UNIVERSIDAD TÉCNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TESIS PREVIO LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TEMA: "IMPLEMENTACION DE UN SISTEMA DE AUTENTICACIÓN PARA CONTROLAR LA SEGURIDAD DE LA RED INALÁMBRICA DE LA BRIGADA DE FUERZAS ESPECIALES No. 9 PATRIA, UBICADA EN EL CANTÓN LATACUNGA "

POSTULANTES:

Cando Salme Mirian del Rosario

Llumitasig Galarza Mónica Elizabeth

DIRECTOR:

Ing. Juan Carlos Rodríguez Trejo

Latacunga, julio 2008

AUTORIA

Los autores certifican que la investigación, redacción y propuesta del presente trabajo son de su exclusiva autoría.

---	---
Cando Salme Mirian	Llumitasig Galarza Mónica
C.I : 050161180-0	C.I.: 050230653-3

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración:

Cumpliendo con lo estipulado en el capítulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que las postulantes, Cando Salme Mirian del Rosario y Llumitasig Galarza Mónica Elizabeth han desarrollado su tesis de grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: "IMPLEMENTACIÓN DE UN SISTEMA DE AUTENTICACIÓN PARA CONTROLAR LA SEGURIDAD DE LA RED INALÁMBRICA DE LA BRIGADA DE FUERZAS ESPECIALES No. 9 PATRIA, UBICADA EN LA CIUDAD DE LATACUNGA ", cumpliendo de esta manera los objetivos respectivos.

En virtud de lo antes expuesto considero que la presente tesis se encuentra habilitada para que las postulantes se presenten al acto de la defensa respectiva.

Latacunga, 07 de julio del 2008.

Ing. Juan Carlos Rodríguez

Director de Tesis.

AGRADECIMIENTO

A Dios por su infinita bondad recibida cada instante de mi vida.

A mi familia por su permanente, comprensión apoyo y cariño.

A la universidad Técnica de Cotopaxi y su Cuerpo Docente por haber formado profesionales con amplios conocimientos técnicos y humanistas para el servicio de la sociedad.

A la Brigada de Fuerzas especiales No. 9 PATRIA por brindar las facilidades necesarias para la elaboración del presente trabajo.

La gratitud más sentida al Ing. Juan Carlos Rodríguez Director de Tesis por su entrega y gran profesionalismo desplegado al compartir sus conocimientos durante el desarrollo de la tesis.

A todas las personas que de una u otra manera hicieron posible este sueño.

Mil Gracias.

DEDICATORIA

A nuestros padres por su ejemplo maravilloso al inculcar en sus hijos el amor, el respeto, la honestidad, el trabajo y cuantos otros valores que engrandecen al ser humano. Para ellos y por ellos nuestro esfuerzo y dedicación.

A nuestros esposos Rogelio y Jorge por el constante apoyo brindado durante la carrera y por animarnos siempre a alcanzar este gran proyecto de nuestra vida.

A nuestros hijos que con sus sonrisas inocentes nos supieron brindar cariño y comprensión durante el tiempo de estudios y el desarrollo de la presente tesis.

Mil Gracias.

ÍNDICE GENERAL

RESUMEN

El servicio de red inalámbrica que no cuenta con un mecanismo de seguridad robusto para la conexión, puede traer consigo muchos problemas como el robo de información y ataques cibernéticos.

Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado. Es por ello, que en esta tesis se aborda uno de los servicios de la seguridad como es la autenticación que asegura que los usuarios que acceden a la red están autorizados siendo de esta manera un importante mecanismo para asegurar las redes inalámbricas.

La seguridad en la transmisión de la información se obtendrá a través del protocolo seguro https, que se basa en el hecho de poder encriptar los mensajes que se envían por la red entre un servidor y un cliente y que solo ellos puedan descifrar los contenidos a partir de una clave común conocida solo por los dos.

En esta tesis se manejará el análisis e implementación de un sistema de seguridad utilizando la autenticación y autorización a través de un protocolo seguro con el cual se realiza una verificación de la información personal del equipo conectado, para saber si tiene la acreditación necesaria y así brindarle el acceso a la red o denegárselo en caso de no tenerlo.

Toda esta gestión ofrece el sistema webRADIUS, garantizando un entorno de red inalámbrico con un alto nivel de seguridad para la Brigada de Fuerzas Especial No. 9 “PATRIA”.

ABSTRACT

The wireless connection that does not have a strong security system may bring many problems such as the theft of information and cyber attacks.

The security in the WLAN is based specially in the protection of the communication between the access point and the wireless clients. It controls the login to this net and protects the administration system of non-authorized access. This is the reason why in the project we cover the security service related with the authentication which verifies that all users that access to the net are authorized so this constitutes an important mechanism device to secure wireless LAN's .

The security in the transmission of the information will be verified by the secure protocol https which is based in the fact of encrypting the messages that are sent via net between a server and a client and in the fact that only the users can decode the contents though a common code known by them.

In this thesis will manage the analysis and implementation of a security system using the authentication a authorization through a secure protocol by means of which a verification of the personal information will be done in the connected equipment to know if the user has the needed accreditation and so let him access to the net or denied it.

The system webRADIUS offers all this capacity guaranteeing a wireless net environment with a high level of security for the Brigada de Fuerzas Especiales No. 9 "PATRIA".

INTRODUCCIÓN

Las tecnologías inalámbricas (Wireless, en inglés) han contribuido en gran manera a otro fenómeno que es la movilidad. Esta ha cambiado en los últimos años, sin que muchos lo perciban, la estructura y la topología de las redes empresariales.

Los dispositivos de almacenamiento de información que antes eran fijos y estaban protegidos por las defensas perimetrales, ahora son móviles y "pasean" por todo el planeta. Computadoras portátiles, PDAs (Ayudante personal digital) y teléfonos celulares portan, muchas veces, archivos con información confidencial de las organizaciones.

La navegación por Internet a través de los dispositivos inalámbricos, hace que el intercambio de información por este medio, incluyendo datos de alto valor, sea una práctica común para los usuarios de las redes inalámbricas, por lo que actualmente se ha puesto un especial énfasis a la seguridad en tales medios de comunicación.

Para tratar de atenuar este defecto, se deben poner en práctica servicios que garanticen la seguridad computacional, tales servicios son la confidencialidad, la integridad, la disponibilidad y la autenticación.

Un sistema posee la propiedad de *confidencialidad* si los recursos manipulados por éste no son puestos al descubierto por usuarios, entidades o procesos no autorizados. Un sistema posee la propiedad de *integridad* si los recursos manipulados por éste no son alterados o destruidos por usuarios, entidades o procesos no autorizados. Un sistema posee la propiedad de *disponibilidad* si los recursos brindan servicio en el momento en que así lo deseen los usuarios, entidades o procesos autorizados. La *autenticación* es el proceso de verificar y asegurar la identidad de las partes involucradas en una transacción. Si este servicio no se llevara a cabo cabe la posibilidad de que una entidad desconocida

asuma una identidad falsa, comprometiendo de esta manera la privacidad y la integridad de la información.

La seguridad en redes inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

Cada vez es más común encontrarnos lugares con servicio de red inalámbrico como es el caso de restaurantes, cafés, hoteles, hospitales, escuelas, e inclusive en nuestra propia casa. En estos lugares se puede acceder al Internet por medio de dispositivos portátiles como Laptops y PDAs de una forma rápida y cómoda sin necesidad de que el usuario se preocupe más que por la duración de la batería o por buscar un enchufe.

Desgraciadamente éstas no son las únicas preocupaciones que se deben tomar en cuenta como administrador de la red. La seguridad es un factor importante que debe estar presente en toda red inalámbrica sobretodo en los lugares que pueden parecer más seguros y confiables, lugares que deben tener un sistema de seguridad robusto para proteger sus recursos más preciados.

La Brigada de Fuerzas Especiales No. 9 “PATRIA” dispone de una red inalámbrica, y es un requerimiento urgente y de mucho interés por parte del Administrador de la Red el implementar la seguridad en la red inalámbrica, para evitar ataques y accesos no permitidos a la red.

Por ser un tema de actualidad y por el requerimiento de la Brigada de Fuerzas Especiales No.9 ”PATRIA” se seleccionó el tema: Implementación de un Sistema de Autentificación para controlar la seguridad de la red inalámbrica de la Brigada de Fuerzas Especiales No. 9 “PATRIA” ubicada en el cantón Latacunga.

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

El servicio de red inalámbrico en la Brigada de Fuerzas Especiales No. 9 "PATRIA" no contaba con un mecanismo de seguridad robusto para la conexión inalámbrica, lo cual ocasionaba que individuos mal intencionados accedan fácilmente a la red para robar información privada o realizar ataques cibernéticos.

La red inalámbrica de la Brigada de Fuerzas Especiales No. 9 "PATRIA" se encuentra habilitada todo el tiempo, lo que ocasionaba que en horas no laborables se conecten y utilicen el servicio de Internet inalámbrico sin ningún control.

Al no contar con un sistema de autenticación era imposible controlar que equipos accedían a la red, este problema ocasionaba que se propaguen con más frecuencia los virus informáticos tanto en las estaciones de trabajo como en los servidores.

Otro de los problemas que se solucionó, fue que el ancho de banda no se sature por el incremento del tráfico en la red.

El objetivo General de esta tesis fue implementar un sistema de autenticación para controlar la seguridad de la red inalámbrica de la Brigada de Fuerzas Especiales No.9 "PATRIA". con la implementación de un sistema de autenticación vía web basado en un protocolo seguro, con el cual se realice una verificación de la información personal del equipo conectado, para saber si tiene la acreditación necesaria y así brindarle el acceso a la red o denegárselo en caso de no tenerlo.

Para el desarrollo de esta tesis y con la ayuda de las técnicas de investigación como las entrevistas y encuestas realizadas a los administradores de la red y a los

usuarios, nos permitió recopilar la información necesaria a fin de determinar los problemas de seguridad y los requerimientos que tenía la red inalámbrica de la Brigada de Fuerzas Especiales No.9 “PATRIA”.

El Internet constituyó para el desarrollo de nuestra tesis una herramienta muy importante, así como también la extensa bibliografía existente en libros y revistas, lo que nos permitió realizar un estudio de los mecanismos de autenticación, autorización, protocolos de seguridad, software y aplicativos de código abierto disponibles en el mercado; se obtuvo la asesoría técnica de profesionales en el área de Redes y Telecomunicaciones para ofrecer a la Brigada de Fuerzas Especiales No. 9 “PATRIA” una solución efectiva y de calidad a su problemática.

Esta investigación constituyó un aporte muy importante para los usuarios y administradores de la red inalámbrica de la Brigada de Fuerzas Especiales No.9 “PATRIA”, ya que con la implementación del sistema de autenticación vía web, se logró restringir el acceso a computadoras que no están autorizadas a operar en el entorno específico, compartir los recursos de la red con total seguridad, protegiendo la información confidencial.

Dentro de este marco el desarrollo de esta tesis nos permitió aplicar y fortalecer nuestros conocimientos adquiridos durante la investigación, con el fin de cumplir el requisito previo a la obtención del título de Ingeniero en Informática y Sistemas Computacionales.

El resto de este documento de tesis está organizado como sigue: en el Capítulo I se describen los conceptos relacionados con un sistema de seguridad para redes inalámbricas, como son: estándares y tecnologías inalámbricas, seguridad inalámbrica, autenticación, protocolos, servidores de autenticación de última generación, dispositivos de red inalámbrica, etc.; necesarios para establecer las bases de este trabajo. En el Capítulo II se presenta un análisis e interpretación de los resultados de las encuestas y entrevistas realizadas a los administradores de la red de la Brigada de Fuerzas Especiales No. 9 “PATRIA”. El Capítulo III, incluye

la implementación del sistema de autenticación vía web basado en un protocolo seguro. Finalmente se dan las conclusiones y recomendaciones obtenidas en este trabajo.

CAPITULO I

AUTENTICACIÓN Y SEGURIDAD EN REDES INALÁMBRICAS

1.1 ESTÁNDARES Y TECNOLOGÍAS DE RED INALÁMBRICA.

Los estándares son un conjunto de especificaciones tecnológicas establecidas por un organismo controlador que en este caso es el Instituto de Ingenieros en Electrónica y en Electricidad, conocida por sus siglas en inglés como IEEE, para que los productores y desarrolladores de tecnología tengan una normativa que les permita lograr que los dispositivos puedan operar entre sí.

Ante la existencia de dispositivos WLAN (Red local inalámbrica) de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades.

1.1.1 Especificación 802.11[1]

"Los estándares de red inalámbrica principiaron con el estándar 802.11, desarrollado en 1997, por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Estos estándares permiten transmisiones de datos de hasta 2 Mbps, transferencias que han sido mejoradas con el paso del tiempo.

[1] Mecanismos de Seguridad [online.Consultado 21-06-2007. Disponible en http://www.redestelecom.com/Actualidad/Análisis/Comunicaciones/Internet/20061110024/2]

Las extensiones a estas reglas se reconocen con la adición de una letra al estándar original, incluyendo 802.11a y 802.11b. La siguiente tabla contiene las variantes relacionadas al estándar 802.11".

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5 GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4 GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4 GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5 GHz para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras –Seguras – Temporales), y AES (Estándar de Encriptación Avanzado).
802.11m	Mantenimiento redes wireless.

Tabla 1-1 Tipos de Estándares

1.1.2 Diseño y componentes del estándar 802.11

Las redes 802.11 están formadas de cuatro componentes físicos principalmente, estos están resumidos en la figura 1-1

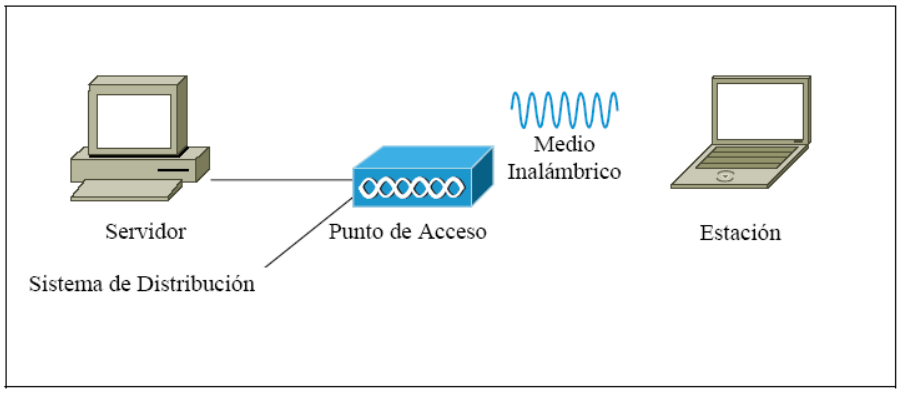


Figura 1-1 Componentes de una red WLAN 802.11

Los componentes son:

Estaciones.

Las redes están construidas para transferir datos entre estaciones. Las estaciones son componentes computacionales con interfaces de red inalámbrica. Típicamente las estaciones son computadoras portátiles o computadoras de bolsillo. Aunque también pueden ser computadoras normales las que se conectan de forma inalámbrica para evitar tener que poner cableado.

Access Point AP (Puntos de Acceso)

Es un dispositivo inalámbrico central de una red inalámbrica WIFI (wireless) que por medio de ondas de radio frecuencia (RF) recibe información de diferentes dispositivos móviles y la transmite a través de cable al servidor de la red cableada. Su principal función es de hacer de puente entre la conexión por cable y la conexión inalámbrica.

Medio inalámbrico

Para mover datos de estación a estación, el estándar utiliza un medio inalámbrico, en un principio eran numerosas las opciones que podían ser usadas para transmitir

información pero las que se utilizaron en primero fue la señal de infrarrojo y el uso de radio frecuencias que con el tiempo se volvieron las más populares.

Sistema de distribución

Cuando muchos puntos de acceso esta conectados para formar una gran área de cobertura, deben comunicarse entre ellos para llevar un seguimiento de todos los movimientos de las estaciones de trabajo.

Servidor

Un servidor es una computadora que realiza algunas tareas en beneficio de otras aplicaciones que se pueden efectuar en dispositivos llamados clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de un ordenador y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final.

1.1.3 Tipos de Redes Inalámbricas

Las redes inalámbricas WI-FI se pueden conectar, básicamente, de 2 maneras muy diferentes.

Redes Inalámbricas Ad Hoc

En esta topología los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

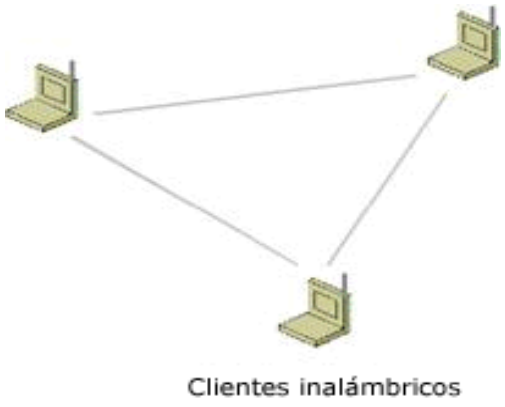


Figura 1-2 Red inalámbrica en modo ad hoc

Red Inalámbrica de Infraestructura

Es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

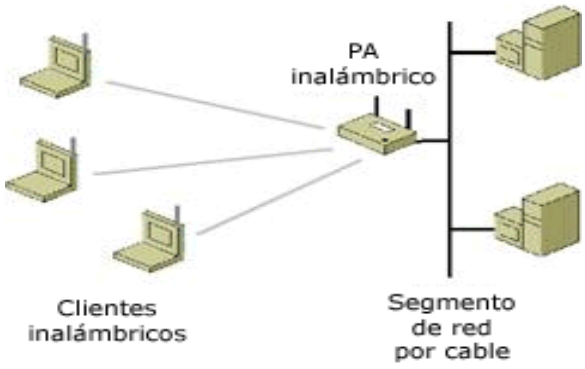


Figura 1-3 Red inalámbrica en modo de infraestructura

1.1.4 Servicios de redes

Un camino para definir la tecnología de red es definiendo el tipo de servicio que ofrece. El estándar 802.11 nos provee de nueve servicios de los cuáles sólo tres son utilizados para mover datos y los restantes seis son utilizados para operaciones de administración de la red. Entre los servicios mas importantes están los siguientes:

a) Distribución

Este servicio es usado por las estaciones móviles cada vez que envían datos. Una vez que un paquete ha sido aceptado por el punto de acceso, éste usa el servicio de distribución para entregarlo a su destino.

b) Integración

Integración es un servicio provisto por el sistema de distribución, el cual permite la conexión del sistema de distribución a una red fuera del estándar IEEE 802.11.

c) Asociación

El envió de las datos a las estaciones móviles es posible gracias a que éstas se registran o se asocian con los puntos de acceso. El sistema de distribución entonces puede usar la información de registro para determinar que punto de acceso utilizar. Cuando se emplea un entorno de red con una seguridad más robusta, la asociación es un precursor de la autenticación, la cuál se explicara más adelante.

d) Reasociación

La reasociación es iniciada por las estaciones móviles cuando por condiciones de fuerza de la señal, dichas estaciones indican que una diferente asociación resultaría más beneficiosa.

e) Disociación

Para terminar con una asociación existente, las estaciones pueden usar el servicio de disociación. Cuando este servicio es usado, cualquier información guardada en el sistema de distribución es removida.

f) Autenticación

La parte física es un componente muy importante en la solución de la seguridad, los puntos de conexión de una red tradicional son limitados, usualmente están en las áreas de oficina cerca del perímetro de los dispositivos de control de acceso. Los equipos de red pueden ser asegurados en clóset especiales, y las conexiones de red de las oficinas y de los cubículos pueden desconectarse cuando no se utilicen, Las redes inalámbricas no pueden ofrecer ese nivel de seguridad física, no obstante se puede depender de rutinas adicionales de autenticación para asegurar que los usuarios que acceden a la red están autorizados.

La autenticación puede ocurrir varias veces durante la conexión de un cliente en la red inalámbrica. Antes de la asociación una estación va a efectuar un intercambio básico de identidad con el punto de acceso que consiste en su dirección MAC (Dirección física de un dispositivo). Este intercambio es el que se conoce con autenticación del estándar 802.11, el cual es muy diferente de la robusta autenticación criptográfica que después le sigue.

g) Des-autenticación

La des-autenticación termina una relación de autenticación. Debido a que la autenticación es necesaria antes de que un usuario de la red sea autorizado, un efecto secundario de la des-autenticación es la terminación de cualquier asociación que se este llevando acabo, en una red con seguridad mas robusta la des-autenticación también borra la información de las llaves.

h) Confidencialidad

En la revisión inicial de 802.11, el servicio de confidencialidad fue llamado privacidad, y fue proveído por el ahora desacreditado protocolo WEP (wireless encryption protocol). Además de nuevos esquemas de encriptación, 802.11i aumenta el servicio de confidencialidad por proveer autenticación basada en usuario y servicios de administración de llaves, dos puntos críticos que WEP no pudo tratar.

1.2 SEGURIDAD EN REDES INALÁMBRICAS

La falta de seguridad en las redes inalámbricas es un problema que, a pesar de su gravedad, no ha recibido la debida atención por parte de los administradores de redes y los responsables de la información.

La seguridad es un requisito esencial para la aceptación de las redes de datos inalámbricas por los usuarios empresariales e instituciones públicas.

La posible carencia de medidas de seguridad adecuadas pueden ocasionar que cualquier persona con una computadora portátil puede encontrar fácilmente el punto de acceso inalámbrico de nuestra red inalámbrica, se introduzca en la red, acceda a la información, utilice nuestra conexión a Internet y obtenga datos importantes que se transfieran en la red inalámbrica, etc. No obstante existen herramientas, funciones y protocolos de seguridad que ofrecen protección adecuada para redes de datos inalámbricas.

Debemos considerar que las redes de datos inalámbricas, no deben ser más vulnerables que las redes de datos cableadas, el nivel de seguridad será dependiente del tipo y funcionalidad de la red; a mayor nivel de seguridad, exige más coste y más capacidad de proceso.

1.2.1 Mecanismos de Seguridad[2]

"En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle.

Como ocurre en otras redes cableadas, la seguridad para redes inalámbricas se centra en la privacidad de los datos y el control de acceso.

La privacidad de la WLAN se consigue mediante el cifrado de los datos con una clave que sólo puede utilizar el destinatario deseado.

Un control de acceso robusto, también denominado autenticación, impide que los usuarios no autorizados se comuniquen a través de los puntos de acceso y garantiza que los clientes se registren únicamente con aquellos puntos de acceso a los que pueden asociarse según la política corporativa. Cuanto más sólida sea la política de control de acceso, más difícil le resultará al intruso acceder a los recursos de la red inalámbrica.

Estos "hoyos" en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red inalámbrica a la cual se conecta.

A continuación detallamos los mecanismos de seguridad usados en redes WLAN, así como las ventajas y desventajas de cada uno de ellos.

1.2.2 Especificación original 802.11

Utiliza tres mecanismos para proteger las redes WLAN:

a) **SSID** (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para

[2] Mecanismos de Seguridad [online.Consultado 21-06-2007. Disponible en http://www.redestelecom.com/Actualidad/Análisis/Comunicaciones/Internet/20061110024/2]

acceder a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal.

b) **Filtrado con dirección MAC** (Control de Acceso al Medio): restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico.

c) **WEP** (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones."

1.2.3 Estándar IEEE 802.1x[3]

"Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores. Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autenticación WEP, y utiliza EAP (Protocolo de Autenticación Extensible) para autenticar y autorizar. Es necesario un servidor que proporcione servicios de

[3] Estándares [online.Consultado 04-07-2007. Disponible en http://www.ciat.cgiar.org/agroempresas/comercio_justo/glosario.htm]

autenticación remota de usuarios entrantes (RADIUS, Servicio Remoto de Autenticación de Usuarios Entrantes).

a) WPA (Wi-Fi Protected Access)

Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de Llaves Integras Seguras Temporales). TKIP fue construido tomando como base el estándar WEP, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. También emplea 802.1X como método de autenticación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autenticación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autenticación.

Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi.

Esta especificación proporciona una mayor encriptación de datos para corregir las vulnerabilidades de seguridad WEP, además de añadir autenticación de usuarios que no se habían contemplado.

b) WPA2 (IEEE 802.11i)

802.11i es el nuevo estándar del IEEE para proporcionar seguridad en redes WLAN. Wi-Fi está haciendo una implementación completa del estándar en la especificación WPA2. Sus especificaciones no son públicas por lo que la cantidad de información disponible en estos momentos es realmente escasa.

WPA2 incluye el nuevo algoritmo de cifrado AES (Estándar de Encriptación Avanzada). Se trata de un algoritmo de cifrado de bloque (RC4 es de flujo) con claves de 128 bits. Requerirá un hardware potente para realizar sus

algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

Para el aseguramiento de la integridad y autenticidad de los mensajes, WPA2 utiliza CCMP (Message Authentication Code Protocol) en lugar de los códigos MIC. Otra mejora respecto a WPA es que WPA2 incluirá soporte no sólo para el modo BSS sino también para el modo IBSS (redes ad-hoc).

c) VPNs e IPSEC

Una VPN es una Red Privada Virtual. Normalmente las VPNs se utilizan para interconectar diferentes sedes geográficamente dispersas de una misma organización o empresa, creando una red privada dentro de una red pública como pueda ser Internet.

Es privada porque se protege mediante cifrado de los datos y autenticación de los usuarios que pretenden entrar en la red. Es virtual porque realmente la red no está interconectada directamente, sino que se utilizan túneles cifrados a través de Internet para conseguir que haya conectividad entre las diferentes sedes.

Además de la topología distribuida en diferentes sedes, las VPN´s se utilizan para que un cliente móvil sea capaz de utilizar la red de su empresa desde cualquier punto. Este escenario se asemeja bastante a lo que ocurre cuando queremos dejar utilizar los recursos de nuestra red a clientes que se conectan a través de un AP. Por esta razón, las VPN´s tienen total vigencia dentro del mundo inalámbrico y hoy por hoy son una solución de seguridad probada y con bastantes garantías.

Existen multitud de tecnologías para crear VPN´s, y diversos protocolos como PPTP (“Point-to-Point Tunneling Protocol”), L2TP (“Layer-2 Tunneling Protocol”) o IPSec “Internet Protocol Security”. Hoy en día la solución más robusta en cuanto a tecnologías VPN es L2TP/IPSec, que proporciona autenticación de usuarios y equipos, una Infraestructura de Clave Pública (“PKI: Public Key Infrastructure”) y asegura la integridad y cifrado en los datos.

d) Firewall

Sistema de defensa basado en la instalación de una "barrera" entre una computadora, un AP o un router y la Red por la que circulan todos los datos.

e) Portales Cautivos

Un portal cautivo (o captivo) es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. A veces esto se hace para pedir una autentificación válida, o para informar de las condiciones de uso de un servicio wireless (que es donde más se encuentran). La arquitectura del sistema de Portal Cautivo es la siguiente: un "gateway" o pasarela encamina las conexiones, mientras que un Servidor de Autenticación define a qué perfil pertenece cada conexión y qué partes de la red podrá visitar en consecuencia."

1.3 AUTENTICACIÓN EN LA SEGURIDAD INALÁMBRICA[4]

"Antes de permitir a las entidades a acceder a la red y a sus recursos asociados, el procedimiento general es autenticar la entidad (un dispositivo o un usuario) y después permitir la autorización basándose en la entidad.

1.3.1 Conceptos Básicos del marco de trabajo AAA

La autentificación, autorización y administración de uso (AAA) puede interpretarse como una estructura para el control de acceso a recursos informáticos, la imposición de políticas, el análisis de uso de recursos y la obtención de la información necesaria para cobrar por este servicio. Estos procesos se consideran vitales para la administración eficaz de redes y la imposición de medidas de seguridad. El modelo AAA resalta los tres aspectos básicos del

[4] Autenticación en redes inalámbricas [online.Consultado 26-06-2007. Disponible en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/908d13e8-c4aa-4d62-8401-86d7da0eab48.mspx?mfr=true

control de acceso de usuarios: la autentificación, la autorización y la administración de uso. Estas especificaciones se describen a continuación:

a) Autenticación

La autentificación es el proceso que proporciona un método para identificar a los usuarios mediante la petición y comparación de un conjunto válido de credenciales. La autentificación se basa en los criterios únicos que posee cada usuario para conseguir el acceso. El servidor conforme con AAA compara las referencias de autentificación del usuario con información almacenada en una base de datos. Si las credenciales se corresponden, se le permite el acceso a los recursos de red solicitados; de no ser así, el proceso de autentificación falla y se niega el acceso a la red

b) Autorización

La autorización va después de la autentificación y es el proceso por el cual se determina si el usuario puede solicitar o utilizar ciertas tareas, recursos de red u operaciones. Normalmente la autorización se produce en el contexto de la autentificación y, una vez que se aprueba al usuario, este puede pasar a utilizar los recursos solicitados. Por ello, la autorización es un aspecto vital para la sana administración de una política de acceso.

c) Administración de uso

El aspecto final de la estructura AAA es la "contabilidad", que se describe mejor como el proceso de medida y grabación del consumo de los recursos de red. Esto permite la monitorización y la generación de informes sobre eventos y su uso para distintos propósitos, incluidos la presentación de facturas, el análisis de tendencias, el uso de recursos, la planificación de capacidad y el mantenimiento activo de la política.

1.3.2 Estándar IEEE 802.1x

Con la proliferación del uso de portátiles y PDAs con capacidades inalámbricas wifi, cada vez es mayor la demanda de conexiones a wireles access point. Las redes inalámbricas se difunden con rapidez, a medida que el IEEE va aprobando nuevos estándares wifi.

La gran comodidad y ventajas que suponen estas nuevas opciones de conexión inalámbricas han hecho que muchísimos usuarios no se hayan percatado de los peligros a que están expuestas las redes inalámbricas (al no haber ya una conexión física) si no adoptan las medidas de seguridad.

En las redes inalámbricas existen dos tramos por los que viajan los paquetes que llevan la información:

1) Un tramo es inalámbrico (aéreo): es el que va desde cada cliente inalámbrico hasta el access point.
2) Otro tramo es cableado: es el que va desde el access point hasta el servidor de la organización.

Al no poder impedir de ninguna manera que la información que está en el aire sea vista por cualquiera, esta debe ser protegida por medio de protocolos de encriptación como WEP, WPA y WPA2.

Pero la encriptación es una protección necesaria, muy necesaria, pero no suficiente pues no sirve para impedir accesos no deseados a nuestra red corporativa.

En los primeros años de este siglo, cuando sólo existía la encriptación WEP y antes que fuera desarrollado el estándar de seguridad 802.11i con la encriptación WPA y WPA2, el IEEE comenzó a buscar soluciones que fueran capaces de mejorar la Seguridad Wifi. El resultado buscado se consiguió adaptando el estándar 802.1x que se había aprobado en 2001 para redes cableadas. En 2004 se finalizó la adaptación para redes inalámbricas WIFI.

Este estándar de seguridad en redes se basa en el control de acceso a puertos. No se abrirá el puerto ni se permitirá la conexión, hasta que el usuario esté autenticado y autorizado contra una base de datos alojada en el Servidor RADIUS.

El estándar 802.1x constituye la columna vertebral de la Seguridad WiFi y es imprescindible y muy recomendable su utilización en toda red empresarial que pretenda lograr una seguridad robusta. 802.1x introduce importantes cambios en el esquema de seguridad wifi.

- Se necesita autenticar a los usuarios antes de conectarse a una red inalámbrica WIFI
- La autenticación se realiza con un protocolo conocido como EAP - Extensible Authentication Protocol. Existen varias versiones de EAP: LEAP, TLS, TTLS, PEAP, FAST
- La autenticación se realiza mediante un servidor de tipo RADIUS

En el esquema de 802.1x, se autentica al usuario y no al dispositivo, como se hacía, por ejemplo en el filtrado de Direcciones MAC (MAC Address). Esto es muy importante porque impide que se pueda entrar a la red, aún cuando a uno le roben o pierda su laptop o PDA. La otra diferencia importante es que con 802.1x, el Punto de Acceso no puede "autorizar" a nadie el acceso a la red. La función de autorización recae en el servidor RADIUS.

El esquema básico de funcionamiento según se define en el estándar es el siguiente:

1. **Servidor de Autenticación:** Es el que verificará las credenciales de los usuarios. Generalmente es un servidor RADIUS.
2. **Autenticador:** Es el dispositivo que recibe la información del usuario y la traslada al servidor de autenticación (esta función la cumple el Punto de Acceso)
3. **Suplicante:** Es una aplicación "cliente" que suministra la información de las credenciales del usuario al Autenticador. (software cliente)

En la figura 1.3 se ve gráficamente una configuración de red inalámbrica WIFI, según el estándar de Seguridad Wifi IEEE 802.1x.

Figura 1-4 Esquema de Seguridad

1.3.3 Autenticación EAP (Extensible Authentication Protocol)

Como se vio en el capítulo anterior del Estándar 802.1x, creado para robustecer la seguridad wifi, se utiliza el protocolo EAP para autenticar a los usuarios. De este se han desarrollado diferentes versiones: EAP-LEAP, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-FAST. Cada uno tiene sus limitaciones y, cada uno soporta diferentes plataformas. Esto obliga al diseñador de una red inalámbrica wifi, a analizar detenidamente que protocolo EAP se va a utilizar para autenticar con el RADIUS - 802.1x. En general, todos los protocolos EAP, requieren la existencia de un certificado digital en el servidor RADIUS para asegurar que nos estamos conectando a la red nuestra y no, a una ajena.

A continuación describiremos a cada uno de las variantes del protocolo EAP:

- **EAP-LEAP**

  a) Desarrollado por Cisco

b) Soporta:
   - Autenticación mutua fuerte
   - Credenciales de seguridad
   - Claves dinámicas de encriptación
c) Requiere Infraestructura de Cisco
d) Requiere certificado digital en el servidor RADIUS
e) Sólo soporta las bases de datos de Microsoft: Active Directory y NT Domain
f) LEAP es vulnerable a ataques de diccionario

- **EAP-TLS**

g) Desarrollado por Microsoft
h) Soporta:
   - Autenticación mutua fuerte
   - Credenciales de seguridad
   - Claves dinámicas de encriptación
i) Requiere certificados digitales en todos los usuarios así como un servidor RADIUS
j) Requiere certificado digital en el servidor RADIUS
k) Sólo soporta las bases de datos de Microsoft: Active Directory y NT Domain

- **EAP-TTLS**

l) Desarrollado por Funk Software y Certicom
m) Emplea:
   - Autenticación mutua fuerte
   - Credenciales de seguridad
   - Claves dinámicas de encriptación
n) Requiere certificados digitales sólo en el servidor RADIUS
o) Se pueden utilizar certificados digitales en los clientes de manera opcional.

p) Compatible con las bases de datos de seguridad preexistentes incluyendo: Windows Active Directory, Dominios NT, Tokens, SQL, LDAP, etc.

- **EAP-PEAP**

q) Desarrolladores: Microsoft/Cisco/RSA
r) No requiere certificados digitales en los clientes
s) Si requiere certificado digital en el Servidor RADIUS
t) También utiliza TLS para establecer el túnel
u) Se incluye en SP1 de Windows XP
v) Se incluye en Windows 2003 Server
w) Intercambio de claves dinámicas
x) Existe incompatibilidad entre la versión PEAP de Cisco y de Microsoft.

A pesar de que ha sido desarrollado conjuntamente por Cisco y Microsoft, en la práctica las versiones comerciales de ambos fabricantes no son totalmente compatibles entre sí y presentan ciertas diferencias.

Ambos TTLS y PEAP trabajan en una forma similar. En el primer paso del protocolo, se debe establecer un túnel TLS usando rutinas similares a EAP-TLS. Los certificados digitales en el servidor de autenticación son usados para validar que la red es confiable antes de proseguir. En el segundo paso, el túnel TLS es usado para encriptar un protocolo de autenticación ampliamente usado como CHAP, que autentifica el usuario en la red. El primer paso comúnmente se refiere como autenticación “externa”, puesto que es un túnel el que protege la segunda autenticación o “interna”. En la figura 1-4 se puede observar la ideología implementada en TTLS y PEAP.

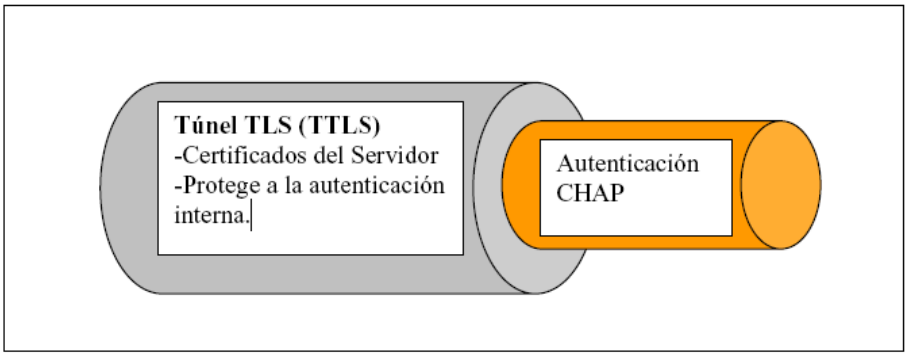


Figura 1-5 Representación del túnel TLS.

- **EAP-FAST**

  y) Desarrollado por Cisco
  z) No requiere certificados digitales en los clientes
  aa) Si requiere certificado digital en el Servidor RADIUS (opcional)
  bb) Soporta Active Directory y LDAP
  cc) Compatible con LEAP y parece fácil de migrar
  dd) Se puede configurar en modo "light" y menos seguro
  ee) Intercambio de claves dinámicas”

COMPARATIVA DE MÉTODOS DE AUTENTICACIÓN EAP: LEAP, TLS, TTLS, PEAP, FAST

	LEAP (Cisco)	EAP-TLS (Microsoft)	EAP-TTLS (Funk Software)	EAP-PEAP	EAP-FAST
Certificado-Cliente	N/A	SI	NO	NO	NO
Certificado-Servidor	N/A	SI	SI	SI	NO/SI
Seguridad Credenciales	Débil	Fuerte	Fuerte	Fuerte	Depende
Bases de datos soportadas	Active Directory Dominios NT	Active Directory	Active Directory Dominios NT Tokens SQL LDAP	Active Directory Dominios NT Novell NDS Tokens LDAP	Active Directory Dominios NT LDAP
Intercambio de claves dinámicas	SI	SI	SI	SI	NO
Autenticación mutua	SI	SI	SI	SI	SI

Cuadro 1-1 Métodos de Autenticación

1.3.4 Protocolo Radius[5]

"El protocolo RADIUS fue desarrollado originalmente por Livingston Enterprises, como un protocolo de control de acceso que verifica y autentifica a usuarios basados en el método comúnmente usado de desafío/respuesta (CHAP). Mientras que el protocolo RADIUS tiene un lugar prominente entre los servicios de proveedores de Internet, también pertenece a cualquier ambiente en donde sea necesaria o deseada la autenticación central, la autorización regulada, y el manejo de cuentas de usuario.

[5] Radius [[online.Consultado 04-07-2007. Disponible en http://www.casadomo.com/proyectoradius.aspx]

RADIUS es el acrónimo de Remote Authentication Dial In User Service. Originalmente estaba pensado para accesos por líneas cableadas, pero cuando se modificó el estándar 802.1x para seguridad WIFI, se adaptó también como herramienta de autenticación para las redes inalámbricas wifi.

1.3.4.1 Funciones de RADIUS en Redes Inalámbricas WIFI

RADIUS cumple varias funciones en la arquitectura de seguridad de una red inalámbrica WIFI, las cuales se detallan a continuación:

- Recibir pedido de conexión de los usuarios wifi.
- Autenticar a los clientes wifi y luego Autorizar su acceso a la red.
- Devolver toda la información de configuración necesaria para que el cliente acceda a la red entre ellas la clave.
- Para robustecer la seguridad wifi, el servidor RADIUS puede generar claves "dinámicas", es decir que las puede ir cambiando cada tanto. El administrador puede configurar el intervalo.

1.3.4.2 Características del protocolo RADIUS

La RFC 2138 identifica las siguientes características clave del protocolo RADIUS:

- Usa algoritmos de encriptación MD5 para las contraseñas
- Soporta alrededor de 50 atributos para la configuración de los equipos de distintas plataformas
- Soporta el modelo AAA (authentication – authorization - accounting)
- Modelo cliente/servidor: Un NAS funciona como un cliente de RADIUS. El cliente es el responsable de transferir la información de usuario a los servidores RADIUS designados y de actuar consecuentemente con la respuesta recibida. Los servidores RADIUS son los responsables de recibir las peticiones de conexión de los usuarios, de llevar a cabo la autentificación y de devolver a continuación todos los detalles de configuración necesarios para que el cliente proporcione los servicios al

usuario. Adicionalmente, el servidor RADIUS puede funcionar como cliente intermediario hacia otros servidores RADIUS o servidores de autentificación similares.

- Seguridad de red: La comunicación entre el cliente y el servidor RADIUS se autentifica mediante el uso de una clave compartida que nunca se envía a través de la red como texto plano. Además, las contraseñas de usuario se envían cifradas entre el cliente y el servidor RADIUS para eliminar la posibilidad de un ataque de escucha.
- Mecanismos de autentificación flexibles: El servidor RADIUS permite usar una amplia variedad de métodos para autentificar a un usuario. Cuando se le proporciona el nombre de usuario y la contraseña original utilizada por el usuario, puede soportar PAP o CHAP, el sistema de acceso de UNIX y otros métodos de autentificación como PAM, LDAP, SQL y demás.

Otros métodos de autentificación soportados por RADIUS, contempla los métodos EAP: EAP-MD5, EAP-TLS, EAP-PEAP (MSCHAPV2, TLS, GTC), EAP-TTLS (PAP, CHAP, MSCHAP, MSCHAPV2, MD5), EAP-GTC, EAP-SIM, EAP-AKA, EAP-MSCHAPVE, LEAP

- Protocolo extensible: Todas las transacciones constan de tuplas Atributo-Longitud- Valor (ALV) de longitud variable. Se pueden añadir atributos nuevos sin perturbar las implementaciones ya existentes del protocolo, con lo que el protocolo resulta más flexible y dinámico para soportar implementaciones nuevas.

1.3.4.3 Funcionamiento de RADIUS

Cuando un usuario intenta registrarse y autenticar en un servidor de acceso usando RADIUS se realiza los siguientes pasos:

1. Cuando el usuario está listo digita un nombre de usuario y contraseña
2. Se envía el nombre de usuario y contraseña encriptada sobre la red al servidor RADIUS.

3. El usuario recibe una de las contestaciones siguientes del servidor RADIUS

   ACCEPT: El usuario es autenticado

   REJET: El usuario no se autentica y es incitado para volver a digitar el nombre de usuario y contraseña, o el acceso se niega

   CHALLENGE: El desafío es emitido por el servidor RADIUS. El desafío colecciona datos adicionales del usuario.

   CHANGE PASSWORD: Es una demanda emitida por el servidor RADIUS y le pide al usuario que seleccione una nueva contraseña

   ACCEPT O REJECT: La respuesta se junta con datos adicionales que se usan para EXEC o autorización de red. Se debe completar primero la autenticación RADIUS antes de usar autorización RADIUS.

Los datos adicionales que se incluyen en los paquetes ACCEPT o REJECT consiste en lo siguiente:

- Servicios que el usuario puede acceder, incluso TELNET, Rlogin, o conexiones de transporte del área local (LAT), y PPP, Serial Line Internet Protocol (SLIP), o servicios de EXEC.
- Parámetros de conexión, incluso dirección IP del host o cliente, lista de acceso, y timeouts del usuario

1.3.4.4 Formato de paquetes RADIUS

El paquete de RADIUS se encapsula en un flujo de datos UDSP sin estado que se envía a los puertos de destino 1812, 1813 Y 1814, que representan respectivamente el acceso, la contabilidad y la intermediación. Por compatibilidad y mantener los valores históricos, algunos servidores siguen funcionando, erróneamente, sobre los puertos 1645 y 1676. Este comportamiento viene de las primeras etapas del desarrollo de RADIUS y en la actualidad entra en conflicto con el servicio de medición de datos (o “datamétrico ").

La RFC especifica que RADIUS utiliza una estructura de paquete esperada para el proceso de comunicación, que muestra la figura 1-5.

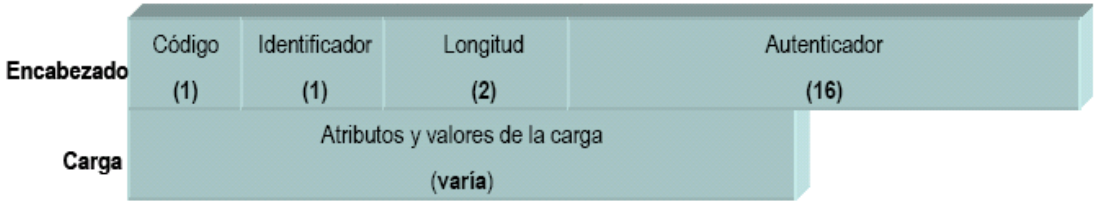


Figura 1-6 Formato del Paquete UDP Radius

A continuación describiremos los elementos del paquete RADIUS

- **Código:** El campo Código tiene una longitud de un octeto e identifica el tipo de paquete RADIUS. Cuando un servidor recibe un paquete con un campo de Código no válido, lo ignora sin ningún tipo de notificación adicional. En la próxima sección analizaremos los tipos de paquete.
- **Identificador:** El identificador es un valor de un octeto que permite al cliente RADIUS comparar una respuesta RADIUS con la petición pendiente correcta.
- **Longitud:** El campo Longitud ocupa dos octetos. Indica la longitud del mensaje RADIUS y representa la correspondiente suma de los campos Código, Identificador, Longitud, Autentificador y Atributo.
- **Autentificador:** Este valor tiene una longitud de 16 octetos y se utiliza para autentificar y verificar la respuesta procedente del servidor RADIUS. También se utiliza como mecanismo de ocultación de contraseñas. Los dos tipos de valor son los autentificadores de Petición y Respuesta. El primer tipo debería ser un valor aleatorio y único usado con los paquetes de Petición de Acceso y Contabilidad. El último tipo se usa en los paquetes de Aceptación de Acceso, Rechazo de Acceso y Desafío de acceso, y contiene un valor hash MD5 unidireccional, calculado a partir de una cadena de valores que consiste en los campos Código, Identificador, Longitud y Autentificador de Petición, y en los atributos de respuesta, seguidos por la clave compartida.

- **Atributos:** La sección de atributos del paquete clasifica diversas características y patrones de comportamiento del servicio, que suele anunciar una característica en particular del tipo de servicio 'Ofrecido o solicitado. La tabla 1-1 muestra los seis tipos de atributo y sus posibles valores."

VALOR DEL ATRIBUTO	LONGITUD EN OCTETOS	TAMANO (EN BITS)	EJEMPLOS
INT (entero)	4	32	256 65536
ENUM (enumerado)	4	32	1 = nombre de usuario 2 = contraseña de usuario 13 = compresión de marco 26 = específico del fabricante
STRING (cadena)	1-253	Variable	"Cualquier cadena" "192.168.111.111" " www.arhont.com "
IPADDR (dirección IP)	4	32	0xFFFFFF 0x00000A
DATE (fecha)	4	32	0xFFFFFF 0x00000A
BINARY (binario)	1	1	0

Tabla 1-2 Tipos de Atributos de RADIUS

1.3.4.5 Tipos de Paquetes

Además de haber visto la estructura de los paquetes RADIUS es importante saber que es lo que hacen los paquetes. Existen cuatro tipos de paquetes que son relevantes para las fases de autenticación y autorización en la transacción AAA.

a) Access-Request (Petición de Acceso)

El paquete de petición de acceso se utiliza para el consumidor deservicios cuando está solicitando un servicio particular de la red. Lo que caracteriza a un paquete de petición es que el valor del campo de código en el encabezado es igual a uno.

La carga útil del paquete de petición de acceso debe incluir el atributo de nombre de usuario para identificar a la persona que quiere obtener acceso al recurso de la red. Es necesario que la carga útil contenga la dirección IP o el nombre canónico del equipo de la red que está solicitando el servicio. Este

también debe contener la contraseña de usuario, la contraseña basada en CHAP, o el identificador de estado, pero no ambos tipos de contraseñas. La contraseña de usuario debe pasarse por una función hash usando MD5. En la siguiente figura 1-6 se puede ver la estructura del paquete Access-Request.

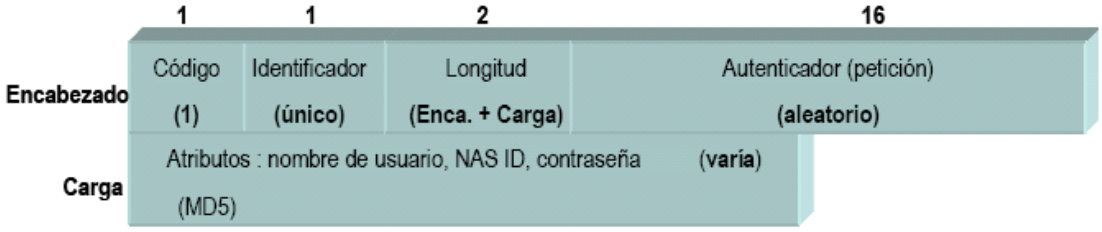


Figura 1-7 Paquete UDP Acces-Request

b) Access-Accept (Acceso aceptado)

Los paquetes de acceso aceptado son enviados por el servidor RADIUS al cliente para reconocer que se conoce la petición del cliente. Si todas las peticiones en la carga útil que forman la petición de acceso son aceptadas, entonces el servidor RADIUS debe fijar el campo de código a dos. El cliente, hasta que recibe el paquete de aceptado, comprueba este con el paquete de respuesta usando el campo de identificación. Los que no sigan este estándar son descartados. En la siguiente figura 1-7 se puede ver la estructura del paquete Access-Accept

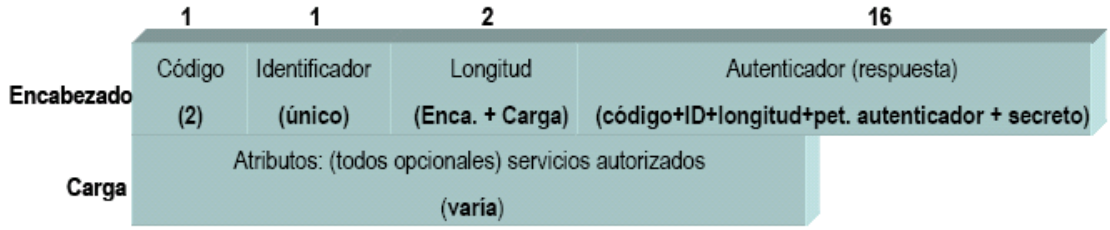


Figura 1-8 Paquete UDP Acces-Accept

c) Access-Reject (Acceso Rechazado)

El servidor RADIUS es requerido para mandar un paquete de acceso denegado de regreso al cliente, si es denegado cualquiera de los servicios pedidos en el paquete de petición de acceso. La negación puede estar basada en políticas de sistemas, privilegios insuficientes, o cualquier otro

criterio (una función para ser implementada individualmente). El acceso denegado puede ser enviado en cualquier momento durante la sección, lo que lo hace ideal para reforzar los tiempos límites de conexión. Sin embargo no todos los equipos soportan recibir el acceso denegado durante la conexión preestablecida. En la siguiente figura 1-8 se puede ver el paquete Acces-Reject.

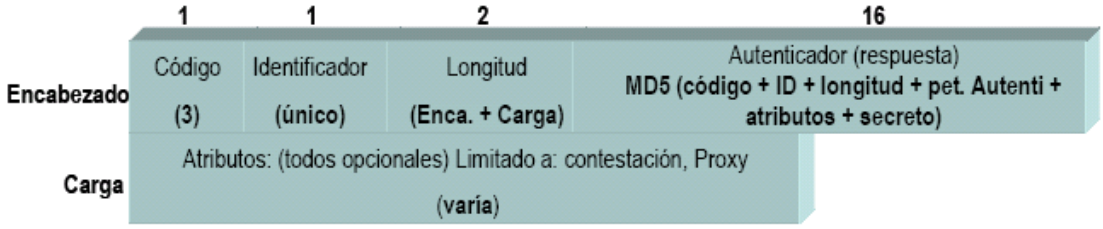


Figura 1-9 Paquete UDP Acces-Reject

d) Acces-Challenge (Desafío de Acceso)

Si el servidor recibe información conflictiva del usuario, requiere más información, o simplemente desea disminuir el riesgo de una autenticación fraudulenta, puede publicar un paquete de desafío de acceso al cliente. El cliente, hasta que recibe el paquete de desafío de acceso, debe entonces publicar una nueva petición de acceso con la información apropiada incluida. En la siguiente figura 1-9 se puede ver la estructura del paquete Acces-Challenge."

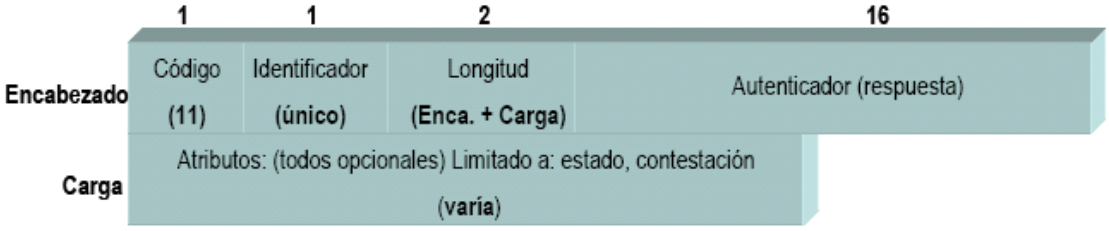


Figura 1-10 Paquete UDP Acces-Challenge

1.4 SERVIDORES Y CLIENTES DEL PROTOCOLO RADIUS[6]

"Existen varios servidores y clientes del protocolo RADIUS que sirven para crear entornos de seguridad para redes inalámbricas. Cada uno de estos clientes y servidores se relacionan porque comparten funciones de autenticación y acceso, aunque no todos utilizan los mismos métodos y protocolos.

También se puede distinguir que algunos se ofrecen en forma comercial, comprando la aplicación o comprando una licencia para poder usar la aplicación, mientras otros incluyen licencia libre y se pueden usar gratuitamente. Otra característica extra que se puede observar es que algunos vienen con la capacidad de ser programados para soportar otros métodos de autenticación y de manejo de cuentas para el acceso.

1.4.1 Servidores RADIUS

Existe un gran número de servidores RADIUS principalmente para entornos UNIX, cada uno de ellos comparte muchas características similares aunque cada servidor busca explotar factores tecnológicos que le den la ventaja sobre los demás. Hay servidores comerciales como también los hay con licencia libre, siendo FreeRADIUS, Cistron y Radiador los servidores más populares. Los servidores que se verán a continuación son: Cistron, ICRadius, XtRADIUS, OpenRADIUS, YARD RADIUS, JRadius, Radiador, AXL RADIUS, Odyssey, Cisco Access Registrar.

[6] VLADIMIROV, Andrew A. ; GAVRILENKO, Konstantin y MIKHAILOVSKY, Andrei A. Hacking Wíreles: seguridad de redes inalámbricas. Madrid: Anaya Multimedia, 2005. 238p.

1.4.1.1 Servidores de licencia libre

a) FreeRADIUS

FreeRADIUS es uno de los servidores RADIUS más modulares y ricos en características disponibles hoy en día, Ha sido escrito por un equipo de desarrolladores que tiene décadas de experiencia recolectada en implementar y desarrollar software RADIUS, en ingeniería de software, y administración de paquetes Unix. El producto es el resultado de la ingeniería entre muchos de los más reconocidos nombres en software libre basado en implementaciones RADIUS, incluyendo una gran cantidad de desarrolladores del sistema operativo Debian GNU/Linux. El servidor FreeRADIUS es distribuido bajo la licencia GNU GPL (versión 2).

El servidor FreeRADIUS está siendo usado al rededor del mundo en instalaciones a gran escala, abarcando múltiples servidores RADIUS como millares de usuarios y millones de sesiones.

FreeRADIUS soporta los siguientes equipos NAS:

- 3Com/USR Hiper Arc Total Control
- 3Com/USR NetServer
- 3Com/USR TotalControl
- Ascend Max 4000 family
- Cisco Access Server family
- Cistron PortSlave
- Computote PowerRack

FreeRADIUS se caracteriza por lo siguiente:

- Ediciones multiplataforma y código fuente
- Soporte para RFC y atributos VS
- Atributos adicionales de configuración del servidor

- Seleccionando una configuración en particular
- Métodos de autorización
- Métodos de autenticación
- Métodos para el manejo de cuentas de usuarios

b) Cistron

Es un servidor de autentificación y manejo de cuentas para servidores de Terminal por medio del protocolo RADIUS, este se ha convertido en uno de los servidores más usados por la comunidad de softwar*e* libre [13]. Fue escrito por Miguel Van Smooreburg. Entre sus características más importantes están:

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

c) ICRadius

ICRadius usa bases de datos de MySQL para guardar toda la información necesaria como archivos de usuarios, archivos de directorios, y también envía información a la base de datos. Esto, en una forma alterna, permite la

manipulación y extracción de datos de una manera rápida y eficiente, con la facilidad y flexibilidad ofrecida por MySql. ICRadius es completamente gratis bajo la licencia GPL. Este sistema usa un formato tabular lo cual facilita el uso de bases de datos.

d) XtRADIUS

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

Este servidor esta basado en el servidor Radius Cistron por lo cual incluye todas sus características, como también otras mejoras.

La comunicación entre el servidor XtRadius y los scripts externos se da usando parámetros de línea de comando o por variables de ambiente.

e) OpenRADIUS

OpenRADIUS es un servidor del RADIUS que funciona en muchos entornos Unix, y tiene varias características interesantes:

- La capacidad de conseguir secretos compartidos, información de autenticación, políticas y perfiles de usuario de cualquier fuente de datos externa disponible.

- Soporte para las bases de datos de contraseña en Unix, incluye NIS/NIS+, archivos de ASCII del estilo Livingston, directorios de LDAP y bases de datos de SQL.
- Esquemas de autentificación y políticas de seguridad completamente modificables, usando un lenguaje de reglas para negocios incorporado. Esto permite que se especifique cómo el servidor toma sus decisiones, basado en cualquier combinación información interna y externa disponible.
- Módulo de interfaz simple, escalable y completamente documentada. Los módulos pueden proveer datos tales como información del usuario, y pueden también almacenar datos tales como registro y uso de cuentas.
- Diccionario extremadamente flexible que puede usarse para apoyar cualquier tipo de atributo no estándar o específico del vendedor, incluye múltiples atributos adentro del mismo VSA, atributos no estándar, IDs o archivos de tamaño, subarchivos, y mucho más.
- Enlaces de tarjetas únicas o múltiples por direcciones IP, y capacidad de escuchar múltiples puertos.
- Libre de usar, modificar, y redistribuir bajo los términos de la licencia pública general GNU.

f) YARD RADIUS

Otro servidor RADIUS para la autorización y manejo de cuentas basado en el RFC RADIUS que fue derivado del servidor original RADIUS 2.1 de la empresas Livingston. Entre las características útiles añadidas al esquema de Livingston están:

- Estado Del Desarrollo: 4 - Beta, 5 – Producción/estable.
- Para administradores de sistema, y la industria de las telecomunicaciones.
- Licencia BSD.
- Múltiples entornos operativos (BSD, Mac, Linux, Unix.).
- Lenguaje de programación C.
- Autenticación de directorios en la red.

- Idioma Inglés.
- Sin interfase.

1) **JRadius**

JRadius es un Cliente y Servidor RADIUS de licencia abierta. Este no es una aplicación independiente sino un módulo que soporta el lenguaje Java para FreeRadius.

JRadius está licenciado bajo la combinación de la librería GNU, y la licencia para público en general GPL, además esta certificado por la iniciativa OSI de software abierto. JRadius esta siendo desarrollado en base a las siguientes metas:

- Utilizar todas las características de los servidores RADIUS existentes.
- Separación y portabilidad de la lógica de los negocios para remarcar en el servidor RADIUS.
- Capitaliza la vasta cantidad de software abierto y otras fuentes existentes de java.
- Despliegue de una nueva lógica sin tener que recomenzar el núcleo de servicios RADIUS.
- Integración con otros sistemas y protocolos de autenticación.

1.4.1.2 Servidores comerciales

a) **Radiator**

Radiador es un altamente configurable y flexible servidor RADIUS el cual soporta autenticación para cerca de 60 diferentes tipos de métodos de autenticación tales como archivos planos , archivos DBM, archivos de contraseña Unix, bases de datos SQL, servidores RADIUS remotos (proxying), programas externos, utilidades de administración de usuarios NT, directorios activos, LDAP, PAM, iPASS, Go Remote, NIS+, Tacas+, Web URL, Vasco Digipass, un amplio

rango de paquetes ISP tales como: Esmerald, Platypus, Rodopi, Hawk-i, la base heredada de datos de usuarios, etc. Entre sus características más importantes tenemos:

- Soporta RadSEC – seguridad confiable del proxying RADIUS.
- Radiator ahora soporta más métodos de autenticación 802.1X que cualquier otro servidor RADIUS dando una amplia gama para escoger clientes de red 802.1X.
- Incluye certificados privados para clientes y servidores para probar la autenticación 802.1X.
- Radiador incluye características que no pueden ser encontradas en ningún otro servidor como prevención de acceso doble, reescritura del nombre de usuario, atributos específicos del vendedor, bloqueo en algún tiempo del día, e interfase grafica de usuario para pruebas.
- Incluye CGI's para configuración, reportes, y utilidades de administración de bases de datos y mucho mas.
- Trabaja con la mayoría de NASs, VDPN, ADSL y puntos de acceso inalámbrico.
- Incluye todo el código fuente.
- Radiador puede ser comprado para ser usado en un solo servidor, o como parte de alguno de los paquetes ofrecidos , para la empresa, para los profesionales , para la casa, etc.
- Trabaja en la mayoría de las plataformas. Unix, Linux, Windows, Mac, VMS.

b) Servidor AXL RADIUS

AXL es un servidor RADIUS complete que puede autenticar, manejar cuentas, y Proxy. La interfase del programa permite al usuario usar métodos de autenticación y de uso de cuentas mediante cualquier método por el que Java puede acceder al mundo, bases de datos, LDAP, archivos planos, URL´s.

AXL no es un servidor que regresa llaves. Este es una interfase de programa al servidor RADIUS. AXL puede realizar todas las funciones de un servidor

RADIUS pero no puede configurarse por si mismo usando archivos o bases de datos, no tiene conocimiento de quien se puede conectar, y no tiene control sobre asuntos de políticas.

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

Se debe proporcionar código para manejar la autenticación, sus políticas, y uso de cuentas. Existen métodos para realizar estos mecanismos: PAP, CHAP, MS-CHAP, LEAP, etc., pero se debe escribir un código para implementar las políticas del método de autenticación a usar y especificar los atributos a regresar.

Algunas características adicionales:

- Incluye integración con el cliente RADIUS
- Se puede empezar secuencias separadas de manejo de cuentas y autenticación.
- Soporte para atributos de Vendedores Específicos.
- Soporte completo para Proxy.
- Proxy dinámico: se puede enlutar cualquier paquete en cualquier parte basándose en una política o en paquetes de atributos del RADIUS.
- Construido con los métodos de autenticación PAP, CHAP, MSCHAP, MSCHAPV2, EAP-MD5, y LEAP.
- Detección rápida de duplicidad de paquetes.
- Soporte para mensajes EAP y mensajes de autenticación.
- E puede establecer el tamaño de los paquetes dinámicamente.
- Tipos de mensajes extendidos.
- No es vulnerable a problemas de seguridad de sobrecarga del búfer (problemas que tienen los escritos en C/C++).
- SNMP es soportado. SNMP V2 puede ser habilitado o deshabilitado.

- Obedece los RFC´s 2865 (Autenticación) y 2866 (Manejo de cuentas) y otros RFC´s relacionados con RADIUS.
- Trabaja con cualquier base de datos que tenga el controlador JDBC.
- El código fuente está muy bien documentado.

c) Servidor Odyssey

El servidor Odyssey es un servidor RADIUS especialmente diseñado para manejar control de acceso y seguridad WLAN. Es una solución de seguridad WLAN completa para pequeñas empresas, y es adicionalmente perfecta para la distribución en sucursales, departamentos autónomos y sitios remotos de grandes organizaciones. En esta última opción el servidor se comunica con la central de copiado de Funk Software´s Steel-Belted RADIUS o con otro servidor compatible RADIUS para WLAN y administración de políticas de acceso 802.1x.

Con Odyseey los administradores de red pueden:

- Establecer políticas de acceso basadas en usuarios, para incrementar la seguridad de control de acceso.
- Acceder a registros de cuentas localmente, o mandarlas a la central del servidor de cuentas, para proveer un registro comprensible de los accesos de red WLAN.
- Explicación exacta para los usuarios de cuentas que se quieren conectar vía EAP-TTLS, aún si ellos quieren tomar ventaja de la habilidad para ocultar su identidad.
- Autenticación de usuarios que se están conectando vía PEAP.

El servidor Odyseey soporta los protocolos de seguridad EAP-TTLS, PEAP, EAP-TLS y LEAP y corre con cualquier punto de acceso inalámbrico compatible con el protocolo 802.1x. Este puede autenticar usuarios a través de las bases de datos de autenticación de WINDOWS, o mandar pedidos de autenticación a Steel Belted Radius u otro servidor RADIUS compatible para autenticación de bases de

datos no-Windows como basadas en LDAP. Este servidor maneja conexiones a cualquier cliente basado en 802.1x incluyendo el Cliente Odyseey.

d) Cisco Access Registrar

Cisco CNS Access Registrar es un servidor RADIUS diseñado para soportar el envió de llamadas, ISDN, y nuevos servicios incluyendo DSL, cable con telco-return, red inalámbrica y voz sobre IP. El servidor fue diseñado de la nada hasta reunir las necesidades de las operaciones de los proveedores de servicio: Cisco CNS Access Registrar provee funcionamiento y escalabilidad de clases-portadoras como también la extensibilidad necesaria para la integración de los sistemas de gerencia de desarrollo de servicios.

Cisco Access Registrar esta construido en una arquitectura multi-secuencias para tomar ventaja de los sistemas de procesadores múltiples y proveer el más alto funcionamiento AAA.

Algunas de sus características más importantes son:

a) **Puntos extendidos:** Los puntos extendidos de Cisco Access Registrar soporta funciones adicionales a la lógica del servidor RADIUS para modificar o realzar funcionalidad extra.
b) **Integración de directorios:** Los directorios sirven como depósito central para la información del usuario, los perfiles del servicio, los perfiles de mando de cuenta, y otra información de servicio. Cisco Access Registrar autentica a usuarios contra un directorio de LDAP y proporciona la flexibilidad de trabajar con una variedad de configuraciones de directorios.
c) **Proxy AAA:** Cisco Access Registrar soporta Proxy RADIUS, envés de autorizar o autenticar en base a un directorio, el servidor electamente usa Proxy para enviar una petición AAA a otro proveedor de servicios, a otro servidor RADIUS o a un servidor RADIUS que

hace de cliente que autentica y autoriza usuarios en base a otros directorios o bases de datos.

d) **Administración de sesión y direcciones:** Cisco Access registrar proporciona administradores de recursos que manejan la locación dinámica de direcciones IP o IPX, y refuerza limite de sesiones de grupo y usuarios alrededor de múltiples servidores de acceso de red."

1.4.2 Clientes RADIUS

Un aspecto que se observa en los clientes basados en la autenticación 802.1z es que son pocas las opciones gratis disponibles, a diferencia de los servidores RADIUS en donde hay muchas opciones gratuitas, existe una tendencia por comercializar las licencias de los clientes, este es el caso de dos de los clientes MDC Aegis y Odysse, clientes que no hace mucho tiempo se ofrecían gratis, ahora se ofrecen de manera comercial por el gran auge que han tenido las redes inalámbricas y por la necesidad creciente de buscar mecanismos para mantenerlas seguras. Los clientes que se verán son: Xsupplicant, Boingo, Aegis, Odyssey, Monarca, AXL.

1.4.2.1 Clientes de licencia libre

a) Xsupplicant

Es una implementación de licencia libre basado en el protocolo IEEE 802.1x. Esta licencia ofrece soporte como autenticador y cliente. Entre sus características encontramos:

- Dirigido a los desarrolladores, usuarios finales y a administradores de sistemas
- Tiene una licencia BSD GNU Licencia publica general (GPL)
- Soporta todos los sistema operativos POSIX (Linux/BSD/sistemas basados en UNX)
- Esta programado en C

b) Boingo

Es un cliente de autenticación basado en 802.1x el cual ha ganado varios reconocimientos. Entre sus características más importantes encontramos las siguientes:

- Es gratis
- Es rápido
- Es fácil de usar.
- Es más seguro que antes
- Es la mejor forma de administrar todas las conexiones de Internet inalámbricas.

1.4.2.2 Clientes Comerciales

a) MDC Aegis

El cliente AEGIS asegura varios dispositivos como computadoras portátiles, computadoras de escritorio, computadoras de bolsillo, por medio de la autenticación basada en 802.1x. MDC Aegis provee soluciones para una amplia gama de sistemas operativos y métodos EAP para la seguridad de las plataformas computacionales en la empresa.

b) Odyseey Client

En palabras de sus creadores; seguridad, fácil de administrar, y compatibilidad son características que ofrece este cliente 802.1x. Si se busca construir un acceso WLAN seguro, o se esta migrando a un acceso 802.1x o ambos, el cliente Odyseey provee seguridad sin igual al precio más bajo en implementación y soporte. Algunas de las características que ofrece este cliente son:

- Cliente 802.1x de triple propósito, permite a los usuarios conectarse a la red inalámbrica de la empresa, a la red ethernet normal, y a la red pública de los aeropuertos, restaurantes, y otros lugares.
- Provee una seguridad robusta sobre los enlaces inalámbricos.

- Establece y refuerza una política uniforme de seguridad en empresas.
- Multiplataforma y multi vendedor
- Fácil de usar y administrar.

c) Cliente Monaca RADIUS

Monaca entrega una suit de estándares fáciles de usar, confiables y de alto desempeño basados en soluciones de seguridad "embedded" que incluye la especificación RADIUS. El cliente RADIUS de Monaca se comunica a través de la red con un servidor RADIUS, que guarda los nombres de usuario, las contraseñas, y autoriza el acceso al usuario, a sistemas o aplicaciones.

Entre sus características tenemos:

- RFC 2865 (RADIUS), RFC 2866 (Uso de cuentas en RADISU), RFC 1994 (CHAP)
- Zero threaring: sólo se activa cuando es llamado, usa muy pocos recursos del sistema.
- Uso completo de código entrante: Una robusta arquitectura evita errores en condiciones demandantes.
- Soporte de métodos de autenticación PAP, CHAP, Autenticación Múltiple de Desafío Respuesta.
- Avanzadas "api´s" muy bien documentadas
- Fácil de instalar y usar.
- Seguridad de alto grado para empresas, sin comprender funcionalidad de los dispositivos.
- Ciclo de desarrollo rápido: Permite desarrollar sistemas para substituirlos por los componentes comerciales usados.

d) Cliente RADIUS AXL

Ampliamente usado para simplificar el acceso al servidor RADIUS en Java o aplicaciones Java. Este incluye un API (Interfase de aplicaciones para programar) que ayuda a construir un cliente RADIUS en cualquier programa Java, desde servelets hasta aplicaciones.

Algunas características:

- Soporta los métodos de autenticación PAP, CHAP, MSCHAP, MSCHAPV2, EAP-MD5, LEAP.
- Extremadamente flexible en la manipulación de atributos.
- Atributos específicos del vendedor soportados.
- Atributos de mensajes de autenticación soportados
- Soporte de diccionario RADIUS
- Interoperabilidad probada.
- Soporta tipos de mensajes extendidos y cualquier tipo de paquetes.

Se han enumerado los diversos clientes y servidores que existen actualmente para poder crear un entorno de seguridad para redes inalámbricas, se puede observar que todos los servidores requieren:

- Instalación de software adicional en los equipos clientes..
- Estas soluciones solo se puede implantar sobre un parque de equipos con determinados sistemas operativos que soporten 802.1X como por ejemplo Windows XP, lo cual es una desventaja para la BFE No 9 PATRIA, ya que muchos de los equipos tienen con sistemas operativos anteriores a Windows XP.
- Se requiere de hardware compatible con el estándar 802.1X, esto indica que la BFE No 9 PATRIA debe adquirir nuevos Access Point que soporten el estándar 802.1X.

Luego de analizar las diferentes alternativas y sus desventajas se ha llegado a la conclusión de que se debe desarrollar una aplicación vía web para eliminar la instalación adicional de software en los equipos clientes, y de que el sistema operativo no sea una limitante para poder realizar una autenticación segura y confiable. Además de poder utilizar el hardware que dispone actualmente la BFE Nº 9 PATRIA.

1.5 SERVIDORES RADIUS DE ÚLTIMA GENERACIÓN.

En los últimos años, Internet dejó de ser un mero divertimento para pasar a ser un medio fundamental de desarrollo de aplicaciones. Hoy en día, podemos hacer mucho más que visitar páginas web y chatear. Se puede realizar muchas tareas vía Internet; una de ellas es la autenticación RADIUS, a través del servidor webRADIUS.

1.5.1 Servidor webRADIUS

Existen muy pocos software que podamos reutilizar para nuestro sistema de autenticación y de esa pequeña porción, gran parte está desactualizada, o no se ajusta a nuestras necesidades.

El proyecto WebRADIUS es un software desarrollado por la necesidad de proporcionar a la BFE No. 9 PATRIA un sistema de autenticación vía web, basado en un protocolo seguro. WebRADIUS combina una metodología de seguridad (protocolos de autenticación y cifrado) que permite una alta efectividad a la hora de autenticar y autorizar un usuario en una red, para que tanto usuarios como administradores encuentren en el sistema una forma fiable de conectarse a la red sin que su privacidad se vea afectada.

WeRADIUS está basado en el esquema de los portales cautivos, en el estándar 802.1x (estándar de autenticación para gestión de redes que permite autenticar al usuario o máquina contra un servicio RADIUS, LDAP o cualquier otro sistema de autenticación e identificación), y cumple con la estructura del modelo AAA (autenticación, autorización, administración de uso).

1.5.1.1 Características del servidor webRADIUS

- Trabaja bajo la plataforma Linux.
- Utiliza el protocolo HTTPS para el envío de paquetes.
- Para la encriptación de la información utiliza el protocolo SSL
- Base de datos MYSQL, para la autenticación se usuarios
- Para la autorización utiliza reglas IPTABLES.
- No requiere de la instalación de ningún cliente RADIUS, ya que por ser una aplicación web utiliza el Internet Explorer o cualquier otro navegador.
- Lenguaje de programación PHP
- Servidor web APACHE
- Interfaces de monitoreo
- Interfaces de administración.

1.5.1.2 Funcionamiento del servidor webRADIUS

WebRADIUS combina una serie de "pasos seguros" que en conjunto crean un sistema robusto. En primer lugar definiremos el proceso de autenticación que se realiza en una red WiFi, ya que en la actualidad requiere un mayor nivel de seguridad por el medio físico de transmisión.

1. El cliente se asocia con un punto de acceso (sin Autenticación inalámbrica) y obtiene una dirección IP con el protocolo DHCP (no se requiere Autenticación para obtener la dirección IP).

2. Una vez que el cliente obtiene la dirección IP, el cliente es forzado a identificarse en una pagina web (HTTPS) con un usuario y una password.

3. Este paquete es enviado al servidor webRADIUS quien es el responsable de verificar la validez de la contraseña y luego autorizar el acceso a la red o al internet a través de reglas IPTABLES

4. Las reglas IPTABLES están basadas en la dirección IP del cliente y los puertos a los cuales tiene acceso.

1.5.2 Autenticación y Autorización por Internet

La publicación de grandes volúmenes de información a través de Internet constituye un medio conveniente de acceder a esa información de una manera ágil y eficaz, contando además con la importante baza de una disponibilidad global. Más aún, la posibilidad de crear un canal de comunicaciones bidireccional, gracias al cual los usuarios no sólo son capaces de recuperar información de un servidor web, sino también de transmitírsela, principalmente a través de formularios, representa una forma igualmente eficiente de suministrar

Sin embargo, nunca debería suministrarse información confidencial por Internet ni almacenarse en servidores web sin ningún tipo de protección, especialmente en lo que se refiere a datos financieros y comerciales sensibles. A medida que crece la cantidad de información públicamente disponible y transportada a través de Internet, también lo hace la necesidad de asegurarla en parte o en su totalidad, protegiéndola de ojos indiscretos, pero no en detrimento de su facilidad de acceso.

1.5.2.1 Protocolos seguros para el web[7]

"La seguridad en la transmisión de la información se basa en el hecho de poder encriptar los mensajes que se envían por la red entre un servidor y un cliente y que solo ellos puedan descifrar los contenidos a partir de una clave común conocida solo por los dos.

Para llevar a cabo esta seguridad se crearon diversos protocolos basados en esta idea:"

1. SSH
2. SSL/TSL
3. HTTPS

[7] MILLER, Stewart S. Seguridad en WiFi. Madrid: McGraw-Hill,2004 268p.

1) **SSH (Secure Shell)**

Este protocolo fue diseñado para dar seguridad al acceso a computadores en forma remota.

Cumple la misma función que telnet o rlogin pero además, usando criptografía, logra seguridad con los datos.
A diferencia de telnet u otro servicio similar, SSH utiliza el puerto 22 para la comunicación y la forma de efectuar su trabajo es muy similar al efectuado por SSL.

Para su uso se requiere que por parte del servidor exista un demonio que mantenga continuamente en el puerto 22 el servicio de comunicación segura, el sshd.

El cliente debe ser un software tipo TeraTerm o Putty que permita hacer pedidos a este puerto 22 de forma cifrada.

La forma en que se entabla una comunicación es la misma para todos los protocolos seguros:

- El cliente envía una señal al servidor pidiéndole comunicación por el puerto 22.
- El servidor acepta la comunicación en el caso de poder mantenerla bajo encriptación mediante un algoritmo definido y le envía la llave pública al cliente para que pueda descifrar los mensajes.
- El cliente recibe la llave teniendo la posibilidad de guardar la llave para futuras comunicaciones o destruirla después de la sesión actual.

2) SSL (Secure Socket Layer) y TLS (Transport Layer Secure)[8]

"El protocolo SSL es un sistema de seguridad desarrollado por Netscape y utilizado actualmente por la mayoría de empresas que comercian a través de Internet. Es un sistema de seguridad ideado para acceder a un servidor garantizando la confidencialidad de los datos mediante **técnicas de encriptación modernas.**

SSL aporta las siguientes características:

a) **Confidencialidad:** Mediante el uso de la encriptación se garantiza que los datos enviados y recibidos no podrán ser interpretados por ninguna otra persona que no sea ni el emisor ni el receptor.
b) **Integridad:** Se garantiza que los datos recibidos son exactamente iguales a los datos enviados, pero no se impide que al receptor la posibilidad de modificar estos datos una vez recibidos.
c) **Autentificación:** El usuario se autentifica utilizando un Certificado Digital emitido por una empresa llamada Autoridad Certificadora, este documento es totalmente infalsificable y garantiza que el usuario es quien dice ser.

SSL opera como una capa adicional entre Internet y las aplicaciones, esto permite que el protocolo sea independiente de la aplicación, siendo posible utilizar FTP, Telnet y otras aplicaciones además de HTTP.

Existen tres versiones del protocolo, la cuarta es una mejora del SSLv3 y se conoce con el nombre de TLS. El protocolo TLS esta basado en SSL y son similares en el modo de operar.

Capas del protocolo SSL

[8] RANDALL K, Nichols y PANOS C, Lekkas. Seguridad para comunicaciones inalámbricas. Madrid: McGraw-Hill,2003. 563p.

Estos protocolos SSL/TLS se componen de dos capas: el Record Protocol y el Handshake Protocol.

a) **El Record Protocol (Protocolo de Registro)** es la capa inmediatamente superior a TCP y proporciona una comunicación segura. Principalmente esta capa toma los mensajes y los codifica con algoritmos de encriptación de llave simétrica como DES, RC4 aplicándole una MAC (Message Authentication Code) para verificar la integridad, logrando así encapsular la seguridad para niveles superiores. La porción de datos del protocolo tiene tres componentes:

   - MAC-DATA, el código de autenticación del mensaje.
   - ACTUAL-DATA, los datos de aplicación a transmitir.
   - PADDING-DATA, los datos requeridos para rellenar el mensaje cuando se usa cifrado en bloque.

b) **El Handshake protocol (Protocolo de acuerdo mutuo)** es la capa superior a la anterior y es usada para gestionar la conexión inicial.

Para establecer una comunicación segura utilizando SSL se tienen que seguir una serie de pasos entre los cuales tenemos:

1. **Solicitud de SSL:**

Antes de que se establezca SSL, se debe hacer una solicitud. Típicamente esto implica un cliente haciendo una solicitud de un URL a un servidor que soporte SSL. SSL acepta solicitudes por un puerto diferente al utilizado normalmente para ese servicio.

Una vez que se ha hecho la solicitud, el cliente y el servidor empiezan a negociar la conexión SSL, es decir, hacen el SSL Handshake.

2. **SSL Handshake:**

Durante el hanshake se cumplen varios propósitos. Se hace autenticación del servidor y opcionalmente del cliente, se determina que algoritmos de criptografía serán utilizados y se genera una llave secreta para ser utilizada durante el intercambio de mensajes subsiguientes durante la comunicación SSL. Los pasos que se siguen son los siguientes:

a) **Client Hello :** El "saludo de cliente" tiene por objetivo informar al servidor que algoritmos de criptografía puede utilizar y solicita una verificación de la identidad del servidor. El cliente envía el conjunto de algoritmos de criptografía y compresión que soporta y un número aleatorio. El propósito del número aleatorio es para que en caso de que el servidor no posea un certificado para comprobar su identidad, aún se pueda establecer una comunicación segura utilizando un conjunto distinto de algoritmos. Dentro de los protocolos de criptografía hay un protocolo de intercambio de llave que define como cliente y servidor van a intercambiar la información, los algoritmos de llave secreta que definen que métodos pueden utilizar y un algoritmo de hash de una sola vía. Hasta ahora no se ha intercambiado información secreta, solo una lista de opciones.

b) **Server Hello :** El servidor responde enviando su identificador digital el cual incluye su llave pública, el conjunto de algoritmos criptográficos y de compresión y otro número aleatorio. La decisión de que algoritmos serán utilizados está basada en el más fuerte que tanto cliente como servidor soporten. En algunas situaciones el servidor también puede solicitar al cliente que se identifique solicitando un identificador digital.

c) **Aprobación del Cliente:** El cliente verifica la validez del identificador digital o certificado enviado por el servidor. Esto se lleva a cabo desencriptando el certificado utilizando la llave pública del emisor y determinando si este proviene de una entidad certificadora de confianza. Después se hace una serie de verificaciones sobre el

certificado, tales como fecha, URL del servidor, etc. Una vez se ha verificado la autenticidad de la identidad del servidor. El cliente genera una llave aleatoria y la encripta utilizando la llave pública del servidor y el algoritmo criptográfico y de compresión seleccionado anteriormente. Esta llave se le envía al servidor y en caso de que el handshake tenga éxito será utilizada en el envío de futuros mensajes durante la sesión.

d) **Verificación:** En este punto ambas partes conocen la llave secreta, el cliente por que la generó y el servidor por que le fue enviada utilizando su llave pública, siendo la única forma posible de desencriptarla utilizando la llave privada del servidor. Se hace una última verificación para comprobar si la información transmitida hasta el momento no ha sido alterada. Ambas partes se envían una copia de las anteriores transacciones encriptada con la llave secreta. Si ambas partes confirman la validez de las transacciones, el handshake se completa, de otra forma se reinicia el proceso.

Ahora ambas partes están listas para intercambiar información de manera segura utilizando la llave secreta acordada y los algoritmos criptográficos y de compresión. El handshake se realiza solo una vez y se utiliza una llave secreta por sesión.

3. **Intercambio de datos:**

Ahora que se ha establecido un canal de transmisión seguro SSL, es posible el intercambio de datos. Cuando el servidor o el cliente desea enviar un mensaje al otro, se genera un digest (utilizando un algoritmo de hash de una vía acordado durante el handshake), encriptan el mensaje y el digest y se envía, cada mensaje es verificado utilizando el digest.

4. **Terminación de una sesión SSL:**

Cuando el cliente deja una sesión SSL, generalmente la aplicación presenta un mensaje advirtiendo que la comunicación no es segura y confirma que el cliente

efectivamente desea abandonar la sesión SSL. En la siguiente figura se muestra todo el proceso del Handshake:

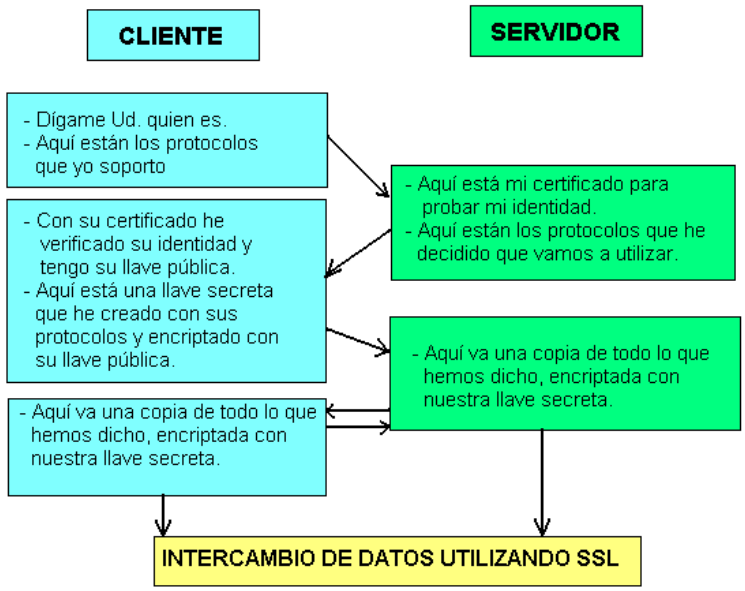


Figura 1-11 Esquema del proceso del Handshake

Aplicaciones e implementaciones del protocolo SSL/TLS

El protocolo SSL/TLS tiene multitud de aplicaciones en uso actualmente. La mayoría de ellas son versiones seguras de programas que emplean protocolos que no lo son. Hay versiones seguras de servidores y clientes de protocolos como el http, nntp, ldap, imap, pop3, etc.

Existen multitud de implementaciones del protocolo, tanto comerciales como de libre distribución. Una de las más populares es la biblioteca openssl que es la que utilizaremos para nuestro proyecto de tesis, escrita en C y disponible bajo licencia GNU. Incluye todas las versiones del SSL y el TLS y un gran número de algoritmos criptográficos, algunos de los cuales ni tan sólo son empleados en el estándar TLS.

3) HTTPS

El protocolo de red HTTPS es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP.

Los protocolos HTTPS son utilizados por navegadores como: Safari, Internet Explorer, Mozilla, Firefox, Opera, entre otros.

Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

El puerto estándar para este protocolo es el 443.

Para conocer si una página web que estamos visitando, utiliza el protocolo https y es, por tanto, segura en cuanto a la transmisión de los datos que estamos transcribiendo, debemos observar si en la barra de direcciones de nuestro navegador, aparece https al comienzo, en lugar de http."

1.5.2.2 Certificados Digitales[9]

"Los certificados digitales son el equivalente digital del DNI, en lo que a la autentificación de individuos se refiere, ya que permiten que un individuo demuestre que es quien dice ser, es decir, que está en posesión de la clave secreta asociada a su certificado.

Para los usuarios proporcionan un mecanismo para verificar la autenticidad de programas y documentos obtenidos a través de la red, el envío de correo encriptado y/o firmado digitalmente, el control de acceso a recursos, etc.

[9] Encriptación [[online.Consultado 04-07-2007. Disponible en http://es.wikipedia.org/wiki/Encriptación]

Un certificado de clave pública es un punto de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave pública pertenece a la entidad identificada y que la entidad posee la correspondiente clave privada.

Los certificados de clave pública se denominan comúnmente Certificado Digital, ID Digital o simplemente certificado. La entidad identificada se denomina sujeto del certificado o subscriptor (si es una entidad legal como, por ejemplo, una persona). “

Los certificados digitales sólo son útiles si existe alguna Autoridad Certificadora (Certification Authority o CA) que los valide, ya que si uno se certifica a sí mismo no hay ninguna garantía de que su identidad sea la que anuncia, y por lo tanto, no debe ser aceptada por un tercero que no lo conozca.

Es importante ser capaz de verificar que una autoridad certificadora ha emitido un certificado y detectar si un certificado no es válido. Para evitar la falsificación de certificados, la entidad certificadora después de autentificar la identidad de un sujeto, firma el certificado digitalmente.

Los certificados digitales proporcionan un mecanismo criptográfico para implementar la autentificación; también proporcionan un mecanismo seguro y escalable para distribuir claves públicas en comunidades grandes.

1.5.2.3 Certificados X.509

El formato de certificados X.509 es un estándar del ITU-T (International Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (International Standards Organization / International Electrotechnical Commission) que se publicó por primera vez en 1988. El formato de la versión 1 fue extendido en 1993 para incluir dos nuevos campos que permiten soportar el control de acceso a directorios. Después de emplear el X.509 v2 para intentar desarrollar un estándar de correo electrónico seguro, el formato fue revisado para

permitir la extensión con campos adicionales, dando lugar al X.509 v3, publicado en 1996.

Los elementos del formato de un certificado X.509 v3 son:

a) **Versión**. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
b) **Número de serie del certificado**. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.
c) **Identificador del algoritmo de firmado**. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
d) **Nombre del emisor**. Este campo identifica la CA que ha firmado y emitido el certificado.
e) **Periodo de validez**. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
f) **Nombre del sujeto**. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.
g) **Información de clave pública del sujeto**. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
h) **Identificador único del emisor**. Este es un campo opcional que permite reutilizar nombres de emisor.
i) **Identificador único del sujeto**. Este es un campo opcional que permite reutilizar nombres de sujeto.
j) **Extensiones**.

Las extensiones del X.509 v3 proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc. Un campo de extensión tiene tres partes:

1. **Tipo de extensión**. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.
2. **Valor de la extensión**. Este subcampo contiene el valor actual del campo.
3. **Indicador de importancia**. Es un flag que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones.

El ITU y el ISO/IEC han desarrollado y publicado un conjunto de extensiones estándar en un apéndice al X.509 v3:

- **Limitaciones básicas**. Este campo indica si el sujeto del certificado es una CA y el máximo nivel de profundidad de un camino de certificación a través de esa CA.
- **Política de certificación**. Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.
- **Uso de la clave**. Este campo restringe el propósito de la clave pública certificada, indicando, por ejemplo, que la clave sólo se debe usar para firmar, para la encriptación de claves, para la encriptación de datos, etc. Este campo suele marcarse como importante, ya que la clave sólo está certificada para un propósito y usarla para otro no estaría validado en el certificado.

El formato de certificados X.509 se especifica en un sistema de notación denominado sintaxis abstracta uno (Abstract Sintax One o ASN-1). Para la transmisión de los datos se aplica el DER (Distinguished Encoding Rules o reglas de codificación distinguible), que transforma el certificado en formato ASN-1 en una secuencia de octetos apropiada para la transmisión en redes reales.”

1.5.2.4 OpenSSL [10]

"Es un proyecto de software desarrollado por los miembros de la comunidad Open Sorce para libre descarga y está basado en SSLeay desarrollado por Eric Young y Tim Hudson. Consiste en un robusto paquete de herramientas de administración y librerías relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS). Estas herramientas ayudan al sistema a implementar el Secure Sockets Layer (SSL), así como otros protocolos relacionados con la seguridad, como el Transport Layer Security (TLS).

Este paquete de software es importante para cualquiera que esté planeando usar cierto nivel de seguridad en su máquina con un sistema operativo Libre basado en GNU/Linux. OpenSSL también nos permite crear certificados digitales que aplicaremos a nuestro servidor, en este caso usaremos un servidor Apache.

1.5.2.5 Servidor Web

Un servidor es una computadora que entrega a otras computadoras (los clientes), una información que ellos requieren bajo un lenguaje común, denominado protocolo. Por lo tanto al ver una página Web es porque el servidor les entrega una página HTML vía protocolo HTTP (HyperText Transport Protocol) o protocolo para la transmisión de hipertexto, a través de una conexión TCP/IP por el puerto 80.

Por lo tanto en el Servidor Web es donde se almacena la información estática accedida y/o las aplicaciones que la generan.

1.5.2.6 Servidor Apache

El servidor HTTP Apache es un software libre, servidor HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Windows, Macintosh y otras, que implementa el protocolo http.

---

[10] VLADIMIROV, Andrew A. ; GAVRILENKO, Konstantin y MIKHAILOVSKY, Andrei A. Hacking Wíreles: seguridad de redes inalámbricas. Madrid: Anaya Multimedia, 2005. 238p.

Apache es un software muy popular reconocido en muchos ámbitos profesionales y tecnológicos por las siguientes razones:

- Corre en una multitud de Sistemas Operativos, lo que lo hace prácticamente universal
- Apache es una tecnología gratuita de código fuente abierto. El hecho de ser gratuita es importante pero no tanto como que se trate de código fuente abierto. Esto le da una transparencia a este software de manera que si queremos ver que es lo que estamos instalando como servidor , lo podemos saber, sin ningún secreto, sin ninguna puerta trasera
- Apache es un servidor altamente configurable de diseño modular. Es muy sencillo ampliar las capacidades del servidor Web Apache. Actualmente existen muchos módulos para Apache que son adaptables a este, y están ahí para que los instalemos cuando los necesitemos. Otra cosa importante es que cualquiera que posea una experiencia decente en la programación de C o Perl puede escribir un modulo para realizar una función determinada
- Apache trabaja con gran cantidad de Perl, PHP y otros lenguajes de script.
- Apache permite personalizar la respuesta ante los posibles errores que se puedan dar en el servidor. Es posible configurar Apache para que ejecute un determinado script cuando ocurra un error en concreto.
- Tiene una alta configurabilidad en la creación y gestión de logs. Apache permite la creación de ficheros de log a medida del administrador, de este modo se puede tener un mayor control sobre lo que sucede en el servidor.

1.5.2.7 Servidor DHCP

DHCP (Dynamic Host Configuration Protocol) son las siglas que identifican a un protocolo empleado para que los clientes, en una red puedan obtener su configuración de forma dinámica a través de un servidor del protocolo. Los datos obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de broadcast, las características del DNS, entre otros. **DHCP** permite acelerar y facilitar la

configuración de muchos clientes en una red evitando en gran medida los posibles errores humanos.

Algunos beneficios del servidor DHCP son:

- Se puede administrar de manera centralizada toda la información de configuración de IP. De esta forma se elimina la necesidad de configurar manualmente los clientes individualmente cuando se implanta por primera vez TCP/IP o cuando se necesitan cambios en la infraestructura de IP.
- Se asegura que los clientes de **DHCP,** obtienen parámetros de configuración de IP precisos y en tiempo, sin intervención del usuario. Como la configuración es automática se elimina gran parte de los problemas.
- Flexibilidad.Utilizando DHCP, el administrador aumenta su flexibilidad para el cambio de la información de configuración de IP, lo que permite que el administrador cambie la configuración de IP de manera sencilla cuando se necesitan los cambios.”

1.5.2.8 Reglas IPTABLES.

IPtables es un sistema de firewall vinculado al kernel de linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servidor que lo iniciamos o detenemos o que se pueda caer por un error de programación, iptables esta integrado con el kernel, es parte del sistema operativo.
Realmente lo que se hace es aplicar reglas. Para ello se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas. Por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall, en nuestro tema de tesis estas reglas se generan dinámicamente a través del sistema webRADIUS.

1.6 DISPOSITIVOS DE RED INALÁMBRICA

1.6.1 Tarjetas de red [11]

El equipo de computación necesita una forma de conectarse a la red ethernet, si la red es inalámbrica, o ambas. Se hace la conexión a través de un adaptador de red, un equipo que provee una interfase de la computadora a red. La mayoría de las computadoras se venden con el adaptador para redes inalámbricas ya preinstalado en la fábrica, y estos adaptadores se construyen cada vez más sobre la tarjeta madre. Por el momento es más común que las computadoras portátiles vengan con adaptadores inalámbricos instalados. La mayor parte de las personas, para conectar la computadora portátil o la de escritorio, necesitan comprar e instalar adaptadores de red inalámbrica por separado. La mayoría de los adaptadores vienen en tres configuraciones: PC cards, USB, o PCI y recientemente han aparecido en Compact Flash y usando la tecnología Bluethoot.. En la siguiente figura se puede ver una tarjeta inalámbrica para computadora portátil.

Figura 1-12 Tarjeta de red PC-Card

[11] Inalámbrica [online.Consultado 04-07-2007. Disponible en http://es.wikipedia.org/wiki/Inalámbrica].

1.6.2 Puntos de Acceso

Los puntos de acceso desempeñan muchas funciones importantes, además de ser las interfaces entre la red normal y el medio inalámbrico, una de sus principales funciones es la de ser estación de camino del tráfico inalámbrico en la red. De hecho, muchas redes inalámbricas usan múltiples puntos de acceso, cada uno actuando precisamente como una estación de camino, extendiendo el alcance de la red local de acceso inalámbrico, ofreciendo puntos físicos adicionales para la conexión. En redes más pequeñas, un solo punto de acceso provee un transmisor y receptor central para todas las computadoras en la red, ruteando tráfico de y hacia varios adaptadores inalámbricos mientras proporciona acceso a los clientes a una o varias redes inalámbricas.

1.6.3 Routers y switches inalámbricos

Los puntos de acceso inalámbricos frecuentemente incluyen la tecnología y características de los routers. Virtualmente todos los vendedores de equipo inalámbrico ofrecen por lo menos un equipo que combina un punto de acceso con un router, resultando en una sola caja pequeña con tres o cuarto puertos para cables ethernet, otro para el cable modem, y los componentes inalámbricos requeridos por el punto de acceso, incluyendo la antena.

Ahora se escucha la palabra router mas comúnmente que switch cuando se habla de ventas de equipo de red a hogares y pequeñas oficinas, pero en la realidad la mayoría de cable/DSL routers también son switches. La diferencia es muy simple, un router conecta dos o mas redes pasando datos a través de ellos, mientras los switches provee interconexión entre computadoras en una sola red aislando el tráfico de cada uno, de tal manera que la señal viaja del origen al destino sin que otra computadora tenga acceso a ellas. En la siguiente figura se puede ver como es un router inalámbrico.

Figura 1-13 Router Inalámbrico

CAPITULO II

2.1 PRESENTACIÓN ANALISIS E INTERPRETACIÓN DE RESULTADOS

2.1.1 Caracterización de la 9-BFE “PATRIA”.

BRIGADA DE FUERZAS ESPECIALES No. 9 “PATRIA”

La Brigada de Fuerzas Especiales No. 9 “PATRIA”, basa sus actividades formando a sus soldados con el curso básico de Paracaidistas, luego del cual profesionaliza a sus miembros con los entrenamientos militares que versan tanto en selva, mar y actividades de montaña.

Prácticamente la historia de la Brigada se remonta al 29 de octubre de 1956, fecha en la cual los bravos pioneros ecuatorianos al mando de un gran soldado visionario el Capt. Alejandro Romo Escobar cumplieron el loco sueño de volar cual cóndor majestuoso sobre el azul profundo del infinito.

El nacimiento de esta élite de Soldados se dio con el destacamento Especial de Paracaidistas con sede en Quito, que luego se convirtió en Escuela de Paracaidistas y mas tarde con la creación de los diferentes grupos se constituyó en la Cuna de los Héroes conocida como Brigada de

Fuerzas Especiales No. 9 “PATRIA”, cuyas instalaciones se encuentran en la gallarda Provincia de Cotopaxi.

Los Soldados boinas rojas han estado, están y estarán presentes en los momentos de mayor peligro y crisis de su pueblo, y consientes de la dura realidad nacional apoyan al desarrollo permanente de la sociedad ecuatoriana, El paracaidista cumplió su función como maestros de la juventud en la instrucción militar estudiantil voluntaria, cumple con acciones de apoyo en coordinación con los gobiernos seccionales para la construcción de comedores escolares, casas comunales, escuelas, áreas de recreación mantenimiento y reconstrucción de aulas, campañas de vacunación, brigadas médicas, capacitación técnica de lideres campesinos para la agroindustria y entrega de material didáctico.

2.1.2 **Análisis de los resultados de las entrevistas realizadas a los administradores de la red.**

ENTREVISTA DIRIGIDA AL PERSONAL TECNICO QUE ADMINISTRA LA RED INALAMBRICA EN EL CENTRO DE COMPUTO DE LA BRIGADA DE FUERZAS ESPECIALES No. 9 “PATRIA”

1.- Como define usted, a una WLAN?

- Una red de área local inalámbrica (WLAN) es un sistema de comunicación de datos flexible que puede reemplazar o extender una red de área local cableada (LAN) para ofrecer funcionalidad adicional.

- Una red de área local cableada tradicional (LAN) envía paquetes de datos desde un equipo a otro a través de cables.

- Una red de área local inalámbrica (WLAN), por el contrario, depende de ondas de radio para transferir datos. Estos datos son sobrepuestos en una onda de radio por medio de un proceso denominado modulación, y esta onda portadora, actúa entonces como el medio de transmisión, ocupando el lugar del cable.

2.- Por qué, implementaron la red WLAN?

- Por las inherentes ventajas económicas y funcionales en su implementación.

- Por su capacidad de procesar y acceder.

- Para compartir recursos y servicios que serán de utilidad entre las unidades, el personal de oficiales y voluntarios

- Soportan un número elevado de usuarios, independientemente de la localización física

- Una infraestructura ya no necesita ser sólida y fija, difícil de movilizar y costosa de cambiar. Por el contrario, con la WLAN puede moverse con el usuario y cambiar tan rápido como la organización lo haga. Por ejemplo, los usuarios pueden permanecer conectados mientras se movilizan a través del campo de cobertura, explotando fácilmente los recursos de la red.

3.- Qué servicios ofrece al momento la WLAN?

- Internet
- Impresión

4.- Qué inconvenientes presenta la utilización de la WLAN?

- Acceso sólo en ciertos lugares

- El método de autenticación de los usuarios, no es muy seguro

5.- Cree usted que la seguridad en la WLAN, es un problema prioritario a resolver?

- Si, debido a que se debe proteger el ingreso a la red, por cuanto se maneja información muy importante y sobre todo confidencial dentro de la unidad.

- Existe personal no autorizado que conoce la clave de acceso y puede ingresar con gran facilidad.

6.- Según usted, cuales podrían ser las medidas a tomar para dar seguridad a la WLAN?

- Contar con una mejor infraestructura tanto en hardware como en software (Access Point, Servidor).

- Implementar un nuevo método de autenticación, para dar seguridad a la información.

7.- Siendo la Autenticación un método para identificar a los usuarios mediante la petición y comparación de datos almacenados previamente en una base de datos.
Cree usted, que sería necesario implementar un sistema de autenticación para controlar el acceso a la red y así proteger la privacidad de los datos?

- Si, siempre y cuando este a la par con la actualidad informática para lo que es necesario ampliar la

compatibilidad con protocolos de autenticación más efectivos

- Que sea un método eficiente y eficaz.

Análisis de los resultados

Según los resultados obtenidos en las entrevistas realizadas podemos determinar que existe una necesidad prioritaria en contar con un servicio de red acorde con las necesidades de la Brigada de Fuerzas Especiales No. 9 "PATRIA" que les permita accesar con rapidez y confianza al manejar información confidencial, y de esta manera aprovechar todos los recursos disponibles, que brinda la WLAN a los usuarios, implementando un sistema de autenticación que permita controlar el acceso a la red.

2.1.3 Análisis de los resultados de las encuestas

La información que se presenta a continuación es el resultado de las encuestas realizadas a 30 personas.

ENCUESTA DIRIGIDA AL PERSONAL DE USUARIOS QUE INGRESAN A LA RED INALAMBRICA DE LA BRIGADA DE FUERZAS ESPECIALES No. 9 "PATRIA"

2.1.3.1 Conoce usted como funcionan las Redes Inalámbricas ?

OPCION	f	%
SI	19	63
NO	11	37
TOTAL	30	100

Cuadro 1

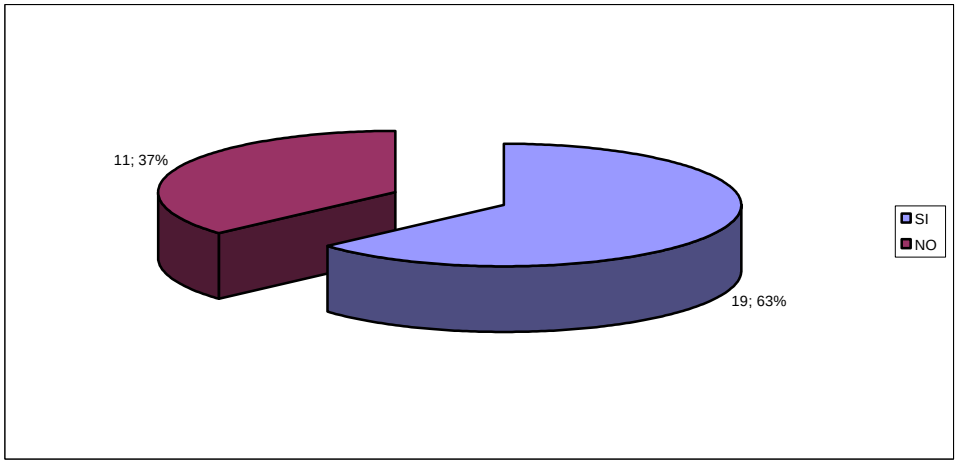


Gráfico 1

Los resultados presentan un CONOCIMIENTO ALTO sobre redes y su funcionamiento.

2.1.3.2 El equipo con el que se conecta a la red es ?

OPCION	f	%
PC(DE ESCRITORIO)	23	76
PORTATIL	5	17
PDA(AYUDANTE PERSONAL DIGITAL)	2	7
TOTAL	30	100

Cuadro 2

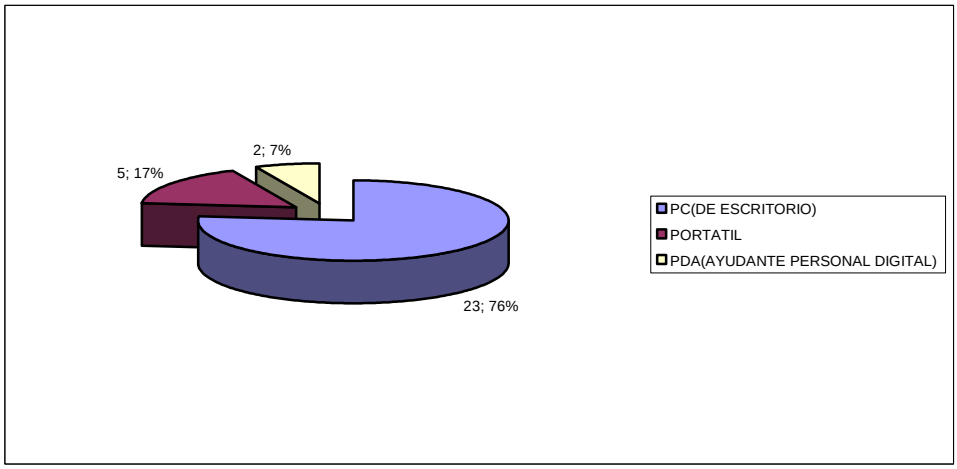


Gráfico 2

El análisis demuestra un ALTO NUMERO de personas que utilizan equipos de computación para realizar sus labores.

2.1.3.3 Resulta fácil para usted, conectarse a la red inalámbrica ?

OPCION	f	%
SI	13	43
NO	17	57
TOTAL	30	100

Cuadro 3

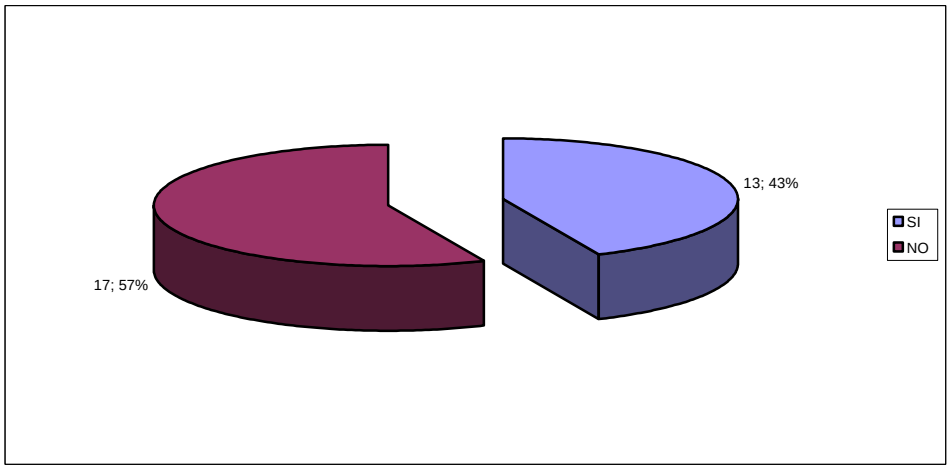


Gráfico 3

Los resultados demuestran una DEBILIDAD ALTA en vista que no existen las facilidades para conectarse a la red y poder desarrollar su trabajo.

2.1.3.4 Usted se conecta al Internet, en cualquier momento ?

OPCION	f	%
SI	10	33
NO	20	67
TOTAL	30	100

Cuadro 4

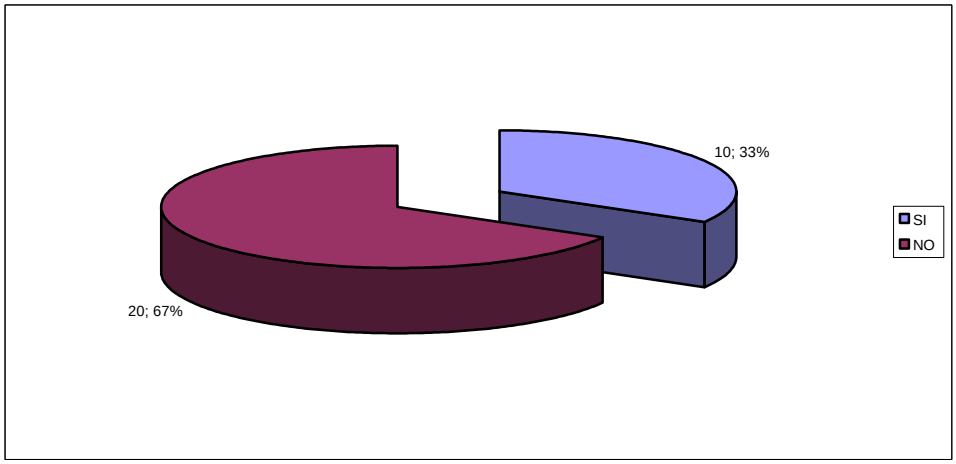


Gráfico 4

Se considera a estos resultados como una DEBILIDAD ALTA en función al avance tecnológico, ya que en estos tiempos todos deberíamos acceder a Internet.

2.1.3.5 Cuando utiliza el Internet desde su equipo, este es: ?

OPCION	f	%
EXCELENTE	7	23
MUY BUENO	11	37
BUENO	5	17
REGULAR	6	20
MALO	1	3
TOTAL	30	100

Cuadro 5

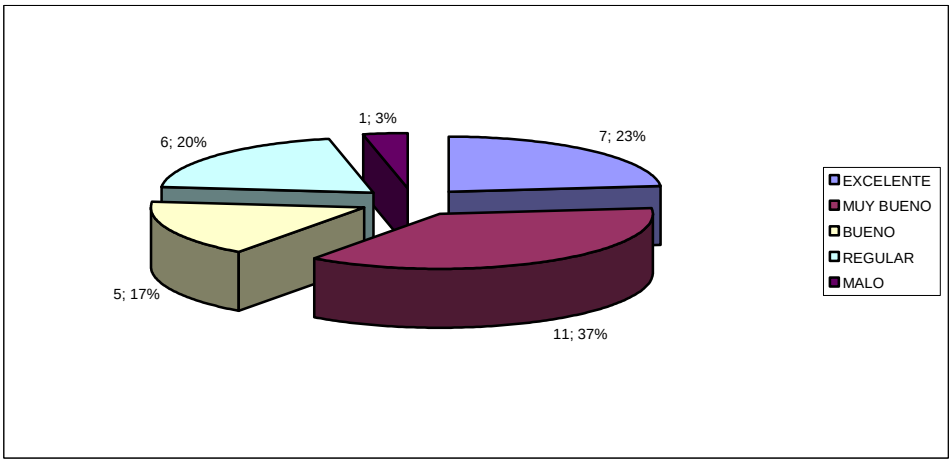


Gráfico 5

En el análisis podemos determinar una DEBILIDAD MEDIA debido a los diversos criterios emitidos por los encuestados.

2.1.3.6 Le parece bien que implementen medidas de seguridad para proteger los datos de la Brigada y los suyos ?

OPCION	f	%
SI	22	73
NO	8	27
TOTAL	30	100

Cuadro 6

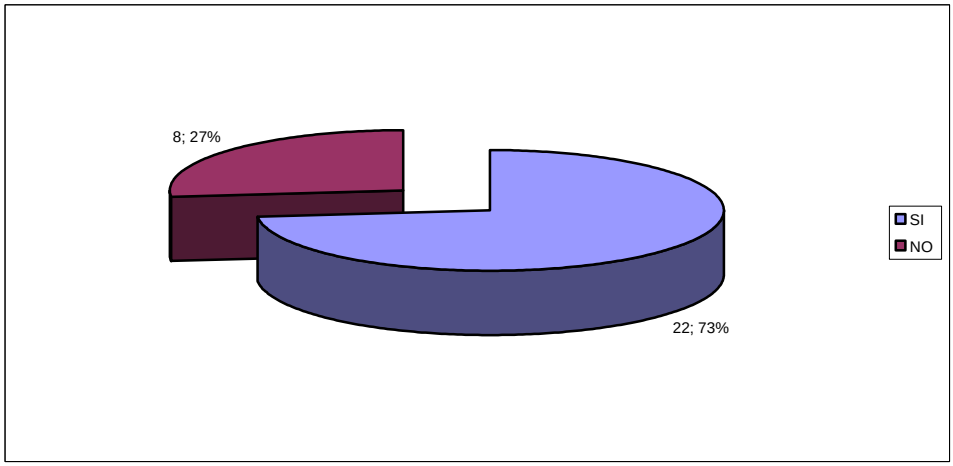


Gráfico 6

Los resultados obtenidos nos dan la idea, la necesidad de proteger los datos de la Brigada, por tratarse muchas veces de información confidencial, y de igual manera de cada uno de los encuestados.

2.1.3.7 Al ingresar a la red le permite digitar el usuario y la contraseña?

OPCION	f	%
SI	7	23
NO	23	77
TOTAL	30	100

Cuadro 7

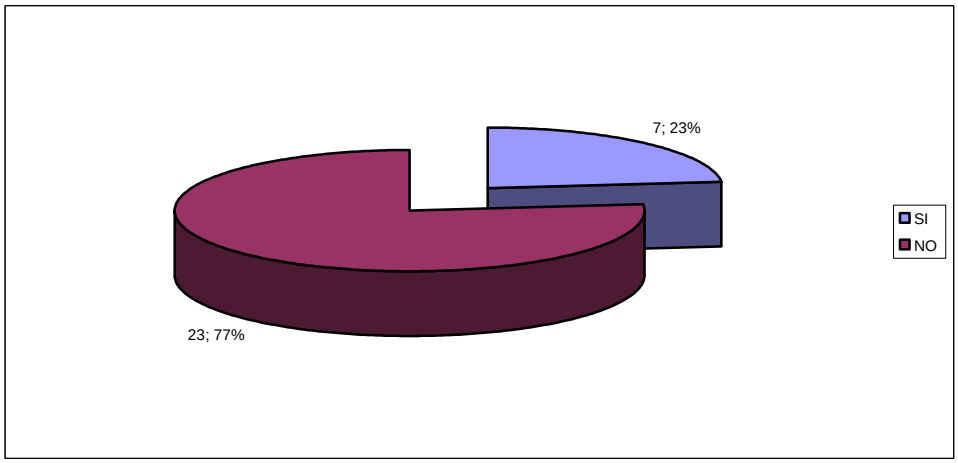


Gráfico 7

De acuerdo a los resultados se puede considerar que la mayoría de usuarios pueden acceder al servicio de Internet sin requerir una clave para ello, lo que conlleva a que el servicio en muchas ocasiones se vuelva lento.

2.1.4 Verificación de la hipótesis

Se trabajó la Tesis con la siguiente hipótesis: "**La implementación de un sistema de autenticación permitirá controlar la seguridad de la red inalámbrica de la 9-BFE "PATRIA**".

A continuación se presentan algunos argumentos que confirman el enunciado de la hipótesis.

- La seguridad en redes tipo inalámbricas, es un factor muy importante debido a la naturaleza del medio de transmisión: el aire. Las características de seguridad en la WLAN (Red Local Inalámbrica), se basan especialmente en la protección a la comunicación entre el punto de acceso

y los clientes inalámbricos, controlan el ingreso a esta red, y protegen al sistema de administración de acceso no autorizado.

- Sin un sistema de control, los procedimientos y mecanismos de seguridad eran tan débiles que se podía tener acceso con relativa facilidad hacia la red LAN desde cualquier usuario sin la debida autorización.

- Al implementar el sistema de autenticación, permitió brindar mayor confianza a los usuarios al manejar información estrictamente confidencial.

- Con el sistema de autenticación se logró dar acceso únicamente a los equipos y usuarios autorizados, restringiendo de esta manera el acceso no autorizado, con lo que se evitó ataques a la red y proliferación de virus informáticos.

- Se disminuyó notablemente el uso del ancho de banda ya que el sistema permitió controlar el tiempo de uso del Internet.

- Con la autorización personalizada a través de puertos, que es lo que dispondrá el sistema de autenticación y autorización, se logró mayor seguridad ya que se restringió todo dando acceso únicamente a lo necesario.

- El sistema de autenticación y autorización vía web estará basado en un protoloco seguro, lo que permite encriptar los mensajes que se envían en la red entre un servidor y un cliente, garantizando de esta manera la seguridad en la transmisión de la información a través de la web.

CAPITULO III

3.1 IMPLEMENTACIÓN DEL SISTEMA DE AUTENTICACIÓN Y AUTORIZACIÓN WEBRADIUS.

Este capítulo abarca la construcción e implementación del entorno de seguridad propuesto en la introducción de este trabajo, para establecer el entorno se usa un sistema de autenticación y autorización vía web basado en el protocolo seguro SSL. La construcción de este sistema de seguridad se presenta a continuación tomando en cuenta los diferentes puntos necesarios como es el uso de una arquitectura de red, los distintos servicios y paquetes instalados y configurados (DHCP, Apache, Mysql, openSSL, sudo, php), la utilización de un servidor webRADIUS, incluyendo su instalación y configuración previa, y las distintas configuraciones de los elementos principales restantes, como el punto de acceso inalámbrico, y el cliente en este caso el navegador web.

3.1.1 Arquitectura de Red utilizada

Para la implementación del sistema de autenticación inalámbrica vía web se utiliza una arquitectura de red simple compuesta por un punto de acceso inalámbrico, un cable ethernet para el acceso a la intranet, un servidor de seguridad, y uno o varios clientes con tarjeta de red inalámbrica. La arquitectura se puede ver en la figura 4 -1.

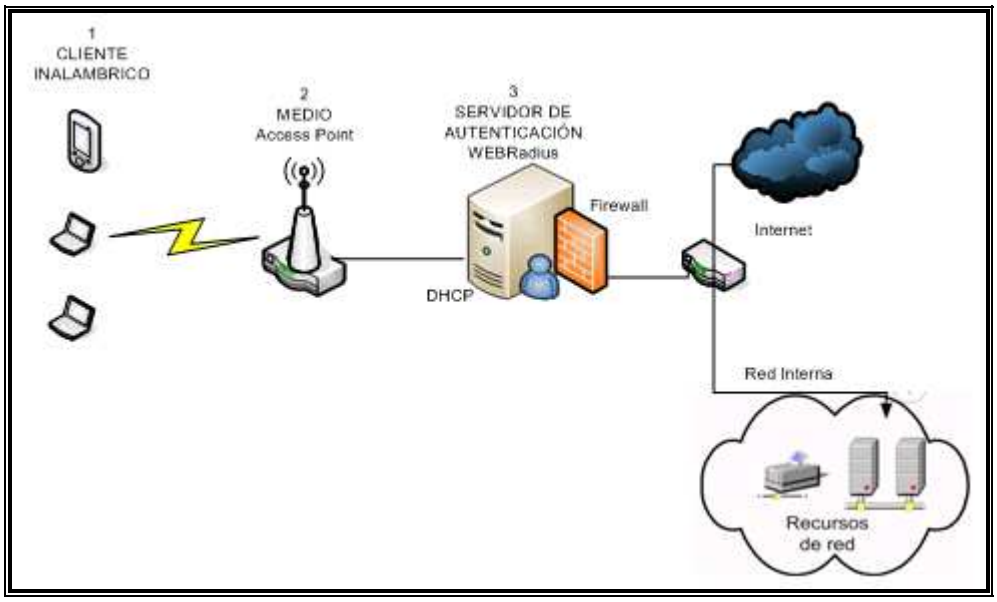


Figura 4-1. Arquitectura de red

El primer elemento de la arquitectura es un cliente inalámbrico que se conecta al punto de acceso a través de una tarjeta de red inalámbrica, el segundo elemento es un punto de acceso que sirve como medio para que el cliente inalámbrico se conecte con el servidor de seguridad y la red ethernet, y el tercer elemento es el servidor de seguridad que contiene los servicios de DHCP para que los clientes obtengan una dirección IP, webRADIUS para administrar la autenticación de los clientes y un firewall para autorizar o denegar el acceso a la red ethernet o al Internet.

3.1.2 Hardware usado

En la implementación del esquema de red utilizado se requiere de los siguientes dispositivos:

Una computadora con ambiente Linux

Un Punto de Acceso.

Una computadora Laptop con sistema operativo Windows XP

3.1.3 Software usado

Sistema operativo Linux Red Hat 9.2

Aplicación webRADIUS

perl-DBI-1.32-5.i386.rpm

Mysql-4.0.12.0

php-4.3.2.tar

apache-1.3.27.tar

Sudo-1.6.3p7.tar

OpenSSL1-0.9.71

Sistema operativo Windows XP con *Service Pack 2*

Cliente Internet Explorer 6 con service pack 1

3.1.4 Instalación y configuración del sistema de seguridad webRADIUS.

Para la instalación del sistema webRADIUS se requiere instalar previamente ciertos componentes que permitirán poner en funcionamiento nuestro sistema de autenticación y autorización de usuarios webRADIUS.

- **Sistema de Autenticación:** Este componente es básicamente una serie de módulos en PHP que se ejecutan en el servidor web para realizar la autenticación y autorización de los usuarios hacia el Internet o la intranet ; y para realizar un registro de la información recopilada por el sistema.
- **Un servidor de bases de datos:** El sistema utiliza MySql. Este servidor puede ser instalado localmente o estar ubicado en cualquier lugar de la intranet y ser utilizado por otras aplicaciones. En la instalación se incluye un sistema para administración de las bases de datos (MysqlAdministrator).
- **Un servidor Web:** El sistema utiliza el servidor Apache el cual se encarga de resolver las peticiones de los clientes utilizando el protocolo de Internet https.
- **PHP:** El interpretador de PHP que se encarga de ejecutar los módulos de la aplicación en PHP.
- **Sudo:** Se utiliza para permitir al usuario que ejecuta el servidor de Internet (Apache) poder ejecutar los comandos iptables Estos comandos son los

que permiten al Sistema webRADIUS autorizar el acceso de las estaciones de trabajo al internet a la intranet.

- **Openssl:** Este paquete contiene herramientas de administración y librerías relacionadas con la criptografía. Con esta herramienta implementaremos el protocolo seguro https.
- **DHCP:** Este servicio permite a los clientes inalámbricos obtener una dirección IP en forma dinámica a través de las MAC-ADRESS.

3.1.5 Proceso de instalación del Servidor

Para la instalación del Sistema de autenticación y autorización webRADIUS se requiere de los siguientes programas y archivos de configuración:

Programas

- apache_1.3.27.tar
- php-4.3.2.tar
- sudo-1.6.3p7.tar
- perl-DBI-1.32-5.i386.rpm
- mysql
- openssl-0.9.7i.tar.gz
- dhcp-3.0pl1-23.i386.rpm

Archivos de configuración

- fwebradius
- httpd.conf
- php.ini
- sudoers
- rc.local
- info.php

Una vez que obtengamos los paquetes y archivos copiamos al directorio **/usr/local/src** para proceder a instalarlos y configurarlos.

Procedemos a descomprimir todos los programas .tar al directorio **/usr/local/src** (haciendo doble clic sobre cada uno de los programas .tar) luego de descomprimir en la dirección **/usr/local/src/** se crearán los siguientes directorios:

- apache-1.3.27
- php-4.3.2
- sudo-1.6.3p7
- openssl-0.9.7i.tar.gz

3.1.5.1 Instalación del Servidor APACHE

El servidor Apache es el servicio que se encarga de resolver las peticiones de páginas de Internet de los clientes utilizando el protocolo de Internet http o https en nuestro caso.

A continuación se presentan las instrucciones de instalación de Apache en el servidor Linux.

2) Ingresamos al directorio /usr/local/src/apache-1.3.27 y ejecutamos la siguiente línea de comando:

#./configure --prefix=/usr/local/apache --enable-module=so
 # make
 # make install

Apache quedará instalado en el directorio

/usr/local/apache

3) Subir el servicio de apache. Ingresamos al directorio /usr/local/apache/bin y ejecutamos lo siguiente:

#./apachectl start

4) Para comprobar que apache se instaló correctamente, abrir un navegador y en la dirección escriba nombre del servidor o la dirección IP del equipo, deberá poder ver la página de prueba de apache que indica:

¡Funciono! El Servidor de Red Apache ha sido instalado en este sitio

5) Configuramos apache copiando del directorio /usr/local/src el archivo **httpd.conf** al directorio /usr/local/apache/conf/

6) Subir el servicio de apache. Ingresamos al directorio **/usr/local/apache/bin** y ejecutamos lo siguiente:

#./apachectl start

3.1.5.2 Instalación de PHP

1) Ingresamos al directorio /usr/local/src/php-4.3.2 y ejecutamos la siguiente línea de comando:

#./configure --with-mysql --with-apache=/usr/local/src/apache-1.3.27
 # make
 # make install

2) Copiar la librería **libphp4.a** de /usr/local/src/php-4.3.2/libs al directorio /usr/local/src/apache-1.3.27/src/module/php4

3) Compilamos nuevamente el apache

#./configure --prefix=usr/local/apache --activate-module=src/modules/php4/libphp4.a
#make
#make install

4) Subir el servicio de apache. Ingresamos al directorio /usr/local/apache/bin y ejecutamos lo siguiente:

#./apachectl start

Configuramos PHP copiando del directorio /usr/local/src/ el archivo php.ini al directorio /usr/local/lib/

5) Reiniciar el equipo

6) Comprobar que el servidor este respondiendo paginas php, para lo cual abrir un navegador y probar con una pagina php (copie el archivo **info.php** desde /usr/local/src al directorio web /usr/local/apache/htdocs), debe obtener la siguiente pagina de respuesta

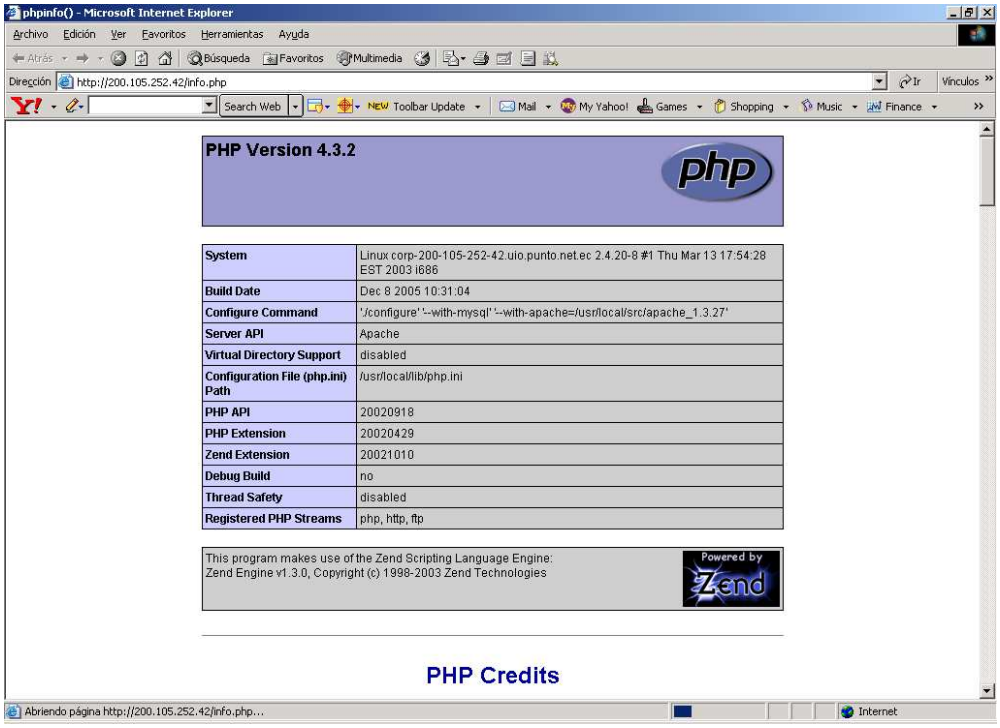


Figura 4-2. Respuesta del servidor apache con resolución PHP.

3.1.5.3 Instalación de SUDO

1) Ingresamos al directorio /usr/local/src/sudo-1.6.3p7 y ejecutamos la siguiente línea de comando:

#./configure

 # make

 # make install

2) Para configurar sudo copie el archivo **sudoers** desde /usr/local/src al directorio /etc

3.1.5.4 Instalación de MySQL

MySQL necesita que el paquete perl este instalado para lo cual procedemos con la siguiente instalación:

1) Ingrese al directorio **/usr/local/src/** y ejecute la siguiente línea de comando

 # rpm –ivh perl-DBI-1.32-5.i386.rpm

2) Ingrese al directorio /usr/local/src y ejecute la siguiente línea de comando:

#rpm –ivh My*

3) Verifique que el servicio **mysql** este subido, ejecutando el siguiente comando.

#ntsysv

4) Ingrese al directorio **/usr/bin** y ejecute la siguiente línea de comando para definir las claves de acceso del administrador (usuario *root*) para MySQL.

 # mysqladmin -u root password '……..'

5) Verifique que se pueda acceder a mysql con la clave que se ingreso

#mysql -u root -p
Ingrese la clave ……

Y debe obtener una consola de mysql, aquí puede ejecutar alguna instrucción sql.

>showdatabases;

Salimos de mysql.

Con esto queda instalado MYSQL.

Una vez instalado MySQL se debe subir la base de datos y copiar el contenido del sistema webRADIUS al directorio /usr/local/apache2/htdocs.

3.1.5.5 Instalación de OPENSSL, creación de certificados y configuración del servidor web seguro (https).

Antes de empezar debemos comprobar que nuestro servidor Apache este compilado con el módulo de seguridad que vamos a utilizar.

Para ver listar los módulos podemos ejecutar:

```
# cd /usr/local/apache2/bin
# ./httpd -l
Compiled in modules:
  core.c
  mod_access.c
  mod_auth.c
  mod_auth_digest.c
  mod_include.c
  mod_log_config.c
  mod_env.c
  mod_setenvif.c
```

mod_ssl.c

prefork.c

http_core.c

mod_mime.c

mod_status.c

mod_autoindex.c

mod_asis.c

mod_cgi.c

mod_negotiation.c

mod_dir.c

mod_imap.c

mod_actions.c

mod_userdir.c

mod_alias.c

mod_so.c

En la lista debe aparecer:

- mod_ssl.c: para poder activar SSL (https).

Para compilar Apache con soporte SSL es necesario tener instalado los fuentes de openssl, ya que al compilar se necesitan los ficheros de cabecera (.h). También necesitamos tener instalado openssl para poder trabajar con los certificados.
Para instalar openssl nos ubicamos en el directorio donde se encuentra el paquete openssl y ejecutamos lo siguiente:

 # /usr/local/src/openSSL1-0.9.71

#./configure

#make

#make install

Ahora ya podemos recompilar nuestro servidor Apache. Nos situamos en el directorio donde tentemos los fuentes de Apache y usamos los siguientes comando:

 # ./configure --prefix=/usr/local/apache2 --with-mpm=prefork --enable-so --ecnable-auth-digest --enable-ssl

 # make

 # make install

Trabajar con SSL nos permite que todos los datos que se transfieren entre el cliente y el servidor vayan cifrados.

Antes de hablar más sobre SSL vamos a definir algunos términos:

RSA Private Keys: fichero digital que podemos usar para descifras mensajes que nos mandan. Tiene una parte pública (que distribuimos con nuestro certificado), que permite a la gente cifrar los mensajes que nos manda. Este mecanismo de clave asimétrica nos asegura que los mensajes cifrados con la clave pública (que distribuimos a mucha gente) sólo pueden ser descifrados con la clave privada (que sólo conocemos nosotros).

Certificate Signing Request (CSR): es un fichero digital que contiene nuestra clave pública y nuestro nombre.

Certification Authority (CA): entidad de confianza encargada de firmar certificados (CSR).

Certificate (CRT): Una vez la CA a firmado el CSR, obtenemos un CRT. Este fichero contiene nuestra clave pública, nuestro nombre, el nombre de al CA, y está firmado digitalmente por la CA. De esta forma otras entidades pueden verificar esta firma para comprobar la veracidad del certificado. Es decir, si obtenemos un certificado que esta firmado por una CA que nosotros consideramos de confianza, podemos confiar también en la autenticidad del certificado.

Ahora que ya tenemos un poco más claros los conceptos, podemos ver que hay varias posibilidades para configurar SSL. Por ejemplo:

- Cualquier cliente puede conectarse a una URL determinada, usando https. En este caso el servidor enviará su certificado al cliente para que este

pueda descifrar la información que le llega del servidor y cifrar la que envía hacia el servidor.

- También podríamos hacer que sólo los clientes que tengan un determinado certificado puedan conectarse a una determinada URL.
- Otra posibilidad es combinar el primer ejemplo con las técnicas de autenticación que hemos visto antes. De forma que cuando intentemos acceder a una determinada URL usando https tendremos que autenticarnos primero.

Creando nuestra propia CA

Existen varias CAs que, previo pago, pueden firmar nuestro CSR. Estas CAs son mundialmente conocidas de forma que cualquier cliente podrá conectarse con confianza a nuestro servidor.

Un ejemplo de este tipo de entidades de certificación puede ser VISA o VeriSign.

En nuestro caso, como estamos probando, nos crearemos nuestra propia CA.
Para facilitar este tipo de tareas el paquete openssl nos proporciona el script CA.sh (o CA.pl en Perl). Ejecutamos:

```
# cd /usr/local/apache2
# /usr/lib/ssl/misc/CA.sh -newca
```

Nos hará las siguientes preguntas:

1. Nombre del certificado de la CA o que pulsemos 'enter' para crearlo. En nuestro caso pulsamos 'enter' para crear uno nuevo.
2. Una 'pass phrase', que nos vuelve a preguntar para confirmarla. Esta será la clave para acceder a la clave privada (la clave privada se guarda cifrada). Deberíamos poner más de una palabra.
3. Cierta información para añadir al certificado: código del país, provincia, localidad, nombre de la organización, de la unidad, etc.

Una vez finaliza la ejecución del script podemos ver que en el directorio /usr/local/apache2 nos ha aparecido un nuevo directorio: demoCA.

El fichero cacer.pem es el certificado de la CA, que luego usaremos para firmar nuestro certificado.

Los subdirectorios están vacíos, a excepción de private, donde encontramos el fichero cakey.pem. Este fichero es la clave de la CA.

Creamos nuestro CSR

Ahora vamos a crear el CSR que debería firmar una auténtica CA (nosotros lo firmaremos con nuestra propia CA, la que hicimos en el apartado anterior). Para esto seguimos los siguientes pasos:

1) Creamos la clave para nuestro servidor Apache (la clave será triple-DES y en formato PEM):

 # openssl genrsa -des3 -out server.key 1024

El comando nos pedirá un 'pass phrase' y nos la vuelve a preguntar para confirmarla.

2) Creamos el CSR (estará en formato PEM), usando la clave generada en el punto anterior:

 # openssl req -new -key server.key -out server.csr

Lo primero que hará será pedirnos la 'pass phrase' que le pusimos a la clave en el punto anterior. Luego nos pedirá los datos que queremos añadir a nuestro certificado. Aquí es importante tener en cuenta que cuando nos pregunte por el 'Common Name' debemos poner el nombre completo del dominio del servidor, por ejemplo, si vamos a acceder usando https://webradius.com/, tendremos que poner webradius.com

Con esto hemos conseguido generar el fichero server.csr.

Creamos nuestro CRT

El último paso es firmar el CSR para conseguir el CRT. Para esto volveremos a usar el script CA.sh. El problema que tiene este script es que trabaja con unos nombres fijos de ficheros, así que antes de ejecutarlo tenemos que renombrar el fichero server.csr.

```
# ln -s server.csr newreq.pem
# CA.sh –signreq
```

Nos pedirá la 'pass phrase' de la clave que hemos usado para generar el certificado de la CA.

Nos mostrará la información de nuestro certificado, y nos preguntará si queremos firmar el certificado. Contestamos que sí.

Nos preguntará si queremos hacer 'comit' de los certificados firmados, es decir si queremos confirmar la operación. De nuevo, contestamos que sí.

Nos habrá generado el fichero newcert.pem. Este fichero lo renombramos por server.crt.

```
# mv newcert.pem server.crt
```

Configuramos Apache

Lo primero es poner los ficheros donde corresponde.

```
# mkdir conf/ssl.key
# mkdir conf/ssl.crt
```

 # mv server.key conf/ssl.key/

 # mv server.crt conf/ssl.crt/

Ahora añadimos al fichero /usr/local/apache2/conf/httpd.conf:

```
<Directory "/usr/local/apache2/htdocs/webradius">
    SSLRequireSSL
</Directory>
```

Esta directiva prohíbe el acceso a no ser que sea HTTP sobre SSL (HTTPS).Con esto conseguimos que para acceder al directorio /usr/local/apache2/htdocs/webradius sea obligatoriamente usando HTTPS

Por último sólo nos queda arrancar Apache. Hay que tener en cuenta que para arrancar Apache con soporte SSL hay que utilizar:

 # /usr/local/apache2/bin/apachectl startssl

Vemos que al arrancar Apache nos pide una 'pass phrase'. Esta es la que usamos al crear nuestro certificado. Esto lo hace porque la clave esta guardada cifrada.

3.1.5.6 Configuración del Servidor DHCP

1) Instalar el programa DHCP Server

#rpm –ivh d.C.-3.0pl1-23.i386.rpm

2) Crear y editar los archivos dhcpd.conf y dhcpd.leases

Crear el archivo **dhcpd.conf**

#cd /etc

#touch dhcpd.conf

Copiar una muestra del archivo:

#cp /usr/share/doc/dhcp-3.0pl1/dhcpd.conf.sample /etc/dhcpd.conf

Editar el contenido del archivo **dhcpd.conf** y configurar de acuerdo a la figura 4-3

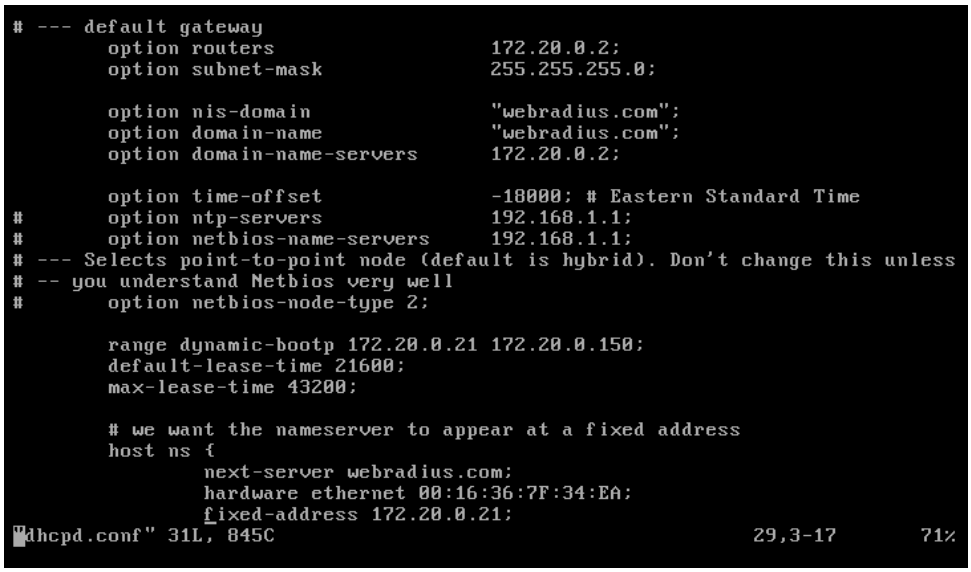


Figura 4-3 Configuración de dhcpd.conf

Crear el archivo dhcpd.leases

#touch /var/lib/dhcp/dhcpd.leases

El archivo **dhcpd.leases** almacena la base de datos de arrendamiento del cliente DHCP. La información sobre de DHCP de cada dirección IP asignada recientemente se almacena de modo automático en la base de datos de arrendamiento. La información incluye la longitud de arrendamiento, a quién se ha asignado la dirección IP, las fechas iniciales y finales de la renta, y la dirección MAC de la tarjeta de interfaz de red utilizada para recuperar el arrendamiento.

3.1.6 Configuración del cliente

Para que el cliente pueda autenticarse en el servidor webRADIUS necesita de una dirección IP la misma que va ha obtener a través del servidor DHCP en forma automática, para configurar la conexión de red seguimos los siguientes pasos:

Click derecho en Mis Sitios de red opción propiedades. En esta ventana seleccionamos obtener una dirección IP automáticamente como se ve en la pantalla siguiente:

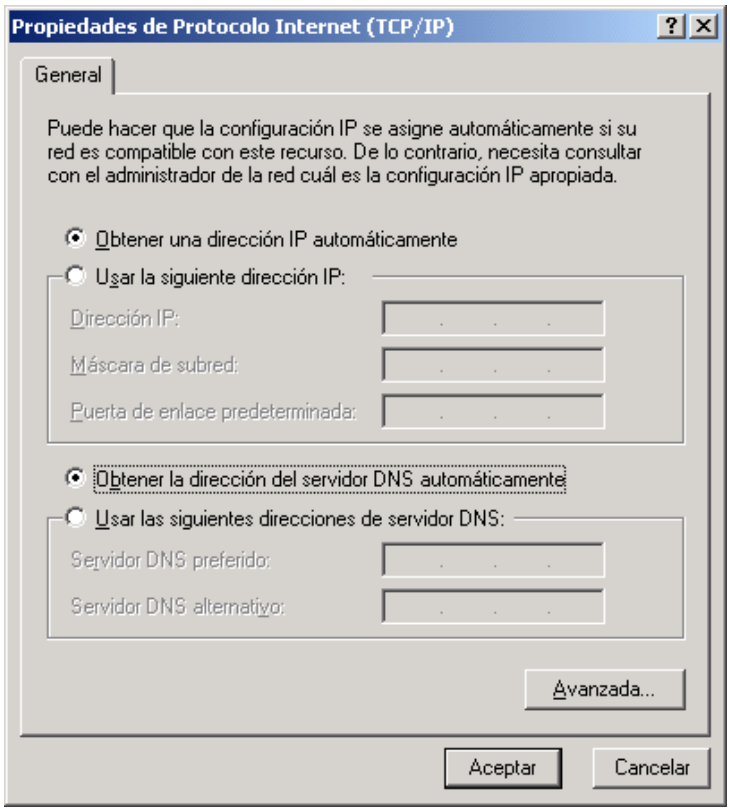


Figura 4-3. Configuración de red en el cliente inalámbrico

Para la autenticación y autorización a través del sistema webRADIUS, utilizaremos el navegador Internet Explorer o cualquier navegadores existente en el mercado, para lo cual debe tener configurado la página de inicio como se muestra en la figura siguiente:

Figura 4-4 Configuración de la página de inicio del navegador

Al iniciar Internet Explorer obtendremos la pantalla de autenticación en donde debemos ingresar el usuario y la clave que debe estar registrado en la base de datos MYSQL del sistema webRADIUS, como se muestra en la figura siguiente:

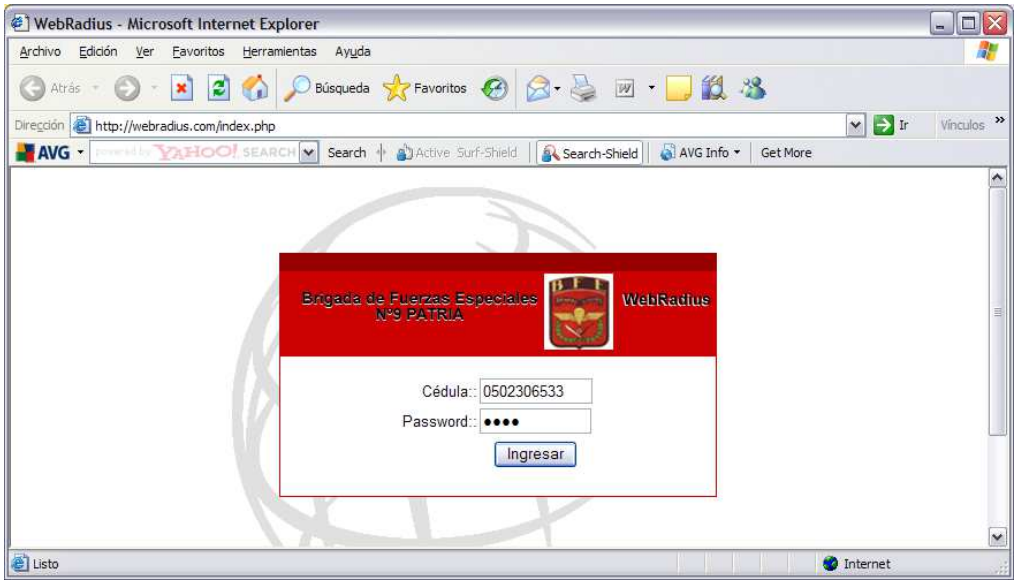


Figura 4-5 Página de autenticación de usuarios

3.1.7 Configuración del Access Point

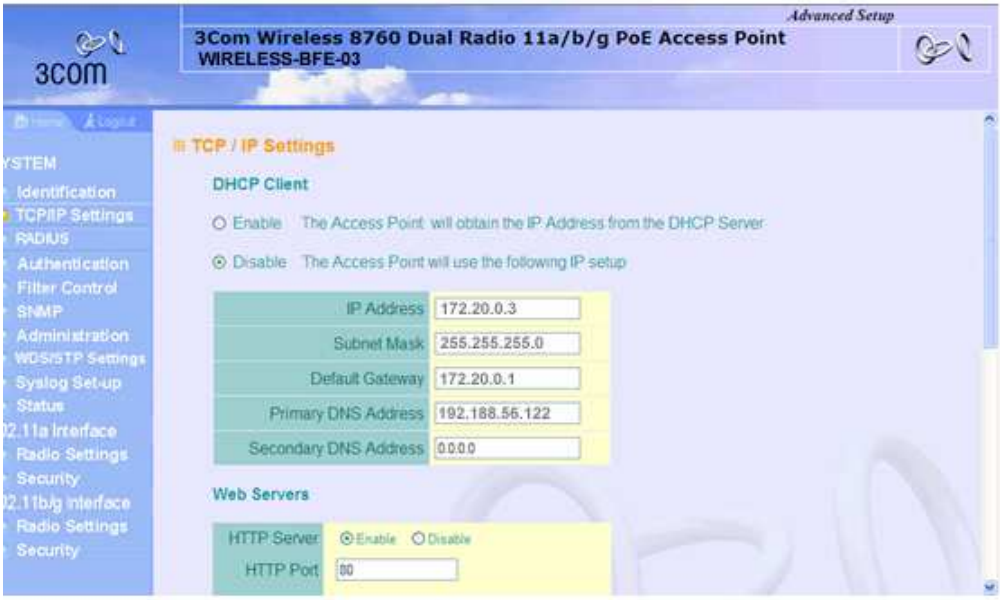


Figura 4-6 Configuración del Punto de Acceso.

3.2 INTERFACES DE ADMINISTRACIÓN Y MONITOREO DEL SISTEMA WEBRADIUS

El sistema webRADIUS para la administración opera bajo tres perfiles de usuarios como son:

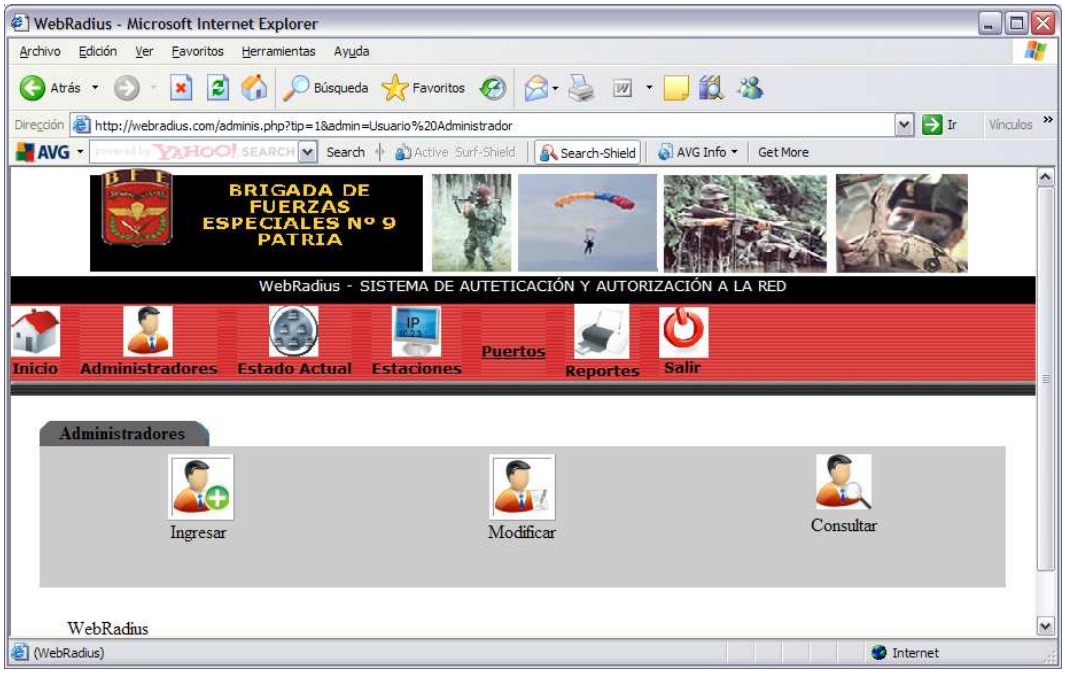
- Usuario Super Administrador
- Usuario Administrador
- Usuario de Monitoreo

1) **Usuario Super Administrador:** Este tipo de usuario tiene privilegios para agregar, modificar y consultar:

- Administradores
- Estaciones
- Puertos
- Autorizar estaciones
- Monitorear el Estado Actual de las estaciones
- Reportes varios

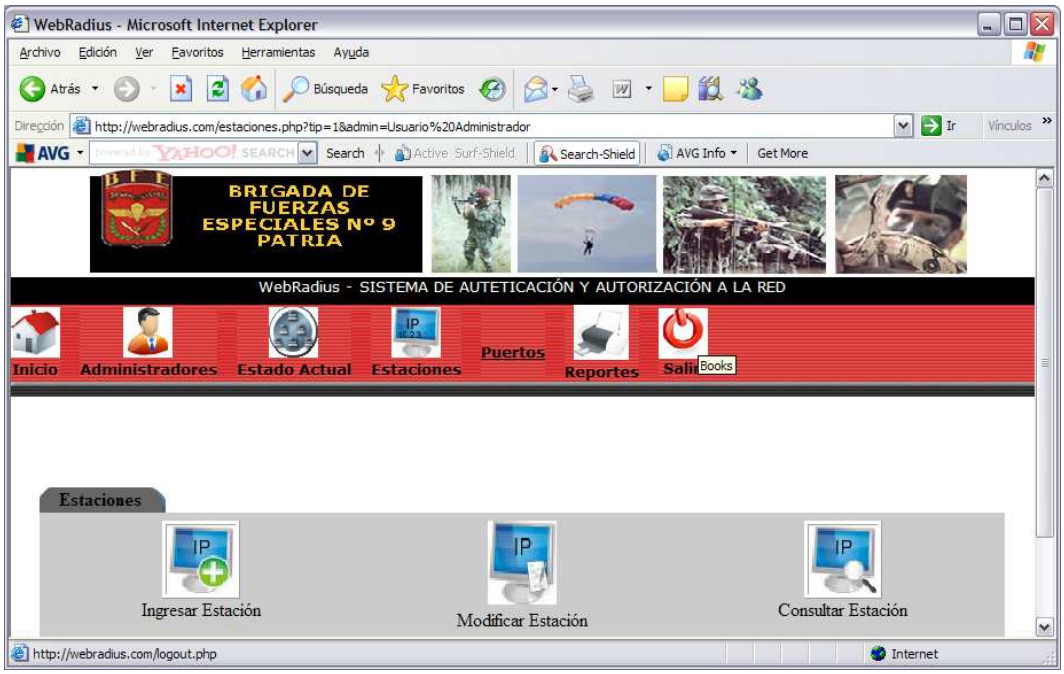
A continuación se muestra cada una de las interfaces del perfil del usuario Super Administrador

3.2.1 Interfaz para gestión de administradores

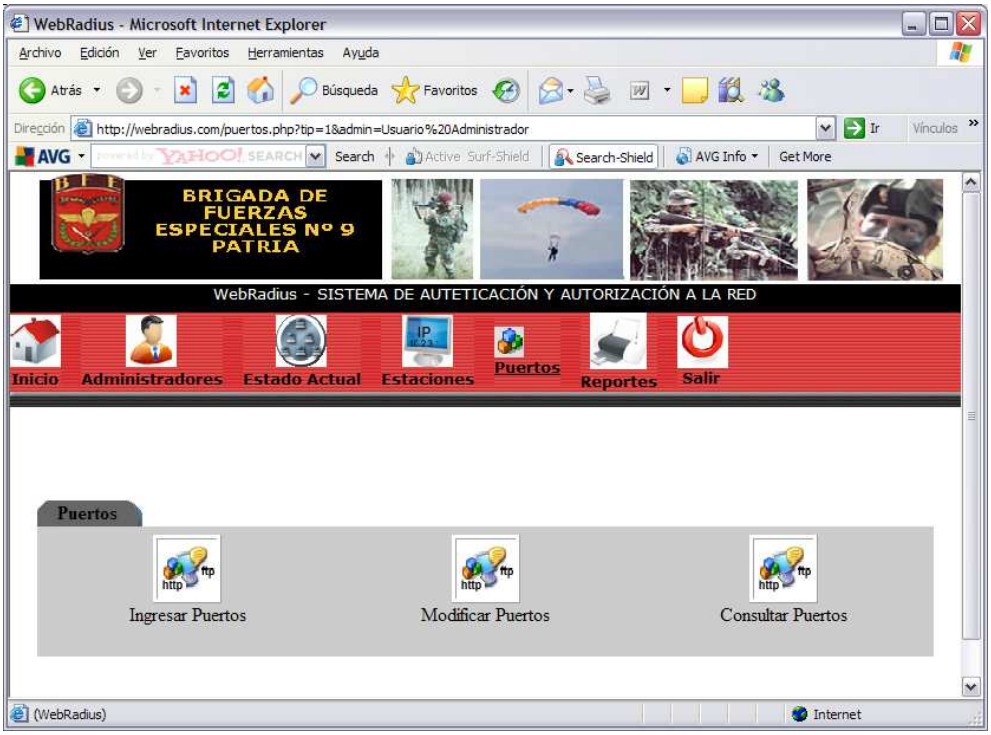


3.2.2 Interfaz para monitorear el estado actual de las Estaciones

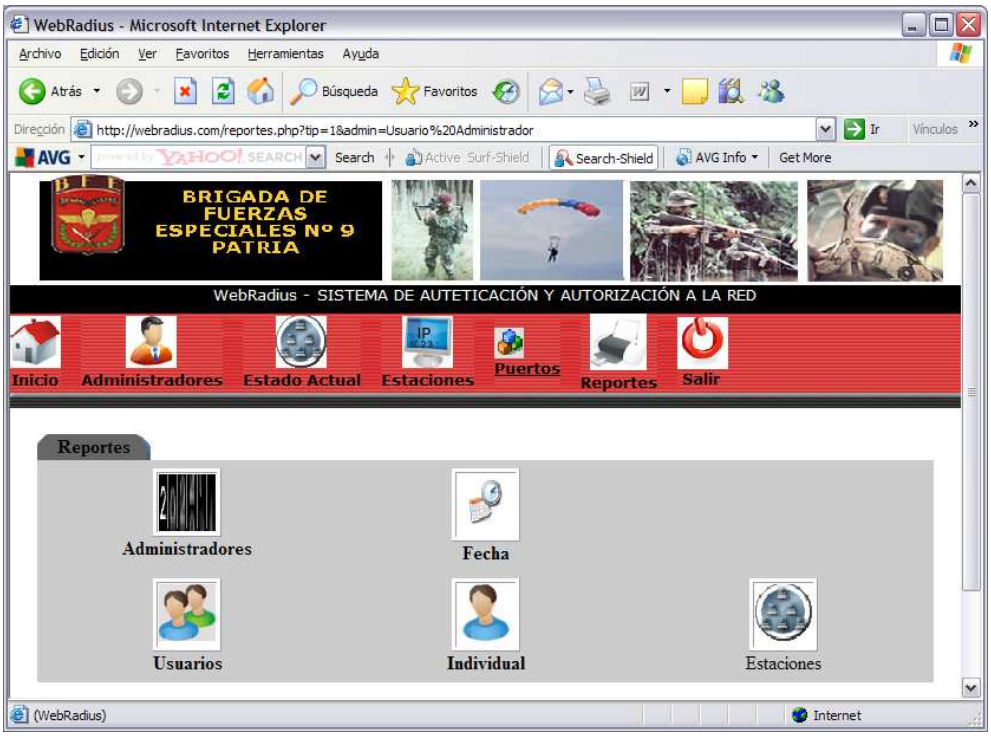
3.2.3 Interfaz para gestión de Estaciones



3.2.4 Interfaz para gestión de Puertos



3.2.5 Interfaz de reportes

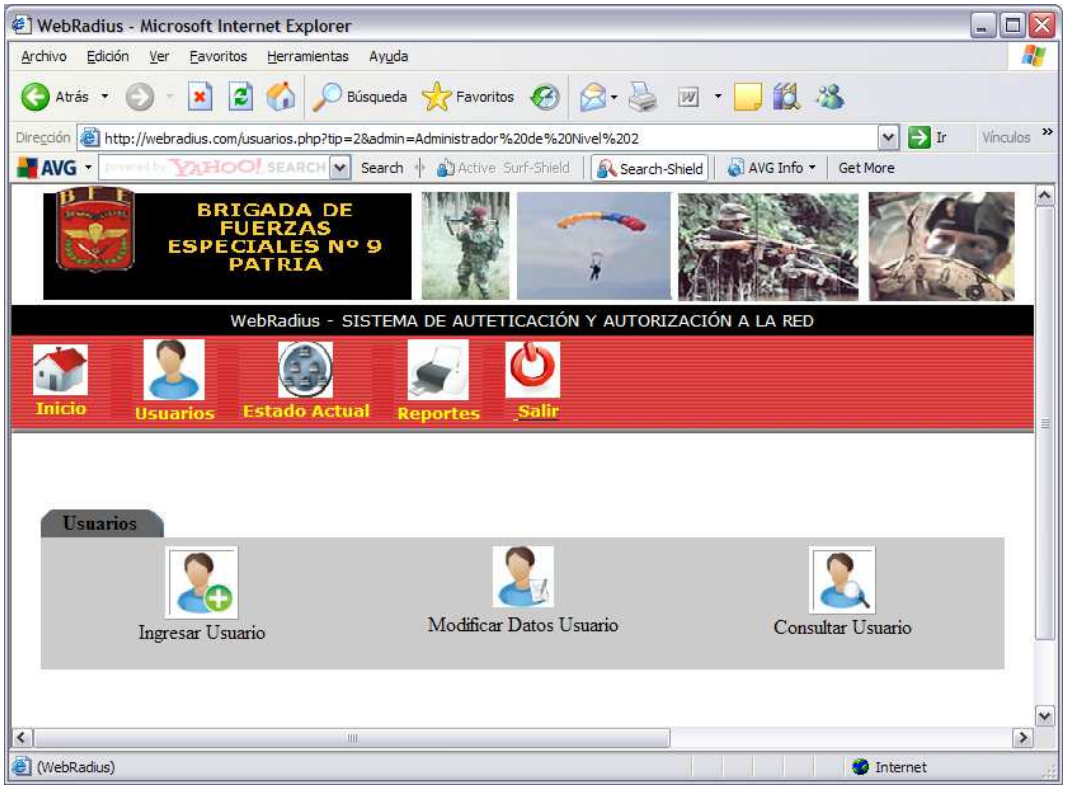


2) **Usuario Administrador:** Este tipo de usuario tiene privilegios para agregar, modificar y consultar:

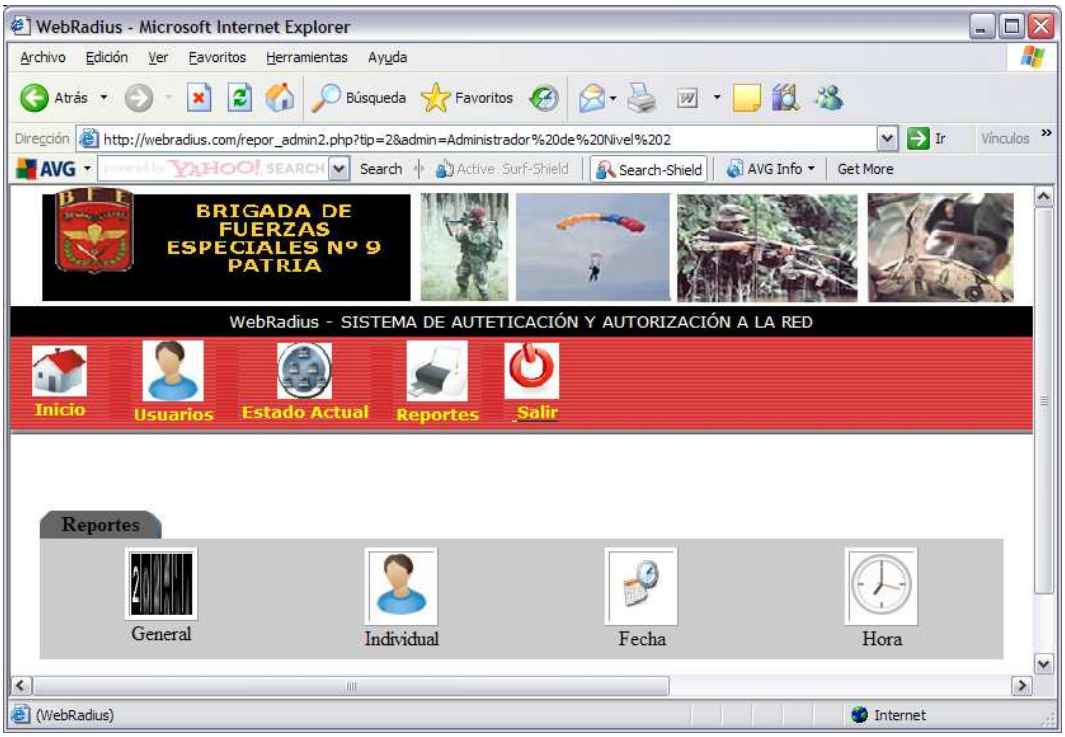
- Usuarios
- Monitorear el Estado Actual de las estaciones
- Reportes varios

A continuación se muestra cada una de las interfaces del perfil del usuario Administrador

3.2.6 Interfaz para gestión de usuarios



3.2.7 Interfaz de reportes



3) **Usuario de Monitoreo:** Este tipo de usuario tiene privilegios restringidos, únicamente puede monitorear el estado actual de las estaciones

Como se pudo apreciar la implementación de la propuesta de esta tesis requiere que se tenga un conocimiento previo de los recursos necesarios para armar un sistema de seguridad inalámbrico. Cada una de las partes usadas como el servidor, el punto de acceso y el cliente deben soportar un mismo protocolo o método de autenticación para que puedan trabajar entre si al validar o restringir el acceso a la red. Un entorno inalámbrico de seguridad como el presentado no funciona con tan solo instalar cada componente, es necesario una configuración y/o programación de cada elemento sobre todo del servidor.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- La seguridad en redes inalámbricas es muy importante para evitar robos de información y ataques a la red.
- La autenticación asegura que los usuarios que acceden a la red están autorizados siendo de esta manera un importante mecanismo para asegurar las redes inalámbricas.
- Los protocolos seguros permiten encriptar los mensajes que se envían por la red entre un servidor y un cliente, garantizando de esta manera la seguridad en la transmisión de la información a través de la web.
- A partir del desarrollo del sistema de autenticación y autorización webRADIUS, para la seguridad de la red inalámbrica, se logró cubrir las falencias de seguridad que se encontraban actualmente en la red inalámbrica de la Brigada de Fuerzas Especiales Nº 9 PATRIA.
- El sistema webRADIUS ofrece un control, monitoreo y administración a través de interfaces gráficas lo que permite a los administradores contar con información confiable de quienes están accesando a la red.

Recomendaciones

- La Brigada de Fuerzas Especiales No. 9 “PATRIA” debe actualizar el equipo informático (servidor, access point, clientes) y sistema operativo, para asegurar el buen funcionamiento del sistema.
- Durante el proceso investigativo se pudo determinar la falta de conocimiento sobre seguridades de parte de los administradores de la red de la Brigada de Fuerzas Especiales No. 9 “PATRIA”, por lo que se recomienda se les capacite constantemente para estar acorde con el avance tecnológico.
- Designar una persona capacitada en el área de sistemas para que administre el sistema de autenticación y autorización webRADIUS.
- Se monitoree periódicamente el acceso de usuarios a la red.

- Respaldar periódicamente la base de datos con el fin de mantener un backup en caso de desastres.
- Implementar otros servicios de red como Active Directory para complementar la seguridad, y de esta manera no permitir que los usuarios puedan cambiar configuraciones establecidas por los administradores.
- Establecer políticas de seguridad, tanto para usuarios como para los equipos.
- La Universidad Técnica de Cotopaxi debe continuar fomentando el desarrollo académico de sus estudiantes incentivando el desarrollo de este tipo de proyectos que dará mayor realce a su imagen institucional.

BIBLIOGRAFÍA

CITADA

1 Autenticación en redes inalámbricas [online. Consultado 26-06-2007. Disponible en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/908d13e8-c4aa-4d62-8401-86d7da0eab48.mspx?mfr=trae]

2 Radius [[online.Consultado 04-07-2007. Disponible en http://www.casadomo.com/proyectoradius.aspx]

3 Encriptación [[online.Consultado 04-07-2007. Disponible en http://es.wikipedia.org/wiki/Encriptación]

4 Estándares [online.Consultado 04-07-2007. Disponible en http://www.ciat.cgiar.org/agroempresas/comercio_justo/glosario.htm]

5 Inalámbrica [online.Consultado 04-07-2007. Disponible en http://es.wikipedia.org/wiki/Inalámbrica].

6 Mecanismos de Seguridad [online.Consultado 21-06-2007. Disponible en http://www.redestelecom.com/Actualidad/Análisis/Comunicaciones/Internet/20061110024/2]

7 MILLER, Stewart S. Seguridad en WiFi. Madrid: McGraw-Hill,2004 268p.

8 RANDALL K, Nichols y PANOS C, Lekkas. Seguridad para comunicaciones inalámbricas. Madrid: McGraw-Hill,2003. 563p.

9 Redes [online.Consultado 04-07-2007. Disponible en http://es.wikipedia.org/wiki/Redes]

10 VLADIMIROV, Andrew A. ; GAVRILENKO, Konstantin y MIKHAILOVSKY, Andrei A. Hacking Wíreles: seguridad de redes inalámbricas. Madrid: Anaya Multimedia, 2005. 238p.

CONSULTADA

11 BATES, Regis J. Comunicaciones inalámbricas de banda ancha. Madrid: McGraw-Hill, 2003. 345p.

12 Como proteger su red inalámbrica [online. Consultado 04 –07-2007. disponible en http://alertaenlinea.gov/docs/alertaenlinea_ inalambrico.pdf]

13 MERCADO, H. Salvador. ¿Cómo hacer una tésis?: tesinas, informes, memorias, seminarios de investigación y monografías. México, D. F.:Limusa, 1998. 294p

14 NORMA TÉCNICA ECUATORIANA NTE INEN 2 396. Documentación. Referencias bibliográficas para libros, folletos e informes. Quito,2005.

15 REINO. Alfredo. Diseño de arquitectura segura para redes inalámbricas [online.Consultado 04 –07-2007. Disponible en http://www.areino.com/alf/docs/ArquitecturaSeguraWireless.pdf]

16 Seguridades en redes WI-Fi inalámbricas [online. Consultado 04 –07-2007. disponible en http://www.pdaexpertos.com/Tutoriales/ Comunicaciones/Seguridad_en_redes_inalambricas_WiFi.shtml]

17 TAFUR PORTILLA, Raúl. La Tesis Universitaria. Lima: Mantaro,1995. 429p.

18 TANENBAUM, Andrew. S. Redes de Computadoras. Tercera Edición. México, D. F. : Prentice Hall, 1997. 813p.

ANEXOS

A1: Entrevista

ENTREVISTA DIRIGIDA AL PERSONAL TECNICO QUE ADMINISTRA LA RED INALAMBRICA EN EL CENTRO DE COMPUTO DE LA BRIGADA DE FUERZAS ESPECIALES No. 9 “PATRIA”

OBJETIVO:

- Determinar la factibilidad de la Implementación de un Sistema de Autenticación para controlar la Seguridad de la Red Inalámbrica en la Brigada de Fuerzas Especiales No. 9 “PATRIA”.

INSTRUCCIONES:

- De la veracidad de sus respuestas, se definirá el real panorama de la inseguridad que al momento padece la red inalámbrica de la Brigada.

1.- Como define usted, a una WLAN?

2.- Por qué, cambiaron la tradicional red de datos por la WLAN?

3.- Qué servicios ofrece al momento la WLAN?

4.- Qué inconvenientes presenta la utilización de la WLAN?

5.- Cree usted que la seguridad en la WLAN, es un problema prioritario a resolver?

6.- Según usted, cuales podrían ser las medidas a tomar para dar seguridad a la WLAN?

7.- Siendo la Autenticación un método para identificar a los usuarios mediante la petición y comparación de datos almacenados previamente en una base de datos.

Cree usted, que sería necesario implementar un sistema de autenticación para controlar el acceso a la red y así proteger la privacidad de los datos?

8.- Los directivos de la Brigada conocen de la problemática en cuanto a la seguridad de la red inalámbrica?

9.- Cuales han sido las acciones tomadas por los directivos de la Brigada, para solucionar el inconveniente de la seguridad en la red inalámbrica?

10.- Se han realizado gestiones ante los directivos de la institución para la capacitación del personal involucrado en la administración de la WLAN?

11.- Existe el presupuesto necesario para la implementación de medidas de seguridad en la WLAN?

A:2 Encuesta

ENCUESTA DIRIGIDA AL PERSONAL DE USUARIOS QUE INGRESAN A LA RED INALAMBRICA DE LA BRIGADA DE FUERZAS ESPECIALES No. 9 “PATRIA”

OBJETIVO:

- Determinar la factibilidad de la Implementación de un Sistema de Autenticación para controlar la Seguridad de la Red Inalámbrica en la Brigada de Fuerzas Especiales No. 9 “PATRIA”.

INSTRUCCIONES:

- Lea detenidamente cada una de las preguntas planteadas así como las alternativas, para que de acuerdo a sus conocimientos nos dé un aporte para el desarrollo del presente proyecto.
- La encuesta es individual y anónima cuyos resultados contribuirán y permitirán el desarrollo del Centro de Computo de la Brigada de Fuerzas Especiales No. 9 “PATRIA”
- Marque con una (x) dentro del paréntesis, en la respuesta que usted estime conveniente.

1.- Conoce usted como funcionan las Redes Inalámbricas?

Si ( ) No ( )

2.- El equipo con el que se conecta a la red es:?

PC (de escritorio) ( ) PORTÁTIL ( )

3.- Resulta fácil para usted, conectarse a la red inalámbrica?

Si ( ) No ( )

4.- Usted se conecta al internet, en cualquier momento?

Si ( ) No ( )

5.- Cuando utiliza el internet desde su equipo, este es:

Rápido ( ) Lento ( )

6.- Le parece bien que implementen medidas de seguridad para proteger los datos de la Brigada y los suyos?

Si ( ) No ( )