MOVILIDAD IP EN REDES 4G

JORGE LUIS MARIMON BLANCO
ALFREDO JOSE HERNÁNDEZ DEL RIO

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR
MINOR COMUNICACIONES Y REDES
CARTAGENA DE INDIAS, D. T. y C.
MAYO DE 2004

MOVILIDAD IP EN REDES 4G

JORGE LUIS MARIMON BLANCO
ALFREDO JOSE HERNÁNDEZ DEL RIO

Trabajo Final presentado como requisito parcial
para aprobar el Minor de Comunicaciones y Redes

Director
ALFONSO DE LA ROSA CARABALLO
Ingeniero de Sistemas

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR
MINOR COMUNICACIONES Y REDES
CARTAGENA DE INDIAS, D. T. y C.
MAYO DE 2004

Cartagena de Indias, Mayo 28 de 2004

Señores
Universidad Tecnológica de Bolívar
Comité de Evaluación de Proyectos
Ciudad

Estimados Señores:

Con el mayor agrado me dirijo a ustedes para poner a consideración el Trabajo Final titulado ¨**Movilidad IP en Redes 4G¨.** El cual fue llevado a cabo por los estudiantes **Jorge Luis Marimón Blanco** y **Alfredo José Hernández del Rió**, bajo mi orientación como asesor.

Agradeciendo su amable atención,
Cordialmente,

Alfonso de la Rosa Caraballo
Ingeniero de Sistemas.

Cartagena de indias, Mayo 28 de 2004

Señores
Universidad Tecnológica de Bolívar
Comité de Evaluación de Proyectos
Ciudad

Estimados Señores:

De la manera mas cordial, nos permitimos presentar a ustedes para su estudio, consideración y aprobación el Trabajo Final Titulado ¨**Movilidad IP en Redes 4G**¨. Trabajo Final Presentado para aprobar el Minor de Comunicaciones y Redes.

Esperamos que este proyecto sea de su total agrado.
Cordialmente,

_____	_____
Jorge Luis Marimón Blanco	Alfredo José Hernández del Rió
Código: 9904025	Código: 0319350

AUTORIZACIÓN

Cartagena de Indias, D. T. y C., Mayo 28 de 2004

Nosotros JORGE LUIS MARIMON BLANCO y ALFREDO JOSE HERNÁNDEZ DEL RIO, identificados con numero de cédula 73´188.932 de Cartagena y 73´167.836 de Cartagena, autorizamos a la **Universidad Tecnológica de Bolívar**, para hacer uso de nuestro Trabajo de Grado y publicarlo en el catalogo online de la biblioteca.

_____ _____

Jorge Luis Marimón Blanco Alfredo José Hernández del Rió

Nota de aceptación

_____
_____
_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, Mayo de 2004

DEDICATORIA

Son pocas las palabras
que a uno le quedan
después de haber
realizado un arduo trabajo,
pero siempre quedan
palabras para dedicar,
y lo primero que pienso
es mis padres a quienes
le dedico este trabajo,
por ser ellos lo que
me ayudaron a realizar
cada una de mis metas,
por eso les agradezco,
por el valor que me
han enseñado.

Jorge Luis Marimón Blanco

AGRADECIMIENTOS

La labor de ser estudiante es gracias al trabajo de los profesores que día a día nos orientan, por eso cabe resaltar la importancia de las personas que ayudaron a realizar este trabajo. Al profesor Francisco Jiménez por inducirnos en el tema, al profesor Roberto Gómez quien nos suministro información valiosa que aporto al proyecto, y a nuestro director de monografía Alfonso de la Rosa Caraballo, quien nos guió en la organización del documento.

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

LISTA DE ECUACIONES

Pág.

LISTA DE ANEXOS

RESUMEN

En esta monografía ¨**Movilidad IP en redes 4G**¨ se describe la infraestructura necesaria para que pueda operar el protocolo IP Móvil dentro de una red 4G, en este caso Inalámbrica, con tecnología IEEE 802.11 con todas sus variantes, como son la a, b, g, h. Esta monografía comienza con una introducción a los sistemas móviles, como parte del proceso que comenzó con la primera generación, donde existían varías redes de radios móviles, pero éstas no eran propiamente sistemas celulares, estos restringían un poco el acceso debido a que la red era completamente analógica. Pasando luego a la segunda generación, al grupo de sistemas que iniciaron o evolucionaron hacia la utilización de técnicas digitales para realizar las transmisiones. Desde luego que la evolución no paro hay, la introducción de tecnología inalámbrica de 3G tiene como finalidad ofrecer nuevos servicios de telecomunicaciones, que necesiten mayores velocidades de transmisión, a los usuarios. Estos servicios no solamente serán para transferencia de información entre usuarios sino también entre dispositivos portátiles que funcionarán a nombre de los usuarios. Mientras esto sucede ya se esta trabajando en algunos centros de investigación en las tecnologías que constituirán las redes inalámbricas de la cuarta generación 4G.

En el siguiente capitulo encontramos de forma muy simplificada la evolución de las tecnologías de la red troncal, así cómo de su arquitectura, complementando reflexiones sobre la evolución del acceso o de la seguridad.

Luego encontramos la movilidad IP a cargo del protocolo IP Móvil, que permite el encaminamiento de paquetes IP hacia nodos móviles que pueden

cambiar rápidamente su punto de conexión a Internet. Este objetivo implica la transmisión de actualizaciones de encaminamientos entre numerosos nodos de la red. Para permitir su uso a través de un gran número de enlaces inalámbricos, es muy importante reducir el tamaño y la frecuencia de estas actualizaciones al mínimo posible.

La importancia de este apartado constituye una pieza fundamental en la comprensión del documento, donde radica la base de la movilidad según será estudiada por esta monografía.

Por ultimo la redes 4G, que constituyen las redes locales del futuro tienen que trabajar con computadoras que cambian de lugar frecuentemente, a veces dentro de la misma red y otras emigrando hacia otras redes. Las redes inalámbricas no usan cables como medio de comunicación. Las computadoras se comunican enviando y recibiendo ondas electromagnéticas que viajan del emisor al receptor a través del espacio. Es importante entender que el nombre de computadora y red inalámbrica se debe al medio de comunicación que usa y nada tiene que ver con movimientos. y siguiendo en este ultimo capitulo tratamos el concepto de la calidad de servicio QoS, movilidad, seguridad y contabilidad basados en IP. Debido a que la principal característica de las propuestas de redes móviles 4G es la utilización de tecnologías IP en el núcleo y en las redes de acceso, para soportar todos los servicios.

Introducción

En los últimos años se han ido produciendo numerosos avances en el campo de las tecnologías de comunicación. Dos de los más relevantes son, sin duda, el rápido desarrollo de la informática portátil y la importante implantación de los sistemas de comunicaciones móviles. La conjunción de ambos factores permite a los usuarios acceder a una red en cualquier momento y en cualquier lugar, aún cuando se encuentren en movimiento.

Sin embargo, los actuales protocolos de *internetworking* (TCP/IP, IPX ó AppleTalk) presentan serias complicaciones a la hora de tratar con nodos que disponen de un cierto grado de movilidad entre redes. La mayoría de las versiones del protocolo IP (Internet Protocol) asumen de manera implícita que el punto al cual el nodo se conecta a la red es fijo.

Por otra parte, la dirección IP del nodo identifica al mismo de manera unívoca en la red a la que se encuentra conectado. Por consiguiente, cualquier paquete destinado a ese nodo es encaminado en función de la información contenida en la parte de su dirección IP que identifica la red en la que está conectado. Esto implica que un nodo móvil que se desplaza de una red a otra y que mantiene su dirección IP no será localizable en su nueva situación ya que los paquetes dirigidos hacia este nodo serán encaminados a su antiguo punto de conexión a la red.

El protocolo *IP Móvil* constituye una mejora del protocolo IP citado anteriormente. ***Mobile IP*** permite a un nodo circular libremente a través de Internet siendo éste siempre accesible mediante una única dirección IP.

1. Sistemas móviles

1.1. Primera Generación 1G

La primera generación de los sistemas de comunicación celular apareció en 1980, donde existían varías redes de radios móviles, pero éstas no eran propiamente sistemas celulares, se basaban principalmente en una sola antena con un número limitado de canales que había disponibles hasta ese entonces. Y que intentaban dar servicio a todos sus abonados.

En una red celular, el área de cobertura está dividida en pequeñas células, normalmente hexagonales, cada una de las cuales es atendida por una estación de radio, la cual restringe su zona de cobertura a la misma célula; las células se agrupan en claustros o racimos, y el número de canales de radío disponibles se distribuye en el grupo de células, de manera que esta distribución se repite en toda la zona de cobertura. De esta manera el espectro de frecuencias puede volver a ser reutilizado en cada nuevo grupo de células, siempre teniendo cuidado de evitar las interferencias entre las células próximas.

Los PLANES que permiten, de forma ininterrumpida la cobertura de una determinada área, son configuraciones a modo de panal de miél, basadas en 4, 7, 12 o 21 células, siendo la de 7 la más usada. El número total de canales por célula, va directamente ligado a la capacidad de manejo de tráfico, depende del número total de canales disponibles y del tipo de plan, según la formula:

$$NumerodeCanalesPorCelula = \frac{NumeroDeCanales}{Plan(4,7,12,21)} \quad \text{(Ec.1)}$$

Así la estructura de la red se basa en la conexión de los terminales móviles al sistema a través de una serie de estaciones base repartidas por un área geográfica, cada radio base atiende a un grupo de células (4, 7, 12, 21).

Las principales características de un sistema celular son:

- Gran capacidad de usuarios.
- Utilización eficiente del espectro.
- Amplia cobertura.

En esta primera generación se utilizaron técnicas de transmisión analógicas, limitados los servicios en su mayoría a voz. Estas características, hemos de remarcarlo, es lo que caracteriza a la primera generación: una red celular, y la utilización de técnicas analógicas.

Los estándares más exitosos fueron:

- Nordic Mobile Telephone (NMT)
- Total Access Communications Systems (TACS)
- Advanced Mobile Phone Service (AMPS).

El NMT que originalmente se creo en Escandinavia, tuvo dos variantes NMT-450 y NMT-900, usando la banda de 450 MHz y la de 900 MHz respectivamente. NMT ofrecía la posibilidad de roaming internacional, esto significó una gran ventaja sobre los sistemas ya existentes.

TACS, estándar de el Reino Unido es otro, actualmente se basa en el protocolo AMPS, pero en la banda de los 900 MHz. Y por ultimo AMPS, de origen Norteamericano, el cual usa la banda de 800 MHz. También en Japón se crearon estándares tales como NTT's MCS.

Notemos, que aunque el mundo avanza hacia nuevos estándares, en algunas partes del mundo todavía se utilizan los sistemas de primera generación, como nuevos, y otros siguen solamente creciendo. Estos estándares se basaban, como se mencionó anteriormente, en tecnología analógica y a partir de este momento la utilización de las redes celulares quedó establecida.

1.2. Segunda Generación 2G

Se le da por nombre de segunda generación, al grupo de sistemas que iniciaron o evolucionaron hacia la utilización de técnicas digitales para realizar las transmisiones. Aquí es donde se hace obvia la frontera entre la primera y la segunda generación de telefonía celular: el cambio análogo-digital. Las redes de la segunda generación presentaban una capacidad mucho mayor con respecto a los de la primera generación. Se logró dividir un canal de frecuencia para poder ser utilizado simultáneamente por varios usuarios, esto, gracias a las técnicas digitales de división por tiempo o código.

Gracias a las técnicas digitales se podía dividir un espacio de tiempo muy pequeño entre varios usuarios, como el espacio de tiempo era pequeño los usuarios no notaban esta división.

También la estructura de las células se modificó: el área de cobertura se dividió en macro, micro y pico células (respecto al área de cobertura y al trafico esperado), esto aumentó la capacidad de los sistemas aún mas. El tamaño de las células era escogido de acuerdo a cálculos probabilísticos y estadísticos, los cuales relacionaban el trafico esperado en área con la capacidad del sistema.

La segunda generación entró en funcionamiento hacia 1991, existen cuatro estándares principales para los sistemas de segunda generación:

- Global System for Mobile Communications (GSM)
- Digital AMPS (D-AMPS) o también llamado TDMA,
- Code División Múltiple Access (CDMA IS-95)
- Personal Digital Cellular (PDC).

De estos cuatro, GSM fue sin duda el que mas éxito tuvo. Estos sistemas se expandieron rápidamente por el mundo. En Europa se adoptó GSM y también en gran parte de el mundo. En Norteamérica se ocupo principalmente D-AMPS y en Japón PDC.

D-AMPS (IS-54), fue aceptada en Norte América principalmente. Este estándar fue creado con el antecedente de ser compatible con el estándar analógico AMPS. Aquí se utiliza un canal digital de control (DCCH) en comparación con el canal análogo de control del sistema AMPS. Así mismo los canales de tráfico se vuelven digitales, y es necesaria la adicción de más información para poder ser entendidos en el receptor. Este estándar tiene su base en el esquema TDMA al igual que GSM.

CDMA (IS-95), es un sistema que incorpora una nueva interfaz aérea. CDMA ya no divide una canal de frecuencia en slots de tiempo, ahora, utiliza un código para separar la transmisión de un usuario de otro, esto es, a un usuario se le agrega un código y a otro usuario se le da uno distinto. Los principios del sistema CDMA, son también la base para los sistemas de 3G.

En cuanto a PDC este fue un sistema creado en Japón, desafortunadamente este no fue muy aceptado fuera de él. Sin embargo esto no detuvo a sus

creadores y fue Japón uno de los países pioneros en varías áreas de investigaciones para desarrollar la 3G.

Las ventajas que ofrecían estos nuevos sistemas fueron:

- Mayor calidad de voz.
- Menores costos de operación de las terminales.
- Mayor nivel de seguridad.
- Roaming internacional.
- Soporte para termínales de menor potencia.
- Una mayor variedad de servicios.

Aunque todos estos sistemas pudieran o no parecerse, es cierto que todos ellos debían ser competitivos, es por esto que entre ellos proveían un cierto tipo y número de servicios.

Podríamos dividirlos en tres tipos: tele servicios, servicios portadores y servicios suplementarios, como se muestra en la Tabla 1.

Estos sistemas tuvieron una gran aceptación en el mundo, principalmente GSM, el cual fue instalado en Europa, parte de Asia, África y América y que hasta el año 2001 contaba, con cerca del 67% del total de los usuarios de telefonía móvil digital en el mundo. Pero también los otros sistemas han tenido su aceptación y su crecimiento.

Categoría de Servicio	Transmisión
Tele servicios	Transmisión de datos a 300, 1200, 2400, 4800, 9600 bps en modo duplex, asíncrono transparente y no transparente, con interconexión a RTC y RDSI. Transmisión de datos desde 2400 hasta 9600 bps en modo duplex, asíncrono transparente y no transparente, con interconexión a redes publicas conmutación de paquetes.
Servicios portadores	Transmisión de datos a 300, 1200, 2400, 4800, 9600 bps en modo duplex, asíncrono transparente y no transparente, con interconexión a RTC y RDSI. Transmisión de datos desde 2400 hasta 9600 bps en modo duplex, asíncrono transparente y no transparente, con interconexión a redes publicas conmutación de paquetes.
Servicios suplementarios	Llamadas en espera Llamadas perdidas

Tabla 1. Servicios 2G

1.3. Segunda Generación avanzada 2.5G

La generación 2.5, es el nombre con el cual se designa a la evolución de los sistemas 2G, y representan a la mayoría de los sistemas establecidos en el mundo, pero en este caso la evolución no fue tan radical como el paso de 1G a 2G. La frontera entre 2G y 2.5G es algo no definido por completo, pero se basa en los servicios ofrecidos por los sistemas para el usuario y para intentar incrementar la capacidad de transmisión. Estos nuevos servicios se vienen a adicionar a los ya proveídos en la 2G. Se siguen clasificando en los tres tipos principales: tele servicios, servicios portadores y servicios suplementarios.

Pero el problema del sistema GSM, es la baja tasa de transmisión de la interfaz aérea. El sistema básico GSM solo podía proveer un tasa de transmisión de datos de 9.6 Kbps, posteriormente se especificó un tasa de

14.4 Kbps. Con estas velocidades y para poder proveer de todos estos servicios a los usuarios, es necesario el incrementar la capacidad del sistema, es por esto que la 2G se caracteriza también por la utilización de una o de varias de las siguientes tecnologías: High-Speed Circuit-Swítched Data (HSCSD), General Packet Radio Services (GPRS), y Enhanced Data Rates for Global Evolution (EDGE).

HSCSD es la tecnología mas fácil para incrementar la velocidad, lo que hace esta técnica es utilizar más de un slot de tiempo para la conexión, con esto, se multiplica la tasa de transferencia a un múltiplo entero de 9.6 Kbps, con esto se capacita al sistema para aplicaciones de tiempo real. Este método es sin duda el más barato, pues solo requiere un software que sea capaz de manejarlo, y obviamente, teléfonos con el soporte necesario.

Pero el precio está en los recursos del sistema, ya que se hace uso de los slots de tiempo, aun cuando no se transmita nada. Y esto, en lugares de alto tráfico, es casi imposible de sostener. Sin embargo, ésta técnica, no es muy usada, ya que la mayoría de los fabricantes se han decidido por GPRS.

GPRS eleva las tasas de transmisión hasta 115Kbps, o incluso más alto si nos olvidamos de la corrección de errores, esto es algo equivalente a una trama de 8 slots. Pero lo más importante es que este sistema es por switcheo, y por tanto los recursos del sistema nos son utilizados continuamente, solamente cuando se transmite algo. GPRS es bueno para aplicaciones que no sean de tiempo real, tales como correo electrónico o navegación por Internet. La utilización de un sistema GPRS es mucho más caro que un sistema HSCSD. Ya que la red necesita nuevos componentes. Este salto fue necesario, ya que sin el GSM no hubiera sobrevivido tanto como lo ha hecho. Incluso este sistema es ya una primera exploración dentro de lo que serian los estándares para la 3G.

Por último, EDGE, originalmente pensado para GSM, posteriormente fue utilizado por varios estándares. La idea que se propone en EDGE, es la de un nuevo esquema de modulación llamado eight-phase shift keying (8PSK). Esto no causa conflictos con la modulación Gaussian minimum shift keying (GMSK) y solo se necesita de una actualización del software de la radio base. Pero aún así el inconveniente viene en que solo puede ser utilizado dentro de cortas distancias, ya que en grandes áreas de cobertura aún es necesario GMSK.

Estos tres métodos pueden combinarse: la de GPRS y EDGE se llama Enhanced GPRS (EGPRS). EGPRS, puede proveer de una tasa de incluso 384 Kbps, pero utilizando todos los recursos de un canal de transmisión. ECSD, es la combinación de EDGE y HSCSD.

También IS-95 (CDMA) es de los servicios más rápidos con velocidades de hasta 144Kbps, colocándose en la segunda posición, atrás de GSM fase II.

Actualmente el mercado mundial de telefonía celular esta repartido de la siguiente manera:

Tecnología	Participación
GSM	69.83%
CDMA	12.85%
TDMA	9.48%
PDC	5.29%
Otras	2.55%

Tabla 2. Participación en el mercado de las tecnologías celulares (Fuente EMC World Cellular Database. Marzo 2003).

1.4. Tercera Generación 3G

Hasta aquí hemos hablado sobre la historia. Pero que es lo que esta pasando en la actualidad. Puesto que todos estos sistemas de 2G y 2.5G tienen que evolucionar hacia la tercera generación 3G. Y es que aún cuando las redes de comunicaciones celulares de 2da generación (GSM en Europa, IS-136 e IS-95 en USA) no han terminado de desplazarse por completo a las de 3ra generación, en los últimos años ha habido una actividad muy fuerte de investigación y desarrollo a nivel internacional para finalizar los estándares de 3G que, eventualmente y de manera gradual, substituirán a las redes de 2G. Mientras esto sucede ya se esta trabajando en algunos centros de investigación en las tecnologías que constituirán las redes inalámbricas de la cuarta generación 4G.

El cambio de 1G a 2G se produjo como una respuesta a la saturación del espectro reservado para comunicaciones celulares (banda de 800 MHz). La tecnología TDMA (IS- 136) logró multiplicar por tres el número de usuarios que FDMA podía atender en un canal, y CDMA (en promedio) incrementó este número a 5. La introducción de tecnología inalámbrica de 3G no se dará como respuesta, solamente, a la saturación del espectro radioeléctrico, sino con la finalidad de ofrecer nuevos servicios de telecomunicaciones, que necesiten mayores velocidades de transmisión, a los usuarios. Estos servicios no solamente serán para transferencia de información entre usuarios sino también entre dispositivos portátiles que funcionarán a nombre de los usuarios.

Con acceso a cualquier servicio de Internet Móvil desde un dispositivo móvil, en cualquier momento, en cualquier lugar, desaparecerán los limites entre comunicación, información, medios y entretenimiento. Se producirá una verdadera convergencia de servicios.

1.4.1. Servicios de 3G

Como objetivo, se propone que los servicios deban cumplir lo siguiente: Se pretende que los usuarios puedan disponer en un mismo terminal de diferentes servicios (Voz y navegación Web al mismo tiempo), poniendo a su disposición los recursos más adecuados a su necesidad (paquetes para navegación, circuito para voz) en cada momento de la conexión.

En cuanto a velocidad, los objetivos son distintos en cada entorno:

- Medio rural: 144 kbps (objetivo 384 kbps), a velocidad máxima de 500Km/h
- Zona suburbana: 384 kbps (objetivo 512 kbps), a 120 Km/h.
- Interior, microcélulas: 2 Mbps.

Deberán soportarse servicios simétricos y asimétricos.
Itinerancia global.
Calidad comparable a la de la telefonía fija.

Todos estos nuevos servicios y especificaciones de los sistemas propuestos para la 3G se juntaron con la creación de IMT-2000 y del 3GPP y 3GPP2, del cual hablaremos mas adelante.

Es importante mencionar la tecnología IP (Internet Protocol) basada en paquetes que constituirá el núcleo de las redes 3G significará que podremos estar en línea de manera constante: "siempre conectados". También se producirá una necesidad creciente de interacción entre usuarios móviles y las máquinas, y de máquina a máquina, a través de conexiones inalámbricas.

1.4.1.1. IMT-2000

IMT-2000 es una iniciativa de la UIT para proporcionar acceso a una variedad de servicios de telecomunicaciones de las redes fijas y a otros servicios que son específicos de los usuarios móviles, por lo que las terminales pueden diseñarse para uso móvil o fijo. Las características fundamentales de IMT-2000 son:

- Cobertura completa para 144Kbps, preferible 384 kbps.
- Cobertura y movilidad limitada para 2Mbps.
- Alta eficiencia espectral.
- Alta flexibilidad para nuevos servicios.
- Compatibilidad entre los diversos sistemas (cobertura mundial).

Las bandas de frecuencias: 1885-2025 MHz y 2110-2200 MHz, con el componente satelital limitado a 1980-2010 y 2170-2200 MHz, se encuentran actualmente identificadas y establecidas en todo el mundo para la operación de los sistemas IMT-2000.

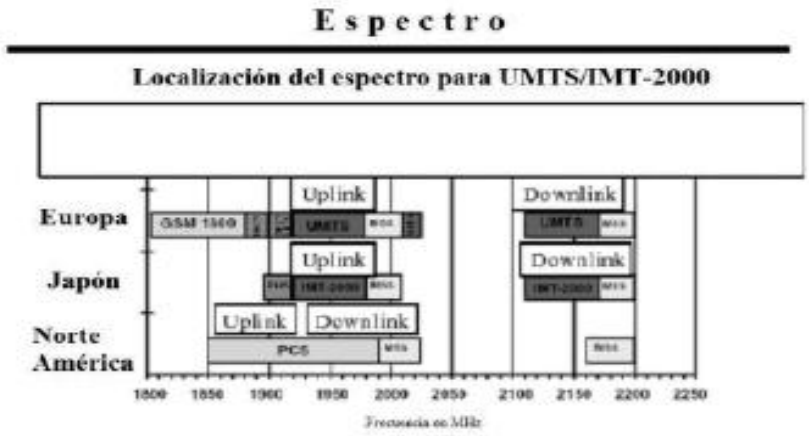


Figura 1. Bandas de frecuencias para IMT-2000.

El sistema IMT-2000 no es solo un sistema celular, si no que es una esfuerzo por proveer un sistema de comunicaciones convergente a nivel mundial, el cual incluya todo tipo de redes, incluyendo: sistemas satelitales, sistemas celulares terrestres (macro, micro y pico-células), sistemas alambrados y sistemas de acceso inalámbrico. Todos estos desarrollos no se han venido dando al mismo tiempo en todo el mundo, por lo que los sistemas de 3G irán apareciendo poco a poco.

1.4.2. Propuesta para 3G

La mayoría de las redes de tercera generación contemplan trabajar en las mismas bandas de frecuencia que las redes de segunda generación existentes. El ancho de banda considerado es de 5 MHz, con lo cual se logra compatibilidad con redes existentes y se pueden proporcionar tasas de bit de 144Kbps y 384 Kbps con facilidad.

Fueron propuestos para IMT-2000 una gran multitud de sistemas, basados en diferentes tecnologías:

- UWC-136/ATDMA(USATIATR-45.3)
- Wims W-CDMA/CDMA (USA TIA TR-46.1)
- NA W-CDMA/WCDMA (USA T1P1-ATIS)
- cdma2000/WDMA (USA TIA TR-45.5)
- SAT-CDMA/49 LEO (South Korea TIA)
- Dect Terrestrial (ETSI Project EP DECT)
- TD-SCDMA/Time-División Synchronous CDMA (China)
- SW-CDMA/Satellite Wideband CDMA (European Space Agency)
- SW-CDMA/Satellite Wideband Hybrid CDMA/TDMA (European Space Agency)

- ICO RTT/ 10 MEO (ICO Global Communications)
- W-CDMA/WCDMA (Japan ARIB)
- CDMA II/Asynchronous DS-CDMA (South Korea TTA)
- CDMA I/Multiband Synchronous DS-CDMA (South Korea TTA)
- UTRA UMTS/UMTS Radio Access (ETSI SMG2)
- Horizons/Horizons Satellite System (Inmarsat)

Dentro de estos estándares propuestos, son cuatro los que se han quedado como principales contendientes para ser elegidos: UTRA-UMTS-(WCDMA), cdma2000, Enhanced-GSM (que incluye: HSCSD, EDGE, GPRS) y UWC-136/EDGE, estos dos últimos se basan en tecnología parecida. Aún se sigue discutiendo sobre cuál de estos sistemas será el indicado para englobar a las telecomunicaciones inalámbricas para la 3G; pero el que mayor auge y popularidad ha tenido es UMTS.

En la figura 2. se muestra la evolución de las redes de segunda generación, tal como esta sucediendo en la actualidad y las tecnologías que la soportan:

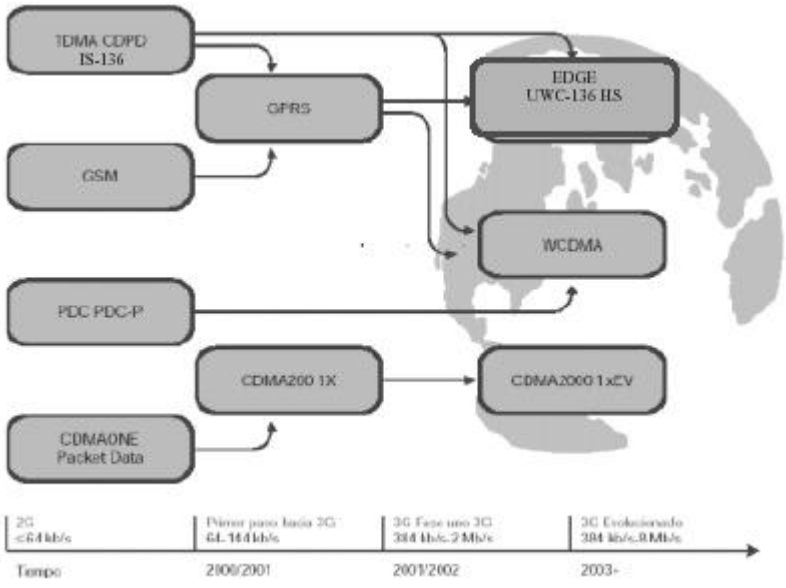


Figura 2. Tecnologías 2G y evolución a 3G

Para los estándares PDC y GSM, el cual utiliza tecnología de Acceso Múltiple por División de Tiempo (TDMA), la tecnología dominante para la evolución hacia tercera generación es WCDMA llamada UMTS, aunque algunos fabricantes se inclinan por la tecnología de GPRS que se apoyara en EDGE. La tecnología WCDMA es del tipo asíncrona, con esparcimiento directo y tasa de transmisión de 4.096 Mbps. El esquema WCDMA ha sido desarrollado como un esfuerzo conjunto entre ETSI (Instituto de Estándares en Telecomunicaciones y Electrónica de Europa) y ARIB (Asociación para Negocios y Radio Industria de Japón). WCDMA maneja canales de 1.25, 5, 10 y 20 MHz de ancho de banda, con tasas de transmisión de 1.024, 4.096, 8.192 y 16.384 Mbps respectivamente. Dentro de esta tecnología, aun se encuentran dos opciones: FDD (Frequency División Dúplex) y TDD (Time División Dúplex).

Para el estándar IS-136, el cual también utiliza tecnología TDMA, la tecnología dominante para la evolución hacía tercera generación es UWC (Universal Wireless Communications), la cual adoptará el modo de alta velocidad (136HS). El estándar UWC-136 contempla dos tecnologías complementarias:

136+ para ambientes exteriores, el cual ofrece un modo expandido de IS-136, usando las mismas frecuencias y anchos de banda (30KHz) para proporcionar tasas de bit de hasta 384 Kbps. La tecnología 136+ emplea modo FDD, con 8 ranuras por trama.

136HS, para ambientes interiores, el cual ofrece tasas de bit de hasta 2 Mbps, y maneja canales de 200 KHz y 1.6 MHz de ancho de banda. Esta tecnología utiliza los modos FDD y TDD, con 16 y 64 ranuras por trama respectivamente. Ambas tecnologías manejan modulación QAM, con longitud

de trama de 4.615ms, código convolucional de tasa variable y salto en frecuencias opcional.

UWC-136, utiliza la tecnología ATDMA (Advanced TDMA). Este usa tres diferentes tipos de portadoras: 30KHz, 200KHz y 1.6MHz. La portadora de 30KHz es la misma que utiliza IS-136, pero con diferente modulación. La portadora de 200KHz utiliza los mismos parámetros que la portadora de GSM-EDGE, ésta es utilizada principalmente para trafico en exteriores y vehicular y provee también tasa de transmisión de 384Kbps. Y por último, la portadora de 1.6MHz, que es utilizada para cobertura en interiores, y la cual puede proveer tasas de 2Mbps.

Por último CDMAONE (IS-95), el cual se basa en la tecnología CDMA, al igual que UMTS. Al principio se evolucionará a CDMA20001X, que brinda voz y datos simultáneos con el doble de capacidad de voz que CDMAONE, y datos en paquetes a velocidades promedio de 144Kbps.

Posteriormente, los operadores podrán implementar la fase dos de CDMA2000, denominada CDMA20001xEV-DO. Dicha implementación permite a los operadores ofrecer en forma dinámica velocidades de datos pico de 2.4Mbps cuando un usuario se encuentra realizando una transmisión de datos únicamente, mientras que las capacidades de CDMA20001X se ofrecen cuando los usuarios usan voz y datos en forma simultánea. Los canales que se planea usar son múltiplos de 1.25MHz (1, 3, 6, 9 y 12).

Estos tres sistemas UWC-136 y UTRA-UMTS-WCDMA y cdma2000 son los contendientes más importantes dentro del IMT-2000, aunque esto es más que nada por el tipo de sistemas antecesores. Es por esto que se crearon dos grupos el 3GPP y el 3GPP2

1.4.3. 3GPP

3GPP Third Generation Partenership Project o Proyectos de Asociación para Tercera Generación[1]. También conocida como sistema IMT-DS (Direct Spread). Creada en diciembre de 1998. 3GPP es una organización que desarrolla las especificaciones para los sistemas de 3G basados en la interfaz aérea UTRA de ETSI (UMTS) esta organización es responsable también por el futuro de las especificaciones de trabajo de GSM, incluye dentro de sus miembros a ETSI, ARIB, T1, Telecommunication Technology Association (TTA), Telecommunications Technology Committee (TTC), y China Wíreless Telecommunications Standard (CWTS).

El 3GPP tiene ya establecidas las especificaciones para el sistema de 3G UMTS, uno de ellos es la utilización de la tecnología de acceso WCDMA. Esta tecnología contempla dos modos Frecuency división dúplex (FDD) y Time división dúplex (TDD).

1.4.4. 3GPP2

3GPP2 es la otra organización mayor de estandarización. Esta es la encargada del estudio sobre el sistema cdma2000, el cual está también basado en la tecnología de acceso CDMA. Conocida también, dentro de IMT-2000, como sistema IMT-MC. La principal diferencia entre 3GPP y 3GPP2 consiste en que 3GPP cambiaría completamente las especificaciones de la interfaz aérea. Mientras que 3GPP2 plantea una interfaz compatible con el sistema IS-95, ya que en Norte América la banda para 3G es la que utiliza el sistema IS-95. El estándar en el que se basa 3GPP2 es cdma2000.

[1] "3GPP - 3rd Generation Partnership Project". http://www.3gpp.org/

Los miembros de 3GPP2 incluyen a: ARIB Association of Radio industries and Businesses, CWTS China Wireless Telecommunication Standards Group, TIA Telecommunications Industry Association, TTA Telecommunications Technology Association, TTC Telecommunications Technology Committee.

Se está acordando una solución IP punto a punto basada en normas para redes CDMA2000 dentro de 3GPP2 (3G Partenership Project Two). 3GPP2 trabaja de manera estrecha con 3GPP para asegurarse de que la red central y la evolución IP de las redes CDMA 3G sean congruentes con la de las redes WCDMA y viceversa.

1.5. Cuarta Generación 4G

Las redes de 3G estarán enfocadas hacía la transferencia de voz y datos con una velocidad máxima de 2 Mbps, velocidad que no es suficiente para proporcionar servicios verdaderamente multimedia (tales como transferencia de archivos de imágenes, video en tiempo real, etc.), los cuales requieren de velocidades que van hasta los 10 Mbps (equivalentes a las de las redes LAN's típicas). Estos servicios multimedia de alta velocidad son el nicho que pretende atacar la tecnología de 4G.

La diferencia básica entre una red de 3G y una de 4G, como se mencionó es la tasa de bit disponible para el usuario. Mientras que las redes de 3G ofrecen accesos hasta de 384 Kbps, con picos de hasta 2 Mbps (con los que podría manejar servicios de audio, datos e imágenes), las redes de 4G ofrecen accesos realmente multimedia, en las que podrá manejarse la transferencia de video en tiempo real, con velocidades equivalentes a las de una LAN básica (10 Mbps) y mayores.

Para lograr esto, se necesita manejar anchos de banda de al menos 20 MHz por canal por lo que la tecnología se considera de banda ancha. Puesto que la potencia necesaria para el transmisor es directamente proporcional al ancho de banda de la señal, el área de cobertura de una estación base para red de 4ta generación es de diámetro reducido; por lo que se prevé que se limitará al radío de una pico célula (hasta de 200 m de radio). Por tanto, la tecnología Inalámbrica de 4ta generación no vendrá a sustituir a la de 3ra, sino a complementarla. En la Figura 3., se muestra la cobertura que proporcionará cada tipo de red.

Los factores que pueden influir en el desarrollo de las redes de 4ta generación son, entre otros:

El auge del Internet, que cada vez se utiliza más por medios inalámbricos. La proliferación de asistentes digitales personales y computadoras personales de bolsillo.

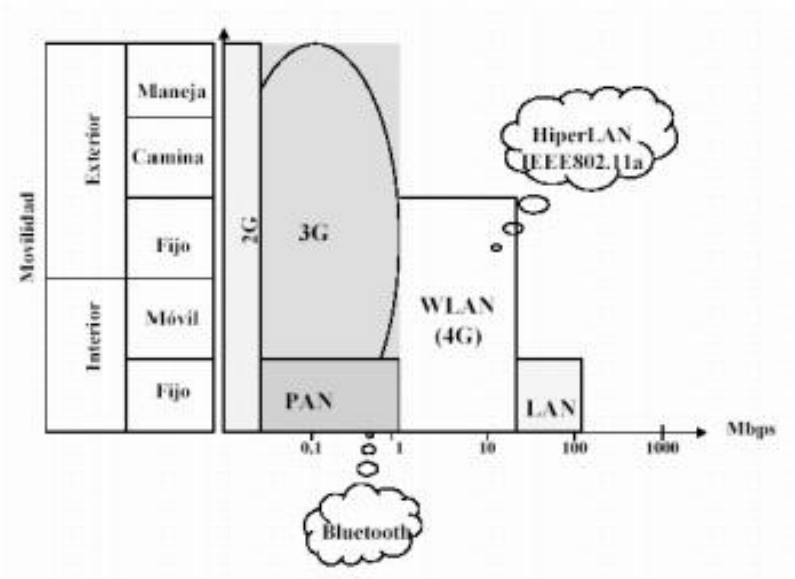


Figura 3. Cobertura por tipo de red.

La disponibilidad de servicios de valor añadido a los usuarios de Internet móvil (transacciones bursátiles, reservaciones aéreas, etc.).

La oferta de servicios llamados transparentes, donde los dispositivos interactúan con otros dispositivos, a nombre de los usuarios.

Las tecnologías que pueden ser decisivas en el desarrollo de las redes de 4ta generación son:

El protocolo IP, como la parte de transporte de la RUM, Red Universal Multimedia (probablemente en esta red no se usen mas números de abonado sino direcciones de red).
La tecnología de antenas adaptivas e Inteligentes (para aprovechar la dimensión espacial de los nodos de acceso al medio).
La tecnología de modulación / transmisión inalámbrica de multicanalizacion en frecuencia con portadoras ortogonales OFDM (para lograr una eficiencia espectral optima.
La tecnología de radios programable ("Software Radios"), la cual permitirá que una terminal pueda hacer ¨Handoff¨ desde una célula perteneciente a un tipo de red, hacia otra célula perteneciente a una red con tecnología Inalámbrica diferente.

La tecnología de redes locales inalámbricas (WLAN's) de banda ancha (que brindaran el acceso a la RUM al usuario móvil). Los nombres de estas tecnologías ya se están dando a conocer, entre ellas tenemos Bluetooth y IEEE802.11a.

Con la 4G podremos mirar videos y recibir correos electrónicos en forma simultanea en tiempo real, o entretenernos con juegos interactivos con

amigos mientras nos trasladamos, donde sea que estemos. Pero 3G y 4G no se refieren sólo a permitir aplicaciones que requieren altas velocidades de transmisión de datos. También se refiere a brindar comodidad y velocidad de acceso.

1.5.1. Tráfico multimedia en redes móviles de cuarta generación

Para la incorporación de flujos de paquetes multimedia en las redes móviles de cuarta generación, las redes 4G deberán tratar con flujos de muy diversa índole, tanto por la arquitectura que suponen (modelo cliente–servidor, o bien punto a punto) como por los requisitos de ancho de banda y tamaño de los paquetes.

La medición del flujo generado, así como el análisis de la tolerancia a una disminución de la QoS recibida, ha proporcionado una serie de consideraciones ciertamente válidas para el diseño eficiente de mecanismos de provisión de QoS:

- Retardo.
- Pérdidas de paquete.
- Ancho de banda disponible.
- Variación del retardo. Jitter

Son características del tráfico generado por las aplicaciones que condicionan el diseño del mecanismo de provisión de QoS, y que serán estudiadas mas adelante en el capitulo de QoS en redes 4G.

2. La evolución de la red y de la arquitectura TCP/IP

La red de acceso conecta los terminales de los usuarios con el núcleo troncal de la red, que es el que concentra los grandes volúmenes de tráfico IP que circulan por Internet. Tanto el acceso, como la red troncal utilizan el marco arquitectural común que crea TCP/IP. La red de acceso, la red troncal y la arquitectura TCP/IP tienen retos importantes y se encuentran en permanente evolución como todo en Internet. Vamos a describir de forma muy simplificada en este apartado la evolución de las tecnologías de la red troncal, así cómo de su arquitectura, complementando las reflexiones ya realizadas sobre la evolución del acceso o de la seguridad.

Como ya hemos analizado la función principal de la arquitectura TCP/IP es desacoplar la red de las aplicaciones, de forma que ambas puedan evolucionar de forma independiente. Esto ha permitido que Internet incorpore nuevas tecnologías de red a medida que aparecen, mientras la red sigue funcionando. La nueva Internet debe seguir manteniendo este principio de funcionamiento, que es una característica común a todas las arquitecturas de redes de telecomunicación estructuradas por niveles y no solo de Internet.

La arquitectura de Internet tiene plateados varios retos importantes que limitan sus posibilidades y que irán haciendo evolucionar las tecnologías de red durante los próximos años. Los más importantes son:

- Introducir un direccionamiento jerárquico que simplifique y haga mas eficiente el encaminamiento de paquetes IP a través de la red.
- Solucionar la escasez de direcciones de la versión actual del protocolo IP, conocida como IPv4 por ser la versión 4 de dicho protocolo.
- Introducir calidades de servicio adecuadas para transmitir voz y vídeo de buena calidad sin perder la eficacia de IP en los servicios de datos.

- Soportar de forma eficaz difusión de contenidos en tiempo real a toda la red y comunicación interactiva de grupos en tiempo real.
- Soportar acceso inalámbrico, movilidad de terminal y movilidad personal.
- Introducir mecanismos de señalización que permitan crear servicios similares a los existentes en las redes telefónicas actuales.
- Incorporar protocolos de seguridad en la arquitectura TCP/IP que permitan proteger la información y las actividades que se realizan a través de Internet.

La solución a todos estos problemas pasa por un rediseño muy significativo de la arquitectura TCP/IP. Durante los últimos años se han desarrollado múltiples propuestas de protocolos que solucionen o mejoren estos problemas. Pasamos a describir algunas de las propuestas que han alcanzado un alto grado de consenso y que parece van a ser los componentes fundamentales de la nueva arquitectura TCP/IP.

2.1. La transición de IPv4 a IPv6

La escasez de direcciones IP públicas, así como la introducción de un direccionamiento jerárquico en Internet son dos problemas cuya solución parece estar asociada a la sustitución del protocolo IP actual (IPv4) de la arquitectura TCP/IP, por la versión 6 de IP (IPv6). IPv6 está considerado actualmente cómo la única vía posible para seguir desarrollando la arquitectura de Internet de acuerdo a los principios de diseño con los que fue concebida.

La introducción de IPv6 será un proceso complejo y costoso, pero creará una arquitectura de Internet mucho más adaptada a los requerimientos de uso actual y sobre todo futuro.

IPv6 facilita también la introducción de protocolos que den solución a los otros retos de la arquitectura TCP/IP, tales como seguridad, movilidad, calidad de servicio, comunicación de grupo en tiempo real, etc. IPv6 es además extensible y permitirá incorporar nuevos protocolos en el futuro a medida que sean demandados. La introducción de los protocolos que implementan los nuevos servicios necesita reconfigurar y modificar todos los routers e implementaciones de IP existentes en Internet, por lo que es muy probable que la introducción masiva de estos nuevos servicios se realice asociada al despliegue de IPv6.

Una Internet basada en IPv4 puede sobrevivir todavía por algún tiempo a base de parches, suponiendo que el crecimiento de la red sea limitado. Pero a medida que pase el tiempo, el coste real y de oportunidad de mantener la arquitectura actual será cada vez mayor. A pesar de que algunos de los nuevos servicios pueden ser desplegados en IPv4, su despliegue requerirá cambios que pueden llegar a tener costos similares a los de la introducción de IPv6, pero sin obtener los beneficios de una nueva arquitectura adaptada al uso masivo que ha alcanzado Internet.

La transición a IPv6 parece haber comenzado ya, tanto en el mundo de la investigación, como en los países del sudeste asiático o en organismos que han comprendido que la transición va a ser compleja y es conveniente empezar a realizarla ya:

La mayoría de las redes académicas europeas, norteamericanas, así como de otros países desarrollados ya han instalado en sus routers doble pila

IPv6/IPv4, para soportar tanto el envío de paquetes IPv6 como IPv4. Por ejemplo, RedIris en España, GEANT en Europa, Internet2 en EEUU, además de muchas otras redes de países desarrollados.

El Departamento de Defensa de EEUU obliga a que cualquier equipo adquirido después de octubre del 2003 soporte IPv6 y todas las redes del DoD deben haber incorporado IPv6 para el 2008.

Los países con economías más desarrolladas de la región Asia-Pacífico, así como los que no poseen suficientes direcciones IPv4 ya han comenzado la transición acelerada a IPv6. Por ejemplo, Japón, Corea, Taiwan, China, etc.
La Comisión Europea, así como la mayoría de los países desarrollados han creado “IPv6 Task Forces” con la finalidad de promover y estudiar la mejor forma de realizar la transición en cada uno de esos países.

Cada vez más ISPs ofrecen servicios precomerciales IPv6 en Europa y Norteamérica.

La introducción de servicios multimedia en UMTS también debe crear una gran demanda direcciones IPv6. Actualmente existen 800 millones de abonados GSM en el mundo y este número crece rápidamente. Todos estos abonados deberán pasar a UMTS en un futuro no muy lejano y necesitarán direcciones IPv6 para los servicios multimedia IMS de 3GPP. El primer gran cambio introducido por IPv6 es por supuesto una nueva dirección de mayor tamaño (128 bits) que permite dar aproximadamente 1038 direcciones públicas diferentes, es decir $340x10^{36}$ direcciones públicas. El número es tan grande que parece imposible agotarlo, aunque es muy probable fue la tecnología del futuro necesite muchas más direcciones de las que podamos imaginar hoy y este espacio también se agote algún día. En 1970 las

aproximadamente 4.000.000.000 direcciones del protocolo IPv4 parecían totalmente suficientes.

La introducción de IPv6 permitirá solucionar o mejorar otros problemas de Internet, tales como:

1. La asignación jerárquica del espacio de direcciones que permita una red más eficaz, escalable y robusta. Las tablas de direccionamiento de los routers son actualmente de gran tamaño debido a las asignaciones de clases A, B y C realizadas durante los primeros años en Internet. Una asignación jerarquizada reduciría mucho el tamaño de las tablas de encaminamiento, haciendo la conmutación mucho más eficaz. Esto no es en realidad un mérito de IPv6, sino de los organismos que asignen direcciones. IPv4 también podía haber tenido un espacio de direccionamiento jerárquico, si las direcciones se hubiesen asignado de otra forma. Hoy en día ya es imposible reordenar el espacio de direcciones de IPv4, por lo que la introducción de un espacio de direccionamiento jerarquizado en Internet solo parece posible en IPv6 donde se están siguiendo unos procedimientos de asignación de bloques de direcciones muy rigurosos.

2. Simplifica la gestión de los PCs conectados a la red, soportando de forma automática la conexión de nuevos PCs (*plug and play*) sin necesidad de configurarlos explícitamente. La renumeración de redes se simplifica significativamente.

3. Elimina más de la mitad de sus campos de la cabecera del paquete IP para simplificar el diseño de los routers. También ha eliminado las funciones más costosas de procesar, tales como fragmentación, opciones, etc.

4. IPv6 incluye como componente obligatorio el protocolo de seguridad IPsec e integra más eficazmente que IPv4 facilidades tales como distintos grados de calidad de servicio (QoS), movilidad IP, multicast o anycast.

El mayor problema para la introducción de IPv6 en Internet está en cómo realizar la transición de IPv4 a IPv6 de forma que no se interrumpa el servicio. Durante los últimos años IETF ha desarrollado múltiples mecanismos de transición y coexistencia entre IPv4 e IPv6[2]. Estos mecanismos están siendo evaluados exhaustivamente por los fabricantes de routers y PCs, así como por grandes proyectos de investigación (en Europa por ejemplo LONG, Euro6IX o 6net), además de por múltiples laboratorios de investigación, tal y como se hace con todos los protocolos importantes de Internet. Estas evaluaciones están mostrando que IPv6, así como los mecanismos de transición han alcanzando un alto grado de madurez.

El mecanismo de transición más importante es la doble pila IPv6/IPv4. Los computadores que instalen doble pila podrán comunicar con ordenadores de la vieja (IPv4) y la nueva (IPv6) Internet. Ya se han realizado múltiples experimentos que han validado completamente la posibilidad de convivencia de ambos protocolos. Además hay muchos otros mecanismos de transición, basados en traductores entre IPv6 e IPv4 o en túneles, que permitirán la interoperabilidad de los nuevos sistemas que sólo tengan IPv6 con el mundo IPv4. Curiosamente uno de los mecanismos, denominado NAT-PT, está basado en NAT. Igual que NAT permite acceder a servicios IPv4 desde una red privada, NAT-PT permite acceder a servicios IPv4 desde una red IPv6.

[2] "Realizing the Transition to IPv6", D. Waddington and F. Chang. IEEE Communications Magazine, June 2002, Vol. 40, No.6, pp. 138-148.

Otro problema, probablemente de mayor envergadura que el anterior, es la migración de aplicaciones a IPv6. Las aplicaciones IPv6 también utilizan TCP, UDP y el interfaz de sockets, pero sobre IPv6 o doble pila (IPv4/IPv6), en vez de sobre IPv4. El interfaz de sockets ha sido adaptado en sus múltiples versiones para utilizar IPv4, IPv6 o doble pila. Su uso es muy similar al que se hacía en IPv4, pero incluye pequeñas diferencias que obligan a realizar nuevas versiones de las aplicaciones existentes, para poder migrar a IPv6. La migración de aplicaciones de IPv4 a IPv6 no es difícil si éstas se han diseñado haciendo un uso adecuado de este interfaz. Incluso, algunos lenguajes como Java hacen que la migración sea prácticamente transparente al pasar a una versión del lenguaje que soporte IPv6, como Java 1.4.

La migración de todas las aplicaciones existentes necesitará un enorme volumen de trabajo, la mayor dificultad está en el porte de las aplicaciones que hicieron mal uso de las direcciones IPv4 y del interfaz de sockets, que requieren un rediseño muy significativo de la aplicación.

2.2. La calidad del servicio TCP/IP

La calidad de servicio de una comunicación a través de una red de transporte se mide por la velocidad máxima de envío de información, las perdidas de bloques de información en la transmisión, así como por el retardo introducido por la transmisión. La enorme eficiencia de Internet se debe a que el protocolo IP se diseño para dar un servicio que no garantiza la calidad de servicio, ni la entrega de los paquetes a su destinatario, conocido en inglés como servicio “Best Effort”. La enorme ventaja de este servicio es su simplicidad, porque los routers pueden tirar paquetes en situaciones de congestión. Cuando no hay congestión la transmisión es de buena calidad,

pero cuando los paquetes pasan por un router congestionado la calidad se degrada y se producen pérdidas y retrasos muy significativos.

A pesar de que el ancho de banda en Internet ha aumentado muy significativamente, sigue habiendo congestión en muchos puntos de la red. Los puntos de congestión degradan la calidad del transporte aunque exista exceso de ancho de banda en todo el resto de la ruta.

La mayoría de las aplicaciones de Internet utilizan el protocolo TCP para proteger frente a las perdidas de paquetes que ocurren en situaciones de congestión, por lo que la existencia de perdidas de paquetes en la red nunca ha sido un problema importante. En cambio, los protocolos de la arquitectura multimedia de Internet envían los flujos de audio y de vídeo como paquetes UDP que no van protegidos frente a las perdidas en la red, por lo que las situaciones de congestión pueden degradar la calidad del audio y vídeo hasta hacerlo ininteligible. La razón de utilizar UDP es que introduce menor retardo que TCP, siendo esto un requisito importante de la transmisión de audio y vídeo.

Por estas razones, tanto IETF, como el mundo investigador, llevan tiempo trabajando en el desarrollo de técnicas que permitan controlar la calidad de servicio directamente a nivel del protocolo IP, de forma que las aplicaciones de envío de audio y vídeo pueden disponer de calidades de servicio IP sin pérdidas ni retrasos significativos.

IETF ha desarrollado dos propuestas de control de la calidad del servicio de transporte de información para la transmisión de voz y vídeo con calidad a través de Internet, que han alcanzado un apoyo considerable y son conocidas como IntServ (Integral Services) y DiffServ (Differentiated Services).

IntServ fue la primera propuesta en aparecer. IntServ proponía en sus primeras versiones utilizar el protocolo de señalización RSVP como un protocolo extremo a extremo de reserva de admisión y recursos que garantizasen la calidad de servicio para cada flujo de tráfico individualmente. IntServ necesita reservar recursos en cada router de forma individualizada para cada flujo, por lo que presenta problemas de escalabilidad. Actualmente ha pasado a ser considerado solamente como un protocolo de señalización para solicitar calidad de servicio en terminales y aplicaciones de usuario. Su función tiene grandes paralelismos con la función de señalización que SIP desempeña por lo que no es descartable que exista una cierta convergencia entre ambos.

DiffServ no es un protocolo de calidad de servicio extremo a extremo, sino que propone marcar los paquetes cuando entran en un dominio DiffServ con una marca de tipo de tráfico que es utilizada por los routers para hacer un reenvío diferenciado de los paquetes. Esto permite que los paquetes de voz y vídeo se marquen como prioritarios para que adelanten a los paquetes no prioritarios de datos (Web, correo, etc) en los routers, minimizando de esta forma el retardo y las perdidas. El bajo costo computacional de esta técnica permite una eficaz integración en los routers IP, por lo que se considera uno de los componentes clave para la integración de voz y datos en Internet. La tendencia actual es a utilizar una combinación de InteServ[3] y DiffServ[4], donde el núcleo central de la red implementa DiffServ, mientras que IntServ y RSVP se utilizan para que las aplicaciones soliciten la calidad de servicio requerida en el acceso así como a los routers del borde de la zona DiffServ, que serían los encargados de marcar los paquetes.

[3] IETF Intserv Working Group - http://www.ietf.org/html.charters/intserv-charter.html
[4] IETF Diffserv Working Group - http://www.ietf.org/html.charters/diffserv-charter.html

También existen defensores de otra estrategia de control de la calidad de servicio, denominada “throw bandwidth”, que propone simplemente aumentar el ancho de banda disponible lo suficiente como para evitar situaciones de congestión en la red. Aunque a primera vista esta propuesta puede parecer carente de lógica, la relación capacidad/costo en los enlaces cableados y en los conmutadores de alta velocidad ha aumentado tanto que quizá la estrategia de tener redes sobredimensionadas sin control de calidad de servicio acabe siendo la solución más económica. Por supuesto esta estrategia no es aplicable en los accesos inalámbricos donde la integración del envío de voz con servicios de datos solo podrá realizarse utilizando alguno de los mecanismos anteriores de control enlaces inalámbricos.

2.3. Movilidad personal y de terminal

La movilidad, tanto de terminal, como personal, crea un escenario de gran complejidad en el que se involucran muchos servicios de Internet, además del tipo de identificación de usuario y de terminal utilizado. Internet ha utilizado tradicionalmente el DNS (Domain Name System) para identificar terminales, dando un nombre simbólico (de dominio) a un terminal y asociando a dicho nombre una dirección IP, que identifica dicho terminal en la red. El DNS permite determinar la dirección IP asociada a un nombre simbólico y viceversa. El protocolo MIP (Mobile IP), en desarrollo en IETF (solo está estable la RFC de MIP para IPv4), está pensado para establecer conectividad con terminales que se desplazan de un punto a otro de la red y son identificados a través de su dirección IP, que se obtiene a partir de la dirección de dominio.

El protocolo MIP actúa a nivel IP, independizando las aplicaciones de la movilidad. Las aplicaciones siguen funcionando, aunque el usuario se haya desplazado de un lugar a otro de la red, incluso funcionan cuando está en movimiento aunque puede sufrir interrupciones temporales significativas de conectividad. La movilidad a nivel de IP se denomina macro-movilidad y permite el cambio de la dirección IP cuando el terminal pasa de una red a otra. El protocolo MIP soporta solamente movilidad de terminal.

Además están los protocolos de micro-movilidad que son complementarios de los de macro-movilidad. Un protocolo de micro-movilidad gestiona desplazamientos dentro de un mismo dominio de celdas de acceso inalámbrico, con el objetivo de minimizar la perdida de información durante el paso de una celda a otra. Existen diversas propuestas para micro-movilidad en desarrollo. HMIP (Hierarchical Mobile IP) es la propuesta en desarrollo en IETF.

La gestión de movilidad proporcionada por SIP[5] da un paso más y permite movilidad personal, es decir que una persona pase a recibir llamadas de un terminal a otro, por ejemplo de su ordenador personal al móvil. Por eso las direcciones SIP identifican usuarios y no terminales. Una dirección SIP tiene forma de URL e identifica a un usuario, por ejemplo "sip:JorgeMarimon@conmutex.com". La estructura del URL es muy similar a la del correo electrónico. SIP ha sido diseñado para que los usuarios no estén asociados a una posición física en la red, sino a un servicio de localización.

[5] "Internet Communications using SIP", H. Sinnreich, A. Johnston. John Wiley & Sons, Inc, 2001, ISBN: 0-471-41399-2.

Cada usuario registra en dicho servicio, cuando se desplaza, su nueva localización o su nuevo terminal.
La creación de una sesión SIP empieza con una solicitud de creación de sesión, enviada por el usuario llamante al servicio de localización de usuarios. Este intenta localizar al usuario llamado en el último terminal registrado. Si la localización funciona correctamente, llamante y llamado se ponen en contacto y establecen la sesión. Cuando un usuario se desplaza de un lugar a otro de la red, debe notificar dicho desplazamiento al servicio de localización de usuarios. El soporte a movilidad personal de SIP es complementario de la macro o la micro movilidad, pudiéndose utilizar los tres conjuntamente.

La gestión de movilidad proporcionada por SIP es enormemente flexible y permite incluso interoperabilidad con la red telefónica. Internet y la red telefónica van a coexistir durante bastante tiempo y hace falta un marco de interoperabilidad entre ambas. Los grupos de trabajo de IETF llevan desarrollando este marco con el objetivo de integrar ambas redes en un marco de uso común, de forma que desde Internet exista acceso a los servicios y usuarios de la red telefónica. Es previsible que en esta área se desarrollen múltiples servicios en el futuro.

Por ejemplo, en telefonía cada usuario se identifica con un número de teléfono, que aunque es una forma poco amigable de identificar usuarios, está tan extendida, que SIP también permite identificar usuarios a través de un número telefónico.

Se están creando algunos servicios muy ambiciosos en esta dirección que integran el acceso a través de teléfono con el acceso a través de Internet. Por ejemplo en un servicio de acceso a través de DNS a perfiles de usuario identificados por números de telefónicos, donde los registros en DNS pueden

guardar perfiles y datos de usuarios asociados a sus múltiples formas de acceso (teléfono fijo y móvil, fax, PCs, etc.), facilitando la localización de las diversas formas de contacto de un usuario determinado.

3. Movilidad IP

3.1. Protocolo IP Móvil

El protocolo IP Móvil fue creado para proporcionar movilidad a los nodos dentro de Internet[6]. Su diseño se basó desde un comienzo sobre las siguientes premisas mínimas e indispensables:

- El nodo móvil debe ser capaz de comunicarse con los demás nodos aún después de haber cambiado su punto de conexión a Internet.
- Esta comunicación debe efectuarse siempre con una única dirección IP para el nodo móvil que deberá ser su dirección IP en la red de origen, se encuentre donde se encuentre.
- El nodo móvil debe ser capaz de comunicarse con otros nodos que no implementen las funciones de movilidad del protocolo Mobile IP.
- El nivel de seguridad y de privacidad de las comunicaciones de un nodo móvil no debe ser menor que el de cualquier otro nodo fijo.
- El medio entre el nodo móvil y su punto de conexión a Internet será a menudo un enlace inalámbrico. Muy probablemente, el nodo móvil estará alimentado por pilas o baterías, lo que hace importante minimizar el consumo reduciendo al mínimo el número de mensajes de señalización.

Para entender en lo que consiste el protocolo de Internet móvil, describiré un ejemplo sencillo de fácil comprensión:
Si nos encontramos de viaje de negocios o vacaciones durante un año pasando por diferentes ciudades, es necesario que las cartas de correo o

[6]Oliver, Miquel. Mobile IP: una solución para proporcionar la movilidad de los terminales en Internet. Universidad Politécnica de cataluña.

nuestra correspondencia lleguen a la dirección correcta donde nos encontramos, si la dirección de nosotros cambia cada dos semanas por que nos encontramos en lugares diferentes, la pregunta que nos deberíamos hacer es, ¿Qué hacer para que las cartas lleguen a su destino en tales circunstancias?

Nuestra Primera solución seria: Enviar una tarjeta de cambio de dirección a todos los interesados en enviarme correo durante el tiempo que yo me encuentre en el lugar. Pero el problema seria el siguiente:

Todas las tarjetas deben enviarse cada vez que se llegue a una nueva ciudad, se deben enviar a todas las personas involucradas en enviar correo, no se puede prevenir el hecho de que algún gracioso envía falsas tarjetas de cambio de dirección.

Una segunda solución seria: Dejar una nota de seguimiento en la oficina postal y toda carta que llegue a la oficina será enviado a la dirección actual donde nos encontremos. Una ventaja seria: solo se envía la tarjeta de cambio a una sola persona, y la seguridad de que la oficina solo hará el seguimiento si esta seguro de la identidad de la persona que envío la tarjeta.

Lo bueno de esta solución es que la oficina postal puede darle seguimiento a esta carta, y los corresponsales pueden volver a enviar sus cartas, si no han recibido un acuse de recibo durante un tiempo dado. Si alguna carta se pierde temporalmente durante un cambio de dirección al momento que este era transmitido esta será devuelta a la anterior dirección, para que vuelva a ser enviada.

Para entender el principio de funcionamiento de lP Móvil según el ejemplo anterior, tendríamos:

carta = paquete de datos Protocolo Internet
dar seguimiento a la carta = tuneleo
oficina correo = ruteador IP móvil

El principal objetivo del protocolo IP Móvil es sencillo: permitir el encaminamiento de paquetes IP hacia nodos móviles que pueden cambiar rápidamente su punto de conexión a Internet. Este objetivo implica la transmisión de actualizaciones de encaminamientos entre numerosos nodos de la red. Para permitir su uso a través de un gran número de enlaces inalámbricos, es muy importante reducir el tamaño y la frecuencia de estas actualizaciones al mínimo posible.

Por otra parte, para que el protocolo IP Móvil pueda ser soportado por el mayor número posible de nodos, se requiere que su implementación software sea lo más sencilla posible en términos de carga computacional y memoria.

De esta manera, tanto computadores portátiles como otros instrumentos con prestaciones hardware reducidas, como por ejemplo buscapersonas, teléfonos celulares u organizadores personales puedan gozar de la funcionalidad del protocolo.

Por último, cabe destacar el importante problema que supone la escasez de direcciones IP versión 4. El protocolo IP Móvil contribuye claramente a la no proliferación de nuevas direcciones IP ya que asigna a cada nodo móvil una única dirección IP en todo momento.

3.1.1. Funcionamiento

¿Que es una tabla de ruteo?

Cuando un paquete llegue a un nodo IP, puede ser que el nodo sea su destino final o cualquier otro nodo es su destino final. Todo nodo IP sea un host o ruteador tiene una tabla de ruteo para tomar sus decisiones de seguimiento de paquetes.

Cada entrada en la tabla tiene cuatro campos:

- Destino
- Longitud Prefijo
- Próximo Router
- Interfaz

3.1.2. Decisión de seguimiento

Cada paquete llega al nodo y esta busca una coincidencia en las entradas de la tabla, para enviarlo al próximo router vía un enlace o interfaz.

Coincidencia (match): si los bits más significativos (longitud-prefijo primeros bits) del campo destino son iguales a los del destino del encabezado del paquete. Si existe más de una coincidencia, se toma la entrada con la mayor longitud-prefijo.

Ejemplo: Tabla de Ruteo

Destino/Long.	Prox. router	Interfaz
7.7.7.99/24	Ruteador 1	a
7.7.7.0/24	Ruteador 2	a
0.0.0.0/0	Ruteador 3	a

Tabla 3. Tabla de Ruteo

Números en **negrillas**: campos de longitud-prefijo.

Ejemplo:

Paquete con encabezado 7.7.7.1

3.1.3. Características de ruteo en IP

Cada nodo toma su propia decisión basándose solo en la dirección destino del encabezado IP, la dirección fuente solo es consultada cuando ocurre un error de envío, la *decisión de ruteo* se toma en base al prefijo de red de la dirección IP, cada nodo en la misma línea debe de tener una dirección de red idéntica.

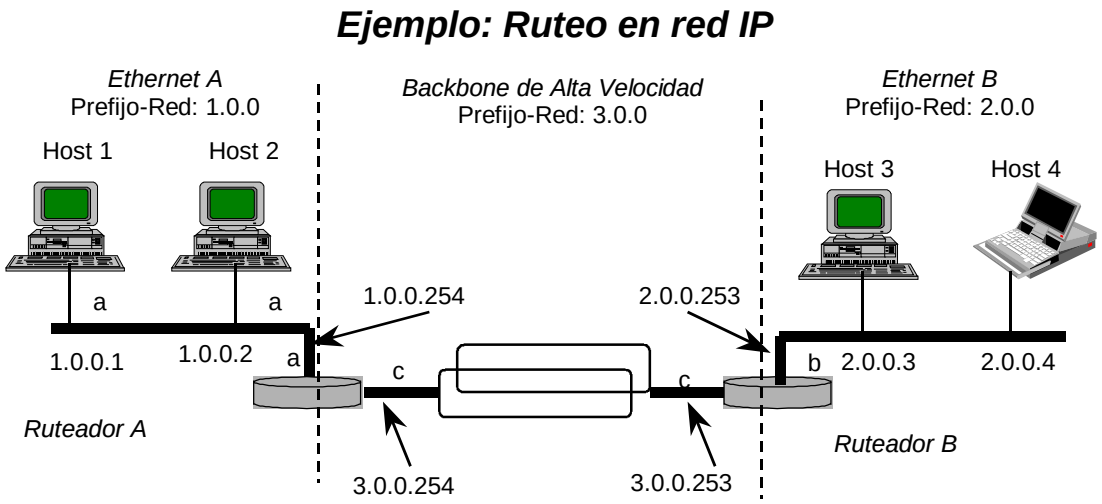


Tabla ruteo Ruteador A

Destino/Long.	Prox. router	I/f
1.0.0.2/ 24	directo	a
0.0.0.0/ 0	1.0.0.254	a

Tabla ruteo Ruteador B

Destino/Long.	Prox. router	I/f
1.0.0.2/ 24	3.0.0.254	c
2.0.0.4/ 24	directo	b
3.0.0.0/ 24	directo	c

Figura 4. Ruteo en red IP

3.1.3.1. Porque solo el prefijo de red

Alternativa a prefijo-red es prefijo-host, cada nodo tiene tabla de ruteo con todos los hosts y ruteadores de la red, en Internet existen cientos-millones de hosts, lo que produciría que los ruteadores necesitarán mucha memoria y la búsqueda de direcciones fuera más lenta, los intercambios de información de los ruteadores serían de billones de bytes y la capacidad de los enlaces en Internet se saturarían.

Las entradas en las tablas de ruteo son creadas, estáticamente, por configuración manual de un ser humano, dinámicamente, a través de paquetes ICMP; dinámicamente, por el cambio automático de información de ruteo en forma de protocolos de ruteo.

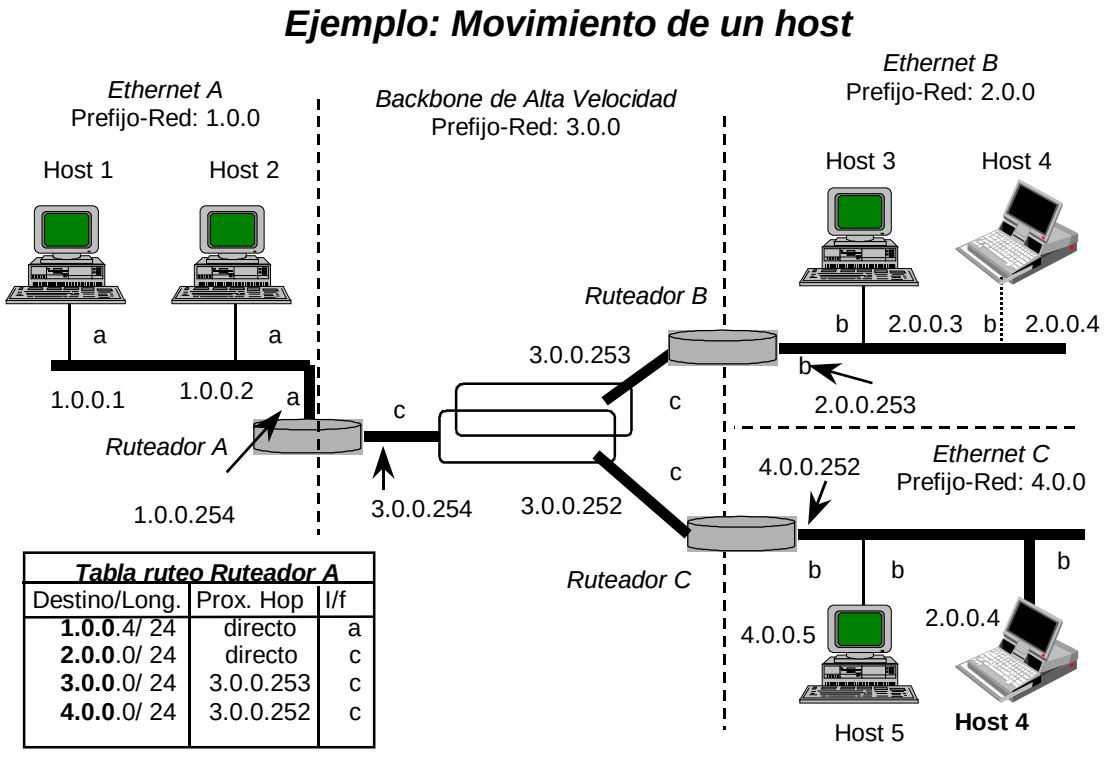


Figura 5. Movimiento de un host

3.1.3.2. Solucionando el problema de ruteo por el cambio del host 4

1. Establecer rutas especificadas host en las tablas de ruteo de los ruteadores A, B y C

Las tablas quedarían:

- **Ruteador A:**
  Destino/Long. **2.0.0.4**/ 32
  Prox. Router: 3.0.0.252,
  Interfaz: c

- **Ruteador B:**
  Destino/Long. **2.0.0.4**/ 32
  Prox. Router: 3.0.0.252
  Interfaz: c

- **Ruteador C:**
  Destino/Long. **2.0.0.4**/ 32,
  Prox. Router: directo
  Interfaz: b

3.1.3.3. Que tipo de ruteo utilizar

En general ruteo especificado en nodo no es bueno, ruteo en base a nodo es bueno para movilidad en Internet, determinar cuando rutas basadas en nodos usados solo en nodos móviles que no están conectadas a sus enlaces hogar es una solución razonable en el contexto del Internet global.

Para calcular el numero de rutas basadas en nodos que se requieren para poder implantar movilidad en Internet dependen del número total de nodos móviles que se espera ver en Internet y del número mínimo de nodos a los que se necesita propagar las rutas de acuerdo a cada nodo móvil y a la velocidad a la que los nodos móviles se mueven de un enlace a otro y el número de rutas que necesitan ser actualizadas.

Para calcular el numero de nodos móviles es necesario:

1. Un incremento dramático en desempeño de memoria y CPU.
2. Decremento en tamaño, peso y consumo de potencia.
3. Computadoras móviles serán un gran factor en el mundo Internet.

La solución debe de considerar, como mínimo, millones de nodos móviles.

3.1.3.4. Cuantas rutas se necesitan por nodo móvil

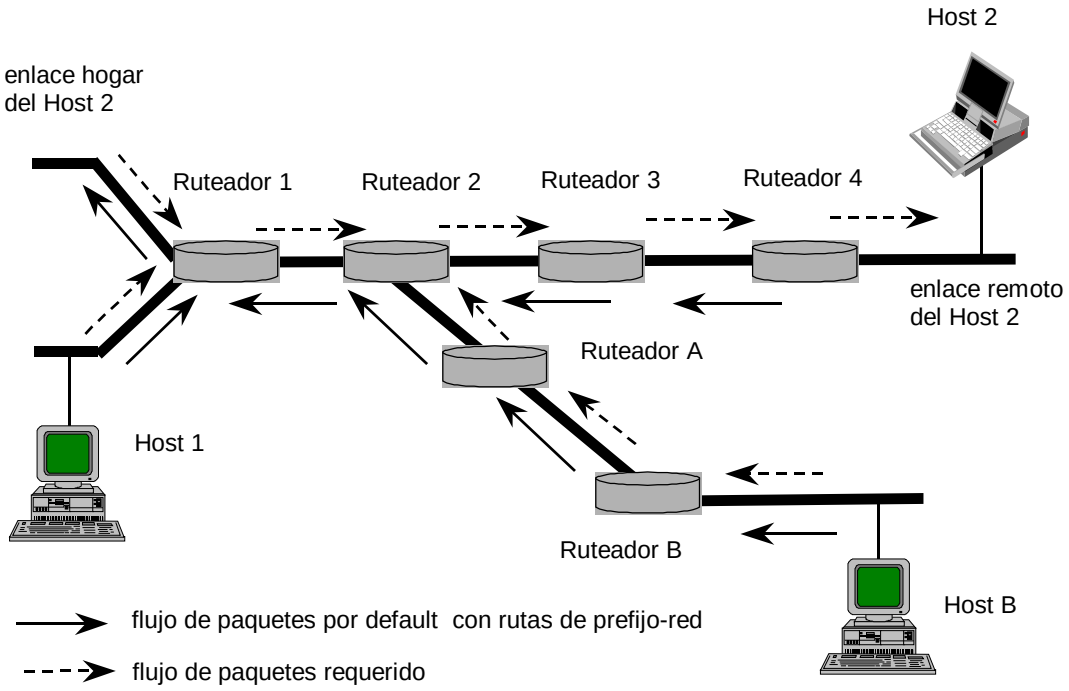


Figura 6. Rutas que se necesitan por nodo móvil

3.1.3.5. Consecuencias por el cambio de nodo

En general las rutas en los nodos de la rama actual al punto viejo deben borrarse y las nuevas rutas deben añadirse en la misma rama. Y la ruta en la misma rama debe de modificarse.

Todo esto debe de propagarse a los nodos por los que paso y a cambios de nodos muy frecuentes, por lo que una buena solución para Internet es una que no requiera de muchos cambios.

3.1.3.6. Para una solución mas robusta por el cambio de nodo

Si las rutas son propagadas solo a un conjunto mínimo de nodos entonces cada uno de estas rutas y los enlaces entre ellos se transforman en puntos de falla y la capacidad de detectar y dar la vuelta a fallas de red no es posible si se usa un mínimo de rutas.

Cualquier tipo de solución involucra propagar información a un número muy grande de nodos.

3.1.3.7. Porque no cambiar la dirección IP

Si lo anterior no fue una buena solución, porque no cambiar la dirección IP cuando el nodo se mueva de enlace.

Ruteo prefijo-red : todos los nodos de un enlace tienen el mismo prefijo-red en su dirección IP.

Cuando un nodo se cambie, debe cambiar este prefijo-red y el nodo debe conservar su prefijo-host siempre y cuando este no sea utilizado por otro en el nuevo enlace.

Una vez cambiada su dirección el nodo debe poder comunicarse en el nuevo enlace usando su nueva dirección IP en todos las comunicaciones futuras.
Sin embargo, ¿qué pasa si se envía un mensaje durante el cambio de dirección?

La conexión TCP dentro de un nodo es identificada a partir de: Dir. Fuente, Dir. Destino, Num. Pto Fuente, Num. Pto. Destino.
La mayor parte de aplicaciones asumen que estos datos no varían durante la conexión.

3.1.3.8. Ventajas del cambio de dirección IP

Se resuelve el problema de "*nomadicidad*". Un nodo nómada es aquel que debe terminar todas sus comunicaciones existentes antes de cambiar su punto de conexión, pero puede empezar nuevas comunicaciones una vez que se conectó de nuevo.
Existen mecanismos dentro de Internet que direccionan nodos nómadas (DHCP).

3.1.3.9. Para encontrar dirección de nodo móvil

El nodo fijo desea enviar paquete a un nodo móvil, este pregunta a DNS, pero existen dos problemas:

- Dirección nodo móvil debe actualizarse en el DNS cada vez que este cambia de enlace.

- Cuando nodo fijo obtiene una dirección del DNS debe tomar en cuenta que este puede cambiar en cualquier momento.

Como conclusión podemos decir que cambiar la dirección IP de un nodo móvil no es una buena solución.

Además de esto, el funcionamiento del protocolo IP Móvil consiste en la consecución de la siguiente serie de operaciones:

- Los agentes local y externo anuncian su presencia al nodo móvil mediante *mensajes de anunciamiento* que se generan periódicamente en la red. Opcionalmente, el nodo móvil puede solicitar tales mensajes a un agente cercano a través de un *mensaje de solicitud de agente*.

- El nodo móvil recibe el mensaje de anunciamiento y determina si se encuentra en su red local o en una red externa. Si el nodo móvil deduce que se encuentra en su red local, opera sin funciones de movilidad. Por otro lado, si ha regresado tras haber sido registrado en otra red, procede a *desregistrarse* a través de su agente local. Si el nodo móvil detecta que se encuentra en una red externa, obtiene su *dirección de auxilio* (care-of-address) en la nueva red. Esta dirección puede ser la del agente externo o una *dirección de auxilio colocada* (colocated care-ofaddress).

- Si el nodo móvil se encuentra fuera del alcance de ningún tipo de agente, el nodo móvil debe obtener su *dirección de auxilio* como una dirección IP local por algún método como, por ejemplo DHCP (Dynamic Host Configuration Protocol). En estos casos, se trata de una dirección de auxilio “colocada”.

- El nodo móvil registra su dirección de auxilio con su agente local. Este proceso se realiza enviando una *solicitud de registro* al agente local y recibiendo de éste un mensaje de contestación.

- Todo paquete destinado al nodo móvil es interceptado por el agente local y enviado mediante *tunneling* por éste hacia la dirección de auxilio. Al otro lado del túnel, el agente extranjero recibe el paquete y lo envía al nodo móvil. Si el nodo móvil posee una dirección de auxilio colocada, el agente extranjero no interviene en la recepción del paquete.

- Por su parte, los paquetes originados por el nodo móvil pueden ser transportados hasta la dirección IP de destino sin pasar necesariamente por el agente local.

3.1.4. Procedimientos

3.1.4.1. Descubrimiento de agente

El *descubrimiento de agente* es un procedimiento utilizado en el protocolo IP Móvil mediante el cual el nodo móvil determina si se encuentra conectado a su red local o a una red extranjera, si se ha desplazado de un enlace a otro, y también sirve para obtener una dirección de auxilio cuando se encuentra conectado a un red extranjera. El procedimiento mediante el cual se realiza el descubrimiento de agente es relativamente sencillo y precisa únicamente de dos tipos de mensaje:

- El de *anunciamiento de agente* y otro de *solicitud de agente*.

3.1.4.2. Anunciamiento de Agente

La primera acción a realizar para permitir la movilidad de un nodo es la de anunciar por parte del agente local o externo de la disponibilidad para aceptar al nodo móvil en su red. El nodo móvil utiliza mensajes de anunciamiento para determinar su punto de conexión actual a Internet. El agente local deberá estar siempre listo para servir a sus nodos móviles. Para evitar una posible saturación debida al exceso de nodos móviles en una determinada red, es factible configurar múltiples agentes locales en una única red local, asignando a cada agente local una porción de la población de nodos móviles.

Por otro lado, es plausible que un agente externo no tenga capacidad para servir a un nodo móvil no perteneciente a su red. Aún en ese caso, el agente externo debe continuar emitiendo mensajes de anunciamiento para que el nodo móvil sepa que se encuentra dentro de su área de cobertura o que no ha fallado.

Ejemplo de Broadcast anuncio agentes

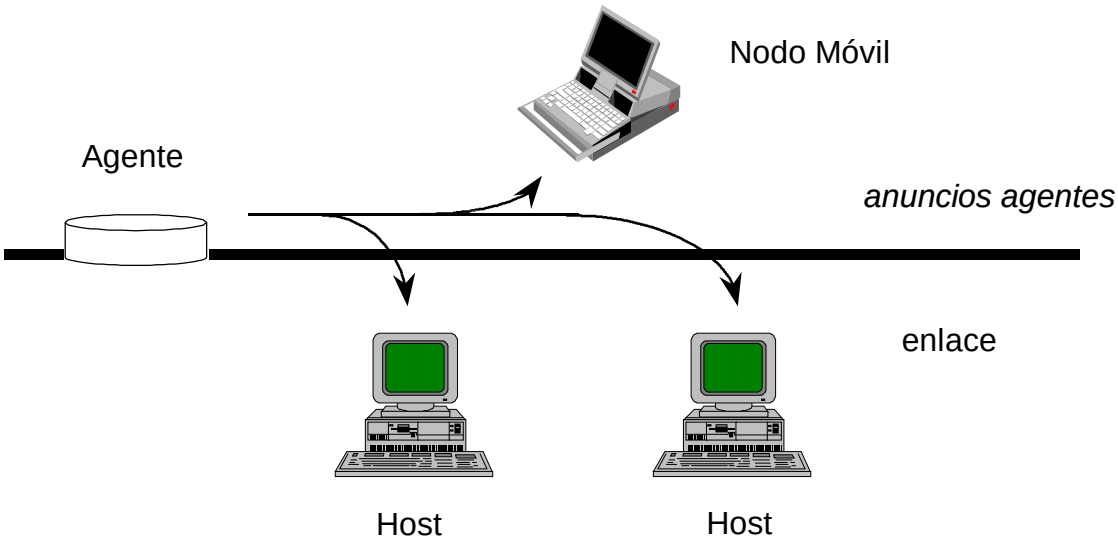


Figura 7. Broadcast anuncio agentes

El mensaje de anunciamiento consiste en un mensaje ICMP de anunciamiento de *router* al cual se le ha añadido una extensión para permitir la gestión de los nodos móviles. Esta extensión tiene la forma que presentamos en la figura.

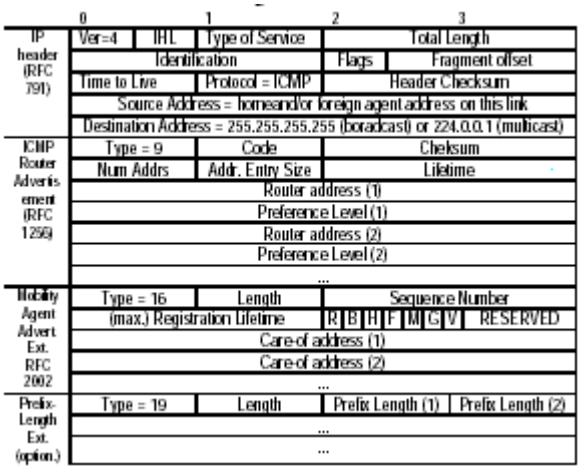


Figura 8. Mensajes de Anunciamiento de Agente

Los campos de la extensión de anunciamiento de agente son los siguientes:

- **Type 16**
- **Length (6+4*N)**, donde N es el número de direcciones de auxilio anunciadas.
- **Sequence number** Número total de mensajes de anunciamiento enviados desde que el agente fue inicializado.
- **Registration lifetime** Tiempo de vida máximo (s) que este agente acepta en una solicitud de registro. (65,535=¥)
- **R** Registro solicitado. Es conveniente registrar con un agente extranjero en vez de usar una dirección de auxilio colocada.
- **B** El agente extranjero no puede aceptar nuevos registros, al estar ocupado (Busy)

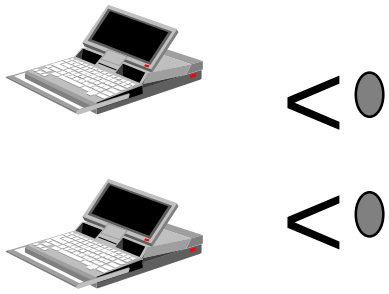
- **H** Este agente ofrece servicios de agente local (Home Agent) en esta red.
- **F** Este agente ofrece servicios de agente extranjero (Foreign Agent) en esta red.
- **M** El agente soporta encapsulado mínimo.
- **G** El agente soporta encapsulado GRE.
- **V** El agente soporta la compresión de cabecera Van Jacobson.
- **Reserved** Reservado.
- **Care-of addresses** La dirección de auxilio anunciada por el agente extranjero.

Para que un nodo móvil pueda averiguar si se encuentra en su red local o, por el contrario, se ha desplazado hacia una red extranjera, tan solo ha de verificar los bits F y H de alguno de los mensajes de anunciamiento que capture. De esta manera, sabrá si el agente está actuando como agente local o externo. La obtención de su dirección de auxilio se realiza a partir del campo de datos *care-of address* del mensaje de anunciamiento de agente.

3.1.4.3. Solicitud de agente

Los mensajes de solicitud de agente son enviados por los nodos móviles que no desean, o pueden esperar hasta la siguiente transmisión periódica de mensajes de anunciamiento de agente. Por lo tanto, el único objetivo de un mensaje de solicitud de agente es forzar a cualquier agente ubicado en el mismo enlace a transmitir un mensaje de anunciamiento de agente de manera inmediata. Esto resulta especialmente útil en aquellos casos en los cuales la frecuencia de los mensajes de anunciamiento es demasiado baja para un nodo móvil que cambia rápidamente de enlace.

Ejemplo de Solicitud de anuncios de agentes



Encabezado IP
Ipsrc = dirección agente
Ipdst=Broadcast
Ipprotocol=ICMP
Anuncio Agente
Estoy en FA xxx HA yyy
FA's Care-of Addres

Figura 9. Solicitud de anuncios de agentes

El formato de los mensajes de solicitud de agente es exactamente idéntico al de los mensajes ICMP de solicitud de *router* (ver Figura 8. Mensajes de Anunciamiento de Agente). La única diferencia reside en que los mensajes de solicitud de agente deben tener su campo de tiempo de vida (Time To Live – TTL) a 1.

3.1.4.4. Registro

El protocolo IP Móvil tipifica varias circunstancias bajo las cuales todo nodo móvil debe registrarse. La primera de ellas es cuando detecta que su punto de conexión a Internet ha variado respecto a un instante anterior. También deberá registrarse si, aún sin haber cambiado su punto de conexión a Internet, el registro anterior está a punto de caducar. Finalmente, cuando el nodo móvil en una red extranjera detecta que su agente extranjero se ha reiniciado.

El procedimiento de registro sirve para solicitar los servicios de un agente externo. Acto seguido, el nodo móvil procede a informar a su agente local de su nueva dirección de auxilio en la red. Por el contrario, si el nodo móvil detecta que ha regresado a su red local tras haber permanecido fuera de

ella, debe iniciar el procedimiento para desregistrarse con su nodo local para poder continuar funcionando como cualquier otro nodo fijo.

El procedimiento de registro comprende los siguientes pasos:

1. El nodo móvil envía un mensaje de *petición de registro*. Según el caso, este mensaje se enviará directamente al agente local o vía el agente externo, previa aceptación del mismo.

2. El agente local recibe la petición de registro y envía a su vez al nodo móvil un mensaje de *contestación de registro*. Éste último informa al nodo móvil si su petición de registro ha sido o no aceptada.

3. Si el nodo móvil no recibe la contestación de registro en un período razonable de tiempo, procede a retransmitir las peticiones de registro con intervalos cada vez más largos entre ellos, hasta recibir contestación.

Para poder llevar a cabo el procedimiento es necesaria la cooperación entre los agentes local y externo, intercambiando mensajes de petición de registro, de respuesta de registro además de datos opcionales.

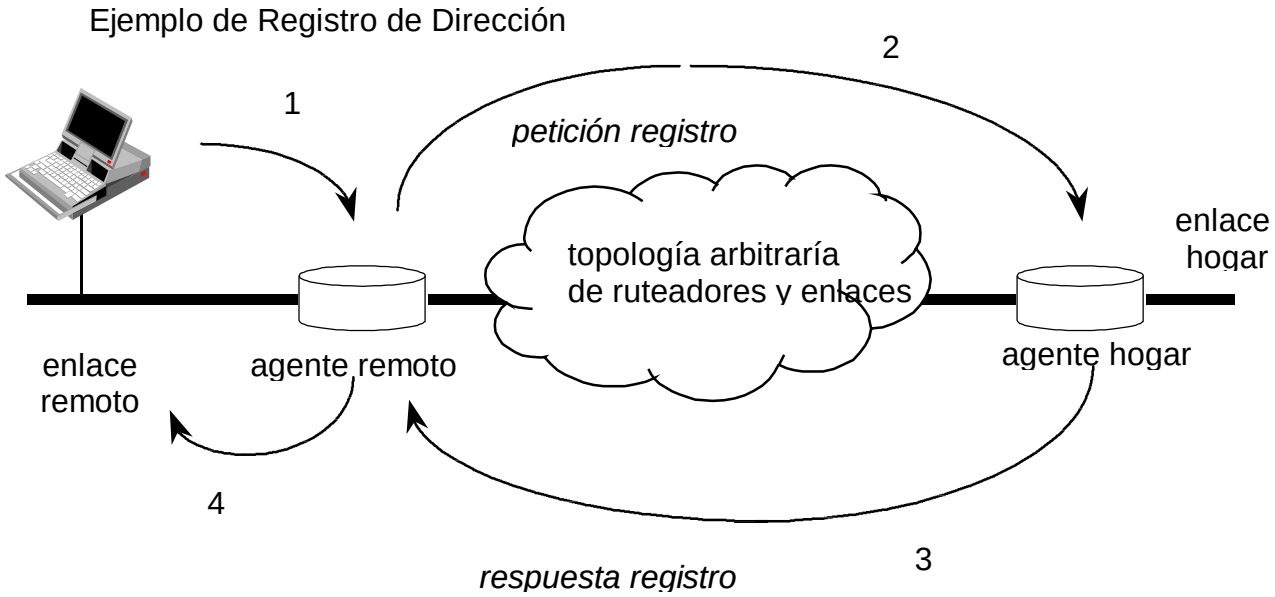


Figura 10. Registro de Dirección

3.1.4.5. Petición de registro

Un nodo móvil se registra con su agente local mediante un mensaje de *petición de registro*. De esta manera, el agente local puede crear o modificar la entrada del nodo móvil en su lista de nodos con movilidad. El mensaje de petición de registro presenta el formato mostrado en la Figura 11. Mensaje de petición de registro.

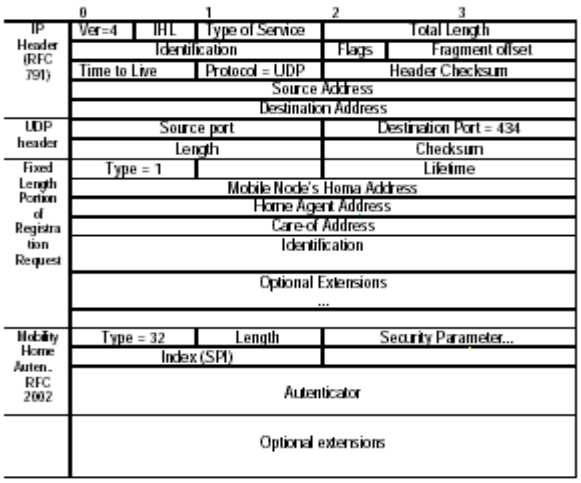


Figura 11. Mensaje de petición de registro.

Los diferentes campos que conforman el mensaje de petición de registro son los siguientes:

- **Type** 1 (Petición de registro)
- **S** El nodo móvil solicita que el agente local mantenga sus anteriores entradas de movilidad.
- **B** El nodo móvil pide solicitud al agente local que tunele hacia él los paquetes de broadcast que se reciban en la red local.
- **D** El nodo móvil informa al agente local que desencapsulará los paquetes que le sean enviados a su dirección de auxilio. Esto implica que el nodo móvil esta utilizando una dirección de auxilio colocada.
- **M** El nodo móvil solicita que el agente local utilice encapsulado mínimo para los paquetes destinados a él.
- **G** El nodo móvil solicita que el agente local utilice encapsulado GRE para los paquetes destinados a él.
- **V** El nodo móvil solicita que el agente local que su agente de movilidad emplee la compresión de cabeceras de Van Jacobson.
- **Reserved** Reservado.
- **Lifetime** Número de segundos restantes antes de la caducidad del registro actual.
- **Home Address** Dirección IP del nodo móvil
- **Home Agent** Dirección IP del agente local del nodo móvil.
- **Care-of Address** Dirección de auxilio = dirección IP a la salida del túnel.
- **Identification** Número de 64 bits creado por el nodo móvil para asociar peticiones de registro con contestaciones de registro. También sirve para proteger contra contestaciones de registro fraudulentas.
- **Extensions** Extensiones

3.1.4.6. Respuesta de registro

Como ya se ha explicado anteriormente, tras la recepción de una petición de registro, el agente local devuelve al nodo móvil un mensaje de *respuesta de registro*.

Si el nodo móvil solicita el servicio a través de un agente externo, será éste quien reciba la contestación de registro y la envíe a continuación al nodo móvil. Por otro lado, si el nodo móvil está utilizando una dirección de auxilio colocada, será él mismo quien reciba el mensaje de respuesta de registro.

Este mensaje informa al nodo móvil sobre el resultado de su petición de registro y del tiempo de vida del registro, que puede ser inferior o igual al solicitado por el nodo móvil. El agente externo no puede en ningún caso modificar el tiempo de vida asignado por el agente local.

El formato del mensaje de respuesta de registro es el mostrado en la Figura12. Mensaje de Respuesta de Registro.

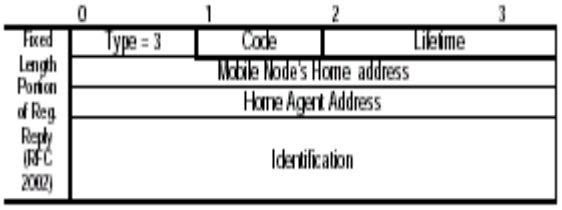


Figura 12. Mensaje de Respuesta de Registro.

Los campos del mensaje son los siguientes:

- **Type** 3 (Contestación de registro)
- **Code** Código indicador del resultado de la petición de registro.

- **Lifetime** Tiempo de vida, en segundos, de la entrada del nodo móvil en la lista de movilidad del agente local.
- **Home Address** Dirección IP del nodo móvil.
- **Home Agent** Dirección IP del agente local del nodo móvil.
- **Identification** Número de 64 bits creado por el nodo móvil para asociar peticiones de registro con contestaciones de registro. También sirve para proteger contra contestaciones de registro fraudulentas.
- **Extensions** Extensiones.

3.1.4.7. Posibles opciones al procedimiento de registro

Además de las acciones anteriormente descritas, el procedimiento de registro permite también llevar a cabo otras interesantes funciones que se enumeran a continuación:

1. Descubrir la dirección de un agente local si el nodo móvil no ha sido configurado con esta información.
2. Seleccionar diferentes tipos de encapsulado de los paquetes.
3. Utilizar la compresión de encabezados de Van Jacobson.
4. Mantener varios registros simultáneos para que cada dirección de auxilio activa reciba una copia de los paquetes destinados al nodo móvil.
5. Desregistrar ciertas direcciones de cuidado manteniendo otras activas.

3.1.5. Tratamiento de los paquetes

Una vez analizados los procedimientos de descubrimiento de agente y de registro, presentamos los diferentes modos en que un paquete puede ser encaminado desde su dirección IP de origen hasta la dirección IP de destino en función de la situación del nodo móvil.

3.1.6. Encaminamiento de los paquetes

En primer lugar, cabe distinguir dos posibles escenarios: uno en el que el nodo móvil está conectado a su red local, o bien si éste se encuentra en una red externa.

3.1.6.1. Nodo móvil en red local

Si el nodo móvil se encuentra en su red local, actúa como si de cualquier otro nodo fijo se tratase. Por lo tanto, las reglas para el encaminamiento de paquetes en este caso son las mismas que para el encaminamiento de paquetes IP hacia cualquier nodo o *router* convencional.

3.1.6.2. Nodo móvil en red extranjera

3.1.6.2.1. Hacia el nodo móvil

El protocolo IP Móvil requiere que los paquetes enviados desde la red local hasta el nodo móvil sean encapsulados. El encapsulado altera el encaminamiento habitual de los paquetes ya que éstos atraviesan un nodo intermedio antes de llegar a su destino. Una vez ha llegado al nodo intermedio, éste procede a desencapsularlo y enviar el paquete original al destinatario final.

De manera general, las operaciones que comprende el envío de un paquete hacia un nodo móvil en una red extranjera son las siguientes:

1. Un *router* en la red local, generalmente el agente local, anuncia que existe conectividad hasta el prefijo de red equivalente al de la dirección local del nodo móvil. Por lo tanto, todo paquete destinado al

nodo móvil es encaminado hacia su red local y, en concreto, es recibido por su agente local.

2. El agente local intercepta el paquete destinado al nodo móvil y consulta su entrada en su lista de movilidad para conocer las direcciones de cuidado registradas.

3. A continuación, el agente local envía una copia del paquete hacia cada dirección de cuidado a través de túneles (*tunneling*).

En cada dirección de auxilio (la del agente externo o una dirección de auxilio colocada), se extrae el paquete original y es entregado al nodo móvil.

Antes de enviar un paquete a través del túnel, el agente local realiza la operación de encapsulado dentro de un nuevo paquete cuya dirección de destino es la dirección de auxilio (ver Figura 13. Operación de Encapsulamiento).

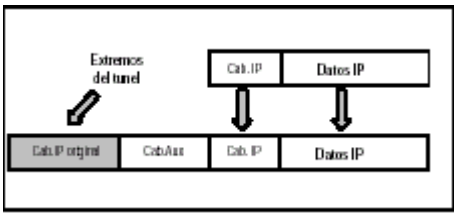


Figura 13. Operación de Encapsulamiento.

Si se trata de una dirección de auxilio de un agente externo, éste deshace el encapsulamiento exterior del paquete para recuperar el paquete original. A continuación consulta el campo de *dirección IP de destino* para comprobar si coincide con alguno de los nodos móviles a los que está prestando servicio. Si es este el caso, el agente externo envía el paquete al nodo móvil a través de la interfaz adecuada. Si la dirección de cuidado es colocada, el nodo móvil

no recibe los servicios de ningún agente extranjero y, por lo tanto, efectúa él mismo las operaciones de desencapsulamiento.

3.1.6.2.2. Desde el nodo móvil

Para poder enviar paquetes a otros nodos, un nodo móvil debe encontrar la dirección de un *router* que pueda dar salida a estos paquetes. Si el nodo móvil depende de un agente externo, existen dos alternativas a la hora de determinar un *router* adecuado:

1. El propio agente extranjero, según especifica el campo *IP Source Address* del mensaje de *anunciamiento de agente*.

2. Cualquier *router* cuya dirección IP aparezca en los campos *Router Address* del mensaje de *anunciamiento de router*, porción del mensaje de *anunciamiento de agente.*

Sin embargo, esta última alternativa tan solo es válida si el nodo móvil es capaz de determinar la dirección de la capa de enlace del router deseado, sin enviar peticiones de *ARP* (*Address Resolution Protocol*) que contengan su dirección IP local.

Si el nodo móvil posee una dirección de auxilio colocada, es decir, no depende de ningún agente externo, también tiene dos alternativas a la hora de seleccionar un *router:*

- Escoger algún *router* que esté enviando mensajes de *anunciamiento de router* (no de agente) en la red en la que se encuentra.

- Mediante el mismo mecanismo por el que obtuvo su dirección de auxilio colocada puede obtener la dirección de un *router* adecuado. Por ejemplo, el protocolo DHCP ofrece todo tipo de información al nodo móvil, incluida la dirección de un *router*.

Contrariamente a los nodos móviles dependientes de un agente externo, los nodos móviles con una dirección de auxilio colocada pueden enviar peticiones ARP con su dirección local.

3.1.7. Tunneling

El término *encapsulado* es un equivalente al de tunelado o *tunneling*. Ello consiste en la inserción de un paquete IP dentro de otro paquete del mismo tipo u otro. El paquete resultante es, a continuación, enviado a un nodo intermedio entre el nodo origen y el nodo destino final.

3.1.7.1. Túnel

Es un camino seguido por un paquete mientras es encapsulado dentro de la carga de otro paquete, consiste en encapsular un paquete transmitido dentro de otro.

El escenario más habitual de utilización de túneles es el presentado en la Figura 14.

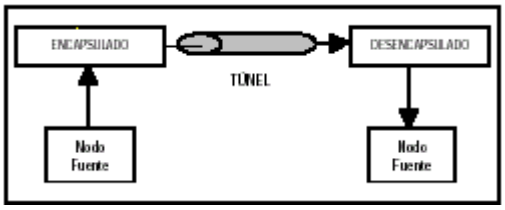


Figura 14. Escenario típico para acciones de tunneling

El nodo encapsulador es generalmente considerado el punto de entrada al túnel y el nodo desencapsulador el punto de salida del túnel.

Actualmente las técnicas de encapsulado IP son especialmente útiles para realizar transmisiones *multicast*, e incluso llevar a cabo acciones de seguridad y privacidad en Internet.

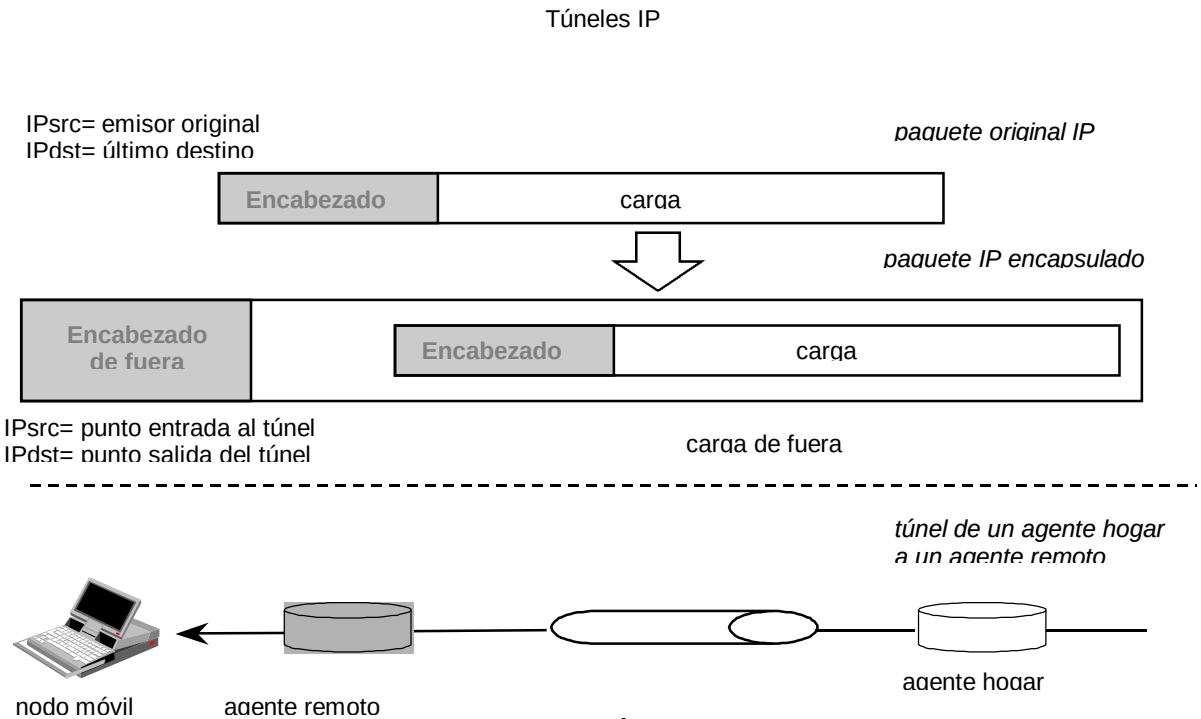


Figura 15. Túneles IP

El protocolo IP Móvil requiere que los agentes locales, los agentes externos y los nodos móviles con una dirección de auxilio colocada soporten el *encapsulado IP-in-IP*. A continuación se presentan éste y otros tipos de encapsulado que el agente local puede emplear para enviar los paquetes a través de túneles.

3.1.8. Tipos de Encapsulado

3.1.8.1. Encapsulado IP-in-IP

El encapsulado IP-in-IP[7] consiste en insertar un una cabecera IP adicional antes de la cabecera propia del paquete inicial como se muestra en la Figura13. de Operación de Encapsulamiento. También es posible insertar otras cabeceras (como por ejemplo, requisitos de seguridad para proteger el paquete original durante el tunelado) entre las dos cabeceras anteriores.

La cabecera exterior contiene información sobre los extremos del túnel. La cabecera interior contiene información sobre los nodos origen y destino del paquete inicial y no puede ser modificada en ningún caso, salvo para decrementar el tiempo de vida (TTL - Time To Live) del paquete, aunque tan solo una vez dentro del túnel, a pesar de que pueda atravesar varios *routers*.

A simple vista podría parecer que resulta imposible saber si se ha producido algún problema con el paquete mientras éste se encuentra dentro del túnel. No obstante, el punto de entrada al túnel mantiene una serie de informaciones, compuesto por un juego de variables que describen las características del túnel. Esta información consta de:

- Máxima MTU (Maximum Transfer Unit) del túnel.
- Longitud del túnel, contabilizada en hops.

[7] Documento Internet Engineering Task Force: Request For Comments RFC 2003 “IP Encapsulation within IP”.

- Si el extremo final del túnel es alcanzable, el punto de entrada al túnel actualiza estas variables mediante *mensajes ICMP* que recibe de los *routers* en el interior del túnel.

3.1.8.2. Encapsulado mínimo

El encapsulado suele conllevar el duplicado innecesario de numerosos campos de la cabecera IP interna. El encapsulado mínimo intenta minimizar al máximo la información de *overhead* de encapsulado para disminuir el tamaño del paquete resultante.

Según puede observarse en la figura de encapsulado mínimo[8], la cabecera IP original es modificada y la cabecera de encapsulado mínimo es insertada entre la cabecera original modificada y la información.

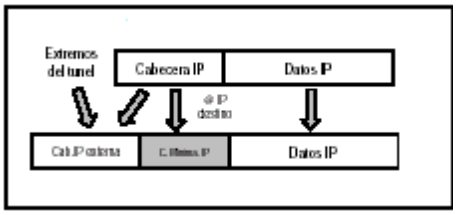


Figura 15. Encapsulado mínimo

Al desencapsular un paquete con encapsulado mínimo, se deberán restaurar los campos modificados en la cabecera original con los datos de la cabecera de encapsulado mínimo, actualizando los campos que así lo requieran como por ejemplo el campo de longitud del paquete, y el de checksum.

[8] Documento Internet Engineering Task Force: Request For Comments RFC 2004 “Minimal Encapsulation within IP”.

A pesar de todo, el encapsulado mínimo no está ampliamente difundido ya que presenta ciertas desventajas. Concretamente, no funciona con paquetes ya fragmentados. Además, este encapsulado fuerza que el valor TTL sea decrementado en cada *router* dentro del túnel por lo que, puede suceder que los paquetes caduquen antes de llegar a su destino.

3.1.8.3. Encapsulado GRE

El encapsulado *GRE (Generic Record Encapsulation)* es el más flexible de los tres estudiados hasta el momento, ya que permite la encapsulación de cualquier tipo de paquete, incluidos los paquetes IP. El formato del paquete GRE es el que se presenta en la Figura 16.

Figura 16. Formato del paquete GRE

Contrariamente a los encapsulados IP-in-IP y mínimo, el encapsulado GRE ha sido específicamente diseñado para prevenir encapsulamientos recursivos. Concretamente, el campo *recur* en la cabecera GRE es un contador que informa del número de encapsulados adicionales que son permitidos. En el protocolo IP versión 6 se está estudiando implementar un mecanismo similar a éste en su documento borrador sobre acciones de tunelado.

3.1.9. Seguridad

Las redes y nodos móviles son particularmente propensos a recibir ataques que comprometan su seguridad. La mayor parte de las veces los nodos móviles se conectaran a Internet a través de redes inalámbricas. Este tipo de

conexiones son particularmente vulnerables a escuchas silenciosas, ataques activos de respuesta *y* otros tipos de ataques activos; es por esta razón por la cual hay que tener un especial cuidado en el tema de la seguridad. A continuación se muestran algunos de los problemas que se pueden encontrar en este protocolo:

- Durante el proceso de registro de un nodo móvil, el agente local debe estar seguro de que la petición que está recibiendo es una petición de un nodo móvil verdadero y no de uno falso. El Protocolo IP móvil intenta solucionar este problema mediante la especificación de una asociación de seguridad entre el host local y el nodo móvil, cuya configuración es manual. Se utiliza un índice de seguridad que se incluye en todos los mensajes que el nodo móvil envía al agente local.

  Este índice está formado por un numero que indica el algoritmo utilizado en la codificación del mensaje y un secreto que solo los dos conocen. Este secreto puede ser o bien un acuerdo por ambas partes para el intercambio de una llave o bien el agente local manda al nodo móvil un dato que espera que le sea devuelto pasado un determinado periodo de tiempo.

- Los usuarios que tengan datos privados que no desean que sean observados por nadie más deben usar mecanismo de seguridad (encriptación) ajenos al protocolo de IP Móvil y que, por lo tanto, no están especificados.

- En las peticiones de registro existe un campo que permite al agente local determinar si dicha petición se ha realizado recientemente y por lo tanto que no es una petición que ya ha sido escuchada y se produzca un duplicado.

Para ello existen dos algoritmos:

- timestamp
- nonces

Todos los agentes locales deben implementar esta protección contra duplicados basados en marcas de tiempo.

3.1.10. Especificaciones de IP MOVIL

Aprobado por grupo IESG en junio 1996.
Producido por IP Routing for Wireless/Mobile Hosts (mobileip).

Documentos estándares IP móvil:

- RFC 2002
- RFCs 2003, 2004 y 1701
- RFC 2005
- RFC 2006
- RFC 1905

Este protocolo soluciona los siguientes problemas:

1. Solución movilidad en IP

    - Escalable, Robusta y Segura.
    - Permite a los nodos mantener sus comunicaciones mientras realizan un cambio de enlace.

- Proporciona un mecanismo para rutear paquetes a nodos móviles que pueden conectarse a cualquier enlace y mantienen la misma dirección IP.

3.1.10.1. Tipos de medios sobre los que opera IP Móvil

- Independiente del medio.
- Mantiene filosofía de diseño de IP.
- Nodo móvil puede moverse de un tipo de medio a otro sin perder conectividad.
- Por supuesto, también permite a un nodo moverse de una red a otra con el mismo medio.

3.1.10.2. Requerimientos IP

1. Nodo móvil debe poder comunicarse con otros nodos después de cambiar su punto de conexión en el enlace.
2. Comunicarse usando solo su dirección IP original, sin importar su punto de conexión.
3. Comunicarse con otros nodos que no soporten las funciones de IP móvil.
4. No debe exponerse a nuevos requerimientos de seguridad, diferentes a los de un nodo en IP fijo.

3.1.10.3. Objetivos de Diseño de IP

- Hacer el tamaño y la frecuencia de las actualizaciones de datos de ruteo lo más pequeño posible.
- Lo más simple posible para implementar software móvil en los nodos.

- Evitar soluciones que requieren de direcciones o grandes piscinas de estas, es decir compatibilidad con IP fijo.

3.1.10.4. Suposiciones hechas por IP Móvil

- Suposición principal: Paquetes Unicast, destinados a un solo receptor.
- Asume que Internet “existe” y que es capaz de entregar cualquier paquete entre dos pares de nodos en la red.
- No le importan cuales protocolos de ruteo dinámico se usan, ni como Internet acomoda millones de host y ruteadores, tan solo que puede usar dichos protocolos.

3.1.10.5. Componentes IP Móvil

3.1.10.5.1. Nodo móvil

Nodo que puede cambiar su punto de conexión de un enlace a otro, sin perder comunicación.

3.1.10.5.2. Agente hogar

Ruteador con una interfaz en el enlace hogar del nodo móvil, el cual:

- El nodo móvil lo mantiene informado de su ubicación actual, representada por su dirección care-of.

En algunos casos, notifica alcance al prefijo-red de la dirección hogar del nodo móvil, atrapando paquetes que están destinados a la dirección hogar del nodo móvil.

Intercepta paquetes destinados a la dirección hogar del nodo móvil y los "tunelea" a la dirección actual del nodo, (i.e. dirección care-of)

3.1.10.5.3. Agente remoto

Ruteador en el enlace remoto del nodo móvil, ayuda al nodo móvil informándole al agente hogar su dirección care-of, en algunos casos proporciona una dirección care-of y destunelea los paquetes enviados al nodo móvil.

Funciona como un ruteador por default para los paquetes generados por el nodo móvil, mientras esta conectado a su enlace remoto.

Estructura de Componentes de IP Móvil

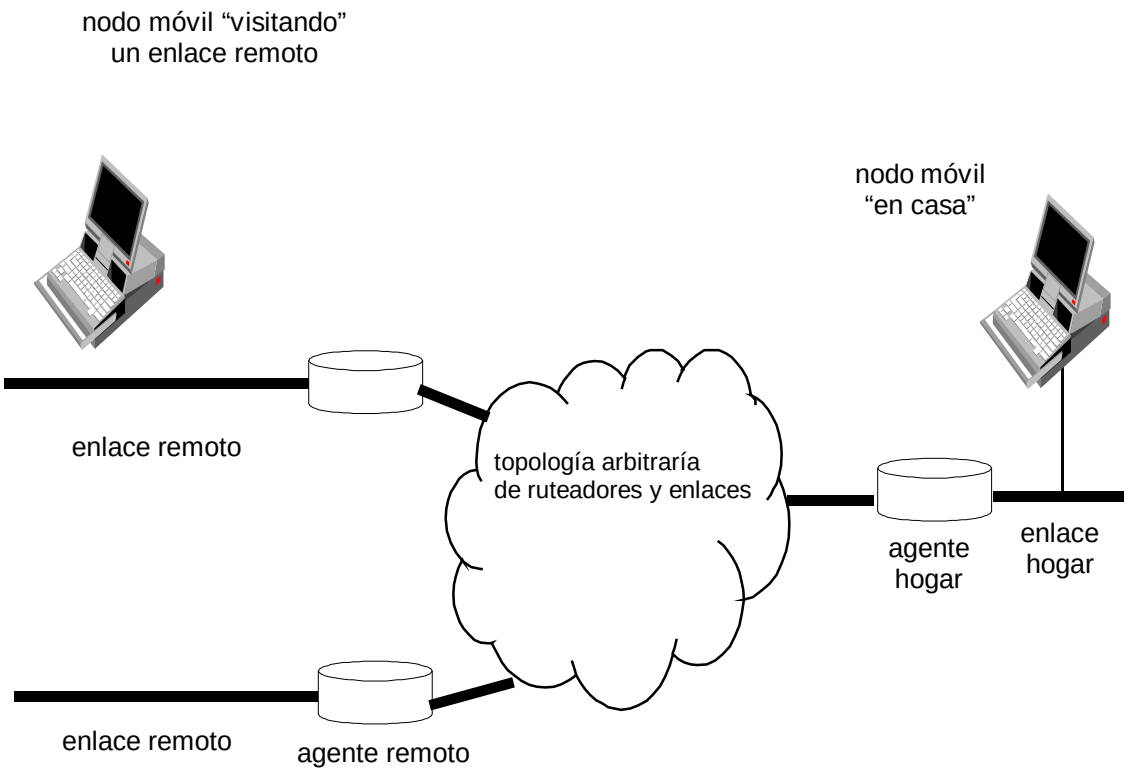


Figura 17. Estructura de Componentes de IP Móvil

3.1.10.5.4. Direcciones care-of

Dirección asociada con un nodo móvil que esta visitando un enlace remoto.

Propiedades:

- Es especifica al enlace remoto del nodo móvil y cambia cada vez que el nodo cambia de enlace.
- Los paquetes con estas direcciones son entregados usando protocolos de ruteo existentes, también es usado como punto de salida de un túnel no es usada como dirección destino o fuente en comunicaciones entre nodos móviles.

3.1.10.5.5. Dirección care-of agente remoto

Dirección IP de un agente remoto que tiene una interfaz con el enlace remoto, puede ser una de las direcciones de los agentes remotos, siempre y cuando el agente tenga al menos una interfaz con el enlace remoto.

El prefijo-red no necesita ser igual al prefijo-red del enlace remoto y puede ser compartida, al mismo tiempo, por varios nodo móviles.

La dirección care-of es una dirección IP cercana al nodo móvil.

Cercana: esta a un salto (hop) del enlace remoto y es una dirección de un agente remoto con una interfaz al enlace remoto, o una dirección temporal de interfaz del nodo móvil.

Usada por el agente hogar para entregar paquetes a un nodo que se encuentra en un enlace remoto.

3.1.10.5.6. Dirección care-of colocada

Dirección IP temporalmente asignada a una interfaz del nodo móvil, prefijo-red debe ser igual al del enlace visitado por el nodo móvil, puede ser usada en el caso de que no existan agentes remotos en un enlace remoto y puede ser usada por un solo nodo móvil a la vez.

Los agentes pueden ser Hosts o deben ser Ruteadores, es algo que debemos preguntarnos.

3.1.10.5.7. Ruteador

Dispositivo que implementa IP y da seguimiento a paquetes no dirigidos explícitamente a él.

3.1.10.5.8. Host

Envía y recibe paquetes pero no da seguimiento.

Entonces por definición agentes hogar y remotos son ruteadores. Es posible implementar agentes en computadoras que parecen más hosts que ruteadores. En general hay una relación administrativa cercana entre un nodo móvil y el propietario del agente hogar del nodo móvil. Nodo móvil, enlace hogar y agente hogar generalmente son operados por la misma entidad administrativa. No existe tal relación el lado de los remotos. El agente remoto puede ubicarse en cualquier red comercial o educativa, en cuyo caso sería administrado por una entidad diferente a la del nodo móvil.

3.1.10.5.9. Obtención de direcciones care-of

Soluciones al nivel de capa de enlace

- CDPD: Cellular Digital Packet Data

Es la solución para lugares de área grande, se instala un modem celular en la computadora y cuando se accede a servicio CDPD este proporciona una dirección válida en la red CDPD ya que soporta varios tipos de protocolos.

Utiliza CLNP para su ruteo, lo cual causa un costo administrativo substancial, pero el problema es que no esta disponible en muchos mercados.

- IEEE 802.11

Es el estándar para redes locales inalámbricas, define un conjunto de transceivers que proporcionan un puente ente el medio alambrado y la infraestructura inalámbrica. Los protocolos hacen que la red de transceivers aparezcan como un solo enlace para el nivel red, lo que provoca que la movilidad sea invisible para IP.

Cualquier cambio en la ubicación que se salga de la frontera de la ruta provoca un cambio de dirección IP e interrumpe las comunicaciones.

Los problemas que se pueden presentar al nivel de enlace son:

La movilidad se da dentro del contexto de un solo medio de comunicación, necesitan n diferentes soluciones de movilidad para N posibles medios, Proporcionan movilidad dentro de un área restringida.

3.2. Configuración del Protocolo IP Móvil en la red del departamento

¿Siguiendo con la movilidad?

El protocolo IP móvil permite que PCs configurados para funcionar en una subred determinada cambien de subred y sigan funcionando exactamente como lo harían si estuviesen en su subred original, sin tener que cambiar su configuración. Es decir, mantienen las conexiones que hubiesen establecido hasta el momento, siguen recibiendo los paquetes dirigidos a su dirección original, y pueden acceder a los recursos de la subred original como si estuviera dentro de ella.

Para ello, es necesario que en ambas subredes existan unos agentes (el de la red original es el Agente Local, y el de la subred visitada es el Agente Externo, que se encargan de facilitar la movilidad. Además, también es necesario que en el PCs que cambia de subred o *Nodo Móvil* tenga instalado un software que le permite registrarse, en cada subred que visita, con el Agente Externo correspondiente, solicitando una dirección provisional (que suele ser la del propio agente), y con su Agente Local informándole de su dirección actual, a la cual deberá redirigir el tráfico que reciba en su dirección original.

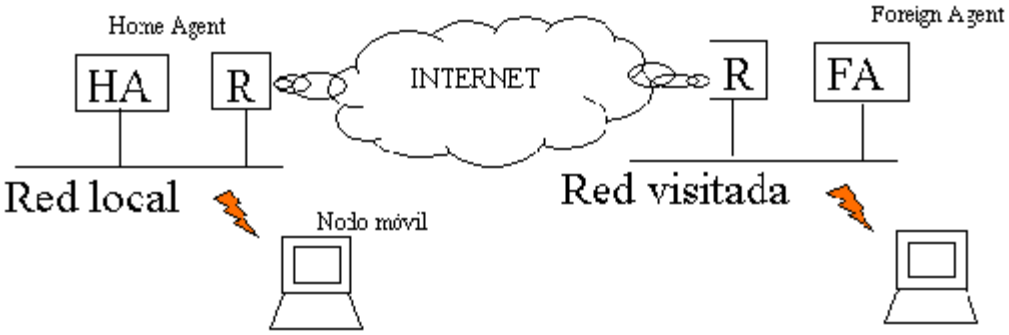


Figura 18. Escenario básico de movilidad en IPv4

3.2.1. Configuración de un nodo móvil IPv4

3.2.1.1. Configuración de nodos móviles IPv4 Linux

3.2.1.1.1. Requisitos

- Kernel 2.2 o superior

Cualquier implementación de Linux es apropiada: RedHat, SuSE, Debian.

Compilación del kernel: opciones necesarias para la instalación del software:

- Packet socket (CONFIG_PACKET)
- Kernel/User netlink socket (CONFIG_NETLINK)
- Routing messages (CONFIG_RTNETLINK)
- IP: Socket Filtering (CONFIG_FILTER)
- IP: tunneling (CONFIG_NET_IPIP)
- IP: advanced router (CONFIG_IP_ADVANCED_ROUTER)
- IP: policy routing (CONFIG_IP_MULTIPLE_TABLES) (for FAs)

Software a instalar: Dynamics-HUT mobile IP

RPMs para determinadas versiones de Redhat y Suse. Si no hay un rpm adecuado, compilar las fuentes, siguiendo las instrucciones del README.

Editar los ficheros de configuración del componente que se desea ejecutar (en este caso, /etc/dynmnd.conf o /usr/local/sbin/dynmnd.conf).

En este fichero, se configuran, entre otros parámetros:

- La dirección local del nodo móvil (MNHomeIPAddress).
- La subred a la que pertenece originalmente, incluida la máscara (HomeNetPrefix), y el gateway de la misma (HomeNetGateway),
- La dirección de su Home Agent (HAIPAddress).
- Las opciones de seguridad posibles, como el uso de AAA (UseAAA TRUE/FALSE), y los posibles parámetros de seguridad punto final del túnel que establecerá el Home Agent, que puede ser en el Foreign Agent (configurar la opción EnableFADecapsulation TRUE) o bien directamente en el MN (opción EnableFADecapsulation FALSE), para lo cual es necesario que el nodo móvil obtenga una dirección provisional en la subred visitada, a través de medios externos a IP móvil como DHCP.

Cada nodo móvil debe tener una asociación de seguridad con su Home Agent. Ésta viene dada por cuatro parámetros, que son:

1. SPI (security parameter index), que le sirve al Home Agent para identificar unívocamente las asociaciones de seguridad con nodos móviles. Debe ser un número entero. Secreto compartido entre el nodo móvil y el home agent (SharedSecret), que debe ser un string de 16 caracteres, algoritmo de autenticación (se puede elegir entre MD5, HMAC/MD5, SHA1 y HMAC/SHA1, y método de protección contra el ataque de respuesta (se puede escoger entre Timestamps y nonces).

   Opcionalmente, y de la misma manera que se ha descrito para los Agentes Locales, los nodos móviles pueden establecer asociaciones de seguridad con los Agentes externos, con los mismos cuatro parámetros.

2. Configuración de AAA para autenticación de nodos móviles.

3. Modo de encapsulamiento o TunnelingMode, que se puede configurar como automático, o bien para que sólo se acepte reverse tunneling o triangle tunnel. Se recomienda configurar a 1 (automático), MNDecapsRouteHandling: Se recomienda configurar a 0 (enrutar todos los paquetes hacia el túnel), MNDefaultTunnelLifetime (tiempo de validez del túnel establecido): Se recomienda configurar a 1 segundo para agilizar las transiciones de subred.

4. Puerto de las peticiones de registro: Se recomienda configurar a 434 por compatibilidad con la RFC.

Periodo para las solicitudes periódicas de agente (Solicitation Interval):

§ Se recomienda configurar a 1000000 (1 segundo) para agilizar las transiciones.

Resto de opciones: se recomienda respetar los valores por defecto.

Ejemplo de fichero de configuración comentado

Demonio a ejecutar para que funcione el nodo móvil: /sbin/dynmnd o /usr/local/sbin/dynmnd.

Para lanzarlo en modo debug: dynmnd --fg –debug

Para utilizar un fichero de configuración del nodo móvil determinado: dynmnd --config

3.2.1.1.2. Monitorización de la actividad del nodo móvil

- Comando dynmn_tool

- Mediante el comando policy, se establece la política que debe seguir el nodo móvil para realizar las transiciones. Se puede elegir entre Early-expire, Newest-FA, Eager-switching y Newest-ADV. Para nodos móviles alambricos, la más apropiada es Newest-ADV, ya que en ningún caso recibirán simultáneamente anunciamientos de dos agentes a la vez. La selección de esta política reducirá el tiempo para las transiciones. También es recomendable en el caso de nodos móviles inalámbricos que realicen transiciones entre subredes con diferente perfil de configuración (identificador, código de cifrado).

- El comando status aporta información sobre el estado del nodo móvil: si se encuentra en su red local (At Home), o si se encuentra fuera de ella, si está establecido el túnel y es capaz de comunicarse (Connected) o no. También informa sobre la dicección care-of que posee en ese momento el nodo móvil.

- El comando list enumera los agentes de los que recientemente se ha recibido un anunciamiento.

- Los comandos update y rescan serán de utilidad cuando se utilice DHCP.

- wireless aporta información sobre los canales de wireless LAN que está recibiendo el nodo móvil, en caso de que posea tarjeta de red inalámbrica.

3.2.1.2. Configuración de nodos móviles IPv4 en WINDOWS

3.2.1.2.1. Requisitos

- Windows 2000, 98 o ME.
- Instalación de WinPcap: está disponible en http://netgroup-serv.polito.it/winpcap/
- Instalación de las DLLs de Cygwin. Se puede optar por:

    1. Instalar sólo las DLLs que se necesitan: cygwin-dll.zip . Sólo hay que descomprimirlo en el mismo directorio que dynmnd.exe y dynmn_tool.exe.
    2. Instalación completa de cygwin: está disponible en http://www.cygwin.com/

Software a instalar: Dynamics-HUT mobile IP

Bajar el software específico para Windows

Editar los ficheros de configuración del nodo móvil (dynmnd.conf). El fichero de configuración de ejemplo viene comprimido con los ejecutables para Windows. También se puede editar un fichero cualquiera y pasárselo como parámetro a dynmnd, mediante --config. Se debe tener cuidado al editar los ficheros de configuración, para no cambiar su formato por el de MSDOS, ya que la aplicación no los reconocería.

Los mismos parámetros para la configuración de nodos móviles linux son válidas:

- La dirección local del nodo móvil (MNHomeIPAddress).
- La subred a la que pertenece originalmente, incluida la máscara (HomeNetPrefix), y el gateway de la misma (HomeNetGateway).
- La dirección de su Home Agent (HAIPAddress).
- Las opciones de seguridad posibles, como el uso de AAA (UseAAA TRUE/FALSE), y los posibles parámetros de seguridad punto final del túnel que establecerá el Home Agent, que puede ser en el Foreign Agent (configurar la opción EnableFADecapsulation TRUE) o bien directamente en el MN (opción EnableFADecapsulation FALSE), para lo cual es necesario que el nodo móvil obtenga una dirección provisional en la subred visitada, a través de medios externos a IP móvil como DHCP.

Cada nodo móvil debe tener una asociación de seguridad con su Home Agent. Ésta viene dada por cuatro parámetros, que son:

1. SPI (security parameter index), que le sirve al Home Agent para identificar unívocamente las asociaciones de seguridad con nodos móviles. Debe ser un número entero. Secreto compartido entre el nodo móvil y el home agent (SharedSecret), que debe ser un string de 16 caracteres, algoritmo de autenticación (se puede elegir entre MD5, HMAC/MD5, SHA1 y HMAC/SHA1, y método de protección contra el ataque de respuesta (se puede escoger entre Timestamps y nonces).

   Opcionalmente, y de la misma manera que se ha descrito para los home agent, los nodos móviles pueden establecer asociaciones de seguridad con los foreign agent, con los mismos cuatro parámetros.

2. Configuración de AAA para autenticación de nodos móviles.

3. Modo de encapsulamiento o TunnelingMode, que se puede configurar como automático, o bien para que sólo se acepte reverse tunneling o triangle tunnel. Se recomienda configurar a 1 (automático) MNDecapsRouteHandling: Se recomienda configurar a 0 (enrutar todos los paquetes hacia el túnel) MNDefaultTunnelLifetime (tiempo de validez del túnel establecido): Se recomienda configurar a 1 segundo para agilizar las transiciones de subred.

4. Puerto de las peticiones de registro: Se recomienda configurar a 434 por compatibilidad con la RFC.

Periodo para las solicitudes periódicas de agente (Solicitation Interval):

§ Se recomienda configurar a 1000000 (1 segundo) para agilizar las transiciones.

Resto de opciones: se recomienda respetar los valores por defecto.

Ejemplo de fichero de configuración comentado

Demonio a ejecutar para que funcione el nodo móvil: dynmnd

Para lanzarlo en modo debug: dynmnd --fg --debug

Para utilizar un fichero de configuración del nodo móvil determinado: dynmnd --config

3.2.1.2.2. Monitorización de la actividad del nodo móvil

- Comando dynmn_tool

- Mediante el comando policy, se establece la política que debe seguir el nodo móvil para realizar las transiciones. Se puede elegir entre Early-expire, Newest-FA, Eager-switching y Newest-ADV. Para nodos móviles alambricos, la más apropiada es Newest-ADV, ya que en ningún caso recibirán simultáneamente anunciamientos de dos agentes a la vez. La selección de esta política reducirá el tiempo para las transiciones. También es recomendable en el caso de nodos móviles inalámbricos que realicen transiciones entre subredes con diferente perfil de configuración (identificador, código de cifrado).

- El comando status aporta información sobre el estado del nodo móvil: si se encuentra en su red local (At Home), o si se encuentra fuera de ella, si está establecido el túnel y es capaz de comunicarse (Connected) o no. También informa sobre la dicección care-of que posee en ese momento el nodo móvil.

- El comando list enumera los agentes de los que recientemente se ha recibido un anunciamiento.

- Los comandos update y rescan serán de utilidad cuando se utilice DHCP.

- wireless aporta información sobre los canales de wireless LAN que está recibiendo el nodo móvil, en caso de que posea tarjeta de red inalámbrica.

3.2.2. Configuración de Agentes en IPv4

3.2.2.1. Configuración de Agentes en IPv4 Linux

3.2.2.1.1. Requisitos

- Kernel 2.2 o superior

Cualquier implementación de Linux es apropiada: RedHat, SuSE, Debian.

Compilación del kernel: opciones necesarias para la instalación del software:

- Packet socket (CONFIG_PACKET)
- Kernel/User netlink socket (CONFIG_NETLINK)
- Routing messages (CONFIG_RTNETLINK)
- IP: Socket Filtering (CONFIG_FILTER)
- IP: tunneling (CONFIG_NET_IPIP)
- IP: advanced router (CONFIG_IP_ADVANCED_ROUTER)
- IP: policy routing (CONFIG_IP_MULTIPLE_TABLES) (for FAs)

Software a instalar: Dynamics-HUT mobile IP

RPMs para determinadas versiones de Redhat y Suse. Si no hay un rpm adecuado, compilar las fuentes, siguiendo las instrucciones del README.

Editar los ficheros de configuración del componente que se desea ejecutar (en este caso, /etc/dynmnd.conf o /usr/local/sbin/dynmnd.conf). En este fichero se configura el modo de funcionamiento de los agentes, las opciones de seguridad para los nodos móviles, los intervalos entre anunciamientos, el tiempo de validez para los registros de los nodos móviles y para los túneles

establecidos, si se exigirá la autenticación a través de, por ejemplo, AAA, los parámetros de las asociaciones de seguridad, etc.

Ejemplos de ficheros de configuración:

Home agent
Foreign Agent

Demonios a ejecutar para que funcionen los agentes:

- HOME AGENT: /usr/sbin/dynhad o /usr/local/sbin/dynhad
- FOREIGN AGENT: /usr/sbin/dynfad o /usr/local/sbin/dynfad

Herramientas para monitorizar los agentes

- HOME AGENT: /usr/sbin/dynhad_tool o /usr/local/sbin/dynhad_tool
- FOREIGN AGENT: /usr/sbin/dynfad o /usr/local/sbin/dynfad

3.2.2.2. Configuración de Agentes de IP Móvil Cisco

ANEXO B. Guía de comandos de Mobile IP en cisco

3.2.2.2.1. Requisitos mínimos para el router

- Router o superior

IOS 12.0(1)T o superior

3.2.2.2.2. Activación de los servicios de HOME AGENT

- (config)#router mobile
- (config)#ip mobile home-agent
- (config)#ip mobile host "dir.local" interface "interfaz"
- (config)#ip mobile secure host "dir.local" spi "num" key ascii "clave-en-string"
- (config)#ip mobile home-agent broadcast replay "intervalo"
- (config-int)#ip irdp

"interfaz" es el interfaz del router que está conectada a la red a la que se pretende dar el servicio de HOME AGENT.

"dir.local" es la dirección del nodo movil al que se pretende dar servicio.

"num" es el SPI (Security Parameter Index), y es un numero mayor que 100.

"clave-en-string" es la clave que se usa como secreto compartido para la asociación de seguridad entre el nodo movil y el home agent. Debe tener 16 caracteres.

"intervalo" es el intervalo con el que el home agent realiza los router advertisements

El comando "#ip irdp" activa el envío de mensajes de anunciamiento en un interfaz determinado.

3.2.2.2.3. Activación de los servicios de FOREIGN AGENT

- (config)#router mobile
- (config)#ip mobile foreign-agent care-of "interfaz"
- (config)#ip mobile foreign-service
- (config-int)#ip irdp

"interfaz" es el interfaz del router que está conectado a la red a la que se pretende dar el servicio de FOREIGN AGENT.

El comando "#ip irdp" activa el envío de mensajes de anunciamiento en un interfaz determinado.

3.2.2.2.4. Monitorización de la actividad

- show ip mobile binding muestra la tabla de nodos moviles registrados con un agente en un momento dado, y los datos relativos a su conexión (dirección careof, tiempo de validez del registro, identificación, opciones, etc). Este comando es para Home Agents.

- show ip mobile globals muestra información global de ip móvil, para cualquier agente.

- show ip mobile host muestra información sobre un nodo móvil en concreto.

- show ip mobile interface muestra la información relativa a IP móvil en un interfaz dado.

- show ip mobile secure muestra las asociaciones de seguridad de un agente con otros agentes o nodos móviles.

- show ip mobile traffic muestra el tráfico de ip móvil intercambiado por el router, clasificándolo según el tipo de paquetes.

- show ip mobile tunnel muestra los túneles activos y los datos de los mismos, para un interfaz determinado.

- show ip mobile violation muestra las violaciones de seguridad de ip móvil.

- show ip mobile visitor muestra los visitantes de otras redes. Este comando es para Foreign Agents.

3.2.3. Configuración de nodos móviles IPv4 que utilicen DHCP

Existe la posibilidad de que los nodos móviles que visitan una subred obtengan la dirección provisional a través de un servidor DHCP en lugar del Foreign Agent. A través de este mecanismo, es posible que los nodos móviles funcionen en redes en las que no existen Foreign Agents. A continuación veremos cómo es posible conseguir ésto, e inconvenientes de este modo de funcionamiento.

3.2.3.1. Requisitos

Configuración del software de movilidad, bien sea para Windows o para Linux, como se explico anteriormente.

Configuración de DHCP en el nodo móvil, bien sea eligiendo la opción *Obtener una dirección IP automáticamente*, tanto para nodos Linux como Windows.

3.2.3.2. Funcionamiento del nodo móvil usando DHCP

Al llegar a una nueva subred, en la cual debe existir un servidor DHCP configurado para proporcionar una dirección IP al nodo móvil, ya sea porque su dirección MAC está registrada en él o porque dispone de un rango de asignación libre, actualizar la dirección IP del interfaz (por ejemplo, en Windows, ejecutar en línea de comandos:

C:\>ipconfig /release
C:\>ipconfig /renew)

En la herramienta de monitorización del nodo móvil dynamics (dynmn_tool), ejecutar cada vez que se cambie de subred y se haya obtenido una nueva dirección:

>disconnect
>update (actualiza la dirección colocated-care-of del nodo móvil a la nueva dirección asignada por el servidor DHCP).
>connect HA (vuelve a establecer el túnel directo desde el Home Agent hasta el interfaz del nodo móvil que ha recibido la nueva dirección a través de DHCP).

El problema de este modo de funcionamiento es que se pierden las conexiones que hubiera establecidas en el nodo móvil en el momento en el que se ejecuta >disconnect, cosa que no sucede si se utiliza desencapsulamiento a través de Foreign Agent. Otra ventaja que posee el

uso de Foreign Agent es que, ya que es éste el que actúa como punto final del túnel, no es necesario asignar una dirección a cada nodo móvil que visita una red, sino que se utiliza la del Foreign Agent para todos ellos.

3.2.4. Configuración de IPv6 móvil

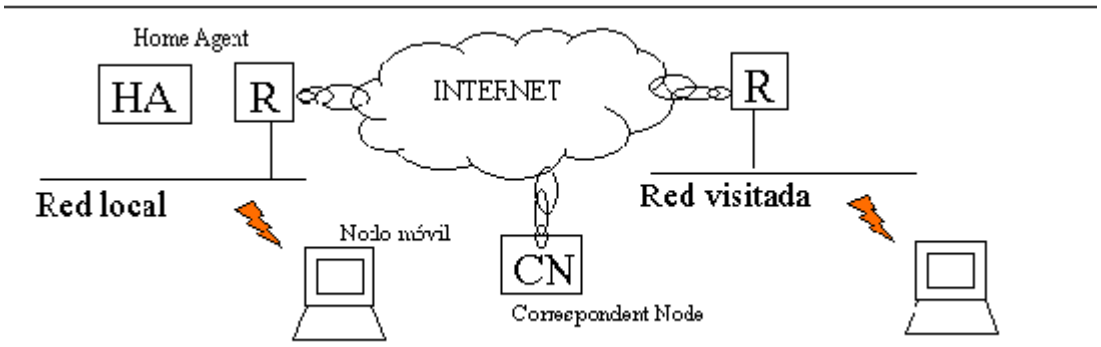


Figura 19. Escenario básico de movilidad en IPv6

En IPv6 desaparecen tanto los Foreign Agents como la obtención de direcciones provisionales en las subredes visitadas por el nodo móvil a través de DHCP. Estos procedimientos son sustituidos por la autoconfiguración a través de la recepción de *Router Advertisements*. Por lo tanto, los elementos que intervienen en la movilidad en IPv6 son los Home Agent y los Mobile Nodes.

Para los nodos que mantienen comunicaciones con éstos últimos, los *Correspondent Nodes*, este proceso puede ser teóricamente transparente.

Existe la posibilidad de utilizar actualización de rutas si éstos tienen instalado el software de movilidad, evitando el enrutamiento triangular. Sin embargo, esta transparencia no es posible para versiones del kernel inferiores a la 2.4.16, por lo que será necesaria la instalación del mismo software que en el Home Agent y Nodo Móvil.

3.2.4.1. Configuración de IPv6 móvil en Linux

- Sistema operativo y kernel (para todos los equipos: Home Agent, Mobile Node y Correspondent Node.)

Cualquier distribución de Linux. Las pruebas se han hecho con SuSE 7.3.

Implementación de MIPv6

- MIPL Mobile IPv6 for Linux, de la Universidad de Helsinki. Esta aplicación es válida para RedHat 6.1, 6.2, 7.0, Suse, Debian con kernel 2.4.x. Para su instalación son necesarios conocimientos de IPv6, y configuración, parcheado y compilación del kernel.

- KERNEL: es posible utilizar USAGI http://www.linux-ipv6.org/ (es una implementación del kernel de Linux con énfasis en el soporte IPv6). Esta implementación tiene la ventaja de que no es necesaria la aplicación de ningún parche, ya que está sincronizada con la implementación de HUT. Además, este kernel posee buen soporte IPv6, por lo que existen diversas aplicaciones para IPv6 que sólo funcionan con este kernel. La versión que se ha usado contiene el kernel 2.4.17.

Sin embargo, también es posible utilizar cualquier kernel 2.4.x de linux, con la ventaja de que es más estable. Sin embargo, en este caso hay que aplicar un parche al kernel de Linux. Este parche se obtiene en la distribución de MIPL.

Para ello, hay que entrar en el directorio donde está el kernel (generalemente /usr/src/linux), y ejecutar:

- % patch -p1 < $MIPL/mipv6-0.9.1-v2.4.16/mipv6-0.9.1-v2.4.16.patch
  siendo $MIPL el path en el que se ha descomprimido el .tar.gz de mipl.

Además, al compilar el kernel deben incluirse al menos las siguientes opciones que se recomiendan:

- CONFIG_EXPERIMENTAL=y
- CONFIG_SYSCTL=y
- CONFIG_PROC_FS=y
- CONFIG_MODULES=y
- CONFIG_NET=y
- CONFIG_NETLINK=y
- CONFIG_RTNETLINK=y
- CONFIG_NETFILTER=y
- CONFIG_UNIX=y
- CONFIG_INET=y
- CONFIG_IPV6=m
- CONFIG_IPV6_IPV6_TUNNEL=m
- CONFIG_IPV6_MOBILITY=m

3.2.4.1.1. Instalación de USAGI

Después de descomprimir las fuentes de USAGI, que se pueden bajar de http://www.linux-ipv6.org/, entrar en el directorio */usagi/ y ejecutar:

- % make prepare TARGET=linux24

Compilar el kernel de linux, haciendo:

- % cd kernel/linux24
- % make mrproper
- % make menuconfig (o "make config" o "make xconfig") (*)
- % make dep
- % make bzImage
- % make modules
- % make modules_install
- % cp arch/i386/bzImage /boot/...
- % cp System.map /boot
- % vi /etc/lilo.conf
- % lilo

Por ser USAGI una implementación experimental, se recomienda que ciertas opciones se seleccionen a NO durante la configuración:

- CONFIG_IPV6_DEBUG=n
- CONFIG_IPV6_6TO4_NEXTHOP=n
- CONFIG_IPV6_NDISC_DEBUG=n
- CONFIG_IPV6_ACONF_DEBUG=n
- CONFIG_IPV6_RT6_DEBUG=n
- CONFIG_IPV6_MLD6_DEBUG=n

- CONFIG_IPV6_MLD6_NO_SUPPRESS_DONE=n
- CONFIG_IPV6_NODEINFO=n
- CONFIG_IPV6_NODEINFO_DEBUG=n
- CONFIG_IPV6_NODEINFO_USE_UTS_DOMAIN=n
- CONFIG_IPV6_MOBILITY=n
- CONFIG_ATM_IPV6

Después, se deben instalar las aplicaciones de USAGI haciendo:

- % cd usagi/usagi
- % ./configure
- % make
- % make install

3.2.4.1.2. Instalación de MIPL Mobile IPv6

Después de descargar y descomprimir las fuentes de MIPL, entrar dentro del directorio mipv6-0.9.1-v2.4.16 y seguir los siguientes pasos:

- % ./configure
- % make
- % make install

3.2.4.1.3. Configuración

La configuración se realiza a través de los ficheros de configuración de Home Agent, Mobile Node y Correspondent Node.

3.2.4.1.4. Uso de MIPv6

Existe un script automático de arranque del servicio MIPv6, llamado mobile-ip6, con las siguientes opciones: {start|stop|status|restart}. Otra posibilidad es cargar el módulo a mano ejecutando insmod.

4. Redes 4G

4.1. Redes Móviles vs. Redes Inalámbricas

En los últimos años han aparecido en el mercado una gran variedad de computadoras personales que se llevan y se traen en un portafolio o en el bolsillo y cuyo rendimiento aumenta considerablemente cuando se conectan a una red.

Debido a esto, las redes locales de hoy tienen que trabajar con computadoras que cambian de lugar frecuentemente, a veces dentro de la misma red y otras emigrando hacia otras redes.

Siendo la computación una ciencia con intensa actividad científica y tecnológica, no es extraño que se difiera en el nombre que se le dan a las cosas.

En el caso de las redes son empleados varios términos técnicos como:

- Inalámbrico.
- Portátil.
- Nómada.
- Móvil.

Como sinónimos y homógrafos. Lo que provoca gran confusión entre quienes no están tan familiarizados con el tema.

Recientemente, han aparecido en el mercado las Redes Locales Inalámbricas (WLANs).

Las computadoras (lógicamente) que forman parte de una red inalámbrica reciben el nombre de Computadoras Inalámbricas.

Las redes inalámbricas no usan cables como medio de comunicación. Las computadoras se comunican enviando y recibiendo ondas electromagnéticas que viajan del emisor al receptor a través del espacio. Es importante entender que el nombre de computadora y red inalámbrica se debe al medio de comunicación que usa y nada tiene que ver con movimientos. Una red inalámbrica considera que sus terminales utilizan dispositivos de radio para realizar el proceso de comunicación.

En una red móvil los dispositivos deben realizar la comunicación aún en movimiento.

4.2. Acceso a Redes 4G

4.2.1. IEEE 802.11

Una WLAN es una red inalámbrica en la que una serie de dispositivos (PCs, workstations, impresoras, servidores,..) se comunican entre si en zonas geográficas limitadas sin necesidad de tendido de cable entre ellos. La gran ventaja de esta tecnología es que ofrece movilidad al usuario y requiere una instalación muy sencilla....(F. R. García, V. Quílez. ¨IEEE 802.11(Wi-Fi): El estándar de facto para WLAN¨ Alcatel. 2003).

Entre los componentes que permiten configurar una WLAN podemos mencionar los siguiente:

- Terminales de Usuario (Clientes), dotados de una Tarjeta Interfaz de Red (NIC) que incluye un transceptor radio y la antena.

- Puntos de Acceso (Access Points o APs), que permiten enviar la información de la red cableada (por ejemplo Ethernet) hacia los NIC/Clientes.
- Controlador de APs necesario para despliegues que requieren varios APs por razones de cobertura y/o tráfico.

Este último suele incorporar funcionalidad de AP, de cliente VPN, de cliente RADIUS para labores de autentificar y autorizar con un servidor AAA apropiado (Autentificación, Autorización y Accounting), de routing y de firewalls.

La existencia en el mercado de dichos dispositivos capaces de interconectarse de forma barata y sencilla ha dado origen a una gran variedad de aplicaciones que sobrepasan ampliamente el ámbito de utilización en entornos empresariales para el que nacieron las WLAN.

4.2.1.1. Estandarización de tecnologías WLAN

Las redes WLAN cumplen con los estándares genéricos aplicables al mundo de las LAN cableadas (IEEE 802.3 o equivalentes) pero necesitan una normativa específica adicional que defina el uso de los recursos radioeléctricos. Estas normativas específicas definen de forma detallada los protocolos de la capa física (PHY) y de la capa de Control de Acceso al Medio (MAC) que regulan la conexión vía radio.

El primer estándar de WLAN lo generó el organismo IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) en 1997 y se denomina IEEE 802.11.

Desde entonces varios organismos internacionales han desarrollado una amplia actividad en la estandarización de normativa de WLAN y han

generado un abanico de nuevos estándares. En USA el grueso de la actividad lo mantiene el organismo IEEE con los estándares 802.11 y sus variantes (b, g, a, e, h, ..) y en Europa el organismo relacionado es el ETSI con sus actividades en Hiperlan-BRAN.

La Tabla 5. muestra las características técnicas de las tres tecnologías WLAN más significativas actualmente.

Estándares WLAN	IEEE 802.11b	IEEE 802.11a	HiperLAN 2
Organismo	IEEE (USA)	IEEE (USA)	ETSI (Europa)
Finalización	1999	2002	2003
Denominación	Wi-Fi	Wi-Fi 5	
Banda de Frecuencia	2.4 GHz	5 GHz	5 GHz
Velocidad Máxima	11Mbps	54Mbps	54Mbps
Throughput Media	5.5Mbps	36 Mbps	45 Mbps
Interfaz Aire	SS-DS	OFDM	OFDM
Disponibilidad comercial	> 500 productos	Algunos productos	2003

Tabla 5. Características de los estándares WLAN más significativos

Es necesario mencionar que parte de la información transmitida en el aire es especifica de la transmisión radio (cabeceras, codificación,..) y por lo tanto no forma parte de la capacidad útil para el usuario. Es decir que los valores de velocidad máxima de 11 Mbps ó de 54 Mbps no son equivalentes al concepto de velocidad aplicado en las redes LAN cableadas.

En la tabla podemos ver el "throughput" de una red WLAN que sería equivalente al de una red Ethernet cableada; como se observa este "throughput" resulta ser sensiblemente inferior al considerado como velocidad máxima de la tecnología.

- IEEE 802.11b lidera los desarrollos actuales y su evolución IEEE 802.11a ya está comenzando su disponibilidad en el mercado. Aunque Hiperlan2 resuelve algunos problemas asociados con el 802.11a en temas vinculados con la robustez frente a interferencias y QoS

(calidad de servicio), es muy probable que haya perdido la carrera comercial respecto a ambos protocolos debido a su retraso para introducirse en el mercado.

La banda de frecuencia de 2,4 GHz es compartida por WLAN y por otras tecnologías (Bluetooth para redes PAN, HomeRF para Home-Networking, hornos de microondas..) lo que incrementa la posibilidad de congestionar dicha banda. Para solventar esta problemática se decidió utilizar también la banda de 5 GHz para aplicaciones WLAN aumentando el ancho de banda disponible y la capacidad de tráfico de forma considerable.
La Figura 20. muestra el mapa actual de frecuencias (2002) para aplicaciones WLAN.

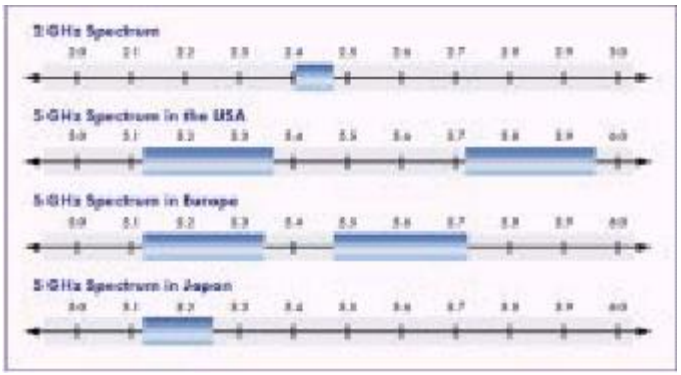


Figura 20. Mapa actual de frecuencias para aplicaciones WLAN

4.2.1.2. IEEE 802.11 b/a

La denominación Wi-Fi (Wíreless-Fidelity) aplicada al protocolo inalámbrico IEEE 802.11b significa que, vía radio, mantiene con fidelidad las características de un enlace Ethernet cableado. Por extensión se conoce como Wi-Fi 5 al protocolo IEEE 802.11a que es el nuevo estándar de la misma familia para la banda de 5 GHz. Dado que estos protocolos Wi-Fi ya están implementados en múltiples productos comerciales podemos

considerar que se han convertido en el estándar para las aplicaciones WLAN en detrimento del estándar Hiperlan2 del ETSI.

A continuación se describen algunos aspectos de interés relacionados con los protocolos Wi-Fi:

4.2.1.3. Topología de Red

Como en la mayoría de redes LAN, en las redes WLAN podemos encontrar dos tipos de topología:

4.2.1.3.1. Red Ad-Hoc y Red Modo Infraestructura

§ Una red "Ad Hoc" consiste en un grupo de PCs que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso.

  Los PCs de la red inalámbrica que quieren comunicarse entre ellos necesitan usar el mismo canal radio y configurar un identificador específico de WiFi (denominado ESSID) en "Modo Ad Hoc".

§ Se conoce como configuración "Modo Infraestructura" a la forma típica de trabajar cuando se utilizan Puntos de Acceso (AP). Si queremos conectar nuestra tarjeta Wi-Fi a uno de ellos, debemos configurarla para trabajar en este modo de trabajo. Es mas eficaz que la red ad-hoc, en la que los paquetes "se lanzan al aire, con la esperanza de que lleguen al destino..", En el Modo Infraestructura la tarjeta de red se configura automáticamente para usar el mismo canal radio que usa el punto de acceso más adecuado (normalmente el mas cercano).

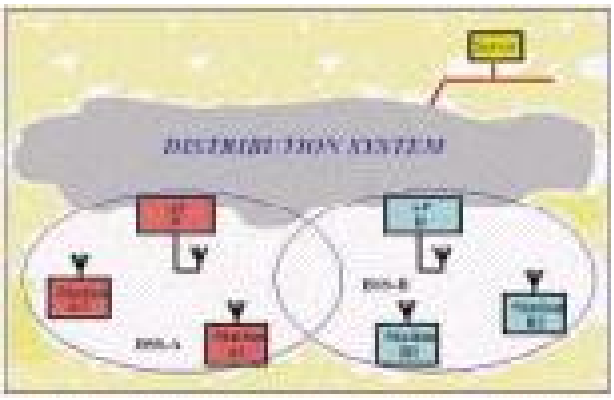


Figura 21. Topología de red con Puntos de Acceso (AP)

La Figura 21. muestra la topología de dos redes WLAN en modo Infraestructura conectadas a un mismo Servidor. El modo Infraestructura es el que se utiliza cuando se quiere conectar una red WLAN a una red cableada.

4.2.1.4. Características Técnicas

Las características técnicas de los protocolos IEEE 8.11 se reflejan en la tabla 5.

Estándar	IEEE 802.11	IEEE 802.11b	IEEE 802.11 g	IEEE 802.11a	IEEE 802.11h
Finalización	1997	1999	Draft en 2002	2002	2003
Frecuencia	2.4 GHz ISM	2.4 GHz ISM	2.4 GHz ISM	5 GHZ	5 GHZ
Velocidad maxima	2Mbps	11Mbps	11Mbps/54Mbps	54Mbps	54Mbps
Interfaz Aire	SS-FH/SS-DS	SS-DS	SS-DS/OFDM	OFDM	OFDM
Otros aspectos	Superado por 802.11b	Disponible en mercado		Disponible en mercado	DCA/Power control

Tabla 5. Características técnicas de los protocolos IEEE 8.11

- IEEE 802.11: Fue el primer estándar disponible y permite dos variantes para el interfaz aire: DSSS (Direct Sequence Spread Spectrum y FH-SS (Frequency Hopped Spread Spectrum). La capacidad alcanzada es de 1 / 2 Mbps (según fabricante).

- IEEE 802.11b es el estándar que lidera los desarrollos actuales de WLAN. Emplea solamente DS-SS y utiliza modulación con forma de onda CCK (Complimentary Code Keying) lo que permite alcanzar hasta 11 Mbps de velocidad.

- IEEE 802.11a, es una evolución del 802.11b, opera en la banda de 5 GHz y ofrece una capacidad de hasta 54 Mbit/s. El interfaz aire utiliza multiplexación OFDM (Orthogonal Frequency División Multiplexing).

- IEEE 802.11g (versión "draft" ó provisional desde Octubre 2002). Con multiplexación OFDM permite hasta 54 Mbps de capacidad máxima en la banda de 2.4 Ghz. Permite interoperabilidad con IEEE 802.11b utilizando un interfaz aire SS-DS y ofreciendo hasta 11 Mbps de capacidad.

- El estándar IEEE 802.11a utiliza la banda de 5 GHz que en Europa no está asignada en este momento de forma prioritaria para aplicaciones WLAN por lo que actualmente tiene que compartir banda con otras aplicaciones.

- La norma IEEE 802.11h es una evolución del IEEE 802.11a que permite asignación dinámica de canales y control automático de potencia para

minimizar los efectos interferentes. Estará disponible a lo largo de este año 2003.

La capa física (PHY) de los estándares IEEE 802.11 se diseñó para cumplir con la regulación de radio frecuencia del FCC (organismo federal USA). Las mismas bandas de frecuencia, con algunas variantes, se utilizan en el resto del mundo.

La Figura 22. muestra el espectro de la banda de 2.4 GHz. Los canales (de 22 MHz cada uno) utilizados por 802.11b son los impares (canales 1,3,5,7,9,11 y13).

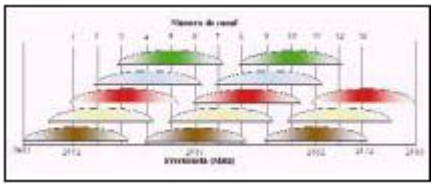


Figura 22. Espectro de la banda 2.4 GHz

Respecto a la capa MAC (Control de Acceso al Medio) podemos mencionar que los estándares IEEE 802.11 utilizan dos posibles mecanismo de acceso:

- CSMA/CA (Carrier Sense Múltiple Access / Collision Avoidance) en el que cada estación escucha a otros usuarios (Carrier Sense) y si el canal esta sin usar la estación está autorizada a transmitir (Collision Avoidance). Pero si está ocupada, cada estación espera hasta que la transmisión presente finalice, y después entra en un procedimiento de "random back". Esto previene que múltiples estaciones intenten obtener el medio inmediatamente después de completarse la transmisión precedente.

- RTS/CTS: Es un procedimiento opcional en el que el terminal que quiera transmitir tiene que enviar al Punto de Acceso una solicitud de envío (Request To Send) a la que el Punto de Acceso accede (Clear To Send) a la transmisión. De esta manera se soluciona el problema del nodo oculto en el que dos transmisores separados no detectan las transmisiones de terminales distantes y los paquetes llegan degradados al punto de acceso. En este caso el punto de acceso coordina el tráfico WLAN al ser el encargado de dar los permisos de transmisión.

4.2.1.5. Capacidad compartida y entornos multi-celda

Como ya hemos visto anteriormente el "throughput" medio de una red WLAN es sensiblemente inferior a la cantidad indicada como velocidad máxima de la tecnología.

- Esto es debido a que parte de la información transmitida se consume en cabeceras radio o en funciones de codificación de canal.

- Adicionalmente la distancia existente entre el terminal y el Punto de Acceso o la existencia de interferencias disminuirán aún más la capacidad práctica transmitida.

- En una red WLAN la capacidad se configura, por defecto, en modo automático para que se regule en función de la calidad del enlace radio.

- Además la capacidad mencionada debe ser compartida por los distintos usuarios que comparten un mismo Punto de Acceso.

- Cuando la capacidad resultante para cada usuario no es suficiente para la aplicación requerida es necesario incrementar el número de Puntos de Acceso en una misma celda (utilizando diferentes canales radio) y así permitir mayores densidades de tráfico.

Para evitar solapamiento entre canales, cuando dos equipos transmiten en el mismo emplazamiento, la norma IEEE 802.11 indica que se debe dejar una separación entre las frecuencias centrales de los canales mayor de 22 MHz.

- Esta condición significa que, en la banda de 2.4 GHz, hasta tres (3) Puntos de Acceso pueden coexistir en una misma celda (suelen emplear los canales 1, 6 y 11 – ver Figura 22).

- La banda de 5 GHz (IEEE 802.11a) permite la utilización de hasta ocho (8) Puntos de Acceso coexistiendo en la misma celda.

- La utilización de dispositivos de banda dual 802.11a + 802.11b permitiría la instalación de hasta once (11) Puntos de Acceso en la misma celda sin solape de frecuencia.

El dimensionado del número de Puntos de Acceso de una red debe garantizar el tráfico en el área considerada pero también la cobertura radioelectrica. En muchas ocasiones la presencia de obstáculos obliga al despliegue de entornos multicelda para garantizar la cobertura del área deseada.

El alcance de estas tecnologías está íntimamente relacionado con las antenas utilizadas y con el entorno de propagación (interior, exterior, obstáculos, …).

Dependiendo de la frecuencia y del número de obstáculos se considera que en aplicaciones de interior (potencia 20 dBm) el alcance típico del 802.11 varía entre 45 y 100 m, sin embargo en aplicaciones de exterior (potencia 30 dBm) y en función de la ganancia de las antenas terminales este alcance puede ser superado ampliamente.

4.2.1.6. Seguridad en IEEE 802.11

La seguridad es uno de los aspectos esenciales para la aceptación de las WLAN por usuarios empresariales o para aplicaciones públicas. Como todas las tecnologías radio, las WLAN no se pueden confinar dentro de los muros de un edificio por lo que deben extremarse las medidas de seguridad, ya que en caso contrario se abriría la red LAN a todo aquel que con una tarjeta WLAN y una antena direccional quiera conectarse.

El protocolo IEEE 802.11 provee seguridad mediante dos atributos:

- Autentificación y el cifrado ó criptografía.

  Autentificación (verificar que una entidad, en este caso un cliente terminal, es realmente quien dice ser) es siempre un paso previo para autorizar a este cliente a comunicarse con otro o con el punto de acceso en el área de cobertura. Existen diferentes opciones para realizar el proceso de autentificación.

Para las WLAN en topologías ad-hoc, la autentificación puede ser en "Open System" o con "Shared Key".

- En un Open System, cualquier terminal cliente puede solicitar la autentificación y el terminal que recibe esta solicitud puede otorgar la autentificación a las estaciones que se encuentran en su lista de usuarios definidos.

- En un sistema Shared Key, solamente las estaciones que comparten una clave secreta pueden ser autentificadas.

Para las topologías en modo infraestructura, la autentificación se resuelve mediante un diálogo entre el cliente y el punto de acceso.

- Los Puntos de Acceso (AP) IEEE 802.11 vienen, por defecto, equipados con capacidad de cifrar según el algoritmo WEP, el cual se utiliza también como base del proceso de autentificación. El algoritmo WEP (Wired Equivalent Privacy) permite que la encriptación se ajuste a 256 bits, 128 bits, 64 bits o deshabilitada. Cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red.

  Sin embargo en el mundo de la criptografía se sabe que, cualquiera que sea la longitud de la clave, siempre hay formas de descifrar los mensajes y por lo tanto es conveniente cambiar las claves frecuentemente. Algunos fabricantes han desarrollado extensiones propietarias de las normas de seguridad (sobre 802.11) para implementar el cambio de claves periódicamente pero el inconveniente es que todos los dispositivos de la red WLAN deben ser suministrados en ese caso por el mismo fabricante.

La tendencia mas reciente es sin embargo emplear el estándar 802.11x como base sólida del mecanismo de autentificación y autorización.

Estos atributos de seguridad que se han descrito operan a nivel físico y de enlace. Pero existen otras vías de añadir mas seguridad al sistema WLAN a otros niveles, tales como jugar con las direcciones MAC de los clientes (nivel 2) o construir VPNs entre el cliente y el servidor correspondiente (nivel 3), con lo que en la práctica puede decirse que la parcela de seguridad está suficientemente consolidada.

4.2.1.7. Roaming: Intercomunicación entre Puntos de Acceso

Los estándares mencionados hasta ahora permiten la conexión de los terminales dentro de una misma subred IP. Hasta ahora si queremos movernos sobre diferentes sub-redes IP debemos utilizar soluciones de un mismo fabricante. Actualmente el IEEE está desarrollando un nuevo estándar que define la intercomunicación entre Puntos de Acceso de distintos fabricantes (facilitando el roaming) y que estará disponible en 2003 (actualmente ya existe una versión preliminar de dicho estándar).

Entre otros temas la norma define el registro de un Punto de Acceso dentro de una red y el intercambio de información cuando un usuario se mueve por una zona cubierta por AP de diferentes fabricantes. Esta norma es conocida como IEEE 802.11 f.

4.2.1.8. Dispositivos WLAN disponibles en el mercado

En 1999 se creó una organización internacional sin ánimo de lucro denominada Wi-Fi Alliance (WECA) que certifica la interoperabilidad de productos de distintos fabricantes basados en la especificación 802.11.

Actualmente pertenecen a la Alianza Wi-Fi 205 compañías y ya han recibido la certificación Wi-Fi® 611 productos diferentes desde que se inició el proceso en Marzo de 2000.

Esta certificación garantiza que productos de distintos fabricantes son capaces de comunicarse entre sí y gran parte de ellos ya están disponibles comercialmente. Existen en el mercado una gran variedad de dispositivos:

- Puntos de Acceso (AP), NIC inalambricos, Portatiles con Wi-Fi integrado, Terminales moviles, Pocket PCs Wi-Fi, Servidores inalámbricos. La Figura 23. muestra algunos de estos dispositivos.

Figura 23. Dispositivos WLAN disponibles en el mercado.
(Punto de Acceso, Tarjeta PCMCIA , Wireless PDA y Tarjeta Compact Flash)

Las tarjetas NIC mas comunes son las que vienen en formato PCMCIA, para portátiles, aunque también las hay en formato PCI, en CompactFlash, Smart Card y similares. Son equivalentes a una tarjeta de red normal, sólo que sin cables. Su configuración a nivel de IP es igual que una Ethernet. Las tarjetas para portátiles o PDAs están a la venta por precios de $100/200. Algunos fabricantes ofrecen PCs y PDAs con el interfaz WLAN integrado. De momento estos componentes tienen un problema de consumo de energía

que debe ser resuelto en el futuro próximo para garantizar el mantenimiento de las aplicaciones. Actualmente una PDA Wi-Fi tiene una autonomía limitada.

4.2.1.9. Aplicaciones WLAN

Originalmente las redes WLAN fueron diseñadas para su empleo en redes empresariales. En este tipo de aplicaciones una sub-red WLAN, compuesta por varios Puntos de Acceso inalámbricos, se conecta a una red cableada que nos permite acceder a todos los servicios disponibles en la empresa.

Pero en la actualidad las redes WLAN han encontrado una gran variedad de nuevos escenarios de aplicación tanto en el ámbito residencial como en entornos públicos:

- Escenario Residencial: Una línea telefónica terminada en un router ADSL al cual se conecta un AP para formar una red WLAN que ofrece cobertura a varios PCs en el hogar.

- Redes Corporativas: Una serie de Puntos de Acceso distribuidos en varios áreas de la empresa conforman una red WLAN autónoma o complementan a una LAN cableada. Son aplicaciones de alta densidad tráfico con altas exigencias de seguridad.

- Acceso público a Internet desde cafeterías, tiendas, ... En estos establecimientos se ofrece a los clientes una tarjeta inalámbrica (NIC) que permiten acceso a Internet desde sus propios portátiles. Es un escenario de acceso, involucrando un bajo número de Puntos de Acceso, parecido al residencial, pero que necesita mayores funcionalidades en el núcleo de red (AAA, billing, ..).

§ Acceso público de banda ancha en pequeños pueblos, hoteles, campus universitarios, .. .En general este escenario necesita múltiples Puntos de Acceso para garantizar la cobertura del área considerada.

Es necesario distinguir entre las redes sin ánimo de lucro (redes libres) que ofrecen un servicio gratuito a una comunidad y las redes que ofrecen servicios de pago a clientes que residen o transitan por la zona de cobertura.

§ WLAN para cobertura de "Hot Spots" (escenario público). Estas redes cubren áreas donde se concentra un gran número de usuarios de alto tráfico como son aeropuertos, estaciones de ferrocarril, centros de congresos, …

La red a instalar requiere un elevado número de Puntos de Acceso así como importantes exigencias de seguridad, gestión de red, facilidades de facturación, etc.

§ Acceso a Internet desde medios públicos de transporte. En los últimos meses se está convirtiendo en un tema de actualidad el hecho de que compañías ferroviarias quieran ofrecer acceso de banda ancha desde sus trenes en movimiento, o compañías aéreas que ofrecen acceso a Internet desde sus vuelos intercontinentales o varias ciudades que disponen de taxis que incorporan una pantalla integrada en el asiento que permite acceder a Internet de banda ancha.

Las primeras aplicaciones públicas de WLAN se instalaron en campus universitarios y son del tipo "redes libres" sin ánimo de lucro. Cuando las redes públicas son del tipo de pago por servicios siempre hay un operador de telecomunicaciones detrás de su gestión. Un operador establecido (especialmente si es móvil) dispone de gran parte de la infraestructura necesaria para ofrecer un servicio de amplia cobertura. Actualmente existen varios tipos de operadores actuando en el sector WLAN:

- Operadores "Wíreless ISP" que ofrecen cobertura local de banda ancha en pueblos o en pequeñas ciudades utilizando WLAN.

- Operadores "Wíreless ISP" que ofrecen cobertura nacional en los puntos de alta densidad de trafico conocidos como "hot spots" (aeropuertos, estaciones, hoteles, …) utilizando WLAN.

- Operadores móviles que complementan su oferta de movilidad global con cobertura WLAN en "hot spots". Esta actuación es debida a dos factores: de un lado evitar que los operadores WLAN anteriores, que ofrecen la cobertura de "Hot Spots" a nivel nacional, capten un porcentaje importante del mercado de servicios de móviles. De otro lado capitalizar su infraestructura de red dado que ya poseen muchos activos necesarios para las redes WLAN tales como plataformas de autentificación, de gestión de red y de servicio, de facturación, etc.

4.2.1.10. Entorno Regulatorio

Los reguladores de los distintos países están actualmente en el proceso de asignación de bandas de frecuencia para aplicaciones WLAN. Cada país tiene una estrategia diferente en este tema y por lo tanto es conveniente que

los usuarios potenciales de WLAN comprueben localmente si solamente pueden desplegar Puntos de Acceso (AP) en aplicaciones de interior o sí también pueden desplegarlos en entornos de exterior y cuales son las frecuencias que deben utilizar.

Actualmente en Europa gran parte de la banda de 5 GHz está reservada para aplicaciones de Hiperlan2 o de tecnologías con asignación dinámica de frecuencias (como 802.11h.). Tecnologías como 802.11a estarían limitadas a usar solamente 150 MHz del total de la banda disponible.

4.2.1.11. Tendencias futuras

Distintos organismos (WECA, IEEE, ETSI, ..) continúan trabajando en la búsqueda de soluciones para mejorar alguna de las limitaciones actuales de la tecnología. Su actividad garantiza que en los próximos meses los aspectos de seguridad y "roaming" estarán plenamente resueltos desde la infraestructura de red.

En el ámbito tecnológico dispondremos de Puntos de Acceso duales (802.11a y 802.11b) y de nuevos NIC para PDAs y Tablet PCs optimizados para minimizar efectos interferentes y maximizar la movilidad, así como de PCs con módems WiFi integrados en silicio.

Asimismo se mejorará de forma drástica el consumo de estos dispositivos inalámbricos (especialmente en soluciones portátiles) que es una de las principales exigencias para garantizar el éxito de las redes WLAN.

4.3. QoS en Redes 4G

Esta nueva arquitectura basada en conmutación de paquetes, requiere la incorporación de técnicas que soporten mecanismos de calidad de servicio (QoS), movilidad, seguridad y contabilidad basados en IP[9].

4.3.1. Descripción de la Arquitectura de Red

La principal característica de las propuestas de redes móviles 4G es la utilización de tecnologías IP en el núcleo y en las redes de acceso, para soportar todos los servicios. Mientras en redes 3G coexistirá un núcleo IP para la red de datos con otro núcleo basado en conmutación de circuitos para la prestación de servicios de voz, en las redes 4G sólo existirá un núcleo IP sobre el que se transportará todo el tráfico.

Una imposición para el núcleo de las redes de cuarta generación será el soporte del protocolo IP en su versión 6, IPv6, con lo que quedarían resueltos problemas como el espacio de direcciones, vital para el despliegue de una nueva red dónde sería deseable el uso de direcciones públicas.

Existen diferentes tecnologías de acceso que aparecerán en un escenario 4G. Se trata de tecnologías complementarias, de manera que todas podrán coexistir, y en función de las necesidades del cliente podrá optar por alguna de las siguientes:

- WCDMA (UMTS)

[9] C. García, P. A. Vico, A. Cuevas, I. Soto, J. I. Moreno. ¨QoS en redes móviles de cuarta generación¨. Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid. 2003

- Wireless LAN 802.11
- Ethernet

En la figura se representan los elementos funcionales de los que se compone una red de cuarta generación.

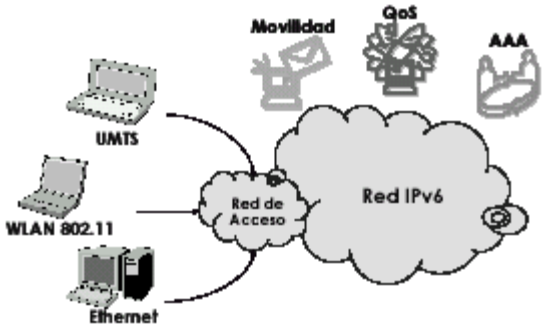


Figura 24. Arquitectura de red de cuarta generación

Los elementos más representativos de esta arquitectura son:

- **QoS**. La tecnología IP tal como se concibió originalmente, no ofrece ningún tipo de garantías de Calidad de Servicio. Sin embargo, existen servicios, entre ellos el telefónico, con rigurosos requisitos de retardo y variación del retardo (jitter), lo que hace necesario añadir funcionalidad a IP para que las redes basadas en este protocolo sean capaces de soportar este tipo de servicios.

- **AAA**. Los sistemas tradicionales de contabilidad basados en la generación de CDR (Call Detail Record) deben ser modificados para soportar de forma eficiente movilidad de usuarios sobre una red basada en datagramas. Adicionalmente deben soportarse mecanismos de autenticación y autorización para ofrecer mecanismos seguros de identificación y acceso de usuarios. En este sentido el

IETF ha definido los sistemas AAA[10], encargados de comprobar la identidad de los usuarios, de controlar los servicios que usan y de tarificarles por ello. Estos sistemas utilizan las redes IP para transportar la información de señalización necesaria. El IETF propone el protocolo DIAMETER[11], sustituto del tradicional RADIUS y capaz de soportar movilidad Inter Dominio (roaming) de usuarios.

§ **Movilidad**. Las redes de 4G deberán soportar mecanismos eficientes que permitan la movilidad de usuarios, que utilizando el mismo o distinto terminal se conecten a la red mediante distintas redes de acceso (WCDMA, WLAN, Ethernet, etc.) operadas por distintas entidades. Esto requiere mecanismos que soporten handover (traspaso) entre subredes bajo igual o distinta tecnología (handover horizontal y vertical) de forma eficiente, teniendo como elemento común el transporte IP.

La base del soporte de movilidad en redes IP son los protocolos Mobile IP. La propuesta de Fast Handover permitirá conseguir handovers sin interrupción apreciable de las comunicaciones.

Esta movilidad requiere interaccionar con los procesos de soporte de QoS en el caso de traspasos entre áreas con distintos recursos de red disponibles y con los mecanismos de AAA para el caso de traspasos entre redes pertenecientes a distintos dominios administrativos.

[10] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence: Generic AAA Architecture; Internet Engineering Task Force, Experimental RFC 2903, August 2000.

[11] Pat R. Calhoun, "Diameter Base Protocol", <draft-ietf-aaa-diameter-10.txt>, April 2002

4.3.2. Soporte de QoS en redes 4G

Existen diferentes iniciativas para proporcionar QoS en una red IP. El IETF divide sus esfuerzos en dos grupos **Intserv** y **Diffserv**.
La implementación de la tecnología **Intserv** presenta problemas de escalabilidad. La tendencia es el uso de **Diffserv** en el núcleo combinado con Intserv como solución en la red de acceso.

Como los principales problemas de recursos aparecen normalmente en la red de acceso, y dado que sobredimensionar el núcleo es relativamente sencillo y barato, el uso combinado de Intserv y Diffserv en el acceso y núcleo respectivamente proporciona un buen compromiso entre costo y eficiencia.

Sin embargo esta solución como técnica de QoS presenta algunas limitaciones:

- En Diffserv, al no existir una reserva extremo a extremo, la QoS no está garantizada al 100%. Lo más que podremos alcanzar es una alta probabilidad de obtener el nivel de calidad de servicio deseado, si bien un buen dimensionado de la capa de transporte asegurará un buen servicio.

- Las reservas realizadas por el usuario se traducirán en un código (DSCP) presente en los paquetes que éste envíe, que determinará el tratamiento de nuestro tráfico. El número de códigos es limitado y será el proveedor el encargado de definir éstos así como su implementación. Aparece entonces la posibilidad de que un mismo código DSCP no tenga el mismo significado para diferentes proveedores de servicio, de manera que la calidad de servicio final

vendrá determinada por la relación entre los diferentes proveedores que se atraviesen.

El modelo se basa en el uso de un elemento encargado de la gestión de calidad de servicio, el **QoSBroker**. Este componente se encarga de administrar la reserva de recursos y gestionar los routers de la red de acceso y del núcleo.

El QoSBroker se comunica con los routers usando el protocolo COPS para el intercambio de información relativa a gestión y administración de la red. COPS[12] define un modelo cliente (routers) servidor (QoSBroker). El QoSBroker, corazón del sistema de calidad de servicio, conocerá el estado de los enlaces hacia cada red de acceso, y podrá autorizar o denegar el acceso de un usuario a la red según la carga. Este elemento mantendrá una relación entre los códigos DSCP utilizados y el comportamiento (PHB) que debe ofrecerse al tráfico. Para ello se ha definido una tabla donde se identifica los servicios.

Service		Relative Priority	Service Parameters	Service description
Name	Class			
S1	EF	1	Peak BW: 32Kbit/s	Real time service
S1G	AF41	2a	unspecified	Signaling
S2	AF21	2b	CIR:256Kbit/s	Priority (urgent) data
S3	AF*	2c	Three drop precedence	Olympic service
S4	BE	3	Peak bit rate: 32Kbit/s	Best effort
S5	BE	3	Peak bit rate: 64Kbit/s	Best effort
S6	BE	3	Peak bit rate: 256Kbit/s	Best effort

Tabla 6. Servicios ofrecidos al usuario

[12] D. Durman et al. “The COPS (Common Open Policy Service) Protocol” RFC 2748, January 2000.

Las especiales características de la clase *Expedited Forwarding* la hacen idónea para servicios en tiempo real como podrían ser conferencias de audio o video conferencias. Este tipo de tráfico no admite un retardo excesivo, ni la variación del mismo (jitter), además de requerir un ancho de banda bien determinado.

Las clases *Assured Forwarding* podrían utilizarse para diferentes tipos de tráfico.

- Por un lado el tráfico de señalización podría tratarse con una clase AF, resultando necesario realizar una previa caracterización del mismo para definir correctamente las técnicas de encolamiento requeridas.

- El tradicional sistema de servicios olímpicos, definiendo las subclases: oro, plata y bronce, según el orden de procedencia en el descarte de paquetes. Este sistema permite una gran flexibilidad para ofrecer una gran variedad de servicios al usuario.

- Finalmente podríamos destinar otra subclase AF, para algún tipo de tráfico de alta prioridad que no deseamos que compita por los recursos con el tráfico de servicios olímpicos.

Por último, resulta interesante definir el tradicional servicio *Best Effort* para el tráfico que no presenta ningún requisito de calidad de servicio. Debido a las especiales características de las redes de 4G dónde el acceso podría ser una red Ethernet con una capacidad de hasta 100 Mbits, resulta necesario imponer un límite al tráfico inyectado por el usuario para evitar el colapso de la red. Este límite se puede implementar a través de la definición de diferentes subclases de tráfico BE, con diferentes límites de ancho de banda, que se corresponderían con diferentes filtros en los routers de acceso.

Como vemos la interacción entre el QoSBroker y los routers determinará la QoS obtenida. Para ello podemos distinguir entre routers frontera o de acceso (Access Router) y routers del núcleo (Core Routers).

Las funciones referentes a QoS que deberán implementar todos los routers serán:

- Clasificación.
- Acondicionamiento
- Encaminamiento de tráfico.

Estas funciones son lo suficientemente sencillas para ser escalables a toda la red. De esta manera no aparecerá ningún problema de implementación en los **Core Routers,** evitando así el principal problema de escalabilidad del modelo Intserv.Por otra parte los **Access Routers** serán los encargados de controlar el acceso a la red, para ello deberán comunicarse con las entidades anteriormente comentadas: AAA Server y QoSBroker.

El módulo encargado de la gestión y provisión de QoS en los router de acceso es el **QoSManager**.

Las principales funciones desarrolladas por este módulo son las siguientes:

- Aplicar algoritmos de gestión y planificación de colas de QoS bajo configuración del QoS Broker. Esta configuración podrá cambiar en tiempo de ejecución.
- Mantener una comunicación COPS con el QoS Broker actuando como cliente PEP.

- § Traducción de los protocolos de autentificación CHAP-DIAMETER para permitir el intercambio de señalización entre el usuario y el AAAC que se encuentra dentro de la red DiffServ.

- § Capturar flujos de tráfico dirigidos hacia el núcleo de red DiffServ. Esos tráficos deberán estar marcados con determinados DSCPs para ser susceptibles de aplicárseles QoS.

- § Generar estadísticas de uso de sus colas e interfaces para su envío al QoSBroker.

4.3.3. QoSManager

4.3.3.1. Implementación

En la figura podemos observar la arquitectura funcional de nuestro Router de acceso, y los diferentes bloques de los que éste se compone. Durante la explicación de los procesos podremos evaluar como estos bloques interoperan entre si.

Figura 25. Diagrama de bloques del router de acceso.

Las principales contribuciones tecnológicas a la hora de implementar el QoSManager se corresponden a sus dos principales funcionalidades: calidad de servicio/conformado y políticas remotas.

Para lo primero se utilizan las librerías TC API (Traffic Control Application Program Interface) de IBM. El TC API es una interfaz programable para manejar los mecanismos de QoS del núcleo (*kernel*) de red en Linux. La funcionalidad de QoS en Linux se limita a clasificar paquetes de red, conformar y planificar. Para ello se desarrollaron una serie de funciones que permiten interactuar desde el espacio de usuario con el *kernel* de red. Esa interacción, transparente al usuario, se realiza mediante los sockets *netlink* y nos permite construir árboles de QoS y obtener estadísticas de ellos.

Respecto a la segunda característica utilizamos el protocolo COPS (Common Open Policy Service). Este protocolo, descrito en la RFC 2748, define un modelo cliente/servidor sencillo para proporcionar control de políticas a protocolos de señalización de calidad de servicio. El protocolo COPS se basa en sencillos mensajes de petición y respuesta utilizados para intercambiar información acerca de políticas de tráfico entre un servidor de políticas (**PDP**, Policy Decision Point) y distintos tipos de clientes (**PEP**s, Policy Enforcement Points). Utiliza TCP como protocolo de transporte, es extensible en semántica y guarda el estado de todas las políticas.

Cada mensaje COPS consta de una cabecera COPS y un conjunto de objetos COPS ya definidos. En la figura podemos ver un ejemplo:

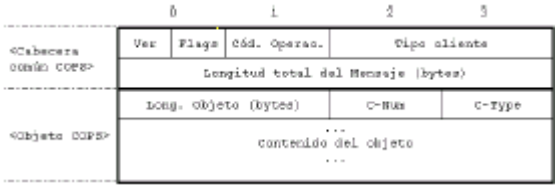


Figura 26. Ejemplo de mensaje COPS

4.3.3.2. Procesos

Se van a describir los diferentes procesos en los que se ve involucrado el router de acceso. De entre ellos cabe destacar el registro y configuración del router, la autorización de un usuario para el uso la red y el proceso de movilidad.

4.3.3.2.1. Registro de un usuario en la red

Cuando un cliente desea registrarse en la red debe contactar en primer lugar con el servidor de AAAC. Mediante conexiones CHAP (red de acceso) y DIAMETER (red) se realiza la autenticación del usuario, por lo tanto, el Router debe encargarse de la conversión entre ambos tipos de protocolos. Antes de que se le envíe al usuario la confirmación de registro, el AAAC debe instalar en el QoSBroker toda la información de conformado para todos los posibles tráficos del cliente. Este intercambio de información se realiza mediante el protocolo COPS. La información transferida, llamada ¨*Servicios de Red*¨, especifica el tiempo de vida del servicio, el ancho de banda, el tamaño de las ráfagas y la prioridad.

Finalmente el usuario, si la autorización ha sido exitosa, debe recibir la confirmación de su registro y una tabla con los DSCPs (Differentiated Services CodePoints) con los que le está permitido marcar sus tráficos de salida.

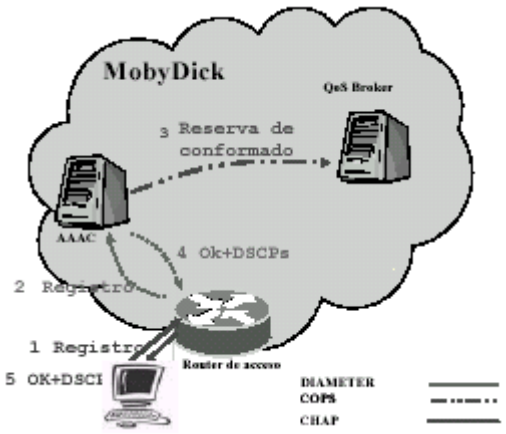


Figura 27. Fase de registro en la red

4.3.3.2.2. Registro y configuración del QoSManager

El QoSManager, al arrancar su sesión COPS, debe registrase en su QoSBroker y acto seguido debe pedirle la lista de correspondencias entre DSCPs y parámetros de calidad de servicio (PHBs). Esa configuración la mantiene el QoSBroker en una tabla llamada: '*tabla de comportamiento'* y se usa en inicializaciones y reconfiguraciones de la interfaz de acceso de nuestro QoSManager.

La información es interpretada en el Router y, mediante las librerías TC API, se crea un árbol de disciplinas de colas en su interfaz de acceso. Los paquetes que viajen hacia la red de acceso recibirán diferentes calidades dependiendo de su DSCP. En la figura podemos ver un esquema de este proceso:

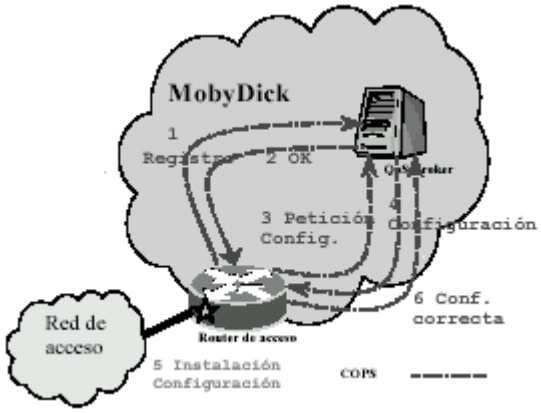


Figura 28. Registro y configuración del router

4.3.3.2.3. Autorización y Acceso a la red por un usuario

Una vez que el usuario está registrado en la red, éste puede comenzar a cursar tráfico a ésta marcando los paquetes con los DSCPs recibidos. La elección de un DSCP determinado vendrá impuesta por el tipo de tráfico enviado.

Cuando el capturador del router de acceso detecta un nuevo tráfico desde la red hogar a la red estudiada, pregunta al QoSBroker si tiene que autorizar ese tráfico o no. En caso afirmativo, el QoSBroker debe enviar al router los parámetros de conformado para ese flujo. Toda la interacción se realiza a través del protocolo COPS.

El router, en la petición, envía al Broker la siguiente información de identificación del tráfico: direcciones IPv6 de origen y destino y el DSCP del tráfico. El QoSBroker comprueba entonces si la conexión estaba previamente instalada por el AAAC. Si la conexión está instalada, el QoSBroker envía al router un mensaje de autorización positiva junto con los parámetros de conformado (régimen binario y ráfaga). Si la conexión no está instalada la respuesta es negativa y el tráfico será bloqueado por el router.

El QoSManager, mientras todo esto ocurre y hasta que el Broker no le confirma la autorización, bloqueará el tráfico por seguridad.

Una vez que el router ha aplicado la orden del QoSBroker debe enviarle a éste un mensaje COPS informándole sobre el éxito o no de la decisión.
Tanto la autorización como el conformado tienen un tiempo de vida en el router. Cuando ese tiempo se agote, el router deberá realizar una nueva petición para saber si ese tráfico continúa estando autorizado para usar los recursos de la red estudiada o deberá ser bloqueado. De esta manera las autorizaciones y el conformado de los tráficos pueden ser refrescados periódicamente. En la figura podemos ver un esquema de este proceso en el caso de una autorización positiva.

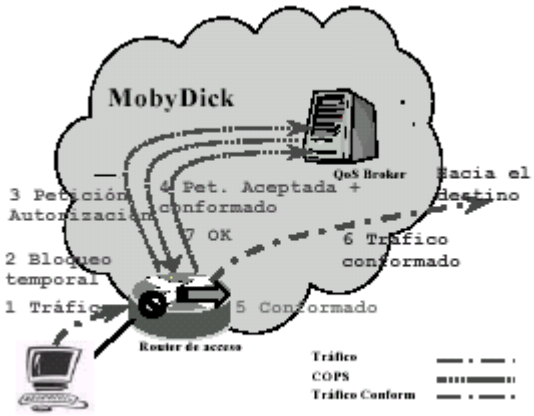


Figura 29. Acceso a la red de un tráfico

4.3.3.2.4. Obtención de estadísticas y reconfiguración

Al mismo tiempo que las capturas y conformados de nuevos tráficos ocurren, el router realiza otras operaciones. En este parte vamos a comentar dos de ellas: la obtención de estadísticas del uso de su interfaz de acceso y la comprobación de peticiones de reconfiguración provenientes del QoSBroker.

Según explicamos en el arranque de nuestro router, el QoSBroker configura las colas de calidad de servicio del interfaz de acceso de éste. Por estas colas pasan todos los tráficos que viajan de la red estudiada a la red de acceso. Mediante unas funciones del TC API, el router puede obtener estadísticas de uso de las colas tales como: régimen binario, paquetes por segundo, descartes por segundo, etc. Estas estadísticas son enviadas al QoSBroker a través de la conexión COPS, por lo que este servidor puede hacer cálculos con ellas y estimar la carga del router. El incremento de tiempo que debe utilizarse entre dos informes de estadísticas consecutivas es también configurado por el Broker mediante un parámetro en el arranque.

Si el algoritmo de planificación del Broker estima necesario una modificación en los parámetros de las colas de acceso del router, puede cambiar la '*tabla de comportamiento*' y ordenar una reconfiguración. De este modo el router volvería a solicitar al QoSBroker la información sobre las colas de QoS y las instalaría de nuevo actualizadas en el interfaz de acceso.

En la figura podemos ver un esquema de este proceso.

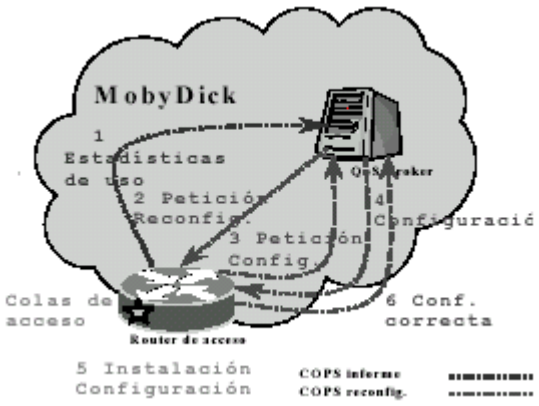


Figura 30. Transferencia de estadísticas y reconfiguración

4.3.3.2.5. MOVILIDAD

El QoSManager permite la interacción con el módulo de '*Fast Hand-Over*' de la red estudiada para traspasos rápidos de la configuración de calidad de servicio de un router a otro.

Cuando un usuario se mueve de una red de acceso gobernada por un router a otra, se dice que se ha producido un '*Hand-Over*'. En nuestro caso interesa que esa operación sea lo más rápida posible para no interferir al tráfico.
En esta acción están implicadas al menos tres máquinas: el antiguo router de acceso, el nuevo y uno o más QoSBrokers.

El router de acceso antiguo debe informar a su QoSBroker sobre el cliente que va a moverse y hacia qué nuevo router de acceso. La información que le pasa el módulo de *Hand-Over* al router y este a su vez le comunica al Broker es la siguiente: CoA antigua, CoA nueva y dirección del nuevo router.
Dado que la transmisión ha de ser inmediata, el módulo de *Fast Hand-Over* debe interrumpir la ejecución del viejo router para que mande el mensaje de traspaso al Broker.

Cuando el QoSBroker recibe el mensaje comprueba si el router destino está dentro de su red. En caso afirmativo, debe buscar todos los tráficos instalados para ese usuario y mandárselos inmediatamente al nuevo router para que este instale las autorizaciones y los filtros de conformado correspondientes.

Si el router nuevo no está en la red que gobierna el primer QoSBroker, éste debe mandar la información de los tráficos del cliente al QoSBroker que administra al nuevo router de acceso. El nuevo Broker enviará la información

al router final y ambos instalarán la parte de configuración que les corresponde.

La información que se transfiere al router de acceso final es el conjunto de todos los tráficos que tenía instalados en la red hogar. Los parámetros son: direcciones de origen y destino, DSCPs e informaciones de conformado.
Una vez que el nuevo router ha recibido el mensaje del Broker, instala todos los tráfico requeridos e informa al servidor de la correcta (o no) instalación de estos.

En la figura podemos ver un esquema de este proceso en el caso de que el mismo QoSBroker gobierne a los dos routers de acceso involucrados.

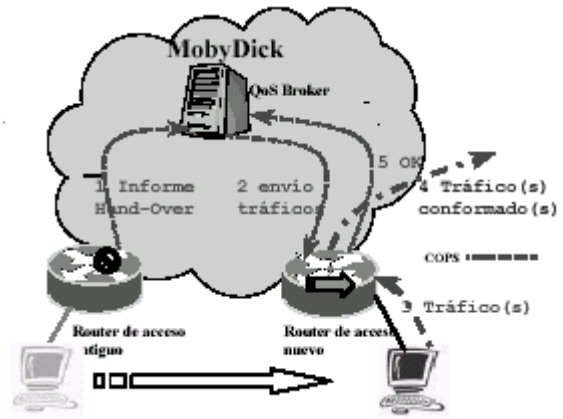


Figura 31. Fast Hand-Over

4.3.3.2.6. BORRADO DE UNA CONEXIÓN CADUCADA

Cuando el QoSBroker ha autorizado una conexión en el router y ésta deja de transmitir paquetes, el programa capturador de tráfico asociado no detecta nada. Por lo tanto, cuando el QoSManager procede a actualizar esa conexión y se percata de que no está en la lista de conexiones capturadas, espera algunos segundos más por tráfico antes de borrarla. La cantidad de

segundos que espera es configurable en el programa. Si el capturador sigue sin detectar tráfico por esa conexión pasado el tiempo de guarda, el router la desautorizará e informará al QoSBroker de ello mediante un mensaje COPS.

CONCLUSIONES

El Protocolo IP Móvil, facilita la movilidad de terminales dentro de redes IP versión 4 sin tener que realizar ninguna modificación ni en el mismo protocolo IP, ni en los elementos de interconexión *routers* encargados de realizar el encaminamiento de los paquetes. De esta manera se permite que un computador portátil pueda moverse con total libertad y acceder a los servicios de red que le ofrece su entorno local desde cualquier parte del mundo sin tener que realizar ningún tipo de modificación en la configuración de sus aplicaciones ni del sistema operativo.

En situaciones en las que la conexión física a la red se produce mediante técnicas inalámbricas, como por ejemplo utilizando redes de área local *wireless*, o bien a través de servicios de datos proporcionados por los sistemas celulares (GSM, GPRS, CDPD, etc.) es cuando se pone de relieve la importancia de poder acceder de forma transparente a cualquier aplicación.

En la última edición del protocolo IP, la denominada versión 6, ya se prevén este tipo de acciones modificando de forma notable todos los aspectos relacionados con el formato de las direcciones de red, así como otros aspectos relacionados con el encaminamiento de los paquetes.

La importancia de implementar Móvil IP, en una red LAN, es que tiene la capacidad de soportar de forma eficaz la difusión de contenidos en tiempo real a toda la red y comunicación interactiva de grupos en tiempo real. Soporta el acceso inalámbrico, movilidad de terminal y movilidad personal.

Se introducen mecanismos de señalización que permitan crear servicios similares a los existentes en las redes telefónicas actuales. Incorpora protocolos de seguridad en la arquitectura TCP/IP que permitan proteger la información y las actividades que se realizan a través de Internet.

La arquitectura que presenta IP Móvil consiste en un Nodo móvil; que puede cambiar su punto de conexión de un enlace a otro, sin perder la comunicación. Un Agente hogar, que es un router con una interfaz en el enlace hogar del nodo móvil, el cual; El nodo móvil lo mantiene informado de su ubicación actual, representada por su dirección care-of; y por ultimo el agente remoto, router en el enlace remoto del nodo móvil, ayuda al nodo móvil informándole al agente hogar su dirección care-of, en algunos casos proporciona una dirección care-of y destunelea los paquetes enviados al nodo móvil.

Las redes de cuarta generación presentan la característica de ser una tecnología inalámbrica, en ella se encuentra el estándar IEEE 802.11, desarrollado para suplir las necesidades de conectividad de los usuarios. Esta tecnología se considera como la única en alcanzar los niveles de calidad que se requieren.

Para estas redes de cuarta generación se necesitan proporcionar QoS de las cuales existen diferentes iniciativas para proporcionar en una red IP Móvil. El IETF divide sus esfuerzos en dos grupos **Intserv** y **Diffserv**. La implementación de la tecnología **Intserv** presenta problemas de escalabilidad. La tendencia es el uso de **Diffserv** en el núcleo combinado con Intserv como solución en la red de acceso.

RECOMENDACIONES

La monografía Movilidad IP en Redes 4G es un texto de consulta para las personas que quieran profundizar en la conceptualización del protocolo mobile IP: Arquitectura, Configuración y Diseño en Redes 4G. Este se desarrollo teniendo como base las ultimas tendencias de los protocolos de comunicaciones móviles aplicados a las redes LAN inalámbricas.

El desarrollo de futuras líneas de investigación en este campo de redes LAN inalámbricas puede darse en el diseño de redes mobile IP entre distintos Proveedores de Servicios de Internet Inalámbrico demostrando las bondades de este nuevo protocolo desarrollo por el IETF para redes móviles.

Otra de las características que presenta este documento es su fácil comprensión, por lo que fue desarrollado para estudiantes con conocimientos en comunicaciones de datos y Telecomunicaciones.

BIBLIOGRAFIA

- Bonilla, Darío. WCDMA vs. GSM COMO INTERFAZ AÉREA PARA TERCERA GENERACIÓN DE TELEFONIA CELULAR. Universidad de las Américas-Puebla. Mayo de 2003

- Perkins, Charles. “Mobile IP: Design, Principles and Practices”. Addison-Wesley. 1997.

- “Mobility Support in IPv6”, <draft-ietf-mobileip-ipv6-24.txt>, David B. Johnson, Charles Perkins, Jari Arkko. June 2003.

- Quemada, Juan. Hacia una Internet de Nueva Generación. Universidad Politécnica de Madrid, UPM. Versión 6, 2 de Enero de 2004. PAG, 51-54.

- Stalling, William. Comunicaciones y Redes de Computadoras. Quinta Edición. Prentice Hall.

- Redes de Acceso de Banda Ancha: Arquitectura, Prestaciones, Servicios y J. Berrocal, E. Vázquez, F. González, M. Álvarez-Campana, J. Vinyes, G. Medinabeitia, V. García, Ministerio de Ciencia y Tecnología, 2003.

Documentos Web

Documento Internet Engineering Task Force: Request For Comments RFC 2002 “IP Mobility Support”. http://www.faqs.org/rfcs/rfc2002.html

Documento Internet Engineering Task Force: Request For Comments RFC 2003 “IP Encapsulation within IP”.

Documento Internet Engineering Task Force: Request For Comments RFC 2004 “Minimal encapsulation within IP”.

Documento Internet Engineering Task Force: Request For Comments RFC 768 “User Datagram Protocol”

Documento Internet Engineering Task Force: Request For Comments RFC 791 “Internet Protocol”

Documento Internet Engineering Task Force: Request For Comments RFC 1256

James d. Solomon, Mobile IP: The Internet Unplugged, editorial Prentice Hall series in computer networking and distributed systems, 1996-97

V. Marques et al., “An Architecture Supporting End-to-End QoS with User Mobility for Systems Beyond 3rd Generation”, IST Mobile Summit 2002

V. Marques et al., “An IP-based QoS Architecture for 4G operator scenarios”, IEEE Wireless Communication, June 2003

C. de Laat et al.: “Generic AAA Architecture” IETF, Experimental RFC 2903, August 2000

IETF, AAA Working Group - http://www.ietf.org/html.charters/aaacharter.html

Pat R. Calhoun, "Diameter Base Protocol", <draft-ietf-aaa-diameter-10.txt>, April 2002

Stefano M. Faccin, "Diameter Mobile IPv6 Application",<draft-le-aaa-diameter-mobileipv6-00.txt>, 2001

Rigney, C. et al, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

G. Dommety, ed. "Fast Handovers in Mobile-IPv6", Internet Draft, work in progress, <draftietf-mobileip-fast-mipv6-3.txt>, July 2001

IETF, Intserv Working Group - http://www.ietf.org/html.charters/intservcharter.html

IETF, Diffserv Working Group - http://www.ietf.org/html.charters/diffservcharter.html

K. Nichols, S. Blake, F. Baker, D. Black. “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, RFC 2474, December 1998.

D. Durman et al. “The COPS (Common Open Policy Service) Protocol” RFC 2748, January 2000

J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. “Assured Forwarding PHB Group”, RFC 2597, June 1999

V. Jacobson, K. Nichols, K. Poduri. “An expedited forwarding PHB”, RFC 2598, June 1999

“*IBM TC API Project*” http://oss.software.ibm.com/developerworks/projects/tcapi/

ANEXO A. GLOSARIO

Primera Generación 1G

Redes de radios móviles, se basaban principalmente en una sola antena con un número limitado de canales, por tecnología analógica.

NMT

Nordic Mobile Telephone; Estándar de primera generación.

TACS

Total Access Communications Systems; Estándar de primera generación.

AMPS

Advanced Mobile Phone Service; Estándar de primera generación.

Segunda Generación 2G

Grupo de sistemas que iniciaron o evolucionaron hacia la utilización de técnicas digitales para realizar las transmisiones. Las redes de la segunda generación presentaban una capacidad mucho mayor con respecto a los de la primera generación.

GSM

Global System for Mobile Communications; Estándar de segunda generación.

D-AMPS

Digital AMPS o también llamado TDMA**;** Estándar de segunda generación.

CDMA IS-95

Code División Múltiple Access**;** Estándar de segunda generación.

PDC

Personal Digital Cellular**;** Estándar de segunda generación.

Segunda Generación avanzada 2.5G

La generación 2.5 se basa en los servicios ofrecidos por los sistemas para el usuario y para intentar incrementar la capacidad de transmisión.

HSCSD

High-Speed Circuit-Swítched Data

GPRS

General Packet Radio Services

EDGE

Enhanced Data Rates for Global Evolution

Tercera Generación 3G

Se da como la respuesta a la saturación del espectro radioeléctrico, con la finalidad de ofrecer nuevos servicios de telecomunicaciones, que necesiten mayores velocidades de transmisión, a los usuarios.

IMT-2000

Es una iniciativa de la UIT para proporcionar acceso a una variedad de servicios de telecomunicaciones de las redes fijas y a otros servicios que son específicos de los usuarios móviles.

FDD

Frequency División Dúplex

TDD

Time División Dúplex

UMTS

Sistema de telecomunicaciones móviles universales, tecnología desarrollada para cumplir con los requerimientos de la tercera generación.

3GPP

Proyectos de Asociación para Tercera Generación. Es una organización que desarrolla las especificaciones para los sistemas de 3G basados en la interfaz aérea UTRA de ETSI (UMTS).

3GPP2

3GPP2 es la otra organización mayor de estandarización. Proyectos de Asociación para Tercera Generación 2.

IPv4

Protocolo Internet versión 4.

IPv6

Protocolo Internet versión 6.

Cuarta Generación 4G

Redes que ofrecen accesos realmente multimedia, en las que podrá manejarse la transferencia de video en tiempo real, con velocidades equivalentes a las de una LAN básica (10 Mbps) y mayores.

NAT

Network Adreess Translation o Traducción de direcciones de red.

TCP

Protocolo de Control de Transporte.

UDP

Unidad de Datos de Protocolos.

DNS

Sistema de Nombre de Dominio.

IP Móvil

El protocolo IP Móvil fue creado para proporcionar movilidad a los nodos dentro de Internet. Desarrollado por IETF para aplicaciones generalmente inalámbricas.

Enlace Hogar o Agente Local

Enlace en el que un nodo especifico debe de estar ubicado y contar con el mismo prefijo-red que la dirección IP del nodo.

Enlace Remoto o Agente Externo

Cualquier enlace diferente al enlace hogar, cuyo prefijo-red difiere de la dirección IP del nodo.

Movilidad

Habilidad de un nodo de cambiar su punto de conexión de un enlace a otro, manteniendo todas las comunicaciones existentes y usando la misma dirección IP en su nuevo enlace.

Nodo móvil

Un nodo que tiene la característica de movilidad.

Aplicaciones móviles

Impresión remota, login remoto y transferencias de archivos son aplicaciones que no se deben interrumpir cuando se mueve de un enlace a otro.

Dirección hogar

Dirección IP permanente asignada al nodo móvil, no cambia cuando un nodo obtiene otro punto conexión, este nodo se comunica con todos usando dirección la hogar.

Enlace hogar

Prefijo-red dirección hogar = Prefijo-red enlace hogar.

Agente hogar

Ruteador que tiene al menos una interfaz con el enlace hogar del nodo móvil.

IEEE 802.11

Tecnología inalámbrica que permite velocidades de datos para aplicaciones multimedia en una red LAN.

IntServ

Servicio Integrados, mecanismos de comprobación para calidad de servicio.

Diffserv

Diferenciación de servicios, mecanismo de comprobación para calidad de servicio.

ANEXO B. GUIA DE COMANDOS MOBILE IP EN CISCO