UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO E IMPLANTACIÓN DE LA RED INALÁMBRICA DEL INSTITUTO DE INGENIERÍA DE LA U. N. A. M.

T E S I S

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

A N A Y A T O R R E S N O E M Í
S A N T O S F R A G O S O D I A N K O

DIRECTOR: ING. MARCO AMBRÍZ MAGUEY

CIUDAD UNIVERSITARIA **MÉXICO, D. F., 2006**

Este trabajo está dedicado a mis padres,
por su apoyo incondicional, pero
sobretodo por el ejemplo a
seguir que han sido para mí.

Agradezco a Guillermo, mi hermano,
por estar siempre conmigo apoyándome.

A Dianko, mi novio, por compartir
juntos este logro.

A Gabriela, por ser mi mejor amiga.

A mi tio Beto y a mi tia Mimi y a mi
familia en general por confiar
siempre en que yo podía.

Al Ing. Marco Ambríz, mi Director de
tesis por guiarme en la realización
de este proyecto.

Un especial agradecimiento a todas
esas personas que me formaron,
mis profesores.

Noemí Anaya Torres

Agradezco a mi madre
por ayudarme y darme la oportunidad
de estudiar.

A mis abuelos por su sustento
y apoyo.

A Noemí por dejarme compartir esta
experiencia con ella

Agradezco al Ing. Andrés Benítez Guzmán
por enseñarme el camino.

Al Ing. Marco Ambríz por permitirnos
colaborar con el Instituto de
Ingeniería.

A mis amigos y profesores, a la Ing. Araceli Martínez y
al M. en I. Alejandro Guzmán por apoyarme
en mi formación.

Gracias.

Dianko Santos Fragoso

ÍNDICE

INTRODUCCIÓN

El Instituto de Ingeniería de la Universidad Nacional Autónoma de México (IIUNAM) es el centro de investigación en diversas áreas de la ingeniería más productivo del país. Es una comunidad integrada por 93 investigadores, 95 técnicos académicos, 409 becarios que realizan trabajos de tesis de licenciatura, maestría y doctorado y 184 personas del área administrativa. Sus instalaciones ocupan 13 edificios en la zona de Ciudad Universitaria, en la ciudad de México, con una extensión de 20,000 metros cuadrados construidos entre laboratorios, cubículos, áreas comunes y un auditorio.

Desde su fundación, la política del Instituto ha sido realizar investigación orientada a problemas generales de la ingeniería, colaborar con entidades públicas y privadas para mejorar la práctica de la ingeniería en el ámbito nacional, proporcionar servicios de ingeniería a los diversos sectores de la sociedad. Asimismo, ha puesto especial atención en la formación de recursos humanos y en difundir los resultados de sus investigaciones, contribuyendo así al desarrollo del país y al bienestar de la sociedad.

La operación del Instituto está regida por su Reglamento Interno. En él, se reconoce que la misión del Instituto es:

"Contribuir al desarrollo del país y al bienestar de la sociedad a través de la investigación en ingeniería y de la formación de recursos humanos".

En lo referente a la actualización tecnológica el Instituto tiene como objetivo continuo el de modernizar el quehacer y la infraestructura del Instituto a través de las siguientes estrategias:

1. Definir la misión y visión del Instituto
2. Definir las líneas de investigación y el tipo de proyectos
3. Modernizar la estructura operativa del Instituto
4. Modernizar los edificios, laboratorios y equipos.

Así mismo, el Instituto de Ingeniería cuenta con una infraestructura moderna, entre la cual destaca el sistema de redes, abarcando temas que tienen que ver con tecnología en convergencia de voz y datos, control de las aplicaciones en la red, calidad de servicio, seguridad, y mayor ancho de banda. Esto ha enriquecido los componentes que integran las redes y abren nuevas opciones para ofrecer más y mejores servicios a través de ellas. Asimismo un valor importante que ofrece esta evolución de las redes lo representa la reducción de costos y la alta flexibilidad y facilidad de implantación.

En el rubro de recursos humanos, los investigadores del Instituto de Ingeniería desarrollan proyectos en las siguientes áreas: Estructuras y Materiales, Geotecnia, Ingeniería Sismológica, Mecánica Aplicada, Sismología e Instrumentación Sísmica, Vías Terrestres, Bioprocesos Ambientales, Hidráulica, Ingeniería Ambiental, Ingeniería de Procesos Industriales y Ambientales, Automatización, Ingeniería Mecánica, Térmica y Fluidos, Ingeniería de Sistemas, Instrumentación y Sistemas de Cómputo.

Muchos de los investigadores que participan en estos proyectos realizan pruebas de campo utilizando equipo de cómputo portátil en los que ejecutan diversas aplicaciones (bases de datos, software de propósito específico, por ejemplo, cálculos matemáticos, procesamiento de imágenes, procesamiento de señales, etc.) con diversos sistemas operativos. Toda la información generada y recopilada necesita ser transferida, procesada y/o respaldada en sus estaciones de trabajo y PC's., por ello es necesario que los investigadores tengan fácil acceso a la red del Instituto de Ingeniería.

Por dichas razones el Instituto de Ingeniería busca soluciones tecnológicas que basen su desarrollo en los conceptos anteriores y que por supuesto, brinden la mejor relación costo-beneficio y protección de la inversión, todo esto unido a la misión de la propia institución que es la investigación y formación de recursos humanos altamente capacitados

Dentro de esta búsqueda, una alternativa que se ofrece al Instituto de Ingeniería con la intención de facilitar el desempeño de las actividades de su personal, es una red inalámbrica; Esta red tiene como objetivos fundamentales la cobertura en áreas de difícil acceso y conectividad rápida en áreas de trabajo y auditorios para eventos masivos donde no haya puntos de red disponibles satisfaciendo los requerimientos de movilidad y fácil conexión que demandan los usuarios. Además, cabe mencionar que se ha visto un incremento en el uso de equipo portátil (Laptop's, PDA's, etc.) capaz de acceder a la red del Instituto de Ingeniería de manera inalámbrica, y la necesidad de comunicarse entre éstos para compartir información y recursos (impresión remota, archivos, correo electrónico, sincronización de información, etc.).

Dentro de este contexto, los objetivos fundamentales para el diseño e implantación de la red inalámbrica del Instituto de Ingeniería se basan en la utilización e integración de tecnología de punta, teniendo como propósito lograr una infraestructura funcional y considerando los aspectos de escalabilidad, adaptabilidad, interoperabilidad y seguridad principalmente.

OBJETIVOS

Objetivo general

Diseñar e implantar la red inalámbrica del Instituto de Ingeniería tomando en cuenta las últimas tecnologías en redes inalámbricas con base en estándares internacionales.

Objetivos particulares

- Adquirir los conocimientos necesarios para el diseño e implantación de redes inalámbricas.

- Tener un panorama amplio sobre las distintas tecnologías y arquitecturas de redes inalámbricas.

- Analizar los requerimientos técnicos y operativos de la red de cómputo del Instituto, así como las necesidades de sus usuarios de acuerdo a las actividades que desarrollan y los recursos que utilizan, considerando los diferentes estándares, tecnologías existentes, sus políticas internas y la seguridad para el diseño de la red inalámbrica.

- Implantar la red inalámbrica del Instituto de Ingeniería.

1

Antecedentes

Introducción

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. Para el diseño de la red inalámbrica del Instituto de Ingeniería es necesario conocer la terminología general necesaria para comprender algunos aspectos de la misma, características básicas con las que cuenta una red inalámbrica, los diversos modos de operación en que se puede configurar, la propagación de la señal en el canal inalámbrico, su método de acceso, así como la modulación y el ancho de banda disponible.

Estos factores son importantes en el diseño de la red inalámbrica del Instituto de Ingeniería ya que nos permiten determinar la eficiencia y la capacidad del sistema de red dentro de un área geográfica, además de definirla como un sistema abierto, es decir, un sistema capaz de establecer comunicación con otras redes de cómputo.

1.1 Características de una red inalámbrica

1.1.1 Definición de una red inalámbrica

Una red inalámbrica (WN, Wireless Network) es una red que no utiliza cables para llevar a cabo sus conexiones, tiene como medio de transmisión el aire, utiliza ondas electromagnéticas para transmitir la información que viaja a través del canal inalámbrico enlazando los diferentes equipos o terminales móviles asociados a la red. Estos enlaces se implementan básicamente a través de tecnologías de microondas y de infrarrojos.

De acuerdo a su alcance las WN se clasifican en:

- Red inalámbrica de área personal (WPA, Wireless Personal Area).
- Red inalámbrica de área local (WLAN, Wireless Local Area Network).
- Red inalámbrica de área metropolitana (WMAN, Wireless Metropolitan Area Network).

La principal ventaja de esta tecnología es que es capaz de ofrecernos la movilidad, facilidad en la reubicación de las estaciones de trabajo que evita establecer cableado, manteniendo unas prestaciones, coste y complejidad de conexión razonables.

En movilidad las redes inalámbricas proporcionan a los usuarios:

1. Acceso a la información en tiempo real
2. Simplicidad y rapidez en la instalación
3. Flexibilidad en la instalación permitiendo a la red llegar a puntos de difícil acceso
4. Costo de propiedad reducido: la inversión inicial requerida puede ser más alta que el costo en hardware de una LAN, sin embargo, la

inversión de toda la instalación y el costo durante el ciclo de vida puede ser significativamente inferior.

Los sistemas WN pueden ser configurados en diversas topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además resulta muy fácil la incorporación de nuevos usuarios a la red, por ende podemos mencionar que otra ventaja de las WN's es la de proporcionar escalabilidad.

1.1.2 Canal inalámbrico

Existe una gran variedad de canales, los cuales pueden ser divididos en dos grupos. Si la conexión entre el transmisor y receptor es sólida, entonces el canal es llamado alámbrico. Si esta conexión se pierde se denomina canal inalámbrico.

El canal inalámbrico es inestable, tiene un bajo ancho de banda y es de naturaleza broadcast. Las transmisiones inalámbricas comparten el mismo medio: el AIRE. Con el medio inalámbrico, nosotros estamos restringidos a un ancho de banda limitado disponible para la operación y no podemos obtener nuevos anchos de bandas o fácilmente duplicar el medio para acomodar a más usuarios, por lo que se ha tenido que desarrollar técnicas que permitan soportar más usuarios en un ancho de banda fijo. En las redes cableadas se incrementa la cantidad de cables permitiendo tener más usuarios conectados, en las redes inalámbricas se reduce el tamaño de la célula aunque se incrementa la complejidad de interconexión entre células. Las redes inalámbricas operan alrededor de 1GHz (celular), 2GHz (PCS y WLANs), 5GHz (WLANs), 28-60GHz (servicio de distribución multipunto local y conexiones punto-punto de estaciones base).

Los factores adversos del canal incluyen: Ruido, Pérdidas por la trayectoria de la señal de radiofrecuencia, Desvanecimientos a bajas velocidades, Interferencia entre símbolos (ISI) a altas velocidades, Desvanecimientos sombra, Interferencia co-canal, Interferencia de canal adyacente, Multitrayectorias y los que varían en el tiempo debido a la movilidad del usuario como son: Interferencia, Obstrucción, Efecto Doppler.

La Comisión Federal de Comunicaciones (FCC) permitió la operación sin licencia de dispositivos que utilicen 1 watt de energía o menos, en tres bandas de frecuencias: 902 a 928MHz, 2.400 a 2.4835MHz y 5.725 a 5.850MHz (Figura 1).

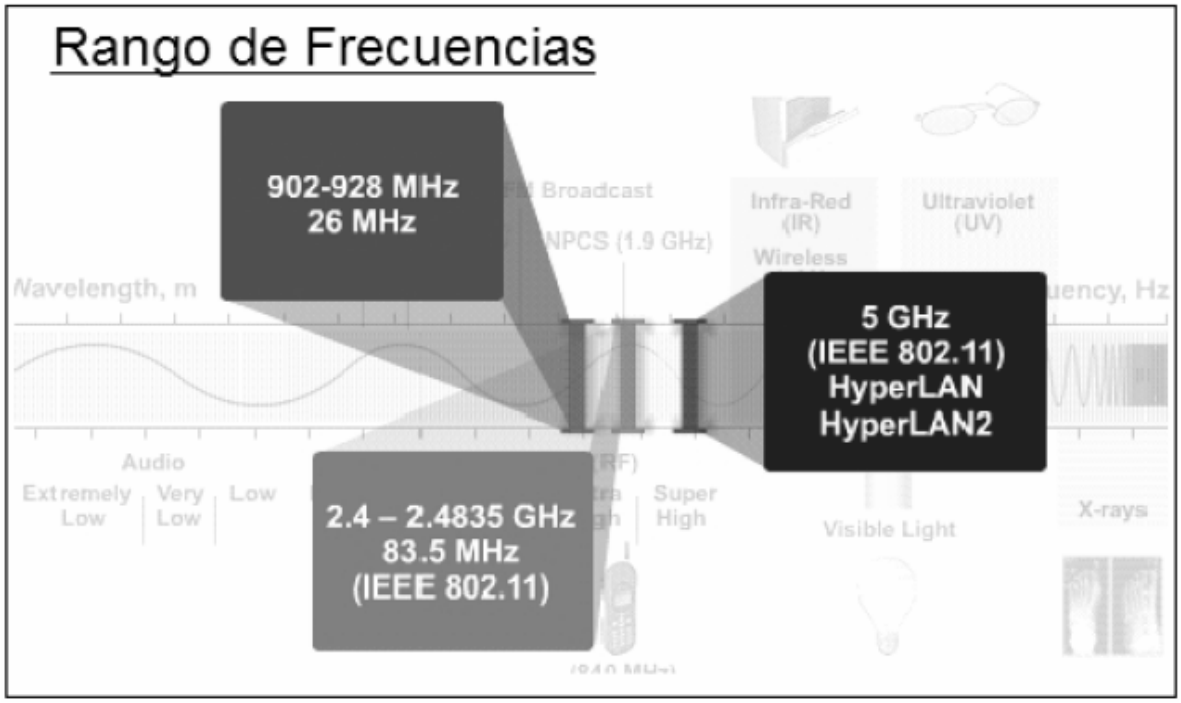


Fig. 1 Espectro Inalámbrico

1.1.3 Propagación de la señal

La propagación de la señal difícilmente puede ser dirigida a un sitio específico ya que las ondas de radio se propagan hacia fuera de la antena esféricamente y pueden variar significativamente dependiendo del terreno, la frecuencia de operación, la velocidad de la terminal móvil, fuentes de interferencia, y otros factores dinámicos.

La propagación es diferente dependiendo del tamaño de las células (éste puede ser femto-, pico-, micro-, macro-, y mega células), de los espacios abiertos, cerrados y áreas urbanas.

La fuerza de la señal depende de la distancia que ha recorrido, de los objetos que la han reflejado, la arquitectura del ambiente, y de la localización de los objetos alrededor del receptor y transmisor.

La frecuencia de operación también afecta las características y diseño del sistema. Para bajas frecuencias las pérdidas en la señal puede ser muy pequeñas en el primer metro, sin embargo, el ancho de banda es menos abundante y el tamaño de las antenas requerido es prohibitivo para un desarrollo a gran escala. La separación de las antenas también tiene que ser mucho más grande. Por otro lado, para altas frecuencias el ancho de banda es más amplio además de que es posible utilizar transmisores de baja potencia (alrededor de 1 W). El tamaño de las antenas se reduce a una pulgada, haciendo a los transmisores y receptores más compactos y eficientes. La desventaja con las altas frecuencias es que existen pérdidas en la señal en el primer metro y cuando pasan por obstáculos tales como paredes.

Las tres características más importantes de la propagación de la señal utilizadas para el diseño, análisis e instalación de redes inalámbricas son: la cobertura efectiva de la señal, la cual la determina el tamaño de la célula y el rango de operación de la estación base para una potencia dada, la tasa máxima de transferencia soportada por el canal y que es influenciada por la estructura multitrayectoria del canal, y las fluctuaciones.

1.1.3.1 Mecanismos de propagación

Los 4 factores que afectan la propagación de la señal son:

1 Pérdidas por trayectorias.
2 Desvanecimientos lentos (Shadow Fading).
3 Desvanecimientos rápidos (Fast Fading).
4 Efecto Doppler.

1.1.3.1.1 Pérdidas por trayectorias

Es la reducción de la potencia de la señal en el receptor en relación con la potencia transmitida. Esas pérdidas son proporcionales a la distancia (elevadas a una potencia adecuada). Se modela de la siguiente manera:

$$P_R = G_T G_R P_T \left(\frac{\lambda}{4\pi d} \right)^2$$

En donde G_T y G_R son las ganancias de las antenas del transmisor y receptor respectivamente; d es la distancia entre el transmisor y el receptor, λ es la longitud de onda, P_T y P_R son las potencias de transmisión y recepción respectivamente.

1.1.3.1.2 Desvanecimientos lentos

La potencia recibida medida en el campo varía aleatoriamente alrededor de una potencia promedio (Figura 5). Estas variaciones en la señal se deben a que ésta es bloqueada por edificios (en espacios abiertos), paredes (en espacios cerrados), y otros objetos en los alrededores. Esto provoca que la fuerza de la señal no sea la misma para un conjunto de puntos que están a una distancia dada. Estos desvanecimientos también son llamados "*desvanecimientos lentos*" debido a que se necesita muchas longitudes de onda para que la señal varíe. Se ha encontrado también que tienen poca dependencia de la frecuencia de operación.

Una buena aproximación es asumir que la potencia medida en decibeles sigue una distribución Gaussiana o Normal (Figura 2), centrada en su valor promedio con desviación estándar que varía de entre los 6 a 10 dB.

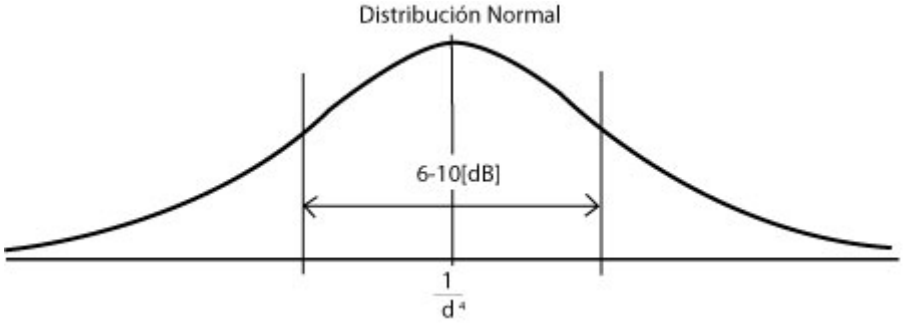


Fig. 2 Distribución Gaussiana o Normal

La siguiente tabla muestra como la señal a una frecuencia de 2.4 GHZ se atenúa cuando pasa a través de diferentes objetos:

Objeto	dB
Ventana en pared de ladrillo	2
Marco de metal, pared de vidrio dentro de edificios	6
Pared de Oficina	6
Puerta de metal en pared de oficina	6
Puerta de metal en pared de ladrillo	12.4
Pared de ladrillo junto a una puerta de metal	3

Tabla 1. Atenuación de la señal al pasar por diversos objetos.

1.1.3.1.3 Desvanecimientos rápidos

Estas pequeñas variaciones en la potencia de la señal se deben a la suma de señales que llegan al receptor con diferentes fases. Esta diferencia de fase se debe a que las señales han viajado diferentes distancias por diferentes trayectorias (Multitrayectorias). Este tipo de fluctuaciones siguen la distribución Rayleigh (Figura 3) para células grandes y la distribución Ricean para células pequeñas (Figura 4).

Estas variaciones en la señal provocan una alta tasa de errores, por lo que es necesario implementar técnicas de control de errores además del uso de antenas direccionales.

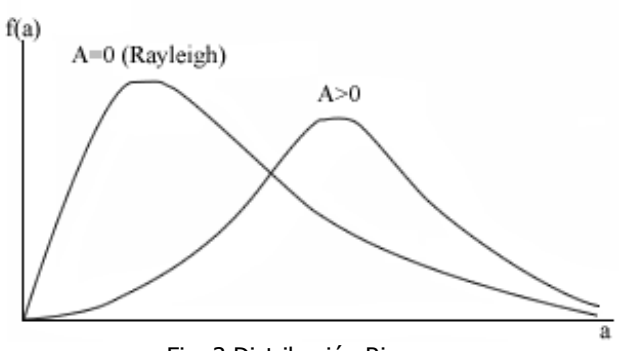


Fig. 3 Distribución Ricean

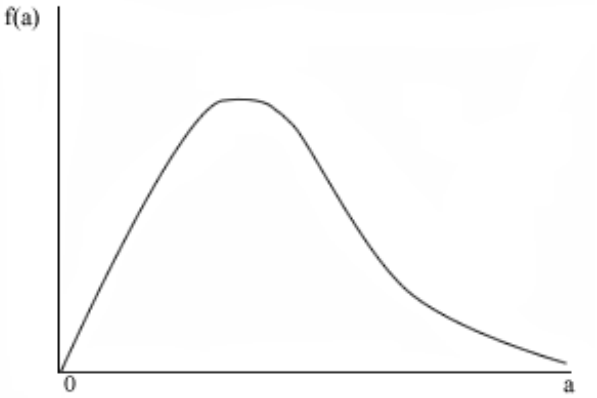


Fig. 4 Distribución Rayleigh

Conjuntando los tres fenómenos anteriores, la variación estadística de la señal de potencia recibida P_R pude ser modelada para sistemas inalámbricos celulares como:

$$P_R = \alpha^2 10^{\frac{x}{10}} g(d) P_T G_T G_R$$

Donde:

$10^{\frac{x}{10}}$ Fluctuaciones Lentas
α^2 Fluctuaciones Rápidas
x y α Variables aleatorias
$g(d)$ Variación inversa de la potencia recibida respecto a la distancia

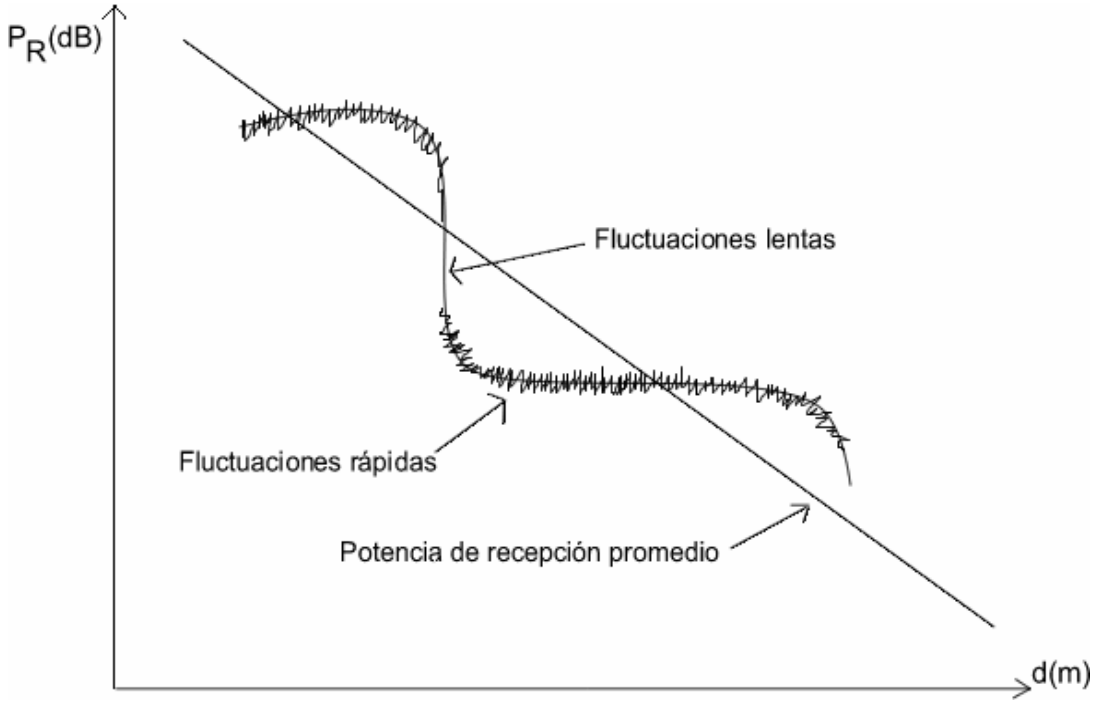


Fig. 5 Factores que afectan la propagación

1.1.3.1.4 Efecto Doppler

Este efecto es causado por el movimiento del usuario (Figura 6). Una forma fácil de entender este fenómeno es con el ejemplo clásico del silbato de una locomotora en movimiento. Las ondas sonoras viajan a la misma dirección del tren cuando este se aproxima, por lo cual éstas se comprimen y el receptor recibe más de ellas en la unidad de tiempo. Al alejarse el tren, las ondas viajan en sentido contrario, recibiendo el espectador menos ondas en la unidad de tiempo, por lo tanto, el sonido es más grave.

Lo que este efecto provoca entonces, es el desplazamiento de la frecuencia (frecuencia doppler) recibida con respecto a la del transmisor. Además se experimentan variaciones de amplitud y de fase en cortas distancias. La potencia de la señal puede cambiar drásticamente sobre la mitad de una longitud de onda.

La máxima frecuencia doppler puede ser calculada de la siguiente manera:

$$f_m = \frac{v_m}{\lambda}$$

En donde:

v_m Es la velocidad del móvil, y
λ Es la longitud de onda de la señal

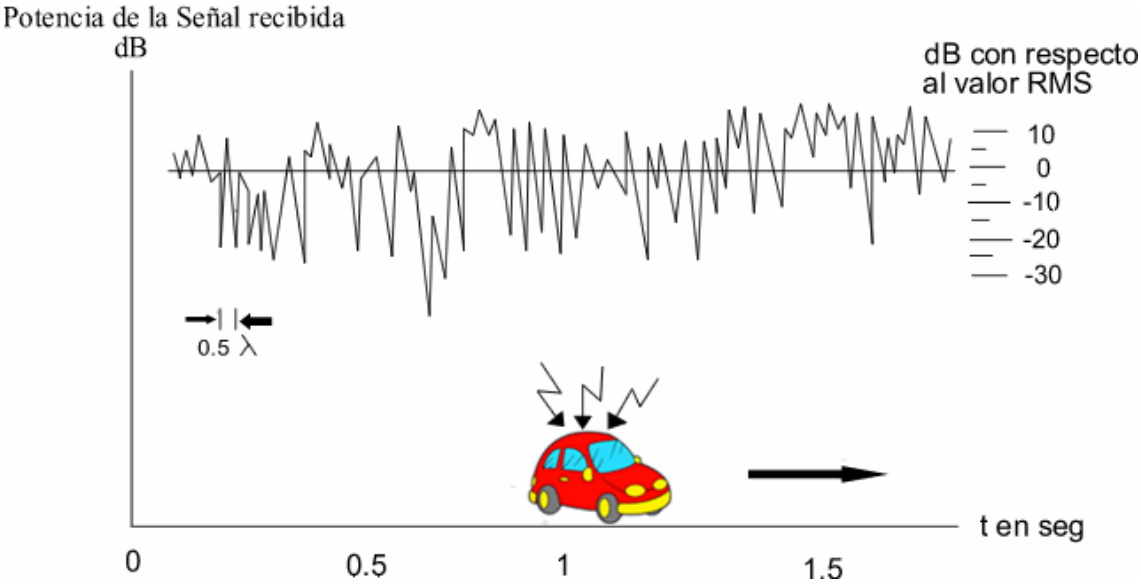


Fig. 6 Desvanecimientos profundos

1.1.3.2 Distorsión

El ancho de banda es dividido en rangos de frecuencias; si al medir los parámetros de atenuación, dispersamiento de retardos y tiempo de propagación en cada uno de estos rangos de frecuencias, varían, se dice que existe distorsión.

Una forma de comparar las señales, para representar el efecto del canal inalámbrico sobre un ancho de banda B es la función de correlación $E(a_1\ a_2)$, donde a_1 y a_2 es la amplitud recibida que se obtiene al promediar de las señales las siguientes variables aleatorias:

$$S_1(t) = \sum_{k=1}^{L} a_k \cos\left[\omega_1\left(t - t_1 - \tau_k\right) + \theta_k + \omega_k t\right]$$

donde:

a_k Amplitud de la señal

θ_k Ángulos adicionales aleatorios uniformemente distribuidos entre 0 y 2π

τ_k Representa el retraso aleatorio extra que tiene cada señal.

ω_k Está definido por: $\omega_k = 2\pi \cos\beta_k \frac{v_m}{\lambda}$

β_k Ángulos de arribo de cada rayo

En la práctica se usa la función de correlación normalizada definida como:

$$\rho_a = \frac{E(a_1 a_2) - E(a_1)E(a_2)}{\sigma_1 \sigma_2}$$

donde: $\sigma_i^{\,2} = E[a_i - E(a_i)]^2 \quad i = 1,2$ que es la varianza de a_i y $E(a_i)$ es su valor promedio.

Lo que la función de correlación indica es si existe distorsión en el canal, por lo tanto, si ρ_a =1 implica que el canal inalámbrico (+movilidad) *NO distorsiona*, lo que significa que todas las componentes espectrales de la señal modulada son afectadas de la misma manera.

Cuando ρ_a = 0 aparecen dos casos:

El canal inalámbrico está distorsionando a la señal original con ancho de banda B.
Si B es muy grande pueden aparecer "ecos", permitiendo que puedan ser resueltas independientemente.

1.1.3.2.1 Dispersamiento de Retardos

La forma del pulso recibido y su tiempo de duración son cambiados debido a la recepción de múltiples señales. La diferencia entre el primero y el último pulso es el dispersamiento de retardo del canal y es representado por τ_k . Lo que esto produce es la interferencia entre símbolos (ISI), que consiste en la superposición de símbolos adyacentes debido a que las componentes directa y reflejada llegan en instantes diferentes (Figura 7). Para evitar este problema, la duración del símbolo se alarga con lo que se tiene un intervalo de guarda, evitando de esta manera que la superposición de símbolos afecte a su contenido. Solamente retrasos muy largos podrían causar interferencia entre símbolos, y retrasos tan largos son extremadamente raros.

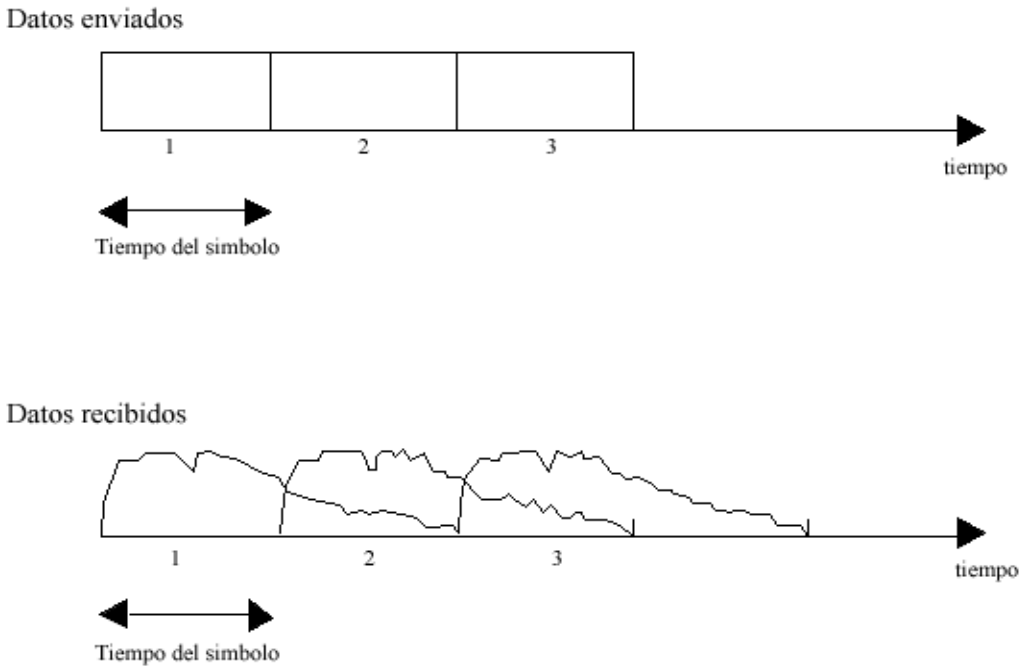


Fig. 7 Dispersamiento de retardos

1.1.3.3 Rangos de propagación de la señal

Rango de transmisión
Una comunicación entre nodos vecinos solo será posible si dichos nodos se encuentran dentro del rango de transmisión. La principal característica de la comunicación cuando estamos dentro de este rango es que la tasa de errores es baja. La máxima distancia que puede abarcar este rango es de 250m (Figura 8).

Rango de detección
Se refiere al rango en el que un nodo es capaz de detectar o escuchar una señal, sin embargo no es posible una comunicación. La máxima distancia que puede abarcar este rango es de 550m aproximadamente (Figura 8)..

Rango de interferencia
Propiamente no existe una distancia máxima que pueda abarcar este rango puesto que está se refiere al rango en el que un nodo ya no es capaz de escuchar una señal como tal, simplemente se percibe como ruido de fondo (Figura 8).

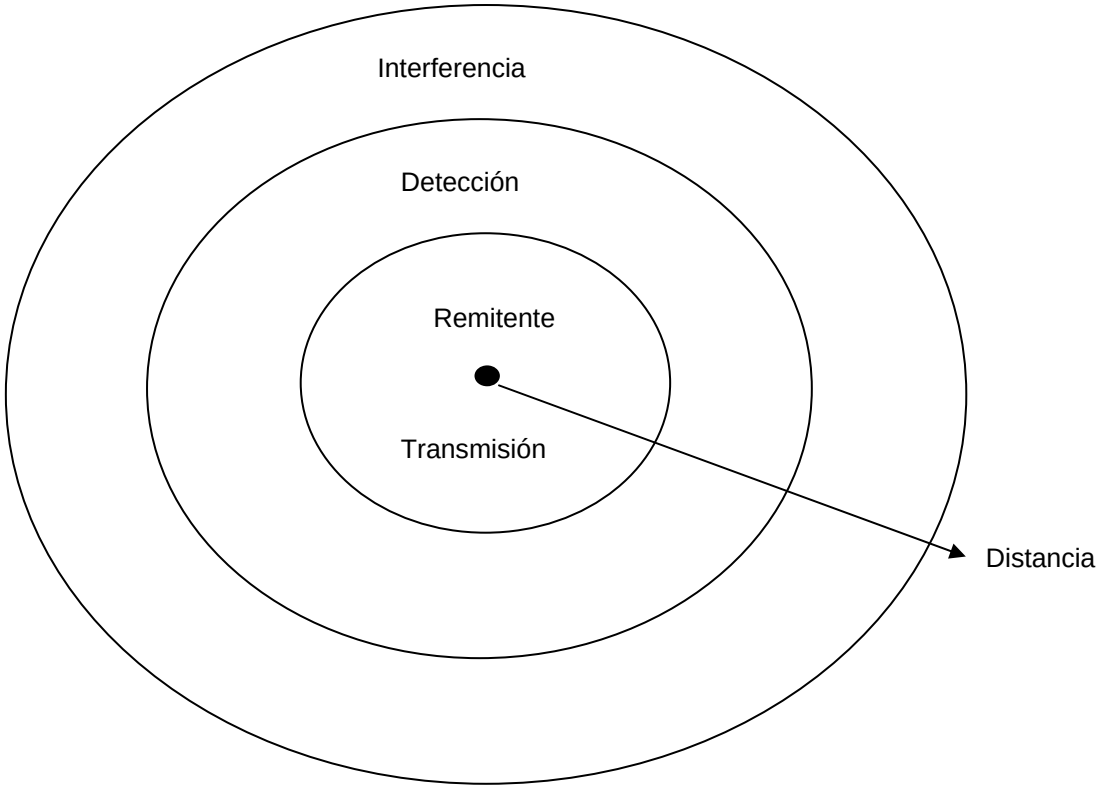


Fig. 8 Rangos de propagación de la señal

1.1.4 Tipos de modulación

Modulación

En general, modulación es el proceso por el cual una propiedad o un parámetro de una señal, se varía proporcionalmente a una segunda señal, así mismo, es el proceso de transformar la información de una fuente de mensaje (banda base) en una manera adecuada de transmisión. Generalmente comprende el traducir la señal de banda base a una portadora de radio a frecuencias que son altas comparadas con la frecuencia en banda base.

En la práctica, bien sea por compartir el canal (por ejemplo el aire) o por poder usar antenas de dimensiones razonables, es necesario modular. Al modular se modifica la amplitud, la frecuencia o la fase de una portadora que puede ser una sinusoide, en función del mensaje (Figura 9).

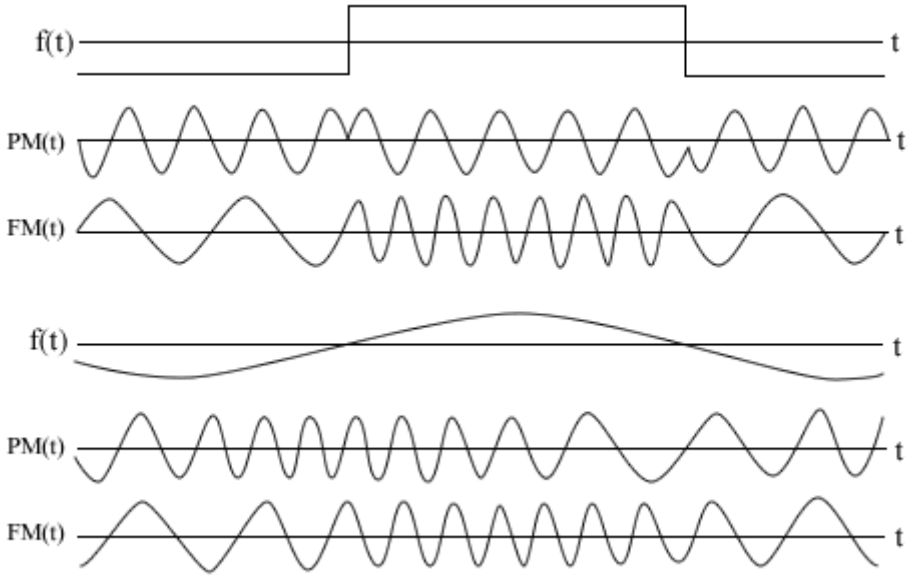


Fig. 9 Ejemplos de modulación en frecuencia y fase.

1.1.4.1 Técnicas de modulación digital

Demodulación: es el proceso de extraer la banda base de la portadora, de tal forma que pueda ser procesada e interpretada por el receptor.

Detección: consiste en extraer los símbolos de directamente de la forma de onda. Existen dos tipos de detección:

1.1.4.1.1 Detección coherente: Es la técnica que requiere una réplica de la onda portadora en el receptor. Dicho receptor usa la réplica para detectar la señal y realiza la correlación cruzada de la señal y la réplica. En esta técnica se procesa la señal recibida con una portadora local con la misma frecuencia y fase. Dentro de esta técnica encontramos:

1.1.4.1.1.1 Phase Shift Keying (PSK). Aunque PSK no es usado directamente, es la base para entender otros sistemas de modulación de fase multinivel. Consiste en variar la fase de la sinusoide de acuerdo a los datos. Para el caso binario, las fases que se seleccionan son 0 y p (Figura 10). En este caso la modulación de fase recibe el nombre de PRK (Phase Reversal Keying).

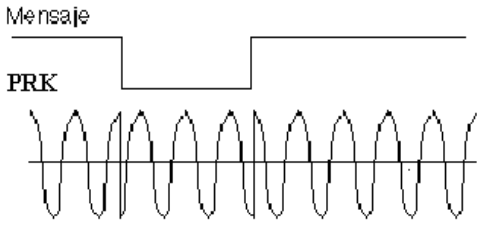


Fig. 10 PSK

1.1.4.1.1.2 Frequency Shift Keying (FSK). Consiste en variar la frecuencia de la portadora de acuerdo a los datos (Figura 11).. Si la fase de la señal FSK es continua, es decir entre un bit y el siguiente la fase de la sinusoide no presenta discontinuidades, a la modulación se le da el nombre de CPFSK (Continuous Phase FSK). Aquí, no ocurre variación de fase de la portadora para dígitos del mismo valor.

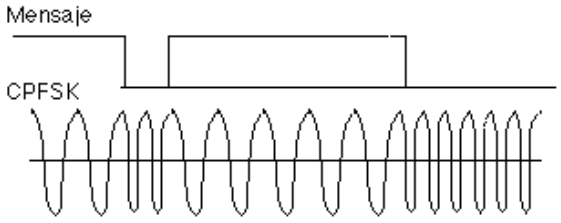


Fig. 11 FSK

1.1.4.1.1.3 Amplitude Shift Keying (ASK). Consiste en cambiar la amplitud de la sinusoide entre dos valores posibles (Figura 12); si uno de los valores es cero se le llama OOK (On-Off keying). La aplicación más popular de ASK son las transmisiones con fibra óptica ya que es muy fácil "prender" y "apagar" el haz de luz; además la fibra soporta las desventajas de los métodos de modulación de amplitud ya que posee poca atenuación. El modulador es un simple multiplicador de los datos binarios por la portadora. A continuación se ilustra un ejemplo de un mensaje en banda base y el resultado de modular en ASK (OOK).

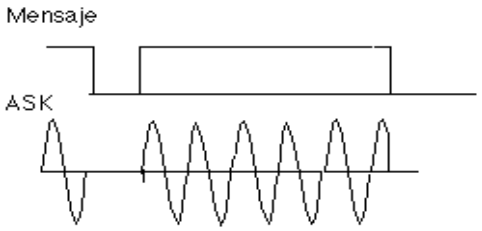


Fig. 12 ASK

1.1.4.1.2 Detección no coherente: No explota la información de referencia de fase y se tiene un receptor menos complejo pero con un peor desempeño (Figura 13). Este tipo de detección no requiere de una onda de referencia. Dentro de esta técnica encontramos:

1.1.4.1.2.1 Differential Phase Shift Keying (DPSK). Variación de la modulación PSK, que tiene como característica un procedimiento de la fase de acuerdo con un dígito a ser transmitido.

1.1.4.1.2.2 Frequency Shift Keying (FSK). Se puede ver como la superposición de dos ondas ASK de manera que el análisis matemático para la obtención del error en este caso, se basa en imaginarse dos ramas de detección ASK y luego hacer una relación entre la salida de las dos ramas. Aquí, puede ocurrir variación de fase de la portadora para dígitos del mismo valor.

1.1.4.1.2.3 Amplitude Shift Keying (ASK). Para eliminar la necesidad de sincronizar las fases de las portadoras de transmisión y recepción, se utiliza un esquema de detección no-coherente como el siguiente:

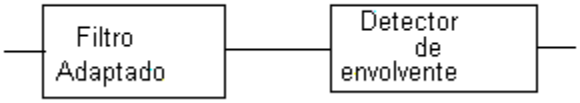


Fig.13 Detección no coherente

La salida del detector de envolvente se toma cada cierto tiempo la decisión de si se envió un 1 ó un 0.

1.1.5 Control de error

Durante la transmisión de información digital a través de un canal se producen errores prácticamente inevitables debido a la presencia de ruido y a otros factores tales como la interferencia intersímbolos, la intermodulación y los ecos. Es por ello que es necesario establecer maneras, si no para evitar los errores, por lo menos para poder reconocer su presencia y si es posible corregirlos.

El proceso de control de error es de gran importancia pues debido a la baja redundancia de los datos digitales, un grupo de números o símbolos alfanuméricos erróneo puede parecerse a otro significando algo muy diferente. El concepto de redundancia lo podemos entender mejor mediante un sencillo ejemplo: el conjunto [00, 01, 10, 11] de mensajes binarios no es redundante porque todas las palabras posibles de dos dígitos binarios están contenidas en el conjunto; un error de transmisión en cualquiera de las palabras la convierte en otra palabra válida del conjunto y no habría manera de detectar el error. La redundancia es de capital importancia en el control de error pues, como lo estableció Shannon, no es posible transmitir sin error si los códigos utilizados tienen cero redundancia.

El primer método de control de error que se utilizó fue el denominado "ecoplex". En este método el transmisor envía un carácter, el cual es recibido en el receptor y retransmitido como un eco hacia el transmisor, de aquí el nombre de ecoplex. En el transmisor se examina el carácter eco recibido para ver si difiere del carácter original; si es diferente simplemente se corrige el error y se transmite de nuevo.
En los sistemas de comunicación actuales el control de error se efectúa mediante la aplicación de códigos especiales que agregan redundancia; Esta redundancia agregada permite detectar y/o corregir los errores ocurridos durante la transmisión de los bloques de datos.

1.1.5.1 Detección y corrección de error

Cuando se recibe un bloque de dígitos binarios es necesario asegurarse de que no contiene errores de transmisión. Si se detecta que el bloque está en error, se tiene dos opciones: una es corregir el error en el sitio y la otra solicitar la retransmisión del bloque.

Esta situación ha producido las dos técnicas de control de error comúnmente utilizadas: la Corrección Directa de Error (Forward Error Correction, FEC) y la Solicitud de Repetición Automática (Automatic Repeat Request, ARQ). En la técnica FEC se utilizan códigos para detectar y corregir los errores en el receptor; mientras que en la técnica ARQ los códigos solamente detectan la presencia de errores en los datos recibidos y se solicita en alguna forma la repetición de los bloques que vienen en error.

Cualquiera que sea la estrategia de control de error, FEC o ARQ, la secuencia transmitida debe ser codificada, es decir, se le debe agregar una cierta redundancia. Esta codificación se efectúa en los CODEC y se localiza en la forma mostrada:

Fig. 14 Esquema del Sistema de Comunicación

1.1.5.2 Solicitud de Repetición Automática (Automatic Repeat Request, ARQ)

El ARQ (del inglés *Automatic Repeat-reQuest*) es un protocolo utilizado para el control de errores en la transmisión de datos, garantizando la integridad de los mismos. Éste suele utilizarse en sistemas que no actúan en tiempo real ya que el tiempo que se pierde en el reenvío puede ser considerable y ser más útil emitir mal en el momento que correctamente un tiempo después. Esto se puede ver muy claro con una aplicación de videoconferencia donde no resulta de utilidad emitir el pixel correcto de la imagen 2 segundos después de haber visto la imagen.

Esta técnica de control de errores se basa en el reenvío de los paquetes de información que se detecten como erróneos (Esto quiere decir que no todos los paquetes de información se detectan como erróneos).

Para controlar la correcta recepción de un paquete se utilizan ACK's (acknowledge) y NACK's de forma que cuando el receptor recibe un paquete correctamente el receptor asiente con un ACK y si no es correcto responde con un NACK. Durante el protocolo que controla recepción de paquetes pueden surgir múltiples problemas (perdida de ACK, recibir un ACK incorrecto, etc.) complicándose así el contenido del ACK y surgiendo nuevos conceptos como el de timeout.

Si el emisor no recibe información sobre la recepción del paquete durante un tiempo fijo (timeout) éste se reenvía automáticamente.

1.1.5.3 Corrección Directa de Error (Forward Error Correction, FEC)

FEC (*Forward Error Correction*) es un tipo de mecanismo de corrección de errores que permite su corrección en el receptor sin retransmisión de la información original. Se utiliza en sistemas sin retorno o sistemas en tiempo real donde no se puede esperar a la retransmisión para mostrar los datos. Este mecanismo de corrección de errores se utiliza por ejemplo, en las comunicaciones vía satélite, en las grabadoras de DVD y CD.

La posibilidad de corregir errores se consigue añadiendo al mensaje original unos bits de redundancia. La fuente digital envía la secuencia de datos al codificador, encargado de añadir dichos bits de redundancia. A la salida del codificador obtenemos la denominada palabra código. Esta palabra código es enviada al receptor y éste, mediante el descodificador adecuado y aplicando los algoritmos de corrección de errores, obtendrá la secuencia de datos original. Los dos principales tipos de codificación usados son:

- Códigos bloque. La paridad en el codificador se introduce mediante un algoritmo algebraico aplicado a un bloque de bits. El descodificador aplica el algoritmo inverso para poder identificar y, posteriormente corregir los errores introducidos en la transmisión.
- Códigos convolucionales. Los bits se van codificando tal y como van llegando al codificador. Cabe destacar que la codificación de uno de los bits está enormemente influenciada por la de sus predecesores. La descodificación para este tipo de código es compleja ya que en principio, es necesaria una gran cantidad de memoria para estimar la secuencia de datos más probable para los bits recibidos.

FEC reduce el número de transmisiones de errores, así como los requisitos de potencia de los sistemas de comunicación e incrementa la efectividad de los mismos evitando la necesidad del reenvío de los mensajes dañados durante la transmisión.

1.2 Dispositivos en redes inalámbricas

1.2.1 Bridge

Un puente o bridge es un dispositivo de capa 2 diseñado para crear dos o más segmentos LAN, cada uno de ellos con un dominio de colisión separado con la finalidad de crear un ancho de banda más utilizable.

El objetivo de un puente es filtrar el tráfico de la LAN, para mantener el tràfico local, permitiendo la conectividad con otros segmentos de la LAN para el tráfico que se dirige allí. Cada dispositivo de red tiene una dirección MAC, el puente

controla qué direcciones MAC tiene en cada lado y con base en dicha lista es capaz de diferenciar si se trata de tráfico local o no.

Al filtrar el tráfico únicamente fijándose en las direcciones MAC, el puente puede enviar rápidamente tráfico representando cualquier protocolo de capa de red, es decir, no se preocupan por los protocolos de capa de red, solo en las tramas que pasan y por ende en la dirección MAC destino.

Las propiedades más importantes de los puentes son:

- Pueden analizar las tramas que llegan y enviarlas con base en la información de la dirección.
- Recogen y pasan paquetes entre dos o más segmentos LAN.
- Crean más dominios de colisión, logrando así, que más de un dispositivo pueda retransmitir simultáneamente sin provocar una colisión.
- Mantienen las tablas de dirección.

1.2.2 Hub

En general, el término Hub se emplea en lugar de repetidor cuando se refiere al dispositivo que actúa como centro de la red. El propósito de un hub es regenerar y reenviar señales de red, esta acción se conoce como concentración.

Dentro de las propiedades más importantes de los hubs están:

- Regenerar y repetir señales.
- Propagar las señales de red.
- No pueden filtrar el tráfico de la red.
- No pueden determinar la mejor ruta.
- Se utilizan como puntos de concentración de la red.

Los hubs se consideran dispositivos de capa 1 porque sólo regeneran la señal y la repiten en todos los puntos, característica que también marca la diferencia entre ellos y los repetidores.

1.2.3 Puntos de Acceso, AP

Son los encargados de recibir la información de las diferentes tarjetas de red de las que conste la red ya sea para su centralización o bien para su encaminamiento.

1.2.4 Switch

Un switch es un dispositivo de capa 2. Todas sus decisiones las toma con base en las direcciones MAC logrando así, que la LAN sea mucho más eficiente; esto lo consiguen conmutando los datos fuera del puerto al que el propio host está conectado.

El propósito de un switch es concentrar la conectividad mientras crea una transmisión de datos más eficiente. Conmuta las tramas de los puertos entrantes a los puertos salientes mientras proporciona a cada puerto un ancho de banda completo.

1.2.5 Router

El router es un dispositivo de capa 3, toma sus decisiones basándose en las direcciones de red, al contrario de las direcciones MAC de capa 2.

El propósito de un router es examinar los paquetes entrantes, elegir la mejor ruta para ellos a través de la red y conmutarlos al mejor puerto de salida. Los routers utilizan un esquema de direcciones diferente al de la capa 3 para tomar decisiones de envío, utilizan direcciones de capa de red, también llamadas Protocolo Internet (IP), o direcciones lógicas; equiparan la información de las tablas de enrutamiento con las direcciones IP de destino de los datos, y envían los datos entrantes hacía la subred y host correctos.

2

Tecnologías en redes inalámbricas

Introducción

En los últimos diez años se han incrementado considerablemente las opciones de comunicación inalámbricas tanto para la prestación de servicios de telecomunicaciones como para otras aplicaciones. Esto es el resultado de la digitalización y la rapidez con la que han evolucionado las técnicas de utilización de las frecuencias mediante mecanismos más eficientes para la transmisión de la información. Por ejemplo, el espectro disperso, es una técnica que consiste en el esparcimiento de la potencia de las señales que contienen información en un ancho de banda mucho mayor que el ancho de banda original de las señales de información mismas, lo cual permite que las comunicaciones sean más difíciles de interceptar y con esto más seguras y confiables y por otro lado, maneja una mejor relación señal a ruido que por consiguiente resulta en comunicaciones de mayor calidad. Otra técnica importante es la de multiplexaje por división ortogonal de frecuencia (*OFDM* por sus siglas en inglés), diseñada para minimizar la interferencia o diafonía entre canales y símbolos, comprimiendo el tren de datos. Con OFDM una señal es dividida en varios canales de banda angosta a diferentes frecuencias. La técnica de espectro disperso, OFDM y otras técnicas más avanzadas han hecho posible la fabricación de diversos equipos, dispositivos y sistemas que se integran a la infraestructura de telecomunicaciones y permiten el despliegue de redes inalámbricas de acceso y transporte más robustas.

En las redes inalámbricas se encuentran dispositivos de diversas tecnologías como *Bluetooth*, *Wi-Fi (Wireless Fidelity)*, *Home RF*, e incluso sistemas de comunicaciones de área amplia como *WIMAX*, con características punto a punto y multipunto que también se utilizan en las redes de transporte enlaces denominados "*Unlicensed National Information Infrastructure (U-NII)*" o "*High Performance LAN (Hiperlan*)".

Es importante mencionar que el desarrollo y las aplicaciones de las tecnologías antes mencionadas giran en torno a las dos primeras capas del modelo OSI (Figura 15), esto es, la capa física y la capa de enlace de datos.

Fig. 15 Modelo OSI

Sistemas como los que se describen en el párrafo anterior, especificamente Wi-Fi, pueden incrementar su potencia en enlaces punto a punto o multipunto cuando se utilizan antenas altamente directivas, dando paso a los bridges inalámbricos, que si bien no están definidos en el estándar 802.11, son una alternativa atractiva desarrollada por varias compañías. La característica básica que diferencía una tecnología de otra es el rango de cobertura. Hasta el momento se tienen 3 categorías básicas: de *Área Personal* (*Bluetooth),* de *Area Local (Wi-Fi)* y de *Área Metropolitana (WIMAX).* Debido a las necesidades y requerimientos del Instituto de Ingeniería la tecnología que satisface los mismos es Wi-Fi, como consecuencia se abordará con mayor profundidad el tema relacionado con la misma con la finalidad de tener las herramientas necesarias para la implantación y manejo de la red inalámbrica que demanda el Instituto.

2.1 Bluetooth

Es la norma que define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales

Funciona a través de una banda disponible a nivel global y mundialmente compatible de corto alcance en un mismo espacio físico, con un alcance máximo de 10 metros entre cada dispositivo que posea esta tecnología.

La tecnología Bluetooth (véase logotipo en la fig. 15) comprende hardware, software y requerimientos de interoperabilidad, por lo que para su desarrollo ha sido necesaria la participación de los principales fabricantes de los sectores de las telecomunicaciones y la informática, tales como: Ericsson, Nokia, Toshiba, IBM, Intel y otros. Posteriormente se han ido incorporando muchas más compañías, y se prevé que próximamente los hagan también empresas de sectores variados.

2.1.1 Antecedentes

En 1994 Ericsson inició un estudio para investigar la viabilidad de una interfase vía radio, de bajo costo y bajo consumo, para la interconexión entre teléfonos móviles y otros accesorios con la intención de eliminar cables entre aparatos. El estudio partía de un largo proyecto que investigaba sobre multi-comunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance, llamado *MC link.* Conforme éste proyecto avanzaba se fue viendo claro que éste tipo de enlace podía ser utilizado ampliamente en un gran número de

aplicaciones, ya que tenia como principal virtud el que se basaba en un chip de radio relativamente económico.

2.1.1.1 SIG (Special Interest Group)

A comienzos de 1997, según avanzaba el proyecto MC link, Ericsson fue despertando el interés de otros fabricantes de equipos portátiles. Se vió que para que el sistema tuviera éxito, un gran número de equipos deberían estar equipados con ésta tecnología.

El proyecto Bluetooth nace en febrero de 1998 de la mano de compañias como: Ericsson, Nokia, IBM, Toshiba e Intel; quienes fundaron el Grupo Bluetooh SIG (Special Interest Group) y se hizo público en mayo de ese mismo año. La idea era lograr un conjunto adecuado de áreas de negocio, dos líderes del mercado de las telecomunicaciones, dos líderes del mercado de los PCS portátiles y un líder de la fabricación de chips. El propósito principal del consorcio fue y es, el establecer un standard para la *interface* aérea junto con su software de control, con el fin de asegurar la interoperabilidad de los equipos entre los diversos fabricantes.

2.1.2 Descripción del programa Bluetooth

2.1.2.1 Escenarios de uso

Bluetooth puede ser usado en diversos escenarios y en cada uno provee ventajas al usuario.

- Sincronización de dispositivos cuando se encuentran próximos, ofreciendo facilidad para mantener actualizadas bases de datos de distintos dispositivos y compartir datos comunes (Figura 16).
- Auriculares inalámbricos. Se puede acceder a laptops o al teléfono celular y realizar llamadas con la posibilidad de manos libres (Figura 17).

Fig. 16 Sincronización de dispositivos

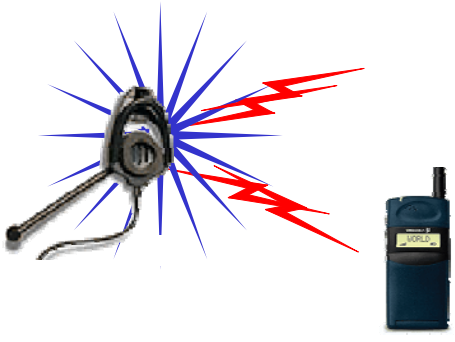


Fig. 17 Dispositivos inalámbricos

- Puntos de acceso a otras redes como LAN's o Internet, estableciendo conexiones remotas (Figura 18).

Fig. 18 Conexiones remotas

2.1.2.2 Banda de frecuencia libre

Para poder operar en todo el mundo es necesaria una banda de frecuencia abierta a cualquier sistema de radio independientemente del lugar del planeta donde nos encontremos. Sólo la banda ISM (Industrial y científico-médica), que va de los 2.400Mhz a los 2.485Mhz cumple con esto y solo, con algunas restricciones en países como Francia, España y Japón.

2 .1.2.3 Salto de frecuencia

Debido a que la banda ISM está abierta a cualquiera, el sistema de radio Bluetooth deberá estar preparado para evitar las múltiples interferencias que se pudieran producir. Éstas pueden ser evitadas utilizando un sistema que busque una parte no utilizada del espectro o un sistema de salto de frecuencia (Frequency Hopping, FH). En los sistemas de radio Bluetooth se utiliza el método de salto de frecuencia debido a que ésta tecnología puede ser integrada en equipos de baja potencia y bajo costo.

2.1.2.4 Definición de canal

Bluetooth utiliza un sistema FH/TDD (Frequency Hopping/Time Division Duplexing), en el que el canal queda dividido en intervalos de 625µs, llamados slots, donde cada salto de frecuencia es ocupado por un spot (Figura 19). Esto da lugar a una frecuencia de salto de 1600 veces por segundo, en la que un paquete de datos ocupa un slot para la emisión y otro para la recepción y que pueden ser usados alternativamente, dando lugar a un esquema de tipo TDD.

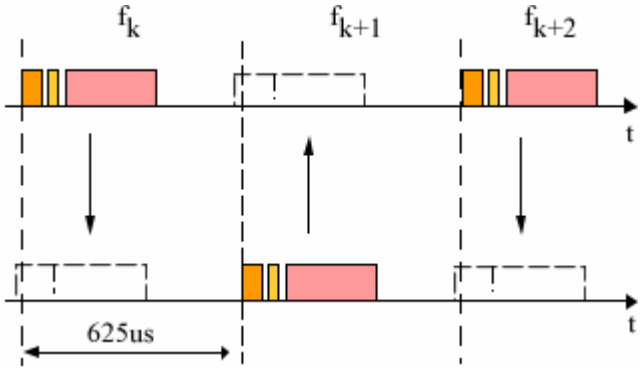


Fig. 19 Sistema FH/TDD

En países donde la banda está abierta a 80 canales o más, espaciados todos ellos a 1Mhz., se han definido 79 saltos de portadora, y en aquellos donde la banda es más estrecha se han definido 23 saltos.

2.1.2.5 Definición de paquete

La información que se intercambia entre dos unidades Bluetooth se realiza mediante un conjunto de slots que forman un paquete de datos. Cada paquete comienza con un código de acceso de 72 bits, que se deriva de la identidad maestra, seguido de un paquete de datos de cabecera de 54 bits. Éste contiene importante información de control, como tres bits de acceso de dirección, tipo de paquete, bits de control de flujo, bits para la retransmisión automática de la pregunta, y chequeo de errores de campos de cabeza. Finalmente, el paquete que contiene la información, que puede seguir al encabezado, tiene una longitud de 0 a 2745 bits (Figura 20). En cualquier caso, cada paquete que se intercambia en el canal está precedido por el código de acceso.

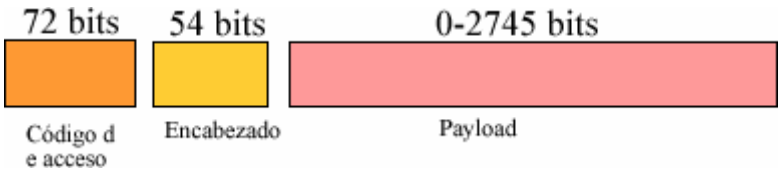


Fig. 20 Formato general para un paquete de datos

2.1.3 Topologia de una Red Bluetooth

2.1.3.1 Piconets

Si un equipo se encuentra dentro del radio de cobertura de otro, éstos pueden establecer conexión entre ellos. Cuando dos o más dispositivos Bluetooth son conectados, esto es, que comparten un mismo canal, forman una red dinámica llamada *Piconet* donde un dispositivo es el maestro y regula el tráfico en el canal mientras el resto, alrededor de 7 dispositivos, son los esclavos. Cuando se solapan las Piconets forman lo que se denomina una *Scatternet*. Cabe destacar que en cada Piconet sólo un dispositivo puede ser designado como maestro, sin

embargo, los esclavos pueden ser registrados en otras redes piconet. Con esto la capacidad de una Piconet es de 1Mbit/s.
Las unidades maestras tienen la capacidad para reservar slots en los enlaces SCO y para los enlaces ACL, se utiliza un esquema de sondeo. A una esclava sólo se le permite enviar un slot a un maestro cuando ésta se ha dirigido por su dirección MAC en el procedimiento de slot maestro-esclavo. Éste tipo de slot implica un sondeo por parte del esclavo, por lo que, en un tráfico normal de paquetes, este es enviado a una urna del esclavo automáticamente. Si la información del esclavo no está disponible, el maestro puede utilizar un paquete de sondeo para sondear al esclavo explícitamente. Los paquetes de sondeo consisten únicamente en uno de acceso y otro de cabecera. Éste esquema de sondeo central elimina las colisiones entre las transmisiones de los esclavos.

2.1.3.1.1 Estableciendo conexión

Para establecer la piconet, la unidad maestra debe conocer la identidad del resto de unidades que están en modo standby en su radio de cobertura. El maestro transmite el código de acceso continuamente en periodos de 10ms, que son recibidas por el resto de unidades que se encuentran en *standby.* El tren de 10ms de códigos de acceso de diferentes saltos de portadora, se transmite repetidamente hasta que el receptor responde o bien se excede el tiempo de respuesta.

Cuando una unidad emisora y una receptora seleccionan la misma portadora de salto, la receptora recibe el código de acceso y devuelve una confirmación de recibo de la señal, es entonces cuando la unidad emisora envía un paquete de datos que contiene su identidad y frecuencia de reloj actual. Después de que el receptor acepta éste paquete, ajustará su reloj para seleccionar el canal de salto correcto determinado por emisor. De éste modo se establece una piconet en la que la unidad emisora actúa como maestra y la receptora como esclava (Figura 21). Después de haber recibido los paquetes de datos con los códigos de acceso, la unidad maestra debe esperar un procedimiento de requerimiento por parte de las esclavas, para poder seleccionar una unidad específica con la que comunicarse.

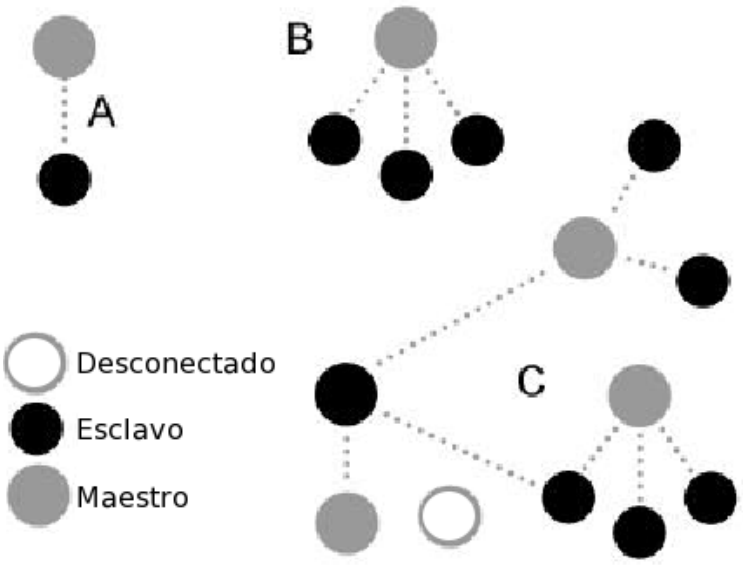


Fig. 21 A) una conexión simple entre dos dispositivos Bluetooth Maestro y Esclavo llamada piconet; B) multiconexión del Maestro con varios Esclavos; C) conexiones entre piconets (solapamiento) produciendo lo que se denomina una Scatternet.

2.1.3.1.2 Comunicación interpiconet

En un conjunto de varias piconets, éstas seleccionan diferentes saltos de frecuencia y están controladas por diferentes maestros, por lo que si un mismo canal de salto es compartido temporalmente por piconets independientes, los paquetes de datos podrán ser distinguidos por el código de acceso que les precede, que es único en cada piconet.

La sincronización de varias piconets no está permitida en la banda ISM. Sin embargo, las unidades pueden participar en diferentes piconets con base en un sistema TDM (división de tiempo múltiplexada). Esto es, una unidad participa secuencialmente en diferentes piconets, a condición de que ésta esté sólo activa en una al mismo tiempo. Cuando una unidad abandona una piconet, la esclava informa el maestro actual que ésta no estará disponible por un determinado periodo, que será en el que estará activa en otra piconet. Durante su ausencia, el tráfico en la piconet entre el maestro y otros esclavos continúa igualmente.

De la misma manera que una esclava puede cambiar de una piconet a otra, una maestra también lo puede hacer, con la diferencia de que el tráfico de la piconet se suspende hasta la vuelta de la unidad maestra. La maestra que entra en una nueva piconet, en principio, lo hace como esclava, a no ser que posteriormente ésta solicite actuar como maestra.

2.1.3.2 Scatternet

Los equipos que comparten un mismo canal sólo pueden utilizar una parte de su capacidad de este. Aunque los canales tienen un ancho de banda de un 1Mhz, cuantos más usuarios se incorporan a la piconet, disminuye la capacidad hasta unos 10 kbit/s más o menos. Teniendo en cuenta que el ancho de banda medio disponible es de unos 80 Mhz en Europa y USA (excepto en España y Francia), éste no puede ser utilizado eficazmente, cuando cada unidad ocupa una parte del mismo canal de salto de 1Mhz. Para poder solucionar éste problema se adoptó una solución de la que nace el concepto de scatternet (Figura 22).

Las unidades que se encuentran en el mismo radio de cobertura pueden establecer potencialmente comunicaciones entre ellas. Sin embargo, sólo aquellas unidades que realmente quieran intercambiar información comparten un mismo canal creando la piconet. Éste hecho permite que se creen varias piconets en áreas de cobertura superpuestas. A un grupo de piconets se le llama scatternet. El rendimiento, en conjunto e individualmente de los usuarios de una scatternet es mayor que el que tiene cada usuario cuando participa en un mismo canal de 1Mhz. Además, estadísticamente se obtienen ganancias por multiplexión y rechazo de canales salto. Debido a que individualmente cada piconet tiene un salto de frecuencia diferente, diferentes piconets pueden usar simultáneamente diferentes canales de salto.

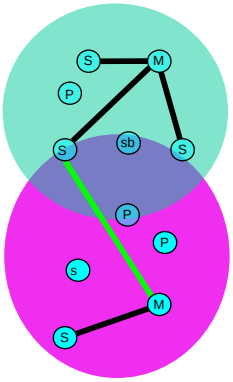


Fig. 22 Solapamiento entre dos piconets

2.1.4 Descripción General de la Arquitectura de Bluetooth

Cada dispositivo Bluetooth contiene un chip transistor, diseñado para un bajo consumo energético y con un corto alcance de rango de 10 metros. Ideal para redes inalámbricas personales de corto alcance, usa la banda frecuencia libre de licencias que oscila entre los 2.402 Ghz y 2.480 Ghz.

Bluetooth soporta transmisión de voz y datos. Los canales de voz admiten transferencias de hasta 64Kbs. Para las transmisiones asimétricas, es decir, de datos, es de 721Kbs en emisión y 57.6Kbs en recepción.

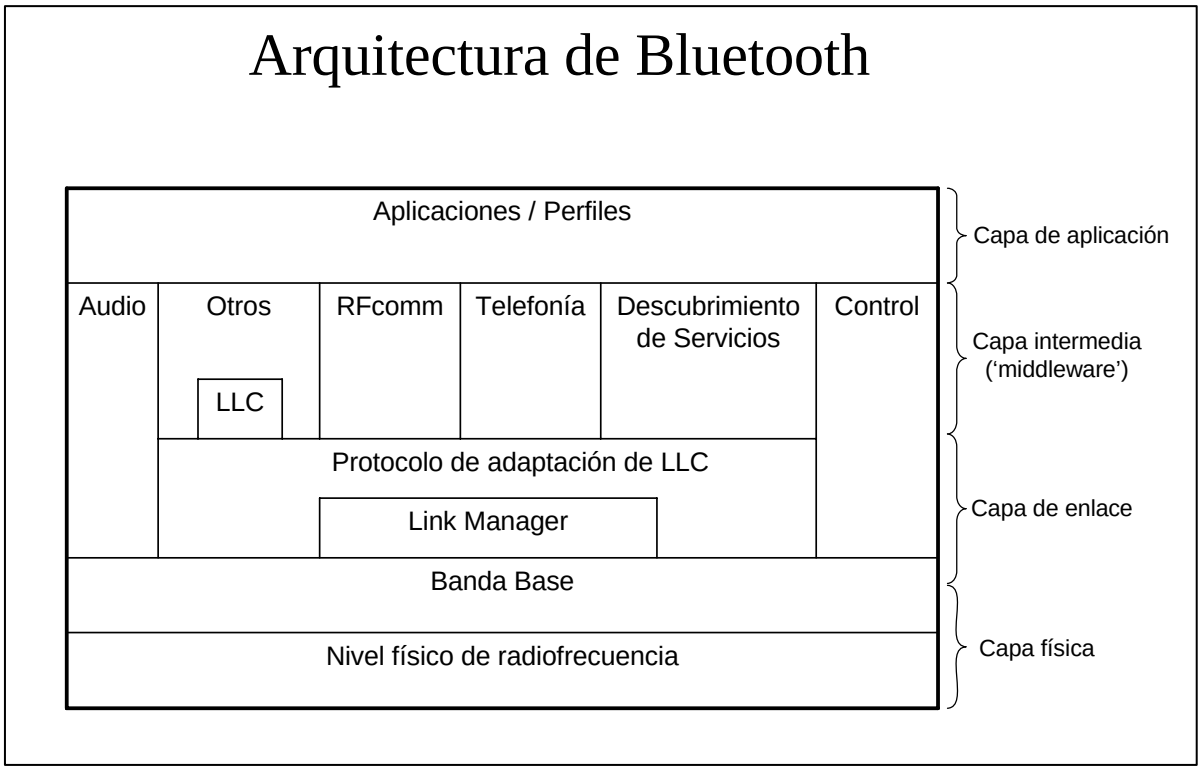


Fig. 23 Arquitectura Bluetooth

Dentro de la tecnología Bluetooth cada dispositivo consiste en tres componentes tecnológicos:

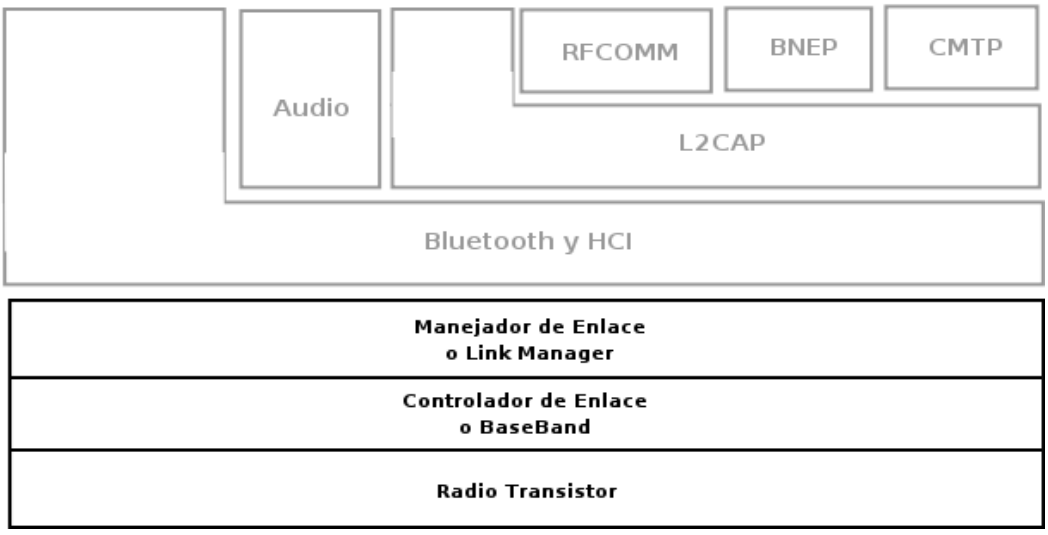


Fig. 24 Componentes de Bluetooth

2.1.4.1 Radio Transistor

Trasmisor y receptor de señales análogas de radio (Figura 24).

Características:

- Bajo consumo energético 1mW,
- Además sus ondas de radio no son dañinas para el corazón.

2.1.4.2 Protocolo Bandabase

Controlador de enlace: Link Controller ó BaseBand. Protocolo que controla y supervisa el establecimiento de una comunicación; controla en enlace; el control de errores; la autentificación y el control de acceso (Figura 24).

Esta capa es la encargada del control de la capa más baja o de Radio Transistor, y el procesamiento de los datos para prepararlos para ser manejados por la capa superior.

Las principales tareas de ésta capa son:

- Administración de la capa de enlace físico (radio transistor) a través del algoritmo de saltos.
- Empaquetar y Desempaquetar los datos.
- Corrección transparente de errores.
- Envío y Recepción de datos.
- Administración de enlaces lógicos y manejo de direcciones de hardware.
- Comunicaciones de Audio y Voz.
- Seguridad de datos, autentificación y cifrado.

2.1.4.2.1 Potencia

El consumo de potencia varia de acuerdo al modo de operación en que se encuentre. A continuación se presenta una tabla de valores según el estado del dispositivo para su respectivo consumo energético.

Estado	Consumo Energético	Tiempo Operativo
Standby	0.3mA	3 Meses
Transferencia de Audio	8 – 30mA	75 horas
Transferencia de Datos	0.3 – 30mA	120 horas

Tabla 2. Valores de potencia

El acoplamiento básicamente consiste en que el maestro pregunta a los esclavos si desean realizar un envío de paquetes y éste controla el tráfico de

datos en la piconet que se genera entre las demás unidades esclavas, enviando y recibiendo señales hacia el maestro.

2.1.4.2.2 Control de errores

Los paquetes de datos están protegido por un esquema **ARQ** (repetición automática de consulta), en el cual los paquetes perdidos son automáticamente retransmitidos, aun así, con este sistema, si un paquete de datos no llegase a su destino, sólo una pequeña parte de la información se perdería. La voz no se retransmite nunca, sin embargo, se utiliza un esquema de codificación muy robusto. Éste esquema, que está basado en una modulación variable de declive delta (CSVD), que sigue la forma de la onda de audio y es muy resistente a los errores de bits. Estos errores son percibidos como ruido de fondo, que se intensifica si los errores aumentan.

2.1.4.3 Manejador de enlace

Link Manager Protocol. Empaqueta los datos y asegura la comunicación con cada nodo o dispositivo remoto. Es el encargado de establecer la conexión, entregar seguridad y la autentificación (Figura 24).

Es el encargado junto al HCI (*Host Controller Interface)* de la comunicación con las capas de más alto nivel.

El Manejador de enlace funciona con un procesador interno en el dispositivo Bluetooth y al comunicarse con las capas de más alto nivel entrega la familia de protocolos necesarios para la comunicación entre dispositivos.

2.1.5 Seguridad

Para asegurar la protección de la información se ha definido un nivel básico de cifrado, que se ha incluido en el diseño del chip de radio para proveer de seguridad en equipos que carezcan de capacidad de procesamiento, las principales medidas de seguridad son:

- Una rutina de pregunta-respuesta, para autentificación.
- Una corriente cifrada de datos.
- Generación de una clave de sesión (que puede ser cambiada durante la conexión).

Tres entidades son utilizadas en los algoritmos de seguridad: la dirección de la unidad Bluetooth, que es una entidad pública; una clave de usuario privada, como una entidad secreta; y un número aleatorio, que es diferente por cada nueva transacción.

2.1.5.1 Autenticación del dispositivo remoto

- Está basado en una llave de autenticación de 128 bits
- La autenticación puede realizarse en ambas direcciones.

2.1.5.2 Cifrado

- Utiliza un algoritmo de menos de 128 bits y,
- Afecta todo el tráfico en un enlace.

2.1.5.3 Inicialización

- Generación de la clave de inicio: Se calcula localmente en cada unidad aplicando el algoritmo E22 a un código PIN que está almacenado en memoria, la longitud del PIN puede ser distinta en cada dispositivo.

2.2 Wi-Fi

802.11 es un estándar de redes inalámbricas que ha sido desarrollado por el Instituto de Ingenieros Electrónicos y Eléctricos (IEEE) cuya especificación se consolidó en el año 1997. Actualmente y debido al gran desarrollo de las redes inalámbricas se está formando en el ámbito doméstico y empresarial como una alternativa muy atractiva y con ventajas importantes respecto al cableado.

En septiembre de 1999 salen a la luz el estándar **802.11b** que ofrece 11Mbps y el **802.11a** que ofrece 54Mbps, si bien los productos de la primera aparecieron en el mercado mucho antes.

La familia 802.11, hoy se encuentra compuesta por los siguientes estándares:

- **802.11a:** (5,1-5,2GHz, 5,2-5,3GHz, 5,7-5,8GHz), 54Mbps. OFDM: Multiplexación por división de frecuencias ortogonal.
- **802.11b:** (2,4-2,485GHz), 11Mbps.
- **802.11c**: Define la operación de puentes inalámbricos.
- **802.11d**: Este protocolo permite el uso de 802.11 en países restringidos por el uso de las frecuencias. Constituye un complemento al nivel de control de Acceso al Medio (MAC) en 802.11 para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11.
- **802.11e**: Su objetivo es proporcionar soporte de QoS (Calidad de Servicio) para aplicaciones de redes LAN y mejorar la eficiencia de los estándares físicos a, b y g de 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video. Acota el retraso máximo, acota un ancho de banda mínimo y acota la probabilidad máxima de perdida de paquetes. Utiliza 3 bits de prioridad (8 niveles).
- **802.11f**: Protocolo de conexión entre puntos de acceso (AP), protocolo IAPP: Inter Access Point Protocol. Su objetivo es lograr la interoperabilidad de Puntos de Acceso (AP) dentro de una red WLAN multiproveedor. El estándar define el registro e Puntos de Acceso (AP) dentro de una red y el intercambio de información entre dichos Puntos de Acceso cuando un usuario se traslada desde un punto de acceso a otro.
- **802.11g**: (2,4-2,485GHz), 36 o 54Mbps. OFDM: Multiplexación por división de frecuencias ortogonal. Aprobado en 2003 para dar mayor velocidad con cierto grado de compatibilidad a equipamiento 802.11b.
- **802.11h**: Superior al 802.11a permite la asignación dinámica de canales (coexistencia con HiperLAN). Regula la potencia en función de la distancia. El objetivo es cumplir los reglamentos europeos para redes WLAN a 5GHz. Los reglamentos europeos para la banda de 5GHz requieren que los productos tendrán control de la potencia de transmisión (TPC) y selección de frecuencia dinámica (DFS). El control TPC limita la potencia transmitida al mínimo necesario para alcanzar al usuario más lejano. DFS selecciona el canal de radio en el punto de

acceso para reducir al mínimo la interferencia con otros sistemas en particular el radar.

- **802.11i:** Este estándar intenta solucionar los problemas de seguridad que actualmente existen en las redes que utilizan el sistema WEP. En contra partida al WEP hace uso de un nuevo protocolo conocido como TKIP haciendo uso de un método de cifrado conocido como WPA. No obstante, solucionar rápidamente la seguridad a los dispositivos ya existentes era el primer objetivo. Esta solución es conocida como WPA2.
- **802.11j**: Permitiría armonización entre IEEE (802.11), ETSI (HiperLAN2) y ARIB (HISWANA). Este estándar permite la utilización de 802.11a en la banda de 4.9GHz japonesa.
- **802.11k:** Define información sobre la señal y la red para facilitar su administración. Proporciona información para descubrir el mejor Access Point disponible.
- **802.11m**: Este protocolo está propuesto para el mantenimiento de las redes inalámbricas actuales.
- **802.11n**: Nivel físico y de enlace de alta velocidad. Entre 108 y 320Mbps. Baja sobrecarga. Se estima que estará disponible en el 2007.
- **802.11p:** Define el acceso inalámbrico para vehículos.
- **802.11r**: Define transiciones rápidas (Fast roaming).
- **802.11s:** Define un protocolo de auto configuración entre Access Points en topologías multisalto.
- **802.11T:** Proporciona métodos de prueba y recomendaciones.
- **802.11u:** Interoperabilidad con redes no 802, por ejemplo, celular.
- **802.11v:** Define la administración de la red inalámbrica. Permite la configuración de los clientes mientras están conectados a redes 802.11
- **802.11w:** Define la protección y administración de los paquetes de la capa MAC.

Una iniciativa que se debe mencionar también es HiperLAN en sus versiones 1 y 2. Se trata de una verdadera analogía inalámbrica para ATM. Fue un competidor de 802.11 que opera en la frecuencia de 5GHz y gozó del apoyo de compañías como Ericsson, Motorola, Nokia; Panasonic y Sony, se llegaron a crear regulaciones por parte de ETSI al respecto, pero no se logró imponer y hoy en día está prácticamente en desuso.

2.2.1 Topología

Las redes Wi-Fi se construyen utilizando dos topologías básicas. Para estas topologías se utilizan distintos términos, como administradas y no administradas, alojadas y par a par, e infraestructura y "ad hoc".

2.2.1.1 Ad Hoc

La arquitectura Ad Hoc concierne a la comunicación punto a punto. Aquí una terminal móvil actúa como router y una o más terminales pueden realizar funciones de control, como la creación o eliminación de una comunicación entre nodos.

En esta topología los propios dispositivos (equipos con tarjeta de red inalámbrica) crean la red mediante la comunicaron entre tarjetas inalámbricas, no existiendo un controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red evitando pasar por un controlador central. Esta topología resulta práctica en lugares en los que pueden reunirse grupos pequeños de equipos que no requieran acceso a otra red. Como ejemplo de este tipo de entorno en los que es aplicable esta topología son un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con cierta frecuencia.

Todos los dispositivos que pertenecen a una WN utilizan un nombre de red para identificarse, así todos los dispositivos que quieran pertenecer a la misma WN deberán utilizar el mismo nombre y solo se podrá establecer comunicación con aquellos dispositivos que tengan asignado este mismo nombre o pertenezcan a la misma WN.

Una comunicación entre nodos vecinos solo será posible si dichos nodos se encuentran dentro del rango de transmisión. La comunicación entre nodos puede contener múltiples saltos, puede requerir de varios enlaces para alcanzar el destino; si un nodo está dentro del rango de transmisión de un nodo vecino pero, esté nodo vecino no es el destino final de la transmisión del paquete se presentan múltiples saltos a través de varios nodos hasta que se llega al nodo destino.

2.2.1.1.1 Descripción de operación

En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación (Figura 25). La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

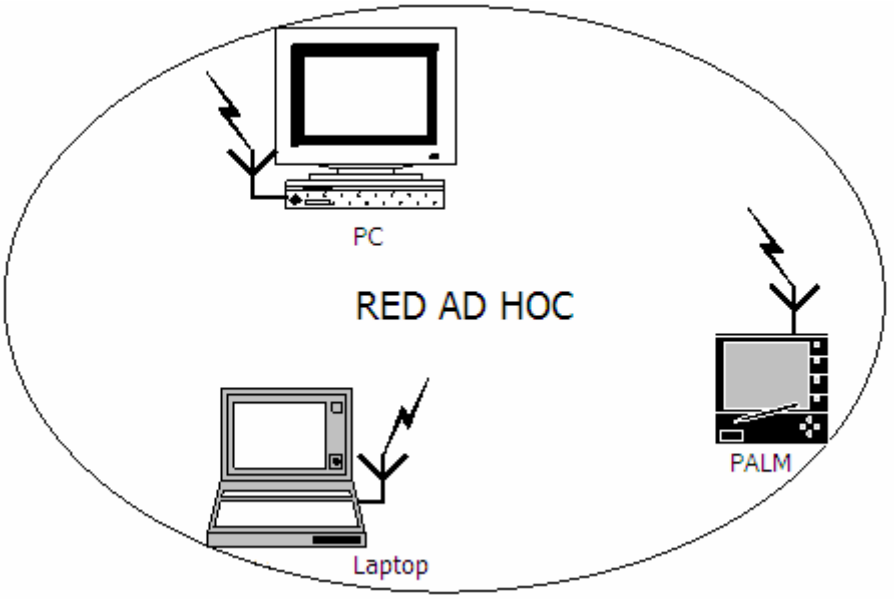


Fig. 25 Topología Ad Hoc

2.2.1.1.2 Enrutamiento en redes Ad Hoc

Los movimientos de los nodos causan que entren y salgan del rango de unos y otros nodos. Como resultado existe continuamente la creación y rompimiento de ligas (links) en la red, causando que la topología de la red varíe dinámicamente con el tiempo. Debido a esto uno de los temas más ampliamente investigado es el de los protocolos de enrutamiento, los cuales pueden ser clasificados dentro de 3 categorías básicas: (1) Protocolos Proactivos, (2) Protocolos Reactivos y (3) Protocolos Híbridos (Figura 26).

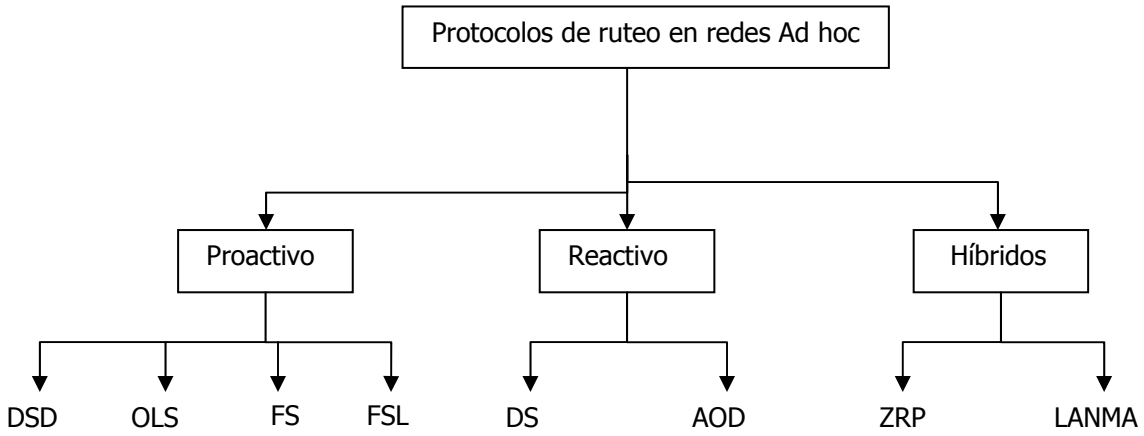


Figura 26. Protocolos de Ruteo

2.2.1.1.2.1 Protocolos Reactivos

Los protocolos Reactivos realizan las operaciones de ruteo entre todos los pares de nodos fuente-destino periódicamente independientemente si es necesario o no. Se basan en los algoritmos ***link-state*** y ***Distance-Vector,*** además

mantienen la ruta más corta en sus tablas de ruteo actualizándolas periódicamente. Tienen la ventaja de mantener un bajo retraso en la entrega de datos y la posibilidad de soportar aplicaciones que utilicen la calidad de servicio (QoS). Además trabajan bien bajo tráfico pesado y alta movilidad. Su principal desventaja es que consumen demasiado ancho de banda al mandar paquetes de actualización, aún cuando éstos no son necesarios.

2.2.1.1.2.2 Protocolos Proactivos

Estos protocolos rastrean la ruta sólo cuando es necesario. Típicamente, estos protocolos realizan el descubrimiento de la ruta cuando un nodo fuente necesita enviar paquetes a un destino que no conoce o cuando una trayectoria se rompe. La desventaja con esto, es que el descubrir una ruta puede involucrar a toda la red, además de que puede ser muy frecuente cuan exista alta movilidad o cuando haya un gran número de nodos fuente-destino. Es más, el descubrimiento de una ruta puede ocasionar retraso en el envío de paquetes ya que un nodo fuente tiene que esperar hasta que la ruta sea determinada.

2.2.1.1.2.3 Protocolos Híbridos

Estos protocolos usan una combinación de proactivos y reactivos, los cuales son aplicados bajo diferentes condiciones, lugares o regiones.

2.1.1.2 Infraestructura

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

2.1.1.2.1 Descripción de operación

El dispositivo inteligente, denominado "estación" en el ámbito de las redes inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red con cable o inalámbrica (Figura 27).

El acceso a la red se administra mediante el protocolo CSMA, que detecta las portadoras y evita las colisiones. Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

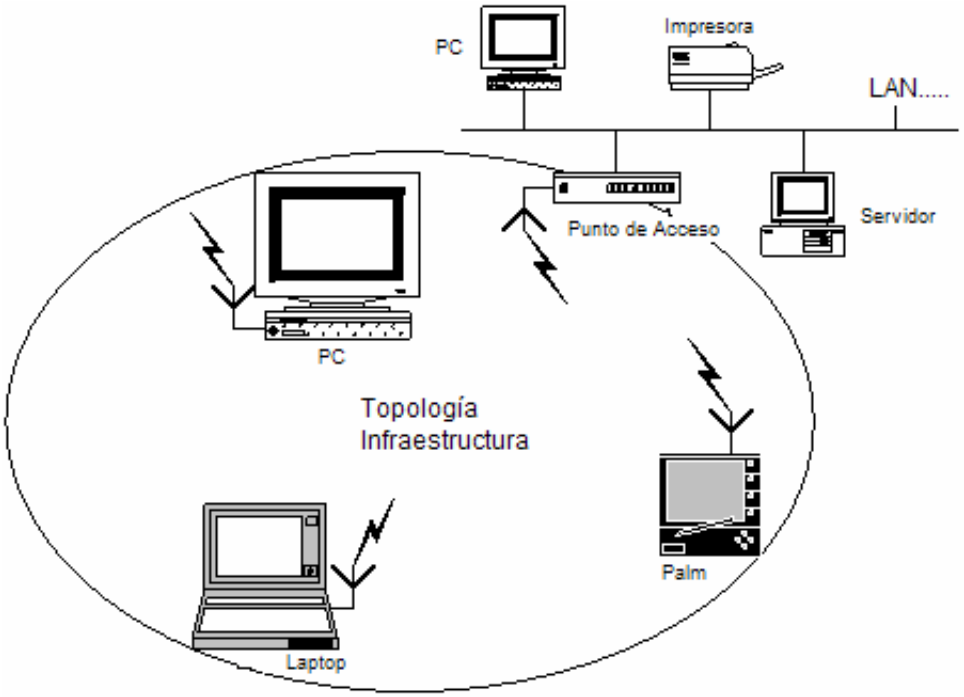


Figura 27. Topología Infraestructura

2.2.2 802.11. Capa Física

Para explicar la capa física es importante aclarar primeramente algunos conceptos:

- **Modulación**: Es el método de emplear una señal portadora y una moduladora (que da forma a la anterior). Cada una de ellas puede ser analógica o digital, con lo cual se obtienen cuatro posibles combinaciones de portadora y moduladora (AA – AD – DA y DD), con las cuales se conforman todas las técnicas de modulación. WiFi en la mayoría de los casos emplea la técnica QAM (Modulación en cuadratura de Fases con más de un nivel de amplitud).
- **Propagación**: Es la forma en la cual "van saliendo" las señales al aire. Aquí es donde verdaderamente se aplican las técnicas de DHSS y FHSS. SS (Spread Spectrum) es la técnica de emplear muchas subportadoras de muy baja potencia con lo cual se "expande" el espectro útil. En cuanto a DH y FH, el ejemplo típico que se emplea para estas técnicas es la analogía con una terminal de trenes, en la cual existen varios andenes. Para DH, los trenes estarían saliendo, primero el andén 1, luego el 2, a continuación el 3, 4, 5... y así sucesivamente, respetando siempre este orden. Para FH, la salida de los trenes no respeta el orden y puede ser aleatoria o acorde a un patrón determinado (WiFi hace un muy buen uso de esto, pues en las subportadoras que recibe mucha interferencia no las usa o emplea menos cantidad de bits en las mismas).
- **Codificación**: Es la asociación de bit a cada "muestra" que se obtiene. WiFi en la mayoría de los casos emplea el código Barker.

La norma 802.11 sigue el mismo modelo o arquitectura de toda la familia 802, es decir especifica la capa física y la subcapa MAC de la capa de enlace (Figura 28).

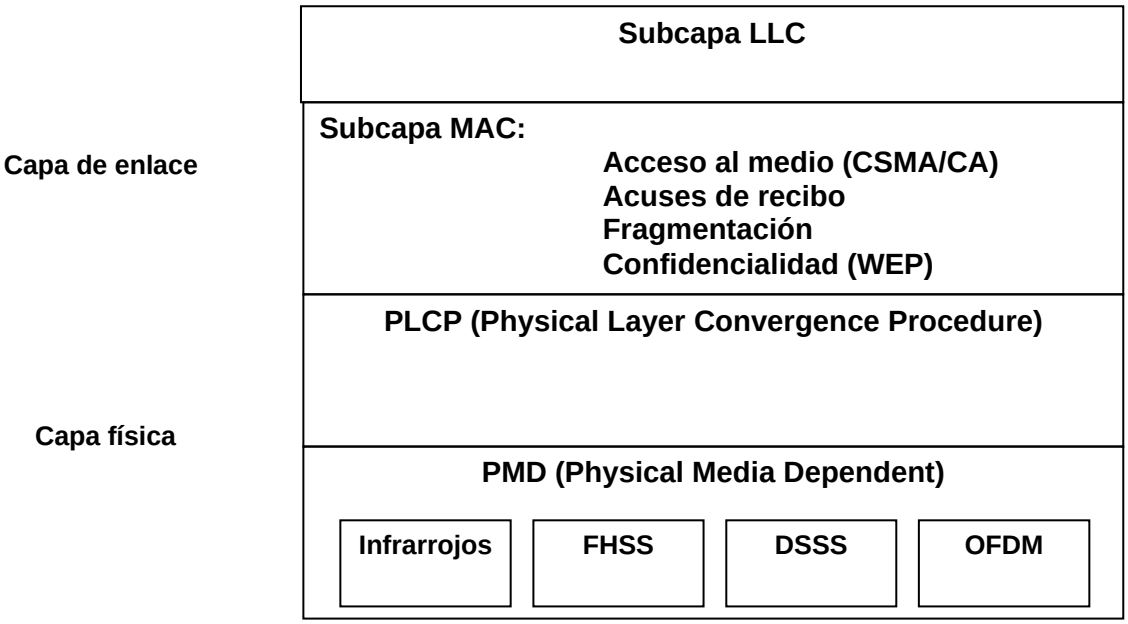


Figura 28. Arquitectura 802.11

La Capa Física de cualquier red define la modulación y la señalización características de la transmisión de datos. En la familia IEEE 802.11 se definen 4 posibles opciones para la elección de la capa física:

- La transmisión por infrarrojos en 802.11 es posible solo en distancias muy cortas (10-20m) y dentro de una misma habitación.

En cuanto a los sistemas de radio hay tres posibilidades, que difieren en la forma como manejan la banda de frecuencias disponible.

- El sistema más antiguo es el FHSS, que funciona a 2.4GHz. Este sistema ha caído en desuso, aunque existen equipos funcionando en muchas instalaciones.
- El DSSS también funciona a 2.4GHz, es más moderno y consigue un mayor rendimiento que FHSS. Es el más utilizado actualmente.
- OFDM es el sistema más moderno y de mayor rendimiento. Corresponde a los suplementos 802.11a/h de la norma y funciona en la banda de 5GHz.

Los medios físicos son incompatibles entre sí, por ejemplo un sistema de radio DSSS no puede comunicarse con uno OFDM pues la banda de radio es diferente (2.4 frente a 5GHz). Incluso FHSS y DSSS son incompatibles, aunque ambos

utilicen la misma banda de frecuencias, ya que organizan los canales de modos completamente diferentes.
Dentro de un mismo medio físico los equipos pueden interoperar, aunque no siempre puedan hacerlo con todas las posibilidades. Por ejemplo un equipo DSSS de segunda generación (802.11b) puede funcionar a 11, 5.5, 2 y 1Mb/s, pero si se comunica con un equipo DSSS de primera generación (802.11) solo podrá hacerlo a 2 o 1Mb/s.
La situación es similar a lo que ocurre en Ethernet, donde un equipo 1000/100/10BASE-T puede interoperar con otro de velocidad inferior, pero no con otro de diferente medio físico (por ejemplo no con uno 100BASE-F).

La mayor parte del espectro radioeléctrico está regulado por la ITU-R y se requiere licencia para emitir. Algunos países tienen normativas propias más restrictivas. Como no sería práctico pedir licencia para cada WLAN el IEEE decidió asignar para esto algunas de las bandas ISM (designadas para aplicaciones de tipo industrial-cientifico-médico, Industrial-Scientific-Medical). Algunas bandas ISM están restringidas a ciertas regiones.

- La banda de 900MHz solo está autorizada como no licenciada en la región 2 de la ITU, que corresponde a Estados Unidos y Canadá.
- La banda de 2.4GHz es la única que tiene aplicación en todo el mundo. Se utiliza en el estándar original 802.11 y en las extensiones 802.11b y 802.11g.
- La banda de 5GHz se utiliza en el estándar 802.11a. Actualmente el uso de este estándar solo está permitido en América, Japón, Singapur y Taiwán.
- La banda de 2.4GHz es la que tienen una mayor anchura de banda. Sin embargo no se utiliza porque los equipos para estas frecuencias son más caros y tienen menor alcance que los de 2.4 ó 5GHz

La capa física la componen dos subcapas:

- PLCP (Physical Layer Convergence Protocol): Se encarga de codificación y modulación. Es una función de convergencia, que adapta las capacidades del sistema físico dependiente del medio (PMD). Esta función define una forma de mapear MPDUs o unidades de datos MAC en un formato de tramas susceptibles de ser transmitidas o recibidas entre diferentes estaciones a través de la capa PMD.

- PMD (Physical Medium Dependence): Es la que crea la interfaz y controla la comunicación hacia la capa MAC (a través del SAP: Service Access Point). Define las características y un medio de transmitir y recibir a través de un medio sin cables entre dos o más estaciones.

2.2.2.1 Espectro Disperso

Dado que la banda de 2.4GHz está disponible sin licencia para todo el que desee emitir en ella, es preciso adoptar algunas precauciones que eviten una excesiva interferencia entre emisiones. Por este motivo se establece que cualquier emisión con una potencia superior a 1mW debe hacerse en espectro disperso. Hay dos formas de hacer una emisión de espectro disperso:

- Direct Sequence (secuencia directa).
- Frecuency Hopping (salto de frecuencia).

2.2.2.1.1 DSSS

Esta técnica, se basa en la generación de un patrón de bits redundante por cada uno de los bits que componen la señal de información y después esta señal se modula mediante una portadora de Radio Frecuencia. Para poder obtener la información de la señal, los receptores, deben realizar el proceso inverso. Se utiliza una secuencia de bits, para codificar cada uno de los bits, conocida como secuencia de Barker o código de dispersión (PseudoNoise), esta formada por 11 bits que tiene propiedades matemáticas que lo hacen ideal para modular radiofrecuencias. El código Barker genera series de objetos de datos llamados chips. Cada bit se codifica y transmite por la secuencia de Barker de 11bits y cada grupo de 11 chips codifica 1 bit de datos. Es una secuencia rápida diseñada para que aparezca la misma cantidad de 1 que de 0 aproximadamente.
La secuencia de bits utilizada para modular cada uno de los bits de información es la llamada secuencia Barker y tiene la siguiente forma:

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

Para generar la secuencia transmitida, se realiza una operación lógica "XOR" entre los datos de usuario y el Código, como se muestra en la siguiente figura:

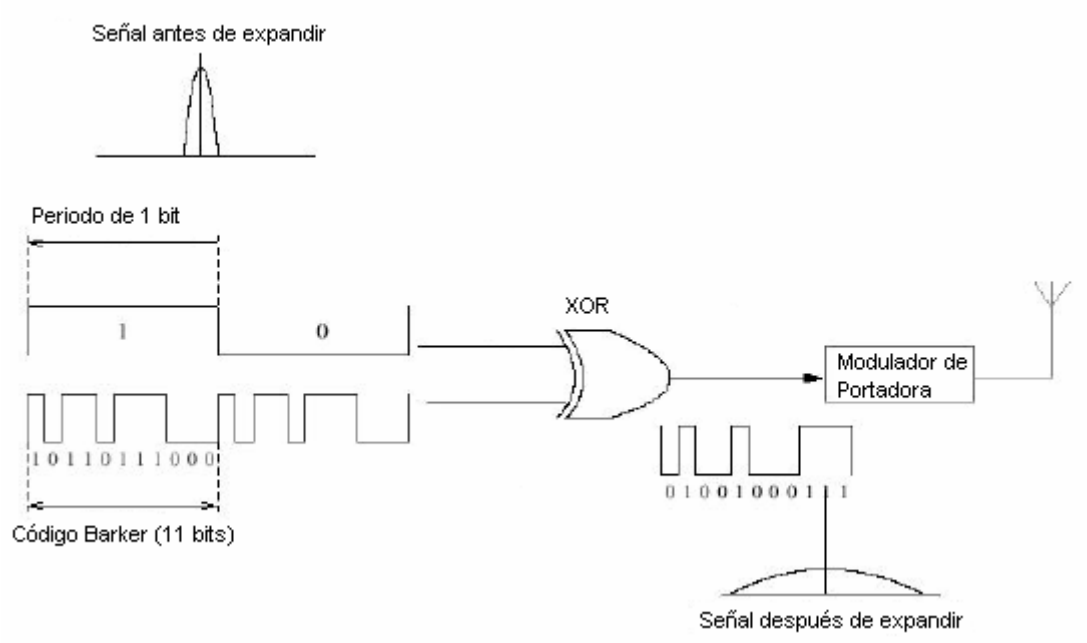


Figura 29. Generación de secuencia transmitida

DSSS tiene definidos dos tipos de modulaciones una vez que se sobrepone a la señal de *chip*: la modulación DBPSK (Differential Binary Phase Shift Keying) y la modulación DQPSK (Differential Quadrature Phase Shift Keying) proporcionando unas velocidades de transferencia de 1 y 2 respectivamente.

En el caso de Estados Unidos y de Europa la tecnología de espectro ensanchado por secuencia directa (DSSS) opera en el rango que va desde los 2.4GHz hasta los 2.4835GHz, es decir, con un ancho de banda total disponible de 83.5MHz. Este ancho de banda total se divide en un total de 14 canales de los cuales cada país utiliza un subconjunto de los mismos según las normas reguladoras para cada caso particular. En topologías de red que contengan varias celdas, ya sean solapadas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias en el sistema si la separación entre las frecuencias centrales es como mínimo de 30MHz. Esto significa que de los 83.5MHz de ancho de banda total disponible podemos obtener un total de 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 del sistema de 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.

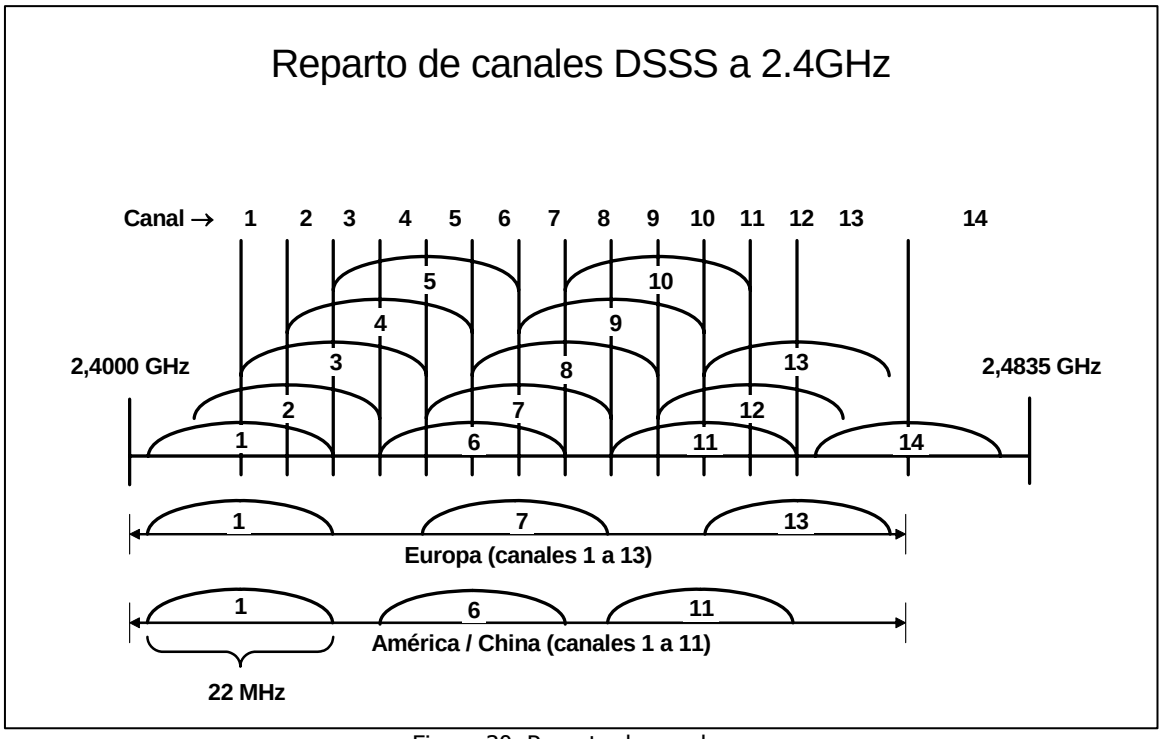


Figura 30. Reparto de canales

Esta figura muestra la división en canales de la banda de 2.4GHz para DSSS. Cada canal está desplazado 5MHz respecto al anterior (excepto el canal 14) y tiene una anchura de 22MHz, por lo que los canales contiguos se solapan. Si se requieren canales completamente separados en Europa se recomienda emplear el 1, el 7 y el 13. En América y China se deben utilizar el 1, el 6 y el 11 pues el 12, 13 y 14 no están permitidos.

En la siguiente figura se muestra una tabla expuesta en el estándar en donde se muestra la frecuencia central, los identificadores de canal (CHNL_ ID), así como los dominios: FCC (US), IC (Canadá), ETSI (Europa) y MKK (Japón). Se indica con una "X" los canales soportados por cada dominio.

		Regulatory domains					
CHNL_ID	Frequency	X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' MKK
1	2412 MHz	X	X	X	—	—	—
2	2417 MHz	X	X	X	—	—	—
3	2422 MHz	X	X	X	—	—	—
4	2427 MHz	X	X	X	—	—	—
5	2432 MHz	X	X	X	—	—	—
6	2437 MHz	X	X	X	—	—	—
7	2442 MHz	X	X	X	—	—	—
8	2447 MHz	X	X	X	—	—	—
9	2452 MHz	X	X	X	—	—	—
10	2457 MHz	X	X	X	X	X	—
11	2462 MHz	X	X	X	X	X	—
12	2467 MHz	—	—	X	—	X	—
13	2472 MHz	—	—	X	—	X	—
14	2484 MHz	—	—	—	—	—	X

Tabla 3. Frecuencia de los Canales

La máxima cantidad de Potencia permitida utilizando esta técnica es:

- USA: 1000mW.
- Europa: 100 mW.
- Japón: 10 mW/MHz

Siendo la cantidad de Potencia mínima de 1 mW.

Formato de la trama PLCP para DSSS:

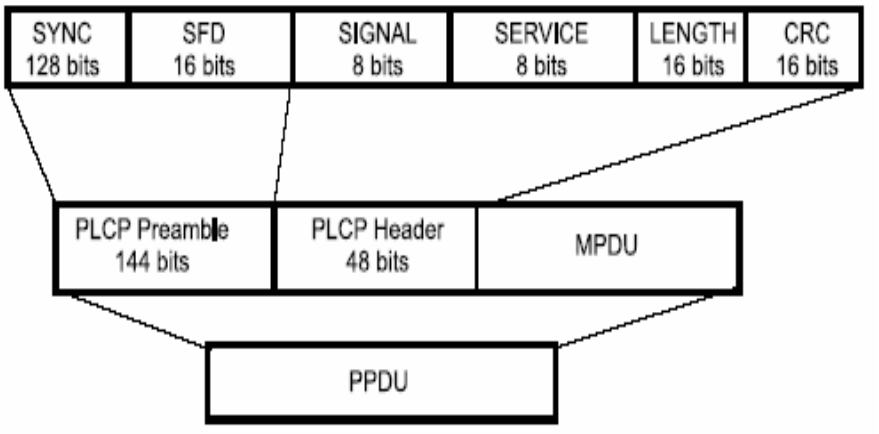


Figura 31. Formato de trama PLCP

- **SYNC:** contiene 128 bits para la sincronización.
- **SIGNAL:** indica modulación DBPSK o DQPSK.

- **LENGTH:** indica el número de microsegundos necesario para transmitir la trama MPDU.
- **SERVICE:** reservado para uso futuro.
- **SFD:** Delimitador de inicio de trama.
- **CRC:** trama para el control de errores.

2.2.2.1.2 FHSS

La tecnología de espectro ensanchado por salto en frecuencia consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada *dwell time* y debe ser inferior a 400ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo. El orden en los saltos en frecuencia que el emisor debe realizar viene determinado según una secuencia pseudoaleatoria que se encuentra definida en unas tablas que tanto el emisor como el receptor deben conocer. La banda de 2.4GHz se divide en 79 canales para USA y Europa, y 23 para Japón. Estos canales son contiguos no solapados de 1MHz de anchura cada uno.

Si se mantiene una correcta sincronización de estos saltos entre los dos extremos de la comunicación se mantiene un único canal lógico a través del cual se desarrolla la comunicación. Para un usuario externo a la comunicación la recepción de una señal FHSS equivale a la recepción de ruido impulsivo de corta duración. En caso de que un agente externo produzca una interferencia esta afectará a algún canal o canales en concreto; si alguna de las emisiones coincide con el canal interferido el receptor no podrá separar la señal del ruido y la trama no será recibida. En ese caso el emisor retransmitirá la trama, confiando que en el siguiente intento pueda realizarse la transmisión con éxito. El estándar IEEE 802.11 define esta tecnología utilizando la modulación en frecuencia FSK, Frequency Shift Keying, y con una velocidad de transferencia de 1Mbps ampliable a 2Mbps.

Formato de la trama PLCP para FHSS:

PLCP Preamble		PLCP Header			
Sync	Start Frame Delimiter	PLW	PSF	Header Error Check	Whitened PSDU
80 bits	16 bits	12 bits	4 bits	16 bits	Variable number of octets

Figura 32. Formato para trama PLCP para FHSS

Este nivel físico recibe la PDU de nivel 2 (es decir la trama MAC completa), arma su Header, lo suma a la PDU recibida y este conjunto es lo que se transmite por el medio inalámbrico. El conjunto total de bits que se inyectarán en el canal de comunicaciones, a través de este nivel se puede clasificar en tres grandes partes:

- **Preámbulo**: Se emplea para sincronizar la transmisión con todos los nodos que vayan a escucharla. Contiene dos campos:
  - Sincronización (SYNC) de 80 bits alternando ceros y unos.
  - Delimitador de inicio de trama (SFD) de 16 bits (0000 1100 1011 1101).
- **Header**: Contiene tres campos:
  - PLW (Physical Length Word): 12 bits que indican la longitud del campo de datos.
  - PSF (Physical Signaling Rate): 4 bits, de los cuales, el primero debe ser cero (Reservado), y las 9 combinaciones de los 3 bits siguientes indican a qué velocidad de transferencia de datos operará esta trama, desde 1 Mbps (000) hasta 4.5Mbps (111), incrementándose de 0.5Mbps.
  - HEC (Header Error Check): 16 bits que emplean la técnica de CRC con el polinomio Generador $G(x) = X^{16} + X^{12} + X^5 + 1$.

- **Datos**: PDU de nivel 2. Cabe destacar aquí que en este nivel, los datos se organizan en bloques de 127 bits, que se irán mezclando en filas y columnas para minimizar los efectos de ráfagas de errores que puedan sufrir en el medio inalámbrico.

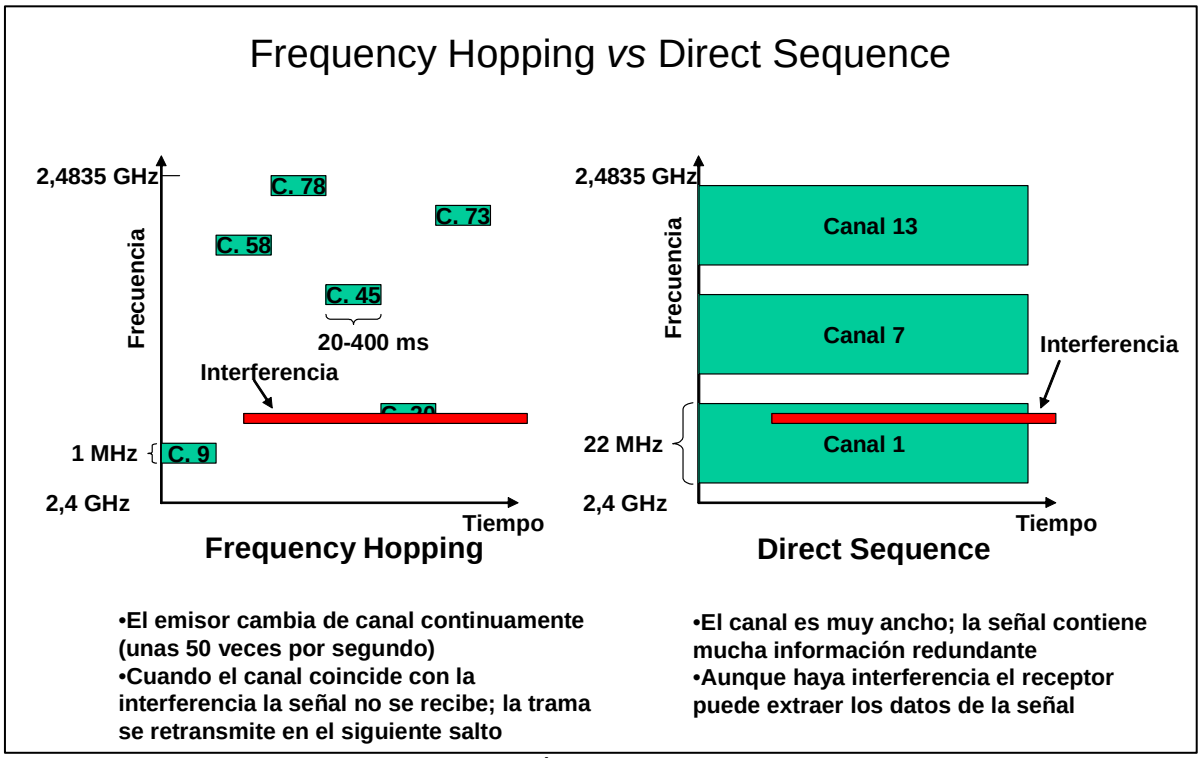


Figura 33. Comparación en Frecuencia FH vs. DS

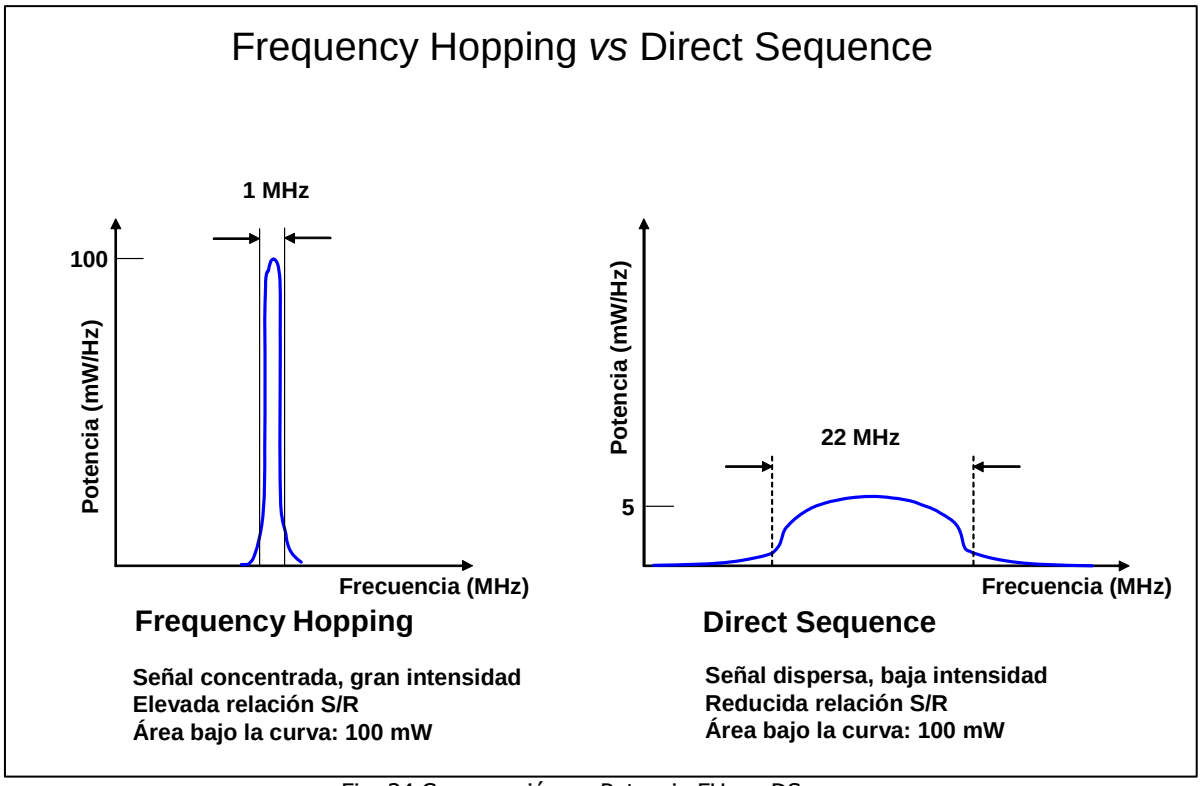


Fig. 34 Comparación en Potencia FH vs. DS

Esta figura trata de explicar de forma simplificada la diferencia entre Frequency Hopping y Direct Sequence. En el caso de FH toda la potencia de emisión (100mW) se concentra en una franja estrecha del espectro, mientras que en DS se reparte en un rango mucho más amplio. Sin embargo la potencia emitida en ambos casos es similar (en el ejemplo los 100mW máximos permitidos en Europa).

En el caso de FH tenemos una señal de banda estrecha pero de gran intensidad, lo cual da una elevada relación señal/ruido. De acuerdo con el teorema de Nyquist un canal estrecho nos permite enviar pocos baudios, pero de acuerdo con la ley de Shannon la elevada relación señal/ruido permitirá enviar muchos bits por baudio.
En el caso de DS tenemos una señal de banda ancha pero de baja intensidad, lo cual nos dará una relación señal/ruido pequeña. Según el teorema de Nyquist tenemos ahora posibilidad de enviar muchos baudios, pero la ley de Shannon nos dice que con una relación señal/ruido pequeña podremos enviar pocos bits por baudio.

2.2.2.1.3 Tecnología de infrarrojos

Una tercera tecnología, de momento no demasiado utilizada a nivel comercial para implementar WLANs, es la de infrarrojos. Los sistemas de infrarrojos se sitúan en altas frecuencias, justo por debajo del rango de frecuencias de la luz visible. Las propiedades de los infrarrojos son, por tanto, las mismas que tiene la luz visible. De esta forma los infrarrojos no pueden pasar a través de objetos opacos pero se pueden reflejar en determinadas superficies. Las longitudes de

onda de operación se sitúan alrededor de los 850-950nm, es decir, a unas frecuencias de emisión que se sitúan entre los $3{,}15x10^{14}$ Hz y los $3.52x10^{14}$ Hz. Los sistemas que funcionan mediante infrarrojos se clasifican según el ángulo de apertura con el que se emite la información en el emisor en:

- Sistemas de corta apertura, de haz dirigido o de visibilidad directa que funcionan de manera similar a los mandos a distancia de los aparatos de televisión. Esto supone que el emisor y el receptor tienen que estar orientados adecuadamente antes de empezar a transmitirse información.
- Sistemas de gran apertura, reflejados o de difusión que radian tal y como lo haría una bombilla, permitiendo el intercambio de información en un rango más amplio.

La norma IEEE 802.11 especifica dos modulaciones para esta tecnología: la modulación 16ppm y la modulación 4ppm proporcionando unas velocidades de transmisión de 1 y 2 Mbps respectivamente. Esta tecnología se aplica típicamente en entornos de interior para implementar enlaces punto a punto de corto alcance o redes locales en entornos muy localizados como puede ser una aula concreta o un laboratorio.

2.2.2.2 Interferencias

- Externas:
  - Bluetooth transmite a 2.4GHz por FHSS. Interfiere menos con DSSS. Nada con 802.11a (5GHz).
  - Los hornos de microondas (funcionan a 2.4GHz) interfieren con FHSS. A DSSS le afectan menos. Nada a 802.11a.
  - Otros dispositivos que funciona en 2.4GHz (teléfonos inalámbricos, mandos a distancia de puertas de garage, etc.) tienen una potencia demasiado baja para interferir con las WLANs.
  - En los sistemas por infrarrojos la luz solar puede afectar la transmisión
- Internas (de la propia señal):
  - Debidas a multitrayectoria (rebotes de la señal en paredes, techos, etc.).

2.2.2.3 Antenas Diversidad

Las antenas diversidad son una aportación reciente a las redes inalámbricas para reducir los problemas producidos por la multitrayectoria. Normalmente se implementan en los puntos de acceso ya que estos dispositivos se encuentran en comunicación con todas las estaciones de la red.

La antena diversidad consiste en dos antenas reales que se conectan por separado al receptor de radio. Cuando el equipo recibe una trama prueba a

utilizar ambas antenas y elige la que considera más conveniente. El sondeo se realiza mientras recibe el preámbulo de la trama, que por ejemplo en el caso de DSSS tiene una longitud de 128 bits (que a 11Mb/s equivale a 11.6 microsegundos).

Cuando ha de emitir una trama a una estación el emisor no puede saber cual de las dos antenas es la más adecuada. En este caso se utiliza la antena que dio mejor calidad la última vez que se recibió una trama de dicha estación. Si la emisión falla se reintenta enviando la trama por la otra antena.

Es importante observar que las dos antenas de una antena diversidad cubren la misma zona, no se pueden utilizar para cubrir zonas diferentes.
Puede resultar sorprendente como una diferencia de unos centímetros puede suponer una diferencia significativa en el efecto multitrayectoria de la señal recibida o emitida por una antena diversidad, cuando en el caso de una emisión de FM hacía falta mover el coche algunos metros. Pero debemos tener en cuenta que la longitud de onda de una emisión de FM es de unos 3m, mientras que la longitud de onda de las emisiones de 2.4GHz es de 12.5cm.

2.2.3 802.11 Subcapa MAC

2.2.3.1 Arquitectura 802.11

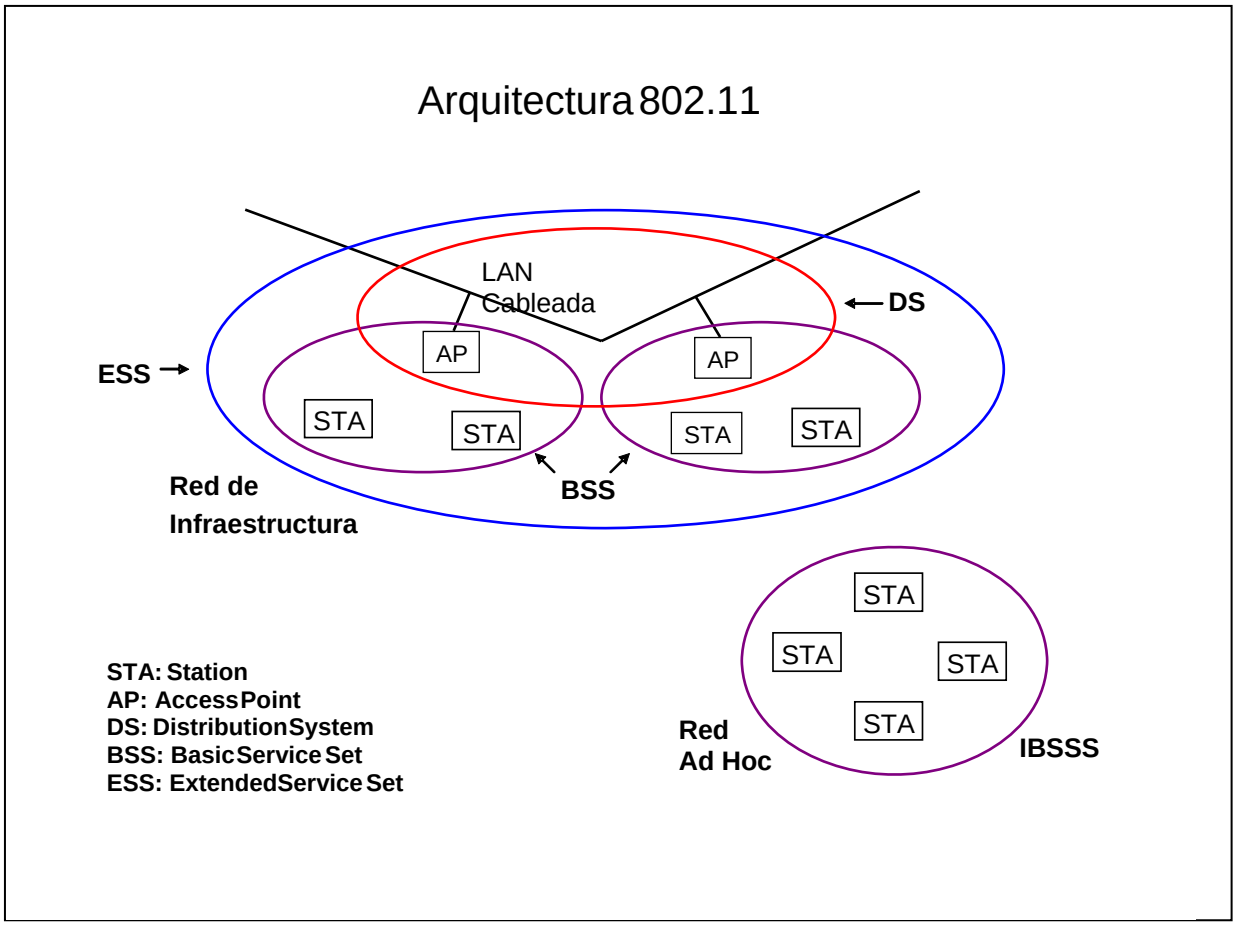


Figura 35. Arquitectura de 802.11

En esta figura se pueden apreciar los componentes que constituyen una red inalámbrica definida por el estándar y además se observan dos tipos de topologías: Infraestructura y Ad hoc. A continuación se describen los distintos componentes que participan en la arquitectura:

- **STA** (Station)**:** Cualquier dispositivo que contiene una interfaz IEEE 802.11 para acceder al medio inalámbrico.
- **BSS** (Basic Service Set): Es el bloque básico de construcción de una LAN 802.11. En el caso de tratarse de únicamente 2 estaciones ser denomina **IBSS** (Independent BSS), es lo que a menudo se denomina "Ad Hoc Netwok".
- **DS** (Distribution System): Es un sistema que se propone para interconectar distintos BSS, e integrar redes de área local (LANs).
- **AP** (Access Point)**:** es el encargado de proveer acceso al DS, todos los datos que se mueven entre BSS y DS se hacen a través de estos AP, como los mismos son también STA, son por lo tanto entidades direccionables.
- **ESS** (Extended Service Set): Tanto BSS como DS permiten crear redes inalámbricas de tamaño arbitrario, este tipo de redes se denominan redes ESS.
- La integración entre una red 802.11 y una No 802.11 se realiza mediante un **Portal**. Es posible que un mismo dispositivo cumpla las funciones de AP y Portal.

2.2.3.2 Servicios Lógicos

802.11 propone dos categorías de servicios empleados en el subnivel MAC:

- Servicios de estación (SS): Son los servicios específicos de las estaciones.

    1. Autenticación.
    2. Deautenticación.
    3. Privacidad.
    4. Manejo de datos (MSDU delivery)

- Servicios de Distribución (DSS): Estos servicios se emplean para pasar en cualquier sentido entre DS y BSS.

    1. Asociación.
    2. Desasociación.
    3. Distribución.
    4. Integración.
    5. Reasociación.

Los servicios, determinarán distintos tipos de mensajes que fluirán por la red, independientemente de su categoría, la totalidad de los servicios (y/o mensajes) son:

a. **Autenticación:** A diferencia de una red cableada, en 802.11 no existe una seguridad a nivel físico para prevenir el acceso no autorizado, por lo tanto este estándar ofrece la capacidad de autenticación por medio de este servicio. Una vez se ha efectuado la asociación se ha de validar a la estación solicitante. Si entre dos estaciones no se establece un adecuado nivel de autenticación, la asociación no podrá ser establecida. 802.11 soporta dos metodologías de autenticación:

- Sistema de Autenticación Abierta (OSA): Cualquier STA puede ser autenticada. (Autenticación Nula).
- Autenticación de Claves Compartidas (Shared Key Authentication): Este mecanismo requiere la implementación de WEP (Wireless Equivalent Privacy).

b. **Deautenticación:** Este servicio es invocado si una autenticación debe ser finalizada. Se trata de una notificación, no una solicitud, por lo tanto no puede ser rechazada, y puede ser invocado tanto por una STA (no AP), como por un AP. Una vez desautenticado no se puede usar la red.

c. **Asociación:** Antes que una STA pueda enviar mensajes vía un AP, la misma deberá encontrarse Asociada a este último. Este servicio permite al DS conectar distintas STA dentro de una red inalámbrica, ubicando a cada una de ellas. En cualquier instante de tiempo, una STA solo podrá estar asociada a un único AP. Este servicio es siempre iniciado por una STA (nunca por un AP).

d. **Desasociación:** Este servicio es invocado si una asociación debe ser finalizada. Se trata de una notificación, no una solicitud, por lo tanto no puede ser rechazada, y puede ser invocado tanto por una STA (No AP), como por un AP.

e. **Reasociación:** Permite cambiar una asociación de un AP a otro, o también cambiar los parámetros de asociación de una STA con el mismo AP. Se utiliza cuando una estación se mueve y cambia al área de cobertura de otro AP dentro del mismo ESS (handover)

f. **Distribución:** Este tipo de mensajes se producen al ingresar información a un DS proveniente de un BSS. El encargado de generar estos mensajes será un AP y su objetivo es alcanzar el destino buscado.

g. **Integración:** Los mensajes que van o vienen dirigidos hacia/desde un portal, harán uso de este servicio. Se encarga de la traducción a formatos diferentes cuando parte del trayecto se hace por una red no 802.11

h. **Privacidad:** 802.11 al igual que sucede con autenticación (y por las mismas causas) provee la posibilidad de cifrar/descifrar el contenido de los mensajes a través de este servicio. Este servicio que es opcional, también se lleva a cabo por WEP. Es muy discutible la solidez del mismo, pero la decisión fue tomada como una medida que permite tener un nivel de seguridad "al menos tan seguro como un cable".

i. **Entrega de los datos (MSDU delivery):** Se encarga del envío de los datos por el enlace de radio una vez que se han cumplido todos los requisitos previos (asociación, autenticación y privacidad).

Estos servicios generan distintos tipos de mensajes, los cuales están clasificados en:

a. Datos. El propósito de las tramas de datos es transportar información, MSDUs a la estación destino.
b. Control. Después de iniciar los procedimientos de autentificación y asociación entre estaciones y puntos de acceso, las tramas de control proporcionan asistencia en la entrega de tramas de datos. Como pueden ser RTS(Request To Send), CTS(Clear To Send), ACK, etc. (subtipos de trama de control).
c. Administración. El propósito de las tramas de administración es iniciar la comunicación entres estaciones y puntos de acceso. Y proporcionar servicios como autentificación, asociación, beacon (tramas guía), etc. (subtipos de trama de administración).

Existe una relación entre asociación y autenticación que provoca los tres "Estados" en los que se puede encontrar una STA en cualquier intervalo de tiempo:

- Estado 1: No autenticado – No asociado.
- Estado 2: Autenticado – No asociado.
- Estado 3: Autenticado – Asociado.

2.2.3.3 Tipos de Movilidad

Existen 3 tipos de transiciones que describen la movilidad de las estaciones a través de la red:

a) **Sin transición:** Define dos subclases:
    1) Estático— sin movimiento.

2) Movimiento Local—movimiento dentro del rango de comunicación de las STAs (por ejemplo, movimiento a través de un BSS).

b) **Transición entre BSS:** Define el movimiento de una estación entre un BSS a otro dentro de un mismo ESS.

c) **Transición entre ESS:** Define el movimiento de una estación entre un BSS dentro de un ESS, a otro BSS dentro de un diferente ESS.

Los diferentes servicios de asociación soportan las tres categorías de movilidad.

2.2.3.4 Descripción funcional del subnivel MAC

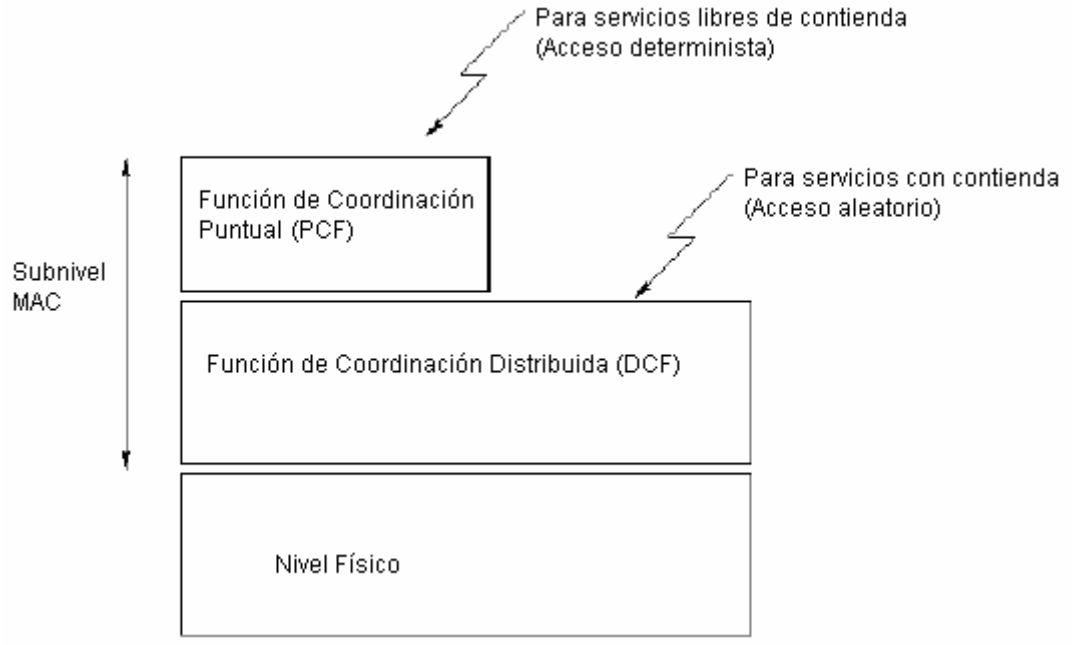


Figura 36. Descripción funcional del subnivel MAC

La arquitectura MAC del estándar 802.11 se compone de dos funcionalidades básicas: la Función de Coordinación Puntual (PCF) y la Función de Coordinación Distribuida (DCF). Definimos función de coordinación como la funcionalidad que determina, dentro de un conjunto básico de servicios (BSS), cuándo una estación puede transmitir y/o recibir unidades de datos de protocolo a nivel MAC a través del medio inalámbrico (Figura 36).

2.2.3.4.1 Función de Coordinación Distribuida (DCF)

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 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 DCF las podemos resumir en estos puntos:

- Utiliza CSMA/CA con RTS/CTS, como protocolo de acceso al medio.
- Necesario reconocimientos de ACKs, provocando retransmisiones si no se recibe.
- Usa un campo 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 tramas (IFS).
- Soporta Broadcast y Multicast sin ACKs.

El protocolo MAC de 802.11 está inspirado en el CSMA/CD de Ethernet. Sin embargo las redes inalámbricas no puede usar el protocolo CSMA/CD debido a que es muy difícil que un emisor de radio detecte otra emisión en curso en el mismo canal en el que está emitiendo. Por tanto el CD (Colision Detect) de Ethernet se ha cambiado por CA (Colision Avoidance).

2.2.3.4.1.1 Espacio entre tramas (IFS: Interframe Space)

Los intervalos de tiempo entre tramas son los IFS y sus valores dependerán de la tecnología de la capa física con la que se este trabajando (FHSS, DSSS ó IR). Se definen cuatro tipos de IFS, para establecer prioridades de acceso al medio:

a) SIFS (Short IFS): Este intervalo se emplea en tramas ACK, CTS o en las sucesivas tramas de una operación de fragmentación. También en cualquier respuesta a un sondeo realizado por un AP. Es el intervalo más corto.

b) PIFS (PCF IFS): Se emplea en modo PCF (Excepto en las respuestas a sondeos)

c) DIFS (DCF PFS): Se emplean en modo DCF par envío de tramas de administración y de datos.

d) EIFS (Extended IFS): Este intervalo se emplea cuando el nivel físico le informa al subnivel MAC que una trama que se ha transmitido, no tuvo una correcta recepción. Se emplea este valor máximo de intervalo, para dar tiempo suficiente a la STA receptora, de informar este error de recepción.

2.2.3.4.1.2 Protocolo CSMA/CA (Carrier Sense Multiple Access / Collision Advoidance)

a) Antes de transmitir información una estación debe testear el medio, o canal inalámbrico, para determinar su estado (libre / ocupado).
b) Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional correspondiente a un DIFS.
c) 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.
d) Una vez finalizada 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 llamada *ventana de contienda* (CW). El algoritmo de Backoff nos da un número aleatorio y entero de ranuras temporales (slot time) 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.
e) Mientras se ejecuta la espera marcada por el algoritmo de Backoff se continua escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos un DIFS o un EIFS, esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a un DIFS o un EIFS, el algoritmo de Backoff queda suspendido hasta que se cumpla esta condición. Cada retransmisión provocará que el valor de CW, que se encontrará entre CWmin y CWmax se duplique hasta llegar al valor máximo.

El envío de mensajes de confirmación (ACK) para cada trama recibida es algo que incorpora la capa MAC de 802.11, ya que las redes de radio con equipos móviles son poco fiables, y era necesario implementar a bajo nivel un mecanismo que asegurara la recepción de la información.

El envío de los ACK debe realizarse de forma rápida y ágil, ya que de lo contrario se puede incurrir en un retardo excesivo hasta que se produzca el reenvío de la trama.

Para evitar que el receptor tenga que competir con cualquier otra estación en el envío de la confirmación el envío de la trama de ACK puede hacerse sin esperar el tiempo reglamentario de un DIFS después de haya terminado la emisión de la trama en curso.

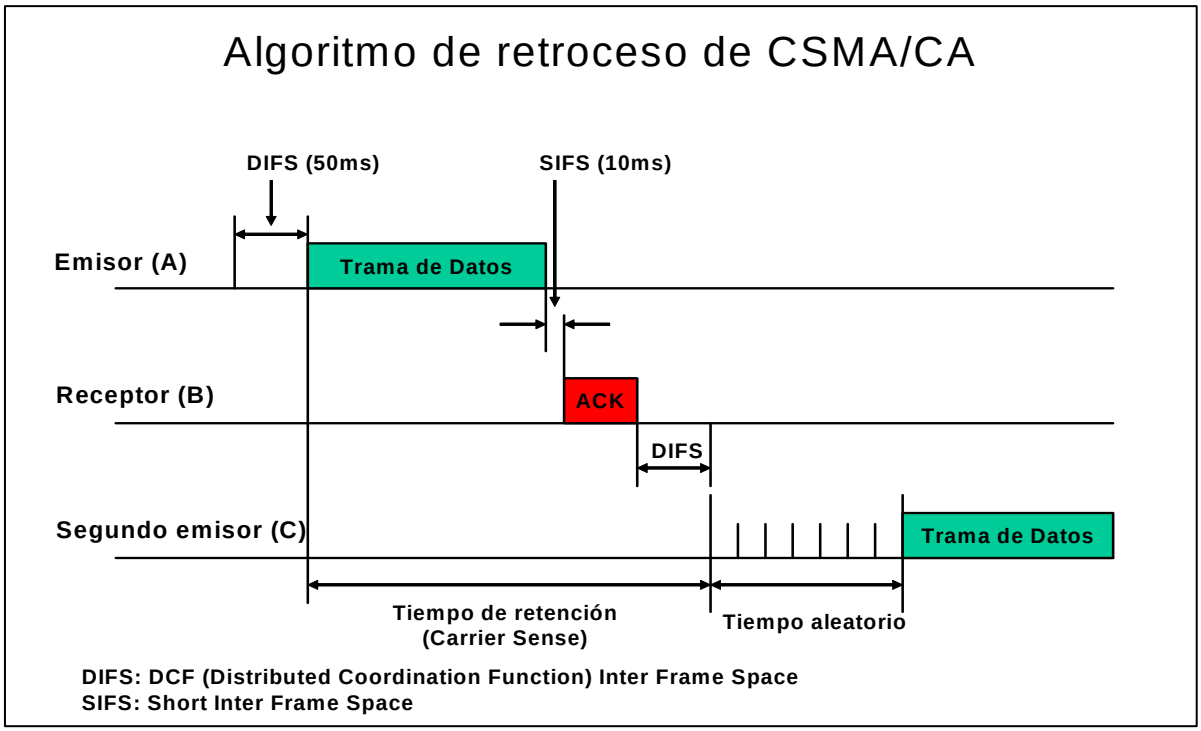


Figura 37. Algoritmo CSMA/CA

Esta figura muestra como funciona el protocolo CSMA/CA en 802.11. Supongamos que una estación (A) desea transmitir una trama hacia B y detecta que el canal está libre. A espera el tiempo DIFS y a continuación empieza a transmitir. De esta forma se asegura que cualquier trama emitida en la red irá separada de la anterior al menos por este espacio de tiempo.

Una vez que ha terminado de emitir su trama A espera una confirmación (ACK) de B. Dicha confirmación es un mensaje de alta prioridad, por lo que no ha de esperar el tiempo habitual (DIFS) después de que termine la trama de A, sino que solo ha de esperar el tiempo SIFS. Durante el tiempo SIFS B ha calculado y comprobado que el CRC de la trama que ha recibido de A es correcto.

En algún momento durante la emisión de la trama de A, C desea enviar una trama a D (no mostrado en la figura). Como detecta que el canal está ocupado C espera, y cuando se produce el ACK de B C sigue esperando, ya que no se ha llegado a producir una pausa lo bastante grande en ningún momento. Cuando por fin termina el ACK de B, C empieza a contar el tiempo y cuando pasa un DIFS sabe que el canal está libre. Entonces no transmite de inmediato sino después del tiempo aleatorio que ha calculado. Esto reduce el riesgo de colisión con otras estaciones que pudieran también estar observando el proceso de A y B y esperando para transmitir a continuación. Si durante el tiempo aleatorio C detecta que alguna estación transmite congelará su contador de tiempo aleatorio para volver a activarlo un DIFS después de que haya cesado toda actividad.

2.2.3.4.1.2.1 Random Backoff Time

Cuando una STA desea transmitir, y la función "Carrier Sense" detecta ocupado el canal, deberá desistir de la transmisión hasta que se desocupe el medio durante un intervalo DIFS finalizada la transmisión anterior si esta llega con éxito, si es motivo de errores, el intervalo de espera deberá ser EIFS. Una vez finalizado cualquiera de estos dos intervalos, generará un valor aleatorio denominado "Random Backoff Time", que deberá esperar antes de transmitir. El objetivo del mismo es minimizar colisiones. Este valor se compone de:

Backoff Time = Random () * Slot Time.

El valor Random está relacionado con CW (Mínima y máxima) y sus límites oscilarán entre 0 y $\mathbf{2^{n-1}}$ Siendo "n" la cantidad de intentos de acceso. Y el "Slot time" un valor que depende de las características físicas del canal.

2.2.3.4.1.2.2 Colisiones

Pueden producirse porque dos estaciones a la espera elijan el mismo número de intervalos (mismo tiempo aleatorio) para transmitir después de la emisión en curso. En ese caso reintentan ampliando exponencialmente el rango de intervalos y vuelven a elegir. Es similar a Ethernet salvo que las estaciones no detectan la colisión, infieren que se ha producido cuando no reciben el ACK esperado. También se produce una colisión cuando dos estaciones deciden transmitir a la vez, o casi a la vez. Pero este riesgo es mínimo.
Cuando una estación ha emitido una trama y no ha recibido el correspondiente ACK deduce que se ha producido una colisión. En este caso la estación repite el proceso antes descrito, pero al tratarse de un segundo intento esta vez se amplía el rango de intervalos para la elección del tiempo aleatorio. De forma análoga a lo que ocurre en Ethernet el número de intervalos crece de forma exponencial hasta un valor máximo a partir del cual el contador se reinicia y el proceso se repite desde el principio.

2.2.3.4.1.2.3 Estaciones Ocultas

En un entorno inalámbrico y celular CSMA/CA presenta una serie de problemas que se resuelven con alguna modificación. Los dos principales problemas que se pueden detectar son:

- Nodos ocultos. Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye.

- 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.

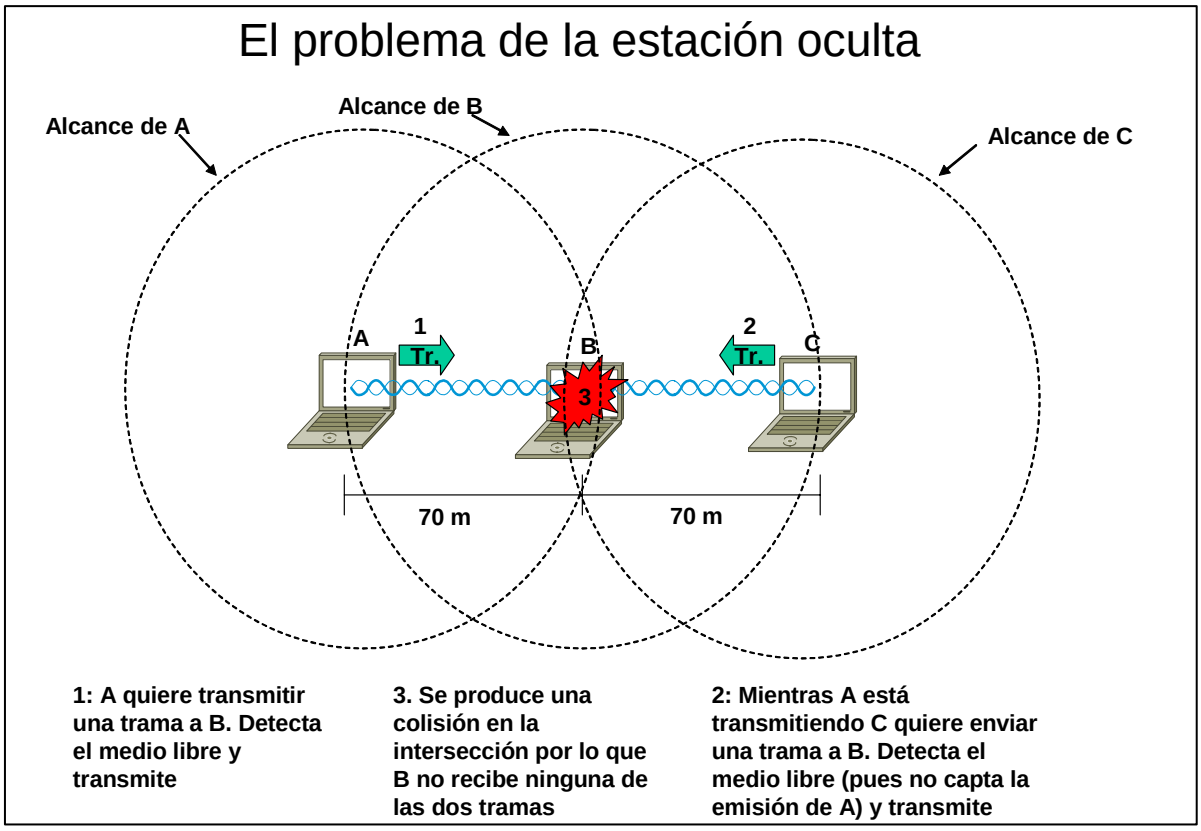


Figura 38. Estaciones ocultas

Supongamos que A quiere enviar una trama a B. A detecta que el canal está libre y empieza a transmitir. Instantes más tarde, cuando A está aún transmitiendo, C quiere también enviar una trama a B; C detecta que el canal está libre, ya que él no está recibiendo la emisión de A pues se encuentra fuera de su radio de cobertura. Por tanto C empieza a transmitir y en B se produce una colisión. Como consecuencia B no recibe correctamente ni la trama de A ni la de C (Figura 38).

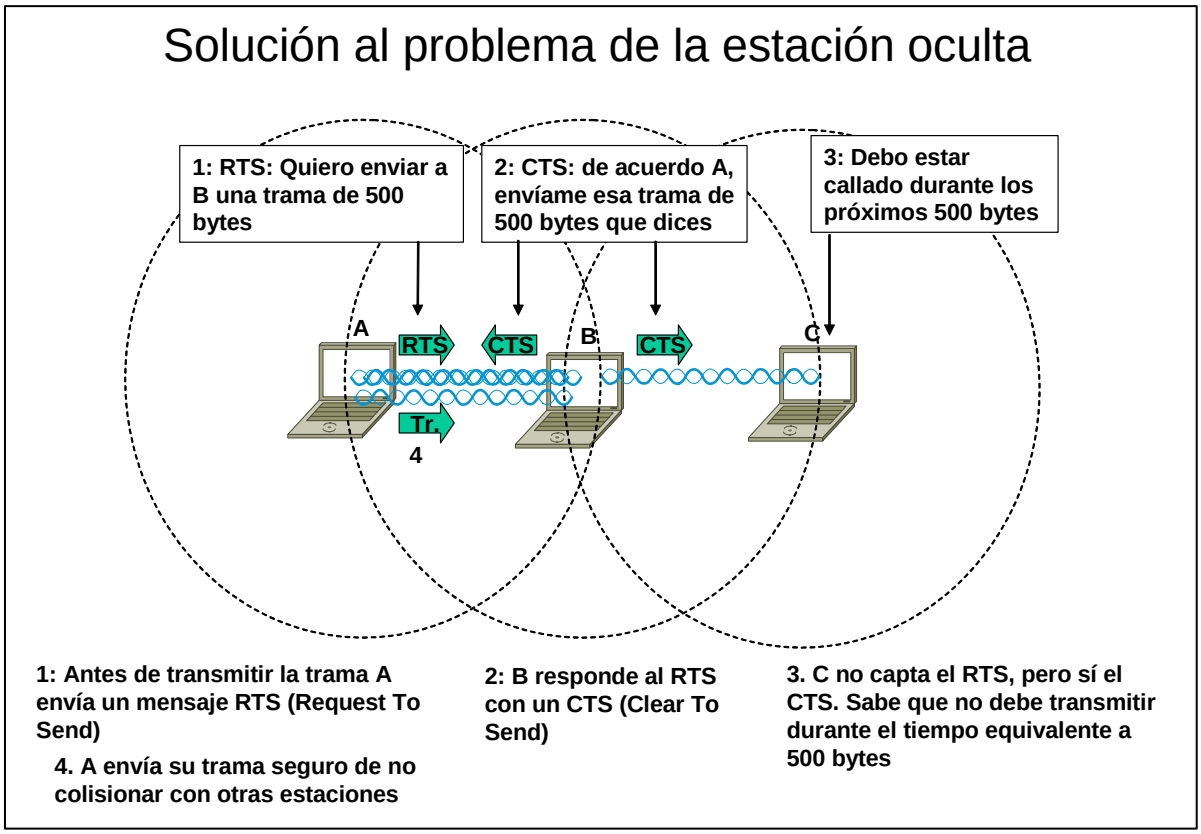


Figura 39. Solución a las Estaciones ocultas

La solución que normalmente se aplica al problema de la estación oculta se basa en el intercambio entre emisor y receptor de dos mensajes previos al envío de la trama.

El emisor A envía un mensaje RTS a B en el que le advierte de su deseo de enviarle una trama; además en dicho mensaje A le informa de la longitud de la misma. Este mensaje no es recibido por C.

Como respuesta al mensaje de A, B envía un CTS en le que le confirma su disposición a recibir la trama que A le anuncia. Dicho mensaje CTS lleva también indicada la longitud de la trama que B espera recibir de A.

C no recibe el mensaje RTS enviado por A, pero sí recibe el CTS enviado por B. Del contenido del mensaje CTS, C puede deducir por cuanto tiempo estará ocupado el canal que comparte con B, pues el mensaje incluye indicación de la longitud de la trama a transmitir y C conoce la velocidad con que se realiza la transmisión (Figura 39).

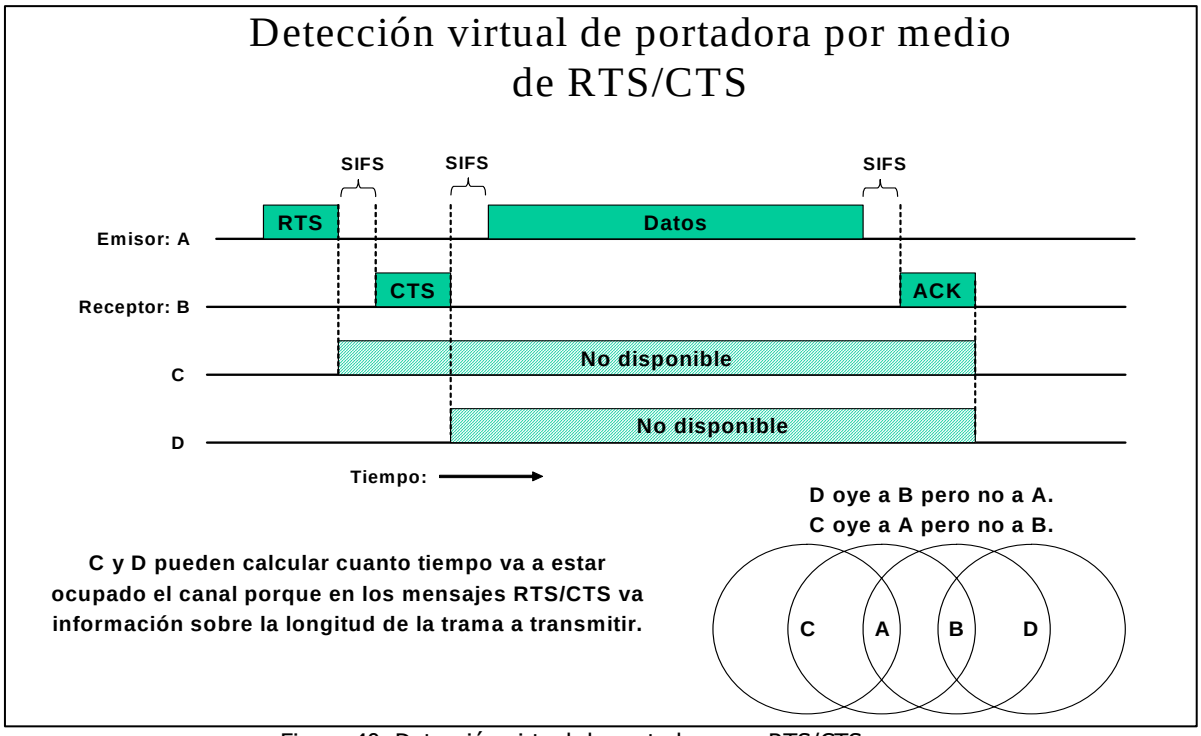


Figura 40. Detección virtual de portadora con RTS/CTS

El uso de mensajes RTS/CTS se denomina a veces *Virtual Carrier Sense*. Permite a una estación reservar el medio durante una trama para su uso exclusivo (Figura 40). Si todas las estaciones se 'escuchan' directamente entre sí el uso de RTS/CTS no aporta nada y supone un overhead (el término "overhead" hace referencia a la información que debe ser mandada para que la red opere apropiadamente, pero que no es parte de los datos que esta transfiriendo el usuario) importante, sobre todo en tramas pequeñas. No todos los equipos soportan el uso de RTS/CTS. Lo que lo soportan permiten indicar en un parámetro de configuración a partir de que tamaño de trama se quiere utilizar RTS/CTS.

2.2.3.4.1.2.3.1 Conocimiento del medio

Las estaciones tienen un conocimiento específico de cuando la estación, que en estos momentos tiene el control del medio porque 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). El NAV es un valor que indica a una estación la cantidad de tiempo que resta antes de que el medio esté disponible.

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.

2.2.3.4.2 Función de Coordinación Puntual (PCF)

Para soportar aplicaciones que requieren servicios cercanos al tiempo real, el estándar 802.11 incluye una segunda función de coordinación para proporcionar acceso libre de contienda al medio inalámbrico.

El servicio libre de contienda no está disponible todo el tiempo. Los periodos de servicio libre de contienda son alternados con el servicio estándar DCF, como se muestra en la figura.

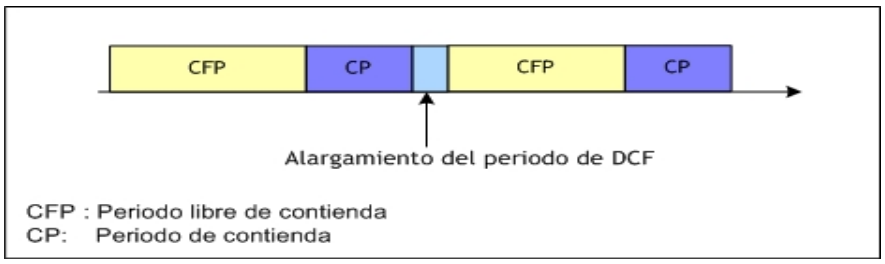


Figura 41. Periodos de tiempo en PCF

El servicio libre de contienda utiliza un método de control de acceso centralizado. El acceso al medio está restringido por el coordinador puntual, que es una función especializada implementada en puntos de acceso. Las estaciones asociadas pueden transmitir datos sólo cuando se les ha permitido por el coordinador puntual (AP).

2.2.3.4.2.1 Operación de la PCF

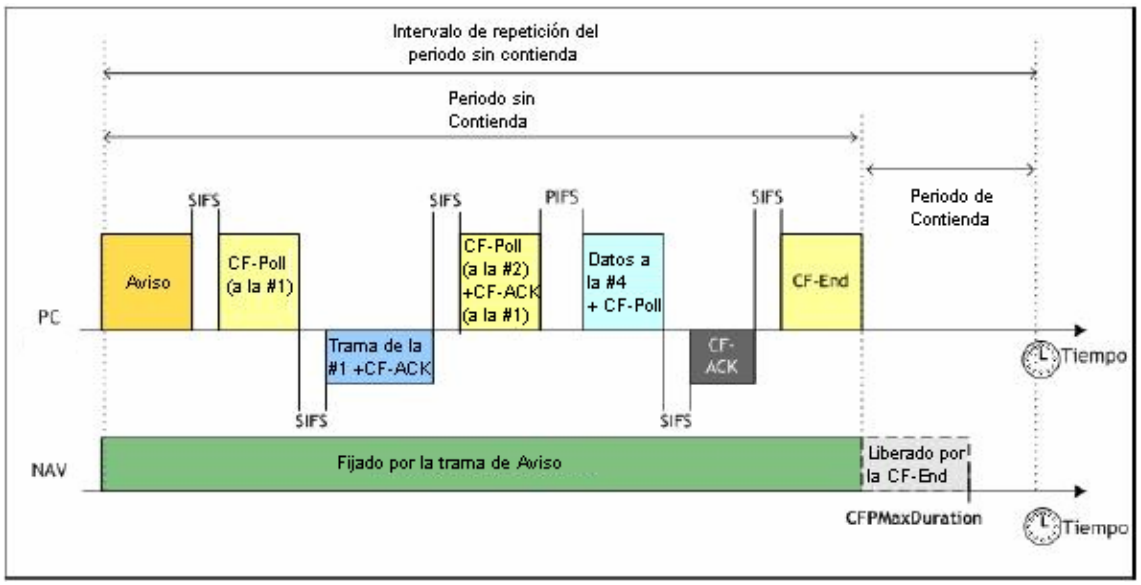


Figura 42. Operación de PCF

La figura muestra una transferencia utilizando la PCF. Cuando se utiliza la PCF, el tiempo en el medio es dividido en periodos libres de contienda (CFP, *Contention Free Period*) y periodos de contienda (CP). El periodo de contienda debe ser lo suficientemente largo para transmitir por lo menos una trama de tamaño máximo y su reconocimiento asociado. Los periodos de servicio libre de

contienda y los basados en contienda son repetidos a intervalos regulares, los cuales son llamados intervalos de repetición libre de contienda. El AP es quien inicia el periodo libre de contienda, enviando una trama de aviso (*Beacon*).

2.2.3.4.2.1.1 Reservación del medio durante el periodo de libre contienda

Al principio del periodo libre de contienda, el AP transmite la trama de aviso. Un componente de esta trama es la máxima duración del periodo libre de contienda, *CPFMaxDuration*. Todas las estaciones que reciben el aviso fijan el NAV a la máxima duración para evitar el acceso de la DCF al medio inalámbrico. Como seguridad adicional para prevenir interferencia, todas las transmisiones libres de contienda son separadas por un solo espacio de intertrama corto (SIFS) y el espacio intertrama del PCF (PIFS). Ambos son más cortos que el espacio de intertrama del DCF, por lo que las estaciones basadas en DCF no podrán ganar el acceso al medio durante este tiempo.

2.2.3.4.2.1.2 La lista de encuesta

La lista de encuesta, es la lista de estaciones que solicitan enviar tramas durante el periodo libre de contienda. Las estaciones entran en la lista de encuesta mediante un mensaje de solicitud de asociación enviado al AP. La petición de asociación incluye un campo que indica si la estación es capaz de responder a las encuestas durante el periodo libre de contienda. Después de que el AP ha ganado el acceso al medio, éste encuesta a cualquier estación incluida en una lista de encuesta para transmisión de datos. Durante el periodo libre de contienda, las estaciones pueden transmitir sólo si el AP solicita la transmisión con una trama de encuesta (CF-Poll) la cual permite la transmisión de una sola trama. Para enviar varias tramas es necesario que el AP envíe varios CF-Poll.

2.2.3.4.3 Fragmentación

Muchas de las interferencias que se producen en las transmisiones por radio afectan la emisión en intervalos muy cortos de tiempo. En estos casos la transmisión de tramas grandes resulta especialmente comprometida, pues el riesgo de que una interferencia estropee toda la emisión es muy grande. En situaciones de elevada tasa de error del medio físico es preferible manejar tramas de pequeño tamaño. Sin embargo el nivel de red, que no tiene un conocimiento de la situación de la red inalámbrica, suministra el paquete al nivel de enlace para que lo envíe en una única trama. Por este motivo el nivel MAC de 802.11 prevé un mecanismo por el cual si el emisor ve que las tramas no están llegando bien puede decidir fragmentarlas para que tengan más probabilidad de llegar bien al receptor. El receptor a su vez reensamblará la trama original para que sea entregada a los niveles superiores, con lo que la fragmentación actuará de forma transparente a ellos.

En el caso de producirse fragmentación cada fragmento se enviará siguiendo el mecanismo de CSMA/CA antes descrito, y recibirá el correspondiente ACK del receptor.

Por cada fragmento se devuelve un ACK por lo que en caso necesario es retransmitido por separado. La fragmentación permite enviar datos en entornos con mucho ruido, aun a costa de aumentar el overhead. Todas las estaciones están obligadas a soportar la fragmentación en recepción, pero no en transmisión (Figura 43). El overhead que puede introducir el uso de la fragmentación es considerable, pero puede ser rentable cuando la red tiene mucho ruido.

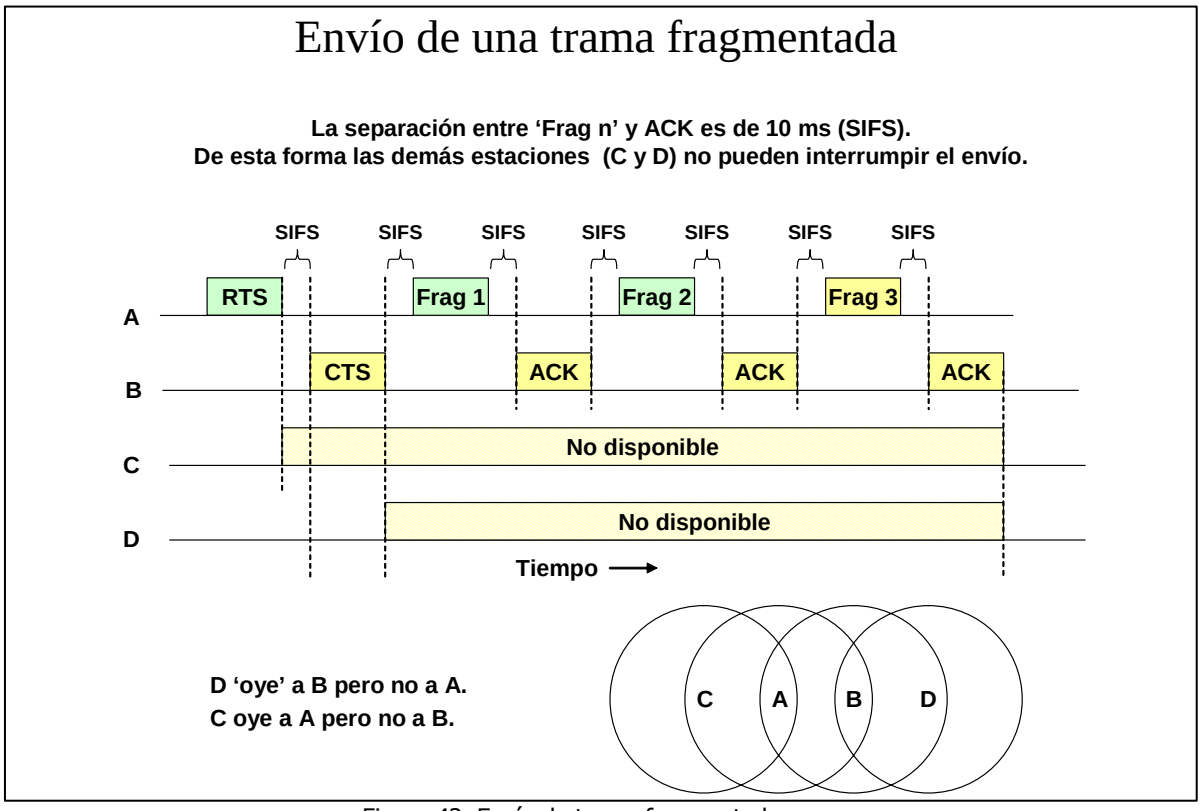


Figura 43. Envío de trama fragmentada

2.2.3.4.4 Entidad de administración de subnivel MAC

La subcapa de administración MAC implementa las siguientes funcionalidades:

- Sincronización.
- Gestión de potencia
- Asociación-Reasociación
- Utiliza el MIB o Management Information Base

2.2.3.4.4.1 Sincronización

La sincronización se consigue mediante una función de sincronización (TSF) que mantendrá los relojes de las estaciones sincronizados. Según el modo de operación, se distinguirá el modo de funcionamiento.

En el modo infraestructura, la función de sincronización recaerá en el punto de acceso, de tal manera que el punto de acceso enviará la sincronización en la trama portadora o Beacon y todas las estaciones se sincronizarán según su valor.

En el modo ad-hoc, el funcionamiento es más complejo. Por una parte, la estación que controle la red establecerá un intervalo de beacon, esto es, una tasa de transferencia de portadoras que permitan la sincronización.
Sin embargo, en este caso, el control está distribuido y entre todas las estaciones se intentará mantener la sincronización. Para ello, toda esta estación que no detecte en un determinado tiempo una trama de sincronización, enviará ella misma una trama de portadora para intentar que no se desincronice la red.

2.2.3.4.4.1.1 Scanning (Exploración)

Antes de autentificarse y asociarse a una estación o punto de acceso es necesario primero determinar si hay presente alguna estación o punto de acceso por trivial que parezca. La estación realiza esta fase de descubrimiento operando en modo de exploración pasivo o activo. Después de unirse a una BSS o ESS, la estación acepta el SSID (Service Set Identifier), TSF (Timing Synchronization Function) valor del temporizador que mantendrá los relojes de las estaciones sincronizados, y parámetros físicos de configuración del punto de acceso.

2.2.3.4.4.1.2 Scanning Pasivo

La estación escucha cada canal durante un periodo de tiempo específico y espera la transmisión de beacons. Estas tramas transportan información del SSID, necesario para que una estación pueda unirse a la red. Una vez que la estación detecta beacon, ésta comienza el proceso de autentificación y asociación.

2.2.3.4.4.1.3 Scanning Activo

La estación envía una trama de prueba (Probe frame) indicando el SSID de la red de la que quiere conectarse. Los puntos de acceso alcanzados responden con una trama de respuesta (Probe Response frame). La estación seleccionará generalmente por nivel de señal recibida, el AP al que desea asociarse. Es posible que una estación envíe tramas de prueba empleando un SSID broadcast produciendo una respuesta por parte de todas la redes que estén dentro del área de cobertura de la estación.

2.2.3.4.4.2 Gestión de Potencia

Una STA puede permanecer en dos estados:

- Despierta (Awake): Está en condiciones normales de operación.
- Dormida (Doze): No está en capacidad de transmitir o Recibir y consume mucho menos potencia.

La transición entre estos dos estados es controlada por cada STA. Estas estaciones se denominan PS-STAs (Power Save Station) y escuchan periódicamente las tramas Beacon, para ver si su AP necesita cambiarla de estado, para enviarle información. El control de este tipo de estaciones lo llevará el punto de acceso, que tendrá conocimiento de qué estación se ha asociado en este modo. El punto de acceso mantendrá almacenados los paquetes que le lleguen con destino a las estaciones limitados de potencia. Por tanto, el punto de acceso mantendrá un mapa de paquetes almacenados y los destinos a quienes tendrá que repartirlos o enviarlos. Cuando el punto de acceso decida enviarle el paquete lo hará enviándole una trama TIM o Traffic Indication Map a la estación para que despierte en el próximo intervalo de portadora. De esta manera, estas estaciones recibirán la información con un desgaste mínimo de potencia.

2.2.3.4.4.3 Asociación

Cuando una estación se enciende busca un AP. Si recibe respuesta de varios atiende al que le envía una señal más potente. La estación se asocia con el AP elegido. El AP le incluye su MAC en la tabla de asociados. El AP se comporta para las estaciones de su celda como un hub inalámbrico. En la conexión entre la celda y el sistema de distribución el AP actúa como un puente.

La asociación implica que la estación continuará enviando este tipo de tramas y podrá provocar una reasociación en función de los parámetros de selección que él mismo utilice y defina.

2.2.3.4.4.3.1 SSID

- Los clientes y el punto de acceso se asocian mediante un SSID (System Set Identifier) común.
- El SSID sirve para la identificación de los clientes ante el punto de acceso, y permite crear grupos 'lógicos' independientes en la misma zona
- Normalmente cada SSID se asocia a una VLAN diferente en la red alámbrica y a una subred IP diferente
- Algunos AP's permiten configurar varios SSID en un mismo equipo.
- El SSID permite organizar y gestionar varias WLAN's que tengan que coexistir en una misma ubicación, incluso si comparten un mismo canal.

2.2.3.4.4.3.1.1 Organización de los SSID

- Normalmente la cobertura de un edificio se hace con varios APs que están conectados a la misma VLAN y tienen el mismo SSID.
- La VLAN tiene asociada una subred IP que es atendida por un servidor DHCP el cual asigna dirección, máscara y router por defecto a los equipos que se conectan a la WLAN.
- El cambio de celda no modifica la dirección IP entretanto se siga dependiendo del mismo SSID y por tanto de la misma VLAN/subred.
- En una WLAN muy grande habría que utilizar varias VLANs; en ese caso los APs recibirían un SSID que dependería de la VLAN a la que se conectan. Si un usuario al cambiar de celda cambia de SSID cambiará de subred, con lo que perderá la comunicación.

2.2.3.5 Formato del Paquete 802.11

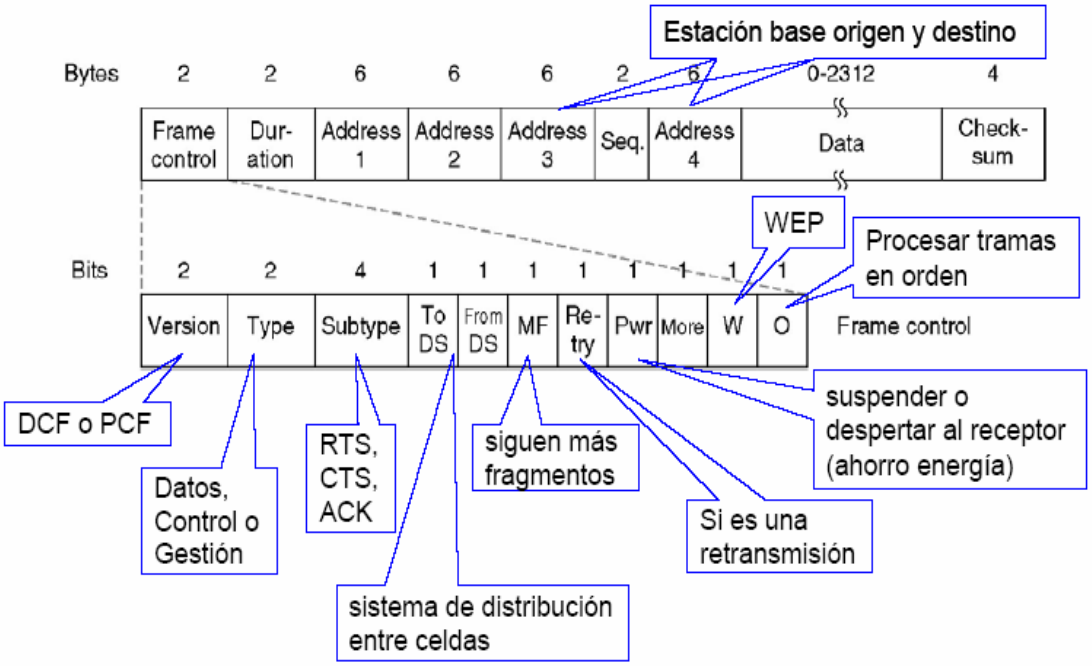


Figura 44. Trama 802.11

2.2.4 Estándar 802.11b

Tuvo sus orígenes en Septiembre de 1999, pero la producción de equipos empezó a principios de 2000, pues los equipos de 1999 eran beta y estaban en ajustes. Uno de los factores importante de estos equipos y que se considera importante, es que por primera vez después de las Bios de las placas madre, los equipos 802.11b y sus sucesores inalámbricos poseen la capacidad de actualizar Firmware; esto permite modificar el software interno de los DSP que controlan las tarjetas (NIC) basados en memorias electrónicamente reescribibles como las E2ROM o las EPROM, con lo que se pueden realizar correcciones a la comunicación inalámbrica de los equipos, hacer mejoras en problemas de seguridad detectados y corregir problemas con sistemas operativos y dispositivos.

Otra cosa importante en esta norma es que se estableció una certificación de compatibilidad de equipos conocida como Wi-Fi lo que permitió la total compatibilidad de los equipos como ocurre con todas la tarjetas de red Ethernet. 802.11b es una prolongación del 802.11 original en la banda de los 2.4GHz del espectro ISM, 802.11b es una extensión de DSSS original, junto con algunas correcciones y mejoras como el uso de menos ancho de banda, de 30MHz. a 25MHz; a los modos DBPSK a 1Mbps y DQPSK a 2Mbps, se agregaron los modos 5.5Mbps y 11Mbps usando la tecnología de 8 a 11-chip llave de códigos complementarios (complementary code keying: CCK), además la mayoría de los dispositivos usan tecnología auto Fall-Back en que el equipo modifica su modulación de acuerdo a la potencia de la señal recibida, con lo que si la señal es potente funcionará automáticamente a 11Mbps. Pero si decae cambiará sólo a 5.5Mbps hasta llegar a 1Mbps. Además 802.11b tomó prestado la capacidad muy útil de los teléfonos celulares y es capas de hacer Roaming y pasar de una celda inalámbrica a otra sin intervención del usuario con lo que se permite la comunicación inalámbrica en movimiento.

2.2.4.1 Uso del espectro

Se permite el uso de todos los canales en Japón, además de que la separación entre frecuencias centrales para los posibles canales de transmisión se reduce de 30MHz a 25MHz (Tabla 4).

		Regulatory domains						
CHNL_ID	Frequency (MHz)	X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32 France	X'40' Japan	X'41' Japan
1	2412	X	X	X	—	—	—	X
2	2417	X	X	X	—	—	—	X
3	2422	X	X	X	—	—	—	X
4	2427	X	X	X	—	—	—	X
5	2432	X	X	X	—	—	—	X
6	2437	X	X	X	—	—	—	X
7	2442	X	X	X	—	—	—	X
8	2447	X	X	X	—	—	—	X
9	2452	X	X	X	—	—	—	X
10	2457	X	X	X	X	X	—	X
11	2462	X	X	X	X	X	—	X
12	2467	—	—	X	—	X	—	X
13	2472	—	—	X	—	X	—	X
14	2484	—	—	—	—	—	X	—

Tabla 4. Canales Disponibles

2.2.4.1.1 Espectro Disperso

Desaparece FHS y para DSSS se proporcionan dos nuevas técnicas de modulación CCK (Complementary Code Keying) y PBCC (Packet Binary Convolutional Coding) que, junto con las dos anteriores, BPSK (Binary Phase Shift Keying) y QPSK (Quadrature Phase Shift Keying), permiten velocidades de 1, 2, 5.5 y 11Mbps.

2.2.4.1.2 Modulación CCK (Complementary Code Keying)

Debido a que las técnicas de modulación que se utilizaban anteriormente eran ineficientes para aplicaciones de comunicaciones en las que se requiere más de 2Mbps, se hace uso de una técnica que adicionalmente permita mejorar la velocidad de transmisión de datos y esta tiene que ver con la forma como se hace el ensanchamiento de la información. La forma tradicional de ensanchamiento del espectro es utilizando el código Barker en velocidades de 1 y 2Mbps. Para poder obtener las velocidades de 5.5 y 11Mbps se utiliza la técnica de CCK que se basa en secuencias complementarias las cuales fueron propuestas inicialmente por M. J. Golay en 1961. Para el caso de la velocidad de 11Mbps se trabaja una secuencia de ensanchamiento de 8 chips, donde chip es una secuencia específica por la cual se reemplaza cada uno de los bits a ser transmitidos.

2.2.4.1.3 Modulación PBCC (Packet Binary Convolutional Coding)

En esta técnica se pueden lograr velocidades de 5.5 y 11Mbps. En ella se utiliza un codificador convolucional que genera dos bits por cada uno de los que se quiere transmitir. La salida del decodificador se emplea con una constelación DQPSK (Diferencial Quadrature Phase Shift Keying) para 11Mbps y en DBPSK para 5.5Mbps. Básicamente lo que se hace es modificar la constelación DPSK basado en una secuencia de 256 bits. Por cada símbolo transmitido la constelación se desplaza 90 grados si el bit de la secuencia es un 1.

2.2.4.2 Modificación en la trama PLCP

Se cuenta con un modo opcional que permite altas transferencias y consiste en la reducción del número de bits del preámbulo para la trama PLCP.

Formato de la trama PLCP (long)

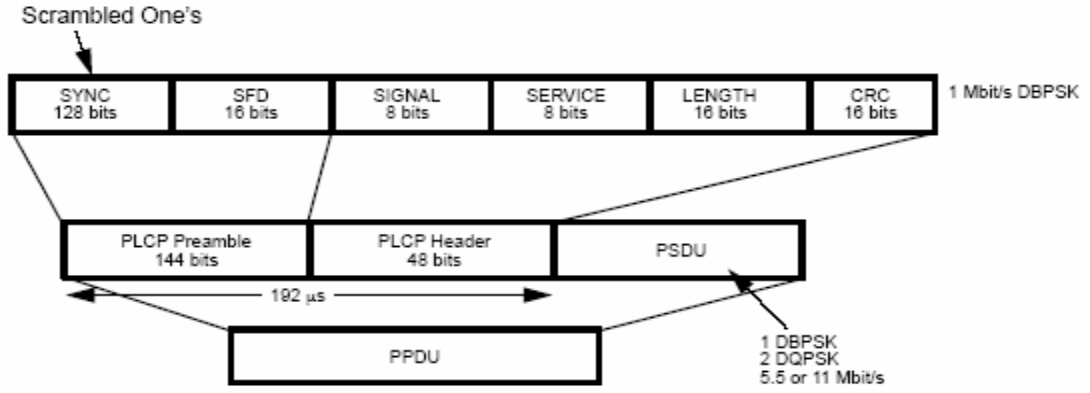


Figura 45. Trama PLCP corta

Formato de la trama PLCP (Short)

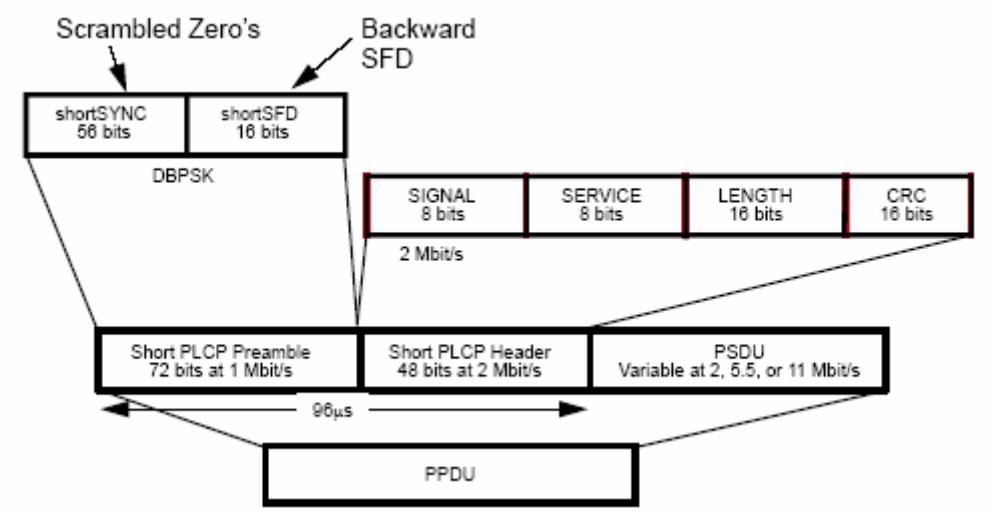


Figura 46. Trama PLCP larga

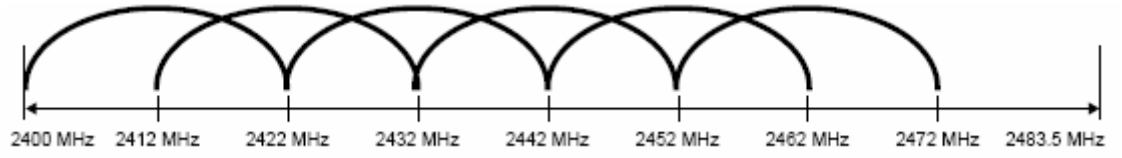
2.2.4.3 Secuencias de Saltos

Además se permite para transferencias de 1 y 2Mbps *Secuencias de Saltos (Hop sequences)*, logrando con esto interoperabilidad con sistemas FHS. Esto se logra sobreponiendo 2 canales con un mínimo de 10MHz entre frecuencias centrales. Entonces se tienen dos conjuntos de canales que pueden ser configurados dependiendo de la técnica de esparcimiento:

Para América:

Set	Number of channels	HR/DSSS channel numbers
1	3	1, 6, 11
2	6	1, 3, 5, 7, 9, 11

Canales No Sobrepuestos

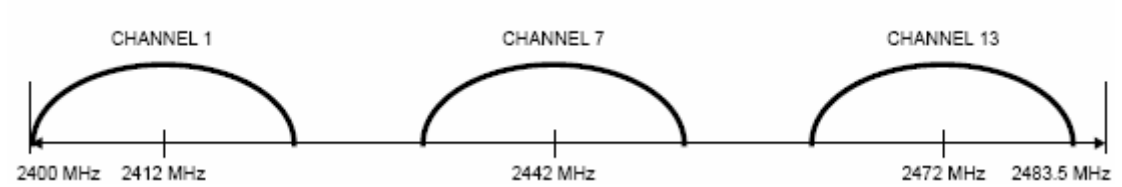


Canales Sobrepuestos

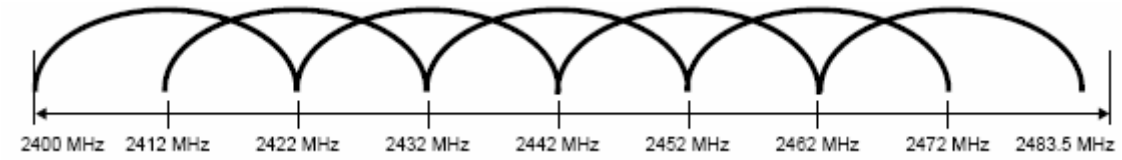
Figura 47. Distribución de canales en América

Para Europa (excepto Francia y España):

Set	Number of channels	HR/DSS channel numbers
1	3	1, 7, 13
2	7	1, 3, 5, 7, 9, 11, 13



Canales No Sobrepuestos

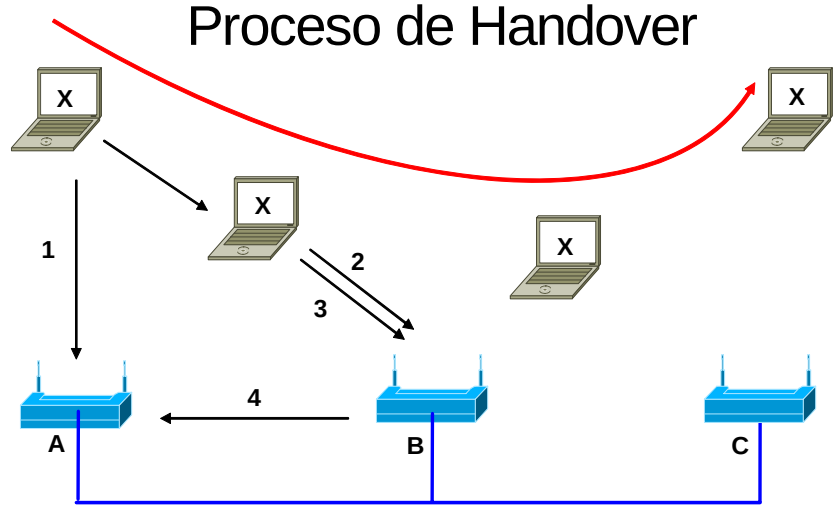


Canales Sobrepuestos

Figura 48. Distribución de canales en Europa

2.2.4.4 Itinerancia ('Roaming' o 'Handover')

- Los AP envían regularmente (10-100 veces por segundo) paquetes beacon para anunciar su presencia a las estaciones que se encuentran en su zona.
- Si una estación se mueve y cambia de celda, detectará otro AP más potente y cambiará su registro. Esto permite la itinerancia ('handover') sin que las conexiones se corten.
- Para que el handover pueda hacerse correctamente debe haber una zona de solapamiento entre las dos celdas (entrante y saliente) y la estación debe permanecer el tiempo suficiente en ella. Por tanto el handover depende del tamaño de la zona de solapamiento y de la velocidad con que se mueve la estación (Figura 49).



1: La estación se enciende. Se autentifica y asocia con el AP A (el más próximo)

2: La estación se mueve y se pre-autentifica con el AP B

3: La estación decide reasociarse con B

4: B notifica a A la nueva ubicación de X con lo que X se desasocia de A.
A envía a B cualquier trama para X en curso

5: X sigue moviéndose por lo que más tarde repite el proceso con C

Figura 49. Roaming

2.2.5 Estándar 802.11a

Este es un estándar que opera en la banda U-NII (Unlicensed National Information Infraestructure), en frecuencias de 5GHz. Posee un ancho de banda de 300 MHz dividiéndose en tres bandas cada una de 100MHz en la que se tiene un nivel de potencia máximo permitido. Esta banda presenta mucho menos interferencia que la banda de 2.4GHz. A cada una de las bandas en las que se divide se les denomina baja media y alta. Equipos que se generan para esta banda dependiendo del país requieren o no licenciamiento. Este estándar soporta tráfico de aplicaciones multimedia con garantía de ancho de banda.

Este estándar codifica la señal utilizando el esquema OFDM (Ortogonal Frecuency Division Multiplexing) la cual divide la información y transmite de forma paralela los datos usando diferentes portadoras. Esta técnica es menos sensible a las multitrayectorias de la señal, soporta velocidades de 6, 9, 12, 18, 24, 36, 48 y 54Mbps con la opción de auto Fall-Back. El sistema utiliza 52 subportadoras que son moduladas utilizando BPSK, QPSK, 16-QAM y 64-QAM. Utiliza la técnica FEC (Forward Error Correction) como protección contra las pérdidas de datos.

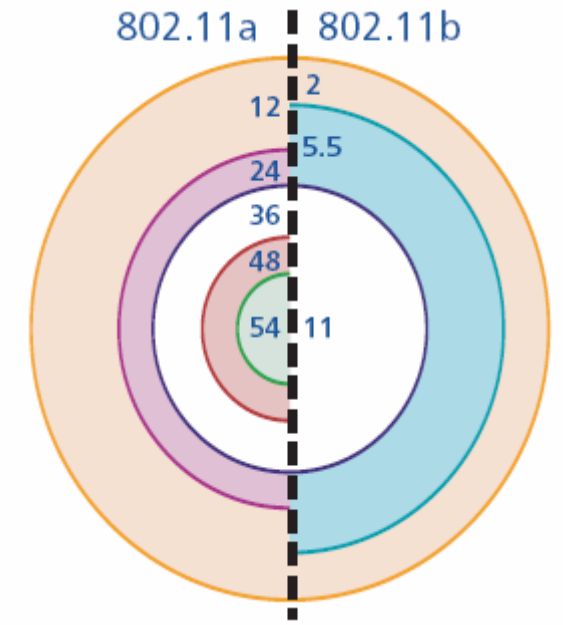


Figura 50. Comparación 802.11a vs. 802.11b

Figura que muestra una comparación de las velocidades de transferencia y los rangos de cobertura.

2.2.5.1 Uso del espectro

En las 3 bandas UNII que ocupa esta norma existen valores diferentes de potencia en cada banda y la FCC (USA) difiere de las normas europeas (ETSI) y japonesas (TELEC). La siguiente tabla muestra los canales permitidos para la FCC, su numeración y la frecuencia central de los mismos.

Regulatory domain	Band (GHz)	Operating channel numbers	Channel center frequencies (MHz)
United States	U-NII lower band (5.15–5.25)	36 40 44 48	5180 5200 5220 5240
United States	U-NII middle band (5.25–5.35)	52 56 60 64	5260 5280 5300 5320
United States	U-NII upper band (5.725–5.825)	149 153 157 161	5745 5765 5785 5805

Figura 51. Canales permitidos para FCC

En la siguiente figura se muestra una representación de los canales para la FCC. La banda baja y media acomodan 8 canales en un total de 200MHz. La banda alta acomoda 4 canales en 100MHZ. La separación entre frecuencias centrales en las tres bandas es de 20MHz.

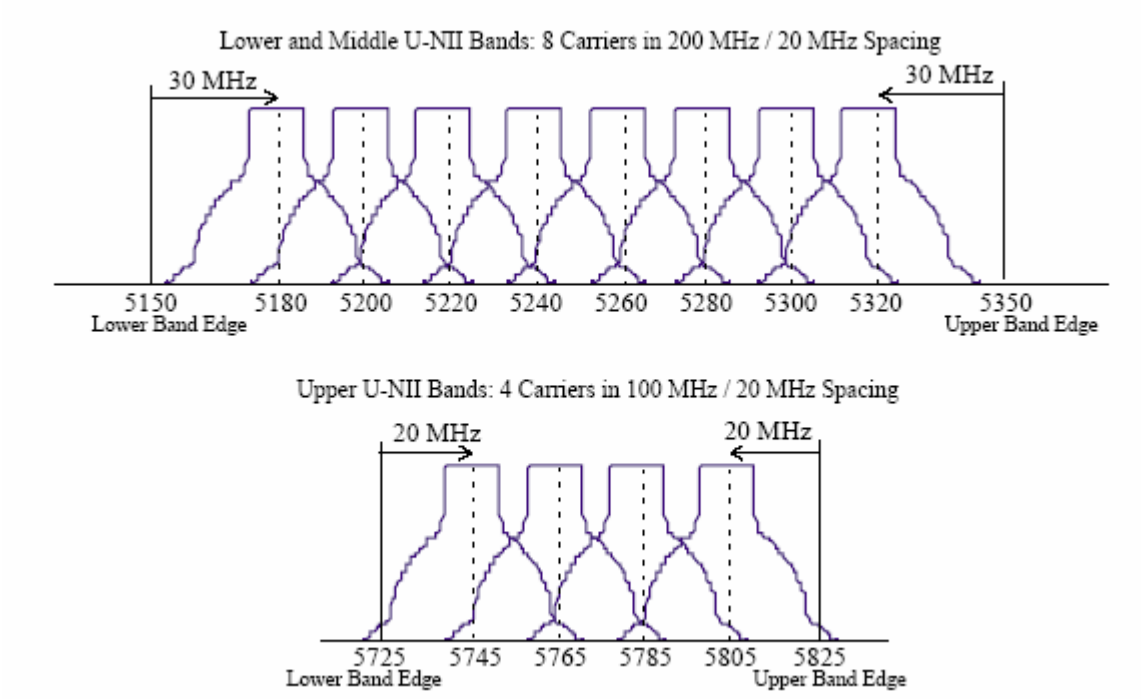


Figura 52. Representación de los canales para la FCC

2.2.5.2 Potencia de transmisión

A continuación se muestra la potencia permitida para Estados Unidos (FCC):

Frequency band (GHz)	Maximum output power with up to 6 dBi antenna gain (mW)
5.15–5.25	40 (2.5 mW/MHz)
5.25–5.35	200 (12.5 mW/MHz)
5.725–5.825	800 (50 mW/MHz)

Tabla 5. Valores de potencia

2.2.5.3 Formato de la Trama PLCP

La siguiente figura muestra la trama de la subcapa PLCP:

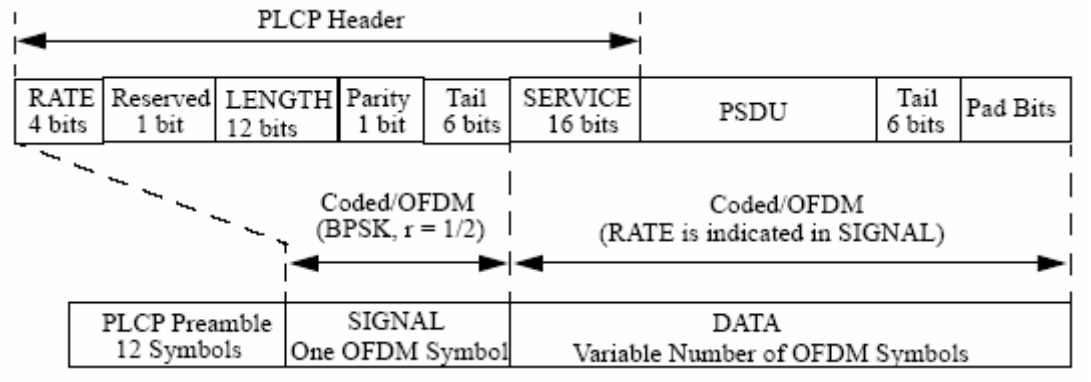


Figura 53. Trama PLCP

- **Preámbulo PLCP:** Este campo contiene 12 símbolos y permite al receptor adquirir una señal OFDM entrante.
- **Transferencia:** Este campo identifica la velocidad de transferencia y tiene los siguientes valores:

Valor del Campo	Velocidad de transferencia
1101	6Mbps
1111	9Mbps
0101	12Mbps
0111	18Mbps
1001	24Mbps
1011	36Mbps
0001	48Mbps
0011	54Mbps

Tabla 6. Velocidades de transferencia

- **Reservado:** Este campo es puesto en cero lógico.
- **Longitud: Este campo indica el número de octetos contenidos en la trama.**
- **Paridad:** Basado en los valores de los campos Velocidad, Reservado y Longitud, este campo contiene el valor de un bit que proporciona paridad positiva.
- **Cola (Tail):** Este campo siempre es puesto en ceros lógicos.
- **Servicio:** Posee 16 Bits, de los cuales del 0 – 6 están llenos de cero y son usados para sincronizar el decodificado en el receptor. Los demás bits remanentes 7 – 15 están reservados para uso futuro.
- **PSDU:** Unidades de servicio de datos.
- **Cola (Tail):** Este campo contiene seis bits (todos ceros) para funciones de procesamiento del receptor.
- **Pad:** Contiene un número de bits para que el tamaño de la trama sea igual a un múltiplo especifico de bits codificados en un símbolo OFDM. Los bits en este campo son todos puestos en cero.

2.2.5.4 Modulación OFDM

Toda la norma 802.11a está basada en el multiplexado de división de frecuencia ortogonal (OFDM), que permite un mejor uso del espectro que Spread Spectrum en la velocidad de datos en un canal, gracias el uso de múltiples canales el sistema es aún más eficiente que 802.11b, pues posee 12 en relación con los 3 de 802.11b, con esto puede manejar mejor los problemas de interferencia. El sistema está compuesto de 52 subportadoras de baja velocidad con una separación de 300 KHz. cada una, en un canal de 20 MHz, todas ellas combinadas en paralelo crean un canal de gran eficiencia (Figura 54).

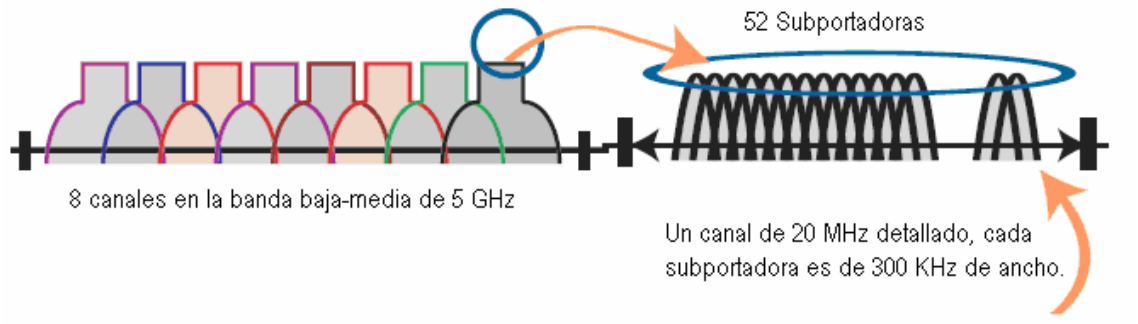


Figura 54. Portadoras en OFDM

Un modulador 802.11a convierte la señal binaria en señales analógicas a través de diferentes tipos de modulación, dependiendo de que velocidad de transferencia sea elegida. Para altas transferencias se utiliza QAM (Modulación de Amplitud en Cuadratura). A continuación se muestra una tabla en donde se observan las diferentes velocidades.

Velocidad de datos (Mbps)	Modulación
6	BPSK
9	BPSK
12	QPSK
18	QPSK
24	16-QAM
36	16-QAM
48	64-QAM
54	64-QAM

Tabla 7. Tipos de modulación según la velocidad

Ventajas:

- Eficiencia espectral. Más datos pueden viajar sobre un ancho de banda mucho menor al de otras tecnologías.
- Alta resistencia a las Multitrayectorias. Es menos probable que las señales reflejadas puedan cancelar la señal principal, haciéndola mas conveniente para interiores.
- Relativa inmunidad hacia la interferencia. Si es bloqueado un camino por donde viajan los datos, las otras portadoras siguen sin afectarse.

Desventajas:

- Costosa. Es más caro producir sus componentes debido a su complejidad.
- Alto consumo de potencia. Sistemas basados en OFDM consumen más potencia que los sistemas basados en 802.11b, siendo esto un problema para las computadoras portátiles.

2.2.5.5 Modulación QAM

La modulación de amplitud en cuadratura (QAM*)*, es una modulación lineal que consiste en modular en doble banda lateral dos portadoras de la misma frecuencia desfasadas 90º. Cada portadora es modulada por una de las dos señales a transmitir. Finalmente las dos modulaciones se suman y la señal resultante es transmitida.

Este tipo de modulación tiene la ventaja de que ofrece la posibilidad de transmitir dos señales en la misma frecuencia, de forma que favorece el aprovechamiento del ancho de banda disponible. Tiene como inconveniente que es necesario realizar la demodulación con demoduladores síncronos.

2.2.5.6 Forward Error Correction (FEC)

Con tanta información en la transmisión es necesaria una protección contra las pérdidas de datos. Forward Error Correction (FEC), es la Corrección de Error Delantera, se agregó en 802.11a pues no existe en 802.11b, es bastante simple, pues FEC consiste en enviar una copia secundaria junto con la

información primaria. Si parte de la información primaria se pierde, el aparato del receptor es el que recupera la información perdida, gracias a un sofisticado algoritmo. Por este medio si parte de la información se pierde, la información puede ser recuperada porque los datos son recibidos y analizados, eliminando la necesidad de retransmitir.

Otra forma de dañar la integridad de la transmisión es el efecto multitrayectoria. Cuando una señal de radio deja el "emisor" de la antena, es irradiada hacia el exterior, y difundida en el viaje. Si la señal es reflejada por una superficie plana, la señal original y el reflejo de la señal podrían alcanzar el "receptor" de la antena simultáneamente. Dependiendo o no del solapamiento de la señal, entonces ellas podrían aumentarse o cancelarse entre ellas. Un procesador de bandabase, o ecualizador, descifra las señales divergentes, sin embargo si el retardo es de bastante tiempo, el retardo de la señal se extiende en la próxima transmisión. OFDM especifica una baja velocidad de símbolos para reducir las posibilidades de que la señal este pasando de los límites de la siguiente transmisión, minimizando la reflexión de múltiples trayectorias.

2.2.5.7 802.11a Modo Turbo 2X

Proxim, desarrollador de dispositivos (chips para WLAN), desarrolló un modo que excedía los 54Mbps planteados originalmente usando el doble de BW o 2 canales simultáneamente, llamado modo 2X lo cual fue aprobado por la FCC, pero los canales para este modo fueron fijados como se muestra en la tabla siguiente. Este modo se ha vuelto bastante común y lo usan muchos fabricantes para lograr 108Mbps, el doble de 54Mbps.

Banda (GHz) modo 2X para la FCC	Número del canal operativo	Frecuencia central del canal (MHz)
UNII 1 banda baja (5,15-5,25)	42	5.210
	50	5.250
UNII 2 banda media (5,25-5,35)	58	5.290
	152	5.760
UNII 3 banda alta (5,725-5,825)	160	5.800

Tabla 8. Bandas utilizadas en modo turbo 2X

2.2.5.8 Ventajas de 802.11a

- Opera a 54Mbps. Esta diferencia es resultado principalmente del esquema de modulación.
- Menor interferencia en el rango de 5Ghz. La banda 2.4GHz es compartida por teléfonos inalámbricos, hornos de microondas, dispositivos Bluetooth, etc.
- Mayor capacidad de usuarios. Esto debido a que existen 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto.

2.2.5.9 Desventajas de 802.11a

- Aceptación. Japón sólo permite la mitad de los canales y en Europa el rango de los 5GHz está reservado para HiperLAN.
- Cobertura. En un rango de 50 metros se necesitaría el doble de Acces points para tener la misma área de cobertura de una red 802.11b.
- Alto consumo de potencia. Esto se debe a la técnica de modulación OFDM.

2.2.6 Estándar 802.11g

Se plantea como una evolución de 802.11b al ver la eficiencia por canal de 802.11a usando OFDM. Aunque el mayor problema es que 802.11b no posee ninguna compatibilidad con OFDM, por lo que se creó un modo mixto en que se logra una comunicación básica entre las 2 normas 802.11 b y g, en este modo 802.11g es menos eficiente que en el modo 802.11g puro. Básicamente el estándar incluye la utilización de OFDM para velocidades de transferencia altas y CCK para compatibilidad con equipos 802.11b. Los canales son los mismos que en 802.11b para esta norma así como la potencia máxima permitida.

2.2.6.1 Compatibilidad con 802.11b

A lo mejor uno caería en la confusión de creer que 802.11g es una extensión de 802.11b, pero no es así, las técnicas DBPSK, DQPSK y CCK de DSSS no son compatibles con OFDM y los sistemas no serían capaces de intercomunicarse si no fuera por el modo de compatibilidad entre 802.11b y 802.11g, solo válido para los equipos 802.11g para extender el alcance y ser compatibles con los equipos 802.11b que están reemplazando.

En los paquetes existe la siguiente forma en general.

1. Preámbulo / cabecera (header).
2. Payload (carga útil).

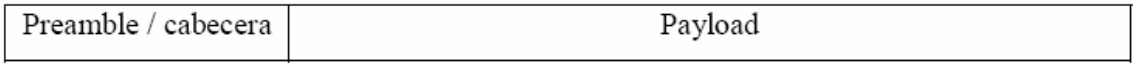


Figura 55. Forma general de los paquetes

El Preamble/Header sirve para alertar a todos los radios que están compartiendo el canal de que una transmisión esta comenzando. El Preamble es una secuencia de 1's y 0's que da un plazo de tiempo para que los radios se alisten. Cuando el Preamble es completado, los receptores deben estar listos para recibir datos. El Header sigue del Preamble y contiene importantes piezas de información, entre éstas, el tamaño en segundos del Payload. De esta manera ningún dispositivo transmitirá durante este periodo de tiempo evitando colisiones.

En 802.11b existe la modulación CCK (complementary code keying) junto con DBPSK y DQPSK, en CCK el paquete es asi:

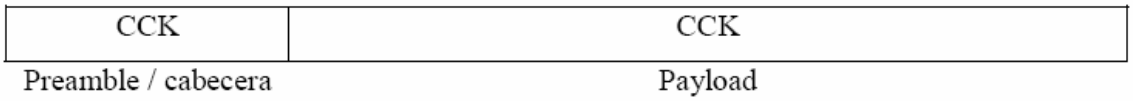


Figura 56. Forma de los paquetes en modulación CCK

Todo el paquete está en modulación CCK donde una sola señal o portadora ocupa todo el BW y es como la aclara en la siguiente figura:

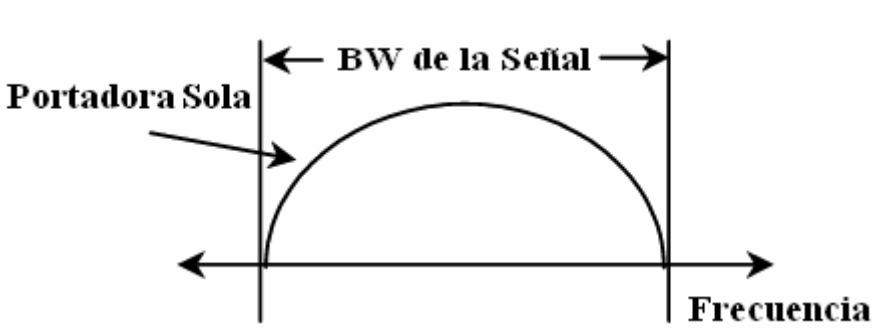


Figura 57. Ancho de banda en CCK

En 802.11g con la modulación OFDM, el paquete tiene la siguiente forma:

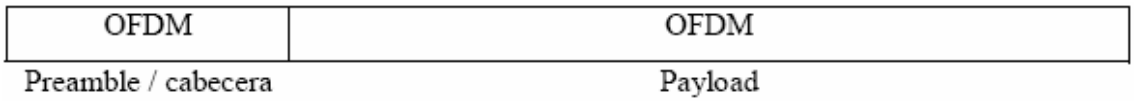


Figura 58. Forma de los paquetes en modulación OFDM

El paquete es similar al anterior, pero esta modulado en OFDM con múltiples portadoras y en las respectivas frecuencias de las normas (Figura 59).

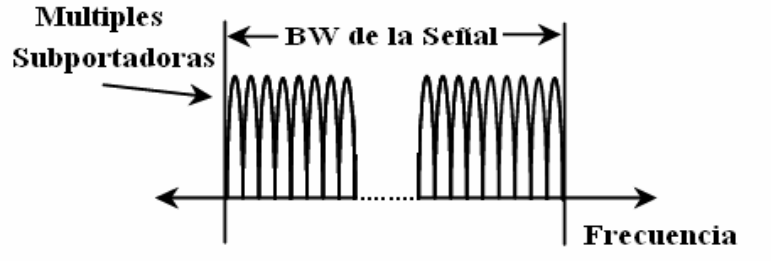


Figura 59. Ancho de banda en OFDM

Para 802.11g existe una forma de comunicarse llamado modo compatible, en el que los equipos 802.11g pueden negociar para pasar de 802.11g a 802.11b, esto sólo lo pueden hacer los equipos 802.11g, los antiguos equipos 802.11b no tienen capacidades OFDM, estas modulaciones se pueden necesitar para que equipos 802.11g alcancen más distancia de lo que OFDM les permite.

El paquete en modo de compatibilidad es el siguiente.

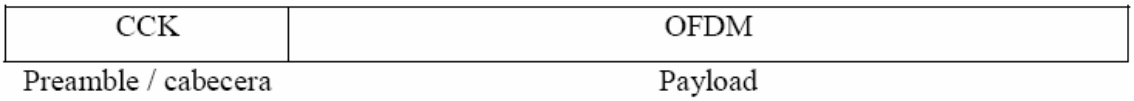


Figura 60. Forma de los paquetes en modo de compatibilidad

De esta manera cuando dispositivos 802.11g operen en presencia de dispositivos 802.11b, el Preamble/Header modulado en CCK es transmitido para alertar a todos los dispositivos 802.11b de que una transmisión va a comenzar y les informa la duración. Entonces, el Payload puede ser transmitido a una mayor velocidad usando OFDM.

Para que pueda darse una correcta sincronización los dispositivos 802.11g cambian el valor del "slot time" (9µs) al de la norma 802.11b (20µs). Aunado a esto, se utiliza el método "RTS/CTS" para mejorar la compatibilidad entre las normas.

En la siguiente tabla se muestra las velocidades de transferencia y la modulación utilizada:

Velocidad de Transferencia (Mbps)	Tipo de transmisión	Tipo de Modulación
54	OFDM	64 QAM
48	OFDM	64 QAM
36	OFDM	16 QAM
24	OFDM	16 QAM
18	OFDM	QPSK
12	OFDM	QPSK
11	DSSS	CCK
9	OFDM	BPSK
6	OFDM	BPSK
5.5	DSSS	CCK
2	DSSS	QPSK
1	DSSS	BPSK

Tabla 9. Velocidades de transferencia según el tipo de modulación utilizada

2.2.7 Puentes inalámbricos (Wireless Bridges)

Los puentes inalámbricos permiten unir redes físicamente separadas entre sí sin necesidad de tender cables. En algunos casos, como cuando se ha de atravesar una vía pública, esto supone un ahorro considerable frente al alquiler de circuitos dedicados. Además permite la conexión a una velocidad mayor de lo que normalmente es posible en enlaces telefónicos.

A pesar de sus ventajas conviene saber cuales son las limitaciones de los enlaces entre puentes inalámbricos. Por un lado, aunque se realice un enlace punto a punto entre dos puentes la comunicación vía radio es half duplex, ya que ambos sentidos de la comunicación comparten un canal.

Físicamente el puente inalámbrico es similar a un punto de acceso, con las adaptaciones necesarias para su nueva función. Dado que el puente es normalmente un dispositivo estático se pueden utilizar antenas muy direccionales para concentrar el haz radioeléctrico en la dirección de la otra antena con la que se desea contactar. Con las condiciones de emisión permitidas es posible llegar hasta una distancia de 10Km siempre y cuando se disponga de visión directa entre las antenas.

A menudo las antenas se colocan en el exterior del edificio, para minimizar el riesgo de que se presenten obstáculos en el camino. Esto conlleva que a menudo se requiera un cable de conexión de cierta longitud entre el puente y la antena. A estas frecuencias la atenuación de la señal producida por el cable es considerable, por lo que es importante minimizar el trayecto de este cable y utilizar en cualquier caso cable de baja atenuación, lo cual significa que se debe instalar el puente lo más cerca posible de la antena alargando el cable de la LAN en caso necesario.

También es posible interconectar entre sí varios edificios en una configuración multipunto, lo cual supone un ahorro en el número de equipos a instalar. Como es lógico en este caso la capacidad será compartida por todos ellos de acuerdo al protocolo CSMA/CA, y será conveniente utilizar mensajes RTS/CTS pues puede haber estaciones ocultas.

El tipo y configuración de las antenas a ubicar en cada edificio dependerá de la distancia y la situación concreta de cada caso.

2.2.7.1 Tipo de Conexiones

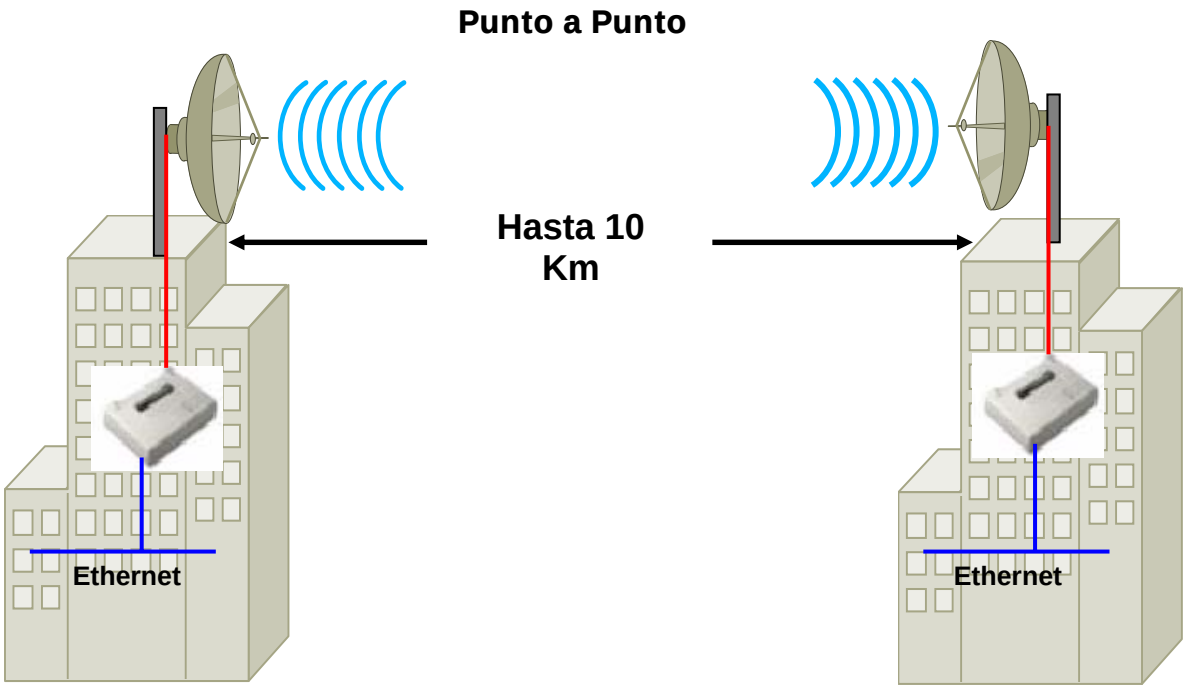


Figura 61. Conexión Punto a punto

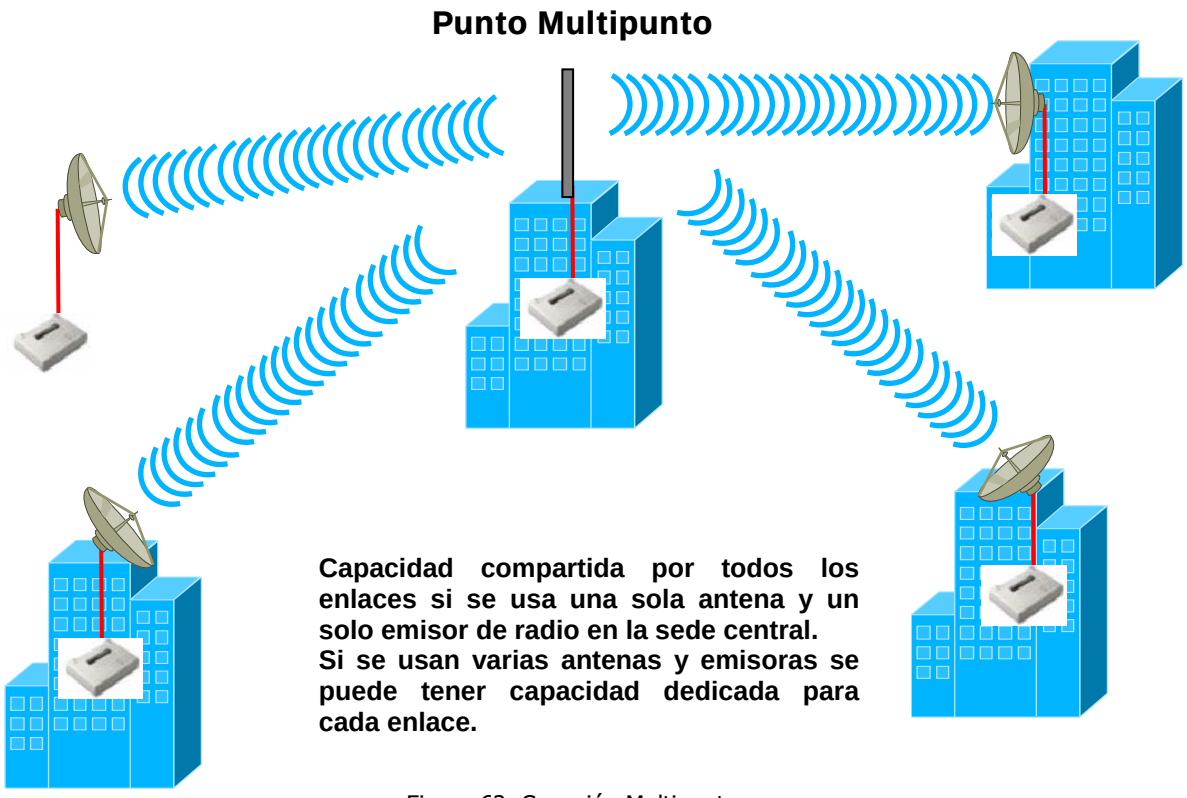


Figura 62. Conexión Multipunto

2.3 WiMAX

WiMAX es una tecnología inalámbrica basada en estándares que proporciona conexiones de banda ancha de alto rendimiento a grandes distancias. La implementación del estándar IEEE 802.16, WiMAX (abreviatura en inglés de Interoperabilidad mundial de acceso de microondas) proporciona capacidad de conexión de red de área metropolitana (MAN) a velocidades de hasta 75Mbps por estación base, con tamaños de células normales de 2 a 10 kilómetros.

Esto representa suficiente ancho de banda que una sola estación de base puede admitir de manera simultánea más de 60 empresas con conectividad tipo T1/E1 o cientos de hogares con conexión tipo DSL (línea digital de suscriptor).

Para cubrir los requerimientos de los diferentes tipos de accesos, dos versiones de WIMAX han sido definidas. La primera esta basada en el estándar IEEE 802.16-2004 y está optimizada para acceso fijo y nómada (tarjetas PCMCIA y CPEs, Costumer Premises Equipment: Equipos que van donde están los usuarios). La certificación inicial de productos se basará en esta versión. La segunda versión esta diseñada para soportar movilidad y portabilidad, y esta basada en el estándar IEEE 802.16e. La siguiente figura ilustra lo explicado anteriormente:

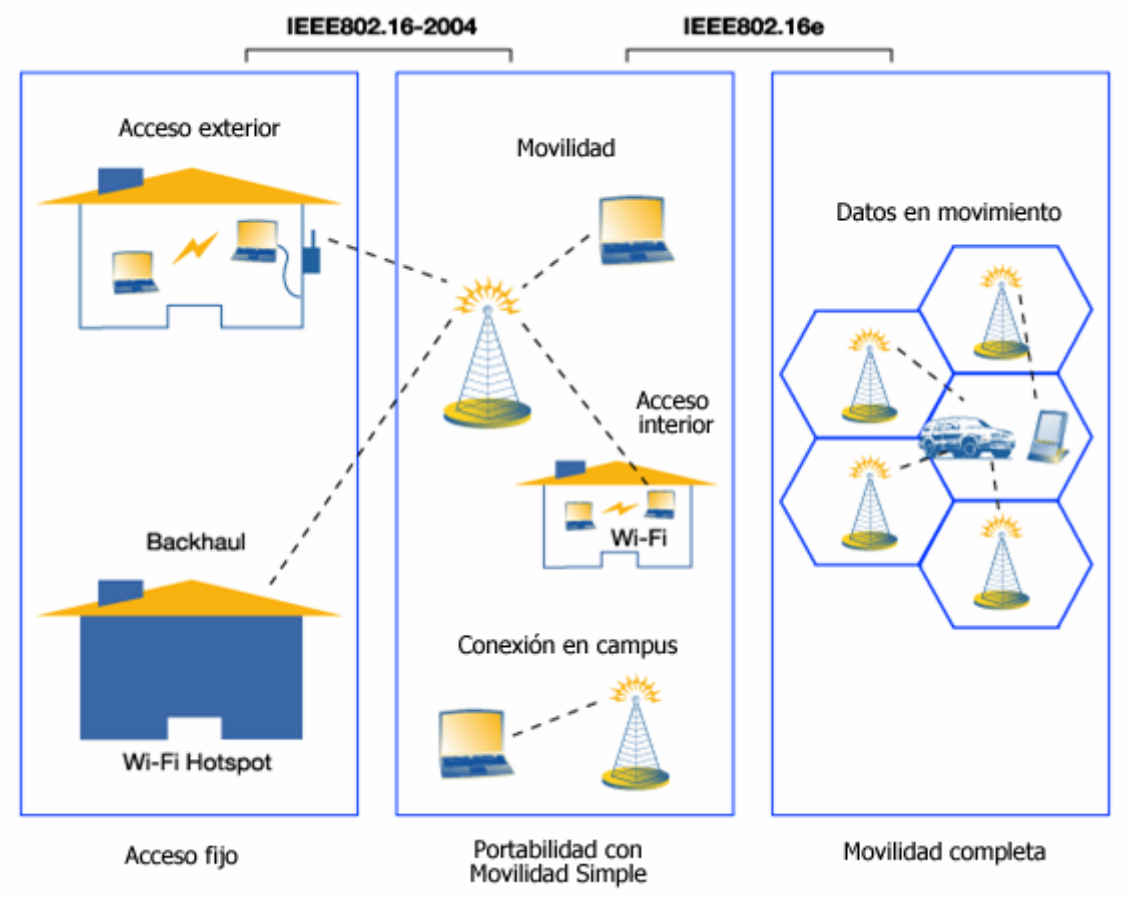


Figura 63. Estándar 802.16

La certificación de los equipos para acceso fijo y nómada comenzó a finales del 2005 además de que a finales de ese mismo año fue aprobada por la IEEE la segunda norma WIMAX que permitirá que computadoras portátiles se conecten a estas redes a final del 2006. Se espera que en el 2007 se certifiquen todos los demás dispositivos de acceso móvil como PDAs y teléfonos móviles.

WiMAX promete dar conectividad inalámbrica de alta velocidad de una manera más simple y redituable que las tecnologías celulares actuales, y ofrece la escalabilidad para dar acceso de banda ancha al alcance del bolsillo. Debido a que la infraestructura inalámbrica se puede extender para proporcionar compatibilidad con los dispositivos móviles y portátiles, WiMAX tiene ventajas adicionales para desarrollar economías que no cuentan con una infraestructura generalizada de banda ancha. Al saltar hacia la tecnología más reciente, obtienen no sólo la mejor conectividad de banda ancha que se tiene en un entorno fijo, sino también el potencial de agregar fácilmente conectividad portátil total para datos de alta velocidad en el futuro.

2.3.1 Estándar IEEE 802.16

WIMAX está basado en los estándares IEEE 802.16 y ETSI HiperMAN. La última versión del estándar IEEE 802.16, 802.16-2004 (previamente conocida como 802.16d) fue ratificada en Julio del 2004 e incluye las versiones 802.16-2001, 802.16c en el 2002, y 802.16a en el 2003. Cubre aplicaciones con y sin línea de vista (LOS y NLOS) en frecuencias de 2-66GHz y especifica únicamente las capas Física y MAC del modelo OSI.

Los cambios introducidos en 802.16-2004 se enfocaron en las aplicaciones fijas y nómadas en las frecuencias 2-11GHz. Dos técnicas de modulación son soportadas en este estándar: OFDM con 256 portadoras y OFDMA con 2048 portadoras.

En Diciembre del 2002, el grupo de trabajo "e" fue creado para soportar operaciones fijas y móviles en frecuencias por debajo de los 6GHz y fue aprobado recientemente (diciembre del 2005) por la IEEE. La nueva versión soporta la técnica de modulación SOFDMA (una variación de OFDMA), la cual permite un número variable de portadoras, además de soportar OFDM y OFDMA. La portadora repartida en el modo OFDMA esta diseñada para minimizar el efecto de la interferencia por dispositivos con antenas omnidireccionales. Además, IEEE 802.16e ofrece mejoras para soportar Múltiples-Entradas Múltiples-Salidas (MIMO) y Sistemas de Antenas Adaptativas (AAS). También proporciona capacidades de ahorro de energía para dispositivos móviles y características de seguridad más extensas.

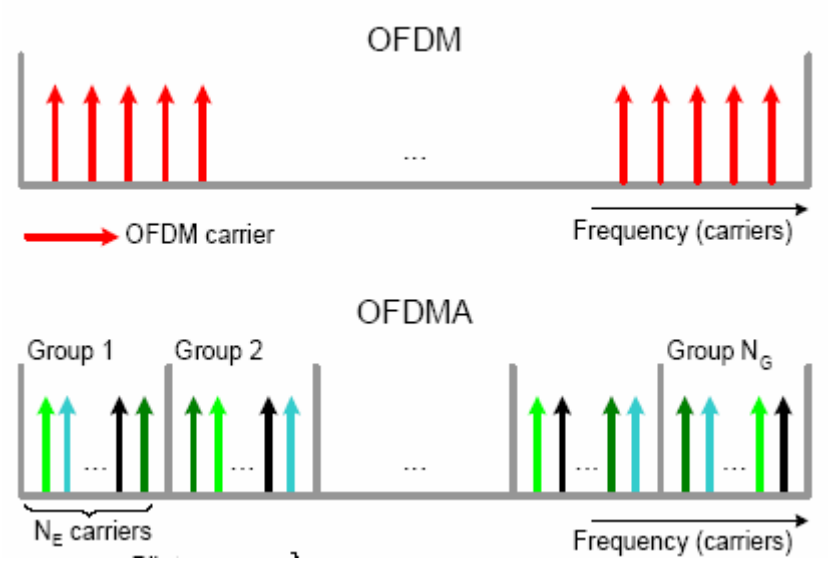


Figura 64. Portadoras en OFDM y OFDMA

En la figura anterior se muestra como en OFDM, todas las portadoras son transmitidas en paralelo con la misma amplitud. OFDMA divide el espacio de portadoras en N_G grupos con N_E portadoras cada uno dentro de N_E subcanales. En OFDMA con 2048 portadoras los valores son los siguientes N_E=32 y N_G=48 para el enlace de subida y para el de bajada N_E=32 y N_G=53.

El estándar ofrece gran flexibilidad de diseño que incluye compatibilidad con las bandas de frecuencia con licencia y exentas de licencia, amplitud de canal que va de 1.5MHz a 30MHz, calidad de servicio (QoS) por conexión y bases sólidas de seguridad. 802.16 está optimizado para ofrecer altas velocidades de datos. La sofisticada arquitectura de Control de acceso al medio (MAC) también puede admitir de forma simultánea multimedia en tiempo real y aplicaciones asincrónicas como VoIP. Esto significa que WiMAX tiene una posición única para sustentar aplicaciones que requieren de QoS avanzado, como son la telefonía por Internet y la transmisión de vídeo en tiempo real.

Una conexión WiMAX soporta servicios paquetizados como IP y voz sobre IP (VoIP), como también servicios conmutados (TDM), E1/T1 y voz tradicional (clase-5); también soporta interconexiones de ATM y Frame Relay.

Sobre los sistemas WiMAX se pueden hablar de un sin número de arquitecturas posibles, las cuales dependen del tipo de aplicación que se esté utilizando.

3

Seguridad

Introducción

En una red convencional (con cables), para que ésta sea atacada, el atacante debe estar conectado físicamente a esa red, lo cual reduce mucho el riesgo de una agresión (en el caso de redes particulares: empresa, casa, etc.), pero cuando hablamos de redes inalámbricas nuestra información está siendo transmitida por medio del aire mediante ondas de radio y ésta puede ser interceptada en una distancia de un radio de, aproximadamente, 100m.

Aunque sabemos que una red informática no puede ser segura al 100%, debemos proporcionar el máximo de seguridad a nuestra red para que, sea sumamente difícil entrar a ella, o "casi nadie" pueda entrar, con lo que estaríamos hablando de un nivel de seguridad alrededor del 99%.

Para ello deberemos tener en cuenta los siguientes aspectos:

- Cualquiera dentro de un radio de 100m, puede ser un intruso potencial.
- La autenticación de los usuarios debe realizarse con seguridad, ya que se están intercambiando datos muy importantes.
- Se debe asegurar la conexión con la red correcta.
- Los datos que se transmitan, deben cifrarse con la utilización de llaves de cifrado adecuadas.

3.1 Tipos de Seguridad

3.1.1 Seguridad de la información

Los objetivos fundamentales en seguridad son: prevenir la revelación, la modificación y la utilización no autorizada de datos, recursos de computadora y de red. La definición del estándar ISO 7498-2 [ISO, 1989] define cinco elementos básicos que constituyen la seguridad de un sistema: la **confidencialidad** de los datos, la **autenticación** de los datos, la **integridad** de los datos, el **control de acceso** (disponibilidad) y el **no repudio**.

Confidencialidad implica que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas. *Autenticación* define mecanismos para garantizar la procedencia de la información, ya sea a nivel de usuario o de computadora. *Integridad* implica que los datos no han sido modificados o corrompidos de manera alguna desde su transmisión hasta su recepción. El *control de acceso* establece la forma en que el recurso está disponible cuando es requerido. El *no repudio* es la garantía de transmisión y recepción de información, busca proteger al emisor de que el receptor niegue haber recibido el mensaje, y proteger al receptor de que el transmisor niegue haber enviado el mensaje.

En seguridad de información, se consideran seis elementos sobre los cuales se han hecho desarrollos en busca de proporcionar ambientes protegidos:

***Seguridad física*:** un elemento de atención básica, los recursos deben ser protegidos físicamente de accesos no autorizados, accidentes, robos, etc. Su objetivo es preservar los recursos de cómputo contra usos u abusos no autorizados, así como proteger los datos que representan y codifican la información de daños, revelaciones y modificaciones accidentales o deliberadas.

Segu*ridad de procedimientos*: elemento enfocado a las medidas de protección en los procesos y procedimientos.

***Seguridad de personal*:** elemento enfocado a la definición de privilegios, y accesos de personal involucrado con los recursos.

***Seguridad de emanación de compromisos*:** elemento enfocado a la definición de responsabilidades y compromisos en el manejo de la información.

***Seguridad de sistemas operativos*:** elemento enfocado a la protección de servicios y usuarios, accesos no autorizados al sistema operativo de una computadora.

***Seguridad de comunicaciones*:** elemento enfocado a la transmisión segura de información a través de medios de comunicación. Su objetivo es proteger los datos que representan y codifican la información durante su transmisión en redes.

Prevención es la palabra clave en seguridad, se han desarrollado una gran diversidad de técnicas y herramientas de prevención a nivel de aplicaciones, siempre dependientes del sistema operativo o la aplicación que se utilice. Los protocolos de seguridad buscan brindar servicios de seguridad en la transmisión de información, sin importar el tipo, procedencia, sistema operativo o aplicación que la genere.

3.2 Servicios de Seguridad

3.2.1 Servicios de autenticación

Los servicios de autenticación son para proporcionar autenticación en el proceso de comunicación entre dos entidades parejas o para la autenticación del origen de los datos.

1. El servicio de autenticación de entidades parejas sirve para proporcionar la capacidad de verificar que la entidad pareja de una asociación es quien dice ser. En concreto, el servicio de autenticación de entidades parejas permite asegurarse de que una determinada entidad no está intentando realizar una mascarada o una réplica no autorizada de una asociación anterior. La autenticación de entidades parejas se realiza típicamente durante la fase de establecimiento de la conexión, o en ocasiones, durante la fase de transferencia de datos.

2. El servicio de autenticación del origen de los datos permite reclamar el origen de las fuentes de los datos recibidos. Sin embargo, el servicio de autenticación del origen de los datos no proporciona protección contra la duplicación o la modificación de unidades de datos. En este caso, debe utilizarse conjuntamente un servicio de integridad de datos. La autenticación del origen de los datos se realiza generalmente durante la fase de transferencia de datos.

Los servicios de autenticación son importantes, puesto que se requieren para las tareas de autorización y contabilidad. La autorización se refiere al proceso de concesión de derechos, lo que incluye la concesión al acceso basada en los derechos de acceso. La contabilidad se refiere a la propiedad que asegura que las acciones de un principal guardarán traza sólo para ese principal.

3.2.2 Servicios de control de acceso

Los servicios de control de acceso sirven para proteger los recursos del sistema contra su utilización no autorizada. Estos servicios están estrechamente relacionados con los servicios de autenticación: un usuario o proceso que pretenda ocupar el lugar de otro usuario deberá autenticarse antes de que un servicio de control de acceso pueda obtener acceso efectivo a un recurso del sistema.

3.2.3 Servicios de confidencialidad de datos

Los servicios de confidencialidad de datos protegen los datos de revelaciones no autorizadas.

1. Los servicios de confidencialidad orientados a conexión proporcionan confidencialidad a todos los datos transmitidos durante la conexión.

2. Los servicios de confidencialidad no orientada a conexión proporcionan confidencialidad de unidades simples de datos.

3. Los servicios de confidencialidad de campo selectivo proporcionan confidencialidad de campos específicos de los datos durante una conexión, o para una unidad de datos.

4. Los servicios de confidencialidad de flujo de tráfico proporcionan protección de información que de otra forma podría resultar comprometida u obtenida indirectamente mediante un análisis de tráfico.

3.2.4 Servicios de integridad de datos

Los servicios de integridad de datos protegen los datos de modificaciones no autorizadas.

1. Los servicios de integridad orientados a conexión con recuperación proporcionan integridad a los datos durante una conexión. Si es posible, permiten la recuperación de fallos de integridad.

2. Los servicios de integridad orientados a conexión sin recuperación proporcionan integridad a los datos durante una conexión. No se recuperan los fallos de seguridad.

3. Los servicios de integridad de campo seleccionado orientados a conexión proporcionan integridad de campos específicos en los datos durante la conexión.

4. Los servicios de integridad no orientados a conexión proporcionan integridad a unidades de datos.

5. Los servicios de integridad de campo seleccionado no orientados a conexión proporcionan integridad de campos específicos dentro de las unidades de datos.

3.2.5 Servicios de no rechazo

Los servicios de no rechazo proporcionan cierta protección contra el remitente de una mensaje o acción que niega serlo, o contra el receptor de un mensaje que niega haberlo recibido. Por lo tanto, se debe distinguir dos servicios de no rechazo:

1. Los servicios de no rechazo con prueba de origen sirven para proporcionar el receptor de un mensaje con prueba de origen.

2. Los servicios de no rechazo con prueba de destino sirven para proporcionar el remitente de un mensaje con prueba de destino.

Dentro del área de Seguridad, se manejan diversos términos para identificar los factores que intervienen, los conceptos principales son: vulnerabilidades, ataques, contramedidas y amenazas.

3.3 Vulnerabilidades

El software está desarrollado por humanos, quienes modelan e implantan programas a su criterio, concepto y conocimiento del lenguaje de programación que utilizan, es común, en consecuencia, encontrar imperfecciones en los sistemas. Son estas imperfecciones las que propician oportunidades para

accesos no autorizados, las que se conocen como vulnerabilidades de los sistemas.

3.4 Ataques

Los ataques son los medios por los cuales se explotan las vulnerabilidades, se identifican dos tipos de ataques: extracción (wiretapping) pasiva y extracción activa.

En la extracción pasiva el atacante escucha, sin modificar mensajes o afectar la operación de la red. Generalmente no puede detectarse este tipo de ataque, pero sí prevenirse mediante mecanismos como el cifrado de información.

Los objetivos del atacante son la intercepción y el análisis de tráfico en la red. Al estar escuchando el tráfico, el atacante puede identificar:

- El origen y destino de los paquetes de comunicación, así como la información de cabecera
- Monitorear el tráfico y horarios de actividad.
- Identificar el uso de protocolos y observar la transferencia de datos entre protocolos que no utilicen cifrado, por ejemplo la versión no segura de telnet o ftp que transfieren la clave de usuario en texto simple.

En la extracción activa el atacante modifica los mensajes o irrumpe la operación de la red. El atacante tiene como objetivo modificar datos o bien crear tráfico falso. Este tipo de ataque, generalmente puede detectarse, pero no prevenirse. La gama de actividades identificadas sobre ataques conocidos puede clasificarse en cuatro categorías:

1. Modificación de mensajes: al interceptar mensajes, se altera su contenido o su orden para irrumpir su flujo normal.
2. Degradación y fraude del servicio: tiene como objetivo intervenir el funcionamiento normal de un servicio, impide el uso o la gestión de recursos en la red. Ejemplo de este ataque es el de negación de servicio (DoS, Denial of Service), donde se suprimen los servicios de SMTP, HTTP, FTP, DNS, entre otros.
3. Reactuación: al interceptar mensajes legítimos, se capturan y repiten para producir efectos diversos, como el ingresar dinero repetidas veces en una cuenta de banco.
4. Suplantación de identidad: Este es uno de los ataques más completos y nocivos. El intruso o atacante adopta una identidad con privilegios en una red y explota esos privilegios para sus fines. Un ataque con prioridad de atención para todo administrador de red es el "spoofing" donde el intruso obtiene servicios basados en la autenticación de computadoras por su dirección IP. Es recomendable seguir una estrategia y de preferencia tener una herramienta para combatirlos.

3.5 Contramedidas

Lo más importante es contar con una Política de Seguridad, un documento legal y con apoyo directivo, que define la misión, visión y objetivos de los recursos de red e información en cuestión. En una política se define lo que es permitido y lo que no, las necesidades de confidencialidad, autenticación y otros servicios de seguridad para los recursos involucrados.

Las contramedidas son entonces, las políticas de seguridad apoyadas por todos los medios técnicos o de procedimientos que se aplican y desarrollan para atender vulnerabilidades y frustrar ataques específicos. Ejemplos: reglamentos, firewalls, antivirus, kerberos, radius, entre muchos otros comerciales o de dominio público.

3.6 Amenazas

Las amenazas están dadas por condiciones de entorno, dada una oportunidad y adversarios motivados y capaces de montar ataques que explotan vulnerabilidades, podría producirse una violación a la seguridad (confidencialidad, integridad, disponibilidad y/o uso legítimo). Los perfiles de capacidades de los atacantes se identifican como sigue:

- Inserción de mensajes solamente.
- Escuchar e introducir mensajes.
- Escuchar y obstruir.
- Escuchar, obstruir e insertar mensajes.
- Escuchar y remitir un mensaje ("hombre en el medio")
- Capacidades activas y pasivas de forma unidireccional o bidireccional

Cada enlace en una red y cada recurso es susceptible a diferente tipo de amenazas, de ataques, y quizá a diferentes atacantes. El análisis de riesgos y el monitoreo constante de vulnerabilidades pueden identificar las amenazas que han de ser contrarestadas, así como especificar los mecanismos de seguridad necesarios para hacerlo.

De acuerdo con la figura 65, las cuatro categorías generales de amenazas que se utilizan en la actualidad son las siguientes:

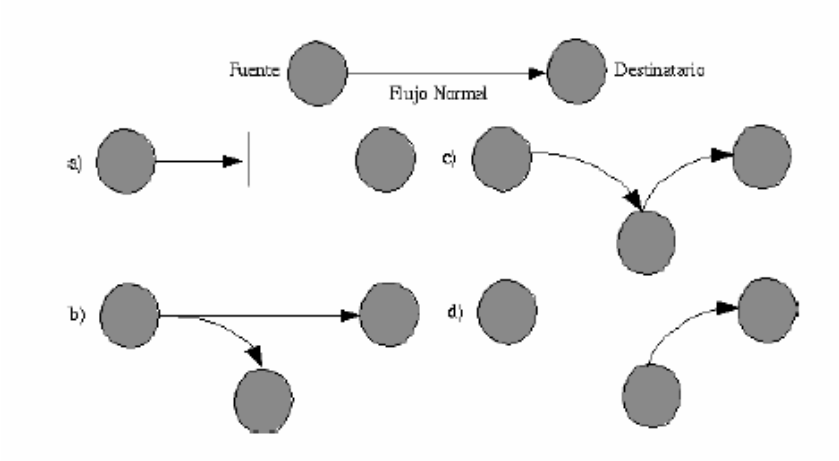


Figura 65. Amenazas

a) *Interrupción*: es una amenaza contra la disponibilidad, el ataque ocasiona que un recurso del sistema deje de estar disponible. Ejemplos: DoS, destruir un elemento de hardware o cortar una línea de comunicación.

b) *Intercepción*: es una amenaza contra la confidencialidad, el ataque produce la captura no autorizada de información en el medio de transmisión. Ejemplos: *Sniffers*, lectura de cabeceras, intercepción de datos.

c) *Modificación*: es una amenaza contra la integridad, el ataque produce no solo el acceso no autorizado a un recurso sino también la capacidad de manipularlo. Ejemplos: modificación del contenido de mensajes interceptados, alterar programas para modificar su funcionamiento.

d) *Falsificación*: es una amenaza contra la autenticidad, el ataque produce que una entidad no autorizada inserte mensajes falsos en el sistema. Ejemplos: sustitución de usuarios, alterar archivos, inserción de mensajes espurios en la red.

3.7 Mecanismos específicos de seguridad

Se han desarrollado una gran variedad de algoritmos, mecanismos y técnicas para brindar protección a los recursos informáticos, y garantizar la integridad, confidencialidad y control de acceso de información.

La confidencialidad es necesaria para mantener un secreto, pero sin autenticación, no puede saberse que la persona con la que se está compartiendo ese secreto, es quien dice ser, y sin la confianza de la integridad del mensaje recibido, no se sabe si el mensaje es el mismo al que fue enviado. Los mecanismos descritos en esta sección están enfocados a garantizar estos aspectos.

3.7.1 Criptología

La Criptología (del griego criptos=oculto y logos=tratado, ciencia) es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: criptografía y criptoanálisis.

La criptografía se ocupa del diseño de procedimientos para cifrar, es decir, para enmascarar una determinada información de carácter confidencial. El criptoanálisis, por su parte, se ocupa de romper esos procedimientos de forma no autorizada, para recuperar la información.
Ambas disciplinas siempre se han desarrollado de forma paralela, pues cualquier método de cifrado lleva siempre emparejado su criptoanálisis correspondiente.
Los algoritmos criptográficos proveen confidencialidad de datos al convertir un mensaje (texto plano) en garabatos (cibertexto) y viceversa. Los sistemas de criptografía se han clasificado como se muestra en la figura. Los sistemas simétricos basan su cifrado y descifrado en una sola llave, los sistemas asimétricos o de llave pública, basan su seguridad en llaves diferentes, una privada para descifrar y una pública para cifrar. Los algoritmos de bloque (Block) no poseen memoria interna, los mismos bloques utilizados para el texto plano son siempre relacionados a los bloques del cibertexto. Los sistemas de ráfaga (Stream) poseen memoria interna, los bloques del texto plano, no siempre son transformados a bloques idénticos de cibertexto. Los algoritmos criptográficos, sin importar su simetría, son conmutativos:

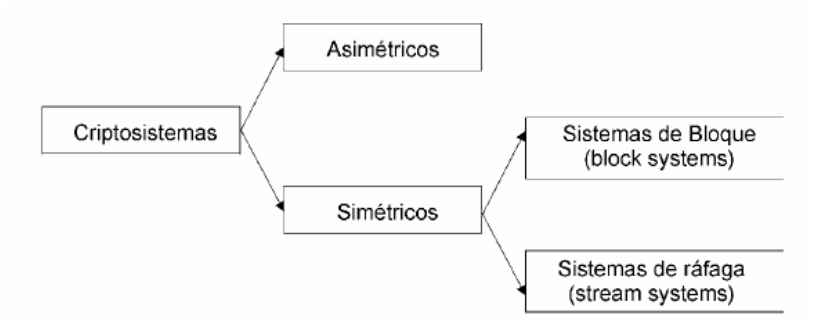


Figura 66. Sistemas de criptografía

Para caracterizar un algoritmo seguro o robusto se manejan tres categorías:

a) Incondicionalmente seguro, solo hay un algoritmo de este tipo y no es implementable, ya que no existe manera de generar números realmente aleatorios, siempre dependen de una semilla,
b) Probablemente seguro, el problema matemático para descifrarlo es altamente complicado ($O(2^n)$),
c) Computacionalmente seguro (2^{70}), se requiere gran capacidad de cómputo para descifrarlo.

3.7.2 Mecanismos de integridad de datos

La integridad, como se ha referido antes, se refiere a la garantía de que la información no ha sido alterada durante su transmisión. Así como hay cibersistemas simétricos y asimétricos, también hay métodos simétricos y asimétricos para garantizar la integridad de mensajes. Los MAC (Message Authentication Codes), son códigos que utilizan funciones hash (un algoritmo criptográfico de un solo sentido que cambia una variable de tamaño arbitrario y la convierte en una variable de tamaño fijo). El MAC se genera al aplicar la función hash a una llave privada con el mensaje, el resultado se transmite en conjunto con el mensaje, y la verificación del MAC permite aplicar la función hash a la llave secreta con el mensaje para producir un compendio temporal, y comparar este compendio con el atado al mensaje. Este proceso se llama transformación fundamental o *keyed hashing*. Es importante realizar el proceso completo, porque solo aplicar la función hash a unos datos no provee autenticación, es como una comprobación de paridad (checksum), una función *keyed hash* es un MAC.

3.7.3 Mecanismos de control de acceso y autenticación

La autenticación es uno de los problemas más complicados en seguridad. Implica reconocer y garantizar que alguien (persona o computadora) es quien dice ser. La autenticación es un servicio básico de seguridad. Puede hablarse de autenticación con criptografía o sin criptografía, los grandes problemas radican en la autenticación de personas y los mecanismos de distribución de llaves y certificados. Las firmas digitales es uno de los mecanismos más utilizados para el intercambio de mensajes en el correo electrónico. Los mecanismos de llaves digitales implican esquemas de confianza, el esquema común es que una persona cree su llave digital, y solicite que al menos otras dos firmen su llave, de esta manera hay al menos dos testigos de que esa llave le pertenece a esa persona.

3.8 Métodos para seguridad en redes inalámbricas

3.8.1 Filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

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

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos

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

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

3.8.2 WEP *(Wired Equivalent Privacy)*

El estándar 802.11b, define el uso del protocolo WEP para proveer a una red inalámbrica de seguridad, cifrando los datos que viajan en las ondas electromagnéticas en las capas más bajas del modelo OSI, capa física y capa de enlace.

3.8.2.1 Cifrado

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso. Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida. El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un *valor de comprobación de integridad* (ICV). Dicho valor de comprobación de integridad se concatena con el texto en claro. El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización. El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto ó que los datos han sido corrompidos. Si los dos valores de ICV son idénticos, el mensaje será autenticado; en otras palabras, las huellas digitales coinciden.

3.8.2.2 Autenticación

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red. De los dos niveles, la autenticación mediante clave compartida es el modo seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el desafío (challenge). La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP. Si no está habilitado, el sistema revertirá de manera predeterminada al modo de sistema abierto (inseguro), permitiendo en la práctica que cualquier estación que esté situada dentro del rango de cobertura de un punto de acceso pueda conectarse a la red. Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes. Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. En tales redes, no es posible realizar una autenticación individualizada; todos los usuarios, incluyendo los no autorizados, que dispongan de la clave compartida podrán acceder a la red. Esta debilidad puede tener como resultado accesos no autorizados, especialmente si el sistema incluye un gran número de usuarios. Cuantos más usuarios haya, mayor será la probabilidad de que la clave compartida pueda caer en manos inadecuadas.

3.8.2.3 Funcionamiento

Se basa en el algoritmo de cifrado RC4 y puede utilizar llaves de 64 ó 128 bits, que en la práctica son de 40 ó 104 bits, ya que los 24 bits restantes son para el IV (Vector de Inicialización).

3.8.2.3.1 Llaves

La llave puede ser de 40 ó 104 bits, se genera a partir de una clave estática de forma automática, aunque también existe software que permite crear la llave manualmente. Esta clave debe ser conocida por todos los clientes que vayan a conectarse a la red, lo que implica que en la mayoría de ocasiones, se utilicen

claves sencillas para poder ser fácilmente recordadas y no se cambien frecuentemente.

A partir de la clave elegida, se generarán cuatro llaves de 40 o 140 bits y solo una de ellas será la llave que se utilizará en el cifrado WEP.

Si introducimos como clave *My Passphrase,* y utilizamos llaves de 64 bits (en realidad 40), estos son los pasos que se seguirán:

1. Se hace una operación XOR con la clave introducida (cadena ASCII) para obtener una semilla de 32 bits:

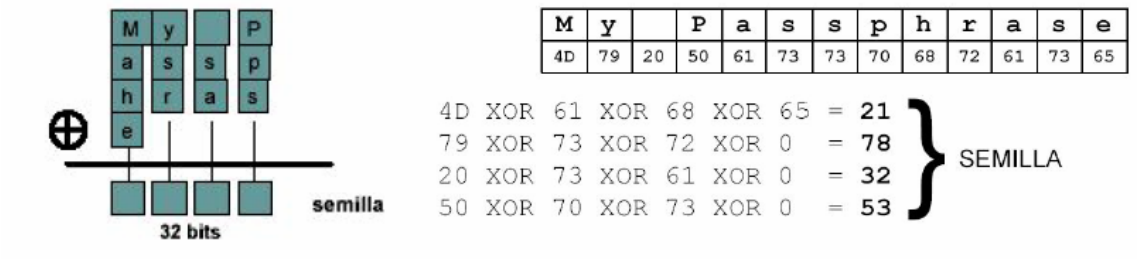


Figura 67. Obtención se semilla

2. El PRNG (*Generador de números pseudoaleatorios*) utiliza la semilla para generar 40 cadenas de 32 bits cada una. 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 40 bits, solo una de ellas se utilizará para cifrar.

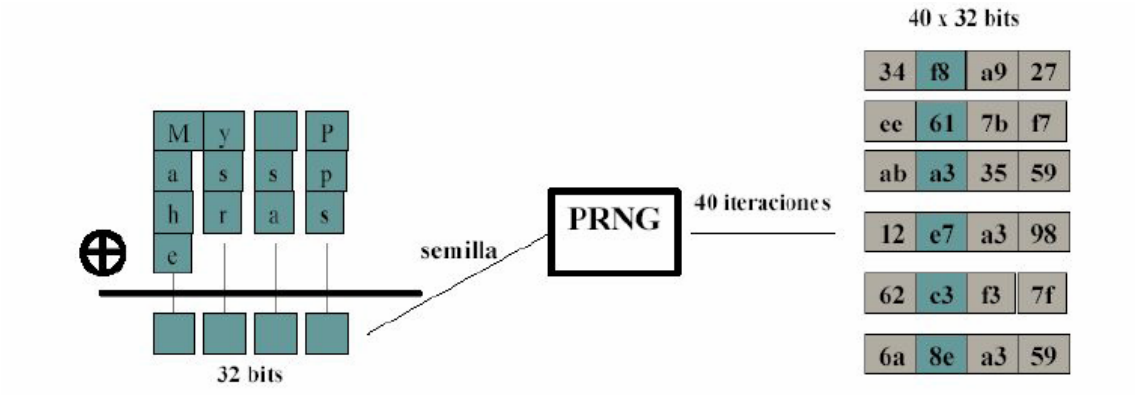


Figura 68. Generación de cadena de 32 bits

3.8.2.3.2 Cifrado

Para generar una trama cifrada mediante WEP, partimos de la trama que se quiere enviar (sin cifrar), que está compuesta por una cabecera (Header) y datos (Payload), para cifrarla se siguen los siguientes pasos:

1. Calcular el CRC de 32 bits del payload de la trama. CRC (*Comprobación de Redundancia Cíclica*), es un algoritmo que genera un identificador único del payload en cuestión, que nos servirá para comprobar que el payload recibido es el mismo que el que ha sido enviado, ya que será

calculado por el emisor y por el receptor. El CRC se añadirá a la trama como *valor de chequeo de integridad*, ICV (*Integrity Check Value*).

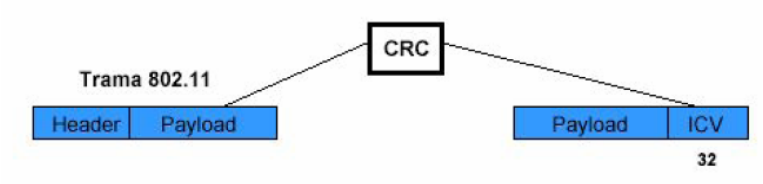


Figura 69. Calculo del CRC

2. Por otro lado debemos seleccionar una llave de las cuatro posibles:

Figura 70. Selección de llaves

3. Se añade el IV (*Vector de Inicialización*) de 24 bits al principio de la llave seleccionada. El IV es un contador que va cambiando a medida que creamos tramas, aunque si se quiere puede ser siempre 0. En el campo IV, aparte del vector de inicialización, también está el número de llave (*keynumber*). Con el IV (IV + keynumber) y la llave conseguimos los 64 bits de la llave final que se utilizará para cifrar la trama.

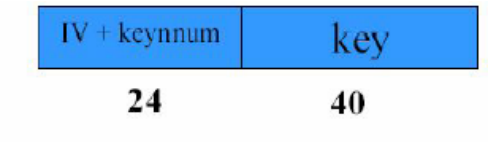


Figura 71. Añadición del IV

4. Aplicamos el algoritmo de cifrado RC4 a la llave de 64 bits y conseguiremos el flujo de llave (*keystream*). Al realizar una operación XOR con el keystream y el conjunto "payload + ICV", obtendremos el "payload + ICV cifrado".

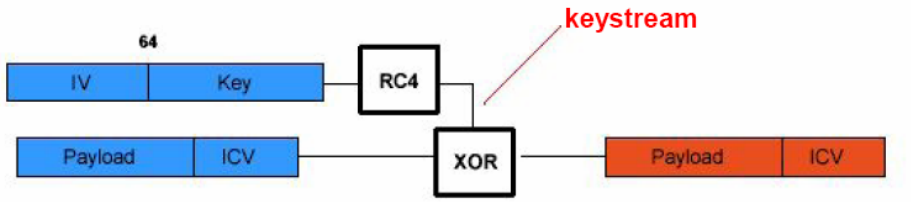


Figura 72. Obtención del payload y ICV cifrado

5. Para finalizar, se añade la cabecera y el "IV + llave" (= llave completa), de forma que se tiene la trama cifrada completa.

Figura 73. Trama cifrada

El proceso completo es el siguiente:

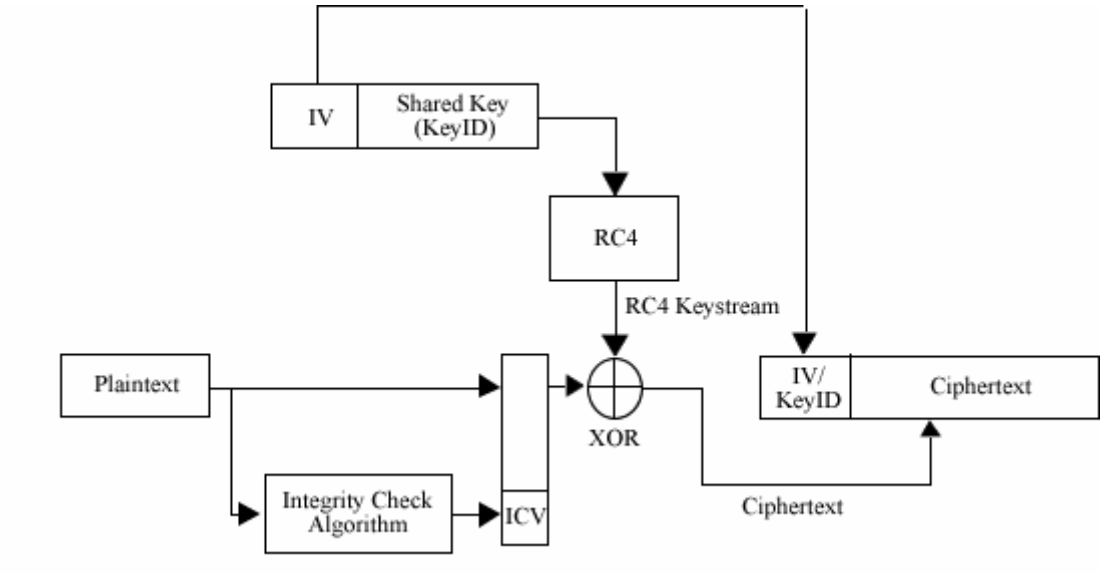


Figura 74. Proceso completo de Cifrado

3.8.2.3.3 Descifrado

Se siguen los siguientes pasos:

1.- Se utiliza el número de llave, que aparece en la trama cifrada junto con el IV, para seleccionar la llave que se ha utilizado para cifrar la trama.

Figura 75. Selección de llave para cifrar

2.- Se añade el IV al principio de la llave seleccionada, para obtener la llave completa de 64 bits. Aplicamos RC4 sobre la llave obtendremos el "keystream" para obtener la trama original (sin cifrar, en texto plano), mediante la operación XOR con el "payload + ICV cifrados".

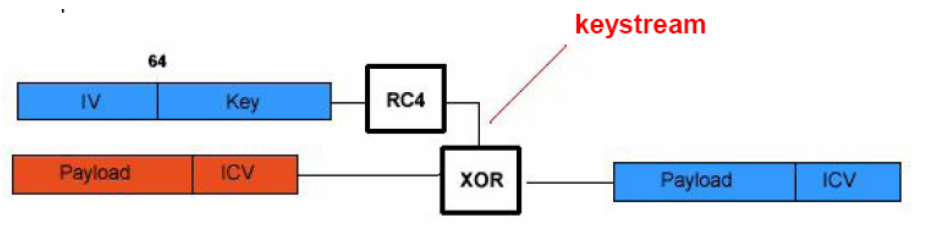


Figura 76. Obtención del payload y ICV cifrados

3.- Ahora volvemos a calcular el CRC del payload obtenido y se compara con el ICV de la trama que se ha recibido, para comprobar si los datos han sido manipulados durante el envío. Si el ICV no coincide, la trama queda descartada.

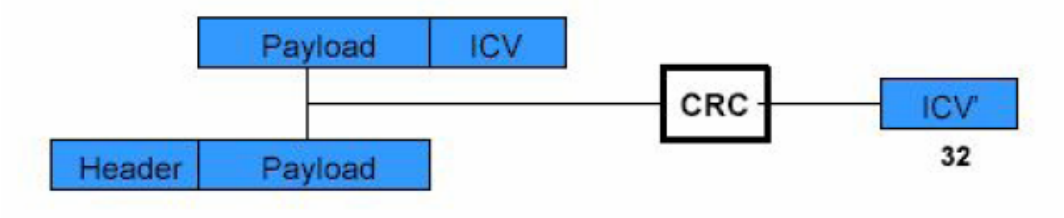


Figura 77. Calculo de el CRC

El proceso completo es el siguiente:

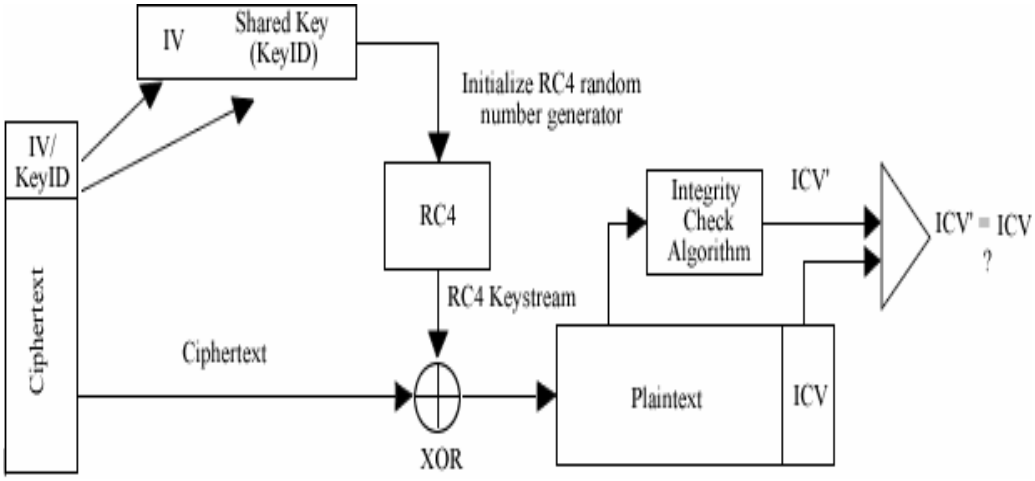


Figura 78. Proceso completo Descifrado

3.8.3 Virtual Private Network, VPN

Una VPN (Virtual Private Network) es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de cifrado y/o autentificación criptográfica. Una VPN es *virtual* porque no es físicamente un red distinta, es *privada* porque la información que transita por los túneles es cifrada para brindar confidencialidad, y es una *red* porque consiste de computadoras y enlaces de comunicación, pudiendo incluir routers, switches y gateways de seguridad.

Para configurar una red inalámbrica utilizando las VPN, debe comenzarse por asumir que la red inalámbrica es insegura. Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un router, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching.

Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

Los servidores de VPN se encargan de autenticar y autorizar a los clientes inalámbricos, y de cifrar todo el tráfico desde y hacia dichos clientes.

Es la solución más segura a la hora de proteger la información que se transmite frente a posibles intrusos que deseen descifrar la información transmitida. Aquí hay dos puntos a considerar: por un lado en el establecimiento del túnel hay varias modalidades para autenticar a los clientes de ese túnel y diferentes tipos de túneles según el nivel OSI en que se trabaje. Por otro lado, la información que se transmite puede cifrarse utilizando el protocolo IPSEC que permite diferentes algoritmos de cifrado (DES o 3DES) con diferentes grados de robustez, además éste protocolo es abierto por lo que es compatible con muchos productos.

3.8.3.1 Estructura de las VPN's

Como se muestra en la figura siguiente, la idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

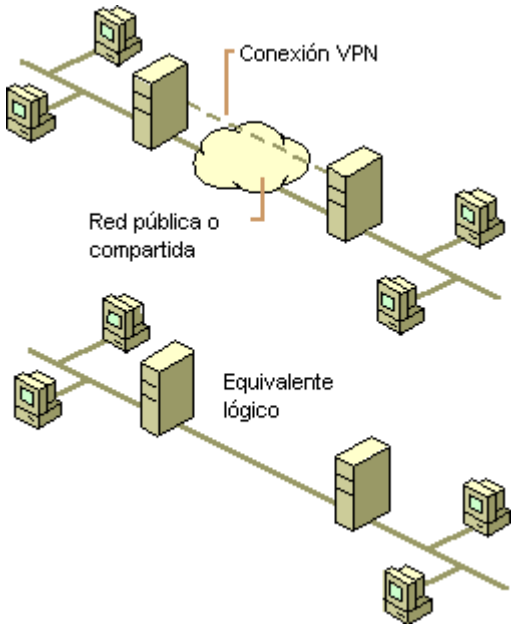


Figura 79. VPN

Las VPNs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN.
La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de cifrado y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

La tecnología de túneles (“Tunneling”) es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original.

Las técnicas de autenticación son esenciales en las VPN’s, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autenticación en VPN’s es conceptualmente parecido al “logeo” en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en un sistema de claves compartidas.

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya algún tercer participante que se haya intrometido en la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Todas las VPNs tienen algún tipo de tecnología de cifrado, que esencialmente empaqueta los datos en un paquete seguro. El cifrado es considerado tan esencial como la autenticación, ya que protege los datos transportados de poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de cifrado que se usan en las VPN: cifrado de clave secreta, o privada, y cifrado de clave pública.

En el cifrado de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información cifrada. Dicha contraseña se utiliza tanto para cifrar como para descifrar la información. Este tipo de cifrado posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

El cifrado de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al cifrar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es descifrada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de cifrado es que resulta ser más lenta que la de clave secreta.

En las VPNs, el cifrado debe ser realizado en tiempo real. Por eso, los flujos cifrados a través de una red son cifrados utilizando cifrado de clave secreta con claves que son solamente buenas para sesiones de flujo.

Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo túnel de IPSec.

3.8.3.2 Protocolos utilizados en las VPNs

3.8.3.2.1 Point-to-Point Tunneling Protocol (PPTP)

Como protocolo de túnel, PPTP encapsula paquetes de cualquier protocolo de red en paquetes IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

Existen dos escenarios comunes para este tipo de VPN:

- el usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- el usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga (Figura 80). El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como son direcciones de origen y destino, longitud del paquete enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP (*Point to Point Protocol*), el paquete es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.

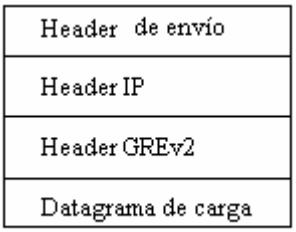


Figura 80. Paquete PPTP

Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, estándar en el que se intercambia un “secreto” y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un estándar propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer

opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no cifra las contraseñas.

Para el cifrado, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

3.8.3.2.2 L2TP

Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

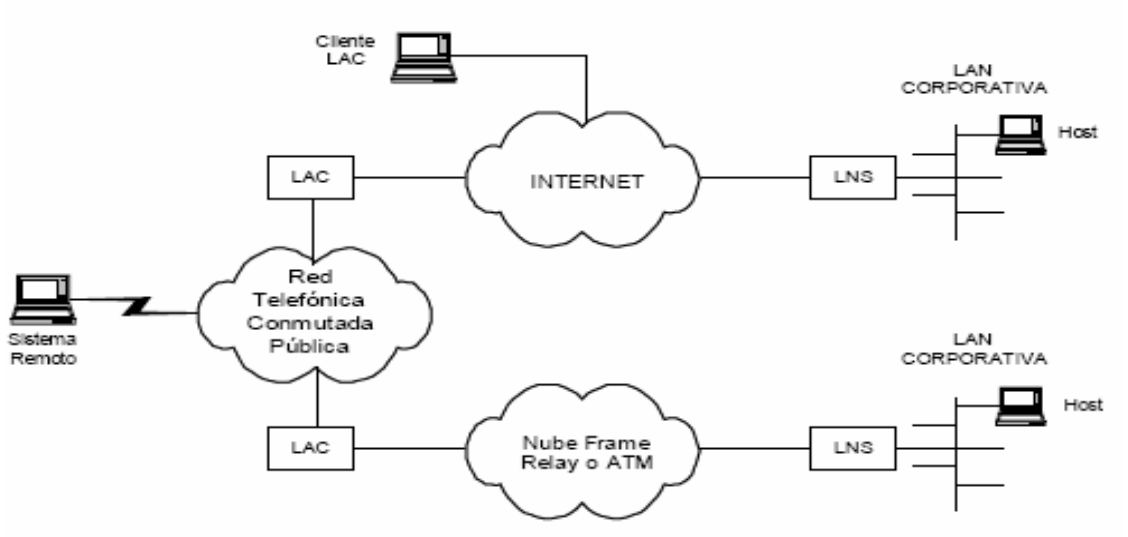


Figura 81. L2TP

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC (Figura 81).

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

El L2TP soporta dos modos de túneles, el modo Obligatorio y el Voluntario:

Túnel Obligatorio L2TP

1. El usuario remoto inicializa una conexión PPP a un ISP.
2. El ISP acepta la conexión y el enlace PPP se establece.
3. El ISP solicita la autentificación parcial para saber el nombre de usuario.

4. El ISP mantiene una lista de todos los usuarios admitidos, para servir el final del túnel LNS.
5. El LAC inicializa el túnel L2TP al LNS.
6. Si el LNS acepta la conexión, el LAC encapsulara el PPP con el L2TP, y entonces enviara a través del túnel.
7. El LNS acepta estas tramas, y las procesa como si fueran tramas PPP.
8. El LNS la autentificación PPP para validar al usuario y entonces asigna una dirección IP.

Túnel Voluntario L2TP

1. El usuario remoto tiene una conexión a un ISP ya establecida.
2. El cliente L2TP (LAC), inicializa el túnel L2TP al LNS.
3. Si el LNS acepta la conexión, LAC encapsula con PPP y L2TP, y lo manda a través del túnel.
4. El LNS acepta estas tramas, y las procesa como si fueran tramas normales de entrada.
5. El LNS entonces usa la autentificación PPP para validar al usuario y asignarle una IP.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

La siguiente figura muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.

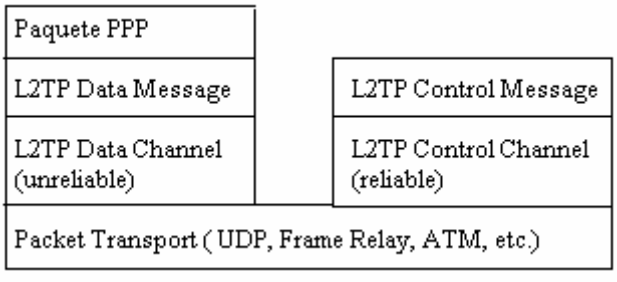


Figura 82. Relación entre marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP.

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son

enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de cifrado, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

3.8.3.2.3 IPSec, Protocolo de Seguridad IP

La nueva tendencia en seguridad es crear protocolos que funcionen a menor nivel que el de aplicaciones, de tal forma que se brinde seguridad tanto a IP como a protocolos de capas superiores de forma transparente para el usuario; protocolos que funcionen sin que el usuario deba hacer o instalar algo particular en su computadora, y protejan su tráfico sin importar la aplicación que lo genere.

IPSec (Internet Protocol Security) es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones, y es mucho más poderoso. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores.

3.8.3.2.3.1 La arquitectura de IPSec

La arquitectura de IPSec define la granularidad con la que el usuario puede especificar su política de seguridad. Permite que cierto tráfico sea identificado para recibir el nivel de protección deseado.

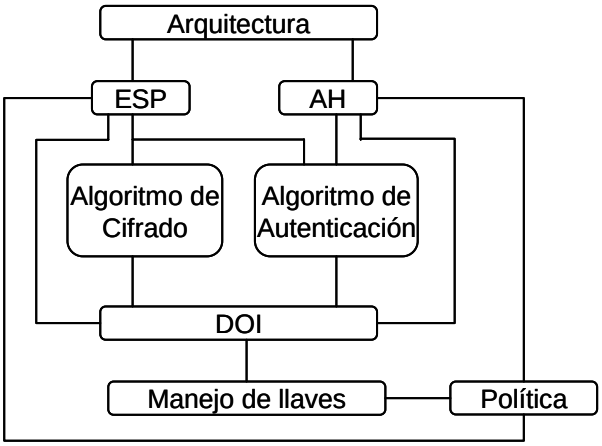


Figura 83. Arquitectura de IPSec

IPsec consta de dos sub-protocolos:

Encapsulated Security Payload (ESP), que protege los datos del paquete IP de interferencias de terceros, cifrando el contenido utilizando algoritmos de criptografía simétrica (como Blowfish, 3DES) (Figura 83).

Authentication Header (AH), que protege la cabecera del paquete IP de interferencias de terceros así como contra la falsificación ("spoofing"), calculando una suma de comprobación criptográfica y aplicando a los campos de cabecera IP una función hash segura. Detrás de todo esto va una cabecera adicional que contiene el hash para permitir la validación de la información que contiene el paquete (Figura 83).

3.8.3.2.3.2 Intercambio de claves

Antes de que se pueda intercambiar información protegida, debe establecerse un acuerdo de seguridad entre los dos equipos. En ese acuerdo de seguridad, denominado asociación de seguridad (SA), los dos equipos establecen el modo de intercambiar y proteger la información.

Con el fin de establecer este acuerdo entre los dos equipos, IETF ha establecido un método estándar de asociación de seguridad y resolución de intercambio de claves denominado Intercambio de claves de Internet (IKE), el cual:

- Centraliza la administración de asociaciones de seguridad, reduciendo el tiempo de conexión.
- Genera y administra las claves secretas compartidas que se utilizan para proteger la información.

El protocolo IKE está diseñado para establecer de manera segura una relación de confianza entre dos equipos, negociar las opciones de seguridad y generar de manera dinámica material de claves criptográficas secretas compartidas. Estas claves proporcionarán autenticidad, integridad y, opcionalmente, cifrado de los paquetes IP que se envían mediante la asociación de seguridad. IKE negocia dos tipos de asociaciones de seguridad:

- Una asociación de seguridad de modo principal (la asociación de seguridad IKE que se utiliza para proteger la propia negociación IKE).
- Asociaciones de seguridad IPSec (las asociaciones de seguridad que se utilizan para proteger el tráfico de la aplicación).

Se pueden configurar las opciones de directivas IPSec para ambos tipos de asociaciones de seguridad.
El servicio IPSec interpreta una directiva IPSec y la amplía a los componentes que necesita para controlar la negociación IKE. La directiva IPSec contiene una definición de un filtro de paquetes. El filtro de paquetes se interpreta de dos formas: una utiliza sólo la dirección y la información de identidad para permitir a IKE establecer una asociación de seguridad de modo principal (la asociación de seguridad IKE); la otra permite a IKE establecer las asociaciones de seguridad IPSec (también conocidas como asociaciones de seguridad de modo rápido).

3.8.3.2.3.3 Modos de funcionamiento de IPSec

El diseño de IPSec plantea dos modos de funcionamiento para sus protocolos: transporte y túnel, la diferencia radica en la unidad que se esté protegiendo, en modo transporte se protege la carga útil IP (capa de transporte), en modo túnel se protegen paquetes IP (capa de red) y se pueden implementar tres combinaciones: AH en modo transporte, ESP en modo transporte, ESP en modo túnel (AH en modo túnel tiene el mismo efecto que en modo transporte).

- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre el cifrado del header TCP y los datos, pero no incluye ningún campo del header IP (Figura 84).
- El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway (Figura 84).

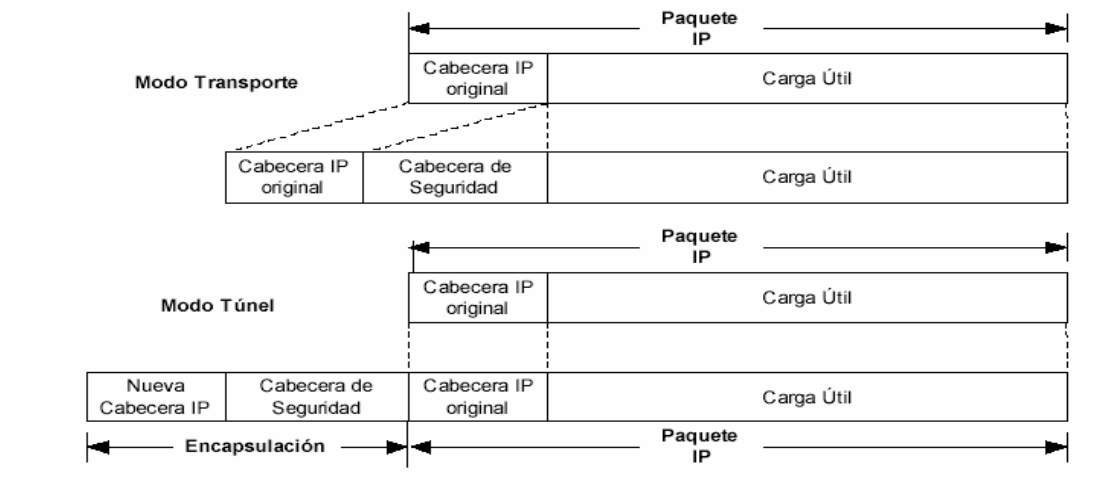


Figura 84. Modos de operación de IPSec

Un ejemplo de paquete AH en modo túnel es:

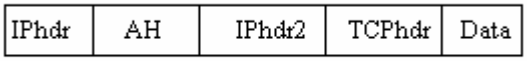


Figura 85. Paquete AH en modo túnel

Un ejemplo de paquete AH en modo transporte es:

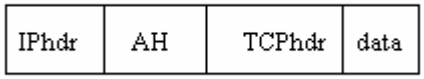


Figura 86. Paquete AH en modo transporte

Como ESP no puede autentificar el header IP más exterior, es muy útil combinar un header AH y ESP para obtener lo siguiente:

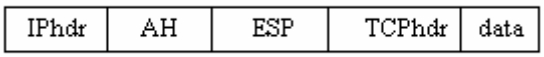


Figura 87. Paquete AH combinado con ESP

Este tipo de paquete se denomina Transport Adjacency. La versión de entunelamiento sería:

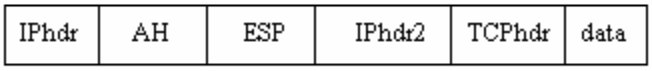


Figura 88. Paquete Transport Adjacency

3.8.4 WPA

WPA es un estándar propuesto en octubre del 2003 por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando el cifrado de los datos y ofreciendo un mecanismo de autenticación. Para ello, toma del estándar 802.11i (el cual no fue ratificado sino hasta junio del 2004), un subconjunto de especificaciones que sólo necesitan ser implantadas mediante software. WPA opera en la capa MAC.

WPA tiene las siguientes las siguientes características:

- **TKIP**. El protocolo de integridad de clave temporal (TKIP) sustituye a WEP con un algoritmo de cifrado nuevo más seguro que el algoritmo de WEP.

- **MIC**. Con WPA, un método conocido como Michael especifica un nuevo algoritmo que calcula un código de integridad de mensaje (MIC) de 8 bytes con las utilidades de cálculo disponibles en los dispositivos inalámbricos existentes.

- **Autenticación 802.1x**. En el estándar WPA se requiere autenticación 802.1x. En el estándar 802.11, la autenticación 802.1x era opcional. En entornos sin una infraestructura de Servicio de usuario de acceso telefónico de autenticación remota (RADIUS), WPA admite el uso de una clave compartida previamente (PSK). En los entornos con una infraestructura RADIUS, se admiten el **Protocolo de Autenticación Extensible (EAP)** y RADIUS.

En septiembre del 2004 aparece **WPA2** totalmente compatible con WPA y con el estándar 802.11i ya ratificado. La característica fundamental que aporta esta nueva versión es la utilización del **Estándar de Cifrado Avanzado (AES)**. Para esta nueva versión es necesario un nuevo procesador que soporte este cifrado.

3.8.4.1 Autenticación con WPA y WPA2

El proceso de autenticación comienza cuando un usuario se asocia con el punto de acceso (AP). El AP bloquea el acceso al la red hasta que el usuario pueda ser autenticado. El usuario proporciona credenciales, las cuales son enviadas al servidor de autenticación. El proceso de autenticación se establece mediante el marco de trabajo IEEE 802.1X/EAP. Con EAP, IEEE802.1X crea una estructura en la cual el cliente y el servidor se autentican mutuamente vía el AP. La autenticación mutua asegura que solo usuarios autorizados accedan a la red y confirma que el cliente esta autenticando a un servidor autorizado.
Si el servidor de autenticación acepta las credenciales del usuario, el cliente se une a la WLAN. Si no, el cliente permanece bloqueado. Una vez que el usuario

ha sido autenticado, el servidor de autenticación y el cliente simultáneamente generan una Pairwise Master Key (PMK).

Comienza entonces un proceso de autenticación entre el cliente y el AP conocido como 4-way handshake., estableciendo e instalando las llaves (TKIP o AES) de cifrado derivadas de PMK.

3.8.4.2 Cómo trabaja WPA con TKIP

En este proceso, después de aceptar las credenciales del usuario, el servidor de autenticación usa 802.1X para producir una única llave para la sesión de ese usuario. TKIP dinámicamente genera una llave única para cifrar cada paquete que es transferido durante la sesión.
MIC es empleado para prevenir la alteración y reenvío de los paquetes. MIC proporciona una función matemática fuerte con la cual tanto el transmisor como el receptor calculan y comparan el valor MIC. Si no coinciden, se asume que el paquete ha sido alterado.

3.8.4.3 Cómo trabaja WPA con AES

Para WPA/802.11i, la implementación de AES se realiza 10 veces cada vuelta. AES usa Counter-Mode/CBC-Mac Protocol (CCMP). CCM es un nuevo modo de operación para un bloque cifrado que permite que una sola llave sea usada para el cifrado y autenticación.

CBC-MAC es usado para generar un componente de autenticación como resultado del proceso de cifrado. AES usa un vector de inicialización (IV) de 48 bits.

3.8.4.4 TKIP

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

En WPA la regeneración de claves de unidifusión y multidifusión es obligatoria, esto es, es necesario volver a teclear las claves de cifrado de unidifusión y globales. En el caso de claves establecidas con un único cliente (unidifusión) es el protocolo TKIP el encargado de hacerlo, manteniendo sincronizadas las claves entre cliente y punto de acceso. En el caso de claves de tráfico global (multidifusión) incluye un sistema que permite al punto de acceso el envío seguro de la nueva clave a los clientes que estén conectados.

TKIP incrementa el tamaño de las claves de cifrado de 40 a 128 bits y sustituye las claves estáticas de WEP por claves dinámicamente generadas y distribuidas

por el punto de acceso tras la autenticación de los usuarios. En WPA existe un algoritmo llamado Michael que se usa para el cálculo de códigos de integridad de mensaje MIC. Este MIC está pensado para evitar que un atacante capture paquetes, los modifique y los reenvié. Michael define una avanzada función matemática que se calcula en cada paquete por parte del emisor y el receptor, incluyéndola el primero en el propio paquete a transmitir. Al recibirse el paquete en el destino se compara el MIC calculado con el contenido en éste y sino coinciden se asume que los datos han sido modificados y por consiguiente, descartando el paquete.

TKIP también proporciona:

- La comprobación de la configuración de seguridad después de determinar las claves de cifrado.
- El cambio sincronizado de la clave de cifrado de unidifusión para cada marco.
- La determinación de una clave de inicio de cifrado de unidifusión exclusiva para cada autenticación de clave previamente compartida

Como se menciono TKIP se basa en WEP, y por ello utiliza las claves de 128-bits compartidas por el usuario y el equipo de red, aunque ahora les añade una operación *hash* (Figura 90) que mejora la seguridad y hace más complicado un ataque. TKIP sigue manteniendo el algoritmo RC4 utilizado en WEP aunque TKIP cambia la clave utilizada cada 10,000 paquetes (Figura 89). Una de las ventajas de TKIP es su compatibilidad con sistemas basados en WEP y la facilidad de actualización de los sistemas WEP a sistemas TKIP.

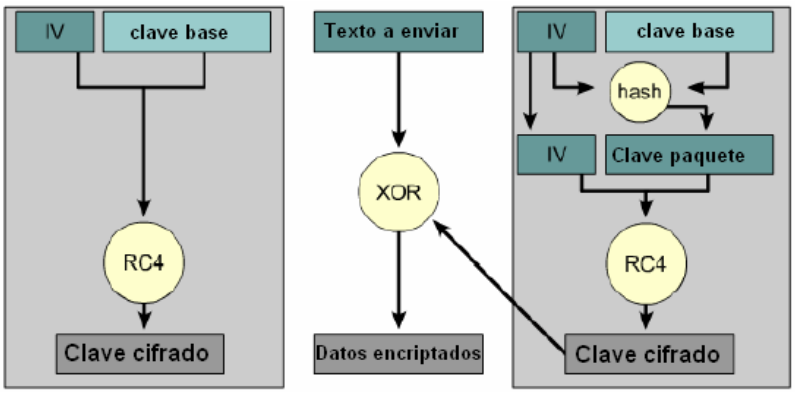


Figura 89. Generación de clave

Una mejora importante es que se genera una nueva clave WEP por paquete enviado:

El IEEE incluyó un método en el cual se utilizaba una clave WEP diferente para cada paquete. Puesto que el IV se incrementa en una unidad para cada paquete y después se hace un hash con la clave WEP base, obtenemos una nueva clave WEP para cifrar cada paquete. Recientemente el IEEE está considerando añadir a los 24 bits del IV la dirección MAC del usuario incrementando así la longitud del mismo.

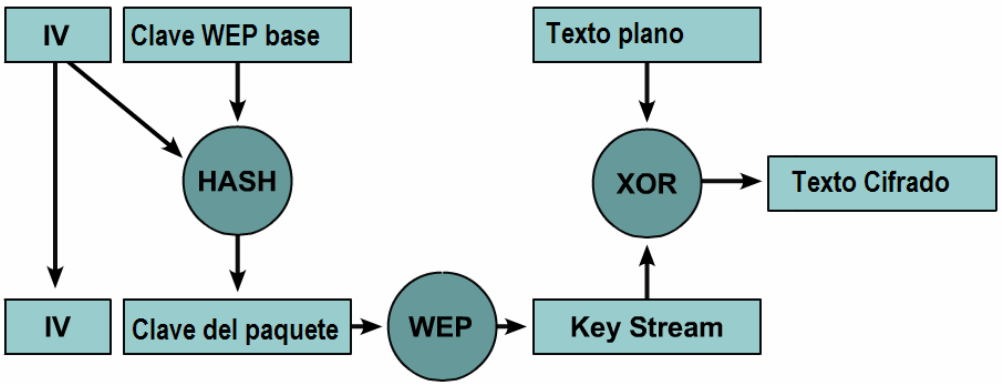


Figura 90. Hasheo

3.8.4.4.1 ***Message Integrity Check*** mejora los problemas que presentaba el campo ICV, que se encargaba de chequear la integridad de lo paquetes que se enviaban por la red Wireless. La forma en que se calculaba este valor de integridad hacía vulnerable al algoritmo WEP fundamentalmente por las siguientes razones:

• Reutilización de Vector de inicialización / Clave base.
• Bit flipping.

Para solucionar el primer problema MIC añade un campo con un número de secuencia a las tramas wireless. Esta parte de la trama viaja cifrada por WEP y el Access Point eliminará cualquier trama que no siga la secuencia.

Para asegurar que las tramas recibidas en el destino no han sido modificadas durante el trayecto, o que alguna trama maliciosa se haya intentado introducir en un flujo ya existente, MIC calcula un código de integridad basado en: una semilla, dirección MAC destino, dirección MAC origen y carga o *payload* (Figura 91).

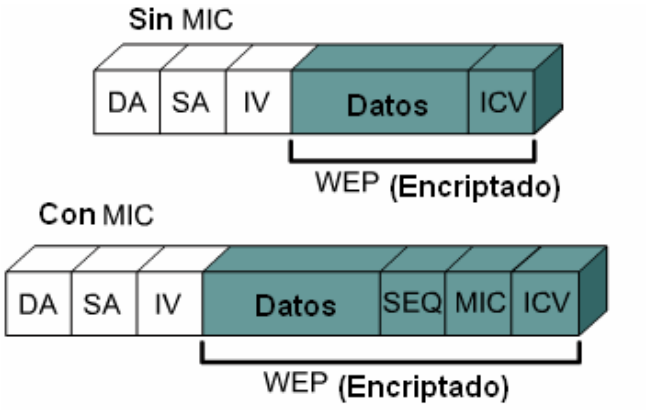


Figura 91. Comparación de Cifrado utilizando MIC

3.8.4.5 AES

En criptografía, **Advanced Encryption Standard, Estándar de Cifrado Avanzado (AES)**, también conocido como **Rijndael**, es un esquema de cifrado por bloque adoptado como un estándar de cifrado por el gobierno de los Estados Unidos, y se espera que sea usado en el mundo entero, como también analizado exhaustivamente, como fue el caso de su predecesor, el Estándar de Cifrado de Datos (DES).

AES es rápido tanto en software como en hardware, es relativamente fácil de implementar, y requiere poca memoria.

3.8.4.5.1 Funcionamiento

AES opera en un arreglo de 4×4 bytes, llamado ***state*** (algunas versiones de Rijndael con un tamaño de bloque mayor tienen columnas adicionales en el state). El proceso de cifrado consta de tres pasos: una adición inicial de la clave de vuelta, n-1 vueltas de cifrado y una vuelta final.
Cada ronda de la aplicación del algoritmo AES (excepto la última) consiste en cuatro pasos:

El paso SubBytes

En la fase de SubBytes, cada byte en el state es reemplazado tomando su valor y substituyéndolo por su correspondiente en una tabla (S-box) de búsqueda fija de 8 bits. Esta operación provee la no linealidad en el cifrado.

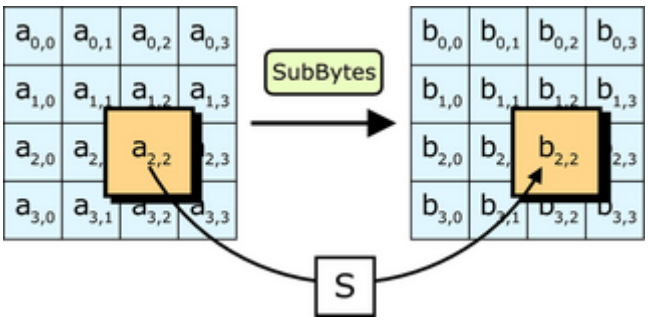


Figura 92. Paso SubBytes

El paso ShiftRows

El paso ShiftRows opera en las filas del state; rota de manera cíclica los bytes en cada fila un determinado número de lugares. La primera fila queda en la misma posición. Cada byte de la segunda fila es rotado una posición a la izquierda. De manera similar, la tercera y cuarta filas son rotadas dos y tres posiciones respectivamente. De esta manera, cada columna del state resultante del paso ShiftRows está compuesta por bytes de cada columna del state inicial.

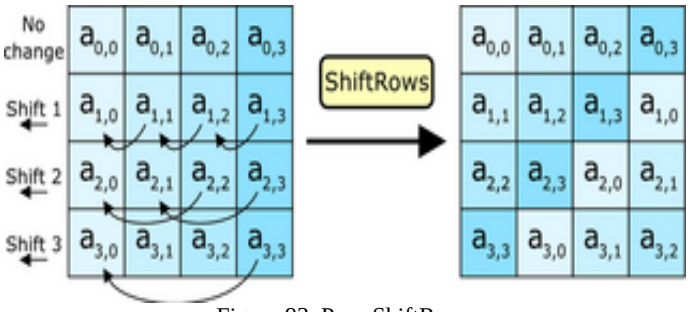


Figura 93. Paso ShiftRows

El paso MixColumns

En el paso MixColumns, cada columna del state es multiplicada por un polinomio constante *c(x)*.

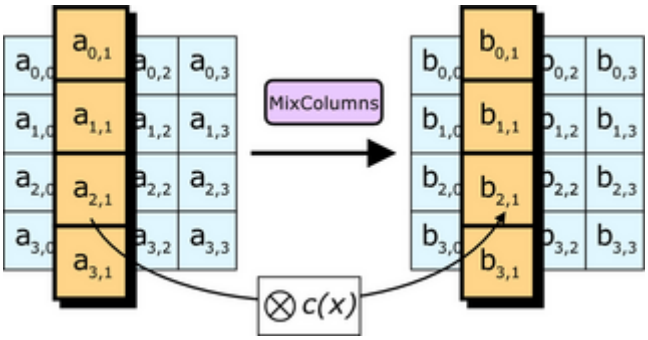


Figura 94. Paso MixColumns

El paso AddRoundKey

En el paso AddRoundKey, la subclave se combina con el state. En cada ronda se obtiene una subclave de la clave principal, cada subclave es del mismo tamaño del state. La subclave se agrega combinando cada byte del state con el correspondiente byte de la subclave usando XOR.

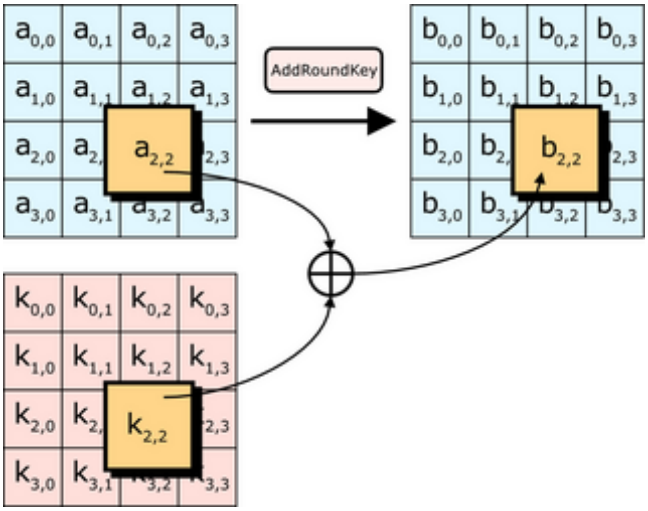


Figura 95. Paso AddRoundKey

La clave de cada vuelta se deriva de la clave de cifrado mediante el esquema de clave. El esquema de clave consiste en dos operaciones: expansión de clave y selección de clave de vuelta de cifrado.

3.8.4.6 802.1x

802.1x es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor, que restringe la conexión de equipos no autorizados a una red. El protocolo fue inicialmente creado por la IEEE (junto con Microsoft, Cisco y otros líderes del sector) para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas. Muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x.

3.8.4.6.1 Funcionamiento de 802.1x

En 802.1x se implementan controles de acceso basados en puertos. En el caso de una red WLAN, un puerto sólo es una conexión entre un punto de acceso (PA) y una estación. Hay dos tipos de puertos en el ámbito de 802.1x: controlados y no controlados. Un puerto no controlado permite que el dispositivo conectado a él se comunique con cualquier otro dispositivo de red. En contraste, un puerto controlado limita las direcciones de red con las que el dispositivo conectado se puede comunicar. 802.1x permite que todos los clientes se conecten a puertos controlados, pero esos puertos sólo pasan tráfico a los servidores de autenticación. Una vez autenticado, el cliente tiene permiso para comenzar a utilizar el puerto no controlado. La magia de 802.1x consiste en que los puertos controlados y no controlados son entidades lógicas que pueden existir en el mismo puerto de red físico.

El protocolo 802.1x involucra tres participantes:

- El suplicante, que es un dispositivo (por ejemplo, un equipo portátil con una tarjeta 802.11b) que solicita acceso a los recursos de red.
- El servidor de autorización/auten-ticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red. 802.1x fue diseñado para emplear servidores RADIUS (Remote Authentication Dial-In User Service), cuya especificación se puede consultar en la RFC 2058. Estos servidores fueron creados inicialmente para autenticar el acceso de usuarios remotos por conexión vía telefónica; dada su popularidad se optó por emplearlos también para autenticación en las LAN.
- El autenticador, que es el equipo de red (switch, enrutador, servidor de acceso remoto...) que recibe la conexión del suplicante. El autenticador actúa como intermediario entre el suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

En 802.1x no se utiliza el protocolo de privacidad equivalente por cable (WEP, Wired Equivalent Privacy) para la autenticación; en su lugar se utiliza el Protocolo de autenticación extensible (EAP, Extensible Authentication Protocol). La principal ventaja de EAP es que permiten elegir el método de autenticación. De manera predeterminada, en 802.1x se utiliza EAP-TLS (EAP-Transport Layer Security, EAP-Seguridad de nivel de transporte), con el que todo el intercambio protegido por EAP se protege con el protocolo TLS (directamente relacionado con el conocido protocolo SSL).

La autenticación del cliente se lleva a cabo mediante el protocolo EAP (Extensible Authentication Protocol) y el servicio RADIUS, de la siguiente manera:

- El proceso inicia cuando la estación de trabajo se enciende y activa su interfaz de red (en el caso alambrado) o logra enlazarse o asociarse con un punto de acceso (en el caso inalámbrico). En ese momento, la interfaz de red tiene el acceso bloqueado para tráfico normal, y lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación.
- La estación de trabajo envía un mensaje EAPOL-Start al autenticador, indicando que desea iniciar el proceso de autenticación.
- El autenticador solicita a la estación que se identifique, mediante un mensaje EAP-Request/Identity.
- La estación se identifica mediante un mensaje EAP-Response/Identity.
- Una vez recibida la información de identidad, el autenticador envía un mensaje RADIUS-Access-Request al servidor de autenticación, y le pasa los datos básicos de identificación del cliente.
- El servidor de autenticación responde con un mensaje RADIUSAccess-Challenge, en el cual envía información de un desafío que debe ser correctamente resuelto por el cliente para lograr el acceso. Dicho desafío puede ser tan sencillo como una contraseña, o involucrar una función criptográfica más elaborada. El autenticador envía el desafío al cliente en un mensaje EAP-Request.
- El cliente da respuesta al desafío mediante un mensaje EAP-Response (Credentials) dirigido al autenticador. Este último reenvía el desafío al servidor en un mensaje RADIUS-Access-Response.
- Si toda la información de autenticación es correcta, el servidor envía al autenticador un mensaje RADIUS-Access-Accept, que autoriza al autenticador a otorgar acceso completo al cliente sobre el puerto, además de brindar la información inicial necesaria para efectuar la conexión a la red.
- El autenticador envía un mensaje EAP-Success al cliente, y abre el puerto de acuerdo con las instrucciones del servidor RADIUS.

3.8.4.6.1.1 EAP (Protocolo de Autenticación Extensible, Extensible Authentication Protocol)

Existen varias variantes del protocolo EAP, según la modalidad de autenticación que se emplee. Se puede hablar de dos grupos de variantes: las que emplean certificados de seguridad, y las que utilizan contraseñas.

Las variantes de EAP que utilizan contraseñas son las siguientes:

3.8.4.6.1.1.1 LEAP (Lightweight EAP). Basado en nombre de usuario y contraseña, que se envían sin protección, por lo que está sujeto a ataques de diccionario. Autentica tanto al cliente frente al AP, como al AP frente al cliente. Intercambio de llaves dinámicas. Soporta las plataformas: Windows, Macintosh y Linux. Requiere RADIUS server e infraestructura Cisco Wireless. Desarrollado por Cisco.

3.8.4.6.1.1.2 EAP-MD5. Emplea un nombre de usuario y una contraseña para la autenticación. La contraseña se transmite cifrada con el algoritmo MD5. Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente). Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada), y el esquema no es capaz de generar claves dinámicas.

Las variantes de EAP que emplean certificados de seguridad son las siguientes:

3.8.4.6.1.1.3 EAP-TLS. Requiere de instalación de certificados en los clientes y en el servidor. Proporciona autenticación mutua fuerte (es decir, el servidor autentica al cliente y viceversa) y soporta el uso de claves dinámicas para WEP. La sesión de autenticación entre el cliente y el autenticador se cifra empleando el protocolo TLS (Transparent Layer Substrate).

3.8.4.6.1.1.4 EAP-TTLS. Permite a los usuarios autenticarse mediante nombre de usuario y contraseña, sin pérdida de seguridad. Ofrece una fuerte autenticación mutua, credenciales de seguridad y llaves dinámicas. Requiere la distribución de certificados digitales sólo a los servidores RADIUS, y no a los clientes. Desarrollado por Funk Software y Certicom.
Primero se establece un túnel virtual privado entre el cliente y el AP, y desde el AP al servidor RADIUS, mediante TLS (Transport Layer Security), que será por donde pase la información de la autenticación, si es usuario es aceptado entrará a formar parte de la red. Se “quitará” el túnel virtual, ya que únicamente es para la autenticación.

3.8.4.6.1.1.5 PEAP. Desarrollado por Microsoft, Cisco y RSA Security. Funciona de manera parecida a EAP-TTLS, en el sentido de que solamente requiere de certificado de seguridad en el servidor. Provee protección a

métodos más antiguos de EAP, mediante el establecimiento de un túnel seguro TLS entre el cliente y el autenticador.

3.9 Firewall

Los firewall son una de las más importantes medidas de seguridad para proteger una computadora personal de los posibles ataques que pueda recibir, tanto a través de un entorno no del todo seguro como el de las redes Wi-Fi, como a través de una conexión de banda ancha a Internet.

El firewall no protege las comunicaciones, sino que protege el equipo para que ningún intruso pueda hacer uso del disco duro o de cualquier otro recurso. Un punto de acceso o un router puede tener también determinadas propiedades de firewall para proteger los recursos de la red. Los firewall llevan a cabo su protección analizando los datos de petición de acceso a los distintos recursos y bloqueando los que no estén permitidos.

Para las aplicaciones en hogar o empresas pequeñas, es posible que sea suficiente con las características de firewall incluidas en el punto de acceso normal. No obstante, existen puntos de acceso profesionales que mejoran fuertemente estas características. Además de lo anterior, un firewall puede ser tanto un equipo hardware específico, como un software instalado en una computadora o bien en un servidor.

3.9.1 Los filtros del firewall

El firewall toma la decisión de qué datos deja pasar y qué otros no analizando los paquetes de información. La principal diferencia entre un firewall y uno menos bueno es la cantidad de información que es capaz de analizar para tomar las decisiones. En la actualidad existen tres tipos de firewalls:

3.9.1.1 Filtrado de paquetes. Éstos facilitan un control de acceso básico basado en la información sobre el protocolo de los paquetes. Simplemente deja o no pasar los paquetes de acuerdo con el protocolo de comunicación que utiliza el paquete. Los routers incluidos en los puntos de acceso ya suelen disponer de este tipo de filtrado. El problema es que esto supone una protección mínima para el usuario.

3.9.1.2 Servidor Proxy. Se trata de una aplicación software que va más allá del simple filtrado del protocolo del paquete. Este tipo de firewalls puede tomar decisiones basado en el análisis completo de todo un conjunto de paquetes asociados a una sesión que tiene el mismo destinatario. Un Proxy, mejora la seguridad, aunque tiene el inconveniente de alentar la comunicación. Además, son más elaborados de configurar.

3.9.1.3 Análisis completo del paquete. Éstos de basan en las misma técnica de filtrado de paquetes, pero, en vez de simplemente analizar la dirección de la cabecera del paquete, va interceptando paquetes hasta que

tiene información suficiente para mantener su seguridad. Posteriormente, entrega estos paquetes al destinatario de la red interna y permite una comunicación directa entre destinatario interno y su extremo externo. Este firewall bloquea todas las comunicaciones generadas e Internet y deja pasar aquellas iniciadas por cualquier computadora interna. El resultado es una comunicación más fluida que con los Proxy, pero la seguridad es menos.

3.9.1.4 Las reglas de filtrado

Las reglas de las que dependen los filtros del firewall se basan en distintos factores, condiciones o características de los paquetes de datos (Tabla 10). Las características más comunes son las siguientes:

Dirección IP. Tanto la dirección IP origen como destino pueden ser utilizadas para controlar los paquetes. Este tipo de filtros se utilizan habitualmente para bloquear la comunicación con ciertos servidores de externos o para bloquear el acceso a Internet de ciertos usuarios.

Nombre de dominio. Esta característica se utiliza de la misma forma que el filtrado de direcciones, pero basados en los nombres de dominio en vez de en las direcciones IP. Éstas pueden cambiarse fácilmente mientras que los nombres de dominio suelen ser más estables.

Protocolos. Los protocolos son también una característica interesante a filtrar. Por ejemplo, se puede dejar pasar el protocolo http para permitir el acceso a páginas web, pero no permitir el protocolo telnet para impedir ejecutar comandos en computadoras remotas, el protocolo ftp para impedir la bajada de archivos potencialmente infectados de virus o el protocolo smtp para impedir que desde la computadora de un usuario se pueda crear un servidor de correo desde donde enviar correos ilegales.

Puertos. Mientras las direcciones IP se utilizan para identificar a los equipos origen y destino de la comunicación, los puertos son unos números que sirven para identificar cada una de las aplicaciones con comunicaciones simultáneas que puede tener un equipo. Generalmente, cada número de puerto se utiliza para una aplicación distinta. Por ejemplo, el servidor web suele utilizar el puerto 80; telnet el 23, etc. Por tanto filtrando el número de puerto de puerto es una forma de filtrar los servicios a los que se puede acceder o ser accedidos.

Contenido. Los firewalls pueden filtrar también los datos que contienen determinadas palabras o frases. En este caso, el firewall analiza todo el contenido de los paquetes en busca de las palabras o frases prohibidas.

PARÁMETRO	SIGNIFICADO
Protocolo	Tipo de protocolo que utiliza el paquete (TCP, UDP)
Dirección IP destino	Identifica la computadora que va a recibir el paquete
Puerto IP del destino	Identifica la aplicación que va a recibir el paquete
Dirección IP del remitente	Identifica la computadora que envió el paquete
Puerto IP del remitente	Identifica la aplicación que envió el paquete
Contenido	Identifica el contenido de la información recibida

Tabla 10. Parámetros en filtrado

3.10 Sistemas de detección y prevención de intrusos

Actualmente existen numerosos tipos de ataques que pueden causar severos daños en la red. En las redes inalámbricas existen algunos que son muy comunes, como son: MAC spoofing, man in the middle, denial of service, IP spoofing y eavesdropping. Para proteger la red de estos daños es necesario contar con un firewall, servidor radius y/o VPN, sin embargo, esto no exenta a la red de vulnerabilidades. Aunado a esto, el hecho de que la naturaleza de la señal inalámbrica sea broadcast complica más la situación debido a que cualquier persona puede captarla e intentar vulnerarla.

Por esta razón, en las redes inalámbricas se ha vuelto indispensable contar también con sistemas que sean capaces de detectar y prevenir cualquier intento de daño que se esté llevando a cabo.

La detección de intrusos es el área aplicada de la seguridad informática encargada de informar de eventos que puedan tener lugar en un sistema informático y pueda ser considerado como parte de un intento de intrusión. Como intrusión se entiende la realización de un acto no autorizado, como pueda ser el acceso a un sistema, la ejecución de programas no autorizados o el ataque a una red informática.

El concepto de intrusión está cercano al de un ataque dirigido, pero algunas de las tareas previas a un ataque, como puede ser la recopilación de información o la búsqueda de servicios, no está directamente tipificada como ataque. Actualmente existe una controversia sobre si dichas actividades constituyen o no una actividad ilegal como lo pueda ser el acceso sin autorización a un sistema informático.

El hecho de que estemos ante un entorno complejo, formado por un sistema de información global interconectado a través de redes públicas de comunicación, hace difícil determinar si las actividades que realizan los sistemas por sí mismos

pueden considerarse ataques cuando son realizados por personas con intención desconocida. Un sistema de detección de intrusos ha de distinguir entre un acceso normal y habitual al sistema, que puede surgir de la puesta en marcha de servicios ofrecidos al exterior (entendiendo como exterior cualquier otro sistema ajeno al que ofrece los servicios), de un intento de vulnerar de algún modo dichos servicios, e incluso de aquellos que no debieran ser públicos, como parte del ataque a dicho sistema. Es, por tanto, un sistema de detección de intrusos aquél capaz de advertir al administrador de todas aquellas situaciones que puedan ser consideradas como elementos o fases de una intrusión. El objetivo de dicho sistema es, en la medida de lo posible, proporcionar conocimiento de la puesta en marcha de un ataque sobre el sistema antes de que dicho ataque tenga éxito. Se ha de considerar, por tanto, como un mecanismo previo de alarma que está indisolublemente unido al mecanismo de respuesta. De esta forma se podrán poner en marcha las medidas necesarias para mitigar el impacto. Los sistemas de detección de intrusos quedan divididos en función, fundamentalmente, del lugar donde realizan la detección. Este lugar puede ser la red, basándose en el análisis del tráfico que pasa por ésta y su contenido, o puede ser el propio sistema operativo (basados en host) sobre el que se monitoriza el uso que las aplicaciones, procesos y usuarios hacen de él.

La técnica tradicionalmente aplicada a la detección de intrusos, en todos sus ámbitos, consisten generalmente en el uso de reconocimientos de patrones para determinar ataques conocidos. De igual forma que la tecnología aplicada a la detección de virus, basada en la introducción de firmas más algunos heurísticos para detectar ligeras desviaciones, la detección de intrusos habitualmente busca en patrones que permiten discriminar un ataque de algo que no lo es.

3.10.1 NIDS, Sistema de detección de intrusos en una Red (Network intrusion detection systems)

Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, scanners de puertos o intentos de entrar en una computadora, analizando el tráfico en la red en tiempo real. Para ello, analiza todos los paquetes, buscando en ellos patrones sospechosos. Los NIDS no sólo vigilan el tráfico entrante, sino también el saliente o el tráfico local, ya que algunos ataques podrían ser iniciados desde el propio sistema protegido. A pesar de la vigilancia, su influencia en el tráfico es casi nula. Para que los NIDS sean efectivos, han de ser actualizados periódicamente. En caso de detectar un ataque contra el sistema, puede tomar medidas protectoras.

Un aspecto negativo de los NIDS actuales es su complicación a la hora de obtener las opciones de configuración óptimas para su ejecución. De otro modo, obtendremos demasiados falsos positivos (falsas alarmas, con gran cantidad de información que luego un administrador tendrá que procesar) o pasará sin advertir ciertos ataques.

3.10.2 HIDS, Sistema de detección de intrusos en un Host (Host Intrusion Detection System)

Mientras que los sistemas de detección de intrusos basados en red operan bajo todo un dominio de colisión o ubican sensores en dominios diferentes, los basados en computadoras realizan su función protegiendo un único host.

Dentro de este gran grupo existen subgrupos que utilizan diferentes vías para detectar las intrusiones. Algunas de estos subgrupos son los siguientes:

- System Integrity Verifiers (SIV): típicamente monitorizan los sistemas de archivos en busca de modificaciones relevantes.
- Log File Monitors (LFM): Revisan los archivos logs en busca de patrones sugerentes.
- Deception Systems (A.K.A. decoys, lures, fly-traps, honeypots): sistemas que aparentan servidores o computadoras vulnerables para desviar la actividad de los intrusos.

3.10.3 Limitaciones

- La aparición de "falsos positivos". Esto es, la detección de ataques que realmente no lo son debidos a que algunos patrones pueden ser, en realidad, accesos legítimos a los servicios.
- Los "falsos negativos". Corresponden estos sucesos a ataques que pasan desapercibidos para el sistema de detección de intrusos.
- La falta de interoperabilidad entre fabricantes,
- La sobrecarga de análisis que lleva a la posibilidad de ataques contra el propio detector de intrusos
- La necesidad de actualizaciones y ajustes continuos del firewall.

3.10.4 Sistema de Prevención de Intrusos (IPS)

Las carencias presentes en soluciones de seguridad tradicionales han impulsado el desarrollo de soluciones conocidas como sistemas de prevención de intrusos (IPS). Mientras productos como firewalls y antivirus perimetrales siguen siendo importantes, no cuentan con la capacidad de detectar y detener, en tiempo real, ataques conocidos, ataques desconocidos y situaciones de negación de servicio.

Un Sistema de Prevención de Intrusos es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de *Prevención de Intrusos* es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos, pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos. Los Sistema de Prevención de Intrusos conforman las nuevas tecnologías proactivas de seguridad informática para proteger servidores y

redes que cuentan con diversas herramientas para bloquear efectivamente ataques de hackers externos y/o internos, de amenazas tanto conocidas como desconocidas.

Los IPS son soluciones preactivas, diseñadas para detectar paquetes maliciosos de entre el tráfico normal (algo que, por ejemplo, los firewalls actuales no llevan a cabo), detener intrusiones en curso y bloquear el tráfico maligno automáticamente, esto es, previo a que el ataque ocasione un daño en su destino final.
Los IDS tradicionales lo único que generan son acciones posteriores, que van desde la simple generación de alertas a reconfigurar políticas del firewall, mientras lo único relacionado con la prevención es “detección y descarte del paquete en tiempo real o en línea”, por lo que un IPS debe ser, antes que nada, un excelente IDS.

Los IPS en red de forma general cuentan con al menos dos interfaces de red, una conocida como interna y otra como externa. Cuando los paquetes llegan a cualquiera de ellas son direccionados a un motor de detección. En este punto, el IPS funciona como IDS tradicional tratando de determinar si el paquete implica un riesgo para la seguridad. Una vez que se identifica un riesgo en el paquete, adicional a generar una alerta, se lleva a cabo un descarte del paquete en tiempo real y el tráfico es marcado como malicioso. Conforme los siguientes paquetes relacionados con la transacción maligna sigan llegando, se descartan de forma automática y los paquetes válidos de comunicación son reenviados a la otra interfaz y a su destino final.

4

Análisis y diseño

4.1 Análisis del Instituto de Ingeniería

Las instalaciones del Instituto de Ingeniería abarcan doce edificios y una parte de la Torre de Ingeniería, que incluye dos pisos y el basamento. Estas instalaciones comprenden laboratorios, cubículos, áreas comunes y un auditorio en 20 mil metros cuadrados.

Para efectos de análisis en lo referente a la red inalámbrica del Instituto de Ingeniería, las consideraciones que se toman en cuenta son las siguientes:

- El rango de cobertura es inversamente proporcional a la velocidad de conexión de un cliente. El máximo rango de cobertura está unido a la mínima velocidad de conexión.

- La elección de una antena apropiada es un factor crítico en maximizar el rango de radio de cobertura.

- El ambiente físico es importante ya que las áreas abiertas dan una mejor cobertura que las áreas cerradas o con obstáculos físicos.

- Las obstrucciones físicas principalmente las metálicas pueden disminuir considerablemente el desempeño de los adaptadores de red inalámbricos.

- La penetración de las ondas electromagnéticas está influenciada por los materiales usados en la construcción de los salones o edificios. Construcciones poco robustas permiten mayores rangos de cobertura que las construcciones de concreto. El metal como el acero es una barrera para la señal.

- El adaptador de red es un dispositivo susceptible a obstrucciones de radio electromagnéticas que pueden disminuir la velocidad y rango (Generadores de microondas).

4.1.1 Análisis de infraestructura

El motivo de este análisis es que las antenas inalámbricas funcionan con ondas de radio que no recorren la misma distancia en todas las direcciones. Las paredes, las puertas, los huecos de ascensores, las personas y otros obstáculos suponen distintos grados de pérdida de señal (atenuación) que provocan que el patrón de la radiación de radiofrecuencia sea irregular e imprevisible.

Así, dependiendo en gran medida de los materiales utilizados en la construcción de los edificios, la señal puede verse afectada y con ello el desempeño de la red inalámbrica. Como se menciono, el Instituto de Ingeniería cuenta con 12 edificios, construidos con diferentes materiales, dentro de los cuales destacan:

- Edificio 1. Muros divisorios de canceleria (perfil tubular y vidrio) fachada celosia.
- Edificio 2. Muros prefabricados Spancret, tabla roca.
- Edificio 3. Vitricota y muros divisorios.
- Edificio 5. Vitricota y concreto.
- Edificio 12. Vitricota y concreto, además tablaroca en los muros falsos divisorios.
- Laboratorios, la mayoría son de tabique rojo cosido con techos de lamina.

En el ambiente inalámbrico existe una clasificación de acuerdo al tipo de área geográfica donde se utilizará esta tecnología, dependiendo básicamente de la presencia de obstáculos, el tipo de obstáculos, si son lugares cerrados, abiertos, con línea de vista, etc.

Para el Instituto de Ingeniería esta clasificación nos lleva, casi en su totalidad, dentro de la categoría de oficinas cerradas, ya que son cubículos donde no existirá línea de vista directa además de que existen demasiados obstáculos entre el cliente y el punto de acceso; los demás se clasifican dentro de oficinas abiertas, ya que son laboratorios con pocos obstáculos para la transmisión de las señales inalámbricas.

Hemos encontrado los siguientes valores que nos ayudan a conocer la atenuación que presenta la señal al atravesar por diversos medios, estos valores son:

- Pared de yeso o similar: 3 dB
- Vidriera con marco metálico: 6 dB
- Pared de ladrillos de escorias: 4 dB
- Ventana de oficina: 3 dB
- Puerta metálica: 6 dB
- Puerta metálica en pared de ladrillo: 12.4 dB

Otros factores que reducen el alcance y afectan al área de cobertura son las paredes de hormigón de fibra vulcanizada, los revestimientos de aluminio, las tuberías y el cableado eléctrico, los hornos microondas y los teléfonos inalámbricos.

De acuerdo al análisis de los factores anteriores se efectuaron pruebas de ubicación y distribución de los puntos de acceso en los diversos edificios del Instituto de Ingeniería. Durante el desarrollo de estas pruebas se observó la degradación de la señal al atravesar las paredes u otras estructuras de los distintos materiales que conforman los edificios, las interferencias provocadas por el uso de equipo industrial utilizado en los laboratorios, así como de microondas, calentadores y las redes inalámbricas existentes en edificios aledaños de otras dependencias.

También se observó el desempeño de la antena según la altura a la que se encontraba y el canal en el cual transmitía. A continuación se detalla los pasos a seguir en la realización de las pruebas:

1. Se colocaba el access point en una ubicación donde considerábamos que abarcaría la mayor área posible con una recepción de la señal aceptable.

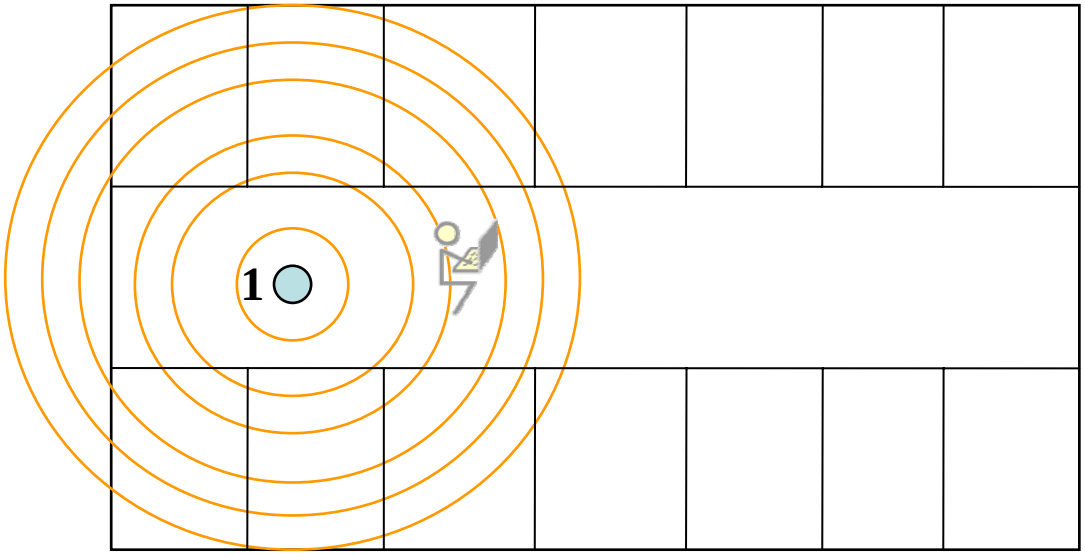


Figura 96. Pruebas Paso 1

2. Se registraban las lecturas de los Mbps a los que se conectaba la laptop en cada uno de los cubículos del piso en análisis.

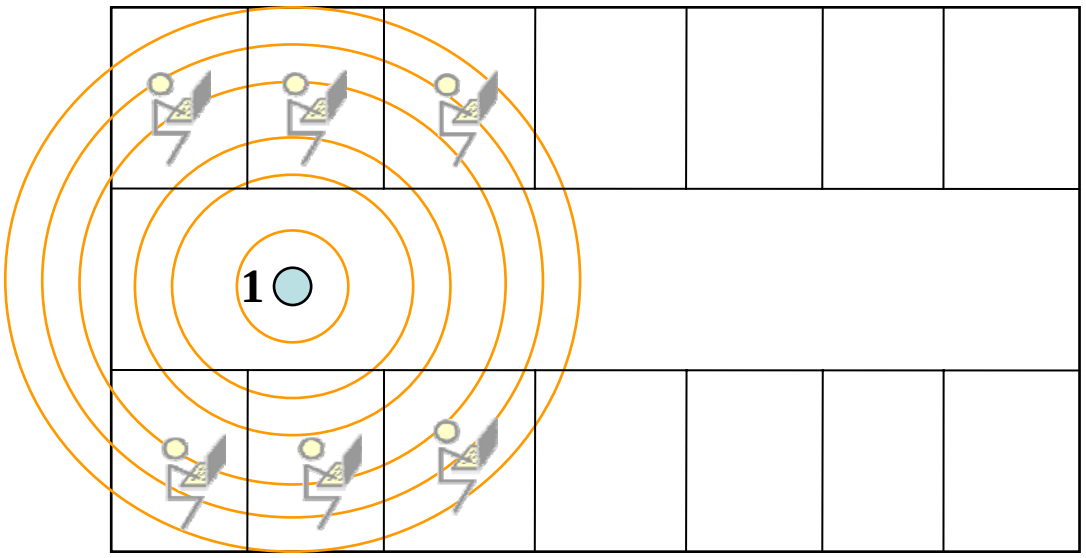


Figura 97. Pruebas Paso 2

3. Si en algún punto se obtenía que la potencia de la señal era baja, cambiábamos el canal y tomábamos nuevamente lecturas.

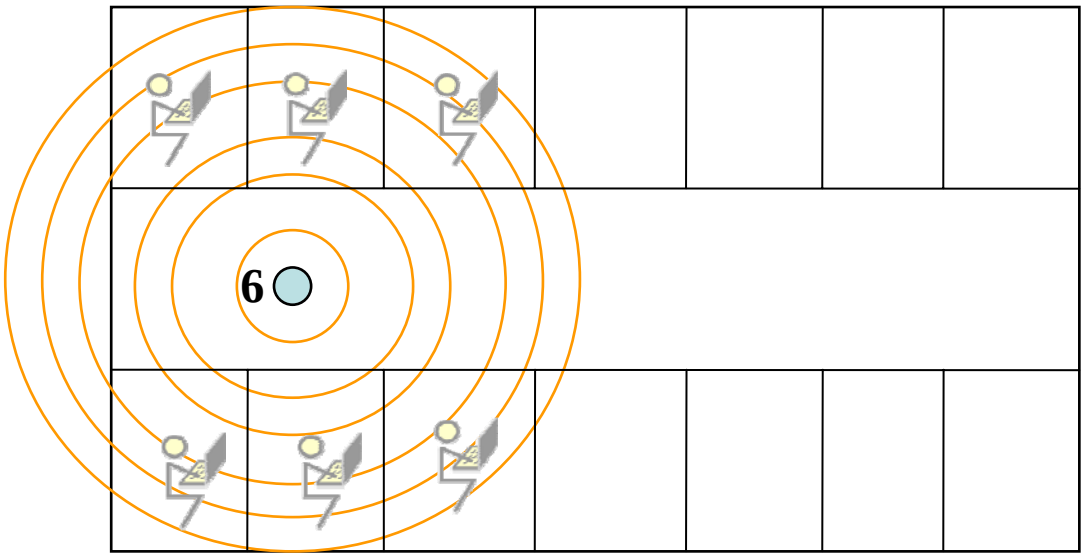


Figura 98. Pruebas Paso 3

4. Colocábamos otro access point para cubrir el área faltante y observábamos el comportamiento de interacción de ambas señales.

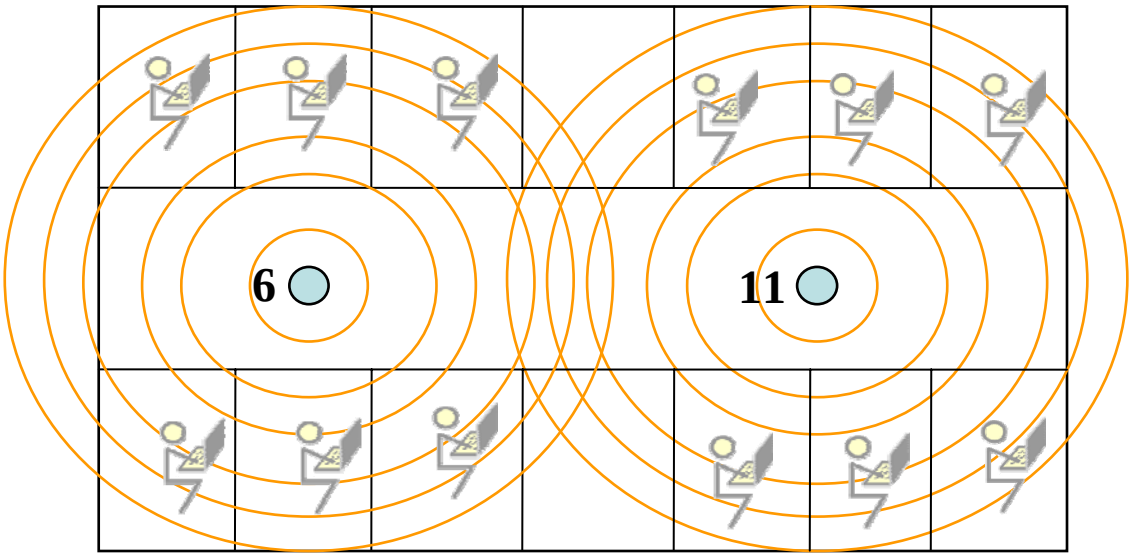


Figura 99. Pruebas Paso 4

El software que utilizamos para realizar las mediciones es el que viene integrado con las tarjetas de red inalámbrica 3com (Figura 100).

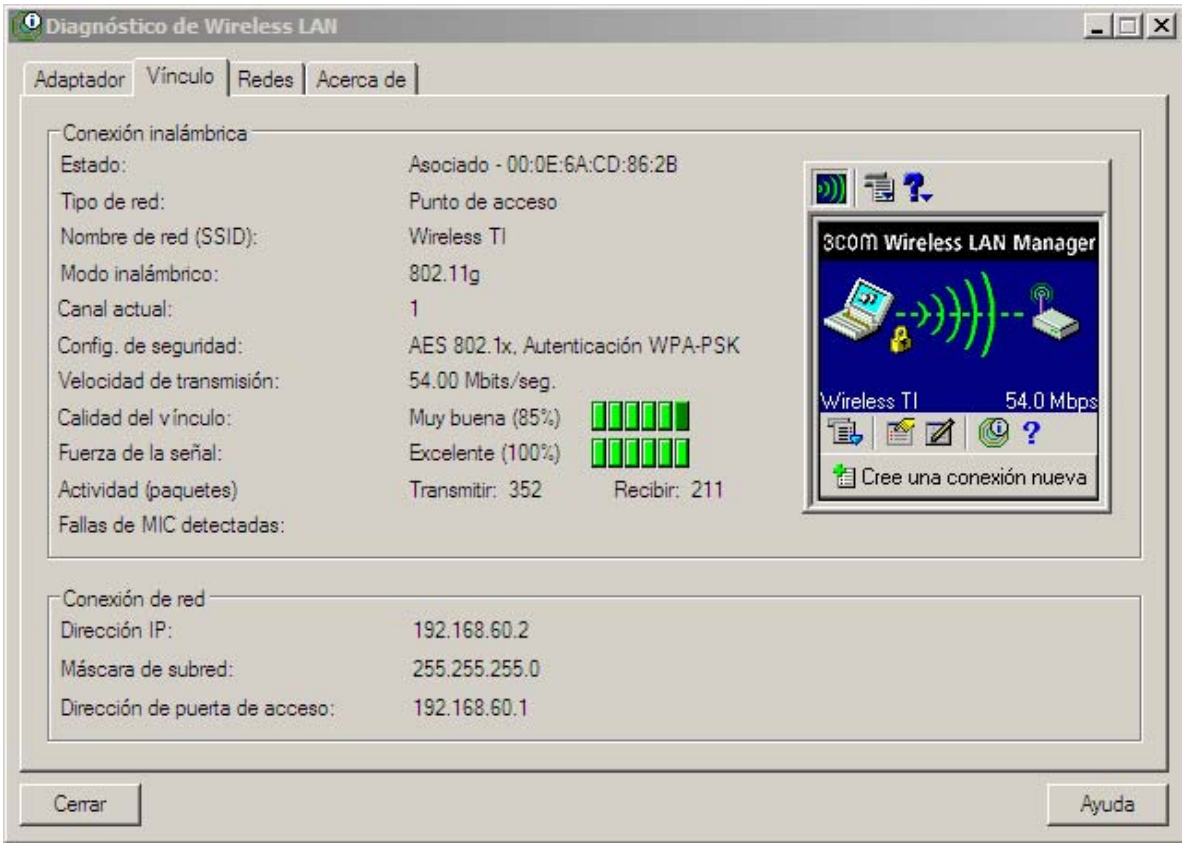


Figura 100. Software 3Com

Cabe mencionar que estas pruebas se llevaron a cabo piso por piso de cada edificio, ya que las condiciones de éstos varían no solo con base en el material con el que están construidos, también de acuerdo al personal que se desempeña en éstos. Podemos mencionar algunas de las situaciones que se presentaron en la realización de estas pruebas:

Edificio 1. Se pensó que con un punto de acceso ubicado en la sala de juntas de la dirección sería suficiente para brindar el servicio a todo el personal de la dirección, sin embargo, la señal se atenuaba considerablemente al atravesar los muros y por ello, finalmente se ubicaron dos puntos de acceso tomando como criterio principal el área de cobertura porque en esta zona no se tiene planeado el uso del servicio masivamente.

Edificio 2. Este edificio presentó pocos problemas, a pesar de que concentra un gran número de usuarios, y por ello muchos cubículos, el material de las paredes no atenúa en gran medida la señal y tampoco existen equipos que produzcan interferencias.

Edificio 4. En este edificio también se tomo como criterio de decisión el área de cobertura que brinda la antena, nuevamente, el material de los muros y la geometría del lugar hicieron necesaria la utilización de dos puntos de acceso.

Edificio 5. Aquí, nos encontramos con la mayor problemática; además de que es el edificio que concentra el mayor número de usuarios, el material de los muros atenúa la señal considerablemente en algunos sectores y, además, cuenta con diversos equipos como frigoríficos, hornos de microondas y calentadores, bombas, etc. que causan interferencia. Para este último caso fue necesario alejar el access point de estos equipos, sin embargo hubo casos en los que esto resultaba imposible porque coincidía la ubicación de los equipos con los sectores en los que los muros degradaban intensamente la señal; para ello se realizaron un gran número de pruebas en prácticamente todas las zonas del edificio hasta que finalmente se logró una buena distribución con una velocidad de transmisión buena y la total cobertura del edificio. Así mismo se presentó interferencia, provocada entre sí por los mismos access, lo que fue solucionado al utilizar canales más separados entre sí y que a su vez estuvieran alejados de la frecuencia en la que operan equipos como hornos de microondas.

Laboratorio de Olas. Éste es considerado una zona abierta, no tiene muros difíciles de atravesar y tampoco concentra un gran número de usuarios. La ubicación del punto de acceso no tuvo ningún inconveniente.

Para la colocación del bridge inalámbrico es obligatorio la línea de vista directa (LOS), por lo que fue necesario instalar mástiles en las partes más altas tanto de la Torre de Ingeniería como de la Mesa vibradora. La distancia entre estos puntos (que es donde se colocarán las antenas), es de 1.5Km. Fue necesaria la instalación previa de pararrayos, así como caja metálica (para colocar los bridges dentro) para la protección de los equipos.

Este análisis se completa con el análisis y diseño de la red inalámbrica que unifique criterios de eficacia y rendimiento con la estética propia de un instituto moderno, dotándole de un contenido completo, con el consiguiente ahorro de costes y una perfecta integración del servicio y su entorno.

4.1.2 Análisis de la red

Algunas de las características más importantes de la red del Instituto de Ingeniería son las siguientes:

- Velocidad de los enlaces de backbone a 2 Gbps que comunican a los diferentes edificios con los servidores centrales del Instituto y con la red Internet.

- Puertos de red de los usuarios a 100Mbps y 1Gbps switcheados para el mejor aprovechamiento del hardware de red de las PC's

- Mayor capacidad del enlace a Red UNAM de 1Gbps.

- Mayor eficiencia en la transmisión de las aplicaciones en la red a través de la segmentación de tráfico con la implementación de VLAN’s controladas en el backbone de la red.

- Comunicación a la Torre de Ingeniería para efectos de redundancia.

- Utiliza la red de datos y su red de cableado estructurado para mejorar y ampliar la cobertura del servicio telefónico.

- Por último, con este sistema es posible soportar redes privadas virtuales (VPN's) permitiendo el acceso a la red del Instituto con todos los servicios que el usuario (investigador) tiene derecho y con esto bajar costos de comunicación (larga distancia) telefónica y de datos hacia el Instituto.

Características más importantes del Firewall (ISA Server 2004):

- Actúa a nivel de aplicación
- Detector de intrusos
- Filtro SMTP
- Facilidad de administración
- Integración con Active Directory
- Autenticación en redes
- Compatibilidad mejorada con VPN
- Capacidades de cuarentena VPN
- Capacidad para crear grupos de usuarios personalizados de servidor de seguridad
- Posibilidad de trabajar con numerosos proveedores

Características de los Servidores:

- La base de servidores está montada sobre plataformas Windows, específicamente Windows 2003 server, que se encargan de administrar el correo electrónico, impresoras, servicios web, etc.
- La administración de los usuarios, computadoras, impresoras, etc., es realizado mediante Active Directory.
- Cuentan con servidores UNIX para la administración de correo electrónico y paginas web.

En todos los edificios se tiene switches que ofrecen velocidades de 100Mb y que son conectados al core principal mediante fibra óptica.

4.2 Requerimientos del Instituto de Ingeniería

El Instituto de Ingeniería como centro de investigación y desarrollo tecnológico, está enfocado a realizar investigación dirigida a la solución de problemas de interés nacional en las áreas de ingeniería, para ello, cuenta con una estructura académico-administrativa formada por investigadores y personal especializado entre los que se encuentran profesores y becarios.

Ahora bien, contextualizándonos en el tema de estudio de esta investigación, al

hablar de la implantación de una red inalámbrica se parte del objetivo establecido por éste de modernizar su estructura operativa, y de que tal modernización refleje como resultado un mejor desempeño de su personal.

Para lograr esta mejora es necesario considerar que en estos proyectos existe la necesidad de colaboración de varios investigadores, profesores, estudiantes y personal administrativo, así como la necesidad de poder colaborar con científicos de otros países, para los cuales requiere contar con disponibilidad y confiabilidad para soportar y facilitar las actividades científicas que se desarrollan en el Instituto, así como mejorar las posibilidades de comunicación entre las personas que trabajan en él y brindarles nuevos servicios que les ayuden a desempeñar de manera más eficiente y productiva su labor, por ejemplo para proyectos que se desarrollan en campo y que es necesario recopilar datos y transferirlos para su procesamiento e interpretación.

Actualmente el Instituto de Ingeniería cuenta con una infraestructura moderna, entre la cual destaca el sistema de redes, por la convergencia de tecnologías de voz y datos, proporcionando con éste un buen servicio de comunicación entre sus usuarios. Sin embargo, no cuenta con la cualidad de movilidad que requiere, no solo para el desarrollo de sus proyectos, también para que los investigadores puedan reunirse en salones o auditorios para efectuar congresos, charlas, etc., sin estar limitados por distancias de cables o número de nodos de red disponibles.

Así mismo se debe considerar que, como se menciono, existe una gran cantidad de estudiantes becarios que participan en el Instituto de Ingeniería, algunos realizan investigaciones específicas y otros prestan un servicio en el cual muchas veces se hace necesario contar con red en cualquier lugar y momento; para el primer caso cabe mencionar que existen cubículos que concentran varios becarios, aquí se hace necesario compartir el nodo de red por lo que, no se les puede dar el servicio simultáneamente a todos los usuarios, sin embargo muchos de ellos cuentan con laptop's con tecnología inalámbrica integrada que no es aprovechada; en el segundo caso, por ejemplo, se encuentran los becarios del área de cómputo, los cuales salen a todos los edificios a prestar servicios y para los cuales siempre es necesario contar con una computadora con acceso a red para efectuar cambios, registros, reservaciones de direcciones, etc.

Es por todo lo anterior que se propone una red inalámbrica que provea la característica de movilidad que el Instituto de Ingeniería requiere, tomando como principal objetivo de esta implantación el desempeño eficaz y productivo de las actividades de sus integrantes, pero también observándolo como un proyecto rentable con la mejor relación costo-beneficio y protección de la inversión, permitiendo aprovechar al máximo todas las capacidades de la red y del personal que soporta su administración. Tal proyecto que tiene como principales beneficios los que a continuación se mencionan:

- Reducción de costos
- Alta flexibilidad
- Facilidad de implantación

4.2.1 Aplicaciones y servicio de red

Al ser la red inalámbrica una extensión del la red LAN del Instituto de Ingeniería, las aplicaciones y servicios que ésta ofrezca, dependerán en mayor medida de los puntos de acceso, de los equipos en que éstos se conecten (switches) y del backbone del Instituto.

Actualmente la red ofrece velocidad en los enlaces de backbone a 2Gbps que comunican a los diferentes edificios con los servidores centrales del Instituto y con la red Internet, puertos de red de los usuarios a 100Mbps y 1Gbps switcheados para el mejor aprovechamiento del hardware de red de las PC's, mayor capacidad del enlace a Red UNAM de 1Gbps.

En cuanto a los puntos de acceso se refiere, deberán garantizar total compatibilidad, interoperabilidad y un funcionamiento que satisfaga las necesidades y requerimientos del Instituto de Ingeniería.

Con todo lo anterior las aplicaciones y servicios de red que la red inalámbrica del Instituto de Ingeniería ofrecerá son:

- Conexión a Intranet e Internet
- Correo electrónico
- Sesiones remotas
- Administración y monitoreo de equipos
- Transferencia de Archivos
- Almacenamiento de datos/respaldo en red
- Videoconferencia de escritorio
- Reproducción de video
- Gestión de Bases de datos

A continuación se muestra una tabla que contiene el ancho de banda que consumen ciertas aplicaciones de Internet.

Aplicación	Ancho de banda/usuario	Notas
Mensajes de Texto	< 1Kbps	Como tráfico es Infrecuente y asíncrono.
Email	1 a 100Kbps	Es intermitente y asíncrono. Archivos adjuntos, virus y spam incrementan significativamente el uso del ancho de banda. Es

		importante aclarar que los servicios de emailo vía web (tal como yahoo o hotmail) deben ser considerados como web browsing, no como email.
Web browsing	50 a 100Kbps	Los web browsers sólo utilizan la red cuando un dato es requerido. La comunicación es asíncrona. Cuantos más datos requieran (imágenes grandes, descargas grandes, etc.) mayor es la utilización del ancho de banda.
Streaming audio	96 a 160Kbps	Cada usuario de este servicio usará una cantidad constante de ancho de banda.
Voz sobre IP (VoIP)	24 a 100Kbps	Cada usuario usará una constante cantidad de ancho de banda dependiendo de la duración de la llamada, el cual es usado en ambas direcciones. No se aceptan retrasos
Streaming Video	64 a 200Kbps	Se evita la latencia utilizando buffers en el cliente. Requiere alta velocidad de conexión y baja latencia para trabajar adecuadamente
Aplicaciones Punto-a-Punto	0 a infinito Mbps	Este tipo de aplicaciones suelen utilizar todo el ancho de banda disponible para transmitir los datos tan rápido como sea posible.

Tabla 11. Ancho de banda consumido según aplicación en Internet

Para estimar el throughput (velocidad con la que se envían y reciben datos) que necesitaría una red, sólo hay que multiplicar el número de usuarios esperados por el tipo de aplicación que usarían. Por ejemplo, 50 usuarios que usan principalmente el web browser consumirán entre 2.5 y 5Mbps o más en horas pico. Por otro lado, 50 usuarios simultáneos de VoIP requerirán de 5Mbps o más en ambas direcciones, y como el access point es half duplex esta cantidad se duplica teniendo 10Mbps.

4.2.2 Conectividad

Los Puntos de acceso deberán estar colocados en los edificios de tal manera que los usuarios obtengan velocidades de conexión aceptables (por arriba de 11Mbps), y que además cubran todas las posibles áreas de trabajo. Deberán estar configurados para evitar interferencias entre ellos, ya que esto minimizaría el desempeño de la red inalámbrica, con balanceo de cargas para

una distribución óptima de usuarios y con característica roaming para que los usuarios puedan trasladarse entre puntos de acceso sin perder conectividad.

4.2.3 Interoperabilidad

La red inalámbrica deberá estar cimentada sobre estándares y normas que garanticen la interoperabilidad entre los diversos elementos de software y hardware que son utilizados en el Instituto de Ingeniería.

4.2.4 Capacidad de desempeño

El avance en el poder de procesamiento de equipos conectados a la red y la creación de aplicaciones que cada vez requieren de un mayor consumo de ancho de banda pueden llegar a ocasionar tráfico excesivo en la red. Los elementos de hardware de la red inalámbrica deberán de ser lo suficientemente flexibles para que permitan ser configurados para llevar a cabo modificaciones y alcanzar un nivel de desempeño óptimo cuando sea necesario.

4.2.5 Administración

Actualmente la plataforma de administración del Instituto de Ingeniería proporciona monitoreo y análisis de tráfico, modificación de las configuraciones de los equipos de manera remota y la generación de diagnósticos sobre el rendimiento y funcionamiento de cada uno de los dispositivos de la red. Por lo tanto, los elementos añadidos para la operación de la red inalámbrica, así como la reestructuración de la red cableada existente, no deben contradecir estas acciones, si no que por el contrario, deben cumplir tajantemente los mismos principios.

4.2.6 Seguridad

El modelo de seguridad que se implantará en la red inalámbrica del Instituto de Ingeniería deberá estar sustentado y guiado por el hecho de que la propagación de la señal inalámbrica es de naturaleza broadcast. Todos los elementos de hardware y software que sean contemplados para la planificación del esquema de seguridad, deberán girar entorno a dicho argumento. Todo esto para ofrecer los elementos básicos de un sistema de seguridad: la confidencialidad de los datos, la autenticación de los datos, la integridad de los datos, el control de acceso (disponibilidad) y el no repudio.

4.2.7 Tolerancia a fallos

Siendo la red inalámbrica una subred de la red LAN, hereda las características tolerantes a fallos en la red. Actualmente la red del Instituto cuenta con:

- Enlaces múltiples, los cuales aseguran que todos los dispositivos principales de red estarán interconectados por lo menos a dos rutas.

- Módulos redundantes y módulos de intercambio rápido (hot swap) en tiempo de operación de la red.
- Fuentes de poder ininterrumpibles, las cuales son capaces de soportar las operaciones de red durante minutos u horas cuando se interrumpe el suministro de energía.

4.2.8 Flexibilidad topológica

Las tecnologías de redes inalámbricas están siendo actualmente desarrolladas con gran rapidez. Por lo tanto, la tecnología que se escoja para la implantación de la red inalámbrica del Instituto de Ingeniería deberá garantizar que en un futuro, ante el inevitable nacimiento de nuevas tecnologías, pueda ser integrada sin que cause conflictos en su operación. Además de que debe permitir integrar dichas tecnologías sin necesidad de un rediseño total o, peor aún, el desuso de ésta.

4.2.9 Documentación

Es importante que la arquitectura de la red inalámbrica del Instituto de Ingeniería esté documentada en su totalidad para tener una base de información útil para la administración, mantenimiento y actualizaciones de la misma. Está documentación puede estar constituida por manuales de instalación, operación y mantenimiento de los equipos de red, reportes de revisiones técnicas del hardware y su software asociado, los proyectos de migración y actualización, las instalaciones de nuevas versiones de software, la integración con otras tecnologías de red y la limpieza periódica de equipos.

4.3 Diseño

4.3.1 Análisis de metodología

En este tema se efectúa la explicación de cada fase que llevaremos a cabo durante el proyecto de la red inalámbrica del Instituto de Ingeniería.

Desde un punto de vista muy general, el proyecto tiene tres grandes etapas:

Fase de Análisis. En esta etapa se efectuará un levantamiento de información que permita conocer el estado actual del Instituto de Ingeniería y con ello, saber cuáles son los requerimientos que debe satisfacer la red inalámbrica. Esta recopilación de información arrojará datos de infraestructura de las instalaciones, así como de la infraestructura técnica de la red. Con este análisis verificaremos que los requisitos son alcanzables y que los objetivos particulares y generales de este proyecto sean satisfechos. Esta etapa es de gran importancia, ya que los resultados obtenidos nos permitirán definir qué hacer para realizar el proyecto. Una vez llevado a cabo este estudio comenzaremos con la fase de diseño.

Fase de Diseño. Durante esta etapa se esquematizan las características técnicas específicas de la red inalámbrica del Instituto de Ingeniería, así como la gestión de los recursos en la forma adecuada para desarrollar el proyecto en cuestión. En esta etapa los factores a considerar son la estructura física y lógica de la red, tecnología, seguridad y administración de la misma. Esta fase toma su importancia del hecho de que nos permite saber cómo llevar a cabo el proyecto para encontrar la solución tecnológica óptima.

Fase de puesta en marcha o implantación. Esta fase se refiere a la puesta en marcha de la red inalámbrica, comprobando que funciona adecuadamente y responde a las especificaciones en su momento aprobadas. En esta etapa se pretende generar el servicio pretendido con la red, integrando todos los factores previamente considerados y validar que la red inalámbrica satisface los requisitos de diseño previamente definidos y realizar, si es necesario, los ajustes necesarios en dicho diseño para corregir posibles errores o inconsistencias.

4.3.2 Arquitectura

Configuración física y lógica de la Red Inalámbrica

Actualmente la red del Instituto de Ingeniería tiene la siguiente estructura:

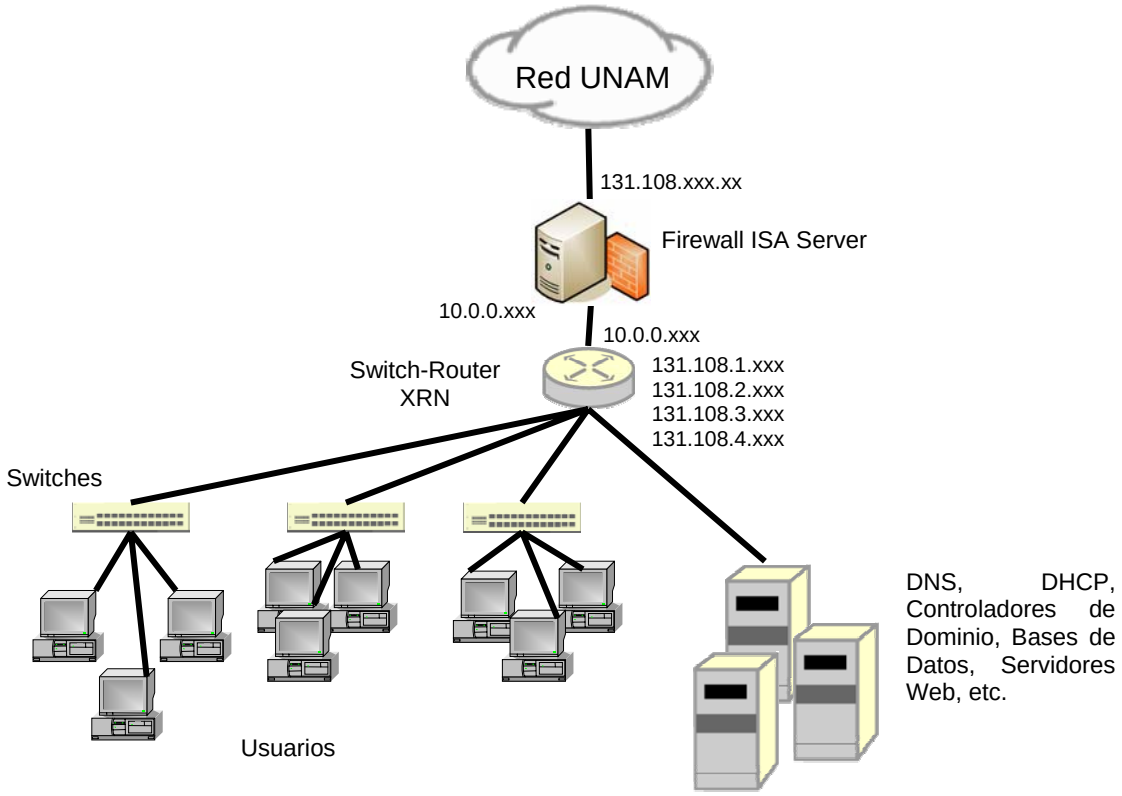


Figura 101. Configuración de la Red Inalámbrica

De este esquema sobresalen dos elementos importantes:

- ISA Server. El cuál está en modo de ruteo, es el elemento que define el perímetro de la red del instituto. Toda información que desee salir o entrar tiene necesariamente que pasar por él.

- Switch-Router XRN. Es el que distribuye todo el tráfico de la red. Sus tablas de ruteo son estáticas por lo que todo paquete que desee salir es mandado hacia el ISA Server, en donde actúan las políticas establecidas.

Al integrar la red inalámbrica no es necesaria la modificación de este esquema ya que por cuestiones de seguridad la wlan del instituto debe ir conectada directamente al firewall. La ventaja que obtenemos con esto, es que podemos tratarla como una red independiente aplicándole diferentes políticas, además de que el firewall estará actuando a nivel de aplicación, propiedad que perderíamos si la conectamos directamente al router. El esquema sería el siguiente:

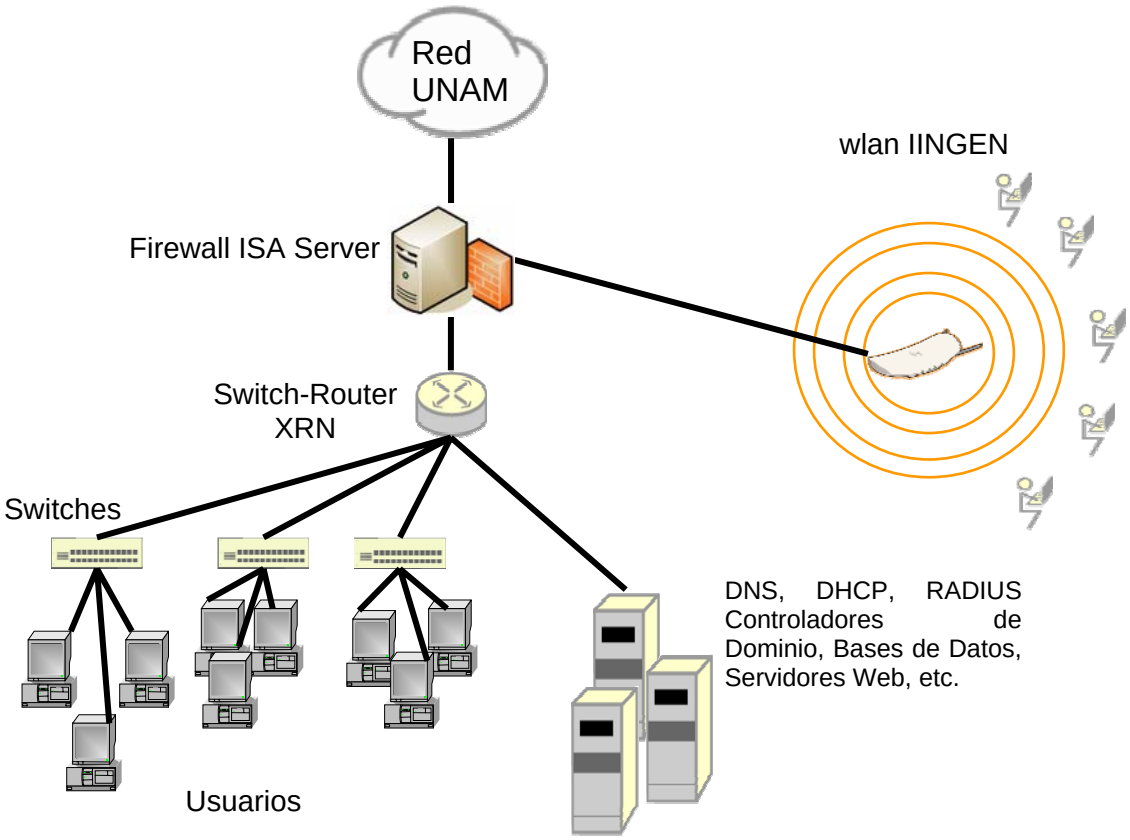


Figura 102. Esquema de conexión como red independiente

4.3.2.1 Red inalámbrica para visitantes

Es importante tener en cuenta lo siguiente:

- Primeramente, definir lo que sería una máquina visitante.
- Con base a la definición anterior se pueden, entonces, establecer las políticas de la red, esto es, los servicios a los que los usuarios de esta red tendrán acceso.

Una vez definidos los dos puntos anteriores se podrán realizar las configuraciones tanto lógicas como físicas. Por lo tanto, se propone:

1. Una máquina visitante será toda aquella que esté fuera del dominio IINGEN y que desee hacer uso de la red para accesar a los diferentes recursos (Internet, Intranet, archivos compartidos, descarga de software, mail, etc.).
2. Debido a que no se tiene ninguna garantía del estado de la máquina, esto es, que tenga antivirus, parches, actualizaciones del sistema operativo, etc., no podrá tener acceso a los recursos del dominio y sólo podrá hacer uso de Internet (protocolo http, puerto 80. Los demás puertos y protocolos quedan excluidos).

Con base en las definiciones anteriores, se puede entonces dividir el problema en dos partes: Una correspondiente al Firewall, y la otra correspondiente a la configuración de Access Points, direccionamiento IP, creación de VLAN's, etc.

La parte que corresponde al Firewall prácticamente ya está resuelta ya que se aplicarían las mismas políticas que se tiene para toda máquina que proviene del exterior (que no pertenece a la red del instituto). Para la otra parte se complican un poco más las cosas; analizando se tienen las siguientes propuestas:

1. Los access points que están actualmente instalados y brindando el servicio de red inalámbrica, cuentan con una característica (no estandarizada) que sería de mucha utilidad. Nos referimos al "**Virtual Access Point"**. Lo que esto permitiría, es tener lógicamente dos access points por cada uno, configurados hasta cierto punto de manera independiente. Esto quiere decir que podríamos tener dos redes inalámbricas por cada access point con su respectivo SSID (que obligatoriamente debe ser diferente) y además separadas por diferentes VLANS, ya que también es posible que los access points soporten la diferenciación (TAG's), logrando así, la separación de ambas redes. Sólo bastaría crear la vlan en el swich-router y asignarle un segmento diferente de direcciones IP's no homologadas. Con respecto a la seguridad, cada virtual access point puede ser configurado de manera independiente, excepto si se desea utilizar servidor Radius para ambas subredes, ya que si se define la utilización de éste para ambas, las dos

harían referencia al mismo servidor definido en el access point. Cabe destacar que no es necesario tener una autenticación rigurosa para los visitantes ya que su acceso a la red es temporal, por lo tanto sólo bastaría con utilizar WPA en modo PSK (Pre-Shared Key). Con esta opción se garantiza que sólo los usuarios que conocen la clave podrían accesar y por otro lado, los paquetes son cifrados con el estándar más fuerte (AES) (Figura 103).

Ventajas:

- No es necesaria la colocación de access points extras para la red de visitantes.
- Se tendría un control de las máquinas visitantes que deseen ingresar a la red.
- Quedaría aislada totalmente la red de visitantes.

Desventajas:

- La administración de la red seria engorrosa ya que lo recomendable sería cambiar periódicamente la clave, y esto se tendría que hacerse en cada uno de los access points.
- Se tendría que ir físicamente a donde se encuentra el usuario para poder meter la clave.

2. Una alternativa bastante atractiva es el **"Portal Cautivo"**. Un portal cautivo es un programa o máquina de una red informática que vigila el tráfico HTTP y forza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal. A veces esto se hace para pedir una autenticación válida, o para informar de las condiciones de uso de un servicio wireless (que es donde más se encuentran). De esta manera los usuarios visitantes al intentar ingresar a la red se les desplegaría una página para que introduzcan un nombre de usuario y contraseña. Existen portales cautivos montados sobre diversas plataformas, siendo Linux y Windows las más comunes.

   Ventajas:

   - Fácil administración
   - Control y registro de los usuarios visitantes que deseen conectarse

   Desventajas:

   - Algunos portales tienen costo, los que no, están montados sobre plataformas Linux, lo cuál desentonaría de la actual plataforma sobre la cual se está administrando.
   - Posibles deficiencias que permitirían a usuarios no autorizados a acceder a la red.
   - No existiría cifrado alguno.

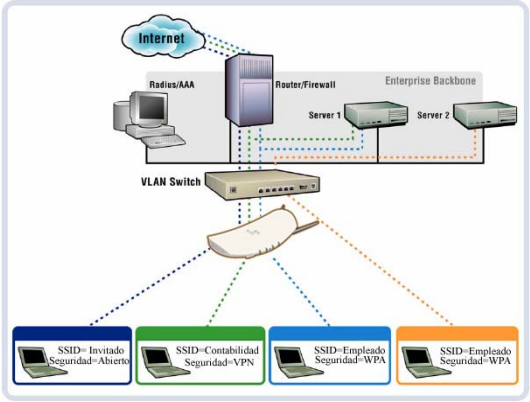


Figura 103. Funcionamiento del Virtual Access

4.3.3 Tecnología

Acces Points 3com 8750

Características:

- Cumple con los estándares 802.11a, b y g.
- Soporta 250 usuarios conectados simultáneamente
- Ofrece una arquitectura dual-band
- En seguridad ofrece:
  - WEP de 64, 128 y 152 bits
  - Listas de control de acceso
  - Soporta el estándar IEEE 802.1x con autenticación vía servidor RADIUS
  - TKIP
  - AES
  - WPA, WPA2
  - EAP
- Roaming
- PoE (Power over Ethernet)
- SNMP (Simple Netwok Managment Protocol)
- Filtrado por VLAN's
- Virtual Access Point
- Filtro de protocolos y puertos
- Tiempo limite de conexión
- Modo Turbo
- Operan con antenas diversidad

Parámetros a Configurar

Frecuencia

Como se mencionó anteriormente el access point, es capaz de trabajar en las frecuencias de 2.4 y 5GHz. Debido al la comercialización del estándar 802.11b/g, ésta será la primera opción aunque de ser necesario, se tiene la

capacidad de ofrecer el servicio a 5GHz sin la modificación del esquema y mejor aún, sin la adición de nuevo equipo.

En áreas donde sea necesario colocar más de dos access poitns se deberá configurar los mismos en diferentes frecuencias para que no haya interferencias entre ellos, como demanda el estándar. La siguiente figura ejemplifica la configuración:

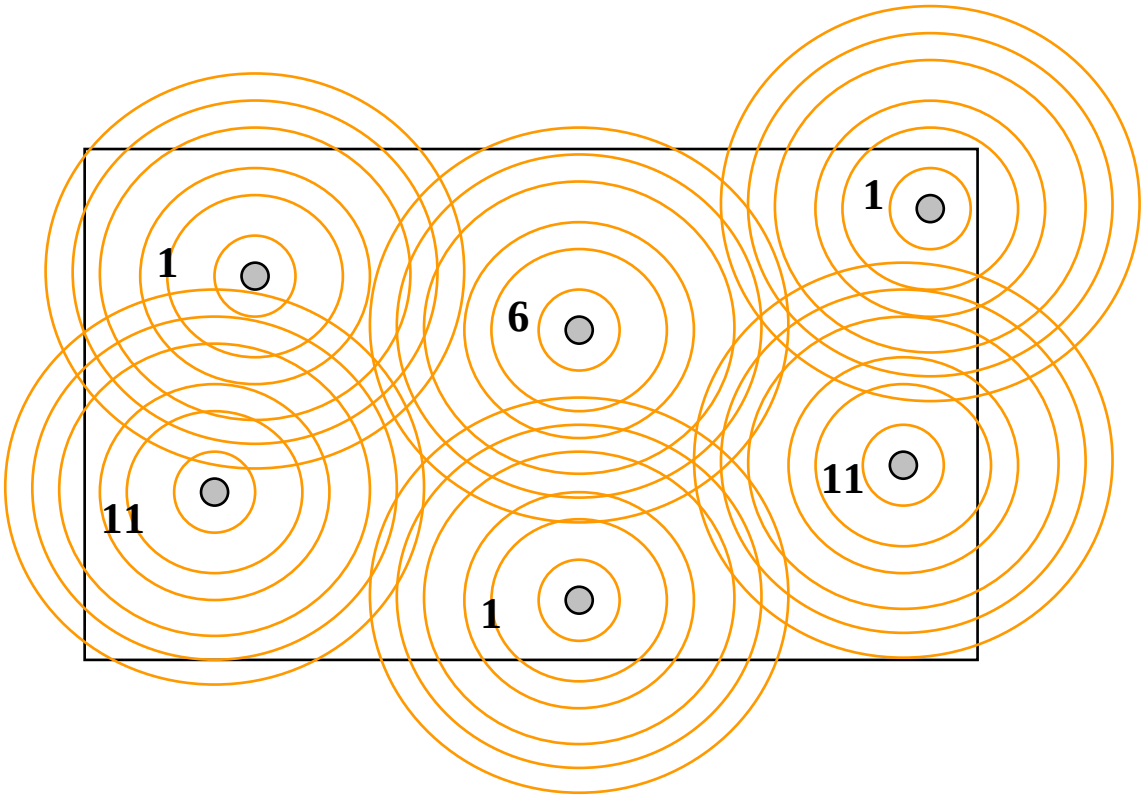


Figura 104. Cobertura de un área por varios AP's

SSID

El SSID es un parámetro importante que ayudará a los usuarios de la red a identificar a cual red deberán asociarse, por eso es importante que se ponga uno que sea fácilmente identificable.

Autenticación y cifrado

En seguridad el protocolo más seguro hasta el momento es WPA, con esto será de manera obligatoria la autenticación mediante un servidor Radius y por el lado del cifrado de datos, AES resulta el estándar más fuerte. Este esquema de seguridad resulta muy ventajoso ya que como ya se cuenta con un dominio, Windows 2003 Server proporciona un servicio de Radius que valida a los usuarios y/o computadoras de Active Directory. La ventaja inmediata de ésto, es que los usuarios no tendrían que validarse dos veces (una para entrar a su computadora y otra al accesar a internet).

4.3.4 Seguridad

4.3.4.1 Bases para el diseño del firewall

Es importante tener en cuenta las siguientes consideraciones para la elaboración de las políticas que impondrá el firewall y que regirán la red inalámbrica del instituto:

- Recursos a los que podrán tener acceso los usuarios de la red inalámbrica.
- Políticas actuales que rigen la red cableada del Instituto de Ingeniería.
- Componentes de la red inalámbrica

4.3.4.2 Políticas del firewall

Existen mecanismos que permiten tener una verdadera equivalencia al cable, sin embargo, es importante que la red inalámbrica pase necesariamente por el firewall debido a que, con ello se subsana cualquier vulnerabilidad que puedan presentar dichos mecanismos. Los recursos a los que tendrán acceso los usuarios de la red inalámbrica deben ser los mismos a los que tienen derecho los usuarios que accedan mediante ethernet. Por lo tanto, las políticas que se apliquen deberán ser las mismas evitando así, que haya incongruencias entre redes.

4.3.4.3 Política interna de seguridad

Las políticas de una red son un documento fundamental, sin el cual el rol de un administrador de sistemas no sólo se complica, sino que se vuelve imposible de realizar. Este documento es la base de toda configuración además de que guía al administrador en su labor. Un documento de políticas de red debe ser firmado por la persona que tenga el cargo más alto del la organización. Solamente de esa manera tendrá suficiente autoridad para ser obligatorio para cualquiera. Algo importante, es recordar que todo documento obligatorio para todo usuario de la red también los es para el administrador.

Este documento generalmente es de un par de páginas en donde se describen las políticas más generales. En contraposición, los procedimientos de seguridad son documentos más largos y detallados que explican a detalle cómo se va a implementar cada uno de los puntos de las políticas. Los procedimientos deben presentar una estructura similar a la de las políticas, y cada uno de sus puntos debe servir de explicación a su contraparte en las políticas. Al estar separados estos documentos, el personal operativo puede adecuar los procedimientos sin pasar por el proceso burocrático que significaría modificar las políticas. Un ejemplo de una política es que el usuario debe tomar las precauciones necesarias para evitar la propagación de virus a través de la información que él maneje, y los procedimientos indicarían cómo debe tratar un usuario la información que introduzca por el método que sea al centro de cómputo. Es importante mencionar que si dejamos puntos sin definir en las políticas y en los

procedimientos, o si hay algunas indicaciones que sean contradictorias, el documento pierde fuerza y puede servir de pie para ataque.

4.3.4.4 Componentes del sistema firewall

- **Ruteador Filtra-paquetes**. Este ruteador toma las decisiones de rehusar ó permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si éste corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP,ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interface de entrada del paquete, y la interface de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, éste será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado.

- **Gateways a nivel aplicación**. Los gateways a nivel aplicación permiten al administrador de red la implantación de una política de seguridad más estricta que la que permite un ruteador filtra-paquetes. Se instala en el gateway un código de proposito-especial (un servicio Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall.

- **VLAN's**. Las redes virtuales incrementan el nivel de seguridad sobre cualquier infraestructura ya que permiten la separación lógica de subredes, además de que permiten una mejor administración de la red.

4.4 Administración de subredes y direcciones IP

4.4.1 VLAN's

Al implantar la red inalámbrica sobre una red virtual (vlan), provee la posibilidad de evitar visibilidad del tráfico de red, previniendo así que accesos no permitidos sean llevados a acabo. El esquema de redes virtuales evita que personal no autorizado haga uso de direcciones IP que solamente corresponden a la red inalámbrica del Instituto de Ingeniería (Figura 105).

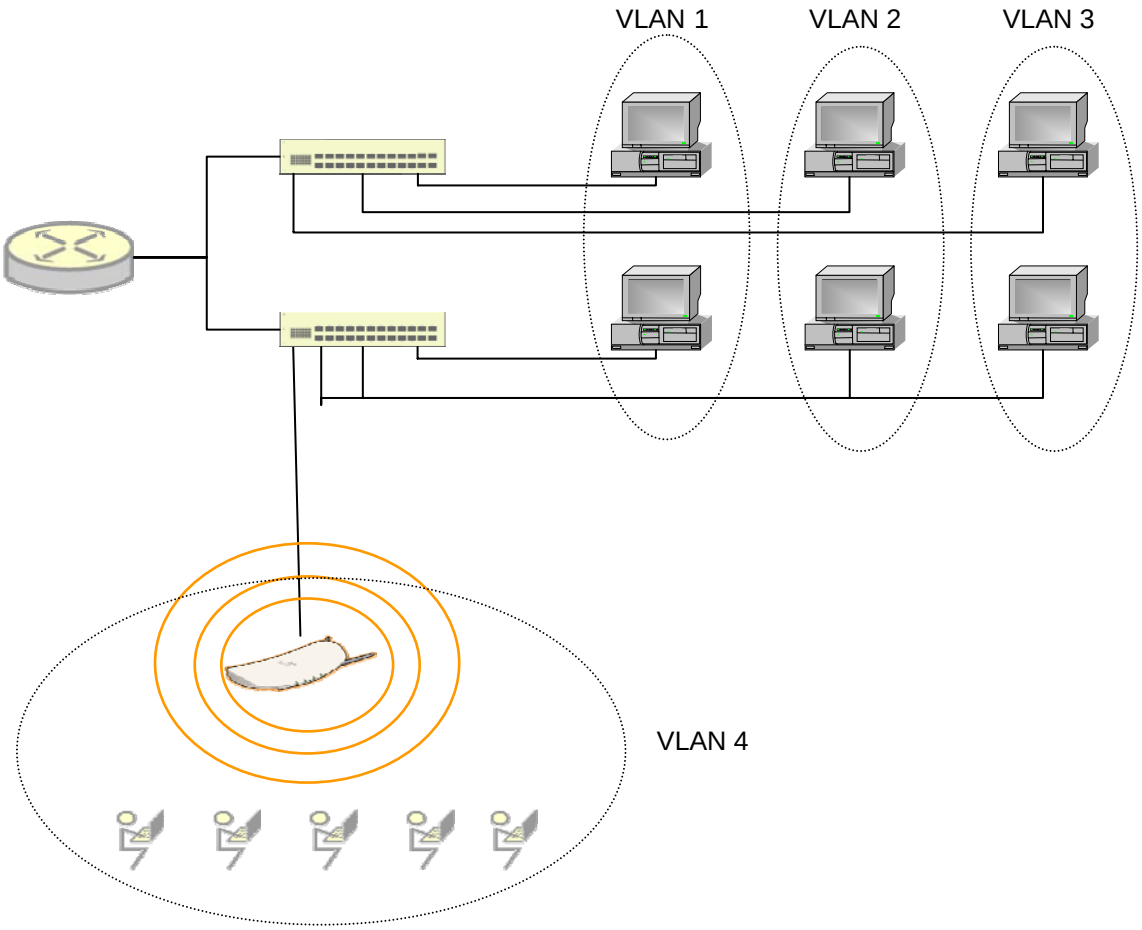


Figura 105. Esquema de administración

4.4.2 NAT

Debido a la escasez de direcciones IP que pudiera presentarse, además de ser una práctica sana de administración y de que proporciona un nivel de seguridad, se hace necesaria la implantación del mecanismo NAT para la red inalámbrica (Figura 106). En este caso, la tarea de traducción la llevaría acabo el firewall ISA Server.

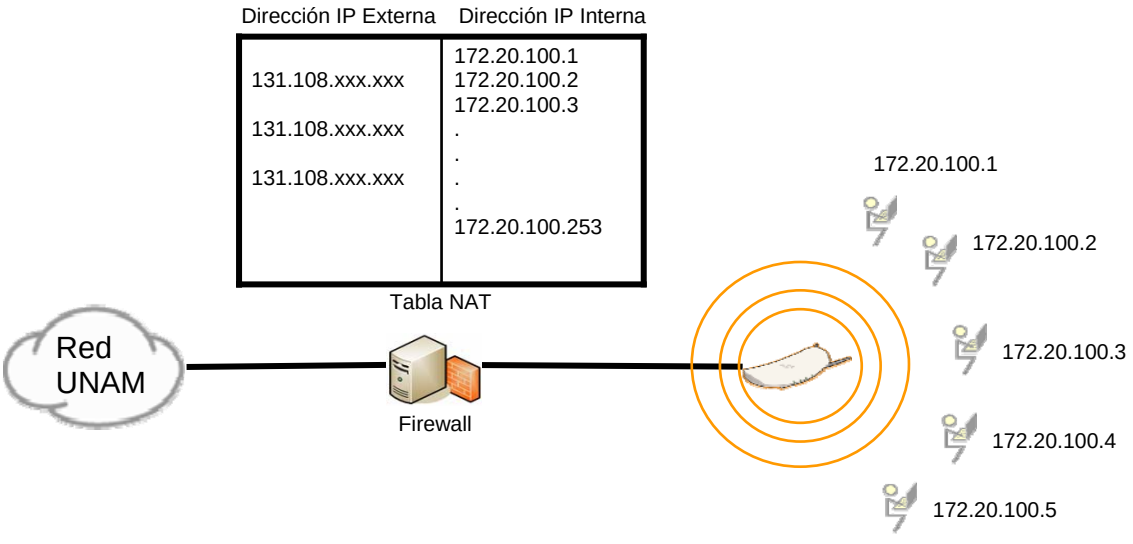


Figura 106. Esquema de Nateo

4.4.3 DHCP

Actualmente la asignación de direcciones IP mediante DHCP se lleva a cabo de manera estática. Esto es, el administrador preasigna manualmente a cada dirección física una dirección IP. Por cuestiones de administración es conveniente seguir con tal práctica, ya que de esta manera se tendría un control sobre los usuarios que deseen hacer uso de la red inalámbrica.

5

Desarrollo y análisis de resultados

Introducción

De acuerdo con los capítulos anteriores, dentro de este capítulo procede explicar la descripción de la última etapa correspondiente a la implantación de la red inalámbrica. Este capítulo se refiere a las pruebas que se llevaron a cabo para verificar el diseño y óptimo funcionamiento de la red y los resultados obtenidos en éstas.

5.1 Implantación

Con base en las características del punto se acceso, debemos mencionar que éste cuenta con la de ser "user friendly", o lo que es lo mismo, fácil de configurarlo.

5.1.1 Descripción de pruebas

Para llegar al punto de implantar la red LAN inalámbrica se realizó un trabajo de planificación y diseño previo sostenido en los resultados de las pruebas que se efectuaron; durante estas pruebas el factor más importante fue la óptima y eficaz distribución de los access points en el Instituto de Ingeniería considerando principalmente: la velocidad de transferencia, interferencias, las condiciones del medio e infraestructura existente.

Así mismo, cabe mencionar que de acuerdo a requerimientos propios del Instituto, la implantación de la red inalámbrica está planeada para cubrir la mayoría de los edificios, sin embargo no están dentro de esta cobertura inicial los edificios 3, 6 y 8.

5.1.2 Descripción de pruebas de cobertura

Las pruebas de cobertura se llevaron a cabo midiendo el alcance en metros y la velocidad de transmisión que tienen los access points, para ello fue necesario explorar cada nivel de los edificios que conforman el Instituto de Ingeniería, ya que, éste no tiene una homogeneidad en las estructuras de éstos.

Por lo anterior, se probó la cobertura que alcanza la señal de los ap´s en zonas libres, y en cada edificio en dirección radial. Se observó que tal alcance variaba mucho de acuerdo a la distribución de los cubículos en cada edificio, así como la presencia de equipo industrial, y la presencia de otras redes.

Una vez observado que no podíamos seguir el mismo patrón de distribución en todos los edificios, se recurrió a colocar access points en diferentes ubicaciones y se fue midiendo la calidad de la señal, logrando conocer la cobertura que ofrecen en ubicaciones específicas. Como se mencionó, esta labor se desarrollo en todos los edificios del Instituto de Ingeniería llegando finalmente a la siguiente distribución, en la que se garantiza la total cobertura de las áreas planeadas con una velocidad de transmisión no menor a 11Mbps, lo que,

permite que todos los usuarios desempeñen sus actividades sin problemas con la red.

Cabe mencionar que los puntos acceso se instalaron en techos y zonas altas lo más despejadas posibles, con el fin de que la señal se propague en la mayor área posible.

5.1.3 Descripción de pruebas de interferencias

De igual manera se hizo necesario examinar los canales de frecuencia en los que operaría cada punto de acceso para obtener el mejor rendimiento y evitar en lo posible interferencias con equipos de otras dependencias e industriales. Por lo anterior, se probó utilizando los canales de frecuencias menos usadas por otros equipos, como hornos de microondas, etc., dando la mayor separación entre los canales evitando con ello las interferencias propias y externas y, tomando en cuenta que el estándar exige un mínimo de separación entre frecuencias centrales de 25MHz.

5.1.4 Distribución de los puntos de acceso

Edificio	Nivel	Ubicación
1	Planta Baja	Pasillo de la Coordinación de Instrumentación Sísmica
1	Piso 1	Sala de juntas de exdirectores, Secretaria Académica
1	Piso 1	Salón de seminarios Emilio Rosenblueth
1	Piso 2	Sala de juntas Dirección
2	Planta Baja	Sala de juntas de Subdirección de Estructuras
2	Planta Baja	Tapanco
2	Piso 1	Coordinación de Mecánica Aplicada, cubículo 204
2	Piso 2	Coordinación de Estructuras y Materiales, cubículo 309
4	Piso 1	Cubo de escalera
4	Piso 1	Cubículo A 105
5	Piso 1	Pasillo, al oriente
5	Piso 1	Pasillo, al poniente
5	Piso 2	Pasillo, al oriente
5	Piso 2	Pasillo, al poniente
5	Piso 3	Pasillo, en el centro
Lab. Olas	Piso 1	En el centro
12	Planta Baja	En el centro
12	Piso 1	En el centro
12	Piso 2	En el centro

Tabla 12. Distribución de los puntos de acceso

Como se mencionó, la distribución planteada en la tabla anterior es producto de la realización de pruebas y se pretende garantizar la total cobertura de las zonas planteadas.

Una vez definido el número de access points necesario para cubrir las áreas requeridas en este proyecto es importante conocer cuánto costará implantar estos dispositivos, así como los costos previos y necesarios para su propia instalación y, los costos de mantenimiento que se generan.

A continuación se presenta una tabla de costos, a manera de resumen, donde se muestra el desglose de los costos antes mencionados.

TABLA DE COSTOS / RED INALÁMBRICA			
Cantidad	**Concepto**	**Costo Unitario**	**Total Costo**
19	Access Point	$11,522.6	$218,929.4
19	Cableado de nodo de red • Cable Categoría 6 • Jacks • Conectores • Faceplate • Remates en panel • Mano de obra	$1,400.0	$26,600.0
	Mantenimiento	$128.22	$2,436.18
		TOTAL	$247,965.58

Tabla 13. Tabla de Costos de la Red Inalámbrica

5.1.5 Modelo de seguridad implantado

Una vez analizados los diferentes mecanismos de seguridad en redes inalámbricas, la tecnología disponible y tomando en cuenta los requerimientos del Instituto de Ingeniería, se optó por implantar un sistema de seguridad utilizando el estándar WPA2, con el método de cifrado AES y autenticando mediante el protocolo 802.1x, creando de esta manera, una infraestructura RADIUS que además permite la utilización del protocolo EAP.

Utilizar este esquema de seguridad trae consigo muchas ventajas ya que, además de ser el sistema más robusto hasta el momento propuesto por la Wi-Fi y la IEEE, el Instituto de Ingeniería ya contaba con la infraestructura necesaria para llevarlo a cabo, por lo que no implicó gastos en recursos adicionales ni una reestructuración en el diseño de la red LAN.

Toda la infraestructura con la que cuenta el Instituto proporciona la propiedad de flexibilidad ya que en caso de que el sistema propuesto llegue en un futuro a ser “hackeado”, pueden realizarse configuraciones lógicas que incrementen el grado de robustez en la red, proporcionando al usuario la confianza para la utilización de la red inalámbrica.

5.2 Administración y mantenimiento de la red inalámbrica

La red inalámbrica se agrega como un elemento más al esquema de administración actual del Instituto de Ingeniería.

Basándonos en la propuesta de diseño del capitulo anterior, el rubro de administración quedo de la siguiente manera:

- La red inalámbrica se agrega como una subred más con su propio direccionamiento, diferenciándose de las otras subredes por el tipo de direcciones IP que se asignan, esto es, este segmento utiliza direcciones no públicas.
- La asignación de las direcciones se realizan a través del DHCP pero de manera estática, es decir, la dirección IP asignada está ligada a la dirección MAC de la tarjeta de red.
- En cuestiones de seguridad, se recurre a la utilización de credenciales para autenticar al usuario en el servidor RADIUS. Tales credenciales son el nombre de usuario y la contraseña válidas en el dominio IINGEN.
- Para que puedan darse de alta computadoras, sobre todo si son visitantes, es indispensable un chequeo de seguridad previo, en el que se constate el estado de la máquina.

El monitoreo del tráfico de esta subred puede efectuarse mediante aplicaciones diversas, como analizadores de protocolo y desde el mismo firewall. Tales puntos de control son críticos para el mantenimiento de las operaciones eficientes de la red.

CONCLUSIONES

El avance tecnológico en el área de las redes inalámbricas se está dando a un paso agigantado impulsado por la Wi-Fi y respaldado por la IEEE. El hecho de utilizar el aire como medio de transmisión trae muchas ventajas, sobre todo económicas pero también desventajas inherentes con las que siempre se tendrá que lidiar.

La movilidad, flexibilidad y la disponibilidad de conexión son características que hacen a las redes inalámbricas por demás atractivas.

Es importante mencionar que las redes inalámbricas representan una alternativa funcional y cada vez más necesaria debido a los constantes desarrollos en su ámbito. En la actualidad no resultan un sustituto a las redes cableadas, si no un complemento más a éstas. La pregunta inmediata que resulta de esto es: ¿Podrán remplazar las redes inalámbricas a las redes cableadas? Esto depende específicamente de dos factores: la velocidad de conexión y la seguridad que proporcionen. Respecto a la velocidad se estima que para el año 2007 sea liberado el estándar 802.11n que promete velocidades por encima de los 500Mbps. Aunque esto suena bastante atractivo recordemos que el cable UTP categoría 6 ofrece velocidades de transmisión de hasta 1Gbps, además de la fibra óptica que en teoría tiene un ancho de banda ilimitado. En lo que a seguridad se refiere, es necesario que cuenten con mecanismos infranqueables debido a la naturaleza broadcast de la señal, pero sin incrementar el overhead en la red.

Con respecto al Instituto, debemos mencionar que un factor importante es que la red inalámbrica tiene como principal objetivo satisfacer las necesidades de sus usuarios a través del uso de tecnologías de vanguardia, independientemente del rol que éstos desempeñen dentro de éste. Así mismo debemos mencionar que la situación actual en el Instituto refiriéndonos a equipos es muy diferente a la de hace algunos años atrás, debido al auge y desarrollo que han tenido las computadoras portátiles; actualmente un gran número de usuarios disponen de esta tecnología y para ellos los nodos de conexión ethernet resultan insuficientes además de que están literalmente desperdiciando esa portabilidad y movilidad propia de sus equipos. Con los puntos de conexión de la red inalámbrica distribuidos en todas partes, la conexión a la red desde cualquier lugar es sumamente cómoda. Como se dijo anteriormente la tecnología inalámbrica trae diversas ventajas pero, va de la mano con la cableada; el II también está conformado con personal que, no cuenta con un equipo portátil móvil, o no necesita desplazarse al cubículo o salón de al lado, mucho menos a otro edificio y, para estos casos la conexión cableada es su mejor opción.

Durante la implantación de la red, se observó que ésta tiene una gran aceptación entre el personal del II, están convencidos de las ventajas que tal red les ofrece, además de que día a día están más en contacto con esta tecnología en aeropuertos, restaurantes, hoteles, bibliotecas, centros de estudio, etc.

La red inalámbrica cuenta con un esquema de administración y mantenimiento fácil de efectuar. Al igual que en la cableada se tiene control de los usuarios que hacen uso de ella, y para efectos de configuraciones en los equipos, ésta resulta muy fácil. Existen elementos necesarios para el funcionamiento de la red que son importantes y que además proporcionan gran flexibilidad de operación como son el firewall y los servidores controladores de dominio, que por otro lado, permiten una mejor administración y la integración de otros elementos como VPN's, la utilización de certificados digitales, portales cautivos, etc., sin que esto represente un cambio abrupto a la arquitectura de la red.

El diseño de la red inalámbrica está sustentado en el análisis de estándares, tecnologías existentes y en los lineamientos del Instituto, de tal manera que su integración no implicó un cambio abrupto en la infraestructura de la red. Cumple así con los requerimientos de funcionalidad como parte integral de los sistemas del Instituto de Ingeniería.

El II, por su naturaleza, está en constante expansión, no sólo de infraestructura, sino también por el personal que se integra cada día y, aquí la red inalámbrica juega también un importante papel, ya que con el diseño implantado estamos hablando de que por cada punto de acceso podemos llegar a tener 20 usuarios conectados simultáneamente por cada 30 metros cuadrados con una aceptable velocidad de transferencia.

Ya hemos hablado de las ventajas que la red ofrece, sin embargo, es necesario también mencionar las desventajas y problemas que trae inherente esta tecnología. Aquí debemos mencionar que las principales desventajas apuntan, a la seguridad y, a la velocidad de transmisión; en este rubro la tecnología cableada está muy adelante, sin embargo, la velocidad que se ofrece con la red inalámbrica es completamente aceptable y permite utilizar todas las aplicaciones de transmisión de datos que los usuarios requieren.

Por otra parte, a lo largo de toda la investigación se ha hecho énfasis en las ventajas que ofrece el contar con esta red inalámbrica y, por lo tanto se habla de una factibilidad organizacional y técnica, sin embargo, podemos cuestionarnos ¿qué tan factible es este proyecto para fines económicos?

Uno de los factores principales para la toma de decisión comprende el determinar su costo. Se deben de establecer los beneficios de la red actual con el objeto de compararlos con la red inalámbrica propuesta.

RED CABLEADA Usuarios Simultáneos	Calidad de servicio	Factores de costo	
1	Excelente	Descripción	Costo*
		Cable Categoría 6	
		Jacks	
		Conectores	
		Faceplate	
		Remates en panel	
		Mano de obra	
		Total	$1,400.0

RED INALÁMBRICA Usuarios Simultáneos	Calidad de servicio	Factores de costo	
20	Muy Buena	Descripción	Costo**
		Access Point	$11,522.6
		Cableado de nodo de red	$1,400.0
		Total	$12,922.6

Los 20 usuarios simultáneos es una estimación hecha con base en la condiciones del Instituto, este número podría incrementarse sólo en auditorios o salones.

De acuerdo a la tabla anterior, podemos decir que la red inalámbrica satisface la tasa de rendimiento sobre la inversión hecha por parte del Instituto. Esta afirmación se complementa si tomamos en cuenta que la calidad de servicio ofrecida cubre las necesidades del Instituto y se cuenta con amplia disponibilidad de conexiones utilizando un sólo dispositivo.

Por lo anterior, podemos responder afirmativamente a la pregunta antes mencionada en función de los beneficios tangibles ofrecidos.

Ahora bien, respondiendo la pregunta planteada en los primeros párrafos, creemos que en el caso específico del Instituto, la tecnología inalámbrica jamás sustituirá por completo a los cables, básicamente por las ventajas que ofrecen y, además, porque es cierto que en cuanto a funcionalidad la red cableada actúa adecuadamente y, cuenta ya con una gran infraestructura siendo ésta producto de una gran inversión que no podemos dejar a un lado, además, hay que recordar que el diseño inalámbrico que se propone está inicialmente sustentado en la tecnología cableada, puesto que los mismos puntos de acceso pertenecen a ésta.

* Precios cotizados por la empresa Adder S.A. de C.V.
** Precios cotizados por la empresa Inster S.A. de C.V.

No habrá mejor indicador de la efectividad y funcionalidad de la red inalámbrica que su utilización real, sin embargo, esta investigación representa una base fundamentada ya que conllevó de un amplio estudio previo al diseño e implantación de la red inalámbrica, así mismo la realización de pruebas exhaustivas en todos los factores críticos cubriendo con ello la satisfacción de los objetivos planteados al inicio de ésta.

Anexo 1

PUERTOS

Cada máquina conectada a una red utilizando el protocolo TCP / IP, tiene asignado un grupo de 4 bloques de un máximo de 3 cifras que van del 0 al 255 que la identifica como única en la red a la que esta conectada, de forma que pueda recibir y enviar información de y a otras máquinas en concreto. A este grupo de cifras se le denomina dirección IP.
La petición, envío y recepción de información la realizan aplicaciones que están corriendo en las máquinas en red, con el fin de realizar diversas tareas. Para poder realizar varias de forma simultánea, la IP tiene asignados 65536 puntos de salida y entrada de datos, algunos de ellos asignados por un estándar, definido por IANA, Internet Assigned Numbers Authority, en el documento rfc1700. Este rango está dividido en tres categorías:

Categoría 1.- Puertos **0** a **1023**. Llamados también "Puertos bien conocidos". Han sido asignados por IANN para emplearse en aplicaciones debidamente identificadas, como el Protocolo para Transferencia de Archivos (FTP).

Categoría 2.- Puertos **1024** a **49151**. Pueden emplearlos las diversas organizaciones y desarrolladores de programas para aplicaciones específicas. Si alguna entidad registra un número o varios números de puerto para una aplicación, deberá notificar a sus usuarios para que abran los puertos correspondientes en el firewall y así permitir que se ejecute la aplicación. Adicionalmente, algunas empresas pueden configurar sus productos para usar un rango de puertos dentro de esta categoría, de nuevo notificando a los usuarios qué puertos abrir para que se establezca la comunicación a través del firewall.

Categoría 3.- Puertos **49152** a **65535**. Pueden asignarlos dinámicamente los puntos terminales, pero no se pueden reservar para una aplicación específica de forma permanente. De nuevo, las entidades que usan estos puertos en alguna aplicación deben notificar a los usuarios qué puertos deben quedar abiertos en el firewall

Definición técnica:

Un puerto es un número de 16 bits, empleado por un protocolo host a host para identificar a que protocolo del nivel superior o programa de aplicación se deben entregar los mensajes recibidos.

Tipos de puertos

Existen dos tipos de puertos, los puertos **TCP, Transmission Control Protocol,** y los puertos **UDP, User Datagram Protocol,** que son utilizados por el protocolo TCP, protocolo que ofrece una gran flexibilidad en conexiones host a host, así como verificación de errores, transmisión "full duplex" (transmisión de datos

simultánea en ambos sentidos), seguridad, entre otras características, evitando que las capas superiores o aplicaciones deban realizar estas tareas y liberando por tanto de carga al sistema.
Todas estas propiedades, dan seguridad y fiabilidad disminuyendo la velocidad en la transmisión de datos por lo que con vista a funciones con menos exigencias tanto en seguridad como en estabilidad, se creó el protocolo UDP que es un simple protocolo de transmisión de datos, sin verificaciones añadidas, verificaciones que deben ser realizadas por las aplicaciones, pero que sin embargo es bastante más rápido.

Utilización de los puertos por parte de las aplicaciones.

Los puertos son abiertos a petición de las aplicaciones o programas que van a utilizarlos. Un programa que precise comunicarse con una aplicación que está funcionando en otra máquina, utilizará un puerto determinado, que tiene reservado para su propio uso, denominado "Puerto de salida", por medio del cual realizará una petición a otro puerto situado en la máquina remota.

Por otra parte, los programas que precisen recibir información desde el exterior, reservarán sus propios puertos, manteniéndolos abiertos con este fin. A estos puertos se les denomina "Puertos en escucha".

El conocimiento de los puertos utilizados por las aplicaciones comunes es de utilidad para el usuario a la hora de afrontar la configuración de dispositivos de enrutamiento o firewalls, permitiendo de este modo explotar las características online de los distintos programas.

A continuación una lista de los puertos más usados y sus aplicaciones:

Puertos Conocidos

Puerto	Protocolo	Servicio
1	TCP	TCPMUX
7	TCP - UDP	ECHO protocol
9	TCP - UDP	DISCARD Protocol
13	TCP - UDP	DAYTIME protocol
17	TCP	QOTD protocol
19	TCP	CHARGEN protocol
19	UDP	CHARGEN protocol
20	TCP	FTP - data port
21	TCP	FTP - control port
22	TCP	SSH - used for secure logins, file transfers and port forwarding

23	TCP	Telnet protocol - unencrypted text communications
25	TCP	SMTP - used for sending E-mails
37	TCP - UDP	TIME protocol
53	TCP	DNS
53	UDP	DNS
67	UDP	BOOTP server; also used by DHCP
68	UDP	BOOTP client; also used by DHCP
69	UDP	TFTP
70	TCP	Gopher protocol
79	TCP	Finger protocol
80	TCP	HTTP - used for transferring web pages
88	TCP	Kerberos - authenticating agent
109	TCP	POP2
110	TCP	POP3
113	TCP	ident
119	TCP	NNTP - used for retrieving newsgroups messages
123	UDP	NTP - used for time synchronization
139	TCP	NetBIOS
143	TCP	IMAP4 - used for retrieving E-mails
161	UDP	SNMP
179	TCP	BGP
389	TCP	LDAP
443	TCP	HTTPS - HTTP over SSL
445	TCP	Microsoft-DS
445	UDP	Microsoft-DS SMB file sharing
465	TCP	SMTP over SSL
514	UDP	syslog protocol
540	TCP	UUCP
591	TCP	FileMaker 6.0 Web Sharing
636	TCP	LDAP over SSL
666	TCP	id Software's DOOM multiplayer game played over TCP
993	TCP	IMAP4 over SSL
995	TCP	POP3 over SSL

Tabla 1. Puertos Conocidos

Puertos Registrados

Puerto	Protocolo	Servicio
1080	TCP	SOCKS proxy
1337	TCP	menandmice.com DNS.
1352	TCP	IBM Lotus Notes/Domino RCP

1433	TCP	Microsoft SQL database system
1434	TCP	Microsoft SQL Monitor
1434	UDP	Microsoft SQL Monitor
1984	TCP	Big Brother
1494	TCP	Citrix MetaFrame ICA Client
1863	TCP	MSN Messenger
2427	UDP	Cisco MGCP
3128	TCP	HTTP used by web caches and the default port for the Squid cache
3306	TCP	MySQL Database system
3389	TCP	Microsoft Terminal Server
3396	TCP	Novell NDPS Printer Agent
3689	TCP	DAAP Digital Audio Access Protocol used by Apple's ITunes
3690	TCP	Subversion version control system
4899	TCP	RAdmin remote administration tool
5190	TCP	AOL and AOL Instant Messenger
5222	TCP	XMPP/Jabber
5269	TCP	XMPP/Jabber
5432	TCP	PostgreSQL database system
6000	TCP	X11
6346	TCP	Gnutella Filesharing
6347	UDP	Gnutella
6667	TCP	IRC
8000	TCP	iRDMI
8080	TCP	HTTP Alternate (http-alt)
8118	TCP	Privoxy web proxy

Tabla 2. Puertos Registrados

Puertos no Registrados

Puerto	Protocolo	Servicio
981	TCP	Software Remote HTTPS management for firewall devices running embedded Checkpoint Firewall-1 software
1337	TCP	WASTE Encrypted File Sharing Program
1521	TCP	Oracle database default listener
1761	TCP	Novell Zenworks Remote Control utility
2082	TCP	CPanel's default port
2086	TCP	Web Host Manager's default port
5000	TCP	Universal plug-and-play (UPnP)

5223	TCP	XMPP/Jabber
5517	TCP	Setiqueue Proxy server client for SETI@Home project
5800	TCP	VNC remote desktop protocol
6112	UDP	Blizzard's Battle.net gaming service
5900	TCP	VNC remote desktop protocol
6600	TCP	mpd
6881	TCP	BitTorrent
6969	TCP	BitTorrent tracker port
8000	TCP	Common port used for internet radio streams such as those using SHOUTcast
27010	UDP	Half-Life and its mods, such as Counter-Strike
27015	UDP	Half-Life and its mods, such as Counter-Strike
27960	UDP	id Software's Quake 3 and Quake 3 derived games
31337	TCP	Back Orifice - remote administration tool
50000	TCP	DB2 database

Tabla 3. Puertos No Registrados

Anexo 2

VIRTUAL ACCESS POINT

Definición.

Un "Virtual Access Point" es una entidad lógica que existe dentro de un Access Ponit físico. Cuando un Access Point soporta múltiples "Virtual APs", cada uno de éstos aparenta ser un Access Point físico independiente, aún cuando sólo un AP físico esté presente. Con esto, cada uno de los Virtual AP puede ser configurado de manera diferente y dar servicio simultáneamente.

El concepto del Virtual Access Point.

Un Virtual AP es una entidad lógica que para una estación es indistinguible del AP físico. En la siguiente figura se muestra una comparación entre una configuración hecha con dos AP físicos y la misma configuración hecha con un AP que soporta Virtual AP.

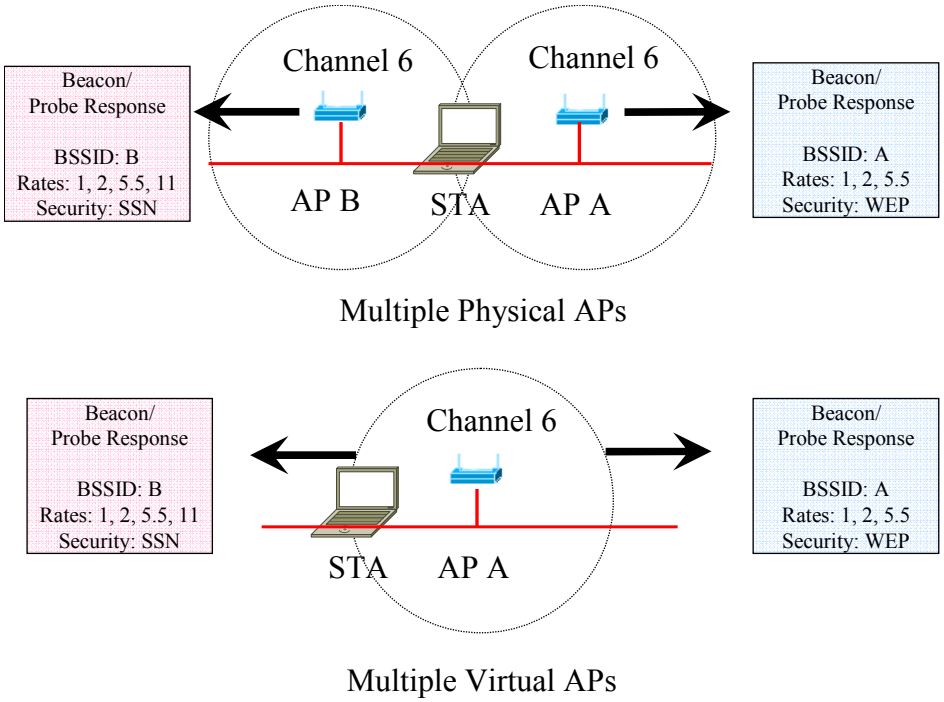


Fig. 1 Funcionamiento del Virtual Access Point

La clave para proporcionar el Virtual AP es implementar pilas del protocolo MAC independientes, esto es, que cada Virtual AP emule la operación de la capa MAC de un AP físico. Es importante notar que la emulación de frecuencias es prácticamente imposible, a no ser que se cuente con múltiples radios, por eso es que en la figura anterior se conserva el canal de transmisión.

Recordemos que para descubrir SSIDs, la estación puede hacerlo mediante el escaneo activo y/o pasivo. En el escaneo pasivo, la estación espera la transmisión de **beacons** y de tramas **Probe Responses**. En el escaneo activo la estación

envía tramas **Probe Request** para obtener la información más rápidamente. Dentro de estas tramas se encuentra el campo SSID. En el estándar IEEE 802.11 se indica que sólo es posible asociarse con un único AP y que sólo un SSID puede ser incluido dentro de estas tramas. Por lo que las estaciones solamente pueden estar asociadas con un SSID a la vez. Para saber con que AP esta asociada una estación, existe otro campo dentro de las tramas de administración, el BSSID (Basic Service Set Identification), el cual es la dirección MAC del AP con el cual está asociada la estación.

Al emular el comportamiento de la capa MAC, los Virtual APs pueden operar con un BSSID por cada SSID y parámetros de seguridad diferentes e independientes. A este método se le conoce como *"Single SSIDs/Beacon, Multiple Beacons, Multiple BSSIDs"*, con el cual, el AP transmite beacons individuales en el intervalo de tiempo estándar y utiliza un único BSSID por cada Virtual AP. Si hay N BSSIDs y el intervalo de tiempo es de ΔT, entonces el intervalo entre beacons será de $\Delta T/N$, por lo que no se incrementa el tiempo requerido para completar un escaneo pasivo o activo.

Ventajas:

- Se puede tener una o más redes inalámbricas independientes por cada AP físico.
- Interoperabilidad completa con el estándar 802.11.
- Políticas de seguridad independientes por cada Virtual AP.
- El tráfico de cada Virtual AP puede ser dirigido hacia una VLAN diferente.

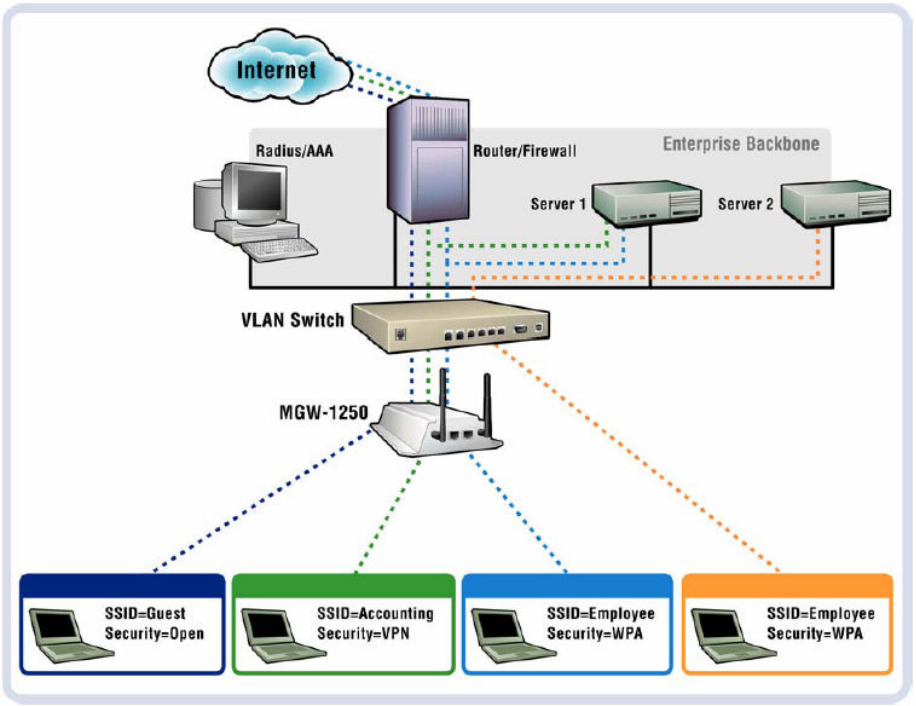


Fig. 2 Esquema de operación del Virtual Access Point

Anexo 3

ALGUNAS TRAMAS 802.11

Hay un concepto importante que debe ser entendido antes de detallar el formato de las tramas: la diferencia entre MSDU (*MAC Service Data Unit*) y MPDU (*MAC Protocol Data Unit*). Ambos términos se refieren a un sólo paquete de datos, pero MSDU representa a los datos antes de la fragmentación, mientras las MPDUs son múltiples unidades de datos tras la fragmentación.

Formato General:

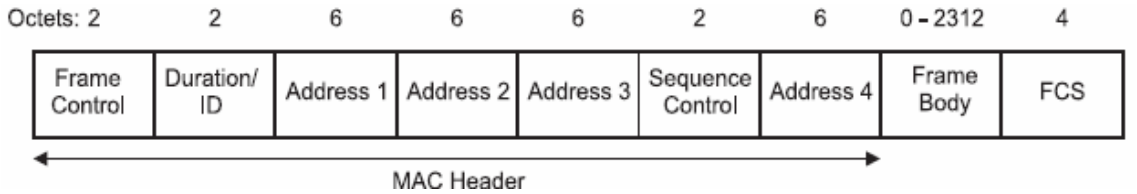


Fig. 1 Formato general de la trama 802.11

Campo Frame Control:

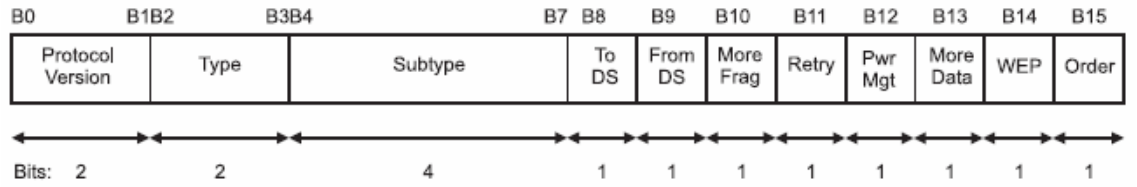


Fig. 2 Campo Frame Control

Recordemos que existen tres tipos de tramas: Datos, Control y Administración. Cada uno de éstas tiene diferentes subtipos, de los cuales se describirán: Beacon, Autenticación, Prueba de petición (Probe request), Prueba de respuesta (Probe response), RTS, CTS y ACK.

Es importante notar que dentro del campo Frame Control originalmente está el subcampo WEP. Con el establecimiento del estándar 802.11i el nombre de este subcampo es cambiado por: *Campo protegido (Protected Frame)* como se ilustra a continuación.

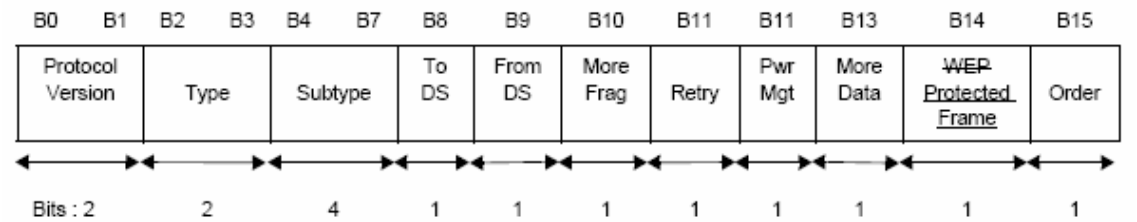


Fig. 3 Campo Frame Control 802.11i

Es importante mencionar también, que únicamente las tramas de Datos y Administración son procesadas por el algoritmo correspondiente, esto es, sólo dichas tramas son encriptadas.

Tramas de Datos

Formato general:

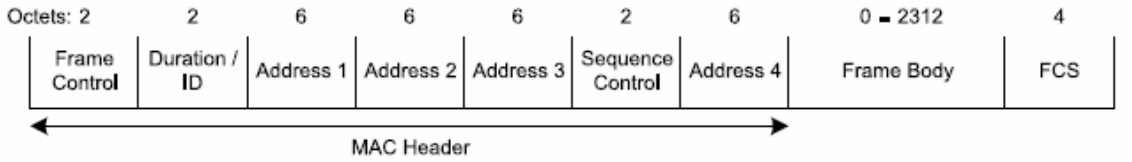


Fig. 3 Formato general de la trama de datos

Tramas de Control

Dentro de la trama de Control el campo Frame Control es puesto de la siguiente manera:

Fig. 4 Campo Frame Control en la trama de control

Trama Request to Send (RTS)

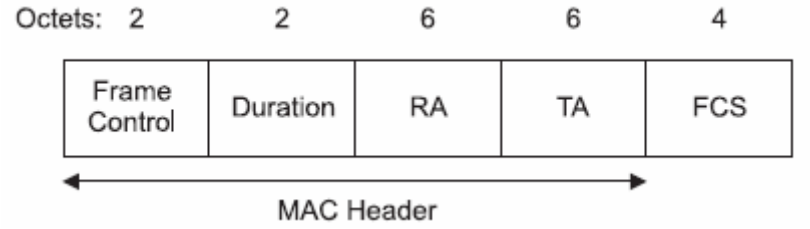


Fig. 5 Trama RTS

RA es la dirección de la estación que va a recibir las tramas de datos o administración. TA es la dirección de la estación que transmite la trama RTS. En el campo Duration, se especifica el valor en microsegundos requerido para transmitir las tramas pendientes de datos o administración, más las tramas CTS, más una trama ACK, más tres intervalos SIFS.

Trama Clear to Send (CTS)

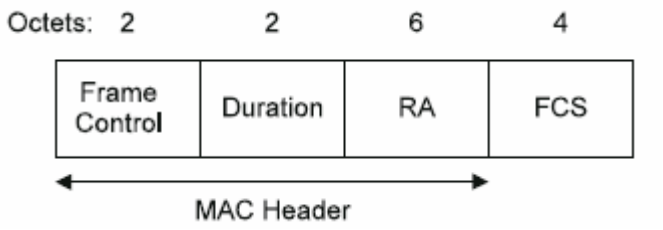


Fig. 6 Trama CTS

El campo RA es copiado del campo TA de la trama inmediata anterior RTS, de la cual, la trama CTS es respuesta. En el campo Duration se encuentra el valor obtenido del campo Duration del la trama inmediata anterior RTS menos el tiempo, en microsegundos, requerido para transmitir la trama CTS y su intervalo SIFS. Si este valor incluye fracciones de microsegundo se redondea al valor inmediato superior.

Trama Acknowledgment (ACK)

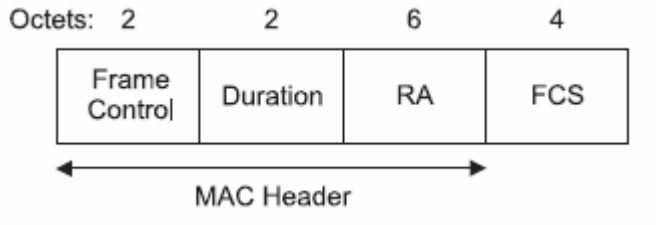


Fig. 7 Trama ACK

RA es copiada del campo Address 2 de la trama de datos, administración o PS-Poll inmediata anterior. El valor del campo Duration depende del subcampo More Fragment bit que se encuentra dentro del campo Frame Control de la trama inmediata anterior de datos o administración. Si este bit es 0 entonces el valor de del campo Duration es puesto en 0. Si es 1, el valor se obtiene del campo Duration de esas tramas menos el tiempo en microsegundos requerido para transmitir el ACK y su intervalo SIFS.

Tramas de Administración

Formato General:

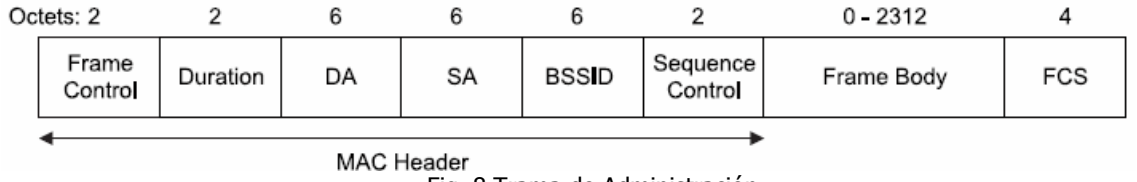


Fig. 8 Trama de Administración

Dentro de las tramas de administración existen componentes de longitud fija obligatoria que se encuentran dentro del campo Frame Body y son definidos como Campos fijos. Los componentes de longitud variable así como los opcionales son definidos como Elementos de información. Por lo tanto, lo que varía dentro de las tramas de administración es la información contenida en el Frame Body.

Beacon

La información contenida dentro del Frame Body es la que se muestra a continuación:

Orden	Información	Notas
1	Timestamp	
2	Intervalo Beacon	
3	Información de capacidad	
4	SSID	
5	Tasas de transferencia aceptadas	
6	FH Parameter Set	Está presente dentro de las tramas Beacon generadas por estaciones que usan frecuency-hopping PHYs
7	DS Parameter Set	Está presente dentro de las tramas Beacon generadas por estaciones que usan direct sequence PHYs.
8	CF Parameter Set	Está presente sólo dentro de tramas Beacon generadas por AP's soportando un PCF.
9	IBSS Parameter Set	Está presente sólo dentro de tramas Beacon generadas por estaciones en un IBSS.
10	TIM	Está presente únicamente dentro de tramas Beacon generadas por AP's.

Tabla 1. Información de la trama Beacon

Autenticación

La información contenida dentro del Frame body es la que se muestra a continuación:

Orden	Información	Notas
1	Número de algoritmo de autenticación	
2	Número de secuencia de transacción de autenticación	
3	Código de estatus	Está reservado y puesto en 0 en ciertas tramas.
4	Texto de desafío	Está presente solamente en ciertas tramas.

Tabla 2. Información de la trama de autenticación

Prueba de petición (Probe Request)

El campo Frame body contiene los siguientes elementos:

Orden	Información
1	SSID
2	Tasa de transferencia soportada

Tabla 3. Información de la trama prueba de petición

Prueba de respuesta (Probe Response)

El campo Frame body contiene los siguientes elementos:

Orden	Información	Notas
1	Timestamp	
2	Intervalo Beacon	
3	Información de capacidad	
4	SSID	
5	Tasas de transferencia soportadas	
6	FH Parameter Set	Está presente dentro de las tramas Beacon generadas por estaciones que usan frecuency-hopping PHYs
7	DS Parameter Set	Está presente dentro de las tramas Beacon generadas por estaciones que usan direct sequence PHYs.
8	CF Parameter Set	Está presente sólo dentro de tramas Beacon generadas por AP's soportando un PCF.
9	IBSS Parameter Set	Está presente sólo dentro de tramas Beacon generadas por estaciones en un IBSS.

Tabla 4. Información de la trama de prueba de respuesta

GLOSARIO

ANCHO DE BANDA DIGITAL.- cantidad de datos que se pueden transmitir en una unidad de tiempo. Por ejemplo, una línea ADSL de 256 kbps puede, teóricamente, enviar 256000 bits (no bytes) por segundo.

ATM.- **Asynchronous Transfer Mode** (Modo de Transferencia Asíncrona) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

BACKBONE.- Mecanismo de conectividad primario en un sistema distribuido. Todos los sistemas que tengan conexión al backbone (columna vertebral) pueden interconectarse entre sí, aunque también puedan hacerlo directamente o mediante redes alternativas.

BAUDIO.- es la unidad informática que se utiliza para cuantificar el número de cambios de estado, o eventos de señalización, que se producen cada segundo durante la transferencia de datos.

BIT FLIPPING.- Bits modificados en las tramas cifradas, el CRC32 es recalculado.

BROADCAST.- es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CODIFICADOR.- Es un circuito combinacional con n entradas y N salidas (con N menor o igual a 2^n, cuya misión es presentar en la salida el código binario correspondiente a la entrada activada.

CRC.- **Cyclic redundancy Code** (Código de Redundancia Cíclica). Se trata de un método matemático a través del cual, permite detectar errores en la información.

DECODIFICADOR.- es un circuito combinacional, que convierte un código de entrada binario de N bits en M líneas de salida (N puede ser cualquier entero y M es un entero menor o igual a 2^N), tales que cada línea de salida será activada para una sola de las combinaciones posibles de entrada.

DESCRIPTAR.- Es la acción inversa a cifrar.

Cifrar.- Es la codificación de los datos por razones de seguridad.

FTP.- **File Transfer Protocol** (Protocolo de Transferencia de Ficheros). Es uno de los diversos protocolos de la red Internet, es el ideal para transferir grandes bloques de datos por la red.

HACKEAR.- Se suele llamar hackeo y hackear a las obras propias de un hacker.

HALF DUPLEX.- hace referencia a la transmisión de información en cualquiera de los dos sentidos, pero sólo en una dirección a la vez.

HASH.- En informática, **Hashing** es un método para resumir o identificar un dato a través de la probabilidad, utilizando una *función hash* o *algoritmo hash*. Un hash es el resultado de dicha función o algoritmo.

HIPERLAN.- **High Performance Radio LAN**, es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz.

HTTP.- **HyperText Transfer Protocol** (protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la Web (WWW).

INTERMODULACIÓN.- Si señales de distinta frecuencia aparecen en el mismo circuito, en ciertas condiciones pueden crear nuevas señales mediante la suma y la diferencia de dichas frecuencias. Este inconveniente se conoce con el nombre de intermodulación y es una de las causas de distorsión en los circuitos de audio.

ISP.- **Internet Service Provider** (Proveedor de servicios de Internet) es una empresa dedicada a conectar a Internet la línea telefónica de los usuarios o las distintas redes que tengan, y dar el mantenimiento necesario para que el acceso funcione correctamente. También ofrecen servicios relacionados, como alojamiento web o registro de dominios entre otros.

ITU.- Unión Internacional de Telecomunicaciones.

ITU-R.- **ITU Radiocommunication Sector**, subcomité de la Unión Internacional de Telecomunicaciones (ITU), encargada de gestionar el espectro de frecuencias radioeléctricas y de las órbitas de los satélites.

LAN.- Es la abreviatura de **Local Area Network** (Red de Área Local). Una red de área local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros.

MAC.- **Medium Access Control** (Control de acceso al medio MAC).

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.

MULTIPLEXAJE.- Es la combinación de múltiples canales de información en un medio común de transmisión de alta velocidad.

PAIRWISE MASTER KEY (PMK).- Clave principal de la jerarquía de pares de claves. Si se usa una PSK (Pre-Shared Key), PMK = PSK. La PSK es generada desde una passphrase (de 8 a 63 caracteres) o una cadena de 256-bit y proporciona una solución para redes domésticas o pequeñas empresas que no tienen servidor de autenticación. Si se usa un servidor de autenticación, la PMK es derivada de la MK de autenticación 802.1X.

PDU.- Protocol Data Units (Protocolo de unidad de datos). Se utiliza para el intercambio entre unidades pares, dentro una capa del modelo OSI.

PPM.- **Pulse Position Modulation** (Modulación por posición de pulsos).

RAS.- **Remote Access Server** (Servidor de Acceso Remoto), permite conectarse a la red por medio de una conexión telefónica. Una vez conectado, puede hacer lo mismo que si estuviera trabajando en un equipo conectado físicamente a la red.

RC4.- Dentro de la criptografía **RC4** es el sistema de cifrado de flujo *Stream cipher* más utilizado y se usa en algunos de los protocolos. RC4 genera un flujo pseudoaleatorio de bits (un *keystream*) que, para el cifrado, se combina con el texto plano usando la función XOR.

SEÑAL MODULADORA.- es una señal de banda base que contiene la información a transmitir (voz, música, video, datos, etc.).

SEÑAL PORTADORA.- es una forma de onda, generalmente senoidal, que es modulada por una señal que se quiere transmitir.

SMTP.- **Simple Mail Transfer Protocol** (Protocolo simple de transferencia de correo electrónico). Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, Celulares, etc).

SNIFFER.- es un programa de captura de las tramas de red .Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.

SPOOFING.- en términos de seguridad informática hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Existen diferentes tipos de spoofing dependiendo de la tecnología a la que nos refiramos, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

TELNET.- es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella.

WEB.- es un sistema de navegación para extraer elementos de información en la Internet.

WLAN.- Abreviatura de **Wireless Local Area Network.**

WN.- Wireless Network (Red inalámbrica).

WPA.- **Wi-Fi Protected Access** (Acceso Protegido Wi-Fi).

REFERENCIAS

[1] IEEE 802.11. 1999. *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"*. ANSI/IEEE Standard 802.11, 1999 Edition.

[2] IEEE 802.11a. 1999. *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5 GHz Band"*. ANSI/IEEE Standard 802.11a, 1999 Edition.

[3] IEEE 802.11b. 1999. *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 2.4 GHz Band"*. ANSI/IEEE Standard 802.11b, 1999 Edition.

[4] IEEE 802.11g. 2003. *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band"*. ANSI/IEEE Standard 802.11g, 2003 Edition.

[5] IEEE 802.11i. 2004. *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements"*. ANSI/IEEE Standard 802.11i, 2004 Edition.

[6] Rappaport, Theodore S. *"Wireless Communications: Principles and Practice"*. 2da. Edción, E.U.: Prentice Hall, 2002.

[7] Flickenger, Rob. *"Wireless Networking in the Developing World"*. Limehouse Book Sprint Team, 2006.

[8] Vigueras Villaseñor, Marco. "*Apuntes de redes"*. UNAM 2003.

[9] Castellanos Goméz, Javier. "*Apuntes de redes inalámbricas para maestría"*. UNAM 2004.

[10] Meza Múgica, Myriam; Medina Castro, Paúl. *"Introducción de mecanismos de calidad de servicio en el protocolo de acceso al medio de redes locales inalámbricas del tipo IEEE 802.11"*. Centro de investigación científica y de educación superior de Ensenada, 2004.

[11] Benítez Guzmán, Andrés Roberto; Martínez Lorenzana, Araceli; Ortega Segura, David. *"Análisis y diseño de la red de cómputo de la Torre de Ingeniería"*, UNAM 2001.

[12] Fuster Sabater, Amparo; Hernández Encinas, Luis. *"Técnicas criptográficas de protección de datos"*. 2da. Edición, Alfaomega, México 2001.

[13] 3com

www.3com.com

[14] Agilent

www.home.agilent.com

[15] Atheros

www.atheros.com/

[16] Bluetooth

spanish.bluetooth.com/Bluetooth/

[17] Cisco

www.cisco.com/

[18] IEEE

www.ieee.org

[19] Microsoft

www.microsoft.com/spain/technet

[20] Wi-fi

www.wi-fi.org/

[21] Wikipedia

www.wikipedia.org/

[22] WiMAX Forum

www.wimaxforum.org/