UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

Carrera de Ingeniería de Sistemas

"Diseño e Implementación de una Red Inalámbrica WLAN basada en el estándar Wi-Fi, utilizando el protocolo de autenticación RADIUS, para el campus universitario del Área de la Energía, las Industrias y los Recursos Naturales No Renovables"

Tesis previa a la obtención del título de Ingeniero de Sistemas

AUTORES:

Mónica María Díaz Samaniego
Pablo Oswaldo Córdova García

DIRECTOR:

Ing. Wilson Augusto Vélez Ludeña

Loja –Ecuador
2010

CERTIFICACIÓN

Ing.
Wilson Augusto Vélez Ludeña
DOCENTE DEL ÁREA DE LA ENERGÍA LA INDUSTRIA Y LOS RECURSOS NATURALES NO RENOVABLES DE LA UNIVERSIDAD NACIONAL DE LOJA

CERTIFICA:

Haber asesorado y revisado durante todo su desarrollo, la tesis titulada: **Diseño e Implementación de una Red Inalámbrica WLAN basada en el estándar Wi-Fi, utilizando el protocolo de autenticación RADIUS, para el campus universitario del Área de la Energía, las Industrias y los Recursos Naturales No Renovables**, realizada por los postulantes Mónica María Díaz Samaniego y Pablo Oswaldo Córdova García. Por lo tanto autorizo proseguir los trámites legales pertinentes para su presentación y defensa.

Loja, 20 julio 2010

Ing. Wilson Augusto Vélez Ludeña
DIRECTOR DE TESIS

AUTORÍA

Los conceptos, opiniones, conclusiones, recomendaciones y más contenidos en el presente trabajo de investigación son responsabilidad de sus autores.

Mónica María Díaz Samaniego Pablo Oswaldo Córdova García

AGRADECIMIENTO

Una vez concluido el presente trabajo investigativo, agradecemos a Dios por permitirnos culminar esta etapa de nuestra vida.

A las autoridades de la universidad y especialmente al Área de la Energía, las Industrias y los Recursos Naturales no Renovables, Carrera Ingeniería de Sistemas.

A nuestro Director de Tesis, Ing. Wilson Vélez, por su valioso aporte de conocimiento y sugerencias para el desarrollo de nuestra investigación.

Los Autores

DEDICATORIA

Dedico este logro con mucho amor y gratitud a mis padres Fredy y María, por su amor, apoyo incondicional y esfuerzo por darme lo mejor de ellos, a mis hijos María Cristina y Pablo Isaac por ser la inspiración y el incentivo para tratar de ser mejor ser humano cada día, a mis hermanos Silvia y Juan Pablo por ser siempre mis amigos incondicionales, mi apoyo y aliento en cada situación de mi vida, y a mi querido esposo Pablo Oswaldo, por su amor, apoyo, y por ser el mejor compañero para mí en este trayecto que hemos recorrido juntos.

Mónica

En el momento que logramos una meta fijada, nos detenemos a pensar quienes fueron las personas que nos ayudaron a lograrla, por eso quiero dedicar el presente trabajo a mis queridos papito Segundo, y mamita Lela por su eterno amor, a mis padres Tito y Fanny por su paciencia, comprensión y absoluto apoyo, a mi amada esposa Mónica, amiga incondicional de toda mi vida por su comprensión amor y empuje, a mis amados hijos María Cristina y Pablo Isaac la fuente de inspiración para ser mejor y correcta persona cada día.

Pablo

ESQUEMA DE TESIS

1. RESUMEN
2. INTRODUCCIÓN
3. REVISIÓN DE LITERATURA
4. PROPUESTA ALTERNATIVA
   4.1. IMPLANTACIÓN
   4.2. PRUEBA DE VALIDACIÓN
5. METODOLOGÍA
6. EVALUACIÓN DEL OBJETO DE INVESTIGACIÓN
7. CONCLUSIONES
8. RECOMENDACIONES
9. BIBLIOGRAFÍA
10. ANEXOS

SUMMARY

This research named "Design and Set up of a wireless WLAN that meets performance Standard Wi-Fi and uses RADIUS authenticate protocol at the Area de la Energia, las Industrias y los Recursos Naturales No Renovables campus" has a deep impact in the wireless technology and it had been growing very fast. This kind of technology has a better connection and also improve the mobility and flexibility on communications devices (cell, computers). It made a big impact and an incredible advance in every single part of life.

Our goal is develop the complete analysis, design and set up of a local wireless. This wireless will let users from The Universidad Nacional de Loja to access to the campus in the buildings of the Área de la Energía, las Industrias y los Recursos Naturales no Renovables. We will create a control access to the wireless to avoid the misuse of these resources because they are very important for the knowledge and development of the students.

We had determined three very important phases: Analysis, Design, and Set-up of the wireless. In the Analysis phase we used research's tools such as interview, survey and site observation. Those tools let us to decided which would be the optimum performance and spectrum of the wireless. In the Design phase we chose the hardware y software to be used. In the last phase we set up the wireless following the IEEE standard, WIFI standard and using RADIUS (Remote Authentication Dial-In User Server).

This research let us to determined that is essential to have a wireless with a control access to let the students to use the Internet service.

1. RESUMEN

El presente trabajo investigativo titulado "Diseño e Implementación de una Red Inalámbrica WLAN basada en el estándar Wi-Fi, utilizando el protocolo de autenticación RADIUS, para el campus universitario del Área de la Energía, las Industrias y los Recursos Naturales No Renovables", tiene fundamental importancia puesto que la tecnología de redes inalámbrica se ha desarrollado en forma acelerada, este tipo de redes mejoran la conectividad facilitando la movilidad y flexibilidad de los equipos de comunicación (celulares, computadoras), determinando grandes beneficios en todos los ámbitos de la actividad humana.

El objetivo general a cumplir es desarrollar un análisis y diseño para la implementación de una red inalámbrica local que permita el acceso al servicio de internet de la Universidad Nacional de Loja, en el campus de los bloques de el Área de la Energía, las Industrias y los Recursos Naturales no Renovables y como parte de la seguridad para esta red proporcionar un control de accesos a la misma evitando que este recurso indispensable para el desarrollo del conocimiento de los estudiantes sea desviado del uso académico o interceptado por otro usuarios.

Para el desarrollo de la investigación hemos definido tres etapas importantes como son: análisis, diseño e implementación. En la etapa de análisis utilizamos instrumentos de investigación como entrevistas, encuestas y observaciones al sitio, que nos permitieron determinar la funcionalidad de la red inalámbrica para el área y delimitar su alcance. En la etapa de diseño detallamos el hardware y software a utilizar para seguir con la siguiente etapa que es implantar la red inalámbrica con las características y seguridades necesarias, cumpliendo con los estándares establecidos para este tipo de red por la IEEE para redes inalámbricas WIFI y utilizando el protocolo para el control de accesos RADIUS (Remote Authentication Dial-In User Server).

Esta investigación nos ha permitido concluir que es necesaria la implementación de una red inalámbrica con acceso controlado que permitirá el ingreso a los estudiantes del área para el uso del servicio de internet.

2. INTRODUCCIÓN

Las redes inalámbricas en la actualidad, desempeñan un papel fundamental en el desarrollo y productividad de cualquier entidad que haga uso de ellas ya sea en el campo empresarial o educativo.

Las tecnologías inalámbricas están experimentando una evolución acelerada, con la finalidad de facilitar la movilidad y conectividad tanto a servicios y aplicaciones desde cualquier lugar que este dentro del alcance de la misma.

Es de gran importancia que nos integremos al avance que está experimentando la tecnología de la comunicación en cuanto a las redes inalámbricas, pues nos permitirá aprovechar de beneficios tales como la movilidad, característica que permite el acceso a los usuarios en tiempo real dentro del área de cobertura; la simplicidad y rapidez de instalación eliminándose la necesidad de extender cables, además una WLAN permite llegar a puntos de difícil acceso para una red LAN cableada, los beneficios a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes. Por otro lado los sistemas de WLAN pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red.

La evolución de las redes inalámbricas se ha visto directamente relacionada con la velocidad, el alcance que pueden conseguir y su costo, cada vez prestan mayores beneficios, en la actualidad tenemos la tecnología 802.11g, disponible en la mayoría de equipos para redes inalámbricas que nos permite una velocidad máxima de 54mbps con un ancho de banda de 2.4Ghz y su costo es accesible para cualquier ambiente a donde desee aplicarse desde el más sencillo hasta el corporativo.

El campus del Área de la Energía, las Industrias, y los Recursos Naturales no Renovables de la Universidad Nacional de Loja, no cuenta con una red inalámbrica que permita principalmente a los estudiantes conectarse al servicio de internet que brinda la

universidad como una herramienta para el proceso de enseñanza aprendizaje. Por esta razón nuestro proyecto se encaminó a efectuar el análisis, diseño e implantación de una red inalámbrica y como parte de esta red un control de accesos que permita la conexión solo a usuarios autorizados.

Para la implantación de la WLAN, se llevó a cabo una etapa de análisis mediante la cual pudimos determinar la funcionalidad de la red y el tipo de seguridad que requerirá en base a ésta funcionalidad. Además pudimos conocer la infraestructura del lugar y tener una idea de cómo se va a distribuir los puntos de acceso y el servidor necesarios para la implementación de la red inalámbrica.

Una vez que hemos analizado el área donde se implantará la red, elaboramos el diseño tanto físico como lógico de la misma, el diseño físico nos permite definir el lugar donde se ubicarán los puntos de acceso y el servidor para la red, en cuanto al diseño lógico se determinó la topología a utilizar y la configuración del software para su funcionamiento y seguridad. Luego de establecer este diseño iniciamos la implantación y prueba del funcionamiento de la WLAN.

Debemos señalar que es de gran importancia el desarrollo de este proyecto debido al aporte que la implantación de esta red significa para el AEIRNNR, pues permite estar al día en cuanto a los avances tecnológicos en lo que respecta a las redes, además permitirá que los estudiantes se agreguen a la red y puedan contar con movilidad y flexibilidad que brinda este tipo de red para hacer uso del servicio de internet. Como futuros profesionales se ha adquirido una valiosa experiencia en este campo que promete ser una fuente de trabajo que posiblemente nos brindará grandes réditos técnicos y económicos, por la importancia que cada día van adquiriendo este tipo de redes en las diferentes áreas como son las pequeñas y grandes empresas, instituciones educativas, instituciones financieras. Así mismo consideramos que la presente investigación constituirá una pauta valedera para nuevas investigaciones de los estudiantes de la carrera.

3. REVISIÓN LITERARIA

3.1. FUNDAMENTACIÓN TEÓRICA

3.1.1. REDES INALÁMBRICAS.

Este tipo de redes constituye una de las tecnologías más poderosas que ha conseguido el ingenio de las telecomunicaciones, y es que el poder comunicar computadoras mediante tecnología inalámbrica hubiera parecido un sueño hace algunos años atrás, pero es una realidad que está a nuestro alcance y nos presta enormes servicios.

Este tipo de redes se basa en la utilización de un enlace que utiliza ondas electromagnéticas ya sea de radio e infrarrojo, en lugar de cableado. Las tecnologías de las redes inalámbricas se diferencian por la frecuencia de transmisión que utilizan, el alcance y velocidad de sus transmisiones. La instalación de este tipo de redes no requiere de cambios significativos en la infraestructura existente del lugar donde se desea implementar lo que ocurre con las redes cableadas.

Podemos mezclar las redes cableadas y las inalámbricas, y de esta manera generar una "Red Híbrida", para poder utilizarlas en caso de ser necesario. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el usuario se pueda desplazar con facilidad dentro de un lugar.

3.1.1.1. CLASIFICACIÓN DE LAS REDES INALÁMBRICAS

Las redes inalámbricas se las puede clasificar dependiendo del alcance o cobertura, de la siguiente manera:

- Redes Inalámbricas de Área Extendida, WWAN (Wireless Wide Area Network)
- Redes Inalámbricas de Area Metropolitana, WMAN (Wireless Metropolitan Area Network)
- Redes Inalámbricas de Area Local, WLAN (Wireless Local Area Network)

- Redes Inalámbricas de Area Personal, WPAN (Wireless Personal Area Network)

Mediante el siguiente gráfico podemos tener claro la cobertura de las redes inalámbricas[1]:

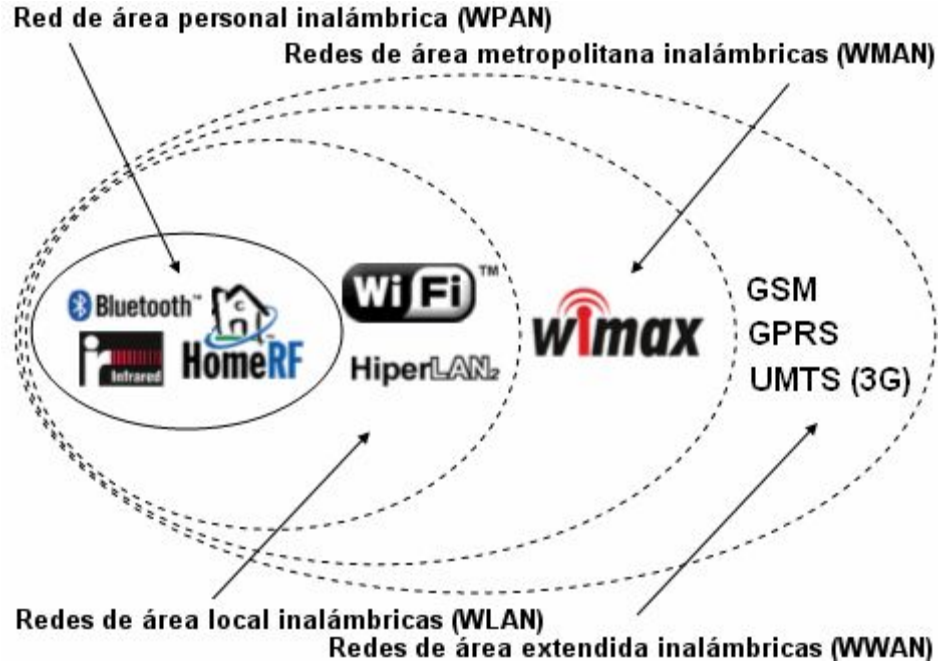


Fig.1. Cobertura de las Redes Inalámbricas

REDES DE ÁREA LOCAL INALÁMBRICAS (WLAN)

Este es un tipo de redes que permite la comunicación inalámbrica entre los equipos sean estos computadores portátiles, agendas electrónicas, etc. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo gran importancia y popularidad en muchos campos, la cual va creciendo conforme se ve en aumento sus prestaciones y aparecen nuevas aplicaciones para las mismas. Son muy utilizadas para compartir el acceso a Internet entre varias computadoras.

El usuario dentro de una red WLAN tiene la posibilidad de transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas. Su aplicación no se limita a las empresas, sino a ambientes

[1] Redes Inalámbricas. [http://es.kioskea.net/contents/wireless/wlintro.php3]

públicos, en áreas metropolitanas, como medio de acceso a Internet o para cubrir zonas de alta densidad de usuarios (hot spots) en las redes de tercera generación (3G). Gran parte de los fabricantes de ordenadores y equipos de comunicaciones como son los PDAs (Personal Digital Assistants), módems, terminales de punto de venta y otros dispositivos están introduciendo aplicaciones soportadas en las comunicaciones inalámbricas. Las nuevas posibilidades que ofrecen las WLANs son: permitir una fácil incorporación de nuevos usuarios a la red, ofrecer una alternativa de bajo costo a los sistemas cableados, además de la posibilidad para acceder a cualquier base de datos o cualquier aplicación localizada dentro de la red.

Cuando nos referimos a redes inalámbricas debemos conocer acerca del grupo de trabajo para este tipo de redes el IEEE 802.11

3.1.1.2. IEEE 802.11 (WIFI)

El IEEE 802.11, constituye un estándar internacional que define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

La importancia de esta tecnología radica en que su uso abre una definición completamente nueva acerca de la infraestructura de una red la misma que no tiene porque ser rígida y fija, difícil de mover y costosa para modificar, en lugar de ello puede moverse con el usuario y cambiar tan rápido como cambie la organización.

Wi-Fi ("Fidelidad inalámbrica") es el nombre de la certificación otorgada por la Wi-Fi Alliance, anteriormente WECA (Wireless Ethernet Compatibility Alliance), que es un grupo que garantiza la compatibilidad entre dispositivos que utilizan el estándar 802.11. Por lo general el nombre del estándar se confunde con el nombre de la certificación. Una red Wi-Fi es en realidad una red que cumple con el estándar 802.11. A los dispositivos certificados por la Wi-Fi Alliance se les permite usar este logotipo:

Con Wi-Fi se pueden crear redes de área local inalámbricas de alta velocidad siempre y cuando el equipo que se vaya a conectar no esté muy alejado del punto de acceso. En la práctica, se pueden integrar ordenadores portátiles, equipos de escritorio, asistentes digitales personales (PDA) o cualquier otro tipo de dispositivo de alta velocidad con propiedades de conexión también de alta velocidad (11 Mbps o superior) dentro de un radio de varias docenas de metros en ambientes cerrados (de 20 a 50 metros en general) o dentro de un radio de cientos de metros al aire libre.

Las especificaciones del IEEE 802.11 en cuanto a estas redes se centra en las dos capas inferiores del modelo OSI, que son la capa física y la de enlace de datos. La capa física indica como son enviados los bits de una estación a otra. La capa de Enlace de Datos, se encarga de describir como se empacan y verifican los bits de modo que no tengan errores. Los dos métodos para remplazar la capa física en una red inalámbrica son la transmisión de Radio Frecuencia y la Luz Infrarroja.

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos mientras que la capa de enlace de datos define la interfaz entre el bus del equipo y la capa física, en particular un método de acceso parecido al utilizado en el estándar Ethernet, y las reglas para la comunicación entre las estaciones de la red. Estas dos capas las estudiaremos a fondo más adelante.

El estándar 802.11 se constituye en el primer estándar el mismo que permite un ancho de banda de 1 a 2 Mbps. El estándar original se ha modificado para optimizar el ancho de banda (incluidos los estándares 802.11a, 802.11b y 802.11g, denominados estándares físicos 802.11) o para especificar componentes de mejor manera con el fin de garantizar mayor seguridad o compatibilidad. En la tabla siguiente se muestra las distintas modificaciones del estándar 802.11 y sus significados:

NOMBRE DEL ESTÁNDAR	DESCRIPCIÓN
802.11	Primer estándar permite un ancho de banda de 1 a 2 Mbps. 1997

802.11ª	Admite un ancho de banda superior (el rendimiento total máximo es de 54 Mbps aunque en la práctica es de 30 Mpbs). Provee ocho canales de radio en la banda de frecuencia de 5 GHz.
802.11b	Ofrece un rendimiento total máximo de 11 Mpbs (6 Mpbs en la práctica) y tiene un alcance de hasta 300 metros en un espacio abierto. Utiliza el rango de frecuencia de 2,4 GHz con tres canales de radio disponibles.
802.11c	No ofrece ningún interés para el público general. Es una versión modificada del estándar 802.1d que permite combinar el 802.1d con dispositivos compatibles 802.11 (en el nivel de enlace de datos).
802.11d	Es un complemento del estándar 802.11 que está pensado para permitir el uso internacional de las redes 802.11 locales. Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo.
802.11e	Está destinado a mejorar la calidad del servicio en el nivel de la *capa de enlace de datos*. El objetivo del estándar es definir los requisitos de diferentes paquetes en cuanto al ancho de banda y al retardo de transmisión para permitir mejores transmisiones de audio y vídeo.
802.11f	El 802.11f es una recomendación para proveedores de puntos de acceso que permite que los productos sean más compatibles. Utiliza el *protocolo IAPP* que le permite a un usuario itinerante cambiarse claramente de un punto de acceso a otro mientras está en movimiento sin importar qué marcas de puntos de acceso se usan en la infraestructura de la red. También se conoce a esta propiedad simplemente como *itinerancia.*
802.11g	Proporciona un ancho de banda elevado (con un rendimiento total máximo de 54 Mbps pero de 30 Mpbs en la práctica) en el rango de frecuencia de 2,4 GHz. El estándar 802.11g es compatible con el estándar anterior, el 802.11b, lo que significa que los dispositivos que admiten el estándar 802.11g también pueden funcionar con el 802.11b.
802.11h	Tiene por objeto unir el estándar 802.11 con el estándar europeo (HiperLAN 2, de ahí la *h* de 802.11h) y cumplir con las regulaciones europeas relacionadas con el uso de las frecuencias y el rendimiento energético.
802.11i	Está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el *AES* (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.
802.11Ir	Se elaboró para que pueda usar señales infrarrojas. Este estándar se ha vuelto tecnológicamente obsoleto.
802.11j	El estándar *802.11j* es para la regulación japonesa lo que el 802.11h es para la regulación europea.

Tabla.1. Modificaciones del estándar 802.11

Rango y flujo de datos

Los estándares 802.11a, 802.11b y 802.11g, llamados "estándares físicos", son modificaciones del estándar 802.11 y operan de modos diferentes, lo que les permite alcanzar distintas velocidades en la transferencia de datos según sus rangos.

Estándar	Frecuencia	Velocidad	Rango
802.11a	5 GHz	54 Mbit/s	10 m
802.11b	2,4 GHz	11 Mbit/s	100 m
802.11g	2,4 GHz	54 Mbit/s	100 m

Tabla.2. Comparación de frecuencia, velocidad y rango de los estándares a,b yg

Los estándares 802.11b y 802.11g, utilizan la banda de 2.4 – 2.5 Ghz. Para esta banda están definidos 11 canales utilizables por los equipos WIFI, estos pueden configurarse de acuerdo a necesidades particulares, y no son completamente independientes (canales contiguos se superponen y se producen interferencias). El ancho de banda de la señal (22MHz) es superior a la separación entre canales consecutivos (5MHz), por eso se hace necesaria una separación de al menos 5 canales con el fin de evitar interferencias entre celdas adyacentes. Por lo general se utilizan los canales 1, 6 y 11, aunque se ha documentado que el uso de los canales 1, 5, 9 y 13 (en dominios europeos) no es perjudicial para el rendimiento de la red.

La asignación de canales generalmente se hace sólo en el Access Point, pues los “clientes” automáticamente detectan el canal, salvo en los casos en que se forma una red “Ad-Hoc” o punto a punto cuando no existe Access Point.

3.1.1.3. TOPOLOGÍAS DE UNA RED INALÁMBRICA

Tenemos dos topologías básicas para este tipo de redes: infraestructura y Ad Hoc.

Infraestructura:

Este tipo de red, nace de una existente para agregar dispositivos inalámbricos a una estación base denominada Punto de Acceso.

El punto de acceso es el encargado de unir la red LAN inalámbrica con la red LAN cableada, este sirve de controlador central de la red inalámbrica. Además este punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión especifica. La extensión y el número de dispositivos dependen del estándar de conexión que se utilice y del producto.

Esta topología es capaz de dotar a la red de muchas más posibilidades, además del evidente aumento en el alcance de la red debido a la utilización de varios puntos de acceso, permite lo que se conoce como roaming, es decir que los terminales se puedan mover sin perder la cobertura y sin sufrir cortes en la comunicación.

Ad Hoc:

También conocidas como redes Peer to Peer, a diferencia de la topología anterior, la red se crea a partir de los propios dispositivos inalámbricos. Su configuración es más sencilla. Cada dispositivo se comunica directamente con los demás dispositivos de la red, esto implica que los datos no pasen por un controlador central.

Este tipo de infraestructura es práctica en lugares donde pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red.

3.1.1.4. COMPONENTES DE UNA RED INALÁMBRICA

Básicamente una red inalámbrica posee los siguientes componentes:

- Adaptadores LAN
- Puntos de acceso
- Puentes LAN

Adaptadores LAN.- Los adaptadores inalámbricos tienen componentes equivalentes a

los de los adaptadores usados en redes cableadas como adaptadores USB y tarjetas de red inalámbricas. También tienen la misma función, permitiendo a los usuarios acceder a la red. Los adaptadores proveen la interface entre el sistema de operación de la red y una antena para crear una conexión transparente.

Punto de Acceso.- El punto de acceso es el equivalente inalámbrico al hub en una LAN. Este recibe y transmite los datos entre la WLAN y la red cableada que soporta un grupo de usuarios con dispositivos inalámbricos. Generalmente, un punto de acceso de conecta con el eje principal de la red, es decir el enlace principal de conexión entre nodos de una red, a través de un cable Ethernet estándar, y se comunica con los dispositivos inalámbricos a través de una antena. El punto de acceso o la antena conectada al mismo. Generalmente se instala en una pared alta o en el techo. Como las células de telefonía celular, múltiples puntos de acceso pueden realizar handoff de un punto de acceso a otro mientras el usuario se mueva de un área a otra. Los puntos de acceso tienen un rango de 20 a 500 metros, y puede soportar de 15 a 250 usuarios dependiendo de la tecnología, configuración y el uso. Es relativamente fácil extender una WLAN agregando más puntos de acceso para reducir la congestión de la red y expandir el área de cobertura. Al tener múltiples puntos de acceso se crean células que se traslapan, creando una conectividad constante en la red.

Puentes LAN para exterior.- Estos conectan LANs en diferentes edificios. El costo de conectar edificios por medio de cable de fibra óptica es alto, una WLAN resulta una alternativa económica. Los puentes utilizados en WLAN soportan tasas de transferencia altas y rangos de varios kilómetros con el uso de antenas direccionales con línea de vista. Ciertos puntos de acceso pueden utilizarse como puentes entre edificios que se encuentran relativamente cerca.

3.1.1.5. CAPA FÍSICA

Mediante la capa física se define la modulación y señalización características de la transmisión de datos.

El IEEE 802.11 define tres posibles opciones para la elección de la capa física:

1. Espectro Expandido por secuencia directa o DSSS (Direct Sequence Spread Spectrum).
2. Espectro Expandido por salto de frecuencia o FHSS (Frecueny Hopping Spread Spectrum)
3. Luz infrarroja en banda base

Se ponen a disposición estas tres opciones debido a la necesidad de proporcionar a los usuarios la posibilidad de elegir en función de la relación entre costes y complejidad de implementación por una parte y prestaciones y fiabilidad por otra.

Existen dos tipos de tecnologías que emplean las radiofrecuencias, la banda estrecha y la banda ancha, también conocida espectro ensanchado, siendo ésta última la que más se utiliza.

La tecnología de espectro ensanchado, utiliza **todo el ancho de banda disponible**, en lugar de utilizar una portadora para concentrar la energía a su alrededor. Esta tecnología sobresale de otras de radiofrecuencias debido a que, por ejemplo, posee excelentes propiedades en cuanto a inmunidad a interferencias y a sus posibilidades de encriptación.

Existen dos tipos de tecnología de espectro ensanchado:

3.1.1.5.1. Espectro Expandido por Secuencia Directa (DSSS)

Esta tecnología para cada bit que compone la señal, genera un patrón de bits redundante (señal de chip). Cuanto mayor sea esta señal, mayor será la resistencia de la señal a las interferencias. El estándar IEEE 802.11 recomienda un tamaño de 11 bits. Para la recepción es necesario realizar el proceso inverso para obtener la información original.

La secuencia de bits utilizada para modular los bits se conoce como secuencia de Barker. Es ida diseñada para que aparezca aproximadamente la misma cantidad de 1 que de 0. Un ejemplo de esta secuencia es el siguiente:

+1 –1 +1 +1 –1 +1 +1 +1 –1 –1 –1

Fig 2. Secuencia de Baker

Cada +1 se convierte en 1 y cada -1 en 0, por lo que la secuencia de Barker seria 10110111000, lo que se aplica por cada bit en el flujo de datos. Cuando se codifica un bit cuyo valor es 1, todos los bits en el código de propagación cambian mientras que para un bit 0 se mantiene igual.

A continuación podemos observar cómo se utiliza la secuencia de Barker para codificar la señal original a transmitir:

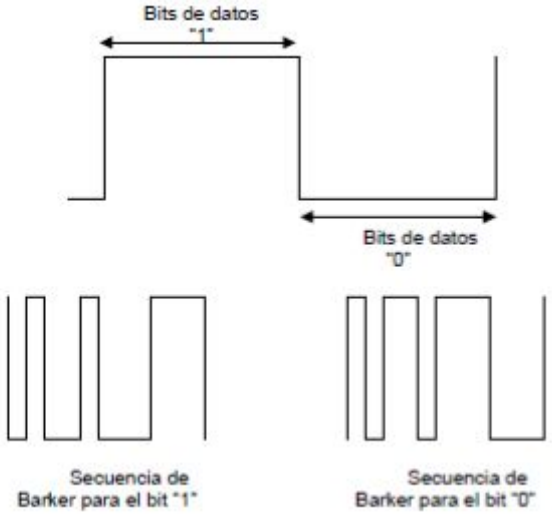


Fig.3. Codificación de Barker

Para la técnica de espectro ensanchado por secuencia directa, el estándar IEEE 802.11 ha definido dos tipos de modulación, DBPSK, Differential Binary Phase Shift Keying y DQPSK Differential Cuadrature Phase Shift Keying que proporcionan en la velocidad de transferencia de 1 y 2 Mbps respectivamente. Recientemente la IEEE ha revisado este estándar, que es el 802.11b en el cual hay mejoras de seguridad y aumenta esta velocidad hasta los 11Mbps, incrementando el rendimiento de redes de este tipo.

DSSS posee 14 canales en la banda de los 2Ghz y cada canal tiene un ancho de banda de 5Mhz. Siendo el canal 1 colocado a 2,412, el canal 2 a 2,417, y asi hasta el canal 13 a 2.472Ghz.

3.1.1.5.2. Espectro ensanchado por salto de frecuencia (FHSS)

Esta tecnología consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada dwell time e inferior a 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

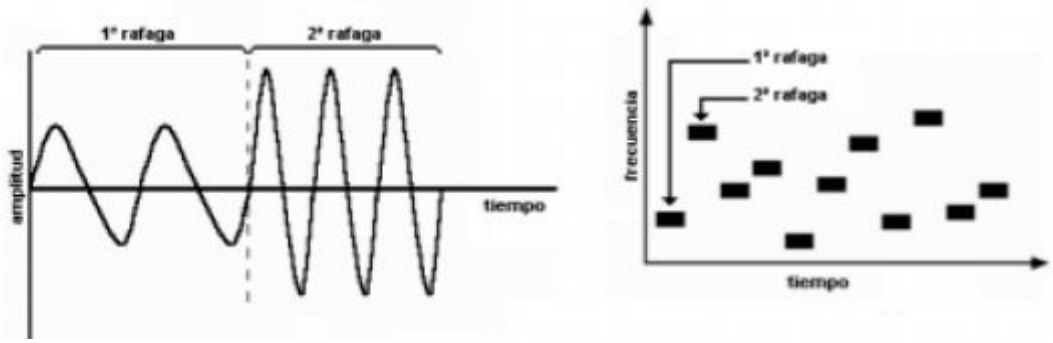


Fig.4. Gráfica de codificación con salto de frecuencia[2]

El orden en los saltos en frecuencia se determina según una secuencia pseudoaleatoria almacenada en unas tablas, y que tanto el emisor y el receptor deben conocer. Manteniéndose la sincronización en los saltos de frecuencias se consigue que, aunque en el tiempo se cambie de canal físico, a nivel lógico se mantiene un solo canal por el que se realiza la comunicación.

Esta técnica también utiliza la zona de los 2.4GHz, la cual organiza en 79 canales con un ancho de banda de 1MHz cada uno. El número de saltos por segundo es regulado por cada país, así, por ejemplo, Estados Unidos fija una tasa mínima de saltos de 2.5 por segundo.

[2] MOLINA, Enrique.2002. Redes Inalámbricas: IEEE 802.11 [http://www.todo-linux.com/manual.todo-linux.com/redes/inalam.htm], [Consulta: 24 nov 2009]

El estándar IEEE 802.11 define la modulación aplicable en este caso. Se utiliza la modulación en frecuencia FSK (Frequency Shift Keying), con una velocidad de 1Mbps ampliable a 2Mbps.

En la revisión del estándar, la 802.11b, esta velocidad también ha aumentado a 11Mbps.

3.1.1.5.3. Tecnología de Infrarrojos.

En esta tecnología, la luz infrarroja es muy tolerante a la interferencia de radiofrecuencia debido a que las ondas de radio operan en una frecuencia totalmente diferente. La Capa Física basada en esta tecnología, utiliza transmisión difusa con una longitud de onda de 0.85 a 0.95 micras, permitiendo velocidades de transmisión de 1 y 2 Mbps. Las LAN IR se basan en la dispersión de la luz infrarroja desde lugares altos, por lo cual el rango de cobertura es mucho más corto. Las señales de infrarrojo no pueden penetrar objetos opacos como las paredes.

La tecnología infrarrojo cuenta con muchas características sumamente atractivas para utilizarse en WLANs: el infrarrojo ofrece una amplio ancho de banda que transmite señales a velocidades altas; tiene una longitud de onda cercana a la de la luz y se comporta como ésta (no puede atravesar objetos sólidos como paredes, por lo que es inherentemente seguro contra receptores no deseados); debido a su alta frecuencia, presenta una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por dispositivos hechos por el hombre (motores, luces ambientales, etc.); la transmisión infrarroja con láser o con diodos no requiere autorización especial en ningún país (excepto por los organismos de salud que limitan la potencia de la señal transmitida); utiliza un protocolo simple y componentes sumamente económicos y de bajo consumo de potencia, una característica importante en dispositivos móviles portátiles.

Las velocidades de transmisión de datos no son suficientemente elevadas y solo se han conseguido en enlaces punto a punto. Por ello, lejos de poder competir globalmente con las LAN de radio frecuencia, su uso está indicado más bien como apoyo y complemento a las LAN ya instaladas, cableadas o por radio, cuando en la aplicación sea suficiente un enlace de corta longitud punto a punto que, mediante la tecnología de infrarrojos, se

consigue con mucho menor coste y potencia que con las tecnologías convencionales de microondas.

3.1.1.6. Capa MAC (acceso al medio)

Esta capa está encargada de proporcionar un servicio de datos fiable a los protocolos de las capas superiores y al mismo tiempo de permitir un acceso ordenado y equitativo al medio inalámbrico compartido.

Para proporcionar un acceso fiable, el estándar 802.11 define un protocolo para el intercambio de tramas de información. La secuencia mínima en este intercambio consiste en el envío de una trama de información del origen al destino y un asentimiento o ACK (Acknowledgment) Acuse de Recibo enviado por el destino en el caso de que la primera trama haya sido recibida correctamente. Todas las tramas a nivel de MAC incorporan un campo de control de errores FCS (Frame Check Sequence, IEEE 32 bits CRC) que es comprobado en cada recepción. Si el origen no recibe el sentimiento o el campo de control falla, la trama es reenviada.

En las redes WLAN tenemos el problema de nodos ocultos, como puede verse en la figura siguiente, los nodos 1 y 3 no se pueden comunicar directamente entre sí provocando problemas de colisiones.

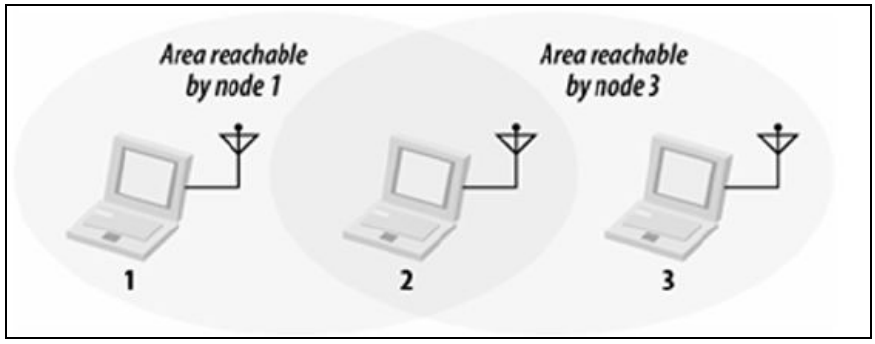


Fig. Problema de nodos ocultos[3]

Adicionalmente a este mecanismo básico de intercambio de tramas, existe una alternativa que proporciona una mayor robustez al protocolo y permite afrontar el problema de los nodos ocultos, conocido como procedimiento RTS/CTS.

[3] GAST Matthew S, Wireless Netwoks The Definitive Guide, 2005. Second Edition. New York 2005.

3.1.1.6.1. Procedimiento RTS/CTS

Este procedimiento de transmisión de múltiples tramas evita el problema de los nodos ocultos. Una estación o nodo que está haciendo uso de este mecanismo debe enviar una trama RTS (Request To Send) al destino antes de transmitir cualquier trama de datos MSDU (Service Data Unit -MAC).

La trama RTS sirve para diversos motivos, reserva el enlace del radio para la transmisión y silencia cualquier estación que pudiera estar escuchando. Una vez que la estación destino recibe la trama RTS de manera correcta, entones debe responder con trama CTS (Clear To Send). A partir de este momento la estación origen podría comenzar a mandar las y tramas MSDU de datos.

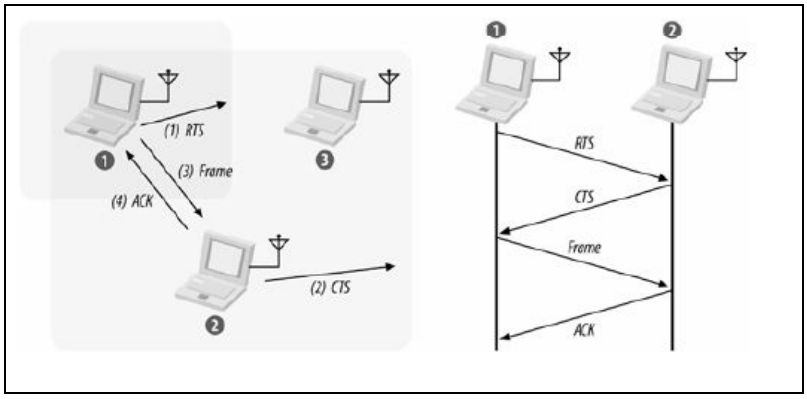


Fig.6. Procedimiento RTS/CTS[4]

Mediante este mecanismo se protege la transmisión entre estaciones frente a inesperadas transmisiones ocultas, además es utilizado por 802.11g para protegerse frente a transmisiones provenientes de posibles estaciones 802.11b.

3.1.1.6.2. Funciones de coordinación MAC

Tenemos dos funciones de coordinación para el acceso al canal de transmisión de acuerdo al estándar 802.11 que son:

- Función de Coordinación Distribuida (DCF – Distributed Coordination Function)

[4] GAST Matthew S, Wireless Netwoks The Definitive Guide, 2005. Second Edition. New York 2005.

- Función de Coordinación Centralizada (PCF Point Coordination Function)

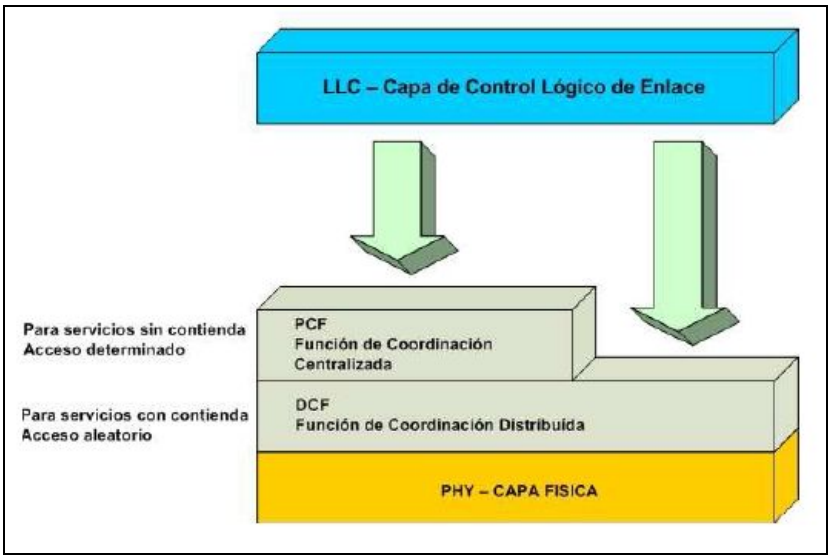


Fig.7. Funciones de Coordinación MAC

- **Función de Coordinación Distribuida (DCF)**

La función de coordinación distribuida proporciona un acceso compartido al medio entre dispositivos con la misma capa física mediante el uso de un protocolo basado en Acceso Múltiple con Detección de Portadora con Prevención de Colisiones CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)[5]. Está establecido que todas las estaciones y dispositivos 802.11 deben incluir obligatoriamente el mecanismo DCF, a diferencia de PCF que es opcional.

DCF Detección o Escucha de Portadora Física : Esta detección se realiza a través de mecanismos físicos y virtuales.

La detección física implica que cualquier estación antes de intentar una transmisión debe realizar una lectura de las condiciones de canal y comprobar que el medio está vacío por un periodo de tiempo IFS (Inter Frame Space). La

[5] GARCIA CARLOS, Propuesta de arquitectura de Q o S en entorno inalámbrico 802.11e basado en Diffserv con ajuste dinámico de parámetros, Tesis Doctoral, Departamento Ingeniería Telemática, Universidad Carlos III Madrid, España

duración de este periodo varia, pero la utilizada justo antes de una transmisión en condiciones normales es llamad DIFS (IFS de Función de Coordinación de Distribuida).

Para evitar una colisión entre dos estaciones que quieren transmitir simultáneamente se utiliza un algoritmo de espera (Backoff) así como la espera de un periodo DIFS.

En caso de que existiesen peticiones de transmisiones pendientes y el medio se encuentra ocupado, la estación espera hasta que el medio se encuentre vacio por un período DIFS. Entonces la estación escoge un número aleatorio entre un rango determinado y usa ese valor como espera adicional antes de transmitir. El rango para elegir la espera aleatoria es llamado Ventana de Contienda CW (Contention Window), que varía de acuerdo con el número de retransmisiones previas.

Si se detecta que el medio pasa a estar ocupado durante el período de espera, el contador se detiene y se reanudara cuando el medio vuelva a estar vacio después del periodo DIFS.

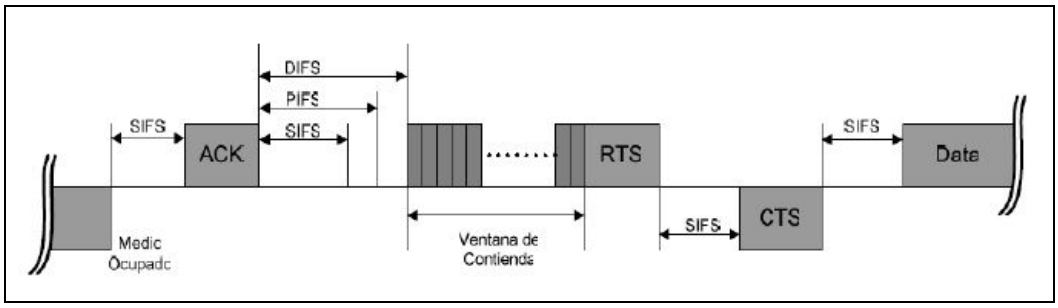


Fig. 8. Modelo de Funcionamiento del mecanismo DCF[6]

Detección o Escucha de Portadora Virtual

[6] GAST MATTHEW S. Wireless Networks The Definitive Guide, Second Edition, O Reilly Media, Inc. United States of America 2005.

Este mecanismo permite la evasión de colisiones. Cada estación mantiene un contador interno llamado NAV (Network Allocation Vector), el cual indica cuando el medio se encuentra ocupado. El valor de la duración se incluye en cada trama transmitida por cada estación (incluyendo tramas RTS, CTS y ACK) el cual indica cuánto tiempo durará la transmisión. Todas las estacione próximas reciben esta trama y usan este valor para actualizar su contador NAV. De manera que en el momento en que una estación quiere comenzar una transmisión, primeramente comprueba que el contador NAV esté en cero.

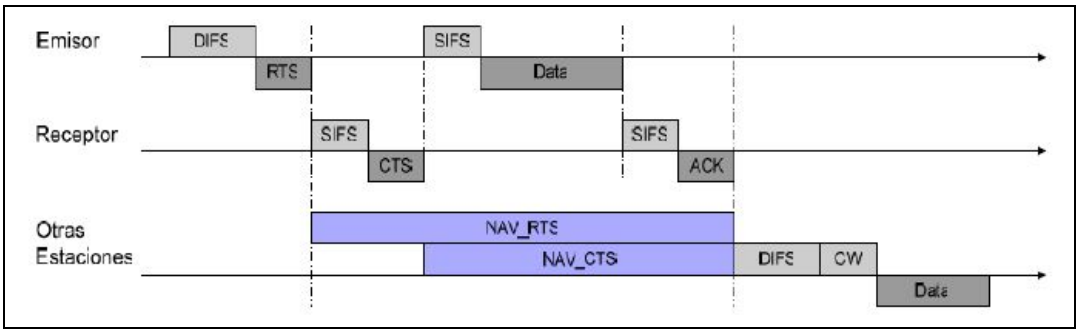


Fig. 9. Utilización de NAV para la detección de portadora virtual[7]

Una vez que la estación consigue acceso al medio ésta puede transmitir la trama de datos MSDU. Entonces espera por un período de tiempo llamado SIFS (IFS corto) para transmitir el asentimiento ACK. La duración del periodo SIFS es más corta que en el caso de DIFS, lo que proporciona a la trama de asentimiento ACK la mayor prioridad para acceder al medio.

- **Función de Coordinación Centralizada:**

Esta función es opcional y los dispositivos 802.11, no están obligados a implementarla. PCF está diseñada para ofrecer soporte de servicios con restricciones temporales para proporcionar calidad de servicio QoS (Quality of Service). Un nuevo elemento denominado Punto de Coordinación PC(Point Coordinator) que se encuentra implementado en el ´Punto de Acceso es el responsable de priorizar el acceso al medio de las estaciones inalámbricas.

[7] GAST MATTHEW S. Wireless Networks The Definitive Guide, Second Edition, O{ Reilly Media, Inc. United States of America 2005

El estándar 802.11 define dos periodos de tiempo entre el envío de dos mensajes de señalización de envío de tráfico DTIM (Delivery Traffic Indication Message), que son:

- Periodo de Contienda CP (Contention Period)
- Periodo de libre contienda CFP (Contention Free Period)

En general, el Punto de Acceso manda de forma periódica tramas beacon (tramas de sincronización que permiten anunciar la existencia de redes 802.11 próximas) aunque estas tramas pueden ser retrasadas si el medio está ocupado. Las tramas beacon (DTIM) son usadas por el PC para indicar el comienzo del CFP. Mediante la grafica siguiente se puede observar cómo se alternan los periodos CFP y PC.

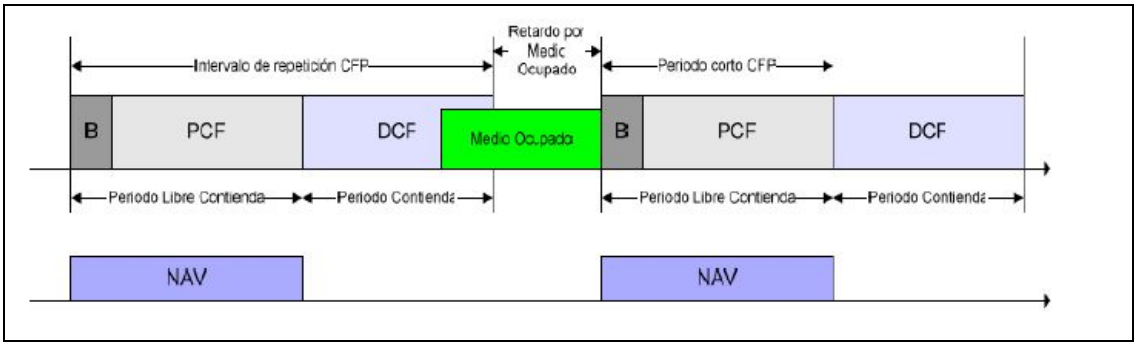


Fig.10. Esquema de funcionamiento de periodos de contienda[8]

Funcionamiento de PCF: Durante el CP todas las estaciones compiten por el medio usando el mecanismo DCF. Durante el CFP, el Punto de Acceso clasifica las transmisiones hacia o desde determinadas estaciones usando un mecanismo de sondeo. No existe contienda (competición por el canal) entre las estaciones durante el ciclo CFP.

[8] GAST MATTHEW S. Wireless Networks The Definitive Guide, Second Edition, O{ Reilly Media, Inc. United States of America 2005

El periodo CFP inicia en cuanto el Punto de Acceso consigue acceso al medio mediante el uso de un espacio de tiempo PIFS (IFS de Función de Coordinación Centralizada) a la llegada de una trama Beacon. El tiempo PIFS es más corto que DIFS, pero mayor que SIFS, y de esta forma PCF logra mayor prioridad que DCF para el acceso pero no interrumpe ninguna comunicación DCF existente. Una vez que PCF consigue el acceso al medio se utiliza el periodo de tiempo SIFS para el intercambio de tramas durante el ciclo CFP.

El sistema de sondeo comienza cuando el PC envía una trama CF-Poll a una de las posibles estaciones. Si el PC tiene alguna trama pendiente de envío, éste podría utilizar una trama de datos incorporado una trama CF-Poll (piggy-backing).

La estación sondeada puede responder con datos junto a una trama CF-ACK, o simplemente con una trama CF- ACK sin no desea enviar más información. Una vez que el intercambio de tramas con una estación termina, el PC envía el CF-Poll a otra estación que estuviese en la lista de estaciones sondeables[9].

Cuando el PC ha terminado con todas las estaciones de la lista, o una vez que la duración del CFP ha espirado, el PC transmite por difusión una trama CF-End anunciando el final del ciclo CFP. A continuación podemos observar el esquema de funcionamiento PCF.

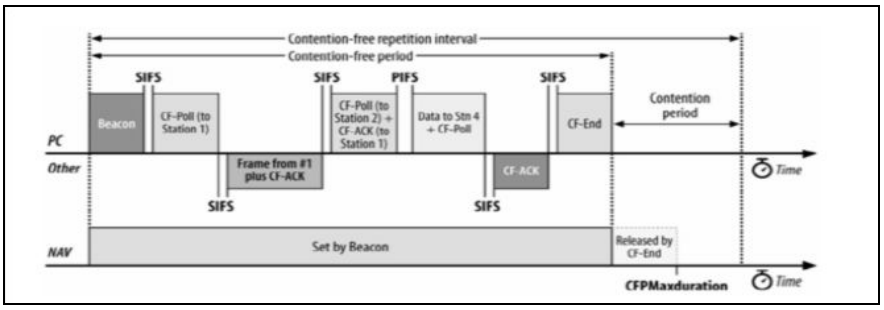


Fig.11. Utilización de PCF[10]

[9] GAST MATTHEW S. Wireless Networks The Definitive Guide, Second Edition, O{ Reilly Media, Inc. United States of America 2005

[10] GAST MATTHEW S. Wireless Networks The Definitive Guide, Second Edition, O{ Reilly Media, Inc. United States of America 2005

Cuando llega una trama Beacon al contador NAV de todas las estaciones se inicializa al valor máximo para proteger el ciclo CFP de transmisiones no deseadas. Entonces el Punto de Acceso transmite por difusión la duración del ciclo CFP en la trama Beacon, y el contador NAV se actualiza adecuadamente.

Cuando finaliza el ciclo CFP, todas las estaciones inicializan su contador NAV a cero cuando reciben la trama CF-END, ocupando la duración del CFP termina. Desde entonces hasta la siguiente trama DTIM todas las estaciones compiten por el medio usando DCF.

Este modo de funcionamiento permite que en una misma red coexistan estaciones con soporte PCF y DCF.

3.1.1.7. Formato de la trama 802.11

Trama se denomina a la información que se emite en una transmisión. Cada trama corresponde a un paquete de datos o paquete de red.

Existen tres tipos de tramas principales:

- Tramas de Datos: transportan datos de protocolo de nivel superior en el cuerpo de la trama. Cada trama inicia con un subcampo de control de trama de 2 bytes. Dependiendo de la red, pueden existir diferentes variedades de tramas de datos.
- Tramas de Control: ayudan a la entrega de tramas de datos, administran el acceso al medio inalámbrico, ejecutan operaciones de limpieza del área y funciones de mantenimiento asociadas a la portadora. Proporcionan funciones de fiabilidad de la capa MAC. A este tipo de trama corresponden: las de Petición de Emisión (RTS), Autorización de Emisión (CTS), Acuse de Recibo(ACK), Sondeo de Ahorro de Potencia (PS-Poll) y las tramas libres de contienda.

- Tramas de Administración: ejecutan funciones de supervisión, se utiliza para asociación y des asociación de estaciones inalámbricas. Forman parte de este grupo las tramas Beacon para sincronización y DTIM.

3.1.1.8. Servicios de red para 802.11

Tenemos nueve servicios para el estándar 802.11, solo se utilizan tres de los servicios para transportar datos, los seis restantes son operaciones de administración que permiten a la red registrar las estaciones móviles.

Se los puede agrupar en servicios del sistema de distribución, servicios de estación y servicios de administración de espectro que es un subgrupo especial de los servicios de estación.[11]

3.1.1.8.1. Servicios del Sistema de Distribución

Estos servicios conectan los Puntos Accesos al Sistema de Distribución, permiten que los Puntos de Acceso extiendan los servicios de la red cableada a la red inalámbrica. Adicionalmente estos servicios se encargan de administrar la asociación de estaciones móviles. En este grupo tenemos los siguientes servicios:

- *Distribución:* utilizado en la entrega de tramas para determinar dirección de destino en redes de infraestructura.
- *Integración:* entrega de tramas a una LAN IEEE 802 fuera de la red inalámbrica.
- *Asociación:* utilizada para establecer conexión entre la estación móvil y el AP.
- *Reasociación:* para cambiar de AP conectado, el AP sirve como pasarela a una estación móvil determinada.
- *Desasociación:* elimina la comunicación de la estación con la red y la conexión con el AP

[11] GAST MATTEWS S, Redes Wireless 802.11, 1ra Edicion Español, ANAYA MULTIMEDIA S.A. España 2006.

3.1.1.8.2. Servicios de Estación:

Mediante estos servicios se permite que una estación móvil se autentique para formar una asociación y pueda transmitir tramas de forma confidencial para proteger los mensajes a medida que recorren el enlace inalámbrico vulnerable. Para este grupo hay los siguientes servicios:

- *Autenticación:* establece la identidad de la estación (dirección MAC) antes de establecer la asociación.
- *Desautenticación*: utilizado para terminar la autenticación y por ende la asociación
- *Confidencialidad:* proporciona protección frente a escuchas secretas.
- *Entrega de MSDU*: entrega de datos al destinatario.

3.1.1.8.3. Servicios de Administración de Espectro

Estos son un subconjunto especial de los servicios de estación, están diseñados para permitir que la red inalámbrica reaccione ante determinadas condiciones de tal forma que cambie dinámicamente las configuraciones de radio frecuencia.[12]

Estos servicios se definen dentro del estándar 802.11h para regulaciones europeas. Para este grupo hay dos servicios que son:

- *Control de Potencia de Transmision TPC (Transmit Power Control):* Reduce la interferencia minimizando la potencia de la estación.
- *Selección Dinámica de Frecuencia DFS (Dynamic Frecuency Selection):* Evita la interferencia con la operación de sistemas de radar en la banda de 5Ghz.

3.1.1.9. Seguridad de redes

[12] GAST MATTHEW S, REDES WIRELESS 802.11, 1ra edición español, ANAYA MULTIMEDIA S.A. España 2006.

Las redes inalámbricas presentan un problema de seguridad importante a considerar como es la autenticación de usuarios y el cifrado de datos. Las señales que se emiten se transportan hasta lugares públicos fáciles de acceder, es por esta razón que se debe identificar el estado de la seguridad de todos los lugares considerados de acceso inalámbrico. La solución de seguridad debe controlar el acceso a la red de usuarios autorizados para el uso del internet.

Uno de los ataques que podríamos recibir es una conexión no autorizada a la red inalámbrica, mediante la cual un intruso podría utilizar el ancho de banda para acceder a Internet, provocando una disminución del rendimiento en la red para sus usuarios legítimos.

Asimismo, se podría emplear la conexión a través de la red inalámbrica para llevar a cabo actividades delictivas en Internet (actividades que se estarían originando desde la propia red de la organización, por lo que ésta podría ser responsable de los daños y perjuicios ocasionados a terceros): ataques contra otras redes, distribución de pornografía infantil, descarga de archivos protegidos por derechos de autor (como la música o las películas), robo de números de tarjetas de crédito, fraudes y amenazas contra otros usuarios.

Otro tipo de ataque seria el análisis de tráfico y sustracción de información confidencial, mediante el uso de de programas llamados "sniffers" para redes inalámbricas, programas especialmente diseñados para interceptar el tráfico transmitido vía radio en este tipo de redes. Entre los más conocidos se puede citar: NetStumbler, AiroPeek, Wireshark, Kismet, Ettercap y Dstumbler; estas herramientas se encargan de analizar las señales transmitidas por los Puntos de Acceso y los equipos con tarjetas inalámbricas y pueden obtener una lista completa de información sobre cada equipo detectado: identificador SSID de la red, protocolo se está usando, tipo de equipo, dirección MAC del equipo, canal de frecuencia que está utilizando, nivel de potencia de la señal entre otros.

La seguridad es un tema importante en las redes inalámbricas porque, al contrario que en una red cableada a la que sólo tienen acceso las personas que físicamente pueden conectarse, cualquier persona que esté cerca pueden conectarse a una red inalámbrica o ver el contenido de los paquetes que circulan por ella si ésta no está convenientemente protegida.

Algunos de los principales protocolos estándar para proporcionar seguridad en redes inalámbricas IEEE 802.11 son:

- WEP (*Wired Equivalent Privacy*). Introducido en 1997 con objeto de proporcionar un nivel de confidencialidad similar al de las redes cableadas. Usa una clave estática de 64 ó 128 bits con el algoritmo RC4. Su uso se desaconseja completamente, ya que aunque es muy fácil de configurar y está muy extendido al ser el primero que surgió, presenta graves fallos de seguridad.

- WPA (*Wi-Fi Protected Access*) fue creado para suplir los múltiples fallos detectados en el protocolo WEP. WPA fue diseñado por el consorcio *Wi-Fi Alliance* basándose en un borrador del estándar 802.11i (es un subconjunto del mismo), y utiliza TKIP (*Temporal Key Integrity Protocol*) como protocolo de cifrado que sustituye a WEP sin necesidad de modificar el hardware existente (podría funcionar actualizando el firmware). En concreto, WPA sigue usando RC4 como algoritmo de cifrado con claves de 128 bits, pero usa TKIP para cambiar dinámicamente estas claves. WPA fue diseñado para ser usado junto a un servidor AAA (habitualmente RADIUS), de manera que se asignan claves distintas a cada uno de los posibles usuarios. Sin embargo, para entornos domésticos o pequeñas oficinas también se puede usar, de forma menos segura, con una única clave compartida (*pre-shared key*, PSK). En este caso hablamos de WPA-PSK.

- WPA2 se basa en el nuevo estándar 802.11i, y el cambio más significativo respecto a WPA es que usa el protocolo de cifrado AES en lugar de RC4. Mientras que WAP puede ejecutarse en el hardware que soporte WEP (tras actualizar el firmware), WAP2 necesita un hardware más nuevo (posterior al

2004). Sin embargo, se sabe que WAP también terminará siendo comprometido a medio plazo y por tanto sólo se recomienda como transición a WAP2.

¿Qué es Temporal Key Integrity Protocol (TKIP)?

Es un protocolo desarrollado para eliminar el problema del uso repetitivo de llaves del protocolo WEP. Este protocolo forma parte de las herramientas de los estándares WPA y 802.11i. TKIP es un estándar que fue creado para facilitar la migración del protocolo WEP a este nuevo protocolo, pues para lograrlo no hay la necesidad de un nuevo dispositivo inalámbrico o hardware, sino basta la actualización de un pequeño programa o "firmware".

El cifrado TKIP es un proceso de dos fases. La primera fase genera una llave por sesión de usuario, a partir de una llave temporal "temporal key", un contador "TKIP sequence counter (TSC)" y la dirección MAC del usuario transmisor. Esta llave temporal "temporal key" es un valor de 128 bits, valor similar al de las llaves WEP. El contador TSC está formado a partir de la dirección fuente, la dirección destino, la prioridad y los datos. Una vez terminada esta fase, un valor llamado "TKIP-mixed transmit address and key (TTAK) es creado. Este valor es usado como una llave de sesión para la segunda fase. En la segunda fase, el valor de TTAK y el vector de inicialización (IV) son usados para producir una llave para poder encriptar todos los datos. Este cifrado se realiza mediante el algoritmo RC4, del mismo modo que WEP lo utiliza. Es por esta razón que el protocolo TKIP es mucho más seguro que su antecesor WEP, pues no usa una misma llave para cifrar los datos, sino que esta llave varía dependiendo de qué usuario se esté comunicando y de qué modo lo haga.

TKIP Message Integrity Check (MIC)

TKIP Message Integrity Check es un protocolo creado para combatir los ataques de modificación de paquetes de información. El protocolo MIC o también denominado Michael, es un método mucho más seguro que el protocolo IVC usado para integridad de paquetes en WEP.

MIC utiliza un algoritmo tipo “hash” a partir de un valor semilla, la dirección MAC destino, la dirección MAC fuente, la prioridad y la carga útil; dando menos oportunidad que un intruso pueda modificar el paquete sin que el algoritmo MIC lo detecte. A su vez MIC es cifrado dentro de la porción de datos, de modo que ningún programa “Sniffer” de algún intruso pueda obtenerlo.

Para poder combatir los ataques contra modificación de paquetes, TKIP y MIC implementan un mecanismo por el cual el punto de acceso involucrado suspende todas las comunicaciones si es que se producen dos fallas MIC en menos de 60 segundos. Si es que esto logra pasar, el punto de acceso retomará actividad dentro de 60 segundos más, y requerirá que todos los usuarios vuelvan a conectarse y negocien nuevamente sus llaves de cifrado. Por otro lado para poder prevenir que este mecanismo sea inválido, debido a la modificación de paquetes por el ruido inherente a las comunicaciones RF; el algoritmo MIC se basa antes en la comprobación de los datos del paquete de información, la cual es realizada por los siguientes algoritmos: “frame check sum (FCS)”, “integrity check sum (ICV)” y “TKIP sequence counter (TSC)”.

3.1.1.9.1. RADIUS

RADIUS (Remote Authentication Dial-In User Server), es un protocolo que nos permite gestionar la “autenticación, autorización y registro” de usuarios remotos sobre un determinado recurso; “autenticación, autorización y registro” más conocido como protocolo AAA, es el acrónimo de su denominación original inglesa “Authentication, Authorization, and Accounting”, a continuación describiremos a que se refiere cada término:

Autenticación (authentication): proceso por el cual se determina si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. El proceso de autenticación se realiza mediante la presentación de una identidad y credenciales por parte del usuario que demanda acceso. Un tipo habitual de credencial es el uso de una contraseña (o password) que junto al nombre de usuario nos permite acceder a determinados recursos.

Existen algunos métodos que implementan el proceso de la autenticación. Algunos de ellos, soportados por RADIUS, son:

- Autenticación de sistema (*system authentication*), típica en un sistema Unix, normalmente realizada mediante el uso del fichero /etc/passwd;
- Protocolos PAP (*Password Authentication Protocol*), y su versión segura CHAP (*Challenge Handshake Authentication Protocol*), que son métodos de autenticación usados por proveedores de servicios de Internet (ISPs) accesibles vía PPP;
- LDAP (*Lightweight Directory Access Protocol*), un protocolo a nivel de aplicación (sobre TCP/IP) que implementa un servicio de directorio ordenado, y muy empleado como base de datos para contener nombres de usuarios y sus contraseñas;
- Kerberos, el famoso método de autenticación diseñado por el MIT;
- EAP (Extensible Authentication Protocol), se trata de un entorno universal de autenticación empleado frecuentemente en redes inalámbricas y conexiones punto a punto. Permite elevar el nivel de seguridad de la autenticación, permitiendo diversos métodos de autenticación y tipos de credenciales a utilizar. Los principales tipos de EAP son:

  - EAP-TLS: Realiza la autenticación estableciendo un túnel cifrado entre los elementos para proteger las credenciales y datos que se intercambian. Utiliza certificados digitales para autenticar a cliente y servidor.

  - PEAP: Realiza la autenticación en dos fases. Primero establece una sesión TLS para autenticar al servidor y posteriormente se establece un segundo túnel para autenticar al cliente, permitiendo realizar autenticaciones de tipo CHAP (como el de Microsoft "MS-CHAP") de manera más segura. Es un protocolo comúnmente soportado por tecnologías de Microsoft.

  - TTLS: También se realiza la autenticación en dos fases, utilizando una sesión de TLS para proteger la autenticación del cliente (similar a PEAP). Puede utilizar tipos de autenticación diferentes a EAP, como CHAP, MS-

CHAP y otros. Este tipo de autenticación no es comúnmente soportado, por lo cual suele requerir un software adicional en el cliente.

- LEAP: Es un método de autenticación desarrollado por Cisco, que usa contraseña para autenticar al cliente. Generalmente se requiere de hardware/software Cisco para soportarlo. Adicionalmente, es susceptible a ataques de adivinación de contraseñas, y no permite autenticar equipos.

- Por último, también se permite la autenticación basada en ficheros locales de configuración del propio servidor RADIUS.

RADIUS posee cuatro tipos de paquetes para autenticación básicos para entender que es lo que está ocurriendo, los cuales se detallan a continuación:

- **Access-Request**: Este paquete consiste en una petición para ser atendido, dando inicio a la secuencia RADIUS.
- **Access-Accept:** Este paquete informa al cliente RADIUS (punto de acceso) que la autenticación es correcta.
- **Access-Reject:** Este paquete informa al cliente RADIUS que la autenticación es incorrecta.
- **Access-Challenge:** Este paquete es usado para hacer un pedido de credenciales de usuario al cliente RADIUS.

"A continuación en la figura 11, se muestra cual es la secuencia de cómo el usuario accede a la red y luego se desconecta de ella.

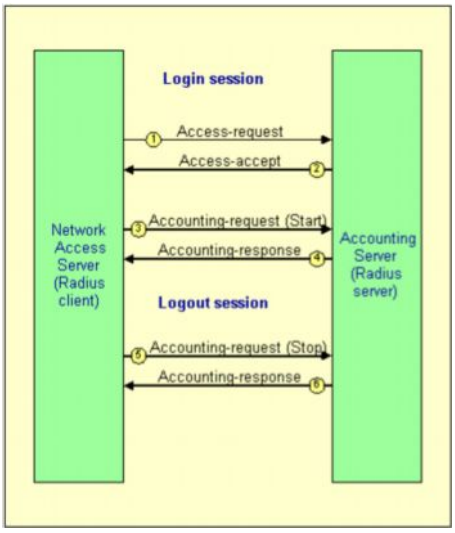


Fig. 12 . Diagrama de secuencia de conexión y desconexión de un cliente a la red.[13]

1. El cliente envía su usuario/contraseña, la información es encriptada con una llave secreta y enviada en un **Access-Request** al servidor RADIUS (Fase de Autenticación).
2. Si la relación usuario/contraseña es correcta, entonces el servidor envía un mensaje de aceptación, **Access-Accept**, con una información extra (Por ejemplo: dirección IP, máscara de red, tiempo de sesión permitido, etc.) (Fase de Autorización).
3. El cliente envía un mensaje de **Accounting-Request** (Start) con la información correspondiente a su cuenta y indicando que el usuario está reconocido dentro de la red (Fase de Accounting).
4. El servidor RADIUS responde con un mensaje **Accounting-Response**, cuando la información de la cuenta es almacenada.
5. Si el usuario ha sido identificado, éste puede acceder a los servicios proporcionados. Finalmente, para desconectarse, enviará un mensaje de **Accounting-Request (Stop)** con la siguiente información:

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

6. El servidor RADIUS responde con un mensaje de **Accounting-Response** cuando la información de cuenta es almacenada"[14].

[13] MÁRQUEZ Adolfo y otros, 2007, RADIUS, Instituto Tecnológico Superior Monterrey. [http://santiagozky.files.wordpress.com/2007/11/radius.pdf].
[14] MÁRQUEZ Adolfo, y otros, 2007, RADIUS, Instituto Tecnológico Superior Monterrey. [http://santiagozky.files.wordpress.com/2007/11/radius.pdf].

Autorización (authorization) consiste en conceder servicios específicos a usuarios determinados entre los que se incluye la "negación de servicio", dependiendo de su propia autenticación, de los servicios que está solicitando, y el estado actual del sistema.
El proceso de autorización determina la naturaleza del servicio que se concede al usuario, como son: la dirección IP que se le asigna, el tipo de calidad de servicio (QoS) que va a recibir, el uso de encriptación, o la utilización obligatoria de túneles para determinadas conexiones.

Los métodos de autorización que normalmente soporta un servidor de RADIUS incluyen bases de datos LDAP, bases de datos SQL (como Oracle, MySQL y PostgreSQL), o incluso el uso de ficheros de configuración locales al servidor.

No se debe confundir los términos autenticación con autorización, ya que la autenticación es el proceso de verificar un derecho reclamado por un individuo (persona o incluso ordenador), mientras que la autorización es el proceso de verificar que una persona ya autenticada tiene la autoridad para efectuar una determinada operación.

Registro (accounting) se trata de realizar un registro del consumo de recursos que efectúan los usuarios. El registro suele incluir aspectos como la identidad del usuario, la naturaleza del servicio prestado, y cuándo empezó y terminó el uso de dicho servicio.

FreeRadius

FreeRadius, es un software de código abierto, es una alternativa libre hacia otros servidores RADIUS, siendo uno de los más completos y versátiles gracias a la variedad de módulos que le componen, tales como una biblioteca BSD para clientes, módulos para soporte en apache, y lo que más nos interesa un servidor de RADIUS. Puede operar tanto en sistemas con recursos limitados así como sistemas atendiendo millones de usuarios.

"En la actualidad incluye soporte para LDAP, SQL, Oracle y otras bases de datos, así como los tipos de autenticación más conocidos como EAP, EAP-TTLS y PEAP.

Actualmente incluye soporte para todos los protocolos comunes de autenticación y bases de datos”[15].

N.A.S. *Network Access Server* (NAS)

Se trata de un sistema que proporciona acceso a la red, es decir, que controla el acceso a un recurso protegido, que puede ser desde un sencillo teléfono para VoIP o una impresora, hasta el acceso a una red inalámbrica o a Internet (proporcionado por un ISP). También se conoce como *Remote Access Server* (RAS) o *Terminal Server*.

Cuando un cliente quiere hacer uso de uno de estos servicios se conecta a NAS, quien a su vez se conecta al servidor de AAA (típicamente RADIUS) para preguntar si los credenciales proporcionados por el cliente son válidos. Dependiendo de esta respuesta, NAS le permitirá acceder o no a este recurso protegido. NAS no contiene ninguna información sobre los usuarios que se pueden conectar ni sus credenciales, sino que utiliza esta información para enviarla a RADIUS, y que éste le informe sobre los permisos del cliente.

Aquí tenemos dos niveles de la arquitectura cliente-servidor. Por un lado, tenemos la típica arquitectura en la que un usuario quiere acceder a un servicio, siendo el usuario el cliente, y el servidor el sistema que proporciona dicho servicio. Pero por otro lado, si consideramos el proceso de AAA, el cliente sería el sistema que proporciona el acceso a la red (por ejemplo NAS), mientras que el servidor es el sistema que autoriza o no dicho acceso (por ejemplo RADIUS). Consideraremos servidores RADIUS aquellos clientes que son los elementos a proteger (por ejemplo, un punto de acceso para la conexión inalámbrica). Entonces los usuarios que quieren acceder al recurso protegido (por ejemplo, la persona que se desea conectar a la red inalámbrica por medio del punto de acceso), no es un cliente de RADIUS sino que se denomina suplicante.

Una ventaja del uso de RADIUS es que sus clientes tan sólo tienen que implementar el protocolo de comunicación con RADIUS, y no todas las posibilidades de AAA existentes (PAP, CHAP, LDAP, kerberos, mySQL, etc.). En el ejemplo del punto de

[15] BARRIOS Joel, Configuración Básica de FreeRadius. [http://www.alcancelibre.org/staticpages /index.php/como-freeradius-basico/print]

acceso, tan sólo necesitamos implementar una solución NAS que realice las consultas a RADIUS.

Otra ventaja del protocolo RADIUS es que, en su comunicación con NAS, nunca transmite las contraseñas directamente por la red (lo que se conoce como en *cleartext*), ni siquiera al usar PAP, sino que usa algoritmos para ocultar las contraseñas como MD5. Sin embargo, al no ser considerado MD5 un sistema de protección de credenciales demasiado seguro, es aconsejable utilizar sistemas adicionales de protección para cifrar el tráfico de RADIUS, como puede ser túneles de IPsec.

3.1.1.9.2. Extensible Authentication Protocol (EAP)

Extensible Authentication Protocol (EAP), es un protocolo desarrollado para autenticación de usuarios de una red, el cual es el resultado de mejorar anteriores intentos fallidos como lo fueron los protocolos "Password Authentication Protocol (PAP)" y "Challenge Handshake Authentication Protocol (CHAP)". Para usar EAP, uno debe especificar dentro del campo de "Type field" que clase de autenticación se va a usar y esto es porque el protocolo EAP soporta distintas técnicas de autenticación (passwords, tarjetas inteligentes, certificados digitales) y esto lo logra sin tener que realizar cambios en su estructura.

El protocolo EAP es incluido en un paquete de tipo "Point-to-Point Protocol (PPP)", esto permite que cualquier dispositivo que soporte PPP también soporte el protocolo EAP. Además el protocolo EAP soporta el estándar 802.1x y esto ha sido logrado en el documento RFC 3748.

El paquete EAP está formado por 5 campos: "code", "identifier", "length", "type" y "data", como se muestra en la figura:

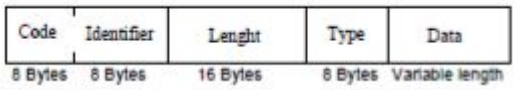


FIG.13. Paquete EAP

Estos permiten identificar la función del paquete, relacionar múltiples usuarios, saber el tamaño del paquete, conocer el tipo de modulación usada y los datos de información

que componen el paquete. Los tipos de modulación EAP conocidos son: EAP-MD5, EAP-TLS, EAP-TTLS, LEAP, PEAP y EAP-FAST.

3.1.1.9.3 Protocolo EAP- PEAP

Protected Extensible Authentication Protocol (PEAP) es un protocolo desarrollado en conjunto por RAS, Microsoft y Cisco Systems, para poder manejar un método de autenticación EAP común a varias compañías.

Una de las principales ventajas de PEAP es tener un fuerte tipo de autenticación EAP que no requiere certificados digitales de los clientes. EAP-PEAP trabaja similarmente como el protocolo EAP-TLS, de modo que crea un túnel cifrado con TLS (Transport Layer Security) para poder realizar la autenticación del usuario hacia el Servidor de Autenticación.

El proceso de autenticación EAP-PEAP empieza mediante una paquete "request packet" del suplicante para ser atendido. El punto de acceso escucha la petición y responde mediante un paquete "response packet". Esta respuesta también preguntará al suplicante por su correspondiente identidad. La identidad será el tipo de EAP, en este caso EAP-Type=PEAP, esto significa que el tipo de autenticación usada por el servidor de autenticación será PEAP. El tráfico de datos se transportará por intermedio del punto de acceso, el cual es llamado también "Authenticator". Una vez que el método de autenticación PEAP es elegido, un túnel cifrado TLS es creado mediante un certificado del servidor de autenticación. Es por este túnel TLS que el proceso de autenticación del suplicante toma lugar.

3.1.1.9.4. Encriptación

La encriptación es un proceso mediante el cual, utilizando una llave o un valor de control, un mensaje (generalmente datos en texto plano) es codificado para evitar que su contenido sea accedido y/o entendido por personal no autorizado. Para poder acceder al mensaje cifrado es necesario desencriptar el mensaje, proceso mediante el cual,

utilizando la llave indicada, se recupera la información del mensaje en su estado original.

Hay dos tipos de encriptación:

a) **Encriptación simétrica**: Mediante este proceso de cifrado de datos, se realiza la encriptación y desencriptación utilizando la misma llave. La encriptación simétrica es un procedimiento rápido, que provee mecanismos para asegurar la confidencialidad e integridad de la información que protege. Por otro lado el hecho de utilizar la misma clave en los procesos mencionados implica realizar una distribución segura de llaves por vías alternas a la que se quiere proteger. Por lo anterior también es recomendado utilizar la llave la menor cantidad de veces posible, idealmente una sola vez. Algunos de los estándares de encriptación simétrica más conocidos son: DES (Data Encription Standard) Triple DES y AES (Advanced Encription Standard)

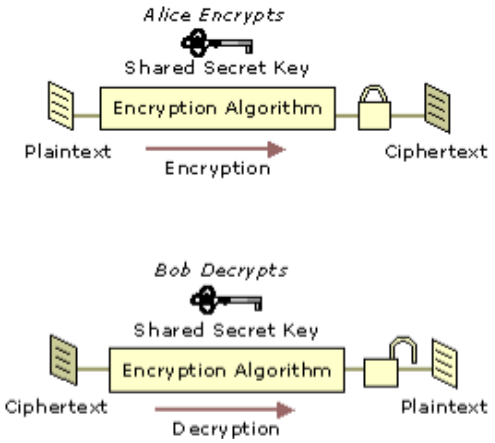


Fig. 14 Encriptación simétrica[16]

b) **Encriptación asimétrica:** Este proceso de cifrado de datos, consiste en la utilización de llaves diferentes para la encriptación y desencriptación, una de estas de carácter privado o secreto y la otra es de acceso público. Conocido también como encriptación de clave pública y se dice que se implementa bajo una infraestructura de clave pública (PKI). Este tipo de encriptación se desarrolló a finales de los años 70's y adicionó nuevas funcionalidades a los mecanismos de encriptación como la posibilidad de realizar autenticación fuerte,

[16] Tipos de Encriptación. 2006. [http://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptación]

no repudio, y el hecho de mejorar y facilitar los esquemas de confidencialidad e integridad. Algunos de los estándares de encriptación asimétrica más conocidos son: RSA (Rivest, Shamir & Addleman), Diffie-Hellman y El Gamal.

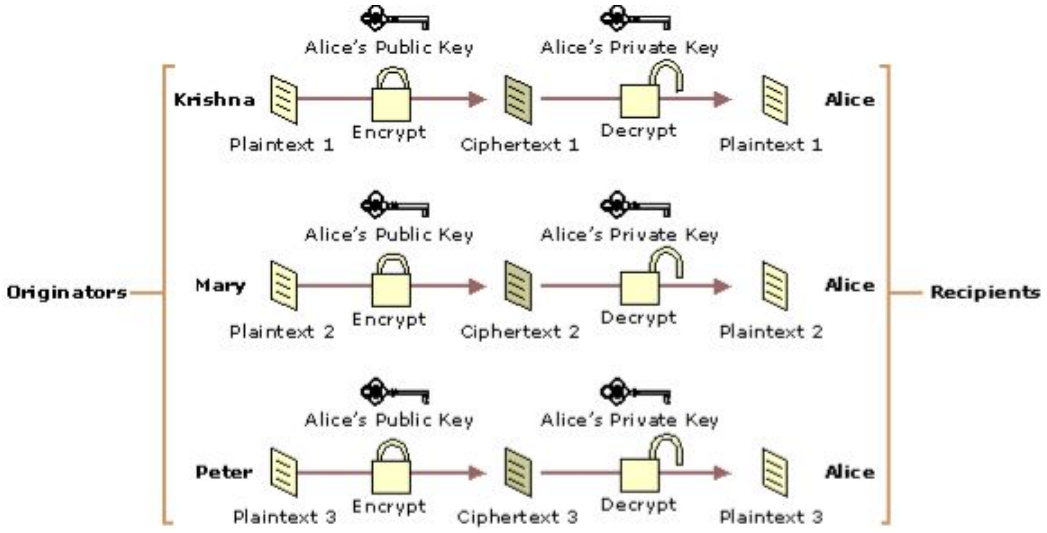


Fig. 15. Encriptación asimétrica[17]

3.1.1.9.5. Estándar 802.1x

El protocolo 802.1X, es un estándar del IEEE, permite realizar el control de acceso a una red mediante un proceso de autenticación que autoriza o impide el acceso de los dispositivos que quieren conectarse a la red. Este estándar puede implementarse tanto en redes cableadas como en redes inalámbricas 802.11. Adicionalmente este tipo de implementación puede utilizarse para administrar las claves utilizadas para proteger la información que trasmiten los dispositivos autenticados.

Para la implementación de una solución basada en 802.1x se requieren como mínimo, los siguientes componentes:

- Usuario que quiere acceder a la red, o "suplicante"
- Punto de acceso que permite o impide el ingreso del suplicante, también llamado "Autenticador"

[17] Tipos de Encriptación. 2006. [http://www.textoscientificos.com/redes/redes-virtuales/tuneles/encriptación]

- Y el servidor de autenticación, quien negocia y valida la identidad del suplicante; y le informa el éxito o fracaso de este proceso al autenticador para que ejecute la acción indicada.

Fig. 16 Componentes para solución 802.1x

1X hace referencia al uso del protocolo de autenticación extensible EAP entre el suplicante (usuarios de acceso inalámbrico), el autenticador (en este caso Access Point) y los servidores de autenticación (como el RADIUS).

Las principales ventajas que presenta el uso de una solución basada en el protocolo 802.1X para WLAN son las siguientes:

- 802.1x es un protocolo estandarizado
- La solución no es de gran costo, debido a que requiere de un servidor Radius del cual muchas empresas disponen.
- La especificación WAP Wi-Fi Protected Access, se basa en estándares que incrementan el nivel de protección de los datos y el control de acceso a la red inalámbrica. WPA, está diseñado para ser compatible con el estándar 802.11i. Esta especificación utiliza el protocolo TKIP, así como el protocolo 802.1x-eap, para autenticar el usuario
- Este protocolo lo está incorporado por todos los principales fabricantes de equipos para redes tanto en sus equipos wireless como para sus soluciones de redes cableadas. Así pues, ello permite unificar el método de autenticación de los usuarios en toda la red, tanto wireless como cableada.
- Permite gestionar el intercambio de credenciales para la autenticación.
- Permite la autenticación por usuario.

- Permite la autenticación mutua entre el cliente y el servidor de validación Radius.
- Permite la reautenticación de forma periódica.
- Gestiona el intercambio de llaves para la encriptación.
- Permite la renovación periódica de las llaves WEP.
- No concreta ningún protocolo específico para la encriptación, y está abierto a cualquiera de los protocolos actuales como WEP, DES o AES.
- Como plataforma para la autenticación de los usuarios finales, 802.1x utiliza el protocolo abierto EAP, que a su vez permitirá la incorporación de nuevos protocolos que sumar a los hoy en día ya existentes como EAP-TTLS,EAP-TLS, LEAP, PEAP, etc.
- Permite la centralización de todo el proceso de validación de usuarios sobre un único servidor Radius, lo que a su vez permite añadir funcionalidades de autorización y accounting.
- Si por algún motivo se desea aumentar el grado de confidencialidad, dicha solución podría tunelizarse.

Desventajas

- Actualmente las llaves de encriptación son WEP con las vulnerabilidades ya conocidas de dicho sistema de encriptación.
- Dicha solución solo se puede implantar sobre un parque de equipos con determinados sistemas operativos que soporten 802.1x como por ejemplo Windows XP.

Soluciones a dichas desventajas:

- Precisamente por ser conocidas las vulnerabilidades de WEP, tenemos que: Con el cambio frecuente y periódico de la clave de encriptación unipersonal minimizamos prácticamente los riesgos asociados al uso compartido y estático de las claves, tal y como se define en el estándar 802.11b. Además los nuevos equipos traen configuración WAP, brindando más seguridad.

4. PROPUESTA ALTERNATIVA

4.1. IMPLANTACIÓN

4.1.1. Instalación de los equipos

Instalación del servidor: La instalación del servidor se hará en el edificio de Administración del Área, esto debido a que el equipo debe estar protegido del acceso y manipulación de personal no autorizado.

Instalación de los puntos de accesos: Para la ubicación de los puntos de acceso se ha tomado en cuenta que estén cerca de donde se va a obtener el acceso a internet y la alimentación de energía, además sitios estratégicos que permitan dar cobertura la mayor cantidad posible de metros alrededor del mismo, esto se detalla en el plano del lugar.

4.1.2. Configuración de equipos

Las pruebas de autenticación se realizaran sobre una Red Inalámbrica modelo parecida a la red propuesta en la solución, con el servidor y access point que se implantarán a futuro.

4.1.2.1. Configuración del Servidor

Se ha instalado el S.O. CENTOS versión 5.5, un servidor de FreeRadius 1.1.3-1.6.el5.i386, librerías para la conexión de FreeRadius con Mysql freeradius-mysql-1.1.3-1.6.el5.i386. Además se instaló PHP5 y el servidor Apache para poder manejar la herramienta Phpmyadmin.
Se debe levantar los servicios de Mysql y apache para poder ejecutar Phpmyadmin, con los siguientes comandos:

```
#service mysqld start
#service httpd  start
```

Además debe dejar los servicios de mysql y apache, con arranque automático, esto para no tener que iniciar cada vez que encienda el servidor, se obtiene con:

```
# chkconfig mysqld on
# chkconfig httpd on
```

Creamos la base de datos RADIUS, en Mysql, donde están almacenados los usuarios a autenticar. Esto mediante un script que viene incluido en freeradius.

Una vez hecho esto configuramos en el FREERADIUS los archivos principales necesarios, los cuales están ubicados en el directorio /etc/raddb, estos son:

- radiusd.conf
- sql.conf
- eap.cfg
- user.cfg
- clientes.cfg

Listado 1: radiusd.conf

Este es el archivo principal donde se configura los argumentos relacionados con **SQL, EAP** y la configuración del dominio al que los clientes se conectarán. En nuestro caso con la base de datos Mysql y EAP es el protocolo para la autenticación de usuario, usada normalmente en redes inalámbricas. También es importante sustituirse todo **${confdir}** encontrado en el archivo por el directorio actual de FreeRADIUS, en nuestro caso **'/etc/raddb'.**

```
        modules {
                pap {
                        auto_header = yes
                        }
                chap {
                        authtype = CHAP
                        }
                pam {
                        pam_auth = radiusd
                        }
                unix {
                        cache = no
                        cache_reload = 600
                        radwtmp = ${logdir}/radwtmp
                        }
$INCLUDE /etc/raddb/eap.conf
        mschap {
                authtype = MS-CHAP
                use_mppe = yes
                require_encryption = yes
                require_strong = no
                }
```

```
ldap {
server = "ldap.your.domain"
basedn = "o=My Org,c=UA"
filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
start_tls = no
access_attr = "dialupAccess"
dictionary_mapping = ${raddbdir}/ldap.attrmap
ldap_connections_number = 5
timeout = 4
timelimit = 3
net_timeout = 1
}
...
preprocess {
huntgroups = /etc/freeradius/huntgroups
hints = /etc/freeradius/hints
with_ascend_hack = no
ascend_channels_per_line = 23
# Mismo motivo que el pasado, pero para hacerlo en el
# preprocesamiento
with_ntdomain_hack = no
with_specialix_jetstream_hack = no
with_cisco_vsa_hack = no
}
...
ippool main_pool {
# Se coloca el rango de IPs disponibles y la máscara de
# red
range-start = 192.168.0.1
range-stop = 192.168.3.254
netmask = 255.255.255.0
cache-size = 800
session-db = ${raddbdir}/db.ippool
ip-index = ${raddbdir}/db.ipindex
override = no
maximum-timeout = 0
}
}
instantiate {
exec
expr
}
authorize {
preprocess
chap
mschap
suffix

post-proxy {
eap
}
```

```
        # EAP, activa el protocolo EAP para autorización. FILES,
        hace que
        # se lea el archivo 'users'. SQL, hace que se entre a la
        base de
        # datos de MySQL para buscar los datos del cliente.
        eap
        files
        sql
        }
        authenticate {
        Auth-Type PAP {
        pap
        }
        Auth-Type CHAP {
        chap
        }
        Auth-Type MS-CHAP {
        mschap
        }
        unix
        # Habilita la autenticación EAP
        eap
        }
        preacct {
        preprocess
        acct_unique
        suffix
        }
        accounting {
        detail
        unix
        radutmp
        # Lee las cuentas localizadas en la base de datos de
        MySQL
        sql
        }
        session {
        radutmp

$INCLUDE /etc/raddb/eap.conf

        # Usa MySQL en el manejo de sesiones
        sql
        }
        post-auth {
        # Usa MySQL para las tareas de post-autenticación
        sql
        }
        pre-proxy {
        }
```

Listado 2: sql.conf.

Una vez que en el archivo de configuración 'radiusd.conf' se ha activado el soporte para SQL, debemos configurar el archivo 'sql.conf'. Éste contiene información sobre el servidor SQL y las consultas que se deben hacer para obtener la información de los usuarios. En las primeras líneas se da información sobre el servidor SQL, después viene la definición de las tablas y por último, las consultas. Escogimos MySQL para almacenar los usuarios de RADIUS debido a que Mysql es soportada por Freeradius y para nosotros constituye la base de datos más conocida y fácil de manejar.

```
sql {
driver = "rlm_sql_mysql"
# Es importante colocar el IP del servidor. El usuario root o el
# usuario que tenga permisos a la base de datos 'radius' que
# después crearemos. Finalmente, se coloca la contraseña
de este
# usuario.
server = "localhost"
login = "radius"
password = "radpass"
# Definición de base de datos y tablas
radius_db = "radius"
acct_table1 = "radacct"
acct_table2 = "radacct"
postauth_table = "radpostauth"
authcheck_table = "radcheck"
authreply_table = "radreply"
groupcheck_table = "radgroupcheck"
groupreply_table = "radgroupreply"
usergroup_table = "usergroup"
nas_table = "nas"
deletestalesessions = yes
sqltrace = no
sqltracefile = ${logdir}/sqltrace.sql
num_sql_socks = 5
connect_failure_retry_delay = 60
sql_user_name = "%{User-Name}"
...
}
```

Listado 3: eap.conf.

En éste archivo configuramos el protocolo de autenticación que se usará por defecto en este caso PEAP, el cual, a su vez, usará MSCHAPV2 (Microsoft Challenge-Handshake Authentication Protocol). Esto debido a que la mayoría de usuarios son de Windows, únicamente el S.O. Window Seven, no puede conectarse debido a que no hay una certificación dentro de Freeradius que le permita hacerlo.

```
eap {
# Se le dice que use tls
default_eap_type = tls
timer_expire = 60
ignore_unknown_eap_types = no
cisco_accounting_username_bug = no
md5 {
}
leap {
}
gtc {
auth_type = PAP
}
tls {
# Se cambian los ${raddbdir} por /etc/raddb/certs
private_key_password = whatever
private_key_file = /etc/ raddb /certs/cert-srv.pem
certificate_file = /etc/ raddb /certs/cert-srv.pem
CA_file = /etc/f raddb /certs/demoCA/cacert.pem
dh_file = /etc/ raddb /certs/dh
random_file = /dev/urandom
}
# Se le dice que use MSCHAPV2
peap {
default_eap_type = mschapv2
}
mschapv2 {
}
}
```

Una vez configurado este archivo, deben crearse ligas simbólicas a los certificados que EAP necesita, para que pueda localizarlos. Para ello, se entra al directorio donde se guardan los certificados y se ejecuta un **rehash.**

```
# cd /etc/f raddb /certs
# c_rehash
```

users.conf: Contiene la información de los usuarios que pueden acceder a la red, en caso de que no se use otro método. En nuestro caso, este archivo no se va a configurar, puesto que se usó una base de datos en MySQL. Todas las configuraciones que tengan como usuario DEFAULT, son las que se asignarán a los usuarios en caso de que no estén especificadas para ellos.

Listado 4: clients.conf

Aquí se especifican los IPs o subredes desde las cuales se aceptarán peticiones. Si llega una petición de acceso desde un IP que no esté registrado aquí, el servidor RADIUS simplemente la ignora, negándole el acceso. En nuestro caso se acepta al localhost y al o los AP que enviarán las solicitudes.

```
client 192.168.0.201{
secret = tesisaeirnnr1
shortname = aeirnnr1
}
client 192.168.0.202{
secret = tesisaeirnnr2
shortname = aeirnnr2
}
```

Una vez finalizada la configuración del servidor Freeradius, podemos poner en ejecución el mismo. Para que usted pueda configurar revise el Manual de Usuario de la WLAN.

Configuración de MySQL

Por medio de PhpMyAdmyn, se creó inicialmente la base de datos de usuarios. Así ya se cuenta con una base de datos para la autenticación. Las tablas más importantes son:

- usergroup: Aquí se define a qué grupo pertenece cada usuario. Sus atributos son:
  id. Identificador de registro.
  UserName. Nombre de usuario.
  GroupName. Grupo al que pertenece el usuario.
- radcheck: Aquí se definen las contraseñas de cada usuario. Sus atributos son:
  id. Identificador de registro.
  UserName. Nombre de usuario.
  Attribute. Tipo de contraseña. En nuestro caso, 'User-Password'.
  Op. Es el operador que se usará para la comprobación. Para nosotros '==‘.
  Value. La contraseña.
- radreply: En esta tabla se definen los atributos sobre la conexión y sesión de los usuarios; por ejemplo, IP asignada y tiempo de espera máximo. En nuestro caso, permitimos que se asignen los de DEFAULT contenidos en el archivo 'users'; por lo tanto, no insertamos nada en la tabla.
- radgroupreply: Similar a radcheck pero permite establecer atributos a un grupo de usuarios completo. Atributos:
  id. Identificador de registro.
  GroupName. Nombre de grupo.
  Attribute. Nombre del atributo que se quiere agregar.
  Nosotros sólo hicimos uso de uno, el tipo de autenticación: 'Auth-Type'.
  Op. Es el operador que se usará para la comprobación. Para nosotros ':='.

Value. El valor del atributo. Nuestro Auth-Type es ‘EAP’.

De esta forma quedan los datos en nuestra base de datos.

id	UserName	GroupName
1	Estud1	Estudiante
2	Estud2	Estudiante

id	UserName	Attribute	Op	Value
1	Estud1	Password	==	Estudpass1
2	Estud2	Password	==	Estudpass2

id	GroupName	Attribute	Op	Value
1	Estudiante	Auth-Type |	==	EAP

4.1.2.2. Configuración del Access Point

Para iniciar la configuración de los Access Point, primero los conectamos por medio de cable a la red del Área, verificamos si están conectados mediante el ping 192.168.1.245 y ping 192.168.1.245, luego con nuestro navegador preferido ingresamos a la página 192.168.1.245 y nos pedirá el usuario (en blanco) y el password (admin).

Fig.17 . Configuración del AP.

Luego aparece la pantalla para configurar las direcciones IP, en donde debemos ir grabando cada cambio realizado.

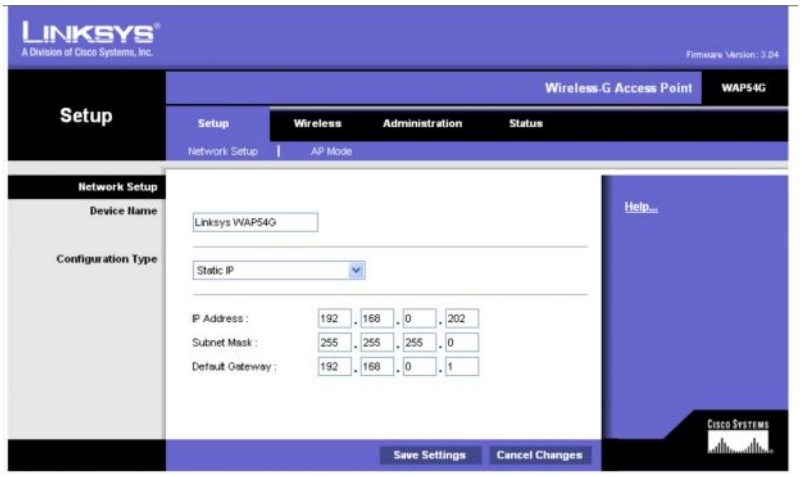


Fig.18 . Configuración del AP.

Luego ingresamos en la pestaña wireless y configuramos el SSID y los canales a utilizar, esto para evitar interferencias.

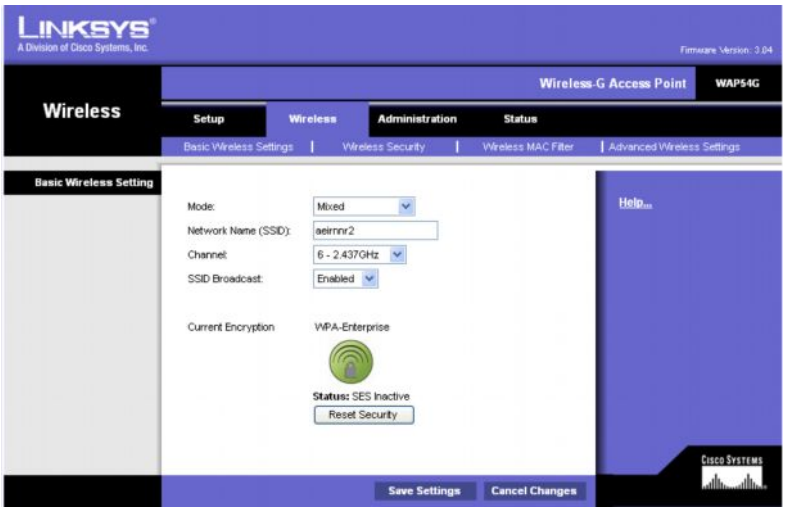


Fig.19 . Configuración del AP.

Ahora vamos a la pestaña de **Wireless Security** y configuramos la dirección IP del servidor, el puerto UDP 1812, la frase secreta especificada en el diseño (tesisaeirnnr1 y tesisaeirnnr2), el modo de seguridad que vamos aplicar WAP-Enterprise

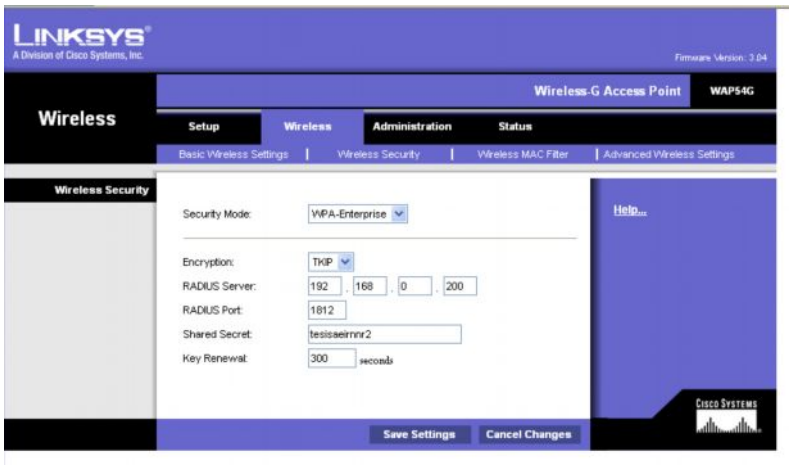


Fig.20 . Configuración del AP.

Hacemos lo mismo para el otro Access Point, con diferente SSID, la frase secreta y la IP.

4.1.2.3. Configuración del Usuario

Para comprobar que todo se ha configurado correctamente, utilizamos un PC Portatil con WI-FI, la prueba consistirá en la conexión de un usuario y su respectiva autenticación en la Red Inalámbrica, por medio de la presentación de su credencial o contraseña, caso contrario no podrá acceder a los recursos de la red.

La computadora portátil se autenticará hacia el servidor Freeradius, para poder hacer uso de la Red Inalámbrica “aeirnnr1”. Esta computadora portátil trabaja bajo el sistema operativo “Windows XP Service Pack 2”, para poder hacer uso de los recursos de la Red Inalámbrica, se configuran algunas opciones de la tarjeta inalámbrica.

Ahora debemos configurar la Conexión Inalámbrica, después de detectar las redes inalámbricas seleccionamos a la que queremos conectarnos, y seleccionamos botón Cambiar configuración avanzada, luego pestaña Redes Inalámbricas.

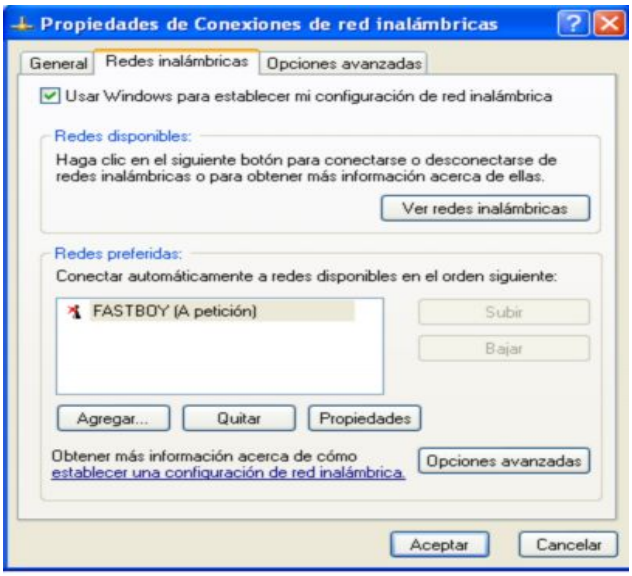


Fig.21. Comprobación de red inalámbrica

Agregamos luego una red, seleccionamos botón "Agregar", colocando los siguientes parámetros para esta nueva red:

SSID = aeirnnr1

Autenticación de Red = WPA

Cifrado de datos = TKIP

Fig.22 . Comprobación de red inalámbrica

En la pestaña autenticación escogemos Tipo de EAP = EAP protegido (PEAP)

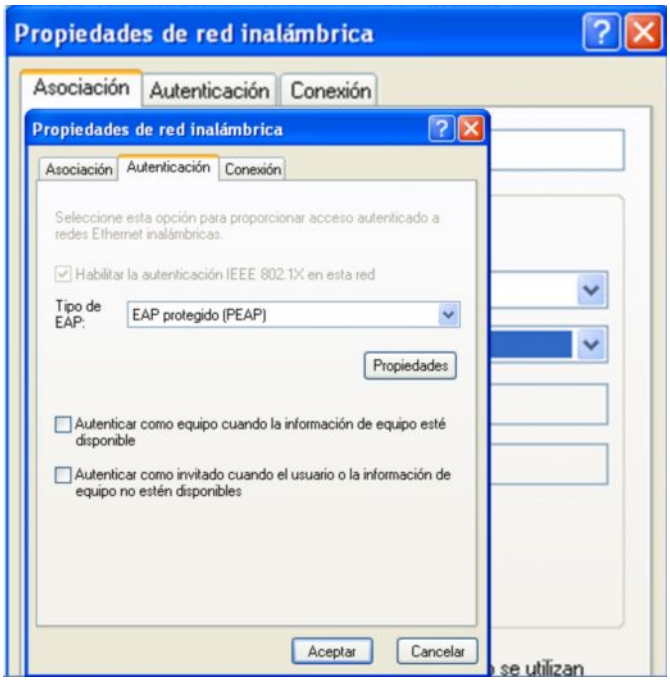


Fig.23 . Comprobación de red inalámbrica

En propiedades de EAP-PEAP, se debe desactivar todas las opciones que aparecen por defecto, puesto que para esta prueba, no hemos hecho uso de ningún tipo de firmas digitales. La configuración deberá quedar como aparece en la figura

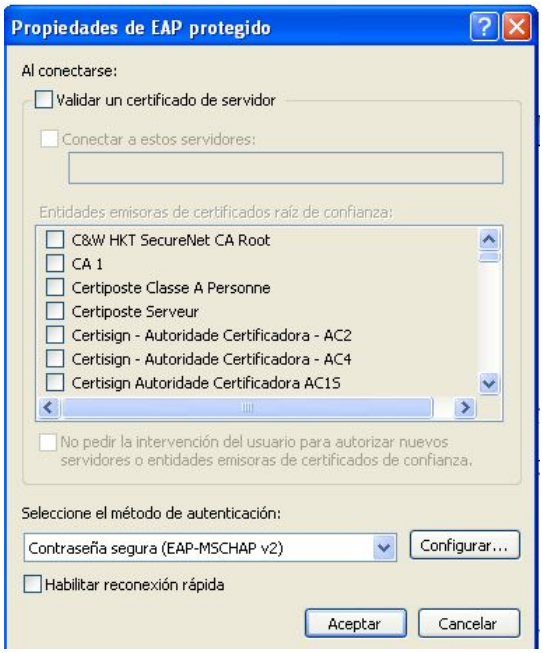


Fig.24 . Comprobación de red inalámbrica

Luego en configurar de Contraseña segura (EAP-MSCHAPV2) desactivamos que nos autentique con el usuario de Windows

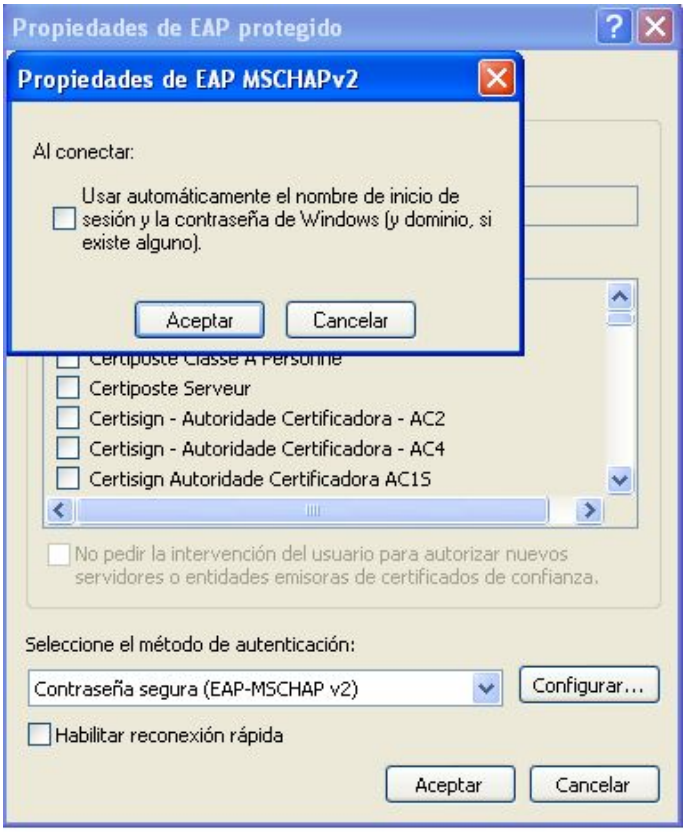


Fig.25 . Comprobación de red inalámbrica

Por último, se debe tener en cuenta que la asignación de dirección IP se realizará de manera automática, por lo que en propiedades del protocolo TCP/IP de la tarjeta inalámbrica se deberá configurar en modo DHCP.

Autenticación de usuarios al sistema.

Se realizó una prueba de autenticación desde una computadora portátil, con las características ya mencionadas, hacia la Red Inalámbrica instalada. El usuario autenticado lleva por nombre de cuenta "estud1" y su respectiva contraseña es "estudiante", pertenece al grupo de usuarios de "estudiantes". Para poder ingresar a la Red Inalámbrica "aeirnnr1", el usuario tendrá que visualizar la red en las "Redes Inalámbricas disponibles" en el sistema operativo :

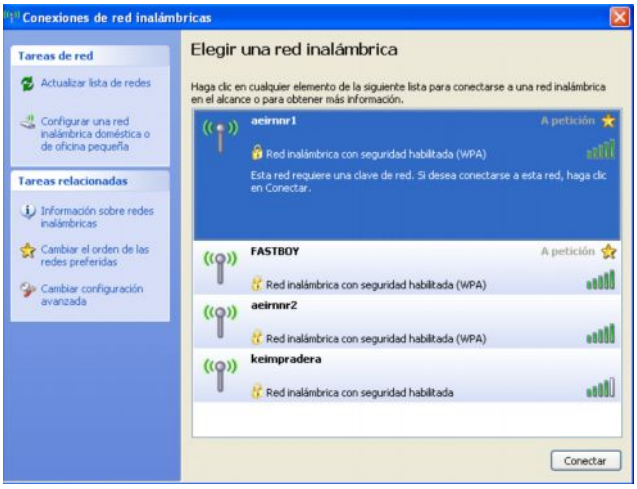


Fig.26 . Prueba de autenticación de red

Luego proceder a ingresar su nombre de usuario y su credencial para acceder a la red.

Fig.27 . Prueba de autenticación de red

Si Radius nos autenticó correctamente nos presentara un mensaje de CONECTADO:

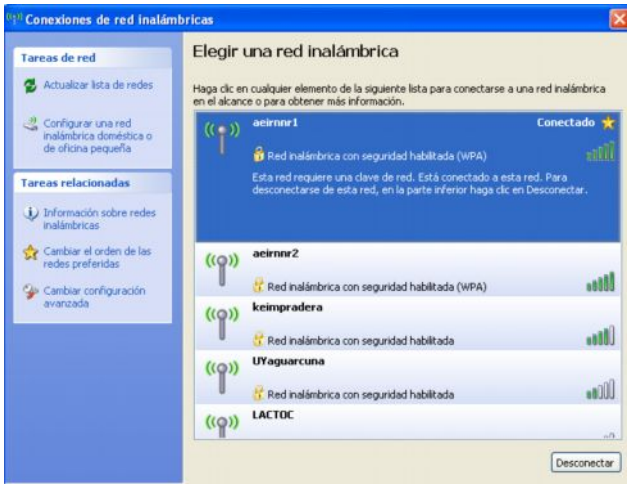


Fig.28 . Prueba de autenticación de red

4.2. PRUEBAS DE VALIDACIÓN

4.2.1. Pruebas Autenticación de Usuarios

En el servidor Freeradius, se necesita abrir un terminal de comandos para poder levantar el servidor en modo "debug" y poder visualizar los resultados de las autenticaciones, esto lo hacemos con el siguiente comando:

 # radiusd –X

Cabe mencionar que el comando "radiusd" debe ser ejecutado en modo administrador, además si toda la instalación y configuración del Servidor se encuentra correctamente hecha, se tendrá un resultado parecido al siguiente:

```
(...)
Module: Instantiated detail (detail)
Module: Loaded radutmp
radutmp:        filename        =
"/var/log/freeradius/radutmp"
radutmp: username = "%{User-Name}"
radutmp: case_sensitive = yes
radutmp: check_with_nas = yes
radutmp: perm = 384
radutmp: callerid = yes
Module: Instantiated radutmp (radutmp)
Listening on authentication *:1812
Listening on accounting *:1813
Ready to process requests.
```

A continuación se muestra el resultado de la autenticación, frente a distintas situaciones:

- El usuario “estud1” ingresó correctamente su nombre y su contraseña. Resultado del servidor:

  Resultado del Servidor:

```
(…)
radius_xlat: 'INSERT into radpostauth (id, user, pass,
reply, date) values ('', 'david',
'Chap-Password', 'Access-Accept', NOW())'
rlm_sql (sql) in sql_postauth: query is INSERT into
radpostauth (id, user, pass,
reply, date) values ('', ' estud1', 'Chap-Password', 'Access-
Accept', NOW())
rlm_sql (sql): Reserving sql socket id: 1
rlm_sql (sql): Released sql socket id: 1
modcall[post-auth]: module "sql" returns ok for request 8
modcall: leaving group post-auth (returns ok) for request 8
Sending Access-Accept of id 8 to 192.168.0.50 port
1142
MS-MPPE-Recv-Key =
0x5c8b5817755dfa71b8d42bfb0281a99873537e5f0a3e92
bc7285e81d8359b3c9
MS-MPPE-Send-Key =
0x43c7e00ff6c88c2c5fe21e570f1715928c2b9961d8834e0
4918888505dbf43d8
EAP-Message = 0x03080004
Message-Authenticator =
0x00000000000000000000000000000000
User-Name = " estud1"
Finished request 8
```

Como se puede observar en el resultado obtenido, el usuario “estud1” fue autenticado satisfactoriamente, al proveer un nombre de usuario y contraseña válidos, esto mediante un Access Accept.

- El usuario “estud1” ingresó correctamente su nombre, pero no así su contraseña.

Resultado del Servidor:

```
(…)
Username = ' estud1' ORDER BY id'
radius_xlat: 'SELECT
radgroupreply.id,radgroupreply.GroupName,radgroupreply.Attribute,r
adgroupre
ply.Value,radgroupreply.op FROM radgroupreply,usergroup WHERE
usergroup.Username = ' estud1' AND usergroup.GroupName =
radgroupreply.GroupName ORDER BY radgroupreply.id'
rlm_sql (sql): Released sql socket id: 1
modcall[authorize]: module "sql" returns ok for request 32
modcall: leaving group authorize (returns updated) for request 32
rad_check_password: Found Auth-Type EAP
auth: type "EAP"
Processing the authenticate section of radiusd.conf
modcall: entering group authenticate for request 32
rlm_eap: Request found, released from the list
rlm_eap: EAP/peap
rlm_eap: processing type peap
rlm_eap_peap: Authenticate
rlm_eap_tls: processing TLS
eaptls_verify returned 7
rlm_eap_tls: Done initial handshake
eaptls_process returned 7
rlm_eap_peap: EAPTLS_OK
rlm_eap_peap: Session established. Decoding tunneled attributes.
rlm_eap_peap: Received EAP-TLV response.
rlm_eap_peap: Tunneled data is valid.
rlm_eap_peap: Had sent TLV failure. User was rejcted rejected
earlier in this
session.
rlm_eap: Handler failed in EAP/peap
rlm_eap: Failed in EAP select
modcall[authenticate]: module "eap" returns invalid for request 32
modcall: leaving group authenticate (returns invalid) for request 32
auth: Failed to validate the user.
Delaying request 32 for 1 seconds
Finished request 32
```

Como se puede observar en esta prueba, el usuario no pudo ingresar a la Red Inalámbrica, por proveer una incorrecta contraseña.

- La cuenta del usuario “estud1” fue borrada, y se procede a autenticar con usuario y contraseña válidos anteriores.

Resultado del Servidor:

```
usergroup.GroupName = radgroupreply.GroupName ORDER BY
radgroupreply.id'
rlm_sql (sql): User estud1 not found in radgroupcheck
rlm_sql (sql): Released sql socket id: 1
rlm_sql (sql): User not found
modcall[authorize]: module "sql" returns notfound for request 24
modcall: leaving group authorize (returns updated) for request 24
rad_check_password: Found Auth-Type EAP
auth: type "EAP"
Processing the authenticate section of radiusd.conf
modcall: entering group authenticate for request 24
rlm_eap: Request found, released from the list
rlm_eap: EAP/peap
rlm_eap: processing type peap
rlm_eap_peap: Authenticate
rlm_eap_tls: processing TLS
eaptls_verify returned 7
rlm_eap_tls: Done initial handshake
eaptls_process returned 7
rlm_eap_peap: EAPTLS_OK
rlm_eap_peap: Session established. Decoding tunneled attributes.
rlm_eap_peap: Received EAP-TLV response.
rlm_eap_peap: Tunneled data is valid.
rlm_eap_peap: Had sent TLV failure. User was rejcted rejected earlier
in this
session.
rlm_eap: Handler failed in EAP/peap
rlm_eap: Failed in EAP select
modcall[authenticate]: module "eap" returns invalid for request 24
modcall: leaving group authenticate (returns invalid) for request 24
auth: Failed to validate the user.
Delaying request 24 for 1 seconds
Finished request 24
Going to the next request
Waking up in 6 seconds...
rad_recv: Access-Request packet from host 192.168.0.50:1146, id=7,
length=243
Sending Access-Reject of id 7 to 192.168.0.50 port 1146
EAP-Message = 0x04070004
Message-Authenticator = 0x00000000000000000000000000000000
```

En el ejemplo anterior, se puede observar que si un usuario no se encuentre registrado en la base de datos de la Red Inalámbrica no podrá acceder a usar los recursos de la red.

4.2.2. Análisis de la encuesta

Se aplicó una encuesta (anexo 1) a siete paralelos de las diferentes carreras del área: Ingeniería de Sistemas, Ingeniería en Geología Ambiental, Ingeniería Electromecánica, el total de encuestados es de 127. De la aplicación de esta encuesta da fe uno de los docentes de la carrera de Ingeniería de Sistemas (anexo 2), esta actividad se llevó a cabo el 22, 23 de marzo del 2010 en las aulas universitarias. La aplicación de ésta encuesta nos permitió conocer el número aproximado de los usuarios de la WLAN, y horario de mayor concurrencia a la red.

2.1. ¿Tiene usted conexión a Internet, en el campus del A.E.I.R.N.N.R.?

RESPUEST	FREC	PORCENTAJE
SI	78	61.42%
NO	47	37.01%
NO CONTESTA	2	1.57%
TOTAL	127	100%

Cuadro No 1: Conexión a Internet en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

Grafico No 1

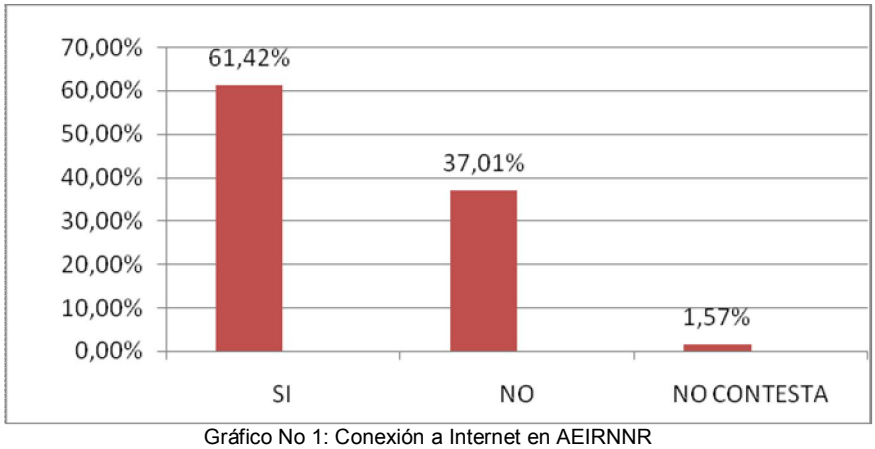


Gráfico No 1: Conexión a Internet en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

Interpretación:

De acuerdo a la gráfica se puede decir que el 61,42% de los estudiantes, es decir en su mayoría tienen acceso al internet del Área, en lugares como la biblioteca, laboratorios, los patios del bloque 3, Feue, el bloque donde funciona la coordinación y el edificio central, estos lugares corresponden a los Bloques I y III, el 37%, señala que no tiene acceso a internet. Un 1.57% no contesta a la interrogante.

2.2. ¿Indique con qué medio se puede conectar a Internet en el campus del AEIRNNR?

RESPUEST	FREC	PORCENTAJE
Inalámbrico	80	62.99%
Cable	27	21.26%
Dos	14	11.02%
NO CONTESTA	6	4.73%
TOTAL	127	100%

Cuadro No 2: Medios de Conexión a Internet en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

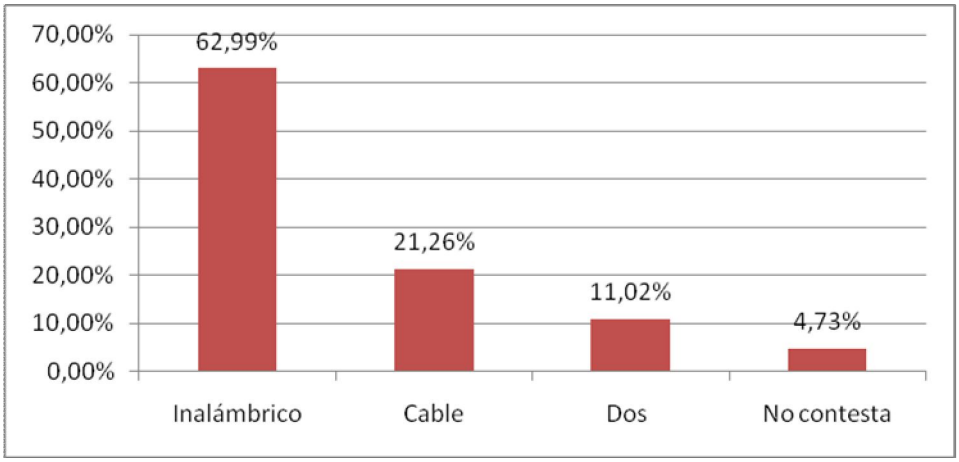


Gráfico No 2: Medios de Conexión a Internet en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

Interpretación:

El 62,99% accede al internet por medio inalámbrico, un 21,26% lo hace por medio de cable, disponible en los centros de cómputo del Área, un 11.02%, manifiesta hacer uso de los dos medios de acceso y un 4,73% no contesta. De acuerdo a estos datos en su mayoría los estudiantes se conectan por medio inalámbrico, en ciertos lugares donde hay señal.

2.3. Si se conecta por medio inalámbrico, por favor indique el horario y el lugar en el cual lo hace.

RESPUEST	FREC	PORCENTAJE
Mañana	30	37,5%
Tarde	16	20,0%
Mañana y tarde	14	17,50%
No contesta	20	25,00%
TOTAL	80	100.00%

Cuadro No 3: Horario de Conexión a Internet inalámbrico en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

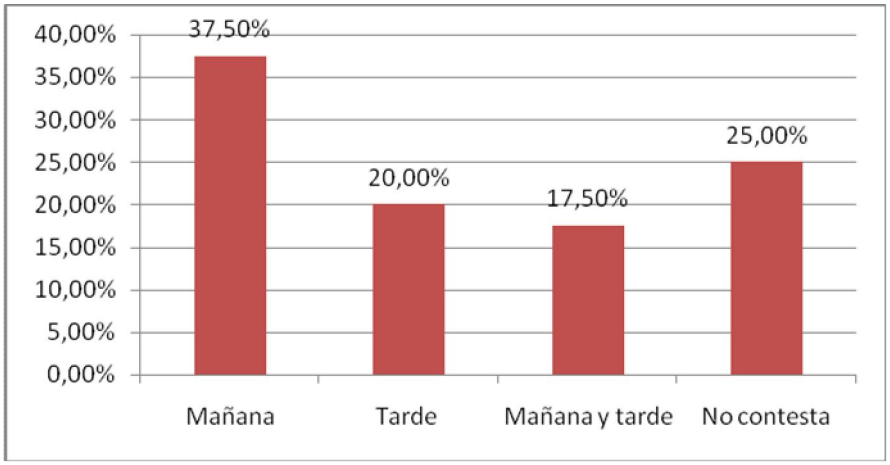


Gráfico No 3: Horario de Conexión a Internet inalámbrico en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

Interpretación:

De los encuestados que respondieron que se conectan por medio inalámbrico, el 37,50% manifiesta que navegan en la mañana, es decir aproximadamente 460 usuarios, un 20% lo hace en la tarde, el 17,50% lo hace en ambos horarios, y un 25% no contesta, de este resultado podemos decir que en el horario de la mañana hay mayor concurrencia al uso del internet.

También se pregunto en este ítem en que lugares se efectuaba la conexión, dando como resultado el lugar más concurrido la biblioteca y el edificio donde está de la asociación de carrera.

En cuanto a la hora más concurrida de uso del internet es de 9 a 10 de la mañana, un 25% del total usuarios.

2.4. ¿Qué medio de conexión le parece más adecuado?

RESPUEST	FREC	PORCENTAJE
INALÁMBRICO	125	98.43%
CABLE	2	1.57%
TOTAL	127	100.00%

Cuadro No 4: Medio de conexión más adecuado en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

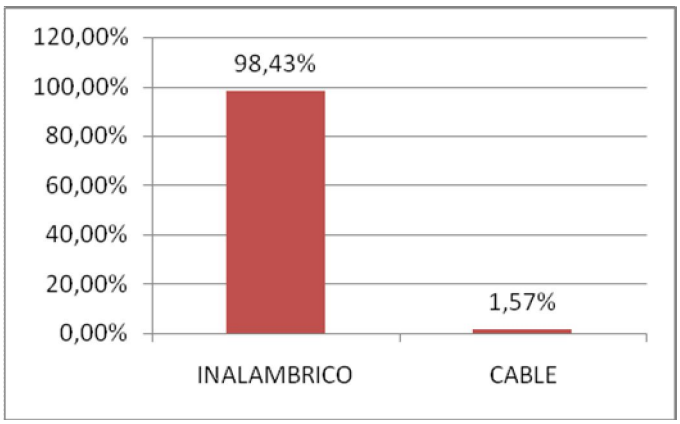


Gráfico No 4: Medio de conexión más adecuado en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

Interpretación:

Podemos visualizar que el 98,43%, casi la totalidad de los encuestados, están de acuerdo en que el medio inalámbrico para conexión a internet es el más adecuado, únicamente

un 1,57% se inclina por la conexión mediante cable. Además expresan el porqué de su respuesta, señalamos desde la de mayor acogida como es la facilidad de conectarse, seguida de la comodidad, la movilidad que pueden tener, poder navegar sin límite de tiempo, facilidad debido a que poseen portátil, pueden conectarse rápidamente, satisfacer la necesidad del servicio de internet, la independencia, lo saturado de la biblioteca, la economía de recursos al no tener que gastar en cybers, y estar a la par con la innovación tecnológica.

2.5. ¿Cree usted que es necesario la implementación de una red inalámbrica en el campus del A.E.I.R.N.N.R. que le permita conectarse a Internet?

RESPUEST	FREC	PORCENTAJE
SI	127	100.00%
NO	0	0.00%
TOTAL	127	100

Cuadro No 5: Necesidad de implementar una WLAN en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

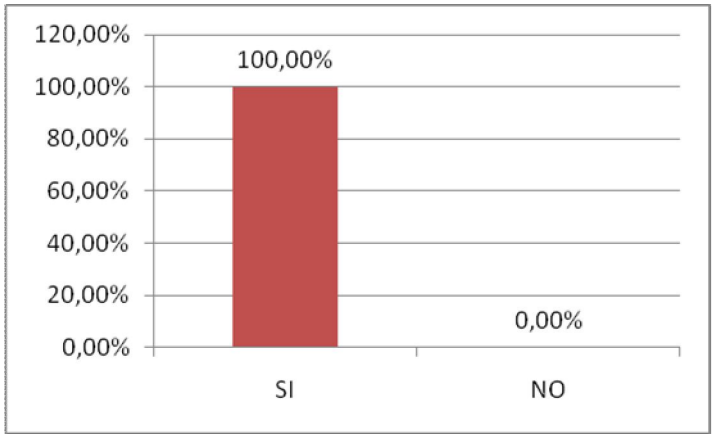


Gráfico No 5: Necesidad de implementar una WLAN en AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

Interpretación:

Como es lo más lógico el 100% de los encuestados manifiesta la necesidad de una red inalámbrica en el Área, que le permita conectarse al internet. Esto por razones tales como posibilidad de mejorar el proceso de aprendizaje al poder consultar en cualquier

momento temas de interés para el estudio, la facilidad de acceder desde cualquier lugar del campus del Área, el espacio de la biblioteca no es suficiente para poder tener acceso todos al internet la WLAN ayudaría a descongestionar la biblioteca, entre otras.

2.6. ¿Tiene Ud. computador portátil para conexión inalámbrica en el campus del A.E.I.R.N.N.R. que le permita conectarse a Internet?

RESPUEST	FREC	PORCENTAJE
SI	49	38,58%
NO	55	43,30%
NO CONTESTA	23	18.12%
TOTAL	127	100.00%

Cuadro No 6: Posee una portátil para conexión a WIFI en el AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

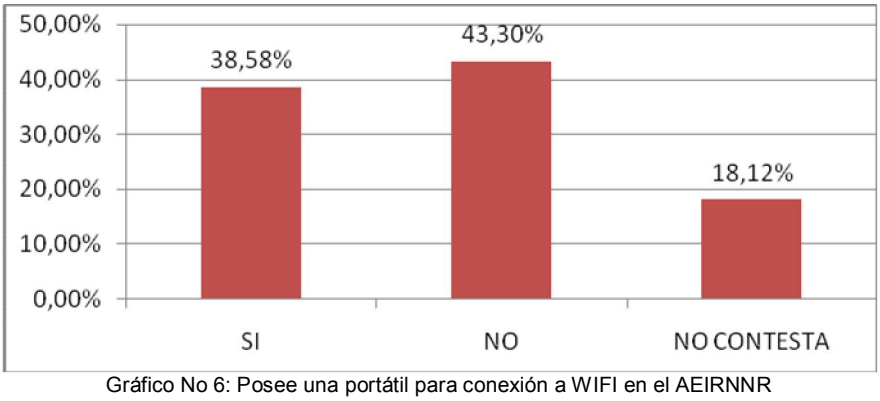


Gráfico No 6: Posee una portátil para conexión a WIFI en el AEIRNNR
Fuente: encuestas aplicadas a los estudiantes del AEIRNNR

Interpretación:

En cuanto a quienes tienen un computador portátil que le permita conectarse a internet mediante inalámbrico, tenemos que un 38,52% si dispone de una portátil, mientras que un 43,30% no posee y un 18,12% no contesta la interrogante.

5. METODOLOGÍA

La presente investigación ha sido desarrollada en base a las siguientes etapas:

- Análisis y determinación de requerimientos
- Diseño
- Implementación

Para obtener la información necesaria utilizamos instrumentos de investigación como son: encuesta, entrevista y visitas para observación del sitio.

Este trabajo se inició con la etapa de análisis para la determinación de requerimientos, para ello se aplicó una entrevista (anexo 3), que nos permitió conocer cómo se da la conexión y administración del servicio de internet al Área. Además mediante observación del lugar se conoció la distribución e infraestructura de los edificios existentes y su tipo de construcción.

Se aplicó una encuesta (anexo1), que permitió conocer la situación actual de los estudiantes con respecto al servicio de internet que posee el Área, y la acogida de la futura red inalámbrica que se implantará, además se pudo conocer el número aproximado de usuarios que tendrá la WLAN.

En base a un estudio de las características de los equipos necesarios y sus configuraciones, a través de consultas de internet, a profesionales y proveedores de equipos, se seleccionó los puntos de acceso a utilizar.

El conocimiento de esta información nos permitió tomar decisiones acerca de las características de la red y el cumplimiento de nuestros siguientes objetivos como son el diseño e implantación de la red inalámbrica.

En la etapa de diseño se consideró el diseño de la red inalámbrica tanto físico, como lógico, y el diseño de las seguridades que se aplicará para controlar los accesos a la red. Para esto se hizo un estudio del software que utilizaremos como sistema operativo es decir CENTOS, el software para el control de accesos en este caso Freeradius, y aquellas aplicaciones que se debían instalar para manejar la base de datos como es Phpmyadmyn, también se decidió la utilización de Mysql como base de datos para almacenar los usuarios y sus claves respectivas.

Una vez terminada la etapa de diseño, continuamos con la implementación de la red inalámbrica, en esta etapa se tuvo que poner en práctica todo lo investigado, ejecutar lo definido en la etapa de diseño en cuanto a la instalación de hardware y software necesario y poner a prueba el conjunto de elementos configurados para que la red inalámbrica quede en funcionamiento.

6. EVALUACIÓN DEL OBJETO DE TRANSFORMACIÓN

En busca del cumplimiento de los objetivos planteados en el Proyecto de Investigación, los cuales dicen lo siguiente:

1. Realizar el análisis y determinación de requerimientos para la implementación de una Red Inalámbrica Local (WLAN), en el campus de los bloques de el A.E.I.R.N.N.R

2. Efectuar el Diseño de la Red Inalámbrica Local (WLAN) en base a los requerimientos obtenidos.

3. Realizar un control de accesos a la WLAN aplicando el protocolo de autenticación RADIUS.

Hemos ido desarrollando las etapas de la investigación detalladas anteriormente en la metodología.

El 1er objetivo denominado **Realizar el análisis y determinación de requerimientos para la implementación de una Red Inalámbrica Local (WLAN), en el campus de los bloques de el A.E.I.R.N.N.R**, se logró cumplir realizando actividades básicas de recolección de información como entrevistas, encuesta (anexo1) y observación del lugar, dentro de lo que es la primera etapa de la investigación Análisis y determinación de requerimientos.

ETAPAS 1: ANÁLISIS Y DETERMINACIÓN DE REQUERIMIENTOS PARA LA IMPLANTACIÓN DE UNA RED WLAN EN EL AEIRNNR

En esta etapa de análisis se delimitó el área que cubrirá la red WLAN a implementar, misma que consta del área externa a todos los edificios que conforman el AEIRNNR de la Universidad Nacional de Loja.

El objetivo principal para el cual se crea esta red es el de proporcionar acceso controlado inalámbrico a internet para los estudiantes, que les permita realizar sus

investigaciones por medio del mismo, desde cualquier lugar externo del campus del área dentro de la UNL.

El Área de la Energía, la Industria, los Recursos Naturales no Renovables de la Universidad Nacional de Loja (A.E.I.R.N.N.R), está ubicada en la ciudadela la Argelia, aquí se tenemos las carreras de Ingeniería en Sistemas, Ingeniería en Electromecánica, Ingeniería en Geología Ambiental y Ordenamiento Territorial, Tecnología en Electricidad, Tecnología en Electrónica y las Carreras Artesanales de Técnicas Constructivas, Técnicas Eléctricas, Mecánica Automotriz y Técnicas en Audio y Video, consta de 6 bloques organizados de la siguiente manera:

Bloque I: Administración Central,
Bloque II: Geología y Minas, Aulas,
Bloque III: Aulas, Asoc. Carrera
Bloque IV: Secretaria General
Bloque V: Biblioteca, Nivel Técnico, Posgrado, Aula Magna
Bloque VI: Taller de Mantenimiento de Computadoras.

Los bloques están conformados de la siguiente forma:

No.	Nombre	# de pisos
1	Bloque 1	1
2	Bloque 2	1
3	Bloque 3	2
4	Bloque 4	1
5	Bloque 5	3
6	Bloque 6	3

El espacio físico consta de 3680m2 aproximadamente.

GRAFICO DEL AREA

La Universidad Nacional de Loja posee el servicio de internet, el mismo que llega hacia el AEIRNNR por medio de fibra óptica desde la Jefatura de Informática de la Administración Central, que es quien administra los ISP hacia el resto de la universidad, ésta se distribuye a los bloques a través de un switch 3com, todos los bloques se enlazan a través de la fibra óptica distribuyéndose a su vez por medio de un switch a cada computador, la señal es controlada por medio un servidor que hace las veces de proxy y de control de contenido. Existen sitios donde hay internet inalámbrico como la Biblioteca, Laboratorios, Asociación de. Carrera, Coordinación y edificio de administración, sitios que pertenecen a los Bloques I y III, pero la conexión se dá con ciertas.

El área tiene 1210 estudiantes y 70 docentes, distribuidos en las diferentes carreras anteriormente señaladas. De acuerdo a nuestra investigación mediante encuestas pudimos conocer que el 38% de los estudiantes de esta Área, es decir aproximadamente 460 usuarios, poseen computador portátil propio y por lo tanto podrían acceder libremente a la red inalámbrica, éste constituye el número de usuarios de la red que vamos a implementar (anexo 2).

El servicio de internet es más concurrido en el horario de 7am a 13pm, esto desde los lugares cercanos donde puede obtenerse la señal.

Un punto importante en cuanto a las WLAN es la seguridad, existen análisis que han evaluado las opciones a escoger para proteger las comunicaciones, nosotros hemos escogido el uso del estándar 802.1X-EAP, por las ventajas que se expuso anteriormente, pero principalmente porque permite cualquier tipo de encriptación a necesidad como WEP, TKIP, AES u otro estándar de encriptación para redes inalámbricas. Además el estándar 802.1x funciona en conjunto con otros estándares como lo son EAP y RADIUS. El estándar 802.1x es solo el mecanismo que deniega cualquier tipo de tráfico hacia la red, excepto paquetes de tipo EAP. Una vez que el protocolo EAP reconoce como válido a un usuario, el estándar 802.1x avisa al punto de acceso para que permita el tráfico al usuario validado.

Funcionalidad, Seguridad y requerimientos técnicos

Para diseñar una red debemos tener claro el tipo de usuario, esto nos permitirá definir las características de la WLAN. Como se señaló anteriormente se trata de usuarios previamente autorizados que puedan navegar en internet.

También debemos señalar que de acuerdo a la funcionalidad requerida en esta red WLAN, puede ser recomendable aislar de manera segura el segmento de acceso inalámbrico y así se puede implementar mecanismo de autenticación no tan robusto.

La **funcionalidad** de la WLAN a implementar, consiste en ofrecer servicio de acceso a la red pública Internet para navegar, destinado a los estudiantes de la UNL del AEIRNNR, asignándose un segmento de acceso inalámbrico controlado por un firewall, donde las políticas de este solo permiten tráfico http a los equipos conectados a ciertas direcciones IP asignadas. De acuerdo a esta funcionalidad, podemos decir que la **seguridad requerida** consiste en una autenticación basada en usuario y contraseña.

La segmentación del acceso inalámbrico es un asunto que ya corresponde a quienes administran las ISP, nuestro trabajo llega hasta controlar el acceso al servicio de internet mediante un usuario y contraseña.

Requerimientos Técnicos

En cuanto a los requerimientos técnicos, para la implantación de esta WLAN vamos a utilizar el protocolo 802.1x y en base a esto vamos a seleccionar los componentes necesarios para esta red.

En Usuarios:

Debemos tomar en cuenta si las plataformas utilizadas por los clientes, soportan el tipo de autenticación elegido o si por el contrario requieren de un componente de software que los habilite para realizarla. Los sistemas operativos de Windows XP, 2000, Vista

poseen la capacidad de conectarse a la red sin la necesidad de un software adicional, mientras que Linux, MACOS y Windows Seven deben tener una certificación para poder acceder al servidor RADIUS.

En el Access Point

• Estándares de trabajo: Se debe tomar en cuenta los estándares los cuales el punto de acceso soporta, en la mayoría de casos 802.11b, 802.11g ó 802.11a .

• Potencia de transmisión. Un factor determinante en la elección de un punto de acceso es la potencia de transmisión del equipo, la cual garantiza una mayor zona de cobertura, no está demás mencionar que un equipo más potente es más costoso. Los equipos actuales garantizan una potencia desde unos 18 milivatios a 200 milivatios.

• Equipo para interiores o exteriores. Revisar de acuerdo a la necesidad si es para interior o exterior. Generalmente los equipos para exteriores son mucho más costosos que los diseñados para interiores, pero si se le provee de una caja de protección, un equipo interior podrá colocarse afueras sin inconveniente.

• Tipo de Antena. La antena para el diseño de la Red Inalámbrica puede ser de distintos tipos dependiendo el uso para el cual se aplica. Existen antenas omnidireccionales las cuales poseen un patrón de radiación uniforme en toda dirección. También se encuentra las antenas dipolos, cuyo patrón de radiación es no uniforme y de menor área de cobertura que las omnidireccionales; cabe mencionar que por lo general son las antenas que vienen con la mayoría de puntos de acceso en el mercado.

• Seguridad. Se debe tomar en cuenta los estándares de seguridad soportados por los puntos de acceso. Actualmente la mayoría de puntos de acceso soportan estándares de encriptación y autenticación como protocolos WEP, WPA, WPA-2, 802.1x, TKIP, AES, entre otros, pero son pocos los puntos de acceso que pueden soportar el emergente estándar 802.11i.

• Al diseñar la Red Inalámbrica se deberá tener presente el costo de los equipos, pues los equipos que posean mejores características tendrán un costo mayor que otros más simples.

En el servidor:

Los principales requerimientos de este componente, para que permita implementar la solución de seguridad basada 802.1x son:

- Compatibilidad con 802.1x
- Soporte de diversos tipos de autenticación EAP (tls, ttls y PEAP)
- Capacidad de registro o Accounting
- Soporte para control de acceso para redes inalámbricas
- Flexibilidad para validar los suplicantes, mediante varios métodos, bases de datos, usuarios locales, directorio de usuarios LDAP, certificados, entre otros.
- Capacidad de integración con otros servicios de red.

ETAPA 2: DISEÑO DE LA RED INALÁMBRICA PARA EL A.E.I.R.N.N.R (WLAN)

Esta etapa nos ha permitido cumplir el segundo objetivo denominado: **Efectuar el Diseño de la Red Inalámbrica Local (WLAN) en base a los requerimientos obtenidos,** para ello elaboramos un diseño físico, lógico y de seguridad de la red inalámbrica.

Las siguientes son características con las cuales debería contar la red inalámbrica y que debemos tener en cuenta en el diseño:

- Autenticación sólida de cliente inalámbrico. Esto debe incluir la autenticación mutua del cliente, el punto de acceso (PA) inalámbrico y el servidor RADIUS.
- Un proceso de autorización para que solamente permita el acceso de red a clientes autorizados.
- Cifrado eficaz del tráfico de la red inalámbrica.
- Administración segura de las claves de cifrado.
- Resistencia a los ataques de denegación de servicio (DoS).

Como ya mencionamos anteriormente, el estándar 802.1x escogido para el control de acceso a la red, en combinación con el método de autenticación segura como EAP, nos permite cumplir con la mayoría de estos requisitos. El estándar WPA constituye un gran paso hacia la seguridad de WLAN y cuenta con el respaldo de la mayoría de los analistas y proveedores, ninguna de las mejoras de WPA se ocupa de los problemas de denegación de servicio inherentes a 802.11 y 802.1X. Pero debemos señalar que estas debilidades no representan un problema tan grave como los otros fallos de WEP, que por un lado brinda un cifrado seguro del tráfico de red pero ofrece un nivel de administración de claves deficiente. La mayoría de los ataques de denegación de servicio demostrados causan únicamente una disrupción temporal en la red.

2.1. Diseño físico de la WLAN

El diseño físico está dado por la ubicación física de cada uno de los puntos de acceso, para esto se ha tomado en cuenta principalmente la estructura de los edificios del AEIRNNR, los mismos que están construidos de concreto y se encuentran alineados a un solo lado del sitio, el área que se desea cubrir que en base a la información obtenida es de 3680m^2. Los sitios para la ubicación de los Access Point se situaron mediante un GPS, con la finalidad de tener precisión del lugar.

También como parte del diseño físico hemos incluido la elección del Access Point y las características que tendrá el servidor.

Selección del Access Point

No es fácil tomar la decisión de qué Access Point elegir, pues existe un sinnúmero de marcas y cientos de modelos.

Tenemos dos grupos de AP, el primer grupo de Access Point "Robustos", que son aquellos que incluyen varias funciones y wireless software muy potentes que permiten diversas configuraciones y que, por ejemplo, serán fáciles de actualizar cuando sea el momento, pero con un precio alto y el segundo grupo de los "Básicos" o "Delgados" que tiene un bajo costo, pero de igual manera sólo traen una antena y el driver necesario para su configuración. Los hay del estándar 802.11b/g, del estándar 802.11a y últimamente del estándar 802.11n. Hay algunos que incorporan muchas funciones para la seguridad wifi o para la gestión de la red inalámbrica, éste aspecto es importantísimo de considerar, ya que existen Puntos de Acceso de muy bajas prestaciones, (generalmente, no de la última generación) que no soportan el estándar de seguridad 802.1x de la IEEE y que no permiten, por supuesto, la autenticación y autorización del usuario. Estos equipos no son capaces de enviar peticiones a servidores RADIUS, según lo requiere dicho estándar. Además, en la actualidad hay que verificar también que soportan WPA.

Se debe evaluar la relación **precio/prestaciones** pues debemos tomar en cuenta que si necesitamos varias decenas o centenas de puntos de acceso inalámbricos, el costo sería elevado. Entonces es conveniente utilizar un Access Point que esté en cuanto a precio en un término medio, pero que cumpla básicamente con los requerimientos que nos permitan utilizar, específicamente el protocolo **802.1x**, el soporte de **WPA**, los estándares **80211a, 802.11b y 802.11g** como mínimo, y la utilización de **RADIUS.**

En base a estas consideraciones y tomando en cuenta la relación precio/prestaciones se ha evaluado algunos modelos de productos disponibles en nuestro mercado y nos inclinamos por el Access Point de marca LinkSys, modelo WAP54G versión 3.1, ya que éste permite el protocolo 802.1x, soporte WPA, RADIUS, y su precio es aceptable tomando en cuenta la posibilidad de incrementar el número de AP a futuro.

Especificaciones Técnicas del Access Point:

Estándares: IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u
Tipo de cables: Categoría 5 (con conectores RJ-45)
Potencia de transmisión: 802.11g: Habitualmente 13,5 +/- 2 dBm a temperatura normal, 802.11b: Habitualmente 16,5 +/- 2 dBm a un intervalo de temperatura normal
Funciones de seguridad: WPA, Linksys Wireless Guard (disponible sólo en EE. UU. y Canadá), encriptación WEP, filtrado de direcciones MAC, activación/desactivación de difusión de SSID. Compatible con estándar 802.1x.
Bits de clave WEP: 64/128 bits
Precio: 150,00. **Certificación**: FCC, CE, Wi-Fi

Características clave

IEEE 802.11g admite velocidades de transferencia de datos de hasta 54 Mbps
Compatible con versiones anteriores de los dispositivos IEEE 802.11b existentes
Admite seguridad WPA y encriptación WEP de 64/128 bits
Interfaz de usuario web incorporada, configuración sencilla desde cualquier explorador web
Firmware actualizable mediante explorador web

Admite las funciones de puente inalámbrico, repetidor inalámbrico, filtrado de direcciones MAC y registro de sucesos

Fig.29 . Access Point Marca Linksys Modelo WAP54g

Una vez definido el tipo de AP a utilizar debemos conocer cuántos son necesarios para satisfacer la demanda actual de usuarios, esto lo podemos conocer con la aplicación de la siguiente fórmula.

Fórmula para Calcular Cantidad de Access Point necesarios:[18]

$$\frac{\text{Ancho de Banda x N° de Usuarios x \% utilización}}{\textit{Velocidad Programada}}$$

Ancho de banda: el necesario de acuerdo al perfil del usuario
Número de usuarios: número de usuarios de la red
% utilización: porcentaje de uso de la red

El ancho de banda de acuerdo al perfil de usuario de la WLAN de el AEIRNNR es de 262,40 Kbps por cada conexión, hemos obtenido este valor tomando en cuenta un estudio hecho en nuestro país por parte de la DGAC (Dirección General de Aviación Civil), en usuarios de los aeropuertos considerando el uso de Internet 32 Kbps, Correo Electrónico 19,2 Kbps, videoconferencia 192 Kbps y transferencia de archivos (FTP) 19,2. Debemos señalar que este ancho de banda sería lo mínimo que necesita el usuario.

262,40Kbps/1024 = 0,2624 Mbps

[18] Curso de Redes Inalámbricas. Conceptos Básicos de Tecnología WIFI y Best Practices de Seguridad en Redes Inalámbricas. [http://www.virusprot.com/cursos/Redes-Inalámbricas-Curso-gratis6.htm#Cobertura-Redes-Wifi]

Tomando en cuenta los datos anteriores el ancho de banda necesario para la red inalámbrica de AEIRNNR seria de 30 Mbps.

El número de usuarios de la red WLAN fue obtenido en base a la aplicación de una encuesta (anexo 1), a una muestra de los usuarios de la universidad, lo cual nos permitió determinar que 460 es el número de usuarios de la red. Y también nos permitió conocer la hora de mayor concurrencia para el uso del servicio de internet, siendo de 9 a 10 am, con un 30 % de usuarios conectados, siendo éste el porcentaje de uso de la red en una hora pico.

En cuanto a la velocidad programada lo vamos a hacer tomando en cuenta los 11Mbps que permite el estándar 802.11b, que es el que utilizaremos.

$$\frac{0{,}2624\text{Mbps x500 x 0.30\%}}{25{,}45\ Mbps} = 1{,}55\ \text{AP}$$

2 Access Point

Proyección de la Capacidad

La proyección del ancho de banda dentro de 10 años seria de 360 Mbps. Esta proyección fue calculada, en base al crecimiento del tráfico de internet que se ha dado en los últimos 10 años el cual es de 1211%, obtenido de estudios estadísticos hechos por Internet Word Start para Ecuador, dando un crecimiento por año promedio de 120%

A continuación tenemos un esquema de la distribución del área, los edificios que la componen y señalamos los lugares adecuados para ubicar los Puntos de acceso.

Los requerimientos básicos del hardware para el servidor son los siguientes: procesador Pentium IV, 256 RAM, HD 40GB, Lector de CD, tarjeta de red, monitor, teclado, mouse. En cuanto a los requisitos de software tenemos: Linux CENTOS 5, Mysql, PHP, Apache, PHPMyAdmyn, Freeradius, librería de conexión FreeRadius-Mysql, cortafuegos.

2.2. Diseño Lógico de WLAN

El diseño lógico de la Red Inalámbrica está enfocado hacia dos puntos básicos, la topología y la configuración.

La topología a utilizar es la de modo infraestructura, pues estamos empleando Access Point, ésta topología permite utilizar varios AP para tener mayor cobertura en la red.

En los puntos de acceso:

Los puntos de acceso deberán configurarse en los siguientes canales:

El punto de acceso **AEIRNNR1** deberá configurarse en el canal 6, y el segundo punto de acceso **AEIRNNR**2, deberá configurarse para trabajar en el canal 11; de esta manera se reduce la posible interferencia que pueda causar entre los dos puntos. Además los puntos de acceso llevarán la siguiente configuración de direccionamiento:

Punto de acceso AEIRNNR 1:
IP estático: 192.168.0.201/24
Palabra secreta: tesisaeirnn1
SSID broadcast: aeirnnr1
Security Mode: WPA-Enterprise
Encriptyon: TKIP
Radius Server: 192.168.0.200
Radius Port: 1812

Punto de acceso AEIRNNR 2:

IP estático: 192.168.0.202/24

Palabra secreta: tesisaeirnn2

SSID broadcast: aeirnnr2

Security Mode: WPA-Enterprise

Encriptyon: TKIP

Radius Server: 192.168.0.200

Radius Port: 1812

La puerta de enlace, será configurada con la dirección asignada por el administrador de la red del Área.

En el servidor:

Vamos a utilizar un servidor RADIUS, esto debido a que contempla el estándar 802.1x básico para la seguridad de las redes inalámbricas. Además gracias a su característica de Autenticación se puede determinar si un usuario tiene permiso para acceder a un determinado servicio de red del que quiere hacer uso. La autenticación se realiza mediante la presentación de una identidad, en este caso el usuario y su contraseña.

Otra característica es la Autorización, ésta se refiere a conceder o no servicios específicos a un determinado usuario, basándose para ello en su identificación, los servicios que está solicitando, y el estado actual del sistema.

Finalmente el Registro (accounting) que permite realizar un registro del consumo de recursos que realizan los usuarios.

RADIUS, nos permite la autenticación en redes inalámbricas (Wi-Fi), sustituyendo métodos más simples de clave compartida (pre-shared key, PSK), que son bastante limitados al gestionar una red cuando ésta alcanza un determinado tamaño.

Además se recomienda RADIUS, cuando se necesita proporcionar un servicio de acceso centralizado, no solo para gestionar el acceso a la propia red, sino también para servicios propios de Internet.

Otros programas adicionales a Freeradius, que instalaremos son Mysql para almacenar la información de los usuarios y nos valdremos de Phpmyadmin para tener un interfaz gráfico con la base de datos.

2.3. Diseño de Seguridad

La seguridad en las redes inalámbricas es un tema de suma importancia, esto debido a que puede ser detectada y accedida con facilidad, pues su medio de transmisión es el aire. Cualquier persona con una computadora portátil puede encontrar el punto de acceso inalámbrico de la red inalámbrica, pudiendo así ingresar en nuestros archivos, utilizar nuestra conexión a internet, obtener datos importantes que se transfieran en la red inalámbrica, etc.

El protocolo de autenticación para garantizar la seguridad de la WLAN para el AEIRNNR seleccionado es el protocolo 802.1x con el método de autenticación EAP-PEAP (mayoría de usuarios tiene S.O. Windows) y WPA como mecanismo de cifrado.

2.3.1. WPA - Wi-Fi Protected Access

El protocolo WPA ha sido elegido para el trabajo entre los clientes de la red inalámbrica y el Punto de Acceso, debido a que implementa un nivel de seguridad mayor que el protocolo WEP puede ofrecer; además de ser un protocolo aprobado por la institución de estandarización Alianza Wi-Fi, es un protocolo que es implementado por diversas marcas y modelos de Access Point y sistemas operativos en las computadoras clientes de la red inalámbrica.

El protocolo WPA provee una seguridad más robusta que WEP, pues corrige ciertas debilidades que presenta este último protocolo; WPA mediante el uso del protocolo Temporary Key Integrity Protocol (TKIP), elimina la reutilización del mismo vector de

inicialización de paquetes de información, además este vector se incrementa de 24 a 48 bits. TKIP hace uso de claves secretas 128 bits para la encriptación de paquetes, estas claves nunca son enviadas en texto claro en los paquetes de datos y además son claves diferentes para la comunicación entre cada cliente y el punto de acceso; estas claves de encriptación van cambiando cada diez mil paquetes de información, de esta manera se provee de una encriptación más eficiente y una mejor seguridad para la red inalámbrica.

WPA hace uso del algoritmo Message Integrity Check (MIC), llamado Michael, para la revisión de la integridad de los paquetes de información. El algoritmo MIC puede detectar posibles ataques e implementa contadores de recepción de paquetes para bloquear posibles nuevos ataques.

Sin embargo, el protocolo WPA no es infalible, el uso del método de encriptación RC4 y el protocolo TKIP, deja la posibilidad de posibles nuevas debilidades. Por esta razón, el lanzamiento del nuevo protocolo 802.11i o llamado WPA2 ha revolucionado la seguridad para las redes inalámbricas. El estándar 802.11i hace uso del concepto "Robust Security Network" (RSN), para lo cual es requerido nuevo hardware y software en los puntos de acceso. El estándar 802.11i implementa un sistema de encriptación Advanced Encryption Standard (AES) y un protocolo de seguridad Counter Mode CBC MAC Protocol (CCMP) mucho más robustos que sus antecesores RC4 y TKIP, lo que lo convierte en el método de seguridad más fuerte para redes inalámbricas de área local. Sin embargo, el estándar 802.11i no es implementado en la mayoría de puntos de acceso y en los que se encuentra implementado, su costo es mucho mayor que los puntos de acceso convencionales, además de ser incompatible con varios equipos como son las tarjetas de red inalámbricas y algunos sistemas operativos.

Por todas las razones expuestas, el protocolo WPA será implementado para la solución, pues cubre varias debilidades del protocolo WEP, y no necesita la utilización de un distinto hardware, como lo requiere el estándar 802.11i.

2.3.2. RADIUS - Remote Authentication Dial-In User Server

RADIUS es un protocolo de autenticación para aplicaciones de acceso a red, el cual usa el puerto 1813 UDP para establecer sus conexiones. Cuando se realiza la conexión hacia una Red Inalámbrica, se envía previamente un nombre de usuario y una contraseña hacia un dispositivo cliente NAS (punto de acceso) sobre el protocolo PPP, el Access Point redirige la petición hacia un servidor RADIUS. El servidor RADIUS comprueba si el usuario se encuentra autorizado, utilizando métodos de autenticación como EAP. Si el usuario y su contraseña son válidos, el servidor de autenticación autorizará el acceso a la Red Inalámbrica, asignándole una dirección IP, mediante el uso de direccionamiento dinámico o DHCP, el cual se encuentra configurado en el punto de acceso.

2.3.3. Servidor de Autenticación Freeradius

Freeradius es una plataforma modular, de gran potencialidad, con diversas y completas características que lo convierte en uno de los más utilizados y potentes servidores RADIUS de clase AAA. Freeradius incluye servidor, clientes y desarrollo de múltiples librerías útiles para el desarrollo de un excelente servicio; puede manejar miles de cuentas de usuarios y millones de peticiones de autenticación al día.

Autenticación de la WLAN del AEIRNNR:

La identidad del usuario viene a ser el número de cédula con el cual está registrado en la base de datos del servidor de autenticación, mientras que las credenciales se implementarán mediante contraseñas, aunque también podría incluirse el uso de certificados digitales.

El protocolo de autenticación usado será EAP-PEAP, este protocolo es usado entre el servidor Freeradius y el Punto de Acceso para el proceso de autenticación de los usuarios.

Existen varios métodos de autenticación que son soportados por el servidor Freeradius, algunos de ellos son:

- EAP-MD5
- EAP-TLS
- EAP-PEAP MSCHAPv2

• EAP-TTLS
• LEAP
• Kerberos

Autorización:
Asimismo, los usuarios autorizados serán registrados en la base de datos MySQL, a la cual el servidor Freeradius se conecta para saber que usuarios pertenecen a la red inalámbrica

Contabilidad:
Este proceso también hace uso de la base de datos para poder registrar el comportamiento de los usuarios en la red inalámbrica.

2.3.4. Base de Datos de Usuarios de la Red

Los datos son almacenados en tablas, cada tabla contiene características en común, por ejemplo tabla de nombre de usuarios, tabla de contraseñas, reporte de los usuarios, entre otros.

La plataforma Freeradius es flexible al momento de seleccionar la base de datos a utilizar, en este caso utilizaremos MySQL.

Base Datos MySQL

MySQL está considerado un sistema de gestión de base de datos relacional, multitarea y multiusuario, que provee una solución robusta, rápida y de fácil uso.

MySQL se basa en un Lenguaje de Consulta Estructurado (SQL), el cual es un lenguaje estándar de computadora para el acceso y la manipulación de base de datos.

Las tablas creadas en MySQL se detallan a continuación:
• nas: Consiste en el cliente o clientes NAS o puntos de acceso los cuales realizan la autenticación hacia el servidor Freeradius,

• radcheck: Contiene todas las contraseñas de cada uno de los usuarios autorizados a hacer uso de la red inalámbrica.
• radgroupcheck: Muestra los grupos de usuarios que contienen un método de autenticación, como por ejemplo EAP-PEAP.
• radgroupreply: Muestra todos los grupos de usuarios creados con sus protocolos y características de cada uno de ellos. Cabe mencionar que los usuarios pertenecientes a un grupo, adoptarán las características del grupo al que forman parte.
• radpostauth: Contiene un reporte sobre los procesos de autenticación realizados satisfactoriamente, cada proceso es almacenado en el día y la hora exacta.
• usergroup: Contiene la tabla de todos los usuarios, indicando los grupos a los que pertenecen.

2.3.5. Aplicación Gráfica para manejo de MYSQL

Una aplicación gráfica nos puede ayudar a trabajar, facilitando la creación de cuentas de usuario, así como poder realizar pruebas de autenticación de los mismos y llevar estadísticas de acceso a la red inalámbrica.

La interfaz gráfica es Phpmyadmin, y está construida en PHP que es un lenguaje de programación utilizado para la creación de contenido dinámico de sitios Web y para la creación de aplicaciones para servidores, permite la conexión a diferentes tipos de servidores de bases de datos tales como MySQL, PostgreSQL, Oracle, ODBC, DB2, entre otros, en donde los primeros tres sistemas de bases de datos garantizan una compatibilidad con el servidor Freeradius.

Phpmyadmin, nos permite la administración de la base de datos en Mysql, a través de internet.

2.4. Diagrama de Solución para una red inalámbrica segura

Una vez definido todos los protocolos y sistemas a usar, podemos presentar el modelo de trabajo a implementar. Este sistema se presenta como un método seguro para una red

inalámbrica, mediante el cual sólo las personas autorizadas podrán acceder a la Red y hacer uso de sus recursos.

El proceso de autenticación de usuarios se realiza mediante un servidor Freeradius, el cual realiza las peticiones a los suplicantes, a través de los clientes NAS. El método de autenticación usado será el EAP-PEAP/802.1x, el cual hace uso de la identidad del usuario y una contraseña para poder acceder a la red.

El servidor Freeradius hará uso de una base de datos creada en MySQL para almacenar la información de todos los usuarios autorizados a acceder a la Red inalámbrica.

Este modelo sistema de seguridad se encuentra esquematizado en la siguiente figura:

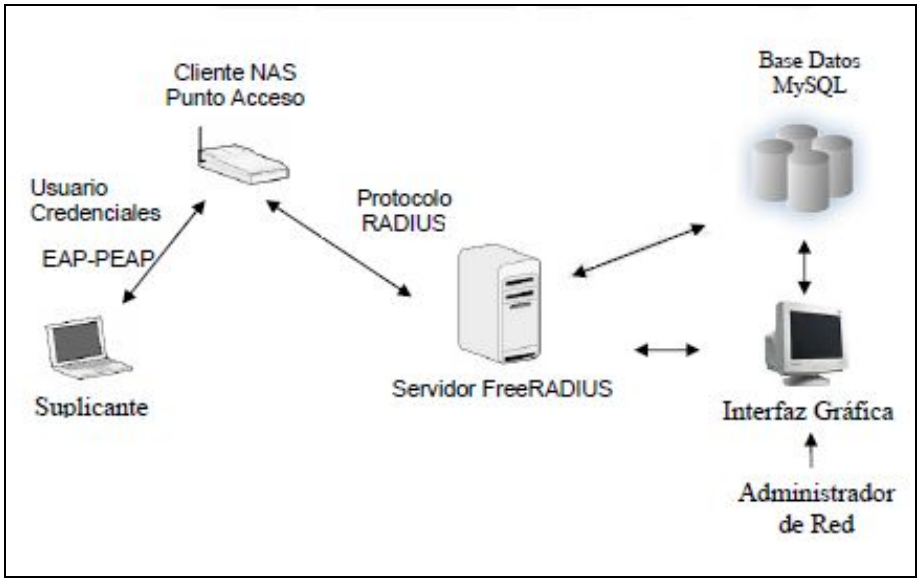


Fig.30 . Diagrama de Red

Una vez concluido el diseño de la red WLAN, damos paso a la implantación de la red y control de accesos a la misma a través del protocolo RADIUS, evidenciado de esta manera el cumplimiento de nuestro objetivo final. Debemos señalar que por políticas que se implantaron en la universidad, en lo que refiere a la concesión de enlaces de internet para las diferentes áreas, la red queda instalada a nivel de laboratorio, y los equipos a disposición de las autoridades del A.E.I.R.N.N.R.

7. CONCLUSIONES

- Para la construcción adecuada de una red inalámbrica, debe hacerse un análisis y diseño previo a la implantación de la misma, esto nos permitirá optimizar recursos, ahorrar tiempo y dinero en la construcción de la red.

- Luego de haber llevado a cabo el análisis, se determinó la funcionalidad que requiere la red inalámbrica para el AEIRNNR, que consiste básicamente en proveer el servicio de internet para navegar en el campus del Área a los estudiantes, y en base a esto se determinó que el tipo de seguridad requerida es la utilización de usuarios y contraseñas para la identificación.

- El espacio físico donde se va a implementar la red inalámbrica, es el área externa a los edificios del AEIRNNR, dentro de la Universidad Nacional de Loja, debemos señalar que en la actualidad existen algunos sitios específicos donde se puede conectar a redes inalámbricas existentes, como la biblioteca, el bloque III, cerca de la Asociación de Carreras, los mismo no dan abastecimiento a todos los usuarios.

- Una vez elaborado el diseño de la red tomando como referencia los requerimientos obtenidos en la etapa de análisis, se determinó claramente que los componentes tanto de software como hardware necesarios para implementar la red serán tecnologías compatibles con los estándares básicos de la IEEE para redes inalámbricas con la finalidad de que se dé un funcionamiento eficiente entre los componentes de la red y que ésta tenga un buen rendimiento,

- De la etapa de diseño de la WLAN también se concluyó que los Access Point seleccionados sean compatibles con el protocolo de autenticación RADIUS, para que puedan también se determinó los sitios donde deben ser ubicados tanto los Access Point como el servidor.

- El protocolo de autenticación RADIUS, es el más apropiado para efectuar el control de accesos de la red inalámbrica, gracias a sus características de AAA (Autenticación, Autorización, Registro), debido a la seguridad que proporciona a la red al permitir la validación de los usuarios.

- La utilización de Freeradius como servidor RADIUS, ha sido una experiencia enriquecedora, pues se trata de una alternativa de software libre muy completa y de gran versatilidad y gratuita, que se puede aplicar en sistemas de pocos recursos, así como también en sistemas atendiendo a millones de usuarios. Además tiene compatibilidad con diversos protocolos de autenticación y soporte para diversas bases de datos.

- Centos, S.O. para servidores, no es un sistema operativo que nos proporcione un buen soporte técnico en caso de ser necesario, siendo esto una gran desventaja de su uso, en este caso no nos permitió instalar la última versión de Freeradius.

- Las redes inalámbricas constituyen en la actualidad, una herramienta que brinda muchos beneficios en cualquier ámbito en donde sean implementadas, ya sea a nivel empresarial o educativo, su contínua evolución permite obtener grandes beneficios en cuanto a las velocidades que puede alcanzar y a precios que cada vez son más accesibles, además de la movilidad y facilidad de instalar gracias a la ausencia de cables.

8. RECOMENDACIONES

- En la etapa de análisis, es recomendable tener claro a qué tipo de usuarios va dirigida la WLAN, esto nos ayudará a definir en forma clara las características de la red, los servicios que esta prestará y las seguridades que deben considerarse, al momento de implementarse.

- Para la etapa de diseño y en base a los requerimientos obtenidos en la etapa de análisis, es muy importante hacer una revisión acerca de las características de los Access Point en cuanto a la compatibilidad con los estándares como el 802.1x, soportar WPA y los estándares 802.11b y g. Además debe evaluar la relación costo/prestaciones.

- Al implementar la red se recomienda tener especial cuidado para no permitir el ingreso de usuarios no autorizados que podrían ocasionar perjuicios a los usuarios autorizados, para esto se debe hacer uso del servidor Radius que mediante el protocolo de autenticación EAP-PEAP valida el ingreso del usuario a la red.

- Se recomienda la utilización del estándar 802.1x debido a que al hacer uso del modo de encriptación WPA (Wi-Fi Protected Access), que es compatible con el nuevo estándar 802.11i, permite integrar a la red nuevas tecnologías, sin tener que desechar los existentes y mantener el buen funcionamiento de la red.

- A la hora de implementar una red, se recomienda dar importancia a la alternativa inalámbrica ya que le dará muchos beneficios en cualquiera que sea el lugar a implantar debido a sus ventajas como son: la desaparición de cables, el costo, la movilidad, la facilidad de instalación.

- Acerca de Freeradius, se recomienda utilizar la versión más actualizada ya que esto nos asegura obtener mayor compatibilidad con diversos sistemas operativos de los usuarios.

- Freeradius permite integrar redes cableadas siempre y cuando las tarjetas Ethernet tengan compatibilidad con Freeradius.

9. BIBLIOGRAFÍA

LIBROS

- GAST Matthew, 2006, REDES WIRELESS 802.11, 1ra edición español, ANAYA MULTIMEDIA S.
- REID Neil y SEIDE Ron. 2005. Manual de Redes Inalámbricas 802.11 (WIFI). McGraw-Hill.
- STALLINGS William. 2004. Comunicación y Redes de Computadoras. Pearson Educación S.A.

SITIOS WEB

- CONCEPTOS BÁSICOS DE REDES WIFI Y SU SEGURIDAD (para principiantes) [http://www.balearsinnovacio.com/blog/wp-content/uploads/2007/09/wephacking.pdf]

- PEREZ Oitsa Ing. 2005. TELEM@TICA. Revista Digital de las Tecnologías de la Información. [http://www.cujae.edu.cu/revistas/telematica]

- 802.1X/EAP, 16 de octubre de 2008.[http://es.kioskea.net/contents/wifi/wifi-802.1x.php3]

- Redes Inalámbricas. [http://es.kioskea.net/contents/wireless/wlintro.php3]

- Diccionario enciclopédico Wikipedia: http://es.wikipedia.org/wiki/Portada

- The Freeradius Project. 2010.[www.freeradius.org]

- PONCE de Miguel E., 2002. Redes inalámbricas: IEEE 802.11. [http://www.todo-linux.com/manual.todo-linux.com/redes/inalámbricas.htm]

- WIFI Redes Inalámbricas [http://wifiw.com/] [marzo 2010]

10. ANEXOS

ANEXO 1

ENCUESTA

UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES
CARRERA DE INGENIERÍA DE SISTEMAS

ESTIMADO ESTUDIANTE, SOLICITAMOS A USTED SU VALIOSA COLABORACIÓN LLENANDO LA PRESENTE ENCUESTA, LE AGRADECEMOS POR SU TIEMPO Y ATENCIÓN.

Carrera: …….. Modulo: …… Horario clases: ……

1. ¿TIENE UD. A SU DISPOSICIÓN INTERNET, EN EL CAMPUS DEL AEIRNNR?
   SI ( ) NO( )
   INDICUE EL LUGAR
   ……
2. ¿INDIQUE POR MEDIO DE QUE SE PUEDE CONECTAR AL INTERNET EN EL CAMPUS DEL AEIRNNR?
   INALÁMBRICO ( )
   CABLE ( )

3. SI UD. SE CONECTA POR MEDIO INALÁMBRICO, POR FAVOR INDIQUE EN QUE HORARIO POR EJEMPLO 8 A 9AM Y EN QUE LUGAR LO HACE.
   MAÑANA ……
   TARDE ……
   LUGAR(ES):
   ……
   ……

4. ¿QUE MEDIO DE CONEXIÓN LE PARECE MEJOR PARA UD.?
   INALÁMBRICO ( )
   CABLE ( )
   ¿POR QUÉ?
   ……
   ……

5. ¿CREE QUE SERIA DE UTILIDAD PARA UD. LA IMPLANTACIÓN DE UNA RED INALÁMBRICA EN EL CAMPUS UNIVERSITARIO, QUE LE PERMITA CONECTARSE A INTERNET DENTRO DEL CAMPUS UNIVERSITARIO?
   SI ( ) NO( )
   POR QUÉ?:
   ……
   ……
   ……
   ……
   ……

GRACIAS POR SU COLABORACIÓN

ANEXO 2

Ing. Wilman Chamba, docente de la Universidad Nacional de Loja, de la Carrera de Ingeniería de Sistemas, a petición de la parte interesada,

C E R T I F I C O:

Que los egresados Mónica María Díaz Samaniego, y Pablo Oswaldo Córdova García, aplicaron en el mes de marzo, una encuesta a estudiantes de las diferentes carreras del AEIRNNR, con la finalidad de obtener información para el desarrollo de su investigación previo a la obtención del título de Ingenieros de Sistemas.

Esto todo cuanto puedo certificar en honor a la verdad, autorizo a los egresados hacer uso del presente en lo que estimen conveniente.

Atentamente

Ing. Wilman Chamba Z.

DOCENTE-UNL

ANEXO 3

Instalación de PhpMyAdmin (opcional)

Para facilitar la administración de las bases de datos se recomienda realizar la instalación de **PhpMyAdmin**.

Phpmyadmin es una aplicación en php que permite realizar de manera gráfica la administración de las bases de datos de MySQL a través de un navegador.

Esta herramienta permite facilitar el proceso de creación y mantenimiento de la base de datos utilizadas por las Aplicaciones de Acción. Usted puede obtener esta herramienta en http://www.phpmyadmin.net/.

La instalación del sistema se realiza simplemente descomprimiendo el archivo **phpMyAdmin** que se encuentra en el directorio phpmyadmin del CD de municipios. Descomprímalo dentro de su directorio (var/www/http**)** de su servidor de Internet.

Cuando realice el proceso de descompactar el archivo se genera un directorio **phpMyAdmin-x.x.x.pl1**,recomendamos renombrarlo a **phpmyadmin** para facilitar el acceso a la herramienta, de tal manera que funcionará en el URL http://localhost/phpmyadmin

Antes de poder utilizar la herramienta es necesario editar el archivo de configuración **config.inc.php** y definir la clave de acceso del super-administrador (root) así:

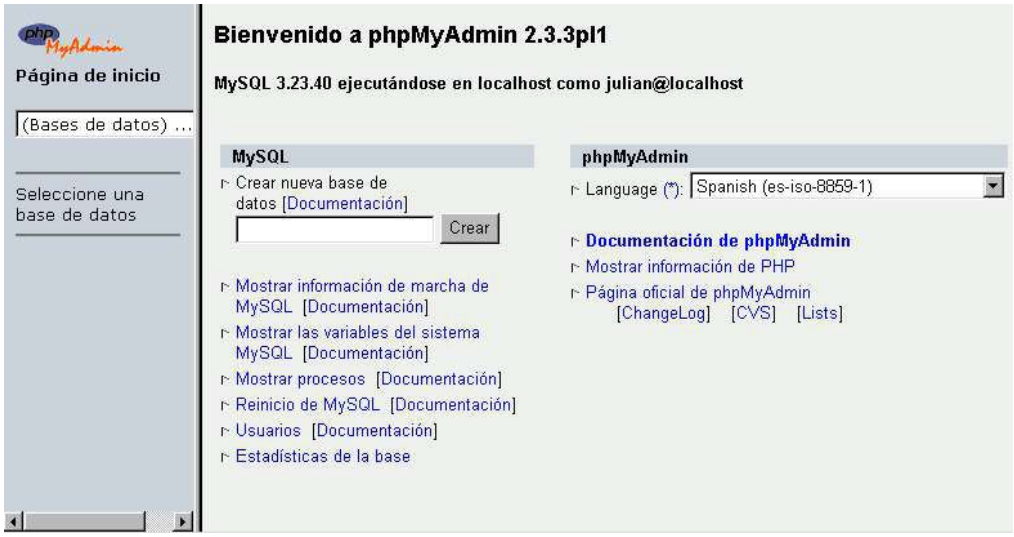
$cfg['Servers'][$i]['user'] = **'root'**; // MySQL user

$cfg['Servers'][$i]['password'] = **'clave asignada'**; // MySQL password

Y definir ruta para acceso a phpmyadmin:

$cfg['PmaAbsoluteUri'] = '**http://var/www/http/localhost/phpmyadmin/**';

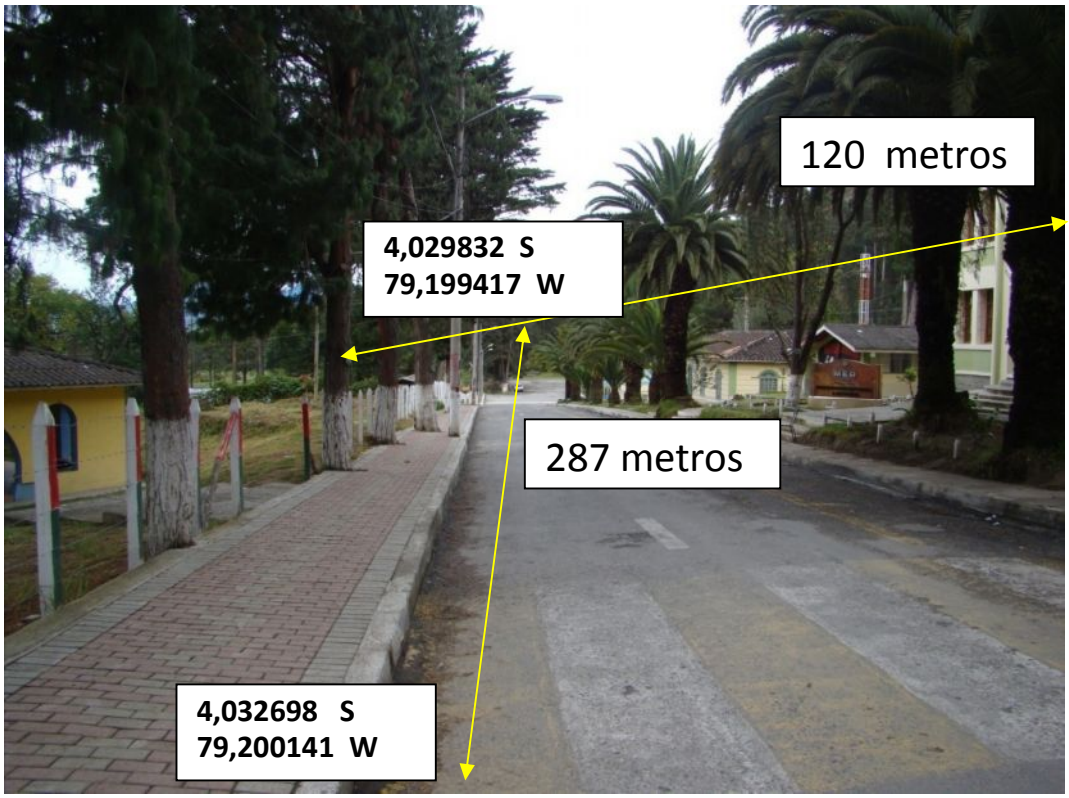
Grabe los cambios y abra el URL **http://localhost/phpmyadmin/**. Deberá aparecer la siguiente pantalla:

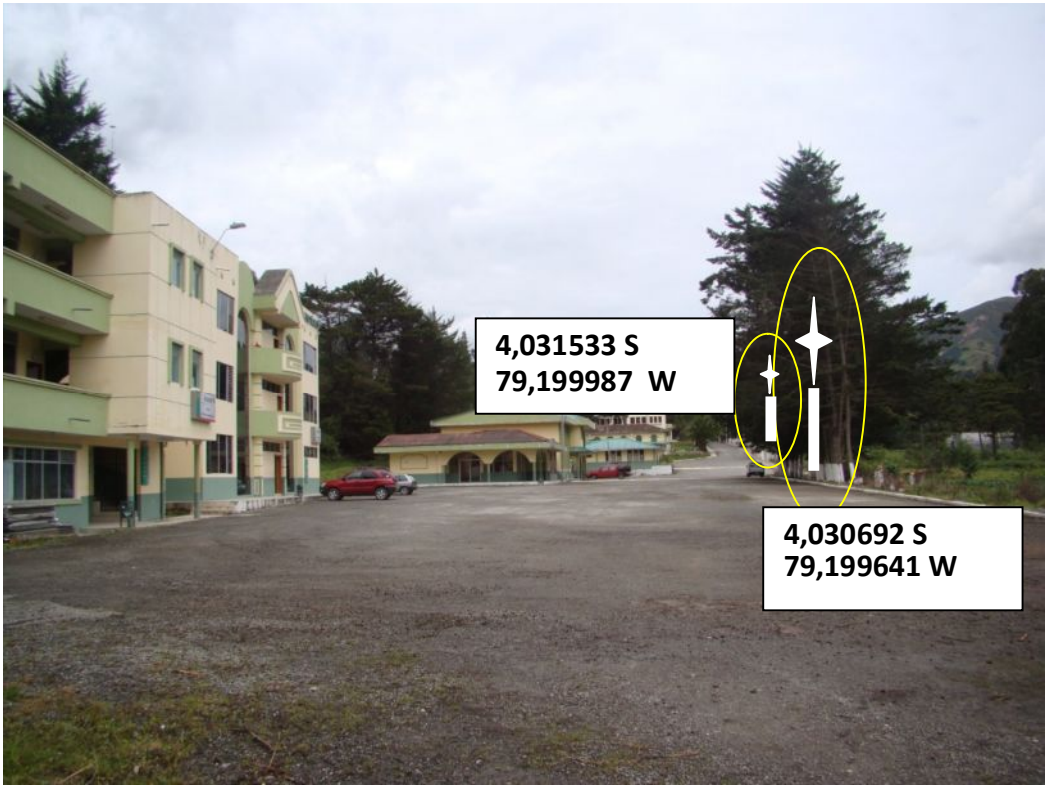


Nota importante: ES UN GRAN RIESGO DE SEGURIDAD PARA EL SISTEMA DEJAR EL SERVIDOR CONECTADO A INTERNET CON PHPMYADMIN SIN RESTRICCIONES DE ACCESO A ESTA HERRAMIENTA. UTILICE LA OPCION DE RESTRINGIR EL ACCESO A UN DIRECTORIO DEL SERVIDOR WEB PARA PROTEGER ESTA HERRAMIENTA DE ACCESOS NO AUTORIZADOS.

ANEXO 4

FOTOS DEL ÁREA





BLOQUES DEL ÁREA

ÍNDICE DE CONTENIDOS

PORTADA I
CERTIFICACIÓN II
AUTORÍA III
AGRADECIMIENTO IV
DEDICATORIA V
ESQUEMA DE TESIS VI
SUMMARY 1
1. RESUMEN 2
2. INTRODUCCIÓN 3
3. REVISIÓN LITERARIA 5
3.1. Fundamentación teórica 5
3.1.1. Redes inalámbricas. 5
3.1.1.1. Clasificación de las redes inalámbricas 5
3.1.1.2. IEEE 802.11 (WIFI) 7
3.1.1.3. Topologías de una red inalámbrica 10
3.1.1.4. Componentes de una red inalámbrica 11
3.1.1.5. Capa física 12
3.1.1.5.1. Espectro Expandido por Secuencia Directa (DSSS) 13
3.1.1.5.2. Espectro ensanchado por salto de frecuencia (FHSS) 14
3.1.1.5.3. Tecnología de Infrarrojos. 15
3.1.1.6. Capa MAC (acceso al medio) 16
3.1.1.6.1. Procedimiento RTS/CTS 17
3.1.1.6.2. Funciones de coordinación MAC 18
- Función de Coordinación Distribuida (DCF) 19
- Función de Coordinación Centralizada: 21
3.1.1.7. Formato de la trama 802.11 24
3.1.1.8. Servicios de red para 802.11 24
3.1.1.8.1. Servicios del sistema de distribución 25
3.1.1.8.2. Servicios de estación: 26
3.1.1.8.3. Servicios de administración de espectro 26
3.1.1.9. Seguridad de redes 26
TKIP 29
3.1.1.9.1. Radius 30
N.A.S. *Network Access Server* (NAS)
3.1.1.9.2. Extensible Authentication Protocol (EAP) 36

3.1.1.9.3 Protocolo EAP- PEAP 36
3.1.1.9.4. Encriptación 37
3.1.1.9.5. Estándar 802.1x 39
4. PROPUESTA ALTERNATIVA 42
4.1. Implantación 42
4.1.3. Instalación de los equipos 42
4.1.4. Configuración de Equipos 42
4.1.4.1. Configuración de servidor 42
4.1.2.2. Configuración del Access Point 50
4.1.2.3. Configuración del usuario 52
4.2. Pruebas de validación 58
4.2.1. Pruebas Autenticación de Usuarios 58
4.2.2. Análisis de la encuesta 62
5. METODOLOGÍA 68
6. EVALUACIÓN DEL OBJETO DE TRANSFORMACIÓN 70
ETAPA 1: ANÁLISIS Y DETERMINACIÓN DE REQUERIMIENTOS PARA LA IMPLANTACIÓN DE UNA RED WLAN EN EL AEIRNNR 70
ETAPA 2: DISEÑO DE LA RED INALÁMBRICA PARA EL A.E.I.R.N.N.R (WLAN) 77
2.1. Diseño físico de la WLAN 78
2.2. Diseño lógico de la WLAN 83
2.3. Diseño de seguridad de la WLAN 85
2.3.1. WPA - Wi-Fi Protected Access 85
2.3.2. RADIUS - Remote Authentication Dial-In User Server 86
2.3.3. Servidor de Autenticación FreeRADIUS 87
2.3.4. Base de Datos de Usuarios de la Red 88
2.3.5. Aplicación Gráfica para manejo de MYSQL 89
2.4. Diagrama de Solución para una red inalámbrica segura 89
7. CONCLUSIONES 91
8. RECOMENDACIONES 93
8. BIBLIOGRAFÍA 95
10. ANEXOS 96
ANEXO 1 96
ANEXO 2 97
ANEXO 3 85
ANEXO 4 90

ÍNDICE DE FIGURAS

Fig.1. Cobertura de las Redes Inalámbricas 6
Fig.2. Secuencia de Baker 13
Fig.3. Codificación de Barker 14
Fig.4. Gráfica de codificación con salto de frecuencia 15
Fig.5. Problema de nodos ocultos 17
Fig.6. Procedimiento RTS/CTS 18
Fig.7. Funciones de Coordinación MAC 19
Fig.8. Modelo de Funcionamiento del mecanismo DCF 20
Fig.9.Utilización de NAV para la detección de portadora virtual 22
Fig.10. Esquema de funcionamiento de periodos de contienda 22
Fig.11. Utilización de PCF 23
Fig.12 . Diagrama de secuencia de conexión y desconexión de un cliente a la red. 32
Fig.13. Paquete EAP 36
Fig.14 Encriptación simétrica 38
Fig.15. Encriptación asimétrica 39
Fig.16 Componentes para solución 802.1x 40
Fig.17 . Configuración del AP. 50
Fig.18 . Configuración del AP. 51
Fig.19 . Configuración del AP. 51
Fig.20 . Configuración del AP. 52
Fig.21. Comprobación de red inalámbrica 53
Fig.22. Comprobación de red inalámbrica 53
Fig.23 . Comprobación de red inalámbrica 54
Fig.24 . Comprobación de red inalámbrica 54
Fig.25 . Comprobación de red inalámbrica 55
Fig.26 . Prueba de autenticación de red 56
Fig.27 . Prueba de autenticación de red 56
Fig.28 . Prueba de autenticación de red 52
Fig.29. Access Point Marca Linksys Modelo WAP54g 80
Fig.30. Diagrama de Red 90

ÍNDICE DE TABLAS

Tabla.1. Modificaciones del estándar 802.11 9
Tabla.2. Comparación de frecuencia, velocidad y rango de los estándares a,b y g 9

ÍNDICE DE CUADROS

Cuadro No 1: Conexión a Internet en AEIRNNR 57
Cuadro No 2: Medios de Conexión a Internet en AEIRNNR 58
Cuadro No 3: Horario de Conexión a Internet inalámbrico en AEIRNNR 59

Cuadro No 4: Medio de conexión más adecuado en AEIRNNR 60
Cuadro No 5: Necesidad de implementar una WLAN en AEIRNNR 61
Cuadro No 6: Posee una portátil para conexión a WIFI en el AEIRNNR 62

ÍNDICE DE GRÁFICOS

Gráfico No 1: Conexión a Internet en AEIRNNR 57
Gráfico No 2: Medios de Conexión a Internet en AEIRNNR 58
Gráfico No 3: Horario de Conexión a Internet inalámbrico en AEIRNNR 59
Gráfico No 4: Medio de conexión más adecuado en AEIRNNR 60
Gráfico No 5: Necesidad de implementar una WLAN en AEIRNNR 61
Gráfico No 6: Posee una portátil para conexión a WIFI en el AEIRNNR 62