CAPITULO I

1. ESTUDIO DE LA CONECTIVIDAD Y SEGURIDAD INALÁMBRICA

1.1. REDES INALÁMBRICAS

1.1.1. Conceptos

Partamos de la definición de inalámbrico, este término se refiere al uso |de la tecnología sin cables la cual permite la conexión de varios computadores entre sí. “Las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar. Con las WLANs la red, por si misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores”.[1]

[1] Carballar, José A. El libro de las Comunicaciones del PC, HP, España, 2006. Pág. 10-39

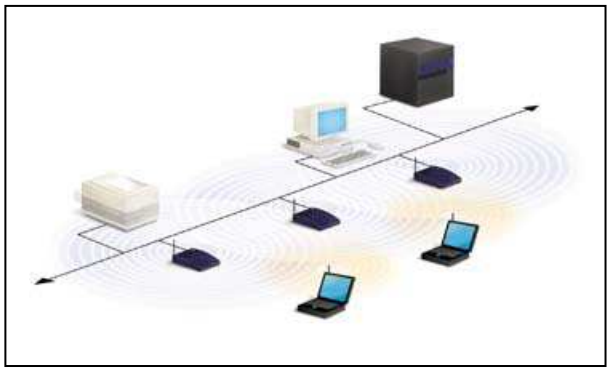

Gráfico 1.1: REDES INALAMBRICAS
Fuente: EL INVESTIGADOR

1.1.2. Orígenes

"Las redes de área local inalámbrica funcionan desde hace varios años en entornos industriales y de investigación.

Se implementaron por primera vez en 1979 como resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

En marzo de 1985 la Comisión Federal de Comunicaciones, FCC, organismo encargado de la regulación de las telecomunicaciones en Estados Unidos, asignó a los sistemas WLAN las bandas frecuenciales 902-928 MHz., 2.400-2.4835 GHz. y 5.725-5.850 GHz también conocidas como ISM (Industrial, Científica y Médica) y que pueden utilizarse bajo licencia administrativa.

Esta asignación de una localización frecuencial fija propició una mayor actividad industrial. En este punto las redes de área local inalámbrica dejaron de ser meramente experimentales para empezar a introducirse en el mercado.

Entre los anos 1985 y 1990 se trabajó en el desarrollo de productos WLAN y finalmente, en mayo de 1991, se publicaron algunos trabajos que hablaban sobre redes inalámbricas que superaban la velocidad de transferencia de 1 Mbps, velocidad mínima a partir de la cual el comité IEEE considera que una red es de área local.

Hasta ese momento las WLAN habían tenido una aceptación marginal en el mercado por dos razones fundamentales: falta de un estándar y precios elevados de la solución inalámbrica". [2]

En estos últimos años se ha producido un crecimiento en el mercado de hasta un 100 % anual. Este hecho es atribuible a dos razones principales:

- El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles que han producido que los usuarios puedan estar en continuo movimiento manteniendo comunicación constante con otros terminales y elementos de la red. En este sentido, las comunicaciones inalámbricas ofrecen una prestación no disponible en las redes cableadas: movilidad y acceso simultáneo a los recursos de la red.

- La conclusión de la definición de la norma IEEE 802.11 para redes de área local inalámbricas el pasado junio de 1997 que ha establecido un punto de referencia y ha mejorado muchos de los aspectos de estas redes.

A pesar del atractivo y funcionalidad de las WLAN, la falta de estándares que brinden confianza a los potenciales usuarios de esta tecnología, fue otra de las razones de la lenta acogida que tuvieron en el pasado. En la actualidad se han definido normas internacionales que regulan la operación y funcionamiento de los elementos y protocolos de WLAN.

[2] Tomado de: www.monografias.com/reporte/redesinal/redinal.htm

Entre las normas más importantes para este tipo de redes tenemos la realizada por e! subcomité 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos de los Estados Unidos (IEEE).

1.1.3. Ámbito de aplicación

En nuestra era han surgido los adictos a la información, gente que necesita estar todo el tiempo en línea. Para estos usuarios móviles, cable de par trenzado, el cable coaxial y la fibra óptica nos son útiles.

Ellos necesitan obtener datos para sus computadores laptops, notebook, de bolsillo, de mano, celulares, de pulsera o reloj, sin estar limitados a la infraestructura de comunicaciones terrestres. Para estos usuarios la comunicación inalámbrica en general veremos que tiene otras aplicaciones importantes además de proporcionar conectividad a los usuarios que desean navegar por la WEB.

1.1.3.1. Espectro Electromagnético

"Se denomina **espectro electromagnético** al conjunto de ondas electromagnéticas o, más concretamente, a la radiación electromagnética que emite (espectro de emisión) o absorbe (espectro de absorción) una sustancia. Dicha radiación sirve para identificar la sustancia de manera análoga a una huella dactilar. Van desde las de menor longitud de onda, pasando por la luz ultravioleta, la luz visible y los rayos infrarrojos, hasta las ondas electromagnéticas de mayor longitud de onda, como son las ondas de radio."[3]

[3] Tomado de: www.wikipedia.org/ondas.html, Espectro Electromagnético, Pablo Sanchez, Mayo 2006.

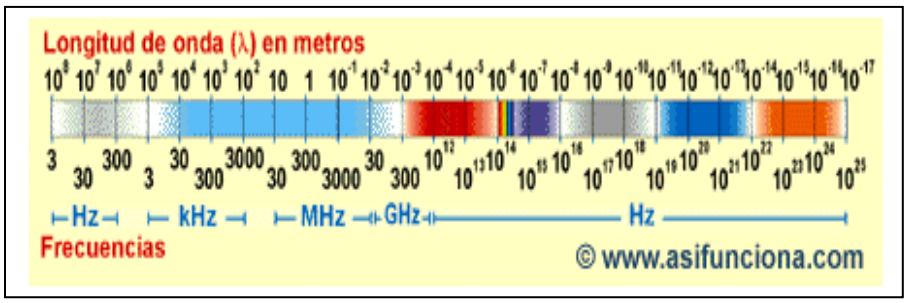

Gráfico 1.2: ESPECTRO ELECTROMAGNÉTICO.
Fuente: WIKIPEDIA, LA ENCICLOPEDIA LIBRE.

1.1.3.2. Ondas Electromagnéticas

"Son ondas producidas por la oscilación o la aceleración de una carga eléctrica. Las ondas electromagnéticas tienen componentes eléctricos y magnéticos. La radiación electromagnética se puede ordenar en un espectro que se extiende desde ondas de frecuencias muy elevadas (longitudes de onda pequeñas) hasta frecuencias muy bajas (longitudes de onda altas)"[4].

1.1.3.3. Ondas de radio.

"Las ondas de Radio son un tipo de ondas electromagnéticas, lo cual confiere tres ventajas importantes: No es necesario un medio físico para su propagación, las ondas electromagnéticas pueden propagarse incluso por el vacío. La velocidad es la misma que la de la luz, es decir 300.000 Km/seg. Objetos que a nuestra vista resultan opacos son transparentes a las ondas electromagnéticas"[5].

[4] Tomado de: www.wikipedia.org/ondaselectro.html, Ondas Electromagnéticas, Pablo Sanchez, Mayo 2006.
[5] Tomado de: Redes de Computadoras, Cuarta Edición, TANENBAUM Andrew, Editorial Prentice Hall, Año 2005, Pág 65

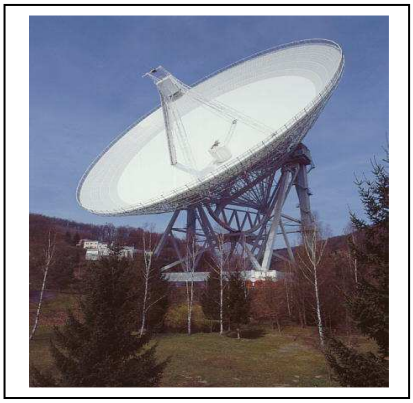

Gráfico 1.3: ONDAS DE RADIO
Fuente: REDES DE COMPUTADORAS. ANDREW TANENBAUM

1.3.3.1.2 Microondas Terrestres

Suelen utilizarse antenas parabólicas. Para conexiones a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas. Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.

Gráfico 1.4: MICROONDAS TERRESTRES
Fuente: REDES DE COMPUTADORAS. ANDREW TANENBAUM

1.1.3.4. Ondas Infrarrojas.

Llamadas también térmicas, llegan hasta la luz visible (el rojo del espectro), se producen por la vibración de los electrones de las capas superiores de ciertos elementos, estas ondas son absorbidas fácilmente

por la mayoría de los materiales. La energía infrarroja que absorbe una sustancia aparece como calor, ya que la energía agita los átomos del cuerpo, e incrementa su movimiento de vibración o translación.

1.1.3.5. Ondas Visibles.

Son la parte del espectro electro-magnético que puede percibir el ojo humano. La luz se produce por la disposición que guardan los electrones en los átomos y moléculas. Las diferentes longitudes de onda se clasifican en colores que varían desde el violeta el de menor longitud de onda hasta el rojo el de mayor longitud de onda (de 4 a $7x10^{-7}$).

1.1.3.6. Ondas Ultravioletas.

Los átomos y moléculas sometidos a descargas eléctricas producen este tipo de radiación. No debemos de olvidar que la radiación ultravioleta es la componente principal de la radiación solar. La energía de los fotones de la radiación ultravioleta es del orden de la energía de activación de muchas reacciones químicas.

1.1.3.7. Rayos X.

Si se aceleran electrones y luego, se hacen chocar con una placa metálica, la radiación de frenado produce rayos X. Los rayos X se han utilizado en medicina desde el mismo momento en que los descubrió Röntgen debido a que los huesos absorben mucho más radiación que los tejidos blandos.

1.1.4. Wireless LAN entre oficinas

La tecnología WLAN puede remplazar a las redes cableadas tradicionales o ampliar su alcance y sus capacidades. De igual modo que sus homologas con cables, el equipo de las WLAN interiores se compone de

una tarjeta PC y adaptadores de clientes PCI e ISA, así como de Puntos de Acceso, que realizan funciones similares a las que realizan los hubs en las redes tradicionales.

1.2. PROTOCOLOS DE TRANSMISIÓN

Los diversos mecanismos de acceso que se han propuesto e implantado para WLAN se agrupan en dos categorías: protocolos con arbitraje (FDMA, TOMA) y protocolos por contención (CDMA/CD, CDMA/CA).

Tipo de configuración WLAN sencilla, entre varias computadoras sin necesidad de usar un Access Point también se han diseñado protocolos que son una combinación de estas dos categorías.

Aunque ya no es habitual su utilización dentro de los sistemas WLAN, el mecanismo de mulitplexación en frecuencia, FDMA, divide todo el ancho de banda asignado en distintos canales individuales. Este es un mecanismo simple que permite el acceso inmediato al canal, pero poco eficiente para su utilización en sistemas que presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa algo más factible es asignar todo el ancho de banda disponible a cada nodo durante un breve intervalo de tiempo de manera cíclica, este sistema llamado multiplexación en el tiempo (TOMA), requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias.

Este último esquema ha sido utilizado con cierto éxito, sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

Por el contrario, el protocolo de acceso múltiple por división de código (COMA), es el mecanismo de acceso por excelencia para que puedan coexistir diferentes redes.

Varias de las primeras redes utilizaban el algoritmo de acceso al medio, CSMA/CD. El cual se caracteriza por comprobar previamente que el medio de comunicación esté libre, antes de iniciar la transmisión. Si se tiene esta condición, entonces se transmite la información y si no, se espera a que se libere el medio.

Como existía la posibilidad de que dos estaciones transmitieran información simultáneamente, este mecanismo exigía que a pesar de iniciar la transmisión se debiera continuar con la vigilancia del canal para detectar posibles colisiones. Cuando esto ocurría, la transmisión era suspendida y las estaciones involucradas en el conflicto debían esperar un tiempo aleatorio antes de repetir nuevamente el algoritmo.

El protocolo 802.11, utiliza un tipo de protocolo conocido como CSMA/CA (Carrier-Sense, Múltiple Access, Colusión Avoidance). Este protocolo introduce una variante en el algoritmo anterior que evita las colisiones en la transmisión, en lugar de descubrir una colisión, fundamentado en el hecho de que la mayor probabilidad de que se produzca una colisión en CSMA/CD se da al terminar una transmisión.

Es decir, al haber más de una estación esperando que una transmisión en curso termine para que ellas puedan comenzar a transmitir, si no se adoptan las medidas oportunas estas estaciones comenzarán, todas a la vez, a enviar información provocando una colisión en el medio.

En el sistema CSMA/CA, cuando una estación identifica el fin de una transmisión, espera un tiempo aleatorio antes de transmitir, disminuyendo así la probabilidad de colisión.

A pesar del buen comportamiento general de este sistema, presenta una deficiencia debida al problema conocido como Terminal Oculto. Este problema se presenta cuando un dispositivo inalámbrico transmite con la potencia justa para que sea escuchado por un nodo receptor, pero no con la suficiente como para que otra estación, que se encuentra a la espera, sepa que hay otra unidad que está transmitiendo. Para resolver este conflicto, se ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo.

Este proceso hace que cuando una estación está lista para transmitir, primero envía una solicitud al punto de acceso (RTS - Request to Send)) quien, si no encuentra problemas, responde con una autorización (CTS -Clear to Send) que permite al solicitante enviar su datos. Cuando el punto de acceso ha recibido correctamente la información, envía una trama de reconocimiento (ACK - acknowledgment packet) notificando al transmisor el éxito de la transmisión.

Independientemente de los protocolos de acceso al medio y para dar soporte a las medidas de seguridad tan necesarias en este tipo de redes, ios sistemas inalámbricos, como complemento adicional y característica optativa para evitar las escuchas indiscretas, disponen de una herramienta de codificación de la información. La seguridad de los datos se realiza mediante una compleja técnica de codificación conocida como WEP (Wired Equivalent Privacy Algorithm).

El sistema WEP se basa en proteger los datos transmitidos en el medio RF, usando una clave generada por un número pseudo aleatorio y un algoritmo de encriptación. Cuando se habilita este sistema, sólo se protege la información del paquete de datos y no protege el encabezamiento de la capa física para que las demás estaciones puedan escuchar el control de datos necesario para la adecuada gestión de la red.[6]

[6] Carballar, José A. El libro de las Comunicaciones del PC, HP, España, 2006. Pág. 120-139

1.3. ORÍGENES DE LAS REDES DE ÁREA LOCAL INALÁMBRICAS

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread-spectrum"(frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en "spread-spectrum". IMS es una banda para uso comercial sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda. La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezara a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativos que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.[7]

[7] www.aironet.com/wireless.php, Origen de la tecnología inalámbrica, Juan Paúl Salvatierra, Octubre 2003.

Gráfico 1.5: REDES WLAN
Fuente: WWW.AIRONET.COM

1.4. TIPOS DE REDES INALÁMBRICAS

1.4.1. Redes de área extensa (WAN)

La revolución más grande de la comunicación si cables se inició con los teléfonos móviles, los cuales han sido el producto electrónico con mayor éxito de todos lo tiempos. Inicialmente solo ofrecían comunicación por voz, ahora con baterías de mayor duración interfaces inteligentes, reconocimiento de voz y mayor velocidad, su uso futuro estará relacionado más con sus nuevos servicios inalámbricos.

1.4.2. Métodos de Acceso celular

Los usuarios que ocupan un área geográfica deben disputarse un número limitado de canales y existen varios métodos de dividir el espectro para proporcionar acceso de forma organizada: El FDMA (Frequency División Múltiple Access), El TDMA (Time Division Multiple Access), El GSM (Global System for Mobile Communications), El CDAM (Code Division Multiple Access). Existen dos tipos principales de señales la analógica y la digital.

1.4.3. Redes de área local (LAN)

Una red de área local es un grupo de computadores y otros equipos relacionados que comparten una línea de comunicación y un servidor común dentro de un área geográfica determinada como un edificio de oficinas. Es normal que el servidor contenga las aplicaciones y controladores que cualquiera que se conecte a la LAN pueda utilizar.

1.4.4. Redes de área local sin cables (WLANs)

Ofrece acceso sin cables a todos los recursos y servicios de una red corporativa (LAN) en un edificio o todo un campus. Proporciona más libertad en el ambiente de trabajo. A través de una red sin cables los trabajadores pueden acceder a la información desde cualquier lugar de la compañía. Lo cual les ofrece numerosas ventajas:

- Acceso fácil y en tiempo real para realizar consultas desde cualquier lugar.
- Acceso mejorado a la base de datos.
- Configuración de red simplificada con mínima implicación MIS.
- Acceso independiente de la localización para administradores de redes.

1.4.5. Redes de área personal (PAN)

Existe dentro de un área relativamente pequeña, que conecta dispositivos electrónicos con ordenadores, impresoras, escáner, aparatos de fax, PDAs y ordenadores notebook, sin la necesidad de cables ni conectores para que sea efectivo el flujo de información. El estándar de comunicaciones sin cables WPAN se centra en temas como el bajo consumo (para alargar la vida de los dispositivos portátiles), tamaño pequeño (para que sean más fáciles de llevar) y costos bajos (para que los productos puedan llegar a ser de uso masivo).

REDES PÚBLICAS DE RADIO

Las redes públicas tienen dos protagonistas principales: "ARDIS" (una asociación de Motorola e IBM) y "Rarn Mobüe Data" (desarrollado por Ericcson AB, denominado MOBITEX). Este último es el más utilizado en Europa.

Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia.

La compañía proporciona la infraestructura de la red, se incluya controladores de áreas y Estaciones Base, sistemas de cómputo tolerantes a fallas. Estas redes se encuentran de acuerdo al modelo de referencia OSI.

ARDIS especifica las tres primeras capas de la red y proporciona flexibilidad en las capas de aplicación, permitiendo al cliente desarrollar aplicaciones de software, por ejemplo una compañía llamada RF Data, desarrolló una rutina de compresión de datos para utilizarla en estas redes públicas).

Los fabricantes de equipos de cómputo venden periféricos para estas redes (IBM desarrolló su "PCRadio" para utilizarla con ARDIS y otras redes, públicas y privadas).

La PCRadio es un dispositivo manual con un microprocesador 80C186 que corre DOS, un radio/fax/módem incluido y una ranura para una tarjeta de memoria y 640 Kb de RAM.

Estas redes operan en un rango de 800 a 900 Mhz. ARDIS ofrece una velocidad de transmisión de 4.8 Kbps. Motorola Introdujo una versión de red pública en Estados Unidos que opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta).

1.4.6 VENTAJAS DE LAS REDES INALÁMBRICAS

La informática inalámbrica no sólo ofrece la libertad de permanecer conectado a medida que se moviliza por una oficina o el hogar. Sino que también brinda la libertad de conectar un equipo portátil móvil a la Internet desde cualquier habitación en casa o desde cualquier lugar donde lo lleve.

El deshacerse de los cables puede ser complicado. Implica el tener que enfrentarse a distintos estándares inalámbricos y todo el hardware y software resultante.

No obstante, la industria inalámbrica estableció el estándar 802.11 b (o WLAN) como el predominante en 1999, lo cual ha reducido los precios a medida que la demanda ha aumentado. En un futuro no lejano, el equipo para redes WiFi diseñado para las empresas y los hogares tendrán precios que equivalen a los de las redes cableadas, siendo fáciles de comprar y configurar.

Entre otras ventajas importantes de las redes inalámbricas tenemos:

- Implementación de redes de área loca! inalámbricas en edificios históricos, de difícil acceso y en general en entornos en donde la solución cableada es inviable.

- Posibilidad de reconfiguración de la topología de la red sin añadir costos adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.

- Redes locales para situaciones de emergencia o congestión de la red cableada.

- Estas redes permiten el acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes, etc.

- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.

- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.

- Interconexión de redes que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red local inalámbrica para interconectar dos o más redes de área local cableada situadas en dos edificios distintos

1.4.7 INTRODUCCIÓN A LA SEGURIDAD

1.4.7.1 Seguridad en Wlan

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología WLAN es la seguridad. Un muy elevado porcentaje de redes son instaladas por administradores de sistemas y redes por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares WLAN como el WEP y el WPA que se encargan de codificar la información transmitida para proteger su

confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios. Actualmente existe el protocolo de seguridad llamado *WPA2* (estándar 802.11i), que es una mejora relativa a WPA, es el mejor protocolo de seguridad para **WLAN** en este momento.

1.4.7.2. Dispositivos para WLAN

"Existen varios dispositivos que permiten interconectar elementos WLAN, de forma que puedan interactuar entre si. Entre ellos destacan routers, puntos de acceso, para la emisión de la señal WLAN y para la recepción se utilizan tarjetas para conectar a los PC, ya sean internas, como tarjetas PCI o bien USB (tarjetas de nueva generación que no requieren incluir ningún hardware dentro del ordenador). Los puntos de acceso funcionan a modo de emisor remoto, es decir, en lugares donde la señal WLAN del router no tenga suficiente radio. Los router son los que reciben la señal de la línea que ofrezca el operador de telefonía, se encargan de todos los problemas inherentes a la recepción de la señal, donde se incluye el control de errores y extracción de la información, para que los diferentes niveles de red puedan trabajar. En este caso el router efectúa el reparto de la señal, de forma muy eficiente. Además de routers, hay otros dispositivos que pueden encargarse de la distribución de la señal, como pueden ser hubs y switch".[8]

1.4.8 AMENAZAS

[8] http://es.wikipedia.org/wiki/Wi-Fi, Tecnologia Wireless Fidelity.

Los ataques activos buscan causar algún daño, como ser: perdida de confidencialidad, disponibilidad e integridad de información ó sistemas.

IP Spoofing: El atacante cambia su dirección IP para poder pasar por alto controles de acceso.

MAC Address Spoofing: El atacante cambia su dirección MAC para pasar por alto los controles de acceso de los Access Points. Como veremos mas adelante, la mayoría de los Access Points posee controles de acceso filtrando direcciones MAC.

ARP Poisoning: Todos los equipos conectados a una red tienen una tabla ARP que asocia direcciones MAC a direcciones IP. Este tipo de ataque busca modificar estas tablas para poder redirigir el tráfico de un equipo a otro de manera controlada.

Man in the middle: Este tipo de ataque se puede ejecutar una vez realizado un ARP Poisoning, en el cual se redirige todo el trafico saliente de un equipo (victima) a otro y este lo envía al destino original. Este tipo de ataque es transparente y la victima no se da cuenta que su trafico de red está pasando por un tercero antes de llegar a destino.

MAC Flooding: Este ataque se consiste en inundar la red con direcciones IP falsas, causando que el Switch pase a funcionar en modo de Hub, ya que no soporta tanto tráfico.

Denial of Service: Este tipo de ataque busca dejar fuera de servicio a la red inalámbrica, utilizando todo el ancho de banda para enviar paquetes basura. También se utiliza normalmente para dejar fuera de servicio a servidores ó aplicaciones.

Injection: El atacante puede insertar paquetes en la red inalámbrica causando que todos los clientes se desconecten ó inundar la red con paquetes basura (generando un DoS).

Replay: El atacante captura paquetes y luego los reinserta en la red inalámbrica con o sin modificación.

Rouge AP: El atacante pone su propio Access Point y engaña a los clientes pensando que es el Access Point verdadero. De esta forma, posee todo el control del tráfico.

1.5. Voz Sobre IP

1.5.1. Introducción

VoIP viene de Voice Over Internet Protocol. Como dice el término VoIP intenta permitir que la voz viaje en paquetes IP y obviamente a través de Internet.

La telefonía IP conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes.

Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y yendo un poco más allá, desarrollar una única red convergente que se encargue de cursar todo tipo de comunicación, ya sea voz, datos, video o cualquier tipo de información.

Cuando se produce un silencio en una conversación, los paquetes de datos de otras conversaciones pueden ser transmitidos por la red, lo que implica un uso más eficiente de la misma.

1.5.2. Componentes de una red de voz sobre paquetes

La transmisión de voz sobre una red de paquetes va a implicar la aparición de nuevos equipos encargados de la integración propiamente dicha, a la vez que se van a seguir utilizando los componentes tradicionales de las redes de voz y las redes de datos convencionales.

Un códec (abreviatura de COdificador/DECodificador) es el hardware o el software encargado de convertir la señal analógica en un conjunto de muestras digitales aptas para su transmisión por la red de paquetes.

En algunos casos realizan, además, una compresión de la señal reduciendo así los requerimientos de ancho de banda. En el punto dedicado a las pasarelas entraremos más en profundidad en la codificación de la señal.

Si ya está claro que la señal de voz requiere de una conversión a formato digital para su transmisión por la red de paquetes, el problema que queda por resolver es el punto en que tiene lugar dicha conversión o, lo que es lo mismo, la ubicación del códec.

La solución depende del tipo de terminales de usuario disponibles. Los teléfonos analógicos convencionales son incapaces de realizar procesamiento alguno de la señal por lo que, en estas ocasiones, el códec se encuentra en la PBX (o IP-PBX, en su caso).
La mayoría de redes de datos se basan en la filosofía cliente/servidor en la que los clientes solicitan ciertos servicios a los servidores. La integración de las redes de voz y las redes de datos ha extendido esta filosofía a entornos telefónicos, surgiendo así la figura del servidor de telefonía.

Las pasarelas, por su parte, se encargan de conectar la red de paquetes a la red telefónica jugando, por tanto, un papel crucial en la integración de los dos

mundos. Centrándonos en el entorno corporativo, las pasarelas proporcionan la interfaz de la red de datos con las PBX tradicionales (o con una IP-PBX).

1.5.3. Calidad de la voz sobre paquetes

Las redes de conmutación de circuitos tradicionales han sido diseñadas y optimizadas para el transporte de voz.

Como consecuencia, la RTPC proporciona una calidad de servicio predecible para el tráfico de voz y prueba de ello es que se ha convertido en el estándar de referencia a la hora de analizar la calidad de la voz en cualquier tipo de red.

La RTPC consigue una alta calidad reservando recursos para cada comunicación y no sometiendo a la señal a ninguna técnica de codificación o conversión analógico-digital.

Sin embargo, en una red integrada de voz y datos, la calidad de la voz deja de estar garantizada y de ser predecible, convirtiéndose en un factor discriminante entre diferentes tipos de redes, equipos y servicios. Por ello, la medida de la calidad de la voz se ha convertido en un aspecto fundamental dentro del entorno de la convergencia de redes.

Existen varios factores que influyen en la calidad de la voz, entre los que se encuentran el retardo, el jitter, las pérdidas de paquetes y la claridad de la voz.

En las redes de conmutación de circuitos tradicionales se han venido empleando las siguientes técnicas de medida:

- Relación señal/ruido (SNR, Signal-to-Noise Ration): es una medida de los niveles de ruido relativos en las señales analógicas y de la distorsión

introducida durante el proceso de cuantificación de un codificador digital. La SNR es muy útil cuando el proceso de codificación conserva la forma de onda de la señal de entrada.

- Distorsión: las técnicas de medida de distorsión evalúan la distorsión no lineal introducida por equipos de procesamiento de señal (por ejemplo, amplificadores).

- Tasa de error de BIT: es una medida de la calidad física de la transmisión sobre una red determinada. Todas estas medidas son adecuadas cuando se conserva la forma de onda de la señal de entrada. Por esta razón, en las redes integradas son necesarios otros tipos de medidas basados en la calidad de la percepción.

Las medidas subjetivas son las más intuitivas y consisten en realizar una llamada telefónica, descolgar el receptor y escuchar qué tal se oye la conversación.

Generalmente, en entornos telefónicos consisten en el empleo de una señal de referencia o la monitorización del tráfico en tiempo real.

Dentro de las medidas objetivas se distinguen dos grupos de medidas que se diferencian en su modo de interaccionar con la red.

El otro gran grupo de medidas objetivas son las medidas pasivas. El inconveniente es que son más complejas que las medidas pasivas y, por lo general, son menos exactas.

Como hemos dicho anteriormente, la medida de la calidad de la señal puede efectuarse mediante comparación empleando para ello un algoritmo específico.

PSQM (Perceptual Speech Quality Measuremeni): es un proceso matemático que proporciona una medida de la calidad de la voz. PSQM ha sido diseñada especialmente para anchos de banda telefónicos (300-3.400 Hz) y para códecs de voz.

PESQ (Perceptual Evaluation of Speech Quality): al igual que las dos anteriores, está optimizada para señales de ancho de banda telefónico

1.5.4 Limitaciones tecnológicas de la voz sobre paquetes

En la calidad de la voz son cinco los factores a tener en cuenta:

- El ancho de banda necesario para cursar las llamadas a través de la red.
- Las pérdidas de paquetes debidas, básicamente, a la limitación del ancho de banda de la red y a la congestión de los routers.
- El retardo sufrido por los paquetes debido al procesamiento a que es sometida la señal de voz y al recorrido de los paquetes de voz por la red.
- El jitter de los paquetes, es el retardo que sufren los paquetes de voz en su tránsito por la red., por lo que cada paquete se transmite independientemente del resto.
- El eco debido al acoplo que sufre la señal entre los distintos sentidos de la comunicación.

1.6 Control y previsión de la congestión

1.6.1 Control

Los nodos de la red (como es el caso de los routers en una red IP o de los conmutadores en una red ATM) disponen de unos buffers en los que se almacenan temporalmente los paquetes antes de ser transmitidos y que se denominan colas de transmisión.

Por otra parte, la disciplina de servicio de la cola define el modo en que los nodos de la red extraen los paquetes de dichas colas para su envío. Si consideramos una red multi-servicio en la que conviven varios tipos de tráfico, deberemos idear algún tipo de mecanismo de priorización del tráfico, puesto que cada uno de esos tipos exige de la red niveles de servicio distintos. En concreto, es necesario asignar mayor prioridad al tráfico de voz con el fin de minimizar el retardo de los paquetes.

Uno de los aspectos que más va a afectar a dicho retardo es la congestión de la red, puesto que, cuanto mayor sea el número de paquetes presentes en la misma, tanto mayor será el consumo de recursos en los nodos de la red y, por tanto, mayor será el retardo introducido por éstos.

La disciplina de servicio más simple trata a todos los paquetes de la misma manera. El algoritmo de selección busca los paquetes en las colas por orden prioridad: mientras haya paquetes de una determinada prioridad, no se transmitirán paquetes de prioridad menor. Sin embargo, PQ es muy adecuada cuando el tráfico de alta prioridad consume poco ancho de banda.

CQ (Custom Queueing) utiliza una cola para cada tipo de tráfico. Por supuesto, el ancho de banda no utilizado por una cola puede ser empleado por el resto.

1.6.2 Previsión

Las técnicas de previsión de la congestión monitorizan las cargas de tráfico de la red con el fin de anticiparse a las posibles situaciones de congestión que pudieran acontecer en los cuellos de botella de la red.

La congestión ocurre cuando las colas de los *routers* se saturan y, por tanto, no son capaces de aceptar más paquetes. Los dos mecanismos principales son RED *(Random Early Detection)* y su versión ponderada, WRED (*WeightedRandom Early Detection).*

El algoritmo RED intenta evitar esta situación de forma preventiva, iniciando un proceso aleatorio de descarte de paquetes cuando detecta una tendencia a la congestión.

En la versión ponderada de RED, la probabilidad de que un paquete sea descartado está determinada por el grado de ocupación de la cola y por un peso asociado al tipo de tráfico al que pertenece el paquete en cuestión.

El objetivo es que los paquetes de mayor prioridad tengan menor probabilidad de descarte.

Servicios suplementarios: una de las mayores ventajas de la VoIP es su capacidad para proporcionar servicios al usuario final.

Capacidad de punto final: los puntos finales tienen la posibilidad de especificar la capacidad que necesitarán para llevar su llamada a buen término. Indicación de protocolos deseados: un punto final puede indicar al gatekeeper en el mensaje de los protocolos que, probablemente, se necesiten para establecer la comunicación con el punto final destino.

Gestión del ancho de banda: si el gatekeeper lo solicita, es posible enviar información detallada sobre los canales de datos, mejorando así el control de la utilización del ancho de banda.

Informes del estado de la llamada: la versión 4 proporciona un mecanismo a través del cual un mensaje IRR que contenga información de múltiples llamadas puede fragmentarse en mensajes más pequeños, lo que permite al punto final enviar toda la información del estado de la llamada al gatekeeper.

Características relacionadas con llamadas a crédito: consiste en poder realizar llamadas cargando los costes de la comunicación a tarjetas prepago.

1.6.3 Mecanismos de control y señalización

H.323 proporciona tres protocolos de control, que son:

- Señalización de llamada H.255/Q: para el control de la señalización asociada a las llamadas.
- RAS H.225.0: para el establecimiento de una llamada desde el origen hasta el destino.
- H.245: para negociación de los flujos de datos.

1.7 Estándar de voz sobre IP H.323v4

1.7.1 Protocolo H.323V4

En un principio, las redes VoIP eran propietarias, en donde cada fabricante diseñaba su propia pila de protocolos que controlaban los mecanismos de señalización, control y codificación de la voz con muy poca o sin ninguna interoperabilidad entre ellas. En 1996, La ITU emitió la recomendación

H.323 titulada "Sistemas Telefónicos Visuales y Equipos para Redes de Área Local que proporcionan una Calidad de Servicio No Garantizada", luego aparecerian otras versiones tales como: H.323V2, H.323V3 y H.323V4.

Esta Norma fue la base de los primeros sistemas de Telefonía Internet ampliamente difundidos.

El protocolo H.323 hace referencia a una gran cantidad de protocolos específicos para codificación de voz, establecimiento de llamadas, señalización, transporte de datos y otras áreas, en lugar de especificar estas cosas en sí. Entre otras cosas, el hecho de que NetMeeting, un cliente H.323 desarrollado por Microsoft para Windows 95, 98, 2000 y Windows NT, se entregue de forma gratuita, es prácticamente una garantía de que esta es la norma que hay que cumplir.

El modelo general se ilustra en la figura 1.1 en el centro se encuentra una Puerta de Enlace (Gateway H.323) que conecta Internet con la Red Telefónica (PSTN o ISDN).

Dicha Puerta de Enlace maneja los protocolos H.323 por el lado de Internet y los protocolos PSTN o ISDN en el lado de la Red Telefónica.

Los dispositivos de comunicación se llaman Terminales. Una LAN podría tener un Gatekeeper, el cual controla los terminales bajo su jurisdicción, llamados zona.

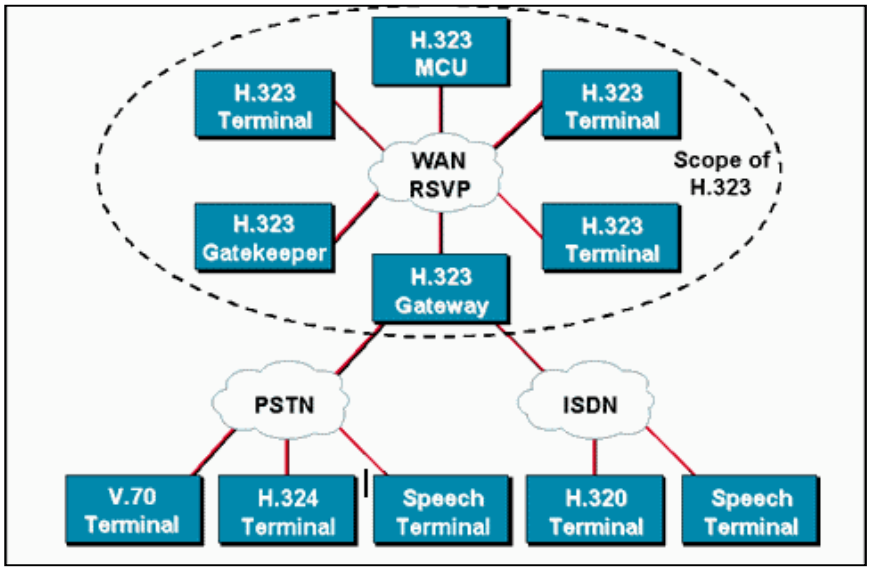

Figura 1.6. Protocolo de Transmisión de Voz H323

Fuente: Integración de Voz y Datos de Huidrobo

La versión 4 de H.323 se aprobó el 17 de noviembre de 2000 y su objetivo básico es la compatibilidad con los protocolos de Voz sobre IP

1.7.2 Entidad

La especificación H.323 define el término genérico entidad como cualquier componente que cumpla con el estándar.

1.7.3 Extremo

Un extremo H.323 es un componente de la red que puede enviar y recibir llamadas. Puede generar y/o recibir secuencias de información.

1.7.4 Terminal H.323V4

Son los clientes que inician una conexión VoIP. Pueden ser de varios tipos:

- **IP Phone:** o teléfonos IP, se muestra en la figura N.1.2

Figura 1.7

- **Soft Phone:** se trata normalmente de una PC multimedia que simula un teléfono IP, por ejemplo, el servicio de NetMeeting utiliza protocolo H.323.

- **MCU's H.323:** se utiliza cuando han de intervenir más de dos partes en una conferencia. La MCU (Multimedia Conference Unit) es responsable de controlar las sesiones y de efectuar el mezclado de los flujos de audio, datos y video.
- **Adaptador para PC:** más conocido como ATA, es un adaptador de teléfono analógico que se conecta al servicio de cable MODEM o al servicio de DSL, que permite obtener telefonía por Internet.

1.7.5 Pila de protocolos H.323V4

El VoIP/H.323 comprende una serie de protocolos que cubren los distintos aspectos de la comunicación:

1.7.5.1 Direccionamiento

- RAS (Registration, Admision and Status): Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del Gatekeeper.

- DNS (Domain Name Service): Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

1.7.5.2 Señalización

- H.225 (RAS): Protocolo que permite a los terminales hablar con el Gatekeeper, solicitar y regresar ancho de banda y proporcionar actualizaciones de estado.

- Q.931: Protocolo de señalización de llamadas, para establecer y liberar las conexiones con la red telefónica RTC.

- H.245: Protocolo de control de llamadas, permite a los terminales negociar ciertos parámetros como: el tipo de Códec, la tasa de bits.

1.7.5.3 Compresión de voz

- Requeridos: G.711 y G.723.1

- Opcionales: G.728, G.729 y G.722

1.7.5.4 Transmisión de voz

- UDP: La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

- RTP (Real Time Protocol): Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

1.7.5.5 Control de la transmisión

- RTCP (Real Time Control Protocol): Es un protocolo de control de los canales.
- RTP: Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

1.8 Componentes de una red

Aunque, estrictamente hablando, los componentes de una red H.323V4 son los terminales, las pasarelas, los gatekeepers y las MCU, haremos mención especial en este apartado a los códecs (tanto de audio como de video) y a la conferencia de datos, dada su importancia por formar parte de varios de los componentes de la red.

1.8.1 Códec de audio

Un códec de audio codifica la señal de audio procedente del micrófono del terminal transmisor y, en el otro extremo, decodifica el audio codificado enviado al hablante del terminal H.323V4 receptor.

Puesto que el servicio mínimo proporcionado por H.323V4 es la comunicación de voz, todos los terminales H.323V4 deben disponer de, al menos, un códec de audio como especifica la recomendación ITU-T G.711 (codificación de audio a 64 kbps).

Sin embargo, esta codificación es la menos adecuada para la comunicación sobre una red de paquetes porque si el ancho de banda de usuario es menor de 64 kbps, así que se han definido otras recomendaciones adicionales como son G.722 (64, 56, y 48 kbps), G.723.1 (5,3 y 6,3 kbps), G.728 (16 kbps), y G.729 (8 kbps), que también se soportan.

1.8.2 Códec de vídeo

Por su parte, un códec de vídeo codifica la señal de vídeo procedente de la cámara del terminal transmisor y, en el otro extremo, decodifica el vídeo codificado enviado al terminal H.323V4 receptor.
Las comunicaciones de vídeo requieren de un mayor ancho de banda que las comunicaciones de voz y, además, su carácter es mucho más aleatorio.
Por tanto, resulta fundamental llevar a cabo una compresión eficiente para conseguir una buena calidad de la señal.
• H.263: está diseñado para transmisiones de baja velocidad sin pérdida de calidad. La calidad del vídeo depende de la técnica de compresión empleada.

1.8.3 Terminal

Un terminal H.323V4 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323V4, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323V4 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

1.8.4 Pasarelas (gateway)

Una pasarela se encarga de traducir los protocolos de llamadas y de la conversión de formatos de la información entre diferentes tipos de redes así como de transmitir información entre redes H323 y no H323.

1.8.5 Gatekeeper

El gatekeeper (GK) es una entidad que proporciona servicios de control de llamadas, la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El GK puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways o pasarelas.

El Gatekeeper realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP o IPBX, tal y como se describe en la especificación RAS.

La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN.

El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la denominada Zona de control H.323.