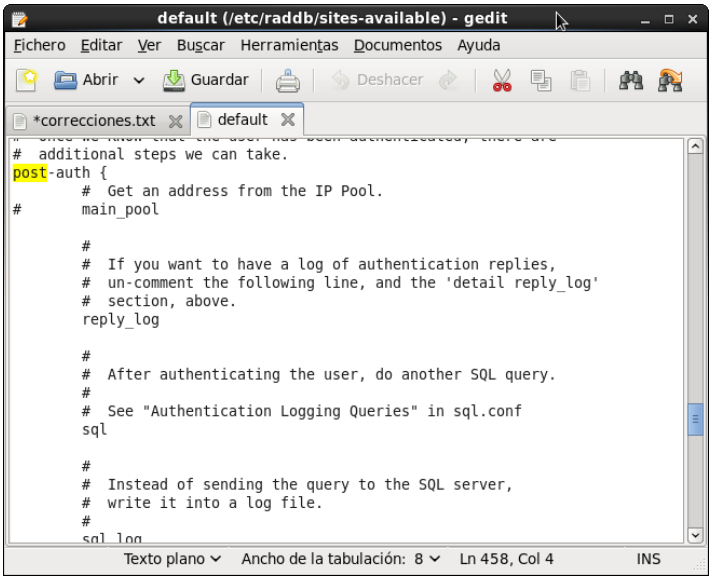


Elaborado por: Jonathan Jara y Diego Mena

Activación del generador de Logs en Radius

Para habilitar la emisión de logs en el servidor radius, se tendrá que editar el mismo archivo **/etc/raddb/sites-enabled/default, y** descomentará el numeral **(#)** en la línea **sql** en la sección **posth auth.**

Figura 51. Sección Posth auth para activar Logs en el archivo default



Elaborado por: Jonathan Jara y Diego Mena

El registro de todos los logs generados se encuentran almacenados en el directorio:

/var/log/radius

Figura 52. Directorio de localización de Logs generados

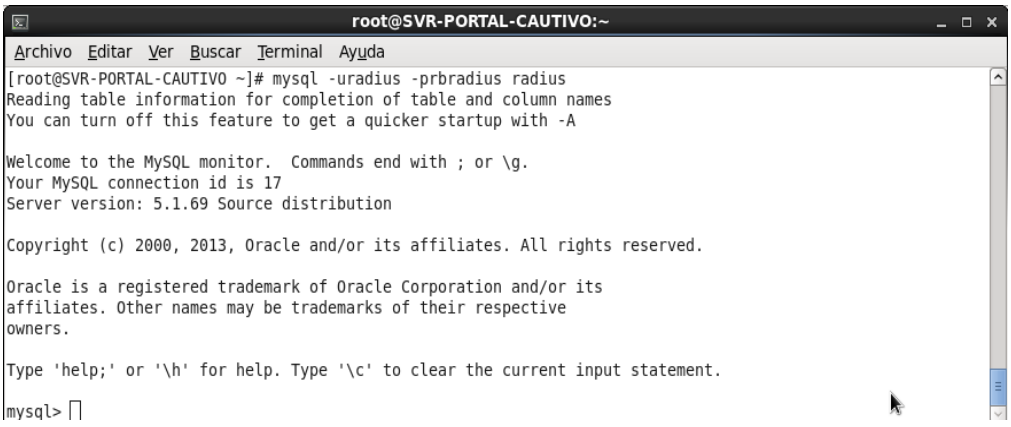
Elaborado por: Jonathan Jara y Diego Mena

Creación de Usuarios en Base de Datos del Portal Cautivo

1. Se deberá ingresar nuevamente a la consola de **MySQL** con las credenciales anteriormente creadas.

   mysql -uradius -psucontraseña radius

   Figura 53. Ingreso a la Consola de MySQL

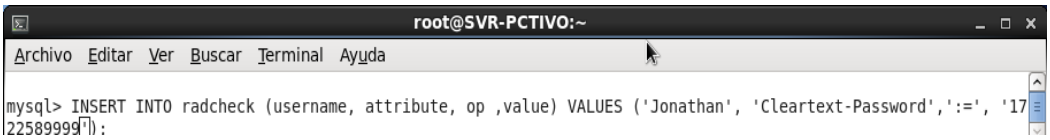


   Elaborado por: Jonathan Jara y Diego Mena

2. Después, se ingresará un usuario de prueba en la tabla **radcheck,** el cual se usará para verificar el funcionamiento de portal cautivo más adelante**,** mediante la siguiente línea de comandos:

   INSERT INTO radcheck (username, attribute, op, value) VALUES ('Jonathan', 'Clearext-Password', ':=', '1722589999');

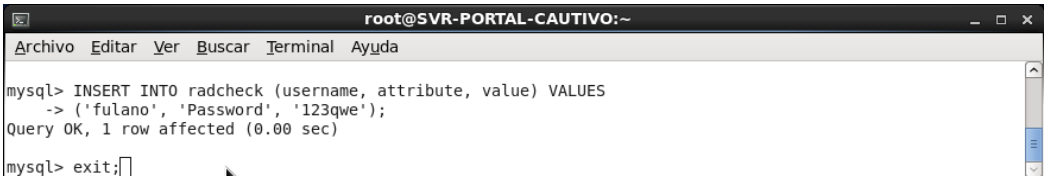
Figura 54. Ingreso de usuarios a la Base de datos del Radius



Elaborado por: Jonathan Jara y Diego Mena

3. Una vez efectuado el procedimiento anterior, se saldrá de la consola MySQL a través del comando **exit.**

Figura 55. Comando para salir de la consola de MySQL

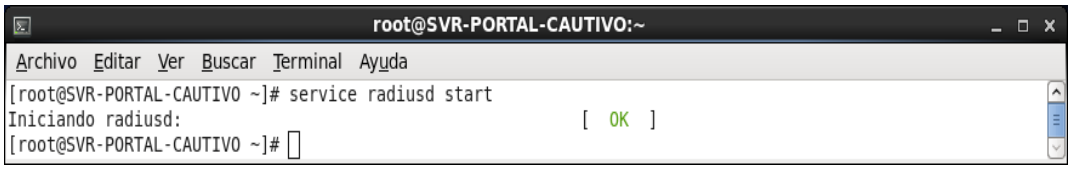


Elaborado por: Jonathan Jara y Diego Mena

4. A continuación, se iniciará el servicio **radiusd**, para verificar que el mismo este configurado correctamente, si se inicia significará que todas las acciones anteriores fueron correctas.

service radiusd start

Figura 56. Inicialización del Servicio Radius



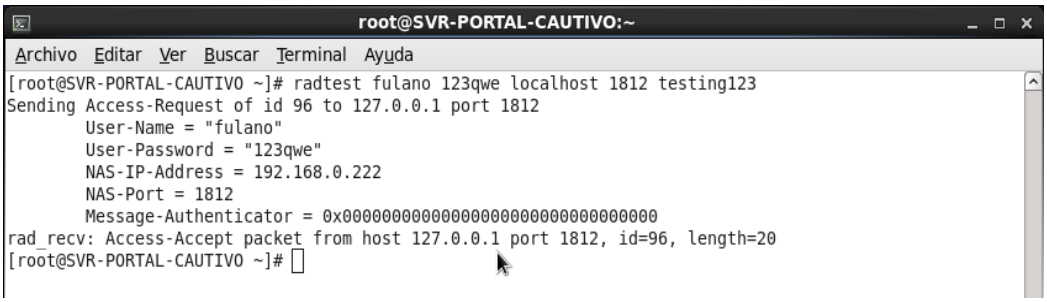
Elaborado por: Jonathan Jara y Diego Mena

5. Finalmente, se verificará que el servicio radius pueda autenticar a través de MySQL utilizando el comando **radtest,** mediante la siguiente línea de comandos:

radtest NombredeUsuario PassUsuario localhost 1812 testing123

- El resultado deberá ser el siguiente para confirmar que radius esta autentificando correctamente:

Figura 57. Prueba de Autenticación Radtest



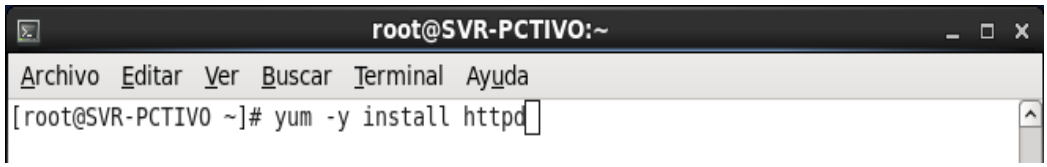
Elaborado por: Jonathan Jara y Diego Mena

3.3.5. Servidor HTTP

Es fundamental tener instalado el servicio http o web, puesto que es una herramienta complementaria para el funcionamiento del portal cautivo ya que el mismo se ejecuta sobre el servicio web.

1. Se descargará e instalará el servicio httpd para Centos 6.2, mediante la siguiente línea de comandos:
   yum -y install httpd

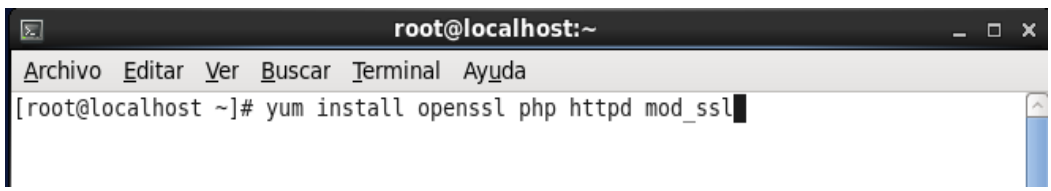
   Figura 58. Instalación de Servicio httpd



   Elaborado por: Jonathan Jara y Diego Mena

2. Después, se descargará e instalará módulos del servicio httpd como openssl, php, mod_ssl que son necesarios para el funcionamiento del portal cautivo.
   yum install openssl php httpd mod_ssl

   Figura 59. Instalación de openssl, php, mod_ssl

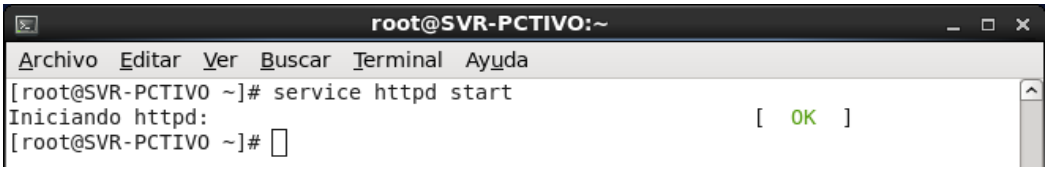


   Elaborado por: Jonathan Jara y Diego Mena

3. A continuación, se iniciará el servicio de httpd para verificar que el mismo se instalo y está funcionando correctamente, mediante la siguiente línea de comandos:

   service httpd start

   Figura 60. Inicialización del Servicio Apache



   Elaborado por: Jonathan Jara y Diego Mena

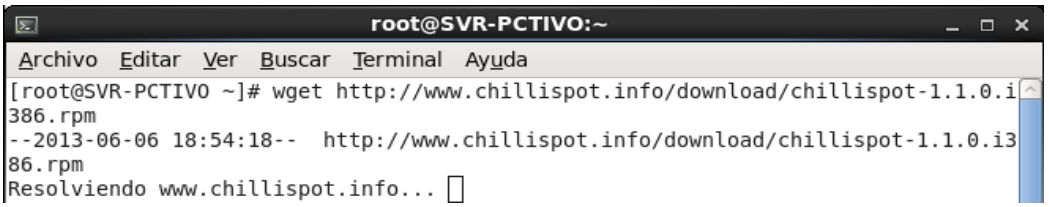
3.3.6. Portal Cautivo - Chillispot

Finalmente se instalará la herramienta que será el portal de seguridad para tener acceso al servicio de navegación web, en este caso utilizaremos **CHILLISPOT** por las robustas características de seguridad sobre redes WLAN que presenta.

1. Se descargará e instalará Chillispot de su página oficial, mediante la siguiente línea de comandos:

   wget http://www.chillispot.info/download/chillispot-1.1.0.i386.rpm

   Figura 61. Descarga del instalador de Chillispot

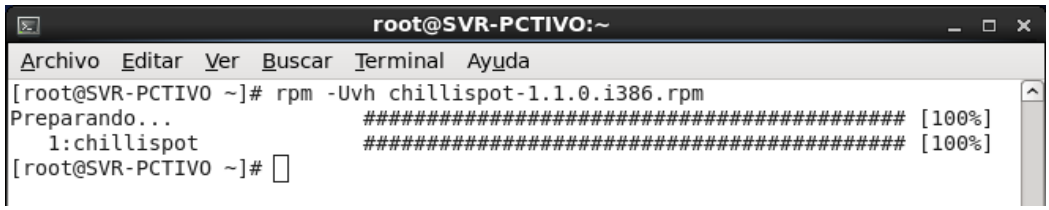


   Elaborado por: Jonathan Jara y Diego Mena

2. Después, se ejecutará el instalador de Chillispot, descargado anteriormente, mediante la siguiente línea de comandos:

   rpm -Uhv chillispot-1.1.0.i386.rpm

Figura 62. Instalación de Chillispot

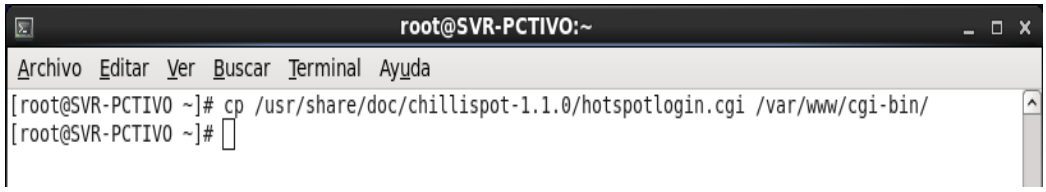


Elaborado por: Jonathan Jara y Diego Mena

3. A continuación, se copiarán los archivos de configuración de Chillispot a directorio del servidor httpd ya instalado anteriormente, mediante la siguiente línea de comandos:

cp /usr/share/doc/chillispot-1.1.0/hotspotlogin.cgi /var/www/cgi-bin/

Figura 63. Copiado del Archivo de Chillispot al directorio del Servidor Apache



Elaborado por: Jonathan Jara y Diego Mena

4. Seguido, se asignará los permisos de propietario APACHE al archivo contendedor del portal cautivo para evitar problemas durante su ejecución, mediante las siguientes línea de comandos:

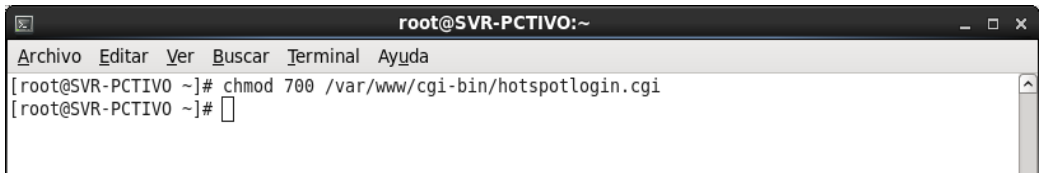
chown -R apache.apache /var/www/cgi-bin/hotspotlogin.cgi

Figura 64. Asignación de permisos de propietario APACHE al archivo .cgi

Elaborado por: Jonathan Jara y Diego Mena

chmod 777 /var/www/cgi-bin/hotspotlogin.cgi

Figura 65. Asignación de permisos al archivo .cgi del Portal Cautivo



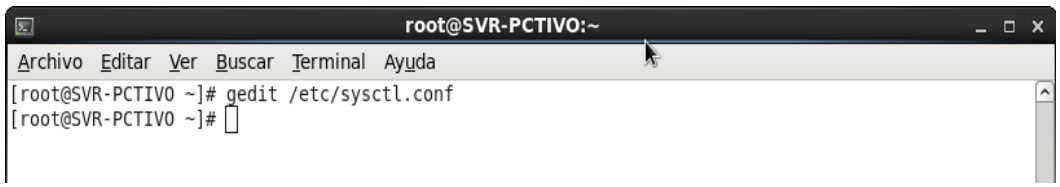
Elaborado por: Jonathan Jara y Diego Mena

5. Después, se deberá definir cuál de las 2 interfaces de red se usará como **LAN** y cuál se usará como **WAN** dentro del servidor para establecer el direccionamiento que llevará cada una de ella.
   - **eth0 - RED WAN**
     Dirección IP asignada según ISP
   - **eth1 - RED LAN**
     Dirección IP asignada según direccionamiento de red LAN interna

6. Seguido, se deberá asignar una dirección IP y puerta de enlace en la interfaz designada para **LAN,** en este caso se utilizaran las siguientes IP's dentro del direccionamiento que tendrá el servidor.
   - **eth1 - RED LAN**
     172.17.49.1
     255.255.254.0 Direccionamiento de red LAN
     172.17.49.5

7. A continuación, se editará el archivo **sysctl.conf** con el fin de habilitar el reenvió de paquetes para IPv4, mediante la siguiente línea de comandos:
   gedit /etc/sysctl.conf

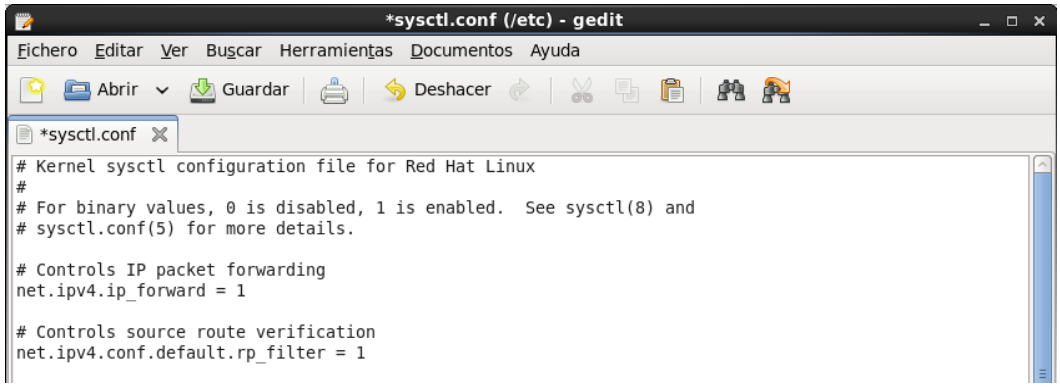
Figura 66. Edición del Archivo de Configuración sysctl.conf



Elaborado por: Jonathan Jara y Diego Mena

8. Se habilitará el reenvió de paquetes para IPv4 reemplazando **1** por **0** en la línea **net.ipv4.ip_forward = 0,** y guardamos los cambios efectuados

Figura 67. Habilitar reenvió de paquetes en la sección net.ipv4.ip_forward

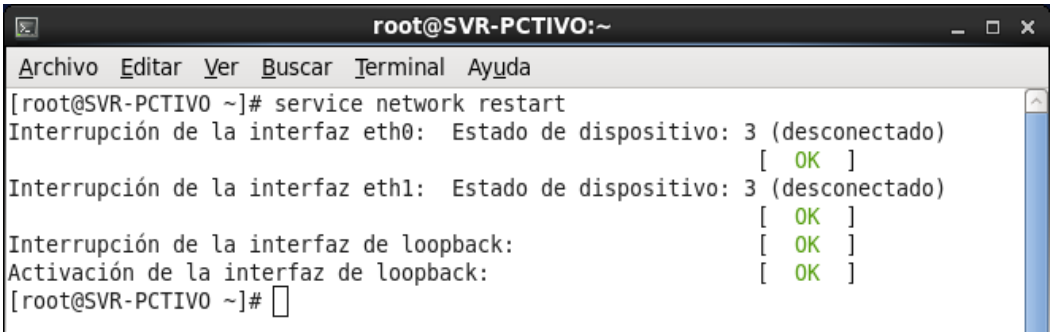


Elaborado por: Jonathan Jara y Diego Mena

9. Seguido, se reiniciará el servicio de red del servidor, mediante la siguiente línea de comandos:

service network restart

Figura 68. Reinicio de Interfaces de Red

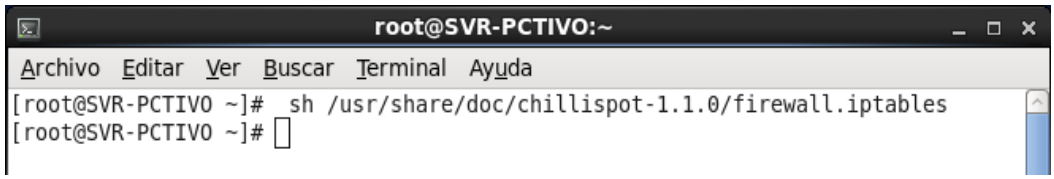


Elaborado por: Jonathan Jara y Diego Mena

10. Después para permitir Firewall y NAT, se ejecutará el script de firewall por defecto de Chillispot que se encuentra ubicado en el directorio **/usr/share/doc/chillispot-1.1.0/firewall.iptables,** mediante la siguiente línea de comandos:

sh /usr/share/doc/chillispot-1.1.0/firewall.iptables

Figura 69. Ejecutar el script de Firewall de Chillispot

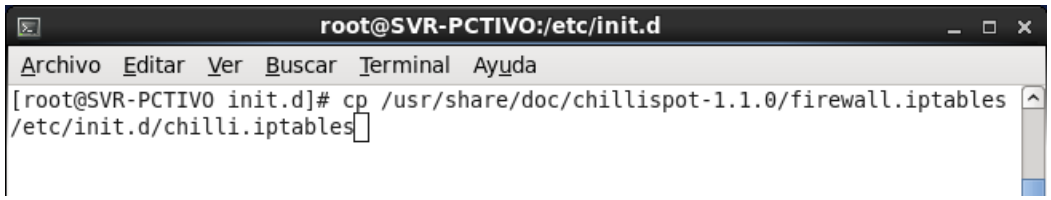


Elaborado por: Jonathan Jara y Diego Mena

11. El script de firewall de Chillispot llamado **firewall.iptables** debe ejecutarse cada vez que se reinicia el servidor de manera automática. Una forma de asegurarse de que esto suceda es copiar el archivo en directorio **/etc/init.d/,** y después se asignarán permisos de ejecución, mediante las siguientes líneas de comando:

cp /usr/share/doc/chillispot-1.1.0/firewall.iptables /etc/init.d/chilli.iptables

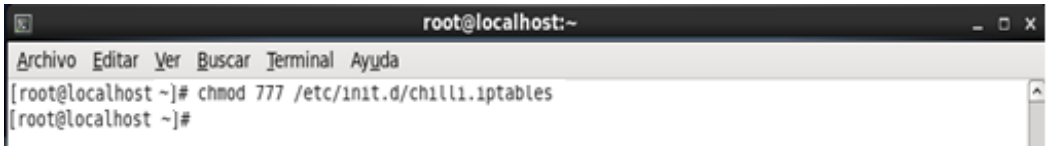
Figura 70. Copiado del script de Firewall de Chillispot



Elaborado por: Jonathan Jara y Diego Mena

chmod 777 /etc/init.d/chilli.iptables

Figura 71. Asignación de permisos del script del Firewall de Chillispot

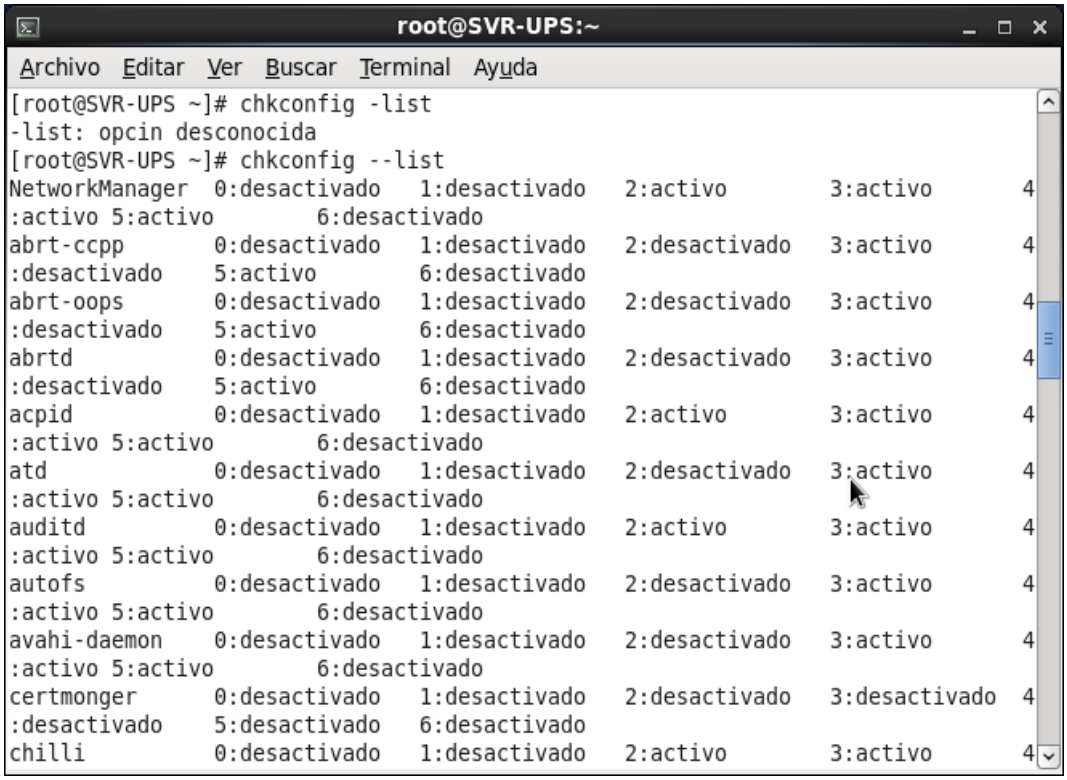


Elaborado por: Jonathan Jara y Diego Mena

12. Se verificará en que runlevels o niveles ejecución se encuentran los servicios que se inicializan automáticamente cuando se inicia el sistema operativo Centos, mediante la siguiente línea de comandos:

chkconfig -list.

Figura 72. Listado de servicios y runlevels



Elaborado por: Jonathan Jara y Diego Mena

13. Después, se creará un enlace simbólico en cada uno de los runlevels o niveles de ejecución **2, 3, 4, 5** que son los niveles donde se encuentran los servicios de inicialización del sistema operativo, para que el script **firewall.iptables** al igual que los servicios del sistema se inicialice automáticamente se cada vez que se reinicie o se apague el servidor, mediante la siguiente línea de comandos:

ln -s /etc/init.d/chilli.iptables /etc/rc2.d/S98chilli.iptables

- **Donde:**

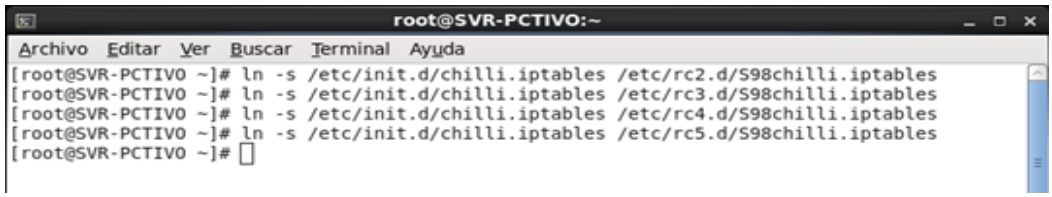
El **rc2.d** indica el runlevel en el que se iniciará, la **S** significa **Start** lo que permite que se inicie el script, el número **98** es la posición en la cual iniciará el script, el orden puede ir desde **1 al 99**, y finalmente se pondrá un nombre al enlace simbólico en este caso se llamara igual que el script que se encuentra en **/etc/init.d.** Se aplicará la misma línea de comandos simplemente variando el número de runlevel en cada una:

ln -s /etc/init.d/chilli.iptables /etc/rc3.d/S98chilli.iptables

ln -s /etc/init.d/chilli.iptables /etc/rc4.d/S98chilli.iptables

ln -s /etc/init.d/chilli.iptables /etc/rc5.d/S98chilli.iptables

Figura 73. Creación de Enlaces Simbólicos Firewall de Chillispot



Elaborado por: Jonathan Jara y Diego Mena

Configuración de Chillispot

1. Para la configuración de Chillispot, se modificará el **chilli.conf** que encuentra en ubicado en el directorio **/etc/chilli.conf,** mediante la siguiente línea de comandos:
   gedit /etc/chilli.conf

   Figura 74. Edición del Archivo de Configuración chilli.conf

   Elaborado por: Jonathan Jara y Diego Mena

2. Primero, se modificará el apartado TUN Parameters, en la sección **net** se descomentará la línea borrando el numeral (#), y se asignará la IP de la red con la trabajara el Chillispot, y deberá quedar de la siguiente manera:
   net 172.17.49.4/23

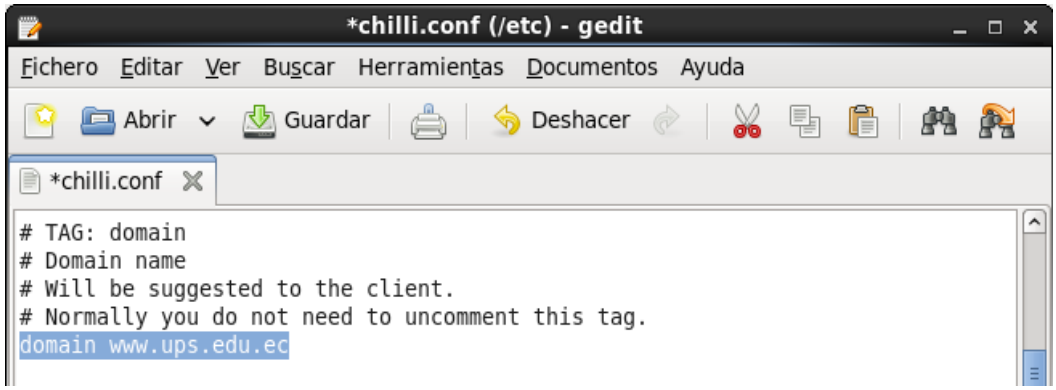
   Figura 75. IP de la red que utilizará Chillispot

   Elaborado por: Jonathan Jara y Diego Mena

3. En el aportado **domain,** se descomentará la línea borrando el numeral (#), y se asignará un nombre de dominio si es necesario, caso contrario se establecerá por defecto el dominio del Chillispot **key.chillispot.org,** y deberá quedar de la siguiente manera:

   domain www.ups.edu.ec

Figura 76. Configuración del Nombre de Dominio

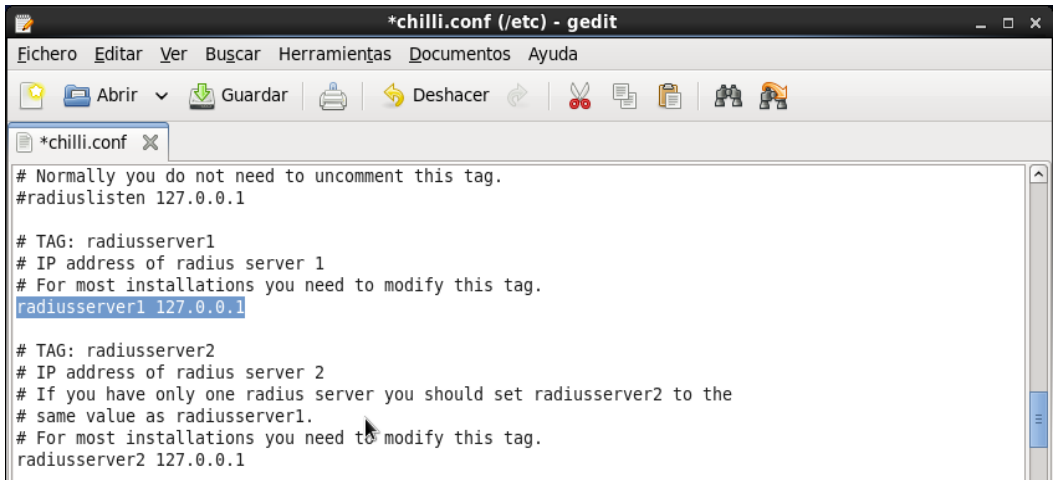


Elaborado por: Jonathan Jara y Diego Mena

4. A continuación en los apartados **radiusserver1 y radiusserver2**, se modificará con la dirección 127.0.0.1 en ambos, y deberá quedar de la siguiente manera:

   radiusserver1 127.0.0.1
   radiusserver2 127.0.0.1

Figura 77. Configuración de Servidores Radius



Elaborado por: Jonathan Jara y Diego Mena

5. Seguido, se modificará el campo **radiussecret,** con una contraseña la cual debe ser estrictamente la misma que se asigne en el archivo **clients.conf** que es parte de los archivos de configuración de **freeradius,** como se puede observar en la Tabla 7, este proceso se realizará con el fin de relacionar los 2 servicios para que trabajen conjuntamente.

Tabla 7. Relación de Contraseñas de Chillispot y Freeradius

SERVICIO	ARCHIVO DE CONFIGURACION	LINEA DE CODIGO
CHILLISPOT	/etc/**chilli.conf**	secret = **passwordR**
RADIUS	/etc/raddb/**clients.conf**	radiussecret **passwordR**

Elaborado por: Jonathan Jara y Diego Mena

gedit /etc/chilli.conf

radiussecret **tesisups**

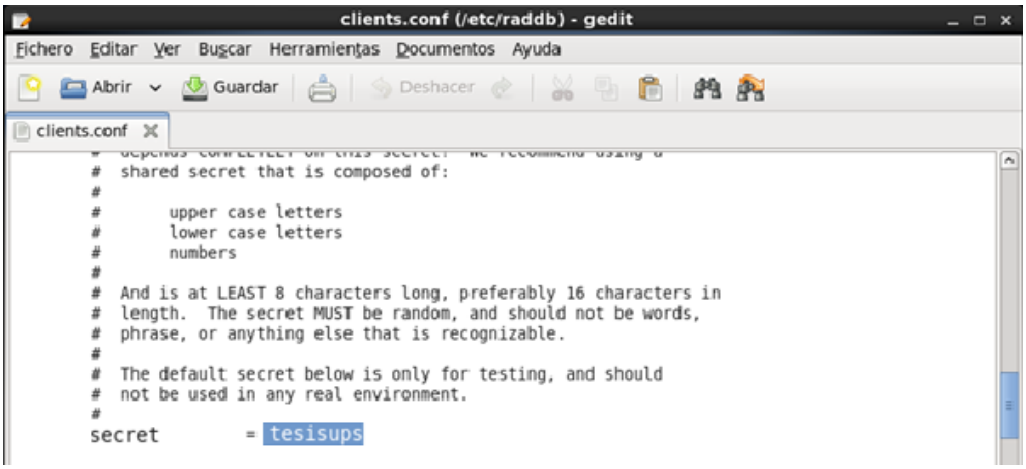
Figura 78. Configuración de la Sección radiussecret en chilli.conf

Elaborado por: Jonathan Jara y Diego Mena

gedit /etc/raddb/clients.conf

secret = **tesisups**

Figura 79. Configuración de la Sección secret en clients.conf



Elaborado por: Jonathan Jara y Diego Mena

6. A continuación en el aparatado **DHCP Parameters,** se deberá cambiar a la interfaz que sale a la red LAN para la generación del servicio DHCP por parte del servicio de Chillispot, quedando de la siguiente manera:

   dhcpif suinterfazLAN

Figura 80. Configuración de Interfaz de Salida de DHCP

Elaborado por: Jonathan Jara y Diego Mena

7. Después buscamos el apartado **uamserver,** se editará la línea y lo único que variará será la dirección IP dependiendo del direccionamiento que se esté usando, quedando de la siguiente manera:

   uamserver https://172.17.49.5/cgi-bin/hotspotlogin.cgi

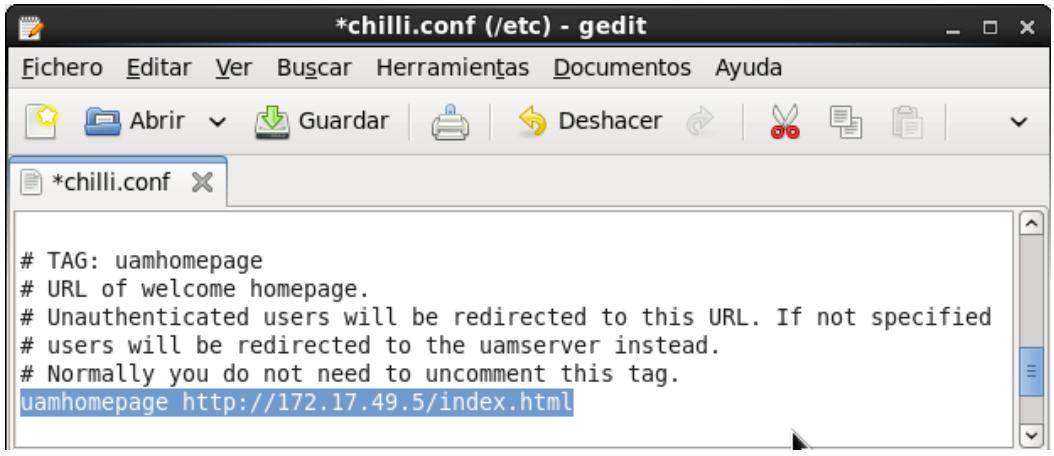
Figura 81. Configuración de Dirección de Portal Cautivo

Elaborado por: Jonathan Jara y Diego Mena

8. El apartado **uamhomepage,** es opcional modificarlo, todo dependerá si se va utilizar una página inicial informativa, reglamentaria etc., la misma que irá antes de acceder al portal cautivo, si fuera el caso se deberá modificar, quedando de la siguiente manera:

   uamhomepage **http://172.17.49.5/index.html**

Figura 82. Configuración de Página Web Inicial

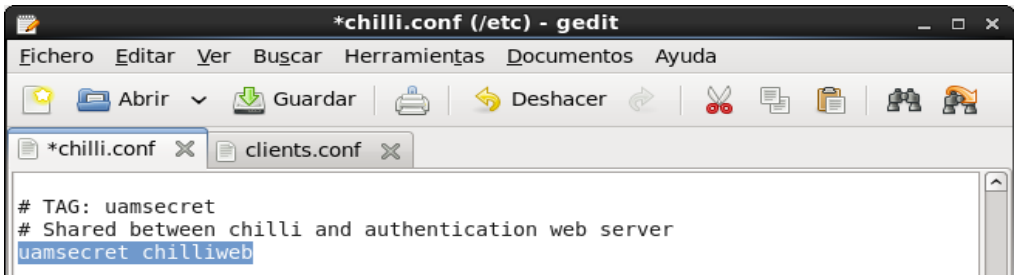


Elaborado por: Jonathan Jara y Diego Mena

9. A continuación en el apartado **uamsecret,** se descomentará la línea borrando el **(#)** inicial y se asignará una contraseña la cual permite la autenticación de Chillispot con el servidor web, quedando de la siguiente manera:

   uamsecret **chilliweb**

Figura 83. Contraseña de autentificación de Chillispot con el servidor Web

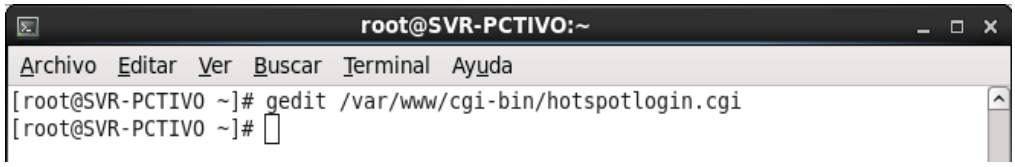


Elaborado por: Jonathan Jara y Diego Mena

10. Para mejorar la seguridad de contraseñas a través de encriptación**,** se editará el archivo **hotspotlogin.cgi** que se encuentra ubicado en el directorio **/var/www/cgi-bin/hotspotlogin.cgi,** mediante la siguiente línea de comandos:

gedit /var/www/cgi-bin/hotspotlogin.cgi

Figura 84. Edición de Archivo Principal del Portal Cautivo

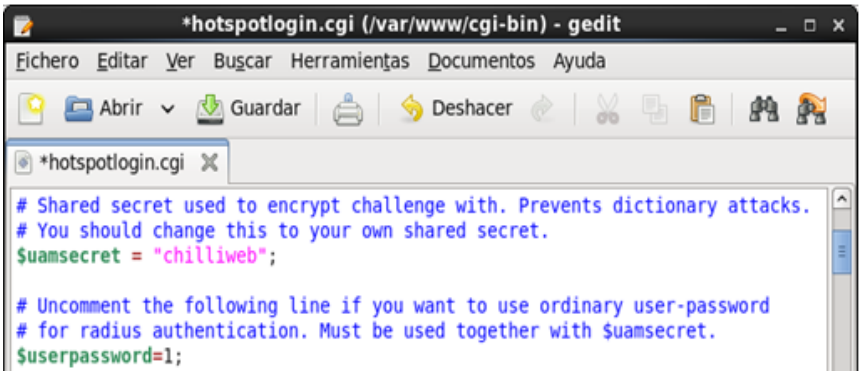


Elaborado por: Jonathan Jara y Diego Mena

11. A continuación, se descomentará líneas **$uamsecret**, y **$userpassword** borrando el numeral **(#)** al inicio de cada una de ellas, y se establecerá en **$uamsecret** el mismo password asignado en el aportado **uamsecret** del archivo de configuración **chilli.conf** y en **$userpassword** cambiamos el valor de 0 por 1, quedando de la siguiente manera:

$uamsecret = "chilliweb"; $userpassword= 1;

Figura 85. Encriptación de Contraseñas del Portal Cautivo



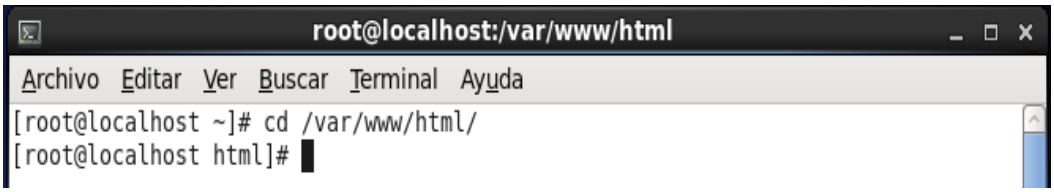
Elaborado por: Jonathan Jara y Diego Mena

12. Si se decide configurar una página web inicial en el apartado **uamhomepage** visto anteriormente, la misma se creará dentro de directorio **/var/www/html,** en cualquier lenguaje web en este caso se utilizará **HTML,** todo el proceso mencionado se realizará mediante las siguientes línea de comandos:

cd /var/www/html/

gedit index.html

Figura 86. Creación de Página Web Inicial

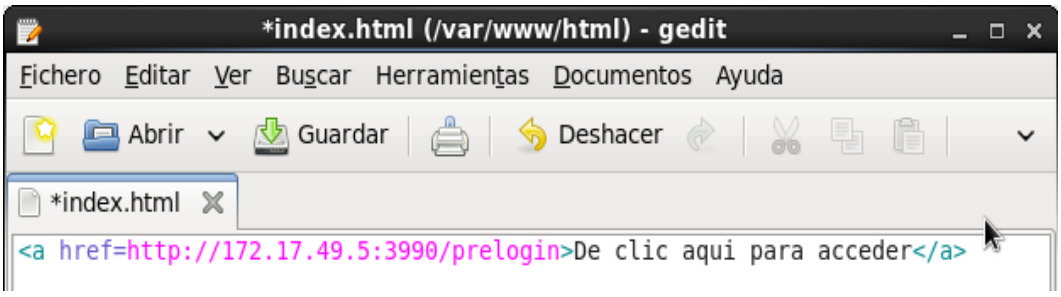


Elaborado por: Jonathan Jara y Diego Mena

13. Y se diseñará una página web informativa inicial, el diseño dependerá de cada administrador del portal cautivo y el fin que tenga el mismo, adicionalmente se ubicará un hipervínculo el cual redireccionará al portal de Chillispot, mediante código que se muestra en la Figura 3.60, la IP variará dependiendo el direccionamiento que se haya establecido en el archivo **chilli.conf.**

De click aquí para acceder

Figura 87. Código Fuente de Pagina Web Inicial

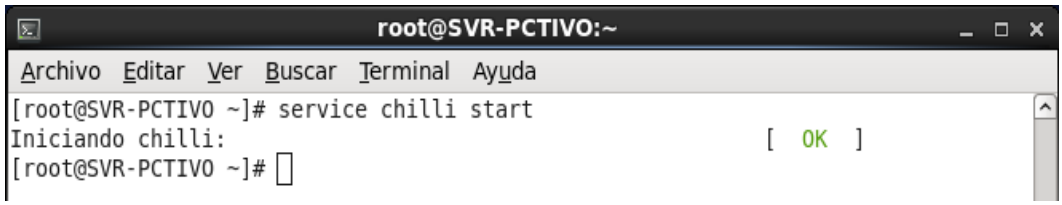


Elaborado por: Jonathan Jara y Diego Mena

14. Finalmente, se levantará el servicio de Chillispot para verificar que todo haya sido configurado correctamente, mediante la siguiente línea de comando:

service chilli start

Figura 88. Inicialización del Servicio Chillispot



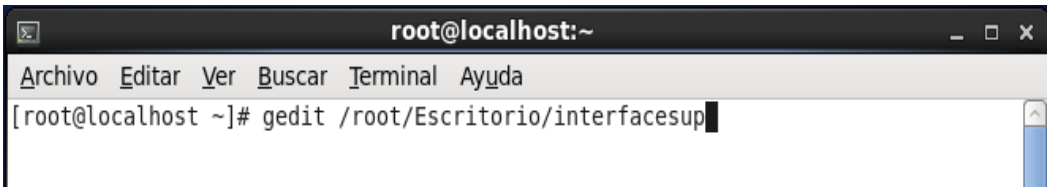
Elaborado por: Jonathan Jara y Diego Mena

3.3.7. Auto Inicialización de Interfaces de Red

Adicionalmente a las instalaciones y configuraciones de los componentes que conforman el portal cautivo, es necesario inicializar las interfaces de red, debido a que el sistema Centos no las levantan de manera automáticamente cada vez que se enciende o se reinicia el mismo, motivo por el que se creará un script que las inicialice de manera automática evitando que se tenga que levantar manualmente cada vez que inicie el servidor.

1. Se creará un script, que en este caso denominado **interfacesup**, donde se utilizará el comando **ifup,** el cual enciende las interfaces físicas las mismas se encuentran apagadas, mediante la siguiente línea de comando:
   gedit /root/Escritorio/interfacesup

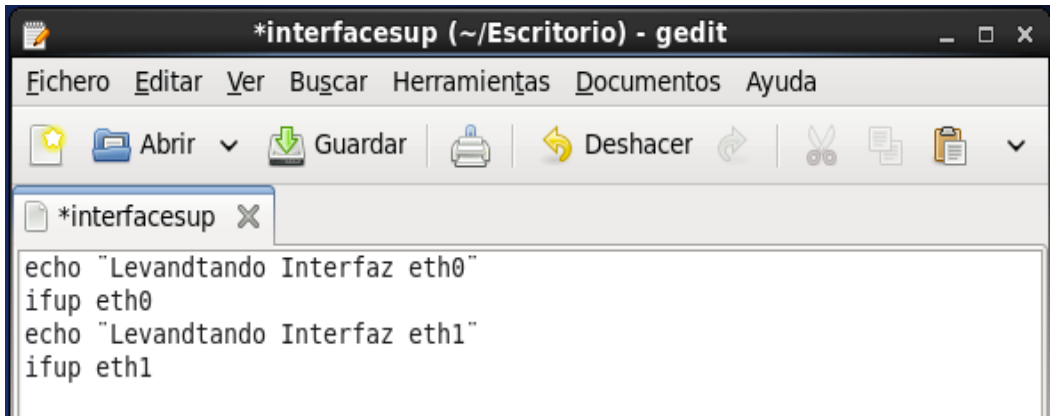
   Figura 89. Creación de Script de Auto levantamiento las Interfaces de Red



   Elaborado por: Jonathan Jara y Diego Mena

2. El código implementado para el funcionamiento del script se muestra en la Figura 3.87 y será el siguiente:
   echo "Levantando Interfaz eth0"
   ifup eth0
   echo "Levantando Interfaz eth1"
   ifup eth1

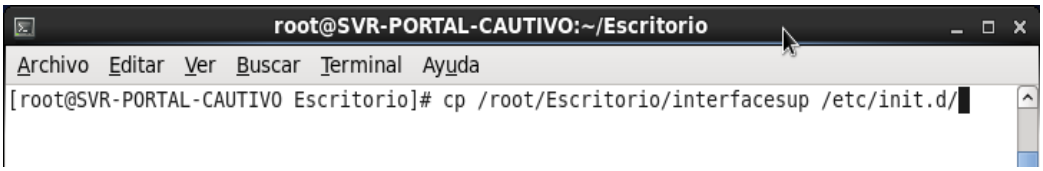
Figura 90. Código del Script para Levantar las Interfaces de Red



Elaborado por: Jonathan Jara y Diego Mena

3. Después, se copiará el script en el directorio **/etc/init.d,** se encuentran todos los archivos de inicialización del sistema, mediante la siguiente línea de comandos:
cp /root/Escritorio/interfacesup /etc/init.d

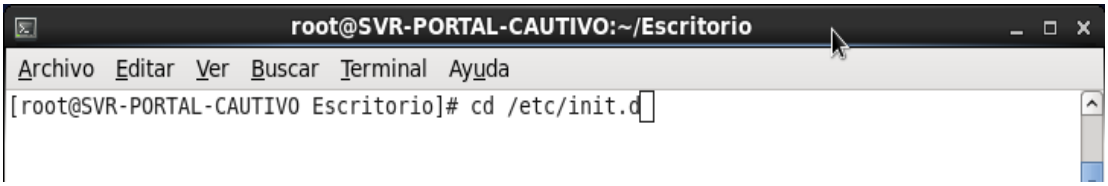
Figura 91. Copiado del Script en el Directorio init.d



Elaborado por: Jonathan Jara y Diego Mena

4. A continuación, se ingresará al directorio **/etc/init.d/** donde se copió el script anteriormente, mediante la siguiente línea de comandos:
cd /etc/init.d

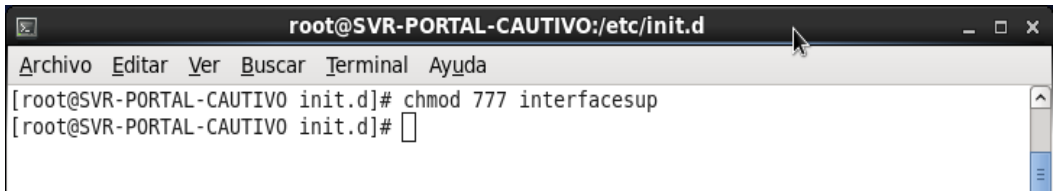
Figura 92. Ingreso al Directorio init.d



Elaborado por: Jonathan Jara y Diego Mena

5. Una vez dentro del directorio, se dará los permisos necesarios para la ejecución del script de **interfacesup,** mediante la siguiente línea de comandos:

Figura 93. Asignación de Permisos al Script



Elaborado por: Jonathan Jara y Diego Mena

6. Seguido, se creará un enlace simbólico en los runlevels **2, 3, 4, 5,** mismo proceso realizado con el script de firewall de Chillispot, en este caso para que se ejecute el script **interfacesup** cada vez que se reinicie o inicie el servidor del portal cautivo, mediante las siguiente líneas de comandos:

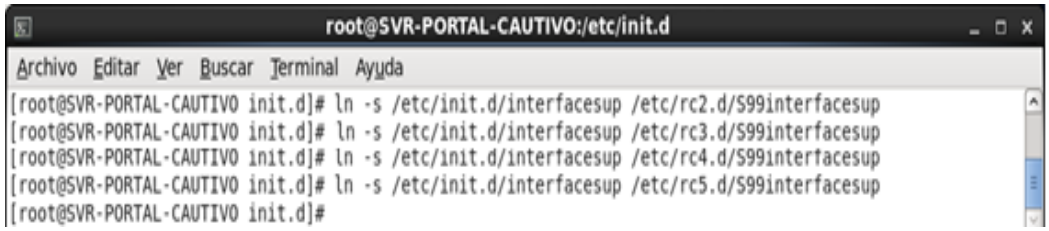
   ln -s /etc/init.d/interfacesup /etc/rc2.d/S99interfacesup

   ln -s /etc/init.d/interfacesup /etc/rc3.d/S99interfacesup

   ln -s /etc/init.d/interfacesup /etc/rc4.d/S99interfacesup

   ln -s /etc/init.d/interfacesup /etc/rc5.d/S99interfacesup

Figura 94. Creación de Enlaces Símbolos Script Interfaces



Elaborado por: Jonathan Jara y Diego Mena

3.5. Gestores de Administración

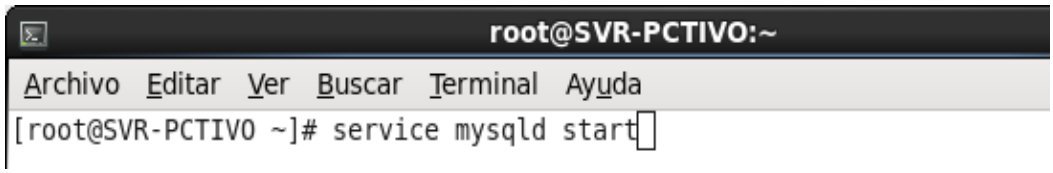
Para facilitar la administración y el manejo del portal cautivo se instalarán 2 gestores de administración con interfaz gráfica, de donde podrá controlar todas actividades generadas por el protocolo radius y el portal cautivo.

3.4.1. Instalación de PHPMYADMIN

1. Primero, se iniciará el servicio mysqld instalado ya anteriormente, mediante el siguiente línea de comandos:

   service mysqld start

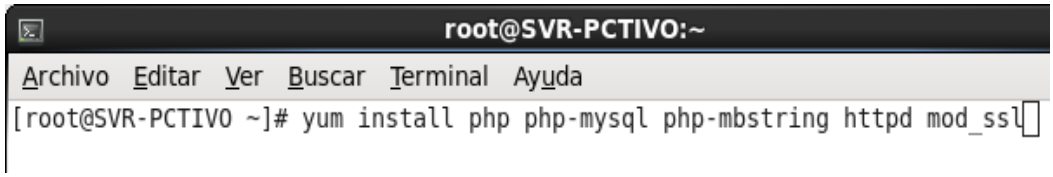
Figura 95. Inicialización de Servicio de MySQL



Elaborado por: Jonathan Jara y Diego Mena

2. A continuación, se bajará todas las dependencias necesarias para que phpmyadmin trabaje correctamente, mediante la siguiente línea de comandos:
   yum install php php-mysql php-mbstring httpd mod_ssl

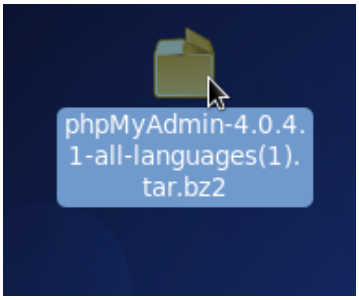
Figura 96. Instalación de las dependencias de PHPMYADMIN



Elaborado por: Jonathan Jara y Diego Mena

3. Después, se descargará el instalador .tar.bz2 de **PHPMYADMIN** en su última versión de la página web oficial.

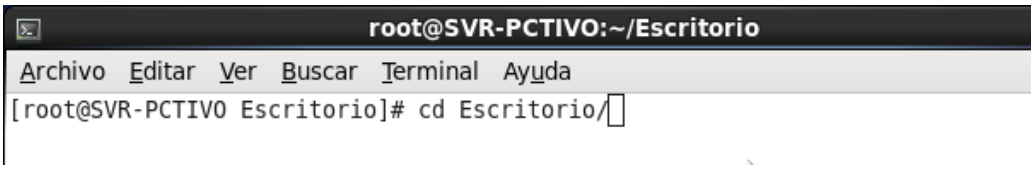
Figura 97. Instalador PHPMYADMIN .tar.bz2



Elaborado por: Jonathan Jara y Diego Mena

4. Seguido, se ingresará al directorio donde se descargo el instalador de **PHPMYADMIN,** el mismo puede variar dependiendo donde se haya descargado el instalador en este caso es el **/Escritorio**, mediante la siguiente línea de comandos:
   cd Escritorio/

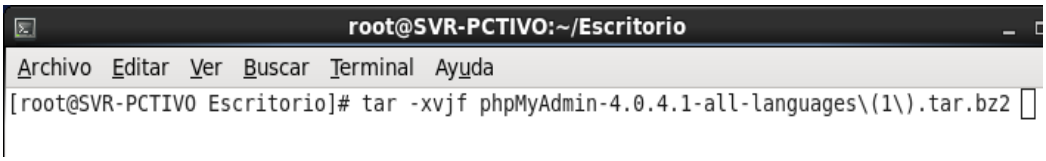
Figura 98. Directorio donde se descargó PHPMYADMIN



Elaborado por: Jonathan Jara y Diego Mena

5. Ahora se, descomprimirá el instalador de **PHPMYADMIN,** mediante la siguiente línea de comandos:
   tar –xvjf phpMyAdmin-4.0.4.1-all-languages\(1\).tar.bz2

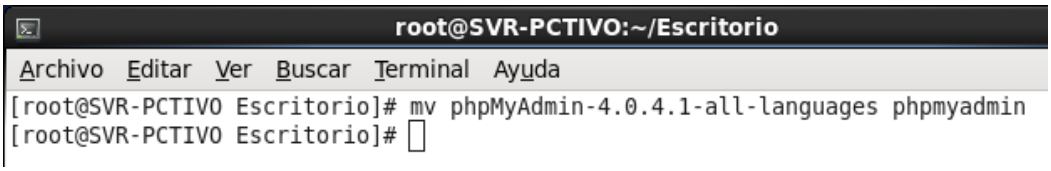
Figura 99. Descomprimir el instalador de PHPMYADMIN



Elaborado por: Jonathan Jara y Diego Mena

6. Se cambiará el nombre de la carpeta descomprimida anteriormente a **phpmyadmin,** mediante la siguiente línea de comandos:
   mv phpMyAdmin-4.0.4.1-all-languages phpmyadmin

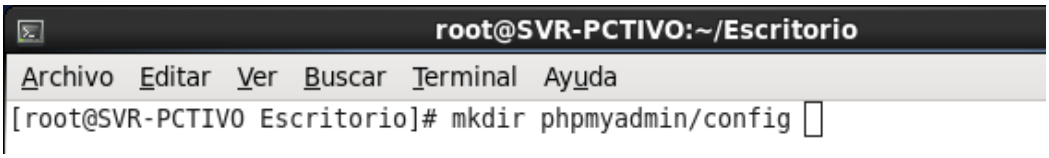
Figura 100. Mover el instalador a la carpeta phpmyadmin



Elaborado por: Jonathan Jara y Diego Mena

7. Después, se creará una carpeta llamada /**config** dentro de la carpeta **phpmyadmin** mediante la siguiente línea de comandos:
   mkdir phpmyadmin/config

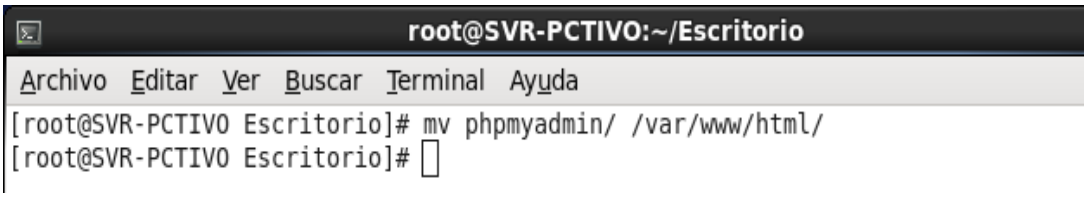
Figura 101. Creación del directorio /config dentro del directorio phpmyadmin



Elaborado por: Jonathan Jara y Diego Mena

8. Seguido, se moverá la carpeta phpmyadmin al directorio **/var/www/html**, que es el directorio principal o raíz Apache, mediante la siguiente línea de comandos:
mv phpmyadmin/ /var/www/html/

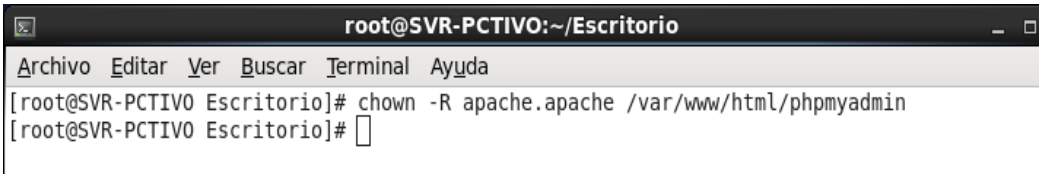
Figura 102. Mover la carpeta phpmyadmin al directorio del servidor Web



Elaborado por: Jonathan Jara y Diego Mena

9. A continuación, se asignará los permisos de propietario Apache al directorio **/var/www/html/phpmyadmin** y los archivos dentro del mismo, dentro del usuario root, mediante la siguiente línea de comandos:
chown -R apache.apache /var/www/html/phpmyadmin

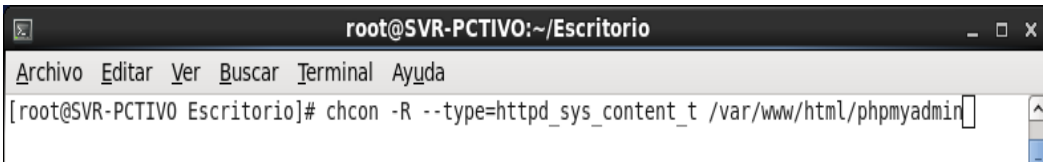
Figura 103. Asignación de permisos de propietario a directorio phpmyadmin



Elaborado por: Jonathan Jara y Diego Mena

10. Se permitirá la ejecución de **phpmyadmin** para que funcione con el servicio httpd, mediante la siguiente línea de comandos:
chcon -R --type=httpd_sys_content_t /var/www/html/phpmyadmin

Figura 104. Asignación de permisos de ejecución con el servicio httpd



Elaborado por: Jonathan Jara y Diego Mena

11. Después, se deberá editar el archivo de configuración **httpd.conf** para permitir la ejecución de **phpmyadmin,** mediante la siguiente línea de comandos:
gedit /etc/httpd/conf/httpd.conf

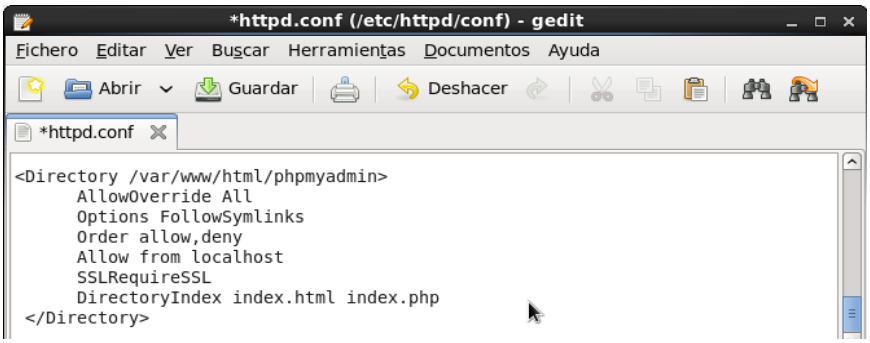
Figura 105. Edición de archivo de configuración httpd.conf

Elaborado por: Jonathan Jara y Diego Mena

12. Seguidamente, se ingresará las siguientes lineas de comandos para permitir el correcto funcionamiento entre phpmyadmin y el navegador web.

<Directory /var/www/html/phpmyadmin>
AllowOverride All
Options FollowSymlinks
Order allow,deny
Allow from localhost
SSLRequireSSL
DirectoryIndex index.html index.php
</Directory>

Figura 106. Parámetros de modificación en archivo httpd.conf

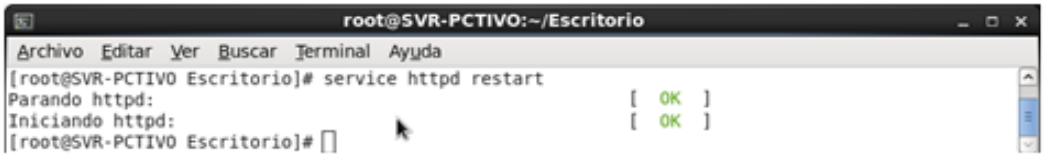


Elaborado por: Jonathan Jara y Diego Mena

13. A continuación, se reiniciará los servicios httpd y mysqld, mediante las siguientes líneas de comandos:

service httpd restart

Figura 107. Reinició del servicio httpd



Elaborado por: Jonathan Jara y Diego Mena

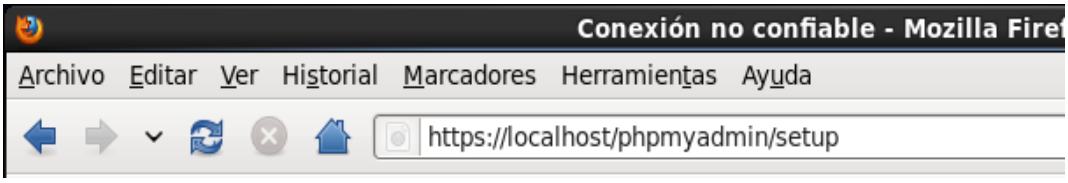
service mysqld restart

Figura 108. Reinició del servicio de myslqd

Elaborado por: Jonathan Jara y Diego Mena

14. Después, se deberá ingresar a un navegador web y se ingresará la siguiente url: **https://localhost/phpmyadmin/setup,** para comenzar la configuración de phpmyadmin.

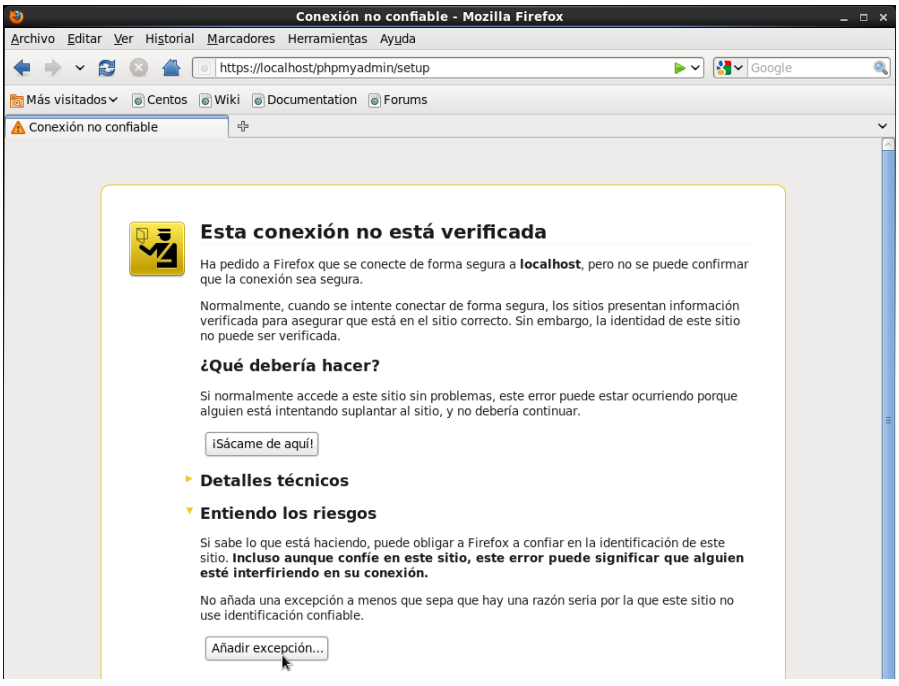
Figura 109. Dirección de configuración de PHPMYADMN



Elaborado por: Jonathan Jara y Diego Mena

15. Puesto que phpmyadmin utiliza **https o puerto de conexión segura** se necesitará dar **Añadir excepción** para poder acceder a la página de administración del mismo.

Figura 110. Página de Verificación de Conexión no Segura



Elaborado por: Jonathan Jara y Diego Mena

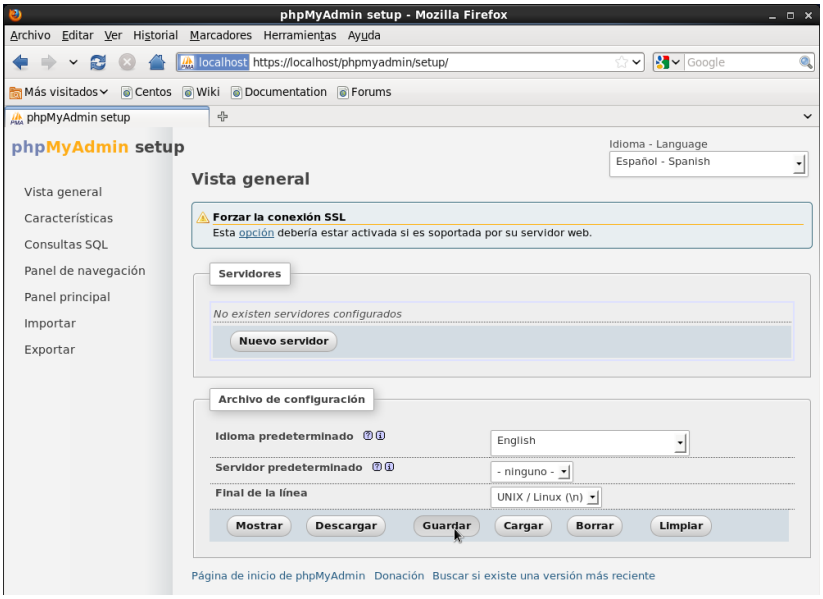
16. A continuación, se presentará una ventana de confirmación, a la cual se le dará clic en **Confirmar excepción de seguridad** para continuar.

Figura 111. Ventana de confirmación de Excepción de Seguridad

Elaborado por: Jonathan Jara y Diego Mena

17. Si las configuraciones anteriores se realizaron correctamente aparecerá la Figura 3.109, caso contrario se revisará los pasos anteriores en busca de alguna falencia. Se dará clic en **Guardar** para crear el archivo **config.inc.php**, el cual se creará en la dirección **var/www/html/phpmyadmin/config.**

Figura 112. Pantalla Inicial de Configuración de PHPMYADMIN



Elaborado por: Jonathan Jara y Diego Mena

18. Nuevamente, se ingresará al directorio de **phpmyadmin** ubicado en el directorio raíz o principal de Apache, mediante la siguiente línea de comandos:

cd /var/www/html/

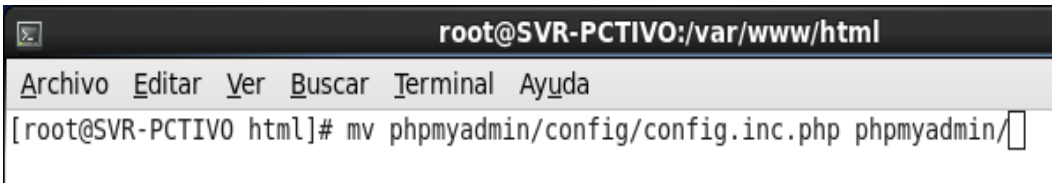
Figura 113. Directorio Principal o Raíz de APACHE

Elaborado por: Jonathan Jara y Diego Mena

19. Luego, se moverá de directorio, el archivo **config.inc.php** que se encuentra en la dirección **/var/www/html/phpmyadmin/config/** solamente la dirección **/var/www/html/phpmyadmin,** mediante la siguiente línea de comandos:

mv phpmyadmin/config/config.inc.php phpmyadmin/

Figura 114. Mover archivo config.inc.php de directorio

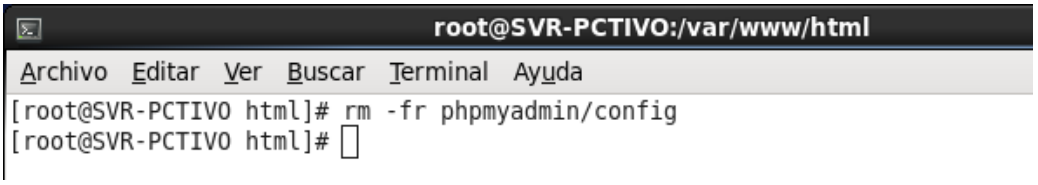


Elaborado por: Jonathan Jara y Diego Mena

20. Después, se eliminará la carpeta **/config,** porque solo será necesaria para generar el archivo **config.inc.php**, esto proceso se lo realizará mediante la siguiente línea de comandos:

rm -fr phpmyadmin/config

Figura 115. Eliminar directorio /config de phpmyadmin



Elaborado por: Jonathan Jara y Diego Mena

21. Seguido, se deberá abrir el archivo **config.inc.php,** para proceder a modificarlo, mediante la siguiente línea de comandos:

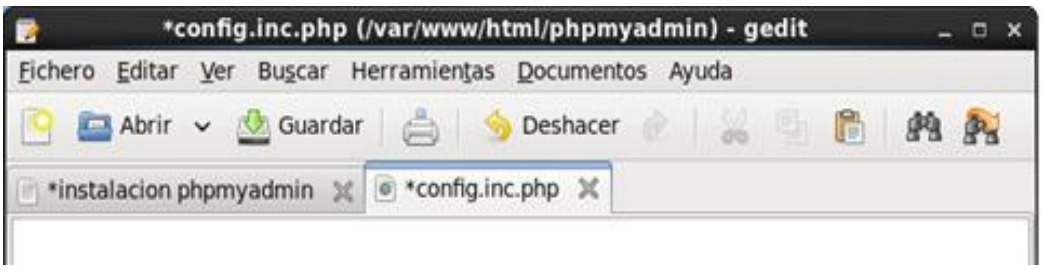
gedit /var/www/html/phpmyadmin/config.inc.php

Figura 116. Edición del archivo config.inc.php

Elaborado por: Jonathan Jara y Diego Mena

22. A continuación, se eliminará la información que el mismo contenga, quedando como se muestra en el Figura 117, vacío.

Figura 117. Archivo config.inc.php vacio

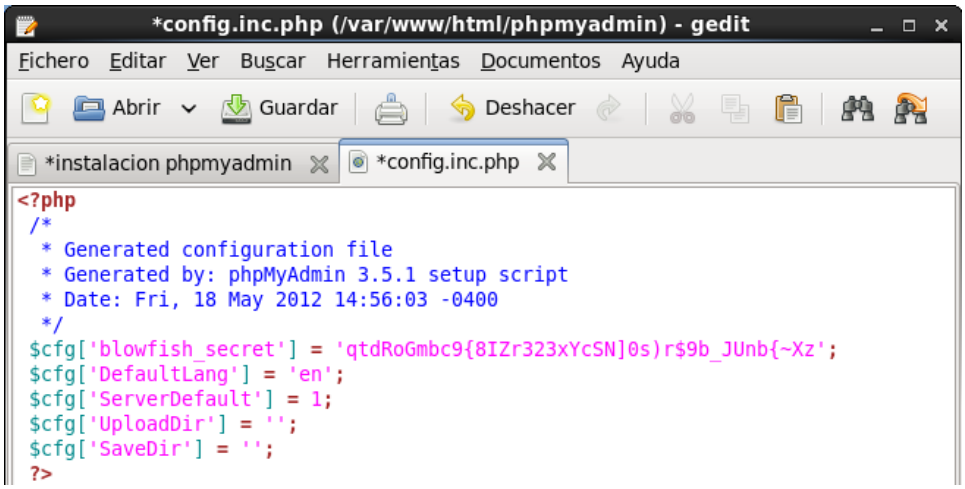


Elaborado por: Jonathan Jara y Diego Mena

23. Después, se agregará el siguiente código al archivo **config.inc.php** de manera que de muestre como la Figura 3.114, y se guardaran todos los cambios efectuados

```
<?php
 /*
  * Generated configuration file
  * Generated by: phpMyAdmin 3.5.1 setup script
  * Date: Fri, 18 May 2012 14:56:03 -0400
  */
 $cfg['blowfish_secret'] =
'qtdRoGmbc9{8IZr323xYcSN]0s)r$9b_JUnb{~Xz';
 $cfg['DefaultLang'] = 'en';
 $cfg['ServerDefault'] = 1;
 $cfg['UploadDir'] = '';
 $cfg['SaveDir'] = '';
 ?>
```

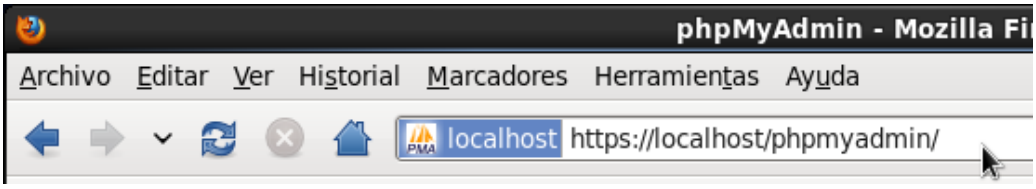
Figura 118. Configuración de archivo config.inc.php



Elaborado por: Jonathan Jara y Diego Mena

24. A continuación, se abrirá un navegador web y se ingresará la siguiente url: **https://localhost/phpmyadmin,** para acceder finalmente a phpmyadmin

Figura 119. Url de acceso a pagina inicial de PHPMYADMIN



Elaborado por: Jonathan Jara y Diego Mena

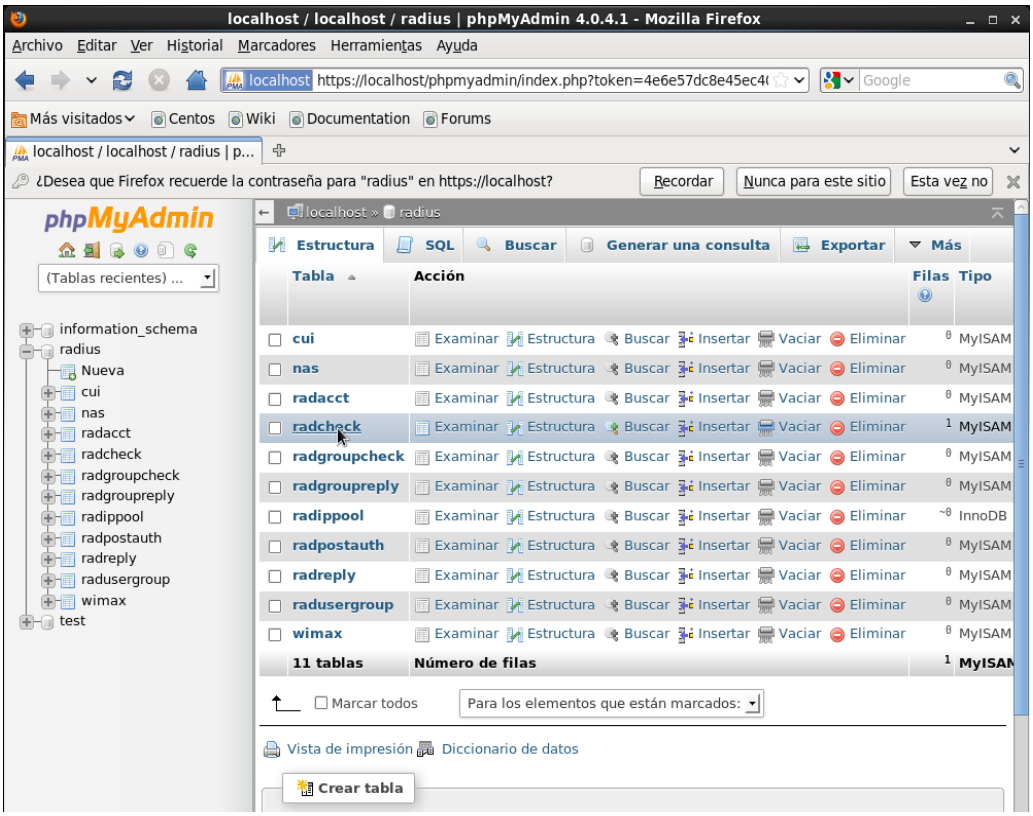
25. En el inicio de sesión, se ingresará el nombre de la base que se desea consultar en este caso será **radius** y la contraseña que será la que se haya configurado la base anteriormente mencionada.

Figura 120. Ingreso de Credenciales de acceso a PHPMYADMIN

Elaborado por: Jonathan Jara y Diego Mena

26. Finalmente, se podrán visualizar todas las tablas que contienen la base de datos **radius** de forma gráfica, facilitando de gran forma la gestión de la misma al administrador del portal cautivo.

Figura 121. Interfaz de administración gráfica de PHPMYADMIN



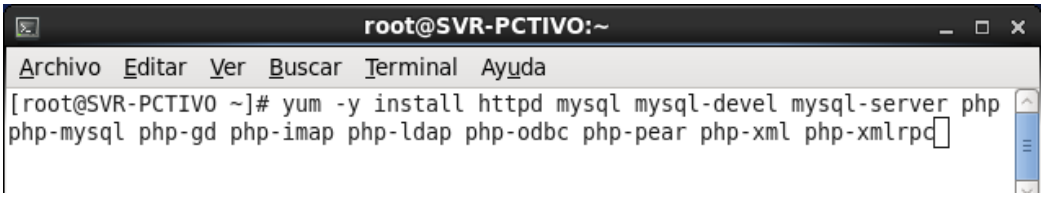
Elaborado por: Jonathan Jara y Diego Mena

3.4.2. Instalación de DALORADIUS

1. Se instalará las dependencias y librerías necesarias para iniciar la instalación de Daloradius, mediante la siguiente línea de comandos:

yum -y install httpd mysql mysql-devel mysql-server php php-mysql php-gd php-imap php-ldap php-odbc php-pear php-xml php-xmlrpc

Figura 122. Instalación de dependencias y librerías para Daloradius

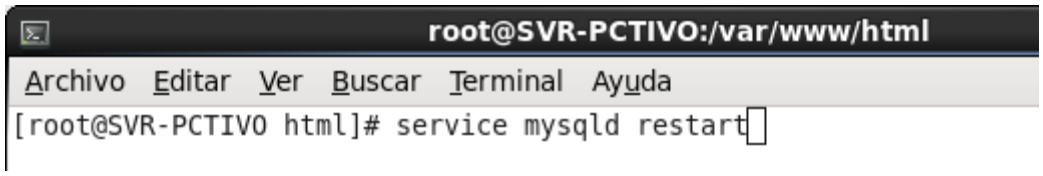


Elaborado por: Jonathan Jara y Diego Mena

2. Después, se reiniciará el servicio de Mysql, mediante la siguiente línea de comandos:

   service mysqld restart

   Figura 123. Reinicio del servicio de Mysql



   Elaborado por: Jonathan Jara y Diego Mena

3. Seguido, se descargar el instalador de Daloradius en versión 0.9.9, mediante la siguiente línea de comandos:

   wget

   http://nchc.dl.sourceforge.net/project/daloradius/daloradius/daloradius-0.9-9/daloradius-0.9-9.tar.gz

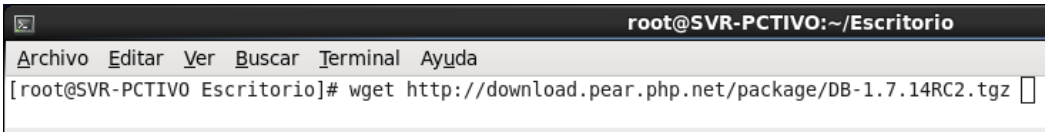
   Figura 124. Descarga del instalador de Daloradius

   Elaborado por: Jonathan Jara y Diego Mena

4. Adicionalmente, se descargará la dependencia **PEAR** para el correcto funcionamiento de Daloradius en el navegador mediante el comando:

   wget http://download.pear.php.net/package/DB-1.7.14RC2.tgz

   Figura 125. Descarga del instalador de dependencia PEAR

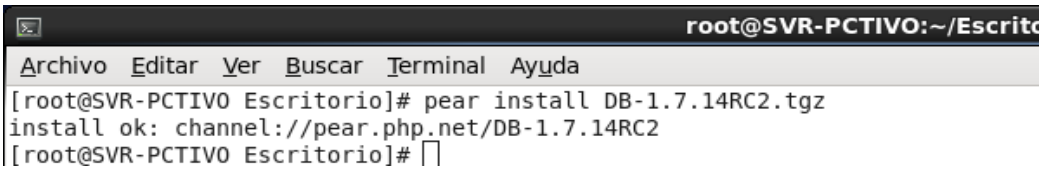


   Elaborado por: Jonathan Jara y Diego Mena

5. Después, se instalará la dependencia **PEAR** descargada anteriormente, mediante la siguiente línea de comandos:

   pear install DB-1.7.14RC2.tgz

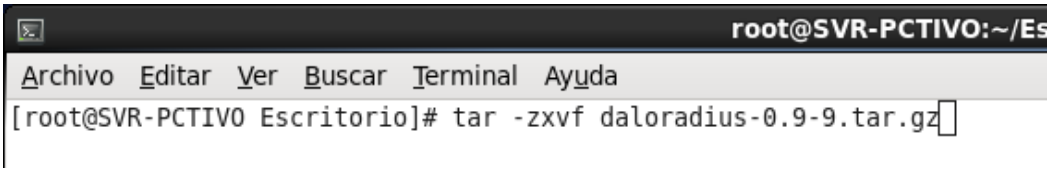
Figura 126. Instalación de dependencia PEAR



Elaborado por: Jonathan Jara y Diego Mena

6. Una vez finalizado el proceso anterior, se descomprimirá el paquete de instalación de Daloradius, mediante la siguiente línea de comandos:
   tar -zxvf daloradius-0.9-9.tar.gz

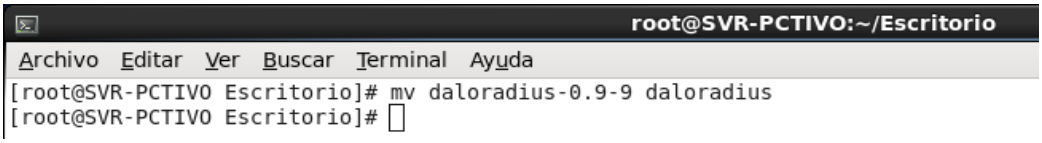
Figura 127. Descompresión del instalador de Daloradius



Elaborado por: Jonathan Jara y Diego Mena

7. A continuación, se cambiará el nombre de la carpeta descomprimida a solo **daloradius,** mediante la siguiente línea de comandos:
   mv daloradius-0.9-9 daloradius

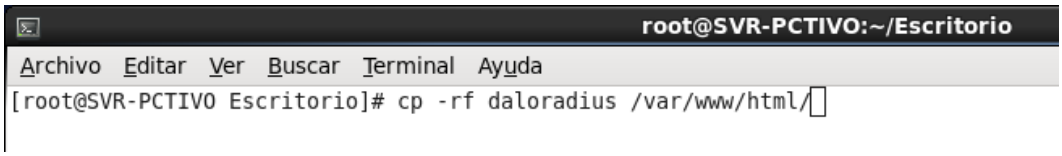
Figura 128. Cambiar el nombre del archivo descomprimida



Elaborado por: Jonathan Jara y Diego Mena

8. Después, se copiará la carpeta **daloradius** a la dirección **/var/www/html,** mediante la siguiente línea de comandos:
   cp -rf daloradius /var/www/html/

Figura 129. Copiar daloradius al directorio del servidor APACHE

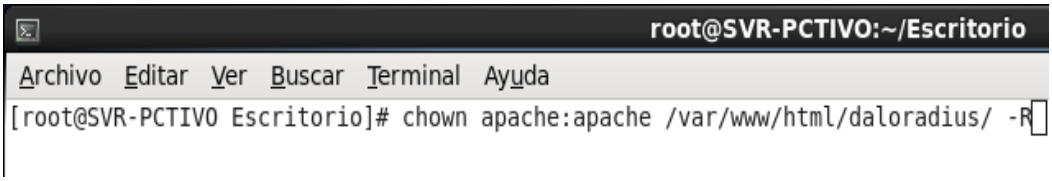


Elaborado por: Jonathan Jara y Diego Mena

9. Seguido, se asignará los permisos de propietario Apache al directorio **/var/www/html/daloradius** y los archivos dentro del mismo, dentro del usuario root, mediante la siguiente línea comandos:

chown -R apache:apache /var/www/html/daloradius/

Figura 130. Asignación de permisos de propietario a directorio daloradius

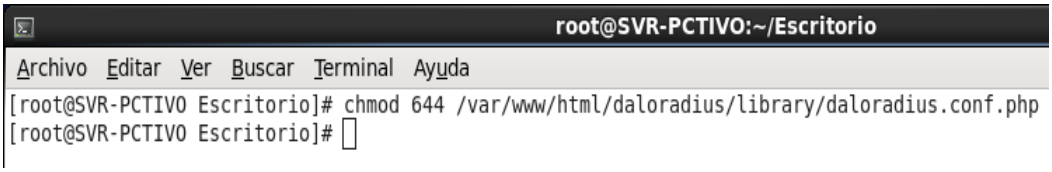


Elaborado por: Jonathan Jara y Diego Mena

10. A continuación, se asignaran los permisos respectivos para el funcionamiento al archivo **daloradios.conf.php,** mediante la siguiente línea comandos:

chmod 644 /var/www/html/daloradius/library/daloradius.conf.php

Figura 131. Asignación de permisos de ejecución, lectura y escritura

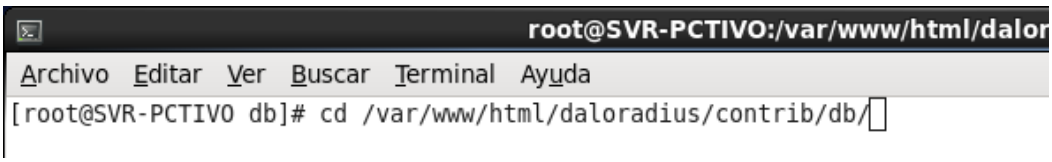


Elaborado por: Jonathan Jara y Diego Mena

11. Luego, se deberá ingresar al directorio **/var/www/html//daloradius/contrib/db/,** mediante la siguiente línea de comandos

cd /var/www/html/daloradius/contrib/db/

Figura 132. Ingreso al directorio /var/www/html/daloradius/contrib/db/

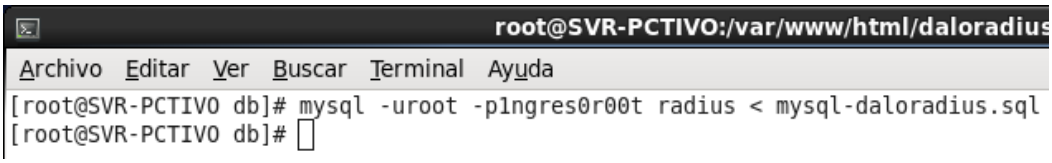


Elaborado por: Jonathan Jara y Diego Mena

12. Seguido, se importará la tabla **daloradius.sql** a la base de datos **radius,** mediante la siguiente línea de comandos:

mysql -uroot -p1ngres0r00t radius < mysql-daloradius.sql

Figura 133. Importación de tabla daloradius.sql a la base de datos radius



Elaborado por: Jonathan Jara y Diego Mena

13. Después, se editará el archivo **daloradius.conf.php,** mediante la siguiente línea de comandos:

gedit /var/www/html/daloradius/library/daloradius.conf.php

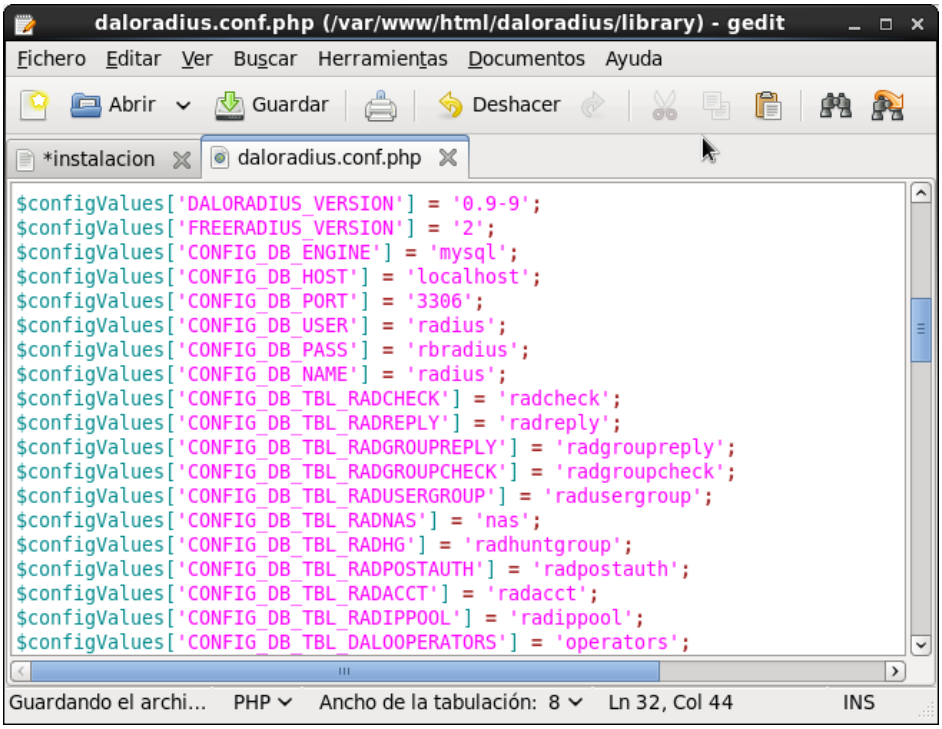
Figura 134. Edición del archivo daloradius.conf.php

Elaborado por: Jonathan Jara y Diego Mena

14. Donde, se modificará los campos **DB_USER** con la base de datos radius y el campo **BD_PASS** con la contraseña que se le asigno a la base de datos radius, quedando el archivo como se muestra en la Figura 3.132, y el código es el siguiente:

```
$configValues['DALORADIUS_VERSION'] = '0.9-9';
$configValues['FREERADIUS_VERSION'] = '2';
$configValues['CONFIG_DB_ENGINE'] = 'mysql';
$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_PORT'] = '3306';
$configValues['CONFIG_DB_USER'] = 'radius';
$configValues['CONFIG_DB_PASS'] = 'rbradius';
$configValues['CONFIG_DB_NAME'] = 'radius';
$configValues['CONFIG_DB_TBL_RADCHECK'] = 'radcheck';
$configValues['CONFIG_DB_TBL_RADREPLY'] = 'radreply';
$configValues['CONFIG_DB_TBL_RADGROUPREPLY'] =
'radgroupreply';
$configValues['CONFIG_DB_TBL_RADGROUPCHECK'] =
'radgroupcheck';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';
$configValues['CONFIG_DB_TBL_RADNAS'] = 'nas';
$configValues['CONFIG_DB_TBL_RADHG'] = 'radhuntgroup';
$configValues['CONFIG_DB_TBL_RADPOSTAUTH'] = 'radpostauth';
$configValues['CONFIG_DB_TBL_RADACCT'] = 'radacct';
$configValues['CONFIG_DB_TBL_RADIPPOOL'] = 'radippool';
```

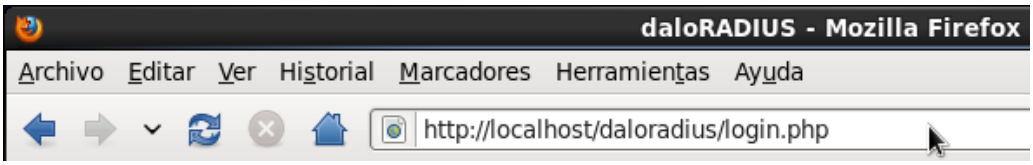
Figura 135. Configuración de archivo daloradius.conf.php



Elaborado por: Jonathan Jara y Diego Mena

15. A continuación, se abrirá un navegador web y se ingresará la siguiente url: **http://localhost/daloradius/login.php,** para acceder a la interfaz web de daloradius

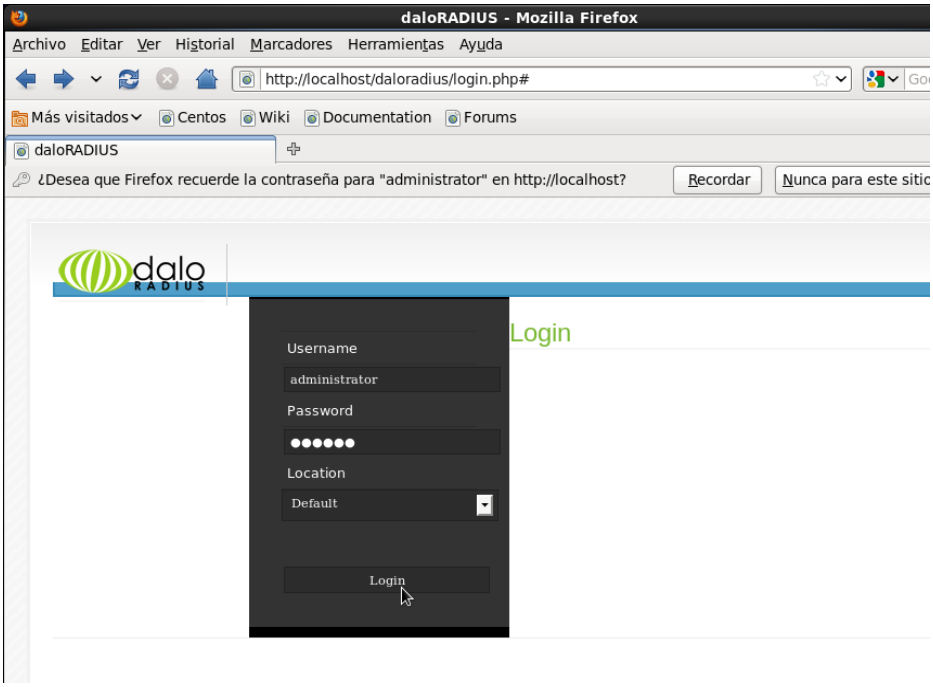
Figura 136. Url de acceso a interfaz de Daloradius



Elaborado por: Jonathan Jara y Diego Mena

16. Para ingresar a Daloradius, se utilizará las siguientes credenciales, usuario **administrator** y la contraseña **radius** que en este caso es la base de datos utilizada por el radius para su funcionamiento.

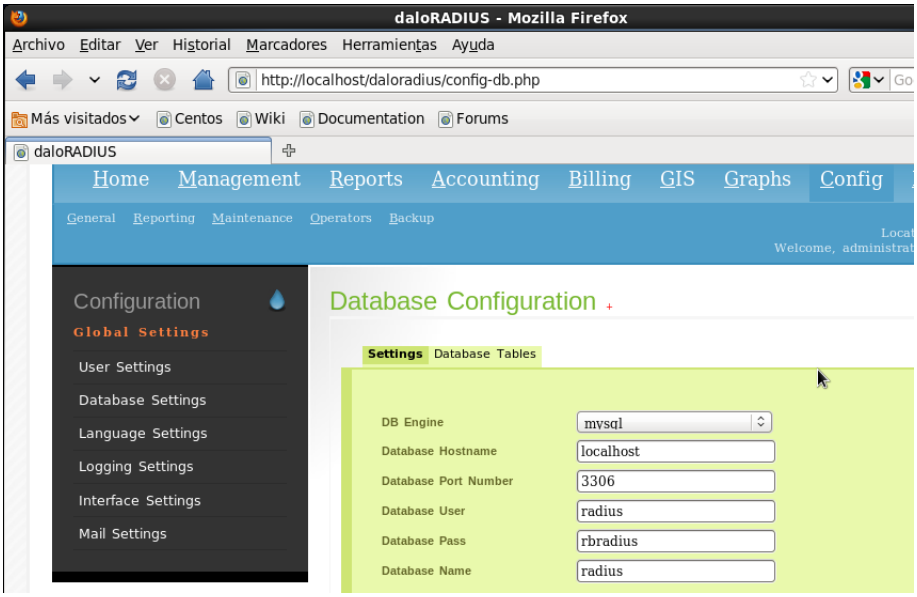
Figura 137. Interfaz de inicio de sesión de DALORADIUS



Elaborado por: Jonathan Jara y Diego Mena

17. Finalmente, se verificará que se utilice la base de datos **radius,** y posteriormente ya se podrá hacer uso del mismo para administrar el portal cautivo.

Figura 138. Interfaz de administración gráfica de DALORADIUS



Elaborado por: Jonathan Jara y Diego Mena

CAPÍTULO 4
ANÁLISIS DE PRUEBAS Y OBTENCIÓN DE RESULTADOS

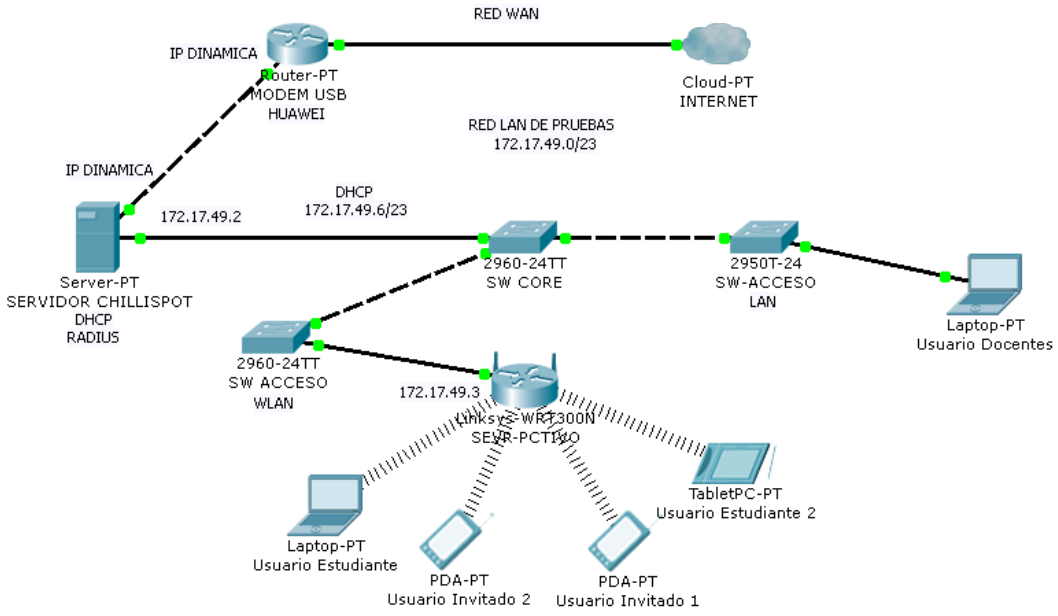
4.1. Escenario de Pruebas

Durante el proceso de desarrollo del portal cautivo es necesario pasar por una etapa de pruebas de funcionamiento con el fin de comprobar su desempeño y detectar todos los posibles errores generados, pudiendo tomar las medidas correctivas a los mismos, para esto se será necesario crear un escenario o red de pruebas para poner en ejecución el portal cautivo y ver su comportamiento en cuanto a seguridad se refiere.

4.2. Propuesta de Red para Escenario de Pruebas

Con el fin de poner en desarrollo el funcionamiento del portal cautivo, se ha propuesto una red para la realización de pruebas de desempeño y funcionamiento del mismo, antes de su ejecución final.

Figura 139. Topología de Red de pruebas



Elaborado por: Jonathan Jara y Diego Mena

El esquema de la red de pruebas implementará un servidor principal el cual contiene alojado al portal cautivo y adicionalmente permite dividir en 2 segmentos de red:

- **Segmento WAN:**

El segmento WAN que en este caso será la conexión con el proveedor de internet.

- **Segmento LAN:**

Para el segmento LAN se utiliza un modem movistar de marca **HUAWEI E367 HSPA+**, el cual está conectado a una laptop de marca Gateway nv57h con sistema operativo Windows 7, la misma que compartirá el servicio de internet al servidor Chillispot mediante un cable UTP categoría 5e. El servidor Chillispot trabaja con 2 tarjetas de red asignadas de la siguiente manera:

Eth0: Se asignó a la tarjeta de red propia de la Mainboard del servidor, y cuya función es recibir el servicio de internet hacia el portal cautivo.

Eth1: Se asignó una tarjeta de red PCI incorporada al servidor de marca TRENDNET, cuya función es interconectar el servidor principal con el Switch de Core de la red para proveer el servicio de Chillispot o el portal cautivo a todo el segmento LAN de la red de pruebas.

Al Switch de Core se conectan 2 Switch de Acceso, uno para simular una red WLAN de pruebas y otro para simular una red LAN cableada, cabe mencionar que todas las conexiones entre dispositivos se realiza mediante cables UTP categoría 5e.

Al Switch de Acceso de la red WLAN, se conecta un Router inalámbrico de marca **LINSYS CISCO WRT320N,** cuya función es dar el servicio de red inalámbrica a los usuarios finales de la red WLAN de pruebas, y es importante mencionar que la su conexión debe de ser únicamente en los puertos LAN del Router.

4.3. Requerimientos de la Red

4.3.1. Requerimientos Físicos

A continuación se realiza una descripción de todos los componentes físicos utilizados en el diseño de la red de pruebas propuesta:

- **Servidor:** Computador de Escritorio

Este equipo se utilizará para la instalación y configuración del servidor del portal cautivo y de todos sus componentes.

Tabla 8. Características de Servidor Principal

CARACTERÍSTCAS	
PROCESADOR	Core 2 Duo
MAINBOARD	Intel Desktop Board DH55HC
DISCO DURO	80GB
MEMORIA RAM	2GB
INTERFACES DE RED	1 Interfaz Fast Ethernet 1 Interfaz Giga Ethernet

Elaborado por: Jonathan Jara y Diego Mena

- **Router Inalámbrico:** Linksys Cisco

Este dispositivo distribuirá la red de manera inalámbrica a los todos posibles clientes o usuarios que van ser uso del portal cautivo.

Tabla 9. Características de Router Inalámbrico

CARACTERÍSTCAS	
MODELO	WRT320N
ESPECIFICACIONES	LAN: 4 Puertos Ethernet 10Base-T/100Base-TX/1000Base-T WAN: 1 Puerto Ethernet 10Base-T/100Base-TX/1000Base-T
ESTÁNDARES SOPORTADOS	11 Mbps IEEE802.11b 54 Mbps IEEE802.11a 54 Mbps IEEE802.11g 600 Mbps IEEE802.11n
CARACTERISTICAS ESPECIALES	DNS Proxy, Filtros MAC, MAC Address SPI, WPA, WPA2

Elaborado por: Jonathan Jara y Diego Mena

- **Switch:** Nexxt Desktop Switch

Este dispositivo tendrá la función de distribuir la red del portal cautivo mediante cable UTP hacia los dispositivos finales.

Tabla 10. Características de Switch de Distribución

CARACTERÍSTCAS	
MODELO	8 Port 10/100 Desktop Switch
PUERTOS	8 Puertos
TIPOS DE PUERTOS	Fast Ethernet
INTERCONEXIÓN	MDI / MDI-X

Elaborado por: Jonathan Jara y Diego Mena

- **Computadores Personales:** Portátiles o Laptop

Las portátiles serán utilizadas como clientes o usuarios de la red, las mismas que verificarán que el portal este realizando la seguridad de acceso a la red.

Tabla 11. Características de las Portátiles

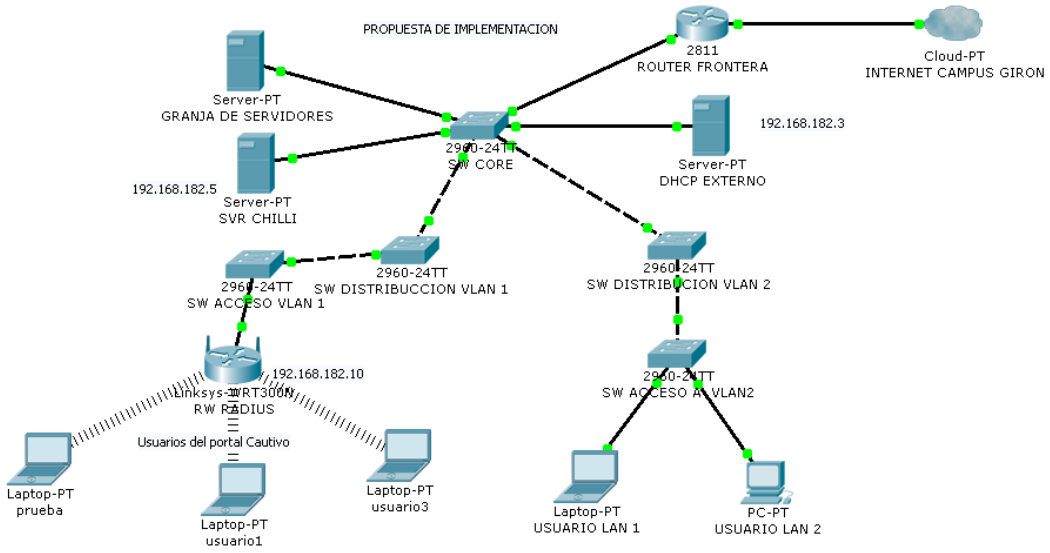
CARACTERÍSTCAS	
MARCA	Gateway
PROCESADOR	Core i3
DISCO DURO	500 GB
MEMORIA RAM	4GB
SISTEMA OPERATIVO	Windows 7 64bits

Elaborado por: Jonathan Jara y Diego Mena

4.3.2. Requerimientos Lógicos

En lo que respecta a la topología lógica de nuestra red de pruebas se utilizara una red de tipo jerárquica. El segmento WAN en la red de pruebas utiliza una IP dinámica ya que el servicio de internet esta dado mediante un modem USB. En lo cuanto a el segmento LAN se opto por simular la red **WLAN-UPS-ESTUDIANTES**, por lo que se utilizo el rango de direcciones IP 172.17.49.0/23.

Figura 140. Topología de red para propuesta de implementación



Elaborado por: Jonathan Jara y Diego Mena

En cuanto al servidor del portal cautivo, este funcionará como frontera entre la red WAN y la red LAN, este utiliza 2 interfaces de red las cuales son designadas como eth0 y eth1. Por la interfaz eth0 se recibe el servicio de internet en este caso se asigna una dirección IP dinámica, pero también funciona con una dirección estática.

La interfaz eth1 es utilizada para conectar al servidor con el segmento LAN de la red de pruebas, esta interfaz utiliza la dirección IP estática 172.17.49.2/23 y un Gateway 172.17.49.5.

Al implementar el servicio de Chillispot, el servidor utiliza adicionalmente una interfaz **TUN-TAP**, la cual es una interfaz lógica que permite simular un dispositivo de capa 3, llamada tun00 la cual efectúa un ruteo de las peticiones hechas por los clientes Chillispot hacia el servidor. La interfaz virtual es llamada tun00, la cual tiene la dirección IP estática: 172.17.49.5/23 y esta funcionará como Gateway de todo el segmento LAN.

El servidor Chillispot entrega el servicio de DHCP a los usuarios finales del segmento LAN por lo que los usuarios tendrán disponibles el pool de direcciones 172.17.49.0/23 iniciando desde la dirección IP 172.17.49.6 en adelante.

En lo que respecta al router WLAN este tiene la dirección IP estática 172.17.49.3, se desactivó la opción de DHCP en el router, puesto que este es generado por el servidor Chillispot hacia los clientes, y se configuró un SSID de nombre **SERV-PCTIVO.**

4.4. Pruebas y Resultados

Las pruebas de funcionamiento del portal cautivo fueron realizadas durante 2 días consecutivos, los cuales fueron el miércoles 10 y jueves 11 de julio del 2013, y se realizaron en 2 escenarios diferentes para observar el comportamiento del portal en diferentes condiciones. El día miércoles 10 se realizaron las pruebas en la biblioteca a partir de las 10:00 de la mañana y finalizaron a las 13:00. El día jueves 11 las pruebas fueron efectuadas en la cafetería a partir de las 10:00 de la mañana hasta la 13.00, cabe indicar que en los 2 días de prueba, el servidor estuvo activo durante 3 horas sin interrupción alguna.

El análisis realizado partió de los datos obtenidos después de realizar las pruebas y a través de todos los registros proporcionados por el software **DALORADIUS**.

A continuación en la Figura 141 se muestran los registros de usuarios creados durante los 2 días de pruebas efectuados, la información que se despliega es la siguiente: Nombre del usuario creado, la fecha de su creación y por quien fue creado.

Figura 141. Registro de usuarios creados en el portal cautivo

1 2

Sección	Item	Fecha de creación	Creado por
userinfo	Prueba	2013-07-11 19:26:47	administrator
userinfo	Victorh	2013-07-11 11:12:55	administrator
userinfo	sebastian	2013-07-11 11:05:04	administrator
userinfo	shabel	2013-07-11 11:04:26	administrator
userinfo	cristhian	2013-07-11 11:03:07	administrator
userinfo	sh@bel	2013-07-11 11:02:09	administrator
userinfo	eddyplus	2013-07-11 10:59:09	administrator
userinfo	juank	2013-07-11 10:55:59	administrator
userinfo	AndreJ	2013-07-11 10:41:53	administrator
userinfo	alejobdp	2013-07-11 10:31:21	administrator
userinfo	michu	2013-07-11 10:31:00	administrator
userinfo	Gabohzh	2013-07-11 10:30:49	administrator
userinfo	Santy	2013-07-11 10:30:29	administrator
userinfo	tefita	2013-07-11 10:30:12	administrator
userinfo	Ottodaisuke	2013-07-10 11:50:33	administrator
userinfo	Alexito	2013-07-10 11:34:08	administrator
userinfo	Antono	2013-07-10 11:09:18	administrator
userinfo	Toño	2013-07-10 11:02:17	administrator
userinfo	victor	2013-07-10 10:58:16	administrator
userinfo	gzambrano	2013-07-10 10:53:24	administrator
userinfo	VSoria	2013-07-10 10:51:35	administrator
userinfo	dfmena	2013-07-10 10:41:55	administrator
userinfo	interops	2013-07-10 10:40:22	administrator

Elaborado por: Jonathan Jara y Diego Mena

- **Prueba 1:** Ingreso de Nuevos Usuarios al Portal Cautivo a través de la interfaz de Daloradius.

Escenario 1: Biblioteca

Figura 142. Prueba de portal cautivo en la Biblioteca

Elaborado por: Jonathan Jara y Diego Mena

Se eligió la biblioteca de la Universidad como primer escenario de pruebas para poner en funcionamiento el portal cautivo, puesto que es un lugar de gran concentración de estudiantes y por ende posibles usuarios. Donde los usuarios pudieron acceder a la red inalámbrica **SERV-PCTIVO** para tener internet de manera gratuita y sin restricciones, tan solo se les solicitó un usuario y una contraseña los cuales se ingresaban a la tabla **RADCHECK** de la base de datos **RADIUS** mediante el gestor Web **DALORADIUS,** para que posteriormente ser utilizados en la autentificación del portal cautivo.

Resultados

En total dentro de este escenario se crearon nueve usuarios, de los cuales en su mayoría utilizaron laptops para conectarse al portal cautivo.

A continuación en la Tabla 12 se muestra todos los usuarios que se conectaron al portal cautivo detallando: el nombre del usuario, la contraseña y la hora en la cual se conectaron al portal.

Tabla 12. Registro de usuarios conectados al portal en Biblioteca

USUARIO	CONTRASEÑA	HORA DE CREACIÓN
interops	1709018954	10:40
dfmena	98y5	10:41
VSoria	1234567	10:51
gzambrano	1721549028	10:53
victor	Vector	10:58
Toño	12345	11:02
Antono	1234	11:09
Alexito	7	11:34
Ottodaisuke	EnolariK123	11:50
TOTAL DE USUARIOS	**9**	

Elaborado por: Jonathan Jara y Diego Mena

Escenario 2: Cafetería

Figura 143. Prueba de portal cautivo en la Cafetería

Elaborado por: Jonathan Jara y Diego Mena

Como segundo escenario de pruebas se escogió la cafetería de la Universidad, ya que también es un lugar de gran afluencia de estudiantes. Donde los usuarios pudieron acceder a la red inalámbrica **SERV-PCTIVO** para tener internet de manera gratuita y sin restricciones, tan solo se les solicitó un usuario y una contraseña los cuales se ingresaban a la tabla **RADCHECK** de la base de datos **RADIUS** mediante el gestor

Web **DALORADIUS,** para que posteriormente ser utilizados en la autentificación del portal cautivo.

Resultados

En total dentro de este escenario se crearon 14 usuarios, de los cuales en su mayoría se conectaron a través de tablets y teléfonos inteligentes.

A continuación en la Tabla 13 se muestra todos los usuarios que se conectaron al portal cautivo detallando: el nombre del usuario, la contraseña y la hora en la cual se conectaron al portal.

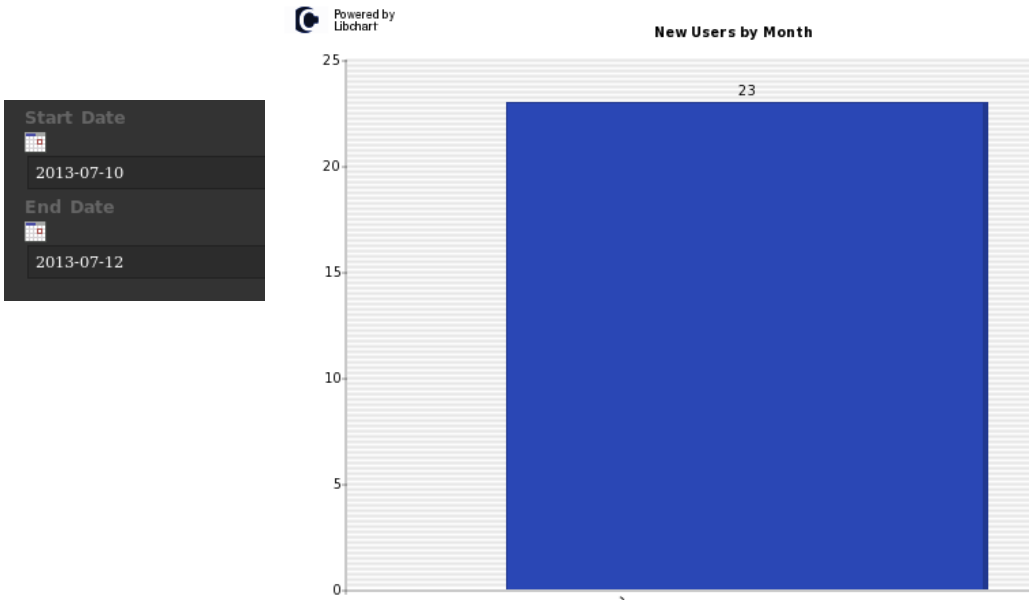
Tabla 13. Registro de usuarios conectados al portal en Cafetería

USUARIO	CONTRASEÑA	HORA DE CREACIÓN
tefita	020392	10:30
Santy	172266	10:30
Gabohzh	17221907	10:30
michu	Michu	10:31
alejobdp	630337	10:31
Andrej	p123	10:41
juank	shonc2	10:55
eddyplus	191180	10:59
sh@bel	Apanipitapa	11:02
cristhian	1601	11:03
shabel	apanipitapa	11:04
sebastian	1993	11:05
Victorh	VICTHORpina25	11:12
Prueba	prb123	19:26
TOTAL DE USUARIOS	**14**	

Elaborado por: Jonathan Jara y Diego Mena

En 2 días de pruebas se han creado un total de 23 nuevos usuarios, los cuales se han registrado en la base de datos **radius** del servidor de Chillispot, y toda esta información puede ser vista de forma grafica utilizando las herramientas de administración del gestor Web **DALORADIUS.**

Figura 144. Gráfica del total de usuarios que se conectaron al portal



Elaborado por: Jonathan Jara y Diego Mena

- **Prueba 2:** Flujo de datos y tiempo de conexión de los usuarios al conectarse al Portal

En esta prueba se medirá el tiempo total que los usuarios se conectaron al portal cautivo, como también el flujo de datos utilizado por los usuarios mientras se encontraban conectados, cabe mencionar que algunos usuarios fueron creados, pero por diversos motivos de cada usuario no se conectaron al portal cautivo.

Escenario 1: Biblioteca

En este escenario de los 9 usuarios creados únicamente 6 fueron los que se conectaron al portal cautivo.

En la Tabla 14 se muestra el tiempo total que estuvo conectado cada usuario al portal cautivo, como también la cantidad de Download y Upload de datos utilizado.

Tabla 14. Registro de usuarios conectados al Portal Biblioteca

USUARIO	TIEMPO TOTAL DE SESIÓN	DOWNLOAD(MB)	UPLOAD(MB)
gzambrano	4 min 58 seg	1,44	0,35849
victor	36 min 52 seg	4,14	9,31
dfmena	1 hora 26 min 47 seg	21,47	3,56
Antono	35 min 26 seg	31,32	1,17
interops	41 min 32 seg	10,68	1,56
Alexito	15 min 43 seg	2,58	1,3
TOTAL	**3 horas 43 min 18 seg**	**71,63**	**17,25849**

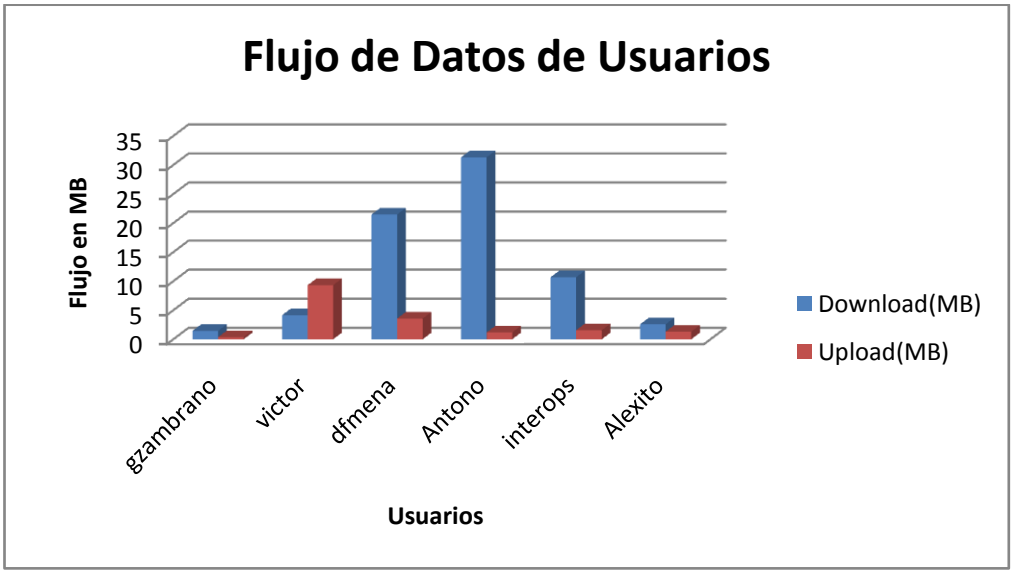
Elaborado por: Jonathan Jara y Diego Mena

Resultados

- **Flujo de Datos:**

En la Figura 145 se muestra que los usuarios **gzambrano** y **Alexito** obtuvieron el menor de consumo de flujo de datos en Download y Upload, esto se debe a que ambos usuarios utilizaron dispositivos móviles como tablets y teléfonos inteligentes al conectarse al portal. Por lo contrario el usuario con mayor consumo de flujo de datos tanto Download como Upload fue **Antono** puesto que mismo utilizo una laptop para conectarse al portal lo que generó mas flujo de Download y Upload.

Figura 145. Gráfica de Flujo de datos de Usuarios



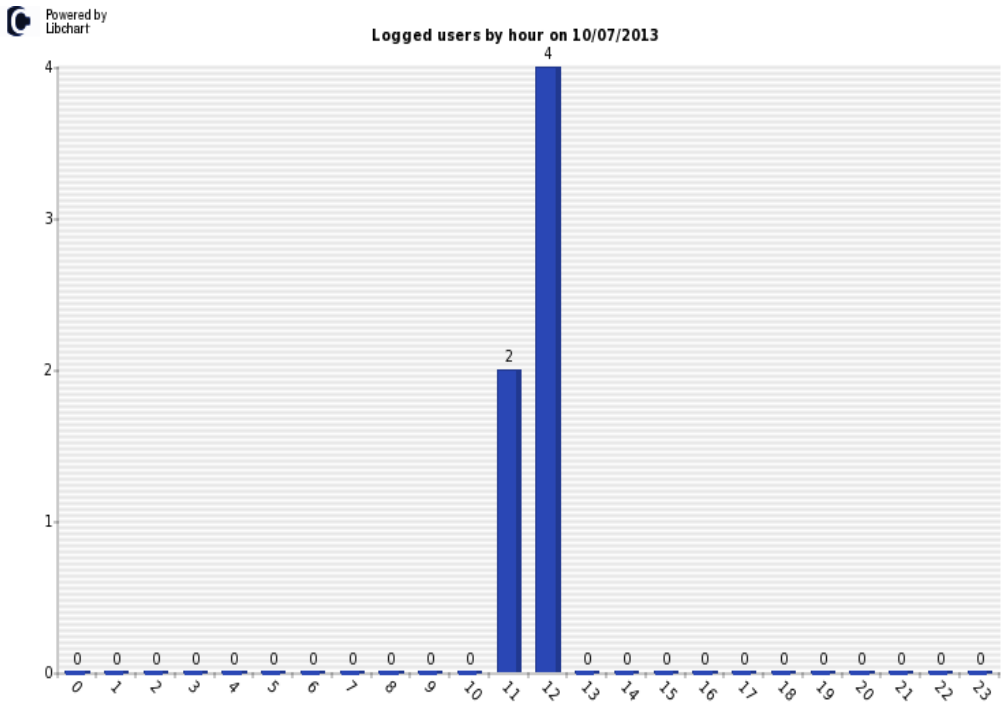
Elaborado por: Jonathan Jara y Diego Mena

- **Tiempo de Conexión:**

Daloradius entre sus características permite obtener el tiempo de conexión y la hora en la que se accedió al portal cautivo por cada usuario, facilitando al administrador el llevar un control de todos los accesos que se han producido al portal cautivo.

Con referencia a la Tabla 14 anterior, se concluye que el usuario **dfmena** es el usuario que permaneció más tiempo conectado con un tiempo total de 1 hora 26 minutos 47 segundos.

Figura 146. Accesos de usuarios en horas especificas en Biblioteca



Elaborado por: Jonathan Jara y Diego Mena

Escenario 2: Cafetería

En este escenario de los 14 usuarios creados únicamente 10 fueron los que se conectaron al portal cautivo. En la tabla se muestra el tiempo total que estuvo cada usuario conectado al portal cautivo, como también la cantidad de Download y Upload de datos utilizado por cada usuario.

Tabla 15. Registro de usuarios conectados al portal en Cafetería

USUARIO	TIEMPO TOTAL DE SESIÓN	DOWNLOAD (MB)	UPLOAD (MB)
tefita	1 hora 1 min 34 seg	10,83	1,62
Santy	36 min 3 seg	16,56	2,48
gabohzh	42 min 42 seg	1,4	0,298
michu	34 min 52 seg	6,77	1,04
alejobdp	18 min 14 seg	0,339	0,119
AndreJ	55 min 41 seg	2,21	0,382
Juank	18 min 57 seg	0,978	0,253
eddyplus	7 min 33 seg	0,474	0,122
cristhian	17 min 32 seg	0,512	0,109
Victorh	7 min 32 seg	0,175	0,435
TOTAL	**5 horas 0 min 40 seg**	**40,248**	**6,858**

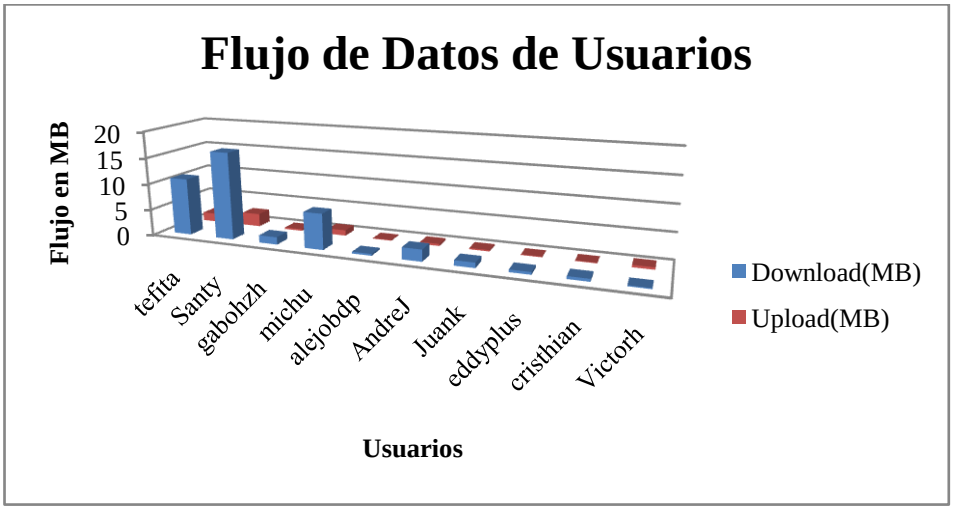
Elaborado por: Jonathan Jara y Diego Mena

Resultados

- **Flujo de Datos:**

En la Figura 147 se muestra que gran parte de los usuarios tienen poco consumo flujo de datos, ya que en este caso la mayoría utilizaron dispositivos móviles para conectarse al portal cautivo lo cuales no generan mucho consumo de flujo de datos. En este caso el usuario **Santy** muestra el mayor consumo de flujo de datos, puesto que utilizo una laptop para conectarse al portal cautivo lo que genera un alto consumo de flujo de datos.

Figura 147. Gráfica de Flujo de datos por Usuarios

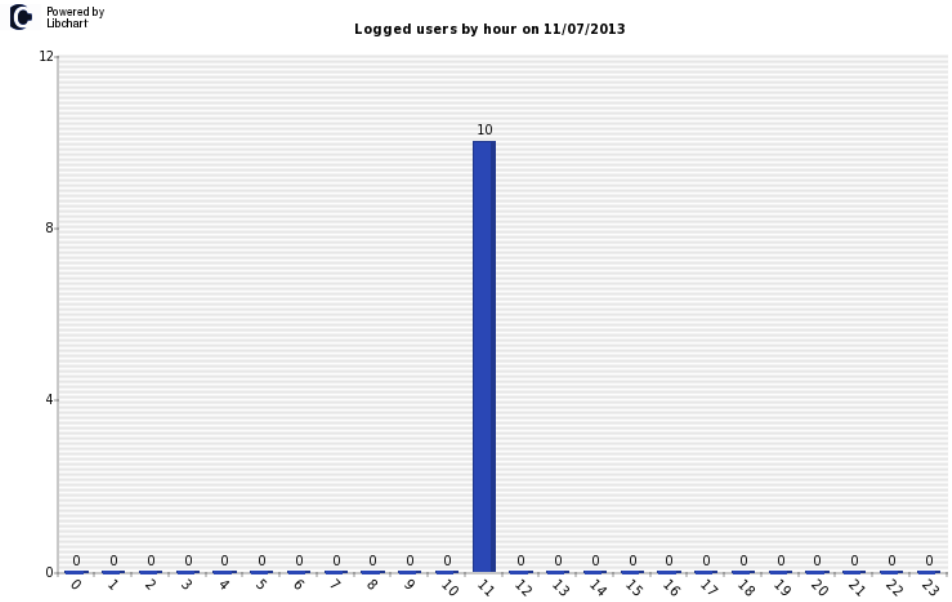


Elaborado por: Jonathan Jara y Diego Mena

- **Tiempo de Conexión:**

Todos los usuarios se conectaron entre las 11:00 y 12:00 de la mañana, y como referencia a la Tabla 15, se concluye que el usuario conectado por más tiempo conectado fue **tefita**, el cual tuvo una permanencia en el portal de 1 hora un 1 minuto y 34 segundos.

Figura 148. Accesos de usuarios por hora en Cafetería



Elaborado por: Jonathan Jara y Diego Mena

- **Prueba 3:** Intentos de logeo o acceso al portal cautivo durante las pruebas

Daloradius adicionalmente muestra cuántos intentos de conexión al portal cautivo se realizan por día. Se utilizó esta herramienta para conocer los intentos de conexión que se realizaron por parte de usuarios los días de prueba.

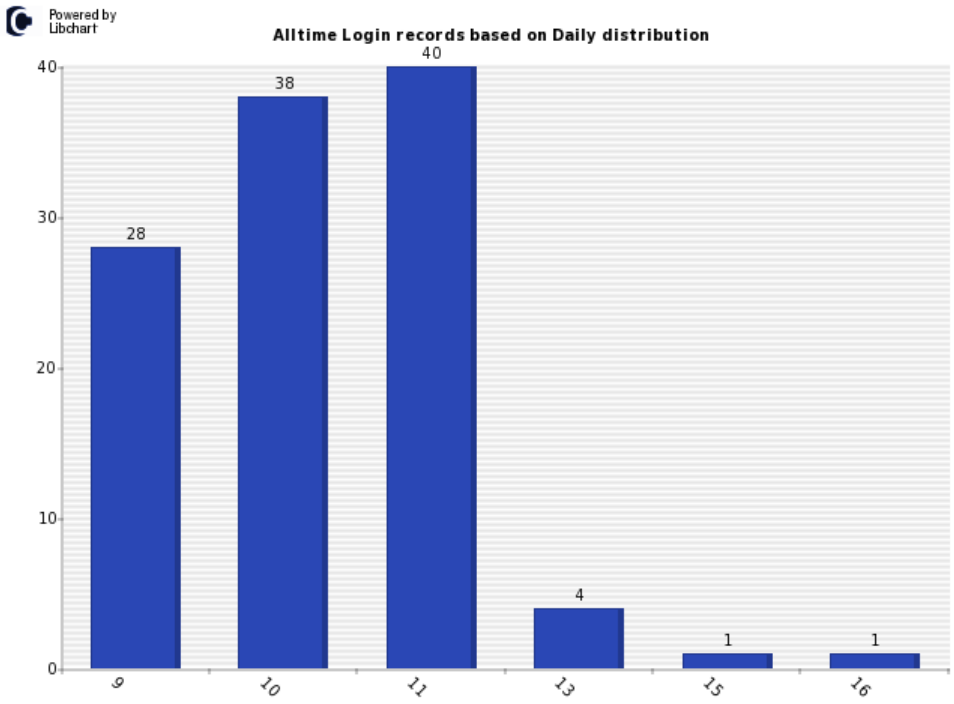
Figura 149. Número de intentos de conexión por día

ALL-TIME LOGINS/HITS STATISTICS	
Logins/Hits count > <	Day of month > <
28	9
38	10
40	11
4	13
1	15
1	16
112	

Elaborado por: Jonathan Jara y Diego Mena

Como se observa en la Figura 149 el día **miércoles 10** de julio se realizaron 38 intentos de conexiones, mientras que el día 11 de julio se realizaron 40 intentos de conexión.

Figura 150. Intentos de acceso al portal por día



Elaborado por: Jonathan Jara y Diego Mena

Según la Figura 150 el **día 11** se realizaron mas intentos de conexión ya que en el escenario de la cafetería la mayoría de usuarios utilizaron dispositivos móviles como Tablets y teléfonos celulares, por lo que son más propensos a cometer errores al momento de insertar el usuario o la contraseña.

- **Prueba 4:** Finalización de sesión de usuarios finales

En esta prueba se muestra la forma en que los usuarios se desloguearon del portal, durante los días de prueba realizados. Pero antes se debe conocer algunos atributos que se muestran dentro de los registros del Daloradius para un mejor entendimiento de los mismos:

- **Nas Reboot:** este atributo se genera cuando existe algún tipo de problema de comunicación entre el NAS y el cliente.

- **Lost Carrier:** este atributo se genera cuando el usuario se desconecta del portal cautivo sin desloguearse. Esto puede darse cuando el cliente sale del área de cobertura del Access Point.
- **Session Time Out:** este atributo se muestra cuando tiempo de sesión del usuario ha expirado. Para poder continuar utilizando el servicio de internet, el usuario debe loguearse nuevamente.
- **User Request:** este atributo se muestra cuando el usuario se desloguea del portal cautivo.

Escenario 1: Biblioteca

En este escenario se obtuvieron los siguientes resultados los cuales fueron por las siguientes razones:

Tabla 16. Número de Finalización de Sesiones Biblioteca

FINALIZACIÓN DE LA SESIÓN	TOTAL
User Request	10
Session Time Out	13
Nas Reboot	5
Lost Carrier	1
TOTAL	29

Elaborado por: Jonathan Jara y Diego Mena

La Tabla 16, muestra que **23** de las veces los usuarios finalizaron la sesión de manera exitosa, ya que para desconectarse del portal cautivo:

- 10 de las veces los usuarios se desconectaron de manera manual antes de la finalización de su tiempo de sesión.
- 13 restantes la desconexión fue por motivo de expiración del tiempo de sesión del usuario, lo cual se toma como una desconexión correcta.

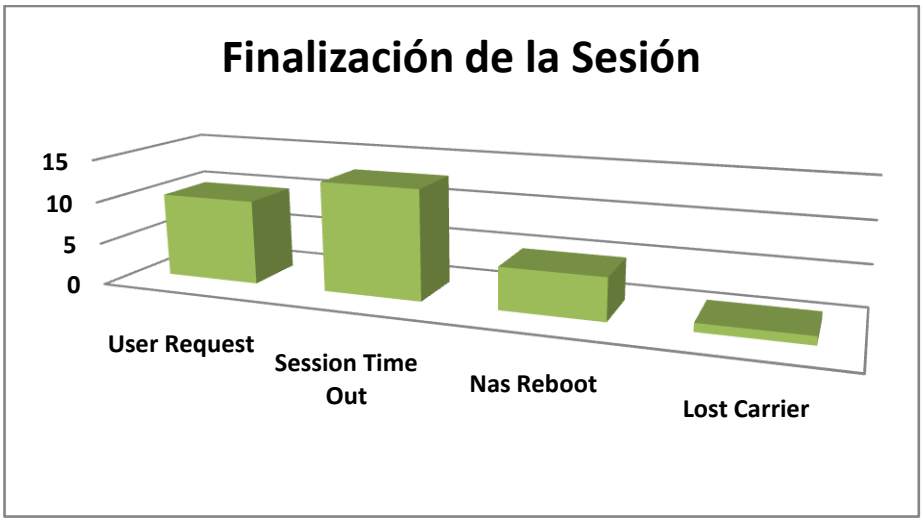
En lo que respecta a las **6** veces restantes, los usuarios finalizaron su sesión de manera abrupta por diferentes razones.

- Las 5 veces que se cerró la sesión, hubo algún tipo de problema en la conexión entre los usuarios y el NAS, esto se debe a que dentro de la biblioteca ya existía

un Router inalámbrico de mayor potencia, lo que pudo generar problemas de comunicación entre el Access Point utilizado para las pruebas y los usuarios finales.

- 1 solo usuario se desconecto del portal cautivo ya que salió fuera del área de cobertura del Access Point.

Figura 151. Finalización de sesión generadas por los usuarios Biblioteca



Elaborado por: Jonathan Jara y Diego Mena

Escenario 2: Cafetería

En este escenario se obtuvieron los siguientes resultados los cuales fueron por las siguientes razones:

Tabla 17. Número de Finalización de Sesiones Cafetería

FINALIZACIÓN DE LA SESIÓN	TOTAL
User Request	3
Session Time Out	13
Nas Reboot	0
Lost Carrier	11
TOTAL	27

Elaborado por: Jonathan Jara y Diego Mena

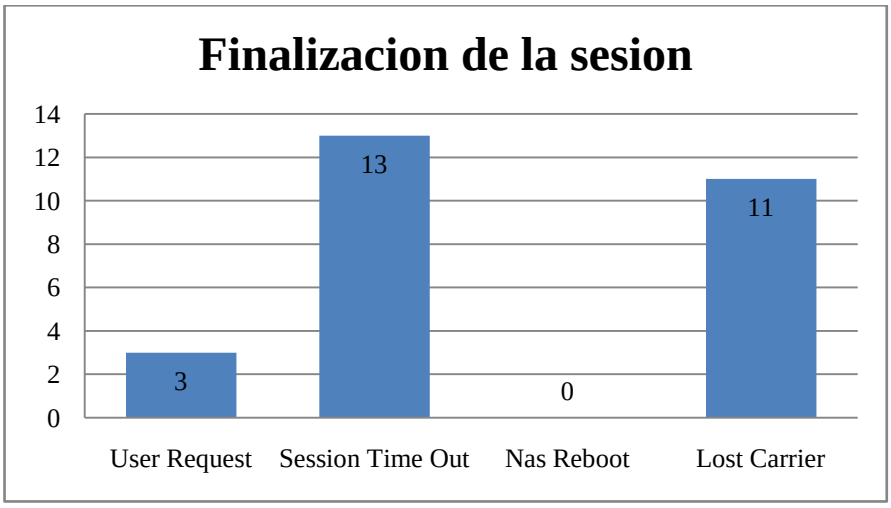
La Tabla 17, muestra que **16** de las veces los usuarios finalizaron la sesión de manera exitosa ya que para desconectarse del portal cautivo:

- 3 de las veces, los usuarios se desconectaron de manera manual antes de la finalización de su tiempo de sesión.
- 13 restantes la desconexión fue por motivo de expiración del tiempo de sesión del usuario, lo cual se toma como una desconexión correcta.

En lo que respecta a las 11 veces restantes, los usuarios finalizaron su sesión de manera abrupta por diferentes razones, entre las que podemos mencionar:

- Perdida de señal por distanciamiento del área de cobertura del Access Point
- Solicitado un usuario y contraseña, y no haber hecho uso del portal.

Tabla 18. Finalización de sesión generadas por los usuarios Cafetería

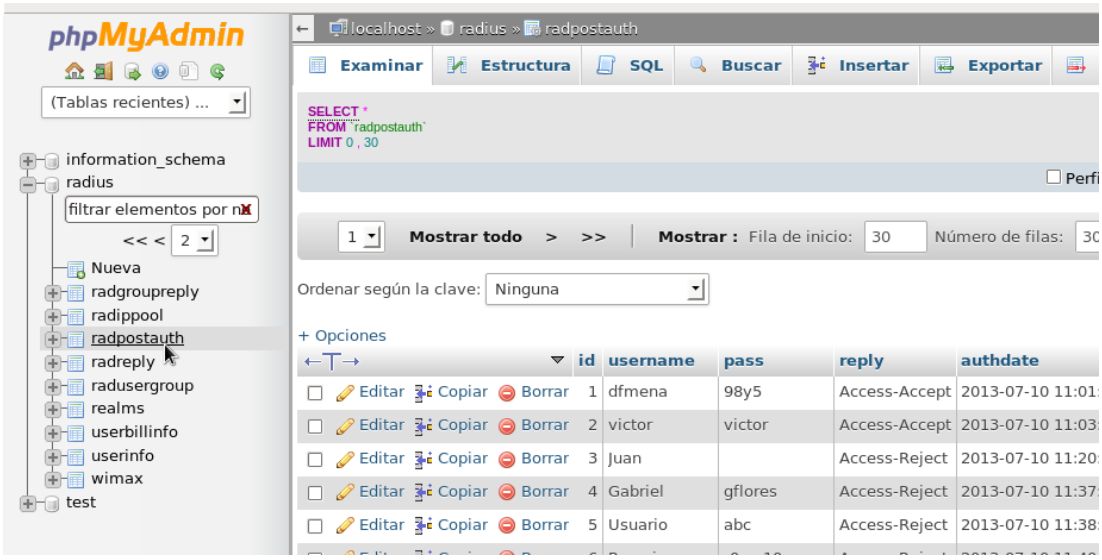


Elaborado por: Jonathan Jara y Diego Mena

- **Prueba 5:** Intentos de conexión fallidos o no autorizados

Para tener un conocimiento más detallado de los intentos de conexión se debe de revisar la tabla **radposthaut** dentro de la base de datos, ya que aquí se guardan todos los intentos de conexión tantos los fallidos como los exitosos. Los intentos fallidos dentro de la tabla **radposthaut** serán registrados como **Access-Reject**, mientras que los intentos exitosos serán registrados como **Access-Accept**.

Figura 152. Interfaz Grafica de phpMyAdmin Tabla **radposthaut**

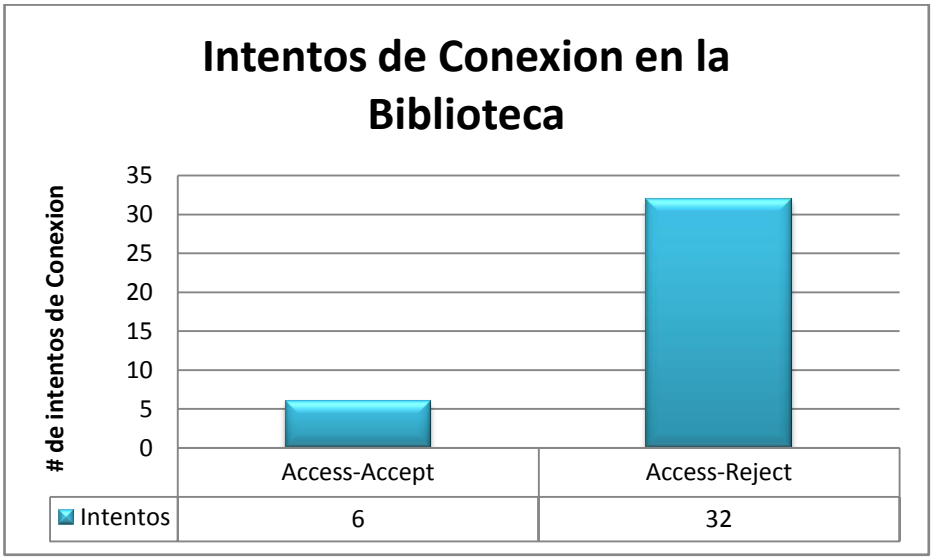


Elaborado por: Jonathan Jara y Diego Mena

Escenario 1: Biblioteca

En este escenario se obtuvieron los siguientes resultados de intentos de conexión, los cuales se muestran en la siguiente grafica:

Figura 153. Intentos de Conexión en Biblioteca

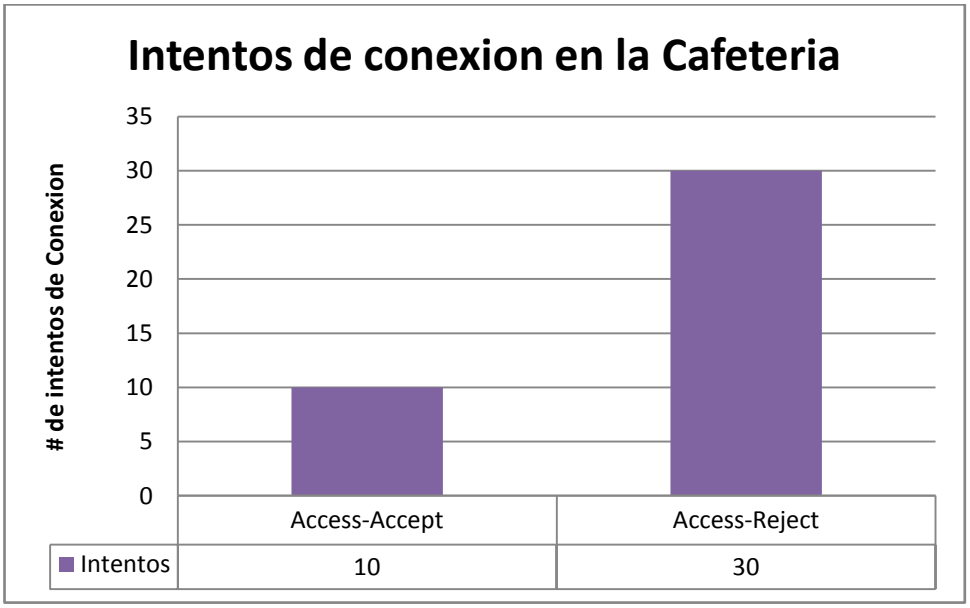


Elaborado por: Jonathan Jara y Diego Mena

Escenario 2: Cafetería

En este escenario se obtuvieron los siguientes resultados de intentos de conexión, los cuales se muestran en la siguiente grafica:

Figura 154. Intentos de Conexión en Cafetería



Elaborado por: Jonathan Jara y Diego Mena

4.5. Estudio de Factibilidad Técnica y Económica

- **Factibilidad Técnica**

La factibilidad técnica tiene como objetivo realizar la evaluación de las tecnologías utilizadas para verificar si es posible implementar y gestionar un portal cautivo para la Universidad. El levantamiento inicial de la red es una forma de obtener información sobre los componentes tecnológicos ya existentes en la Universidad para implementar el portal cautivo, o de ser necesario adquirir nueva tecnología para poner en marcha el proyecto.

El análisis de factibilidad técnico del portal cautivo se basa en 2 grandes aspectos: Hardware, que es la parte física y software que comprende todos programas necesarios para el funcionamiento del portal cautivo

Hardware

Ya que el sistema trabajará únicamente en la red inalámbrica de la Universidad Politécnica Salesiana, el equipo donde se implemente el portal cautivo deberá cumplir con las siguientes características:

Tabla 19. Características técnicas del Servidor Principal

MODELO	DELL PRECISION WST5400
Case	Torre
Procesador	2x Intel Xeon Quad Core 2.50 GHz
Memoria	8 GB
Disco Duro	1 TB HDD
Unidad Óptica	CDRW/DVD
Tarjeta de Video	Nvidia Quadro FX 4800 (1536 MB)
Tarjeta de Red	10/100/1000 Giga Ethernet
Puertos	Serial, Parallel, 2x PS/2, RJ-45, 8x USB 2.0, Audio
Monitor	21" Dell E207WFP.
Teclado	Dell SK-8115
Mouse	Dell MS111

Elaborado por: Jonathan Jara y Diego Mena

Evaluando el hardware existente y tomando en cuenta la configuración mínima necesaria, la Universidad podría utilizar alguno de los servidores que se encuentran en el DataCenter para instalar el portal cautivo, ya que estos satisfacen los requerimientos tanto de hardware por mucho o también se podría realizar una inversión inicial para la adquisición de un nuevo equipo, en el caso de que exista algún contratiempo con los servidores y no sea posible utilizarlos.

Con respecto a la infraestructura, la Universidad ya cuenta con una infraestructura de red funcional y por ende con los equipos de Networking que la componen, por lo no será necesario el adquirir equipos de Networking adicionales.

Software

En lo que respecta a plataforma, el portal cautivo puede funcionar en diferentes sistemas operativos de libre licenciamiento, en este caso se opto por utilizar la distribución Centos 6.2 ya que este es más enfocado a trabajar como servidor.

En cuanto a componentes de software necesarios para implementar el portal cautivo tenemos:

- Mysql
- Freeradius 2.0
- Chillispot
- Daloradius
- Phpmyadmin

- **Mysql**

Es un sistema de gestión de base de datos de libre distribución, el cual utiliza un esquema de licenciamiento dual, esto quiere decir que puede ser usado de manera libre como de manera privativa. Para el servidor se instalará la **Versión 5.1.69.**

- **Freeradius**

Es un servidor de radius de libre distribución, que cuenta con una licencia GPLv2, el cual permite la autentificación y la contabilización del acceso a una red. Para el servidor se instalara la **Versión 2.1.12-4.**

- **Chillispot**

Es un portal cautivo de libre distribución, el cual cuenta con licencia GLP, este trabaja junto a un servidor radius **(Freeradius)** para autenticar usuarios de una red que deseen utilizar el servicio de internet. Para el servidor se instalará la **Versión 1.1.0**, la cual es la última versión que se ha publicado de este software.

- **Daloradius**

Es una plataforma web para RADIUS, escrito en lenguaje PHP y Javascript, la cual se distribuye con licencia GLPv2 y es utilizada para la gestión de forma grafica de un servidor Freeradius. Esta plataforma es compatible con muchas gestores de bases de datos como: MySQL, PostgreSQL, SQLite, MSSQL. Para el servidor se instalará la **Versión 0.9.9-2**, por ser la más estable.

- **Phpmyadmin**

Es una herramienta de software libre, la cual se distribuye con licencia GLPv2, que permite la administración de una base de datos Mysql a través de la web y está escrito en lenguaje PHP. Para el servidor se instalará la **Versión 4.0.4.1.**

Tabla 20. Resumen Componentes del Portal Cautivo

SOFTWARE	VERSION	TIPO DE LICENCIA	CARACTERISTICAS
Mysql	5.1.69	Dual (Privativa, GPL)	Sistema de Gestión de Base de Datos
Freeradius	2.1.12-4	GLPv2	Servidor Radius
Chillispot	1.1.0	GLP	Portal Cautivo
Daloradius	0.9.9-2	GLPv2	Plataforma Web de Administración de RADIUS
Phpmyadmin	4.0.4.1	GLPv2	Plataforma Web de Administración de BDD

Elaborado por: Jonathan Jara y Diego Mena

Ubicación

El servidor se instalara dentro del data center que se encuentra en el quinto piso del edificio principal. Se deberá crear una **VLAN** temporal llamada **VLAN-PRUEBAS,** la cual estará enfocada únicamente a la red inalámbrica de la Universidad dentro del Switch de Core para realizar las pruebas correspondientes.

- El Servidor cumplirá la función de servidor AAA o Radius, el mismo que trabajará como un puente de acceso entre la red inalámbrica de la Universidad y el Servicio de Internet.

- El Servidor de Chillispot utiliza 2 tarjetas de red, en la primera se configurará el acceso del internet al portal cautivo y la segunda será la responsable de dar el servicio DHCP a los usuarios finales de la red inalámbrica, para la comunicación con el proxy

El estudio de factibilidad técnica determina que es viable la implementación del presente proyecto, ya que la Universidad cuenta con la infraestructura tecnológica necesaria para desarrollar y poner marcha el portal cautivo dentro la misma.

- **Factibilidad Económica**

La Factibilidad económica tiene como objetivo realizar un análisis del costo de inversión que representará la implementación del portal cautivo para la Universidad Politécnica Salesiana en el campus Sur, para lo cual se tomará en cuenta varios aspectos dentro de este proceso.

1. Costos de Infraestructura de Red
2. Costos de Equipos y Licencias
3. Costos de Instalación y Puesta en Marcha
4. Costos de Operación y Mantenimiento

Costos de Infraestructura de Red

En el análisis de costos con respecto a la infraestructura de red, la Universidad no tendrá que realizar gasto alguno, ya que cuenta con una infraestructura de red ya establecida y funcional, simplemente es adjuntar el nuevo servidor a la infraestructura de red ya existente y realizar las configuraciones respectivas.

Costos de Equipos y Licencias

Los costos por equipos representaran gastos para la Universidad solo en el caso de no utilizar alguno de los servidores ya existentes para incorporar el portal cautivo. Cabe recalcar que es necesario un servidor que pueda soportar toda la carga de trabajo del portal cautivo.

Se propone utilizar un equipo Dell Workstation modelo T5400 como servidor del portal cautivo ya que satisface los requerimientos de hardware para un correcto funcionamiento del portal cautivo, en la siguiente tabla se muestra un precio referencial del costo que generará la compra de este equipo y una tarjeta de red adicional:

Tabla 21. Detalle de Costos del Servidor Principal

CANTIDAD	DESCRIPCIÓN	VALOR UNITARIO	VALOR TOTAL
1	**DELL PRECISION WST5400** PROCESADOR 2X INTEL XEON QUAD CORE 2.50 GHZ MEMORIA RAM 8 GB DDR II SDRAM DELL UNIDAD ÓPTICA CDRW/DVD DISCO DURO 2 TB SATA 7200RPM DELL	$1500.00	$ 1500.00

	TARJETA DE RED 10/100/1000 GIGA ETHERNET TARJETA DE VIDEO NVIDIA QUADRO FX 4800 (1536 MB) PUERTOS SERIAL, PARALELO, 2X PS/2, RJ-45, 8X USB 2.0, AUDIO TECLADO MOUSE		
1	**TARJETA DE RED GIGABIT HP PCI EXPRESS X1** 10/100/1000 MBP	$ 105.00	$ 105.00
		SUBTOTAL	$ 1605.00
		12% IVA	$ 192.60
		TOTAL	**$ 1797.60**

Elaborado por: Jonathan Jara y Diego Mena

En la parte de licenciamiento del software la inversión no representará gasto alguno puesto que el sistema operativo como también los componentes el portal cautivo esta implementado totalmente en sistemas y componentes con los cuales se implementa el portal cautivo es libre distribución y licenciamiento.

Tabla 22. Detalle de Costos de Licenciamiento

CANTIDAD	DESCRIPCIÓN	VALOR UNITARIO	VALOR TOTAL
1	**LICENCIA DISTRIBUCIÓN CENTOS**	$ 0.00	$ 0.00
1	**LICENCIA CHILLISPOT**	$ 0.00	$ 0.00
1	**LICENCIA FREERADIUS**	$ 0.00	$ 0.00
1	**LICENCIA MYSQL-SERVER**	$ 0.00	$ 0.00
1	**LICENCIA PHPMYADMIN**	$ 0.00	$ 0.00
1	**LICENCIA DALORADIUS**	$ 0.00	$ 0.00
		SUBTOTAL	$ 0.00
		12% IVA	$ 0.00
		TOTAL	**$ 0.00**

Elaborado por: Jonathan Jara y Diego Mena

- **Costos de Instalación y Puesta en Marcha**

Estos costos no representarán ningún tipo de gasto para la Universidad, ya que será designado al Departamento de Informática ya existente en la Universidad efectuando la instalación física del servidor y las respectivas configuraciones de los dispositivos que intervienen en el funcionamiento del portal cautivo, en base a los parámetros manual de instalación descrito en el capítulo 3 del presente proyecto, y las pruebas para la comprobación del correcto funcionamiento del portal en la red inalámbrica.

5. Costos de Operación y Mantenimiento

Una vez que se haya instalado y probado el óptimo funcionamiento del portal cautivo en la red inalámbrica del campus, se deberá tomar en cuenta adicionalmente todos los factores que implican mantener en optimas condiciones el portal cautivo, las actividades que se deben realizarse para lograr este propósito son, entre otras, administración del portal, solución de problemas, administración de usuarios en la base de datos, configuraciones adicionales, etc. Para evitar que sea un gasto adicional para Universidad estas actividades serían designadas al Departamento de Informática ya existente en la institución.

Inversión Total

A través del análisis de todos los costos que implican la implementación el portal cautivo en la red inalámbrica de la Universidad se muestran los datos de manera global y el costo final del proyecto**.**

Tabla 23. Detalle General de Costos

COSTOS DE IMPLEMENTACIÓN	VALOR
COSTO DE INFRAESTRUCTURA DE RED	$ 0.00
COSTO DE EQUIPOS Y LICENCIAS	$ 1797.60
COSTO DE INSTALACIÓN Y PUESTA EN MARCA	$ 0.00
COSTO DE OPERACIÓN Y MANTENIMIENTO	$ 0.00
COSTO TOTAL	**$ 1797.60**

Elaborado por: Jonathan Jara y Diego Mena

CONCLUSIONES

1. Mediante el estudio de factibilidad técnica y factibilidad económica se puede determinar que la implementación del presente proyecto es totalmente viable, puesto que la universidad ya cuenta con la infraestructura tecnológica de red necesaria para su desarrollo y puesta en marca, generando un costo muy bajo de inversión para la universidad.

2. Las pruebas realizadas con portal cautivo dan como resultado que de todos los intentos de conexión, únicamente 13% de los intentos fueron exitosos mientras que 87% restante fueron rechazados por el portal cautivo, esto se debe a que el usuario por algún motivo pudo haber ingresado sus credenciales de forma errónea o por otro lado que los usuarios que intentaron logearse no constaban dentro de la base de datos del servidor freeradius, por lo que son tomados como usuarios ajenos a la universidad o no intentos de conexión fallidos.

3. El software Daloradius y Phpmyadmin son herramientas graficas que trabajan vía navegador web, las cuales en conjunto muestran los intentos de conexión, reportes de usuarios conectados, tiempos de conexiones, cantidad de conexiones en día, generar tablas y graficas de la mayoría de registros anteriormente mencionados y exportar dichos registros a archivos .csv, lo que facilita al administrador de la red la tarea de la administración del portal cautivo como también documentación y generación de reportes del mismo.

4. Los intentos de conexión se pueden conocer a través del software Daloradius como en la tabla radpostauth de la base de datos de freeradius, obteniendo los usuarios que se logean con éxito como también usuarios que por diversas razones como ingresar incorrectamente sus credenciales de autentificación o ser usuarios no autorizados, no pudieron acceder a el servicio de internet.

5. El portal cautivo propuesto posibilita el acceso a internet a través de la red Wi-Fi en toda la universidad utilizando políticas de tiempo de sesión en cada uno de los usuarios. En lo que respecta a la restricción y administración de los

sitios web permitidos, estas seguirán siendo realizadas por el servidor proxy de la universidad.

6. La credenciales de acceso al portal cautivo pueden seguir manteniendo el esquema de acceso como el resto de servicios que brinda la universidad como el aula virtual, el correo institucional y el servicio de Internet, donde se utiliza como usuario la dirección de correo institucional y como password la cédula de identidad lo que asegura que puedan tener acceso solo los usuarios vinculados directamente a la universidad evitando de esta forma cualquier tipo de hackeo o pirateo de claves, ya que las mismas serán únicas para cada usuario.

RECOMENACIONES

1. Se recomienda verificar que todas las versiones de los componentes a instalar sean las más actuales, ya que de este modo se podrá utilizar mayor cantidad de características de configuración y disponibilidad de los servicios de los mismos, para una futura escalabilidad en la implementación del portal cautivo.

2. Por motivos de escalabilidad se recomienda invertir en un servidor dedicado con el cual se pueda obtener todas las prestaciones de un equipo especializado, para soportar todo el tráfico de datos generado por el portal cautivo, tanto por las peticiones de los usuarios hacia el servidor Freeradius, como de todos los datos de retorno que el servidor ofrece al beneficiario como son autenticación y autorización.

3. Se recomienda la implementación del portal cautivo en la Universidad ya que primero no requiere de una gran inversión para su instalación, ni profesionales expertos para su configuración y desarrollo, además por la seguridad que este brindaría a la red inalámbrica que no posee un método dedicado a proteger este medio.

LISTA DE REFERENCIAS

abanet.net. (2013). *Acrónimos*. Recuperado el 20 de febrero de 2013, de http://www.abanet.net/acronimos.html

Apache. (2013). *Welcome to the mod_perl world*. Recuperado el 10 de marzo de 2013, de http://perl.apache.org/

Aries, B. (2013). *Ventajas de Apache Web Server*. Recuperado el 10 de enero de 2013, de http://www.ehowenespanol.com/ventajas-apache-web-server-lista_109947/

Autónoma, U. N. (Octubre de 2000). *Hubs y Switches*. Recuperado el 16 de febrero de 2013, de http://html.rincondelvago.com/hubs-y-switches.html

barcodesinc.com. (2010). *barcodesinc.com*. Recuperado el 4 de febrero de 2013, de http://www.barcodesinc.com/images/models/lg/Cisco/1040.jpg

Bestofmedia, T. (21 de Febrero de 2012). *tomsitpro.com*. Recuperado el 12 de enero de 2013, de http://www.tomsitpro.com/articles/local_area-network.-wi-fi-wireless-networking,2-262-5.html#

Byffalo, T. (2013). *Tecnología Estándar - Tecnologías 802.11 Inalambricas*. Recuperado el 10 de mayo de 2013, de http://www.buffalotech.fr/es/wireless-802-11-technologies.html

centos-55.blogspot.com. (14 de Febrero de 2011). *Definición de Centos*. Recuperado el 2 de marzo de 2013, de http://centos-55.blogspot.com/2011/02/definicion-de-centos.html

channelprosmb.com. (31 de Mayo de 2013). *Nomadix Targets SMBs with New Public Access Gateway*. Recuperado el 9 de junio de 2013, de http://www.channelprosmb.com/images/main_article_images/nomadix-ag-2400.jpg

Ciberaula. (2010). *Una Introducción a APACHE*. Recuperado el 10 de marzo de 2013, de http://linux.ciberaula.com/articulo/linux_apache_intro.

Colemanres, J. (3 de Febrero de 2008). *Estándares IEEE 802*. Recuperado el 12 de febrero de 2013, de http://estandaresieee802redes.blogspot.com/

Computrad. (2012). *Cisco Catalyst 3750G-24TS Switch*. Recuperado el 14 de abril de 2013, de http://www.1st-computer-networks.co.uk/CISCO-3750G-24TS.php

Cworld-System. (2012). *Los Enlaces Inalambricos*. Recuperado el 21 de mayo de 2013, de http://www.cworld-system.com/enlaces-inalambricos.html

Cyberprimo. (2010). *Servidores: Qué son y Para qué sirven*. Recuperado el 24 de mayo de 2013, de http://www.cyberprimo.com/2010/02/servidores-que-son-y-para-que-sirven.html

cyclopaedia.net. (2013). *Protocolo AAA*. Recuperado el 18 de abril de 2013, de http://es.cyclopaedia.net/wiki/Protocolo-AAA

Definicionabc. (2013). *Definición de Switch*. Recuperado el 11 de mayo de 2013, de http://www.definicionabc.com/tecnologia/switch.php

Diaz, R. (7 de Enero de 2013). *Protocolos capa Enlace*. Recuperado el 6 de abril de 2013, de http://www.slideshare.net/ricardosava/protocolos-capa-enlace-ricardo-sava-diaz

docente.ucol.mx. (2013). *Estándar IEEE 802.1n*. Recuperado el 12 de junio de 2013, de http://docente.ucol.mx/al971848/public_html/IEEE.htm

Domínguez, A. (18 de Septiembre de 2013). *Seguridad en Apache: modSecurity*. Recuperado el 22 de octubre de 2013, de http://openwebinars.net/seguridad-en-apache-modsecurity/

Duchi, F., & Guerrero, E. (Febrero de 2011). Implementación de una Red Inalámbrica mediante LMDS- servicio de distribución local Multipunto, en el Banco Nacional de Fomento - Sucursal Quinindé, Provincia de Esmeraldas . Latacunga, Ecuador: Universidad Técnica de Cotopaxi.

Dukee, A. (6 de Agosto de 2011). *Redes*. Recuperado el 24 de marzo de 2013, de http://www.slideshare.net/MasterTeam/redes-8789838

Dyllan. (2009). *¿Qué es un router?* Recuperado el 20 de marzo de 2013, de http://es.kioskea.net/faq/2757-que-es-un-router.

Eagle, A. (2 de junio de 1999). *Características de los Sistemas Linux*. Recuperado el 4 de mayo de 2013, de http://xml.cie.unam.mx/xml/Linux/glinux-2.html

Eegle, G. (2010). *Que es Nat?* Recuperado el 13 de mayo de 2013, de http://www.voobly.com/forum/thread/9566

elinux.com.mx. (s.f.). *Principales características de Linux*. Recuperado el 2 de febrero de 2013, de http://www.elinux.com.mx/1-aprendiendo-linux/11-blog-de-historia/114-principales-caracteristicas-de-linux

Esquivel, F. (14 de Abril de 2013). *Diferencias entre HTTP y HTPPS*. Recuperado el 15 de febrero de 2013, de http://tegnologiafernanada.bligoo.com.mx/diferencias-entre-http-y-htpps

Fernandokatz. (Septiembre de 2010). *Introducción a la Redes Inalambricas*. Recuperado el 3 de junio de 2013, de http://www.buenastareas.com/ensayos/Introduccion-a-Las-Redes-Inalambricas/691290.html

Fierro, M., & Gonzales, F. (2011). Estudio comparativo de aplicaciones para la Implementación de portales cautivos empleando Interconectividad entre los locales de bonny restauran. Riobamba, Chimborazo, Ecuador: ESPOCH .

Garcia, S. (20 de Febrero de 2008). *Proyecto Entorno AAA*. Recuperado el 8 de febrero de 2013, de http://proyectoaaa.blogspot.com/2008/02/que-es-aaa.html

Gonzalez, J. (25 de Julio de 2011). *nstalación Básica Centos 6 (Modo Gráfico)* . Recuperado el 20 de agosto de 2013, de http://jorgegonzalezmartos.wordpress.com/2011/07/25/instalacion-basica-centos-6-modo-grafico/

guayaquil.olx.com.ec. (2012). Recuperado el 3 de mayo de 2013, de http://guayaquil.olx.com.ec/redes-router-tew-652brp-routers-trendnet-150mbps-iid-121357762

Ingeniatic. (2011). *WLAN (Wireless Local Area Network)*. Recuperado el 23 de febrero de 2013, de http://ingeniatic.net/index.php/tecnologias/item/668-wlan-wireless-local-area-network

Jara, P., & Nazar, P. (2010). *Estándar IEEE 802.11X*. Recuperado el 10 de enero de 2013, de http://www.edutecne.utn.edu.ar/monografias/standard_802_11.pdf

kioskea.net. (Octubre de 2013). *WPAN (Wireless Personal Area Network)*. Recuperado el 20 de junio de 2013, de http://es.kioskea.net/contents/821-wpan-wireless-personal-area-network

Kisokea. (Octubre de 2013). *Introducción a Wifi*. Recuperado el 12 de febrero de 2013, de http://es.kioskea.net/contents/wifi/wifiintro.php3

lacasainfantil.com. (1 de Septiembre de 2010). *Mapa Mundial en Blanco*. Recuperado el 17 de mayo de 2013, de http://www.lacasainfantil.com/materiales-y-recursos/mapa-mundi-en-blanco

laserwifi.com. (2012). *Descripción del estandar para redes Wi-Fi IEEE 802.11n*. Recuperado el 20 de febrero de 2013, de http://www.laserwifi.com/estander802n.11.htm

Linux, W. (2013). *Núcleo Linux*. Recuperado el 20 de mayo de 2013, de http://es.wikipedia.org/wiki/N%C3%BAcleo_Linux

Machines, S. (2011). *http://www.tecnohackers.net*. Recuperado el 20 de marzo de 2013

Maldonado, A. (Septiembre de 2012). Implantación de un portal cautivo que permita el control de acceso al servicio de Internet a los estudiantes del Colegio San Luis Gonzaga a través de una autenticación de usuarios mediante un servicio AAA

implementado en un servidor Radius. Quito, Pichincha, Ecuador: Universidad Politecnia Salesiana.

Medina, L. A. (2012). *Como Instalar Linux*. Recuperado el 4 de mayo de 2013, de http://www.comoinstalarlinux.com/como-instalar-centos-linux-como-servidor/

Microsoft. (2013). *Protocolo RADIUS*. Recuperado el 13 de mayo de 2013, de http://technet.microsoft.com/es-es/library/dd197481%28v=ws.10%29.aspx

mountakhab.net. (2010). *SWITCH CISCO Catalyst 3750G 48 Ports*. Recuperado el 21 de marzo de 2013, de http://mountakhab.net/forum/index.php?showtopic=76522

Navarrete, C. (14 de Octubre de 2009). *Evaluación de la tecnología IEEE 802.11n con la plataforma OPNET*. Recuperado el 10 de mayo de 2013, de upcommons.upc.edu/pfc/bitstream/2099.1/7834/1/memoria.pdf

Novoa, P., & Reyes, F. (Octubre de 2007). Análisis, estudio y Site Survey para investigar la factibilidad con respecto a la cobertura de señal wireless basada en el estándar 802.11 (wi-fi) en el campus sur de la Universidad Politécnica Salesiana. Quito, Pichincha, Ecuador: Universidad Politecnica Salesiana.

ocw.uniovi.es. (31 de Julio de 2010). *Características Principales*. Recuperado el 20 de marzo de 2013, de http://ocw.uniovi.es/mod/resource/view.php?id=1242

ordenadores-y-portatiles.com. (2013). *Los 3 modos de un Access Point*. Recuperado el 25 de febrero de 2013, de http://www.ordenadores-y-portatiles.com/access-point.html

Pérez, R. O. (2011). *Seguridad basada en Redes Inalambricas*. Recuperado el 20 de mayo de 2013, de http://cefirefp.edu.gva.es/fileadmin/Apunts/Informatica/Jornades_Professorat_08/IBNS_wireless.pdf

Pestrebol. (2013). *A.A.A*. Recuperado el 20 de marzo de 2013, de http://pestrebol.com.ar/aaa.html

QualDev. (2012). *AAA*. Recuperado el 12 de marzo de 2013, de http://qualdev.uniandes.edu.co/wikiDev/lib/exe/fetch.php?media=development:requirements:invesitgacion_inicial_aaa.ppt.

Ramirez, C. (junio de 2010). Evolución de la Tecnologias de Núcleo de la Redes de Telefonia Móvil. Guatemala: Universidad de San Carlos de Guatemala.

Ramírez, M. (21 de Octubre de 2012). *Servidores*. Recuperado el 7 de marzo de 2013, de http://emigt.bligoo.com.mx/servidor

redesjeaneth.blogspot.com. (13 de Marzo de 2013). *Redes Computacionales* . Recuperado el 19 de febrero de 2013, de http://redesjeaneth.blogspot.com/p/red-inalambrica-las-redes-inalambricas.html

Redolfi, W. (Mayo de 2010). *Conectividad Inalambrica*. Recuperado el 8 de febrero de 2013, de http://tecnologiadeconectividad.blogspot.com/

slideshare.net. (27 de Septiembre de 2010). *Access Point*. Recuperado el 16 de marzo de 2013, de http://www.slideshare.net/locos222/access-point-5296110

slideshare.net. (4 de Noviembre de 2012). *Evolucion del linux*. Recuperado el 23 de abril de 2013, de http://www.slideshare.net/vivifarah97/evolucion-del-linux-15026035

slideshare.net. (28 de Septiembre de 2010). *Redes inalambricas Guía #2*. Recuperado el 7 de febrero de 2013, de http://www.slideshare.net/karito199317/guia-2-5311919

slideshare.net. (17 de Octubre de 2013). *Servidores web*. Recuperado el 4 de marzo de 2013, de http://www.slideshare.net/samuelsemg/servidores-web-27279559

Solano, J., & Oña, M. (2009). Estudio de Portales Cautivos de Gestión de acceso Inalámbrico a Internet de la ESPOCH. Riobamba, Chimborazo, Ecuador: ESPOCH.

tape4backup.com. (2012). *2504 Wireless Controller with 15 AP Licenses*. Recuperado el 4 de febrero de 2013, de http://www.tape4backup.com/air-ct2504-15-k9.php

technet.microsoft. (2013). *Protocolo RADIUS*. Recuperado el 14 de marzo de 2013, de http://technet.microsoft.com/es-es/library/dd197481%28v=ws.10%29.aspx

Tecnomagnific. (2011). *Switch y Router*. Recuperado el 18 de mayo de 2013, de http://www.tecnomagnific.com/html/preguntasswitchyrouter.html

tecnoteresiano.wikispaces.co. (2013). *Linux*. Recuperado el 18 de marzo de 2013, de http://tecnoteresiano.wikispaces.com/Linux

todo-redes.com. (s.f.). *Access Point (Punto de Acceso)*. Recuperado el 7 de enero de 2013, de http://todo-redes.com/access-point-punto-de-acceso.html

tuexpertoit.com. (2009). Recuperado el 9 de mayo de 2013, de http://www.tuexpertoit.com/2009/12/18/las-empresas-optan-por-la-modernizacion-de-su-infrestructura-ti-en-lugar-de-su-sustitucion/

tynex.com. (2012). *Cisco CATALYST 3750 12 SFP DC POWERED STD MULTILAYER IMAGE*. Recuperado el 6 de marzo de 2013, de http://www.tynex.com/images/Upload/products/X/SWCH288.jpg

upload.wikimedia.org. (2011). Recuperado el 10 de febrero de 2013, de http://upload.wikimedia.org/wikipedia/commons/d/d2/Tipus_xarxa.gif

Uruguay, U. O. (2013). *Proyecto de Infraestructura Tecnológica*. Recuperado el 12 de mayo de 2013, de http://www.ort.edu.uy/index.php?cookie_setted=true&id=AAAHAIAL

viasatelital.com. (2010). *Router Cisco 7604*. Recuperado el 12 de mayo de 2013, de http://viasatelital.com/blogs/wp-content/uploads/2012/01/Router-Cisco-7604.jpg

Villagas, D. (2009). *ESTANDAR-IEEE-80211*. Recuperado el 25 de enero de 2013, de http://es.scribd.com/doc/13842125/ESTANDAR-IEEE-80211

Vitaloni, J. (2008). *Que es el wi-fi "N"?* . Recuperado el 12 de marzo de 2013, de http://www.ebpi.com.ar/tecnologia/tecnologia_20110603_ruterwifi.html

websolut. (15 de Octubre de 2013). *Router y Modem*. Recuperado el 22 de octubre de 2013, de http://ws.saoinetwork.com/?p=361

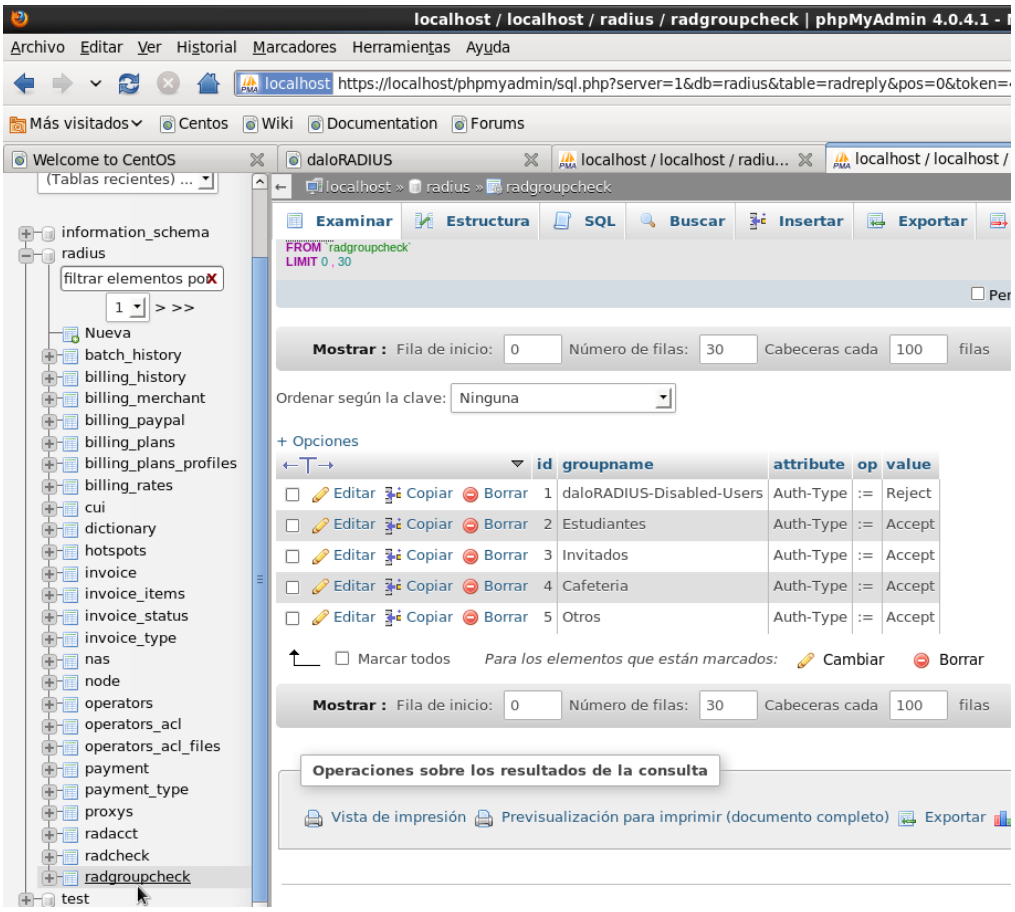
WordPress. (2008). *Definición de Router?* Recuperado el 25 de mayo de 2013, de http://definicion.de/router/

world-point.ch. (2011). *Cisco 2851 Voice Bundle - routeur*. Recuperado el 14 de mayo de 2013, de http://www.world-point.ch/cisco-2851-voice-bundle-routeur-p-462.html

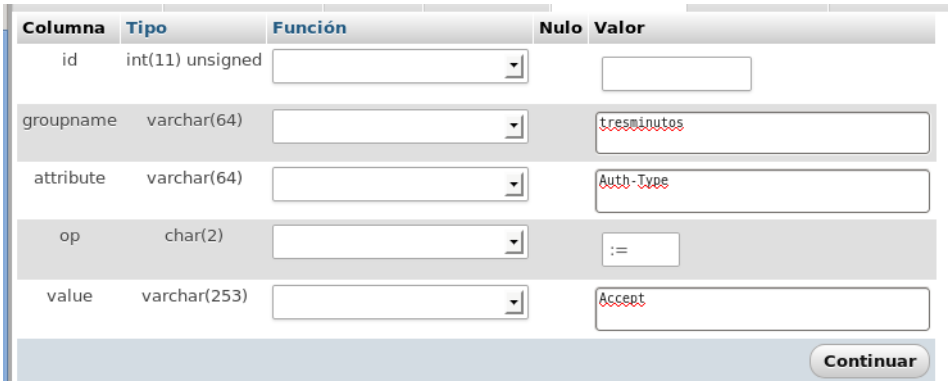
ANEXOS

Anexo 1. Daloradius - Asignación de límite de tiempo a un grupo de usuarios

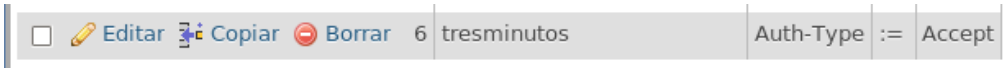
1. Para aplicar el límite de tiempo de sesión a un grupo de usuarios primero se debe crear un grupo en la tabla **radgroupcheck**, para lo cual se debe de dar clic en la pestaña insertar.



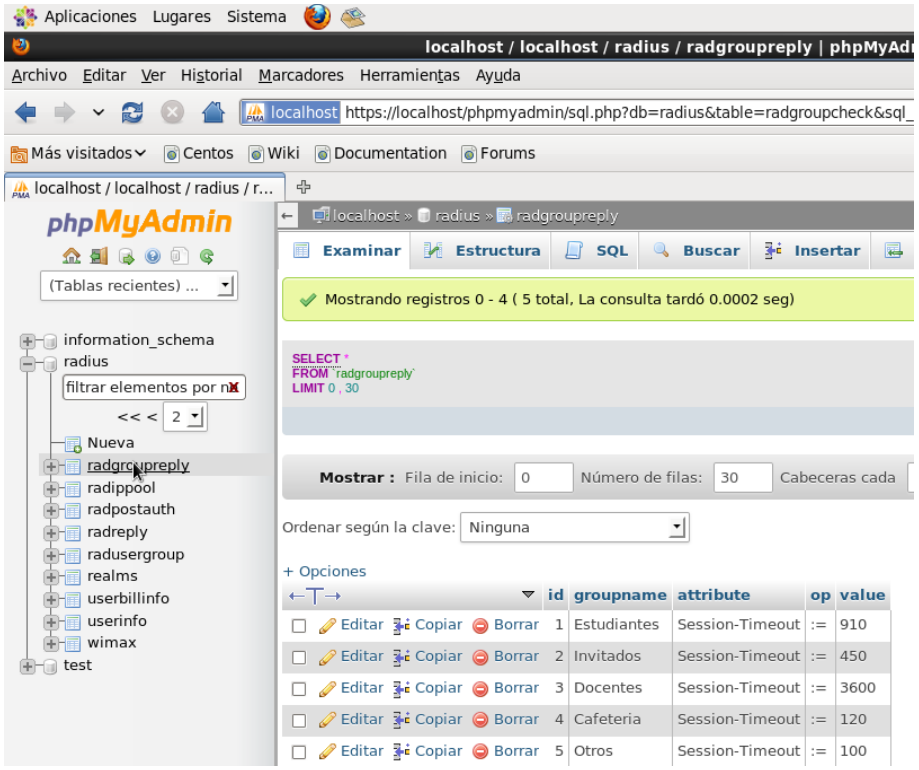
2. Para crear un usuario, se deberá ingresar los siguientes parámetros:
   - **groupname:** Aquí se ingresará el nombre del nuevo grupo.
   - **attribute:** El atributo que se ingresará será **Auth-Type** para que elija automáticamente el protocolo de autentificación, es decir que el protocolo de autentificación será el que es usado por defecto por el servidor radius.
   - **value:** Se asignará el valor **Accept** para que el portal cautivo acepte las peticiones de autentificación de los usuarios pertenecientes a este grupo.



3. Seguido, se dará clic en continuar y verificar la creación del grupo



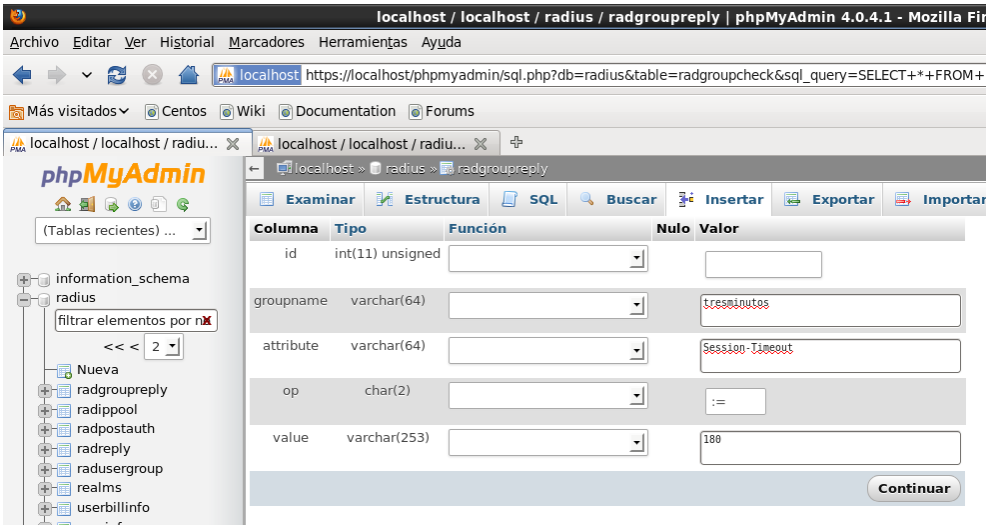
4. Ahora para crear la regla del límite de sesión de tiempo en un grupo, se utilizará la tabla **radgroupreply**.



5. Se dará clic en insertar y llenar los siguientes parámetros para crear la regla al grupo deseado:

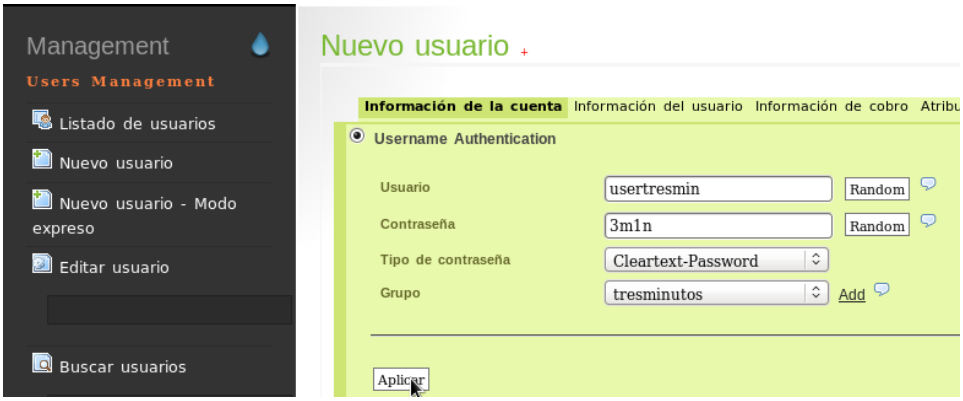
- **groupname:** Aquí se ingresará el nombre de grupo al cual se le aplicara la regla del límite de tiempo de sesión
- **attribute:** Aquí se ingresará el parámetro Session-Timeout, el cual es el tiempo límite que la sesión permanecerá activa.

- **value:** Será el valor en segundos que durará la sesión abierta



6. Seguido, se dará clic en el botón continuar para crear la nueva regla de tiempo límite de sesión para un grupo.

7. Ahora, se creará un usuario utilizando el software Daloradius, en el campo grupo se elegirá el nuevo grupo creado anteriormente y dar clic en aplicar.

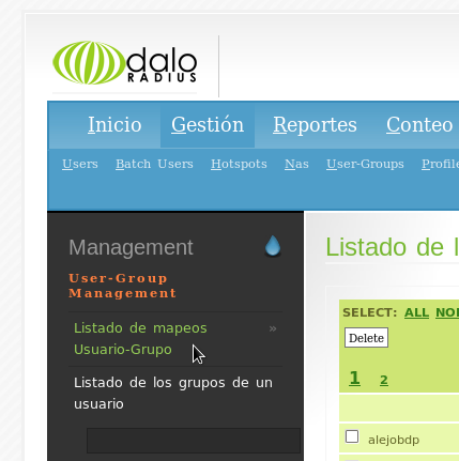


8. A continuación, se verificará que la regla del tiempo se aplique al usuario que se encuentra dentro del grupo tres minutos

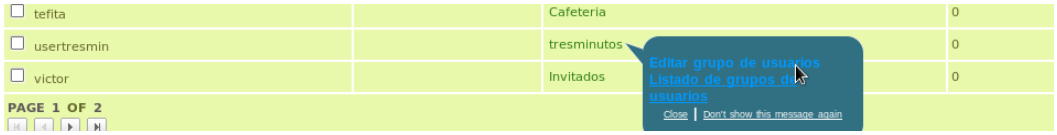
9. Y finalmente como se observa en la imagen el usuario finaliza la sesión puesto que el tiempo límite asignado al grupo llego al final.

Anexo 2. Daloradius - Cambiar de grupo a una usuario determinado

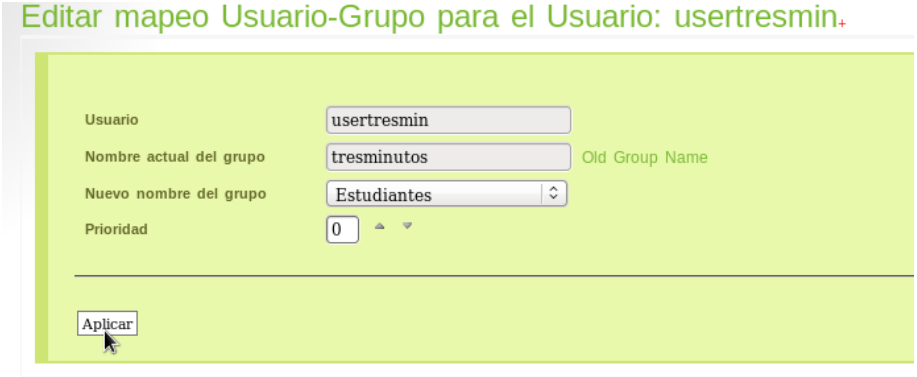
1. Se deberá ingresar a Daloradius a la sección de Gestión y elegirá en la opción listado de mapeo **Usuario-grupo,** como se muestra en la imagen



2. Después se buscará el usuario al que desea modificar el grupo, y se dará clic en el grupo y elegir la opción editar grupo de usuarios



3. Seguidamente, se escogerá el grupo al que se desee cambiar el usuario dentro de la opción **nuevo nombre del grupo** y después se dará clic en aceptar



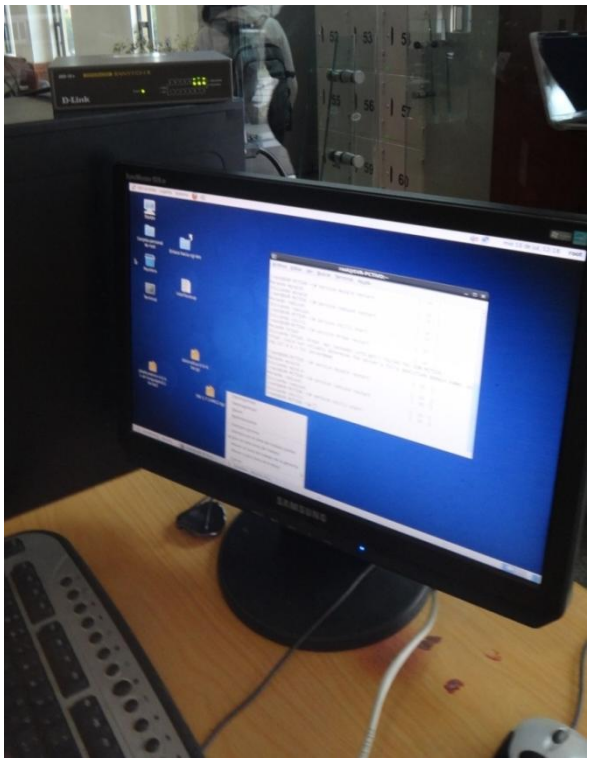
4. A continuación, se verificará que se haya efectuado el cambio de grupo exitosamente

5. Y finalmente, el cambio se verá reflejando dentro del portal cautivo


PORTAL CAUTIVO UPS - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
PORTAL CAUTIVO UPS
https://172.17.49.5/cgi-bin/hotspotlogin.cgi?res=notyet&uamip=172.17.49.5&uampor
Google
Portal Cautivo UPS
Usuario: usertresmin
Contraseña: ••••
Autenticar

Anexo 3. Ubicación de infraestructura de red física para pruebas realizadas en la universidad

Servidor Principal

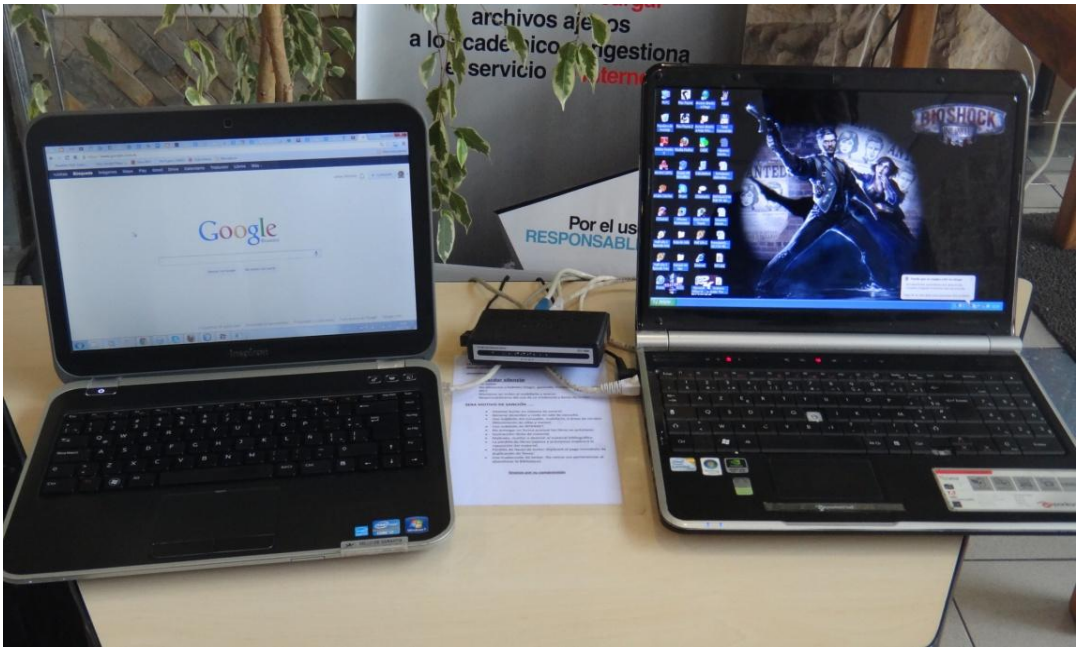


Switch de Core y Distribución

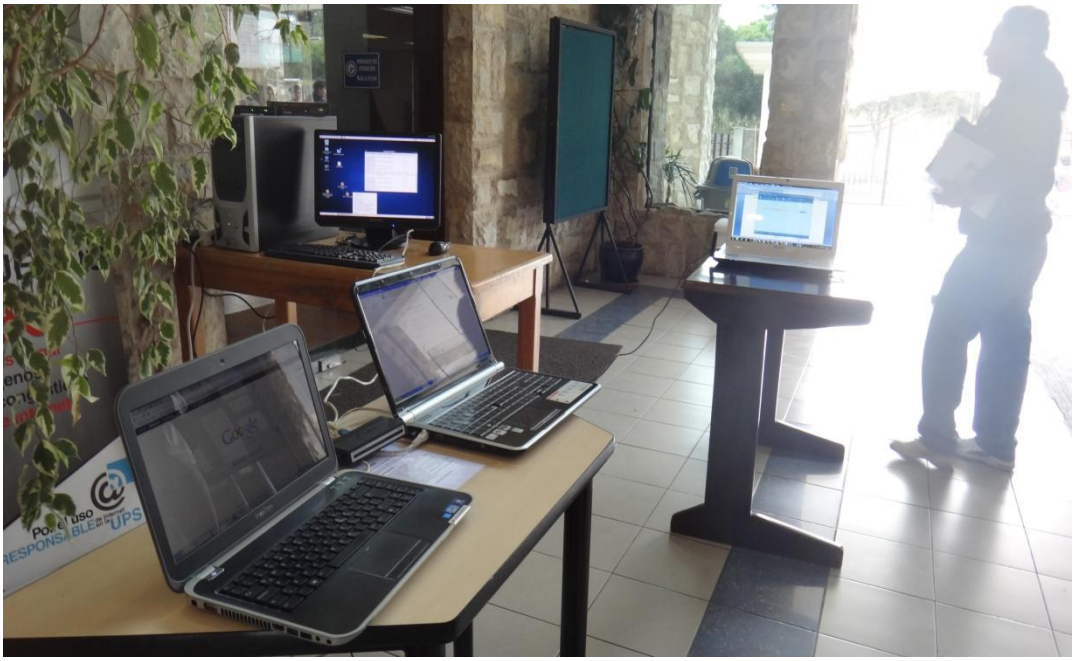
Servidor de Internet (Modem GSM)

Router Inalámbrico

Parte de red LAN



Esquema de General de red de Pruebas



GLOSARIO

AAA: Authentication, Authorization and Accounting.

ACL: Lista de Control de Acceso.

AJAX: Java Script asíncrono y XML.

APACHE: Servidor web HTTP de código abierto.

ASP: Active Server Pages.

ASP.NET: Framework para aplicaciones web desarrollado por Microsoft.

BSD: Berkeley Software Distribution.

BSS: Conjunto de estaciones inalámbricas que pueden comunicarse entre sí.

CGI: Interfaz de entrada común.

CHAP: Protocolo de autenticación por desafío mutuo.

CNAC: Closed Network Access Control.

CRC: Comprobación de redundancia cíclica.

CSMA/CA: Acceso Múltiple con Detección de Portadora y Prevención de Colisiones).

DBPSK: Modulación por desplazamiento diferencial de fase.

DQPSK: Differential Cuadratura Phase Shift Keying.

DSSS: Espectro ensanchado por secuencia directa.

EAP: Protocolo Extensible de Autenticación.

FREEBSD: Avanzado sistema operativo para arquitecturas x86 compatibles (como Pentium® y Athlon™).

FTP: Protocolo de Transferencia de Archivos.

GNU: Es un acrónimo recursivo que significa **GNU No es Unix** (GNU is Not Unix).

GNU/LINUX: Combinación del núcleo o kernel libre similar a Unix denominado Linux con el sistema GNU.

GPL: Licencia Pública General de GNU.

HOTSPOT: Lugar que ofrece acceso a Internet a través de una red inalámbrica y un Enrutador.

HTML: Lenguaje de marcado hipertextual.

HTTP : Protocolo de transferencia de Hipertexto.

HTTPD: Demonio de HTTP en Linux.

HTTPS: Protocolo de transferencia de Hipertexto Seguro.

IDS: Sistema de detección de intrusos.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.

IP: Protocolo de Internet.

ISP: Proveedor de servicios de Internet.

JAVA: Lenguaje de programación y la primera plataforma informática creada por Sun Microsystems en 1995.

JSP: JavaServer Pages.

LAN: Red de Área Local.

LDAP: Protocolo Ligero de Acceso a Directorios.

LWAPP: Protocolo Ligero para Puntos de Acceso.

MAC: Medium Access Control.

MACOS: Sistema Operativo de Macintosh.

MIMO: Múltiple entrada múltiple salida

MYSQL: Sistema de gestión de bases de datos relacional, multihilo y multiusuario.

NAS: Servidor de acceso a la red, o punto de entrada.

NCSA: Centro Nacional de Aplicaciones de Supercomputación.

OFDM: Multiplexación por División de Frecuencias Ortogonales.

OPENBSD: Sistema operativo LIBRE de tipo Unix, multiplataforma y basado en BSD.

OPENSSL: Robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía.

OPENWRT: Distribución de Linux basada en firmware usada para dispositivos empotrados tales como routers personales.

OSA: Open System Authentication.

OSI: Sistema Abierto de Interconexión.

P2P: Peer to Peer.

PERL: Lenguaje de programación que toma características del lenguaje C interpretado bourne shell.

PHP: Hypertext Preprocessor.

PYTHON: Lenguaje de programación interpretado cuya filosofía hace hincapié en una sintaxis muy limpia y que favorezca un código legible.

RFC: Request For Comments.

RFID: Identificación por radiofrecuencia.

RHEL: Red Hat Enterprise Linux.

ROAMING: Capacidad de cambiar de un área de cobertura a otra sin interrupción en el servicio o pérdida en conectividad.

SNMP: Protocolo Simple de Administración de Red.

SQL: Lenguaje de consulta estructurado.

SSH: Intérprete de órdenes segura.

SSI: Conjunto de directivas que se escriben en las páginas HTML y que se evalúan en el servidor web.

SSID: Nombre de una red inalámbrica (Wi-Fi).

SSL: Capa de conexión segura.

TCP: Protocolo de Control de Transmisión.

TUN/TAP: Dispositivos virtuales del núcleo de la red.

UDP: Protocolo de datagrama de usuario.

UNIX: Sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969.

URL: Localizador de recursos uniforme.

VLAN: Red de área local virtual.

VPN: Red privada virtual.

WEBDAV: Web Distributed Authoring and Versioning.

WEP: Wired Equivalent Privacy.

WI-FI: Mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

WIMAX: Interoperabilidad mundial para acceso por microondas.

WISP: Wireless Internet Service Provider.

WLAN: Wireless Local Area Network.

WPA: Wi-Fi Protected Access.

XML: Lenguaje de marcas extensible.