



## CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

[www.cef.es](http://www.cef.es)

[info@cef.es](mailto:info@cef.es)

## Índice Tema 15

---

1. Comunicaciones emergentes: IP móvil. Características técnicas. Modos de operación.
2. IP móvil. Normativa reguladora. Ventajas e inconvenientes.
3. Comunicaciones emergentes: PLC. Características técnicas. Modos de operación.
4. PLC. Normativa reguladora. Ventajas e inconvenientes.

1

2

3

4

5



## CENTRO DE ESTUDIOS FINANCIEROS

VIRIATO, 52	28010 MADRID	914 44 49 20
PONZANO, 15	28010 MADRID	914 44 49 20
G. DE GRÀCIA, 171	08012 BARCELONA	934 15 09 88
ALBORAYA, 23	46010 VALENCIA	963 61 41 99

www.cef.es

info@cef.es

### TEMA 15

**Comunicaciones emergentes: IP móvil y PLC (Power Line Communications). Características técnicas. Modos de operación. Seguridad. Normativa reguladora. Ventajas e inconvenientes.**

#### **1. COMUNICACIONES EMERGENTES: IP MÓVIL. CARACTERÍSTICAS TÉCNICAS. MODOS DE OPERACIÓN.**

IP móvil es un protocolo estándar que se desarrolla en Internet dando efectividad a esa movilidad gracias a ciertas aplicaciones y protocolos de un nivel superior como los del tipo TCP.

Aunque podamos acceder a Internet desde numerosas fuentes por todo el mundo, normalmente no esperamos beneficiarnos de ello hasta que llegamos a un punto más familiar: la casa, la oficina, o en la escuela. Sin embargo, la creciente variedad de dispositivos inalámbricos que ofrecen conexión a través de IP, tales como PDAs, equipos de bolsillo, y teléfonos móviles, está comenzando a cambiar nuestra opinión de Internet.

Para entender el contraste entre las realidades actuales de las conexiones IP y las futuras posibilidades, consideremos la evolución que ha ocurrido en telefonía en lo que se refiere a movilidad los últimos 20 años. Una evolución análoga en el dominio de redes es pasar de la dependencia de puntos con accesos fijos a la flexibilidad producida por la movilidad. Acaba de comenzar.

Ordenadores y redes móviles no se deben confundir con los ordenadores y las redes portátiles que tenemos hoy en día. En una red móvil, las actividades no se interrumpen cuando el usuario cambia el punto de acceso del ordenador a Internet. En vez de eso, la reconexión necesaria ocurre automáticamente.

La informática móvil ofrece muchas ventajas. El acceso seguro a Internet en cualquier momento, en cualquier lugar, nos ayuda a liberarnos de los lazos que nos atan a nuestras mesas de trabajo. Pensemos cómo los teléfonos móviles nos han dado una nueva libertad para realizar nuestro trabajo. Llevamos todo el entorno informático al completo nos da la posibilidad no sólo de extender esa flexibilidad, sino de cambiar radicalmente la forma de trabajo existente. Internet móvil nos dará la posibilidad

de montar una estructura informática allí donde estemos. Esto es especialmente conveniente en una LAN inalámbrica de trabajo, donde los límites entre los puntos de acceso no están delimitados y son a menudo invisibles.

La evolución de las redes móviles se diferencia de la de la telefonía en algunos aspectos importantes. Los puntos finales de una conexión de teléfono son normalmente humanos; las aplicaciones informáticas son capaces de interaccionar entre las ellas sin intervención humana. Ejemplos obvios de esto son los dispositivos informáticos móviles en aeroplanos, naves, y automóviles.

El establecimiento de una red móvil puede llegar a depender también de los dispositivos de localización, tales como un sistema global de satélites, para trabajar con el acceso inalámbrico al Internet.

Existe otra diferencia, pasaron muchos años para que los teléfonos móviles llegaran a ser baratos y lo suficientemente ligeros para ser considerados útiles. Pero los dispositivos informáticos móviles e inalámbricos, tales como PDAs y organizadores de bolsillo han encontrado ya la aceptación del usuario, así que la aceptación de la informática móvil será popular más rápidamente.

Sin embargo, todavía hay algunos obstáculos técnicos que deben ser superados antes de que las redes móviles se extiendan. El más fundamental es la manera en que el protocolo de Internet, el que conecta las redes de Internet actualmente, encamina los paquetes a sus destinos según direcciones IP. Estas direcciones se asocian a una localización fija de la red mientras que un número de teléfono fijo se asocia a un enganche en la pared. Cuando el destino del paquete es un nodo móvil, significa que cada nuevo punto de acceso está asociado a un nuevo número de red y, por lo tanto, a una nueva dirección IP, haciendo imposible una movilidad efectiva.

IP móvil (RFC 3220) es un estándar propuesto por un grupo en la Internet Engineering Task Force, diseñado para solucionar este problema permitiendo que el nodo móvil utilice dos direcciones de IP: una fija casera y una que cambia en cada nuevo punto de acceso. Más información:

<http://computer.org/internet/>

También añadir que el IP móvil cambiará con la versión 6. El producto supone un esfuerzo importante dentro del IETF, dirigir una actualización de la versión actual de IP. Aunque la IPv6 soportará movilidad a un mayor grado que IPv4, seguirá teniendo la necesidad de una IP móvil para dar movilidad y transparencia a los usos y protocolos de más alto nivel tales como TCP.

Hay muchos intereses en la informática móvil y, al parecer, en el IP móvil como manera de hacer uso de ella. Una búsqueda rápida en la Web buscando artículos relacionados con IP móviles nos dio alrededor de 60.000 resultados, un resultado impresionante teniendo en cuenta la carencia notoria de selectividad para tales procedimientos. Los IP móviles forman la base directamente o indirectamente de muchos esfuerzos y productos de la investigación de hoy en día. El Cellular Digital Packet Data (CDPD), por ejemplo, ha creado una infraestructura ampliamente desplegada de las comunicaciones basada en una especificación anterior del bosquejo del protocolo. Además, la mayoría de los proveedores importantes han desarrollado productos para IP móviles.

La perspectiva para IP móviles en el complejo mercado del Internet no está muy claro y sigue habiendo algunos problemas técnicos como la seguridad. Sin embargo, una vez que las soluciones de la

seguridad sean sólidas, los usuarios pueden finalmente comenzar a gozar de la facilidad de uso que es la promesa del IP móvil.

Cada nodo móvil siempre es identificado por su home-address, independientemente de su punto actual de acceso a Internet. Mientras está situado fuera de su casa, un nodo móvil también se asocia a una «care-address», la dirección que proporciona información sobre su punto actual de acceso a Internet. El protocolo asegura el registro de la care-address con un agente de casa (Home-Agent), que envía datagramas destinados al nodo móvil por un túnel a la «care-address». Después de llegar al final del túnel, cada datagrama es entonces entregado al nodo móvil.

La versión IPv4 asume que la dirección IP de un nodo identifica unívocamente el punto de acceso a Internet. Por lo tanto, un nodo debe localizarse por su IP donde recibe los datagramas destinados a dicha dirección; si no, los datagramas destinados al nodo no podrían ser entregados. Para que un nodo pueda cambiar su punto de acceso sin perder su capacidad de comunicación, uno de los dos mecanismos siguientes debe ser empleado:

- a) El nodo debe cambiar su dirección IP siempre que cambie su punto de acceso.
- b) Las rutas específicas de host deben propagarse con las reglas de enrutamiento de Internet.

Ambas alternativas son a menudo inaceptables. La primera hace imposible que un nodo sea capaz de mantener las conexiones de transporte y de las capas superiores cuando el nodo cambia de IP. La segunda tiene problemas de escala severos, considerando sobre todo el crecimiento explosivo en las ventas de ordenadores (móviles).

Exigencias de Protocolo: Un nodo móvil debe ser capaz de comunicarse con otros nodos después de cambiar su punto de acceso a Internet, aún sin cambiar su dirección IP.

- Un nodo móvil debe ser capaz de comunicarse con otros nodos que no tienen estas funciones de movilidad.
- El nodo móvil debe estar autenticado para protegerlo contra ataques remotos de cambio de dirección.

IP móvil introduce las nuevas entidades siguientes:

- Nodo Móvil:

Un host o un router que cambia su punto de acceso de una red a otra. Un nodo móvil puede cambiar su posición sin cambiar su dirección IP; puede seguir comunicándose con otros nodos de Internet en cualquier posición con su dirección de IP (permanente), asumiendo que la conectividad del punto de acceso está disponible.

- Agente de casa (Home Agent).

Un router en una red de nodos móviles que crea túneles para la entrega de datagramas (dentro de un túnel) al nodo móvil cuando está lejos la casa, y mantiene la información de la posición actual del nodo móvil.

- Agente Extranjero (Foreign Agent).

Un router situado en la red de nodos móviles visitada que provee servicios de routing al nodo móvil mientras éste es registrado. El agente extranjero elimina el túnel y entrega los datagramas al nodo móvil encapsulado en un túnel por el agente de casa de dicho nodo móvil.

- Descripción de Protocolo: Los siguientes servicios de apoyo se definen para IP Móvil:
- Descubrimiento de Agente (Agent Discovery).

Agentes de casa y agentes extranjeros pueden anunciar su disponibilidad para cada enlace al cual ellos proporcionan el servicio. A un nodo recién llegado móvil pueden enviar una solicitud al enlace para aprender si está presente cualquier agente.

- Registro.

Cuando el nodo móvil está lejos de la casa, registra su «care\_of\_address» con su agente de casa. Dependiendo de su método de acceso, el nodo móvil se registrará directamente con su agente de casa, o por medio de un agente extranjero que reenvía el registro al agente de casa.

- Esquema del funcionamiento de un Protocolo móvil IP:

- Agentes de movilidad (p. ej., agentes extranjeros y agentes de casa) anuncian su presencia vía mensajes de Anuncio de Agente. Un nodo móvil opcionalmente puede solicitar un Mensaje de anuncio de Agente a alguno de los agentes de movilidad existentes en la zona, mediante un mensaje de Solicitud de Agente.
- Un nodo móvil recibe este anuncio de Agente y determina si el mismo está en su red de casa o en una red extranjera.
- Cuando el nodo móvil detecta que está en su red de casa, funciona sin los servicios de movilidad. Si retorna a su red de casa después de haber registrado en otra parte, el nodo móvil borra su registro con su agente de casa, mediante el intercambio de mensajes de Petición de Registro y Respuesta de Registro.
- Cuando un nodo móvil detecta que se ha movido a una red extranjera obtiene una «care\_of\_address» de la red extranjera. La «care\_of\_address» puede ser provista o por un anuncio de un agente extranjero, o por algún mecanismo de asignación externo como DHCP.
- El nodo móvil que funciona lejos de la casa registra entonces su nueva «care\_of\_address» con su agente de casa por intercambio de mensajes de Petición de Registro y Respuesta de Registro, posiblemente vía un agente extranjero.
- Los datagramas enviados a la dirección de casa del nodo móvil son interceptados y encapsulados por el agente de casa a la «care\_of\_address», recibida en el punto final del túnel (bien un agente extranjero o en el nodo móvil mismo), y finalmente entregado al nodo móvil.
- En la dirección inversa, los datagramas enviados por el nodo móvil son generalmente entregados a su destino utilizando los mecanismos estándar de routing IP encaminamiento de mecanismos, que no tienen que pasar necesariamente por la casa agente.

Cuando se encuentra lejos de casa, IP Móvil usa el protocolo tunneling para ocultar la dirección de casa del nodo móvil a los routers que intervienen entre su casa y su posición actual. El túnel se termina en la «care\_of\_address» del nodo móvil. La «care\_of\_address» debe ser una dirección a la cual los datagramas pueden ser entregados vía IP convencional. En la «care\_of\_address», el datagrama original es desencapsulado (del túnel) y entregado al nodo móvil.

IP móvil proporciona dos modos alternativos para la adquisición de la «care\_of\_address»:

- La «care\_of\_address» de agente extranjero es una «care\_of\_address» proporcionada por un agente extranjero por medio de mensajes de Anuncio de Agente. En este caso, la «care\_of\_address» es una dirección IP del agente extranjero y el agente extranjero es el punto final del túnel. Para recibir datagramas encapsulados en un túnel, los desencapsula y entrega el datagrama más interno al nodo móvil. Este modo de adquisición es el preferido porque permite muchos nodos móviles para compartir la «care\_of\_address» y aprovecha el ya limitado espacio de direcciones de IPv4.
- Una «co-located-care\_of\_address» es una «care\_of\_address» adquirida por el nodo móvil como IP local a través de algunos medios externos, que el nodo móvil asocia entonces con uno de sus interfaces de red. La dirección puede ser dinámicamente adquirida como una dirección temporal por el nodo móvil, como por ejemplo DHCP, o puede ser poseída por el nodo móvil como una dirección a largo plazo para su empleo sólo por unos visitantes de una red extranjera.

El utilizar una «co-located-care\_of\_address» tiene la ventaja de que permite a un nodo móvil funcionar sin un agente extranjero.

Una IP encamina los paquetes desde el punto final de la fuente a un destino permitiendo que los routers remitan los paquetes de la red de entrada a la red de salida según las tablas de encaminamiento. Éstas mantienen como norma general la información del siguiente salto (interfaz de salida) para cada dirección IP de destino, según el número de las redes con las cuales esa dirección IP está conectada. El número de red es derivado de la dirección IP, enmascarando algunos de los bits de peso inferior. Así, la dirección IP lleva normalmente la información consigo misma que especifica el punto de acceso del nodo de la IP.

Para mantener las conexiones existentes en la capa de transporte mientras el nodo móvil se mueve de un lugar a otro, se debe guardar la misma dirección IP. En el TCP (la mayoría abrumadora de conexiones a Internet), las conexiones son indexadas en un conjunto de cuatro números que contienen las direcciones IP y los puertos de acceso de ambos puntos finales de la conexión. Cambiar cualquiera de estos cuatro números hará que la conexión se interrumpa y se pierda. Por otra parte, la entrega correcta de paquetes al punto actual de acceso del nodo móvil depende del número de red contenido dentro de la dirección IP del nodo móvil, que cambia en cada punto de acceso. Cambiar la ruta requiere una nueva dirección IP asociada al nuevo punto de acceso.

La IP móvil ha sido diseñada para solucionar este problema permitiendo que el nodo móvil utilice dos direcciones IP. En la IP móvil, la «home-address» es estática y se utiliza, por ejemplo, para identificar conexiones TCP. La dirección «care-of-address» cambia en cada nuevo punto de acceso y puede ser como la dirección topológica del nodo móvil; indica el número de red e identifica así el punto de acceso del nodo móvil con respecto a la topología de la red.

La «home-address» hace que el nodo móvil pueda continuamente recibir datos sobre su red casera, donde el IP móvil requiere la existencia de un nodo de red conocido como el agente casero «home-

agent». Siempre que el nodo móvil no se una a su red casera «home-address» (y por lo tanto se une a lo que se llama una red extranjera «foreign-network»), el agente casero consigue todos los paquetes destinados para el nodo móvil y consigue entregarlos al punto actual de acceso del nodo móvil.

Siempre que el nodo móvil se mueva, registra su nueva dirección con su agente casero. Para conseguir una conexión entre un nodo móvil y su red casera, el agente casero entrega el paquete de la red casera a la dirección «care-of-address». La entrega posterior requiere que el paquete esté modificado de modo que la dirección «care-of-address» aparezca como la IP de destino. Esta modificación se puede entender como una transformación del paquete o, más específicamente, cambio de dirección. Cuando el paquete llega a la dirección «home-address», se aplica la transformación inversa de modo que el paquete tenga de nuevo la dirección casera «home-address» del nodo móvil como la dirección IP destino. Cuando el paquete llega al nodo móvil, enfocado a la dirección casera «home-address», será procesado por TCP o cualquier protocolo de un nivel más alto, que la recibe de la capa de procesos de la IP del nodo móvil (es decir, capa 3).

En IP móviles, el agente casero «home-agent» redirige los paquetes de la red casera «home-network» a la dirección «care-of-address», construyendo una nueva cabecera IP que contiene la dirección del nodo móvil como la dirección IP de destino. Esta nueva IP líder blindada o encapsula el paquete original, haciendo que la dirección casera del nodo móvil no tenga ningún efecto en la ruta del paquete encapsulado hasta que llega a la dirección. Tal encapsulación, también llamada tunneling, pasa por alto los efectos usuales en routing IP.

La IP móvil está montada con la cooperación de tres mecanismos diferentes:

- Descubrir la dirección «care-of-address».
- Registro de la dirección «care-of-address».
- Tunneling de la dirección.

Descubrir la dirección «care-of-address»: el proceso de descubrimiento de la IP se ha construido encima de un protocolo estándar existente, anuncio de ruta, especificado en la norma RFC 1256. El descubrimiento de la IP móvil no modifica los campos originales de los anuncios existentes en el «router» sino que los extiende simplemente a las funciones de movilidad asociadas. Así, un anuncio del «router» puede llevar la información sobre los «routers» por defecto, como antes y además llevar información adicional sobre una o más direcciones «care-of-address». Cuando los anuncios del «router» se extienden para contener la dirección «care-of-address», se conocen como anuncios del agente «agent-advertisement». Los agentes caseros y los agentes extranjeros difunden normalmente los anuncios del agente en intervalos regulares (p. ej., una vez al segundo o una vez cada pocos segundos). Si un nodo móvil necesita conseguir una dirección «care-of-address» y no desea esperar el anuncio periódico, el nodo móvil puede difundir o lanzar una solicitud que sea contestada por cualquier agente extranjero o el agente casero que la reciba.

Una IP móvil utiliza dos direcciones IP: una casera fija «home-address» y otra «care-of-address» que cambia en cada nuevo punto de acceso.

Los agentes caseros usan anuncios agentes para darse a conocer, incluso si no ofrecen ninguna dirección «care-of-address». Sin embargo, no es posible asociar preferencias a las diferentes direcciones «care-of-address» en el anuncio de la ruta, como en el caso de los antiguos routers.



El grupo de funcionamiento IETF se preocupaba de que los valores dinámicos preferidos desestabilizasen el funcionamiento de la IP móvil. Porque nadie podría defender las asignaciones estáticas preferentes, a excepción de los agentes de «backup» de la movilidad, que no ayudan a distribuir la carga del router, el grupo decidió eventualmente no utilizar las asignaciones preferentes con la lista de direcciones.

Así, un anuncio del agente «agent-advertisement» realiza las funciones siguientes:

- Permite la detección de los agentes de la movilidad.
- Enumera una o más direcciones «care-of-address».
- Informa al nodo móvil sobre las características especiales proporcionadas por los agentes extranjeros, por ejemplo, las técnicas alternativas de encapsulación.
- Deja que los nodos móviles determinen el número de red y el estado de su conexión.
- Deja al nodo móvil averiguar si el agente es un agente casero, agente extranjero, o ambos, y por lo tanto si está en su red casera o en una red extranjera.

Los nodos móviles utilizan el procedimiento de solicitudes al router según lo definido en la norma RFC 1256 para detectar cualquier cambio en el sistema de agentes de la movilidad disponibles en el punto de acceso actual (en la terminología de IP móvil esto se llama solicitud del agente «agent-solicitation»). Si los anuncios no son detectados por un agente extranjero que había ofrecido previamente una dirección «care-of-address» al nodo móvil, el nodo móvil debe suponer que el agente extranjero no está dentro de la gama del interfaz de la red del nodo móvil. En esta situación, el nodo móvil debe comenzar a buscar una nueva dirección «care-of-address», o utilizar posiblemente una dirección «care-of-address» conocida por los anuncios. El nodo móvil puede decidir esperar otro anuncio si no ha recibido ningún anuncio recientemente de dirección o puede enviar una solicitud al agente.

Registro de la dirección «care-of-address»: una vez que el nodo móvil tiene una dirección, su agente casero debe investigarla. El proceso comienza cuando el nodo móvil, posiblemente con la ayuda de un agente extranjero, envía una petición de registro con la información de la dirección «care-of-address». Cuando el agente casero recibe esta petición, (como normal general) agrega la información necesaria a su tabla de «routing», aprueba la petición y envía la contestación del registro de vuelta al nodo móvil. Aunque el agente casero no es requerido por el protocolo móvil de la IP para manejar peticiones del registro poniendo al día entradas en su tabla de «routing», hacerlo así ofrece una buena estrategia de la puesta en práctica.

Autenticación: Las peticiones del registro contienen los parámetros y las banderas que caracterizan el túnel a través del cual el agente casero entregará los paquetes a la dirección. Los túneles se pueden construir de varias maneras, descritas brevemente en la siguiente sección. Cuando un agente casero acepta la petición, comienza a asociar la dirección casera del nodo móvil a la dirección, y mantiene esta asociación hasta que termina la vida del registro. El trío que contiene la dirección casera «home-address», la dirección «care-of-address», y la vida del registro se llama un «binding» del nodo móvil. Una petición del registro se puede considerar un «binding-update» enviada por el nodo móvil.

Una «binding-update» es un ejemplo de redirección remota, porque se envía remotamente al agente casero para afectar la tabla de rutas del agente casero. Esta vista del registro hace necesaria una autenticación más clara. El agente casero debe estar seguro de que el registro fue originado por el

nodo móvil y no por otro falso nodo que fingía ser el nodo móvil. Un nodo malévolo podría hacer al agente casero alterar su tabla de rutas con información errónea de la dirección, y el nodo móvil sería inalcanzable a todas las comunicaciones entrantes del Internet.

La necesidad de autenticar la información del registro ha desempeñado un papel importante en la determinación de los parámetros de diseño aceptables para la IP móvil. Cada nodo móvil y agente casero deben compartir una asociación de la seguridad y poder utilizar el Message Digest 5, norma RFC 1321, a 128-bits para crear firmas digitales fijas para las peticiones de registro. La firma es digitalizada ejecutando el algoritmo codificado con el MD5 de todos los datos de registro y de las extensiones que preceden la firma.

Para asegurar la petición del registro, cada petición debe contener datos únicos, de modo que dos diversos registros en términos prácticos nunca tengan el mismo código MD5. Si no, el protocolo sería susceptible a ataques, en los cuales un falso nodo podría registrar los registros válidos, para más adelante atacar con eficacia interrumpiendo la capacidad del agente casero de hacer un túnel a la corriente de la dirección del nodo móvil en ese último momento. Para asegurarnos de que esto no sucede, la IP móvil incluye dentro del mensaje del registro un campo de identificación especial que cambia con cada nuevo registro. La semántica exacta del campo de identificación depende de varios detalles, que se describen en mayor longitud en el protocolo de especificación. Brevemente, existen dos maneras principales de hacer el campo de identificación único.

Uno debe utilizar una marca de tiempo «timestamp»; entonces cada nuevo registro tendrá una marca de tiempo actualizada y se diferenciará así de registros anteriores. La otra es hacer que la identificación sea un número aleatorio, con suficientes posibilidades de que sea altamente improbable que dos valores independientemente elegidos para el campo de identificación sean iguales. Cuando se utiliza el azar, la IP móvil define un método que proteja tanto la petición del registro como la contestación al ataque, y solicita 32 posibilidades en el campo de identificación. Si el nodo móvil y el agente casero llegan demasiado lejos en la sincronización para el uso de marcas de tiempo, o si pierden la pista de los números al azar previstos, el agente casero rechazará la petición del registro e incluirá la información para permitir la resincronización dentro de la contestación.

Usar números al azar en vez de marcas de tiempo evita los problemas que vienen de los ataques en el protocolo del NTP que pueden hacer que el nodo móvil pierda la sincronización de tiempo con el agente casero o publicar las peticiones del registro identificados para que en un futuro puedan ser utilizados por un falso nodo.

El agente extranjero también almacena el campo de identificación para los registros pendientes, incluyendo la dirección casera del nodo móvil, la dirección de la capa del acceso de los medios del nodo móvil (MAC), el número de acceso de la fuente para la petición del registro del nodo móvil, la vida del registro propuesto por el nodo móvil y la dirección del agente casero. El agente extranjero puede limitar la vida del registro a un valor configurable que le sitúe en los anuncios del agente. El agente casero puede reducir la vida del registro, que incluye como parte de la contestación del registro, pero nunca puede aumentarla.

Agente casero automático descubridor: Cuando el nodo móvil no puede entrar en contacto con su agente casero, el IP móvil tiene un mecanismo que deja que el nodo móvil trate de registrarse con otro agente casero desconocido en su red casera. Este método de agente casero automático descubridor trabaja usando una dirección IP de la difusión en vez de la IP del agente casero como objetivo para la petición del registro. Cuando el paquete de la difusión llega a la red casera, otros agentes caseros en la red enviarán una impugnación al nodo móvil; sin embargo, su aviso de impugnación contendrá su di-

rección para que el nodo móvil utilice un mensaje recientemente obtenido del registro. Observe que la difusión no es una difusión que abarque todo Internet, solamente una difusión que alcance solamente nodos de la IP en la red casera.

**Tunneling de la dirección «care-of address»:** Las operaciones al hacer un túnel en la IP móvil son: El mecanismo de la liberación que debe ser soportada por todos los agentes de la movilidad usando la IP móvil es IP-dentro-IP. Usando IP-dentro-IP, el agente casero, la fuente del túnel, inserta una nueva IP cabecera, o cabecera del túnel, delante de la IP cabecera de cualquier datagrama tratado a la dirección casera del nodo móvil. La nueva cabecera de túnel utiliza el nodo móvil de la dirección como dirección IP de destino, o el destino del túnel. La dirección IP de la fuente del túnel es el agente casero, y la cabecera del túnel utiliza el 4 como el número más alto del protocolo, indicando que la siguiente cabecera del protocolo es otra vez una cabecera IP. En IP-dentro-IP se preserva la cabecera entera de la IP original como la primera parte de la carga útil de la cabecera del túnel. Por lo tanto, para recuperar el paquete original, el agente extranjero tiene simplemente que eliminar la cabecera del túnel y entregar el resto al nodo móvil.

¿Cómo cambiará la IP móvil cuando se adopte la versión 6 de la IP?: IPv6 incluye muchas características para fortalecer la movilidad, cosa que faltaba en la versión 4 (versión actual), incluyendo autoconfiguración de direcciones sin estado y descubrimientos de vecinos. IPv6 también procura simplificar drásticamente el proceso de reenumerar, que puede ser crítico para un futuro enrutamiento de Internet. Ante el número creciente de ordenadores con acceso a Internet, una movilidad eficiente ayudará decisivamente al futuro funcionamiento de Internet. Esto, junto con la importancia creciente de Internet y de las Web, indica la necesidad de prestar atención al soporte a la movilidad.

Sesiones de pruebas de interoperatividad han indicado que la especificación de la IP móvil es so-  
nido realizable y de interés a través de la comunidad de Internet.

El soporte a la movilidad en IPv6, según lo propuesto por el grupo de funcionamiento de la IP móvil, sigue el diseño de la IPv4 móvil. Conserva las ideas de una red casera, de un agente casero, y del uso de la liberación al entregar los paquetes de la red casera al punto actual de acceso al nodo móvil. Mientras que el descubrimiento de la dirección todavía es requerido, un nodo móvil puede configurar su dirección usando la autoconfiguración de direcciones sin estado y descubrimiento de vecinos. Así, los agentes extranjeros no requieren soportar movilidad en IPv6. Hacer un túnel IPv6-dentro-IPv6 está también especificado.

La movilidad de la IPv6 toma prestadas de la optimización de la ruta ideas especificadas para la IPv4, en particular la de entregar actualizaciones obligatorias «binding-updates» directamente a los nodos correspondientes. Cuando se sabe la dirección del nodo móvil, un nodo correspondiente puede entregar los paquetes directamente a la dirección casera del nodo móvil sin ninguna ayuda del agente casero. La optimización de la ruta tiende a mejorar drásticamente el funcionamiento de los nodos del móvil IPv6. Es realista requerir esta funcionalidad adicional de todos los nodos IPv6 por dos razones. Primero, en un nivel práctico, los documentos de los estándares IPv6 todavía están en una primera etapa de estandarización, así que es posible imponer requisitos adicionales en los nodos IPv6. En segundo lugar, el proceso de actualizaciones obligatorias se puede llevar a cabo como una modificación bastante simple al uso del caché destino de la IPv6

Problemas que surgen con una IP móvil:

El mayor problema que nos surge con una IP móvil es el de la seguridad, pero existen otros obstáculos técnicos. También se sigue refinando y ampliando el protocolo dentro de las comunidades académicas y comerciales y dentro del IETF.

Deficiencias del routing: la especificación de la IP tiene el efecto de introducir un túnel en la trayectoria de la ruta seguida por paquetes enviados por el nodo correspondiente al nodo móvil. Los paquetes del nodo móvil, por otra parte, pueden ir directamente al nodo correspondiente sin hacer el túnel requerido. Esta asimetría es capturada por «term triangle routing», donde un solo lado del triángulo va del nodo móvil al nodo correspondiente, y el agente casero forma el tercer vértice que controla la trayectoria tomada por datos del nodo correspondiente al nodo móvil. La ruta en triángulo «term triangle routing» se alivia por el uso de técnicas en la optimización de la ruta, pero eso requiere cambios en los nodos correspondientes, que se tomarán un largo tiempo para desplegar para la IPv4. Se espera que la ruta en triángulo «term triangle routing» no sea un factor para la movilidad de la IPv6.

Temas de seguridad: mucha atención se centra en lograr que la IP móvil coexista con las características de seguridad que se usan en Internet. Los cortafuegos, en particular, causan dificultades para la IP móvil porque bloquean toda clase de paquetes entrantes que no resuelven los criterios especificados. Los cortafuegos de empresa se configuran como norma general para bloquear los paquetes entrantes vía Internet, que parecen emanar de ordenadores internos. Aunque esto permite el manejo de los nodos internos de Internet sin gran atención a la seguridad, presenta dificultades para los nodos móviles que desean comunicarse con otros nodos dentro de sus redes caseras de la empresa. Tales comunicaciones, partiendo del nodo móvil, llevan la dirección casera del nodo móvil, y serían bloqueadas así por el cortafuego.

Según lo propuesto por el grupo de funcionamiento de la IP móvil, el soporte de movilidad para la IPv6 sigue el diseño para la IPv4 móvil, usando la encapsulación para entregar los paquetes de la red casera al punto de acceso móvil.

Filtración del ingreso. Las complicaciones también se presentan en las operaciones con filtro de ingreso. Muchos routers desechan los paquetes que vienen de dentro de la empresa si los paquetes no contienen una dirección IP de la fuente configurada por una de las redes internas de la empresa.

Ya que los nodos móviles utilizarían su dirección casera como la dirección IP de la fuente de los paquetes que transmiten, esto presenta sus dificultades. Las soluciones a este problema en la IPv4 móvil implican normalmente hacer un túnel de los paquetes salientes de la dirección, pero entonces la dificultad es cómo encontrar un objetivo adecuado para el paquete tunelizado del nodo móvil. El único convenio universal posible es el agente casero, pero ese objetivo introduce otra importante anomalía de la ruta para las comunicaciones entre el nodo móvil y el resto de Internet. La IPv6 móvil también ofrece una solución en la opción de la opción de destino de la dirección casera.

#### Seguridad:

Uno de las diferencias más grandes entre IPv6 e IPv4 es que se espera que todos los nodos IPv6 implementen autenticación fuerte y características de encriptación para mejorar la seguridad en Internet. Esto es una simplificación importante para la movilidad IPv6, puesto que todos los procedimientos de la autenticación se pueden asumir que ya existen para cuando sean necesarios y no tienen que ser especificados en el protocolo móvil IPv6. Incluso con las características de seguridad en IPv6, sin embargo, el grupo de funcionamiento para la movilidad IPv6 especifica el uso de los procedimientos de la identificación lo menos posible. Las razones de esto son dos. Primero, una buena autenticación incrementa el coste del funcionamiento, así que se debe requerir solamente de vez en cuando. En segundo lugar, las preguntas sobre la disponibilidad de la gestión de Internet están lejos de ser resueltas ahora mismo.

En contraste con la optimización de la ruta en IPv4, en los nodos correspondientes a la IPv6 no se hace túnel de los paquetes a los nodos móviles. En su lugar, se utilizan las cabeceras de la ruta de la

IPv6, que ejecutan una variación de la ruta de la fuente de la IPv4. Un número de recientes ofertas para la movilidad de soporte en la IPv4 especificaron un uso similar de las opciones de la ruta de la fuente, pero dos problemas principales imposibilitaron su uso:

- Las opciones de la ruta de la fuente de la IPv4 requieren que el receptor de paquetes con su fuente en ruta siga la trayectoria invertida al remitente a lo largo de los nodos intermedios indicados. Esto significa que los falsos nodos que usaban las rutas de la fuente de posiciones remotas dentro de Internet podrían hacerse pasar por otros nodos, un problema exacerbado por la carencia de los protocolos de la identificación.
- Las rutas existentes exhiben un funcionamiento no estable al manejar las rutas de la fuente. Por lo tanto, los resultados de desplegar otros protocolos que utilizan las rutas de la fuente no han sido favorables.

Sin embargo, las objeciones al uso de las rutas de la fuente no se aplican a la IPv6, porque la cualidad más cuidadosa de la IPv6 elimina la necesidad de enrutar la fuente de ida y vuelta y permite que las rutas ignoren las opciones que no necesitan su atención. Por lo tanto, los nodos correspondientes pueden utilizar cabeceras de ruta sin penalización. Esto permite que el nodo móvil se determine fácilmente cuando el nodo correspondiente no tiene la apropiada dirección. Los paquetes entregados por liberación, en vez de por las rutas de la fuente en una cabecera de la ruta se deben haber enviado por los nodos correspondientes que necesitan recibir actualizaciones «binding-updates» obligatorias del nodo móvil.

Otras características apoyadas por la movilidad de IPv6 incluyen:

- Coexistencia con el filtro de ingreso a Internet.
- Suaves handoffs, que en la IPv4 móvil se especifica para los agentes extranjeros como parte de la optimización de la ruta.
- Renumerar redes caseras.
- Agente casero automático descubridor.

## 2. NORMATIVA REGULADORA. VENTAJAS E INCONVENIENTES.

La normativa viene regulada en las siguientes direcciones:

<http://www.ietf.org/rfc/rfc3220.txt>

Este documento especifica las mejoras de protocolo que permiten un «routing» transparente a los datagramas IP que envían los nodos móviles en Internet.

<http://www.ietf.org/rfc/rfc1256.txt>

Este documento especifica una extensión del protocolo -Internet Control Message (ICMP)- que permite a los hosts conectados a redes «multicast» o «broadcast» descubrir las direcciones IP de los routers vecinos.

### Percepciones del usuario de validez:

El diseño del IP móvil se funda en la premisa de que las conexiones basadas en el TCP deben sobrevivir los cambios de la celda. Sin embargo, la opinión no es unánime en la necesidad de esta característica. Mucha gente cree que las comunicaciones del ordenador al portátil son suficientemente potentes y que no hay necesidad de aumentar la validez de las conexiones que apoyan las comunicaciones. La analogía se realiza en el método de traer las páginas Web seleccionando la URL apropiada. Si una transferencia falla, se debe intentarlo otra vez. Esto es equivalente a hacer que el usuario responsable del protocolo de retransmisión y para ser aceptado dependa de la opinión de que los ordenadores e Internet no pueden hacer las cosas correctamente a la primera.

### Lento crecimiento del mercado inalámbrico de las LAN:

El IP móvil se ha dirigido como solución para el mantenimiento y las comunicaciones de las redes inalámbricas LAN, pero el mercado inalámbrico de las LAN se ha desarrollado lentamente. Es difícil saber las razones de este desarrollo lento, pero con la ratificación reciente del protocolo IEEE 802.11 MAC, las LAN inalámbricas pueden llegar a ser más populares. Por otra parte, la anchura de banda para los dispositivos inalámbricos ha ido mejorando constantemente, de modo que los dispositivos de radio e infrarrojos en el mercado ofrecen hoy tasas de datos de multimegabytes por segundo. Un acceso inalámbrico más rápido sobre capas MAC estandarizadas podía ser un catalizador importante para el crecimiento de este mercado.

### Competición de otros protocolos:

El IP móvil bien puede plantar cara en una competición de protocolos alternativos tunelados tales como PPTP y L2TP. Estos otros protocolos, basados en el PPP, ofrecen menos portabilidad en los ordenadores portátiles. Aunque la operación portátil no será en última instancia una solución a largo plazo, puede parecer absolutamente atractiva a corto plazo en ausencia de la implementación completa de la IP móvil. Si estos métodos alternativos se hacen ampliamente disponibles, no queda muy claro si el uso del IP móvil es depreciado o por el contrario más deseable inmediatamente, pues la gente experimenta la conveniencia de la informática móvil. En el futuro, será también posible que la IP móvil pueda especificar el uso de tales protocolos alternativos al hacer un túnel para capitalizar en su despliegue en las plataformas que no soportan la liberación IP-con-IP.

La IP móvil se ha estudiado en un número de proyectos inalámbricos de comunicación e investigación. En la universidad de California en Berkeley, la IP móvil se está utilizando para construir enlaces entre medios diferentes (p. ej., infrarrojos, LANs inalámbricas, móviles de área amplia, y satélites), dependiendo de las tarifas de error y de la disponibilidad de la anchura de banda. Otros factores tales como coste y servicio de predicción pueden también ser considerados. El proyecto del Monarch CMU ha sido el foco de la investigación en redes inalámbricas del campus, IP móvil, IPv6 móvil, y redes *ad hoc*. Otros esfuerzos académicos han estado dándose en la universidad de Portland, la de Alabama, la de Tejas, la UCLA, la de Macquarie, la SUNY Binghampton, la de Singapur, el instituto de la tecnología real sueco, y muchos otros.

Los actuales borradores de proyectos del IETF que emplean IP móviles incluyen el protocolo de establecimiento del túnel y el registro local de IP móviles con agentes extranjeros jerárquicos. Las últimas aplicaciones usan la capacidad de anunciar varios agentes extranjeros para arreglar jerarquías de los agentes de la movilidad. Esto puede ayudar a cortar el número de los registros que deben transitar Internet entre las redes caseras y extranjeras, DHCP para redes móviles con TCP/IP,

para investigar la validez del protocolo de configuración dinámica del anfitrión para proporcionar direcciones a nodos. La opción de configuración de la IPv4 para PPP IPCP es una nueva extensión a PPP que permitirá a usuarios de marcado manual emplear más eficientemente sus direcciones dinámicas de IP como direcciones.

#### **CONCLUSIÓN:**

El proceso de la estandarización del IETF requiere que los grupos de funcionamiento demuestren rigurosamente la interoperabilidad entre varias prácticas independientes antes de que el protocolo pueda avanzar. El software del ftp ha recibido dos sesiones de prueba de la interoperabilidad, y muchos proveedores se han aprovechado de la oportunidad. Los resultados de la prueba han dado confianza añadida y la especificación móvil del IP es buena, realizable, y de interés diverso a través de la comunidad de Internet. Solamente algunas revisiones de menor importancia se han necesitado para asegurar que la especificación se puede interpretar únicamente en una dirección por los ingenieros y los programadores del protocolo de red que deben ponerlo en ejecución.

Es posible que la implantación de la IP móvil seguirá a la de la IPv6, o que los requisitos para soportar movilidad en los nodos IPv6 den ímpetu adicional al despliegue de ambos, IPv6 y una red móvil.

### **3. COMUNICACIONES EMERGENTES: PLC. CARACTERÍSTICAS TÉCNICAS. MODOS DE OPERACIÓN.**

PLC son las siglas de Power Line Communication, la tecnología que permite la transmisión de voz y datos a través de la red eléctrica existente. Ha sido una tecnología usada desde hace tiempo para comunicaciones que utilizaban pequeños anchos de banda. Hoy en día la tecnología PLC nos permite transmitir datos a alta velocidad.

La idea de utilizar el cable eléctrico para transmisión de información no es nueva.

El uso de PLC en sus orígenes se limitaba al control de líneas eléctricas y a la transmisión a baja velocidad de las lecturas de los contadores. Más adelante, las propias empresas eléctricas empezaron a utilizar sus propias redes eléctricas para la transmisión de datos de modo interno.

Durante finales de los noventa los avances tecnológicos realizados permiten alcanzar velocidades de transmisión de Megabits.

#### **Ventajas:**

- Velocidades de transmisión de hasta 45 Mbps.
- Proceso de instalación sencillo y rápido para el cliente final.
- Enchufe eléctrico (toma única de alimentación, voz y datos).
- Sin necesidad de obras ni cableado adicional.
- Equipo de conexión (modem PLC).

- Transmisión simultánea de voz y datos.
- Conexión de datos permanente (activa las 24 horas del día).
- Permite seguir prestando el suministro eléctrico sin ningún problema.
- La principal: se emplea la infraestructura existente.
- Los servicios ofertados son competitivos en calidad y en precio.
- Alternativa válida a las conexiones ADSL.
- Permite un despliegue masivo de la tecnología, ya que la red ya está implantada.

PLC permite actualmente la transmisión de datos a velocidades de hasta 135 Mbps, lo que posibilita la transformación de la red eléctrica en una auténtica red de banda ancha.

PLC utiliza las redes de distribución de electricidad para la transmisión de datos. La energía eléctrica llega a los usuarios en forma de corriente alterna de baja frecuencia (50 ó 60 Hz).

Para PLC se utiliza alta frecuencia (1,6 – 30 MHz) para transportar datos, voz y vídeo.

Una red PLC se descompone en los siguientes tramos:

- Tramo de Media Tensión (entre 15 y 50 Kilovoltios) que abarca desde la central generadora de energía hasta el primer transformador elevador.
- Tramo de Transporte o de Alta Tensión (entre 220 y 400 Kilovoltios) que conduce la energía hasta la subestación de transporte.
- Tramo de Media Tensión (de 66 a 132 Kilovoltios) entre la subestación de transporte y la subestación de distribución.
- Tramo de Media Tensión (entre 10 y 50 Kilovoltios) desde la subestación de distribución hasta el centro de distribución.
- Red de Baja Tensión (entre 220 y 380 Voltios) que distribuye la energía dentro de los centros urbanos para uso doméstico, comercial e industrial.

La razón de utilizar unas tensiones tan elevadas es que, a mayor tensión, menor es la intensidad necesaria y menores pérdidas que crea la resistencia del cable.

El modem PLC de cabecera ubicado en el centro de transformación de media tensión de la operadora eléctrica, acopla y desacopla la señal de datos de la señal eléctrica. Puesto que la red eléctrica de baja tensión está compartida entre 100-300 casas en Europa, el modem de cabecera se encargaría de soportar el tráfico procedente de todos estos usuarios, asignando dinámicamente la capacidad de los canales de datos disponibles a los usuarios basándose en su demanda instantánea y en el tipo de tráfico de datos a enviar; pues el tráfico de datos en tiempo real (como la voz o el vídeo), que requieren un retardo mínimo, es priorizado respecto a otros tipos de tráfico.



Los centros de transformación se unirán entre sí mediante PLC u otra tecnología, uniendo uno de ellos al centro de servicios conectado a Internet u otras redes de telecomunicaciones, y desde el que también se podrán supervisar y controlar remotamente los equipos PLC instalados y gestionar datos de los clientes como la lectura de contadores. Por último, el operador deberá también, en algunos casos, instalar en el cuarto de contadores de cada edificio una pasarela residencial que es un repetidor encargado de amplificar la señal y retransmitirla hasta todos los enchufes de los hogares u oficinas.

El cliente, al contratar el servicio, deberá comprar e instalar un pequeño modem PLC donde se conectarán los equipos de transmisión de datos, como un PC. Este modem dispondrá de un puerto para ser conectado al enchufe y otro, generalmente USB (aunque también, según el modelo, puede ser RS-232 o Ethernet), para ser conectado al PC del mismo modo que un modem ADSL. El modem PLC se encarga de separar la señal de baja frecuencia del suministro eléctrico (a 50 Hz en Europa y a 60 Hz en Estados Unidos) de la que transporta los datos (de 1,6 a 30 MHz actualmente). Este funcionamiento es muy similar al del *splitter* ADSL, que separa la señal de voz analógica tradicional (que ocupa la banda de 300-3.400 Hz) de los datos. Para ello el modem tiene en su interior dos filtros: uno de paso bajo, que dejará circular la electricidad y al cual se conectarán los electrodomésticos, televisores y demás aparatos del hogar; y otro de paso alto, que separará la onda portadora de información. Esta última será tratada por el modem con el fin de convertirla en datos útiles para el PC (vídeo, imagen, voz, etc.) en forma de protocolo IP. Este filtro se encarga también de limpiar los ruidos variables generados en la red por todos los aparatos eléctricos conectados y que podrían introducir distorsiones muy significativas en la transmisión de datos, y de ofrecer privacidad a la comunicación de datos basada en VLAN y protección mediante mecanismos de encriptación.

Todas las compañías eléctricas están interesadas en desplegar esta tecnología (tanto empresas a nivel nacional como pequeñas corporaciones o cooperativas locales). Independientemente de inversiones previas, todas ellas ven en PLC una tecnología de acceso que les puede abrir otros mercados y ofrecer nuevos servicios.

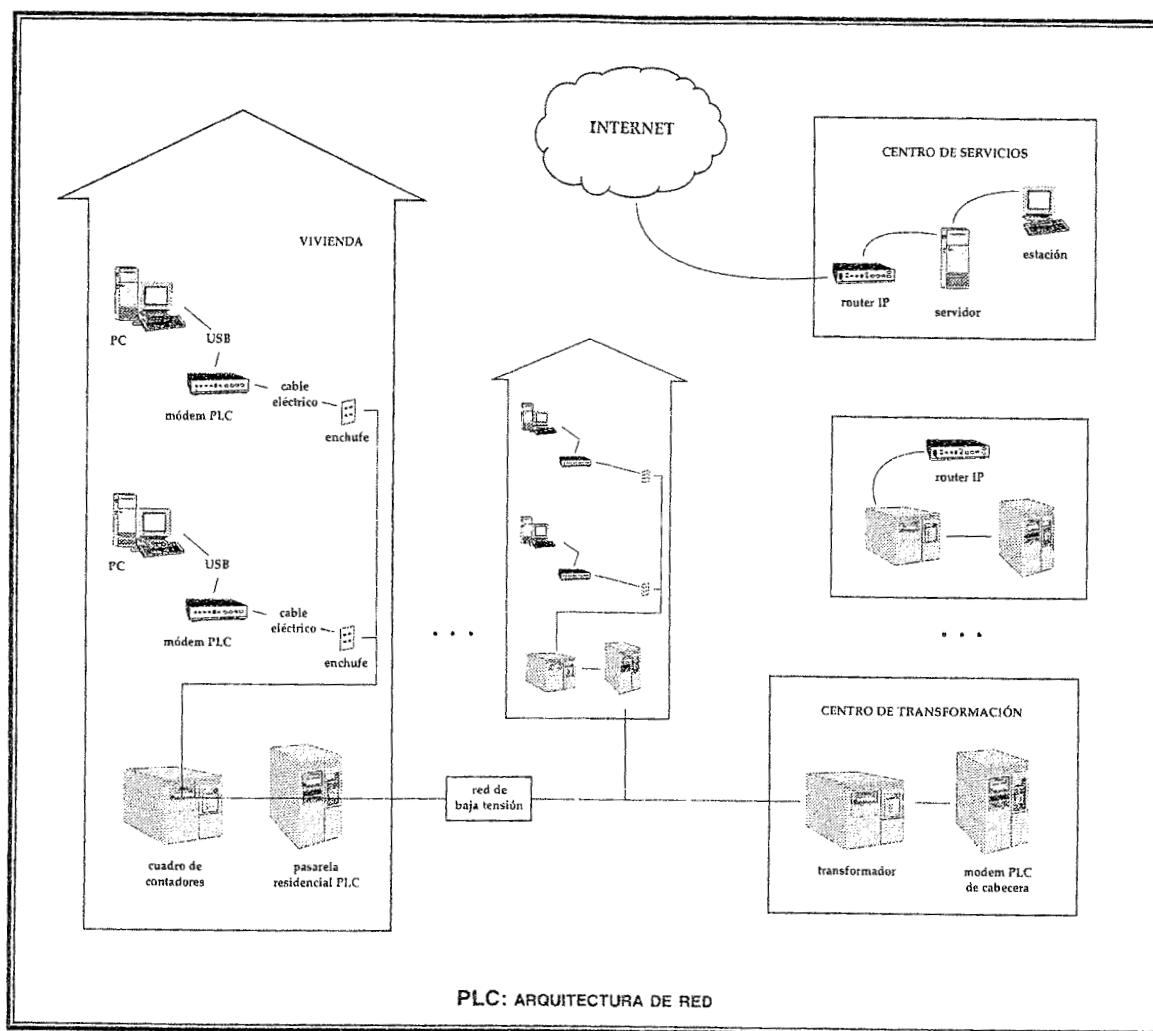
PLC representa una esperanza para mucha gente que desea acceder a la banda ancha, pero no puede ya que vive en pequeños municipios donde el ADSL y el Cable no llegan. ¿Es una esperanza real? Aproximadamente, ¿qué masa crítica debe tener un municipio para que la tecnología PLC sea viable?

Ciertamente lo es, ya que de hecho se están realizando pruebas para dotar de acceso a Internet a municipios donde la implantación de otro tipo de tecnologías resulta difícil. En cuanto a la masa crítica necesaria para el despliegue de PLC, este dato depende de varias variables, tales como el índice de penetración deseado, la topología de la red eléctrica en la zona, precio de los equipos, otro tipo de intereses distintos a los económicos, etc.

A continuación vamos a mostrar los equipos usados en una red PLC. Comenzaremos con el modem PLC que necesita una empresa o un usuario doméstico en su casa. Este equipo no sólo proporciona acceso a Internet sino también servicio telefónico de voz.

El modem de usuario se conecta con un equipo denominado «Repetidor». Este equipo puede atender hasta 256 modems y se sitúa en el cuarto de contadores del edificio o manzana.

A su vez, el «Repetidor» se conecta con equipo «Head End». Estos equipos se encuentran en los centros de transformación de la compañía energética.



El usuario final simplemente enchufa su modem PLC a la red eléctrica. El modem establece comunicación con el «Repetidor» de dicho edificio o manzana situado en el cuarto de contadores. Esta comunicación es protegida por algoritmos propietarios de DS2 implementados en hardware y transcurre en el tramo de baja tensión.

La velocidad en este tramo es de 45 Mbps actualmente, pero con claro camino de evolución. Estos 45 Mbps son realmente 27 Mbps en sentido descendente (bajada) y 18 en sentido ascendente (subida), con la que la comunicación es asimétrica y se comparten entre todos los usuarios que colgarán de dicho Repetidor, con un máximo de 256 usuarios.

Muchas personas se asustan un poco cuando comprenden que los 45 Mbps se quedan en 27 Mbps de subida y 18 Mbps de bajada a compartir entre todos los usuarios. La gente argumenta que en el caso de ADSL, el usuario tiene una conexión individual hasta la central ya que el par de cobre no lo comparte con nadie. Aunque esto sea cierto, todas las conexiones ADSL son agregadas por un multiplexor ATM y salen por el mismo enlace hasta el siguiente tramo de red. En este punto concreto, Telefónica decide cuántos ADSLs meter por Mbit/s de salida de que dispone.

En el caso de PLC esta concentración ocurre antes, en el equipo repetidor concretamente. Al final, el usuario dispone de un ancho de banda de salida a Internet mínimo determinado por la concen-

tración (número de conexiones que se juntan por Mbit/s de salida) y la velocidad máxima está determinada por la cantidad de usuarios que en este momento estén usando su conexión ADSL, teniendo en cuenta la máxima teórica sea de 256 Kbps o 2 Mbps.

En PLC ocurre lo mismo, si 100 usuarios de un mismo equipo «Repetidor» están conectados, la velocidad máxima teórica de bajada es de 270 Kbps, pero si lo están tan sólo 10 usuarios la velocidad máxima teórica de bajada es de 2,7 Mbps mientras que en ADSL nunca vamos a pasar de los 256 Kbps o 2 Mbps ya que éste es nuestro máximo teórico, haya o no muchos usuarios conectados. Desde ese punto de vista, PLC escala de una manera no igualada por ADSL.

Continuando con la explicación de la arquitectura de la red, el siguiente tramo de la red transcurre entre el «Repetidor» y su «Head End» correspondiente. Después, tal y como se puede ver en la figura, pasamos a un nivel en el que los equipos «Head End» se comunican entre sí. Este nivel corresponde a la red de Media Tensión. Aquí, las velocidades actuales son de 135 Mbps.

Para dar salida a Internet uno o varios de los «Head End» se conecta a una red de transporte clásica como las que describíamos en el apartado segundo de este artículo. Esta red de transporte suele ser SDH/Sonet o Gigabit Ethernet, que últimamente está teniendo una enorme adopción. Esta red de transporte proporciona la salida a Internet.

#### **4. PLC. NORMATIVA REGULADORA. VENTAJAS E INCONVENIENTES.**

La red eléctrica es un medio compartido. ¿Cómo se controla la privacidad de los datos que el usuario envía tanto en el tramo modem de usuario-Repetidor como en el tramo Repetidor-Headend? Existen tecnologías propietarias del diseñador del chip que proporcionan esta funcionalidad con un éxito completo.

Sabemos que ya se está trabajando en ofrecer soporte de tecnologías como VLANs. ¿En qué estado de desarrollo se encuentra este soporte? Los equipos actuales son capaces de soportar entornos donde se implementan VLANs basadas en el estándar 802.1q.

¿Es posible hacer VPNs en las que alguna o los dos extremos tengan conexión PLC? ¿Es posible activar tecnologías de encriptación como IPSEC? Sí. No existe ningún problema para este tipo de conexiones seguras.

Para proveer con la seguridad requerida, la «HomePlug Powerline Alliance» ha definido un mecanismo de encriptación DES de 56 bits, así que una vez que una señal está encriptada un dispositivo con un mecanismo de encriptación diferente no podrá interpretar y por consiguiente habremos conseguido el objetivo de mantener la privacidad.

¿Cómo se puede asegurar qué productos elaborados por diversos proveedores sean compatibles para lograr que funcione una red PLC? Para conseguir esta compatibilidad se creó la «HomePlug Alliance» formada por las trece industrias líder del sector en marzo de 2000. Como resultado de su trabajo elaboraron la especificación «HomePlug 1.0» que fue liberada en junio de 2001.

La especificación HomePlug 1.0 está disponible para todos los miembros de la «HomePlug Powerline Alliance».

• **VENTAJAS E INCONVENIENTES.**

- Economía de instalación.
  - Sin obra civil.
  - Cada instalación en un transformador da acceso entre 150-200 hogares.
- Modelo económico.
  - Con los costes de la tecnología actual: despliegue viable.
  - Se barajan escenarios de reducción de costes a medio plazo.
- Anchos de banda muy superiores a ADSL.
  - El límite de velocidad para ADSL es 2Mb.
  - PLC puede llegar a ofrecer velocidades superiores a los 10Mb.
- Emisiones electromagnéticas.
  - Equiparables a ADSL y muy inferiores a la telefonía móvil.
- Monopolio en el bucle local.
  - No existen alternativas a ADSL y el operador dominante tiene más del 90 por 100 de cuota de mercado.
  - Cualquier enchufe en casa se convertirá en un acceso a los servicios.

• **UNA VISIÓN SOBRE EL «HOME-NETWORKING».**

Mientras es relativamente fácil conectar un modem de banda ancha a un PC, es mucho más duro compartir el modem entre varios PC, especialmente si están en salas diferentes de la casa. Una vez que se consigue un acceso de banda ancha, se necesita una red doméstica para compartir ese ancho de banda entre varios PC. Una vez que comienza el uso de la red, se encuentran valores añadidos como compartir archivos y periféricos. En pocos años han crecido las ventas rápidamente de medios digitales como: las cámaras digitales de vídeo, cámaras digitales de fotografía, ficheros de música MP3, DVD de juegos y música. Muchos sistemas portátiles de teléfono usan tecnologías digitales. La grabadora digital de vídeo (DVR) ha tenido un crecimiento exponencial de sus ventas y su funcionalidad está siendo incluida en todos los PC. Las ventas de TV digitales también crecen. Algunas compañías han introducido equipos para actuar como servidores domésticos para audios y vídeo.

Muchos de estos dispositivos se conectan juntos hoy para formar pequeñas redes. USB se usa para conectar impresoras, compartir ficheros MP3, y para volcar fotos desde las cámaras digitales a los PC. IEEE 1394 («FireWire») se usa para conectar las cámaras de vídeo a computadoras personales. Ethernet conecta PC a modem de banda ancha. Una variedad de interfases analógicas y digitales se

usan para interconectar DVD de juegos, DVRS, TV digitales, y otros conjuntos digitales. Los hogares tienen muchos tipos de cableados para conectarse a distintas fuentes. Cada tipo de cableado se instaló para un propósito específico: cables eléctricos para conectar a fuentes de potencia, cable telefónico para distribuir los teléfonos alrededor del hogar desde la línea telefónica entrante y así por cada nuevo tipo de dispositivo que se instala en un hogar. Cada usuario es un individuo con necesidades específicas basado sobre su estilo de vida, situación económica, educación, por ello prevemos una persona que pueda comprar para el hogar y electrónica de consumidor. Con tantos posibles dispositivos en un hogar hoy en día, veamos algunas necesidades de este tipo de usuario:

- Cuando los usuarios tienen un modem de banda ancha y más de un PC, y especialmente cuando los PC están en salas diferentes, necesitan una red local para compartir la conexión a Internet, los diversos archivos y compartir periféricos como las impresoras.
- Si la gente tiene preocupación para proteger los sistemas y los datos en su casa de cualquier intruso exterior, necesitan un cortafuego (firewall).
- La gente que trae al hogar su PC portátil desde la oficina y quiere conectarlo al PC de casa y al modem de banda ancha, establece redes inalámbricas para este fin.
- Mucha gente descarga música desde los CD de música o directamente desde Internet en formato MP3 a sus discos duros del PC doméstico. Desearían escuchar música desde Internet directamente así como poder transmitir desde sus sistemas estéreo domésticos y eso significa que su red conecte estos sistemas tanto a sus PC o directamente a Internet.
- A la gente le gustaría integrar los diversos sistemas de telefonía y los servicios inalámbricos, analógicos e IP basados en tecnología digital o no y compartirlos a través de la casa.
- Ellos desean transferir información desde los asistentes digitales personales (PDAS), cámaras digitales y PC dondequiera estén en la casa sin tener que desenchufarlos de un lugar y enchufarlos en otro.
- La gente quiere almacenar y compartir los vídeos y fotos digitales en su casa, y en las de otros como familiares y amigos utilizando para ello la conexión de banda ancha de Internet.

Los requerimientos necesarios para cumplir las necesidades de usuario indicadas anteriormente se centran en las cinco categorías siguientes de aplicaciones digitales:

Datos, Telefonía, Audio, Vídeo y automatización.

Las aplicaciones de datos incluyen el uso compartido de Internet de texto, datos, e-mail, y Chat, incluye compartición de datos y periféricos entre PC y otro PC con una conexión de banda ancha. La mayoría de estas aplicaciones trabajará satisfactoriamente a la tarifa de datos de 5 Mb/s o menos.

Los servicios de telefonía incluyen todas las formas de comunicaciones interpersonales de voz. Comenzar con los servicios de voz y luego agregando la telefonía de vídeo y multimedia. Los servicios de voz requieren que tasa de datos (15-64 kb/s) mientras que el vídeo requiere tasas algo más altas (128-384 kb/s). La voz y el vídeo son altamente sensibles al jitter y a la demora y operan satisfactoriamente sobre redes diseñadas para apoyar calidad de servicio (QoS) desde el punto de vista de la anchura de banda.

Las aplicaciones de audio incluyen la distribución de audio digital desde discos compactos, ficheros MP3, radio en Internet, y un servidor de medios domésticos a lo largo de la casa dando salida a cualquier conjunto de altavoces y cascos. Estas aplicaciones requieren tasas de datos desde 128 kb/s a 1 Mb/s (dependiendo de la compresión) y operan sobre redes diseñados QoS.

Las aplicaciones de vídeo incluyen la distribución de contenido digital de vídeo desde la conexión de banda ancha, DVD de juegos, al servidor doméstico de medios así como de cualquier vídeo de la casa bien que esté en un PC, una TV, una consola de juegos o un Webpad. El vídeo contempla muchos formatos incluyendo la definición +estándar convencional (SD) y definición alta (HD). SD de vídeo requiere 1.5-8 Mb/s por canal, mientras HD requiere 19.39 Mb/s por canal. Estas aplicaciones operan la mayoría satisfactoriamente sobre redes diseñadas para apoyar QoS.

Telemetría y el control incluyen una amplia variedad de aplicaciones. Incluyen controles de audio y vídeo, controles de electricidad y gas; la seguridad doméstica, incluyendo el acceso externo mediante cámaras de vídeo; electrodomésticos; y en general comunicación doméstica entre dispositivos.

