

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

SEGURIDAD DE REDES INALAMBRICAS EN UN AMBIENTE ACADEMICO

T E S I S

PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACION

PRESENTA:

LUIS ALBERTO GONZALEZ CERVANTES



DIRECTOR DE TESIS:

ING. RICARDO FEDERICO VILLARREAL MARTINEZ

CIUDAD UNIVERSITARIA 2005

AGRADECIMIENTOS

A ***DIOS*** por su amor incondicional y revelarme cada día algo nuevo acerca de mi mismo.

A mis Padres por su **AMOR**, **COMPRENSIÓN**, **TOLERANCIA** y **RESPETO** en cada momento de mi vida.

"A Dios le pedí todo para disfrutar de la vida,

me concedió vida para poder disfrutar de todo.

Le pedí lujos y fama, me concedió amigos y amor"

GRACIAS…… por tener poco que pedir y tanto que agradecer.

A pesar de mi mismo las peticiones que no hice me fueron concedidas.

AA

Í n d i c e

Contenido **Pagina**

Introducción.....1
Antecedentes.....3

Capitulo 1 Redes Inalámbricas
1.1 Tipos de Redes Inalámbricas.....7
1.1.1 Redes Infrarrojas.....8
1.1.2 Redes de Radio Frecuencia.....10
1.2 Conjunto de Protocolos 802.11.....20
1.3 Factor de Reuso.....30
1.3.1 Redes Ad-Hoc.....31
1.3.2 Redes de Infraestructura.....31
1.4 Factor de Distancia.....35
1.5 Puntos de Acceso.....36

Capitulo 2 Seguridad de la Información en las Redes Inalámbricas
2.1 Comunicación Segura.....38
2.1.1 SSL (Secure Socket Layer).....40
2.1.2 SSH (Secure Shell).....43
2.2 Seguridad en el Sistema Operativo.....46
2.2.1 Windows.....46
2.2.2 Linux.....48
2.3 Seguridad en los Puntos de Acceso.....49
2.3.1 Autenticación.....51
2.3.2 Filtrado de Direcciones MAC.....66
2.4 Seguridad a través del Gateway.....68

Capitulo 3 Puntos Vulnerables en las Redes Inalámbricas
3.1 Ataques y Riesgos.....73
3.1.1 Fácil Acceso.....73
3.1.2 Vulnerabilidades de WEP.....75
3.1.3 Rendimiento Limitado.....80
3.1.4 MAC Spoofing.....82
3.2 Negación de Servicio.....83
3.2.1 Puntos de Acceso No Autorizados.....83

3.3 Uso Indebido....86
3.4 Riesgo en el Medio....86

Capitulo 4 Soluciones para contrarrestar los puntos vulnerables de seguridad en WLAN's
4.1 Autenticación y Encripción....88
4.1.1 RADIUS....89
4.1.2 Operación de un Servidor RADIUS....91
4.2 IPSec VPN....93
4.2.1 Trama de IPSec....107
4.2.2 Métodos de Autenticación....108
4.2.3 Operación de IPSec....108
4.2.4 IPSec Movil....109
4.3 Descripción del Protocolo 802.1x....110
4.3.1 Operación del protocolo 802.1x....111

Implementación de una Subred Inalámbrica Segura para el IIMAS....122

Conclusiones....137

Apéndices....i

Glosario....xix

Bibliografía

I n t r o d u c c i ó n

Objetivo de la propuesta.

Detectar y analizar los puntos vulnerables de las redes inalámbricas y proponer alternativas de solución que contrarresten las fallas encontradas; tomando en cuenta las necesidades de las distintas áreas que conforman al Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS) de la Universidad Nacional Autónoma de México.

Justificación

Dada la problemática encontrada en el IIMAS causada por la insuficiencia tanto de nodos físicos como de direcciones IP (*Internet Protocol*) homologadas pertenecientes al segmento asignado a dicho instituto. En la actualidad se ha venido resolviendo este problema mediante la creación de subredes que desahogan el uso tanto de dichos nodos como de direcciones. Existen lugares donde resulta insuficiente o no se cuenta con la infraestructura de red necesaria para realizar alguna actividad. Aquí es donde las redes inalámbricas son una alternativa que puede dar solución a esta problemática aprovechando sus condiciones de movilidad y portabilidad que las caracterizan. Además de traer consigo otros beneficios como la disminución de riesgos de una posible infección de virus informático y del mal uso de los recursos que ponen en riesgo la integridad de la información que circula a través de la red. Sin embargo al tratarse de un medio de transmisión libre cualquier individuo ajeno a esta institución puede llegar a tener acceso no autorizado sin la necesidad de una conexión directa a los nodos de la red cableada. Lo único que necesita es colocarse en un área cercana al perímetro del instituto en donde la señal pueda ser captada.

Para evitar estas contingencias, se analizaran varios mecanismos de seguridad que permitirán implementar una subred inalámbrica segura.

Un punto importante a considerar para la implementación de las redes inalámbricas es que este instituto cuenta en su padrón con diversos usuarios, tales como estudiantes de posgrados en Ciencia e Ingeniería de la Computación o en Ciencias Matemáticas o de la Especialización en Estadística Aplicada, investigadores en diferentes áreas de la ciencia, personal técnico académico especializado y personal administrativo. Dada la existencia de toda esta diversidad de áreas, cada una cumpliendo con un propósito en especifico, los recursos informáticos que necesita un investigador no son los mismos que los de una persona en el área administrativa o un estudiante. Es evidente que las necesidades de cada una de estas áreas son distintas por lo que los mecanismos de seguridad van a estar de acuerdo con el área en específico en donde se implemente una subred inalámbrica.

Es por este motivo de suma importancia encontrar el balance entre los puntos vulnerables y sus posibles soluciones para proponer una subred inalámbrica segura para cualquier área dentro de un ambiente académico que sea una extensión y de apoyo a la red cableada del Instituto de Investigación en Matemáticas Aplicadas y Sistemas de la Universidad Nacional Autónoma de México.

Antecedentes

En México, entre otros países se deben resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad. No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas últimas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas y de esta manera generar una "Red Híbrida".

Se pueden diseñar redes de cómputo considerando al sistema cableado como la parte principal y la parte inalámbrica como la que proporciona movilidad adicional al equipo, para que el operador se pueda desplazar con facilidad dentro de un almacén, oficina, salón, biblioteca, etc.

El precio inicialmente alto para sufragar costos de investigación y desarrollo hoy día está bajando rápidamente, debido a la altísima demanda que se está teniendo. Estudios recientes, indican que la demanda de usuarios domésticos se ha disparado. El uso de dispositivos, NIC (*Network Interface Card*) o tarjetas que permiten usar estas redes locales inalámbricas, pronto será mayor en las casas que en las grandes empresas.

Por otro lado, las WLAN (*Wireless Local Area Network*) tienen sus propios problemas que dificultan en gran medida la transmisión de datos. Las frecuencias empleadas para la transmisión son las ISM (*Industrial, Scientific and Medical*) bandas de propósito general. Estas bandas son las de 900MHz, 2.4GHz y 5GHz respectivamente. Como esté es un medio de transmisión difícil, al tratarse de

bandas libres, no tienen la protección de una banda con licencia.

Con dispositivos móviles la cobertura no siempre está asegurada, se tiene una alta tasa de errores de bit, el problema de los nodos ocultos / expuestos, etc. Por lo que la calidad no se puede asegurar ni en tiempo ni en espacio. La movilidad se tiene que conseguir eliminando la necesidad de cables y de recarga de baterías, por lo que el consumo de baterías es un factor importante. Casi siempre el consumo de baterías y el alcance están en contraposición. Para llegar más lejos hace falta una señal con mayor intensidad y para una señal con mayor intensidad se necesita mayor potencia y con ello mayor consumo de batería.

Al eliminar los cables se eliminan muchos puntos de falla que incluso en ocasiones son difíciles de localizar o que eventualmente vuelven a fallar y que implican un costo. En un cableado estructurado, los cables se encuentran expuestos y son con los que el usuario o el personal de limpieza llega a tener contacto haciéndolos vulnerables.

En general el uso de tecnología inalámbrica facilita el enlace de equipos de una forma fácil y rápida. Es muy útil en casos en los que se improvisan oficinas o éstas sufren modificaciones constantemente y requieren comunicación entre sus equipos, cuando no se pueden realizar trabajos de obra civil por costos, en ambientes hostiles o de difícil acceso, o por tratarse de un edificio de valor histórico. Adicionalmente la comunicación inalámbrica permite movilidad lo cual es muy práctico, sin embargo se sacrifica velocidad por comodidad. La velocidad de una red inalámbrica esta lejos de alcanzar las velocidades de transmisión que se logran con medios de transporte guiados. Por lo que, mientras la tecnología inalámbrica no permita una comunicación veloz y global, seguiremos haciendo uso de las redes inalámbricas sólo para los últimos metros, resultando la red

inalámbrica una subred de una red cableada. Un factor importante en la decisión sobre el diseño cableado o inalámbrico son las aplicaciones que se estén corriendo en nuestra red, en el caso de comunicación e intercambio de información, la solución que brinda la velocidad de una red inalámbrica es aceptable, no así cuando las aplicaciones realizan procesos distribuidos y cálculos que requieran de mayor velocidad o transmisión de audio y video que consumiría el ancho de banda del canal haciendo lenta, intermitente o incluso imposible el resto de la comunicación.

La seguridad es un factor importante, al no existir límites físicos y puesto que estamos transmitiendo por el aire. Esto facilita la escucha de los datos sin protección por parte de personas ajenas, por lo que resulta difícil hablar de canales seguros. En una red cableada este control resulta ser más sencillo dado que únicamente pueden conectarse quienes posean un cable desde su computadora a los equipos de red. En una red inalámbrica cualquier persona con un equipo portátil y una antena puede captar la señal y poner en riesgo nuestra información, motivo por el cual las redes inalámbricas se convierten en vulnerables e inseguras.

La amplia cobertura de zonas de las redes inalámbricas es uno de los principales motivos para una constante preocupación e interés por la seguridad. Un atacante puede ubicarse en un lugar en el que nadie espere encontrarlo y mantenerse lo suficientemente lejos del área física de la red. Otro motivo es el extenso uso de las propias redes inalámbricas, se estima que en el año 2006 el número de dispositivos de hardware con capacidades inalámbricas sobrepasará los cuarenta millones de unidades[1], sobre todo a medida que el precio de estas unidades disminuya. Las redes inalámbricas son fáciles de encontrar y no requieren de mucho esfuerzo para

[1] Hacking Wireless, Seguridad de Redes Inalámbricas, Vladimirov, Andrew, Anaya Multimedia, 2005.

realizar una conexión. Incluso aunque estén protegidas mediante WEP (*Wired Equivalent Protocol*) medida de seguridad para el estándar 802.11 de la IEEE (*Institute of Electrical and Electronics Engineers*)

Las estadísticas muestran que en promedio el 30% de todos los puntos de acceso a redes inalámbricas alrededor del mundo cuentan con WEP habilitado en su configuración, el otro 70% restante su configuración es la predeterminada de fabrica sin ningún mecanismo de seguridad[2]. Este tipo de desatenciones pone en riesgo la seguridad de cualquier infraestructura inalámbrica basada en el 802.11.

Se puede pensar que gran parte de esa muestra son redes domesticas, puntos de acceso públicos o pequeñas comunidades inalámbricas. Sin embargo estudios e investigaciones han revelado que gran cantidad de este porcentaje de redes sin control pertenecen a organizaciones gubernamentales y grandes empresas. El factor humano, principalmente la carencia de formación de los usuarios e incluso de los administradores de sistemas, suponen la mayor fuente de inseguridad en el entorno inalámbrico. Por lo que la solución a la inseguridad no se va a resolver con el surgimiento de nuevos y más seguros estándares, ya que la realidad demuestra que no existe un sistema seguro en un cien por ciento, sólo el que no se encuentra conectado a la red. Sin embargo es posible adoptar ciertos mecanismos o sistemas de seguridad que dificulten lo más posible el acceso no autorizado a la información de una institución o empresa.

[2] Hacking Wireless, Seguridad de Redes Inalámbricas, Vladimirov, Andrew, Anaya Multimedia, 2005.

C a p í t u l o 1

REDES INALÁMBRICAS

1.1 Tipos de redes inalámbricas

Las redes inalámbricas se diferencian de las redes convencionales principalmente en la capa física y en la capa de enlace de datos; según el modelo de referencia OSI (*Open Systems Interconnection*). El modelo OSI es un estándar internacional que desde 1983 establece las bases para la comunicación entre dos computadoras, este modelo propone dividir en siete niveles las tareas necesarias para establecer la comunicación entre computadoras, los cuatro primeros niveles cumplen con funciones de comunicación mientras que los tres restantes con funciones de proceso como lo muestra la siguiente figura.

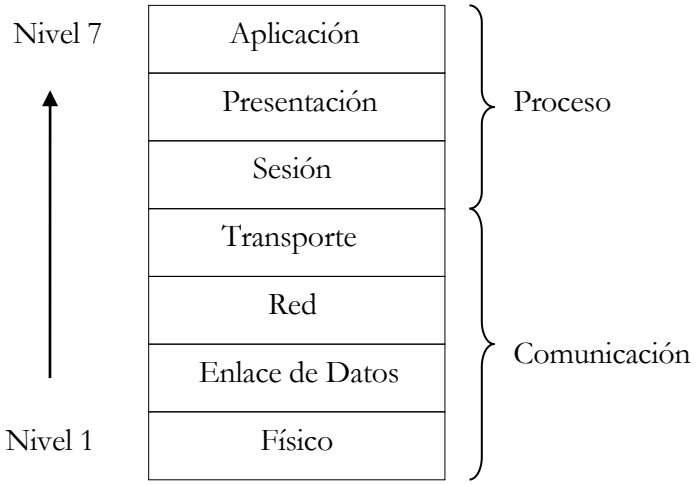


Fig. 1.1 Modelo de referencia OSI

En las redes inalámbricas la capa física PHY (*Physical*) indica cómo son enviados los bits vía radio frecuencia o por luz infrarroja y la capa de enlace de datos denominada MAC (*Medium Access Control*) se encarga de describir cómo se empacan y verifican los bits de modo que no existan errores.

1.1.1 Redes infrarrojas

Las redes de luz infrarroja están limitadas por el espacio, por lo que normalmente este tipo de tecnología es utilizada en lugares en donde los equipos se encuentran en una sola habitación. Este tipo de tecnología utiliza un dispositivo, transmisor y receptor, que envía un haz de luz infrarroja, hacia otro que la recibe. De acuerdo al ángulo de apertura con que se emite la información en el transmisor, los sistemas infrarrojos pueden clasificarse en sistemas de corta apertura y en sistemas de gran apertura, reflejados o difusos.

- Los sistemas infrarrojo de corta apertura, están constituidos por un cono de haz infrarrojo altamente direccional y funcionan de manera similar a los controles remotos de los televisores y otros equipos de consumo; el emisor debe orientarse hacia el receptor antes de transferir información, lo que limita un tanto su funcionalidad. Por ejemplo, resulta muy complicado utilizar esta tecnología en dispositivos móviles, pues el emisor debe reorientarse constantemente. Resumiendo, este tipo de sistemas tienen una funcionalidad mejor en enlaces punto a punto exclusivamente, por ello se considera que es un sistema inalámbrico más orientado a la portabilidad que a la movilidad.

- Los sistemas de gran apertura utilizan un ángulo mucho más amplio por lo que el transmisor no tiene que estar alineado con el receptor. Una topología muy común en esta tecnología, consiste en colocar un transmisor hacia el

cuál se orientan los dispositivos inalámbricos y desde el cual la información es difundida hacia estos mismos. Desgraciadamente la dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor, que limita la velocidad de transmisión (la trayectoria reflejada llega con un retraso al receptor).

La tecnología de haz infrarrojo comercial ofrece un amplio ancho de banda que transmite señales a velocidades de hasta 4Mbps[1] (Megabits por segundo) con un rango de operación entre 10 a 20m; tiene una longitud de onda cercana al color rojo de la luz visible 700nm (nanometros) y se comporta como ésta (no puede atravesar objetos sólidos como paredes, por lo que resulta mas seguro contra receptores no autorizados). Debido a su alta frecuencia, presenta una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por otro tipo de dispositivos eléctricos (motores, luces ambientales, etc.). La transmisión infrarroja 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.

Entre las limitaciones principales de esta tecnología se pueden señalar las siguientes: es sumamente sensible a objetos móviles que interfieren y perturban la comunicación entre emisor y receptor; las restricciones en la potencia de transmisión limitan la cobertura de estas redes a unos cuantos metros; la luz solar directa y otras fuentes de luz pueden interferir en la señal.

[1] http://www.clarinet.com

Conexiones posibles actualmente usando tecnología de infrarrojos

Las velocidades de transmisión de datos en esta tecnología no son suficientemente elevadas y resultan mas eficientes en enlaces punto a punto, por ejemplo entre teléfonos celulares. Por ello, lejos de poder competir globalmente con las LAN (*Local Area Network*) de radiofrecuencia, su uso está indicado más bien como un apoyo o complemento a las LAN ya instaladas, cableadas o por radio.

1.1.2 Redes de Radiofrecuencia

Las redes inalámbricas que utilizan este tipo de tecnología pueden clasificarse en dos grupos: en sistemas de banda estrecha (*Narrow band*) o de frecuencia dedicada y en sistemas basados en espectro disperso o expandido (*Spread spectrum*) ocupado por el estándar IEEE 802.11.

Sistemas de Frecuencia Dedicada

Este tipo de sistemas son muy similares a la forma en que se difunden las ondas de las estaciones de radio comerciales. Es necesario sintonizar una determinada frecuencia tanto en el receptor como en el emisor con el propósito de prevenir las posibles interferencias. Este tipo de señales se expanden sobre un área muy amplia y pueden atravesar objetos sólidos como paredes. Sin embargo estas transmisiones tienen problemas debido a las reflexiones que experimentan las ondas de radio; para evitarlas en lo posible, estas transmisiones están normalizadas por la FCC (*Federal Communications Commission*), Agencia Federal del Gobierno de Estados Unidos. En México la comisión encargada de regular estas transmisiones es la COFETEL (Comisión Federal de Telecomunicaciones).

Un ejemplo de este tipo de sistemas lo encontramos con Motorola. En octubre de 1990, introdujo un concepto de WLAN al que llamo WIN (*Wireless In-building Network*). El sistema de Motorola, llamado Altair, opera en una frecuencia dedicada en la banda de 18GHz del espectro radioeléctrico la cual requiere de la autorización de autoridades gubernamentales.

Sistemas en Espectro Expandido

Los productos comerciales que utilizan infrarrojo o frecuencias dedicadas, aportan únicamente un tercio del mercado de WLAN. Las otras dos terceras partes transmiten información en bandas del espectro que no requieren autorización para su uso.[2] Estas son las llamadas bandas para aplicaciones industriales, científicas y médicas. En mayo de 1985, la FCC asignó las bandas ISM (*Industrial, Scientific and Medical*) 902-928MHz, 2.400-2.483GHz, 5.725-5.850GHz a las redes inalámbricas basadas en espectro expandido. Dicha comisión simplemente asigna la banda y establece las normas o directrices de utilización, pero no decide sobre quién debe o no transmitir en dichas bandas.

El espectro expandido tiene sus orígenes durante la segunda guerra mundial y evolucionó con las necesidades de la guerra. Esta tecnología consiste en esquemas de señalización basados en formas de codificación independientes de la información transmitida. Para la técnica de espectro expandido por secuencia directa se usa un ancho de banda mayor que el mínimo requerido para transmitir la información Sin embargo para la técnica de salto de frecuencia, la señal se dispersa en una gran cantidad de canales a lo largo del ancho de banda de la frecuencia. Es por esto que el termino expandido o disperso depende mucho de la técnica que se este empleando. El ancho de banda mayor permite que las interferencias no afecten a una

[2] Instituto Nacional de Estadística e Informática del Perú

transmisión de espectro expandido por secuencia directa. Por otra parte el salto de frecuencias constantes en pequeños intervalos de tiempo evita también la posibilidad de ser afectados por posibles interferencias.

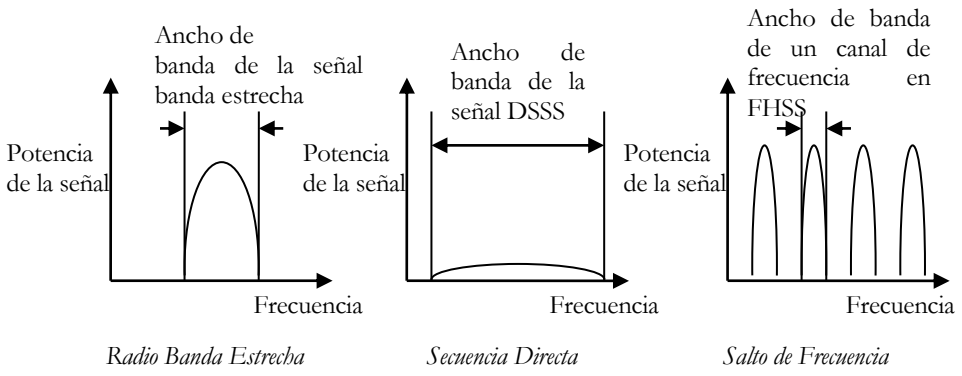


Fig. 1.2 Espectro Expandido

Dos técnicas distintas de espectro expandido.

Secuencia Directa *(Direct Sequence Spread Spectrum, DSSS).*

Esta técnica expande la señal a lo largo del ancho de banda. La potencia es reducida, razón por la cuál no es detectada por los receptores de frecuencias dedicadas debido a su baja energía. DSSS combina el flujo de datos con una alta velocidad en la codificación digital de los mismos, cada bit es mapeado dentro de un patrón o código de bits conocido Este patrón es conocido como secuencia de Barker de 11 bits y tiene la siguiente forma:

+1 -1 +1 +1 -1 +1 +1 +1 -1 -1 -1

A cada bit codificado se le conoce como *chip*.

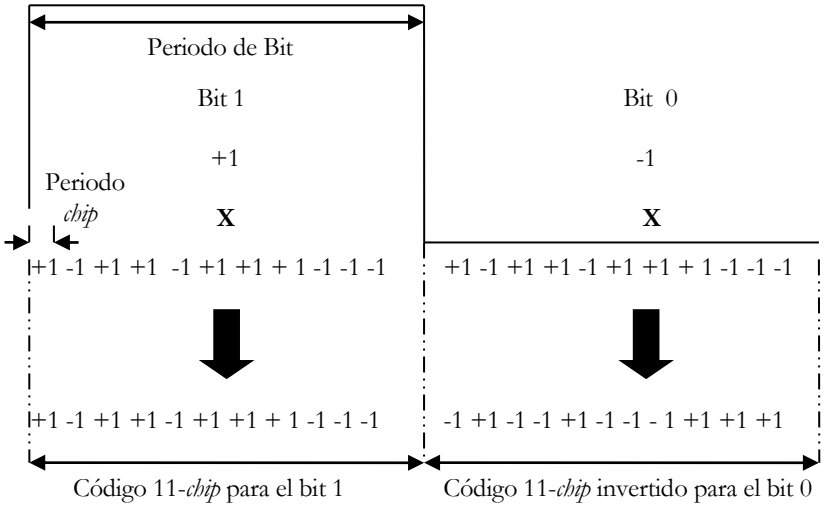


Fig. 1.3 DSSS usando un código 11 *chip*

La figura muestra como los bits de información pueden ser expandidos 11 veces a través de un código 11-*chip*, es importante resaltar que cuando el bit de información es un cero el código es multiplicado por -1 resultando lo que se denomina un código 11-*chip* invertido; entre mas grande sea este código se requiere de un mayor ancho de banda. Por otra parte la interferencia producida por una frecuencia de banda estrecha durante la transmisión es prácticamente suprimida por el uso de este código como se muestra en la siguiente figura.

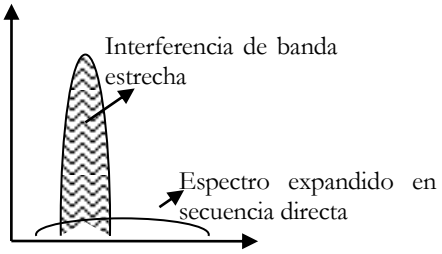


Fig. 1.4 Interferencia de banda estrecha suprimida en DSSS

Una vez codificado cada bit de información, el receptor realiza la operación inversa al compactar y mapear con el mismo código la secuencia de bits procesados para regresar al bit de datos original. El receptor debe estar perfectamente sincronizado para recibir el código correcto por lo que mientras la transmisión puede llevarse de una manera asíncrona cada paquete DSSS debe estar precedido por una petición de sincronización con el receptor de dicho paquete.

Cuando el código es generado por el receptor y es perfectamente sincronizado con la señal recibida, el proceso de volver compactar esa expansión de bits produce lo que se le denomina picos de alta auto correlación como se muestra a continuación.

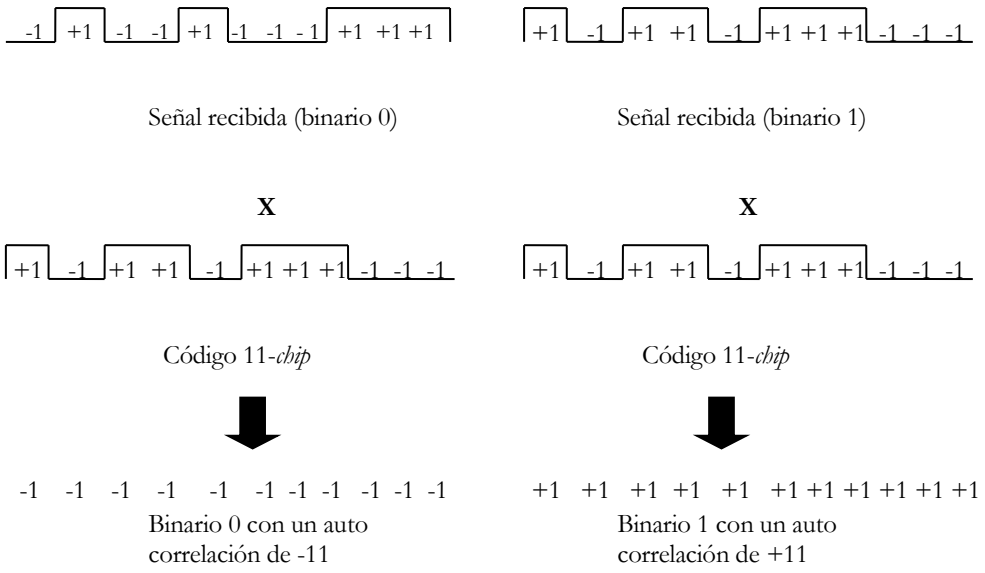


Fig. 1.5 Código sincronizado con una alta auto correlación

Si el código es cambiado de posición uno o más intervalos *chip* tanto a la derecha como a la izquierda el resultado es una baja auto correlación.

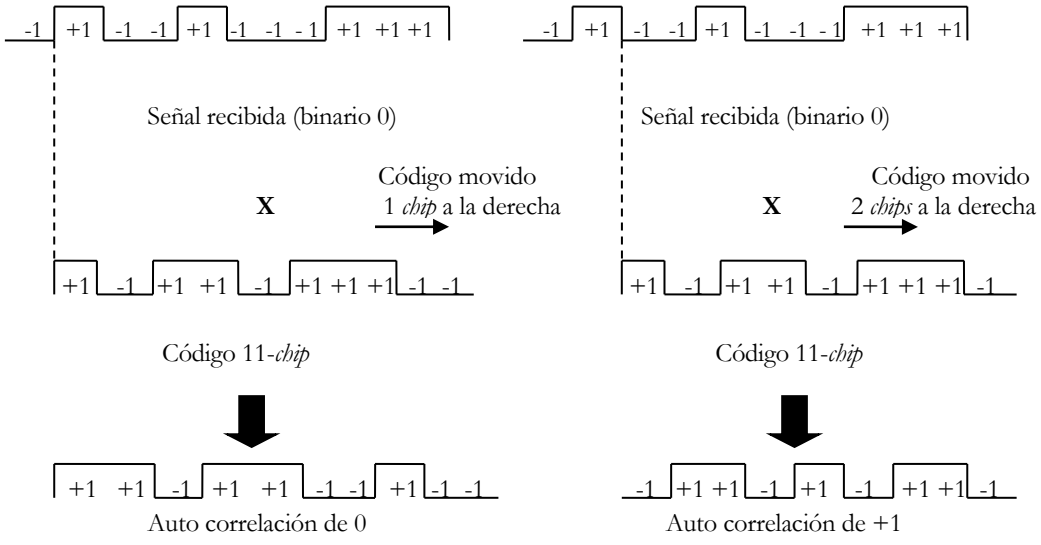


Fig. 1.6 Código con una baja auto correlación

La alta auto correlación ocurre de manera periódica por lo que la presencia de interferencias puede ser rechazada dado que no coinciden con los picos deseados.

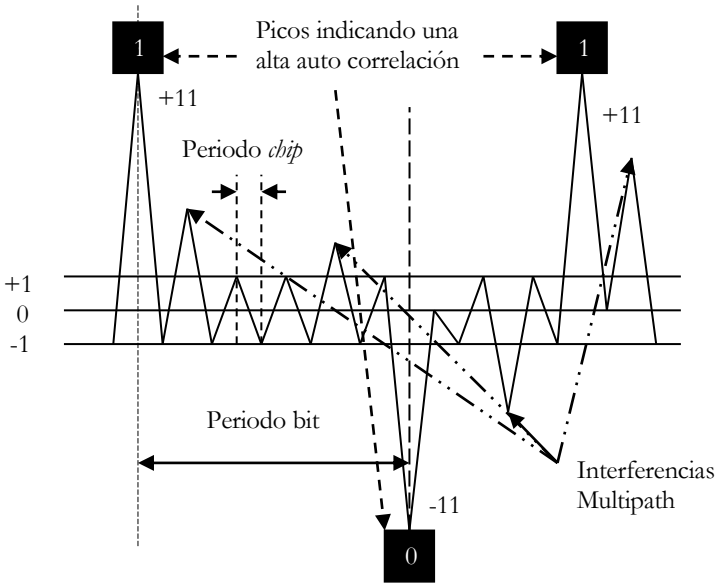


Fig.1.7 Picos de auto correlación en una señal DSSS

DSSS opera en el rango que va desde los 2.4GHz hasta los 2.4835GHz, con un ancho de banda total disponible de 83.5MHz. Este ancho de banda se divide en un total de 11 canales con un ancho de banda de aproximadamente 22 MHz por canal de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular. En el caso de México son 11 canales.

En topologías de red en donde existe un área cubierta por varios dispositivos, los canales pueden operar simultáneamente sin apreciarse interferencias. La separación entre las frecuencias es de 30MHz. Esto significa que de los 83.5MHz de ancho de banda total disponible se pueden obtener hasta 3 canales independientes que pueden operar simultáneamente en una determinada zona geográfica sin que aparezcan interferencias en un canal procedentes de los otros dos canales. Esta independencia entre canales nos permite aumentar la capacidad, en cuanto a cobertura, de una forma lineal con el número de puntos de acceso operando en un canal que no se esté utilizando y hasta un máximo de tres canales.

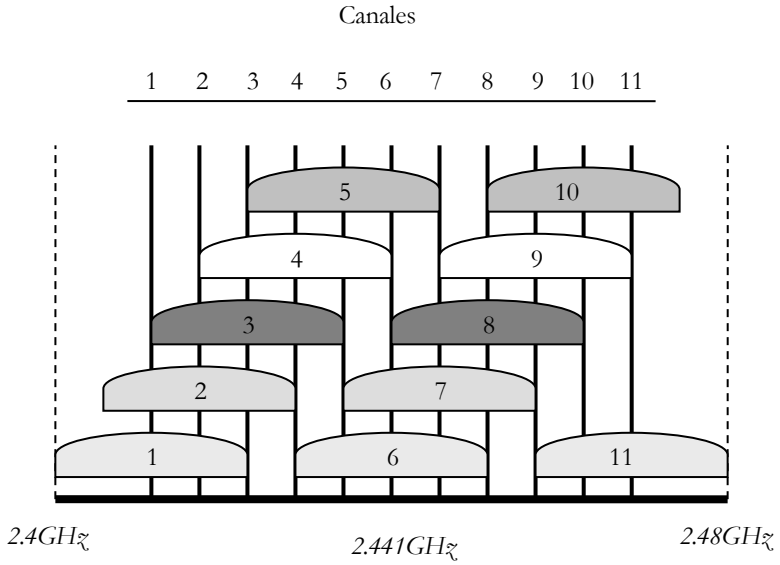


Figura 1.8 DSSS

Salto de Frecuencia (*Frequency Hopping Spread Spectrum,* FHSS).

La técnica consiste en transmitir una parte de la información en un determinado canal dentro de la frecuencia durante un intervalo de tiempo llamado *dwell time*, inferior a 400ms. Una vez transcurrido este tiempo se cambia la frecuencia del canal de emisión y se sigue transmitiendo a otro canal. De esta manera cada tramo de información se va transmitiendo en un canal distinto durante un intervalo de tiempo muy corto a lo largo de todo el ancho de banda de la frecuencia de 2.4GHz.

Este procedimiento equivale a realizar una partición de la información en el dominio del tiempo. El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según un patrón de salto conocido tanto por el emisor como por el receptor. Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación el efecto pareciera que, aunque vamos cambiando de canal físico con el tiempo, se mantiene un único canal a través del cual se desarrolla

la comunicación. El número de canales en el patrón de saltos esta restringido a 75 o más canales con un ancho de banda aproximado de 1MHz.

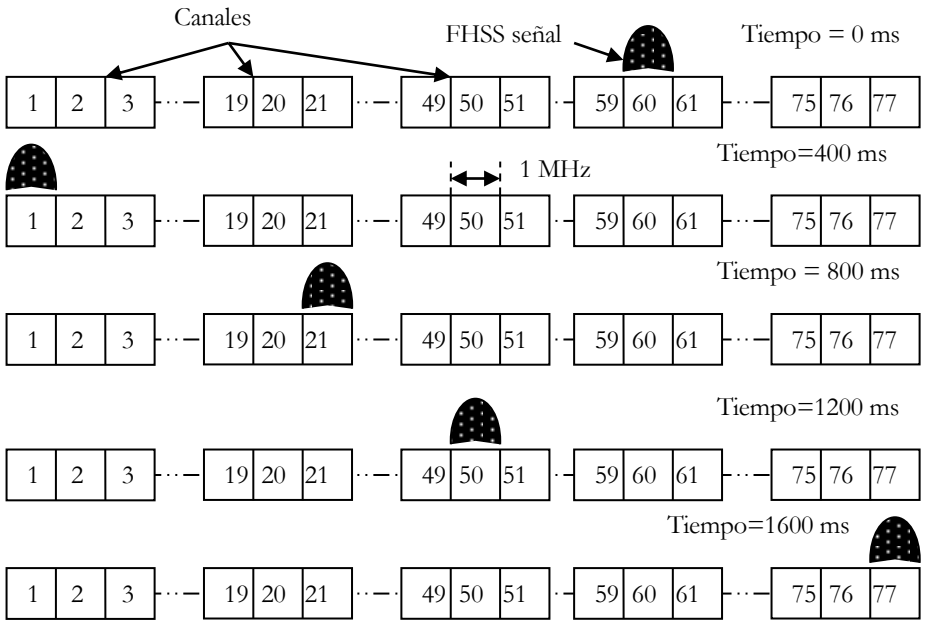


Fig. 1.9 FHSS

Diferencias, ventajas y desventajas de las técnicas de modulación.

- FHSS reduce el ruido eléctrico y permite que coexistan varias comunicaciones en la misma banda de frecuencias.

- El aprovechamiento o rendimiento (relación entre bits informativos y número total de bits enviados) del canal es mejor con DSSS que con FHSS. Esto se debe a que FHSS utiliza un protocolo más complejo que DSSS. Este

protocolo permite mayores capacidades en cuanto a movilidad y robustez que el que usa DSSS que es mas sencillo y proporciona velocidades de transferencia de datos más elevadas en conexiones punto a punto (entre salto y salto FHSS necesita un tiempo para revisar la banda, identificar la secuencia de salto y asentarse en la misma).

- La capacidad de proceso o *throughput* efectivo total de la red es superior en FHSS debido a que puede ofrecer un mayor número de canales sin traslape.

- La ventaja de FHSS frente a DSSS es que con esta técnica podemos tener varios puntos de acceso en la misma zona geográfica sin que existan interferencias si se cumple que dos comunicaciones distintas no utilizan el mismo canal dentro de la frecuencia en un mismo instante de tiempo.

- Un aspecto importante a considerar es la interferencia denominada *multipath* o de múltiples vías asociada estrechamente a las comunicaciones por radio. Esta interferencia consiste en una distorsión de la señal, originada por la reflexión múltiple de las ondas de radio en estructuras como paredes, puertas, etc. Esto hace que la señal dispersada llegue a la antena receptora con una serie de múltiples señales en instantes ligeramente diferentes, lo que genera una atenuación de la señal conocida como *fading*. En este contexto, FHSS es inmune debido a su propia estructura, ya que al estar basado en el salto a diferentes frecuencias, el *multipath* queda automáticamente contrarrestado. Sin embargo, DSSS puede solucionar este problema aumentando la capacidad de la antena, lo que genera un mayor costo y mayor complejidad.

- Comercialmente en el mercado en la actualidad en México solo se encuentran puntos de acceso que operan con DSSS.

1.2 Conjunto de protocolos 802.11

802.11 es un estándar desarrollado por el Instituto de Ingenieros Eléctricos y Electrónicos IEEE enfocado a redes inalámbricas y cuyas primeras especificaciones se remontan al año 1990. La norma ha sufrido diversas extensiones a lo largo de estos años con el fin de obtener modificaciones y mejoras. De esta manera, tenemos las siguientes especificaciones:

- **802.11**: Especificación para 1-2Mbps en la banda de los 2.4GHz, usando FHSS o DSSS.
- **802.11b**: Extensión del 802.11 para proporcionar 11Mbps usando DSSS. También conocido como Wi-Fi (*Wireless Fidelity*) promulgado por el WECA (*Wireless Ethernet Compatibility Alliance*) para certificar productos 802.11b capaces de interoperar con los de otros fabricantes. El costo es económico y el alcance es habitualmente entre 30 y 46 metros en interiores según la estructura, los materiales de construcción y la distribución.
- **802.11a**: Estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54Mbps, apoyándose en la banda de los 5GHz, usando OFDM (*Orthogonal Frequency Division Multiplexing*). A su vez, elimina el problema de las interferencias múltiples que existen en la banda de los 2.4GHz (hornos microondas, teléfonos digitales, etc.). Su costo es relativamente más caro y el alcance es entre 8 y 23 metros en interiores.
- **802.11g**: Extensión de 802.11 para proporcionar 20-54Mbps usando DSSS y OFDM. Es compatible hacia atrás con 802.11b y tiene mayor alcance y

menor consumo de potencia que 802.11a. Su costo es relativamente económico y su alcance es entre 30 y 46 metros en interiores según la estructura, los materiales de construcción y la distribución.

- **802.11i**: Estándar en experimentación, el cual es una actualización que pretende dotar Wi-Fi de una mayor seguridad. Cabe mencionar que 802.11i se aplicará sobre los equipos 802.11a/b/g existentes.

Específicamente el estándar 802.11 describe la funcionalidad de las capas de acceso MAC y física PHY. El principal objetivo del servicio descrito en el estándar es la entrega de unidades de datos MSDU (*MAC Service Data Units*) entre unidades de control lógico de conexión LLC (*Logical Link Controls*).

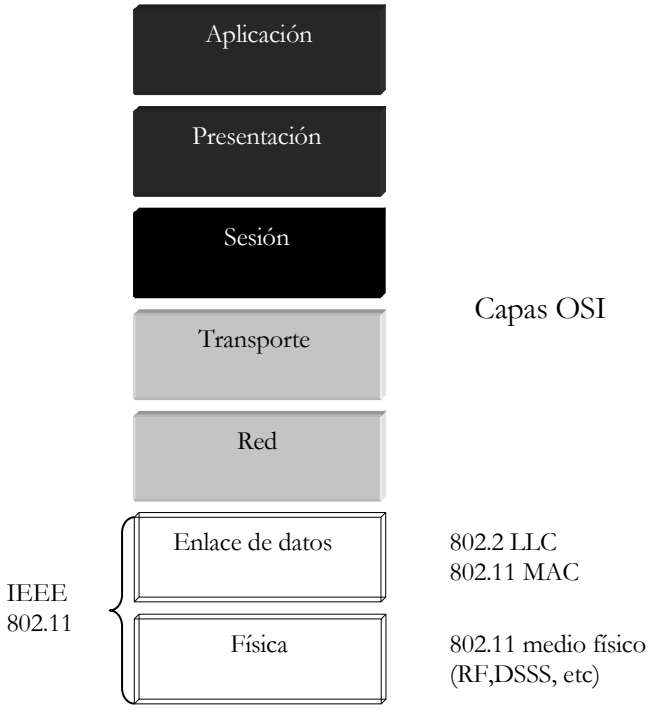


Figura 1.10 Modelo de referencia OSI

La capa física de cualquier red define la modulación y la señalización características en la que se van a transmitir o recibir los datos. En la capa física, se definen dos métodos o tecnologías de transmisión RF e infrarrojo.

Asimismo la capa MAC tiene similitudes a la de *Ethernet* cableada (IEEE 802.3) usando el protocolo CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*) para la detección de colisiones, pero en este tipo de redes descubrir dichas colisiones es difícil debido a que se trata de un medio inalámbrico. Un factor importante es determinar si un canal está vacío, para este fin se utiliza un algoritmo de estimación de desocupación de canales o lo que es lo mismo CCA (*Clear Channel Assessment*), el cuál realiza una medición de la energía RF (*Radio Frecuencia*) de la antena y determina la intensidad de la señal recibida, denominada RSSI (*Received Signal Strength Indication*). Además, la capa MAC controlará aspectos como los de sincronización y los algoritmos del sistema de distribución, que se definen como el conjunto de servicios que propone el modo infraestructura.

Nivel de acceso al medio

La arquitectura MAC del estándar 802.11 se compone de dos funcionalidades básicas: la función de coordinación puntual PCF (*Point Coordination Function*) y la función de coordinación distribuida. DFC (*Distributed Function Coordination*).

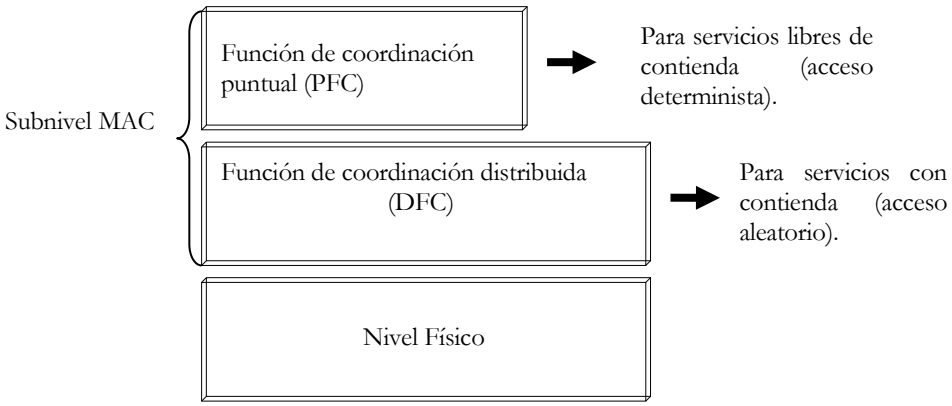


Figura 1.11 Arquitectura MAC del 802.11

Función de Coordinación Distribuida

Se define función de coordinación como la funcionalidad que determina, dentro de un conjunto básico de servicios BSS (*Basic Service Set*), cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico. En el nivel inferior del subnivel MAC se encuentra la función de coordinación distribuida y su funcionamiento se basa en técnicas de acceso aleatorias de pelea o contienda por el medio. El tráfico que se transmite bajo esta funcionalidad es de carácter asíncrono ya que estas técnicas de contienda introducen retardos aleatorios y no predecibles, no tolerados por los servicios síncronos.

Las características de DFC las podemos resumir en estos puntos:

- Utiliza MACA (*Multi Access Collision Avoidance*) como protocolo con (CSMA/CA con RTS (*Request To Send*)/CTS (*Clear To Send*) para acceder al medio

- Realiza los reconocimientos de ACK (*Acknowledgement*), provocando retransmisiones si no se recibe

- Usa un campo de *Duration/ID* que contiene el tiempo de reserva para transmisión y ACK. Esto quiere decir que todos los nodos conocerán al escuchar cuando el canal volverá a quedar libre

- Implementa fragmentación de datos

- Concede prioridad a tramas mediante el espaciado entre éstas IFS (*Inter Frame Space*)

- Soporta *Broadcast* y *Multicast* sin ACK

Intervalos de espaciado estándar

El estándar 802.11 define varios intervalos de espaciado estándar (IFS) que aplazan el acceso de una estación al medio y proporcionan varios niveles de prioridad. Cada intervalo indica el tiempo entre el final de la trama anterior y el comienzo de la trama siguiente:

- SIFS (Short IFS): Es el intervalo más corto y proporciona la prioridad máxima, permitiendo a algunas tramas acceder al medio antes que otras. Las tramas ACK, CTS emplean este intervalo.

- PIFS (PCF IFS): Se utiliza en las estaciones que operan bajo el modo de función de coordinación puntual y lo emplean para conseguir el medio.

- DIFS (DCF IFS): Se utiliza en las estaciones que operan bajo el modo de función de coordinación distribuida y lo emplean para conseguir el medio.

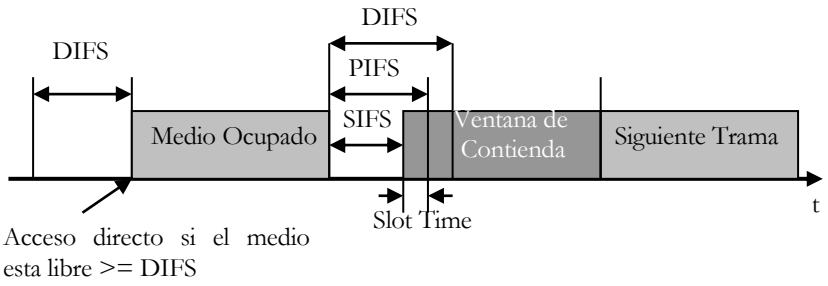


Figura 1.12 Intervalos de espaciado

Protocolo de Acceso al medio CSMA/CA y MACA

El algoritmo básico de acceso a este nivel es muy similar al implementado en el estándar IEEE 802.3 y es el llamado CSMA/CA. Este algoritmo funciona tal y como se describe a continuación:

1. Antes de transmitir información una estación debe revisar el medio, o canal inalámbrico, para determinar su estado (libre/ocupado).

2. Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada espaciado entre tramas IFS.

3. Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.

4. Una vez que finaliza esta espera, debida a la ocupación del medio, la estación ejecuta el llamado algoritmo de *backoff*, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda CW (*Cotention Window*). El algoritmo de *backoff* nos da un número aleatorio y entero de ranuras temporales (*slot time*), de 20μs, y su

función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

5. Mientras se ejecuta la espera marcada por el algoritmo de *backoff* se continúa escuchando el medio de tal manera que si éste se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranuras temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de *backoff* queda suspendido hasta que se cumpla esta condición.

Cada retransmisión provocará que el valor de CW, que se encuentra entre CWmin y CWmax, se duplique hasta encontrar su valor máximo.

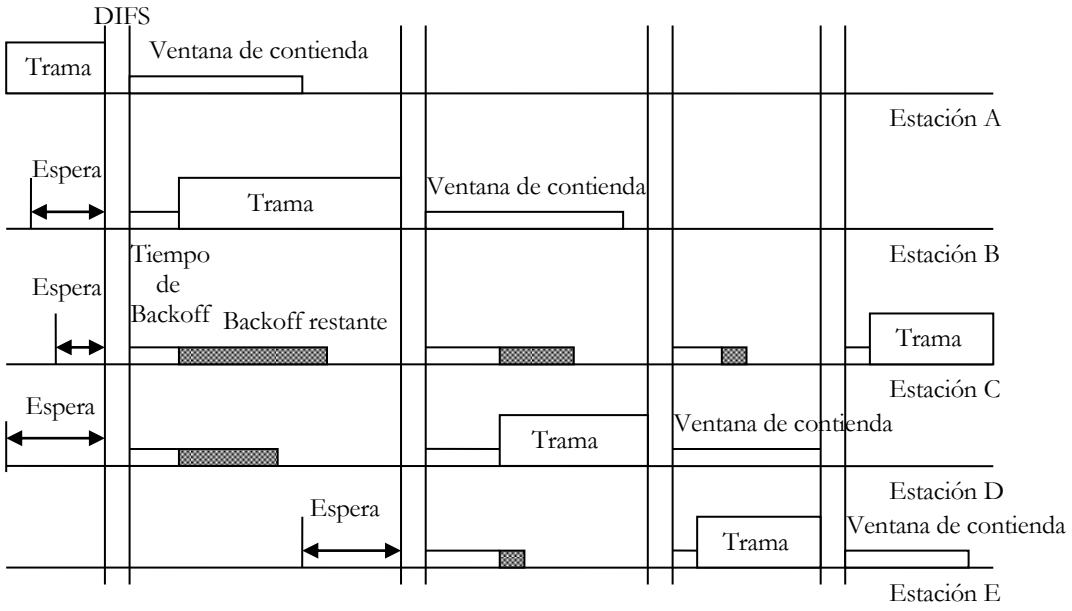


Figura 1.13 Algoritmo CSMA/CA

Sin embargo, CSMA/CA en un entorno inalámbrico y celular presenta una serie de problemas:

- Nodos ocultos. Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye. Esto puede romper un 40% o más de las comunicaciones en un ambiente LAN muy cargado. Ocurre cuando hay una estación en un grupo de servicio que no puede detectar la transmisión de otra estación y así descubrir que el medio está ocupado.

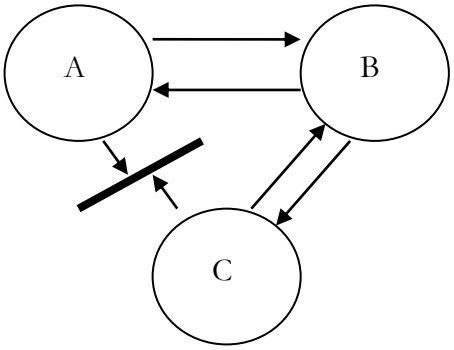


Figura 1.14 Nodo oculto

En la *figura 1.14* las estaciones A y B se pueden comunicar. Sin embargo, una obstrucción impide a la estación C recibir de la estación receptora A y no puede determinar cuándo está ocupado el canal. Por lo tanto ambas estaciones A y C podrían intentar transmitir a la vez a la estación B el uso de las secuencias RTS/CTS.

- Nodos expuestos. Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

La solución que propone 802.11 es MACA. Según este protocolo, antes de transmitir el emisor envía una trama RTS, indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS, repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos.

Los métodos para evitar los nodos ocultos y expuestos pueden seguir dos normas:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS

- Al escuchar un CTS, hay que esperar según la longitud

La solución final de 802.11 utiliza MACA con CSMA/CA para enviar los RTS y CTS.

Las estaciones tienen un conocimiento específico de cuándo una estación, que tiene el control del medio mientras está transmitiendo o recibiendo, va a finalizar su periodo de reserva del canal. Esto se hace a través de una variable llamada NAV (*Network Allocation Vector*) que mantendrá una predicción de cuándo el medio quedará liberado. Tanto al enviar un RTS como al recibir un CTS, se envía el campo *Duration/ID* con el valor reservado para la transmisión y el subsiguiente reconocimiento. Las estaciones que estén a la escucha modificarán su NAV según el valor de este campo *Duration/ID*. En realidad, hay una serie de normas para modificar el NAV, una de ellas es que el NAV siempre se situará al valor más alto de entre los que se disponga.

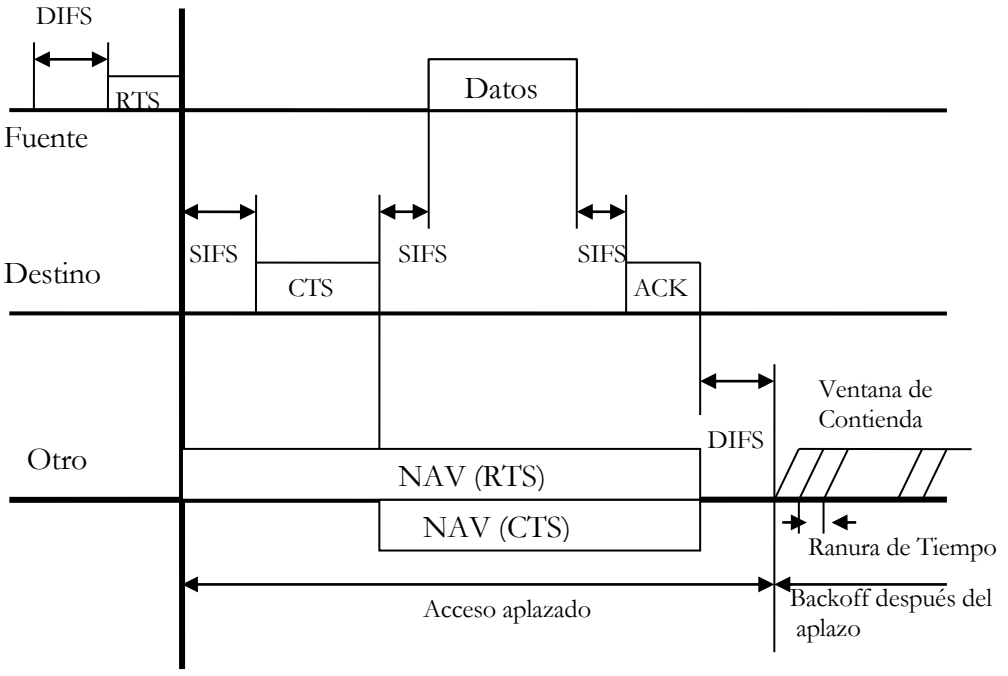


Figura 1.15 MACA

Función de Coordinación Puntual

Como podemos observar en la *Figura 1.11* por encima de la función de coordinación distribuida DFC se sitúa la función de coordinación puntual PFC. Como método de acceso opcional el estándar 802.11 define que esta función es asociada a las transmisiones libres de contienda que utilizan técnicas de acceso deterministas. Esta funcionalidad está pensada para servicios de tipo síncrono que no toleran retardos aleatorios en el acceso al medio, por ejemplo aplicaciones de video *streaming*, o voz donde la transmisión debe producirse de un modo adecuado.

Los puntos de acceso tienen la opción de ser configurados para operar bajo este modo. Sin embargo no todos los fabricantes cuentan con esta posibilidad de acceso al medio inalámbrico. Dentro del punto de acceso se encuentra lo que se denomina un punto coordinador PC (*Point Coordinator*) cuya función es determinar cuáles estaciones pueden transmitir durante un periodo de tiempo dado, que se denomina periodo libre de contención CFP (*Contention Free Period*).

El PC circula a través de todas las estaciones operando en el modo PFC y va eligiendo alguna de estas durante un determinado periodo de tiempo. Por ejemplo el PC quizá primero elija a la estación A y durante un periodo específico de tiempo esta estación pueda transmitir tramas de datos, negando esta posibilidad a cualquiera otra estación. El PC entonces elegirá la siguiente estación y continuará descendiendo en la lista de estaciones elegidas en la que cada una de estas tendrá su oportunidad de enviar datos. La concesión de estas transmisiones se lleva acabo bajo un riguroso listado y no se permitirá que se envíen dos tramas hasta que la lista se haya completado.

De esta manera, PFC es un protocolo libre de contención el cual habilita a las estaciones para transmitir tramas de datos de manera síncrona con un tiempo regular de retraso entre la transmisión de las mismas. Esto hace posible una mayor efectividad en la transmisión de una información fluida, como lo son los casos de voz y video por Internet como ya se ha mencionado.

Para más información sobre el formato de una trama MAC ver el *apéndice A*.

1.3 Factor de reuso

802.11 establece que las redes inalámbricas tendrán una estructura celular. Una célula será el área donde las estaciones inalámbricas puedan comunicarse entre si o con un punto de acceso. Sólo puede haber un punto de acceso por célula. Con una única célula podemos crear una red independiente o una extensión de una red cableada. Los dos modelos básicos reconocidos por el estándar son:

- Redes Ad-hoc o punto a punto.

- Redes de infraestructura.

1.3.1 Redes Ad-hoc (punto a punto)

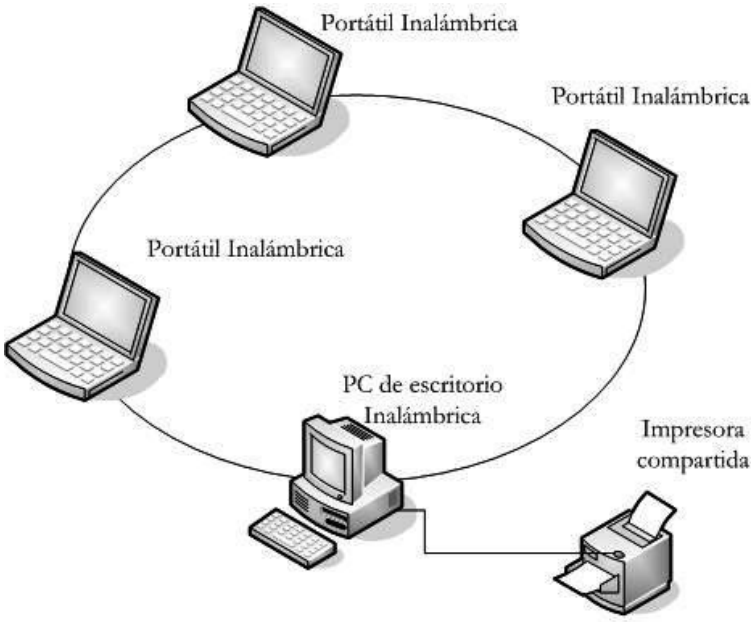


Figura 1.16 Redes ad-hoc

El estándar denomina a este modo como un servicio básico independiente IBSS (*Independent Basic Service Set)* con un costo bajo y flexible. Las comunicaciones entre los múltiples nodos se establecen sin el uso de ningún servidor u otro medio como pueden ser los puntos de acceso.

1.3.2 Redes de infraestructura.

En este modo, cada cliente de la red envía todas sus comunicaciones a una central o punto de acceso. Para efectuar el intercambio de datos, préviamente los clientes y los puntos de acceso establecen una relación de confianza. Los puntos de acceso pueden emplearse dentro de la LAN inalámbrica como:

- *Gateway* o *Router* (puerta de enlace o ruteador) para comunicarse con redes cableadas externas (Internet, intranet, etc.).

- Repetidor de algún otro punto de acceso, ya comunicado con una red cableada.

- *Bridge* (puente) hacia otros puntos de acceso para extender los servicios de acceso.

- AP de datos entre el área de cobertura, abarcando los 30-46 metros en un entorno cerrado (dependiendo de la disposición y objetos que bloqueen las ondas de radio) o los aproximadamente 100 metros en espacios abiertos.

Estos puntos de acceso dependiendo de su fabricante tienen aproximadamente un soporte de 60 NICs (*Network Interface Cards*), o de 253 NICs si se trata de un ruteador inalámbrico, dentro de su área de servicio. Sin embargo algunos mecanismos de seguridad como la lista de filtrado MAC sólo tienen un soporte hasta de 40 direcciones MAC de estos NICs. Para solucionar este problema se opta por poner en funcionamiento varios puntos de acceso al mismo tiempo, ampliando así las posibilidades de *roaming* de un equipo móvil, sin perder la conexión, ya sea configurándolo como repetidor o como una nueva infraestructura con características en común con las ya existentes en el entorno.

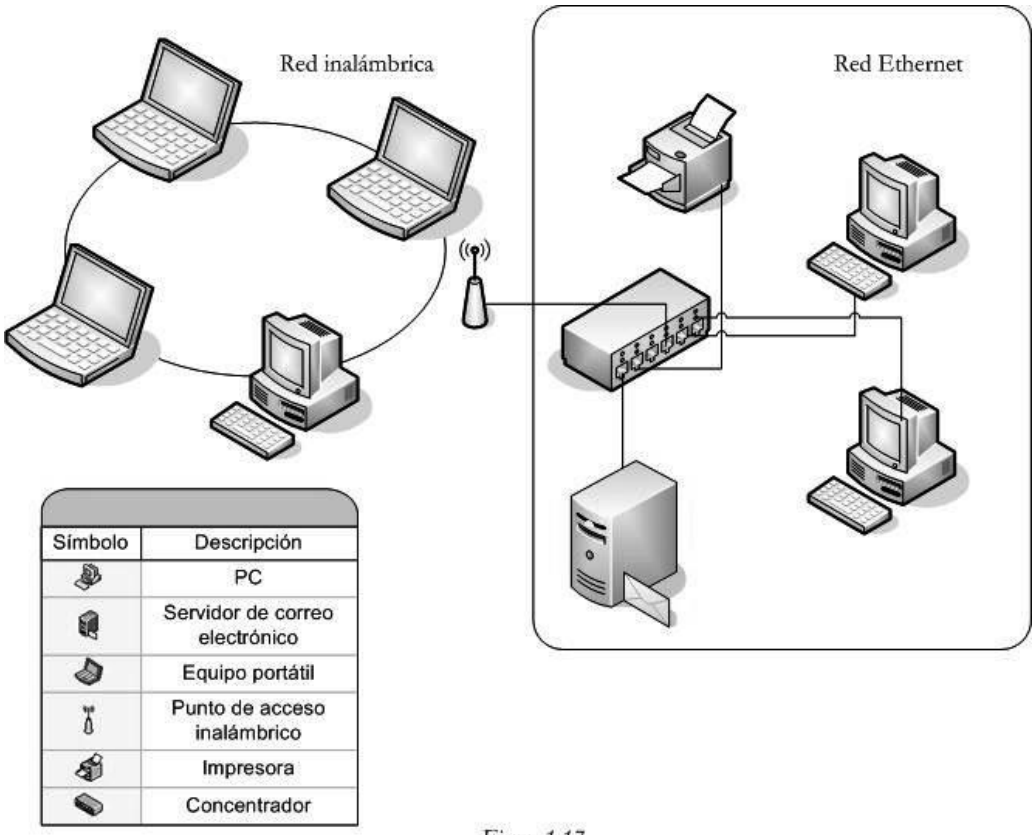


Figura 1.17
Redes de infraestructura

También es posible unir varias células mediante la instalación de múltiples puntos de acceso o puentes (*bridges*) que a su vez estarían unidos por un bus troncal (*backbone*).

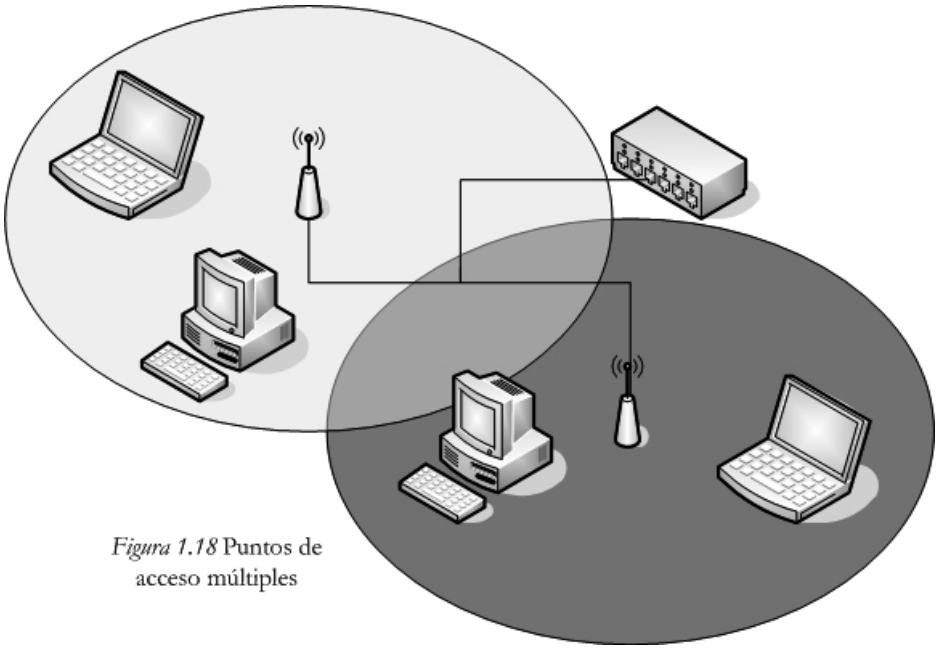


Figura 1.18 Puntos de acceso múltiples

Además de la ampliación de la zona de servicio, la subred inalámbrica proporciona la posibilidad de desplazarse dentro de ella por parte de los equipos portátiles, que al perder contacto con su punto de acceso pasan a buscar otro, sin perder la comunicación.

En los sistemas celulares, el área de cobertura de un operador es dividida en celdas. Una celda corresponde a una zona cubierta por un transmisor o una pequeña colección de transmisores. El tamaño de la celda depende de la potencia del transmisor, banda de frecuencia utilizada, altura y posición de la antena, el tipo de antena, la topografía del área y la sensibilidad del radio receptor.

Por lo anterior, el concepto de reuso de frecuencias (*Frequency Reuse*) se refiere al uso de las mismas frecuencias portadoras para cubrir distintas áreas separadas por una distancia suficientemente grande para evitar interferencia co-canal.

El factor de reuso es el número de conjunto de canales requeridos para el sistema de planos celulares. En la siguiente figura se muestra un ejemplo del factor de reuso para un sistema de planos celular donde K es el factor de reuso.

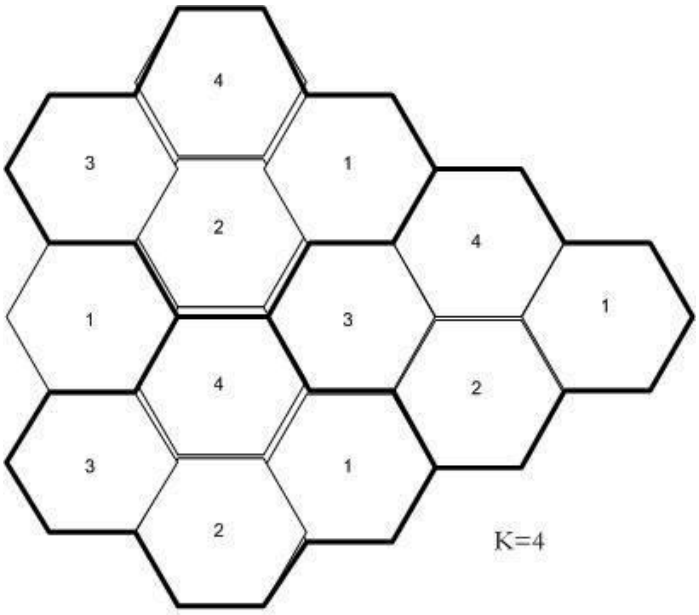


Figura 1.19 Factor de reuso

1.4 Factor de distancia

Este factor está en función del diseño del producto y de la forma de propagación de la señal, enfocándonos exclusivamente a lugares cerrados. Las interacciones con objetos sólidos, paredes, ventanas, metales e incluso la misma gente, afectan a la propagación de la señal. Este problema es más notable cuando hablamos de propagación vía infrarrojo pero como la mayor parte de los sistemas de redes inalámbricas usan radio frecuencia RF este problema no es tan notorio debido a que una de las características de las RF es la posibilidad de penetrar en la mayor parte de lugares cerrados y con obstáculos.

El rango de cobertura de una LAN inalámbrica va de 30m a 100m. Claro que esto puede extenderse y obtener un mayor grado de movilidad utilizando un mayor número de puntos de acceso que permiten navegar a través de toda la red inalámbrica, similar a lo que se usa en la telefonía celular.

A continuación se muestra una tabla con las perdidas de la señal inalámbrica según el medio por el que esté atravesando[3].

Medio	Perdida (dB)
Ventana en pared de ladrillo	2
Pared de vidrio con marco de metal	6
Paredes en general (no de ladrillo, tabla roca)	6
Puertas de metal	6
Puerta de metal en pared de ladrillo	12.4
Pared de ladrillo a lado de puerta de metal	3

1.5 Puntos de Acceso

Los puntos de acceso son dispositivos que validan y retransmiten la información recibida, por lo que la colocación de estos debe hacerse en un punto en el cual puedan abarcar toda el área en la que se encuentren nuestros equipos.

[3] http://linksys.custhelp.com

La ubicación de un punto de acceso inalámbrico debe ser en un lugar alto y central. Si la red consiste de varios pisos, es conveniente ubicar el punto de acceso inalámbrico en el piso más alto. Si el usuario quiere conectarse desde afuera del recinto hacia dentro, el punto de acceso inalámbrico deberá ubicarse cerca de una ventana. Es necesario mantenerlo retirado de objetos de metal grandes, así como de hornos de microondas y teléfonos inalámbricos de frecuencia 2.4GHz. Si se tienen teléfonos inalámbricos que operen en esa frecuencia es necesario cambiar el canal en el que transmite el punto de acceso[4].

La mayoría de las antenas de los equipos inalámbricos son antenas internas incluidas dentro del mismo dispositivo sea éste un punto de acceso o un adaptador de red inalámbrico. Estas antenas ofrecen la gran ventaja de la comodidad al formar parte del propio dispositivo, pero tienen el inconveniente del alcance. Si se necesita aumentar el alcance sin instalar nuevos puntos de acceso, la mejor solución es colocar una antena con mayor alcance.

[4] http://linksys.custhelp.com

C a p í t u l o 2

SEGURIDAD DE LA INFORMACIÓN EN LAS REDES INALÁMBRICAS

2.1 Comunicación Segura

El término de seguridad de la información se refiere a la prevención y a la protección, a través de ciertos mecanismos, para evitar que ocurra de manera accidental o intencional, la transferencia, modificación, fusión o destrucción no autorizada de la información. Es importante remarcar que en el flujo de la información no debe existir ningún tipo de obstáculo para que la información llegue al destinatario[1]. Las categorías generales de ataques o amenazas son las siguientes:

- Interrupción: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la *disponibilidad*. Un ejemplo de este tipo de ataque es la destrucción de un elemento de hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.
- Intercepción: un usuario no autorizado consigue el acceso a un recurso. Este es un ataque contra la *confidencialidad*. Este usuario puede ser una persona física o un programa de software. Un ejemplo de este ataque es tener acceso a una línea para hacerse de datos que circulen por la red y

[1] http://www.fi-b.unam.mx/index2.html.

realizar la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de los paquetes para revelar la identidad de uno o mas de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

- Modificación: un usuario no autorizado no solo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la *integridad*. Un ejemplo de este ataque lo encontramos en el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- Suplantación: un usuario no autorizado inserta objetos falsificados en el sistema. Este es un ataque contra la *autenticidad*. Un ejemplo de este ataque es la inserción de mensajes ilegítimos en una red o añadir registros a un archivo.

Uno de los principales problemas de una red inalámbrica son los aspectos de seguridad de la información en el tráfico de la misma, dado que cualquier individuo con una antena y una computadora portátil puede interceptar el tráfico entre las estaciones clientes y el punto de acceso, obteniendo de este acto, algún beneficio modificando o eliminando información. Por este motivo uno de los primeros pasos a considerar en el diseño e implementación de una infraestructura inalámbrica es la seguridad.

Comúnmente las estaciones inalámbricas, en su mayoría, son equipos portátiles *laptops*. Esto con el fin de aprovechar sus condiciones de movilidad y portabilidad que las hacen diferentes a una estación normal. Estos equipos normalmente son administrados por el propio usuario por lo que no existe un control directo sobre

estos, debilitando de esta manera la seguridad y por lo que se convierten en un punto idóneo de ataque sobre toda la infraestructura inalámbrica.

Existen dos principales consideraciones de seguridad para el uso de una computadora cliente dentro de una red inalámbrica. La primera es el compromiso por el propio usuario de no alterar, robar o eliminar información que no le pertenezca, así como de no proveer a un individuo externo a la institución una puerta de entrada a toda la infraestructura de red. Como podemos ver esta primera consideración se vuelve muy vulnerable ya que no puede depender la integridad de las personas. Los individuos en su mayoría, salvo algunas excepciones, no cuentan con conocimientos sólidos en cómputo y seguridad, por lo que son un riesgo latente. Una alternativa es que existan políticas de uso con algún tipo de sanción considerable al individuo que sea detectado en algunos de los actos anteriormente citados. La segunda consideración, es usar métodos seguros de comunicación con otros servicios de red externos a la infraestructura inalámbrica como lo son SSL (*Secure Socket Layer*) y SSH (*Secure Shell*).

2.1.1 SSL (Secure Socket Layer)

Supongamos que deseamos hacer una transferencia bancaria de una cuenta a otra, dado que para realizar esta operación es necesario enviar información confidencial como el número de cuenta, el monto del traspaso y la clave de autenticación. Es muy importante que esta operación se efectué de manera privada. SSL utiliza un esquema de llave pública / privada en donde la llave pública se utiliza para encriptar el mensaje y la llave privada para desencriptarlo, la diferencia entre éstas radica en que en la llave de carácter público, cualquier persona tiene la posibilidad de acceder a ella, mientras que en la de carácter privado sólo una persona es capaz de desencriptar los mensajes recibidos y por lo tanto es de vital importancia su

anonimato. Así, la transferencia bancaria se realiza mediante una llave pública proporcionada por el banco que nosotros utilizamos al hacer algún traspaso y que sólo el banco tenga la posibilidad de leer mediante una llave privada.

Aun con este tipo de mecanismo continúa existiendo la posibilidad de que alguien intercepte y modifique el mensaje que estamos enviando a la institución bancaria dado que estamos utilizando una llave de carácter pública. Para evitar este problema existe un mecanismo llamado *Message Digest* que consiste en crear un pequeño resumen del mensaje para poder enviarlo al banco junto con el mensaje completo y de esta manera cuando el banco recibe el mensaje crea su propio *digest* y lo compara con el que enviamos, si ambos coinciden esto significa que el mensaje fue recibido intacto.

Ahora el siguiente problema es asegurarnos que el *digest* llegue a su destino en forma segura. Para resolverlo, existe otro mecanismo llamado firmas digitales (*Digital Signatures*). Al incluir el mensaje que enviamos dentro de una firma digital nos aseguramos de que nadie mas pueda cambiar el *digest*. Las firmas digitales utilizan también una llave privada para encriptar el *digest* y una llave pública para realizar la operación contraria enviando y comprobando tanto la autenticidad del mismo, como la coincidencia de este con el *digest* creado por el banco.

Aunque hemos enviado el mensaje al banco. Y hemos firmado y asegurado la integridad del mismo, aun necesitamos estar seguros que realmente existe una comunicación con el banco, es decir, necesitamos saber que la llave publica que estamos utilizando corresponde a la llave privada que posee el banco y a su vez el banco necesita verificar que la firma del mensaje realmente corresponde a nuestra firma. Para solucionar esto existen los certificados los cuales asocian una llave pública con la identidad real del individuo, servidor, o cualquier otro tipo de

entidad, así como también contienen la vigencia del mismo y la identificación de la entidad certificadora que emitió el certificado.

El protocolo SSL es un protocolo que se sitúa entre la capa de red y la capa de aplicación, según el modelo OSI. Este protocolo proporciona mecanismos para establecer una comunicación segura entre un cliente y un servidor, utilizando, como hemos visto, autenticación, firmas digitales y métodos de encriptación. SSL soporta un rango de algoritmos de criptografía, algoritmos de *digest* y de *digital signatures*. Esto le permite a los servidores, la posibilidad de elegir entre qué tipos de algoritmos se van a utilizar para establecer la comunicación entre el cliente y el servidor al inicio de una sesión.

Una sesión de SSL se establece por medio de un *handshake*[2] entre el cliente y el servidor, la secuencia varía si el servidor entrega un certificado o solicita el certificado del cliente.

Uno de los usos mas comunes de SSL es el de establecer una comunicación Web segura entre un navegador (*Browser*) y un Webserver. HTTPS (Hyper Text Transfer Protocol Secure) es básicamente HTTP sobre SSL. Es importante hacer notar que el uso de HTTPS no impide en caso alguno el uso de HTTP, es por este motivo que la mayoría de los navegadores hacen una advertencia cuando una página Web tiene elementos o entornos no seguros a una que sí los tiene y viceversa, es decir, (*http -> https o https -> http*) también puede observarse este cambio en el icono en forma de candado que aparece en la parte inferior derecha de los navegadores que indica si la página es segura (candado cerrado) o insegura (candado abierto) como se muestra en la siguiente figura.

[2] Intercambio de señales entre maquinas conectadas a un canal de comunicación para asegurar la conexión mutua.

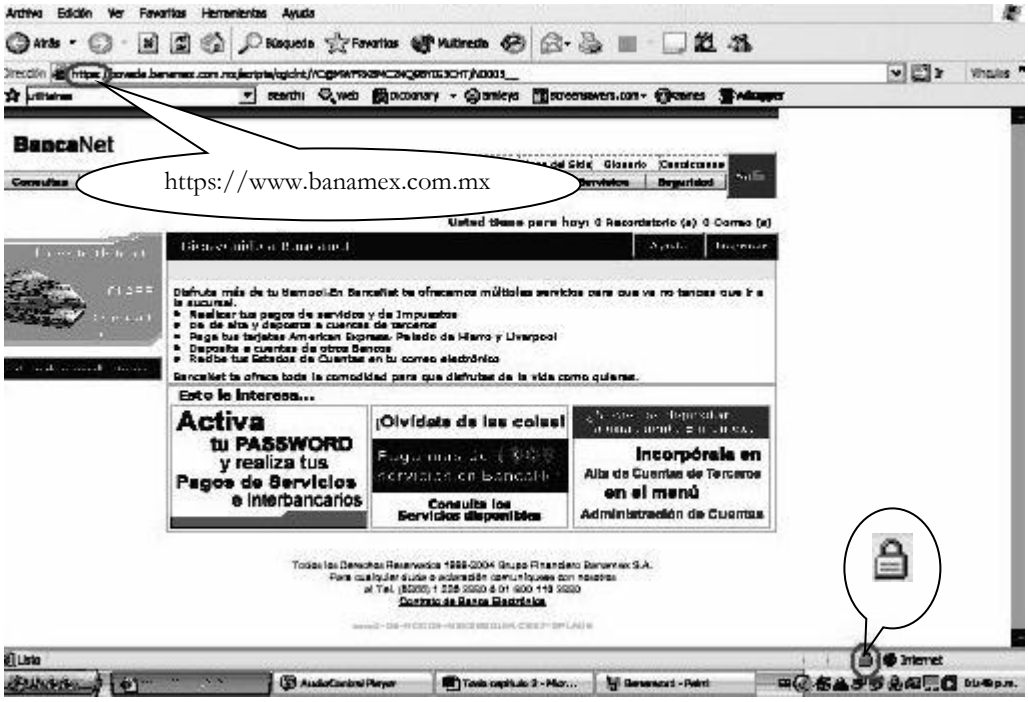


Figura 2.1 Sitio Web con SSL

2.1.2 SSH (Secure Shell)

SSH al igual que SSL utiliza mecanismos de llaves públicas y criptografía. La diferencia radica en que estas llaves no dependen de una autoridad certificadora que las emita. SSH puede usar varios cifrados simétricos cuando transfiere datos entre *hosts* permitiendo a los usuarios elegir el nivel de seguridad más adecuado según su necesidad. Cuando llamamos un comando *shell* en una estación cliente sobre una red inalámbrica, éste debería usar SSH en vez de *telnet* o un comando *r* (*rlogin, rcmd,* etc.) ya que SSH usado de una manera adecuada nos asegura que la integridad de los documentos y el tráfico de la red esté protegido contra *hackers*.

SSH permite tanto la redirección del flujo de datos a través de un mecanismo de "túneles" como el uso de algoritmos para su cifrado. Esto significa que una aplicación a ejecutar en lugar de ser gestionada directamente por los puertos del servidor y del cliente, es encapsulada en un túnel establecido al realizar la conexión, con la posibilidad de cifrar la información.

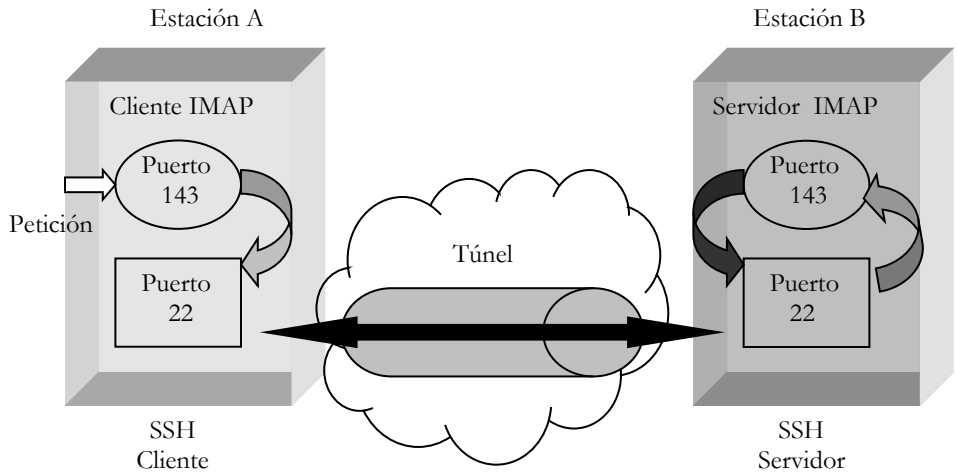


Figura 2.2 SSH

Suponiendo que tenemos una estación A en la que se ejecuta un cliente IMAP para leer o enviar correos electrónicos y deseamos conectarnos a una estación B en la que se encuentra el servidor IMAP para realizar dicha operación. El proceso que SSH realiza para establecer una conexión segura entre el cliente y el servidor se puede definir a través de los siguientes puntos.

- El usuario en la estación A abre un túnel con la estación B a través de la conexión por SSH.

- El usuario hace una petición de cliente IMAP para acceder a su servidor en la estación B. SSH, en la estación A, redirecciona la salida del puerto 143 al puerto 22.
- La petición viaja encapsulada a través del túnel hasta la estación B por el puerto 22.
- SSH recibe la petición y la redirecciona al puerto original (puerto 143) que utiliza el servidor IMAP para procesar la petición y entregar una respuesta.
- SSH recibe la respuesta del servidor IMAP y la vuelve a redireccionar al puerto 22 para regresarla a través del túnel.
- La respuesta viaja encapsulada a través del túnel hasta la estación A por el puerto 22.
- SSH recibe la respuesta y la entrega al cliente IMAP (estación A) permitiendo al usuario leer o enviar correos electrónicos de forma segura, protegido de usuarios maliciosos.

Habitualmente este tipo de conexiones son inseguras debido a que la contraseña de la cuenta de correo electrónico circula libremente sin ser cifrada entre las estaciones A y B. Sin embargo con SSH, se redireccionan este tipo de conexiones para pasar a través del túnel, cifrando de forma segura los datos. Este mecanismo de túneles y redireccionamiento de puertos nos permite ejecutar protocolos inseguros como Telnet, SMTP, IMAP, POP de manera segura.

2.2 Seguridad en el sistema operativo

Como ya hemos visto, cualquier computadora conectada a una red inalámbrica corre el riesgo de ser atacada por algún *hacker* cercano. Sin embargo una buena configuración en los dispositivos puede reducir estos riesgos. En la actualidad existen una variedad extensa de sistemas operativos como UNIX, FreeBSD, OpenBSD, Mac OSX, Linux, Windows, etc. En esta investigación nos enfocaremos a los dos sistemas operativos de mayor uso en el ambiente académico: MS Windows y Linux

2.2.1 Windows

Uno de los sistemas operativos más populares en el mundo de las computadoras, a nivel usuario, sin lugar a duda es Windows. El uso de Windows lejos de resultar un beneficio aumenta las probabilidades de sufrir un ataque cuyá probabilidad sea menor en otros sistemas operativos.

Para poder tener una estación segura conectada a una red inalámbrica, con Windows, hay que considerar ciertas medidas:

- Actualizaciones rutinarias o revisiones de los controladores o *firmware* de los dispositivos, ya sean tarjetas inalámbricas o puntos de acceso, permitirá obtener un mejor rendimiento de los dispositivos en cuestión.

- Continuamente, y como consecuencia de la creación de nuevos mecanismos, de ataques informáticos, surgen actualizaciones (*service pack*) del sistema operativo, las cuales tienen el propósito de ir llenando los *bugs* (errores) que se van descubriendo en el sistema y que pueden ser puntos

vulnerables para la seguridad tanto de la información como del mismo equipo. Estas actualizaciones pueden realizarse vía Web de forma automática o manual según la configuración más conveniente pero son de vital importancia ya que nos permiten disminuir el riesgo de contagio de virus informático y cerrar las posibles puertas por donde pueda un usuario no autorizado modificar o eliminar la información.

- Otro punto de igual importancia es el uso de un software antivirus, el cual se pueda actualizar periódicamente con el fin de obtener las nuevas definiciones de virus informático y tener una mejor protección.

Hay que considerar que sistemas operativos como Windows 98 y ME no están diseñados para obtener su mejor rendimiento en un ambiente de red por lo que es recomendable utilizar las versiones más recientes como Windows 2000 o XP. Sin embargo estos sistemas operativos aunque tienen un mejor rendimiento en este ambiente, son más propensos a ser atacados e infectados por virus informáticos como consecuencia de su mismo diseño. Por eso es importante remarcar la importancia de realizar las actualizaciones pertinentes periódicamente.

Windows, con excepción de XP, no cuenta con un *firewall* personal dentro del sistema operativo. La función de un *firewall* consiste en filtrar todas las comunicaciones que realiza el equipo permitiendo o denegando el acceso a ciertos servicios como el de Web, el de correo o el de IRC. En el mercado existen muchas opciones de productos de los que podemos disponer según nuestras necesidades: desde un filtrado de ciertos tipos de servicios o puertos hasta algunos que ya incluyen un análisis antivirus. Cada *firewall* puede ser configurado manualmente según las necesidades creando las reglas de filtrado para satisfacerlas. Bloquear una

dirección IP específica y cerrar ciertos tipos de servicios como el de Chat por ejemplo.

Si estamos trabajando sobre este sistema operativo, y vamos a compartir o extraer información con otros usuarios de la red, es muy importante que una vez realizada la operación se proceda a deshabilitar estas propiedades en nuestro equipo y así evitar que alguien no autorizado robe la información.

Otra consideración importante, dado que facilita la configuración de una red inalámbrica es la instalación del *service pack 2* para Windows XP. Además de contar con un *firewall* personal también cuenta con una utilería de configuración de redes inalámbricas que funciona de manera eficiente y automática.

2.2.2 Linux

Linux es un poderoso sistema operativo que configurado adecuadamente puede resistir cualquiera de estos ataques. Es una opción a considerar en el diseño e implementación de una red inalámbrica. Linux es uno de los sistemas operativos de mayor uso en el ambiente académico dada su condición de software libre.

En el mercado existen bastantes dispositivos inalámbricos que soportan este sistema operativo. Sin embargo la instalación de los controladores de estos dispositivos no es una tarea fácil. Sobre todo para un usuario catalogado como común, dado que se requieren ciertos conocimientos para realizar la configuración. Aunque también cabe resaltar que en la actualidad y dado el auge que han tenido, en el mercado, las redes inalámbricas, distribuciones como SUSE, Fedora y Mandriva ya cuentan con una opción de configuración de redes inalámbricas, lo cuál nos permite una instalación más rápida sin necesidad de una configuración

complicada del *kernel* como en las versiones anteriores de diferentes distribuciones como Red Hat Linux , Mandrake, Slackware y Debian.

2.3 Seguridad en los puntos de acceso

En la actualidad existen en el mercado inalámbrico una extensa gama de marcas de puntos de acceso. Estos manejan de manera independiente sus propias características de configuración mediante un *frimware*, como se muestra en la siguiente figura.

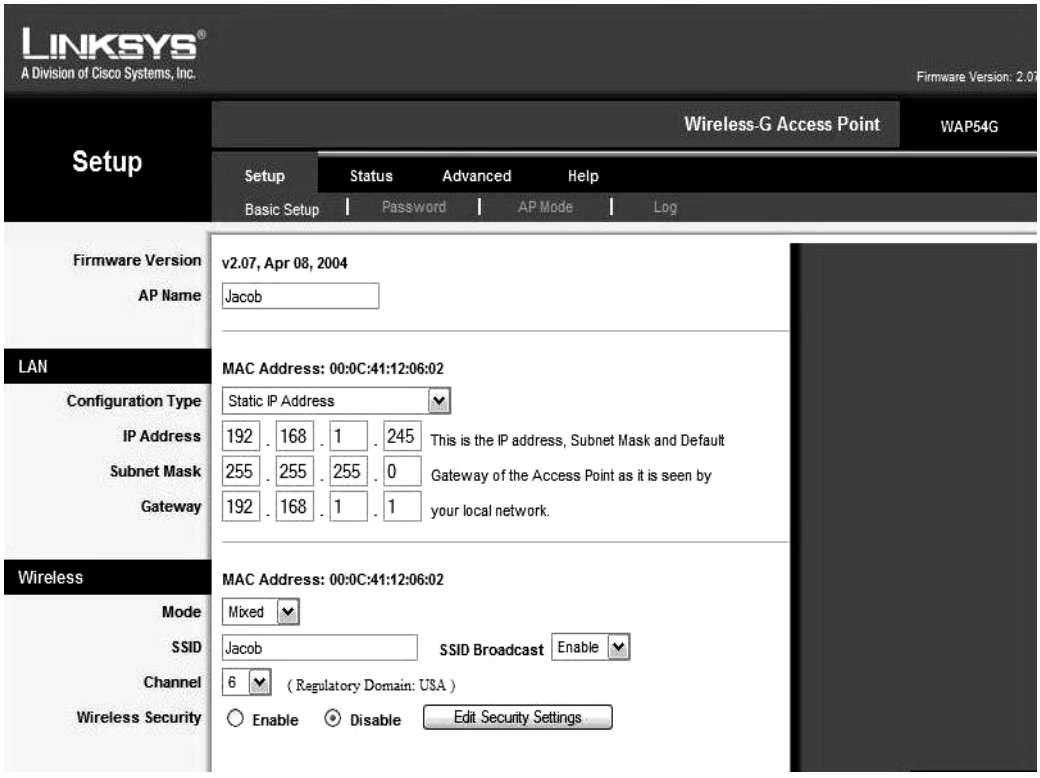


Figura 2.3 Firmware de un Punto de Acceso

Este *firmware* nos permite realizar las modificaciones de funcionamiento del punto de acceso de acuerdo a las necesidades y desde cualquier estación conectada a la misma red. La mayoría de los puntos de acceso convergen en características muy similares en aspectos de seguridad y sus métodos de autenticación como son el WEP (*Wired Equivalent Privacy*) o el filtrado de las direcciones MAC (*Media Access Control*) entre los más utilizados.

Los puntos de acceso cuentan con una contraseña de entrada a su *firmware*. Esta es una contraseña que maneja el fabricante de dicho dispositivo. El primer paso antes de realizar cualquier modificación al *firmware* es cambiar esta contraseña de entrada de fábrica por una propia con características que sólo el administrador de la red conozca. De esta manera se evita que cualquier intruso con una *laptop*, una tarjeta inalámbrica y un software de rastreo, como *Netstumbler* entre otros, pueda obtener la dirección MAC del punto de acceso, el modelo, el fabricante del dispositivo y por lo tanto conocer la contraseña de fabrica que usa dicho fabricante y sabotear el dispositivo.

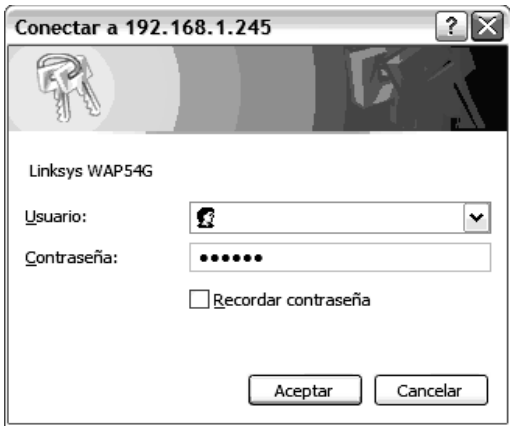


Figura 2.4 Entrada de contraseña para firmware

2.3.1 Autenticación

En las redes administradas se emplean diferentes mecanismos de autenticación para garantizar que únicamente puedan conectarse dispositivos autorizados, como lo son:

- *Open* (abierto): Un sistema abierto sólo implica que no se lleva a cabo ninguna autenticación. Todas las estaciones están autorizadas a acceder a la red. No obstante, puede emplearse el cifrado WEP.

- *Shared Key* (clave compartida) según IEEE 802.11: Este sistema emplea la clave WEP para la autenticación.

WEP (Wired Equivalent Privacy)

Este es un protocolo incorporado al estándar 802.11b de la IEEE, el cual usa un algoritmo *RC4* para encriptar los paquetes de información enviados a través de un punto de acceso a una tarjeta inalámbrica, este algoritmo es el mismo utilizado por SSL, uno de los protocolos más comunes utilizados en la seguridad de la información como los mencionamos con anterioridad.

RC4

RC4 es un cifrador de flujo de datos que usa la operación XOR entre la salida del generador del flujo de datos (*keystream*) y el texto sin cifrar del mensaje. Este algoritmo usa un concepto de estados ordenados en el proceso encripción y

desencripción[3]. La primera parte del algoritmo utiliza KSA (*Key Sheduling Algorithm*). KSA tiene la función de obtener el valor de los estados *S* y ordenarlos mediante el siguiente algoritmo:

Initialization:
for i = 0…… N-1
S[i] = i
j = 0
Scrambling:
for i = 0…..N-1
j = j + S [i] +K [i mod 1]
Swap (S[i], S[j])

N = número de iteraciones, que normalmente es de 256.
K es cada bit de la llave o *password*. Por ejemplo:
Supongamos que tenemos la siguiente llave, *password =6152* por lo tanto *K* va estar definida por *K [0]=6, K [1]=1, K [2]=5 y K [3]=2.*

Nota: El termino *mod* se refiere al valor del residuo originado por una división. Por ejemplo: 6 *mod* 4 =2 ó lo que es lo mismo 6/4 es igual 1 con un residuo igual a 2.

Posteriormente, en una segunda parte del algoritmo, *RC4* utiliza PRGA (*Pseudos Random Generation Algorithm*) para generar el flujo de datos (*keystream*) *Z* que se usará para realizar la operación XOR con el texto sin cifrar del mensaje a enviar.
El algoritmo PRGA se define como:

[3] Wireless Maximum Security, Peikari, Cyrus, SAMS, USA 2002.

Initialization:

i = 0

j = 0

Generation Loop: i =i + 1

j = (j + S[i]) mod 1

Swap (S[i], S[j])

Output z = S(S[i] + S [j])

El proceso que realiza *RC4* para obtener el *keystream* se muestra en la siguiente figura.

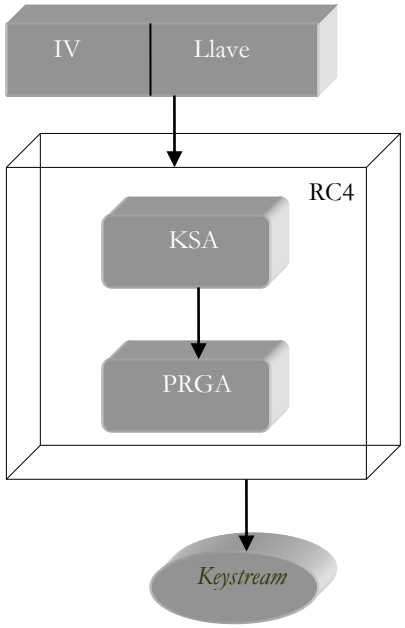


Fig. 2.5 Algoritmo RC4

Para poder tener una mejor comprensión sobre el funcionamiento de WEP es necesario retomar algunos conceptos como la criptología.

Criptología (Encriptar/Desencriptar)

La criptología es definida como el estudio de encriptar y desencriptar información mediante algoritmos, los cuales a menudo necesitan de una clave o llave llamada también *password* , la cual tiene el fin de dar el acceso a la información que hemos encriptado. Existen dos principales técnicas para encriptar: simétrica y asimétrica.

- Simétrica: Este proceso se caracteriza en que tanto para encriptar como para desencriptar se utiliza la misma llave o *password*. Por ejemplo, si deseamos encriptar la palabra *Wíreless* tendremos que seguir los siguientes pasos:

    - Tomamos la palabra y separamos cada letra colocando el numero 1 entre cada una.

        Wireless → W 1 i 1 r 1 e 1 l 1 e 1 s 1 s

    - Convertimos las letras a su correspondiente número dentro del alfabeto.

        W 1 i 1 r 1 e 1 l 1 e 1 s 1 s → 23 1 9 1 18 1 5 1 12 1 5 1 19 1 19

    - Sumamos 2 a cada uno de los valores.

        23 1 9 1 18 1 5 1 12 1 5 1 19 1 19 (+2) → 25 3 11 3 20 3 7 3 14 3 7 3 21 3 21

        Y de esta manera tenemos la palabra *Wireless* encriptada.

Wireless → 25 3 11 3 20 3 7 3 14 3 7 3 21 3 21

Ahora para realizar el algoritmo de forma inversa tendremos que seguir los siguientes pasos:

- Primero restamos 2 a la última cadena de valores

  25 3 11 3 20 3 7 3 14 3 7 21 3 21 (-2) → 23 1 9 1 18 1 5 1 12 1 5 1 19 1 19

- Convertimos al alfabeto los valores obtenidos.

  23 1 9 1 18 1 5 1 12 1 5 1 19 1 19 ----- W 1 i 1 r 1 e 1 l 1 e 1 s 1 s

- Y por ultimo removeremos los unos entre cada letra y tenemos

  W 1 i 1 r 1 e 1 l 1 e 1 s 1 s ------ Wireless

Como mencionamos anteriormente este tipo de criptografía usa un *password* o llave que asiste a la encripción del mensaje. Retomemos el mismo ejemplo pero ahora usando la palabra *WEP* como llave.

- Convertimos cada letra a su valor en el alfabeto.

  W i r e l e s s
  23 9 18 5 12 5 19 19

- Hacemos lo mismo para la palabra que va hacer nuestro *password* o llave en este caso la palabra es *WEP*.

W e p
23 5 16

- Fusionamos las dos palabras repitiendo la llave cuantas veces sea necesario.

23 9 18 5 12 5 19 19
\+ *23 5 16 23 5 16 23 5*
46 14 34 28 17 21 42 24

De esta manera tenemos un ejemplo sencillo de una encripción simétrica ya que para poder desencriptarla es necesario conocer o deducir que la llave o *password* es *WEP*. Este tipo de encripción es rápida solo que nuestra seguridad depende de mantener en secreto la palabra llave.

- Asimétrica: Este tipo de encripción es más compleja pero mucho más segura. La encripción asimétrica requiere de dos llaves una pública y otra privada. Cada llave requiere del uso de la otra para descifrar un mensaje. Es decir podríamos hacer una analogía con el siguiente ejemplo. Si alguien quiere enviarnos un mensaje de manera segura de tal manera que sólo nosotros podamos abrirlo, podría sellar el mensaje en una caja usando un candado del que sólo nosotros tenemos la llave, de esta manera sin llave, nadie incluso el remitente puede reabrir el mensaje después de asegurarlo.

> Hay que hacer notar que este tipo de encripción requiere que cada uno tenga acceso a una copia de nuestro candado también conocido como llave pública. La encripción asimétrica también tiene sus desventajas, una de ellas es la pérdida de estas llaves, en estos casos la única opción es encontrar un método para encontrar el *password*, lo cual se considera como un acto ilegal que es penado por la ley en muchos países.

Es importante aclarar que ninguno de estos métodos nos garantiza en un 100% la seguridad de la red inalámbrica.

Como ya lo hemos mencionado anteriormente WEP esta basado en el algoritmo *RC4* y utiliza claves de 64bits o de 128bits. Estas claves que en realidad son de 40 o 104bits respectivamente, ya que los otros 24bits restantes se utilizan como vector de inicialización, se generan a partir de una clave estática o *password* de forma automática.

La clave debe ser conocida por todos los clientes que quieran conectarse a la red inalámbrica que utiliza WEP. Esto implica que esta clave sea fácil de recordar para el usuario y que no se cambie de forma frecuente. A partir de esta clave se generan 4 llaves de 40 bits. Solo una de ellas se utilizara para la encripción WEP, como se muestra en las siguientes figuras.

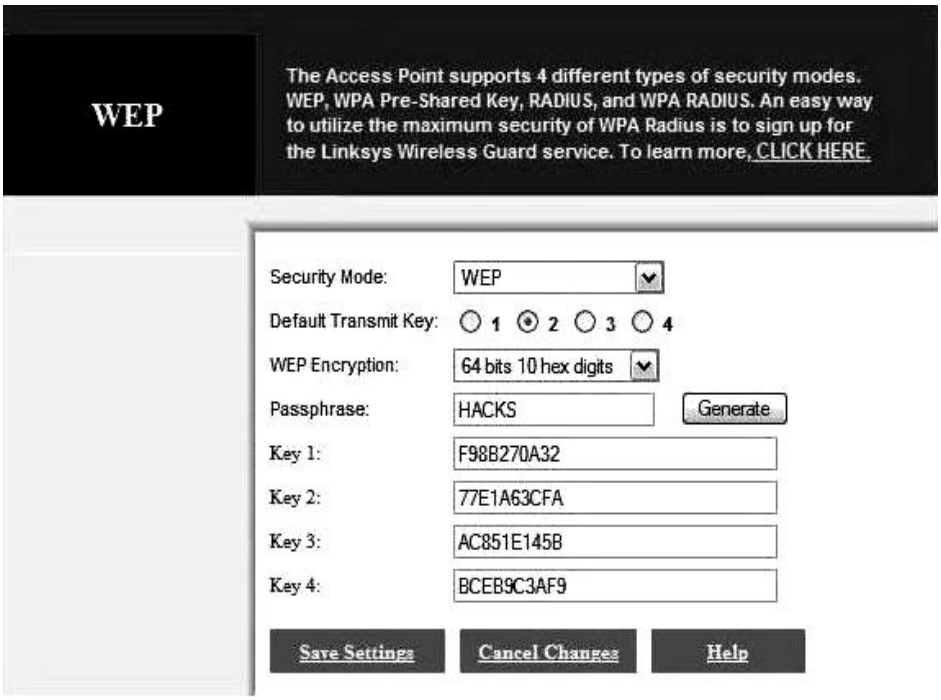


Figura 2.6 WEP 64bits

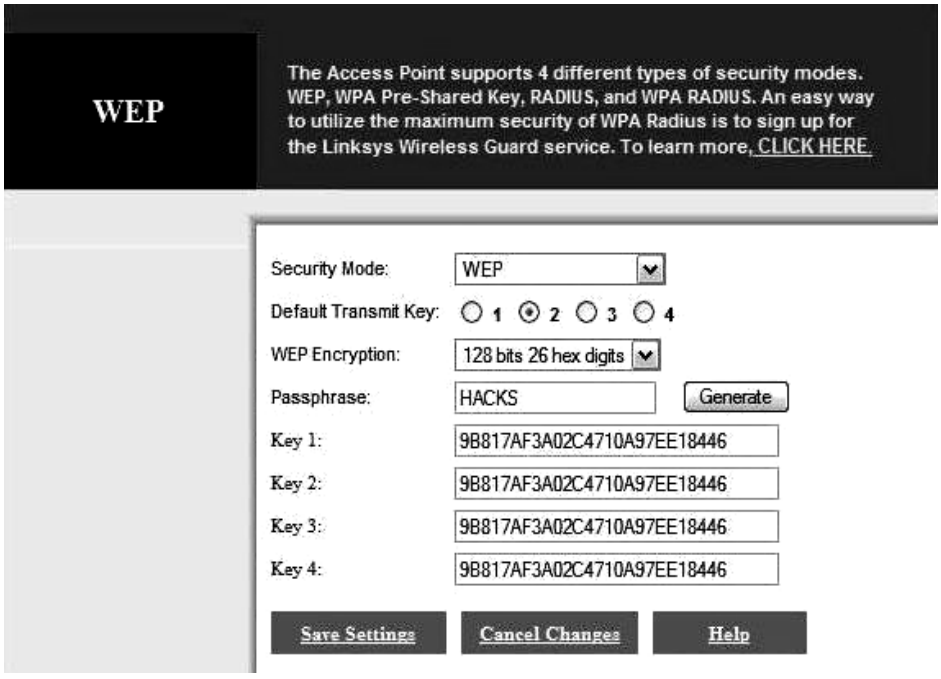


Figura 2.7 WEP 128bits

Cuando creamos una llave, estas letras y/o números son convertidos a su equivalente binario. Por ejemplo, tomemos la palabra HACKS como llave

H(ASCII) – 072(ANSI) – 01001000(binario)
A(ASCII) – 065(ANSI) – 01000001(binario)
C(ASCII) – 067(ANSI) – 01000011(binario)
K(ASCII) – 075(ANSI) – 01001011(binario)
S(ASCII) – 083(ANSI) – 01010011(binario)

Por lo tanto tenemos que el equivalente binario de cada letra contiene 8bits y el total es de 40bits en unos y ceros.

HACKS – 0100100001000001010000110100101101010011

El proceso para generar las llaves consiste en una operación XOR con la cadena ASCII de nuestra llave, la cual queda transformada en una cadena de 32bits que utilizara un generador de números pseudo aleatorios PRNG (*Pseudo-Random Number Generator*) para generar 40 cadenas de 32 bits cada una.

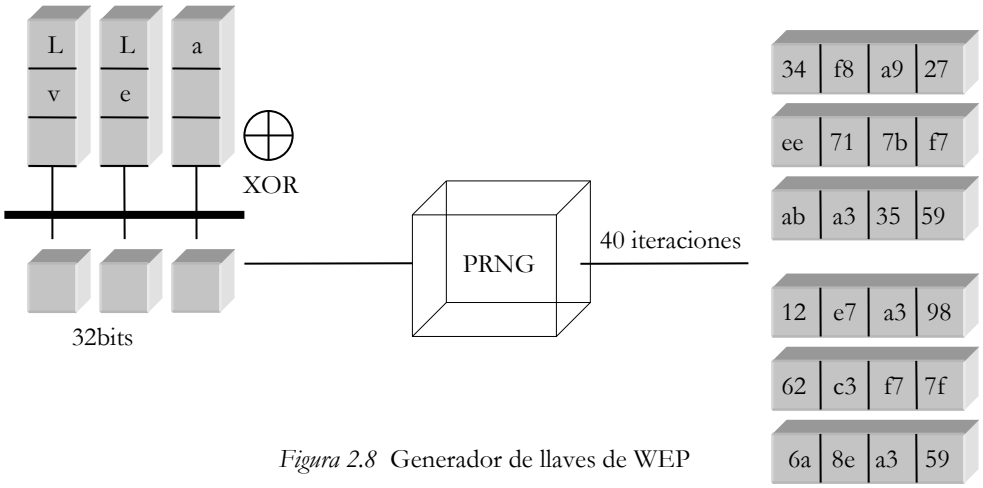


Figura 2.8 Generador de llaves de WEP

Se toma un bit de cada una de las 40 cadenas generadas por el PRNG para construir una llave y se generan 4 llaves de 40bits.

Para generar una trama encriptada con WEP se sigue el siguiente proceso: partimos de la trama que se quiere enviar, esta trama sin cifrar está compuesta por una cabecera (*Header*) y contiene unos datos (*Payload*). El primer paso es calcular el CRC (*Cyclic Redundancy Check*) de 32 bits de los datos de la trama que se quiere enviar. El CRC es un algoritmo que genera un identificador único de los datos en concreto, que nos servirá para verificar que el dato recibido es el mismo que el enviado.
Para ver mas información sobre como calcular el CRC ver el *apéndice B.*

El siguiente paso es añadir este valor CRC a la trama.

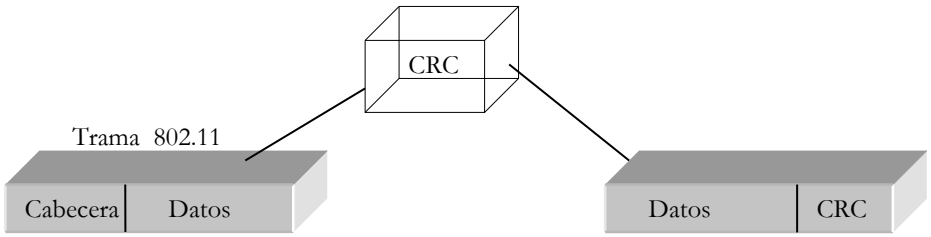


Figura 2.9 Trama WEP

Por otra parte seleccionamos una llave de 40 bits, de las 4 llaves posibles:

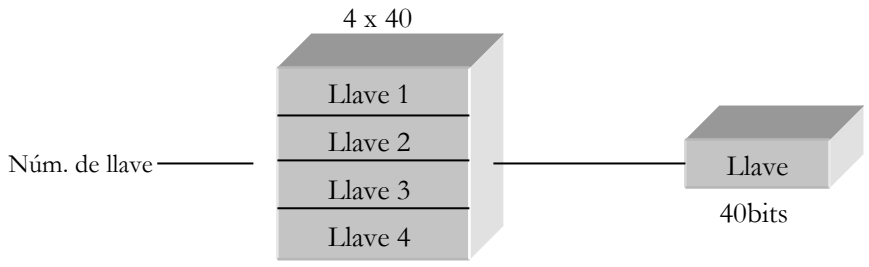


Figura 2.10 Selección de una llave

Y añadimos el Vector de Inicialización (IV) de 24bits al principio de la llave seleccionada:

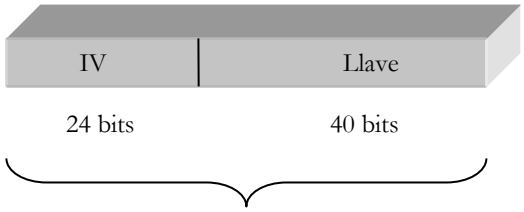


Figura 2.11 Trama de la llave

El vector de inicialización es simplemente un contador que suele ir cambiando de valor a medida que vamos generando tramas, aunque según el estándar 802.11b también puede ser siempre cero. Con el IV de 24bits y la llave de 40bits conseguimos los 64bits de llave total que utilizaremos para encriptar la trama. En el caso de utilizar encriptación de 128bits tendríamos 24bits del IV y 104bits de la llave. Una vez en este punto, aplicamos el algoritmo *RC4* al conjunto *IV + llave* y obtenemos el *keystream*.

Realizando una operación XOR con este *keystream* y el conjunto *Datos* + *CRC* obtendremos los *Datos'* + *CRC'* cifrados. Este proceso puede verse en la siguiente figura. Se utiliza el IV y la llave para encriptar los *Datos* + *CRC*:

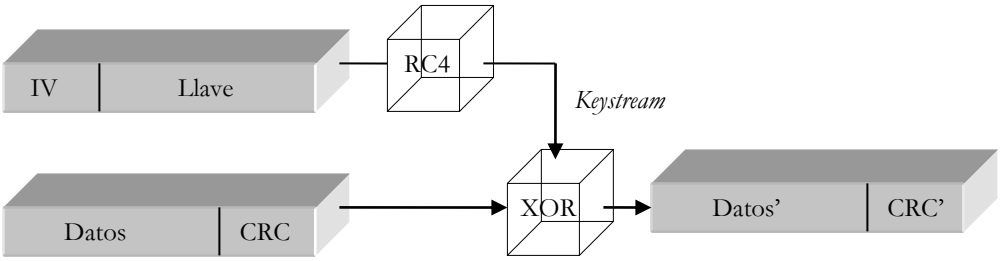


Figura 2.12 XOR entre los datos y la llave

Después añadimos la cabecera y el *IV+llave* sin cifrar y así queda la trama definitiva lista para ser enviada:

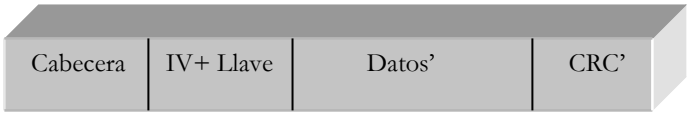


Figura 2.13 Trama de datos con WEP

El proceso de encriptación en conjunto se ve resumido en el siguiente esquema:

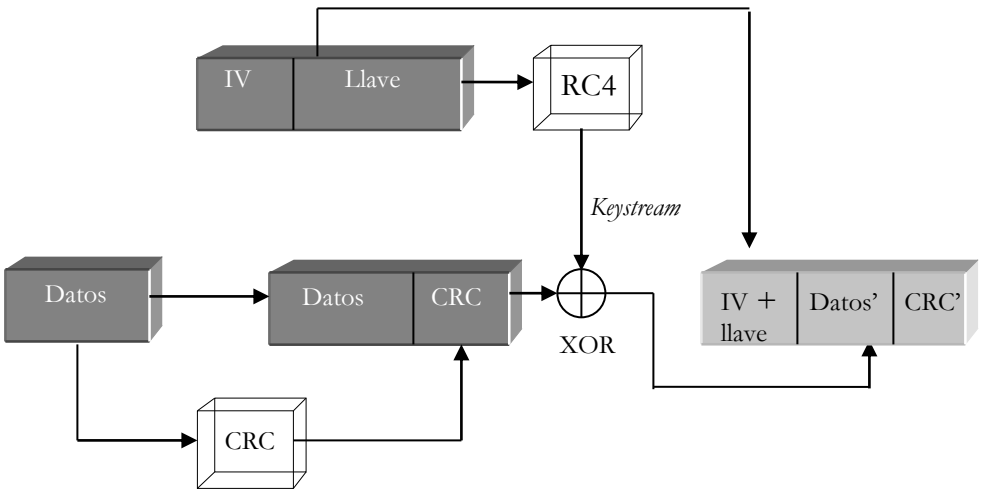


Figura 2.14 Proceso de encripción WEP

Ahora el proceso que se realiza para desencriptar una trama encriptada con WEP es el siguiente:

Se utiliza el número de llave que aparece en la trama cifrada junto con el IV para seleccionar la llave que se ha utilizado en cifrar dicha trama. Se añade el IV al principio de la llave seleccionada, consiguiendo así los 64bits de llave. Aplicando *RC4* a esta llave obtenemos el *keystream* válido para obtener la trama en texto sin cifrar o texto plano (*plaintext*) realizando una XOR con los *Datos' + CRC'* cifrados y la llave completa.

Una vez obtenido el texto plano, se saca el CRC que viene con la trama y se vuelve a calcular un nuevo CRC de los datos obtenidos para posteriormente realizar una comparación con el original CRC. El proceso completo puede verse en el siguiente esquema:

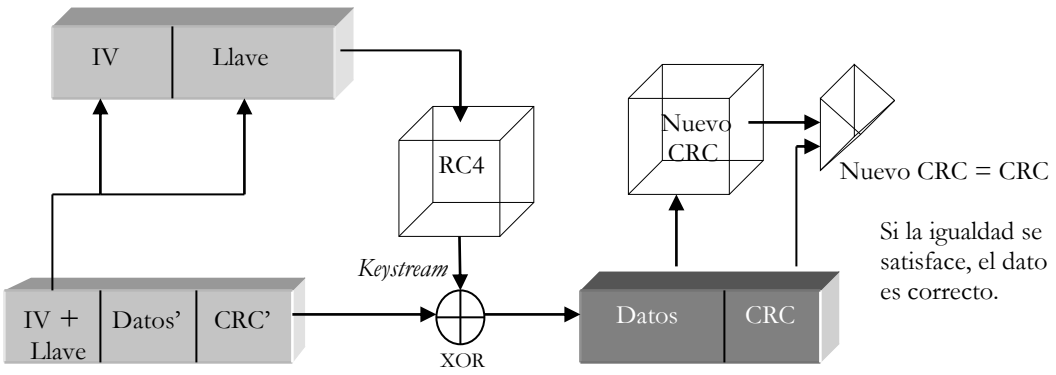


Figura 2.15 Proceso de Desencripción de WEP

WPA (Wi-Fi Protected Access)

Este protocolo soluciona las debilidades de WEP, las cuales mencionaremos en el siguiente capítulo. Entre sus características se encuentra la distribución dinámica de claves de manera automática, así como también la inclusión de vectores de inicialización de 48bits, el doble que el utilizado por WEP, que nos permite un mayor número de combinaciones de claves diferentes. WPA sigue siendo un algoritmo *RC4*, solo que con algunas diferencias como es la utilización de un nuevo código de nombre MIC (*Message Integrity Code o Michael*) que funciona para verificar la integridad de los mensajes en lugar del CRC de 32bits que utiliza WEP. Así también el protocolo TKIP (*Temporal Key Integrity Protocol*) el cual se encarga de la generación de una nueva clave para cada paquete.

WPA puede funcionar de dos modos:

- WPA-PSK (*Pre Shared Key*) con clave inicial compartida. Este modo está orientado a pequeñas redes dado que todas las estaciones y el punto de acceso utiliza una clave compartida. Esta clave sólo es utilizada como un punto de inicio para la autenticación, es decir como una clave de acceso a la red, pero no interviene en el cifrado de los datos como en el caso de WEP.

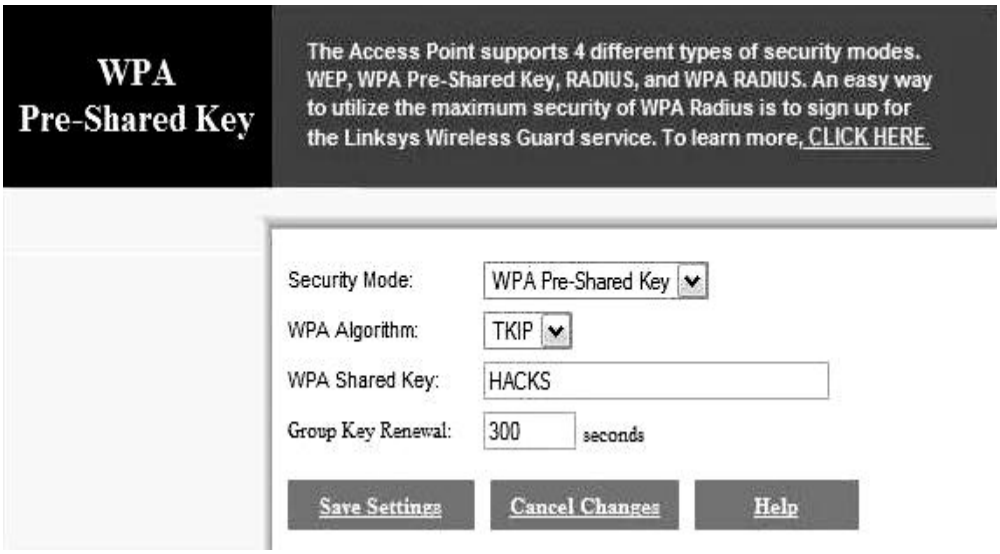


Figura 2.16 WPA

- RADIUS (*Remote Authentication Dial-In User Service*) WPA-EAP (*Extensible Authentication Protocol*). Este es el modo orientado a empresas que requiere de un servidor configurado para desempeñar las tareas de autenticación, autorización y contabilidad de nuestra red inalámbrica.

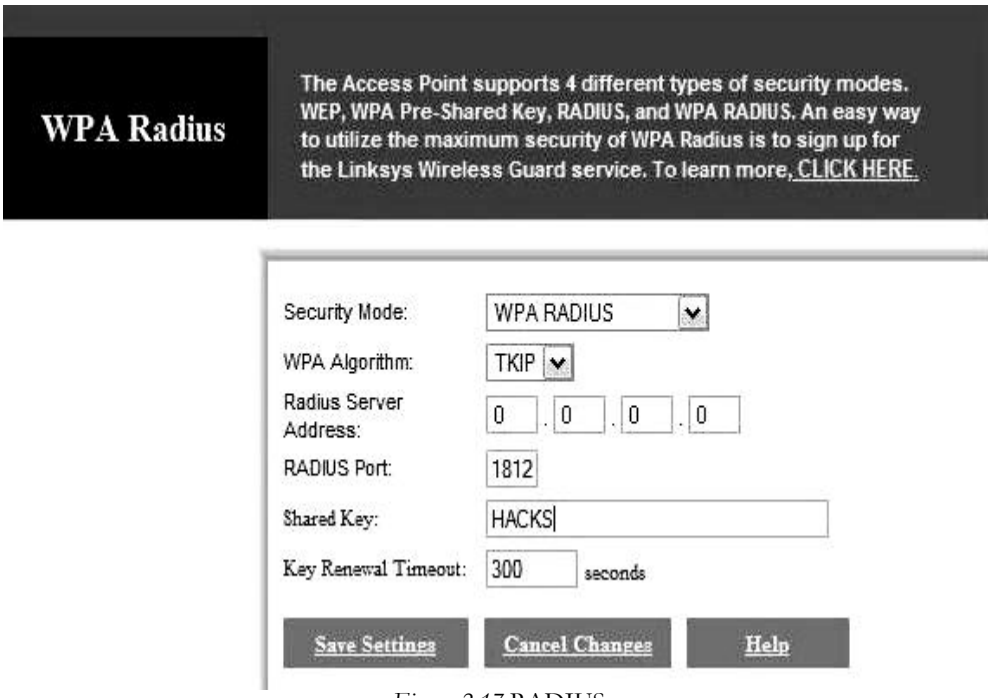


Figura 2.17 RADIUS

WPA es un subconjunto de lo que será en un futuro el IEEE 802.11i, creado precisamente para proporcionar seguridad en las redes inalámbricas. En éste existe lo que podríamos llamar WPA2 el cual incluye un nuevo algoritmo de cifrado AES (*Advanced Encription Standard*) que se caracteriza por contar con claves de 128bits y utilizar CCMP (*Counter-Mode / Cypher Block Chaining /Message Authentication Code Protocol*) en lugar de los códigos MIC; y especificar la administración de claves. Además de dar soporte no únicamente a las redes de infraestructura si no también a las ad-hoc.

2.3.2 Filtrado de direcciones MAC

El envió de datos de una máquina a otra puede causar problemas si no se conoce la dirección MAC de la máquina receptora, para resolver este problema existe un

sistema de resolución para determinar direcciones llamado ARP (*Address Resolution Protocol*). Esencialmente ARP es una tabla con una lista de direcciones IP y sus direcciones físicas MAC correspondientes.

Cuando un sistema necesita comunicarse con un *host* local busca la dirección IP en su tabla de enrutamiento IP, que normalmente se mantiene en memoria. Si no existe la IP en su tabla local, El *host* difunde una solicitud de ARP que contiene la dirección IP de destino. El *host* de destino reconoce que se trata de su dirección de IP y lee la consulta. Lo primero que hace el *host* de destino es actualizar su propia tabla de traducción de direcciones con la dirección física del origen. El *host* destino envía la respuesta que contiene su propia dirección física. Cuando el *host* origen reciba la respuesta, actualiza su tabla y se prepara para empezar a transmitir datos.

Una dirección MAC es un identificador de hardware único asignado por el fabricante a cada dispositivo de red. Este número consta de 48bits en 6bytes hexadecimales.



Figura 2.18 Dirección MAC de una tarjeta inalámbrica

Los puntos de acceso cuentan con una tabla dentro de su *firmware* que nos permite llevar un control de los dispositivos o tarjetas inalámbricas que se van a conectar a la red inalámbrica como lo muestra la siguiente figura.

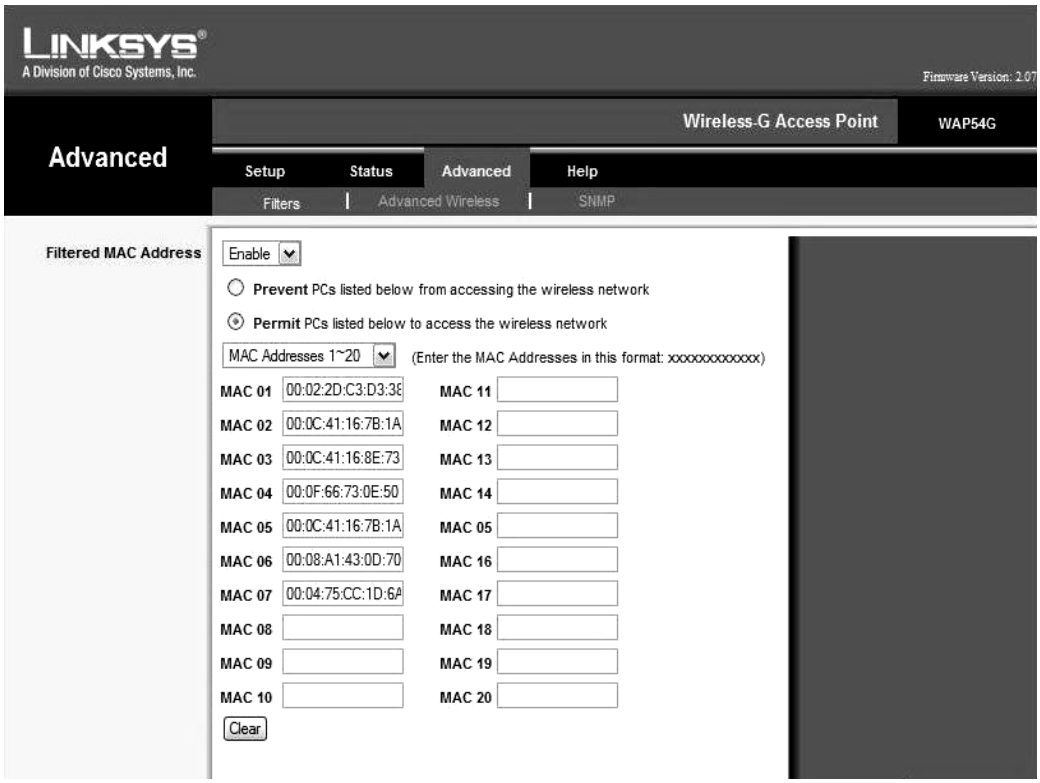


Figura 2.19 Listado de direcciones MAC

Esta tabla nos indica las direcciones MAC de los dispositivos a los cuales se les va a permitir el acceso a la red inalámbrica. Si alguien desea tener acceso y la dirección MAC de su dispositivo no se encuentra dentro de esta tabla, el punto de acceso no le permitirá realizar la conexión. Este método requiere de una administración con una diaria actualización.

2.4 Seguridad a través del Gateway

Un *gateway* es la puerta de enlace entre dos redes con características diferentes. La puerta de enlace entre una red cableada y una subred inalámbrica debe cumplir con

ciertas características que nos proporcionen la seguridad precisa de acuerdo a nuestras necesidades. El *firewall* debe estar configurado con las reglas adecuadas para permitir o bloquear cierto tipo de conexiones, como la entrada por el puerto 22 para el SSH, si se desea que los usuarios hagan uso de este tipo de servicios.

El primer punto importante a considerar en la instalación del *gateway* / *firewall* es la elección del sistema operativo, dado que este dispositivo debe permanecer encendido todo el tiempo debemos tomar en cuenta un sistema operativo estable y que no sufra de constantes ataques, por lo que Windows no sería la opción más recomendable, un *firewall* en UNIX / Linux puede ser la mejor opción.

El segundo punto se refiere a la conexión, es importante no conectar nuestro punto de acceso como una estación más de nuestra red cableada como nos muestra la siguiente figura.

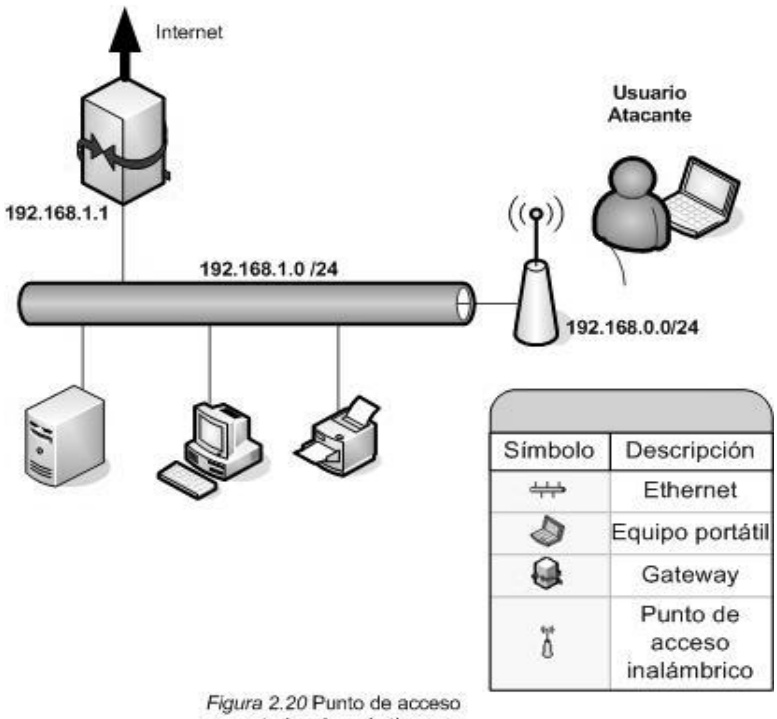


Figura 2.20 Punto de acceso conectado a la red ethernet

Esto ocasionaría que un atacante, una vez conseguido el paso a través de la subred inalámbrica, pueda tener el control y acceso a la información de las estaciones conectadas a la red principal. Con el objetivo de minimizar este riesgo. El punto de acceso deberá estar conectado directamente al *gateway* como en la siguiente figura:

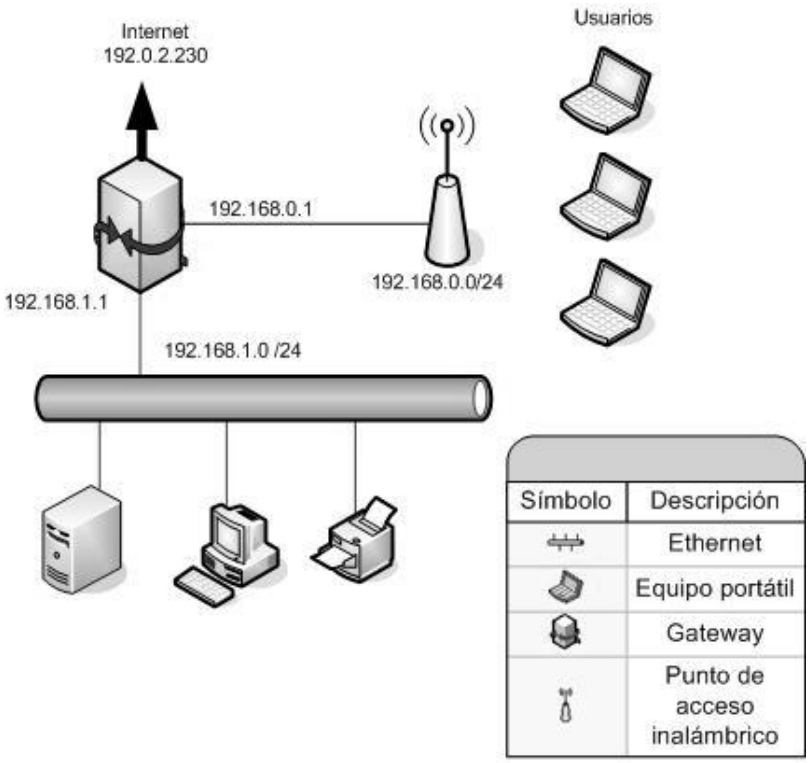


Figura 2.21 Punto de acceso conectado al gateway

Algunas veces, dependiendo del área de cobertura o la demanda de usuarios a los cuales se les proporcionara el servicio, se requiere de más de un punto de acceso. En estos casos es necesario configurar dichos puntos de acceso como repetidores o puentes de la misma subred conectados al mismo *gateway*.

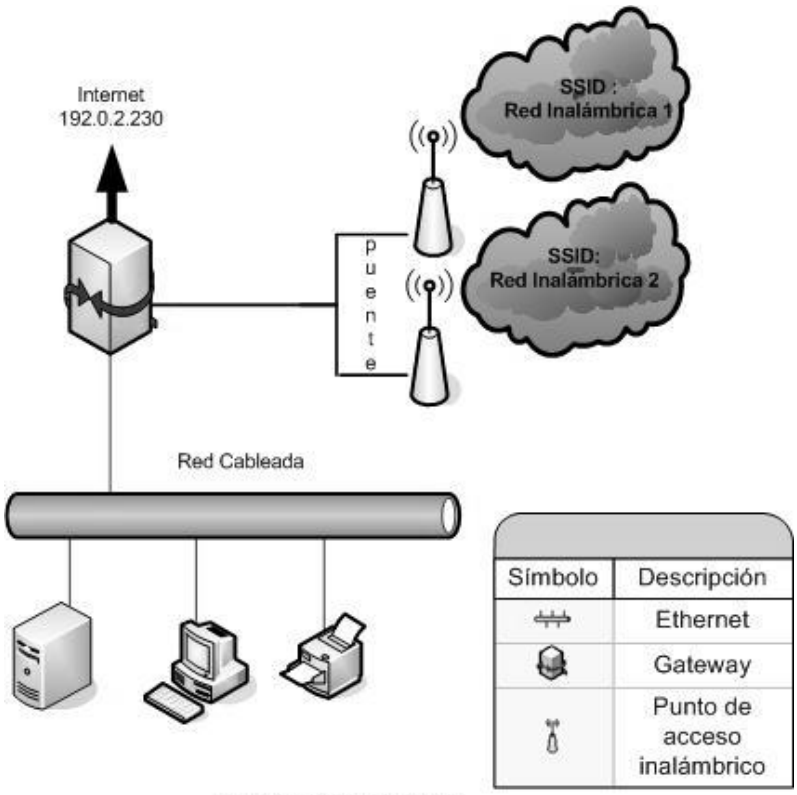


Figura 2.22 Varios puntos de acceso de una misma red

C a p i t u l o 3

PUNTOS VULNERABLES EN LAS REDES INALÁMBRICAS

3.1 Ataques y Riesgos

Las redes inalámbricas no pueden ser aseguradas de la misma forma que una red cableada. Existe una diversidad de procedimientos mediante los cuales una red inalámbrica puede ser atacada. El ataque puede provenir de cualquier sitio en donde la señal pueda ser detectada, esto puede ser incluso fuera de las propias instalaciones de la institución. Cualquier persona mal intencionada con una computadora portátil, una tarjeta inalámbrica y el software necesario para rastrear la señal significa un peligro potencial para la infraestructura inalámbrica debido a que puede estar haciendo uso de los recursos de Internet sin que nadie se percate, así como también poner en riego información confidencial de dicha institución.

3.1.1 Fácil Acceso

Encontrar una red inalámbrica es un procedimiento sencillo. Por ejemplo, como ya mencionamos en el capitulo anterior el sistema operativo Windows XP, con su más reciente actualización *service pack 2* cuenta con una utilería para redes inalámbricas, la cual detecta de manera automática las redes disponibles en el área. Esta utilería resulta muy eficiente para los usuarios pero peligrosa si hablamos de cuestiones de seguridad ya que no es posible mantener un control de todos los usuarios que utilizan la red.

Estos puntos de acceso a red necesitan anunciar su presencia para hacer posible que los usuarios puedan acceder a ésta y utilizar todos los recursos disponibles de la misma. Para esto emiten periódicamente una señal denominada *Beacon Frames*, esta señal nos muestra información valiosa para el usuario como el SSID de la red, la intensidad de la señal, así como la seguridad de la misma. En la actualidad este riesgo puede ser evadido. La mayoría de los puntos de acceso cuentan en su *firmware* de configuración una opción de no emitir esta señal o de manejar los intervalos en segundos para que esta señal sea emitida, haciendola transparente a este tipo de utilerías, y a otras herramientas de monitorización.

La siguiente figura muestra la señal inalámbrica sin y con la emisión de *Beacon Frames*

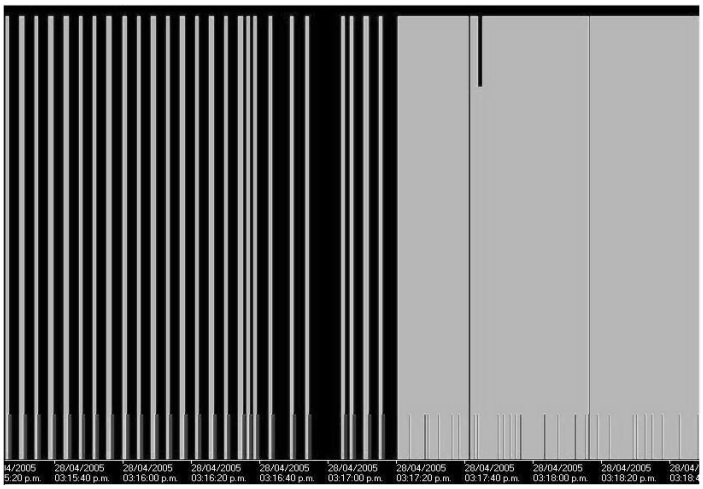


Figura 3.1 Señal inalámbrica

En la figura 3.1 se puede observar como la señal sin la emisión de *Beacon Frames* contiene huecos a diferencia de la que si emite esta señal.

3.1.2 Vulnerabilidades de WEP

Como hemos visto el objetivo de WEP no es garantizar por completo la seguridad de la red si no más bien de proteger los datos contra usuarios mal intencionados.

WEP como ya hemos visto se basa en un algoritmo de cifrado RC4, que cifra constantemente los datos que circulan entre un punto de acceso y un nodo cliente, utilizando una clave secreta compartida de 64bits o de 128bits, formando un túnel virtual entre estos dos.

Uno de los problemas de este estándar es que 24bits de los 64bits o 128 bits destinados para la clave son utilizados para el vector de inicialización, no cifrado.

El ataque se inicia rastreando una gran cantidad de paquetes provenientes de numerosos clientes, entre mas grande sea el numero de paquetes capturados mayor será la probabilidad de éxito. Como el vector de inicialización se encuentra en texto sin cifrar y dado que existen aproximadamente 17 millones de posibles combinaciones para formar dicho vector, por lo tanto se hace latente la posibilidad de que dicho vector se repita.

Una vez que se tengan dos paquetes que utilicen el mismo vector de inicialización, se puede realizar un XOR sobre los paquetes y obtener la clave.

Un ejemplo sencillo para observar esto es el siguiente:

Supongamos que tenemos en texto sin cifrar la letra A (ASCII) -065 (ANSI) -10000001 (Binario) con la siguiente llave 01110001. Si hacemos un XOR entre el texto sin cifrar y la llave obtenemos el siguiente texto cifrado:

Texto sin cifrar	1 0 0 0 0 0 0 1
Llave	0 1 1 1 0 0 0 1
XOR	
Texto cifrado	1 1 1 1 0 0 0 0

Para obtener la llave necesitamos ahora realizar un XOR entre el texto claro y el mensaje cifrado.

Texto sin cifrar	1 0 0 0 0 0 0 1
Texto cifrado	1 1 1 1 0 0 0 0
XOR	
Llave	0 1 1 1 0 0 0 1

Y de esta manera obtenemos la llave que se utilizó para encriptar el texto plano.

Como podemos observar, resulta simple extraer una llave de datos encriptados si se tiene ambas partes, un texto cifrado y el texto sin cifrar. El texto cifrado es sencillo de capturar, todo lo que se necesita es un *sniffer* inalámbrico y capturar una gran cantidad de datos encriptados. El problema ahora es cómo encontrar el valor de un dato original, es decir sin cifrar.

Esto puede ser complicado. La primera opción sería tener acceso a la red desde atrás del *firewall,* instalar un *sniffer* desde a dentro y capturar una gran cantidad de datos antes de ser encriptados. Esta alternativa resulta un tanto paradójica o redundante por que significaría que el atacante ya tiene acceso no autorizado a

la red interna. El beneficio de realizar este procedimiento sería obtener servicio anónimo de Internet, lo cual resulta más fácil en redes inalámbricas sin el uso de WEP.

La segunda y más probable opción para predeterminar un dato sin cifrar es enviar y recibir un mensaje predecible. Para facilitar esto una sesión de Chat o un *email* puede proveer al atacante el texto sin cifrar que necesita y usar éste para obtener la llave secreta.

WEP usa valores conocidos como vectores de inicialización IV. El algoritmo RC4 utiliza este valor, lo concatena con la llave y forma lo que se llama un paquete llave exclusivo con el que se va a encriptar cada paquete de información que será enviado a través de la red. Cada vector de inicialización es una especie de contador de cada paquete el cual es asignado de manera aleatoria.

WEP usa 3bytes de IV por cada paquete de datos transmitidos sobre la red inalámbrica. Un byte consta de 8bits. Por lo tanto el tamaño total del IV es de 24bits (8bits X 3bytes). Si calculamos todos los posibles IV, podríamos tener una lista de 2^{24} posibles llaves. Este número es derivado del hecho que cada bit puede ser un " 0 " o un " 1 " lógico (2) y son un total de 24bits (^{24}). Esto da como resultado 16, 777,216 pareciera una cantidad grande de posibles IV, pero en cuestión de comunicaciones es relativamente pequeño. La razón es la probabilidad de repetición.

El vector de inicialización, como ya vimos, es un número aleatorio. Esto significa que no se necesita esperar 16,777,216 posibilidades para que se repita un número. Uno puede comenzar a ver repeticiones, por colisiones, después de los 5000 paquetes de transmisión. Considerando un promedio de 1,500bytes de paquetes transmitidos por dispositivo inalámbrico, una colisión puede

esperarse con la transferencia de un archivo de 7-10MB (5000 paquetes X 1,500 bytes = 7,000,000 bytes).

Supongamos que un atacante envió un *email* con el carácter " 2 " repetido una y otra vez. Aunque esto pareciera un mensaje raro e inofensivo puede resultar de mucha ayuda para un atacante de la red.

El atacante primero monitorea la red con un *sniffer*, cuando el dato previsible es transferido, ahora se mantiene en un estado de escucha hasta encontrar un IV. Una vez hecho esto, el atacante tiene tres piezas importantes de información el dato original usando IV, el texto cifrado generado por la transmisión del dato original con el IV y el texto, no conocido, cifrado generado en otro paquete con el IV. El siguiente paso es realizar cálculos para descifrar el dato desconocido encriptado.

Como ya sabemos se puede deducir la llave de encripción de un texto cifrado si conocemos el dato original y el texto cifrado. Esto es posible representarlo mediante la siguiente ecuación.

Keystream = (Texto cifrado)XOR(Texto sin cifrar)

Ahora, considerando lo que ya sabemos, hemos capturado dos textos cifrados *Texto cifrado* $_{1\&2}$ y conocemos el texto sin cifrar " 2 ", *Texto sin cifrar*$_2$ por lo tanto podemos calcular el texto sin cifrar que nos interesa *Texto sin cifrar*$_1$

Texto cifrado $_1$ *XOR Texto cifrado* $_2$ = *Texto sin cifrar* $_1$ *XOR Texto sin cifrar* $_2$
Texto sin cifrar $_{1\&2}$ *XOR Texto sin cifrar* $_2$ = *Texto sin cifrar* $_1$

La siguiente tabla nos muestra este concepto:

	Texto Cifrado$_1$		*Texto Cifrado*$_2$		*Texto sin Cifrar* $_{1xor2}$
1	00000010	XOR	01000011	=	01000001
2	00000010	XOR	01010010	=	01010000
3	00000100	XOR	01000110	=	01000010
4	00000010	XOR	01000000	=	01000010
5	00000010	XOR	01000100	=	01000110
6	00000100	XOR	01011010	=	01011110
7	00000010	XOR	01000001	=	01000011
8	00000010	XOR	01010111	=	01010101
9	00000100	XOR	01000110	=	01000010

Como podemos ver, hemos encontrado la fusión entre realizar un XOR entre dos textos cifrados. Ahora dada la información que conocemos, en este caso el texto sin cifrar " 2 ", podemos realizar la misma operación XOR y obtener el texto sin cifrar desconocido como nos muestra la siguiente tabla:

	Texto sin Cifrar $_{1xor\,2}$		*Texto sin Cifrar* $_2$		*Texto sin Cifrar* $_1$
1	01000001	XOR	00110001	=	01110000
2	01010000	XOR	00110001	=	01100001
3	01000010	XOR	00110001	=	01110011
4	01000010	XOR	00110001	=	01110011
5	01000110	XOR	00110001	=	01110111
6	01011110	XOR	00110001	=	01101111
7	01000011	XOR	00110001	=	01110010
8	01010101	XOR	00110001	=	01100100
9	01000010	XOR	00110001	=	01110011

Ahora que ya encontramos el valor del texto sin cifrar, antes desconocido procedemos a realizar su conversión a código ASCII.

	Texto sin Cifrar $_1$		ASCII
1	01110000	=	c
2	01100001	=	o
3	01110011	=	n
4	01110011	=	t
5	01110111	=	r
6	01101111	=	a
7	01110010	=	s
8	01100100	=	e
9	01110011	=	ñ

La debilidad de WEP no se encuentra en el protocolo por sí mismo si no en el número limitado de vectores de inicialización IV del proceso. Es por esto que otros protocolos como WPA aumentan la longitud en bits de sus llaves para tener un mayor número de IV. Sin embargo esto no da una solución al problema con colisiones que puede ser detectado por un atacante y realizar todo este proceso de obtención de la llave.

El hecho es que los paquetes transmitidos a través de una red inalámbrica pueden develar bastante información de valores que un atacante puede ocupar para deducir partes de la llave para encriptar los datos sobre dicha red.

3.1.3 Rendimiento limitado

Un punto de acceso, a través de su conexión a la red cableada, puede ser victima de recibir un flujo de datos superior al que puede emitir**.** Un ataque *ping*

flood desde un segmento de *fast ethernet* puede saturar rápidamente el punto de acceso.

El estándar 802.11 ha sido diseñado para permitir la coexistencia de varias redes en un mismo canal. Todo lo que el atacante necesita es llenar de tráfico a un ritmo elevado el canal de radio utilizado por un punto de acceso y este punto de acceso se saturará.

Es especialmente importante recordar que en muchos casos el tráfico normal de una red es suficiente para saturar la misma, y no tiene necesariamente que ser tráfico mal intencionado o tratarse de un ataque. Aplicaciones cliente/servidor pueden transmitir archivos de datos de gran tamaño de forma simultanea a varios clientes provocando una saturación de los puntos de acceso inalámbricos.

Un elevado porcentaje de conexiones a una velocidad baja puede considerarse un indicador de la existencia de alguna interferencia externa, o simplemente un indicador de que probablemente los puntos de acceso están demasiado lejos de los usuarios o la existencia de obstáculos físicos entre los puntos de acceso y los clientes.

La saturación de un canal de un punto de acceso en concreto puede indicar que existe demasiado tráfico, tanto entre el punto de acceso y la red cableada como entre el punto de acceso y sus clientes inalámbricos. Una posible solución puede ser la colocación de puntos de acceso alternativos para que los usuarios puedan hacer uso de estos y no vean interrumpidas sus actividades.

3.1.4 MAC Spoofing

Aunque no esta definido en el estándar 802.11, la mayoría de los fabricantes de puntos de acceso inalámbricos han implementado controles de acceso a nivel MAC para ayudar a reforzar la naturaleza inherentemente insegura de dicho estándar. Cuando se utiliza un control de acceso MAC el administrador definirá una lista de direcciones MAC clientes aprobadas que podrán conectarse al punto de acceso. Aunque este proceso puede ser factible en redes pequeñas, requiere que el administrador supervise las direcciones MAC de todos los clientes inalámbricos y puede suponer una sobrecarga de trabajo para el administrador en grandes instalaciones. Hay que tener en consideración que este control no supone un buen mecanismo de seguridad ya que es relativamente sencillo detectar una dirección MAC, disfrazarla mediante software y obtener el libre acceso a la red..

Se puede detectar cualquier dirección MAC de las estaciones clientes con acceso a la red utilizando un *sniffer* inalámbrico. El procedimiento resulta sencillo. Un monitoreo de la infraestructura inalámbrica, la detección de los clientes que se asocien con éxito a un punto de acceso y el encubrimiento, mediante software, de la dirección MAC resulta suficiente para autentificarse como un cliente autorizado.

Como no hay una estandarización sobre esta alternativa de seguridad, y por lo tanto no está definido en las especificaciones del 802.11, esto trae como consecuencia que no exista ningún atributo dentro de su señal, a diferencia de WEP, que permita identificar que se está utilizando una lista de control de acceso basada en direcciones MAC, pero normalmente, podrá imaginarse este hecho mediante una simple deducción. Si dispone de un SSID correcto y de una clave WEP adecuada pero, a pesar de todo, no puede asociarse a la red,

seguro que el administrador está utilizando filtrado MAC u otro esquema como el 802.1x. que analizaremos en el siguiente capítulo.

3.2 Negación de servicio

Como ya hemos analizado en capítulos anteriores la principal diferencia entre las redes cableadas y las inalámbricas se encuentran en la capa física y de datos según el modelo OSI. Una ataque físico de negación de servicio DoS puede originarse desde cualquier sitio lo suficientemente alejado del punto de acceso, para no ser descubierto físicamente y donde la señal sea suficiente para detectarla. Las redes inalámbricas pueden sufrir un DoS mediante la presencia de interferencias en el rango de frecuencias ISM de 2.4Ghz, debido a que en dicha frecuencia también operan algunos otros dispositivos como teléfonos inalámbricos, radios de policía, monitores de niños, etc. Toda esta gama de dispositivos pueden provocar la posible pérdida de paquetes o la interrupción del servicio. En otros casos un atacante puede elaborar un dispositivo que produzca el suficiente ruido necesario en la banda de frecuencias de 2.4Ghz como para disminuir la eficiencia de la red.

3.2.1 Puntos de acceso no autorizados

Resulta sumamente sencillo adquirir, dado su bajo costo, un punto de acceso inalámbrico. En una institución esta práctica puede resultar peligrosa en aspectos de seguridad. Cualquier departamento dentro de la misma puede decidir adquirir e instalar su propio punto de acceso sin la adecuada coordinación de los administradores de la red.

Es un hecho que estos puntos de acceso funcionan utilizando su configuración por defecto o de fábrica la cual carece de todas las medidas de

seguridad aplicables, por lo que una instalación sin supervisión de este tipo de dispositivos se vuelve un punto vulnerable de toda la infraestructura de red.

Otra ofensiva provocada por este tipo de actividades surge cuando un atacante a la red inalámbrica coloca un punto de acceso no autorizado entre los usuarios de la misma y el punto de acceso autorizado. A este tipo de ataque también se le conoce como *man in the middle*. Realizar esta actividad es un procedimiento sencillo. Un monitoreo cerca del lugar permite al atacante detectar datos importantes como el SSID de la red, la dirección MAC del dispositivo, el fabricante, la intensidad de la señal, el modo en el que opera el canal en el que transmite, sus métodos de seguridad, etc..

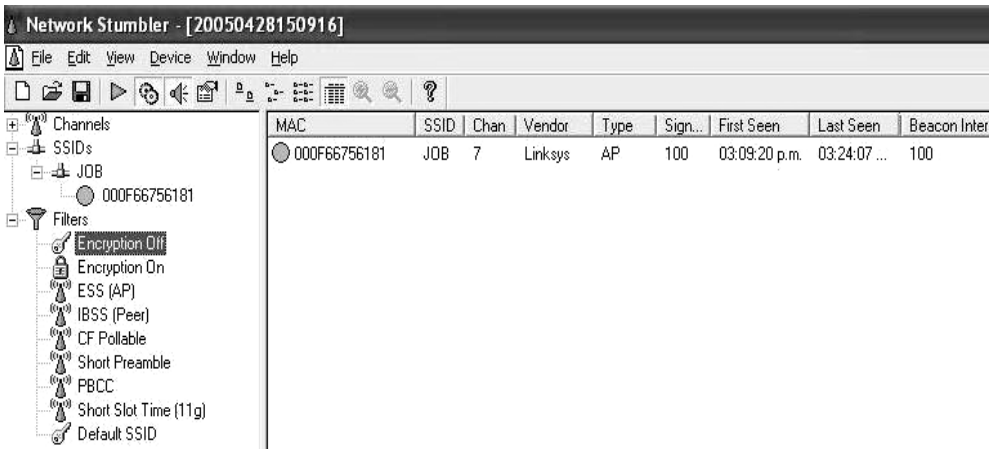


Figura 3.2 Monitoreo de una red inalámbrica

Conociendo estos datos el atacante puede colocar un punto de acceso configurado de tal forma que tenga el mismo SSID, con el mismo modo de operación, el mismo canal de transmisión, incluso hasta del mismo fabricante.

Todo esto tiene un propósito, hacerse pasar por un punto de acceso autorizado y conseguir que los usuarios se conecten a éste, para de esta manera obtener

datos importantes como la dirección MAC de tarjetas autorizadas, la llave WEP, etc. Hay que resaltar el hecho de que el punto de acceso no autorizado no necesariamente tiene que suministrar algún servicio, ya que ningún software de tarjetas inalámbricas, incluso la utilería de Windows XP nos asegura que este dispositivo realmente esté conectado a una red cableada. Simplemente se reducen a mostrar las señales emitidas por cualquier punto de acceso inalámbrico.

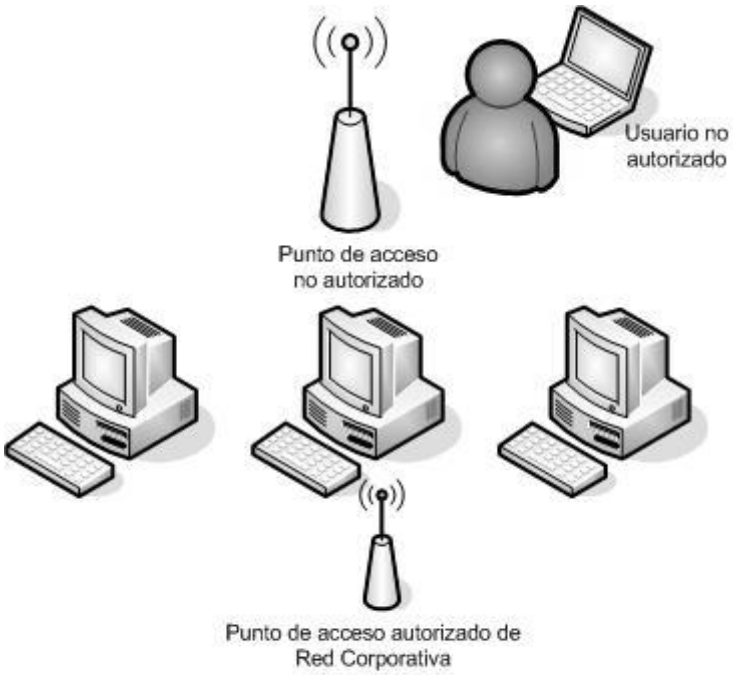


Figura 3.3 Punto de Acceso No autorizado

Una adecuada auditoria de manera periódica y una coordinación con los respectivos departamentos para la instalación y funcionamiento de estos puntos de acceso pueden resolver en gran parte estos problemas.

3.3 Uso indebido

Un atacante puede hacer uso de la red para conectarse a Internet o conectarse a la red corporativa que se encuentra atrás del punto de acceso. El uso indebido quizá no llegue a causar ningún problema operacional pero no por eso deja de ser ilícito en el uso de este tipo de redes. Un atacante en este caso quizá simplemente quiera acercarse al punto de acceso, asociarse a la red y revisar su correo electrónico. Sin embargo también un usuario mal intencionado puede mandar *spam* a una gran cantidad de correos electrónicos o más peligroso, conectarse a los servidores que forman parte de la red corporativa y atentar contra la información ahí almacenada.

Realmente no importa los fines que el atacante tenga, su uso es inaceptable en cualquiera de estos casos. A diferencia con las redes cableadas, en las cuales para realizar este tipo de actividades es necesario tener la presencia física dentro de la infraestructura de la red. En las redes inalámbricas el atacante tiene una mayor libertad en cuanto a espacio y tiempo para planear y desarrollar un ataque por lo que la administración segura de este tipo de tecnología requiere, como ya mencionamos anteriormente de una continua auditoria y supervisión de la red con el fin de detectar cualquier anomalía que ponga en peligro la integridad de la infraestructura inalámbrica.

3.4 Riesgo en el medio

Cuando aseguramos una red tenemos que tener en consideración los riesgos asociados con cada uno de los diferentes ataques. Preguntas como " ¿Qué puede pasar? ", " ¿Cómo puede pasar? ", " ¿Qué va ocurrir cuando pase? " y " ¿Qué tan difícil es de defender? " empiezan a tomar importancia.

Un ataque que el día de hoy resulta ser una teoría bien fundamentada quizá el día de mañana pueda ser extensamente distribuida en un código de programación. Pongamos por ejemplo el caso de WEP el cual comenzó como un artículo que describía los problemas teóricos con el protocolo. Quizá muy pocas personas tengan la habilidad de tomar estas vulnerabilidades y escribir un código para explotarlas. Sin embargo en la actualidad en el mercado de software, tanto libre como comercial existen una variedad de herramientas que son de bastante utilidad para aumentar la probabilidad de romper con estos protocolos de seguridad.

Una red doméstica usualmente no es un blanco atractivo para los atacantes. La red de un banco cuyo tráfico normal implica usuarios, contraseñas y dinero es un blanco de mucho mayor interés para un atacante. Estos hechos nos llevan a tomar decisiones importantes con el fin de salvaguardar la integridad de una red inalámbrica. Un adecuado análisis sobre el tipo de información que se va transmitir a través de la red, el tipo de servicio que requiera el usuario y las posibles amenazas de otorgarlo, serán el camino necesario para llegar a legislar las políticas de seguridad necesarias para dar siempre el mejor servicio y brindar a los usuario la protección que requieran tanto en su hardware como en su información.

C a p í t u l o 4

SOLUCIONES PARA CONTRARRESTAR LOS PUNTOS VULNERABLES DE SEGURIDAD EN WLAN'S

4.1 Autenticación y Encripción.

Conceptos importantes dentro de la seguridad informática como Autenticación, Autorización y Contabilidad AAA (*Authentication Authorization and Accounting*) son fundamentales en la implementación de un sistema informático seguro. Esta estructura tiene como función el control de acceso a recursos informáticos mediante la imposición de políticas.

El primer concepto "*Autenticación*" proporciona un método para identificar a los usuarios mediante la petición y comparación de un conjunto de criterios únicos característicos de cada usuario para conseguir el acceso.

La "*Autorización*" va después de la autenticación y es el método por el cual se determinan los permisos del usuario para realizar ciertas tareas o hacer uso de ciertos recursos de red u operaciones.

Por ultimo la "*Administración*" es el método de medición y registro del consumo de los recursos de red, mediante la monitorización y generación de informes.

4.1.1 RADIUS

RADIUS es un protocolo de seguridad con un enfoque cliente/servidor para autentificar a usuarios remotos. Este protocolo fue creado bajo la necesidad de un método que conjuntara los tres conceptos fundamentales citados anteriormente: autenticación, autorización y administración de uso.
Las características de este protocolo son:

- Un NAS (*Network Access Service*) que funciona como cliente, por lo que es responsable de transferir la información de usuario a los servidores RADIUS designados y de actuar con la respuesta recibida. Los servidores RADIUS son lo responsables de recibir las peticiones de conexión de los usuarios, realizar la autenticación y devolver los detalles de configuración necesarios para que el cliente proporcione los servicios al usuario.

- La comunicación entre el cliente y el servidor RADIUS se autentifica mediante el uso de una clave compartida que nunca se envía a través de la red como texto sin cifrar. Además, las contraseñas de usuario se envían cifradas entre el cliente y el servidor RADIUS para eliminar la posibilidad de un ataque.

- El servidor RADIUS soporta una amplia variedad de métodos para autentificar a un usuario. Cuando se le proporciona el nombre de usuario y la contraseña original utilizada por el usuario, puede soportar CHAP (*Challenge Handshake Autentication Protocol*) o PAP (*Password Authentication Protocol*) entre otros.

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

El paquete RADIUS se encapsula en un flujo de datos UDP (*User Datagram Protocol*) que se envía a los puertos 1812, 1813 y 1814, según la IANA (*Internet Assigned Numbers Authority*) y que representan respectivamente el acceso, la contabilidad y la intermediación para este protocolo.

UDP fue elegido en vez de TCP (*Transmission Control Protocol*) por razones definitivamente técnicas. RADIUS es un protocolo basado en transacciones con las siguientes características:

- Si la petición de acceso a un servidor de autenticación primario falla, un servidor secundario o alterno puede atender la petición. Para esto es necesario guardar una copia de la petición sobre la capa de transporte para tener en cuenta la transmisión alterna

- Los requisitos de la sincronización de este protocolo en particular son perceptiblemente diferentes a los que TCP proporciona. Por un lado RADIUS no requiere una detección receptiva o sensible de datos perdidos. El usuario puede esperar algunos segundos para que la autenticación se efectué. Sin embargo no está dispuesto a esperar varios minutos la autenticación. Por lo tanto la entrega confiable de datos TCP dos minutos después no resulta útil para este caso. El uso de un servidor alterno seria la solución más eficiente.

Para más información sobre la estructura de paquete que utiliza RADIUS ver el *apéndice C*

4.1.2 Operación de un servidor RADIUS

Cuando un cliente NAS (*Network Access Service*), en este caso un punto de acceso inalámbrico, esta configurado a usar un servidor RADIUS, cualquier usuario de este cliente presenta la información que lo autentifica con éste. Una vez que el cliente haya obtenido esta información procede a autentificarse con el servidor. Para hacer esto, el cliente crea una petición de acceso que contiene atributos tales como el nombre de usuario, la contraseña, el identificador del cliente y la identificación del puerto al que el cliente esta teniendo acceso. Cuando se presenta la contraseña, esta se oculta utilizando un método basado en RSA MD5. La petición de acceso es sometida al servidor RADIUS vía red, si no se recibe respuesta alguna por parte de este, se vuelve a enviar otro número de veces. El cliente puede seguir enviando mensajes de petición de acceso incluso a un servidor(es) alternativo(s) en el caso en el que el servidor primario o principal se encuentre abajo (fuera de servicio) o no sea alcanzable por la red.

Una vez que el servidor recibe la petición, válida al cliente que la envía. Una petición de un cliente sin la clave compartida debe ser rechazada. Si el cliente es valido, el servidor RADIUS consulta una base de datos de usuarios para encontrar el nombre de quien proviene la petición. La petición del usuario entra en la base de datos que contiene una lista de ciertos requerimientos que debe encontrar para obtener el acceso, incluyendo también la contraseña del usuario, el cliente y el puerto por el cual el usuario tiene el acceso. Sí ninguna condición es encontrada, el servidor RADIUS envía una respuesta de rechazo de acceso que indica que esta

petición de usuario es inválida. El servidor puede incluir un mensaje de texto dentro de la respuesta de rechazo para que sea mostrada por el cliente al usuario.

En caso contrario, si se encontraron todas las condiciones, el servidor RADIUS puede emitir lo que se denomina un "*acceso-desafío*" como respuesta para que el usuario responda. Esto puede ser incluido en un mensaje de texto que va a hacer mostrado por el cliente al usuario para un respuesta. El cliente entonces reenvía nuevamente su petición de acceso original con una nueva identificación de petición, con los atributos de usuario y contraseña remplazados por la respuesta (cifrada) e incluyendo el estado del atributo *acceso-desafío* sea 0 o 1, el cual tiene que estar presente en la petición. El servidor puede responder a esta nueva petición de acceso con un "*acceso- aceptar*" o un "*acceso-rechazar*" u otro acceso "*desafío*".

Si todas las condiciones son encontradas, la lista de configuración de valores para el usuario es colocada dentro de la respuesta *acceso-aceptar*. Estos valores incluyen el tipo de servicio por ejemplo: SLIP (*Serial Line Internet Protocol*), PPP (*Point to Point Protocol*), *login user* y todos los valores necesarios para proporcionar el servicio deseado. Para SLIP y PPP estos pueden incluir valores como la dirección IP o la mascara de subred o algún tipo de compresión de paquetes.

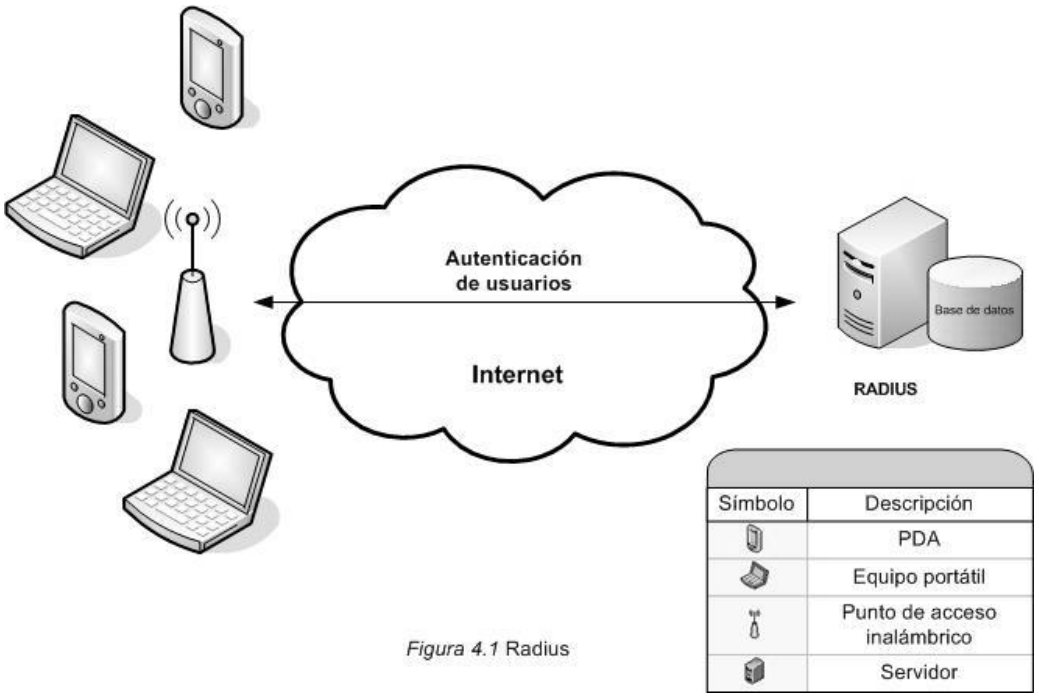


Figura 4.1 Radius

4.2 IPsec VPN.

Una red privada virtual (*Virtual Private Network*) es una forma de utilizar una infraestructura de telecomunicaciones pública, como Internet, para ofrecer a los usuarios remotos un acceso seguro a la red de su empresa o institución. Debido a que las redes inalámbricas utilizan bandas de frecuencias libres y usuarios imprevistos pueden tener acceso a ellas por equivocación o con mala intención, este tipo de redes son buenas candidatas para el despliegue y mantenimiento de redes VPN.

Las redes VPN mantienen los procesos de seguridad y protocolos de túnel como L2TP (*Layer Two Tunneling Protocol*), IPSec (*Internet Protocol Secure*) y PPTP (*Point to Point Tuneling Protocol)* entre los mas utilizados. De hecho los protocolos, mediante el cifrado de datos en el extremo emisor y el descifrado en el receptor, envían los

datos a través de un túnel en el que no se pueden introducir datos que no se hayan cifrado correctamente.

La parte *Virtual* (virtual) del término hace referencia a la coexistencia de dos redes independientes dentro de un único segmento de red, como la coexistencia de IP, IPX (*Internetwork Packet Exchange*) en la misma LAN, o de tráfico IP, IPSec, y L2TP atravesando Internet. La parte *Private* (privada) representa que la interacción solo se puede dar en los extremos finales del canal y por nadie más. Por ultimo la parte de *Network* (red) hace referencia como cualquier número de dispositivos que tengan en común algún modo de comunicación entre si, sin importar su ubicación geográfica.

La ventaja básica de las comunicaciones VPN reside en la reducción de costos para la interconexión con sitios remotos, opuesto a lo que significaría económicamente hablando un sistema de líneas propias o alquiladas por alguna organización. Las líneas dedicadas suelen instalarse para aplicaciones críticas cuando se necesita garantizar una tasa de datos muy alta entre las estaciones, pero cuando la transferencia de datos sobre redes públicas no es fiable y no se puede garantizar la disponibilidad de ese servicio. El medio inalámbrico se convierte en una opción de un costo barato. Sin embargo no se pude dejar de hacer a un lado todos los riesgos de seguridad que implican este tipo de tecnologías, y que hemos mencionado en el capitulo anterior.

Otro de los motivos más importantes para el uso de redes VPN recae en la necesidad de privacidad en las comunicaciones de datos. Todas las comunicaciones internas que se transmitan al exterior deben ocultarse de un observador externo mediante el uso de criptografía y mecanismos de autenticidad.

La autenticación y los mecanismos de cifrado tradicionales de 802.11a/b/g por si solos no ofrecen suficiente protección contra usuarios mal intencionados experimentados. Mientras que el uso de 802.1X junto con un servidor RADIUS queda fuera del alcance de las redes inalámbricas pequeñas estándar, la mayoría de los dispositivos de seguridad de redes del mercado pueden hacer funcionar una VPN consiguiendo un nivel de protección similar.

La implementación de una VPN puede ser a través de *hardware* o *software*. Las VPNs basadas en *hardware* utilizan equipos dedicados a determinadas funciones de red como los ruteadores. A diferencia con las VPNs basadas en *software* en donde el sistema operativo emplea bastantes recursos del procesador en brindar otros servicios aparte de éste.

VPN por *hardware*

La siguiente implementación hace referencia al ruteador inalámbrico WRV54G de la empresa *Linksys*, el cuál cuenta con *Quick VPN*. Programa que se instala en un equipo portátil o de escritorio y que nos permite establecer una conexión VPN entre el ruteador y el equipo en cuestión.



Fig. 4.2 Ruteador Inalámbrico WRV54G

Para realizar la configuración es necesario seguir la siguiente secuencia de pasos:

Es necesario tener conectado el ruteador inalámbrico y un equipo de cómputo al mismo concentrador o *hub*.

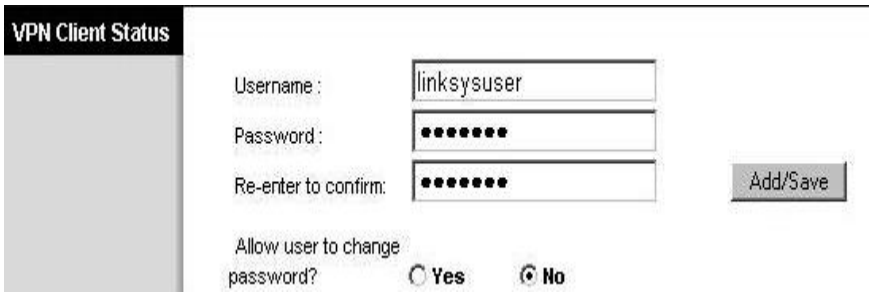
- Abrir el navegador de Internet que se este utilizando, en el equipo de cómputo y escribir la dirección IP del ruteador.



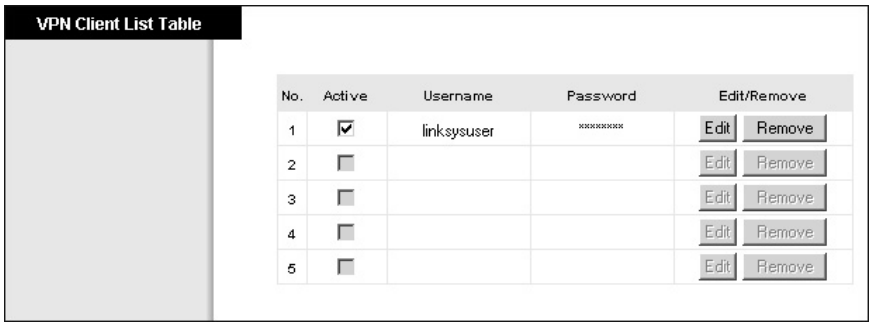
- Aparecerá la ventana de acceso al *firmware* en donde se necesita el nombre de usuario y contraseña. Una vez conectado con el ruteador desde el *setup* entrar a las restricciones de acceso y a la opción de acceso a clientes VPN.



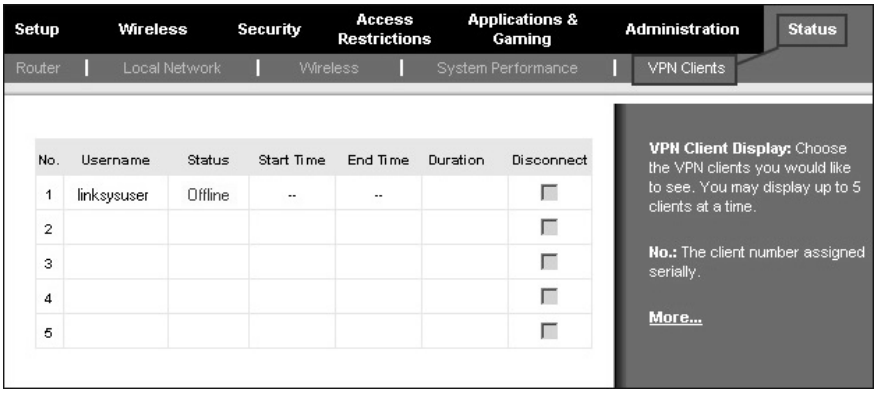
- Se ingresan los datos de los usuarios que se van a conectar.



- Después de crear las cuentas de usuario, cada una deberá aparecer en la tabla de la lista de clientes VPN.



- Una vez que se hayan agregado todos los usuarios y guardado todos los cambios, podemos monitorear el estado de la conexión de los usuarios.



Una vez configurado el ruteador inalámbrico es necesario realizar la configuración de los clientes.

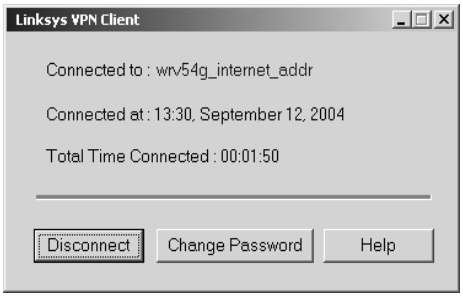
- Se realiza la instalación del software en los equipos que se desean como clientes de la VPN y se ejecuta el programa.



- Cuando aparezca la ventana de *Linksys VPN client* es necesario escribir la información requerida como nombre del perfil, nombre de usuario, contraseña, y la dirección del servidor.



Si la conexión se realiza con éxito, entonces aparecerá una ventana con el estado de la conexión y un icono en la barra de herramientas.



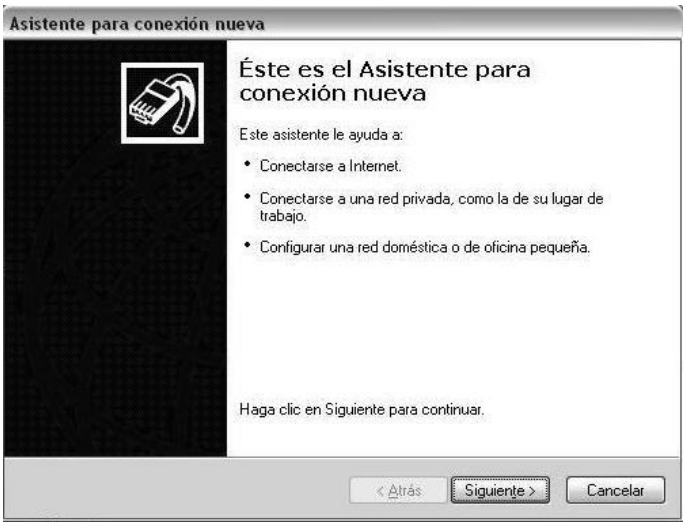
VPN por *software.*

A continuación se citan una serie de pasos para implementar un VPN en el sistema operativo *Windows* XP:

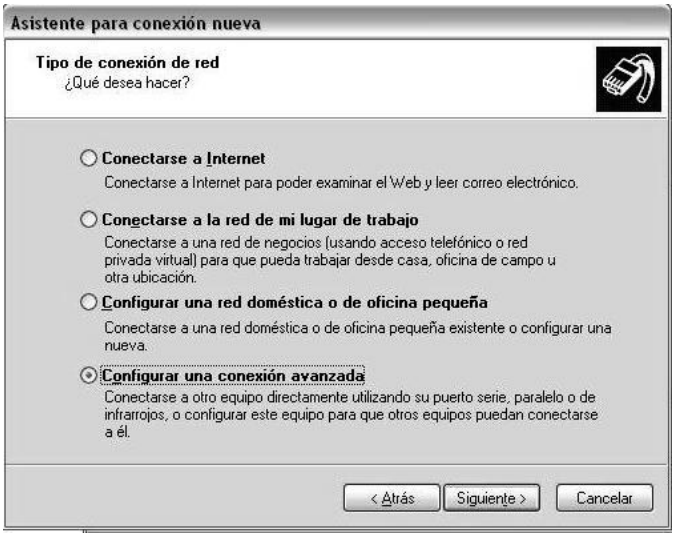
Primero que nada es necesario instalar un servidor VPN para poder realizar una conexión remota de un cliente VPN.

Servidor VPN

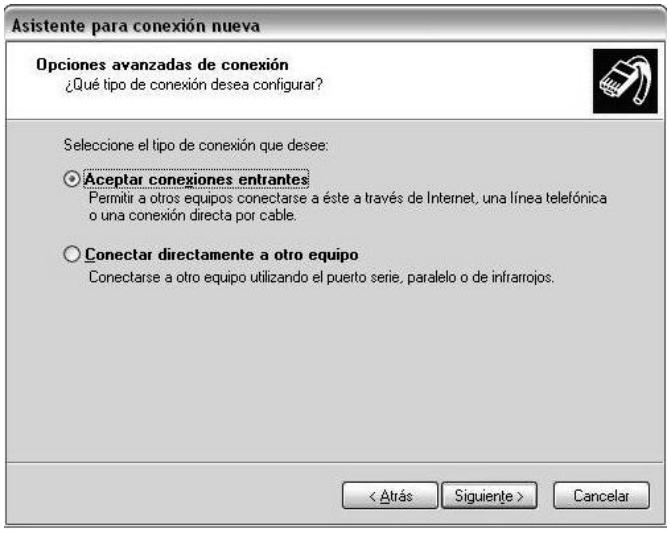
- Vamos al *panel de control* y abrimos las *conexiones de red*. En las tareas de red elegimos *crear una conexión nueva*, a continuación se ejecuta el asistente para conexión nueva.



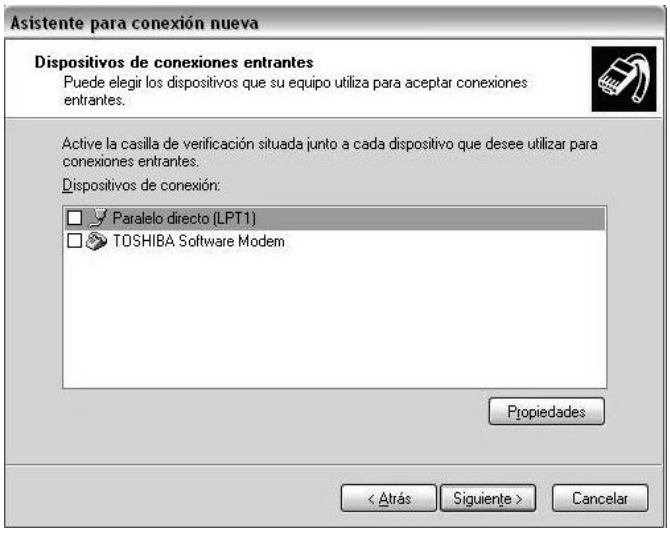
- Pulsamos el botón *siguiente* y seleccionamos *configurar una conexión avanzada.*



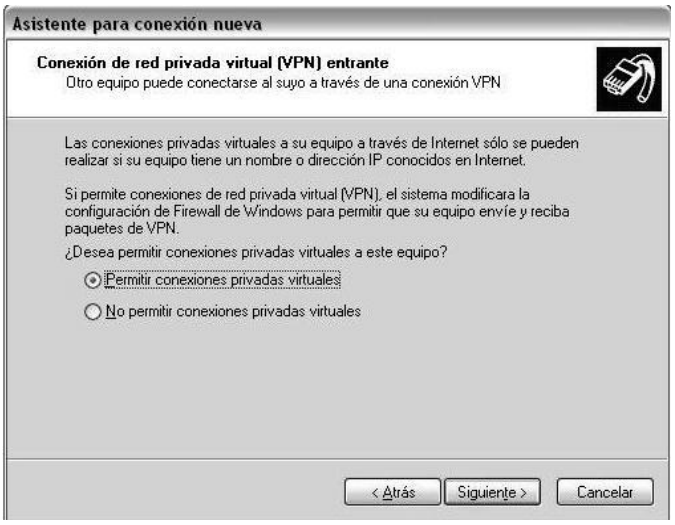
- Pulsamos *siguiente* y seleccionamos la opción de *aceptar conexiones entrantes.*



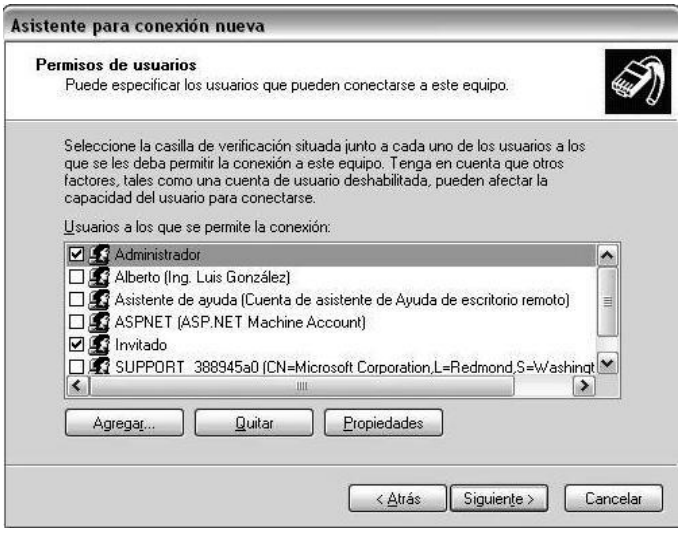
- En la ventana dispositivos de conexiones entrantes no seleccionamos ninguno, pues no deseamos que se conecten a este equipo usando el puerto paralelo u otro dispositivo.



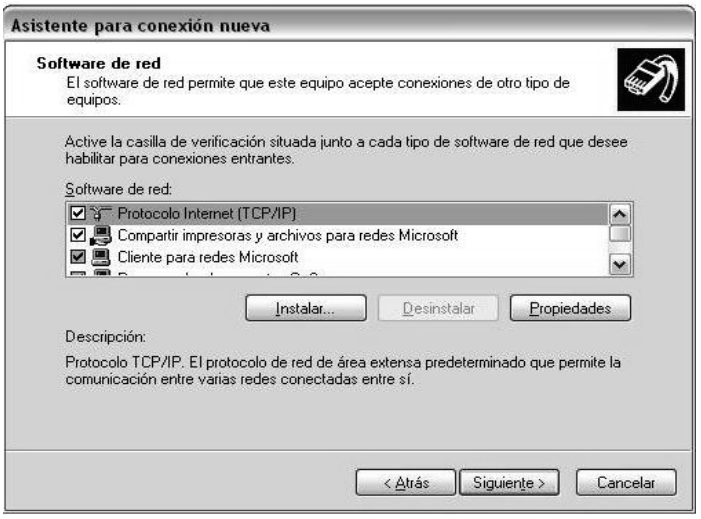
- Pulsamos *siguiente* y en la ventana *conexiones red privada virtual (VPN) entrante* seleccionamos la casilla *permitir conexiones virtuales privadas*.



- En la ventana *permisos de usuarios* seleccionamos los usuarios que tendrán permiso para conectarse al servidor usando VPN, con la posibilidad de crear nuevos usuarios.



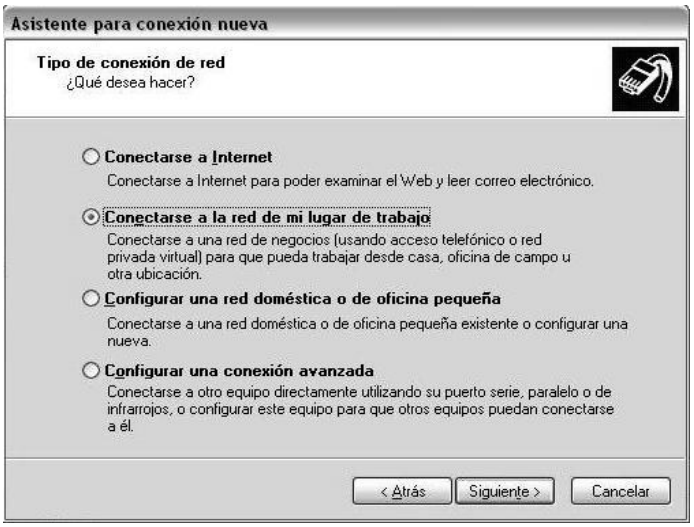
- En la ventana *software de red* habilitamos los protocolos que usaremos en la VPN. y finalizamos la instalación del servidor VPN.



Ahora que ya tenemos habilitado el servicio y listo para recibir para recibir la conexión de clientes VPN. El siguiente paso es configurar una conexión cliente en un equipo remoto para que se conecte con este equipo.

Cliente VPN

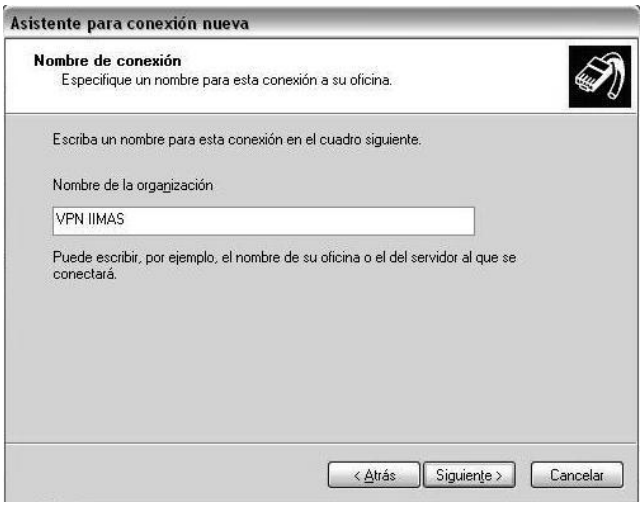
- Abrimos las *conexiones de red* y seleccionamos *crear una conexión nueva*. En el asistente seleccionamos la casilla *conectarse a la red de mi lugar de trabajo*.



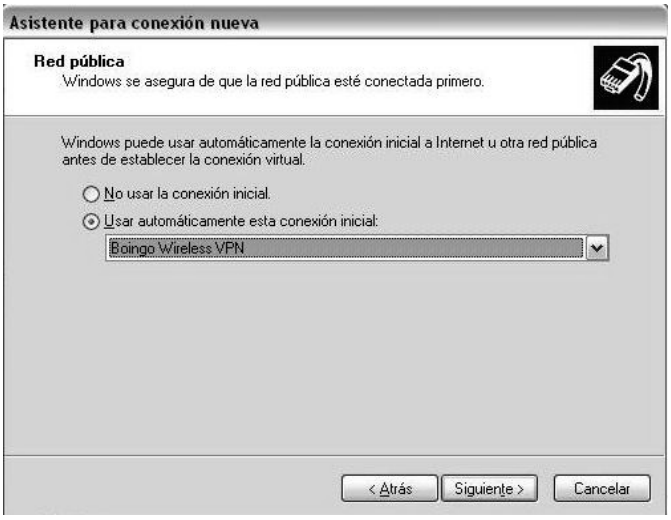
- Seleccionamos *conexión de red privada virtual.*



- En la siguiente ventana le damos un nombre a la conexión y pulsamos *siguiente*.



- En la ventana *red publica* seleccionamos la opción *usar automáticamente esta conexión inicial* si deseamos utilizar una conexión vía modem. En caso contrario si estamos utilizando una red LAN ethernet seleccionamos la opción restante.



- Por ultimo escribimos la dirección IP del servidor VPN al que queremos conectarnos y finalizamos el asistente.



Ahora que tenemos configurado el servidor, el equipo remoto puede realizar una conexión segura VPN.



Hasta ahora hemos observado un par de procedimientos para la implementación de una VPN. Sin embargo es necesario conocer un poco más sobre el protocolo

IPSec, el cuál puede utilizar dos protocolos para brindar seguridad, ESP (*Encapsulating Security Payload)* o AH (*Authentication Header*). El primero cifra y autentifica los paquetes mientras que el segundo solo los autentifica. Para más información sobre estos protocolos ver el *apéndice D*.

IPSec es el protocolo mas reconocido, soportado y estandarizado de todos los protocolos VPN. IPSec es un marco de trabajo de estándares abiertos que produjo un conjunto de protocolos seguros que pueden ejecutarse sobre conectividad mediante el protocolo IP ya existente. Ofrece servicios de autenticación y cifrado de datos en la tercera capa del modelo OSI y puede implementarse en cualquier dispositivo que se comunique sobre IP. IPSec puede proteger todo el tráfico que se transporte sobre IP. También se usa junto con protocolos de túnel de la capa 2 para conseguir cifrado y autenticación para tráfico no IP.

4.2.1 Trama de IPSec

IPSec permite definir la precisión con la que el usuario puede especificar su política de seguridad, pudiendo determinar que cierto tráfico sea identificado para recibir el nivel de protección deseado.

IPSec está diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación.

Por defecto hay ciertos algoritmos estándar que deberán soportar todas las implementaciones para asegurar la interoperabilidad en el mundo global de Internet. Dichos algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones *hash*. El administrador puede determinar el uso de otro tipo de algoritmos, como algoritmos de cifrado de clave simétrica IDEA,

Blowfish o el más reciente AES, que él considere más adecuados para un entorno determinado.

Para más información sobre la trama IPSec ver el *apéndice D*

4.2.2 Métodos de autenticación

El primer método de autenticación se basa en el conocimiento de un secreto compartido que es una cadena de caracteres que únicamente conocen los dos extremos que quieren establecer una comunicación IPSec. Mediante el uso de funciones *hash* cada extremo demuestra al otro que conoce el secreto sin revelar su valor; así los dos se autentican mutuamente. Debe configurarse un secreto distinto para cada par de estaciones, por lo que el número de secretos crece muy rápidamente cuando aumenta el número de estaciones.

El segundo método es el de certificados digitales. Este es adecuado para la interconexión de muchas estaciones IPSec. Es conocido que para el uso de este método de autenticación es necesario utilizar certificados digitales X509. El uso de certificados permite distribuir de forma segura la clave pública de cada estación, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere de la aparición de un elemento más, PKI (*Public Key Infrastructure*).

4.2.3 Operación de IPSec

- Inicio de una sesión IPSEC:

  Primera fase - Intercambio de llaves.

  Segunda Fase- Establecimiento de las SA's. En esta segunda fase

ambos sitios requieren acordar los parámetros de seguridad de IPSEC (IPSec SADB).

Estos parámetros serán:

IPSec peer: Punto de terminación del túnel de IPSec.

IPSec proxy: Tráfico a ser encriptado/desencriptado.

IPSec transform: Encripción y hashing.

IPSec lifetime: Tiempo de regeneración de la SA

- Encripción/desencripción de paquetes. Se completan las dos fases del inicio. Las SA's son creadas en ambos extremos IPSec. Utilizando la información negociada SADB los paquetes de salida son encriptados y los paquetes de entrada son desencriptados.

- Reconstrucción de las SA's después de la expiración del tiempo. Para asegurarse que las llaves no son comprometidas son cambiadas periódicamente. Las SA son reconstruidas cuando el tiempo expira o el volumen de datos ha sido excedido ocasionando que otra SA con idénticos parámetros sea definida

4.2.4 IPSec Móvil

Una situación típica es la de un cliente que se conecta desde una ubicación remota a través de un enlace inalámbrico y obtiene una dirección IP distinta asignada mediante DHCP (*Dynamic Host Configuration Protocol*) que cambia de vez en cuando. Ya que una de las direcciones IP es dinámica, no puede utilizarse para verificar la identidad. Por eso el uso de certificados X.509 resulta un método alternativo de autenticación para este tipo de redes.

4.3 Descripción del protocolo 802.1x

Uno de los mecanismos mas utilizados para realizar el control de conexiones entre un cliente y un servidor de autenticación es el uso de bases de datos en las que se capturan manualmente los datos de usuarios autorizados, ya sean identificadores de usuario o direcciones MAC. Sin embargo, esta solución puede presentar problemas de escalabilidad cuando estas bases de datos crecen demasiado o los usuarios cambian frecuentemente.

La especificación 802.1X es un estándar de control de acceso desarrollado por la IEEE que plantea tres entidades básicas como son el cliente, el punto de acceso y el servidor de autenticación. En lo que respecta a los protocolos que componen la especificación 802.1X, el estándar es bastante flexible al no limitar los mecanismos de autenticación a ninguna solución concreta, sino que es posible hacer uso de cualquier tipo de especificación convenientemente adaptada al marco 802.1X. Esta flexibilidad nos va a permitir hacer uso de protocolos basados en certificados digitales como elementos fundamentales a la hora de verificar la autenticidad de los usuarios.

La importancia del uso de certificados digitales radica en su capacidad para aliviar los problemas de escalabilidad asociados a las soluciones fundamentadas en el uso de bases de datos. Estos elementos permiten que un usuario desconocido para el sistema pueda hacer uso de la red con solo proporcionarle el certificado adecuado. Además en este certificado pueden incluirse ciertos atributos acerca del usuario, como el tiempo máximo que puede utilizar la red, los servicios a los que puede acceder o los recursos que puede utilizar.

4.3.1 Operación del protocolo 802.1.x

Cuando un equipo se conecta a un punto de acceso, antes este debe de realizar una asociación en la que se da a conocer su identificador al punto de acceso para que este a su vez informe al resto de la red que dicho equipo se encuentra bajo su área de cobertura. Es en esta fase cuando debe realizarse el proceso de control de acceso para ver si realmente el usuario tiene permiso para hacer uso de la red.

802.11 como hemos mencionado permite utilizar diferentes mecanismos de autenticación. Su funcionamiento se basa en el concepto de puerto, visto este como el punto a través del cual se puede acceder a un servicio proporcionado por un dispositivo, que para este caso es el punto de acceso inalámbrico. En un principio todos los puertos están desautorizados, excepto el que utiliza el punto de acceso para comunicarse con el servidor. Cuando un nuevo usuario entra en su área de cobertura, este le proporciona al punto de acceso información de autenticación, dependiente del mecanismo utilizado, que este reenvía al servidor de autenticación. Cuando este le contesta, si la respuesta es que el usuario puede hacer uso de la red, autoriza un puerto para que lo utilice el usuario.

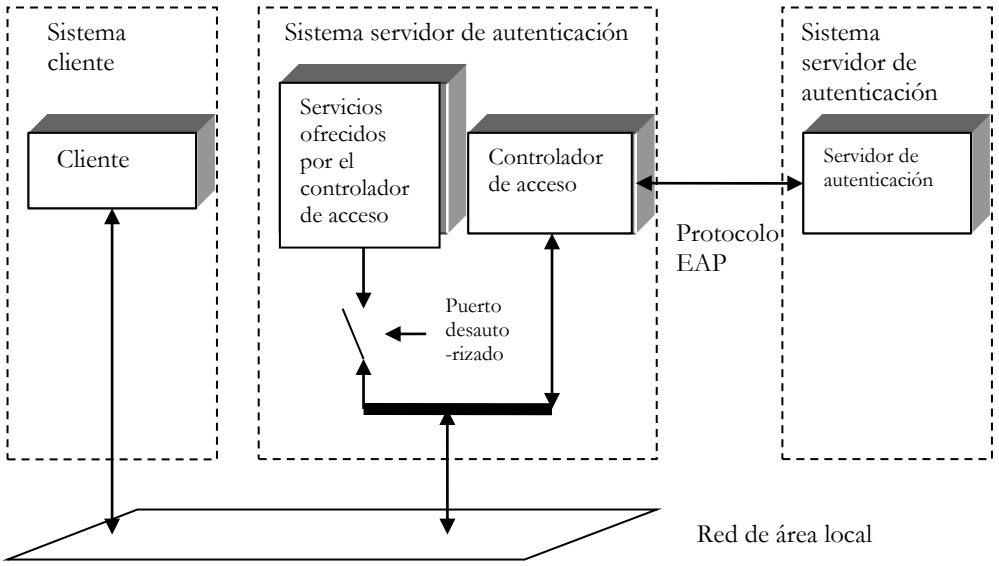


Figura 4.3 802.1x

Como podemos observar, la información de autenticación se encapsula en el protocolo EAP (*Extensible Authentication Protocol*), un mecanismo genérico de transmisión de datos de autenticación que puede ser conformado en distintos subprotocolos entre los que, por ejemplo, se encuentra EAP-MD5, que basa la autenticación del usuario en el uso de un *login* y un *password*, o EAP- TLS, que se basa en el uso del protocolo TLS (*Transport Layer Security*) y permite la autenticación mutua entre los dos extremos. EAP-TLS durante la fase de establecimiento de la conexión, este protocolo hace uso de certificados X.509 para identificar a las partes, lo cual constituye un mecanismo robusto de autenticación y dicha fase genera también una clave compartida por los dos extremos que puede utilizarse para derivar claves para el cifrado de las transmisiones inalámbricas.

Finalmente, los paquetes EAP se transmiten mediante el protocolo EAPOL, el cual especifica cómo encapsular los paquetes EAP en una red de área local tanto *ethernet* como 802.11.

Aunque en la especificación 802.1X se habla de los servidores de autenticación en términos genéricos, en la práctica se trata de elementos diseñados según los criterios del marco AAA (*Authentication, Authorizationand Accounting*). Este marco define los elementos básicos necesarios para autenticar usuarios, manejar peticiones de autorización y realizar la contabilidad del sistema. Un servidor AAA debe ser capaz de recibir peticiones, examinar el contenido de dichas peticiones, determinar qué autorización se está pidiendo, recuperar las políticas que necesite de un repositorio, evaluar la petición y obtener la respuesta a la petición, o bien reenviar la petición a otro servidor AAA.

RADIUS es un protocolo encuadrado dentro del marco AAA y utilizado principalmente en entornos donde los clientes son elementos de acceso a la red como los puntos de acceso). Estos elementos mandan información al servidor cuando un nuevo cliente intenta conectarse, tras lo cual el servidor realiza el proceso de autenticación del usuario y devuelve al elemento de acceso la información de configuración necesaria para que éste trate al cliente de la manera adecuada. Toda la comunicación entre el elemento de acceso y RADIUS se encuentra cifrada mediante un secreto compartido que nunca se transmite por la red. RADIUS satisface completamente los requisitos al soportar el protocolo EAP-TLS

Una de las alternativas para implementar mecanismos autorización, si no se quiere mantener una base de datos con los permisos de cada usuario, es la utilización de certificados digitales. Un certificado es una estructura que contiene información del usuario en cuanto a identidad o permisos, y que va firmado digitalmente por una entidad de confianza. Dado que los certificados de clave pública X.509 (los más ampliamente extendidos) se utilizan exclusivamente para propósitos de identidad, el uso de certificados PKI, nos permite plasmar de forma sencilla los

privilegios asociados a un usuario individual o a un grupo de usuarios en conjunto. Este tipo de certificados pueden ser utilizados también para representar la pertenencia de un usuario a distintos grupos de privilegios.

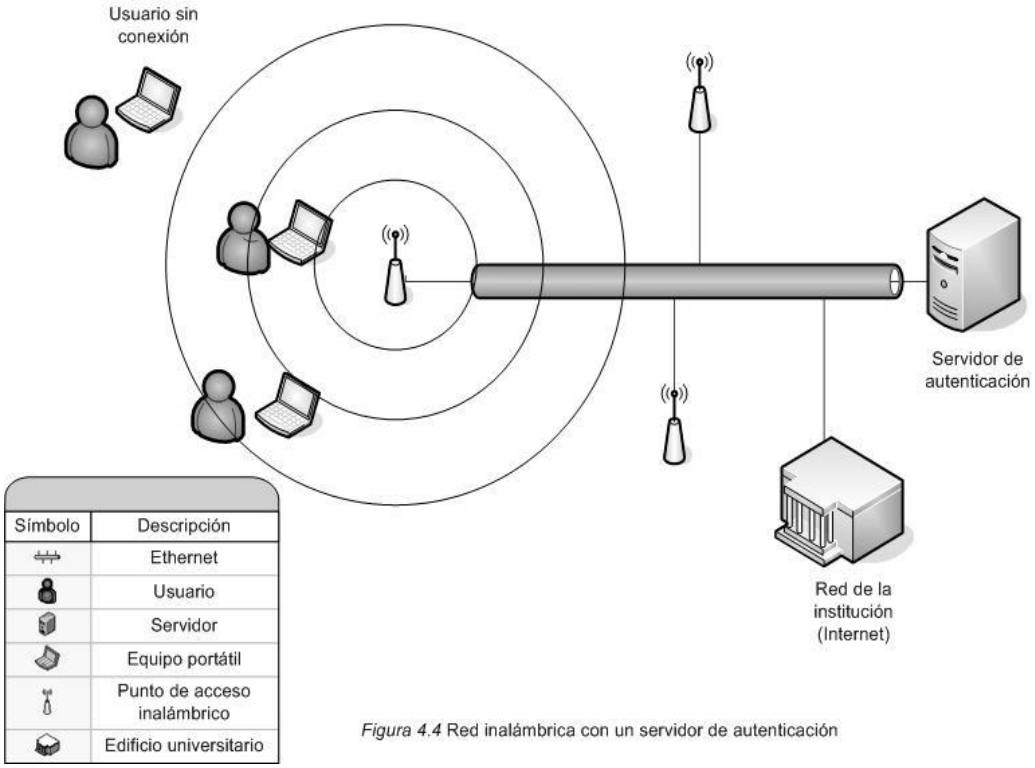


Figura 4.4 Red inalámbrica con un servidor de autenticación

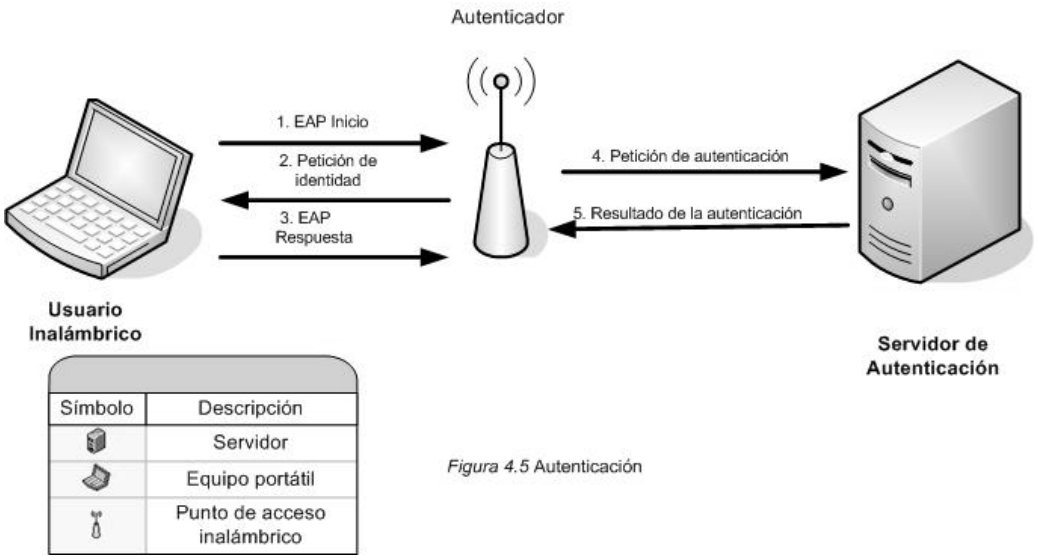


Figura 4.5 Autenticación

Todo el proceso consta en si de tres fases: autenticación, autorización y distribución de la clave de cifrado WEP. Una vez conectado el cliente, el sistema realizará periódicamente un proceso de renegociación de la clave WEP. Del mismo modo, también gestionará la posibilidad de que el usuario se desplace hacia el área de cobertura de otro punto de acceso, todo ello con el fin de reaprovechar la asociación para que el proceso de conexión a través del nuevo punto de acceso se realice de forma eficiente.

En la siguiente figura podemos observar la configuración desde *firmware* de un punto de acceso cuya seguridad va estar soportada por un servidor de autenticación.

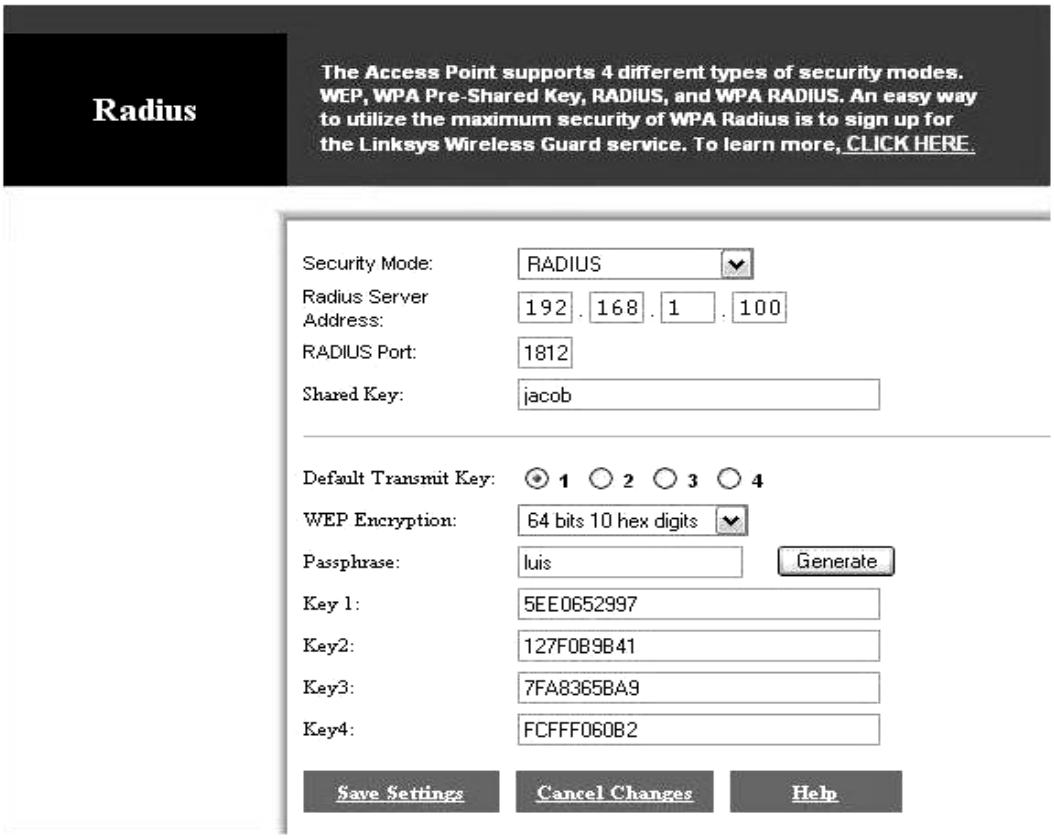


Figura 4.6 Firmware de configuración de un punto de acceso con RADIUS

- *Autenticación*

La primera fase funciona siguiendo el estándar IEEE 802.1X, es decir, cuando el cliente entra en el área de cobertura del punto de acceso, este le pide su identidad, y el cliente se la proporciona.

Tras esta fase inicial se realiza el proceso de establecimiento de conexión TLS entre los extremos, donde según el estándar tanto el cliente como el servidor de autenticación se autentican mutuamente mediante certificados X.509 y

negocian los parámetros de configuración necesarios para establecer el canal de comunicación seguro.

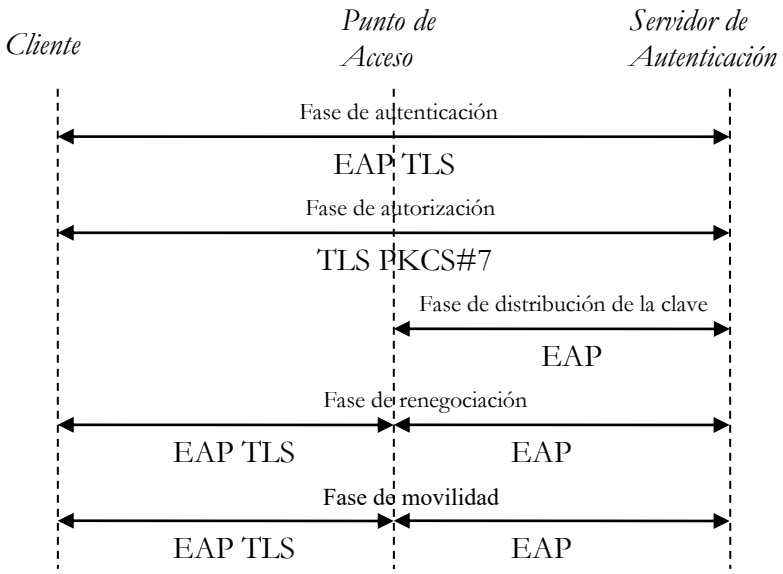


Figura 4.7 Proceso de autenticación

Una vez terminada la negociación, se establece un canal TLS entre el cliente y el servidor de autenticación basado en la posesión por ambas partes de un secreto compartido *Shared Key* que posteriormente se utilizará para derivar la clave WEP.

- *Autorización*

En esta fase el cliente indica al servidor de autenticación cual es el tipo de conexión que desea en cuanto al ancho de banda requerido y el tiempo que va a estar conectado, junto con los certificados PKI que demuestran que dicho usuario está autorizado a realizar el uso de la red que pide. Entonces el

servidor evalúa los certificados y comprueba si todo es correcto y si el nivel de privilegios del cliente es el necesario, continuando con el protocolo si todo va bien y desautorizando al cliente a acceder a la red si hay algún problema. De esta forma no es necesario acceder a ninguna base de datos de usuarios para comprobar los permisos de los mismos, sino que sólo se necesita confiar en las entidades emisoras de dichos certificados de autorización.

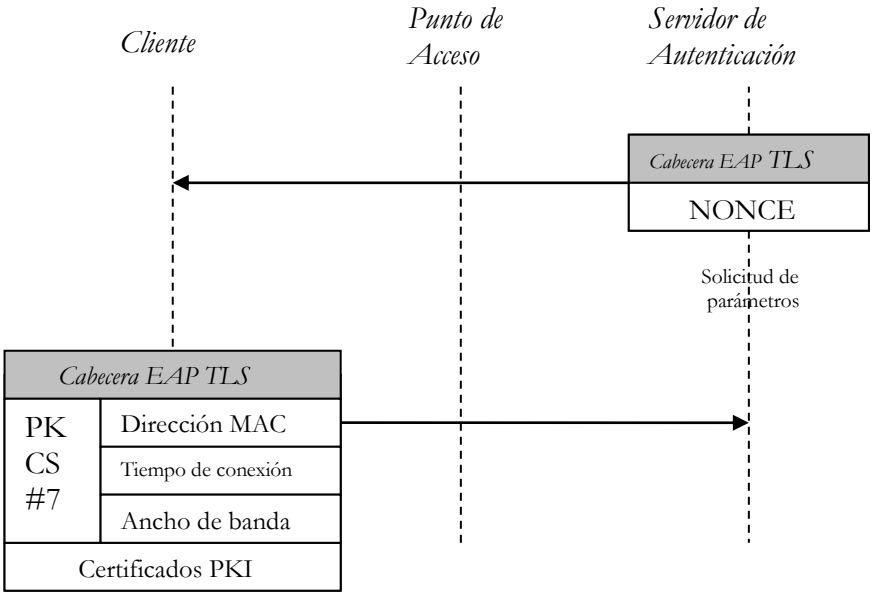


Figura 4.8 Proceso de autorización

Los parámetros del cliente se mandan en una estructura firmada PKCS#7, de manera que el servidor de autenticación pueda estar seguro de que nadie ha modificado estos parámetros. Además, toda la información relativa a la autorización del cliente, parámetros y certificados, se manda a través del canal TLS establecido anteriormente, de manera que solo pueden haber sido enviados por parte del cliente con el que se ha iniciado el proceso de conexión.

Dicha estructura PKCS#7 contiene el certificado del cliente con el que se ha realizado la firma para que el servidor pueda verificar que la firma es correcta. En el mensaje mediante el cual el servidor le pide al cliente sus parámetros de conexión, se incluye un identificador de 4 octetos aleatorio, que posteriormente se utilizará para derivar la clave WEP junto con la dirección MAC del punto de acceso y la clave maestra de la conexión TLS anteriormente establecida.

- *Distribución de la clave*

En esta fase del protocolo únicamente participan el punto de acceso y el servidor de autenticación, y consiste en que éste último le pase al primero un descriptor de la clave WEP que debe utilizar con el cliente, así como el tipo de servicio que el cliente espera que se le ofrezca. Esta clave WEP la habrá generado el servidor como resultado de una función de resumen digital MD5 aplicada sobre la concatenación de la clave maestra generada por EAPTLS, la dirección MAC del punto de acceso, y la carga *nonce* comentada anteriormente. Por su parte, el punto de acceso debe comprobar que en su situación actual puede soportar las necesidades del nuevo cliente, es decir debe comprobar que la suma total del ancho de banda necesitado por todos los usuarios que actualmente hay conectados, junto con el requerido por el nuevo cliente, no sobrepase su capacidad; y que vaya a estar disponible el tiempo que el cliente requiere; informando al servidor de autenticación sobre la decisión que tome. Tras estas fases, el proceso de conexión ha terminado, si todo se ha realizado correctamente, el servidor de autenticación notifica al punto de acceso la autorización por su parte a que el cliente haga uso de la red. El punto de acceso traslada entonces al cliente esta decisión para que inicie la comunicación. El cliente, que habrá generado la misma clave WEP que obtuvo

el punto de acceso, puede comenzar a hacer uso de la red, con la garantía de que sus mensajes son sólo descifrables por el punto de acceso, dado que la clave WEP generada es distinta para cada usuario.

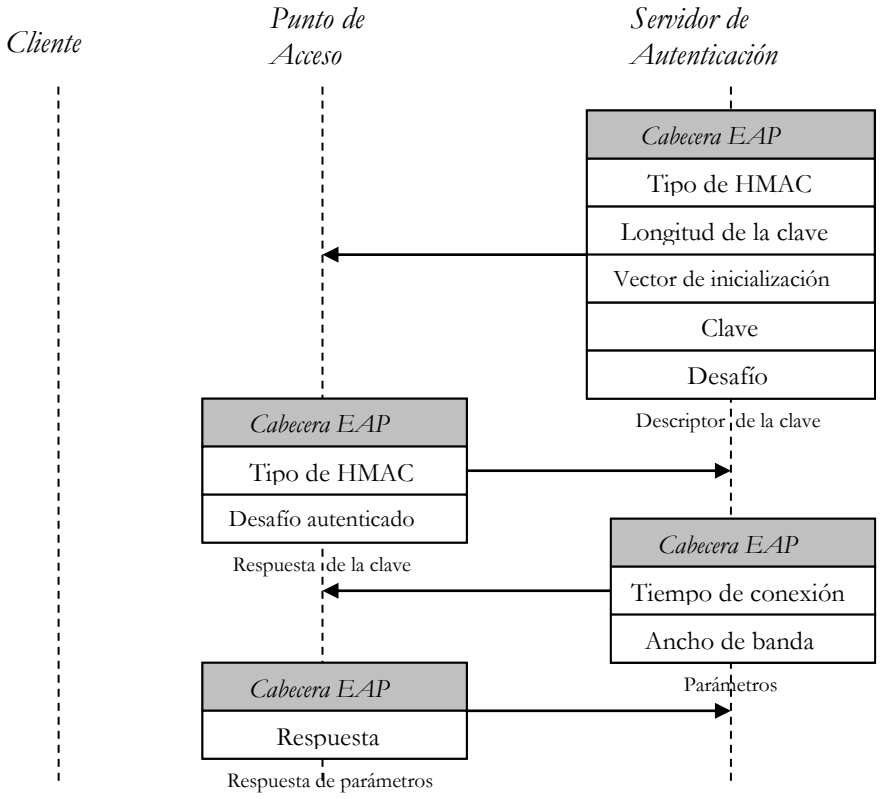


Figura 4.9 Proceso de distribución

Periódicamente, y dependiendo de esta periodicidad del nivel de seguridad que quiera el usuario, es posible renegociar la clave WEP que se está utilizando para cifrar la comunicación entre el cliente y el punto de acceso. Para ello, el cliente inicia un proceso de renegociación de conexión TLS. En esta ocasión, no será necesario que el cliente mande sus parámetros, a no ser que quiera cambiarlos, sino que únicamente se realiza esta fase para indicar al cliente cual es la nueva cadena

aleatoria para generar la clave WEP. De esta manera al terminar el nuevo proceso de conexión, tanto el punto de acceso como el cliente tendrán la nueva clave WEP a utilizar para cifrar sus comunicaciones.

Cuando un cliente detecta que está en el área de cobertura de un nuevo punto de acceso, en lugar de iniciar el proceso de conexión descrito desde el principio, inicia un proceso de renegociación de conexión TLS. Al basarse la nueva conexión en la anterior, la generación del secreto compartido se puede realizar de forma más ligera, y además se evita que el servidor de autenticación tenga que validar de nuevo al usuario. Una consecuencia directa es también que de forma automática se inicia la fase de renegociación de clave WEP, lo cual implica un cambio de la misma para trabajar con el nuevo punto de acceso.

IMPLEMENTACIÓN DE UNA SUBRED INALÁMBRICA SEGURA PARA EL INSTITUTO DE INVESTIGACIONES DE MATEMATICAS APLICADAS Y EN SISTEMAS DE LA UNAM.

Dadas las necesidades expuestas al inicio de esta investigación, causadas por la insuficiencia tanto de direcciones IP homologadas como de nodos en algunas áreas del instituto. Ha surgido la necesidad de implementar una subred inalámbrica que sirva de apoyo a la red cableada y satisfaga las necesidades de los usuarios. Tal es el caso del edificio anexo del IIMAS en donde se encuentra ubicada la Biblioteca y en donde se imparte la docencia para los Posgrados en Ciencias Matemáticas o de la Especialización en Estadística Aplicada y Ciencia e Ingeniería de la Computación. Sin embargo como ya hemos analizado a lo largo de esta investigación es de suma importancia considerar los mecanismos de seguridad a implementar y de esta manera no debilitar la infraestructura de red de todo el instituto.

El edificio anexo esta conformado por tres pisos. En el primero se encuentra la Biblioteca, en el segundo se encuentra el Posgrado en Ciencias Matemáticas o de la Especialización en Estadística Aplicada y en el tercero el Posgrado en Ciencia e Ingeniería de la Computación. Como podemos observar son tres áreas con perfiles de usuarios diferentes y por lo tanto con diversas necesidades.

En primer lugar tenemos la Biblioteca, en esta área los usuarios necesitan tener acceso a la información que Internet les proporciona. Para esto hay que tener en

cuenta las siguientes consideraciones; para poder definir que equipo cumple con los mejores mecanismos de seguridad para implementar la subred.

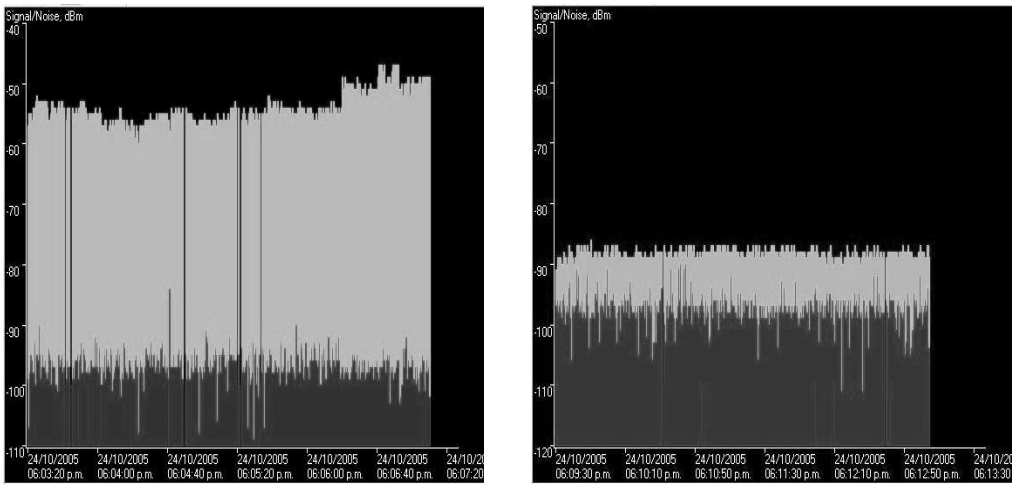
- Es un espacio público al que cualquier persona puede tener acceso y hacer uso del servicio.
- Cada usuario es propietario de su equipo, por lo que no es posible y factible la administración y configuración del mismo. Lo cual también implicaría perder demasiado tiempo que se puede aprovechar en otras actividades.
- Es de vital importancia evitar que cualquier usuario pueda tener una conexión directa con algún equipo que se encuentre dentro del instituto, sea este una computadora personal, una impresora, un servidor, etc.

De acuerdo a lo anterior y después de investigar las funciones que ofrecen algunos equipos en el mercado, se llego a la conclusión que el mejor equipo para satisfacer estos puntos es el ruteador inalámbrico WRT54G de la marca Linksys.

Este ruteador maneja los estándares 802.11b/g de 11Mbps y 54 Mbps, nos da la posibilidad de crear una subred inalámbrica a través de un servidor dinámico de direcciones IP (DHCP) y cuenta con un *firewall* que nos permite bloquear algunos puertos de acceso a ciertos protocolos considerados como vulnerables.

Una vez que se cuenta ya con el dispositivo que se va a implementar. Ahora es necesario seleccionar el punto estratégico en donde se va a colocar para poder obtener el mejor rendimiento.

Para esta tarea fue necesario realizar una caminata a lo largo de toda el área y perímetro de la biblioteca, algunos autores definen esta actividad con el nombre de *Warchalking*. Esta actividad requiere de una computadora portátil (*laptop*), una tarjeta de red inalámbrica que soporte los estándares 802.11b/g y la ejecución del software de monitoreo (*netstumbler*) que nos permitió verificar la intensidad de la señal en cada espacio del área en cuestión y así poder determinar los puntos donde hay buena señal o donde la señal es baja en intensidad como lo muestra la siguiente figura.



Intensidad de señal buena Intensidad de señal baja

Fig 4.10 Intensidad de señales con netstumbler.

Después de realizar esta caminata, se determino que el mejor lugar para colocar el dispositivo es el "primer nivel de la Biblioteca" como se muestra en la siguiente figura.

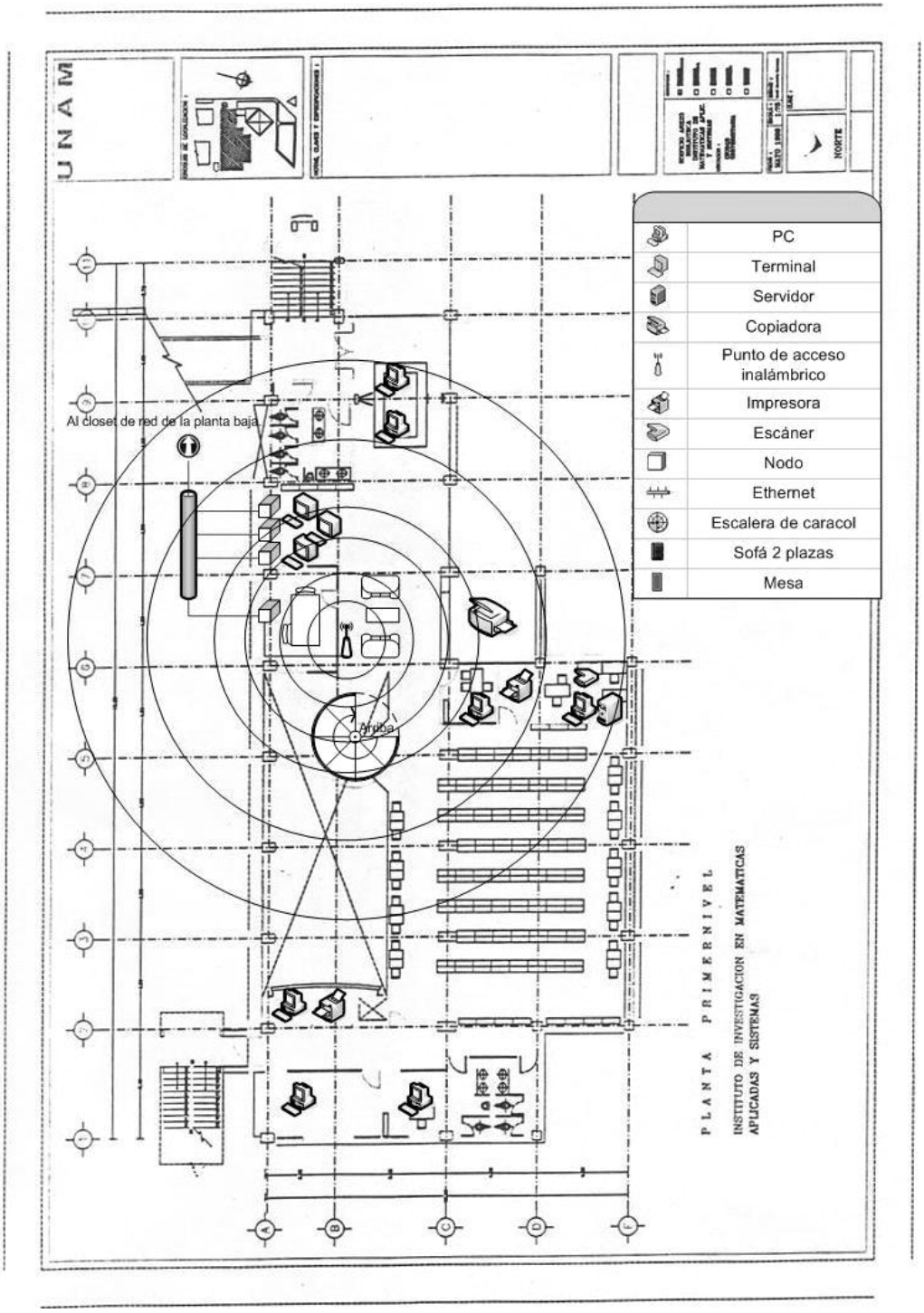


Fig 4.11 Colocación del ruteador inalámbrico en la Biblioteca.

Como podemos observar en la figura, el ruteador se encuentra en un sitio en donde su cobertura alcanza toda el área de la biblioteca en sus dos niveles.

Una vez colocado el ruteador inalámbrico, es necesario pasar a la parte de configuración de las opciones que nos interesan. Primero la creación de una subred mediante el servidor de DHCP

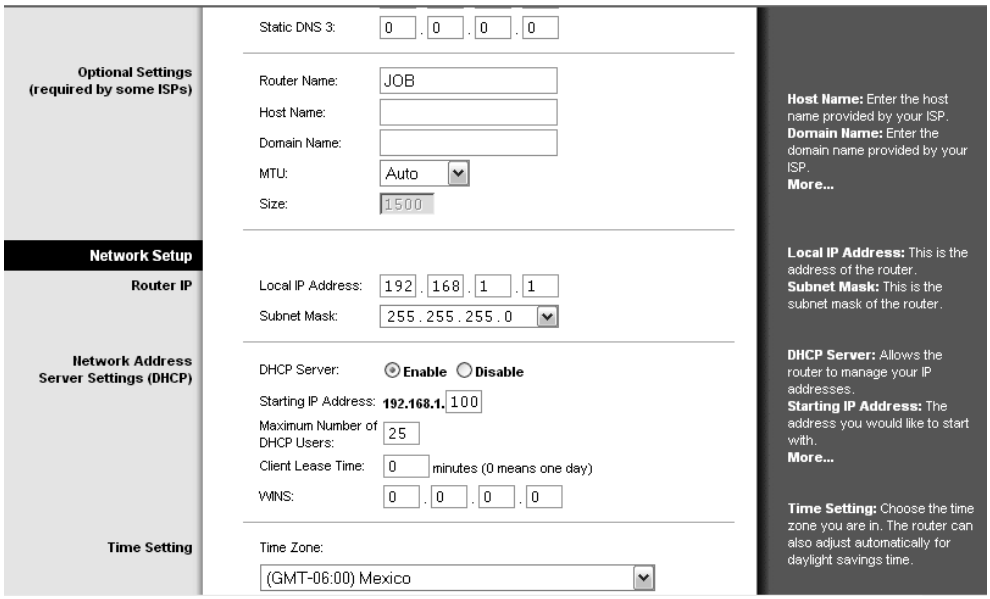


Fig. 4.12 Servidor DHCP de ruteador inalámbrico

Para este caso fue necesario crear una subred que empezara con la siguiente *dirección IP 192.168.1.100* para posteriormente determinar el número máximo de usuarios para este servicio. En este caso el número de usuarios fue de 25, como resultado de un sondeo que nos permitió observar que los usuarios que utilizaban sus equipos portátiles en esta área no excedían de 10; razón por la cual se asigno este valor. Sin embargo este valor puede variar según las necesidades que se presenten en un futuro. En la actualidad prácticamente todos los equipos portátiles

y algunos otros dispositivos que se ofrecen en el mercado, cuentan con una tarjeta de red inalámbrica en su *hardware*.

Ahora es necesaria la configuración de políticas de acceso del *firewall* para bloquear ciertas conexiones como se muestra en la siguiente figura.

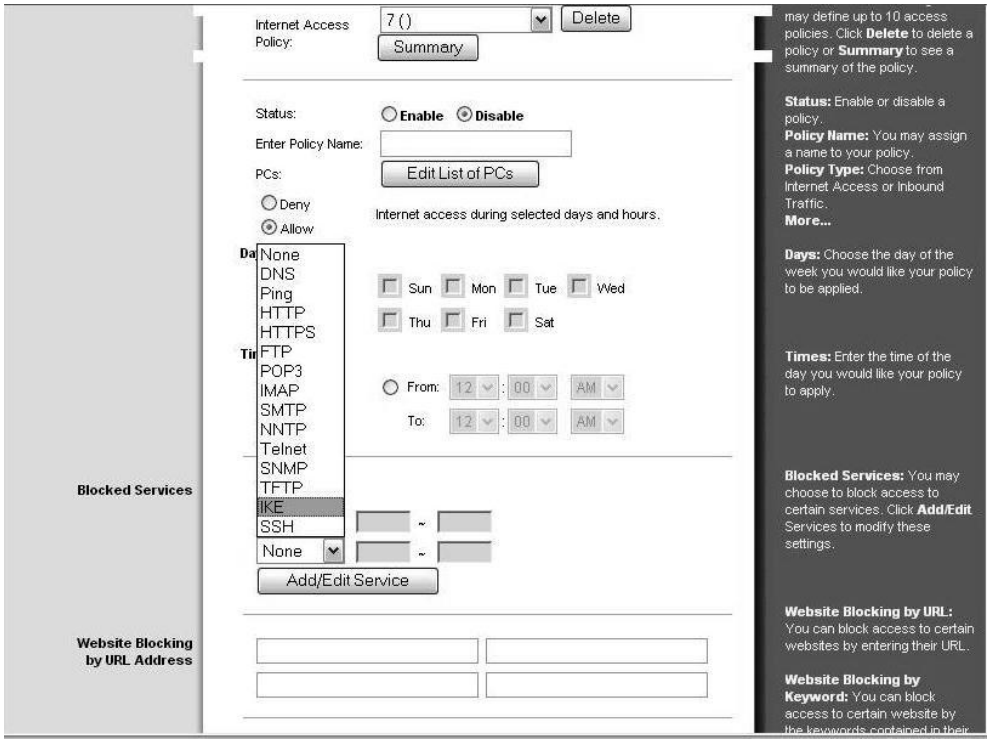


Fig. 4.13 Políticas de acceso de ruteador inalámbrico

Como se puede observar hay una extensa lista de protocolos administrables, tales como SSH, Ping, Telnet, FTP, entre algunos otros; de esta manera podemos seleccionar los servicios que requerimos para tener una subred inalámbrica con la posibilidad de que ningún equipo en esta área que este utilizando dicha subred pueda conectarse directamente por alguno de estos protocolos a un equipo dentro

del Instituto y mantener segura la información que circula a través de la red cableada del mismo.

La siguiente área en donde se requiere el acceso inalámbrico es el Posgrado en Ciencias Matemáticas o de la Especialización en Estadística Aplicada. Los usuarios de esta área constantemente hacen latente su necesidad de conectarse con sus equipos portátiles a Internet. Sin embargo no requieren de una conexión directa con algún servidor o un equipo en específico. Razón por la cuál se determino que la mejor opción para la implementación de una subred inalámbrica en esta zona, es la instalación de un repetidor inalámbrico que sea una extensión de la subred implementada en la biblioteca. Dicho repetidor tiene que ser del mismo fabricante que el que va a emitir la señal para poder realizar una conexión con éste. En este caso se tiene un WAP54G de Linksys, el cuál es un punto de acceso que nos permite configurarlo como un repetidor.

La instalación de un repetidor se puede realizar con un proceso similar al caso anterior (W*archalking*). Para esto es necesario verificar la intensidad de la señal fuente o emitida, que para este caso va ser la señal que emita el ruteador inalámbrico instalado en la Biblioteca y una vez detectado el lugar donde la señal es baja pero todavía alcanza a ser detectada por la tarjeta de red inalámbrica. Se coloca el repetidor en este sitio y se configura en el mismo canal que transmite la señal fuente con el modo de operación como repetidor como lo muestra la siguiente figura.

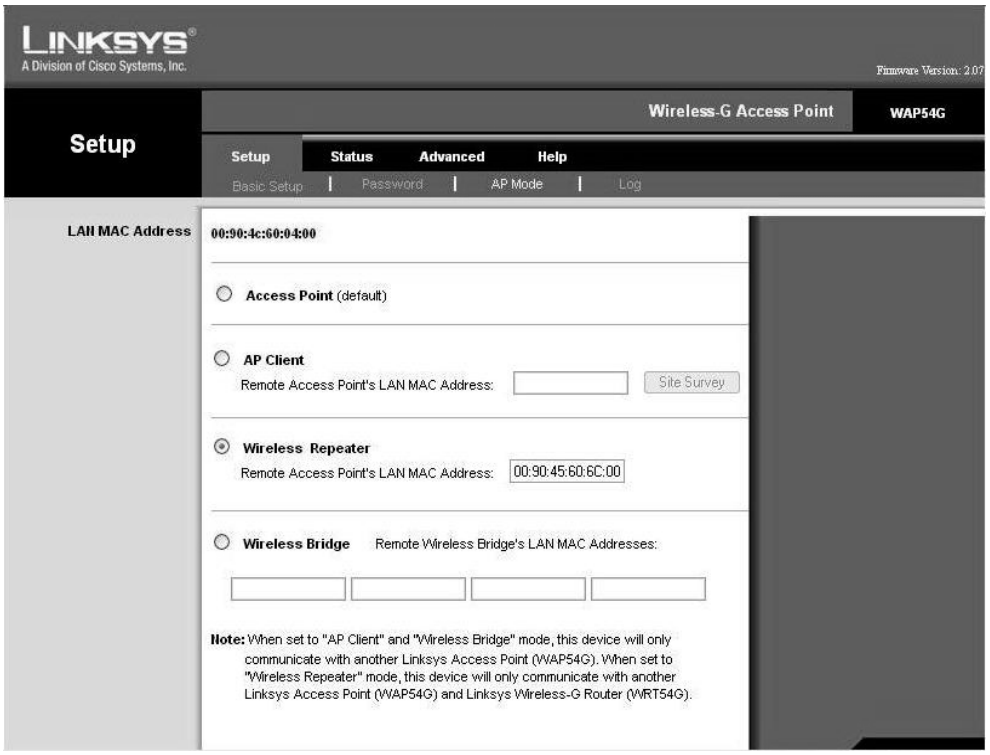


Fig 4.15 Configuración de un AP como repetidor

Como podemos observar en la figura para poder conectar un repetidor inalámbrico es necesario conocer la dirección MAC o física del dispositivo que emite la señal. Esta dirección dentro del *firmware* de cualquier punto de acceso o ruteador inalámbrico se conoce como *LAN MAC Address* y es necesaria conocerla antes de configurar un repetidor.

De esta manera el repetidor respetara las mismas reglas o políticas de acceso de la señal fuente y no necesita la conexión de algún cable *ethernet* a su puerto correspondiente. En la siguiente figura podemos observar la colocación del repetidor que cubre el área del segundo piso resaltando el hecho que no es necesario la conexión directa a la red cableada del área en cuestión.

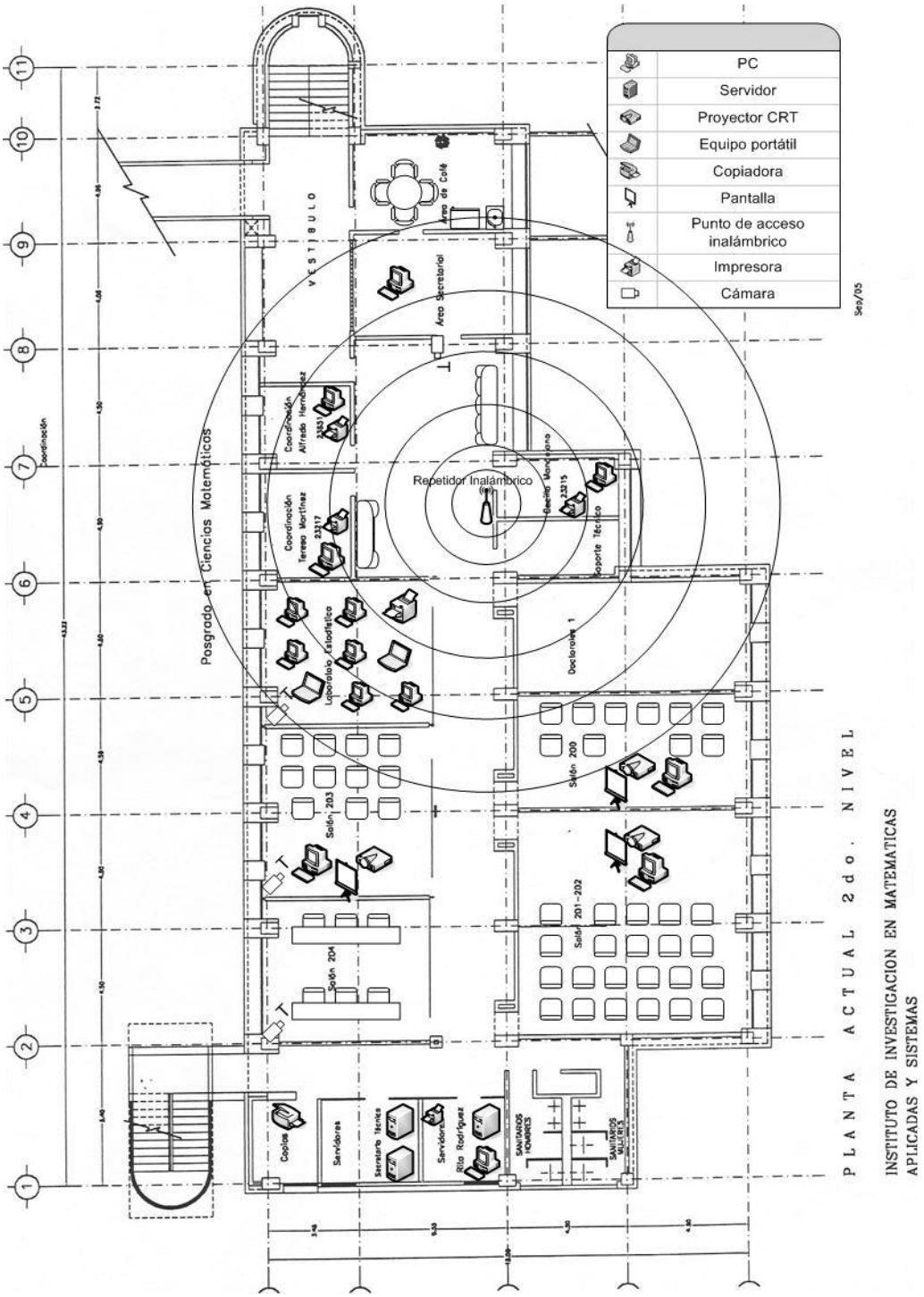


Fig 4.15 Colocación del repetidor inalámbrico.

En tercer lugar tenemos el Posgrado en Ciencias e Ingeniería en Computación.

Para la implementación de un subred en este sitio es necesario analizar el perfil de los usuarios que van a tener acceso a dicha subred. Como hemos mencionado anteriormente los mecanismos de seguridad van a estar de acuerdo con el tipo de necesidades y usuarios que presenta el área. Los usuarios en esta área tienen los conocimientos suficientes tanto para poner en riesgo la seguridad de la información como para que sus necesidades sean mayores a simplemente el acceso a Internet como por ejemplo la conexión a servidores para la transferencia de archivos, el uso de bases de datos, etc. Razones por las cuales tenemos que considerar otras alternativas de solución diferentes a las anteriores sin poner en riesgo la seguridad de la información que circula a través de la red cableada del Instituto.

La propuesta para este sitio es la instalación de un servidor RADIUS (802.1x) para la autenticación de usuarios que permita o deniegue el acceso a la subred inalámbrica. Este servidor puede ser montado en el sistema operativo LINUX[1] o en Windows[2] en sus versiones de servidor 2000 o 2003. En LINUX es importante resaltar que después de hacer varias pruebas en distintas distribuciones tales como Red Hat, Mandrake, Fedora, etc. Se encontró que la más estable es la distribución Debian. En el caso de Windows es importante considerar la instalación de un *firewall* por *software* o *hardware* que evite tanto la infección de virus informático como la intrusión de *hackers*, además de realizar todas las actualizaciones correspondientes como hemos mencionado en capítulos anteriores para poder mantener una estación segura.

[1] En Linux el servicio se conoce como *freeRADIUS*
[2] En Windows el servicio se conoce con el nombre IAS (*Internet Access Service*)

Una vez instalado y configurado el servidor RADIUS (802.1x) al igual que el ruteador inalámbrico. Cada vez que el usuario quiera realizar una conexión para utilizar la subred inalámbrica aparecerá una ventana como la siguiente, en la que se le solicita su cuenta y contraseña.



Fig. 4.16 Ventana de autenticación de subred inalámbrica.

La colocación mas adecuada del ruteador inalámbrico y del servidor RADIUS (802.1x), considerando las técnicas anteriores de monitoreo se muestra en la siguiente figura.

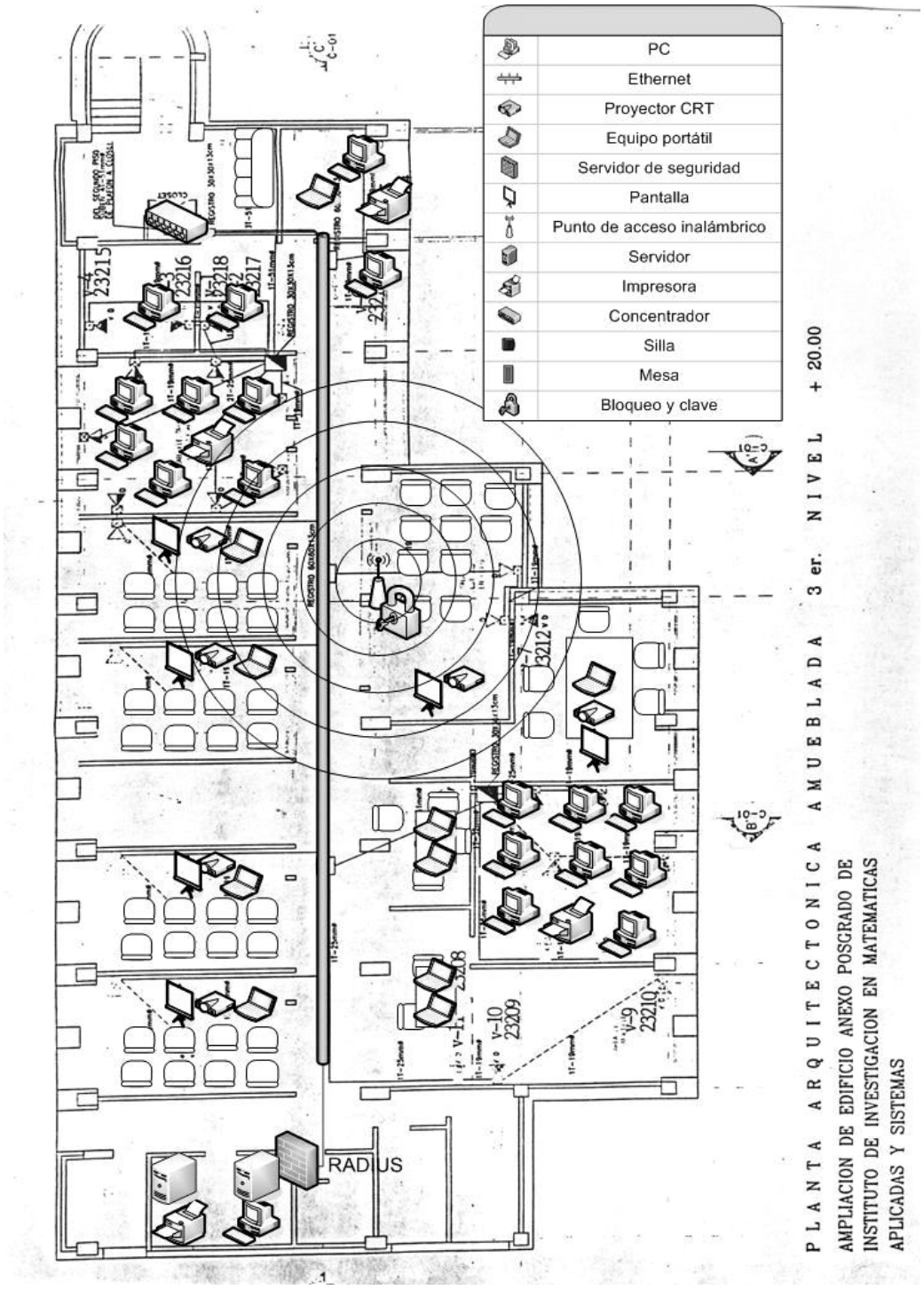


Fig. 4.17 Colocación del ruteador inalámbrico y del servidor RADIUS para el PCIC.

El servidor se encuentra en un espacio con acceso restringido como se puede observar en la figura.

Por ultimo existe otra área dentro del Instituto que presenta la misma problemática. Tal es el caso del segundo piso del edificio principal del instituto en donde se encuentra el departamento de Modelación Matemática de Sistemas Sociales. En este piso podemos encontrar varias circunstancias que nos invitarían a la implementación de una subred inalámbrica entre las que resaltamos las siguientes:

- Hay varias oficinas con dos o más usuarios con un solo nodo.
- Hay usuarios con más de un equipo de cómputo que necesita el acceso a la red.
- Hay espacios reservados para investigadores visitantes que también requieren acceso a este servicio.
- Muchas de las direcciones IP homologadas que requieren todos estos equipos pueden desocuparse y emplearlas en otra área con mayor necesidad.
- Muchos usuarios comparten sus impresoras en la red, poniendo en riesgo su información.

De esta manera y dadas todas estas circunstancias. El tendido de nuevos cables a lo largo de las canaletas cada vez que se requieran o la colocación de concentradores de manera aleatoria e irresponsable que reducen el rendimiento de la red son suficientes razones para implementar una subred inalámbrica. Sin embargo los usuarios deben tener la entera confianza de que su información se mantenga segura y alejada de posibles *hackers*.

Para realizar esta implementación es necesario un ruteador inalámbrico que nos permita la posibilidad de crear una subred, como ya lo observamos anteriormente y un servidor de RADIUS (802.1x) de autenticación para comprobar la conexión legitima de los usuarios de este piso.

La tecnología inalámbrica ofrece algunas otras alternativas como la implementación de un servidor de impresión, que en este caso en particular seria de mucha utilidad y de esta manera evitar que algunos usuarios tengan que compartir sus equipos en red para realizar impresiones.

La colocación del ruteador inalámbrico y el servidor RADIUS (802.1x) se puede observar en la siguiente figura.

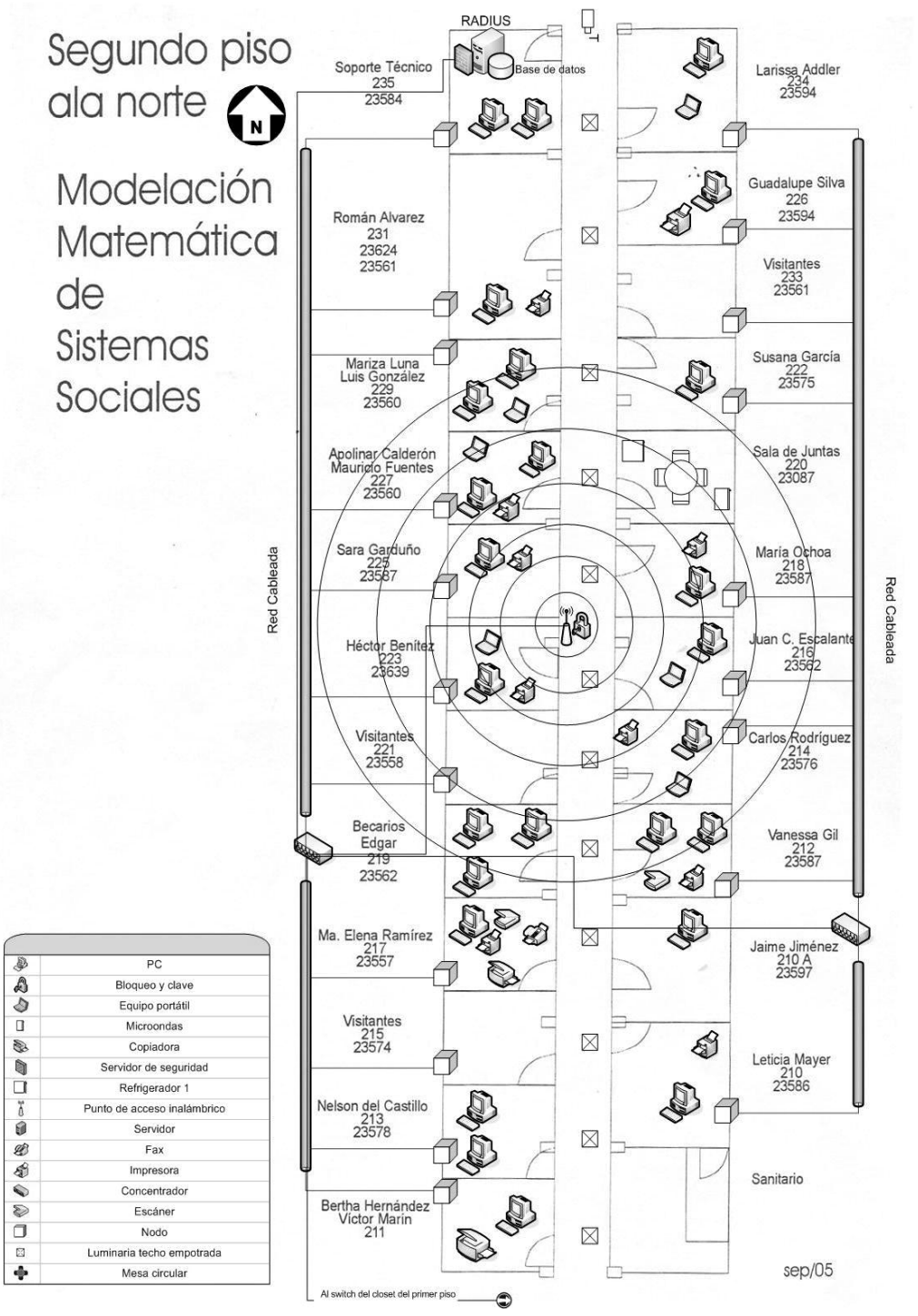


Fig 4.18 Colocación del ruteador inalámbrico y de servidor RADIUS para MMSS

CONCLUSIONES

El uso de las redes inalámbricas ha aumentado considerablemente en los últimos años. En la actualidad muchas instituciones educativas, gubernamentales, empresas privadas, comercios y restaurantes proporcionan los servicios de conexión a Internet y correo electrónico a través de un enlace inalámbrico. Sin embargo esa popularidad trae sus consecuencias ya que entre mas común se vuelva el uso de una red inalámbrica mas factible va hacer el desarrollo de herramientas por parte de *hackers* que exploten sus vulnerabilidades.

Como hemos podido observar a lo largo de este documento existe una gran diversidad de métodos o técnicas que ponen en riesgo la seguridad de la información que se transmite a través de una red inalámbrica. Sin embargo encontramos y analizamos mecanismos de seguridad que contrarresten dichas técnicas y las aplicamos a la problemática del IIMAS, la cuál se plantea en el capitulo anterior.

Por lo tanto concluimos que la solución a estas necesidades, con sus respectivas problemáticas, fue la implementación de mecanismos de seguridad que complementan los ya existentes en esta tecnología, como es el caso de los servidores de autenticación, la instalación y configuración de *firewalls,* la administración y monitoreo constante de la subred inalámbrica para detectar intrusos, con lo cual se corrigieron las anomalías planteadas.

Las subredes inalámbricas implementadas en las áreas requeridas del Instituto ofrecen un excelente rendimiento y desempeño de los equipos instalados, satisfaciendo las necesidades de los usuarios, con la confianza de que tanto la información como la infraestructura de la red cableada del Instituto se encuentran seguras.

De esta manera la medida para mantener los canales seguros en una subred inalámbrica para un ambiente académico va a depender del tipo de necesidades del área donde se requiera implementar y del perfil de los usuarios que la van a utilizar.

Considerando todos estos puntos las redes inalámbricas son una alternativa eficaz y de bajo costo para esos metros, en donde el diseño, estructuración y mantenimiento de un cableado estructurado resultaría una opción más costosa para una institución o empresa.

Sin embargo es importante resaltar el hecho que dado el continuo avance de la tecnología. Actualmente muchas de las soluciones planteadas en este documento para contrarrestar los puntos vulnerables de las redes inalámbricas, algunas de éstas ya se incluyen o están por incluirse en un futuro próximo en el *hardware* de algunos dispositivos que proporcionan este tipo de servicio. Como por ejemplo la creación de redes privadas virtuales, la integración de un servidor RADIUS, la creación de nuevos estándares (802.11i) o la implementación de *software* o *hardware* especifico para el monitoreo y administración de redes inalámbricas. Aspectos que al inicio de esta investigación no se contaba con ellos y que dado el auge que las redes inalámbricas han tenido y la necesidad de tener acceso a la información en cualquier lugar en que nos encontremos, se han venido desarrollando rápidamente.

Apéndice A

Formato de las tramas MAC

Las tramas MAC contienen los siguientes componentes básicos:

- Una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia

- Un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama

- Una secuencia *checksum* FCS (*Frame Check Sequence*) que contiene un código de redundancia CRC (*Cyclic Redundancy Check*) de 32bits.

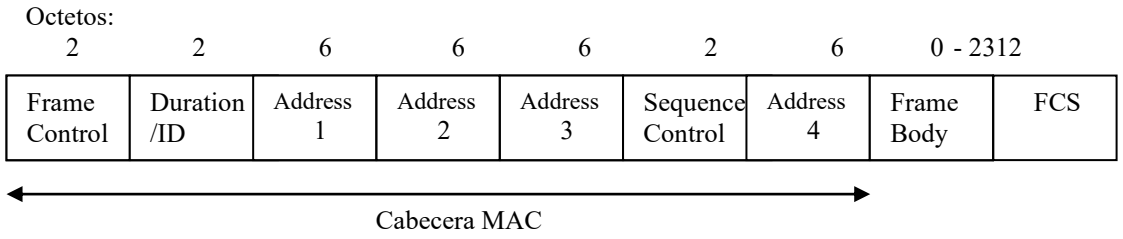
Las tramas MAC se pueden clasificar según tres tipos:

- Tramas de datos: Su propósito es transportar información MSDU a la estación destino.

- Tramas de control. Después de iniciar los procesos de autentificación y asociación entre estaciones y puntos de acceso, las tramas de control proporcionan asistencia en la entrega de tramas de datos. Por ejemplo, los reconocimientos ACK, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda.

- Tramas de gestión. El propósito de este tipo de tramas es iniciar la comunicación entre estaciones y puntos de acceso. Y proporcionar servicios como autentificación, asociación, *Beacon* (tramas guía), etc.

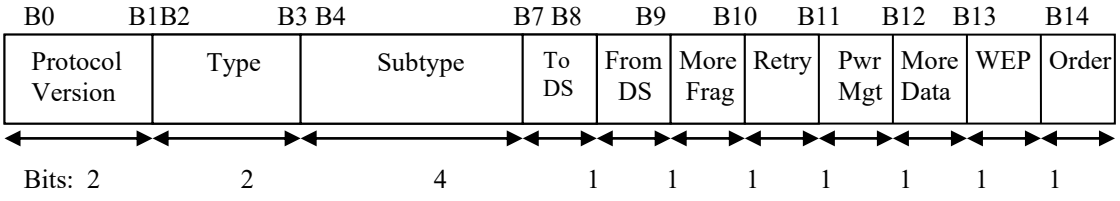
El formato de la trama MAC genérica tiene el siguiente aspecto:



Trama MAC

Los campos que componen esta trama son:

- *Frame control.* A su vez este campo de control de la trama tienen la siguiente estructura:



Trama de control

  - *Protocol Version*. Como su nombre lo indica hace referencia a la versión del protocolo según el estándar IEEE 802.11.
  - *Type.* Este campo identifica el tipo de trama: de datos, control o de gestión
  - *Subtype.* Este campo define la función de la trama: petición, respuesta de asociación, autentificación, desautentificación, RTS, CTS, ACK, *Beacon*, Data, etc.

- *ToDS/FromDS* (*Distribution System*). Identifica si la trama se envía o se recibe al sistema de distribución o punto de acceso. En redes ad-hoc, tanto ToDS como FromDS están en "0" El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución, para ello se tiene en "1" tanto ToDS como FromDS.
- *More fragments*. Este campo identifica si un fragmento de una misma trama MSDU continúa en la siguiente trama.
- *Retry*. Se activa si la trama es una retransmisión.
- *Power Management*. Se activa si la estación utiliza el modo de economía de potencia.
- *More Data*. Se activa si la estación tiene tramas pendientes en un punto de acceso.
- *WEP*. Se activa si se usa el mecanismo de autentificación y encriptado.
- *Order*. Se utiliza con el servicio de ordenamiento estricto para indicar que la trama se está enviando.

- *Duration/ID*. Este campo contiene un valor de duración de transmisión de trama y es necesario para implementar el mecanismo virtual de detección de portadora.

- Los Campos *Address1-4* contienen direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la estación que recibe y el punto de acceso.

- El campo *Sequence Control* (control de secuencia) contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.

- *Frame Body*. El cuerpo de la trama varía según el tipo de trama que se quiere enviar. En este campo, las tramas de gestión se indican en el parámetro SSID (*Service Set Identifier*) a la que pertenece cada punto de acceso.

- El campo FCS contiene el *checksum*.

Apéndice B

Cálculo del CRC.

Supongamos que tenemos la siguiente secuencia de datos *D=101110* lista para ser enviada, con un polinomio generador *G=1001* y con *r* (bits de comprobación)=*3*.

- El primer paso es calcular 2^r.

$2^r=2^3=8$ que en binario es *1000*.

- El segundo paso es realizar el producto entre la secuencia de datos y el resultado anterior ($D\cdot 2^r$).

$$
\begin{array}{rl}
 & 101110 \\
D\cdot 2^r = & \underline{X\ 1000} \\
 & 000000 \\
 & 000000 \\
 & 000000 \\
 & \underline{101110} \\
 & 101110000.
\end{array}
$$

- El tercer paso es dividir el resultado anterior entre el polinomio generador *G*.

$$
\begin{array}{r}
\quad 101011 \\
1001\ /\ 101110000 \\
\underline{1001} \\
101 \\
\underline{000} \\
1010 \\
\underline{1001} \\
110 \\
\underline{000} \\
1100
\end{array}
$$

```
 1001
  1010
  1001
   011 = Residuo
```

Esto implica que los datos a enviar van a ser *D* + *Residuo* = *101110 011*.

El receptor para verificar que los datos enviados son correctos divide los datos recibidos (*101110011*) entre el polinomio generador *G*, si el residuo es igual a cero, los datos son correctos, en caso contrario existirá un error y el dato tendrá que ser retransmitido.

```
      101011
1001 / 101110011
     1001
      101
      000
      1010
      1001
       110
       000
       1101
       1001
        1001
        1001
        0000 = Residuo
```

Por lo tanto los datos recibidos son correctos.

Se tienen definidos estándares internacionales para polinomios generadores de 8,12,16 y 32 bits. En este caso los protocolos de la IEEE adoptaron el polinomio de 32 bits, el cuál tiene la siguiente secuencia[1]:

[1] Computer Networking, Kurose, James, Addison Wesley, USA 2002

$$G_{CRC-32} = 100000100110000010001110110110111.$$

$$G_{CRC-32} = x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{5}+x^{4}+x^{2}+x^{1}+x^{0}$$

A p é n d i c e C

Trama del paquete RADIUS

La RFC (*Request For Comments*) especifica que RADIUS utiliza una estructura de paquete como la siguiente.

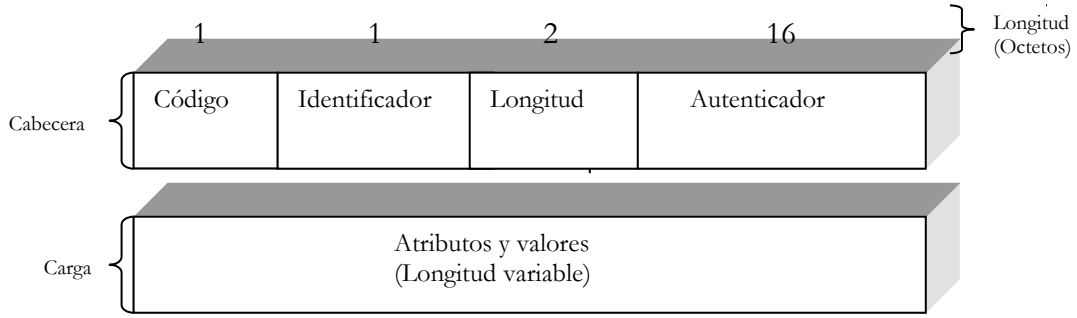


Figura 4.1 Trama RADIUS

- *Código*: El campo de código tiene una longitud de un octeto e identifica el tipo de paquete de RADIUS. Cuando un servidor recibe un paquete con un campo de código no valido, lo ignora sin ningún tipo de notificación adicional. El servidor RADIUS identifica los tipos de mensaje de acuerdo con el campo código de paquete. La siguiente tabla muestra la descripción de estos códigos.

Código RADIUS	*Descripción*
1	**Petición de acceso**
2	**Aceptación de acceso**
3	**Rechazo de acceso**
4	**Petición de contabilidad**
5	**Respuesta de contabilidad**
11	**Desafió de acceso**
12	**Estado del servidor (experimental)**

13	**Estado del cliente (experimental)**
255	**Reservado**

Tabla 4.2 Tipos de mensaje

- *Identificador*: Es un valor de un octeto que permite al cliente comparar una respuesta con la petición pendiente.

- *Longitud*: Este campo ocupa dos octetos e indica la longitud del mensaje y representa la correspondiente suma de los campos código, identificador, longitud, autentificador y atributo.

- *Autenticador*. Este valor tiene una longitud de 16 octetos y se utiliza para autentificar y verificar la respuesta procedente del servidor RADIUS. También se utiliza como mecanismo para ocultar contraseñas. Los dos tipos de valor son los autenticadores de petición y respuesta. El primer tipo es un valor aleatorio y único usado con los paquetes de petición de acceso y contabilidad. El segundo tipo se usa en los paquetes de aceptación de acceso, rechazo de acceso o desafió de acceso y contiene un valor *hash* MD5 (*Message Digest Algorithm* 5), calculado a partir de una cadena de valores que consiste en los campos código, identificador, longitud y autenticador de petición además de los atributos de respuesta, seguidos por la clave compartida.

- *Atributos*: Este campo clasifica las características del servicio, anunciando el tipo de servicio ofrecido o solicitado. La siguiente tabla muestra los seis tipos de atributos y sus posibles valores.

Valor del atributo	**Longitud en octetos**	**Tamaño (en Bits)**	**Ejemplos**
INT (Entero)	4	32	256, 65536
ENUM (Enumerado)	4	32	1= nombre de usuario 2= contraseña de usuario 13= compresión de marco 26= especifico del fabricante
STRING (Cadena)	1-253	Variable	"Cualquier cadena" "192.168.111.111" "www.arhoton.com"
IPADDR (Dirección IP)	4	32	0xFFFFFF 0x00000A
DATE (Fecha)	4	32	0xFFFFFF 0x00000A
BINARY(Binario)	1	1	0

Tabla 4.1 Atributos

Apéndice D

Trama del protocolo IPSec.

IPSec está compuesto por:

- Protocolo de autenticación *Authentication Header* (AH).
- Protocolo de encriptación *Encapsulating Security Payload* (ESP).
  Ambos son protocolos de seguridad de tráfico.
- Protocolo y procedimiento para el manejo de llaves encriptadas. *Internet Key Exchange* IKE que permite a dos estaciones negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

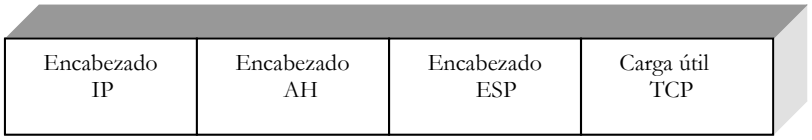


Figura 4.3 Trama IPSec

IPSec fue diseñado por un grupo de la IETF (*Internet Engineering Task Force*). El objetivo de la creación de este protocolo era el desarrollo de un estándar único que proporcionara seguridad, interoperativa y flexibilidad para las redes IPv4 e IPv6

Tanto AH como ESP se basan en las asociaciones de seguridad SA (*Security Association*) que negocian las propiedades de una conexión segura usando IKE. Una asociación de seguridad contiene información negociada entre dos

participantes de la VPN. Entre esta información se incluyen las claves criptográficas y sus tiempos de vida, los algoritmos criptográficos utilizados, el protocolo IPSec y su modo de operación

Protocolo AH

Este protocolo garantiza la integridad y autenticación de los datagramas IP. Proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en su tránsito. Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.

El protocolo consiste en una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo.

A este protocolo el IANA le ha asignado el puerto 51. Esto significa que el campo "*Protocolo de la cabecera IP*" contiene el valor 51, en lugar de los valores 6 ó 17 que se asocian a TCP y UDP respectivamente. Es dentro de la cabecera AH donde se indica la naturaleza de los datos de la capa superior.

En la siguiente figura se ilustra el formato de la cabecera AH. Por encima de esta cabecera iría la cabecera IP. El autenticado del mensaje comprendería tanto la cabecera IP más la cabecera AH.

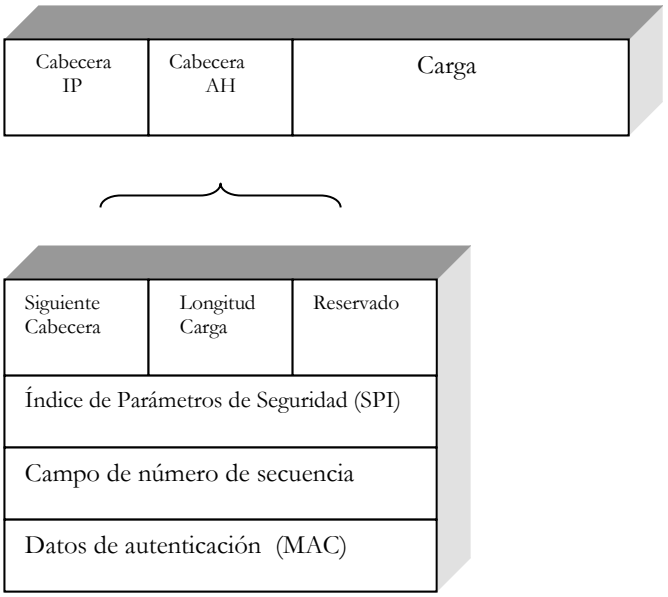


Figura 4.4 Cabecera AH

- El campo *Siguiente cabecera* de 8bits indica cual es el protocolo que se encuentra en el segmento de datos.

- El campo *Longitud de carga* de 8bits es la longitud de la cabecera.

- El campo *Reservado* es un campo que, como su nombre lo dice, está reservado para su uso futuro, debe estar puesto a cero para evitar que afecte al calculo de la autenticación.

- El campo SPI de 32bits que nos indica cuales son los parámetros de seguridad específicos a la SA que estamos utilizando.

- El *número de secuencia* de 32bits es el que tiene este datagrama en la SA.

- El campo MAC contiene la autentificación de la cabecera AH de la cabecera IP. Este campo tiene una longitud variable, que habitualmente suele ser de 96bits. Los datos pueden ser un segmento TCP o un datagrama UDP o IP.

El funcionamiento del protocolo AH se basa en un algoritmo HMAC (*Keyed-Hashing for Message Authentication*) que es un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función *hash* a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que se denomina extracto. Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

El emisor calcula un extracto del mensaje original, el cual se copia en uno de los campos de la cabecera AH. El paquete así construido se envía a través de la red, repitiéndose el cálculo del extracto en el extremo receptor y comparándolo con el recibido en el paquete. Si son iguales, el receptor tiene la seguridad de que el paquete IP no ha sido modificado en su tránsito y que procede efectivamente del origen esperado.

Esto permite afirmar que la seguridad de este protocolo reside en que el cálculo del extracto es imposible sin conocer la clave, y que dicha clave sólo la conocen el emisor y el receptor.

Protocolo ESP

Su función primordial es proporcionar confidencialidad. Para ello, el protocolo especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP.

El formato de la cabecera es más complejo. Consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP. Por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo.

En la siguiente figura se muestra la estructura de un datagrama ESP, en la que se observa cómo el contenido o carga útil viaja cifrado. Por encima de esta cabecera iría la cabecera IP.

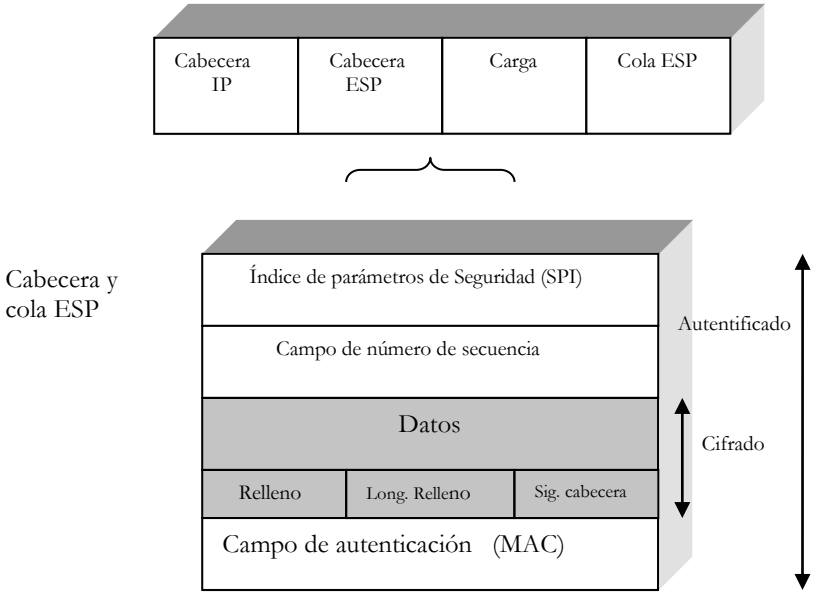


Figura 4.5 Cabecera ESP

- El campo SPI de 32bits indica cuales son los parámetros de seguridad específicos a la SA que estamos utilizando.

- El *número de secuencia* de 32bits que tiene este datagrama en la SA. Los datos pueden ser un segmento TCP o un datagrama UDP o IP.

- El campo de *relleno* tiene una longitud variable.

- El campo *longitud de relleno* indica cual es el tamaño del relleno en bytes.

- En el campo *Siguiente Cabecera* de 8bits se indica cual es el protocolo que se encuentra en el segmento de datos.

- El campo MAC contiene la autenticación de la cabecera ESP. El IANA le ha asignado el número de identificación de protocolo 50. Por lo tanto en el campo protocolo de la cabecera IP contendrá el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Este campo está cifrado, como la carga útil del resto del mensaje. El posible atacante que leyera el paquete no sabría si el contenido es TCP o UDP, circunstancia que es favorable si tratamos de ocultar la información.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8bytes o 16bytes, en la mayoría de los casos).

Por esta razón existe un campo de relleno, tal como se observa en la *figura 4.5*, el cual tiene una función adicional; es posible añadir caracteres de relleno al campo de datos para ocultar así su longitud real y por lo tanto las características del tráfico. Un usuario mal intencionado suficientemente hábil podría deducir cierta información a partir del análisis de ciertos parámetros de las comunicaciones, aunque estén cifradas, tales como el retardo entre paquetes y su longitud.

La función de relleno está pensada para dificultar este tipo de ataques. Para enviar los mensajes, el emisor toma el mensaje original, lo cifra utilizando una clave determinada y lo incluye en un paquete IP, a continuación de la cabecera ESP.

Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits confusos. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales.

La seguridad que se proporciona está en la robustez del algoritmo de cifrado, es decir, que un usuario malintencionado no puede descifrar los datos sin conocer la clave. La clave ESP únicamente la conocen el emisor y el receptor.

Protocolo IKE

Es un protocolo de control que se encarga de poner en contacto y negociar los algoritmos, claves y demás elementos para la comunicación segura con IPSec entre dos estaciones.

El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SA's correspondientes. La

utilidad del protocolo IKE no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos. El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec.

Dicha negociación se lleva a cabo en dos fases:

- Establecimiento de un canal seguro y autentificado: Esta fase es común a cualquier aplicación. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de las estaciones, para ello es necesario un paso adicional de autenticación.

- Negociación de los parámetros de seguridad específicos de IPSec a través del canal seguro: Durante esta fase se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambas estaciones se informan del tráfico que van a intercambiarse a través de dicha conexión.

GLOSARIO

A

ACK (*Acknowledgement*). Es un mensaje de confirmación de la estación receptora si la transmisión fue correcta.

Access Point. (*Punto de Acceso*). Un dispositivo de conectividad que comunica redes cableadas e inalámbricas y que controla los parámetros de red de las redes WLAN.

AES. (*Advanced Encription Standard*) También conocido como Rijindael. Es un esquema de cifrado por bloque adoptado como un estandar de encriptación, el cuál tiene un tamaño de bloque fijo de 128bits, con llaves de 128, 192 o 256bits respectivamente.

Algoritmo. Es un conjunto explícito de instrucciones que tienen definido un comienzo y un punto final. Es decir un procedimiento a seguir para llegar a un objetivo.

B

Backbone. Es el sistema principal de una red, llámese red primaria o principal.

Bit. Es la unidad de información más pequeña. Puede tener solo dos valores o estados (0 o1).

Beacon Frames. Señal emitida que ayuda a los clientes de una red inalámbrica a detectar puntos de acceso cercanos.

Blowfish. Algoritmo de criptografía diseñado por Bruce Schneier en 1993 de dominio publico para utilizarse libremente por cualquier persona.

Bridge. (*Puente*) Dispositivo que posibilita la conexión entre redes físicas cableadas e inalámbricas. Hace posible la conexión entre dos o más LANs

Broadcast. Difusión de información a múltiples estaciones o receptores simultáneamente.

C

CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*). Un protocolo de contención de la capa 2 utilizado en las redes inalámbricas compatibles con 802.11 y que utiliza respuestas ACK positivas para los marcos transmitidos, para evitar las colisiones en las redes.

CHAP. (*Challenge Handshake Autentication Protocol*) Método de autentificación en el cual el NAS genera un valor aleatorio y lo envía al usuario quien regresa un CHAP por respuesta con un identificador y con el nombre de usuario. EL NAS entonces envía un paquete de petición de acceso al servidor RADIUS con el nombre de usuario como Usuario y el identificador como la Contraseña.

Checksum. Suma de comprobación de verificación. Valor total de los dígitos o bits, que sirve para fines de comprobación.

CRC. (*Ciclyc Redundance Code*) Un valor de comprobación matemático básico utilizado para detectar violaciones de integridad de los datos transmitidos. Suele calcularse dividiendo la longitud del marco mediante un número primo y los atacantes pueden falsificarlo con facilidad.

D

Diffie-Hellman. Fue el primer algoritmo asimétrico. Solamente se puede utilizar para intercambiar claves simétricas, pero esto es una de las principales funciones de

los algoritmos asimétricos. Es muy utilizado en sistemas de Internet con confidencialidad de clave simétrica (VPNs, SSL, etc.).

dB. (*Decibelio*) Unidad de medida de diferencias relativas de potencia en términos de ganancia o pérdida.

DHCP (*Dynamic Host Configuration Protocol*). Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadoras conectadas a la red informática que los requieran (máscara de subred, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP.

E

Encriptar. Codificación de datos, transformando de lenguaje claro en lenguaje cifrado, con el fin de proteger su carácter privado o secreto de manera que solamente puedan recibirlos las terminales que dispongan de los programas decodificadores apropiados.

Escalabilidad. Es la capacidad de un sistema informático de adaptarse a un número de usuarios cada vez mayor, sin perder calidad en los servicios. En general, se podría definir como la capacidad del sistema informático de cambiar su tamaño o configuración para adaptarse a las circunstancias cambiantes. Por ejemplo, una empresa que establece una red de usuarios por Internet, no solamente quiere que su sistema informático tenga capacidad para acoger a los actuales clientes, sino también a los clientes que pueda tener en el futuro y, también, que pueda cambiar su configuración si es necesario.

EAP. (*Extensible Authentication Protocol*) El protocolo de autentificación extensible EAP de PPP es un protocolo general para la autentificación de PPP que soporta múltiples mecanismos de autentificación. EAP.

F

Fading. Perdida de intensidad. Variación de intensidad de las señales radioeléctricas en el punto de recepción, causada por la alteración de las condiciones del medio de propagación.

Firewall. (*Cortafuegos*) Software o hardware que se encarga de brindar seguridad para que intrusos no puedan acceder a la red sin autorización.

Firmware. Microprogramación incorporada en forma estable e imborrable, de solo lectura.

Firmas digitales. Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje.

H

Hacker. Individuo aficionado a la programación y/o las redes, que suele estar interesado en la seguridad de la información.

Handshake. Intercambio de señales entre maquinas o terminales conectados a un canal de telecomunicaciones para asegurar la conexión mutua

Hash. Función para fines exclusivamente de comprobación.

HMAC (*Keyed-Hashing for Message Authentication*) es un algoritmo de autentificación de llave secreta. HMAC puede utilizar cualquier función hash de criptografía como MD5 o SHA-1, en combinación con una llave secreta compartida

Host. Computadora central distribuidora de información y de programas destinados a otras maquinas.

Hub. (*Concentrador*) Es un dispositivo que conecta varios segmentos de red formando un solo segmento y opera en la capa 1 (nivel físico) del modelo OSI.

I

IMAP. (*Internet Message Access Protocol* o anteriormente llamado *Interactive Mail Access Protocol*) Cuando se utiliza un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios pueden leer y borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo. IMAP lo utilizan principalmente los usuarios que acceden a su correo desde varias máquinas.

IRC. (*Internet Relay Chat*) Sistema multiusuario de charla (*chat*).

IPX. (*Internetwork Packet Exchange*) Protocolo de red de Netware que se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas.

IPv4. Es la versión 4 del Protocolo IP (*Internet Protocol*). Esta fue la primer versión del protocolo que se implemento extensamente, y forma la base de Internet. IPv4 usa direcciones de 32 bits, limitándola a 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs).

IPv6. Es la versión 6 del Protocolo IP. Es la versión que está destinada a sustituir al actual estándar IPv4. IPv6 usa direcciones de 128 bits, cuadruplicando el tamaño de la dirección IPv4 y permitiendo, literalmente, trillones de direcciones más que éste.

IPSec SADB (*Security Associations Date Base*) Cada maquina que participa en la comunicación guarda la información de las asociaciones de seguridad en su base de datos de asociaciones de seguridad (SADB).

K

Keystream. Flujo de clave.

L

LAN. (*Local Area Networks*) La LAN más antigua y popular, ARCnet, fue lanzada en 1977 por Datapoint y fue originalmente diseñada para compartir múltiples discos de almacenamiento Datapoint 2200. Como todas las LANs antiguas, ARCnet era originalmente específica según cada vendedor. Los esfuerzos de estandarización por parte del IEEE resultaron en la serie IEEE 802. Actualmente hay dos tecnologías comunes de cableado para LAN, Ethernet y Token Ring.

L2TP. (*Layer Two Tunneling Protocol*) Protocolo que se utiliza para establecer túneles PPP sobre una red IP pública. Se basa en PPP para el establecimiento de una conexión de marcado empleando la autentificación PAP o CHAP. El protocolo no ofrece cifrado por si mismo, pero puede utilizarse junto con otros protocolos o mecanismos de cifrado en la capa de aplicación para servir a las necesidades de seguridad.

M

MD5. (*Message Digest Algorithm 5*) En criptografía, MD5 es un algoritmo de reducción criptográfico de 128bits ampliamente usado, representado típicamente como un número de 32 dígitos hexadecimal. El siguiente código de 28bytes ASCII será tratado con MD5 y veremos su correspondiente hash de salida:

MD5("Esto si es una prueba de MD5") = e07186fbff6107d0274af02b8b930b65

Un simple cambio en el mensaje nos da un cambio total en el la codificación *hash*, en este caso cambiamos dos letras, el "si" por un "no".

MD5("Esto no es una prueba de MD5") =dd21d99a468f3bb52a136ef5beef5034

Modo Infraestructura. En este modo, cada cliente de la red envía todas sus comunicaciones a una central o punto de acceso AP (*Access Point*) para efectuar el intercambio de datos.

Multicast. Es el envío de la información en una red a múltiples destinos simultáneamente, usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen. En comparación con multicast, los envíos de un punto a otro en una red se le denomina unicast, y el envío a todos los nodos en una red se le denomina broadcast.

Multipath. Señal de propagación por trayectos múltiples.

N

Netstumbler. Es una herramienta para el monitoreo de redes inalámbricas. Este programa despliega algunos datos importantes como el ESSID de la red, el canal en el que transmite y la dirección MAC del punto de acceso.

O

OFDM. (*Orthogonal Frequency Division Multiplexing*) Una técnica de codificación en la capa física en la que se multiplexan varios subcanales de datos más lentos en un único canal combinado rápido. Se utiliza en las redes compatibles con los estándares 802.11a y 802.11g. Debido a las características de esta modulación, las distintas señales con distintos retardos y amplitudes que llegan al receptor contribuyen

positivamente a la recepción, por lo que existe la posibilidad de crear redes de radiodifusión de frecuencia única sin que existan problemas de interferencia.

P

PAP. (*Password Authentication Protocol*) Método de autentificación en el cual el NAS toma el identificador PAP y contraseña y lo envía en un paquete de petición de acceso como nombre de usuario y contraseña

PPP. (*Point to Point Protocol*) Definido en el RFC 1661, este protocolo se usa en redes que usen una interconexión punto a punto y se diseñó para sustituir a SLIP. Las redes punto a punto son aquellas en las que se usa cada canal de datos para comunicar únicamente a 2 nodos, en contraposición a las redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos.

Payload.. Definido como la carga útil de la trama

Ping flood. El comando ping permite enviar paquetes ICMP (*Internet Control Message Protocol*) a otra computadora, con el objetivo de saber si esta encendida y es alcanzable a través de la red. Además muestra un resumen estadístico acerca del por ciento de paquetes perdidos y las velocidades de transmisión. Un ataque *Ping Flood*, consiste en saturar la red enviando un número de paquetes ICMP suficientemente grande. Esta saturación causará una degradación del servicio importante, o incluso la desconexión del sistema.

PKI. (*Public Key Infrastructure*) Permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes. Un usuario puede firmar digitalmente mensajes usando su clave privada, y otro usuario puede validar que dicha firma (usando la clave pública del usuario contenida en el certificado que ha sido emitido por una autoridad de certificación de la PKI). Esto permite a dos (o

más) entidades establecer una comunicación que garantiza la confidencialidad y la integridad del mensaje y la autentificación de los usuarios sin tener que intercambiar previamente ninguna información secreta.

R

Redes Ad-hoc. Una red ad-hoc es una red inalámbrica compuesta por estaciones inalámbricas sin ningún punto de acceso.

RADIUS. (*Remote Authentication Dial-In User Service*) Sistema de autenticación y contabilización, empleado por la mayoría de proveedores de servicio de Internet (ISP's). Cuando el usuario realiza una conexión a su ISP, debe introducir su nombre de usuario y contraseña, información que pasa a un servidor RADIUS que revisará la petición con la información correcta y autorizará el acceso al sistema del ISP si es así.

RFC. (*Request For Comments*) Conjunto de archivos de carácter técnico donde se describen los estándares o recomendaciones para Internet. En el caso de la informática están hechos para hacer compatibles los programas entre sí y que se pueda usar diferente software para la misma función.

Router. (*Enrutador o Ruteador*) Es un dispositivo de hardware o software de interconexión de redes de computadoras que opera en la capa 3 (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

RTS/CTS. (*Request To Send / Clear To Send*)Una implementación práctica que utiliza una negociación en cuatro pasos: RTS ->CTS ->Data ->ACK. El protocolo suele utilizarse para aliviar el problema de los nodos ocultos.. Si cualquier estación desea enviar datos primero tiene que enviar un marco RTS, esperar un CTS de respuesta, antes de que se permita que la transmisión tenga éxito

RSA. El sistema criptográfico con clave pública RSA recibe su nombre por la inicial del apellido de sus inventores: Ronald Rivest, Adi Shamir y Leonard Adleman. Todo usuario de dicho sistema hace pública una clave de cifrado y oculta una clave de descifrado. Cuando se envía un mensaje, el emisor busca la clave pública de cifrado del receptor y una vez que dicho mensaje llega al receptor, éste se ocupa de descifrarlo usando su clave oculta. Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10100) elegidos al azar para conformar la clave de descifrado. La seguridad de este algoritmo radica en que no hay maneras rápidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales. La computación cuántica podría proveer una solución a este problema de factorización.

Roaming. Se refiere a la habilidad de moverse de un área de cobertura de un AP a otra sin la interrupción del servicio ni pérdidas de conectividad

S

SA. Es una clase de conexión que permite establecer los servicios de seguridad del tráfico. En cada SA los servicios de seguridad pueden hacer uso de AH o ESP pero no de ambos. Para utilizar los dos se deberá establecer dos SA.

Sniffer. En un programa que detecta y corrige errores monitoreando toda la información que pasa a través de una red de computadoras

SLIP. (*Serial Line Internet Protocol*) Es una forma simple para encapsular datagramas IP sobre líneas sincrónicas. Este sistema se hizo famoso en los años 80 y principios de los 90 cuando las conexiones domiciliarias a internet por medio de módems no superaban los 2400bps.

Slot time. Intervalo o ranura de tiempo

Spam. Es el hecho de enviar mensajes electrónicos (habitualmente de tipo comercial) no solicitados y en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

Streaming. Emisión continúa. Condición de un dispositivo que permanece en estado de emisión por un periodo de tiempo anormalmente largo.

Switch. Es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.

T

TCP. (*Transmissión Control Protocol*)Protocolo de comunicación de redes, popularizado por Internet, que permiten la transmisión de información en redes de computadoras.

TKIP. (*Temporal Key Integrity Protocol*) Un protocolo de cifrado basado en RC4 que carece de muchas debilidades originales del protocolo WEP estático. TKIP es usado en WPA y es compatible hacia atrás con WEP y no precisa la actualización de hardware.

TLS (*Transport Layer Security*) es una versión estandarizada por el IETF del protocolo SSL que pretende abarcar toda la capa de transporte del modelo OSI.

Throughput. Rendimiento. Medida de la velocidad de transferencia de datos o información por el sistema considerado.

Tuplas. Una tupla es una lista inmutable. Una tupla no puede modificarse de ningún modo después de su creación.

U

UDP. (*User Datagram Protocol*) Protocolo del nivel de transporte basado en el intercambio de datagramas. Un datagrama es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar el fragmento hacia el receptor, de manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en la computadora destino. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

W

Warchalking. Etiquetado de la presencia de redes inalámbricas descubiertas y de sus propiedades mediante tiza o pintura, empleando un conjunto de símbolos.

Wi-Fi. Cuando un producto es comprobado que funciona correctamente con otros dispositivos 802.11b, recibe el certificado Wi-Fi como garantía de interoperabilidad y buen funcionamiento.

X

XOR. Es una operación lógica muy simple que consiste en escribir un 0 cuando los caracteres son los mismos y un 1 cuando los caracteres son diferentes como se muestra en la siguiente tabla.

Original bit	XOR bit	bit Resultante
1	1	0
0	0	0
1	0	1
0	1	1

X.509 es un estándar de certificados para firmar documentos y garantizar la seguridad y fiabilidad en las comunicaciones. El X.509 está definido por la RFC3280 del IETF.

BIBLIOGRAFÍA

Potter, Bruce & Fleck, Bob.
802.11Security,
O´Relly, USA, 2003.

Peikari, Cyrus & Fogie, Seth .
Wireless Maximum Security,
SAMS, Indiana USA, 2003.

Collazo, Javier.
Diccionario Collazo de Computación
Ingles-Español,
McGraw-Hill, 2001.

McClure,Stuart & Scambray,Joel.
Hackers 4,
McGraw Hill, España, 2003.

Carter, Brian & Shumway, Russel.
Wireless Security, end to end,
Wiley Publishing, USA, 2003.

Raya, Jose luis & Raya, Cristina.
Redes Locales,
Alfaomega, España, 2002.

Vladimirov, Andrew & Gavrilenko, Konstantin.
Hacking Wireless,
Anaya Multimedia, España, 2005.

Bing, Benny.
High-Speed Wireless ATM and LAN's
Artech House, USA, 2000.

Barret, Daniel.
SSH, The Secure Shell.
O'Reilly, USA, 2001.

Stojmenovic, Ivan.
Handbook of Wireless Networks and Mobile Computing,
Wiley Interscience Publication, USA, 2002.

Regis, J (Bud) Bates.
Comunicaciones Inalámbricas de Banda Ancha,
McGraw Hill, España, 2003.

Gast, Matthew.
802.11 Wireless Networks: The Definitive Guide, USA,
O'Reilly, 2003.

Flickenger, Rob.
Building Wireless Community Networks,
O'Reilly, USA, 2003.

Hassell, Jhonathan.
RADIUS,
O'Reilly, USA, 2002.

Engst, Adam & Fleishman, Glenn.
Wireless Networking Starter Kit,
Peachpit Press, USA, 20

Kurose, James.
Computer Networking,
Addison Wesley, USA 2002

Paginas WEB:

http://www.cisco.com

http://www.3com.com.mx

http://www.usr.com

http://www.ieee.org

http://www.etsi.org

http://www.ietf.org

http://www.pcm.gob.pe

http://www.wi-fi.org

http://www.microsoft.com

http://www.linksys.com

http://www.wlana.org

http://httpd.apache.org/docs 2.0/ssl/ssl_intro.html

http://www.net.princeton.edu

http://foro.elhacker.net

http://www.pcenlinea.com

http://www.zaragozawireless.org

http://www.isocmex.org.mx/firm_dig.html

http://www.freeradius.org/

http://www.intel.com

http://www.iana.org

http://www.wikipedia.org

http://www.airsnort.shmoo.com

http://www.wi-fizone.org

http://www.rfc-es.org

http://www.wi-fiplanet.com

http://www.netstumbler.org