ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

Estudio de Portales Cautivos de gestión de acceso Inalámbrico a Internet de la ESPOCH

TESIS DE GRADO

Previa a la obtención del título de

INGENIERO EN SISTEMAS INFORMÁTICOS

Presentado por:

Johanna Morayma Solano Jiménez.

Mercedes Beatriz Oña Garcés.

RIOBAMBA – ECUADOR

2009

Al Ing. Daniel Haro
Ing. Jorge Menéndez.
Ing. Byron Vaca.
Ing. Gonzalo Allauca.

Colaboradores de tesis; por su ayuda para la realización del presente trabajo de investigación.

A mis padres, mi madre Morayma Jiménez, que durante todo este tiempo ha estado junto a mí apoyándome para superar esta meta, con su comprensión y palabras de aliento. A mis hermanos Deyci, Heyler, Jefferson a pesar de su distancia siempre estuvieron apoyandome, mi sobrinita Leslie, mi felicidad de seguir adelante. Papito adorado, mi angelito, cada una de las letras de este trabajo son para ti.

Johanna Solano Jiménez

A Dios por llenar mi vida de bendiciones, a mis padres por su apoyo, dedicación y confianza incondicional, a mis hermanos por su inmenso cariño por su amistad, a la bendición más hermosa de mi vida mi hijo Diogo Matías porque con su amor, ternura y comprensión ha sido mi motivación principal, a René por su paciencia, por su apoyo, por sus consejos, por su amor y a todas aquellas personas que de una u otra manera me han brindado su apoyo absoluto e incondicional para lograr que mis sueños se hagan realidad.

Gracias los quiero mucho. Dios los bendiga siempre.

Mercedes Oña Garcés.

FIRMAS DE RESPONSABILIDADES

NOMBRE	**FIRMA**	**FECHA**
Dr. Romeo Rodríguez **DECANO DE LA FIE**	…….	……
Ing. Iván Menes **DIRECTOR DE ESCUELA**	……..	……
Ing. Daniel Haro **DIRECTOR DE TESIS**	…….	……
Ing. Jorge Menéndez **MIEMBRO DEL TRIBUNAL**	…….	……
Ing. Carlos Rodríguez **DIR. CENTRO DE DOCUMENTACIÓN**	…….	……
NOTA DE LA TESIS	…….	

"Nosotras Johanna Morayma Solano Jiménez y Mercedes Beatriz Oña Garcés, somos responsables de las ideas, doctrinas y resultados expuestos en esta tesis, y el patrimonio intelectual de la tesis de Grado pertenece a la ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO".

----------	**----------**
Johanna Morayma Solano Jiménez	Mercedes Beatriz Oña Garcés.

INDICE DE ABREVIATURAS

AAA: Authentication, Authorization and Accounting.

ACL: Access Control List.

AP: Access Point.

ASCII: American Standard Code for Information Interexchange

BACKUP: Copia de seguridad.

BSS: Conjunto de Servicio Básico.

BSSID: Basic Service Set Identifier.

CHAP: Método de Autenticación.

CGI: Common Gateway Interface.

CGI2: Common Gateway Interface II.

DHCP: Protocolo de Configuración Dinámica.

DNS: Domain Name System.

EAP: Extensible Authentication Protocol**.**

ESSID: Identificador del conjunto de servicio extendido.

FREERADIUS: Realiza la autenticación.

HOST: Dirección IP.

HTTP: Protocolo de Transferencia de Hipertexto.

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos.

LAN: Red Área local.

IP: Internet Protocolo.

MAC: Medium Access Control.

MD5: Algoritmo de cálculo

NAS: Envía paquetes.

NAS1: Envia paquetes.

NMPEC: Network Management Private Enterprise Code.

OSI: Open System Interconnection.

PAP: Password Authentication Protocol.

PCI: Versión de una red Inalámbrica.

PCMCIA: Versión de una red Inalámbrica.

PDA: Asistente Digital Personal.

RADDB: Directorio de configuración del Radius.

RADIUS: Remote Authentication Dial IN.

RADIUSD.CONF: Archivo de configuración del servidor FreeRadius.

ROOT: Nombre convencional de la cuenta de usuario.

SSID: Service Set IDentifier.

SSL: Encriptación.

Spoofing: Técnicas de suplantación de identidad.

TKIP: Protocolo de Integridad de Clave Temporal.

UDP: Protocolo de Datagrama de Usuario.

UL / DL: Velocidades de transmisión de datos por usuario.

USB: Bus universal en serie.

UTC: Tiempo Universal Coordinado.

VLAN: Red de área local virtual.

VPN: Red Privada Virtual.

VSA: Atributos específicos del fabricante.

WEP: Wired Equivalent Privacy.

WPA: WI-FI Protected Access.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

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

El uso de WLAN ha crecido exponencialmente es por eso que las instituciones buscan formas de hacer más eficientes sus redes actuales, tanto en aspectos de seguridad como con el aprovechamiento de los recursos disponibles. Dentro de este contexto, se vuelve necesario emplear mecanismos para administrar de forma eficiente el recurso de red disponible para el correcto funcionamiento de los diferentes servicios dentro de la red, como el empleo de mecanismos de control de acceso a usuarios o autenticación.

La Escuela Superior Politécnica de Chimborazo posee una infraestructura de red WLAN muy organizada la cual proporciona servicios a los usuarios a través de la autenticación WEP que es considerada como no segura en base al estudio de esta metodología realizado en el presente documento.

El estudio para la implementación de un portal cautivo método de control de acceso a usuarios de internet de la ESPOCH es el tema central de este estudio cuyo enfoque se da en el análisis de herramientas que permiten la autenticación de usuarios y el acceso a internet.

La estructura de este documento se encuentra conformada por cuatro capítulos los cuales se detallan a continuacion:

El capítulo I Marco Referencial, contempla en principio la descripción de las razones fundamentales para efectuar el estudio de portales cautivos y que objetivos nos permitirá alcanzar.

En segunda instancia el capítulo II Marco teórico, da una referencia teórica sobre las redes inalámbricas, sus componentes, funcionamiento, amenazas contra su seguridad, los métodos de protección, este capítulo también presenta información en general de los portales cautivos como su funcionamiento, tipos, componentes.

El capítulo III contiene el análisis comparativo de los portales cautivos seleccionados para el estudio en base al cual se determinó el mejor para su implementación en la WLAN de la ESPOCH.

En el capítulo IV, al tener ya un portal cautivo seleccionado se detallarán los procesos realizados en el proyecto para su implementación. Finalmente se exponen las conclusiones y recomendaciones que ha dejado el proyecto para dar claridad a los conceptos desarrollados y servir de base a futuros desarrollos de la misma área.

CAPITULO I

1. MARCO REFERENCIAL

1.1. ANTECEDENTES

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

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

Un portal cautivo sencillo obliga al visitante a que por lo menos mire (así no lea) y acepte las políticas de uso, pulsando un botón en la página. Supuestamente esto puede absolver al proveedor del servicio de cualquier culpa por el uso anormal y/o ilegal del servicio. En otros portales se provee publicidad para el proveedor y/o sus patrocinadores y el usuario deberá hacer clic en la publicidad o cerrar la ventana en las cuales aparecen estos comerciales antes de continuar con el uso del servicio. En algunos casos se debe ingresar una identificación y/o clave asignada antes de acceder a Internet, con el objetivo de desalentar a quienes quieran usar estos servicios para usos no autorizados.

La falta de gestión del Internet inalámbrico provoca el uso indebido del mismo lo que puede ocasionar problemas legales al proveedor por lo cual el siguiente anteproyecto proporcionará a la ESPOCH la absolución de responsabilidad de acciones realizadas por los usuarios del internet inalámbrico gratuito, al presentar el contrato de uso de internet a los usuarios al momento de iniciar la conexión, además se asignará programación que limite el tamaño de los archivos a descargar o la velocidad a la cual se descargan los mismos, permitiendo asignar a los usuarios tiempo de navegación y ancho de banda según lo considere el administrador del Portal Cautivo.

1.2. JUSTIFICACIÓN

Un portal cautivo es un conjunto de páginas web que emergen en cualquier petición que hagan los clientes, para identificar y tener el control sobre los usuarios. En este caso analizaremos los Portales Cautivos (AirMarshal y Chillispot).

AirMarshal contiene gran cantidad de características y permite asignar tiempo de navegación al usuario, Chillispot es configurable en modo texto. Se escogerá el mejor

en características y que se ajuste al problema a resolver según el análisis comparativo que se realice.

Este proyecto surge por la necesidad de poder brindar seguridad y gestionar el acceso indebido a Internet en una red Inalámbrica utilizando Portales Cautivos. En la cual utilizaremos software libre bajo la distribución Centos5 de Linux ya que es una plataforma estable bajo la cual se encuentran los Servidores de la ESPOCH.

En el caso de las tecnologías inalámbricas, caracterizadas por su extrema dependencia de las condiciones del entorno y su baja eficiencia en escenarios con múltiples dispositivos móviles, el acceso a Portales Cautivos cobra un especial interés.

De este modo, nos aseguramos que las aplicaciones que requieran un tiempo de latencia bajo o un mayor consumo de ancho de banda, realmente dispongan de los recursos suficientes cuando los soliciten. Por ello, una de las principales metas de Portales Cautivos es la priorización, esto es, el dar más relevancia a unas conexiones frente a otras.

1.3. OBJETIVOS

OBJETIVO GENERAL

- Investigar los Portales Cautivos, que permitan gestionar el acceso a la Red Inalámbrica de la ESPOCH.

OBJETIVOS ESPECÍFICOS

- Analizar problemas de seguridad en la Red Inalámbrica de la ESPOCH.
- Estudio de los Portales Cautivos (AirMarshal y Chillispot) y evaluación comparativa de los mismos
- Implementar un Portal Cautivo en la Red inalámbrica de la ESPOCH.
- Desarrollar un Interfaz web de configuración en el Portal Cautivo seleccionado.

1.4. HIPÓTESIS

La Implementación de un Portal Cautivo en la Red Inalámbrica de la ESPOCH mejorará la gestión del acceso al Internet.

CAPITULO II

2. MARCO TEÓRICO

2.1. INTRODUCCIÓN A REDES INALÁMBRICAS

Desde hace relativamente poco tiempo, se está viviendo lo que puede significar una revolución en el uso de las tecnologías de la información. Esta revolución puede llegar a tener una importancia similar a la que tuvo la adopción de Internet por el gran público.

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de

computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada.

También es útil para hacer posibles sistemas basados en plumas. Pero la realidad es que esta tecnología está todavía en pañales y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 2 Mbps, las redes cableadas ofrecen velocidades de 10 Mbps y se espera que alcancen velocidades de hasta 100 Mbps. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, y pensando futuristamente se espera que las redes inalámbricas alcancen velocidades de solo 10 Mbps.

Existen dos amplias categorías de Redes Inalámbricas:

- *De Larga Distancia*.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN); sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps.
- *De Corta Distancia*.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre sí, con velocidades del orden de 280 Kbps hasta los 2 Mbps.

2.2. 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.*

- **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 *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.

- **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.

- **Estaciones**

  Las estaciones son dispositivos computacionales que poseen una interfaz de red inalámbrica. Típicamente estos dispositivos son *Notebooks, PDA,* etc. pero pueden ser computadoras normales en lugares en que se ha optado no realizar

un cableado de red y utilizar tecnologías inalámbricas solamente. Adicionalmente varios fabricantes de dispositivos electrónicos están utilizando 802.11 para comunicar dispositivos no computacionales.

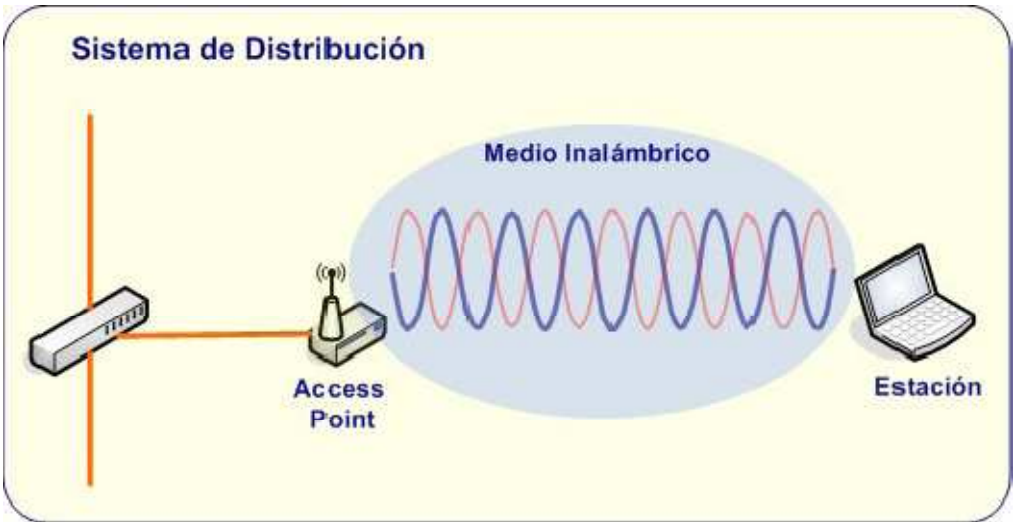


Figura II.1. Componentes de la infraestructura inalámbrica

2.3. FUNCIONAMIENTO DE UNA RED INALÁMBRICA.

El funcionamiento de una red inalámbrica ver figura II.2 es muy similar al funcionamiento de los teléfonos móviles.

Por un lado, se dispone de equipos de usuario: cualquier ordenador con una tarjeta de red inalámbrica instalada (en sus diferentes versiones: USB, PCMCIA, PCI…). Por el otro, se encuentran los equipos de acceso (denominados también puntos de acceso), que son los encargados de proporcionar la "cobertura" a los equipos de usuario y permitir a los usuarios acceder a los distintos recursos de la red (páginas web, servidores de ficheros…)

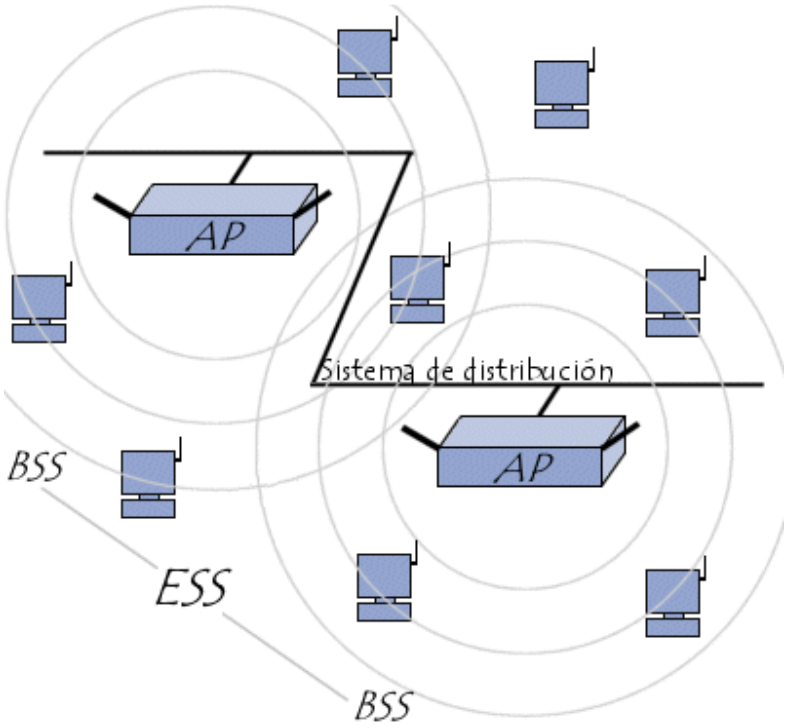


Figura II.2 Funcionamiento de la red inalámbrica

La configuración formada por el Access Point y las estaciones ubicadas dentro del área de cobertura se llama *conjunto de servicio básico* o BSS. Estos forman una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS) que es un identificador de 6 bytes (48 bits).

Cuando una estación se une a una célula, envía una *solicitud de sondeo* a cada canal. Esta solicitud contiene el ESSID (identificador del conjunto de servicio extendido), que la célula está configurada para usar y también el volumen de tráfico que su adaptador inalámbrico puede admitir. Si no se establece ningún ESSID, la estación escucha a la red para encontrar un SSID.

Cada punto de acceso transmite una señal en intervalos regulares (diez veces por segundo aproximadamente). Esta señal, que se llama señalización, provee información

de su BSSID, sus características y su ESSID, si corresponde. El ESSID se transmite automáticamente en forma predeterminada, pero se recomienda que si es posible se deshabilite esta opción.

Cuando se recibe una solicitud de sondeo, el punto de acceso verifica el ESSID y la solicitud del volumen de tráfico encontrado en la señalización. Si el ESSID dado concuerda con el del punto de acceso, éste envía una respuesta con datos de sincronización e información sobre su carga de tráfico. Así, la estación que recibe la respuesta puede verificar la calidad de la señal que envía el punto de acceso para determinar cuán lejos está. En términos generales, mientras más cerca un punto de acceso esté, más grande será su capacidad de transferencia de datos.

Por lo tanto, una estación dentro del rango de muchos puntos de acceso (que tengan el mismo SSID) puede elegir el punto que ofrezca la mejor proporción entre capacidad de carga de tráfico y carga de tráfico actual.

2.4. SEGURIDAD EN REDES INALÁMBRICAS

AMENAZAS DE SEGURIDAD EN REDES INALÁMBRICAS

El acceso sin necesidad de cables, la razón que hace tan populares a las redes inalámbricas, es a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere.

Cualquier equipo que se encuentre a 100 metros o menos de un punto de acceso, podría tener acceso a la red inalámbrica.

La tabla II.1 presenta las amenazas de seguridad más relevantes en redes inalámbricas.

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

Tabla II.1 Amenazas de seguridad más relevantes a redes inalámbricas

Fuente:

MÉTODOS PARA GARANTIZAR SEGURIDAD EN REDES INALÁMBRICAS

Para poder considerar una red inalámbrica como segura, debería cumplir con los siguientes requisitos:

- Las ondas de radio deben confinarse tanto como sea posible. Esto es difícil de lograr totalmente, pero se puede hacer un buen trabajo empleando antenas

direccionales y configurando adecuadamente la potencia de transmisión de los puntos de acceso.

- Debe existir algún mecanismo de autenticación en doble vía, que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que el cliente está autorizado para acceder a ella.
- Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva.

Existen varios métodos para lograr la configuración segura de una red inalámbrica; cada método logra un nivel diferente de seguridad y presenta ciertas ventajas y desventajas. Se hará a continuación una presentación de cada uno de ellos.

Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica.

Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas. Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.

- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 bytes en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.
- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un sniffer, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador, empleando programas tales como AirJack6 o WellenReiter, 7 entre otros. De este modo, el atacante puede hacerse pasar por un cliente válido.
- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

Wired Equivalent Privacy (WEP)

El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante cifrado. WEP opera a nivel 2 del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

En líneas generales *WEP* requiere de los siguientes datos de entrada para realizar el cifrado:

- Los datos que la trama deberá transportar como carga o *payload.* Estos son provistos por la capa superior del stack de protocolos.
- Una clave secreta, utilizada para cifrar la trama. Dependiendo de la implementación, las claves pueden ser especificadas como una cadena de bits o por el número de clave, ya que *WEP* permite almacenar cuatro claves de forma simultánea.
- Un *Vector de Inicialización (IV),* utilizado junto con la clave secreta en la transmisión del marco.

Luego de realizar el proceso de cifrado, *WEP* ofrece como resultado: Una trama cifrada, lista para transmitir sobre redes no confiables, con suficiente información en la cabecera para permitir su descifrado en el receptor del marco.

Como se ve en la Ilustración, el driver y la interfaz de hardware son responsables de procesar los datos y de enviar la trama cifrada utilizando la siguiente secuencia:

1. La trama 802.11 entra en la cola de transmisión. Esta trama consiste en una cabecera y en el *payload. WEP* protege solamente el *payload* y deja la cabecera intacta.

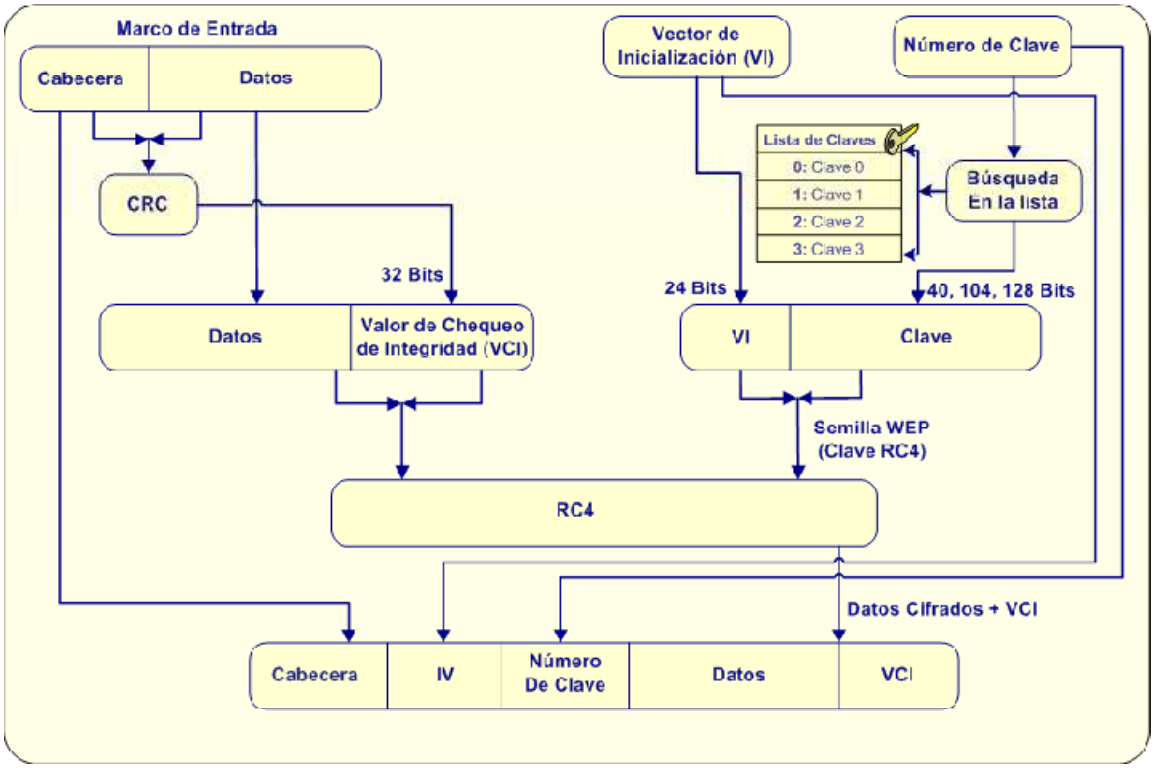


Figura II.3. Operaciones que lleva a cabo WEP

2. Se calcula un V*alor de Chequeo de Integridad (ICV)* sobre el *payload* original. EL *Chequeo de Secuencia de la Trama (FCS)* no ha sido calculado en este punto, por lo que no se incluye en el cálculo del *ICV.* El *ICV* es un *CRC*[1], y por lo tanto es predecible y *criptográficamente inseguro* para chequeos de integridad.

3. La *Clave de Cifrado de la Trama (FEK) o WEP seed* se ensambla en este punto, esta consta de dos partes: la *clave secreta* y el v*ector de inicialización (IV)*. Los *stream ciphers* producen el mismo flujo de salida para la misma clave, por lo que el *IV* se utiliza para producir flujos de salida distintos para cada trama transmitida y se coloca como prefijo de la clave secreta. El estándar 802.11 no establece ninguna restricción para el algoritmo usado para elegir los *IV.* Algunas

[1] *Cyclic Redundancy Check,* Chequeo de Redundancia Cíclico.

implementaciones asignan los *IV* de forma secuencial, otras lo asignan a través de un algoritmo pseudoaleatorio. La selección del *IV* tiene algunas implicaciones de seguridad, ya que una "pobre" selección en el *IV* puede comprometer la clave.

4. La *Clave de Cifrado de la Trama* se usa como clave *RC4* para cifrar el *payload* de la Trama original del paso 1 y el *ICV* del paso 2. El proceso de cifrado casi siempre es realizado con hardware especializado para el algoritmo *RC4* en la placa inalámbrica.
5. Como último paso, se ensambla la trama a transmitir formada por el *payload cifrado,* la cabecera original, y una cabecera *WEP,* formada por el *IV y número de clave*. Una vez ensamblada la nueva trama se calcula el *FCS* y
6. se realiza la transmisión. El descifrado de la trama se realiza en orden inverso.

El algoritmo WEP resuelve aparentemente el problema del cifrado de datos entre emisor y receptor. Sin embargo, existen dos situaciones que hacen que WEP no sea seguro en la manera que es empleado en la mayoría de aplicaciones:

- La mayoría de instalaciones emplea WEP con claves de cifrado estáticas (se configura una clave en el punto de acceso y no se la cambia nunca, o muy de vez en cuando). Esto hace posible que un atacante acumule grandes cantidades de texto cifrado con la misma clave y pueda intentar un ataque por fuerza bruta.
- WEP no ofrece servicio de autenticación. El cliente no puede autenticar a la red, ni al contrario; basta con que el equipo móvil y el punto de acceso compartan la clave WEP para que la comunicación pueda llevarse a cabo.

Existen en este momento diversas herramientas gratuitas para romper la clave secreta de enlaces protegidos con WEP. El primer programa que hizo esto posible fue WEPCrack, que consiste en una serie de scripts escritos en lenguaje Perl diseñados para analizar un archivo de captura de paquetes de un sniffer. La herramienta AirSnort9 hace lo mismo, pero integra las funciones de sniffer y rompedor de claves, y por lo tanto es más fácil de usar. Airsnort captura paquetes pasivamente, y rompe la clave WEP cuando ha capturado suficientes datos.

VPN

Una red privada virtual (Virtual Private Network, VPN) emplea tecnologías de cifrado para crear un canal virtual privado sobre una red de uso público. Las VPN resultan especialmente atractivas para proteger redes inalámbricas, debido a que funcionan sobre cualquier tipo de hardware inalámbrico y superan las limitaciones de WEP.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN.

Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

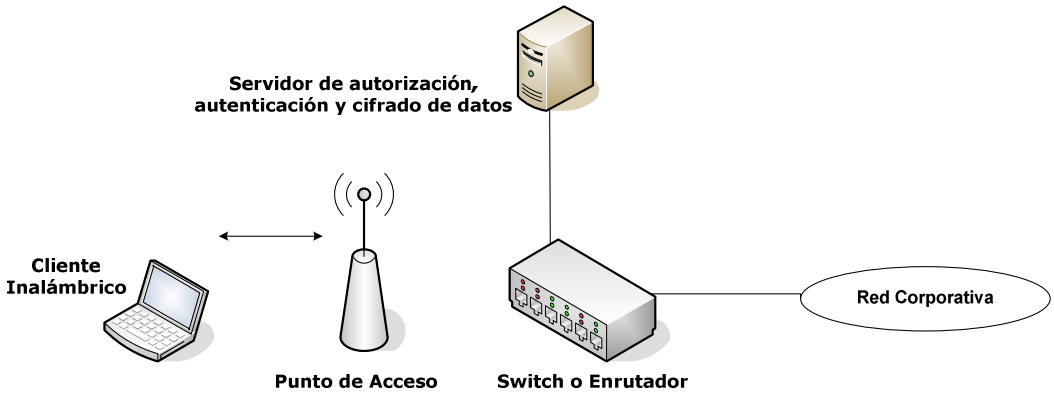


Figura II.4 Estructura de una VPN para acceso inalámbrico seguro.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes. Dado que los datos se cifran en un nivel superior del modelo OSI, no es necesario emplear WEP en este esquema.

La utilización de las VPN añade bastante seguridad a las redes inalámbricas pero tiene ciertas desventajas una de ellas es la económica pues cada túnel tiene un costo para la empresa y cuando se trata de proteger a cientos o miles de usuarios de una red inalámbrica WIFI, las VPN se convierten en extremadamente costosas. Otro inconveniente es que las VPN han sido pensadas y diseñadas para conexiones "dial-up" punto a punto, pero las redes inalámbricas WIFI transmiten ondas de RF (irradian) por el aire que es un medio compartido.

802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red.11 El protocolo fue inicialmente creado por la IEEE para uso en redes de área local

alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

El protocolo 802.1x involucra tres participantes:

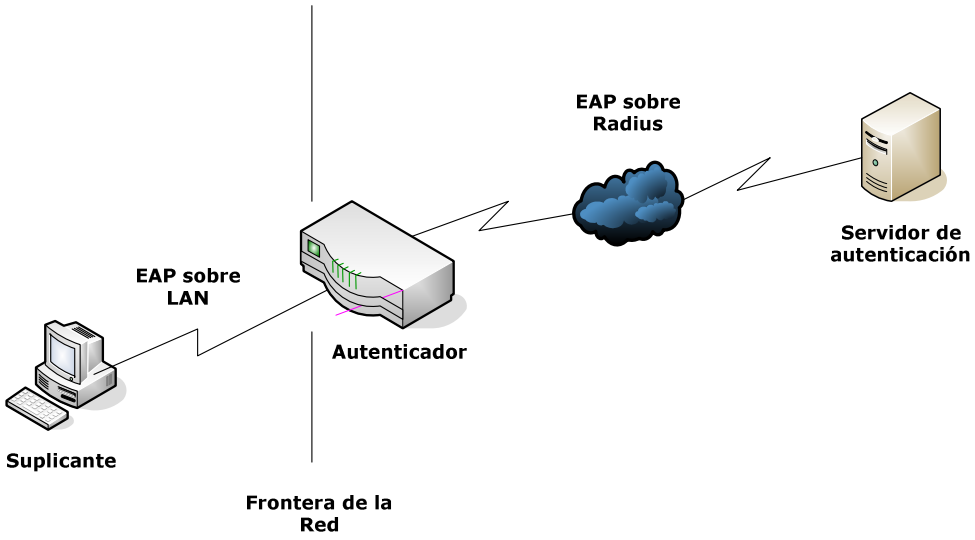


Figura II.5 Arquitectura de un sistema de autenticación 802.1x.

- El suplicante, o equipo del cliente, que desea conectarse con la red.
- El servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto...) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente

permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS.

WPA (WI-FI Protected Access)

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación.

Para solucionar el problema de cifrado de los datos, WPA propone un nuevo protocolo para cifrado, conocido como TKIP (Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre punto de acceso y cliente cada cierto tiempo, para evitar ataques que permitan revelar la clave. Igualmente se mejoraron los algoritmos de cifrado de trama y de generación de los IVs, con respecto a WEP.

El mecanismo de autenticación usado en WPA emplea 802.1x y EAP. Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- Modalidad de red empresarial: Para operar en esta modalidad se requiere de la existencia de un servidor RADIUS en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

- Modalidad de red casera, o PSK (Pre-Shared Key): WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

La principal debilidad de WPA es la clave compartida entre estaciones. Cuando un sistema basa su seguridad en una contraseña siempre es susceptible de sufrir un ataque de fuerza bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería plantear mayores problemas. Se debe pensar que hay un momento de debilidad cuando la estación establece el diálogo de autenticación. Este diálogo va cifrado con las claves compartidas, y si se entienden entonces se garantiza el acceso y se inicia el uso de claves dinámicas. La debilidad consiste en se conoce el contenido del paquete de autenticación y conocemos su valor cifrado. Ahora lo que queda es, mediante un proceso de ataque de diccionario o de fuerza bruta, intentar determinar la contraseña.

2.5. SEGURIDAD EN LA RED INALÁMBRICA DE LA ESPOCH

La ESPOCH utiliza como método de seguridad en su red inalámbrica la autenticación WEP como ya se indicó anteriormente este método no proporciona un alto nivel de seguridad y confidencialidad, entre sus deficiencias tenemos las siguientes:

- No provee ningún mecanismo para establecer claves sobre un medio inseguro, por lo que las claves son compartidas por todas las estaciones en un *BBS* y a veces entre varios *BBS.*
- Utiliza un algoritmo de cifrado sincrónico sobre un medio en el que es muy difícil asegurar la sincronización durante una sesión completa.
- Usa una clave por marco transmitido, concatenado el *IV* directamente con la *PSK* para producir una clave para *RC4* para resolver el problema anteriormente planteado*.* Esto expone la clave maestra a ataques del tipo *FMS (Fluhrer-Mantin-Shamir).*
- Es muy limitado el espacio de claves debido a que la clave maestra es configurada de forma manual y es estática, y a que el *IV* sólo tiene 24 bits de largo. A causa de esto en una red con tráfico medio se produce repetición de claves cada aproximadamente 5 horas.
- La reutilización de claves es altamente probable, debido a que 802.11 especifica que el recambio del *IV* es opcional.
- El *ICV* no protege la integridad de la cabecera 802.11, permitiendo ataques de redirección.
- No tiene protección contra ataques de repetición.

Un Portal Cautivo es la combinación de algunos de los métodos revisados anteriormente, el siguiente capítulo está destinado a estudiar de manera más profunda este método que proporciona un alto grado de seguridad a las WLAN.

2.6. PORTALES CAUTIVOS

INTRODUCCIÓN A PORTALES CAUTIVOS

Un portal cautivo es un servicio web para el acceso a Internet. Con él se recoge todo el tráfico http y se re direccionan estas peticiones a un conjunto de páginas especiales, previamente definidas, como paso previo para permitir al usuario la navegación normal.

Es decir, antes de que el usuario pueda salir a Internet, está obligado a pasar por determinadas páginas en donde, normalmente, deberá autenticarse y se le muestra información importante de diversa índole, como puede ser instrucciones de uso, recomendaciones o acuerdos de utilización del servicio de acceso a Internet. Una vez que el usuario cumple con los requisitos exigidos en estas páginas iníciales, se permite su navegación a Internet con toda normalidad, siempre y cuando los sitios que quiera visitar estén permitidos.

A primera vista este servicio se asemeja bastante al trabajo que realiza un cortafuegos, firewall, y a las que realiza un proxy, pero en la práctica un portal cautivo no sustituye a ninguno de ellos. Pensado para gestionar el acceso a Internet, su ámbito de actuación está limitado al tráfico http, peticiones que atiende en función de la autenticación válida del usuario que las solicita y de reglas que permiten o prohíben alcanzar los sitios solicitados, todo ello en un entorno dirigido a través de páginas web

predefinidas. Los portales cautivos operan detrás del firewall, cuando estos están presentes y pueden combinarse con el trabajo de proxy.

Por otra parte, la facilidad de configuración de este servicio permite crear y personalizar las páginas que se muestran al usuario y Administrador, sin que sea imprescindible contar con programadores.

La idea del portal cautivo surge y se desarrolla en Linux, plataforma en la que encuentra el más amplio catálogo de este servicio. Aunque en menor medida, es también fácil encontrar desarrollos en entorno Windows.

Para montar este servicio se necesita un equipo dimensionado al número de conexiones que se esperan, con al menos dos tarjetas de red, sistema operativo y un programa de portal cautivo. Para el equipo, no es imprescindible presupuestar un ordenador tipo servidor, ya que no es un servicio que tenga un elevado con-sumo de recursos de proceso.

Un portal cautivo proporciona un servicio de control de acceso web que si bien está orientado a redes abiertas, normalmente asociadas a enlaces inalámbricos, pueden aplicarse en multitud de situaciones: eventos, aulas, puntos de acceso tipo kiosco, puntos de venta-expositores, oficinas remotas…

Un portal cautivo resuelve de manera sencilla y limpia el acceso a Internet, facilitando la conexión de usuarios externos y brinda la oportunidad de ofrecer nuevas aplicaciones de conexión que en entornos con pocos recursos técnicos, no resultan viables. La facilidad de instalación, configuración y uso, está propiciando su rápida difusión.

TIPOS DE PORTALES CAUTIVOS

Hay dos grandes tipos de portales cautivos y un subtipo. El que hace falta un nombre de usuario y contraseña (una cuenta) y en el que simplemente se debe aceptar las condiciones de ingreso. El subtipo que puede ser de las dos es la variante "walled garden". Esta última es la que limita a un grupo de sitios web pero no permite el acceso a internet en general (o a ciertos puertos.) Un ejemplo complejo de todo esto sería un WiFi Access Point en un aeropuerto que permite ver información de vuelos, anuncios y sitios de anunciantes, sin tener que ingresar un usuario y contraseña. Pero, con una cuenta se puede ingresar a la web en general, inclusive usar algún mensajero instantáneo y bajar correo con Outlook Express.

FUNCIONAMIENTO DE PORTALES CAUTIVOS

Una herramienta común de autenticación utilizada en las redes inalámbricas es el portal cautivo. Este utiliza un navegador web estándar para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso Aceptable) a los usuarios antes de permitir el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC).

Para comenzar, el usuario abre su computadora portátil y selecciona la red. Su computadora solicita una dirección mediante DHCP y le es otorgada. Luego usa su navegador web para ir a cualquier sitio en Internet.

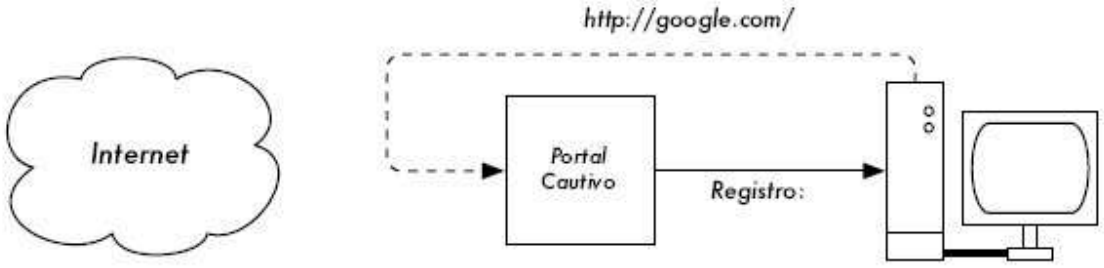


Figura II.6. El usuario solicita una página web y es redireccionado.

En lugar de recibir la página solicitada, al usuario se le presenta una pantalla de registro. Esta página puede solicitarle al usuario que ingrese su nombre de usuario y una contraseña, simplemente oprime el botón de "registro" (login). El punto de acceso u otro servidor en la red verifica los datos. Cualquier otro tipo de acceso a la red se bloquea hasta que se verifiquen las credenciales.

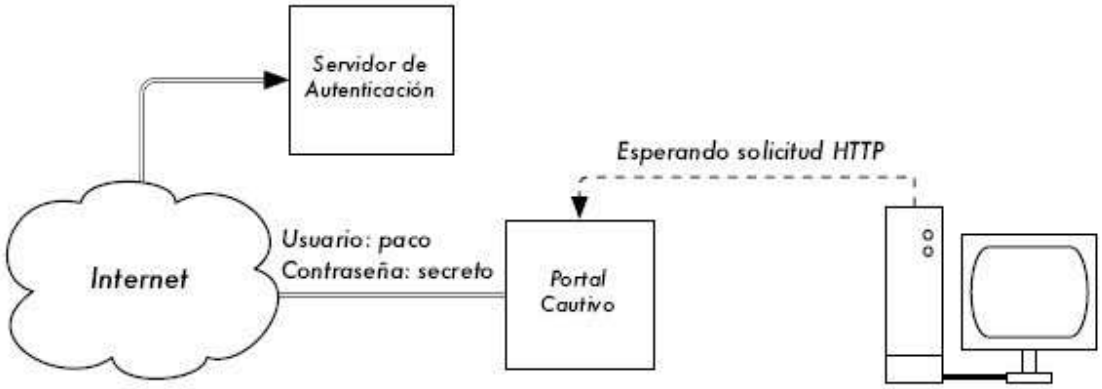


Figura II.7 Verificación de Credenciales

Una vez que el usuario ha sido autenticado, se le permite el acceso a los recursos de la red, y en general es re direccionado al sitio web que solicitó originalmente.

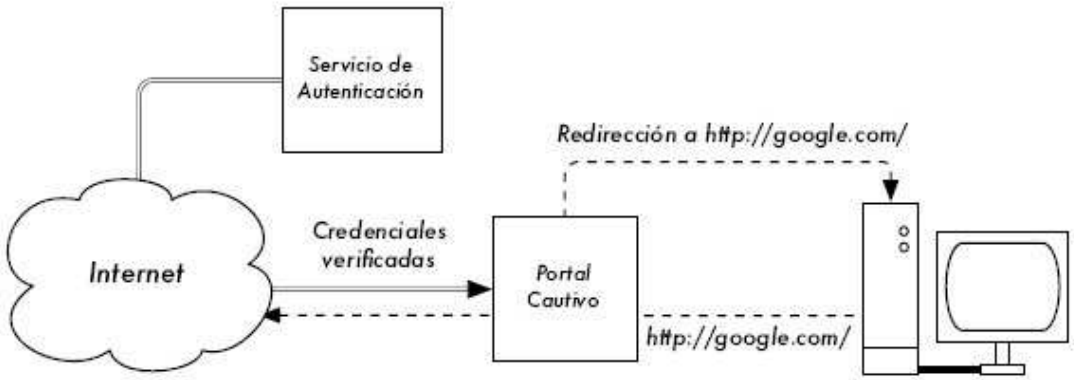


Figura II.8 Se permite acceso al resto de la red

Los portales cautivos no proveen encriptación para los usuarios de redes inalámbricas, en su lugar confían en las direcciones MAC e IP del cliente como identificadores únicas. Si bien esto no es necesariamente muy seguro, muchas implementaciones van a solicitar que el usuario se re-autentique periódicamente. Esto puede hacerse automáticamente, minimizando una ventana emergente (pop-up) del navegador, cuando el usuario se registra por primera vez.

2.7. PROTOCOLO RADIUS

RADIUS es un protocolo de control de acceso que autentica usuarios a través de un método muy común denominado genéricamente *desafío/respuesta.* El proceso que lleva a cabo se denomina *AAA.*

El proceso de *AAA* se puede sintetizar en las siguientes preguntas que realiza el servidor de acceso al cliente:

- ¿Quién eres?
- ¿Qué servicios estoy autorizado a darte?
- ¿Qué hiciste con los servicios mientras los usabas?

La *Autenticación* es el proceso de verificar la identidad que ha declarado un cliente (máquina o persona). Uno de los métodos más comunes para realizar esta tarea es utilizar un nombre de usuario y una contraseña. El objetivo principal de este proceso es formar una *relación de confianza* entre el cliente y el servidor.

El proceso de *Autorización* consta de un conjunto de reglas para decidir qué puede hacer un usuario autenticado en el sistema. Las reglas son definidas por los administradores del sistema.

El *Registro* es el proceso que documenta el uso de los recursos hecho por los usuarios que acceden al sistema. Los datos recabados por el proceso de *Registro* se pueden utilizar para controlar autorizaciones realizadas, cobrar la utilización de recursos, medir tendencias en el uso de recursos, y para realizar actividades relacionadas con la planificación del crecimiento.

Las características generales del protocolo, definidas en la *RFC2865*, son:

- Usa un modelo *Cliente/*Servidor, donde el modelo de seguridad que se utiliza se denomina *hop-by-hop,* y se basa en un secreto compartido entre el *NAS1 y* el *Servidor* que no se transmite en la red.
- Utiliza *UDP/IP* para las conexiones.
- Es un protocolo *stateless*, es decir sin estado.
- Soporta una gran variedad de métodos de autenticación, que otorgan una gran flexibilidad. Soporta *PAP, CHAP, EAP, Unix,* entre otros.
- El protocolo es *extensible*. Todas las transacciones utilizan un trío de valores *Atributo-Longitud-Valor*, y permite agregar definiciones de valores sin comprometer el funcionamiento de las implementaciones existentes.

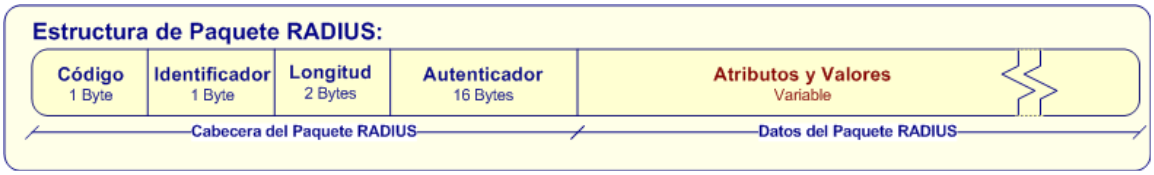


Figura II.9 Estructura del paquete Radius

El protocolo se comunica a través de los puertos UDP/1812 y UDP/1813. En la figura II.9 se puede apreciar la estructura del paquete *RADIUS.* En la Tabla II.2 se puede observar el significado de los campos del paquete *RADIUS.*

Campo	Descripción
Código	Este campo es el que distingue el tipo de mensaje *RADIUS.* Los paquetes con código inválido se descartan. Los códigos permitidos son: *Access-Request (1), Access-Accept (2), Access-Reject (3), Accounting-Request (4), Accounting-Response (5), Access-Challenge (11), Status-Server (12), Status-Client (13), Reservado (255).*
Identificador	Este valor se utiliza para relacionar una respuesta a una solicitud. También permite que el servidor *RADIUS* detecte las solicitudes duplicadas que se realizan en un corto período de tiempo, comparando la dirección *IP* y el puerto *UDP* origen, junto con el identificador.
Longitud	Indica la longitud (incluye *Código, Identificador, Longitud, Autenticador y Datos)* y si el paquete es más largo se descarta el excedente y si el paquete es más corto se descarta. Las longitudes válidas oscilan entre 20 *bytes y*

	4096 bytes.
Autenticador	Con este valor se verifica la integridad de los datos. Existen dos tipos diferentes de valores: *Solicitud y Respuesta.* El primer valor se calcula de forma aleatoria. El segundo valor se calcula con el algoritmo *MD5* en función de los siguientes parámetros: *Código, Identificador, Longitud, Autenticador de la solicitud, Datos, Secreto).*
Atributos y Valores	Este campo de longitud variable es el que contiene los pares *atributo-valor* que intercambia el servidor con el *NAS.*

Tabla II.2 Descripción de los campos de un paquete RADIUS.

Fuente:

En los procesos de *Autenticación y Autorización* son relevantes cuatro tipos de paquetes: *Access-Request, Access-Accept, Access-Reject, y Access-Challenge.* El primer paso del proceso de autenticación lo ejecuta el usuario.

El cliente solicita acceso a un servicio particular al enviar al *Servidor RADIUS* un paquete del tipo *Access-Request*. El paquete debe contener ciertos atributos que son significativos para el proceso de autenticación. Por ejemplo, debe contener atributos que identifiquen al *NAS (NAS-IP-Address y/o NAS-Identifier*), la contraseña del usuario *(User-Password o CHAP-Password)* y debería contener nombre de usuario *(User-Name)* y el puerto de conexión *(NAS-Port y/o NAS-Port-Type*). El paquete *Access-Request* puede contener atributos adicionales. Si el *atributo User-Password* está presente, no debe transmitirse en texto plano, sino utilizando un *hash MD5.* Al recibir el paquete, el servidor debe determinar y comunicar si el usuario tiene permitido el acceso a través del *NAS* y al tipo de servicio que ha solicitado. Todos los paquetes válidos de este tipo

deben ser contestados por el servidor, ya sea con un paquete del tipo *Access-Accept,* del tipo *Access*-Reject o del tipo *Access-Challenge.*

Una vez que el servidor ha procesado un paquete tipo *Access-Request* y ha determinado que todos los atributos son aceptables y se puede conceder acceso al usuario, envía un paquete del tipo *Access-Accept*. Este paquete debe proveer la información necesaria para realizar configuración específica a fin de comenzar con la utilización del servicio. El campo *Autenticador* debe contener la respuesta correcta para el campo *Autenticador* de paquete tipo *Access-Request* que ha recibido previamente.

El servidor puede enviar al usuario un desafío que requiera de una respuesta para disminuir el riesgo de una autenticación fraudulenta. Si este es el caso se envía al cliente un paquete del tipo *Access-Challenge* al que el cliente debe responder con un paquete del tipo *Access-Request* que incluya los atributos apropiados. En el paquete *Access-Challenge* se pueden incluir uno o más atributos *Reply-Message* y un atributo *State*. Adicionalmente sólo se puede incluir alguno de los siguientes atributos: *Específicos-del-Fabricante*, *Idle-Timeout, Session-Timeout o Proxy-State.*

Si el servidor determina, al procesar el paquete *Access-Request*, que debe negar el acceso porque alguno de los atributos recibidos no es aceptable (por política de sistema, privilegios insuficientes u otro criterio), debe enviar un paquete del tipo *Access-Reject*. Este tipo de paquete puede incluir uno o más atributos *Reply-Message* con el texto que el *NAS* debe mostrar al usuario y uno o más atributos *Proxy-State.* No se permiten otro tipo de atributos. Los paquetes del tipo *Access-Reject* pueden ser enviados en cualquier instancia de una sesión, por lo que son muy útiles para aplicar límites de tiempo en la duración de la sesión.

Una vez que se lleva a cabo el proceso de autenticación puede empezar el proceso de *Accounting o* Registro, para esto usa el puerto 1813/*UDP*. El cliente (*NAS o Proxy Server)* envía un paquete del tipo *Accounting-Request* al *Servidor de Accounting*

RADIUS. Este servidor puede ser el mismo servidor RADIUS utilizado para los procesos de *Autenticación y Autorización* u otro servidor configurado para tal propósito.

Este paquete de tipo *Accounting*-Request, *denominado Accounting-Start,* transmite la información que se registrará como utilización del servicio por parte del usuario. Al recibir este paquete el servidor debe transmitir un paquete del tipo *Accounting-Response* si puede almacenar satisfactoriamente el contenido del paquete y no debe transmitir ninguna respuesta si existe algún tipo de falla en el proceso de almacenamiento. A excepción de los atributos *User-Password, CHAP-Password, Reply-Message y State,* se pueden enviar todos los atributos que pueden estar en un paquete *Access-Request o Access-Accept.* El paquete *Accounting-Request* debe contener el atributo *NAS-IP-Address y/o NAS-Identifier.* Si está presente en el paquete o si estuvo presente en el paquete *Access-Accept*, el atributo *Framed-IP-Address* debe contener la dirección *IP realmente* asignada al usuario.

Cuando el cliente finaliza una sesión envía un paquete *Accounting*-Request, denominado *Accounting-Stop*, que incluye las estadísticas de uso (duración de la sesión, volumen de datos transferidos, etc.). El servidor debe confirmar que pudo almacenar esta información con éxito enviando un paquete tipo *Accounting-Response*. El cliente debería reenviar el paquete *Accounting-Respose* hasta que el servidor confirme la operación de almacenamiento.

Como se puede apreciar en los procesos *AAA*, *RADIUS* transporta toda la información necesaria para llevar a cabo estos procesos en *Atributos. Los atributos se transmiten con el formato que se observa en la* figura II.10 y en la Tabla II.3

Figura II.10 Formato de Transmisión de Transmisión de Atributo Radius

Campo	Descripción
Tipo	Este valor especifica el "número de atributo" que lo define, estos números están definidos en las RFC2865 y RFC2866. El número 26 está designado para *Vendor Specific Attributes (VSA).* Los valores 192-223 están reservados para uso experimental, los valores 224-240 están reservados para uso de cada implementación específica y los valores 241-255 están reservados para uso futuro.
Longitud	Este valor indica la longitud del atributo transmitido, incluyendo los campos tipo, longitud y valor.
Valor	Este valor puede ser de longitud cero y puede tener los siguientes tipos de dato: *texto, cadena, dirección IP, número entero y tiempo.*

Tabla II.3 Formato de Atributos Radius

Fuente:

En la descripción del campo *valor* se especifican cinco tipos de dato soportados cuyo formato es:

- *Texto*: de 1 a 253 *bytes* que deben contener caracteres con codificación *UTF-8.* En lugar de enviarse con longitud cero debe omitirse el atributo.

- *Cadena:* de 1 a 253 *bytes* que deben contener *datos binarios*. En lugar de enviarse con longitud cero debe omitirse el atributo.
- *Dirección IP:* valor de 32 bits con el *byte* más significativo en primer lugar.
- *Número Entero:* valor de 32 bits sin signo con el *byte* más significativo en primer lugar.
- *Tiempo:* valor de 32 bits sin signo con el *byte* más significativo en primer lugar. Se debe codificar como el número de segundos desde el 01/01/1970 a las 00:00:00 UTC.

Muchas de las definiciones de atributos establecen un conjunto de valores posibles por *enumeración* para dicho atributo, el tipo de dato utilizado en esos casos es *número entero*.

El *Tipo 26* está reservado para uso de *Vendor Specific Attributes (VSA,* Atributos específicos del fabricante), y debe usar un formato especial para encapsular las definiciones de los atributos *VSA* dentro del campo *valor*. En la figura II.11 se muestra el formato de atributos VSA.

Figura II.11 Formato de Atributos VSA

Los sub-campos son similares a los campos de un atributo normal, salvo el sub-campo *ID Fabricante*. Este campo es un código de 32 bits que representa al fabricante y que

está definido en el documento *RFC1700* como *"Números Asignados".* Este código se denomina *Network Management Private Enterprise Code (NMPEC).*

CAPITULO III

3. ESTUDIO COMPARATIVO

3.1. INTRODUCCIÓN

El presente capítulo tiene como objetivo fundamental, analizar en detalle cada uno de los portales cautivos que se han seleccionado para el estudio comparativo denominados CHILLISPOT Y AIR MARSHAL.

Se analizaran las herramientas de tal forma que se pueda apreciar su facilidad de instalación, configuración, la forma en que se afecta la utilización del procesador, tiempos de respuesta a los usuarios y demás prestaciones que estos dos free software para portales cautivos nos ofrecen.

3.2. PORTALES CAUTIVOS A ANALIZAR

Los portales cautivos a analizar son Chillispot y Air Marshal, en esta sección analizaremos los puntos teóricos más importantes acerca de cada uno de éstos.

CHILLISPOT

Chillispot es un portal cautivo de código abierto o punto de acceso y de LAN inalámbrico controlado. Se utiliza para la autenticación de los usuarios de una LAN inalámbrica. Soporta acceso basado en web que es el patrón actual para la autenticación de los HotSpots públicos y soporta Wi-Fi Protected Access (WPA y WPA2). Autenticación, autorización y contabilidad (AAA) está a cargo de su servidor Radius.

Para trabajar chillispot necesita dos servicios adicionales externamente proporcionados:

- Un portal Web al que los usuarios son redireccionados.
- Un servidor Radius para autenticación. La mayoría de las veces el Servidor Radius y el Servidor Web estarán integrados.

El sistema de autenticación chillispot consta de dos partes principales, una es el demonio Chillispot que se encarga de gestionar los clientes de la subred y pedirles autenticación y la otra consta del servidor radius llamado Freeradius que es quien realiza la autenticación en este caso con el servidor de base de datos.

Software y equipo Necesario:

- Chillispot
- Radius server, en este caso es utilizado el Freeradius
- Servidor Web, Apache2.
- Soporte SSL para el servidor web, apache-SSL.

- Access Point inalámbrico o Router inalámbrico

La topología de la red propuesta para el sistema es el siguiente:

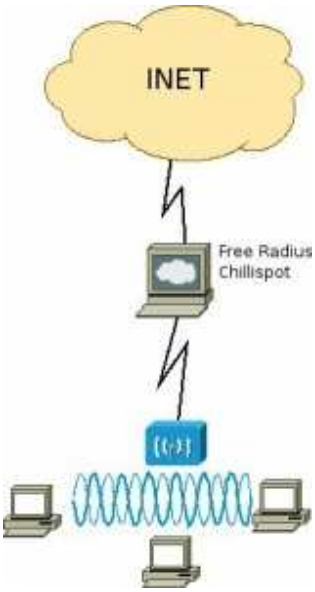


Figura III.1 Topología red Chillispot

Chillispot crea una interfaz de red virtual que se vale de la interfaz de red física por el cual está conectada la red inalámbrica, por esta interfaz virtual chillispot habilita su propio servidor DHCP.

Chillispot tiene dos componentes principales:

- Una aplicación de en espacio de usuario denominada *chilli* que es el *Portal Cautivo* en sí mismo, y cumple las funciones de *Servidor DHCP, Cliente RADIUS, Proxy-RADIUS, y Redirector*.
- Un archivo CGI*2* en el servidor web, denominado *hotspotlogin.cgi,* el cual es un script, programado en *Perl,* que se encarga de enviar los datos de autenticación a *chilli.* Este script, genera un *desafío-CHAP* para validar el usuario y la clave de

acceso, que ha recibido del cliente, a través del servidor web cifrado con HTTPS, y envía el mismo a *chilli*.

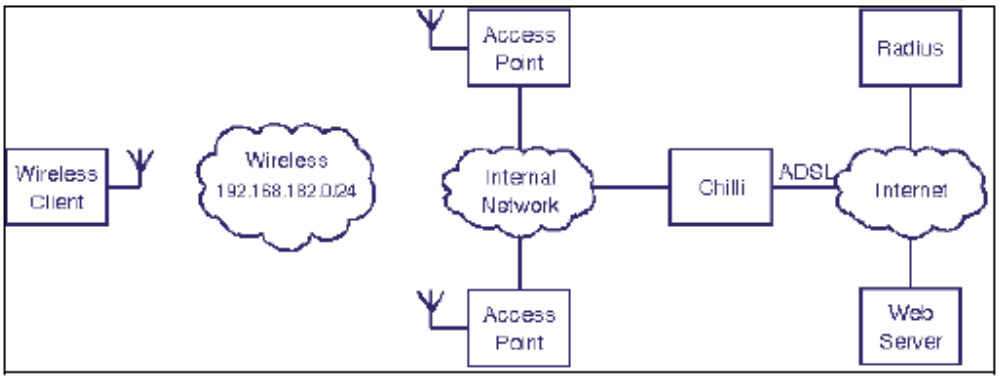


Figura III.2 Esquema de red Chillispot

Características de Chillispot

Las principales características de *Chillispot* son las siguientes:

- Soporta dos métodos de autenticación distintos *UAM (Universal Access Method) y WPA/RSN (Wireless Protected Access).*
- Soporta Autenticación, Autorización y Registro (AAA) contra un *servidor RADIUS.*
- Posee un servicio de *DHCP* propio para ambos métodos de autenticación. Con *WPA/RSN* soporta asignación de direcciones *IP* a través de atributos RADIUS, funcionando como proxy.
- La autenticación con *UAM* soporta *SSL.*
- Soporta cualquier *AP.*
- Soporta *scripts* de inicio y final de conexión para cada cliente.
- Funciona utilizando NAT o Routing.
- Realiza diferentes controles a través de los valores de los atributos *RADIUS* de los diccionarios *wispr y chillispot.* Esto permite controlar los volúmenes de

tráfico entrante/saliente de un usuario en particular, realizar controles de ancho de banda, etc.

AIR MARSHAL

Air Marshal es un Portal Cautivo que proporciona un método conveniente de controlar el acceso a redes públicas y privadas, aprovechando las tecnologías Web. Los usuarios simplemente se conectan y se encuentran un saludó con una página web para pedir un nombre de usuario y contraseña para poder acceder a la red.

Los principales beneficios de esta solución provienen de clientes que no requieren más conocimientos, software o configuración especial. Los clientes pueden acceder rápido y fácilmente tener acceso a la red, independientemente del tipo de dispositivo o sistema operativo utilizado.

Mientras que el objetivo principal es la autenticación que ofrecen beneficios adicionales, tales como la capacidad de dirigir nuevos usuarios a iniciar un proceso de suscripción, los fondos de una cuenta ofrecen un acceso limitado a servicios tales como seleccionar un sitio web de la empresa o la información relacionada con un determinado lugar.

Air Marshal es especialmente adecuado para una amplia gama de ambientes incluyendo hoteles, cibercafés, universidades, Internet y HotSpots guest redes.

Características de Air Marshal

- Único servidor admite miles de sesiones concurrentes.
- La contraseña de cifrado basado en navegador.
- Cifrado SSL
- Configurable interfaz Web HTML.

- Pantalla de estado de usuario.
- ADMIN interfaz integrada.
- Configuración de un jardín.
- Sesión activa lista.
- Locales de gestión de cuentas.
- Acceso anónimo.
- Replicación de datos de clientes.
- Web proxy transparente.
- Máxima UL / DL velocidades de transmisión de datos por usuario.
- Periodo de sesiones, la interrupción comercial.

Beneficios de Air Marshal

- Optimizar los despliegues a gran escala.
- Ofrece una mayor seguridad de contraseña de inicio de sesión, además de la encriptación SSL.
- El Estándar de la industria para el cifrado y la autenticación mutua. Establece la identidad, protege la información sensible de clientes, como contraseñas de cuentas.
- Personaliza el aspecto y, conexión a la suscripción de servidor, gestión de cuentas y los sitios de publicidad.
- Permite a los usuarios visualizar en cuenta las estadísticas, como el tiempo y los datos utilizados y los restantes.
- Fácil de usar el 100% basado en web y la configuración de cuenta local simplifica la configuración del sistema de gestión de tareas.

- Ver quién está en línea, incluida la duración en tiempo real y uso de ancho de banda. Permite desconectar de sesiones activas.
- Los Complementarios proporciona un acceso limitado a seleccionar los servicios tales como el registro de nuevos clientes, gestión de cuentas, sitios web de la empresa o información relacionada con un determinado lugar.
- Configurar cuentas de acceso local con fecha de caducidad, límites de tiempo y de datos y el máximo de carga / tipos de descarga de datos. Útil para pequeñas instalaciones o especiales de acceso administrativo.
- Proporciona el acceso de invitados a la red con un conjunto opcional de limitaciones, como carga / descarga de datos y las tasas diarias de tiempo y restricciones de uso de datos. Esto es útil en situaciones en las que puede proporcionar un cierto nivel de servicio gratuito, como una o dos horas de servicio por día, ofrecer el apoyo de publicidad o simplemente requieren acceso a los usuarios leer y aceptar los términos de un acuerdo de servicio antes de acceder a la red.
- Todos los datos enviados o recibidos por un usuario en base a un monitor remoto / colector de datos. Útil para fines de diagnóstico o de interceptar.
- Dirige a las peticiones HTTP de los servidores proxy transparente en una base por usuario. Permite la elección de los usuarios de la aceleración y servicios de filtrado de contenidos.
- Evita que solo los usuarios puedan monopolizar los recursos de la red. Permite niveles de oferta de servicios.
- Periódicamente obliga a los usuarios a ver serie de mensajes comerciales (publicidad).
- Publicidad apoyado acceso. Oferta de servicios diferenciados.

3.3. ELEMENTOS NECESARIOS PARA LA IMPLEMENTACIÓN DEL PORTAL CAUTIVO.

Para la implementación de un portal cautivo se necesita:

- Software Portal Cautivo: es un Software que obliga a los clientes http en red a ver una página especial (generalmente para autentificación), antes de salir a internet. Esto se hace interceptando todo el tráfico http. Se pueden ver en la mayoría de los **Wifi hotspots**.
- Servidor de Autenticación, como su nombre lo indica será el encargado de autenticar al usuario para determinar si podrá acceder o no a Internet.
- Access Point, dispositivo que permitirá la comunicación entre el servidor de autenticación y los terminales de los usuarios.

3.4. AMBIENTE DE PRUEBAS

El ambiente de pruebas se realizó en base al escenario ilustrado en la figura III.3, la descripción de las características de equipos y software utilizado se encuentran en la tabla III.1 y III.2 respectivamente.

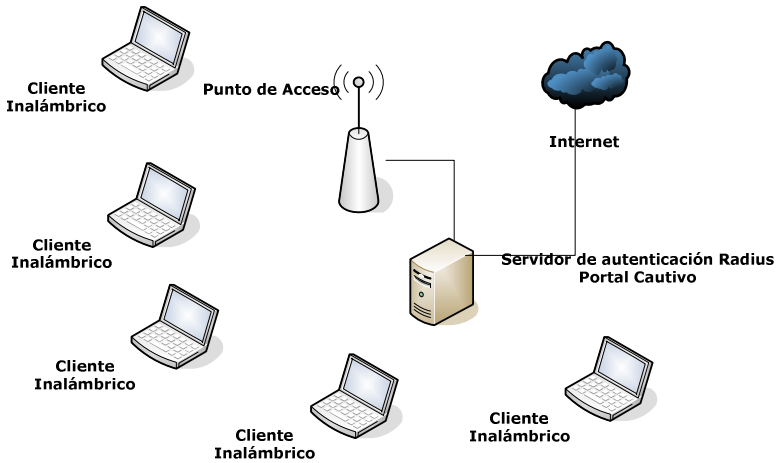


Figura III.3 Escenario de pruebas

Equipo	Descripción
Access Point	Cantidad: 1 Servicio DHCP: Deshabilitado Velocidad Transmisión:
Servidor	Cantidad: 1 Sistema Operativo: Centos 5.3 Memoria RAM: 2GB Interfaces de Red : 2
Cliente Inalámbrico	Cantidad: 5

Tabla III.1 Equipos utilizados en el ambiente de pruebas

Software	Descripción
Chillispot	Software para implementar portal cautivo.
Air Marshal	Software para implementar portal cautivo.
FreeRadius	Servidor de autenticación.
Mysql	Servidor de base de datos.
Radlogin	Software que permite evaluar las respuestas del servidor radius a cada portal cautivo simulando n conexiones.

Tabla III.2 Software utilizado en el ambiente de pruebas

3.5. SELECCIÓN DE LAS HERRAMIENTAS PARA PORTALES CAUTIVOS

Las herramientas para la implementación son las mencionadas anteriormente Chillispot y Air Marshal.

Ambas herramientas han sido utilizadas para la implementación de portales cautivos en universidades, aeropuertos, hoteles, etc. Como lo referencian las páginas:

http://toip.reuna.cl/wiki/images/Anexo_Complementario_1_3.pdf

http://www.iea-software.com/products/airmarshal1.cfm

3.6. DETERMINACIÓN DE PARÁMETROS DE COMPARACIÓN

Para realizar un estudio comparativo entre estos dos portales, es muy importante seleccionar y describir correctamente los parámetros de medición, porque de esta forma se obtiene un resultado adecuado en la selección del portal ya que con el resultado final se elegirá la herramienta que más se adapte y ofrezca mejores prestaciones a la gestión de seguridad al acceso a internet inalámbrico de la ESPOCH.

Con lo anterior en mente se define el estudio comparativo en base a los parámetros detallados en la tabla III.4:

PARÁMETROS	JUSTIFICACIÓN
Datos cuantitativos	Permitirán contabilizar y calificar cada uno de los elementos utilizados en el servidor RADIUS por las herramientas de portal cautivo Chillispot y Air Marshal para su funcionamiento.
Datos cualitativos	Facilidad de instalación, facilidad de configuración, seguridad, versión, funcionalidad, descripción del portal, herramientas de desarrollo, interfaz del administrador, interfaz de usuario
Evaluación	- La evaluación cuantitativa se realizará mediante la comparación de resultados arrojados por estudios estadísticos realizados sobre el servidor RADIUS al trabajar con los portales cautivos. - La evaluación cualitativa se calificará en una escala de 1 a 3, donde 3 es el puntaje máximo.

Tabla III.3 Parámetros del estudio comparativo

3.7. ANÁLISIS CUANTITATIVO Y CUALITATIVO

ANÁLISIS CUANTITATIVO

El análisis cuantitativo de los portales cautivos Air Marshal y Chillispot se realizó en base al Tiempo de Respuesta de las peticiones de autenticación de usuario, permitiendo evaluar el rendimiento del servidor radius frente a cada portal cautivo.

Para realizar este análisis se utilizó la herramienta de benchmarking Radlogin4 disponible en http://www.iea-software.com/products/radlogin4.cfm la cual permite simular n conexiones al servidor radius y realizar un estudio estadístico en base a los resultados generados. La figura III.4 muestra la interfaz de esta herramienta que permite realizar los test al servidor.

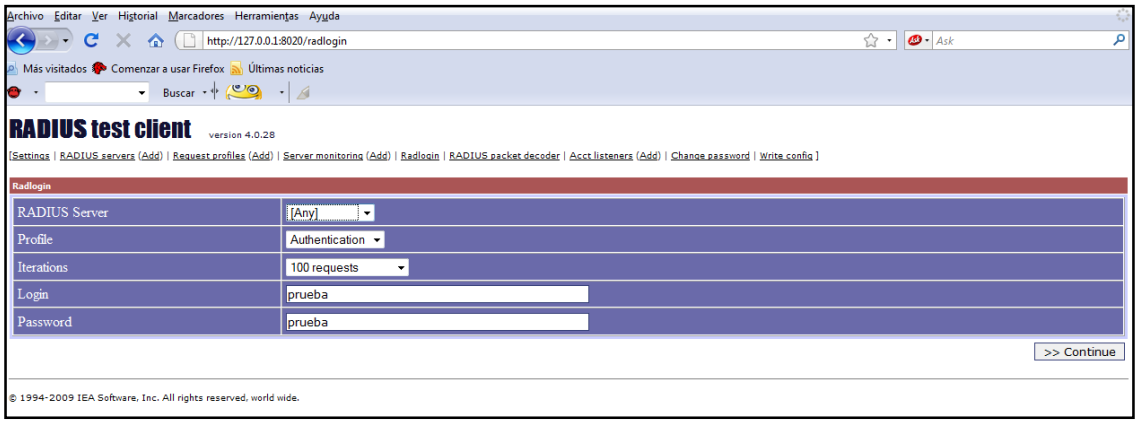


Figura III.4. Herramienta Radlogin

El número de conexiones simultáneas al servidor estará definido por el tamaño de la muestra obtenida de la población de usuarios que utilizan el internet inalámbrico de la ESPOCH.

A continuación se detalla el proceso realizado para el análisis cuantitativo:

Tamaño de la muestra

El número de conexiones concurrentes está entre 95 y 125.

La media de estos valores es:

$$\overline{x} = \frac{1}{N} \sum_{i=1}^{N} x_i$$

$$\overline{x} = \frac{1}{2}(95 + 125)$$

$$\overline{x} = \mathbf{110}$$

El tamaño de la muestra se calculo en base a la siguiente fórmula estadística:

$$n = \frac{Z^2 pqN}{NE^2 + Z^2 pq}$$

Donde:

n es el tamaño de la muestra;

Z es el nivel de confianza;

P es la variabilidad positiva;

q es la variabilidad negativa;

N es el tamaño de la población;

E es la precisión del error.

$$n = \frac{(0{,}95)^2(0{,}5)(0{,}5)(110)}{(110)(0{,}05)^2 + (0{,}95)^2(0{,}5)(0{,}5)}$$

$$n = \frac{24{,}81}{0{,}50}$$

$$n = 49{,}62$$

El tamaño de la muestra a ser utilizado es de 50 conexiones concurrentes a internet. Mediante la herramienta radlogin se simuló la conexión de cada usuario de manera simultánea obteniendo como media los resultados presentados en la tabla III.5:

Portal Cautivo	**Tiempos de Respuesta**
Chillispot	0.41 ms
Air Marshal	1.11 ms

Tabla III.4 Tiempos de Respuesta obtenidos

La media de estos valores se computo por medio de la hoja de cálculo Excel.

Con el resultado anterior podemos decir que el Portal Cautivo con mayor tiempo de respuesta es Chillispot.

ANÁLISIS CUALITATIVO

Los parámetros cualitativos se refieren a las cualidades de las herramientas, es decir que no se las ve pero se las puede percibir.

A continuación se muestra la tabla III.6 con los puntajes que pueden ir de 1 a 3, mediante esto se obtiene un puntaje total que permitirá escoger el portal cautivo óptimo.

La equivalencia de los puntajes es la siguiente:

Puntaje	Descripción	Porcentaje
1	Bueno	(Desde 1% hasta 30%)
2	Muy Bueno	(Desde 31% hasta 70%)
3	Sobresaliente	(Desde 71% hasta 100%)

Tabla III.5 Equivalencia de puntajes

DESCRIPCIÓN DE PARÁMETROS.

La tabla III.7 muestra la descripción de los parámetros cualitativos a evaluar en este análisis comparativo.

PARAMETRO	DESCRIPCIÓN
Open Source	Es el término con el que se conoce al software distribuido y desarrollado libremente, da a los

	usuarios la libertad de uso, modificación y distribución.
Facilidad de Instalación	Este es uno de los principales aspectos al momento de elegir el software a utilizar, para la instalación y configuración del portal cautivo.
Facilidad de Configuración	El administrador debe poder configurar el portal cautivo de manera fácil, intuitiva.
Seguridad	La seguridad es una parte fundamental para la elección del portal cautivo a utilizar ya que debemos tener en cuenta que el servidor estará conectado en red y puede recibir ataques externos.
Versión	Indica un avance o mejora de los elementos de configuración que forman la línea base de un producto o una configuración del mismo, controla características como: mecanismo de almacenaje de cada uno de los ítems que deba gestionarse (archivos de texto, imágenes, documentación...), posibilidad de modificar, mover, borrar cada uno de los elementos y el histórico de las acciones realizadas con cada elemento pudiendo volver a un estado anterior dentro de ese historial.

Funcionalidad	El usuario tiene que saber qué es lo que se espera hacer, es decir por ejemplo que los botones funcionen correctamente y no haya sorpresas.
Descripción del Portal	Especifica con qué fin fueron creados cada uno de los Portales ya que son principalmente utilizados para la autenticación para tener acceso a Internet.
Lenguajes que soporta	Es una técnica estándar de comunicación que permite expresar las instrucciones que han de ser ejecutadas en una computadora. Consiste en un conjunto de reglas sintácticas y semánticas que definen un lenguaje informático. Un lenguaje de programación permite a un programador especificar de manera precisa: sobre qué datos una computadora debe operar, cómo deben ser estos almacenados y transmitidos y qué acciones debe tomar bajo una variada gama de circunstancias. Todo esto, a través de un lenguaje que intenta estar relativamente próximo al lenguaje humano o natural, tal como sucede con el lenguaje Léxico.
Interfaz del Administrador	Es la forma en que el Administrador puede

	comunicarse con una computadora, y comprender todos los puntos de contacto y poder interactuar entre el usuario y el equipo. Sus principales funciones son: Administrar la configuración del portal cautivo y verificar que usuarios se encuentran conectados.
Interfaz del Usuario	Es la forma en que el usuario puede autenticarse y acceder al servicio de internet a través del portal cautivo.

Tabla III.6 Descripción de Parámetros

ANÁLISIS COMPARATIVO

La tabla III.8 presenta el análisis comparativo cualitativo de los portales cautivos mencionados.

Parámetros	**Portal Air Marshal**	**Portal Chillispot**
Open Source	No es un open source, es un free software que permite al usuario su libre uso y distribución pero no su libre modificación.	Posee todas las características de un open source
Facilidad de Instalación	Sencilla	Sencilla
Facilidad de Configuración	Sencilla mediante	Compleja se realiza

	interfaz web	modificando el archivo de configuración en un editor de texto
Seguridad	Confiable	Confiable
Versión.	2.0.0	1.1.0
Funcionalidad	El Usuario entiende su funcionamiento	El usuario entiende su funcionamiento
Descripción de los Portales	Creado para su aplicación pública o privada	Creado para su aplicación pública o privada
Lenguajes que soporta	HTML	CGI, HTML, PHP, JAVASCRIPT
Interfaz del Administrador	Amigable y fácil de utilizar	No existe interfaz
Interfaz del Usuario	Amigable y fácil de utilizar	Amigable y fácil de utilizar

Tabla III.7 Análisis Comparativo Cualitativo

DESCRIPCIÓN DE RESULTADOS

- **Open Source:** Por sus características open source, se obtiene:
  - ✓ Air Marshal, debido a que no es un open source pero si un free software recibe un 20% (puntaje 1).

- ✓ Chillispot, debido a que es un software de libre uso, modificación y distribución recibe un 100% (puntaje 3).

- **Facilidad de Instalación:** Por su proceso de instalación, se obtiene:
  - ✓ Air Marshal, debido a que en el proceso de instalación se utiliza comandos sencillos en Linux, recibe un 100% (puntaje 3).
  - ✓ Chillispot, debido a que en el proceso de instalación se utiliza comandos sencillos en Linux, recibe un 100% (puntaje 3).

- **Facilidad de Configuración:** Por su proceso de configuración, se obtiene:
  - ✓ Air Marshal, debido a que proporciona una interfaz web sencilla de utilizar para configurar el portal, recibe un 100% (puntaje 3).
  - ✓ Chillispot, debido a que el proceso de configuración es complejo por la edición del archivo correspondiente en modo texto, recibe un 30% (puntaje 1).

- **Seguridad:** Por el nivel de seguridad, se obtiene:
  - ✓ Air Marshal, puede recibir ataques de spoofing, recibe un 60% (puntaje 2).
  - ✓ Chillispot, puede recibir ataques de spoofing, recibe un 60% (puntaje 2).

- **Versión:** Por las características y la facilidad de uso:
  - ✓ Air Marshal, versión 2.1.0, presenta características modernas que permite el fácil manejo por su interfaz grafica, recibe un 100% (puntaje 3).

- ✓ Chillispot, en su versión 1.0.0, presenta características modernas, pero su manejo es complejo por su modo texto, recibe un 50% (puntaje 2).

- **Funcionalidad:** Por la funcionalidad de su interfaz de autenticación.
  - ✓ Air Marshal, tiene una interfaz clara y sencilla, recibe un 100% (puntaje 3).
  - ✓ Chillispot, tiene una interfaz clara y sencilla, recibe un 100%(puntaje 3).

- **Descripción del Portal:** Por el fin con que fueron creados.
  - ✓ Air Marshal, puede ser aplicado en áreas o lugares públicos o privados, recibe 100% (puntaje 3).
  - ✓ Chillispot, puede ser aplicado en áreas o lugares públicos y privados, recibe 100% (puntaje 3).

- **Lenguajes que soporta:** Por la variedad de lenguajes que soporta el Portal.
  - ✓ Air Marshal, soporta pocos lenguajes, recibe 25% (puntaje 1).
  - ✓ Chillispot soporta varios lenguajes, recibe 100% (puntaje 3).

- **Interfaz del Administrador:** Por la diversidad en su presentación y facilidad en el manejo.
  - ✓ Air Marshal presenta una mayor facilidad de manejo, debido a la interfaz gráfica sencilla que posee, recibe 100% (puntaje 3).
  - ✓ Chillispot, presenta una menor facilidad de manejo, debido que a se realiza la edición del archivo chilli.conf para lo cual el administrador revisa el archivo y lo modifica, recibe 50% (puntaje 2).

- **Interfaz de Usuario:** Por la diversidad en su presentación y facilidad en el manejo.
    - ✓ Air Marshal, soporta una interfaz agradable, su comunicación y manejo es sencillo, recibe 100% (puntaje 3).
    - ✓ Chillispot, soporta un tipo de interfaz agradable al usuario, su comunicación y manejo es sencillo, recibe 100% (puntaje 3).

Determinación de Dependencia entre los Portales Cautivos y los aspectos Cualitativos evaluados

En base a los resultados obtenidos se procederá a encontrar el valor de chi cuadrado que nos permitirá determinar si existe algún grado de dependencia entre las variables Portal Cautivo y Parámetro Cualitativo.

Para este análisis partimos de la tabla III.9 detallada a continuación.

		Portal Cautivo		
		Air Marshal	Chillispot	**Total**
Parámetro Cualitativo	Open Source	1	3	4
	Facilidad de Instalación	3	3	6
	Facilidad de Configuración	3	1	4
	Seguridad	2	2	4
	Versión	3	2	5
	Funcionalidad	3	3	6
	Descripción del Portal	3	3	6
	Lenguajes que soporta	1	3	4
	Interfaz de Administrador	3	2	5
	Interfaz de Usuario	3	3	6
	Total	25	25	50

Tabla III.8 Tabla de Contingencia

Determinamos Frecuencias relativas marginales:

P (Air Marshal) = $\frac{25}{50}$ = 50%

P (Chillispot) = $\frac{25}{50}$ = 50%

P (Open Source) = $\frac{4}{50}$ = 8%

P (Facilidad de Instalación) = $\frac{6}{50}$ = 12%

P (Facilidad de Configuración) = $\frac{4}{50}$ = 8%

P (Seguridad) = $\frac{4}{50}$ = 8%

P (Versión) = $\frac{5}{50}$ = 10%

P (Funcionalidad) = $\frac{6}{50}$ = 12%

P (Descripción del Portal) = $\frac{6}{50}$ = 12%

P (Lenguajes que soporta) = $\frac{4}{50}$ = 8%

P (Interfaz de Administrador) = $\frac{5}{50}$ = 10%

P (Interfaz de Usuario) = $\frac{6}{50}$ = 12%

Frecuencias relativas conjuntas:

P (Air Marshal y Open Source) = $\frac{1}{50}$ = 2%

P (Air Marshal y Facilidad de Instalación) = $\frac{3}{50}$ = 6%

P (Air Marshal y Facilidad de Configuración) = $\frac{3}{50}$ = 6%

P (Air Marshal y Seguridad) = $\frac{2}{50}$ = 4%

P (Air Marshal y Versión) = $\frac{3}{50}$ = 6%

P (Air Marshal y Funcionalidad) = $\frac{3}{50}$ = 6%

P (Air Marshal y Descripción del Portal) = $\frac{3}{50}$ = 6%

P (Air Marshal y Lenguajes que soporta) = $\frac{1}{50}$ = 2%

P (Air Marshal e Interfaz de Administrador) = $\frac{3}{50}$ = 6%

P (Air Marshal e Interfaz de Usuario) = $\frac{3}{50}$ = 6%

P (Chillispot y Open Source) = $\frac{3}{50}$ = 6%

P (Chillispot y Facilidad de Instalación) = $\frac{3}{50}$ = 6%

P (Chillispot y Facilidad de Configuración) = $\frac{1}{50}$ = 2%

P (Chillispot y Seguridad) = $\frac{2}{50}$ = 4%

P (Chillispot y Versión) = $\frac{2}{50}$ = 4%

P (Chillispot y Funcionalidad) = $\frac{3}{50}$ = 6%

P (Air Marshal y Descripción del Portal) = $\frac{3}{50}$ = 6%

P (Air Marshal y Lenguajes que soporta) = $\frac{3}{50}$ = 6%

P (Air Marshal e Interfaz de Administrador) = $\frac{2}{50}$ = 4%

P (Air Marshal e Interfaz de Usuario) = $\frac{3}{50}$ = 6%

Frecuencias relativas teóricas esperadas en caso de independencia:

E (Air Marshal y Open source) = 50% x 8% = 4%

E (Air Marshal y Facilidad de instalación) = 50% x 12% = 6%

E (Air Marshal y Facilidad de configuración) = 50% x 8% = 4%

E (Air Marshal y Seguridad) = 50% x 8% = 4%

E (Air Marshal y Versión) = 50% x 10% = 5%

E (Air Marshal y Funcionalidad) = 50% x 12% = 6%

E (Air Marshal y Descripción del Portal) = 50% x 12% = 6%

E (Air Marshal y Lenguajes que soporta) = 50% x 8% = 4%

E (Air Marshal e Interfaz de Administrador) = 50% x 10% = 5%

E (Air Marshal e Interfaz de Usuario) = 50% x 12% = 6%

E (Chillispot y Open source) = 50% x 8% = 4%

E (Chillispot y Facilidad de instalación) = 50% x 12% = 6%

E (Chillispot y Facilidad de configuración) = 50% x 8% = 4%

E (Chillispot y Seguridad) = 50% x 8% = 4%

E (Chillispot y Versión) = 50% x 10% = 5%

E (Chillispot y Funcionalidad) = 50% x 12% = 6%

E (Chillispot y Descripción del Portal) = 50% x 12% = 6%

E (Chillispot y Lenguajes que soporta) = 50% x 8% = 4%

E (Chillispot e Interfaz de Administrador) = 50% x 10% = 5%

E (Chillispot e Interfaz de Usuario) = 50% x 12% = 6%

Frecuencias absolutas teóricas esperadas en caso de independencia:

E (Air Marshal y Open Source) = 25/50 * 4 = 2

E (Air Marshal y Facilidad de instalación) = 25/50 * 6 = 3

E (Air Marshal y Facilidad de configuración) = 25/50 * 4 = 2

E (Air Marshal y Seguridad) = 25/50 * 4 = 2

E (Air Marshal y Versión) = 25/50 * 5 = 2,5

E (Air Marshal y Funcionalidad) = 25/50 * 6 = 3

E (Air Marshal y Descripción del Portal) = 25/50 * 6 =3

E (Air Marshal y Lenguajes que soporta) = 25/50 * 4 = 2

E (Air Marshal e Interfaz de Administrador) = 25/50 * 5 = 2,5

E (Air Marshal e Interfaz de Usuario) = 25/50 * 6 = 3

E (Chillispot y Open Source) = 25/50 * 4 = 2

E (Chillispot y Facilidad de instalación) = 25/50 * 6 = 3

E (Chillispot y Facilidad de configuración) = 25/50 * 4 = 2

E (Chillispot y Seguridad) = 25/50 * 4 = 2

E (Chillispot y Versión) = 25/50 * 5 = 2,5

E (Chillispot y Funcionalidad) = 25/50 * 6 = 3

E (Chillispot y Descripción del Portal) = 25/50 * 6 =3

E (Chillispot y Lenguajes que soporta) = 25/50 * 4 = 2

E (Chillispot e Interfaz de Administrador) = 25/50 * 5 = 2,5

E (Chillispot e Interfaz de Usuario) = 25/50 * 6 = 3

Determinación del valor de Chi Cuadrado

$$x^2 = \frac{\Sigma_{i=1}^{h}\Sigma_{j=1}^{k}(nij - Eij)^2}{E_{ij}}$$

Reemplazando obtenemos:

$$x^2 = \frac{(1-2)^2}{2} + \frac{(3-2)^2}{2} + \frac{(3-3)^2}{3} + \frac{(3-3)^2}{3} + \frac{(3-2)^2}{2} + \frac{(1-2)^2}{2} + \frac{(2-2)^2}{2} + \frac{(2-2)^2}{2}$$
$$+ \frac{(3-2{,}5)^2}{2{,}5} + \frac{(2-2{,}5)^2}{2{,}5} + \frac{(3-3)^2}{3} + \frac{(3-3)^2}{3} + \frac{(3-3)^2}{3} + \frac{(3-3)^2}{3} + \frac{(1-2)^2}{2}$$
$$+ \frac{(3-2)^2}{2} + \frac{(3-2{,}5)^2}{2{,}5} + \frac{(2-2{,}5)^2}{2{,}5} + \frac{(3-3)^2}{3} + \frac{(3-3)^2}{3}$$

$$x^2 = 0{,}5 + 0{,}5 + 0{,}5 + 0{,}5 + 0{,}1 + 0{,}1 + 0{,}5 + 0{,}50 + 0{,}1 + 0{,}1$$

$$x^2 = 3{,}4$$

El valor de chi cuadrado es de 3,4 por lo cual podemos decir que los portales cautivos dependen de las características o parámetros cualitativos que éstos proporcionan, por lo tanto es importante realizar su análisis comparativo cualitativo.

3.8. RESULTADOS DEL ANÁLISIS COMPARATIVO

RESULTADO ANÁLISIS CUANTITATIVO

Los resultados obtenidos en el análisis cuantitativo se describen en la tabla III.10 y se ilustran en la figura III.5.

Portal Cautivo	Tiempos de Respuesta
Chillispot	0,41 ms
Air Marshal	1,11 ms

Tabla III.9 Resultado Cuantitativo

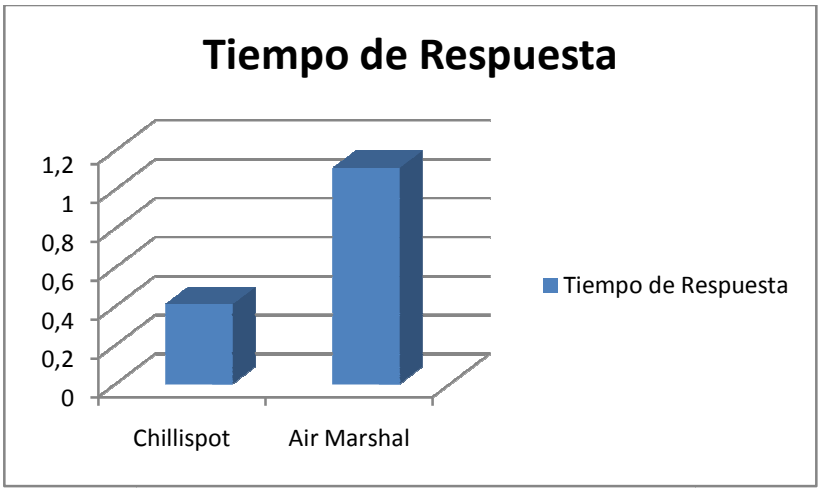


Figura III.5 Resultado Cuantitativo

RESULTADO ANÁLISIS CUALITATIVO

A continuación vamos a mostrar en la tabla III.11 y en la figura III.5 el promedio parcial de todos y cada uno de los parámetros cualitativos que son primordiales en el estudio de los portales cautivos considerados.

Parámetros de comparación	**Portal Air Marshal**	**Portal Chillispot**
Open Source	1	3
Facilidad de Instalación	3	3
Facilidad de Configuración	3	1
Seguridad	2	2
Versión	3	2
Funcionalidad	3	3
Descripción del Portal	3	3
Lenguajes que soporta	1	3
Interfaz del Administrador	3	2
Interfaz del Usuario	3	3
TOTAL	**25**	**25**

Tabla III.10 Promedios parciales cualitativos del análisis comparativo

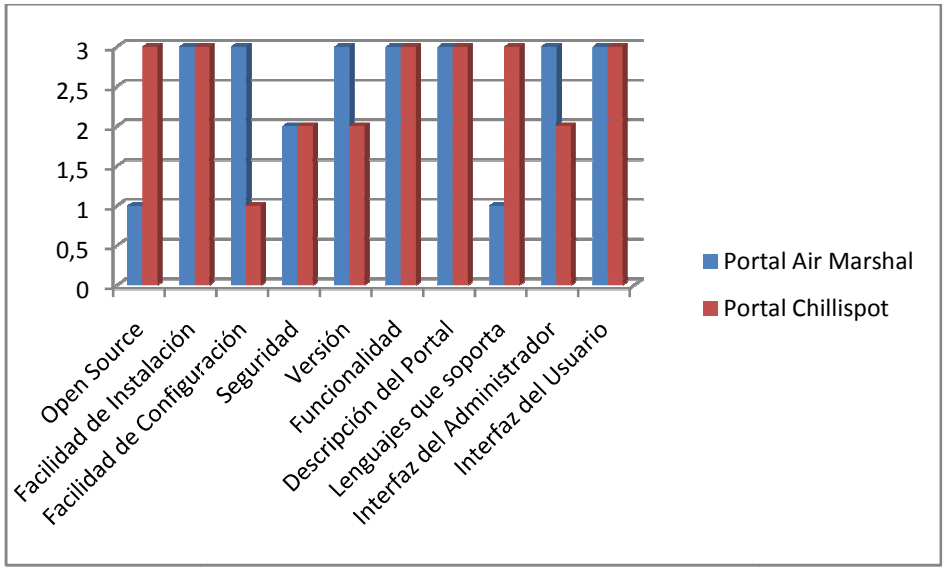


Figura III.6 Promedios parciales cualitativos del análisis comparativo

En la tabla III.12 se muestra el promedio total cualitativo, el cual está dado por la mediana de las notas parciales anteriormente mencionadas, de tal forma que se obtenga como resultado la mejor herramienta para la implementación del portal cautivo.

VARIABLES	PORTALES CAUTIVOS	
	CHILLISPOT	AIR MARSHAL
PROMEDIO	3	3
EQUIVALENCIA	Sobresaliente	Sobresaliente

Tabla III.11 Promedio Total Cualitativo

La figura III.6 presenta una gráfica de los resultados obtenidos en el análisis cualitativo.

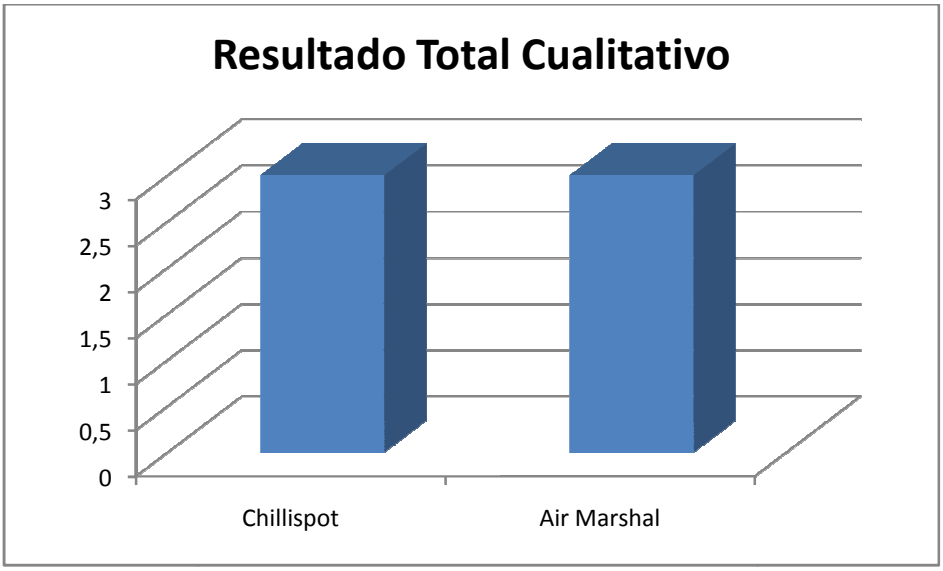


Figura III.7 Promedio Total Cualitativo

3.9. CONCLUSIONES DEL ANÁLISIS COMPARATIVO

Para dar una conclusión a este capítulo referente al estudio comparativo de los portales cautivos Chillispot y Air Marshal como se mostró en los resultados anteriores Chillispot es superior a Air Marshal en forma cuantitativa pero en la parte cualitativa no, debido a:

- Chillispot tiene un tiempo de respuesta mínimo a conexiones simultáneas con el servidor de autenticación Radius ya que ocupa menos del 50% del tiempo en que lo hace Air Marshal.
- En características Air Marshal y Chillispot presentan una valoración igual lo que quiere decir que ambos portales son aptos cualitativamente para su utilización.

- Chillispot presenta una gran ventaja sobre Air Marshal ya que es una herramienta open source la cual permite a los desarrolladores modificarla y crear ambientes de trabajo a su gusto.

CAPITULO IV

4. IMPLEMENTACIÓN DE UN PORTAL CAUTIVO PARA GESTIONAR EL ACCESO A LA RED INALÁMBRICA DE LA ESPOCH

4.1. INTRODUCCIÓN

El presente capítulo muestra la configuración del servidor RADIUS, y de los archivos necesarios para la implementación del portal cautivo en la Escuela Superior Politécnica de Chimborazo.

El estudio comparativo nos permitió determinar que ambos portales cautivos muestran excelentes prestaciones cualitativas sin embargo en cuanto a tiempos de respuesta Chillispot es superior a Air Marshal por esta razón y debido a que Chillispot es una herramienta Open Source que permite desarrollar aplicaciones de acuerdo a la

infraestructura de intercambio de datos manejada por esta institución como lo son los WebServices, el portal cautivo a implementar en la red de la ESPOCH es Chillispot.

Se debe mencionar que la situación actual de acceso a la WLAN de la ESPOCH se realiza mediante la autenticación WEP descrita en capítulos anteriores, con la implementación de este portal el acceso se realizará mediante una página de autenticación que tomará las credenciales del usuario (Username y Password) para validarlos con el servidor de autenticación radius y permitir o no el acceso a internet.

4.2. FREERADIUS

FreeRadius es uno de los servidores Radius más óptimos disponibles hoy en día. Desarrollado por un grupo de diseñadores que tienen más de una década de experiencia colectiva llevando a cabo y desplegando software RADIUS y software de ingeniería en UNIX. El producto es el resultado en la unión entre muchos de los nombres conocidos en aplicaciones basadas en software libres RADIUS, incluyendo a varios diseñadores del Debían el sistema operativo de GNU/Linux, y es distribuido bajo el GNU GPL (versión 2). FreeRadius es una completa recopilación, de un servidor RADIUS. La configuración guarda muchas similitudes a Livingston, antiguo servidor RADIUS.

Actuando como un servidor proxy RADIUS.

4.3. CONFIGURACIÓN DEL SERVIDOR RADIUS

INSTALACIÓN DE FREERADIUS

Pasos para la instalación:

1. Descomprimir el archivo tar xvf freeradius-server-2.0.0.tar.bz2

2. Ingresar a la carpeta descomprimida cd freeradius-server-2.0.0

3. Generar archivos para la compilación ./configure --prefix=/usr --sysconfdir=/etc

4. Compilar make

5. Instalar make install

CONFIGURACIÓN DE RADIUSD.CONF

Radiusd.Conf es el archivo de configuración del servidor FreeRadius puede encontrarse dentro de /etc/raddb/radiusd.conf, a continuación se presentarán los aspectos más importantes a configurar dentro de él:

- Configuración de la ubicación de los archivos radius.
- Configuración de la ubicación de los archivos log.
- Configuración de la ubicación de los archivos de librería.
- Configuración de la ubicación de los archivos de ejecución.
- Configuración de tiempos de envío de paquetes.
- Configuraciones de puertos.
- Configuración de seguridad.
- Configuración del proxy.
- Configuración del módulo de configuración.

4.4. CONFIGURACIÓN DEL ARCHIVO CLIENTS.CONF

El archivo Clients.Conf se encuentra en /etc/raddb/clients.conf presenta la descripción y credenciales de los diferentes dispositivos que consultan al RADIUS (Aps, NAS, etc).

4.5. CONFIGURACIÓN DEL ARCHIVO SQL.CONF

El archivo sql.conf permite configurar la comunicación entre el servidor radius y la base de datos mysql, en él se configura:

- Motor de base de datos.
- Driver de conexión.
- Dirección del servidor de BD.
- Usuario
- Password
- Nombre de la base de datos
- Nombre de tablas a utilizar

Este archivo se encuentra en /etc/raddb/sql.conf

4.6. CONFIGURACIÓN DEL PORTAL CAUTIVO

INSTALACIÓN DE CHILLISPOT

Pasos para la instalación:

1. Descargar el archivo chillispot-1.1.0.i386.rpm
2. Instalar el paquete chillispot-1.1.0.i386.rpm mediante la instrucción:

   #rpm -Uhv chillispot-1.1.0.i386.rpm
3. Copiar el archivo que contiene la interfaz de usuario del portal cautivo:

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

4. Cambiar permisos al archivo mencionado.

   #chmod ugo+x /var/www/cgi-bin/hotspotlogin.cgi

5. Mostrar los módulos

   Modprobe tun

6. Editar el archive modprobe.conf mediante la instrucción vi /etc/modprobe.conf y agregamos la línea " alias char-major-10-200 tun"

7. Actualizar el módulo

   module_upgrade

8. Ejecutar el firewall de chillispot

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

9. Copiar el firewall de chillispot para que se ejecute al inicio del sistema

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

10. Modificar los permisos del firewall de chillispot

    chmod u+x /etc/init.d/chilli.iptables

CONFIGURACIÓN DE CHILLI.CONF

Chilli.Conf es el archivo de configuración del portal cautivo Chillispot puede encontrarse dentro del directorio etc, a continuación se presentarán los aspectos más importantes a configurar dentro de él:

- Dirección de red de paquetes de datos externos a la red.
- Direcciones IP dinámicas.
- Direcciones IP estáticas.
- Servidores DNS.
- Dominio de la red.
- Dirección IP por la que escucha al servidor radius.
- Dirección IP del servidor radius.

- Puerto de autenticación radius.
- Puerto de contabilidad radius.
- Password del servidor radius.
- Interfaz por la que se proporciona DHCP.
- URL del servidor web para manejar la autenticación.

RESUMEN DE LA CONFIGURACIÓN

Este proyecto consta de las siguientes etapas para su implementación:

1. Instalación del Sistema Operativo para el Servidor: Linux CentOS 5.
2. Instalación del Servidor FreeRADIUS.
3. Configuración del Servidor FreeRADIUS.
4. Enlace de la Base de Datos del RADIUS con MySql.
5. Comprobación del funcionamiento del Servidor FreeRADIUS.
6. Instalación del Portal Cautivo.
7. Configuración del Portal Cautivo.
8. Configuración del equipo (ACCESS POINT).

   Configuraciones Básicas.

   Habilitando Accounting.
9. Configurando
10. Compilación del Apache y PHP para Linux.
11. Interface en PHP.
12. Pruebas finales de funcionamiento.

CONCLUSIONES

- El presente Estudio Comparativo permitió determinar como mejor portal cautivo, para diseño e implementación de una red inalámbrica con autenticación de terminales, a la herramienta Chillispot la cual brinda un porcentaje menor al 50% en tiempo de respuesta al portal Air Marshal y se ajusta a los requerimientos de transferencia de información de la ESPOCH como son los WebServices.
- El sistema planteado es un sistema de uso simple desde el punto de vista del usuario, los procesos de seguridad se realizan de manera transparente el usuario no se percatará que dentro del sistema se realizan verificaciones adicionales de seguridad.
- Chillispot ofrece su código fuente al momento de su adquisición por lo tanto si alguien desea aportar algún proyecto o corregir algún error, lo puede hacer sin necesidad de tener que comprar ninguna licencia. Lo contrario pasa con Air Marshal porque aunque compremos su licencia, no podremos tener acceso a su código fuente.
- Debido a que no proveen una fuerte encriptación, los portales cautivos no son una buena elección para aquellas redes que requieren una protección fuerte y limiten el acceso solamente a usuarios confiables. En realidad se adaptan mejor para cafés, hoteles y otros lugares de acceso público donde se esperan usuarios casuales de la red.
- Uno de los aspectos no desarrollados en esta tesis es la limitación de tiempo para uso de internet a los usuarios debido a que Chillispot no brinda este servicio, se debe considerar que la mayoría de los usuarios se conectarán a la red con propósitos investigativos por lo tanto no es recomendable limitar su tiempo de

navegación ya que se puede interrumpir cualquier acción importante que se esté realizando.

RECOMENDACIONES

- Si se emplea mecanismos de autenticación con nombres de usuario y clave, es necesario concientizar a los usuarios la importancia de mantener sus claves seguras con normas básicas como que no deben anotarlas en ningún lugar como recordatorio o que no deben facilitárselas a otras personas.
- Debido a que la presente Tesis está basada en una infraestructura que emplea como elementos principales servidores, es recomendable establecer políticas de respaldo de la información, de los equipos más críticos, en este caso del servidor RADIUS, así como también de una política de respaldo continua de la información de base de datos y configuraciones de los equipos.
- Debido a que algunos portales ofrecen solo autenticación sin ninguna encriptación de password o datos del usuario, es importante verificar que el portal ofrezca los requerimientos en seguridad como obtener información acerca de la técnica de encriptación y protocolos.
- Escoger únicamente los paquetes necesarios a ser instalados en nuestro servidor porque de lo contrario se puede llegar a ocupar demasiado espacio en disco.
- La aplicación de autenticación de chillispot interactúa con una aplicación externa para registro de nuevos usuarios que interactúa con los WebServices de la ESPOCH se recomienda investigar sobre portales cautivos que muestren un código más flexible en sus aplicaciones de autenticación que permitan el consumo de WebServices en su propia interfaz de manera que el registro de los usuarios sea transparente.

RESUMEN

La finalidad de esta tesis fue el estudio Comparativo de los portales cautivos (Air Marshal, Chillispot) e Implementación de una Aplicación Web de configuración utilizando el portal cautivo seleccionado aplicado en DESITEL (Departamento de Sistemas y Telemática) de la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO". Para demostrar que el uso de este portal, permite alcanzar un alto grado de seguridad.

Destacando los parámetros de evaluación como: Facilidad de instalación, facilidad de configuración, seguridad, funcionalidad, Interfaz del Administrador, entre otros midiendo en Análisis Cuantitativo y Cualitativo cada uno de estos obteniendo en tiempo de respuesta: Chillispot (**0.41ms),** Air Marshal (**1.11ms).** Como Portal Cautivo idóneo Chillispot.

El desarrollo de la aplicación se realizó sobre el sistema operativo GNU/LINUX, debido a la estabilidad, además se ocupó FREERADIUS que garantiza la conexión para la autenticación, interoperabilidad y sobre todo seguridad.

Para el registro de los usuarios se utilizo Web Services, lo cual nos ayudó a consumir la información del Sistema Académico y Recursos Humanos de la ESPOCH.

Como conclusión se puede decir que el Portal escogido garantiza una interfaz amigable, por lo que se recomienda la implantación y utilización del sistema desarrollado cuyas funcionalidades y seguridad fueron suficientemente probadas.

SUMMARY

The purpose of this thesis was a comparative study of the captive portal (Air Marshal, Chillispot) and Implementation of a Web application configuration using the captive portal DESITEL selected applied (Department of Systems and Telematics) of the Higher Polytechnic School of Chimborazo ".To demonstrate that the use of this site, allows a high degree of safety.

Highlighting the evaluation parameters such as: Easy installation, easy configuration, security, functionality, Interface Manager, including measuring quantitative and qualitative analysis in each of these getting in response time: Chillispot (0.41ms), Air Marshal (1.11ms). Portal Cautivo Chillispot as appropriate.

The application development was done on GNU / Linux operating system, due to stability, he also ensures that the connection FreeRADIUS for authentication, interoperability, and especially security.

For the registration of users are using Web Services, which helped us to take the Academic Information System and Human Resources of the ESPOCH.

In conclusion we can say that the choice guaranteed a portal interface, which recommends the introduction and use of the developed system and safety features which were substantiated.

ANEXOS

ANEXO A

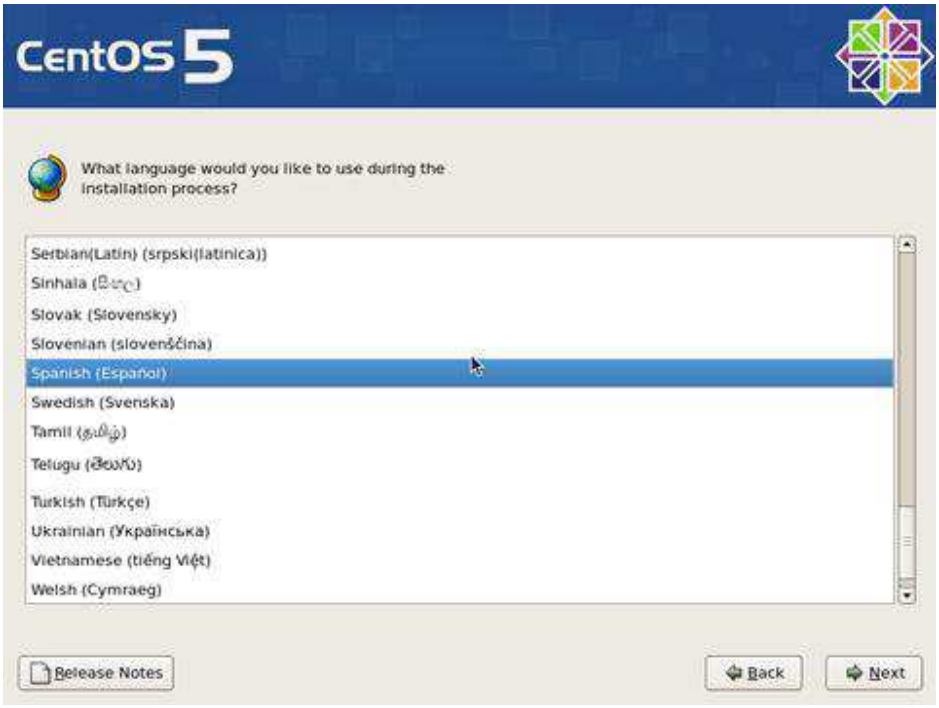
INSTALACIÓN EN MODO GRÁFICO DE CENTOS 5

Inserte el disco DVD de instalación de CentOS 5 y en cuanto aparezca el diálogo de inicio (boot), pulse la tecla ENTER o bien ingrese las opciones de instalación deseadas.

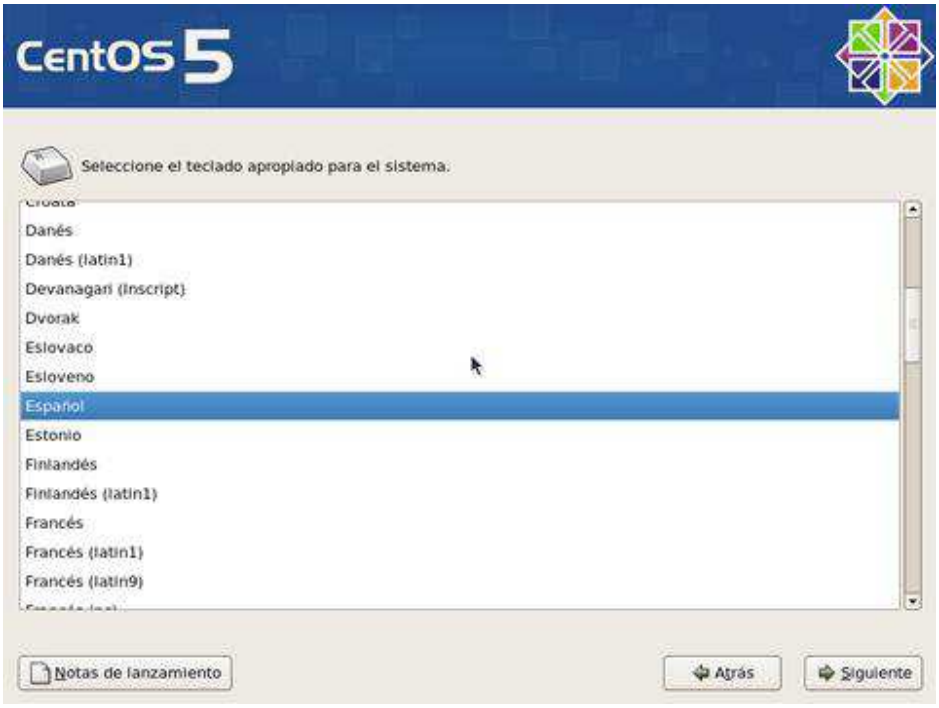
Si desea verificar la integridad del disco a partir del cual se realizará la instalación, seleccione **«OK»** y pulse la tecla ENTER, considere que esto puede demorar varios minutos. Si está seguro de que el disco o discos a partir de los cuales se realizará la instalación están en buen estado, seleccione **«Skip»** y pulse la tecla ENTER.

Haga clic sobre el botón «Next» en cuanto aparezca la pantalla de bienvenida de CentOS.

Seleccione **«Spanish»** como idioma para ser utilizado durante la instalación.



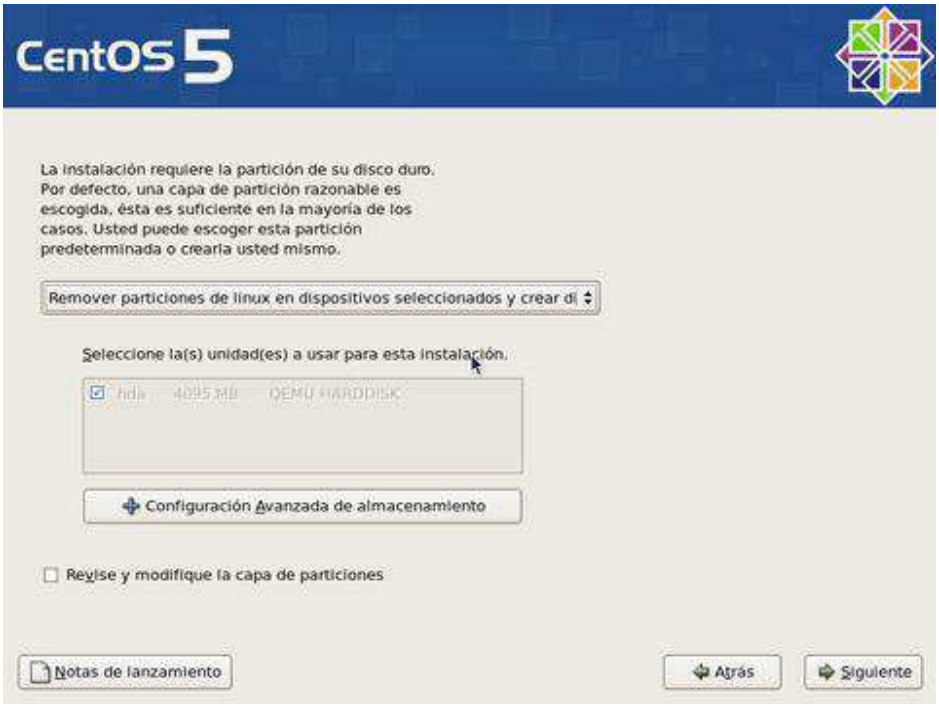
Seleccione el mapa de teclado que corresponda al dispositivo utilizado. El mapa **«Español»** o bien **«Latinoamericano»** de acuerdo a lo que corresponda. Al terminar, haga clic sobre el botón **«Siguiente»**.



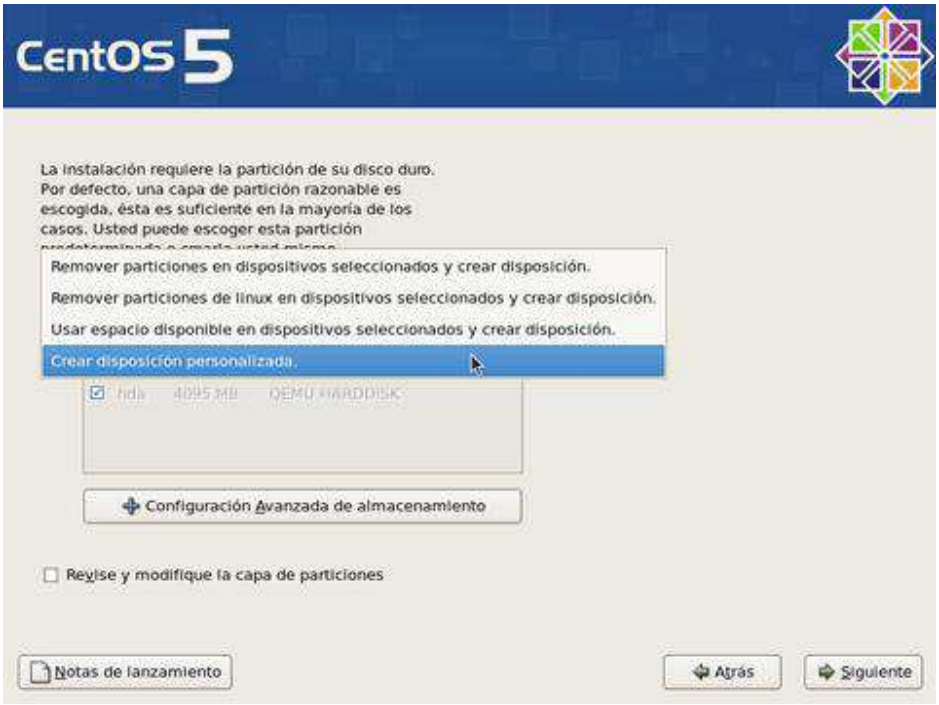
Salvo que exista una instalación previa que se desee actualizar (no recomendado), deje seleccionado **«Instalar CentOS»** y haga clic en el botón **«Siguiente»** a fin de realizar una instalación nueva.

Para crear las particiones de forma automática, lo cual puede funcionar para la mayoría de los usuarios, puede seleccionar:

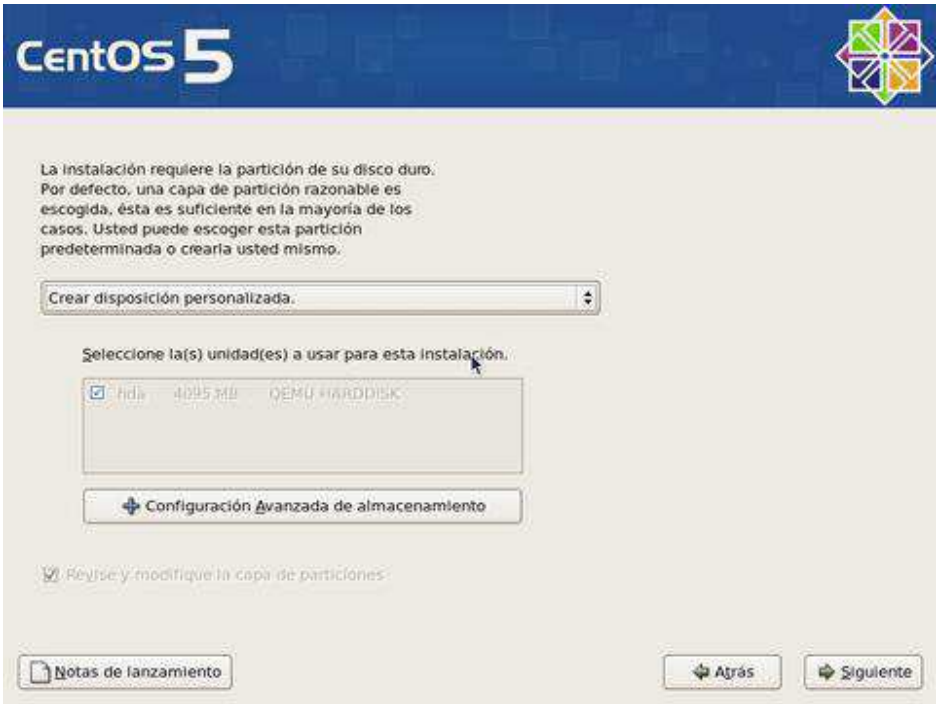
- **«Remover particiones en dispositivos seleccionados y crear disposición»**, lo cual eliminaría cualquier partición de cualquier otro sistema operativo presente, y creará de forma automática las particiones necesarias.
- **«Remover particiones de GNU/Linux en dispositivos seleccionados y crear disposición»**, lo cual eliminaría cualquier partición otra instalación de GNU/Linux presente, y creará de forma automática las particiones necesarias.
- **«Usar espacio disponible en dispositivos seleccionados y crear disposición»**, lo cual creará de forma automática las particiones necesarias en el espacio disponible.



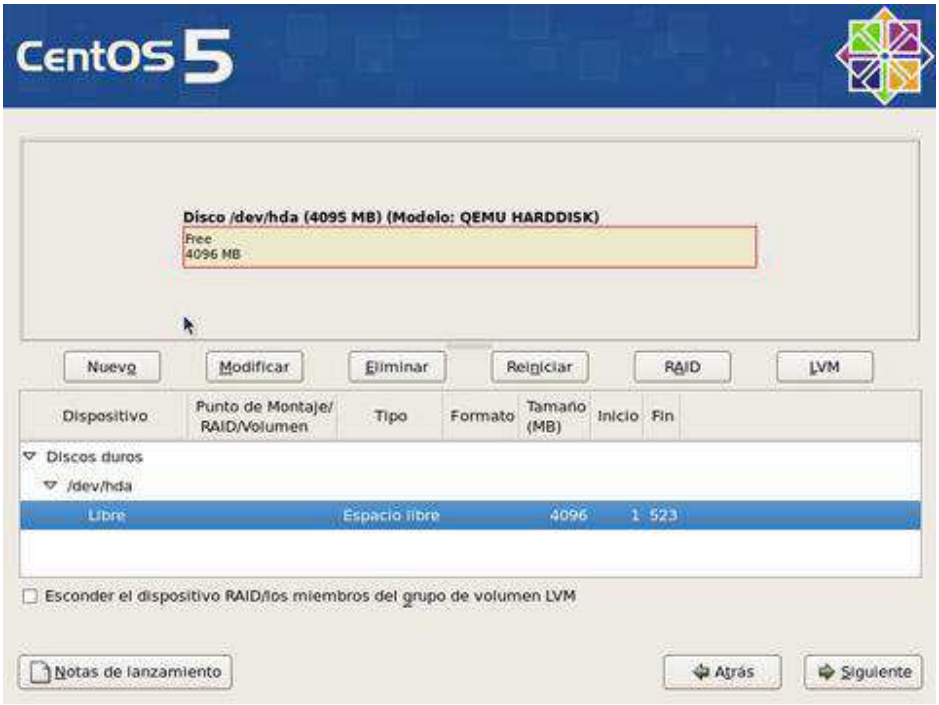
Conviene crear una disposición que permita un mayor control. Seleccione **«Crear disposición personalizada»**.



Una vez seleccionado **«Crear disposición personalizada»**, haga clic sobre el botón **«Siguiente»**.



La herramienta de particiones mostrará el espacio disponible. Haga clic en el botón **«Nuevo»**.

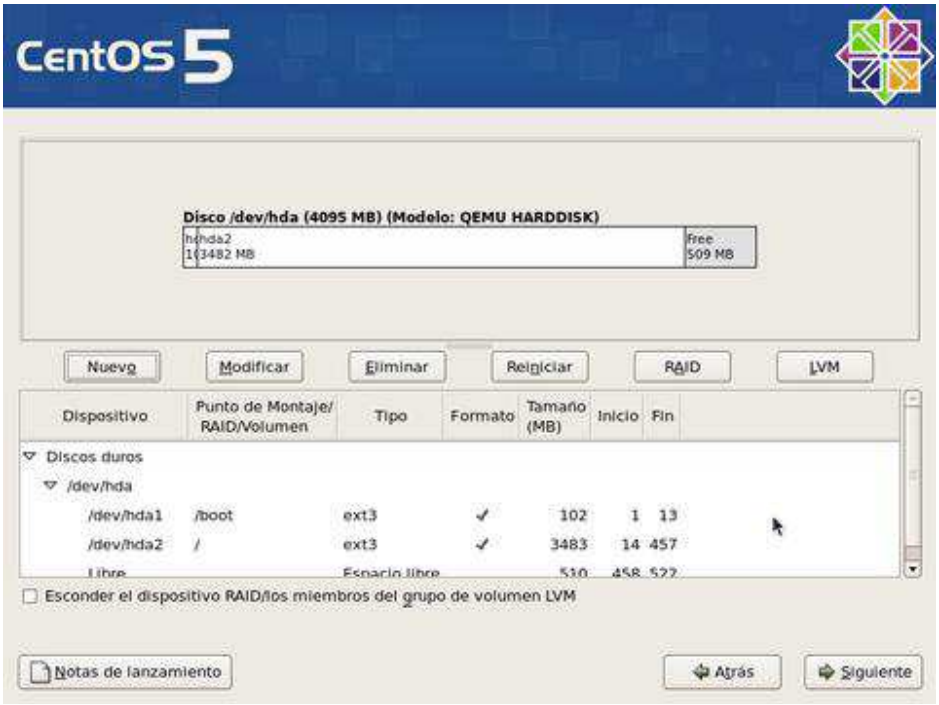


Asigne 100 MB a la partición /boot y defina ésta como partición primaria, siempre que la tabla de particiones lo permita.

Si está conforme, haga clic otra vez en el botón **«Nuevo»** y proceda a crear la siguiente partición.

Asigne a la partición / el resto del espacio disponible menos lo que tenga calculado asignar para la partición de intercambio (200% de la memoria física, o cuanto baste para 2 GB). Se recomienda asignar / como partición primaria, siempre que la tabla de particiones lo permita.

Si está conforme, haga clic otra vez en el botón **«Nuevo»** y proceda a crear la siguiente partición.



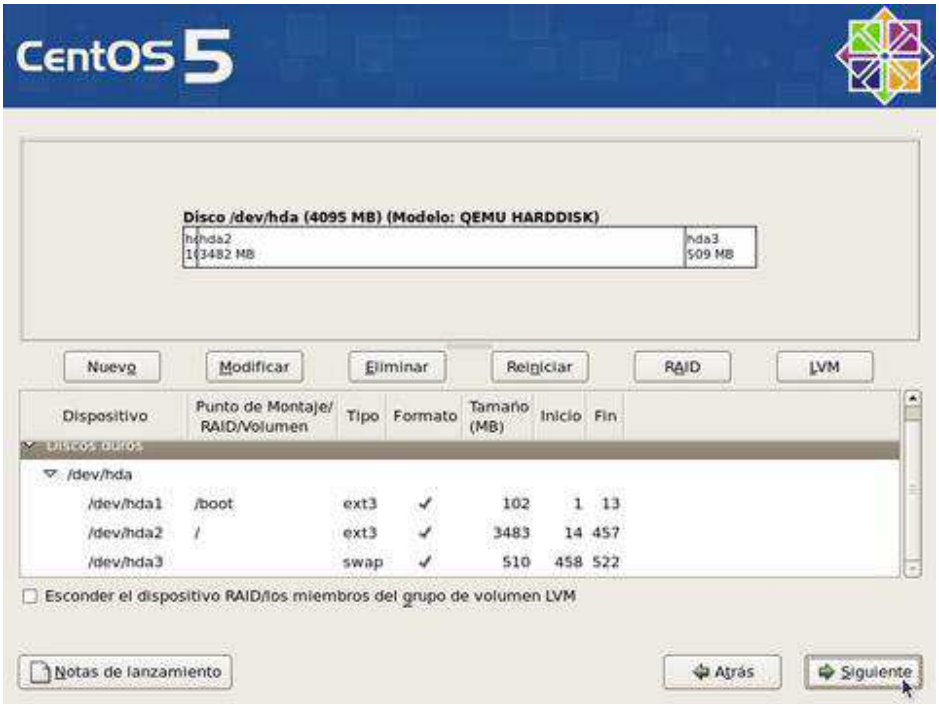
La partición para la memoria de intercambio no requiere punto de montaje. Seleccione en el campo de **«Tipo de sistema de archivos»** la opción **«swap»**, asigne el 200% de la memoria física (2*RAM). Por tratarse de la última partición de la tabla, es buena idea asignarle el espacio por rango, especificando valores ligeramente por debajo y ligeramente por arriba de lo planeado.

Otras particiones que se recomienda asignar, si se dispone del espacio en disco duro suficiente, son:

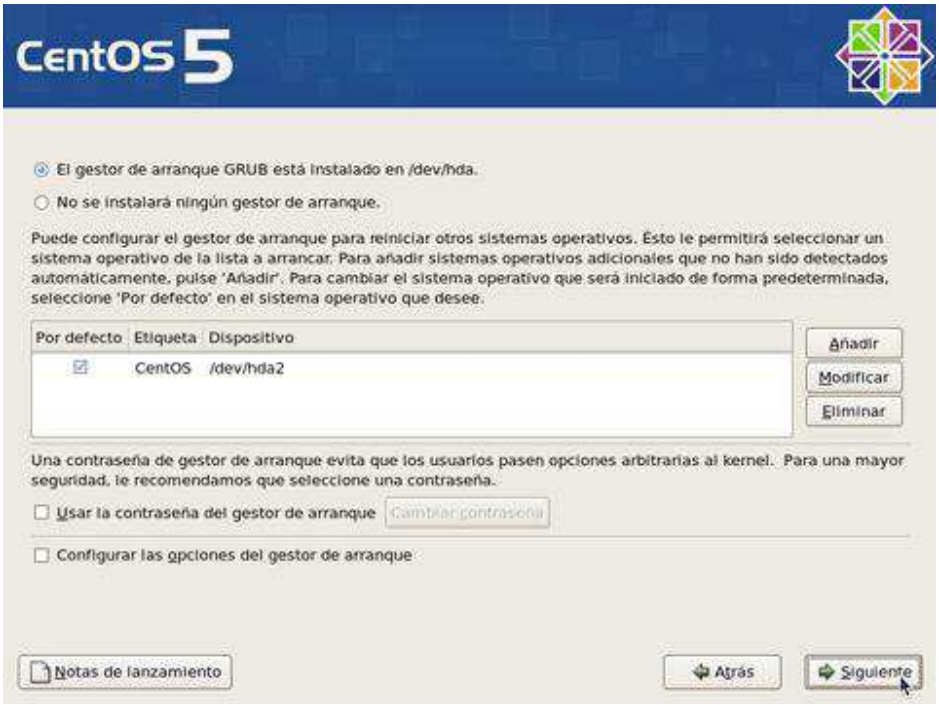
/usr	Requiere al menos 1.5 GB en instalaciones básicas. Debe considerarse el sustento lógico a utilizar a futuro. Para uso general, se recomiendan no menos de 5 GB y, de ser posible, considere un tamaño óptimo de hasta 8 GB en instalaciones promedio.
/tmp	Requiere al menos 350 MB y puede asignarse hasta 2 GB o más dependiendo de la carga de trabajo y tipo de aplicaciones. Si por ejemplo

	el sistema cuenta con un grabador de DVD, será necesario asignar a /tmp el espacio suficiente para almacenar una imagen de disco DVD, es decir, al menos 4.2 GB.
/var	Requiere al menos 512 MB en estaciones de trabajo sin servicios. En servidores regularmente se le asigna al menos la mitad del disco duro.
/home	En estaciones de trabajo se asigna al menos la mitad del disco duro a esta partición.

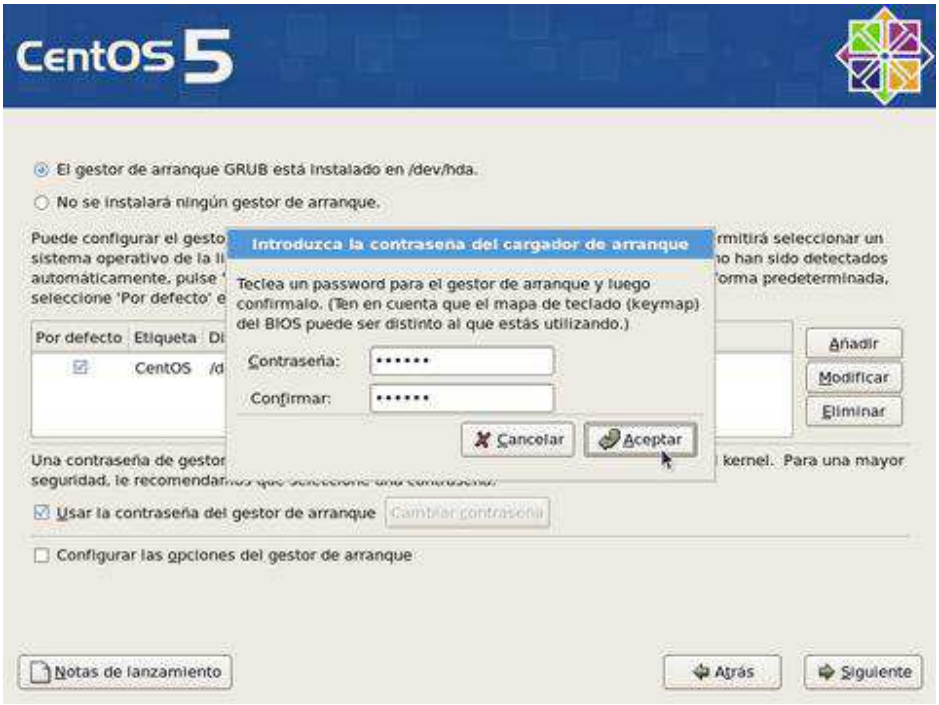
Si está conforme con la tabla de particiones creada, haga clic sobre el botón **«siguiente»** para pasar a la siguiente pantalla.



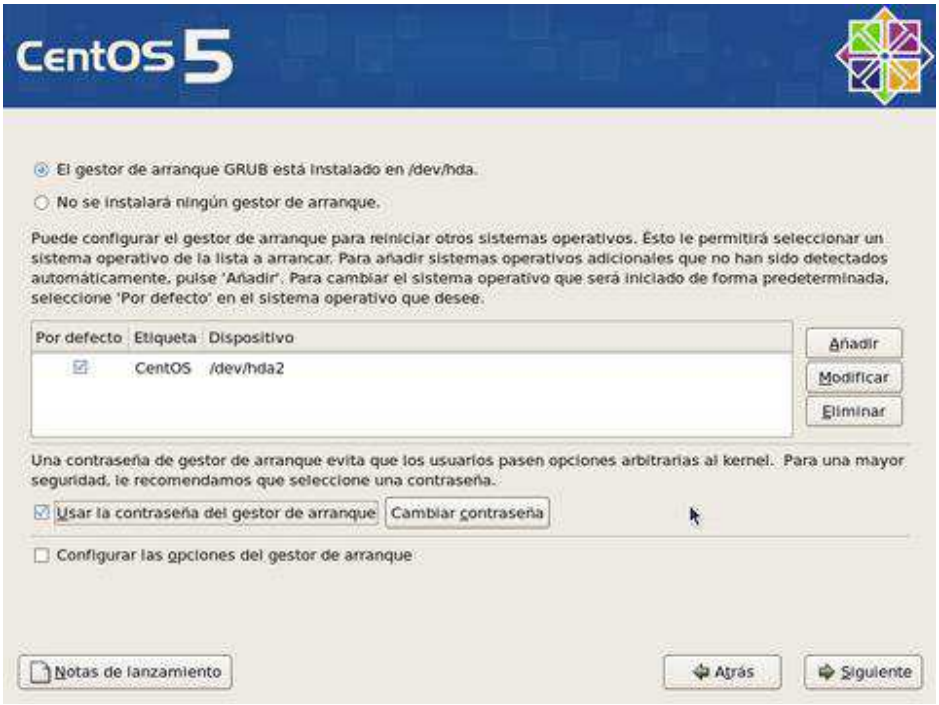
Ingresará a la configuración del gestor de arranque. Por motivos de seguridad, y principalmente con la finalidad de impedir que alguien sin autorización y con acceso físico al sistema pueda iniciar el sistema en nivel de ejecución 1, o cualquiera otro, haga clic en la casilla **«Usar la contraseña del gestor de arranque»**.



Se abrirá una ventana emergente donde deberá ingresar, con confirmación, la clave de acceso exclusiva para el gestor de arranque. Al terminar, haga clic sobre el botón **«Aceptar».**



Al terminar, haga clic sobre el botón **«Siguiente»**.



Para configurar los parámetros de red del sistema, haga clic sobre el botón **«Modificar»** para la interfaz eth0.

En la ventana emergente para modificar la interfaz eth0, desactive la casilla **«Configurar usando DHCP»** y especifique la dirección IP y máscara de subred que utilizará en adelante el sistema. Si no va a utilizar IPv6, también desactive la casilla. Confirme con el administrador de la red donde se localice que estos datos sean correctos antes de continuar. Al terminar, haga clic sobre el botón **«Aceptar»**.

Asigne un nombre de anfitrión (HOSTNAME) para el sistema. Se recomienda que dicho nombre sea un FQDN (Fully Qualified Domain Name) resuelto al menos en un DNS local. Defina, además, en esta misma pantalla, la dirección IP de la puerta de enlace y las direcciones IP de los servidores DNS de los que disponga. Si desconoce que dato ingresar, defina éste como **localhost.localdomain**. Al terminar, haga clic sobre el botón **«Siguiente»**.

Seleccione la casilla **«El sistema horario usará UTC»**, que significa que el reloj del sistema utilizará UTC (Tiempo Universal Coordinado), que es el sucesor de GMT (Greenwich Mean Time, que significa Tiempo Promedio de Greenwich), y es la zona horaria de referencia respecto a la cual se calculan todas las otras zonas del mundo. Haga clic con el ratón sobre la región que corresponda en el mapa mundial o seleccione en el siguiente campo la zona horaria que corresponda a la región donde se hospedará físicamente el sistema.

Asigne una clave de acceso al usuario **root**. Debe escribirla dos veces a fin de verificar que está coincide con lo que realmente se espera. Por razones de seguridad, se recomienda asignar una clave de acceso que evite utilizar palabras provenientes de cualquier diccionario, en cualquier idioma, así como cualquier combinación que tenga relación con datos personales.

Al terminar, haga clic sobre el botón **«Siguiente»**, y espere a que el sistema haga la lectura de información de los grupos de paquetes.

En la siguiente pantalla podrá seleccionar los grupos de paquetes que quiera instalar en el sistema. Añada o elimine a su conveniencia. Lo recomendado, sobre todo si se trata de un servidor, es realizar una instalación con el mínimo de paquetes, desactivando todas las casillas para todos los grupos de paquetes. El objeto de esto es solo instalar lo mínimo necesario para el funcionamiento del sistema operativo, y permitir instalar posteriormente solo aquello que realmente se requiera de acuerdo a la finalidad productiva que tendrá el sistema. Al terminar, haga clic sobre el botón **«Siguiente»**.

Se realizará una comprobación de dependencias de los paquetes a instalar. Este proceso puede demorar algunos minutos.

Antes de iniciar la instalación sobre el disco duro, el sistema le informará respecto a que se guardará un registro del proceso en si en el fichero **/root/install.log**. Para continuar, haga clic sobre el botón **«Siguiente»**.

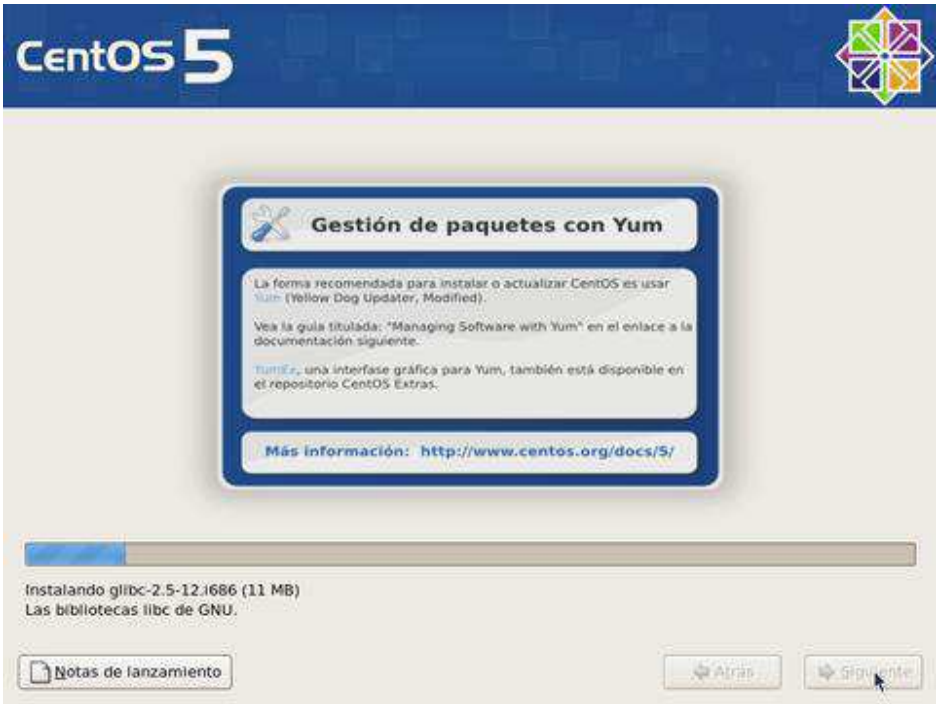
Si iniciará de forma automática el proceso de formato de las particiones que haya creado para instalar el sistema operativo. Dependiendo de la capacidad del disco duro, este proceso puede demorar algunos minutos.

Se realizará automáticamente una copia de la imagen del programa de instalación sobre el disco duro a fin de hacer más eficiente el proceso. Dependiendo de la capacidad del microprocesador y cantidad de memoria disponible en el sistema, este proceso puede demorar algunos minutos.

Espere a que se terminen los preparativos de inicio del proceso de instalación.

Se realizarán preparativos para realizar las transacciones de instalación de paquetes.

Iniciará la instalación de los paquetes necesarios para el funcionamiento del sistema operativo. Espere algunos minutos hasta que concluya el proceso.



Una vez concluida la instalación de los paquetes, haga clic sobre el botón **«Reiniciar»**.

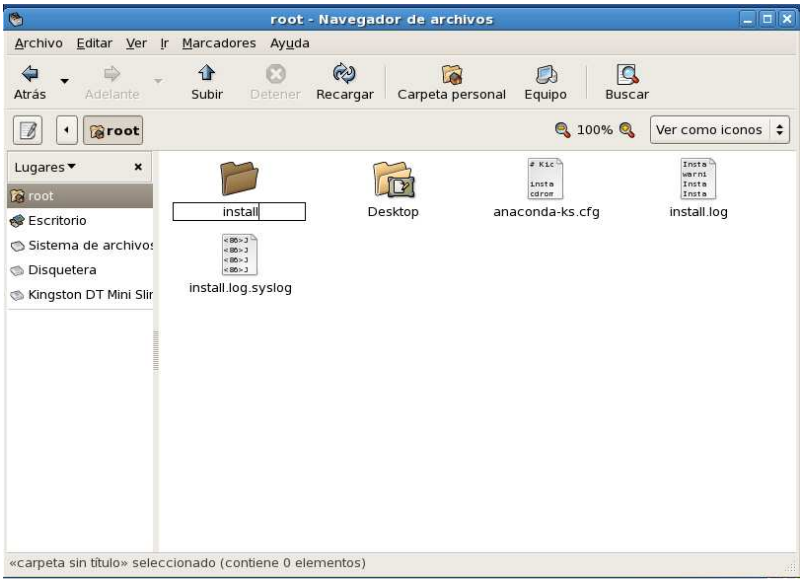

CentOS 5
Enhorabuena, la instalación ha sido completada.
Remueva cualquier medio de instalación usado durante el proceso y pulse "Reiniciar" para reiniciar su sistema.
Notas de lanzamiento
Atrás
Reiniciar

ANEXO B

INSTALACION Y CONFIGURACION DE FREERADIUS Y CHILLISPOT

En estos momentos, procederemos con la instalación y configuración de FreeRadius y Chillispot.

Creamos una carpeta "install" en la carpeta personal del root, en dicha carpeta pondremos nuestros archivos a instalar.



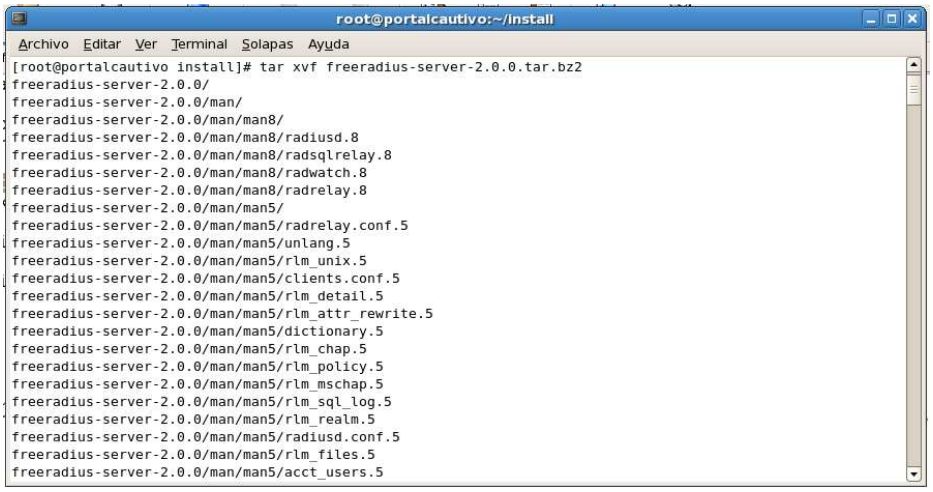
Abrimos un terminal y nos movemos a la carpeta install creada anteriormente:

cd /root/install

Descargamos el archivo freeradius-server-2.0.0.tar.bz2 (desde www.freeradius.org)

Descomprimimos nuestro archivo en /root/install con el comando:

tar xvf freeradius-server-2.0.0.tar.bz2



Nos ubicamos en la carpeta descomprimida y ejecutamos los siguientes comandos para poder instalar el servidor FreeRadius:

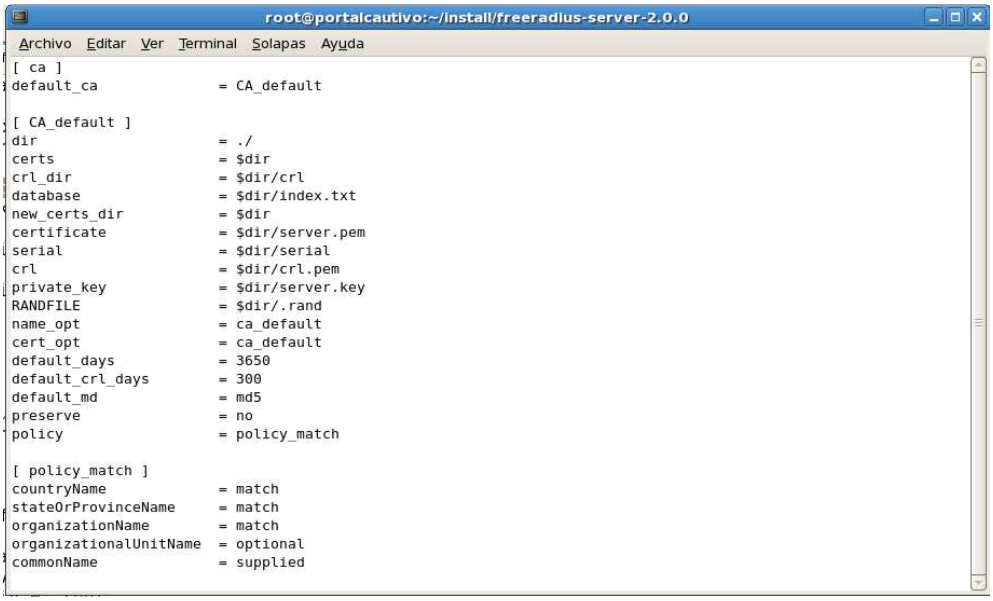
cd freeradius-server-2.0.0

./configure --prefix=/usr --sysconfdir=/etc (Especificar lo que hace)

make

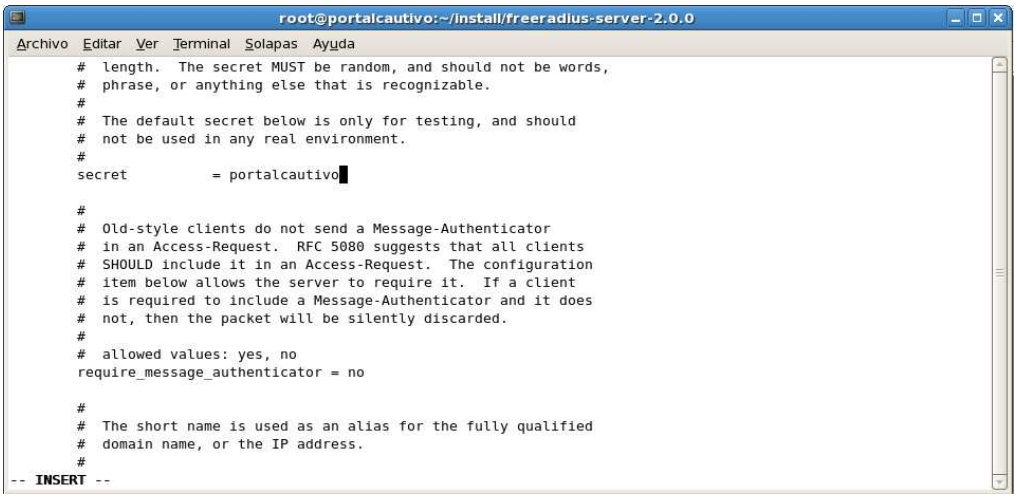
make install

Modificamos los archivos server.cnf, ca.cnf y client.cnf que se encuentran en /etc/raddb/certs; para que se creen los certificados correspondientes a nuestra empresa o entidad. Para una mayor duración de los certificados, modificamos la línea default_days de 365 a 3650 y default_crl_days de 30 a 300.



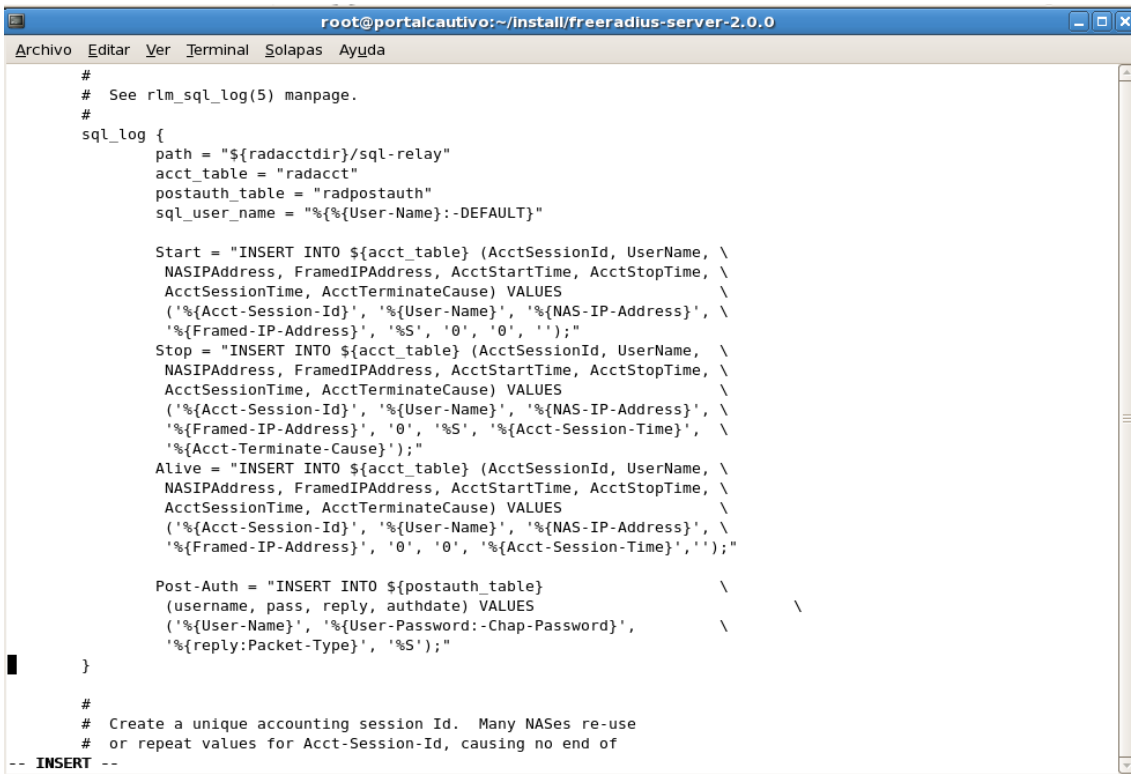
Modificamos en el archivo clients.conf la línea secret, que será la contraseña de nuestro servidor FreeRadius.

vi /etc/raddb/clients.conf



Modificar el archivo radiusd.conf ==> este archivo contiene información necesaria sobre los archivos de configuración de FreeRadius y también de la manera de conectarse a través de MySQL. Des comentar la parte que dice "sql_log".

vi /etc/raddb/radiusd.conf



Modificar las siguientes líneas dentro del archivo sql.conf

vi /etc/raddb/sql.conf

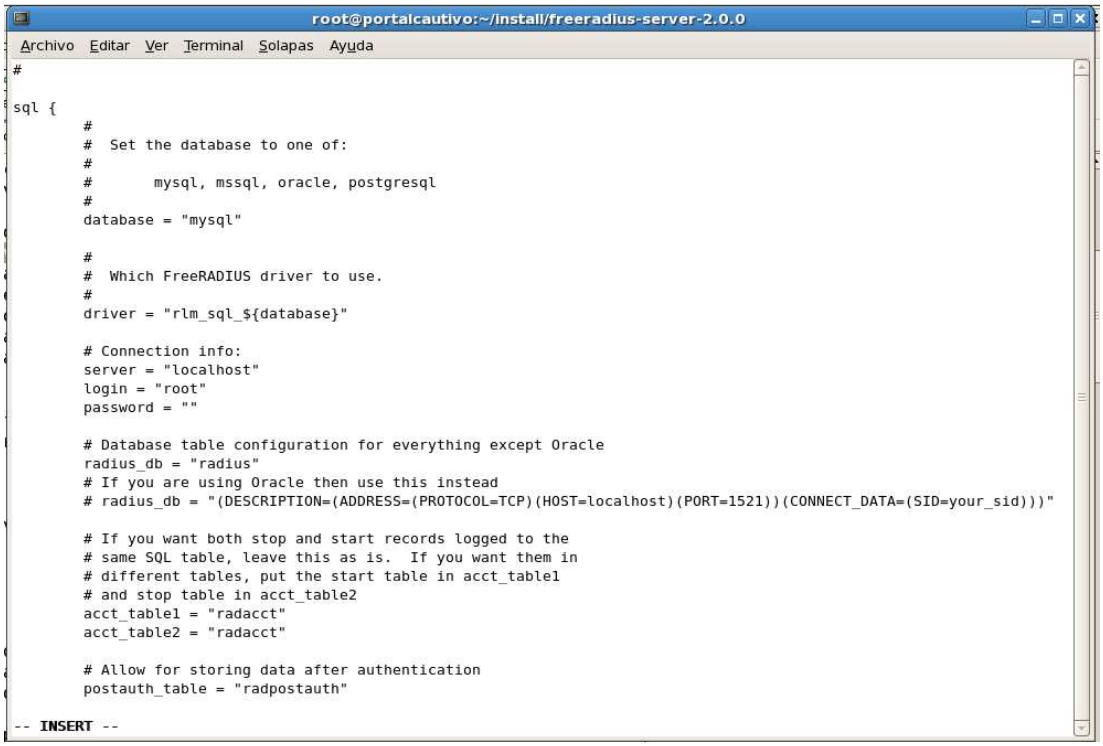
database = "mysql"

server = "localhost"

login = "root"

password = ""

radius_db = "radius"



default ==> este archivo se encuentra en /etc/raddb/sites-available, descomentar las líneas que contengan "sql" o "sql_log" en los apartados "authorize" y "accounting".

Podemos registrar nuestros usuarios usando MySQL, tenemos q crear una base de datos en blanco llamada "radius" y luego ejecutar los archivos *.sql q se encuentran dentro del directorio /etc/raddb/sql/mysql/.

Lo recomendable es hacer esto vía web con el programa webmin q más abajo detallo una breve explicacion de instalacion. Se recomienda no habilitar el soporte SSL en webmin.

Los archivos *.sql deben ejecutarse en la sección de ejecutar archivos sql.

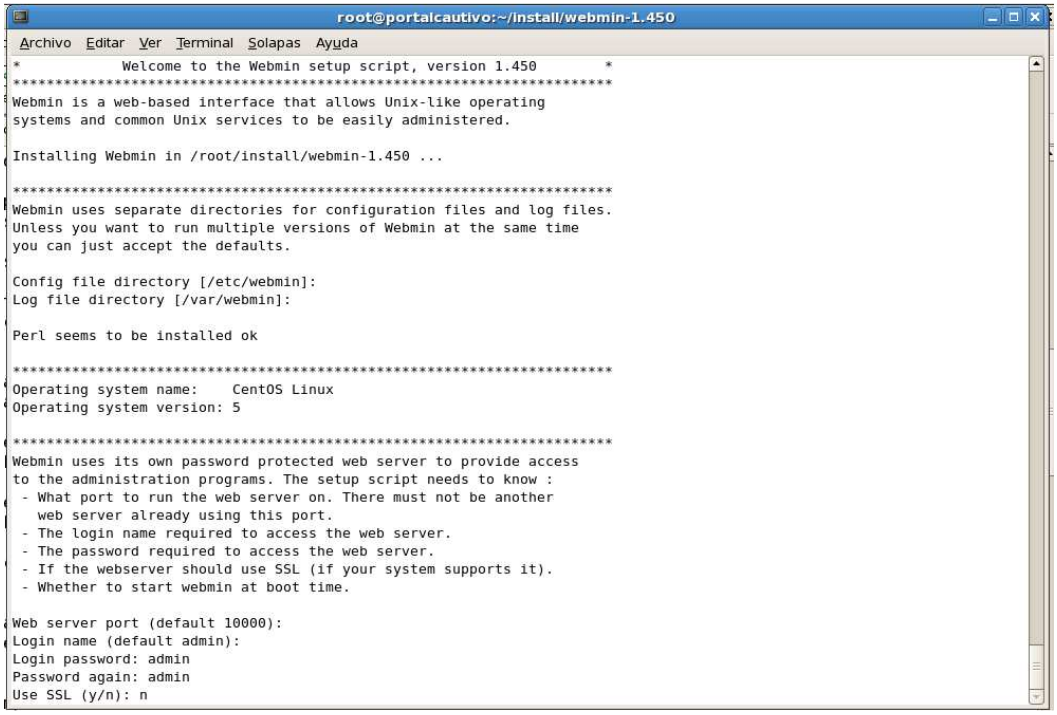
Descargamos el paquete webmin-1.4xx.tar.gz (de la página www.webmin.com)

tar xvf webmin-1.4xx.tar.gz

cd webmin-1.4xx

./setup.pl

Realizamos una instalación sencilla, aceptando por defecto el directorio de archivos de configuración y de los logs. También aceptamos el puerto por defecto que es el puerto 10000, el usuario dejamos que se llame "admin" y el password es "admin". Podemos cambiar el usuario y su password. Por último deshabilitamos el soporte SSL y aceptamos q arranque webmin cuando arranque el sistema.



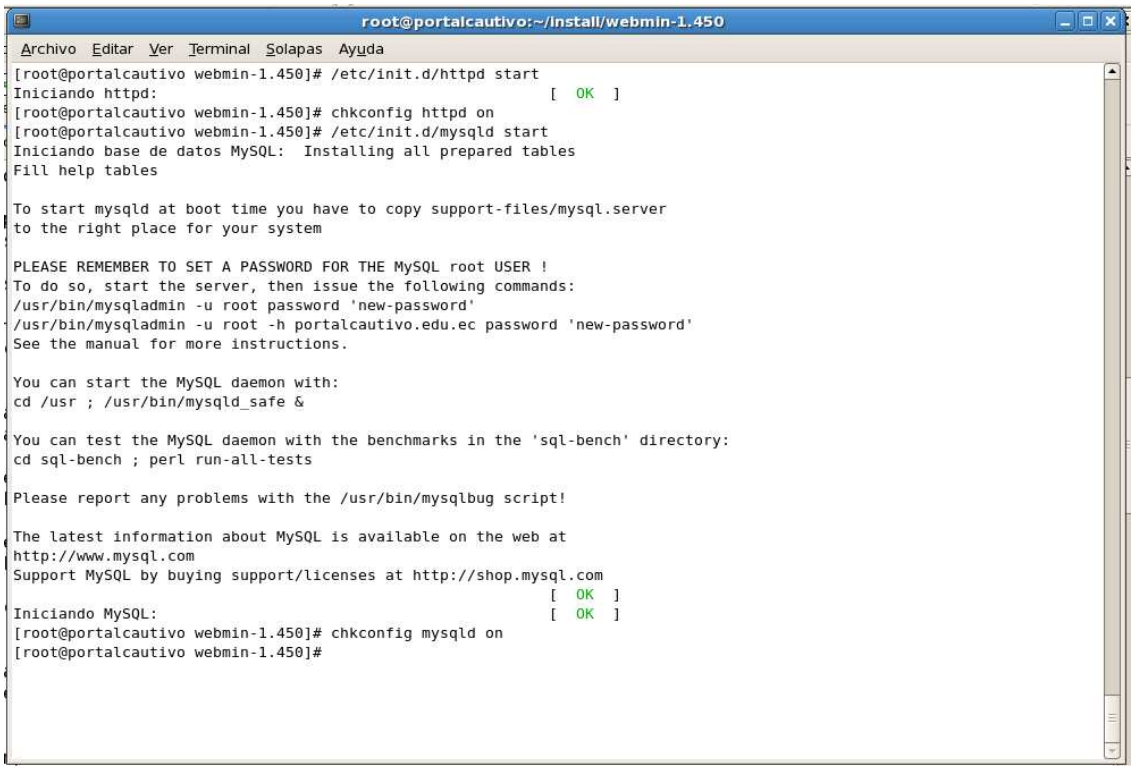
Una vez instalado, tenemos que arrancar nuestro servidor web apache y nuestra base de datos MySQL, de la siguiente manera:

/etc/init.d/mysqld start (arrancamos el servidor mysql)

chkconfig mysqld on (nuestro servidor mysql se iniciara con el sistema)

/etc/init.d/httpd start (arrancamos el servidor web apache)

chkconfig httpd on (nuestro servidor web apache se iniciara con el sistema)



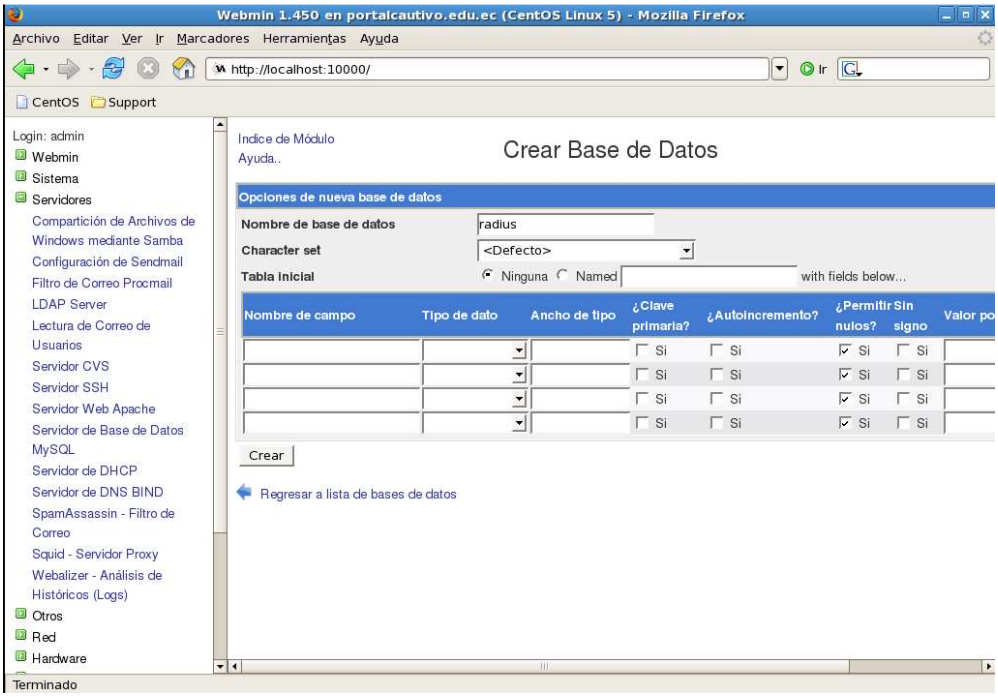
Ponemos en nuestro browser mozilla firefox, lo siguiente para ejecutar el paquete webmin:

http://localhost:10000/

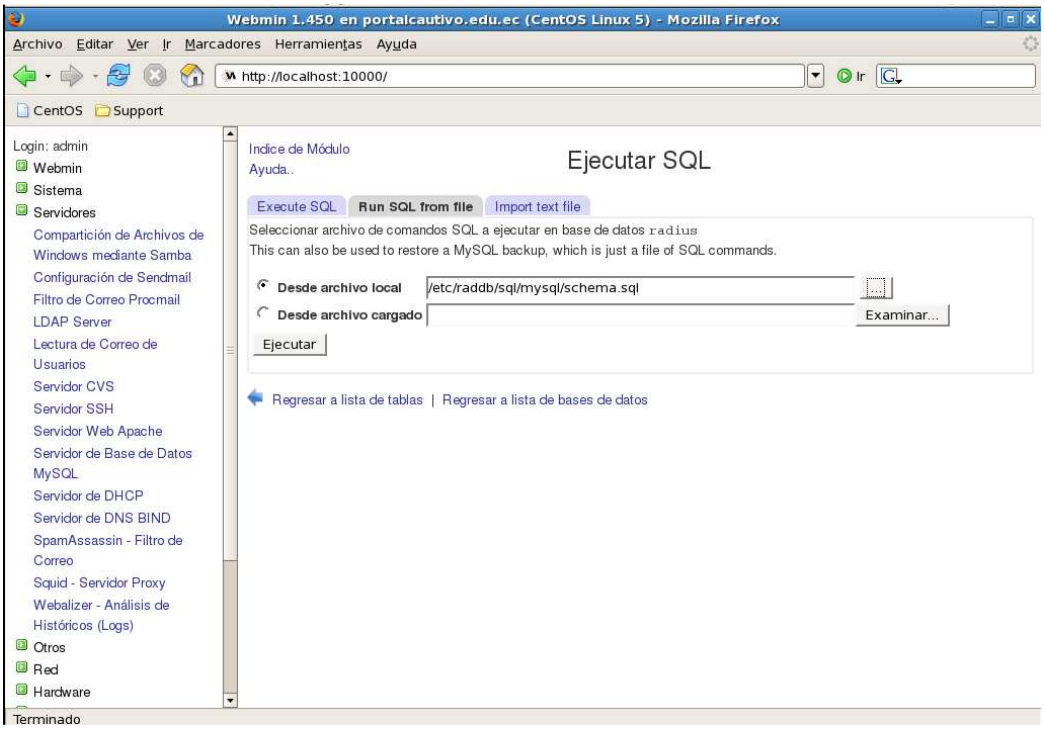
Luego de autenticarnos, podemos ingresar a la interfaz web para configurar nuestro sistema. Se puede cambiar el idioma del webmin a español o dejar el idioma inglés por defecto.

Ahora tenemos que ir al apartado Servidores y ubicarnos en Servidor de Base de Datos MySQL, luego de esto se nos mostrara una pantalla en la cual elegimos crear una nueva base de datos.

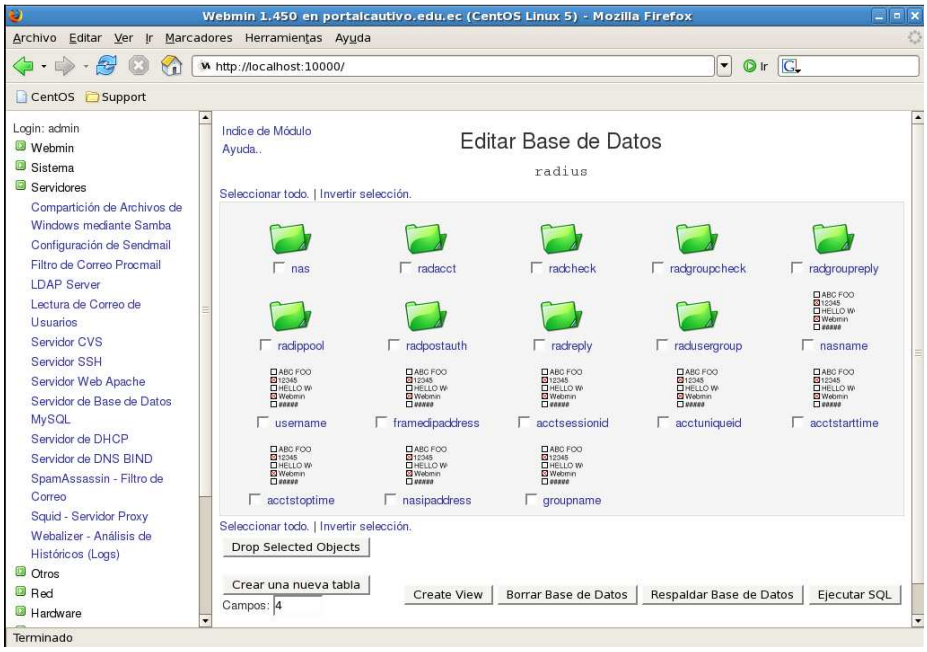
Creamos una base de datos llamada radius y no ponemos nada en el resto de campos.



Luego damos clic sobre la base de datos radius y damos clic en ejecutar SQL para poder ejecutar los archivos sql. Escogemos la opción Run SQL from file y ubicamos nuestros archivos sql.



Cuando se haya ejecutado los tres archivos sql, nuestra base de datos radius deberá quedar de la siguiente manera:



Una vez q tengamos nuestra base de datos radius con las tablas correspondientes, procedemos a llenar la tabla "radcheck" que es la tabla más importante ya que en esta se almacenan los usuarios.

El formato de los campos, es el siguiente:

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

ANEXO C

CONFIGURACIÓN DE LA COMUNICACIÓN ENTRE EL ACCESS POINT Y EL SERVIDOR

La comunicación entre el Access Point y el servidor radius se realiza mediante la conexión de las interfaces de red. Se debe tener en cuenta los siguientes aspectos:

Deshabilitar dhcp en el Access Point.

El AP debe estar en la misma red que el servidor.

El servidor debe tener una interfaz conectada directamente al AP.

ANEXO D

ARCHIVOS DE CONFIGURACIÓN UTILIZADOS EN LA IMPLEMENTACIÓN

RADIUSD.CONF

El archivo de configuración # -*- text -*-

##

radiusd.conf -- FreeRADIUS server configuration file.

Configuración de la ubicación de los archivos radius

#prefix = /usr

exec_prefix = ${prefix}

sysconfdir = /etc

localstatedir = ${prefix}/var

sbindir = ${exec_prefix}/sbin

logdir = ${localstatedir}/log/radius

raddbdir = ${sysconfdir}/raddb

radacctdir = ${logdir}/radacct

confdir = ${raddbdir}

run_dir = ${localstatedir}/run/radiusd

Configuración de la ubicación de los archivos log

log_destination = files

Configuración de la ubicación de los archivos de librería

libdir = /usr/lib

Configuración de la ubicación de los archivos de ejecución

pidfile = ${run_dir}/radiusd.pid

Configuración de tiempos de envío de paquetes

max_request_time = 30

cleanup_delay = 5

max_requests = 1024

Configuraciones de puertos

```
listen {
        ipaddr = *
        port = 0
        type = auth
}
listen {
        ipaddr = *
        port = 0
        type = acct
}
hostname_lookups = no
allow_core_dumps = no
regular_expressions = yes
extended_expressions        = yes
log {
        syslog_facility = daemon
        file = ${logdir}/radius.log
        stripped_names = no
```

```
        auth = no
        auth_badpass = no
        auth_goodpass = no
}
checkrad = ${sbindir}/checkrad
```

Configuración de seguridad

```
security {
        max_attributes = 200
        reject_delay = 1
        status_server = yes
}
```

Configuración del proxy

```
proxy_requests  = yes
$INCLUDE proxy.conf
$INCLUDE clients.conf
snmp  = no
$INCLUDE snmp.conf
thread pool {
        start_servers = 5

        max_servers = 32
        min_spare_servers = 3
        max_spare_servers = 10
        max_requests_per_server = 0
}
```

Configuración del módulo de configuración

```
modules {
        pap {
                auto_header = no
        }
        chap {
                authtype = CHAP
        }
        pam {
                pam_auth = radiusd
        }

        unix {
                radwtmp = ${logdir}/radwtmp
        }

$INCLUDE eap.conf
        ldap {
                server = "ldap.your.domain"
                basedn = "o=My Org,c=UA"
                filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
                ldap_connections_number = 5
                timeout = 4
                timelimit = 3
                net_timeout = 1
```

```
        tls {
                start_tls = no
        }
        dictionary_mapping = ${confdir}/ldap.attrmap
        edir_account_policy_check = no
realm IPASS {
        format = prefix
        delimiter = "/"
}
realm suffix {
        format = suffix
        delimiter = "@"
}
realm realmpercent {
        format = suffix
        delimiter = "%"
}
realm ntdomain {
        format = prefix
        delimiter = "\\"
}
checkval {
        item-name = Calling-Station-Id
        check-name = Calling-Station-Id
        data-type = string
}
```

```
preprocess {
        huntgroups = ${confdir}/huntgroups
        hints = ${confdir}/hints
        with_ascend_hack = no
        ascend_channels_per_line = 23
        with_ntdomain_hack = no
        with_specialix_jetstream_hack = no
        with_cisco_vsa_hack = no
}
files {
        usersfile = ${confdir}/users
        acctusersfile = ${confdir}/acct_users
        preproxy_usersfile = ${confdir}/preproxy_users
        compat = no
}
detail {
        detailfile = ${radacctdir}/%{Client-IP-Address}/detail-%Y%m%d
        detailperm = 0600
        header = "%t"
}
detail auth_log {
        detailfile = ${radacctdir}/%{Client-IP-Address}/auth-detail-%Y%m%d
        detailperm = 0600

 }
 detail reply_log {
```

```
        detailfile = ${radacctdir}/%{Client-IP-Address}/reply-detail-%Y%m%d
       detailperm = 0600
}
sql_log {
        path = "${radacctdir}/sql-relay"
        acct_table = "radacct"
        postauth_table = "radpostauth"
        sql_user_name = "%{%{User-Name}:-DEFAULT}"
        Start = "INSERT INTO ${acct_table} (AcctSessionId, UserName, \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '%S', '0', '0', '');"
        Stop = "INSERT INTO ${acct_table} (AcctSessionId, UserName,  \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '0', '%S', '%{Acct-Session-Time}',  \
         '%{Acct-Terminate-Cause}');"
        Alive = "INSERT INTO ${acct_table} (AcctSessionId, UserName, \
         NASIPAddress, FramedIPAddress, AcctStartTime, AcctStopTime, \
         AcctSessionTime, AcctTerminateCause) VALUES                 \
         ('%{Acct-Session-Id}', '%{User-Name}', '%{NAS-IP-Address}', \
         '%{Framed-IP-Address}', '0', '0', '%{Acct-Session-Time}','');"

        Post-Auth = "INSERT INTO ${postauth_table}                   \
```

```
                (username, pass, reply, authdate) VALUES                        \
                ('%{User-Name}', '%{User-Password:-Chap-Password}',      \
                '%{reply:Packet-Type}', '%S');"
        }
        acct_unique {
                key = "User-Name, Acct-Session-Id, NAS-IP-Address, Client-IP-Address,
NAS-Port"
        }
        $INCLUDE sql.conf
radutmp {
                filename = ${logdir}/radutmp
                case_sensitive = yes
                check_with_nas = yes
                perm = 0600
                callerid = "yes"
        }
        radutmp sradutmp {
                filename = ${logdir}/sradutmp
                perm = 0644
                callerid = "no"
        }
        attr_filter attr_filter.post-proxy {
                attrsfile = ${confdir}/attrs
        }
        attr_filter attr_filter.pre-proxy {
                attrsfile = ${confdir}/attrs.pre-proxy
```

```
}
attr_filter attr_filter.access_reject {
        key = %{User-Name}
        attrsfile = ${confdir}/attrs.access_reject
}
attr_filter attr_filter.accounting_response {
        key = %{User-Name}
        attrsfile = ${confdir}/attrs.accounting_response
}
counter daily {
        filename = ${confdir}/db.daily
        key = User-Name
        count-attribute = Acct-Session-Time
        reset = daily
        counter-name = Daily-Session-Time
        check-name = Max-Daily-Session
        reply-name = Session-Timeout
        allowed-servicetype = Framed-User
        cache-size = 5000
}
always fail {
        rcode = fail
}
always reject {
        rcode = reject
}
```

```
always noop {
        rcode = noop
}
always handled {
        rcode = handled
}
always updated {
        rcode = updated
}
always notfound {
        rcode = notfound
}
always ok {
        rcode = ok
        simulcount = 0
        mpp = no
}
#  The module also registers a few paircompare functions
expr {
}
est {
}
expiration {
        reply-message = "Password Has Expired\r\n"
}
logintime {
```

```
        reply-message = "You are calling outside your allowed timespan\r\n"
        minimum-timeout = 60
}
exec {
        wait = yes
        input_pairs = request
        shell_escape = yes
        output = none
}
exec echo {
        wait = yes
        program = "/bin/echo %{User-Name}"
        input_pairs = request
        output_pairs = reply
        shell_escape = yes
}
ippool main_pool {
        range-start = 192.168.1.1
        range-stop = 192.168.3.254
        netmask = 255.255.255.0
        cache-size = 800
        session-db = ${confdir}/db.ippool
        ip-index = ${confdir}/db.ipindex
        override = no
        maximum-timeout = 0
}
```

```
}



instantiate {
        exec
        expr
        expiration
        logintime
}
$INCLUDE policy.conf
```

CLIENTS.CONF

```
# -*- text -*-
##
client localhost {
        #  Allowed values are:
        #        dotted quad (1.2.3.4)
        #       hostname    (radius.example.com)
        ipaddr = 127.0.0.1
        secret          = portalcautivo
        allowed values: yes, no
        require_message_authenticator = no
        nastype     = other    # localhost isn't usually a NAS...
}
```

Sql.conf

```
# -*- text -*-
## sql.conf -- SQL modules
#  Configuration for the SQL module
#
sql {
        database = "mysql"
        driver = "rlm_sql_${database}"
        # Connection info:
        server = "localhost"
        login = "root"
        password = ""
```

```
        # Database table configuration for everything except Oracle
        radius_db = "radius"
        acct_table1 = "radacct"
        acct_table2 = "radacct"
        postauth_table = "radpostauth"
        authcheck_table = "radcheck"
        authreply_table = "radreply"

        groupcheck_table = "radgroupcheck"
        groupreply_table = "radgroupreply"
        usergroup_table = "radusergroup"
        deletestalesessions = yes
        sqltrace = no
        sqltracefile = ${logdir}/sqltrace.sql
        num_sql_socks = 5
        connect_failure_retry_delay = 60
        nas_table = "nas"
        $INCLUDE sql/${database}/dialup.conf
}
```

CHILLI.CONF

```
# TAG: fg
# Include this flag if process is to run in the foreground
#fg

# TAG: debug
# Include this flag to include debug information.
#debug

# TAG: interval
# Re-read configuration file at this interval. Will also cause new domain
# name lookups to be performed. Value is given in seconds.
#interval 3600

# TAG: pidfile
# File to store information about the process id of the program.
# The program must have write access to this file/directory.
#pidfile /var/run/chilli.pid

# TAG: statedir
# Directory to use for nonvolatile storage.
# The program must have write access to this directory.
# This tag is currently ignored
#statedir ./
```

```
# TUN parameters


# TAG: net
# IP network address of external packet data network
# Used to allocate dynamic IP addresses and set up routing.
# Normally you do not need to uncomment this tag.
#net 192.168.182.0/24

# TAG: dynip
# Dynamic IP address pool
# Used to allocate dynamic IP addresses to clients.
# If not set it defaults to the net tag.
# Do not uncomment this tag unless you are an experienced user!
#dynip 192.168.182.0/24

# TAG: statip
# Static IP address pool
# Used to allocate static IP addresses to clients.
# Do not uncomment this tag unless you are an experienced user!
#statip 192.168.182.0/24


# TAG: dns1
# Primary DNS server.
# Will be suggested to the client.
```

```
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
#dns1 192.168.1.1

# TAG: dns2
# Secondary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
#dns2 172.16.0.6

# TAG: domain
# Domain name
# Will be suggested to the client.
# Normally you do not need to uncomment this tag.
#domain espoch.edu.ec

# TAG: ipup
# Script executed after network interface has been brought up.
# Executed with the following parameters: <devicename> <ip address>
# <mask>
# Normally you do not need to uncomment this tag.
#ipup /etc/chilli.ipup

# TAG: ipdown
# Script executed after network interface has been taken down.
```

```
# Executed with the following parameters: <devicename> <ip address>
# <mask>
# Normally you do not need to uncomment this tag.
#ipdown /etc/chilli.ipdown

# TAG: conup
# Script executed after a user has been authenticated.
# Executed with the following parameters: <devicename> <ip address>
# <mask> <user ip address> <user mac address> <filter ID>
# Normally you do not need to uncomment this tag.
#conup /etc/chilli.conup

# TAG: conup
# Script executed after a user has disconnected.
# Executed with the following parameters: <devicename> <ip address>
# <mask> <user ip address> <user mac address> <filter ID>
# Normally you do not need to uncomment this tag.
#conup /etc/chilli.condown

# Radius parameters

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

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

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

# TAG: radiusauthport
# Radius authentication port
# The UDP port number to use for radius authentication requests.
# The same port number is used for both radiusserver1 and radiusserver2.
# Normally you do not need to uncomment this tag.
#radiusauthport 1812

# TAG: radiusacctport
# Radius accounting port
# The UDP port number to use for radius accounting requests.
# The same port number is used for both radiusserver1 and radiusserver2.
# Normally you do not need to uncomment this tag.
#radiusacctport 1813
```

TAG: radiussecret

Radius shared secret for both servers

For all installations you should modify this tag.

Password del servidor radius

radiussecret portalcautivo

TAG: radiusnasid

Radius NAS-Identifier

Normally you do not need to uncomment this tag.

#radiusnasid nas01

TAG: radiusnasip

Radius NAS-IP-Address

Normally you do not need to uncomment this tag.

#radiusnasip 127.0.0.1

TAG: radiuscalled

Radius Called-Station-ID

Normally you do not need to uncomment this tag.

#radiuscalled 00133300

TAG: radiuslocationid

WISPr Location ID. Should be in the format: isocc=<ISO_Country_Code>,

cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<ssid/ZONE>

Normally you do not need to uncomment this tag.

#radiuslocationid isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport

TAG: radiuslocationname

```
# WISPr Location Name. Should be in the format:
# <HOTSPOT_OPERATOR_NAME>,<LOCATION>
# Normally you do not need to uncomment this tag.
#radiuslocationname ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport

# Radius proxy parameters
# TAG: proxylisten
# IP address to listen to
# Normally you do not need to uncomment this tag.
#proxylisten 10.0.0.1

# TAG: proxyport
# UDP port to listen to.
# If not specified a port will be selected by the system
# Normally you do not need to uncomment this tag.
#proxyport 1645

# TAG: proxyclient
# Client(s) from which we accept radius requests
# Normally you do not need to uncomment this tag.
#proxyclient 10.0.0.1/24

# TAG: proxysecret
# Radius proxy shared secret for all clients
# If not specified defaults to radiussecret
# Normally you do not need to uncomment this tag.
```

#proxysecret testing123

Remote configuration management

TAG: confusername

If confusername is specified together with confpassword chillispot

will at regular intervals specified by the interval option query the

radius server for configuration information.

Normally you do not need to uncomment this tag.

#confusername conf

TAG: confpassword

If confusername is specified together with confpassword chillispot

will at regular intervals specified by the interval option query the

radius server for configuration information.

Normally you do not need to uncomment this tag.

#confpassword secret

DHCP Parameters

TAG: dhcpif

Ethernet interface to listen to.

This is the network interface which is connected to the access points.

In a typical configuration this tag should be set to eth1.

Interfaz por la cual el servidor proporciona DHCP

dhcpif eth1

TAG: dhcpmac

```
# Use specified MAC address.
# An address in the range  00:00:5E:00:02:00 - 00:00:5E:FF:FF:FF falls
# within the IANA range of addresses and is not allocated for other
# purposes.
# Normally you do not need to uncomment this tag.
#dhcpmac 00:00:5E:00:02:00

# TAG: lease
# Time before DHCP lease expires
# Normally you do not need to uncomment this tag.
#lease 600

# Universal access method (UAM) parameters
# TAG: uamserver
# URL of web server handling authentication.
uamserver https://192.168.182.1/cgi-bin/hotspotlogin.cgi
#uamserver https://192.168.182.1/ejemplo/index.php

# TAG: uamhomepage
# URL of welcome homepage.
# Unauthenticated users will be redirected to this URL. If not specified
# users will be redirected to the uamserver instead.
# Normally you do not need to uncomment this tag.
#uamhomepage http://192.168.182.1/welcome.html

# TAG: uamsecret
```

```
# Shared between chilli and authentication web server
#uamsecret ht2eb8ej6s4et3rg1ulp

# TAG: uamlisten
# IP address to listen to for authentication requests
# Do not uncomment this tag unless you are an experienced user!
#uamlisten 192.168.182.1

# TAG: uamport
# TCP port to listen to for authentication requests
# Do not uncomment this tag unless you are an experienced user!
#uamport 3990

# TAG: uamallowed
# Comma separated list of domain names, IP addresses or network segments
# the client can access without first authenticating.
# It is possible to specify this tag multiple times.
# Normally you do not need to uncomment this tag.
#uamallowed www.chillispot.org,10.11.12.0/24

# TAG: uamanydns
# If this flag is given unauthenticated users are allowed to use
# any DNS server.
# Normally you do not need to uncomment this tag.
#uamanydns
```

MAC authentication

TAG: macauth

If this flag is given users will be authenticated only on their MAC

address.

Normally you do not need to uncomment this tag.

#macauth

TAG: macallowed

List of MAC addresses.

The MAC addresses specified in this list will be authenticated only on

their MAC address.

This tag is ignored if the macauth tag is given.

It is possible to specify this tag multiple times.

Normally you do not need to uncomment this tag.

#macallowed 00-0A-5E-AC-BE-51,00-30-1B-3C-32-E9

TAG: macpasswd

Password to use for MAC authentication.

Normally you do not need to uncomment this tag.

#macpasswd password

TAG: macsuffix

Suffix to add to MAC address in order to form the username.

Normally you do not need to uncomment this tag.

#macsuffix suffix

BIBLIOGRAFIA

BIBLIOGRAFÍA EN INTERNET

AIR MARSHAL

http://AirMarshal\CaptivePortal-HotSpotAuthenticationGateway-AirMarshal.mht

2009/05/26

http://en.wikipedia.org/wiki/Air_Marshal

2009/04/26

http://www.ecualug.org/2009/06/23/forums/archivo_de_configuracion_principal_de_airmarshal

2009/05/08

ASOCIACIÓN DE USUARIOS GNU/LINUX:

http://www.linuca.org/body.phtml?nIdNoticia=288.

2009/04/01

http://www.cmt.es/cmt/document/decisiones/2003/RE−03−11−13−02.pdf.

2009/04/10

http://soporte.ecci.ucr.ac.cr/node/15.

2009/05/01

CHILLISPOT

http://www.chillispot.org/download.html.

2009/04/13

http://en.wikipedia.org/wiki/ChilliSpot

2009/04/16

http://www.linuca.org/body.phtml?nIdNoticia=288

2009/06/09

http://HowtoDebianLenny5+Chillispoat+Freeradius+Apache2«Herymx'sGround Zero.mht.

2009/04/22

FORO "WIRELESS" EN HISPALINUX.

http://listas.hispalinux.es/mailman/listinfo/wireless.

Cursos: Herymx´s Ground Zero mht.

HERRAMIENTA

http://www.iea-software.com/products/radlogin4.cfm.

2009/06/06

NAVEGADORES

http://www.mozilla.org/

2009/03/05