VoWiFi & IM:

Comunicaciones móviles en la red global

Daniel Calvache López
Ingeniería Informática

Consultor: **Víctor Carceler Hontoria**

Fecha: Junio 2006

No es que nos falte valor para emprender las cosas porque sean difíciles, sino que son difíciles precisamente porque nos falta valor para emprenderlas.

Lucio Anneo Séneca
Filósofo y escritor hispanorromano (Córdoba, 4 aC- Roma, 65)

Agradecimientos

A mi mujer por su paciencia y comprensión durante todos estos años en la UOC…

Resumen ejecutivo

En el marco del congreso mundial de telefonía móvil celebrado en Barcelona en Febrero de 2006, Microsoft anunció con cierta indiferencia por parte de los medios el futuro lanzamiento de una aplicación VoIP que permitirá a los usuarios de su popular suite ofimática "Office" realizar llamadas telefónicas gratuitas mediante cualquier dispositivo Wi-Fi que incorpore el software "Windows Mobile". Algunos analistas ya prevén que este servicio gratuito al estilo del popular Skype llevado a los teléfonos móviles puede suponer billones de dólares de pérdidas para los operadores de telefonía móvil tradicional, si se tiene en cuenta la ingente cantidad de dispositivos móviles que incorporan sistemas operativos Windows, la continua expansión de zonas de cobertura Wi-Fi tanto en entornos privados cómo en espacios públicos (hotspots), y sobretodo, el gran paso que supone el hacer converger definitivamente la movilidad, los datos y la voz en una única red mundial y de libre uso: la red de redes Internet.

Durante los primeros capítulos del informe se lleva a cabo un estudio básico del estado del arte de de las distintas tecnologías que hacen posible este nuevo escenario, no tanto desde el punto de vista estrictamente técnico (cuya descripción ya ha sido objeto de innumerables proyectos) sino más bien desde el punto de vista de su aplicación práctica y su previsible evolución futura. Durante el proyecto se hará especial inciso en los servicios adicionales que pueden complementar a la voz sobre la red de datos, como por ejemplo la mensajería instantánea, así como una evaluación de los diferentes proyectos de código abierto actualmente en desarrollo que persiguen esta integración.

En una segunda fase se estudia la fusión de la tecnología de transmisión de datos sin hilos (WiFi) con la de transmisión de voz sobre IP (VoIP) en lo que se ha dado a llamar VoWiFi (voz sobre WiFi). En este capítulo se aborda el estudio de las ventajas e inconvenientes que presenta esta nueva tecnología, las posibilidades prácticas que aporta de cara a futuras aplicaciones, y adicionalmente se establece un foco especial en la integración de este tipo de plataformas con servicios de mensajería instantánea (IM) y Chat. Para finalizar el capítulo dedicado a VoWiFi se lleva a cabo un estudio de algunas aplicaciones de código abierto (*Open Source*) que permiten construir y llevar a cabo soluciones de este tipo: sistemas operativos, centralitas digitales de VoIP, servidores de mensajería instantánea, clientes tanto de voz como de Chat, etc.

Y para finalizar, una vez estudiadas las distintas tecnologías que permiten dar forma a los escenarios en los que se integran estas nuevas aplicaciones, como conclusión final se implementa un proyecto de implantación práctica consistente en el diseño, implementación, puesta en marcha y desarrollo de un plan de pruebas de una plataforma VoWiFi mediante software libre, utilizando Asterisk@Home como centralita digital y Wildfire Jabber Server como servidor de mensajería instantánea, haciendo uso de diversos clientes de acceso de código abierto tanto de VoIP como de IM.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

I. Introducción

1. Descripción del proyecto

El presente proyecto lleva por título “VoWiFi & IM: Comunicaciones móviles en la red global”. Concebido y vertebrado en tres grandes bloques, el proyecto arranca con un breve estudio de las tecnologías sobre las que se fundamenta VoWiFi, como son la transmisión de datos en medio inalámbrico (WiFi) y la codificación de voz sobre protocolo IP (VoIP). Una vez revisada la base tecnológica sobre la que se sustentan estas tecnologías desde un punto de vista conceptual, el segundo gran bloque se dedica a estudiar las posibilidades que ofrece su fusión en un nuevo concepto bautizado como VoWiFi, que no es mas que la transmisión inalámbrica de voz digitalizada sobre protocolo IP. Durante este capítulo se lleva a cabo un estudio de las ventajas e inconvenientes que aporta esta nueva plataforma tecnológica, así como los servicios adicionales a los que se puede asociar, especialmente en el campo de la mensajería instantánea. Para finalizar este segundo bloque se incluye además un estudio de las principales aplicaciones de código abierto (*Open Source*) que permiten implementar este tipo de plataformas. Y por último, como conclusión del proyecto, se lleva a cabo el diseño, instalación, configuración y puesta en marcha de una plataforma VoWiFi y mensajería instantánea mediante las herramientas *Open Source* anteriormente estudiadas, con el objetivo de aplicar los conceptos teóricos en una solución real bajo un entorno de laboratorio que puede ser fácilmente extrapolable a cualquier instalación real.

2. Objetivos del proyecto

El objetivo principal del proyecto es el estudio de la tecnología VoWiFi tanto desde el punto de vista de su base técnica como de sus posibles aplicaciones actuales y futuras, especialmente en lo que se refiere a la integración de servicios adicionales como la mensajería instantánea. Una vez analizados los conceptos teóricos se realiza un estudio de las principales herramientas de código abierto que permiten implementar este tipo de plataformas, para finalmente concluir con la instalación práctica de una plataforma de laboratorio.

Los resultados obtenidos se distribuyen entre los siguientes apartados que conforman el índice general del proyecto:

- Estudio básico de la tecnología WiFi.
- Estudio básico de la tecnología VoIP.
- VoWiFi: Presente y futuro.
    - Aplicaciones Open Source.
- Aplicación práctica: diseño, puesta en marcha y plan de pruebas.

3. Distribución temporal

3.1. Definición del proyecto y fase de investigación

- **Objetivo:** definir los objetivos y el alcance concreto del proyecto. Una vez identificados los objetivos y el contenido a desarrollar, llevar a cabo una fase de investigación de conceptos teóricos a partir de documentos y estudios previos acerca de la materia.
- **Duración:** 15 días
- **Resultado**: índice general del proyecto junto con sus objetivos principales. Como resultado de la etapa de investigación se obtendrá un repositorio de documentación a partir de la cual desarrollar los conceptos teóricos.

3.2. Estudio tecnología WiFi

- **Objetivo:** descripción básica de la tecnología WiFi desde el punto de vista legal, tecnológico, y sus previsiones de futuro.
- **Duración:** 5 días
- **Resultado**: capítulo dedicado a la tecnología WiFi.

3.2. VoWiFi: Presente y futuro

- **Objetivo:** descripción básica de la tecnología VoWiFi, ventajas e inconvenientes, posibilidades de convergencia de servicios como mensajería, videoconferencia, video streaming, etc.
- **Duración:** 15 días
- **Resultado**: capítulo dedicado a la tecnología VoWiFi.

3.2. Aplicaciones Open Source

- **Objetivo:** estudio de las aplicaciones de código abierto que permiten implementar plataformas VoWiFi (sistemas operativos, centralitas digitales VoIP, servidores de mensajería instantánea, clientes de VoIP, clientes de mensajería instantánea, etc.
- **Duración:** 10 días
- **Resultado**: capítulo dedicado a las aplicaciones *open source*.

3.2. Aplicación práctica: diseño, puesta en marcha y pruebas

- **Objetivo:** diseño e instalación de una plataforma VoWiFi y mensajería instantánea en entorno de laboratorio utilizando aplicaciones de código abierto. Una vez instalada se realizarán pruebas de funcionamiento.
- **Duración:** 20 días
- **Resultado**: plataforma funcional VoWiFi de laboratorio para probar el funcionamiento de la tecnología de voz IP sobre WiFi juntamente con la mensajería instantánea.

4. Calendario de trabajo

En el siguiente diagrama de Gantt se resume el calendario de trabajo del proyecto:

	Nombre de tarea	Duración	Comienzo	Fin
1	**Definición del proyecto y fase de investigación**	15 días	lun 13/03/06	vie 31/03/06
2	**Estudio tecnología WiFi**	**5 días**	**lun 03/04/06**	**vie 07/04/06**
3	Estudio legal	2 días	lun 03/04/06	mar 04/04/06
4	Estudio tecnológico	2 días	mié 05/04/06	jue 06/04/06
5	Previsiones de futuro	1 día	vie 07/04/06	vie 07/04/06
6	**Estudio tecnología VoIP**	**5 días**	**lun 10/04/06**	**vie 14/04/06**
7	Estudio legal	2 días	lun 10/04/06	mar 11/04/06
8	Estudio tecnológico	2 días	mié 12/04/06	jue 13/04/06
9	Previsiones de futuro	1 día	vie 14/04/06	vie 14/04/06
10	**VoWiFi: Presente y futuro**	**15 días**	**lun 17/04/06**	**vie 05/05/06**
11	Ventajas e incovenientes	1 día	lun 17/04/06	lun 17/04/06
12	Convergencia de servicios: videoconferencia, streaming, etc.	2 días	mar 18/04/06	mié 19/04/06
13	Mensajería instantanea	2 días	jue 20/04/06	vie 21/04/06
14	**Aplicaciones Open Source**	**10 días**	**lun 24/04/06**	**vie 05/05/06**
15	Sistema operativo	2 días	lun 24/04/06	mar 25/04/06
16	Centralitas VoIP	2 días	mié 26/04/06	jue 27/04/06
17	Servidores IM (Instant Messaging)	2 días	vie 28/04/06	lun 01/05/06
18	Clientes VoIP	2 días	mar 02/05/06	mié 03/05/06
19	Clientes IM	2 días	jue 04/05/06	vie 05/05/06
20	**Aplicación práctica: diseño, puesta en marcha y pruebas**	**20 días**	**lun 08/05/06**	**vie 02/06/06**
21	Plataforma WiFi	5 días	lun 08/05/06	vie 12/05/06
22	Asterisk@Home	5 días	lun 15/05/06	vie 19/05/06
23	Wildfire Jabber Server	5 días	lun 22/05/06	vie 26/05/06
24	Clientes Mensajería Instantánea	5 días	lun 29/05/06	vie 02/06/06
25	**Documentación**	**10 días**	**lun 05/06/06**	**vie 16/06/06**
26	**Proyecto finalizado**	0 días	vie 16/06/06	vie 16/06/06

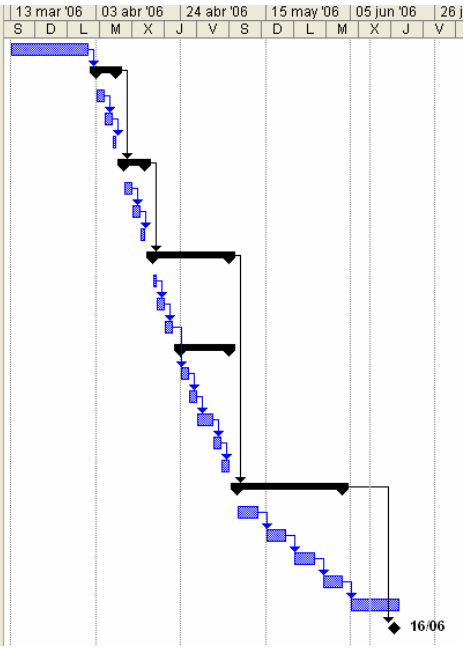


Figura 0-1: Diagrama de Gantt del proyecto

Capítulo 1 : Estudio sobre la tecnología Wifi.

1. Introducción

Wi-Fi es una marca creada por la Wi-Fi Alliance (http://www.wi-fi.org) para describir los productos de red inalámbrica de área local (WLAN) basados en los estándares 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

Contrariamente a lo que suele aceptarse entre los miembros de la comunidad tecnológica, originalmente el nombre Wi-Fi no responde al acrónimo de "*Wireless Fidelity*" sino que únicamente se trata de una marca ideada por la consultora internacional Interbrand Corporation, empresa especializada en servicios de creación de marcas, estrategias de *branding*, identidad corporativa y desarrollo de nombres (http://www.interbrand.com).

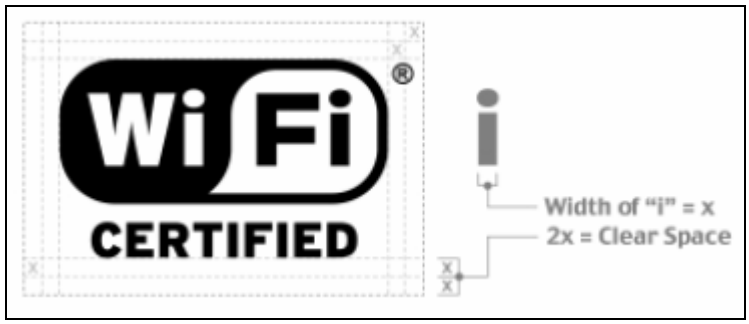


Figura 1-1: Logotipo de Wi-Fi

Los miembros de la *Wireless Ethernet Compatibility Alliance* (lo que actualmente es la Wi-Fi Alliance) contrataron a la consultora Interbrand, creadora de marcas como "Prozac", "Compaq", "oneworld" o "Imation", para que crearan un nombre y un logotipo que pudieran utilizar como sello de interoperabilidad y herramienta de marketing en los productos que cumplieran con la norma "*IEEE 802.11b Direct Sequence*". Según indica Phil Belanger, uno de los fundadores de la alianza, la frase "*Wireless Fidelity*" apareció posteriormente a la marca debido a que algunos de sus miembros iniciales no acababan de entender una marca que no tuviera un significado, y por tal motivo durante la etapa inicial de la alianza se incluyó la frase "*The Standard for Wireless Fidelity*" junto con la marca y el logotipo.

2. Wireless LAN y el protocolo IEEE 802.11

Una *Wireless LAN* (WLAN) es un sistema de transmisión de datos diseñado para proporcionar acceso a la red desde cualquier dispositivo electrónico mediante ondas de radio, utilizando el estándar IEEE 802.11.

En entornos corporativos, las WLAN se utilizan habitualmente como enlace final entre redes cableadas existentes y grupos de usuarios finales, proporcionándoles acceso inalámbrico a la totalidad de recursos y servicios de la red corporativa repartidos a lo largo de la infraestructura LAN, MAN o WAN. Las WLAN llevan multitud de años presentes en la comunidad tecnológica, pero su aceptación global y su incorporación masiva a las industrias dependen de la existencia de un nivel de estandarización suficiente que asegure un grado extenso de compatibilidad y fiabilidad entre dispositivos de diferentes fabricantes.

La especificación 802.11 [IEEE Std 802.11 (ISO/IEC 8802-11: 1999)] como estándar fue ratificada por el Instituto de Ingenieros Eléctricos y Electrónicos en el año 1997, y proporcionaba velocidades de acceso al medio de 1 y 2Mbps además de una serie de métodos fundamentales de señalización y otros servicios. Como todos los estándares del IEEE, la especificación 802.11 se define en los dos niveles más bajos del modelo ISO (nivel físico y nivel de enlace).

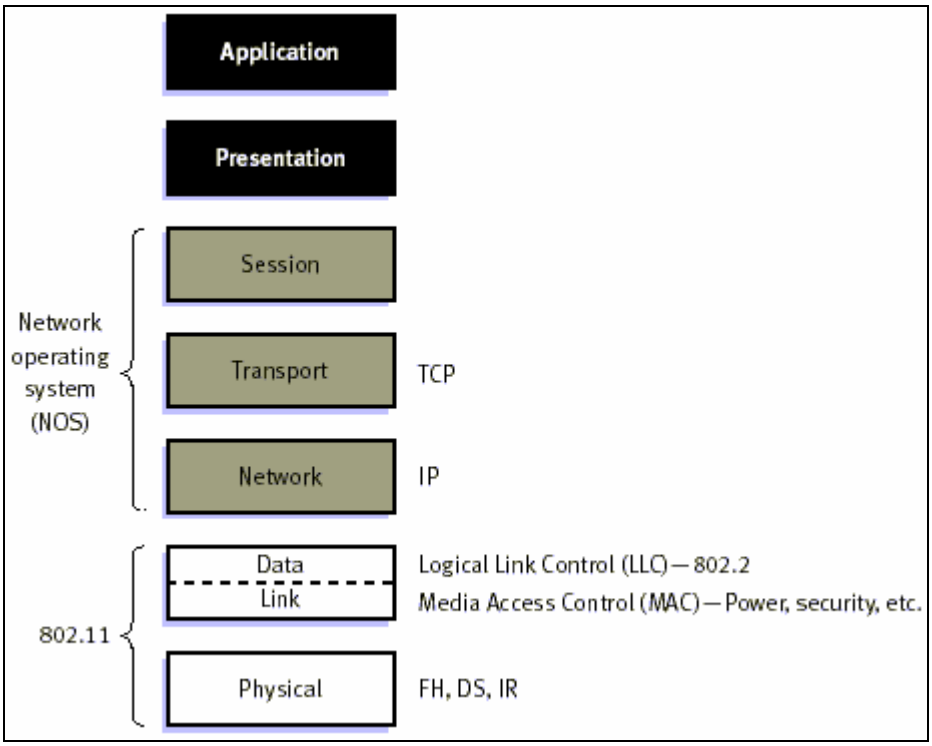


Figura 1-2: IEEE 802.11 y el modelo ISO

La principal ventaja de las redes de área local inalámbricas es la movilidad de los dispositivos de acceso, permitiéndoles acceder a los recursos de la red prácticamente desde cualquier ubicación física que disponga de cobertura.

Otra de las ventajas de la tecnología inalámbrica es la reducción de costes que supone en localizaciones difíciles de cablear mediante sistemas de conexionado físico, como por ejemplo en edificios antiguos o estructuras regias, además de la disminución de los costes totales de propiedad (TCO) en entornos dinámicos que requieren modificaciones frecuentes, gracias a los costes mínimos en cableado e instalación por dispositivo y usuario.

3. Arquitectura IEEE 802.11

Cualquier dispositivo con procesador, portátil, móvil o fijo que accede a una red 802.11 se conoce como estación. La diferencia entre una estación portátil y una móvil es que la portátil se puede mover entre diferentes puntos pero solo se utiliza en uno (por ejemplo un ordenador portátil se puede colocar en cualquier mesa de la oficina, pero una vez sentado el usuario trabaja estáticamente desde aquella ubicación), mientras que un dispositivo móvil accede a la red en movimiento (por ejemplo un usuario consulta el correo electrónico desde su PDA mientras camina desde su mesa hacia el comedor de la empresa situado en la planta superior del edificio).

Cuando dos o más estaciones quieren establecer comunicación entre ellas forman lo que se conoce como una *Basic Service Set* (BSS). Si estas estaciones no se encuentran conectadas a una base común la configuración toma el nombre BSS independiente (IBSS), también conocida como red *Ad-Hoc*, donde las estaciones se comunican de igual a igual (*peer to peer*). En este tipo de configuración no existe ninguna base y nadie coordina los permisos para transmitir, con lo cual son configuraciones adecuadas para instalaciones temporales con un número limitado de estaciones.

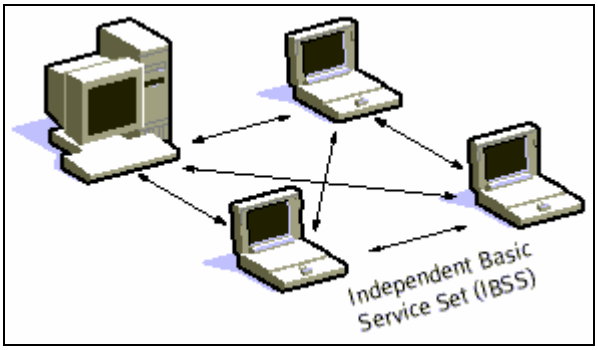


Figura 1-3: Independent Basic Service Set o red "Ad-Hoc"

Cuando los BSS individuales se interconectan entre sí la red adquiere entonces infraestructura, que en el caso de 802.11 está formada de varios elementos. Los BSS se interconectan mediante DS (*Distribution System*) a través de dispositivos de acceso o *Access Points* (AP), que no son más que estaciones centrales con entidad propia que funcionan como punto de acceso común a modo de concentrador o *hub*. El uso de redes con BSS y DS lleva al siguiente nivel en la jerarquía: el *Extended Service Set* (ESS), en el cual la red completa se muestra como un servicio independiente de la capa lógica de control (LLC).

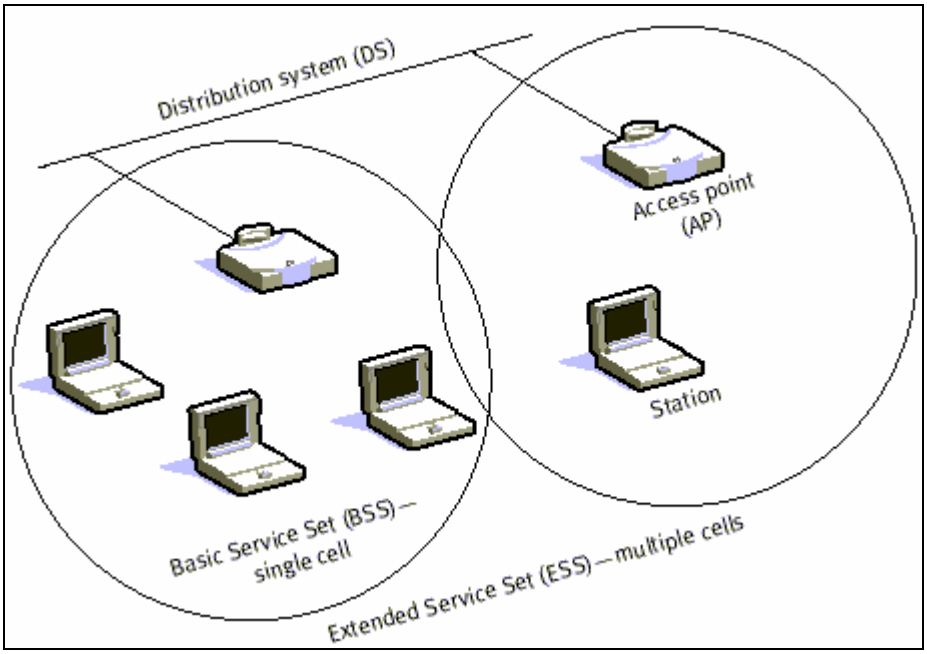


Figura 1-4: Modo infraestructura

La implementación de los DS (*Distribution System*) no está especificada por la norma 802.11 aunque sí lo están los servicios que debe soportar, que se encuentran divididos en dos secciones:

1. Servicios de estación (SS)
    a. Autenticación
        i. Open System Authentication.
        ii. Shared Key Authentication.
    b. Desautenticación
    c. Privacidad
    d. Distribución MAC Service Data Unit (MSDU).

2. Servicios de sistemas de distribución (DSS)
    a. Asociación.
    b. Reasociación.
    c. Desasociación.
    d. Distribución.
    e. Integración.

En un sistema sin hilos el medio físico no se encuentra accesible de la misma forma que en un medio cableado, ya que para controlar el acceso a la red es necesario que las estaciones se identifiquen previamente. El primer paso es asegurar que la estación es quien realmente dice ser para que pueda proceder a su asociación, objetivo llevado a cabo por el servicio de autenticación. La norma 802.11 define dos tipos de autenticación: autenticación abierta (*Open Key Authentication*) en la cual cualquier estación que requiera acceso al medio podrá hacerlo sin más, y la autenticación de clave compartida (*Shared Key Authentication*) en la cual la estación debe estar en posesión de una clave conocida y compartida con el punto de acceso para poder obtener acceso al medio (en este último caso se utiliza el algoritmo de privacidad del protocolo WEP o *Wired Equivalent Privacy*).

La desautenticación se lleva a cabo cuando la estación o el propio punto de acceso quieren finalizar la autenticación de una estación, momento en el cual se produce una desasociación de la estación con el medio.

La privacidad en la especificación nativa 802.11 se basa en un algoritmo de encriptación cuyo objetivo es evitar que una estación conectada al medio pueda tener acceso al tráfico de otras estaciones (*eavesdrooping*), y se lleva a cabo mediante el uso de un protocolo opcional llamado WEP (*Wired Equivalent Privacy*). Todas las estaciones comienzan transmitiendo en texto plano sin encriptar hasta que son autenticadas (*plaintext*), y posteriormente pueden proseguir trabajando en texto plano o encriptado (*ciphertext*) en caso de utilizar WEP (una de las razones por la cual WEP es opcional es debido a las leyes que restringen la exportación de algoritmos de encriptación fuera de los Estados Unidos de América).

Y como último de los servicios de estación se encuentra el servicio de distribución MSDU, el cual se encarga de asegurar que la información en el servicio de datos MAC es entregada correctamente entre los servicios de control de acceso al medio de los puntos de acceso.

Por otro lado, los primeros tres servicios de DSS tienen que ver con la movilidad y la asociación de las estaciones con los puntos de acceso (AP), mientras que los servicios de distribución e integración son los encargados de llevar los datos del emisor a su destino a través del AP (ya sea un destino conectado al mismo punto de acceso o no).

3.1 La capa física

Las tres capas físicas definidas originalmente en la especificación 802.11 incluían dos técnicas de radio de amplio espectro además de una especificación difusa de infrarrojos.

Los estándares de radio operaban en la banda de radio 2.4GHZ de la ISM (*Industrial, Scientific & Medical*), frecuencia abierta reconocida por las agencias reguladoras internacionales y por tanto de libre uso, asegurando así una buena compartición del espacio radioeléctrico con mínimas interferencias. Los estándares originales de 802.11 definían unas tasas de transmisión de 1Mbps y 2Mbps utilizando técnicas FHSS (*Frequency Hopping Spread Spectrum*) o DSSS (*Direct Sequence Spread Spectrum*), dos sistemas de señalización diferentes e incapaces de interoperar entre ellos: el mecanismo FHSS divide la banda de los 2.4GHz en 75 subcanales de 1MHz, mientras que el DSSS la divide en 14 canales de 22MHz.

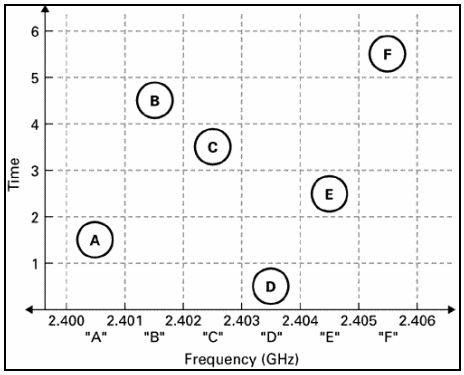


Figura 1-5: Técnica FHSS

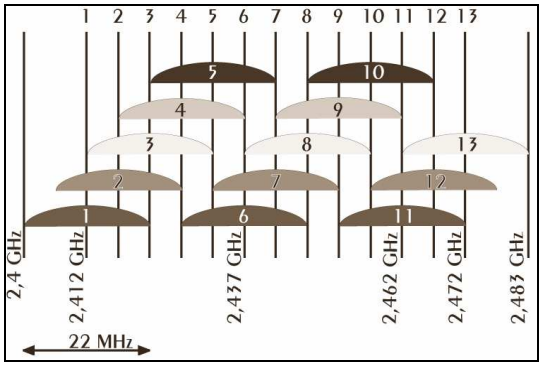


Figura 1-6: Técnica DSSS

3.2 La capa de enlace

El estándar 802.11 define dos subcapas dentro de la capa de enlace de datos: la *Logical Link Control* (LLC) y la *Media Access Control* (MAC). El estándar utiliza el mismo método de direccionamiento de 48 bits que el resto de redes locales 802, con lo cual es muy sencillo interconectar redes inalámbricas con redes cableadas del grupo de IEEE.

El control de acceso al medio (MAC) de la norma 802.11 es conceptualmente muy similar al utilizado en las redes Ethernet, el cual permite que diversos usuarios utilicen de forma concurrente un mismo medio de transmisión gracias a mecanismos de detección y evitado de colisiones:

En el caso de Ethernet (802.3) se utiliza el protocolo *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD), mientras en las redes inalámbricas basadas en 802.11 se utiliza una versión ligeramente modificada llamada *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) o bien el *Distributed Coordination Function* (DCF).

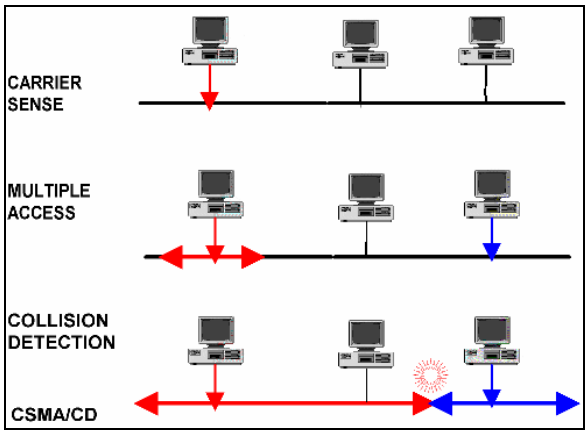


Figura 1-7: CSMA/CD de IEEE 802.3 (Ethernet)

El funcionamiento básico del protocolo CSMA/CA es el siguiente: cualquier estación que desee transmitir efectúa previamente un sondeo del medio. En caso de que no detecte actividad introduce un tiempo aleatorio de espera y posteriormente (siempre que siga sin haber actividad) comienza a transmitir. Si el paquete de datos es recibido correctamente por la estación receptora, esta envía un ACK (*Acknowledge*) que completa el proceso una vez recibido por el emisor. Por otro lado, si el emisor no recibe la señal de ACK ya sea porque el receptor no recibió el paquete de datos o bien porque el ACK no ha llegado correctamente, entonces se entiende que se ha producido una colisión y el paquete se vuelve a enviar después de esperar otro intervalo aleatorio de tiempo.

De esta manera el protocolo CSMA/CA permite compartir el acceso al medio aéreo, y gracias al mecanismo explícito de ACK es muy fácil gestionar los problemas relacionados con la transmisión de radio como por ejemplo las interferencias. Como contrapartida, este mecanismo añade una carga de gestión adicional que las redes ethernet no tienen, y por tanto, el rendimiento de las redes 802.11 siempre será menor que el de su equivalente 802.3 cableada.

Otro problema de la capa MAC específico de las redes inalámbricas es el problema del "nodo oculto", que describe el escenario en el cual dos estaciones ubicadas en lugares opuestos de un punto de acceso pueden escuchar actividad en el propio AP, pero no entre ellas (habitualmente debido a la propia distancia o a algún objeto que obstruya las ondas electromagnéticas). Para solucionar este problema la especificación 802.11 describe un protocolo opcional a nivel MAC llamado *Request to Send/Clear to Send* (RTS/CTS). Cuando se utiliza esta característica, la estación emisora transmite un RTS y espera a que el punto de acceso (AP) responda con un CTS. Como todas las estaciones de la red pueden escuchar al punto de acceso, el CTS provoca que el resto de estaciones retrasen sus propias transmisiones, lo que permite a la estación emisora enviar y recibir el ACK sin peligro de que se produzca una colisión. Generalmente este mecanismo de RTC/CTS se suele reservar para la transmisión de los paquetes más grandes, debido a que introduce una gestión adicional que penaliza sensiblemente el rendimiento general de la red.

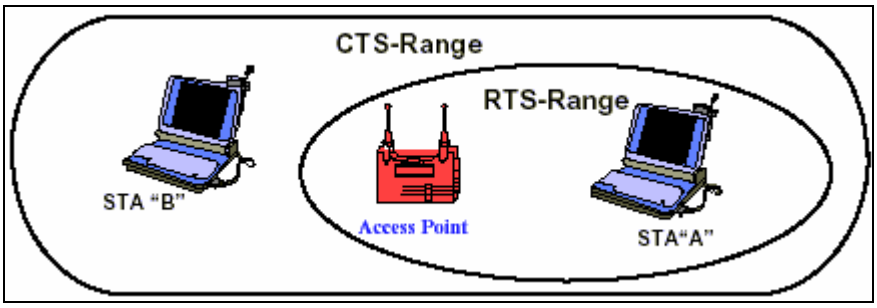


Figura 1-8: Mecanismo RTS/CTS de 802.11

Por último, la capa MAC de 802.11 proporciona dos mecanismos adicionales que aseguran la robustez en las transmisiones: el CRC *checksum* y la fragmentación de paquetes. Cada paquete que se forma dispone de un código CRC (Código de Redundancia Cíclica) que permite asegurar que los datos no se han corrompido durante la transmisión (esta característica es diferente a las redes ethernet, donde la gestión de errores la realizan los protocolos de nivel superior como TCP/IP). En cuanto a la fragmentación de paquetes, esta técnica permite romper paquetes grandes en diversos paquetes más pequeños, lo cual es muy útil en redes congestionadas o en las cuales hay un grado importante de interferencias y por tanto la probabilidad de que los paquetes grandes puedan corromperse es más elevada.

3.3 Transmisión de datos en tiempo real

Los datos sensibles al tiempo como la voz o el video están soportados en la especificación MAC de 802.11 a través de la Función de Coordinación de Puntos (PCF). Al contrario que en el DCF (donde el control está distribuido entre todas las estaciones), en modo PFC un único punto de acceso (AP) controla el acceso al medio. Si un BSS tiene activado el modo PCF, el tiempo queda enlazado entre el sistema configurado en PCF y el modo DCF (CSMA/CA). Durante los períodos en los cuales el sistema se encuentra en modo PCF, el punto de acceso consulta a cada una de las estaciones en busca de datos en intervalos de tiempo sucesivos, y de esta forma, ninguna estación está autorizada a enviar datos mientras no sea consultada por el AP. Por tanto, como el PCF le otorga a cada estación un turno para poder transmitir de forma predeterminada, el sistema adquiere una latencia máxima garantizada (aunque este sistema es muy ineficiente en grandes redes).

4. Estándares IEEE 802.11

Uno de los mayores problemas que han afectado a la demanda de redes inalámbricas ha sido siempre su ancho de banda limitado. Las tasas de transmisión soportadas originalmente por el estándar 802.11 eran demasiado bajas para dar servicio a la mayoría de servicios de las empresas, y por tanto, eran un factor que penalizaba la adopción de WLANs. Ante esta realidad palpable, el IEEE ratificó el estándar 802.11b (también conocido como 802.11 *High Rate*) que permitía transmisiones de hasta 11Mbps, al que siguieron dos estándares más como son el 802.11a y el 802.11g, cada uno de les cuales aportaba mejoras a la especificación original (el 802.11a apareció posteriormente al 802.11b aunque fue propuesto con anterioridad, debido a que el segundo era más fácil y rápido de implementar).

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Standard Ratified	Sep. 99	Sep 99	May 2003
Raw Data Rates	54 Mbps	11 Mbps	54 Mbps
Average Actual Throughput	4-5 Mbps	27 Mbps	20-25 Mbps(tbd)
Frequency	5 GHz	2.4 GHz	2.4 GHz
Available Spectrum	300 MHz	83.5 MHz	83.5 MHz
Modulation Encoding	OFDM	DSSS/CCK	DSSS/PBCC
# Channels/ non-overlapping	12/8	11/3	11/3

Figura 1-9: Tabla comparativa estándares 802.11

En los siguientes apartados se describen las características más importantes de cada uno de los nuevos estándares.

4.1 IEEE 802.11b

Gracias la especificación 802.11b, los usuarios móviles pudieron obtener niveles de rendimiento, velocidad y disponibilidad similares a los proporcionados por Ethernet. La arquitectura básica, características y servicios de esta nueva especificación estaban definidos en el propio 802.11 original y únicamente difería en la capa física, la cual añadía tasas de datos superiores (soportando velocidades de 5.5Mbps y 11Mbps) además de una conectividad más robusta.

Para cumplir con estas nuevas características se tuvo que seleccionar el método DSSS como única técnica de acceso físico, ya que el *frequency hopping* (FHSS) no podía soportar velocidades tan altas sin violar las regulaciones actuales de la FCC (*Federal Communications Commission*). El resultado es que los sistemas 802.11b pueden interoperar con sistemas DSSS 802.11 de 1 y 2Mbps, pero no con sistemas FHSS de la misma velocidad.

Cuando los dispositivos se sitúan fuera del alcance óptimo de trabajo a 11Mbps o bien existen interferencias, automáticamente emiten a velocidades inferiores que pueden variar entre los 5.5Mbps hasta 1Mbps. De igual forma al recuperar la cobertura o desaparecer las interferencias, la velocidad de transmisión vuelve a incrementarse a tasas superiores.

Finalmente, una de las principales desventajas de la norma 802.11b es que la banda de frecuencia que utiliza está muy saturada, y por tanto, está sujeta a interferencias por parte de otras tecnologías de red, hornos microondas, teléfonos inalámbricos en la banda de los 2.4GHz, o dispositivos Bluetooth por citar algunos ejemplos. Además, hay algunas restricciones que limitan a 802.11b, incluyendo falta de interoperabilidad con dispositivos de voz o de mecanismos de calidad de servicio (QoS) para proveer contenidos multimedia.

4.2 IEEE 802.11a

La especificación 802.11a (que apareció posteriormente a la 802.11b aunque fue propuesta con anterioridad) proporciona una velocidad mucho más elevada que su predecesora con una tasa máxima de 54Mbps operando en el rango de frecuencia de los 5GHz y permitiendo hasta 8 canales simultáneos.

802.11a utiliza un nuevo esquema de codificación llamado OFDM (*Orthogonal Frequency Division Multiplexing*) que ofrece ventajas en lo que se refiere a disponibilidad de canales y tasas de transmisión de datos (la disponibilidad de canales es un parámetro significativo porque cuantos más canales independientes haya disponibles, más escalable es la red inalámbrica). El 802.11a utiliza OFDM para definir un total de 8 canales de 20MHz sin solapamiento entre ellos a lo largo de 2 bandas (cuando el anterior 802.11b utilizaba únicamente 3 canales).

Todas las redes inalámbricas utilizan rangos del espectro de frecuencias no licenciados, con lo cual pueden sufrir interferencias y por tanto errores de transmisión. Para evitar estos errores, tanto 802.11a como 802.11b reaccionan reduciendo la tasa de transferencia a nivel de capa física (1, 2 y 5.5Mbps la norma 802.11b, y 48, 36, 24, 18, 12, 9 y 6Mbps en el caso de 802.11a). Pero la mayor tasa de transferencia no es la única ventaja de la especificación 802.11a, sino que también utiliza un rango de frecuencia más alto (5GHz), el cual es bastante más amplio y está menos saturado que la banda de los 2,4GHz y que (como se ha comentado anteriormente) utilizan otros dispositivos como teléfonos inalámbricos, microondas, dispositivos Bluetooth, etc.

Finalmente, una de las principales desventajas de la norma 802.11a es que no es directamente compatible con 802.11b, y por tanto, necesita de productos puente que puedan soportar ambos tipos de redes inalámbricas simultáneamente. Y además, curiosamente la especificación 802.11a solamente está disponible con la mitad de ancho de banda en Japón (es decir un máximo de 4 canales), ya que allí únicamente se puede utilizar la banda más baja.

4.3 IEEE 802.11g

El último de los estándares evolucionados de la norma IEEE 802.11 es el 802.11g.

Aunque la banda de frecuencia de los 5GHz ofrece múltiples ventajas también tiene problemas, el más importante de ellos la compatibilidad. Las diferentes frecuencias de trabajo de 802.11a y 802.11b implican que no puedan convivir, y para solucionar esta limitación, el IEEE desarrolló el estándar 802.11g con el objetivo de extender la velocidad y el alcance del 802.11b original, consiguiendo además que fuera compatible con los dispositivos y sistemas antiguos. El estándar opera íntegramente en la banda de los 2,4GHz y utiliza un mínimo de dos modos (ambos obligatorios) junto con dos modos adicionales opcionales. Los modos de acceso/modulación obligatorios son los mismos modos CCK (*Complementary Code Keying*) utilizados por 802.11b (de aquí la compatibilidad) y el modo OFDM (*Orthogonal Frequency Division Multiplexing*) utilizado por 802.11a (aunque en este caso en la frecuencia de los 2,4GHz). El modo obligatorio CCK soporta 11Mbps y el modo OFDM hasta un máximo de 54Mbps. Y por último, los dos modos opcionales restantes son el PBCC-22 (*Packet Binary Convolutional Coding*) con una tasa de 22Mbps, y el modo CCK-OFDM con una tasa máxima de 33Mbps.

La ventaja clara del estándar 802.11g es que mantiene la compatibilidad con el 802.11b (junto con su aceptación a nivel mundial) y además ofrece tasas de transferencia rápidas. No obstante, el número de canales no crece ya que éstos son función del ancho de banda y no de la modulación de la señal de radio (y en este aspecto el 802.11a gana con sus 8 canales respecto a los 3 disponibles tanto en 802.11b como en 802.11g). Y por último, otra de las desventajas de 802.11g es que también trabaja en la banda de los 2,4GHz, y por tanto, está sujeto a múltiples interferencias tal como le ocurría al 802.11b.

5. La seguridad en WiFi

Los sistemas de seguridad disponibles en WiFi son básicamente el WEP (*Wireless Equivalent Privacy*), el más reciente estándar 802.1x, el cual define una serie de métodos y técnicas que corrigen y mejoran las limitaciones de WEP (autenticación, encriptación e integridad de los datos), o la versión intermedia WPA (*WiFi Protected Access*).

5.1 Seguridad en IEEE 802.11

La especificación original 802.11 definía la autenticación, la encriptación y la integridad de los datos del tráfico inalámbrico.

- Autenticación:

  - *Open system authentication*: Identificación mediante la MAC del cliente.
  - *Shared Key authentication*: El cliente comparte una clave secreta con el punto de acceso.

- Encriptación e integridad:

  - WEP: Proporciona servicios de confidencialidad encriptando los datos entre los clientes y el punto de acceso (AP). La integridad de los datos se asegura mediante un valor de comprobación de integridad (ICV – *Integrity Check Value*) que se incluye en la porción encriptada de la trama. El WEP define 2 tipos de claves compartidas:

    - *Multicast/global key*: Es una clave de encriptación que protege el multicast y broadcast desde el punto de acceso hacia los clientes.
    - *Unicast session key*: Es una clave que protege el tráfico unicast entre el punto de acceso y el cliente.

La encriptación WEP utiliza el cifrado de flujo simétrico RC4 con claves de encriptación de 40 y 104 bits (aunque las claves de 104 bits no están especificadas en el estándar 802.11). Habitualmente, en WEP se habla de claves de 128 bits, que no es más que el resultado de añadir la clave de 104 bits con los 24 bits del vector de inicialización (IV – *Initialization Vector*). El IV es está en la cabecera de cada trama 802.11 que se utiliza durante el proceso de encriptación y desencriptación.

El principal problema del WEP es que la inicialización y distribución de las claves de encriptación no está definida, es decir, que las claves se tienen que distribuir a través de un canal “seguro” independiente, y configurarlas de forma manual en los dispositivos cliente. Por otro lado, tampoco existe un mecanismo automatizado para cambiar estas claves de forma periódica, cosa que las hace muy vulnerable ante un atacante que consiguiera una clave con métodos criptoanalíticos (situación posible ya que existen vulnerabilidades conocidas).

5.2 El estándar IEEE 802.1X

El estándar IEEE 802.1X define el control de acceso a la red basado en puerto, utilizado para proporcionar acceso de red autenticado en redes ethernet. El control de acceso utiliza las características de la infraestructura de redes locales conmutadas para autenticar los dispositivos conectados a un puerto. Aunque este estándar fue diseñado para redes ethernet cableadas, ha sido adaptado para ser aplicado también en redes 802.11.

El IEEE 802.1X define 4 figuras básicas:

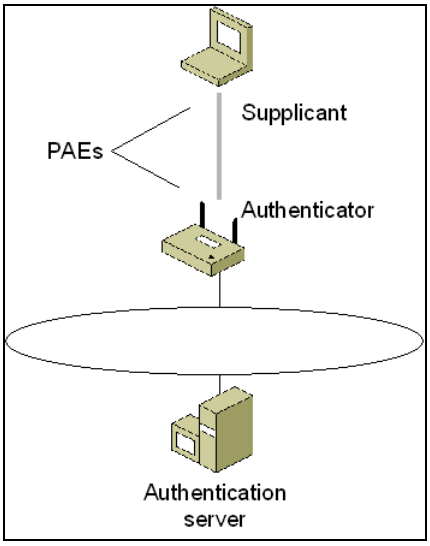


Figura 1-10: Figuras 802.1X

- Entidad de acceso al puerto (PAE – *Port Access Entity*): Equivalente a la figura de un puerto LAN.
- Autenticador (*Authenticator*): Puerto LAN que fuerza la autenticación del cliente antes de darle acceso a los servicios disponibles desde este puerto.
- Solicitante (*Supplicant*): Es el puerto LAN que solicita acceso a los servicios accesibles de la red.
- Servidor de autenticaciones (*Authentication server*). Es el servicio encargado de verificar las credenciales presentadas por el solicitante, y responder indicando si el acceso a los servicios de la red es aceptado o rechazado. Este servicio lo puede dar el propio punto de acceso (el cual tendrá una base de datos propia con credenciales de usuario), o bien un servidor dedicado externo como por ejemplo un servidor RADIUS (*Remote Authentication Dial-In User Service*).

El mecanismo estándar de autenticación del IEEE 802.1X es el EAP (*Extensible Authentication Protocol*), junto con su EAP-TLS que utiliza certificados de usuario basados en mecanismos de infraestructuras de clave pública (PKI), o el PEAP (*Protected EAP*) que utiliza autenticación PEAP-MS-CHAP v2.

5.3 WiFi Protected Access (WPA)

Aunque el 802.1X soluciona algunos de los problemas del 802.11 original, todavía existen vulnerabilidades en el método de encriptación WEP y la integridad de los datos. La solución definitiva a estos problemas llegará con el futuro estándar 802.11i, pero hasta entonces, los fabricantes han acordado un estándar intermedio conocido como WPA, el cual persigue los siguientes objetivos:

- Conseguir redes inalámbricas seguras. WPA requiere autenticación 802.1X, encriptación y gestión de claves *unicast* y globales.
- Solucionar los problemas de WEP mediante una actualización del software.
- Proporcionar una solución de red segura para entornos de oficinas pequeñas y (SOHO – *Small Office and HOme*), que a priori, no dispone de servidores RADIUS para llevar a cabo la 802.1X. En este caso, WPA.
- Ser totalmente compatible con el nuevo estándar 802.11i.
- El WPA define la autenticación, la encriptación y la integridad de los datos del tráfico inalámbrico.

- Autenticación:

- Con los dos estándares anteriores la autenticación era opcional mientras que con WPA es un requisito, y es una mezcla del *Open System* y de la autenticación 802.1X (con clave compartida PSK en caso de no disponer de RADIUS, o con EAP si se dispone).

- Encriptación:

- Con 802.1X, la renovación de claves *unicast* era opcional, y ni este ni el 802.11 proporcionaban mecanismos para cambiar la clave global. Con WPA, la renovación de tanto la clave *unicast* como la multicast (*rekeying*) es obligatoria. El TKIP cambia la clave en cada trama. WPA soporta como métodos de encriptación el TKIP (obligatorio) y el AES WPA.

- Integridad:

- Con el 802.11 y WEP, la integridad la proporciona un campo ICV de 32 bits añadidos a la trama. Con WPA se utiliza un método llamado MICHAEL que especifica un nuevo algoritmo más seguro y eficiente.

6. Principales competidoras de WiFi

Las dos principales competidoras de WiFi desde el punto de vista del presente estudio son las especificaciones HiperLAN2 y HomeRF.

- HiperLAN2

  HiperLAN2 es una tecnología LAN que opera en la banda de frecuencia libre de los 5GHz (de 5.4GHz a 5.7GHz). La tecnología fue desarrollada dentro del proyecto BRAN (*Broadband Radio Access Networks*) del *European Telecommunications Standardization Institute* (ETSI) con el objetivo de poder transportar células ATM, paquetes IP, paquetes *firewire*, y datos digitales de teléfonos móviles. Mientras que 802.11a es una especie de ethernet inalámbrica, HiperLAN2 es habitualmente conocida como la ATM inalámbrica.

HiperLAN2 está basada en enlaces orientados a conexión, aunque también puede aceptar tramas ethernet (protocolo sin conexión). El estándar 802.11a está optimizado para transmisión de datos, mientras que HiperLAN2 se ajusta mejor a contenidos multimedia inalámbricos gracias a su soporte integrado de calidad de servicio (QoS)

- HomeRF

  El HomeRF fue prácticamente la primera tecnología inalámbrica doméstica que se creó, y tomó forma a mediados de 2000. El nombre de la tecnología significa *Home Radio Frequency*, y utiliza ondas de radio para transmitir datos con un alcance de entre 20 y 40 metros. Utiliza SWAP (*Shared Wireless Access Protocol*), un estándar híbrido desarrollado a partir del 802.11 que permite la conexión de hasta 127 dispositivos de red con una velocidad de transmisión de 2Mbps. Esta velocidad limitada se convierte en una de sus mayores desventajas, que aún siendo suficiente para compartición de ficheros e impresión de archivos medianos, es insuficiente para transmitir información multimedia o ficheros pesados. Por otro lado, se trata de una solución barata y que no interfiere con Bluetooth.

La siguiente tabla sumariza las distintas tecnologías inalámbricas de transmisión de datos, junto con sus características principales y sus aplicaciones recomendadas:

Aplicación	Tecnología clave	Velocidad	Lo bueno	Lo malo
Networking empresarial	802.11	2 Mbps/ 1.2 Mbps	LAN inalámbrica	Lenta, cara y con poca seguridad
	802.11b	11 Mbps/5.5 Mbps	Más rápida, más barata y más robusta que el 802.11	La seguridad no es muy fiable. Interferencias.
	802.11g	54 Mbps	Más rápida que la anterior.	Compatibilidad. Interferencias.
Networking empresarial y WMAN	802.11a	54 Mbps	Rápida, más usuarios simultáneos, pocas interferencias.	Coste, menos rango de alcance y fácilmente obstruible
	HiperLAN/2	54 Mbps/24 Mbps	Sponsorizada por los grandes fabricantes. Soporta servicios orientados a conexión (p.e. voz)	Cara. Menor implantación frente a 802.11a
Networking doméstico	HomeRF	2 Mbps/1 Mbps (10Mbps HomeRF2)	Rápida y asequible para entornos domésticos	Poca implantación fuera del entorno doméstico.

Figura 1-11: Comparativa tecnologías WLAN

7. Aspectos legales

WiFi, al utilizar frecuencias del espectro radioeléctrico de libre uso, se debe ceñir a una reglamentación tanto por parte de las autoridades españolas como por parte de organismos superiores a nivel internacional competentes en asuntos de telecomunicaciones. Algunos aspectos que deben cumplir las señales utilizadas por WiFi incluyen parámetros como el uso, la potencia, el alcance, etc.

Los organismos reguladores del espectro radioeléctrico pueden clasificarse en función de su competencia geográfica:

- Organismos de ámbito mundial
  - ITU (*International Telecommunications Union*)
- Organismos de ámbito continental
  - CEPT (Conférence Européenne des administrations des Postes et des Télécommunications)
  - FCC (Federal Communications Commission)
- Organismos de ámbito nacional (España)
  - Ministerio de Ciencia y Tecnología, a través de la Secretaria de Estado para las Telecomunicaciones y la Sociedad de la Información.
  - Agencia Estatal de Radiocomunicaciones.
  - Comisión para el Mercado de las Telecomunicaciones (CMT)

8. Previsiones de futuro

Después de duras discusiones con intereses opuestos entre los miembros del IEEE, a principios de 2006 se aprobó un primer borrador de la nueva especificación 802.11n, que previsiblemente no estará finalizada hasta principios de 2007.

Los beneficios de 802.11n son muy considerables respecto a sus predecesores. El rendimiento esperado en los primeros productos a nivel de capa física alcanzarán los 300Mbps utilizando dos antenas, y con el tiempo podrá escalar hasta los 600Mbps utilizando cuatro. El ancho de banda real a nivel de aplicación se espera en 100Mbps, equivalente a los 100/10Base T de las redes ethernet. En el alcance de 802.11n también se espera un incremento de hasta un 50% mediante el uso de la tecnología de formación de emisión (*Beam Forming*) que enfoca la energía en una dirección concreta tanto en recepción como en emisión.

Por su parte, el uso de la tecnología STBC (*Space Time Block Coding*) reducirá la pérdida de señal mediante el uso de múltiples antenas por redundancia (esta tecnología en particular es clave para mejorar la percepción de los usuarios de VoIP).

Y finalmente, la agregación de paquetes y los protocolos de aceptación de bloque reducirán el consumo de energía y la colisión de datos en entornos de redes congestionadas mediante lo que se conoce como super-trama, utilizada para enviar múltiples paquetes a la vez.

En definitiva, la próxima generación de 802.11 será ideal para lo que se está llamando en la industria "*triple play service provision*", o lo que es lo mismo, voz, video y datos, y aunque a corto plazo no vaya a reemplazar a la Ethernet cableada en la empresa, para aquellas compañías que utilicen 100/10BaseT el nuevo 802.11n puede ser una alternativa más barata.

Capítulo 2 : Estudio sobre la tecnología VoIP.

1. Introducción

VoIP responde a las siglas de *Voice over Internet Protocol* (voz sobre protocolo de Internet). Como indican los términos, la tecnología VoIP busca transmitir la voz (básicamente la voz humana) a través de paquetes IP, y por extensión, a través de Internet. La VoIP puede utilizar hardware acelerador para conseguir sus objetivos y también puede ser utilizada en entornos de PC y dispositivos móviles de última generación (como por ejemplo asistentes de datos personales o PDAs).

En los inicios de las telecomunicaciones se descubrió que era posible enviar señales analógicas hacia destinos remotos también de forma digital: antes de enviarlas es necesario digitalizarlas con un ADC (*Analog to Digital Converter*), transmitirla a través de un medio adecuado, y finalmente volver a transformarla de nuevo a su formato analógico mediante un DAC (*Digital to Analog Converter*) para poder utilizarla. La VoIP funciona básicamente de esta manera, digitalizando las señales de voz en paquetes de datos, enviándolos a través de una red basada en IP, y reconvirtiéndola de nuevo a voz en su destino.

Los formatos digitales pueden ser controlados y tratados mucho más eficazmente que las señales analógicas. Es posible comprimirlos, enrutarlos, convertirlos a nuevos formatos mejorados, etc, además de que las señales digitales son más inmunes al ruido y a las interferencias que las analógicas, pudiendo detectarse e incluso corregirse valores recibidos incorrectamente. Las redes TCP/IP están formadas por paquetes IP que contienen una cabecera (para controlar la comunicación) y una carga para transportar datos. La VoIP utiliza esta carga para viajar transportar los datos por la red hasta llegar a su destino.

Figura 2-1: VoIP

Cuando se utiliza la red telefónica conmutada tradicional (PSTN) habitualmente la tarificación se realiza en base al tiempo total de uso de la línea. Además, la red telefónica básica no permite establecer conversaciones con más de una o dos personas de forma simultánea. Por el contrario, mediante la tecnología VoIP es posible hablar durante todo el tiempo deseado con una o diversas personas de forma simultánea (siempre que éstas se encuentren conectadas a la red en ese momento) y, aspecto muy importante, sin costes asociados a la duración de la conversación. Adicionalmente, y como una de las ventajas más atractivas a medio plazo, a la vez que se transmite voz se puede transmitir cualquier otro tipo de contenido multimedia como imagen, video, datos, mensajería instantánea, etc.

La pregunta que se plantea después de describir superficialmente todas las ventajas de la VoIP sobre las redes conmutadas de telefonía analógica tradicional es muy sencilla: ¿Por qué todavía no utiliza todo el mundo esta tecnología? La respuesta es que, a día de hoy, todavía existen algunos problemas para integrar la arquitectura de VoIP con Internet. Como es de suponer, la comunicación de voz debe ser un flujo de datos en tiempo real (no es viable hablar con una persona y tener que esperar varios segundos para que le llegue la señal y posteriormente recibir su respuesta). Este requisito va en contra de la arquitectura heterogénea de Internet, que está compuesta de multitud de enrutadores y caminos alternativos con tiempos de tránsito RTT (*Round Trip Time*) muy elevados, con lo cual evidentemente es necesario modificar algo para conseguir que la VoIP sobre Internet funcione correctamente. En general, el objetivo debe ser asegurar un ancho de banda y una calidad de servicio (QoS) suficiente para el tráfico de VoIP.

2. Tecnología VoIP

Para realizar una comunicación VoIP es necesario disponer de los siguientes elementos:

1. Conversor analógico a digital (ADC) para transformar las señales analógicas (voz) en digitales (bits).

2. Posteriormente los bits deben ser comprimidos en un formato adecuado para transmitirlos de forma eficiente (existen una serie de protocolos que se describen más adelante).

3. En este punto se deben insertar los paquetes de voz en paquetes de datos utilizando un protocolo de tiempo real (normalmente RTP sobre UDP sobre IP).

4. Se necesita un protocolo de señalización para llamar a los usuarios, como por ejemplo el ITU-T H323 o SIP.

5. En recepción será necesario desensamblar los paquetes, extraer los datos, y convertirlos de nuevo a su formato de señales de voz analógicas para enviarlas a la tarjeta de sonido (o auricular del teléfono).

6. Todo el proceso anterior debe ser llevado a cabo en tiempo real, ya que cualquier intervalo de espera no deseado en una conversación puede provocar que su calidad sea inaceptable.

Figura 2-2: Tecnología VoIP

2.1 Conversión analógica a digital

Esta conversión se realiza mediante hardware, habitualmente a través de un ADC integrado en el dispositivo.

Hoy en día cualquier tarjeta de sonido permite convertir a 16 bits una banda de 22050Hz (para muestrearla es necesaria una frecuencia de 44100Hz según el principio de Nyquist), obteniendo un throughput de 2 bytes * 44100 muestras por segundo = 88200 bytes/s (176.4 kBytes/s para una señal estéreo).

Para trabajar con VoIP no es ni mucho menos necesario un throughput de 176.4 kBytes/s con el que crear los paquetes de voz, con lo cual, la calidad de muestreo proporcionada por cualquier tarjeta de sonido del mercado es más que suficiente.

2.2 Algoritmos de compresión

Una vez se dispone de datos digitales es necesario convertirlos a un formato que pueda ser transmitido de forma eficiente. Los dos más interesantes son los siguientes:

- PCM (Pulse Code Modulation), Estándar ITU-T G.711
    - El ancho de banda de la voz es de 4 kHz, con lo que el ancho de banda del muestreo tiene que ser de 8 kHz (según criterio de Nyquist).
    - Cada muestra se presenta con 8 bits (teniendo 256 valores posibles).
    - El throughput es de 8000 Hz *8 bit = 64 kbit/s, igual que una línea de teléfono habitual.
    - En su aplicación real se utilizan las variantes mu-law (Norteamérica) y a-law (Europa), las cuales codifican las señales analógicas en una escala logarítmica utilizando 12 o 13 bits en vez de los 8 bits originales (ver Estándar ITU-T G.711).

- ADPCM (*Adaptive Differential PCM*), Estándar ITU-T G.726

  Convierte solo las diferencias entre el paquete de voz actual y el anterior, requiriendo 32 kbps (ver Estándar ITU-T G.726).

    - LD-CELP, Estándar ITU-T G.728
    - CS-ACELP, Estándar ITU-T G.729 y G.729a
    - MP-MLQ, Estándar ITU-T G.723.1, 6.3kbps, Truespeech
    - ACELP, Estándar ITU-T G.723.1, 5.3kbps, Truespeech
    - LPC-10, capaz de alcanzar los 2.5 kbps

Estos últimos protocolos son los más importantes porque garantizan una banda mínima muy baja utilizando codificación de origen. También los codecs G.723.1 tienen un MOS (*Mean Opinion Score*, utilizado para medir la fidelidad de la voz) muy alto, pero hay que tener en cuenta los requisitos de elaboración que necesitan que pueden llegar hasta los 26MIPS.

2.3 RTP (Real Time Transport Protocol)

Los paquetes de datos de VoIP se encapsulan en paquetes RTP (RFCs 1889 y 1890), que a su vez se encapsulan en paquetes UDP-IP.

Lo primero, VoIP no utiliza TCP porque es demasiado pesado para dar servicio a aplicaciones en tiempo real, con lo cual se utiliza UDP (datagramas) que es mucho más sencillo y ligero.

Segundo, UDP no lleva un control acerca del orden en el cual llegan los paquetes a su destino o cuanto tiempo tardan en hacerlo (concepto de datagrama). Ambos aspectos son muy importantes desde el punto de vista de la calidad de la voz (facilidad para entender lo que la otra persona está diciendo) y la calidad de la conversación (facilidad con la que se puede desarrollar la conversación). El protocolo RTP soluciona el problema permitiendo al receptor reordenar los paquetes en su secuencia original y descartando los paquetes que se hayan podido perder (evitando así esperas demasiado prolongadas) o estén tardando demasiado en llegar. No se necesitan todos y cada uno de los paquetes que codifican una cadena para que esta sea inteligible, pero sí que es necesario disponer de un flujo constante y ordenado.

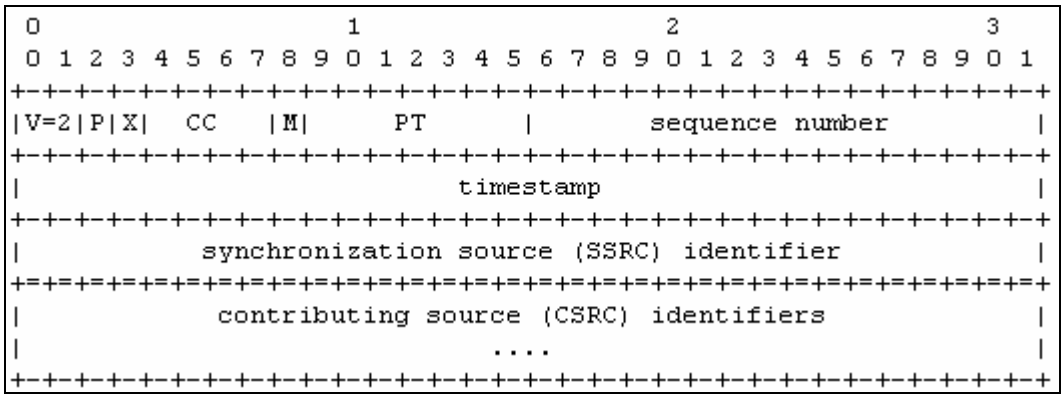


Figura 2-3: Paquete Real Time Protocol

2.4 Calida de servicio (QoS)

Como se ha comentado en anteriores apartados, las aplicaciones VoIP requieren un flujo de datos en tiempo real debido a que se espera un intercambio interactivo de datos durante las conversaciones. Desafortunadamente, el protocolo TCP/IP no puede garantizar este tipo de propósito, únicamente hace lo que puede (*best effort*) para conseguirlo. Por lo tanto, y ha falta de mecanismos definitivos para hacerlo, es necesario utilizar algunos trucos o políticas que permitan manejar el flujo de paquetes a través de cada uno de los enrutadores que atraviesen.

Algunos de las estrategias utilizadas son las siguientes:

1. El campo TOS del protocolo IP para describir el tipo de servicio al cual pertenece el paquete de datos. Los valores altos indican poca urgencia, mientras que los valores bajos indican mayor urgencia en tiempo real.

2. Métodos de encolado de paquetes:

    a. FIFO (*First in First Out*), el método más sencillo que permite pasar a los paquetes siguiendo el mismo orden de llegada.
    b. WFQ (*Weighted Fair Queuing*), consiste en un pase racional de paquetes (por ejemplo, al FTP no se le permite consumir la totalidad del ancho de banda disponible) dependiendo del tipo de flujo de datos, habitualmente un paquete UDP y uno TCP de forma equitativa.
    c. CQ (*Custom Queuing*), los usuarios pueden decidir la prioridad.
    d. PQ (*Priority Queuing*), hay un número (habitualmente 4) de colas cada una de las cuales con una prioridad: primero se envían los paquetes de la primera cola, y cuando esta está vacía, se continúan enviando los de la segunda cola, y así sucesivamente.
    e. CB-WFQ (*Class Based Weighted Fair Queuing*), igual que en el caso del WFQ pero, además, incluye en concepto de clases (hasta 64) y el valor de ancho de banda asociada a cada una.

3. Capacidad de *shaping*, que permite limitar al emisor en un ancho de banda fijado en descarga y en subida.

4. Mecanismos de evitado de colisión, como RED (*Random Early Detection*).

2.5 El protocolo de señalización H323

El protocolo H323 es una definición robusta y largamente utilizada que permite la intercomunicación entre una gran variedad de dispositivos.

1. Terminales cliente que inician conexiones VoIP. Aunque los terminales pueden hablar directamente entre ellos sin más, es necesario disponer de elementos adicionales para dotarles de una visión escalable.

2. Porteros *(Gatekeepers)*, cuya función básica es llevar a cabo los siguientes servicios:
    a. Traducción de direcciones, para utilizar nombres simbólicos en vez de direcciones IP.
    b. Control de admisión, para permitir o denegar el uso a dispositivos y usuarios.
    c. Gestión de ancho de banda.

3. Pasarelas (*gateways*), puntos de referencia para conversiones TCP/IP – PSTN (voz IP y red telefónica conmutada básica).

4. Unidades de control multipunto (MCU) para permitir conferencias múltiples.

5. Servidores *Proxy*.

El protocolo de señalización H323 no solo sirve para servicios VoIP, sino que también se puede utilizar en comunicaciones de video y de datos. En lo que se refiere a VoIP, el H323 puede soportar codecs de audio G.711, G.722, G.723, G.728 y G.729, mientras que en el caso de video soporta h261 y h263.

2.6 El protocolo SIP

Internet y las comunicaciones móviles han calado profundamente tanto en el entorno profesional a gran escala como en el ámbito doméstico. El uso de aplicaciones de mensajería instantánea se está incrementando año tras año, y en este escenario, el protocolo SIP (*Session Initiation Protocol*) juega un papel fundamental.

Analizando el estado actual de las telecomunicaciones se puede observar como lentamente se está pasando de disponer de redes separadas para voz y datos, a tener una única red convergida para todos los tipos de comunicación. Prácticamente todas las aplicaciones multimedia son directamente utilizables sobre infraestructuras estándares basadas en tecnología IP (cada una con sus limitaciones o matices), incluyendo dispositivos fijos y móviles. El protocolo SIP permite equipar de forma definitiva a las plataformas para este nuevo subsistema multimedia IP (IMS).

El protocolo SIP es un protocolo reciente de nivel de aplicación definido como estándar en el RFC 3261, y desarrollado dentro del ETF (*Internet Engineering Task Force*) MMUSIC (*Multiparty Multimedia Session Control*) como una alternativa al H323. Se trata de un protocolo de señalización petición-respuesta para establecer e iniciar sesiones de voz, video y mensajería instantánea a través de Internet. No obstante, SIP es independiente de los detalles de la sesión (entendiendo las sesiones como un grupo de emisores y receptores que se intercomunican, junto con el estado en el que se encuentran los extremos durante la comunicación). Por tanto, el protocolo SIP no incluye todos los elementos necesarios para una comunicación completa entre usuarios sino que únicamente la hace posible (la comunicación se consigue por otros medios), y tampoco es un protocolo de descripción de sesión (SDP, que describe y codifica las capacidades de los participantes en la sesión) ni proporciona control de conferencias. La principal ventaja de este hecho es que es compatible con diferentes arquitecturas y escenarios de servicios de Internet.

La principal función del protocolo SIP es la de ayudar a los iniciadores a distribuir invitaciones a los potenciales participantes en la sesión, independientemente de dónde se encuentren. Para conseguir este propósito SIP utiliza una amplia variedad de protocolos (p.e. SOAP, HTTP, XML, VXML, WSDL, o SDP), cada uno de los cuales está encaminado a dar solución a diferentes aspectos. Además, SIP controla el funcionamiento de MGCP y MEGACO. Algunas funciones específicas son las siguientes:

- Traducción de nombres y localización de usuarios. Asegura que los interlocutores está localizado y la llamada les llega correctamente.
- Negociación de características. Gestiona los acuerdos mediante los cuales se establecen las características soportadas por el grupo involucrado en la llamada (chat, audio, video, etc).
- Gestión de participantes en la llamada. El usuario puede agregar a otros usuarios en la llamada, ponerlos en espera o cancelar su participación mientras la sesión está activa.

- Cambios en las características de la llamada. Permite al usuario cambiar las características de la llamada en curso, como por ejemplo otorgar la posibilidad de usar únicamente voz para un usuario, y otorgar el uso de voz y vídeo para otro usuario diferente durante la misma sesión.
- SIP también aporta otras capacidades interesantes como la encriptación y la seguridad.

SIP incluye diversas entidades, cada una con una función diferente:

1. *SIP Terminal*
   Soporta la comunicación bidireccional y en tiempo real con otras entidades SIP.

2. *SIP User Agent*
   Son los puntos finales de la llamada. El software de agente de usuario conmuta entre los modos UAC y UAS en base a los mensajes, dependiendo de si es el emisor o el receptor de una llamada. Pueden ser teléfonos o aplicaciones de escritorio.

   a. *User Agent Client (UAC)*
      Es el agente que inicia la llamada.

   b. *User Agent Server (UAS)*
      Es el agente que recibe la llamada. Esta entidad puede recibir y responder llamadas de SIP, y puede aceptarlas, rechazarlas o redirigirlas.

3. *SIP Network Server*
   Este dispositivo gestiona la señalización asociada con múltiples llamadas y permite que se establezcan llamadas de igual a igual (*peer-to-peer*) utilizando un protocolo cliente servidor. Su principal función es proporcionar resolución de nombres y localización de usuarios, además de pasar los mensajes a otros servidores utilizando protocolos de siguiente salto (*next-hop*).

   a. Proxy Server
      Son equipos de red que actúan tanto de clientes como de servidores para otras entidades. Su función es asegurar que las peticiones son enrutadas hacia la entidad apropiada identificada por su URI (*SIP Uniform Resource Identifier*). Los servidores *proxy* pueden operar en dos modos distintos:

      1. *IP stateful Proxy Server*
         Recuerdan las peticiones entrantes que reciben y las respuestas que envían.

      2. *SIP stateless Proxy server*
         “Olvidan” la información una vez enviada.

   b. Redirect Server
      Reciben las peticiones SIP y envían la respuesta a las direcciones adecuadas.

   c. Registrar Server.
      Aceptan peticiones de registro. Estos servidores mantienen la base de datos que contienen la información de todos los agentes de usuario

registrados con un dominio SIP particular, permitiendo por tanto a los usuario actualizar su localización y su información de políticas.

4. Back-to-Back User Agents
   El B2BUA es una combinación de UAC y UAS que mantiene información del estado del diálogo y participa en todas las solicitudes enviadas.

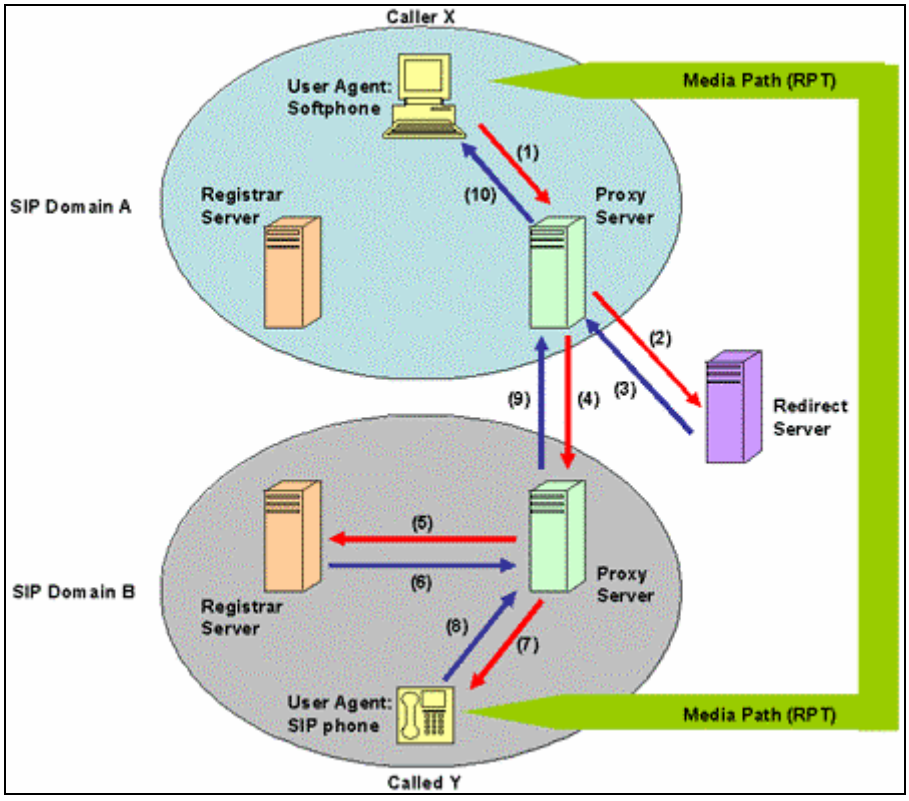


Figura 2-4: SIP Sesión SIP en diferentes dominios

En definitiva, SIP capacita a los diferentes fabricantes de la industria de la VoIP diseñar productos de telefonía interoperables. Los usuarios pueden utilizar una centralita PBX (*Private Brach Exchange*) IP de un fabricante, una pasarela de otro, y un teléfono de un tercero con la seguridad de que todos los elementos trabajarán perfectamente entre ellos. El protocolo SIP está reemplazando rápidamente al H323 en el terreno de la VoIP.

3. Aspectos legales

El problema al que se enfrenta el desarrollo de la VoIP para usuarios finales en España es de definición del propio servicio, es decir, si se puede considerar telefonía o no. La Comisión del Mercado de las Telecomunicaciones (CMT) lo ha diferenciado, y el Gobierno lo ha denominado "servicio vocal nómada con capacidad multimedia". El principal operador de telecomunicaciones de España (Telefónica) está de acuerdo con esta distinción, mientras que el resto del sector (los competidores de Telefónica) sostiene todo lo contrario.

Las operadoras de telefonía están sujetas a una regulación que las obliga, entre otras cosas, a la ofrecer servicios como el acceso a números de emergencia (112), garantizar unos niveles de calidad, la interconexión o la portabilidad del número. Además, al existir un operador dominante (Telefónica), hay reglas específicas que intentan garantizar la libre competencia, como el llamado *price cap* (sistema económico establecido por la autoridad competente que regula los precios máximos de las tarifas anuales de empresas en vías de privatización) o la supervisión constante de ofertas y precios por parte de la CMT.

Si la Voz sobre IP no se considera telefonía (sino un mero servicio de comunicaciones electrónicas) esto implica que el servicio tiene que cumplir con menos requisitos.

El Ministerio de Industria, Turismo y Comercio ha presentado al Consejo Asesor de las Telecomunicaciones el borrador de resolución por el que se atribuyen recursos de numeración para los servicios de telefonía sobre IP. En el borrador de la Resolución se atribuyen dos rangos de numeración para la prestación de servicios VoIP: un rango de numeración específica (prefijo 51) y otro rango de numeración geográfica (prefijo 8). El Ministerio ha concluido que este segundo rango (el 8) va a ser compartido por el servicio telefónico fijo tradicional y una modalidad de los nuevos servicios nómadas. De esta manera, los casi 7 millones de números geográficos atribuidos a los servicios de VoIP en el rango 8 tendrán limitado su ámbito de nomadismo al distrito telefónico donde resida el abonado. Para ambos tipos de numeración, específica y geográfica, se exige a los operadores el encaminamiento gratuito de las llamadas al centro de atención de emergencias 112.

Según el borrador de Industria, los planes nacionales de numeración deben proporcionar los recursos públicos de numeración necesarios para permitir la prestación efectiva de todos los servicios. Además, indica que los rangos de numeración en los que se preste la telefonía IP deben permitir el suministro de características adicionales al servicio telefónico, entre ellas “el nomadismo”, es decir, que el usuario pueda utilizar estos servicios independientemente de su ubicación geográfica.

4. Previsiones de futuro

Según previsiones de la firma de análisis *Gartner*, especialista en consultorías del ámbito de la tecnología, el sistema tradicional de telefonía disminuirá considerablemente de aquí a 2008, mientras que en el mismo periodo, las comunicaciones IP aumentarán en un 38 por ciento. Igualmente, un informe presentado recientemente por el Grupo CDW sobre la VoIP en España indica que esta tecnología “robará” a la telefonía fija entre 1.570 y 2.230 millones de minutos (alrededor de 40 millones de horas de conversación) a lo largo de este año, lo que permitirá a los españoles ahorrar hasta 150 millones de euros en llamadas de larga distancia (provinciales, interprovinciales e internacionales).

La tecnología VoIP ha crecido de la nada hasta llegar a una industria multimillonaria en cuestión de apenas un lustro, y la mayoría de expertos predicen que hacia el año 2015 entre el 35 y el 50% del mercado global de telefonía utilizará tecnología VoIP. Por tanto, la VoIP tiene asegurado un futuro brillante que promete continuar creciendo de forma espectacular en un futuro cercano.

Por otro lado, con cada vez más compañías de desarrollo de software implicadas en el mercado de la VoIP, la tecnología se está recreando a sí misma a pasos forzados. Se cree que el futuro de la VoIP es lo que se ha venido a llamar VoIP 2.0, visión que se encuentra enfocada más hacia los servicios que no solo hacia el simple ahorro de costes (objetivo inicial más importante de la VoIP). Compañías como Google, Microsoft o sobretodo Skype no paran de ofrecer cada vez más servicios relacionados con VoIP de forma gratuita, y se prevé que llegará un día no muy lejano en el que probablemente se verán forzadas a “cobrar” por ellos, ya sea de forma directa (cobro por el servicio) o indirecta (publicidad).

Gracias a la nueva generación VoIP 2.0 los usuarios no solo podrán hacer llamadas telefónicas gratuitas o muy baratas, sino que también podrán experimentar accesos a la información hasta ahora desconocidos (voz, video, texto, correo electrónico, mensajería instantánea, etc), desde cualquier ubicación (casa, hotel, aeropuerto, terraza de un bar, etc), y desde cualquier dispositivo (teléfono móvil, PDA, ordenador portátil, etc).

Capítulo 3 : VoWiFi

1. Introducción

VoWiFi responde a la fusión de las siglas de *Voice over Internet Protocol* (voz sobre protocolo de Internet) y WiFi.

La unión de las tecnologías WiFi y VoIP con toda seguridad se impondrá como la telefonía móvil del futuro. VoWiFi es una tecnología híbrida que aprovecha lo mejor de cada uno de sus componentes: WiFi le aporta la libertad de las comunicaciones sin hilos y el ahorro de costes en infraestructura de cableado, y VoIP le aporta la convergencia sobre IP con la consecuente reducción de costes en telecomunicaciones. Además, la banda de transmisión de WiFi permite un potencial de llamadas superior al de un dispositivo base-estación tradicional DECT (*Digital Enhanced Cordless Telecommunications*) que limita el alcance entre el terminal y la base mientras que WiFi permite mucha más libertad de movimientos.

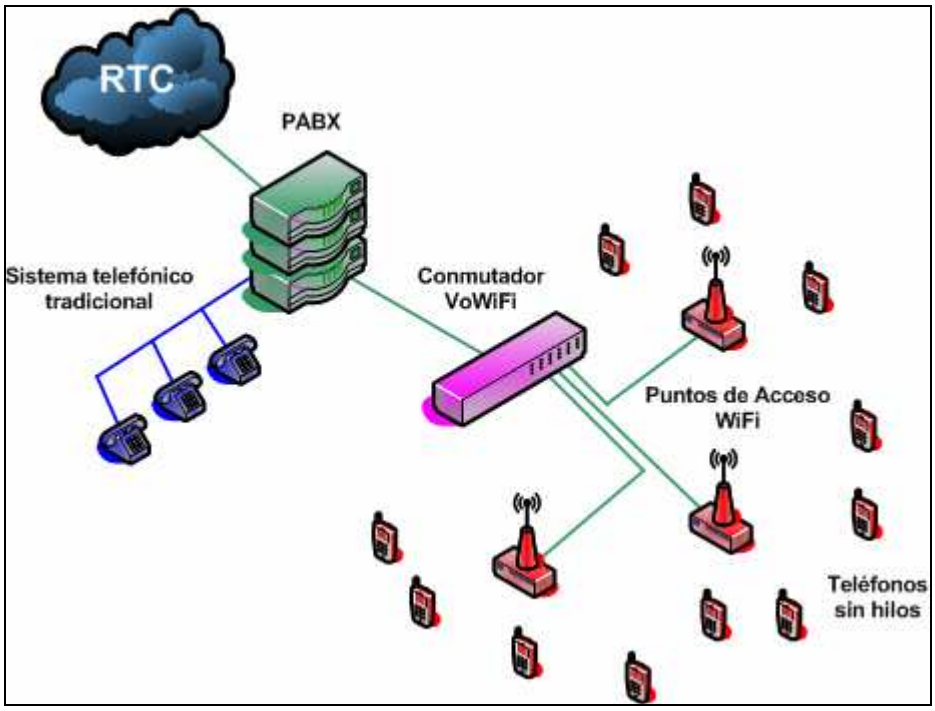


Figura 3-1: Arquitectura de un sistema VoWiFi

VoWiFi explota los mismos mecanismos y protocolos que VoIP (H323 y SIP), pero no utiliza en cambio los procedimientos de servicios diferenciados de QoS (*Diffserv*) o de reserva de flujo RSVP (*Resource Reservation Protocol*) ya que WiFi concede la misma prioridad de acceso a todos los recursos (es decir, no dispone de mecanismos de QoS). Para suplir esta limitación el IEEE trabaja sobre una alternativa a la norma 802.11 que definirá clases de servicios con el fin de trabajar con prioridades.

La definición 802.11k se propone optimizar la asignación de los recursos de la red inalámbrica según la calidad de la conexión. Cada terminal cliente informará a su punto de acceso de sus características de conexión, y en función de esta información, éstos le asignarán los recursos adecuados para garantizar su buen funcionamiento y la disponibilidad de esa conexión en concreto. Por su lado, el 802.11r se propone optimizar el mecanismo de *roaming* (salto de célula) en las transiciones entre un punto de acceso y otro (por ejemplo en el caso que el terminal se encuentre en movimiento).

Los primeros productos VoWiFi están basados en una versión pre-estándar. Dos de los fabricantes pioneros en sacar al mercado productos de infraestructura VoWiFi son Cisco y Alcatel, que completan su oferta con la de multitud de fabricantes que comercializan teléfonos inalámbricos IP.

2. Ventajas e inconvenientes de VoWiFi

Con la gran proliferación de redes inalámbricas WiFi para transmisión de datos entre ordenadores, muchas de las empresas que actualmente ya disponen de esta tecnología se encuentran actualmente en proceso de añadir capacidades de voz, aprovechando de esta forma el ahorro de costes y las mejoras en la productividad que aporta el hecho de no tener que establecer una infraestructura de red separada para las comunicaciones de voz.

La sensación de los responsables de IT de las grandes corporaciones es que VoWiFi es una tecnología de futuro que permite preparase para los avances que sufrirá el mercado. La idea fundamental es que aunque VoWiFi (tal como se conoce hoy en día) puede ser una fantástica plataforma para el futuro, todavía se trata de una tecnología joven que se encuentra en pleno proceso de maduración y desarrollo. Por tanto, parece ser que la implementación actual de VoWiFi todavía no está preparada para poder reemplazar a otras plataformas tecnológicas, especialmente en áreas como la seguridad y la fiabilidad. Si embargo, sí que se ve como una plataforma a partir de la cual mejorar los estándares y continuar su maduración.

La existencia de una única infraestructura inalámbrica es ya de por sí una buena razón para que las empresas se decidan por la tecnología VoWiFi por encima de una red de voz dedicada, pero como tecnología reciente que es, estas organizaciones deben sopesar los pros y los contras de ser *early adopters* (pioneros en el uso). Independientemente del potencial de VoWiFi, la decisión de si desplegar el sistema de comunicación de voz basado en esta nueva tecnología o en cambio utilizar tecnologías habituales no está clara. En los siguientes apartados se lleva a cabo un análisis de los principales aspectos a tener en cuenta antes de tomar este tipo de decisiones.

2.1 Mejoras en los estándares VoWiFi

Cuando se presentaron los primeros estándares inalámbricos a principios de los 90 con velocidades de 2Mbps, las tasas de transmisión eran demasiado bajas para poder dar servicio a niveles empresariales. Con la aparición de la especificación 802.11b estas tasas se incrementaron considerablemente hasta los 11Mbps, cosa que contribuyó a una rápida adopción del uso de redes inalámbricas en las empresas para transmisión de datos. Y más recientemente, las tasas de transmisión de 54Mbps que soporta el estándar 802.11g todavía han contribuido más a la rápida implantación de puntos de acceso WiFi en entornos empresariales, y ya comienza a ser viable la posibilidad de añadir tráfico de voz a la misma infraestructura inalámbrica de datos.

Mientras que las organizaciones pueden estar gastando gran cantidad de recursos en migrar sus infraestructuras de 802.11b a 802.11g para aumentar la velocidad de conexión de las aplicaciones, la vedad es que la industria de voz inalámbrica prácticamente solo tiene dispositivos de voz 802.11b (11Mbps). Esta restricción en los dispositivos de voz (teléfonos) significa que aunque la red soporte velocidades 802.11g (54Mbps), los puntos de acceso trabajarán automáticamente en modo 802.11b en lo que se refiere a voz. Además de suplir las limitaciones de velocidad en los dispositivos de voz, los fabricantes se encuentran a la espera de que la industria de solución a otras barreras importantes antes de invertir de forma contundente en productos VoWiFi:

1. Calidad de servicio (QoS). Rendimiento de voz inconsistente o llamadas interrumpidas.

2. Seguridad. Encriptación y autenticación lenta y poco fiable.

3. Interoperabilidad. La naturaleza propietaria de algunos de los productos de los fabricantes.

Los principales protagonistas de la industria, incluyendo el IEEE y la Wi-Fi Alliance, están hoy en día desarrollando mejoras en los estándares para dar solución a estas barreras. Por ejemplo, el estándar 802.11i (ratificado en Junio de 2004) implementa una autenticación y una seguridad mejoradas, o el estándar 802.11e (aprobado en Septiembre de 2005) define medidas de calidad de servicio (QoS) para priorizar el tráfico de voz respecto el otro tipo de tráfico en la red. Los nuevos estándares asignan a las aplicaciones de tiempo real (incluyendo voz i video) una mayor prioridad sobre las aplicaciones de transmisión de datos, como pueden ser las simples transferencias de ficheros. En la actualidad los pioneros en el uso de WiFi no tienen más opción que confiar en métodos de QoS de terceros, con lo cual se crean claros problemas de interoperabilidad. El nuevo estándar 802.11e justamente acaba de establecer las normas de QoS que asegurarán los niveles de compatibilidad entre los distintos fabricantes.

2.2 Administración y mantenimiento

Normalmente los sistemas de voz tradicionales cableados son mantenidos por profesionales especializados casi siempre externos a la compañía que los utiliza (como por ejemplo los técnicos expertos en centralitas). En cambio, los sistemas VoWiFi acaban siendo mantenidos en un alto porcentaje por el departamento de IT de la propia empresa, con lo cual, los roles asignados a cada grupo de profesionales dentro de la compañía acaba siendo un factor muy importante a la hora de decidir entre implementar un sistema de comunicaciones de voz tradicional o un sistema VoWiFi. Hoy por hoy, los sistemas de voz tradicionales son bastante más fiables y fáciles de mantener y no llevan asociada la preocupación de que otros dispositivos puedan afectar a la infraestructura, y por tanto, son mucho más estables y requieren menos horas de mantenimiento una vez instalados.

A medida que se añaden nuevos dispositivos IP a la red VoWiFi, como ordenadores portátiles o PDAs, es necesario reajustar la arquitectura de red y su capacidad con puntos de acceso adicionales, con lo cual la tarea de mantenimiento es muy importante. El hecho de unificar la administración de la red de datos con la red de voz en un único departamento (departamento de IT) puede ser en sí una ventaja para algunas empresas, con el ahorro de costes que representa en cuanto al coste total de propiedad del sistema.

2.3 Costes

Los sistemas de comunicación de voz tradicionales necesitan una red separada para la transmisión de las señales, mientras que VoWiFi utiliza la misma red de datos WLAN que da servicio al tráfico de los equipos informáticos y sus aplicaciones. Si una organización ya dispone de una red de datos inalámbrica, en ese caso también dispone de la infraestructura troncal para soportar VoWiFi. No obstante, aún teniendo ya una red WiFi pueden ser necesarios algunos ajustes como por ejemplo asegurar que la capacidad de la red es suficiente y que no existen zonas oscuras sin cobertura que puedan provocar cortes en las llamadas.

Existe una percepción errónea bastante común que consiste en pensar que siempre es más barato instalar un sistema VoWiFi en una WLAN existente que un sistema de voz tradicional, porque en este caso únicamente es necesario comprar los terminales IP de voz y unos pocos puntos de acceso adicionales. En realidad esto no siempre es así, ya que es necesario desarrollar una auditoria con el objetivo de asegurar que la WLAN está bien dimensionada y soportará la carga y la cantidad de datos adicionales que generarán las aplicaciones de voz.

La firma internacional de consultoría y análisis tecnológico Gartner estima que una WLAN que deba soportar voz cuesta aproximadamente el doble que una WLAN que vaya a soportar únicamente datos, debido al mayor número de puntos de acceso necesarios para asumir ambos tipos de tráfico. El soporte de voz obliga a que no haya puntos negros de cobertura, mientras que en una red únicamente de datos las “lagunas” de cobertura no son tan críticas.

2.4 Seguridad

Al tratarse de una tecnología madura y disponer de una infraestructura dedicada, los sistemas de voz tradicionales proporcionan un alto grado de seguridad además de tener pocas posibilidades de sufrir “ataques”.

A día de hoy, los pioneros en el uso de VoWiFi tienen que basarse en sistemas propietarios para gestionar la seguridad cuando se implementa una red de voz y datos. El nuevo estándar 802.11i establece las nuevas reglas de seguridad con la introducción de WPA2 (*WiFi Protected Access 2*). La adopción de este nuevo estándar establecerá una línea de base para la seguridad con mejoras considerables esperadas durante mucho tiempo. Aunque a día de hoy se han llevado a cabo mejoras significativas en cuanto a la seguridad disponible en entornos VoWiFi, la verdad es que todavía son susceptibles ante los *hackers* y los virus informáticos.

2.5 Escalabilidad

Los sistemas tradicionales de voz tienen una capacidad de crecimiento prácticamente ilimitada, teóricamente al igual que los sistemas VoWiFi con la adición de sistemas de pasarela (*gateways*). Aunque los sistemas VoWiFi no tienen límite en el número de dispositivos soportados a lo largo de la empresa, el número de puntos de acceso (AP) puede verse limitado en áreas muy saturadas, que puede traducirse en imposibilidad de establecer llamadas o en llamadas interrumpidas. Por lo tanto, es estrictamente necesario llevar a cabo una consultoría previa para determinar las áreas de cobertura y la capacidad requerida antes de elegir entre una solución de voz en cada situación específica.

Figura 3-2: Teléfono móvil VoWiFi

Uno de los grandes retos que actualmente se está planteando entorno a la tecnología de transmisión de voz IP sobre redes inalámbricas gira entorno al llamado *roaming*, o que la capacidad de que los teléfonos y dispositivos de usuario puedan intercambiar su conexión entre redes WiFi y redes celulares tradicionales (GSM o UMTS) cuando el aparato se encuentre fuera de cobertura WiFi (lo que se está dando en llamar teléfonos *dual-mode*), y que muchos fabricantes ya están ofreciendo en el mercado en forma de teléfonos híbridos (aunque todavía no exista una posibilidad técnica clara de sacarles partido).

3. Convergencia de servicios

Con la integración en una misma red de la transmisión de datos y de voz, utilizando la misma infraestructura física, lógica, protocolos, e incluso dispositivos, la evolución inmediata de la tecnología lleva hacia la integración de servicios que hasta ahora se consideraban heterogéneos e independientes, como pueden ser los datos, la voz, el video, el correo electrónico, la mensajería instantánea, las aplicaciones web, etc.

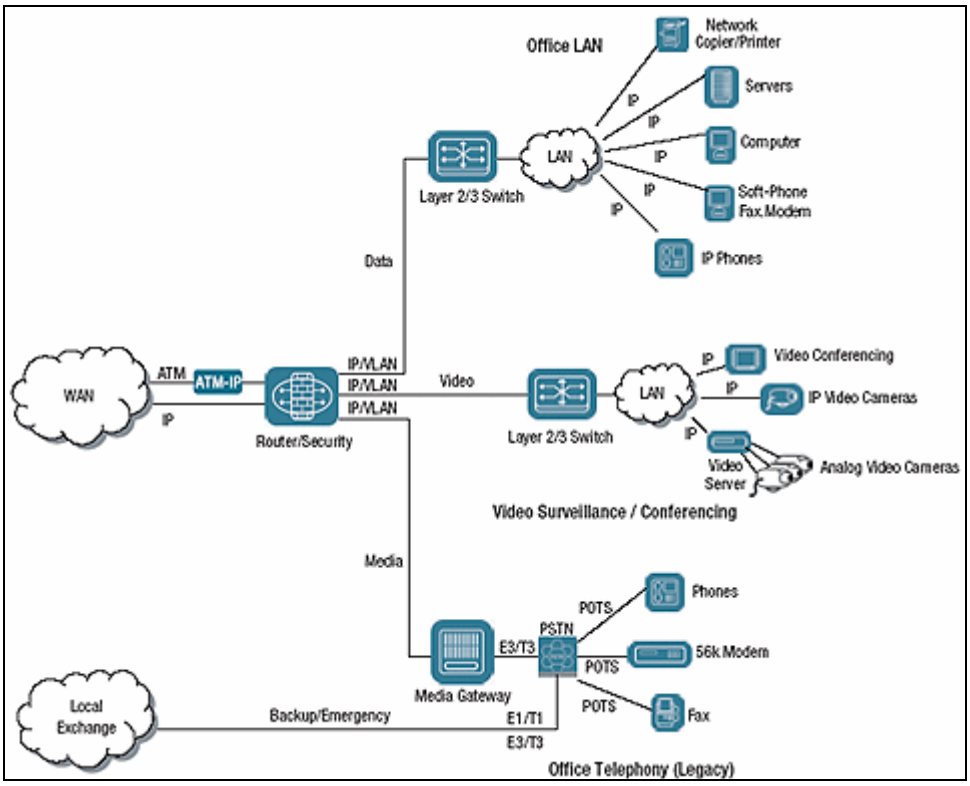


Figura 3-3: Convergencia de servicios en redes IP

Algunos de los retos que según los analistas deberán afrontar las empresas durante los próximos meses se basan los siguientes aspectos:

1. Las promesas que habían lanzado sobre las aplicaciones VoIP deberán ser cumplidas.

   El mercado empresarial ha apostado por las comunicaciones VoIP para eliminar costes en llamadas y reducir costes en infraestructura, pero sin duda los mayores beneficios de las comunicaciones convergidas y la transformación de los procesos de negocio siguen sin haberse conseguido. Las empresas piden que las aplicaciones VoIP aprovechen sus inversiones en comunicaciones IP integrando la voz con las aplicaciones empresariales y el contenido, no solo a nivel de centro de llamadas (*call center*) sino a lo largo de todo el negocio.

2. Convergencia

   Implementando los estándares y los protocolos asociados, las empresas llevarán a cabo avances rápidos hacia una única red (red IP) para transportar múltiples tipos de tráfico como voz, datos, y video. La convergencia aporta múltiples beneficios a las empresas y a los usuarios de la tecnología, incluyendo reducciones en los costes de operación y en el coste total de propiedad (*Total Cost of Ownership* - TCO).

3. Colaboración, presencia y mensajería instantánea.

   Estas soluciones típicamente han sido servicios externalizados, pero a partir de 2006 y en adelante se está produciendo un impulso muy importante para llevar estas soluciones hacia el interior de las propias empresas (por ejemplo, WebEx o AOL IM son soluciones externalizadas). La convergencia de servicios proporcionará una vía para que los clientes consoliden sus redes y lleven sus soluciones de voz, datos y video hacia sus redes internas seguras. Durante los próximos cuatro o cinco años se prevé que las compañías converjan sus redes y desplieguen aplicaciones de valor añadido como por ejemplo servicios avanzados de colaboración. Aquellos responsables de TI que en su día se mostraron reacios a adoptar telefonía IP probablemente se verán obligados a contemplar los valores que aporta la convergencia a sus organizaciones.

4. Mensajería unificada

   Se incrementará la confianza en las comunicaciones unificadas y las soluciones de colaboración serán útiles para la productividad organizacional y de los empleados, ayudarán a optimizar las comunicaciones empresariales, y mejorará las relaciones con los clientes (danto acceso a los trabajadores a cualquier tipo de mensaje, ya sea de voz, de datos, fax, video, chat, etc).

5. Preocupación por los virus en teléfonos móviles, PDAs y SmartPhones

   El despliegue masivo e incontrolado de PDAs y SmartPhones derivará en un problema de seguridad con el tiempo. Los problemas alrededor de la movilidad tienen que ser afrontados con diligencia, ya que actualmente no se ha dedicado el esfuerzo que seguramente merece.

6. La mensajería instantánea (IM) y el intercambio P2P (*Peer-to-peer*) se convertirá en un gran dolor de cabeza

   La adopción masiva y continuada de la IM y el P2P expondrá a las organizaciones a nuevas amenazas. Las empresas se verán obligadas a controlar y asegurar estas tecnologías que pueden llegar a ser disruptivas para el rendimiento tanto de las infraestructuras como de la productividad de sus trabajadores.

4. La mensajería instantánea

No es difícil predecir hacia donde apunta el futuro de la mensajería instantánea. Está claro que la IM es el punto de inflexión perfecto para los proveedores de telecomunicaciones tradicionales. Si se realiza un pequeño análisis de los proveedores actuales de comunicaciones móviles, muchos de ellos ni siquiera disponen de la identidad de sus usuarios finales (como por ejemplo es el caso de los usuarios de teléfonos móviles con tarjetas prepago) como en cambio sí tienen empresas proveedoras de IM como MSN, AOL, yahoo, skype, etc. Echando un vistazo a los esquemas de direccionamiento de los usuarios finales, el futuro es poder identificarlos por su identidad y no por su número de teléfono como se ha hecho hasta ahora, gracias a la rápida penetración de Internet y la banda ancha en el ámbito doméstico.

De alguna forma, se puede decir que los proveedores de mensajería instantánea actuales se podrían acabar convirtiendo en un equivalente de las compañías telefónicas, los cuales ofrecerán servicios de portadora que incluirán cada vez más servicios de valor añadido y de interconectividad entre sistemas heterogéneos. Es probable que en el futuro las compañías de acceso a Internet suplan totalmente a las compañías exclusivamente telefónicas, ofreciendo junto con el acceso a Internet servicios de telefonía de calidad, correo de voz, videoconferencia, conectividad con mensajería instantánea de cualquier otro proveedor (MSN Messenger, yahoo, google, skype, AOL, etc), espacio para almacenar archivos, fotos personales, documentos, blogs, páginas web, etc.

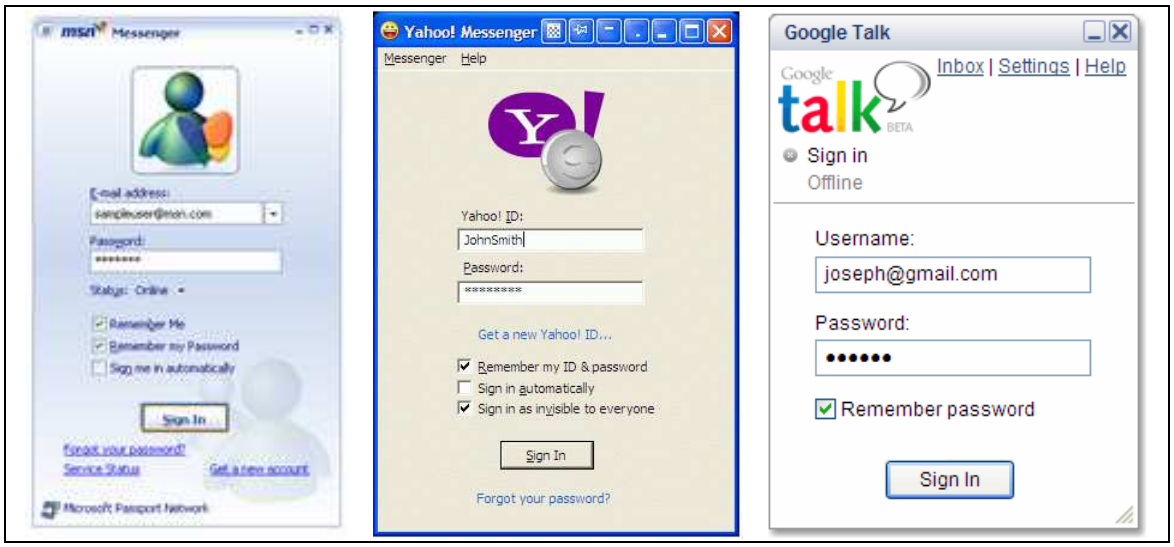


Figura 3-4: Aplicaciones públicas de Mensajería Instantánea

En cuanto a la implantación de la IM a nivel empresarial, día tras día está ganando en popularidad gracias a que cada vez se aprecian más los beneficios de utilizar IM en vez del correo electrónico o el correo de voz (mientras que la IM es instantánea y por tanto en tiempo real, el correo electrónico y los buzones de voz no dejan de ser servicios *offline*). La mensajería instantánea permite revolucionar las comunicaciones gracias a las posibilidades que ofrece en cuanto a compartición de datos y colaboración remota, haciendo estas actividades mucho más productivas (por ejemplo

permite llevar a cabo reuniones virtuales entre interlocutores situados en distintos puntos del mundo, compartir documentos en tiempo real, compartir escritorios de trabajo, etc).

Según los analistas el uso de IM a nivel empresarial está creciendo aproximadamente un 20% anual, y se estima que a finales de 2004 ya se utilizaba en un 70% de todas las compañías norteamericanas. Como dato interesante, durante el año 2005 la mensajería instantánea superó definitivamente al correo electrónico como medio principal de colaboración en tiempo real. Un caso concreto: en la multinacional IBM, el 77% de los empleados aseguran que la IM ha cambiado su forma de comunicarse, disminuyendo el tiempo que deben invertir con el correo electrónico y el correo de voz, en el teléfono, y en reuniones presenciales.

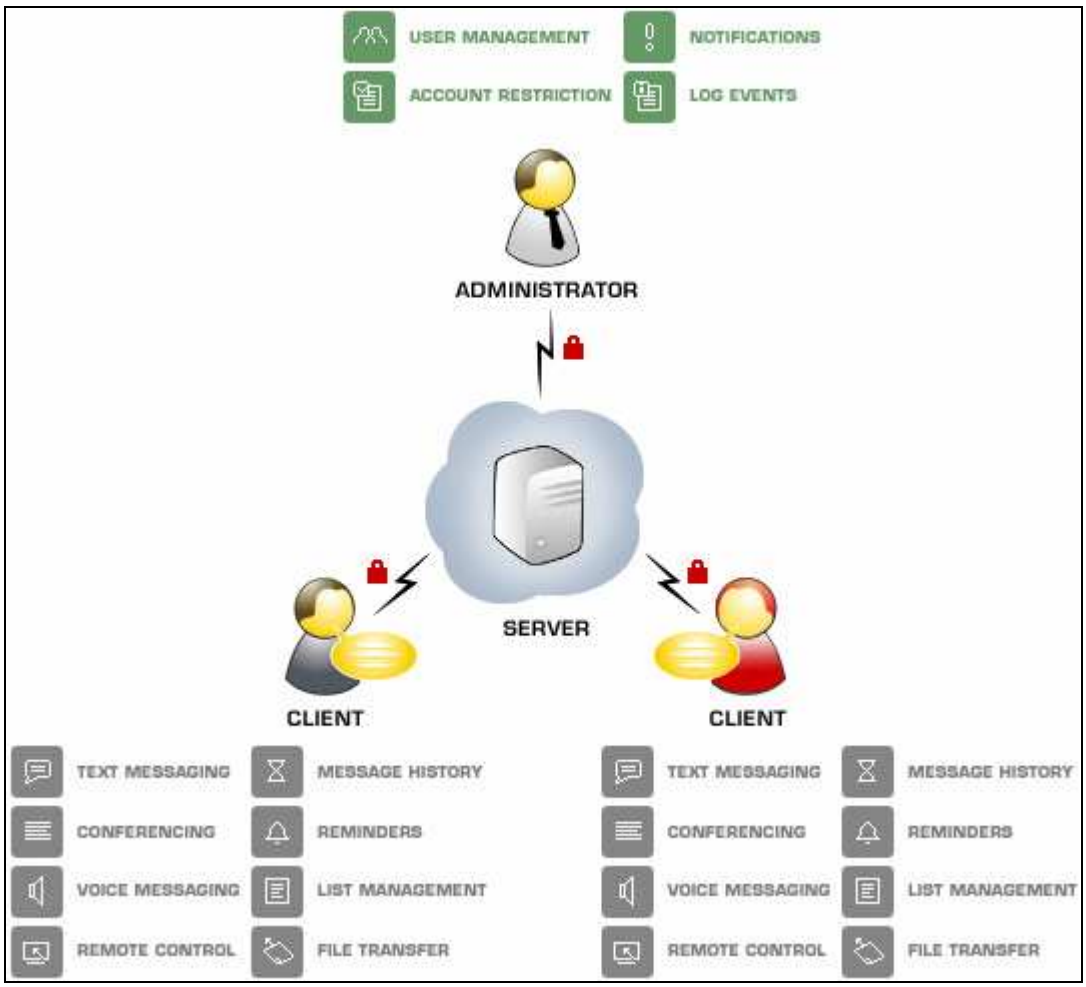


Figura 3-5: Mensajería Instantánea

El futuro de la IM permitirá llevar las comunicaciones a nuevos contextos, en los cuales los nombres de las personas involucradas en un documento, archivo de audio, video, o cualquier otro tipo de fichero, aparecerán en el propio documento como enlaces “vivos”. De esta forma, será posible pasar el cursor sobre el link, comprobar si el autor está en línea o no, y si es así, iniciar una conversación (voz o chat) en tiempo real directamente con esa persona independientemente de donde se encuentre. Esta colaboración contextual puede ser extendida a socios, proveedores, o clientes finales a criterio de las empresas, con lo cual abre un espectro de posibilidades muy interesantes.

Finalmente, los analistas consideran que para asegurar que la mensajería instantánea alcance su máximo potencial es necesario dar solución definitiva a tres factores determinantes:

1. Interoperabilidad.

Este concepto se refiere a la capacidad de que diferentes sistemas puedan comunicarse entre sí. Hasta ahora esto ha sido un problema para los usuarios debido a que las principales aplicaciones de mensajería se financian a través de la publicidad, y por tanto tienen que ser propietarias para crear valor añadido que haga aumentar su uso (y por tanto sus ingresos). Esta restricción “artificial” va en contra de lo que predica la IM, y que precisamente incrementa su valor con cada nuevo usuario que se añade a la red. Por tanto, uno de los retos de la mensajería instantánea es ir hacia plataformas abiertas y transparentes, sin importar que software o sistema operativo se esté utilizando, de forma que un usuario de MSN Messenger pueda consultar si otro usuario de Google Talk se encuentra conectado, y establecer una comunicación de forma ágil y directa.

2. Seguridad.

Cuando se habla de seguridad la mensajería instantánea se convierte en un problema de igual que en el caso del correo electrónico. Muchas empresas intentan añadir encriptación a sus servicios de mensajería instantánea, aunque este problema sea solo la punta del iceberg. Para proporcionar una buena seguridad, las aplicaciones de mensajería instantánea deberían autenticar a los usuarios confirmando su identidad contra una fuente de confianza como por ejemplo un directorio corporativo, de forma que un usuario siempre sepa que la persona con la que está interactuando es quien realmente dice ser.

3. Selección de comunidad.

Relacionado con la seguridad aparece la idea de la selección de comunidad. Las aplicaciones de mensajería instantánea deben proporcionar a las empresas la flexibilidad de elegir la comunidad de personas que va a ser incluida en la red. Estas pueden incluir a todo el mundo de una empresa colaboradora, un grupo de clientes, o individuos claves en compañías suministradoras. El poder de selección aumenta sensiblemente la seguridad, pero debe ser fácil de gestionar y tiene que funcionar de forma transparente.

En definitiva, es importante tener en cuenta dos aspectos en relación con la IM actual y futura. La primera es que todas las posibilidades ya son viables desde el punto de vista tecnológico. La segunda es que, si existe algún obstáculo, es debido a la imposibilidad de que la industria de TI se ponga de acuerdo en los estándares abiertos necesarios para hacer de la IM un éxito completo.

4. Aplicaciones Open Source

En los apartados anteriores se han descrito de forma básica los principales elementos que conforman una solución de VoWiFi y mensajería instantánea clásica.

Como parte fundamental de los objetivos del proyecto se incluye un estudio de las herramientas de código abierto (*open source*) disponibles actualmente en el panorama de Internet y que permiten implementar los distintos módulos necesarios de las plataformas VoWiFi e IM. El resultado del estudio puede observarse en los siguientes apartados.

4.1 Sistema operativo

El sistema operativo *open source* por excelencia es obviamente Linux, y por tanto, será linux el sistema seleccionado como plataforma de instalación de los módulos correspondientes a la parte de servidor (tanto la parte de centralita telefónica IP como el propio servidor de mensajería instantánea).

Una de las preguntas habituales a la hora de elegir una compilación de Linux es cuál de ellas escoger. La respuesta a la pregunta admite tantas respuestas como interlocutores, con lo cual la conclusión final acaba siendo que la compilación a utilizar puede ser la que cada administrador prefiera.

De la interminable multitud de compilaciones de Linux disponibles en la red, las más extendidas como servidores para instalar los servicios de VoWiFi y mensajería instantánea probablemente sean las siguientes:

- Debian Gnu/Linux (http://www.debian.org)
- Fedora Project (http://fedora.redhat.com)
- Suse Linux (http://www.suse.org)
- CentOS (http://www.centos.org)

Figura 3-6: Principales distribuciones de Linux

De entre todas las anteriores posiblemente sorprenda la presencia de una compilación bastante desconocida como es CentOS, basada en el código de Red Hat Enterprise Edition y que pretende ser una versión de Linux *Enterprise* totalmente gratuita y soportada por la propia comunidad de usuarios (al contrario que la versión *Enterprise* de Red Hat que ya no es una compilación de libre distribución ni gratuita).

Por todos estos motivos, el sistema operativo seleccionado para llevar a cabo la instalación en laboratorio será CentOS.

4.2 Centralitas telefónicas digitales

No ha pasado mucho tiempo desde que las telecomunicaciones, tanto de voz como de datos, formaban parte de productos propiedad del selecto club de compañías que crearon la tecnología, y por otro lado había un segundo club de compañías que utilizaba los productos para proporcionar servicios a los usuarios finales. A principios de lo 90 las telecomunicaciones se abrieron gracias a la explosión de Internet, los precios cayeron, y multitud de nuevas compañías y servicios emergieron a la luz mientras aparecía el concepto de software libre gracias al cual los programadores colaboraban en el desarrollo desinteresado de aplicaciones útiles para la comunidad global. No obstante, las comunicaciones de voz (a pesar de estar presentes prácticamente en todos los puntos del planeta) siguieron siendo propietarias en forma de centralitas telefónicas cerradas y con un altísimo coste tanto de adquisición como de mantenimiento.

Esta situación se solucionó con la aparición de diversos proyectos de software libre el objetivo de los cuales era implementar centralitas telefónicas IP basadas en software libre, y que con la ayuda de los periféricos adecuados en forma de tarjetas de interconexión con las redes tradicionales, permitían sustituir las caras centralitas telefónicas tipo “caja negra” por centralitas digitales abiertas y gratuitas.

En la actualidad, los proyectos de desarrollo de centralitas digitales *open source* más prestigiosos son los siguientes:

- Asterisk (http://www.asterisk.org).
- SIPfoundry (http://www.sipfoundry.org).
- OpenPBX (http://www.openpbx.org).
- Open IP PBX / OpenH323Gatekeeper (http://sourceforge.net/projects/openippbx).
- SkypeJi (http://sourceforge.net/projects/skypeji/).

De todos los proyectos indudablemente el que más aceptación ha tenido entre la comunidad tecnológica es Asterisk. Se trata de la implementación de una PBX completa mediante software, y puede instalarse directamente sobre Linux, BSD o MacOSX. Asterisk proporciona tecnología VoIP mediante diversos protocolos y además puede interoperar con prácticamente cualquier equipo de telefonía basado en estándares utilizando un hardware de muy bajo coste. Algunas de sus características más interesantes incluyen servicios de buzón de voz con directorio de usuarios, llamadas en modo conferencia, contestador automático, cola de llamadas, llamada a tres, identificación de llamada, ADSI, SIP o H323 (tanto cliente como pasarela).

Figura 3-7: Asterisk

Por todos estos motivos, la plataforma de centralita digital IP seleccionada para llevar a cabo la instalación en laboratorio es Asterisk.

4.3 Servidores de mensajería instantánea

En lo que se refiere a servidores de mensajería instantánea (IM) de código abierto, hoy por hoy no se pueden encontrar muchas alternativas, siendo básicamente dos las propuestas más extendidas entre la comunidad *open source*: por un lado se encuentra el servidor Jabber en calidad de líder, y como alternativa está Wildfire, la versión *open source* del servidor comercial de mensajería instantánea de la compañía Jivesoftware y que también está basada en Jabber.

- Jabber (http://www.jabber.org).
- Wildfire (http://www.jivesoftware.org).
- IServerd (http://iserverd.khstu.ru).

Jabber es una alternativa abierta, segura y gratuita para los servicios de mensajería instantánea actuales como AIM, ICQ, MSN o Yahoo. Técnicamente, Jabber es una compilación de protocolos y tecnologías de flujo de tráfico XML que permiten a dos entidades conectadas a la red intercambiar mensajes, información de presencia y otros tipos de información estructurada prácticamente en tiempo real. Además, Jabber ofrece algunas otras ventajas clave como pueden ser:

1. Abierto. Los protocolos Jabber son libres, abiertos, públicos y fácilmente comprensibles. Además, existen múltiples implementaciones de clientes, servidores, componentes, y librerías de código que permiten añadir de forma sencilla nuevas funcionalidades y servicios.

2. Estándar. El organismo IETF (*Internet Engineering Task Force*) ha formalizado los protocolos troncales de transmisión de flujo XML como tecnología de mensajería instantánea y presencia aprobada bajo el nombre de XMPP (*Extensible Messaging and Presence Protocol*), cuyas especificaciones han sido publicadas en los RFC 3920 y RFC 3921.

3. Estable. Las primeras tecnologías Jabber fueron desarrolladas en 1998, y actualmente existen cientos de desarrolladores trabajando con ellas, decenas de miles de servidores Jabber funcionando en Internet, y millones de personas utilizando Jabber para su mensajería instantánea.

4. Descentralizado. La arquitectura de la red Jabber es similar a la del correo electrónico.

5. Seguro. Cualquier servidor Jabber puede ser aislado de la red pública de Jabber (por ejemplo en la red de intranet de una compañía). Además, en las especificaciones troncales XMPP se ha incluido una seguridad robusta basada en el uso de SASL (*Simple Authentication and Security Layer*) y TLS (*Transport Layer Security*).

6. Extensible. Aprovechando la potencia de los espacios de nombre XML, cualquiera puede añadir funcionalidades personalizadas sobre los protocolos básicos. Para mantener la interoperabilidad, las extensiones comunes son gestionadas por la *Jabber Software Foundation*.

7. Flexible. Las aplicaciones basadas en Jabber, más allá de la mensajería instantánea incluyen gestión de red, sindicación de contenidos, herramientas de colaboración, compartición de ficheros, juegos, y monitorización remota de sistemas.

Figura 3-8: Servidor de IM Jabber

Por todos estos motivos, la tecnología de servidor de mensajería instantánea seleccionada para llevar a cabo la instalación en laboratorio es Jabber, en su versión Wildfire Jabber Server.

4.4 Clientes de VoIP

Técnicamente cualquier aplicación que implemente el protocolo SIP (*Session Initiation Protocol*) o cualquier otro protocolo de iniciación de sesión a nivel de cliente (p.e. H323) puede utilizarse como cliente de VoIP. En el caso del escenario *open source* pueden encontrarse cientos de posibilidades. En la siguiente tabla se enumeran alguna de las opciones disponibles para cada sistema operativo:

Nombre	Descripción	Win.	Linux	Mac
Cockatoo			x	
Ekiga	Softphone SIP, H.323 audio y video		x	
FreeSWITCH		x	x	x
Kphone			x	
Linphone			x	
minisip			x	
MjUA	Softphone SIP multiplataforma sencillo, escrito en java y basado en el snack MjSip	x	x	
OpenWengo	Un softphone completo multiplataforma con diversas funcionalidades.	x	x	
OpenZoep	Teléfono GPL y motor de cliente de IM	x	x	
PhoneGaim		x	x	
pjsua	Pequeña consola basada en UA SIP con sonido, RTP/RTCP, SIMPLE, etc.	x	x	x
SIP Communicator	Softphone basado en Java	x	x	x
SFLphone	Cliente VoIP open source multiplataforma y multiprotocolo.		x	
Shtoom	Softphone SIP escrito en Python	x	x	x
sipXezPhone	De SIPfoundry, basado en sipXtapi	x	x	
sipXphone	De SIPfoundry, anteriormente conocido como Pingtel.	x	x	
Twinkle			x	
X-Lite	Sin duda el mejor teléfono VoIP software	x	x	x
YATE	Teléfono multiprotocolo y multiplataforma.	x	x	

Probablemente X-Lite sea el *Softphone* cliente de VoIP libre más completo del mercado. Sus principales características incluyen tecla de mute, rellamada, grabación de llamadas, desvío de llamadas, conferencia, videoconferencia, agenda personal, gestión de ancho de banda, gran diversidad de codecs, cancelación de eco, gestión de pérdida de paquetes, reducción de ruidos, seguridad, temporizadores, etc. con lo cual se trata de una de las aplicaciones libres más completas disponibles actualmente.

En base a la gran diversidad de ventajas que incorpora este teléfono VoIP libre, el cliente VoIP seleccionado para llevar a cabo la instalación en laboratorio es la aplicación X-Lite (http://www.xten.net).

Figura 3-9: Softphone VoIP X-Lite de CounterPath

4.4 Clientes de mensajería instantánea

En la actualidad existen literalmente cientos de clientes Jabber, dado que en teoría cualquier cliente que pueda trabajar con el estándar XMPP puede utilizarse para conectar con un servidor Jabber. La siguiente lista, sin ánimo de ser exhaustiva, describe algunos de los principales clientes para los distintos sistemas operativos:

Nombre	Descripción	Win.	Linux	Mac
Cocinella	Tiene pizarra compartida. Software Libre. Gratuito.	x	x	x
Exodus	Muy popular y potente. Software Libre. Gratuito.	x		
Gajim	Software Libre. Gratuito.	x	x	
Gossip	Para entornos GNOME2, muy orientado hacia el usuario final. Software Libre. Gratuito.		x	
Jabbin	Cliente libre desarrollado a partir de Psi.	x	x	x
JAJC	Código cerrado. Gratuito.	x		
Neos	Muy orientado hacia usuarios de Windows, sobre todo XP. Soporte videoconferencia, pizarra y un mini-navegador. Código cerrado. Gratuito.	x		
Pandion	Diseño muy agradable. Código compartido. Anteriormente conocido como Rhymbox. Gratuito.	x		
Psi	Apariencia muy sencilla y vistosa. Software Libre.	x	x	x
Tkabber	Muy potente y configurable. Software Libre. Gratuito.	x	x	x

En vista de la gran cantidad de clientes disponibles, para la instalación en laboratorio se ha seleccionado uno de los más extendidos entre la comunidad de Internet como es Coccinella, está disponible para la mayoría de sistemas operativos del mercado, e incluye funcionalidades adicionales interesantes como por ejemplo:

- Transferencia de ficheros.
- Sistema de plug-ins (reproducción de audio e imágenes).
- Chat en grupo.
- Emoticones y avatares.
- Multilenguaje.
- Conexiones seguras (TLS y SASL).
- Protocolo de mensajería instantánea abierto estándar (Jabber/XMPP).
- Pizarra compartida integrada.

Figura 3-10: Cliente IM Coccinella

Capítulo 4 : Aplicación práctica: Plataforma VoWiFi & IM

1. Introducción

Una vez descritos los conceptos tecnológicos sobre los cuales se fundamenta la tecnología VoWiFi y la IM (Mensajería Instantánea) por un lado, y recopilados los proyectos de código abierto y las aplicaciones libres que permiten implementarlas de forma gratuita por otro, el último paso es diseñar, instalar y configurar una pequeña plataforma real en un entorno de laboratorio, con el objetivo de probar que la integración de las soluciones VoWiFi con los servicios de mensajería instantánea ya es posible hoy día utilizando aplicaciones de código abierto.

2. Descripción general del laboratorio

Para implementar la plataforma de pruebas se dispone de un entorno de laboratorio formado por diversos elementos físicos. La descripción básica de cada uno de los dispositivos es la siguiente:

2.1 Infraestructura de red

La red WiFi está soportada por un punto de acceso Router 3Com ADSL WiFi 802.11g, que permite conexiones WiFi de 54Mbps y hasta 4 conexiones Ethernet 10/100Mbps.

Figura 4-1: Router 3Com WiFi

2.2 Infraestructura de servidores y clientes

Para llevar a cabo la instalación de los elementos servidores y de los clientes se dispone de un total de 3 equipos informáticos con las siguientes características:

- Ordenador clónico Intel Pentium 4 Hyper Threading 1GB RAM, conexión Ethernet 100Mbps.

  En este equipo se instala el sistema operativo Linux CentOS más las aplicaciones Asterisk@Home y el servidor Jabber Wildfire.

- 2x Ordenador portátil IBM ThinkPad T42 Intel Pentium 600MHz 1GB RAM, conexión 802.11g WiFi.

  En estos equipos se instalan los clientes de VoIP X-Lite y de mensajería instantánea Coccinella.

Figura 4-2: IBM Thinkpad T42

3. Arquitectura de la plataforma

La arquitectura instalada en el laboratorio es muy sencilla, e incluye los elementos mínimos para implementar un servicio de VoWiFi y mensajería instantánea integrada.

Los elementos que la componen junto con su configuración básica se puede observar en el siguiente gráfico:

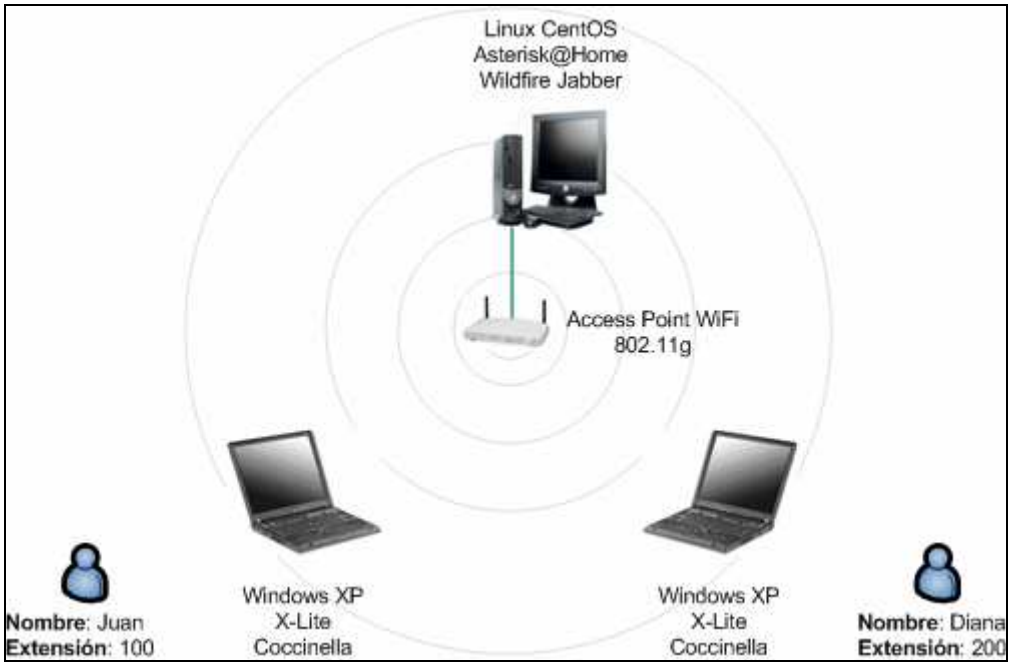


Figura 4-3: Arquitectura de la plataforma de laboratorio

Las características de recursos hardware de los equipos son las clásicas en equipos actuales, y en todos los casos son más que suficientes para la instalación de las respectivas aplicaciones y servicios en un entorno de validación en laboratorio.

4. Configuración de componentes Hardware

4.1 Infraestructura WiFi

La configuración del punto de acceso WiFi es la siguiente:

Red WiFi	803.11g
Canal	8
SSID	uoc-lab
SSID Broadcast?	No
Encriptación	WPA-PSK
Técnica de encriptación	TKIP
Pre-shared Key (PSK)	fdrq3q8uew87cwnhuweHJHEW324c21CWEV%&435
Servidor DHCP	Activado

Las tarjetas 803.11g de las estaciones cliente han sido configuradas manualmente para conectar con la red WiFi del laboratorio, habiéndoles proporcionado el SSID y la clave PSK correctas. El propio punto de acceso proporciona direcciones IP del rango 192.168.1.x/24 a las estaciones cliente mediante DHCP.

5. Configuración de componentes Software

5.1 CentOS

Se realiza una instalación del sistema operativo CentOS con sus opciones por defecto, teniendo en cuenta que se trata de un entorno de laboratorio, y por tanto, no es necesario personalizarla u optimizarla para una situación concreta (cosa que sí debería hacerse en caso de tratarse de una instalación de producción).

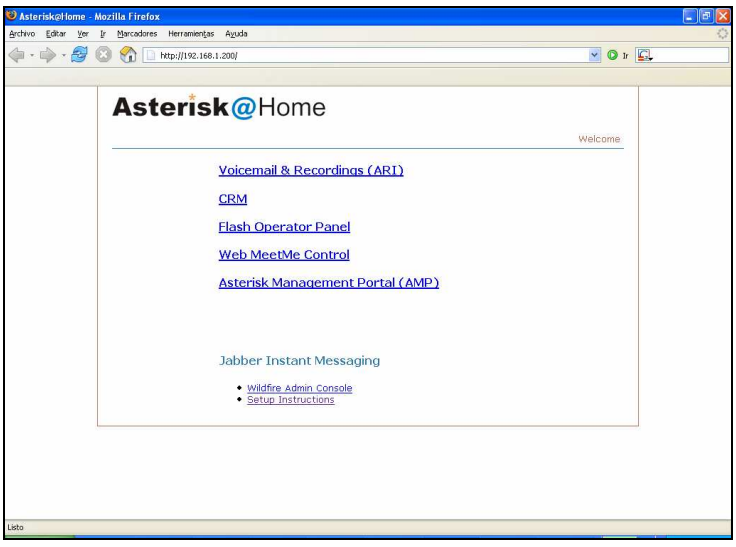
Sistema operativo	CentoOS 4.2		
Nombre del servidor	asterisk1.local		
Dirección IP	192.168.1.200		
Disco	Sistema de ficheros /dev/sda2 /dev/sda1 none swap	Tamaño 2.4G 2.4G 185M 1024MB	Montaje / /boot /dev/shm

5.2 Asterisk@Home

El servicio de centralita telefónica digital por software se lleva a cabo a través de la aplicación Asterisk@Home version 2.5.

Una de las ventajas de Asterisk@Home es que las diferentes configuraciones se realizan mediante la herramienta AMP (*Asterisk Management Portal*), una sencilla consola central a la que puede accederse desde cualquier navegador web.

Para abrir la consola únicamente hay que introducir la dirección IP del servidor en el navegor web, ya que el servicio se encuentra ubicado en el puerto web por defecto (TCP/80).



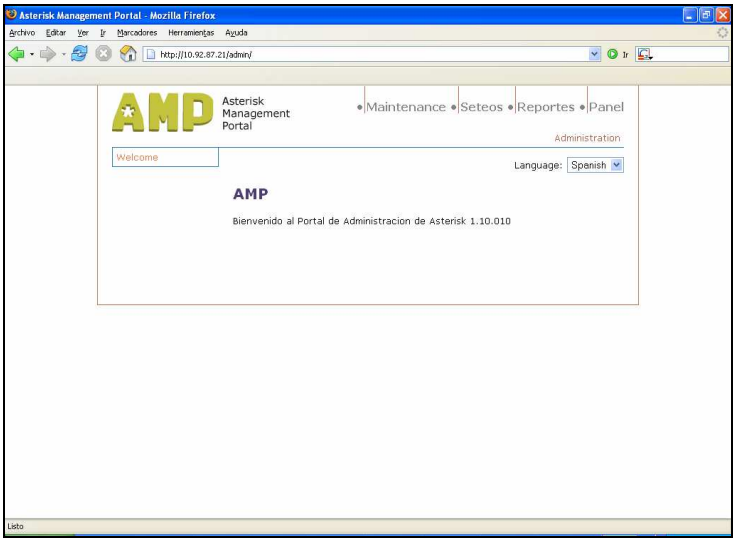


Figura 4-4: Consolas de configuración de Asterisk@Home

Una vez instalado el software, el primero de los pasos es añadir un par de usuarios con sus respectivas extensiones telefónicas. Para llevar a cabo la prueba se han configurado un total de dos usuarios agregando dos entradas SIP nuevas desde el menú *Setup -> Extensiones*, cada una con los siguientes datos de configuración:

Usuario 1	
Número de extensión	100
Nombre mostrado	Juan
Opciones de extensión	-
Opciones de dispositivo	**Código secreto**: UOC100 **dtmfmode**: rfc2833 (por defecto)

Usuario 2	
Número de extensión	200
Nombre mostrado	Diana
Opciones de extensión	-
Opciones de dispositivo	**Código secreto**: UOC200 **dtmfmode**: rfc2833 (por defecto)

El número de extensión es el número de teléfono interno asignado al usuario en la propia centralita. El código secreto es una palabra de paso que se utilizará para validar que únicamente el teléfono de cada usuario pueda registrarse en su línea correspondiente, y el parámetro *dtmfmode* indica qué modo de marcación se va a utilizar para realizar las llamadas (en este caso, marcación por tonos).

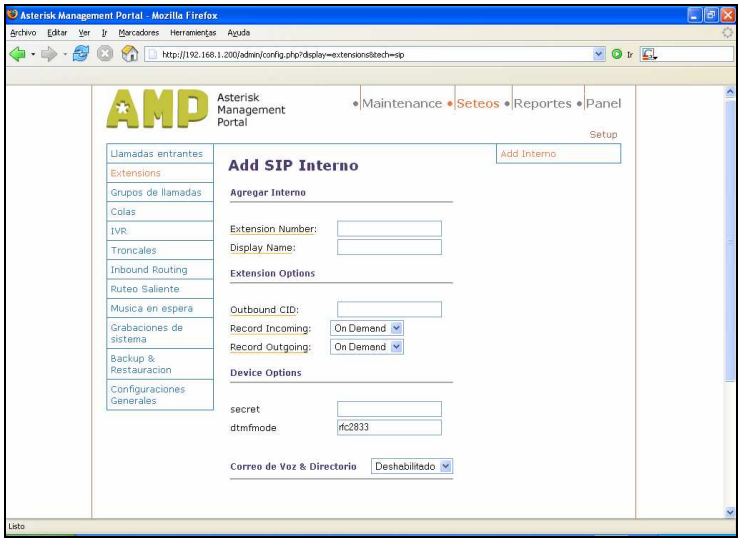


Figura 4-5: Creación de usuarios SIP

Una vez creados los usuarios en la base de datos de usuarios de la centralita ya podrían conectarse y realizar llamadas entre ellos mediante dispositivos VoIP compatibles con H323 o SIP.

5.3 Cliente VoIP X-Lite

Para poder realizar y recibir llamadas VoIP utilizando los usuarios SIP creados en el punto anterior es necesario disponer de dispositivos de acceso adecuados, ya sean teléfonos digitales IP o bien aplicaciones *softphone*. Tal como se ha indicado en puntos anteriores, existen en la red una enorme cantidad de clientes VoIP disponibles de forma gratuita. Para llevar a cabo las pruebas de laboratorio se utilizará el cliente libre SIP X-Lite de CounterPath (http://www.xten.net/). Se trata de un cliente VoIP del tipo *softphone* (es decir, es un teléfono 100% software que se instala como un programa sobre un sistema operativo con soporte para audio, en este caso, Microsoft Windows XP SP2).

Una vez instalado el teléfono X-Lite como una aplicación más del sistema operativo, la configuración necesaria (en el caso del primero de los usuarios de laboratorio) se puede observar en la siguiente figura:

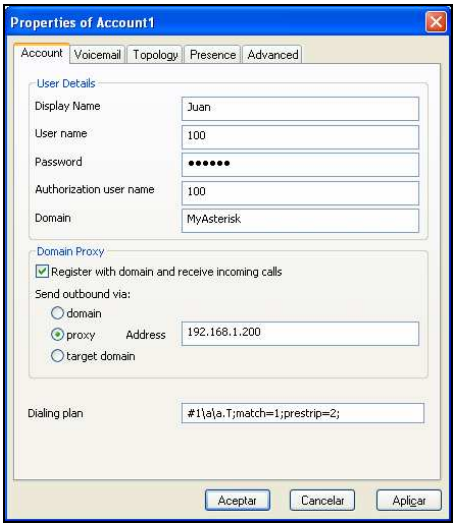


Figura 4-6: Configuració X-Lite

Una vez guardada la configuración, el teléfono VoIP establece automáticamente la conexión con la centralita digital Asterisk e inmediatamente se pone en línea, tal como se puede apreciar en la siguiente imagen.

Figura 4-7: Softphone X-Lite conectado a la centralita IP

La configuración del segundo teléfono (correspondiente al usuario Diana) se lleva a cabo de forma similar en la otra estación portátil con Windows XP.

5.4 Servidor Jabber Wildfire

El segundo de los grandes servicios de la plataforma es el correspondiente al servidor de mensajería instantánea.

En este caso la aplicación seleccionada para ser integrada con Asterisk@Home en el laboratorio es el servidor basado en Jabber "Wildfire". Una de las características de esta compilación es la capacidad de poder agregarle *plugins* que aporten funcionalidades añadidas al propio servicio de IM. En la lista de *plugins* disponibles en la propia web del producto (http://www.jivesoftware.org/wildfire/plugins.jsp) se encuentra un *plugin* de interconexión con Asterisk, y será mediante la instalación de este *plugin* que se llevará a cabo la integración de ambos servicios.

La instalación del plugin que permite integrar el servidor Wildfire con Asterisk es tan sencilla como copiar el fichero .jar en el directorio *WILDFIRE_HOME/plugins* y reiniciar el servidor. La configuración de Wildfire puede llevarse a cabo desde cualquier navegador web, simplemente conectando contra la dirección IP del servidor en el puerto 9090, abriendo de esta forma la consola central de configuración.

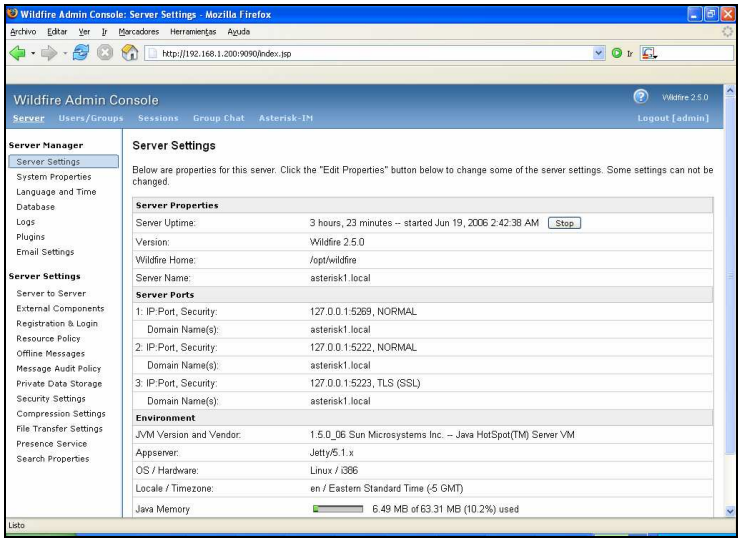


Figura 4-8: Wildfire Admin Console

Al instalar el plugin de Asterisk aparece en la consola de administración un nuevo menú correspondiente a esta aplicación, desde el cual se pueden configurar los parámetros de conexión con la centralita:

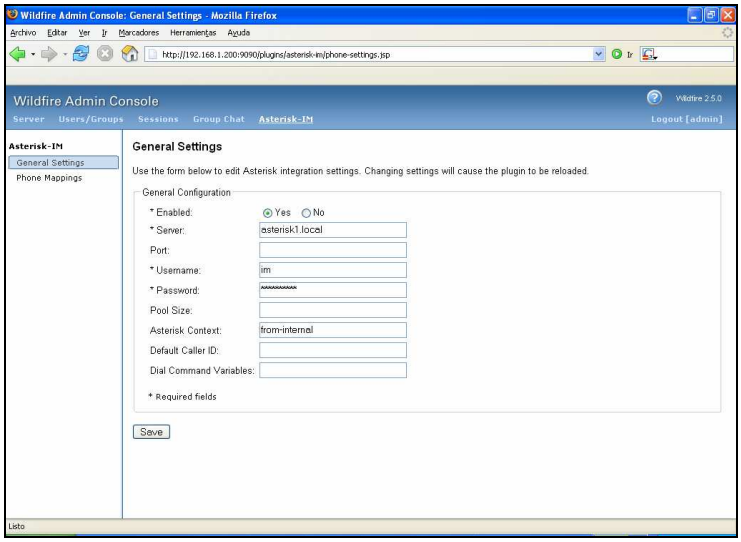


Figura 4-9: Integración Wildfire / Asterisk en la Admin Console

Mediante este *plugin* de integración es posible fusionar las funcionalidades de VoIP y de IM en un mismo servicio coordinado, dando de alta la misma lista de usuarios en el servidor Wildfire que en Asterisk, e informando los campos correspondientes al número de teléfono o extensión SIP dentro de la centralita.

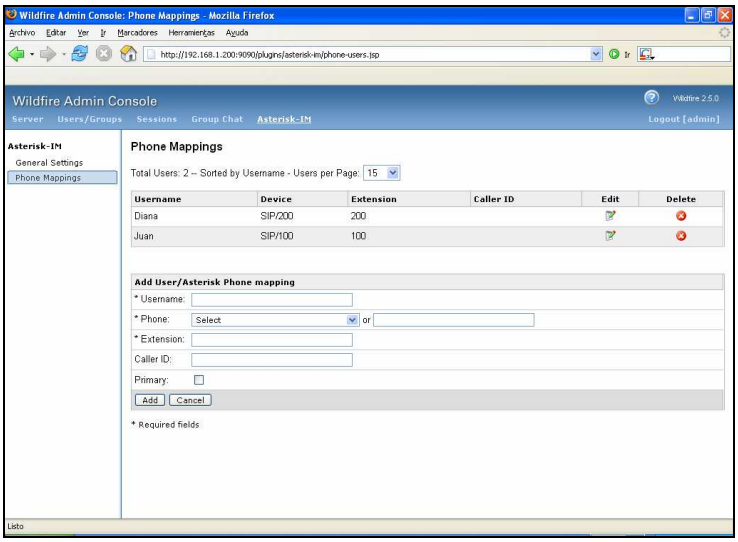


Figura 4-10: Usuarios de Asterisk en el servidor Jabber

Una vez replicada la lista de usuarios de Asterisk en Wildfire, el servidor está listo para dar servicio de IM integrada con VoIP desde el cliente de IM adecuado.

5.5 Cliente Jabber Coccinella

Por último, una vez instalados los servidores Asterisk@Home como centralita de VoIP y Wildfire como servidor de IM por un lado, y el cliente X-Lite para realizar llamadas telefónicas por otro, únicamente falta disponer de un cliente de mensajería instantánea compatible con la tecnología XMPP propia de Jabber.

Como ya se ha indicado en anteriores apartados el cliente seleccionado para realizar la configuración de prueba en el laboratorio es Coccinella (http://hem.fyristorg.com/matben), ya que se trata de uno de los clientes libres más avanzados y que incluye gran cantidad funcionalidades adicionales además de la capacidad de chat.

Una vez instalado el cliente Jabber Coccinella como una aplicación más del sistema operativo, la configuración necesaria (en el caso del primero de los usuarios de laboratorio) se puede observar en la siguiente figura:

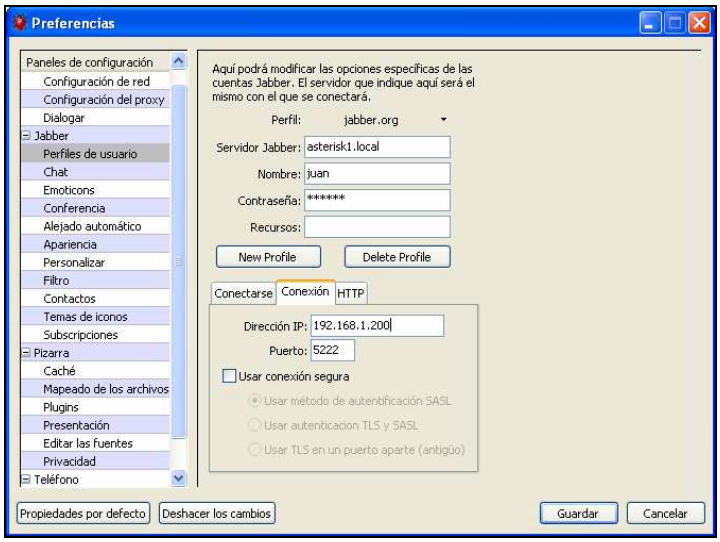


Figura 4-11: Configuración del cliente Jabber Coccinella

Una vez guardados los datos de configuración (servidor Jabber, usuario, contraseña e IP del servidor) ya se puede activar la conexión del cliente, mediante el correspondiente botón. Una vez conectado con el servidor, el cliente está listo para poder iniciar y recibir sesiones de mensajería instantánea como llamadas de teléfono.

Figura 4-12: Cliente Jabber Coccinella

6. Prueba global de la plataforma VoWiFi & IM

Llegados a este punto ya se dispone de la plataforma VoWiFi totalmente instalada y configurada, tanto desde el punto de vista de la red, como de los servidores y los clientes finales. Por último, y para comprobar el funcionamiento global del servicio, se realiza una prueba general de todos los módulos consistentes en una interacción real entre los dos usuarios de ejemplo creados en el sistema: Juan y Diana.

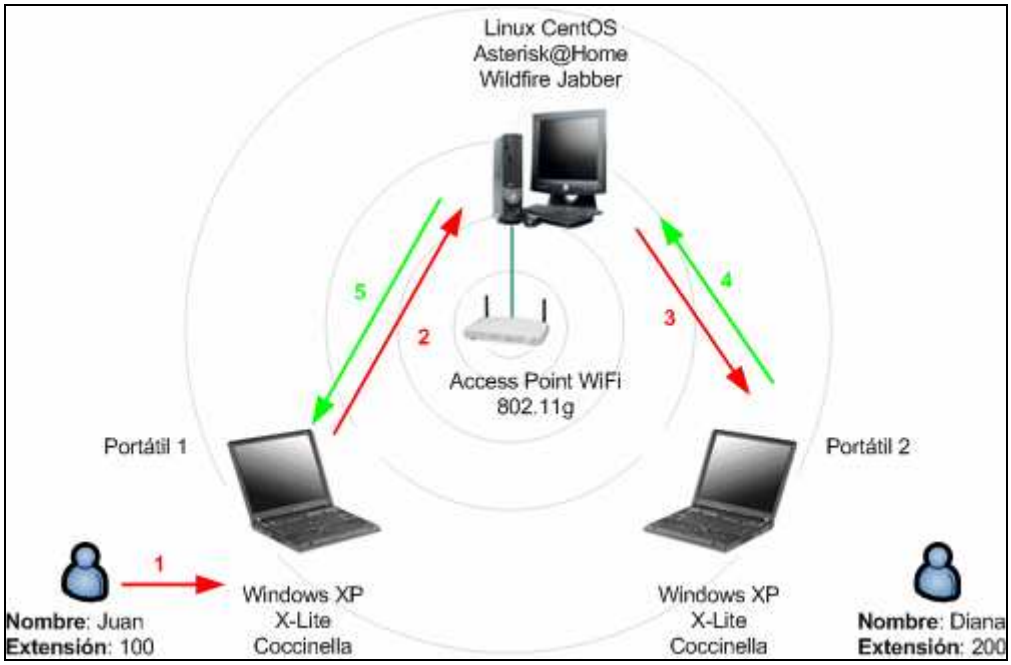


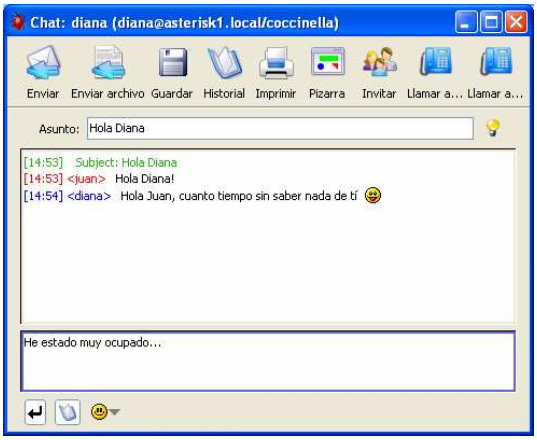
Figura 4-13: Prueba de funcionamiento global de la plataforma

El guión completo de la prueba global de funcionamiento de la plataforma es el siguiente:

1. El usuario “Juan” desde el portátil 1 abre sesión en sus clientes VoIP X-Lite y Jabber Coccinella.

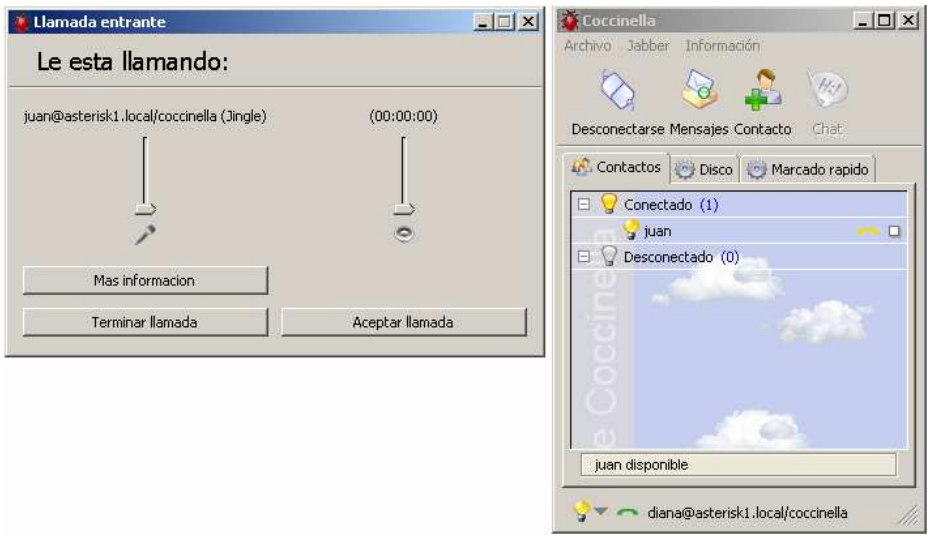
2. La usuaria “Diana” desde el portátil 2 abre sesión en sus clientes VoIP X-Lite y Jabber Coccinella. Se puede comprobar como a Diana le aparece el contacto de Juan como conectado (en ese mismo instante cambia también el estado de Diana para Juan).

3. Juan detecta que Diana se ha conectado, y haciendo doble clic sobre su nombre inicia una sesión de mensajería instantánea a la que ella contesta.



4. Juan prefiere hablar directamente con Diana desde el mismo cliente de mensajería instantánea, así que con el botón derecho sobre el contacto de Diana selecciona la opción “Llamar”.

5. Diana recibe la llamada y puede decidir entre aceptarla o rechazarla.



6. Juan prefiere utilizar su *Softphone* para hablar con Diana, ya que obtiene una calidad de sonido muchísimo mayor al tratarse de una aplicación optimizada para VoIP (al contrario que el cliente Jabber). Como sabe que Diana está conectada gracias al control de presencia del servidor Jabber Wildfire (servidor IM), desde el cliente X-Lite marca directamente la extensión de Diana y espera su respuesta.

7. El Softphone de Diana comienza a sonar avisando que hay una llamada entrante de Juan. Diana acepta la llamada y descuelga, comenzando así una sesión de VoIP directamente a través del servidor Asterisk, en este caso de forma independiente del servidor Jabber de mensajería instantánea.

Durante el ciclo de pruebas anterior se ha verificado el funcionamiento completo de una plataforma básica de VoWiFi: los usuarios “Juan” y “Diana” que trabajan desde dos ordenadores portátiles conectados a una red WiFi han sido capaces de ver si el otro se encuentra conectado o no, establecer una comunicación de mensajería instantánea y finalmente llevar a cabo una llamada VoIP, utilizando únicamente aplicaciones de software libre.

Por lo tanto, ha quedado comprobado que en la actualidad ya existe una posibilidad real de crear plataformas de VoIP integradas con servicios de mensajería instantánea, y que las conexiones pueden establecerse sin problemas a través de redes inalámbricas basadas en 802.11g (WiFi), todo ello utilizando aplicaciones de servidores y clientes basadas en la filosofía *Open Source*.

En conclusión, la tecnología VoWiFi puede considerarse el embrión de una tecnología de futuro que permitirá la convergencia definitiva de las redes de telecomunicaciones de voz y datos, sobre las cuales se construirá un paraguas de servicios de valor añadido como la mensajería instantánea cuyo único límite será la imaginación del hombre. Aunque hoy en día VoWiFi no pueda considerarse una alternativa madura a las plataformas de voz tradicionales, está claro que representa un punto de partida muy interesante y que evolucionará vertiginosamente en los próximos años ya sea a partir de las tecnologías actuales o bien a partir de nuevas propuestas de futuro como pueden ser las redes inalámbricas de alta velocidad WiMAX.

Glosario

ACD : Automatic Call Distribution
ADSL : Asymmetric Digital Subscriber Line
AES : Advanced Encryption Standard
ALG : Application Layer Gateway
ASN.1 : Abstract Syntax Notation One
ATM : Asynchronous Transfer Mode
BSS : Basic Service Set
CA : Collision Avoidance
CCMP : Counter Mode CBC MAC Protocol
CD : Collision Detection
CMT : Comisión del Mercado de las Telecomunicaciones
CNAF : Cuadro Nacional de Atribución de Frecuencias
CODEC : Coder / Decoder
CRC-32 : Cyclic redundancy check (32 bits)
CTS : Clear to Send
DCF : Distributed Coordination Function
DIFS : Distributed Coordination Function Interframe Space
DoS : Denial of Service
EAP : Extensible authentication protocol
EIFS : Extended Interframe Space
ESS : Extended Service Set
FXO : Foreign Exchange Office
FXS : Foreign exchange station
GSM : Global System for Mobile communications
HR/DSSS : High rate direct sequence spread spectrum
IAX2 : Inter Asterisk eXchange Protocol version 2
IBSS : Independant Basic Service Set
ICM : (Banda) Industrial, Científica y Médica
ICNIRP : Comisión Internacional de Protección contra la Radiación No Ionizante
ICV : Integrity Check Value
IEEE : Institute of Electrical and Electronics Engineers
IETF : Internet Engineering Task Force
IP : Internet Protocol
ITU : Internacional Telecommunication Union
ITU-T : ITU Telecommunication Standardization Sector
IV : Initialisation Vector
IVR : Interactive Voice Response
LAN : Local Area Network
MAC : Media Access Control
MCU : Multipoint Control Unit
MGCP : Media Gateway Control Protocol
MIC : Message Integrity Code
Michael : Ver MIC
MIME : Multipurpose Internet Mail Extensions
MP3 : MPEG-1 Part 3 Layer 3
MPEG : Moving Picture Experts Group
NAT : Network Address Translation
NAV : Network Allocation Vector
NIST : National Institute of Science and Technology
OFDM : Orthogonal frequency division multiplexing
OMS : Organización Mundial de la Salud
OSA : Open System Authentication
OSI : Open Systems Interconnection
PDA : Personal Digital Assistant
PFC : Point Coordination Function
PIFS : Point coordination Interframe Space

PIRE : Potencia isótropa radiada equivalente
POTS : Plain old telephone service
PSTN : Public switched telephone network
QoS : Quality of Service
RADIUS : Remote Authentication Dial In User Service
RAS : Registration, Admisión and Status
RC4 : Rivest Cipher 4 (algoritmo de cifrado)
RDSI : Red Digital de Servicios Integrados
RFC : Request For Comments
RSN : Robust Security Network
RSVP : Resource ReSerVation Protocol
RTCP : RTP Control Protocol
RTP : Real Time Protocol
RTS : Request to Send
RTSP : Real Time Streaming Protocol
SDP : Session Description Protocol
SIF : Short Interframe Space
SIP : Session Initiation Protocol
SKA : Shared Key Authentication
SSID : Service Set Identifier
STUN : Simple Traversal of UDP Through Network Address Translation devices
TCP : Transport Control Protocol
TDM : Time Division Multiplexing
TKIP : Temporal Key Integrity Protocol
UAC : User Agents Client
UAS : User Agents Server
UDP : User Datagram Protocol
UMTS : Universal Mobile Telecommunications System
UN : Notas de Utilización Nacional
UPnP : Universal Plug and Play
URI : Uniform Resource Identifier
URL : Uniform Resource Locator
VoIP : Voice Over IP
VoWIFI : Voice over WIFI
VoWLAN : Voice over wireless LAN
VPN : Virtual Private Network
WEP : Wired Equivalent Privacy
Wifi : Wireless Fidelity
WMM : Wireless Multimedia
WPA : Wi-Fi Protected Access
WPA2 : Wi-Fi Protected Access 2

Bibliografía

Libros

"**Asterisk: The Future of Telephony**" Jim Van Meggelen, Jared Smith, y Leif Madsen. Copyright 2005 O'Reilly ISBN: 0-596-00962-3."

Enlaces Web

3Com
http://www.3com.com

Cisco Systems
http://www.cisco.com

ComputerWire
http://www.computerwire.com

"Livephone"
http://livephone.us

HP
http://www.hp.com

IBM
http://www.ibm.com

"IT-Wireless"
http://www.it-wireless.com

The Wi-Fi Alliance
http://www.wi-fi.org

"Wi-Fi Planet"
http://www.wi-fiplanet.com

Wi-Fi Technology Forum
http://www.wi-fitechnology.com