

**PROPUESTA PARA LA IMPLEMENTACION DE MOVILIDAD  
SOBRE IPV6 EN LA RED DE DATOS DE LA UNIVERSIDAD  
DEL CAUCA**



**ANEXOS**

**JANETH PATRICIA CHACÓN MELO  
PASTOR OVIDIO BENAVIDES PIAMBA**

**UNIVERSIDAD DEL CAUCA  
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES  
DEPARTAMENTO DE TELECOMUNICACIONES  
POPAYÁN  
2006**

## TABLA DE CONTENIDO

	Pág.
<b><u>ANEXO A: TERMINOLOGIA RELACIONADA CON MOVILIDAD - RFC 3753</u></b>	
<b>1. INTRODUCCIÓN</b> .....	<b>1</b>
<b>2. TÉRMINOS GENERALES</b> .....	<b>2</b>
<b>3. REDES DE ACCESO MÓVIL Y REDES MÓVILES</b> .....	<b>9</b>
<b>4. TERMINOLOGÍA DE HANDOVER</b> .....	<b>14</b>
4.1. ALCANCE DEL HANDOVER .....	14
4.2. CONTROL DEL HANDOVER .....	16
4.3. CONECTIVIDAD SIMULTÁNEA PARA ACCEDER A LOS ENRUTADORES .....	17
4.4. ASPECTOS FUNCIONALES Y DESEMPEÑO .....	18
4.5. MICRO DIVERSIDAD, MACRO DIVERSIDAD Y DIVERSIDAD IP .....	19
4.6. PAGING, MODOS Y ESTADOS DEL NODO MÓVIL .....	20
4.7. TRASLADO DEL CONTEXTO .....	22
4.8. DESCUBRIMIENTO DE UN CANDIDATO A ENRUTADOR DE ACCESO .....	22
4.9. TIPOS DE MOVILIDAD .....	23
<b>5. TERMINOLOGIA ESPECÍFICA PARA EL ESTABLECIMIENTO DE UNA RED MOVIL AD-HOC</b> .....	<b>25</b>
<b>6. TERMINOLOGIA RELACIONADA CON SEGURIDAD</b> .....	<b>26</b>

## **ANEXO B: LAS EXTENSIONES DE IPv6 MÓVIL Y SUS MENSAJES**

<b>1. INTRODUCCION</b> .....	<b>27</b>
<b>2. TRASPASO USANDO EL PROTOCOLO MIPV6</b> .....	<b>28</b>
2.1. ROUTER SOLICITATION .....	28
2.1.1. Source link-layer address .....	29
2.2. ROUTER ADVERTISEMENT .....	29
2.2.1. Source link-layer address .....	30
2.2.2. MTU .....	31
2.2.3. Prefix information .....	31

2.3.	NEIGHBOR SOLICITATION.....	32
2.3.1.	Source link-layer address .....	33
2.4.	BINDING UPDATE .....	33
2.4.1.	Binding authorization data .....	34
2.4.2.	Nonce indices.....	34
2.4.3.	Alternate care-of address .....	35
2.5.	BINDING ACKNOWLEDGE .....	36
2.5.1.	Binding authorization data .....	36
2.5.2.	Binding refresh advice .....	37
<b>3.</b>	<b>HIERARCHICAL MOBILE IPV6 – HMIPV6.....</b>	<b>38</b>
<b>4.</b>	<b>FAST MOBILE IPv6 - FMIPv6 .....</b>	<b>40</b>
<b>5.</b>	<b>FAST HANDOVER FOR HIERARCHICAL MIPv6 – HMIPv6 .....</b>	<b>43</b>
<b>6.</b>	<b>TRASPASO HMIPV6 CON BINDING AL MAP, HA Y CN .....</b>	<b>44</b>
6.1.	ROUTER SOLICITATION.....	44
6.2.	ROUTER ADVERTISEMENT .....	44
6.2.1.	MAP option.....	44
6.3.	LOCAL BINDING UPDATE .....	45
6.4.	BINDING UPDATE .....	45
6.5.	BINDING ACKNOWLEDGE .....	45
<b>7.</b>	<b>TRASPASO HMIPV6 CON BINDING AL MAP .....</b>	<b>46</b>
7.1.	INTERCAMBIO DE MENSAJES DESDE EL MN SIN CAMBIO DE DOMINIO.....	46
<b>8.</b>	<b>TRASPASO CON FMIPV6.....</b>	<b>47</b>
8.1.	ESCENARIO PREDICTIVO.....	47
8.2.	ESCENARIO REACTIVO .....	47
8.2.1.	Router solicitation for proxy advertisement (rtsolpr) .....	48
8.2.2.	Proxy router advertisement (prrtadv) .....	49
8.3.	FAST BINDING UPDATE (FBU).....	51
8.4.	FAST BINDING ACKNOWLEDGE (FBAck).....	52
8.4.1.	Alternate care-of address .....	53
8.5.	HANDOVER INITIATE (HI).....	54
8.5.1.	Link-layer address of mn .....	54
8.6.	HANDOVER ACKNOWLEDGE (HAck) .....	55
8.7.	FAST NEIGHBOR ADVERTISEMENT (FNA).....	57

<b>9. TRASPASO CON F-HMIPV6 .....</b>	<b>58</b>
---------------------------------------	-----------

## **ANEXO C: ESTANDARIZACION RELACIONADA CON MOVILIDAD**

<b>1. INTRODUCCION .....</b>	<b>59</b>
<b>2. TIPOS DE ORGANISMOS DE ESTANDARIZACION .....</b>	<b>60</b>
2.1. ALIANZAS DE TECNOLOGÍA .....	60
2.2. ORGANIZACIONES DE ESTÁNDARES.....	60
2.3. ASOCIACIONES DE LA INDUSTRIA .....	60
<b>3. ESTADO DE LA ESTANDARIZACIÓN RELACIONADA CON MOVILIDAD.....</b>	<b>61</b>
3.1. 3GPP.....	61
3.2. OMA.....	63
3.3. 3GPP2.....	66
3.4. IEEE 802.....	67
3.4.1. El estándar IEEE 802.11 .....	67
3.4.2. Capas IEEE 802.11 .....	68
3.5. REDES DE AREA PERSONAL INALAMBRICAS .....	70
3.5.1. El estándar IEEE 802.15 .....	70
3.6. REDES AD-HOC.....	73
3.7. REDES DE ÁREA METROPOLITANA .....	75
3.7.1. El estandar IEEE 802.16 .....	75
3.7.2. El estandar IEEE 802.20 .....	78
3.7.3. El estandar IEEE 802.21 .....	78
3.8. SEGURIDAD.....	79
<b>4. ORGANIZACIONES DE ESTÁNDARES .....</b>	<b>80</b>
4.1. IETF .....	80
4.2. UIT .....	80
4.3. ETSI.....	82
<b>5. LA ESTANDARIZACIÓN A MEDIO PLAZO .....</b>	<b>83</b>

## **ANEXO D: ANALISIS FINANCIERO DE LAS PROPUESTAS DE DISEÑO**

<b>1. INTRODUCCION</b> .....	<b>84</b>
2. ESTUDIO FINANCIERO DE LA PROPUESTA No. 1 .....	85
3. ESTUDIO FINANCIERO DE LA PROPUESTA No. 2 .....	88

## **ANEXO E: SERVICIOS PRESTADOS SOBRE LAS REDES MOVILES.**

<b>1. INTRODUCCION</b> .....	<b>92</b>
<b>2. REGLAS Y PROTOCOLOS</b> .....	<b>93</b>
2.1.ARQUITECTURA Y PROTOCOLOS PARA SERVICIOS REDES GPRS Y UMTS ....	93
2.1.1. La arquitectura de RI (red inteligente).....	95
2.1.2. La arquitectura de Camel .....	95
2.1.3. El estándar mobile ip .....	96
2.1.4. La arquitectura de OSA .....	97
2.2. LOS SERVICIOS DE LAS REDES 3G .....	102
<b>3. ESTANDARIZACIÓN DE LOS SISTEMAS CELULARES DE TERCERA GENERACIÓN</b> .....	<b>104</b>
3.1. IMT – 2000 .....	104
3.1.1. Historia del imt – 2000.....	104
3.1.2. Especificaciones del espectro de imt-2000.....	106
3.2. EL SISTEMA UMTS .....	107
3.3. EL SISTEMA CDMA2000.....	108
3.3.1. Historia del 3gpp y 3gpp2.....	108
3.3.2. Sistemas cruzados en cdma2000 (especificaciones).....	109
3.3.3. Sistemas hdr en cdma2000.....	109
3.4. EL SISTEMA UWC-136.....	109
3.4.1. Historia evolución 2g is-136 a 3g uwc-136 .....	109
3.4.2. Descripción del sistema uwc-136 (estándares técnicos).....	110
<b>4. ASPECTOS LEGALES Y REGULATORIOS</b> .....	<b>112</b>
4.1. USUARIOS Y PRIVACIDAD.....	112
4.2. SEGURIDAD .....	112
4.3. LEGISLACIÓN EN EL SECTOR COMUNICACIONES.....	114

4.3.1. Licencias .....	114
4.3.2. Leyes relacionadas con la movilidad en colombia .....	114
4.4. COMPETENCIA .....	115
4.5. ACCESO .....	116
4.6. COMPATIBILIDAD ENTRE TECNOLOGÍAS.....	116
<b>REFERENCIAS BIBLIOGRAFICAS.....</b>	<b>117</b>

## LISTA DE FIGURAS

	Pág.
FIGURA A-1: Arquitectura de Red de Referencia .....	¡Error! Marcador no definido.
FIGURA B-1: Diálogo de Traspaso con Binding al HA .....	¡Error! Marcador no definido.
FIGURA B-2: Mensaje de Router Solicitation.....	¡Error! Marcador no definido.
FIGURA B-3: Opción source link-layer address del Router Solicitation.	¡Error! Marcador no definido.
FIGURA B-4: Mensaje de Router Advertisement. ....	¡Error! Marcador no definido.
FIGURA B-5: Opción Source Link-layer Address del Router Advertisement. ....	¡Error! Marcador no definido.
FIGURA B-6: Opción MTU del Router Advertisement. ....	¡Error! Marcador no definido.
FIGURA B-7: Opción Prefix Information del Router Advertisement.	¡Error! Marcador no definido.
FIGURA B-8: Mensaje de Neighbor solicitation.....	¡Error! Marcador no definido.
FIGURA B-9: Opción Source link-layer address del Neighbor solicitation.	¡Error! Marcador no definido.
FIGURA B-10: Mensaje de Binding Update. ....	¡Error! Marcador no definido.
FIGURA B-11: Mobility option: Binding Authorization Data del Binding Update.....	¡Error! Marcador no definido.
FIGURA B-12: Mobility option: Nonce Indices del Binding Update.	¡Error! Marcador no definido.
FIGURA B-13: Mobility Option: Alternate Care-of Address del Binding Update.....	¡Error! Marcador no definido.
FIGURA B-14: Mensaje de Binding Acknowledge.....	¡Error! Marcador no definido.
FIGURA B-15: Mobility Option: Binding Authorization Data del Binding Ack. ....	¡Error! Marcador no definido.
FIGURA B-16: Mobility Option: Binding Refresh Advice del Binding Ack.	¡Error! Marcador no definido.
FIGURA B-17: Diálogo de traspaso Dialogo en MIP Jerárquico.....	38
FIGURA B-18: Es cenario FMIPv6t.....	40
FIGURA B-19: : Diálogo en Fast MIPv6 con escenario predictivo .	¡Error! Marcador no definido.

FIGURA B-20: FMIPv6. Diálogo en Fast MIPv6 con escenario reactivo .	¡Error! Marcador no definido.
FIGURA B-21: Fast Handover. Escenario Reactivo. ....	¡Error! Marcador no definido.
FIGURA B-22: Mensajes Router Solicitation for Proxy Advertisement.	¡Error! Marcador no definido.
FIGURA B-23: Mensajes Router Solicitation for Proxy Advertisement.	¡Error! Marcador no definido.8
FIGURA B-24: Formato del campo Options. ....	¡Error! Marcador no definido.9
FIGURA B-25: Mensajes Proxy Router Advertisement. ....	¡Error! Marcador no definido.0
FIGURA B-26: New Router Prefix Information del Proxy Router Advertisement.....	50
FIGURA B-27: New Router's Link-layer Address del Proxy Router Advertisement.....	50
FIGURA B-28: Mensajes Fast Binding Update.....	51
FIGURA B-29: Mobility Options del Fast Binding Update. ....	52
FIGURA B-30: Mensajes Fast Binding Acknowledge. ....	52
FIGURA B-31: Alternate Care-of Address del Binding Ack.....	53
FIGURA B-32: Mensaje Handover Initiate.....	54
FIGURA B-33: Link-layer Address of MN del Handover Initiate.....	54
FIGURA B-34: Previous/New Care-of Address del Handover initiate. ....	55
FIGURA B-35: Mensajes Handover Acknowledgment. ....	55
FIGURA B-36: New Care-of Address del Handover Ack. ....	56
FIGURA B-37: Mensajes Fast Neighbor Advertisement.....	57
FIGURA B-38: Link-layer Address of MN del Fast Neighbor Advertisement.....	57
FIGURA C-1: Topología de una red IEEE 802.11 .....	64¡Error! Marcador no definido.
FIGURA C-2: Modos de funcionamiento de APs con WDS.....	65
FIGURA C-3: Pila de protocolos de las redes IEEE 802 ...	¡Error! Marcador no definido.6
FIGURA C-4: Torre de protocolos de Bluetooth .....	68¡Error! Marcador no definido.
FIGURA C-5: Escenario de aplicación de Zigbee .....	69
FIGURA C-6: Redes inalámbricas con y sin infraestructura .....	70
FIGURA C-7: Visión de una red de área metropolitana.....	73
FIGURA E-1: La Arquitectura de RI.....	95
FIGURA E-2: Elementos de Red de CAMEL.....	96
FIGURA E-3: Arquitectura de OSA. ....	98
FIGURA E-4: Comunicación entre redes a través de Parlay. ....	100
FIGURA E-5: Arquitectura de JAIN. ....	101

FIGURA E-6: Familia de Sistemas IMT - 2000.....	¡Error! Marcador no definido.06
FIGURA E-7: Opción Prefix Information del Router Advertisement.....	106
FIGURA E-8: Arquitectura del Sistema UMTS .....	107

## LISTA DE TABLAS

	Pág.
TABLA C-1: Revisiones fundamentales de la norma IEEE 802.11 .....	71
TABLA C-2: Comparativa de los distintos estándares para redes inalámbricas ....	74 ¡Error!
<b>Marcador no definido.</b>	
TABLA D-1: Costo Total Facultad de Salud .....	82
TABLA D-2: Costo Total Sector Tulcán .....	83
TABLA D-3: Costo Total Sector Ingenierías .....	84
TABLA D-4: Costo Total Sector Educación .....	84
TABLA D-5: Costo Total Museo Natural .....	84
TABLA D-6: Costo Total Zona Céntrica .....	85
TABLA D-7: Costo Total Sector Las Guacas .....	85
TABLA D-8: Relación del Valor Total de la Propuesta No. 1 .....	85
TABLA D-9: Costo Total Facultad Ciencias de la Salud .....	86
TABLA D-10: Costo Total Sector Tulcán .....	87
TABLA D-11: Costo Total Sector Ingenierías .....	89
TABLA D-12: Costo Total Sector Educación .....	89
TABLA D-13: Costo Total Museo Natural .....	90
TABLA D-14: Costo Total Zona Céntrica .....	91
TABLA D-15: Costo Total Sector Las Guacas .....	91
TABLA D-16: Costo Total Edificios Particulares .....	92
TABLA D-17: Relación del Valor Total de la Propuesta No. 2 .....	92

**ANEXO A:**

**TERMINOLOGIA RELACIONADA CON MOVILIDAD  
RFC 3753**

### 1. INTRODUCCIÓN

Este documento presenta la terminología que es usada para documentos y discusiones dentro del Grupo de trabajo Seamoby. Otros grupos de trabajo relacionados con movilidad podrían tomar ventaja de esta terminología, con el propósito de crear una terminología común para el área de movilidad en redes IP.

Algunos términos y definiciones que no están directamente relacionadas con el mundo IP, son incluidos con el propósito de armonizar la terminología. Por ejemplo. “Punto de Acceso” (“Access Point”) y “Estación Base” (“Base Station”) hacen referencia al mismo componente; desde el punto de vista de IP, pero “Enrutador de Acceso” (“Access Router”) tiene un significado muy diferente. La terminología presentada puede también, eso se espera, ser adecuada para cubrir redes móviles ad-hoc.

La terminología propuesta no pretende imponer ninguna nueva terminología. Más bien los autores recibirán discusiones sobre más definiciones exactas, así como términos faltantes o innecesarios. Este trabajo es un proyecto cooperativo entre personas de muchos diferentes entornos de ingenierías y así ya presentar un primer paso en la armonización de la terminología.

La terminología en este documento está dividida en varias secciones. Primero, hay una lista de términos para uso general y redes de acceso móvil seguido por términos relacionados con *handovers*, y finalmente algunos términos usados dentro de los grupos de trabajo MANET y NEMO.

### 2. TÉRMINOS GENERALES

- **Bandwidth (Ancho de Banda)**

El ancho total de la banda de frecuencias disponible para ser usada por un canal de comunicaciones. Usualmente medida en Hertz (Hz). El ancho de banda limita la tasa de transferencia de información máxima posible a través del canal.

- **Bandwidth Utilization (Utilización del Ancho de Banda)**

La tasa real de transferencia de información realizada sobre un enlace, expresada como un porcentaje de la tasa de transferencia de información máxima teórica, de acuerdo con la Ley de Shannon (Tasa máxima teórica en la cuál dígitos libres de errores pueden ser transmitidos sobre un canal de ancho de banda limitado en la presencia de ruido).

- **Beacon (Torre de Aviso) Señal de Localización**

Un mensaje de control emitido por un nodo (especialmente, una estación base) informando a todos los otros nodos en su vecindario de la presencia continua del nodo de transmisión, posiblemente junto con el estado adicional o la información de configuración.

- **Binding Update - BU (Actualización de Asociación)**

Un mensaje que indica el último movimiento de un nodo móvil y en particular su dirección de entrega (care-of address)

- **Care-of-Address - CoA (Dirección de Entrega)**

Una dirección IP asociada con un nodo móvil mientras visita un enlace foráneo; el prefijo de subred de esta dirección IP es un prefijo de subred foráneo. Un paquete direccionado al nodo móvil el cual llega a la red base del nodo móvil cuando el nodo móvil esta lejos de su base y ha registrado una dirección de entrega será enviado a esa dirección por el Agente Base en la red base.

- **Channel (Canal)**

Una subdivisión del medio físico permitiendo posiblemente compartir usos independientes del medio. Los canales pueden ser aprovechables por la subdivisión del medio dentro de muestras discretas de tiempo, o bandas espectrales discretas o códigos de secuencia desasociados.

- **Channel Access Protocol (Protocolo de Acceso al Canal)**

Un protocolo para mediar el acceso a y posiblemente la localización de, los diversos canales disponibles dentro del medio físico de comunicaciones. Los nodos participantes en el protocolo de acceso al canal acuerdan comunicarse solamente

cuando ellos tienen un permiso no contestado a uno de los canales, así que no habrá interferencia.

- **Channel Capacity (Capacidad del Canal)**

La capacidad total de un enlace para llevar información (generalmente bits) por unidad de tiempo. Con un determinado ancho de banda, la capacidad máxima teórica del canal es asignado por la Ley de Shannon. La capacidad real del canal es determinado por el ancho de banda del canal, el sistema de codificación utilizado y la relación señal a ruido.

- **Control Message (Mensaje de Control)**

Información transmitida entre dos o más nodos de red para mantener el estado del protocolo, el cual puede estar desligado de cualquier aplicación específica.

- **Distance Vector (Vector Distancia)**

Una característica de algunos protocolos de enrutamiento en los cuales por cada destino deseado, un nodo mantiene información sobre la distancia a ese destino y un vector (próximo salto) hacia ese destino.

- **Fairness (Ecuanimidad)**

Una propiedad de los protocolos de acceso al canal, con la cual un medio se hace disponible equitativamente a todos los nodos asequibles de la red. Ecuanimidad no implica estrictamente igualdad, especialmente en casos donde los nodos suministran acceso de enlace según prioridad desigual o clasificación.

- **Flooding (Inundación)**

El proceso de envío de datos o mensajes de control a cada nodo dentro de la red bajo consideración.

- **Foreign Subnet Prefix (Prefijo de Subred Foráneo)**

Una secuencia de bits que consiste en varios números de los bits iniciales de una dirección IP, la cuál identifica un enlace foráneo del nodo dentro de la topología Internet.

- **Forwarding Node (Nodo de Reenvío)**

Un nodo que desempeña la función de reenvío de datagramas desde uno de sus vecinos a otro.

- **Home Address -HoA (Dirección Local)**

Una dirección IP asignada a un nodo móvil, usada como la dirección permanente del nodo móvil. Esta dirección está dentro del enlace local del nodo móvil. Los mecanismos convencionales de enrutamiento IP entregarán paquetes destinados por una dirección local de un nodo móvil, a su enlace local [9].

- **Home Agent -HA (Agente Local)**

Un enrutador sobre un enlace local de un nodo móvil, en el cual el nodo móvil ha registrado su dirección de entrega (care-of address) actualizada. Mientras el nodo móvil está lejos de su localidad, el agente local intercepta paquetes en el enlace local destinados a la dirección local del nodo móvil, encapsulándolos y haciéndolos tunelarse a la dirección de entrega registrada del nodo móvil.

- **Home Subnet Prefix (Prefijo de Subred Local)**

Una secuencia de bits que consiste en varios números de los bits iniciales de una dirección IP, el cuál identifica un enlace local del nodo dentro de la topología Internet (Por ejemplo, el prefijo de subred IP correspondiente a la dirección local del nodo móvil, definida como en [9]).

- **Interface (Interfase)**

Un punto de unión de un nodo a un enlace.

- **IP Access Address (Dirección IP de Acceso)**

Una dirección IP (generalmente asignada dinámicamente) que un nodo usa para designar su punto de unión actualizado a la red local. La dirección IP de acceso es típicamente reconocida desde la dirección local del nodo móvil; de hecho, mientras está visitando una red foránea la dirección IP de acceso puede ser considerada no apta para usarse como una dirección de punto final por algunas aplicaciones excepto las de ciclo de vida más corto. En lugar de eso, la dirección IP de acceso es típicamente usada como la dirección de entrega (care-of address) del nodo.

- **Link (Enlace)**

Un equipo de comunicación o medio físico que puede soportar comunicaciones de datos entre múltiples nodos de red, tal como un Ethernet (simple o cruzado). Un enlace es la capa inmediatamente debajo de IP. En un modelo de capas de red, la Capa de Enlace (Capa 2) está normalmente debajo de la Capa de Red (IP) (Capa 3), y encima de la Capa Física (Capa 1).

- **Asymmetric link (Enlace Asimétrico)**

Un enlace con características de transmisión las cuales son diferentes dependiendo de la posición relativa o características de diseño del transmisor o receptor de datos en un enlace. Por ejemplo, el rango de un transmisor puede ser mucho más alto que el rango de otro transmisor en el mismo medio.

- **Link establishment (Establecimiento de Enlace)**

El proceso de establecer un enlace entre el nodo móvil y la red local. Este puede implicar la asignación de un canal u otros recursos inalámbricos locales, posiblemente incluyendo un nivel mínimo de servicio o ancho de banda.

- **Link-Layer Trigger - L2 Trigger (Activador de la Capa de Enlace L2)**

Información desde la capa de enlace que informa a la capa de red acerca de los eventos detallados implicados en la secuencia handover en la capa de enlace. Los activadores L2 no son específicos de alguna capa de enlace particular, pero en cambio representan generalizaciones de la información disponible de la capa de red desde una amplia variedad de protocolos de capa de enlace [4].

- **Link State (Estado de Enlace)**

Una caracterización de algunos protocolos de enrutamiento en los cuales cada nodo dentro de la red esta esperando mantener información acerca de cada enlace dentro de la topología de la red.

- **Link-Level Acknowledgment (Confirmación del Nivel de Enlace)**

Una técnica del protocolo, generalmente utilizada sobre medios inalámbricos, que requiere que los vecinos confirmen la recepción de paquetes (generalmente solo unicast) desde el transmisor. Tal estrategia pretende evitar la pérdida de paquetes o retardo resultante de la deficiencia, o características no deseadas de los protocolos de alto nivel. Las confirmaciones de recibo de la capa de enlace son generalmente usadas como parte de algoritmos de solicitud de repetición automática (Automatic Repeat-Request - ARQ) para incrementar la confiabilidad del enlace.

- **Local Broadcast (Emisión Local)**

La entrega de datos a cada nodo dentro del rango del transmisor.

- **Loop-Free (Bucle cerrado - Libre)**

Una propiedad de los protocolos de enrutamiento por medio del cual el camino tomado por un paquete de datos desde la fuente al destino nunca viajara a través del mismo nodo intermedio dos veces antes de llegar al destino.

- **Medium Access Protocol - MAC (Protocolo de Acceso al Medio)**

Un protocolo para permitir el acceso a, y la posible asignación de, medios de comunicación físicos. Los nodos participantes en el Protocolo de Acceso al Medio pueden comunicarse solamente cuando tienen un acceso no contestado al medio, así que allí no habrá interferencia. Cuando el medio físico es un canal radio, el MAC es el mismo Protocolo de Acceso al Canal.

- **Mobile Network Prefix (Prefijo de Red Móvil)**

Una secuencia de bits que consiste en varios números de los bits iniciales de una dirección IP, la cuál identifica la red móvil completa dentro de la topología Internet. Todos los nodos en una red móvil necesariamente tienen una dirección que contiene este prefijo.

- **Mobility Factor (Factor de Movilidad)**

La frecuencia relativa del movimiento de un nodo, comparado con la frecuencia de iniciación de la aplicación

- **Multipoint Relay - MPR (Retransmisión Multipunto)**

Un nodo el cual es seleccionado por su vecino a un salto para retransmitir todos los mensajes broadcast que este recibe. El mensaje debe ser nuevo y el campo de tiempo de vida del mensaje debe ser mayor que uno. La transmisión multipunto es una técnica para reducir el número de re-transmisiones redundantes mientras se difunde un mensaje broadcast en la red.

- **Neighbor (Vecino)**

Un "vecino" es cualquier otro nodo al cual los datos pueden ser transmitidos directamente por el medio de comunicaciones sin contar con la participación de ningún otro nodo de transporte.

- **Neighborhood (Vecindario)**

Todos los nodos que pueden recibir datos sobre el mismo enlace desde un nodo cuando y cuantas veces éste transmita datos.

- **Next Hop (Próximo Salto)**

Un vecino que ha sido seleccionado para transportar los paquetes a lo largo del camino a un destino particular.

- **Payload (Carga Útil)**

Los datos existentes dentro de un paquete, no incluyen cabeceras de protocolos de red, que no fueron insertadas por una aplicación. Notese que las Cargas Útiles son diferentes entre capas: los datos de Aplicación son la carga útil de TCP, los cuales son la carga útil de IP, donde los tres son la carga útil de los protocolos de capa de Enlace, etc. De esta manera, es importante identificar el ámbito cuando se habla de Cargas Útiles.

- **Prefix (Prefijo)**

Una secuencia de bits que consiste en varios números de los bits iniciales de una dirección.

- **Routing Table (Tabla de Enrutamiento)**

La tabla donde los nodos de reenvío mantienen la información (incluyendo el próximo salto) para varios destinos.

- **Route Entry (Entrada de la Ruta )**

Una entrada para un destino específico (unicast o multicast) en la tabla de enrutamiento.

- **Route Establishment (Establecimiento de la Ruta)**

El proceso de definir una ruta entre una fuente y un destino.

- **Route Activation (Activación de la Ruta)**

El proceso de puesta en servicio de una ruta después de que esta ha sido establecida.

- **Routing Proxy (Proxy de Enrutamiento)**

Un nodo que dirige por encima los paquetes, por ejemplo, por tunelaje, entre compañeros que se comunican. El Agente Local y el Agente Foráneo son ejemplos de proxies de enrutamiento, ya que reciben paquetes destinados al nodo móvil y le hacen tunelaje a la dirección actualizada del nodo móvil.

- **Shannon's Law (Ley de Shannon)**

Una ley que define la tasa máxima teórica en la cual dígitos libres de errores pueden ser transmitidos sobre un canal de ancho de banda limitado en la presencia de ruido. No existe un sistema de codificación para corrección de errores prácticos que pueda acercarse al límite de desempeño teórico dado por la ley de Shannon.

- **Signal Strength (Señal de Potencia)**

La potencia perceptible de la señal que lleva los bits de datos, como la vista por el receptor de la señal.

- **Source Route (Ruta Fuente)**

Una ruta fuente desde el nodo A al nodo B es una lista ordenada de direcciones IP, empezando con la dirección IP del nodo A y terminando con la dirección IP del nodo B. Entre A y B, la ruta fuente incluye una lista ordenada de los saltos intermedios entre A y B, así como el índice de interfaz de la interfaz a través de la cual el paquete debe transmitirse para alcanzar el próximo paso. La lista de saltos intermedios podría no incluir todos los nodos visitados, algunos saltos pueden ser omitidos por una u otra razón.

- **Spatial Re-use (Re- Utilización de Espacio)**

Uso simultaneo de canales con características físicas idénticas o muy cercanas, pero localizados espacialmente distantes, lo suficientemente apartados para evitar la interferencia (Por ejemplo, la interferencia co-canal)

- **System-wide Broadcast (Emisión a toda la red)**

De la misma forma que el flooding (inundación), pero usado en contraste a difusión local.

- **Subnet (Subred)**

Una subred es un grupo lógico de nodos de red conectados. En redes IP, los nodos en una subred comparten una mascara de red común (en IPv4) o un prefijo de red (en IPv6)

- **Topology - Network Topology (Topología de Red)**

Una estructura de interconexión de una red: Que nodos se conectan directamente entre si y a través de que enlaces ellos se conectan. A algunas topologías simples se les ha dado nombres, tales como 'Topología de Bus', 'Topología de Malla', 'Topología de Anillo', 'Topología de Estrella', y 'Topología de Árbol'.

- **Triggered Update (Actualización Activada)**

Una actualización de la ruta solicitada, transmitida por un enrutador a lo largo del camino al destino.

### 3. REDES DE ACCESO MÓVIL Y REDES MÓVILES

Con el fin de soportar la movilidad del host, un conjunto de nodos hacia el borde de la red pueden necesitar tener funciones específicas. Tal conjunto de nodos forma una red de acceso móvil que puede o no hacer parte de la Internet global. La *Figura A-1* presenta dos ejemplos de tales topologías de Red de Acceso. La *Figura A-1* describe una arquitectura de referencia que ilustra una red IP con componentes definidos en esta sección.

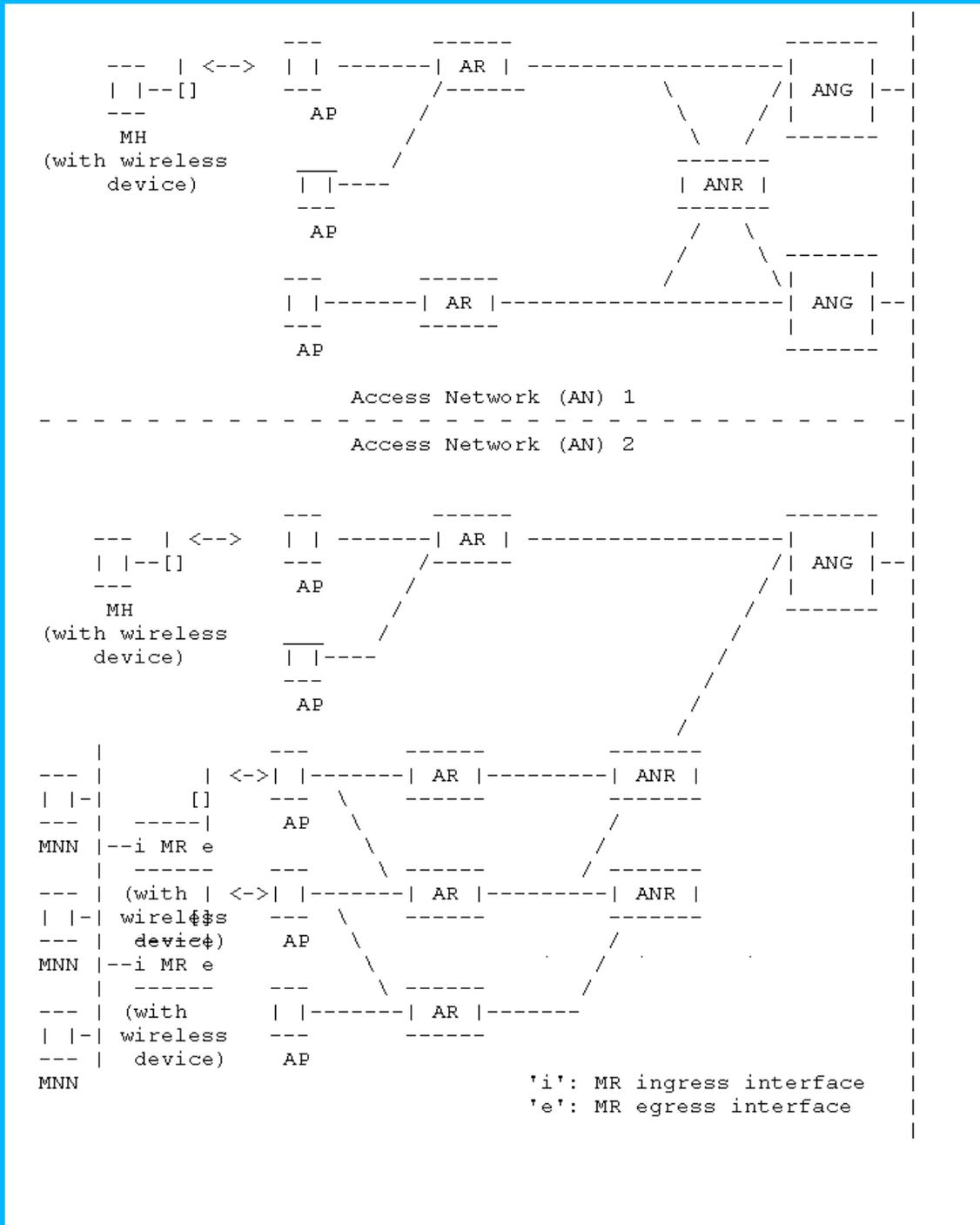
Se pretende definir el concepto de la Red de Acceso (AN) que también puede además soportar una movilidad mejorada. Es posible que para soportar enrutamiento y QoS para nodos móviles, los protocolos de enrutamiento existentes (Por ejemplo, OSPF, Open Shortest Path First, Abrir Primero el Camino más Corto [14]) puede no ser apropiado para mantener el envío de información por esos nodos móviles cuando ellos cambian sus puntos de conexión a la Red de Acceso. Estas nuevas funciones son implementadas en enrutadores con capacidades adicionales.

Se pueden distinguir tres tipos de componentes de una Red de Acceso: Enrutadores de Acceso (AR), que maneja el último salto al móvil, generalmente sobre un enlace inalámbrico; Gateways de Red de Acceso (ANG), que constituye la frontera del lado fijo de la red y protege la red fija desde los protocolos de red especializados; y (opcionalmente) otros Enrutadores de Red de Acceso internos que también pueden necesitarse en algunos casos para apoyar las funciones. La Red de Acceso consta del equipo necesario para soportar este enrutamiento especializado, por ejemplo, AR o ANG. AR y ANG pueden ser el mismo nodo físico.

Además, se presenta unos cuantos términos básicos en redes móviles, es decir, Red Móvil, Enrutador Móvil (MR), y nodo de red móvil (MNN). Más terminología para discutir sobre redes móviles se puede encontrar en [13]. Una discusión más completa de redes móviles puede encontrarse en los documentos del Grupo de Trabajo NEMO.

**NOTA:** Esta arquitectura de referencia no es la más apropiada para las personas que trabajan con Redes Móviles Ad-hoc MANET).

Figura A-1: Arquitectura de Red de Referencia



- **Mobile Node - MN (Nodo Móvil)**

Un nodo IP capaz de cambiar su punto de conexión a la red. Un Nodo Móvil puede ser un host móvil (sin funcionalidad de reenvío) o un Enrutador Móvil (con funcionalidad de reenvío).

- **Mobile Host - MH (Host Móvil)**

Un nodo móvil que esta en un terminal y no un enrutador. Un Host Móvil es capaz de enviar y recibir paquetes, es decir, ser una fuente o destino de tráfico, pero no un transportador de este.

- **Fixed Node - FN (Nodo Fijo)**

Un nodo, ya sea un host o un enrutador, incapaz de cambiar su punto de conexión a la red y su dirección IP sin interrumpir las sesiones abiertas.

- **Mobile Network (Red Móvil)**

Una red completa, moviéndose como una unidad, la cuál dinámicamente cambia su punto de conexión a la Internet y de esta manera su accesibilidad en la topología. La red móvil esta compuesta de uno o más Subredes IP y esta conectada a la Internet global a través de uno o más Enrutadores Móviles (MR). Se asume que la configuración interna de la red móvil es relativamente estable con respecto al MR.

- **Mobile Router - MR (Enrutador Móvil)**

Un enrutador capaz de cambiar su punto de conexión a la red, moviéndose de un enlace a otro. El MR es capaz de remitir paquetes entre dos o más interfases y ejecutando posiblemente un protocolo de enrutamiento dinámico modificando el estado por el cual este paquete se remite.

Un MR que actúa como una gateway entre una red móvil completa y el resto de la Internet tiene uno o más interfase(s) de salida y una o más interfase(s) de entrada. Los paquetes de retorno enviados al resto de la Internet son transmitidos a través de una de las interfases de salida del MR; los paquetes remitidos a la red móvil son transmitidos a través de una de las interfases de entrada del MR.

- **Ingress interface (Interfase de Entrada)**

La interfase de un MR ligada a un enlace dentro de la red móvil.

- **Egress interface (Interfase de Salida)**

La interfase de un MR ligada al enlace local si el MR es local, o ligado a un enlace foráneo si el MR esta en una red foránea.

- **Mobile Network Node - MNN (Nodo de Red Móvil)**

Cualquier nodo (terminal o enrutador) localizado dentro de una red móvil, ya sea permanente o temporalmente. Un nodo de red móvil puede ser un nodo móvil o un nodo fijo.

- **Access Link - AL (Enlace de Acceso)**

Un enlace del último salto entre un Nodo Móvil y un Punto de Acceso. Es decir, un equipo o medio sobre el cual un Punto de Acceso y el Nodo Móvil pueden comunicarse con la capa de enlace, esta es, la capa inmediatamente abajo de IP.

- **Access Point - AP (Punto de Acceso)**

Un punto de Acceso es un dispositivo de la capa 2 que esta conectado a uno o más Enrutadores de Acceso y ofrece la conexión de enlace inalámbrico al Nodo Móvil. Los Puntos de Acceso algunas veces son llamados Estaciones Base o Puntos de Acceso Receptor-Transmisor. Un Punto de Acceso puede ser una entidad separada o estar co-localizado con un Enrutador de Acceso.

- **Radio Cell (Celda Radio)**

EL área geográfica dentro de la cual un Punto de Acceso proporciona cobertura inalámbrica, es decir, donde la radiocomunicación entre un Nodo Móvil y el Punto de Acceso específico es posible.

- **Access Network Router - ANR (Enrutador de Red de Acceso)**

Un enrutador IP en la Red de Acceso. Un Enrutador de Red de Acceso puede incluir funcionalidades específicas de la Red de Acceso, por ejemplo, las relacionadas con movilidad y/o QoS. Esta es la diferencia entre enrutadores comunes y enrutadores que están relacionados con funcionalidades específicas de la Red de Acceso.

- **Access Router - AR (Enrutador de Acceso)**

Un Enrutador de Red de Acceso que reside en la frontera de una Red de Acceso y esta conectado a uno o más Puntos de Acceso. Los Puntos de Acceso pueden ser de diferentes tecnologías. Un Enrutador de Acceso ofrece conectividad IP a los nodos móviles, actuando como un enrutador predeterminado a los Nodos Móviles que actualmente este prestando servicio. El Enrutador de Acceso puede incluir inteligencia más allá de un simple servicio de reenvío ofrecido por enrutadores IP comunes.

- **Access Network Gateway - ANG (Gateway de Red de Acceso)**

Un Enrutador de Red de Acceso que separa una Red de Acceso de otras redes IP, en gran medida de la misma forma como un enrutador gateway común. La Gateway de Red de Acceso mira a las otras redes IP como un enrutador IP convencional. En

una red pequeña, un ANG puede también ofrecer los servicios de un AR, particularmente ofreciendo conectividad IP a los nodos móviles.

- **Access Network - AN (Red de Acceso)**

Una red IP que incluye uno o más Enrutadores de Red de Acceso.

- **Administrative Domain - AD (Dominio Administrativo)**

Una colección de redes bajo el mismo control administrativo y se agrupan para propósitos administrativos [5].

- **Serving Access Router - SAR (Enrutador de Acceso de Servicio )**

El Enrutador de Acceso normalmente ofrece la conectividad a la MN. Este es usualmente el punto de partida para la MN en su camino hacia un nuevo Router de Acceso (el cual registra el tiempo que el Router de Acceso de Servicio toma el rol del anterior Enrutador de Acceso). Puede ser que varios Enrutadores de Acceso de Servicio presten servicio al Nodo Móvil al mismo tiempo.

- **New Access Router - NAR (Enrutador de Acceso Nuevo)**

El Enrutador de Acceso que ofrece conectividad al Nodo móvil después de un handover.

- **Previous Access Router - PAR (Enrutador de Acceso Anterior)**

Un Route de Acceso que ofrece conectividad al Nodo Móvil anterior a un handover. Este es el Enrutador de Acceso de Servicio que suspenderá o ha dejado de ofrecer conectividad al Nodo Móvil. Con frecuencia también llamado Old Access Router (OAR), Enrutador de Acceso antiguo.

- **Candidate Access Router - CAR (Enrutador de Acceso Candidato)**

Un Enrutador de Acceso al cuál el Nodo Móvil puede hacer un handoff. Ver la sección 4.8

### 4. TERMINOLOGÍA DE HANDOVER

Estos términos se refieren a las diferentes perspectivas y estrategias para soportar los diferentes aspectos de movilidad. Pueden hacerse distinciones según el alcance, el rango de superposición, características de desempeño, características de diversidad, cambios de estado, tipos de movilidad y métodos de control de técnicas handover.

- **Roaming (Itinerancia)**

Un término fundamentado en el operador que implica acuerdos formales entre operadores que permiten que un móvil obtenga conectividad desde una red foránea. Roaming (un aspecto particular de la movilidad de usuario) incluye, por ejemplo, la funcionalidad por la cual los usuarios pueden comunicar su identidad a la AN local y que los acuerdos entre ANs puedan ser activados y puestos en servicio y las aplicaciones en la red local del MN se puedan hacer disponibles al usuario localmente.

- **Handover (Traspaso)**

El proceso por el cual un MN activo (En el Estado Activo, ver la sección 4.6) cambia su punto de conexión a la red, o cuando se intentó tal cambio. La red de acceso puede proporcionar características para minimizar la interrupción de sesiones en proceso. También se denomina **Handoff**.

Hay diversos tipos de handover clasificados según diversos aspectos implicados en el Handover. Alguna de esta terminología sigue la descripción en [4].

#### 4.1. ALCANCE DEL HANDOVER

- **Layer 2 Handover (Handover Capa 2)**

Un handover donde la MN cambia de APs (o algún otro aspecto del canal de radio) conectado a la misma interfase del AR. Este tipo de handover es transparente al enrutamiento de la capa IP (o este aparece simplemente como reconfiguración de la capa de enlace sin ninguna implicación de movilidad).

- **Intra-AR Handover (Handover dentro del AR)**

Un handover que cambia la interfase de red del AR al móvil. Es decir, se mantiene el mismo Serving Access Router - SAR (Enrutador de Acceso de Servicio) pero tienen lugar los cambios de las rutas internas al AR.

- **Intra-AN Handover (Handover dentro del AN)**

Un handover donde el MN cambia de ARS dentro de la misma AN. Tal handover no es necesariamente visible fuera de la AN. En caso de que la ANG que da servicio al MN cambie, este handover es visto afuera de la AN debido al cambio en las trayectorias de enrutamiento. Notese que la ANG puede cambiar solamente para algunos de los flujos de datos de la MN.

- **Inter-AN Handover (Handover entre AN)**

Un handover donde el MN se mueve a una nueva AN. Esto requiere soporte para macromovilidad. Notese que esto debería involucrar la asignación de una nueva dirección de acceso IP (Por ejemplo una nueva care-of address) al MN.

- **Intra-Technology Handover (Handover dentro de la Tecnología)**

Un handover entre equipos de la misma tecnología.

- **Inter-Technology Handover (Handover entre Tecnologías)**

Un handover entre equipos de diferentes tecnologías.

- **Horizontal Handover (Handover Horizontal)**

Este implica MNs que se mueven entre puntos de acceso del mismo tipo (en términos de cobertura, tasa de datos y movilidad), tales como, UMTS a UMTS o WLAN a WLAN

- **Vertical Handover (Handover Vertical)**

Este implica MNs que se mueven entre puntos de acceso de diferente tipo, tales como, UMTS a WLAN

Notese que la diferencia entre un handover horizontal y vertical es vaga. Por ejemplo, un handover desde un AP con enlace WLAN 802.11b a un AP con enlace WLAN 802.11g se puede considerar como handover vertical u horizontal, dependiendo del punto de vista personal.

Notese también que la capa IP percibe interfases de red y direcciones IP, más que las tecnologías específicas usadas por esas interfases. Así, los handovers horizontales y verticales pueden o no ser anunciados a la capa IP. Generalmente un handover puede ser percibido si la dirección IP asignada a la interfase cambia, la interfase de red misma cambia (la cual puede también cambiar de dirección IP), o hay una interrupción del enlace, por ejemplo, cuando el nodo móvil se sale de su cobertura por un momento. Por ejemplo en una red GPRS, un handover horizontal sucede generalmente inadvertido por la capa IP. Similarmente un handover horizontal WLAN puede ser notado si la dirección IP de la interfase cambia. Por otra parte, los handovers verticales a menudo cambian la interfase de red y, por lo tanto son detectados en la capa IP. No obstante, algunas tarjetas

de red específicas son capaces de intercambiar entre las tecnologías de acceso (Por ejemplo GPRS a UMTS) sin cambiar la interfase de red. Por otra parte, cualquiera de los dos handovers puede o no dar lugar al cambio de AR. Por ejemplo, un AR podría controlar puntos de acceso Bluetooth y WLAN, y el nodo móvil podría hacer handover verticales y horizontales bajo el mismo AR sin cambiar su dirección IP o incluso la interfase de red.

### 4.2. CONTROL DEL HANDOVER

Un handover debe ser uno de los de los siguientes dos tipos (a):

- **Mobile-Initiated Handover (Handover iniciado por el Móvil)**  
El MN es el único que toma la decisión inicial para comenzar el handover.
- **Network-Initiated Handover (Handover iniciado por la Red)**  
La Red toma la decisión inicial para comenzar el handover.

Un handover también es uno de lo siguiente dos tipos (b):

- **Mobile-Controlled Handover (Handover controlado por el Móvil)**  
El MN tiene el control primario sobre el proceso del handover.
- **Network-Controlled Handover (Handover controlado por la Red)**  
La Red tiene el control primario sobre el proceso del handover.

Una decisión de handover normalmente involucra algún tipo de medidas acerca de cuando y donde el handover se realizará. Por consiguiente, un handover es además cualquiera de estos tres tipos (c):

- **Mobile-Assisted Handover (Handover con ayuda del Móvil)**  
La información y medida del MN son usadas por el AR para decidir en la ejecución de un handover.
- **Network-Assisted Handover (Handover con ayuda de la Red)**  
Un handover dónde la AN recolecta información que puede usarse por el MN en una decisión del handover.

- **Unassisted Handover (Handover sin ayuda)**

Un handover dónde ninguna ayuda es proporcionada por el MN o el AR.

Nótese que es posible que tanto el MN como el AR, hagan las medidas y decidan en el handover. Un handover también es uno de lo siguientes dos tipos (d):

- **Push Handover**

Un handover iniciado ya sea por el PAR, o donde el MN inicia un handover a través del PAR.

- **Pull Handover**

Un handover iniciado ya sea por el NAR, o donde el MN inicia un handover a través del NAR.

El handover es también proactivo o reactivo (e):

- **Planned Handover (Handover Planificado)**

Un handover proactivo (esperado) donde alguna señalización pueda hacerse antes de que el MN se conecte al nuevo AR, por ejemplo, construyendo un túnel temporal desde el AR anterior al nuevo AR.

- **Unplanned Handover (Handover No Planificado)**

Un handover reactivo (no esperado) donde ninguna señalización se hace antes del movimiento del MN desde anterior AR al nuevo AR.

Los cinco tipos de handover (a-e) son en la mayoría de los casos independientes, y cada handover debe ser clasificado de acuerdo a cada uno de estos tipos.

### 4.3. CONECTIVIDAD SIMULTÁNEA PARA ACCEDER A LOS ENRUTADORES

- **Make-Before-Break - MBB (Conexión antes de Desconexión)**

Durante un handover MBB, el MN hace la nueva conexión antes de que la anterior se rompa. Así, el MN puede comunicarse simultáneamente con el antiguo y el nuevo AR durante el handover. Este no debe confundirse con “soft handover” (handover flexible) el cual depende de macrodiversidad, descrito en la Sección 4.5.

- **Break-Before-Make - BBM (Desconexión antes de Conexión)**

Durante un handover BBM, el MN rompe la antigua conexión antes de que la nueva conexión sea hecha. Así, el MN no puede comunicarse simultáneamente con el antiguo y el nuevo AR.

#### 4.4. ASPECTOS FUNCIONALES Y DESEMPEÑO

- **Handover Latency (Latencia del Handover)**

La latencia es la diferencia entre el tiempo en que el MN puede en último lugar enviar y/o recibir un paquete IP por vía del PAR, y el tiempo en que el MN puede enviar y/o recibir un paquete IP a través del NAR. Adaptado de [4].

- **Smooth Handover (Handover Suave)**

Un handover que busca principalmente minimizar la pérdida de paquetes, sin la preocupación explícita por los retrasos adicionales en el envío de paquetes.

- **Fast Handover (Handover Rápido)**

Un handover que busca principalmente minimizar la latencia del handover, sin el interés explícito en la pérdida de paquetes.

- **Seamless Handover (Handover sin Interrupciones)**

Un handover en el cual no hay cambio en la capacidad de servicio, seguridad, o calidad. En la práctica, será de esperarse un poco de degradación en el servicio. La definición de un handover sin interrupciones en el caso práctico deberá ser tal que otros protocolos, aplicaciones o usuarios finales, no detecten ningún cambio en la capacidad de servicio, seguridad o calidad, que tuviera relación con su (normal) operación. Como consecuencia, lo que sería un handover sin interrupciones para una aplicación menos exigente, podría no ser sin interrupciones para otra aplicación más exigente. Ver [7] para mas discusión sobre este tema.

- **Throughput (Rendimiento)**

La cantidad de datos desde una fuente a un destino procesado por el protocolo por el cual el rendimiento será medido, por ejemplo, IP, TCP, o el protocolo MAC. El rendimiento difiere entre las capas protocolares.

- **Goodput**

El ancho de banda usado, menos el volumen de control de mensajes, cabeceras de protocolos de paquetes de datos y paquetes perdidos debido a errores CRC.

- **Pathloss (Pérdidas de trayectoria)**

Una reducción en la fuerza de la señal causada por viajar a través del medio físico que constituye el enlace.

- **Hidden-Terminal Problem (Problema del Terminal Oculto)**

El problema por el cual un nodo transmisor puede fracasar en su esfuerzo por transmitir datos debido a interferencia destructiva que solo es perceptible en el nodo receptor, no en el nodo transmisor.

- **Exposed Terminal Problem (Problema del Terminal Expuesto)**

El problema por el cual un nodo transmisor A impide a otro nodo B transmitir, aunque el nodo B podría seguramente haber transmitido a cualquier otro excepto el nodo transmisor A.

### 4.5. MICRO DIVERSIDAD, MACRO DIVERSIDAD Y DIVERSIDAD IP

Ciertas interfases de aire (Por ejemplo, el Sistema de Telecomunicaciones Móviles Universales (UMTS), Red de acceso de radio terrestre (UTRAN) corriendo en modo Duplas por División en Frecuencia (FDD) requiere o por lo menos apoya la combinación de macrodiversidad. Esencialmente, esto se refiere al hecho de que un solo MN puede enviar y recibir sobre canales de radio independientes (“Ramas de diversidad”) al mismo tiempo; la información recibida sobre diferentes ramas es comparada y la que provenga de la mejor rama pasara a las capas superiores. Esto puede usarse tanto para mejorar el desempeño global, y para proporcionar un tipo de handover sin costuras a la capa 2, dado que una nueva rama puede ser agregada antes de que la antigua sea borrada. Ver también [6].

Es necesario diferenciar entre Combinación/Diversidad que ocurre en las capas físicas y enlace radio, donde la unidad de datos pertinente es la trama radio, y que ocurre en la capa 3, la capa de red, donde lo que es considerado es el propio paquete IP.

En las siguientes definiciones micro y macro diversidad se refieren a las capas protocolares debajo de la capa de red, y la diversidad IP se refiere a la capa de red.

- **Micro Diversity (Micro Diversidad)**

Por ejemplo, dos antenas en el mismo transmisor envían la misma señal al receptor sobre un camino ligeramente diferente para superar el desvanecimiento

- **Macro Diversity (Macro Divers dad)**

Acciones de duplicación o combinación que tienen lugar sobre APs multiples, posiblemente ligados a diferentes ARS. Esto puede requerir el apoyo de la capa de

red para mover las tramas radio entre las estaciones base y un punto central de combinación.

- **IP Diversity (Diversidad IP)**

Se refiere al proceso de duplicación de paquetes IP y enviarlos al receptor a través de más de un punto de conexión. Esto es semánticamente permitido por IP porque este no garantiza la exclusividad de los paquetes y se asumen los protocolos de nivel superior para eliminar los duplicados siempre que eso sea importante para la aplicación.

### 4.6. PAGING, MODOS Y ESTADOS DEL NODO MÓVIL

Los sistemas móviles pueden emplear el uso de estados del MN con el propósito de funcionar más eficientemente sin degradar el desempeño del sistema. El término “modo” también es común y significa lo mismo que “estado”.

Un MN siempre esta en uno de los siguientes tres estados:

- **Active State (Estado Activo)**

Cuando el AN conoce el SAR del MN y el MN puede enviar y recibir paquetes IP. La conexión de acceso puede no estar activa, pero la capa radio puede establecer uno sin la ayuda de la capa de red. El MN tiene una dirección IP asignada.

- **Dormant State (Estado Latente)**

Un estado en el cual el móvil restringe su capacidad de recibir tráfico IP normal reduciendo su supervisión de los canales radio. La AN conoce el Área de Pagina del MN, pero el MN no tiene ningún SAR y de esta manera los paquetes no pueden ser entregados al MN sin paging inicial de la AN. A menudo también es llamado Estado Ocioso (Idle State).

- **Time-slotted Dormant Mode (Modo Inactivo por periodos de tiempo)**

Una aplicación del modo inactivo en la cual el móvil alterna entre periodos de no escuchar ningún tráfico de radio y de escuchar tráfico. Las aplicaciones del modo inactivo por periodos de tiempo se sincronizan típicamente con la red para que la red pueda entregar los mensajes de paging al móvil durante los periodos de escucha.

- **Inactive State (Estado Inactivo)**

El MN no esta ni en Estado Activo ni Latente. El MN ya no esta escuchando para cualquier paquete, por lo menos no periódicamente, y no esta enviando paquetes. El MN puede estar apagado, o puede haber cerrado todas las interfaces para

conservar drásticamente la potencia, o puede estar fuera del rango de un punto de acceso radio. El MN no tiene necesariamente una dirección IP de acceso desde la AN.

**NOTA:** De hecho, así como el MN esta en uno de estos tres estados, la AN también almacena en que estado considera que el MN esta. Normalmente éstos son consistentes; las definiciones citadas anteriormente se asumen de esta manera.

Aquí están algunas definiciones adicionales para paging, teniendo en cuenta las anteriores definiciones de estados.

- **Paging (Canal de mensajería)**

Un procedimiento iniciado por la Red de Acceso para pasar un MN Latente a un estado activo. Como resultado del paging, el MN establece un SAR y las rutas IP son establecidas.

- **Location Updating (Actualización de la Ubicación)**

Un procedimiento iniciado por el MN, por el cual este le informa a la AN que ha pasado a una nueva área de paging.

- **Paging Area (Area de Paging)**

Una parte de la Red de Acceso, típicamente conteniendo un número de ARs/APs, los cuales corresponden a alguna área geográfica. La AN mantiene y actualiza una lista de todos los MN Latentes presentes en el área. Si el MN esta dentro del radio de cobertura del área en que podrá recibir mensajes de paging enviado dentro de esa área de paging.

- **Paging Area Registrations (Registros del Area de Paging)**

La señalización desde un nodo móvil modo latente hacia la red, por la que establece su presencia en una nueva área paging. De esta manera los registros de área paging permiten a la red mantener una idea aproximada de donde esta localizado el móvil.

- **Paging Channel (Canal de Paging)**

Un canal radio dedicado a la señalización de móviles modo latente para propósitos de paging. En la práctica, el canal de paging lleva solo el tráfico de control necesario para el enlace radio, aunque algunos protocolos de paging tienen disposición para llevar el trafico arbitrario (y de esta manera podría usarse potencialmente para llevar IP)

- **Traffic Channel (Canal de Traffic)**

El canal radio sobre el cual el trafico IP es típicamente enviado aun móvil activo. Este canal es usado para un móvil que esta activamente enviando y recibiendo

tráfico IP, y no está continuamente en un modo móvil latente. Para algunos protocolos de enlace radio, este puede ser el único canal disponible.

### 4.7. TRASLADO DEL CONTEXTO

- **Context (Context)**

La información sobre el estado actual de un servicio asociado a la ruta, requiere restablecer el servicio asociado a la ruta sobre una nueva subred sin tener que realizar el cambio completo de protocolo con el MN desde el principio.

- **Feature Context (Contexto Característico)**

La colección de información que representa el contexto para una característica dada. El contexto completo asociado con un MN es la colección de uno o más contextos característicos.

- **Context Transfer (Traslado del Contexto)**

El movimiento del contexto desde uno de los enrutadores u otra entidad de la red hacia otro, como un medio de re-establecer los servicios asociados a la ruta, en una nueva subred o colección de subredes.

- **Routing-related Service (Servicio Asociado a la Ruta)**

Una modificación al acuerdo de enrutamiento predeterminado hacia y desde el MN. Inicialmente establecer los servicios asociados a la ruta requiere usualmente un intercambio de protocolo con el MN. Un ejemplo de un servicio asociado a la ruta es la compresión de cabecera. El servicio puede también estar indirectamente asociado al enrutamiento, por ejemplo, la seguridad. La seguridad no puede afectar la decisión de reenvío de todos los enrutadores intermediarios, pero un paquete puede caerse si falla un chequeo de seguridad (no puede encriptarse, falla la autenticación, etc.). La caída de paquetes es básicamente una decisión del enrutamiento.

### 4.8. DESCUBRIMIENTO DE UN CANDIDATO A ENRUTADOR DE ACCESO

- **Capability of an AR (Capacidad de un AR)**

Una característica del servicio ofrecida por un AR que puede ser de interés para un MN cuando el AR está siendo considerado como un candidato handoff.

- **Candidate AR - CAR (AR Candidato)**

Un AR al cual el MN tiene una opción de realizar handoff a nivel IP. Esto significa que el MN tiene la interfase radio adecuada para conectar a un AP que es atendido por este AR, así como la cobertura de este AR se superpone con la del AR al cual el MN esta actualmente conectado.

- **Target AR - TAR (AR Designado)**

Una AR con el que se comienzan los procedimientos para el handoff de nivel IP del MN. El TAR se selecciona después de ejecutar un Algoritmo de Selección que tiene en cuenta las capacidades de los CARs, las preferencias del MN y cualquier otra política local.

### 4.9. TIPOS DE MOVILIDAD

Se puede diferenciar entre movilidad de host y de red, y varios tipos de movilidad de red. La terminología relacionada más a las aplicaciones como el Protocolo de Inicio de Sesión, como la movilidad personal, están fuera del alcance de este documento.

- **Host Mobility Support (Soporte de Movilidad de Host)**

Se refiere a la función de permitir a un nodo móvil cambiar su punto de conexión a la red, sin interrumpir la entrega de paquetes IP desde y hacia ese nodo. Puede haber diferentes sub-funciones que dependen de que nivel actual de servicio esta suministrandose; en particular, el soporte para movilidad de host usualmente implica modos de operación activo y latente, dependiendo de si el nodo tiene corriendo o no cualquier sesión. Los procesos de la Red de Acceso se requieren para seguir el punto actual de conexión de todos los MNs o establecerlo a voluntad. Se requiere la localización exacta y procesos de enrutamiento con el fin de mantener la integridad de la comunicación. La movilidad de host se denomina a menudo “Movilidad de Terminal”.

- **Network Mobility Support (Soporte de Movilidad de Red)**

Se refiere a la función de permitir a una red completa cambiar su punto de conexión a Internet, y de esta manera, su alcanzabilidad en la topología, sin interrumpir la entrega de paquetes IP desde y hacia esa red móvil.

Dos subcategorías de movilidad se pueden identificar dentro de la movilidad de host y la movilidad de red.

- **Global Mobility (Movilidad Global)**

Lo mismo que Macro movilidad.

- **Local Mobility (Movilidad Local)**

Lo mismo que Micro movilidad.

- **Macro Mobility (Macro-Movilidad)**

La movilidad sobre un área grande. Esta incluye soporte de movilidad y procedimientos asociados de registro de dirección, que se necesitan cuando un MN se mueve entre dominios IP. Handovers Entre- ANs típicamente involucran los protocolos de macro-movilidad. IP Móvil, puede verse como un medio para proporcionar macro-movilidad.

- **Micro Mobility (Micro-Movilidad)**

Movilidad sobre un área pequeña. Usualmente esto significa movilidad dentro de un dominio IP con un énfasis en el soporte para el modo activo que usa el handover, aunque también puede incluir los procedimientos del modo Latente. Los protocolos de Micro-movilidad sacan provecho del área de movimiento por movimientos limitados asociados a cambios y señalización en la red de acceso.

- **Local Mobility Management - LMM (Gestión de la Movilidad Local)**

La gestión de movilidad Local (LMM) es un término genérico para protocolos que tratan con la gestión de movilidad IP limitada dentro de la red de acceso. Mensajes LMM no se enrutan fuera de la red de acceso, aunque un handover puede activar mensajes de IP móvil a ser enviados a los nodos correspondientes y agentes locales.

### 5. TERMINOLOGIA ESPECÍFICA PARA EL ESTABLECIMIENTO DE UNA RED MOVIL AD-HOC

- **Cluster (Grupo)**

Un grupo de nodos situados dentro de la proximidad física cercana, generalmente todos dentro del alcance uno del otro, los cuales pueden ser agrupados con el fin de limitar la producción y propagación de información de enrutamiento.

- **Cluster Head (Cabeza de Grupo)**

Una Cabeza de Grupo es un nodo (a menudo elegido en el proceso de formación del grupo) que tiene conocimiento completo acerca de los miembros del grupo e información del estado de enlace en el grupo. Cada grupo debe tener una única Cabeza de Grupo.

- **Cluster Member (Miembro del Grupo)**

Todos los nodos dentro de un grupo excepto la Cabeza del Grupo son llamados miembros de ese grupo.

- **Convergence (Convergencia)**

El proceso de acercarse a un estado de equilibrio en el cual todos los nodos en la red están de acuerdo en una colección consistente de estado acerca de la topología de la red, y en el cual los mensajes de control hasta este momento son necesarios para establecer la consistencia de la topología de red.

- **Convergence Time (Tiempo de Convergencia)**

El tiempo que requiere una red para alcanzar la convergencia después de un evento (generalmente, el movimiento de un nodo móvil) que cambie la topología de red.

- **Laydown**

La localización física relativa de los nodos dentro de la red Ad-Hoc.

- **Pathloss Matrix (Matriz de Pérdidas de Trayectoria)**

Una matriz de los coeficientes que describen las pérdidas de trayectoria entre dos nodos cualesquiera en una red Ad-Hoc. Cuando los enlaces son asimétricos, la matriz también es asimétrica.

- **Scenario (Escenario)**

El conjunto de variables <Laydown, Matriz de Pérdidas de Trayectoria, Factor de Movilidad, Tráfico> que caracterizan una clase de redes Ad-Hoc.

### 6. TERMINOLOGIA RELACIONADA CON SEGURIDAD

Esta sección incluye terminología comúnmente usada alrededor de de redes móviles e inalámbricas. Solamente se presentara un subconjunto relacionado con movilidad de la terminología completa de seguridad.

- **Authorization-Enabling Extension (Extension Habilitando-Autorizacion)**

Una autenticación que hace un (registro) mensaje aceptable al último destinatario del mensaje de registro. Una Extensión Habilitando-Autorización debe contener un SPI (vea abajo) [10].

- **Mobility Security Association (Asociacion de Seguridad de Movilidad)**

Una colección de contextos de seguridad, entre un par de nodos los cuales pueden ser aplicados a los mensajes de protocolos relacionados con movilidad intercambiados entre ellos. En IP Móvil, cada contexto indica un algoritmo y modo de autenticación, un secreto (una llave compartida, o el apropiado par de llaves publica/privada), y un estilo de protección de la repetición en uso. Las asociaciones de seguridad de movilidad se pueden almacenar separadamente de la base de datos de la política de seguridad IPsec del nodo (SPD) [10].

- **Registration Key (Llave de Registro)**

Una llave usada en la asociación de seguridad de movilidad entre un nodo móvil y un agente foráneo. Una llave del registro se utiliza típicamente solamente una vez o muy pocas veces, y solamente para los propósitos de verificar un volumen pequeño de los datos de autenticación [12].

- **Security Context (Contexto de Seguridad)**

Un contexto de seguridad entre dos nodos define la manera en que dos nodos escogen autenticarse mutuamente, e indica un algoritmo y un modo de autenticación.

- **Security Parameter Index - SPI (Indice del Parámetro de Seguridad)**

Un índice que identifica un contexto de seguridad entre un par de enrutadores entre los contextos disponibles en la Asociación de Seguridad de Movilidad.

La especificación de IPv6 Móvil incluye más terminología de seguridad relacionada con todo lo concerniente a MIPv6 [9]. La Terminología sobre el mecanismo Challenge/Response (*Desafío/Respuesta* - Una técnica común de autenticación por medio de la cual un individuo es incitado, *el desafío*, a proporcionar una cierta información privada, *la respuesta*) MIP puede encontrarse en [11].

## **ANEXO B:**

### **LAS EXTENSIONES DE IPv6 MÓVIL Y SUS MENSAJES**

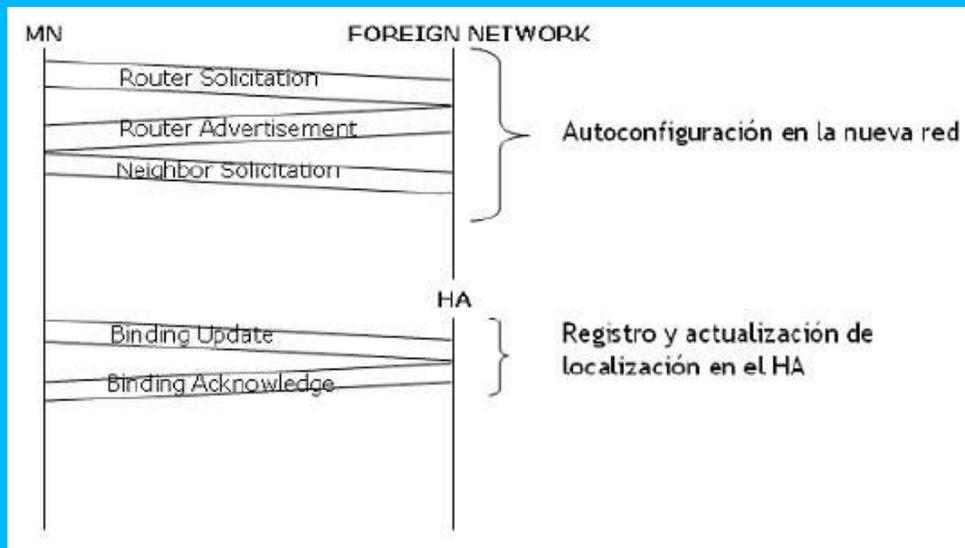
## 1. INTRODUCCION

En este anexo se comentan detalladamente los mensajes intercambiados entre un terminal móvil y la red cuando el MN se cambia de Access Router para los protocolos de movilidad MIPv6, HMIPv6, FMIPv6 predictivo y reactivo, F-HMIPv6.

## 2. TRASPASO USANDO EL PROTOCOLO MIPV6

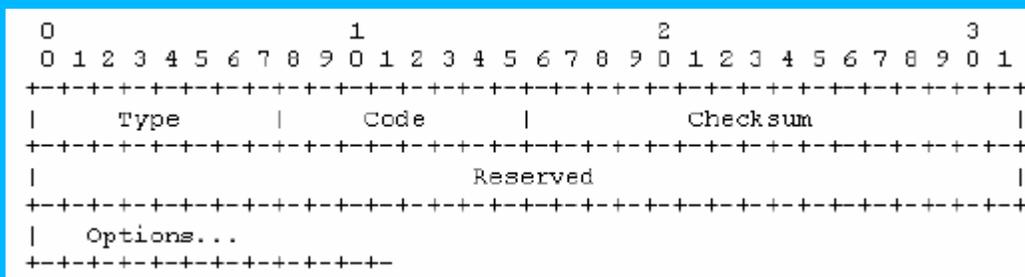
- En este caso el MN envía 3 mensajes:
  - *Router Solicitation*: entre 48 y 56 bytes.
  - *Neighbor Solicitation*: entre 64 y 72 bytes.
  - *Binding Update*: entre 56 y 96 bytes.
- En este caso el MN recibe 2 mensajes:
  - *Router Advertisement*: entre 56 y 104 bytes.
  - *Binding Acknowledge*: entre 56 y 72 bytes.

Figura B-1: Diálogo de Traspaso con Binding al HA



### 2.1. ROUTER SOLICITATION

Figura B-2 : Mensaje de Router Solicitation.



- **Campos Fijos**

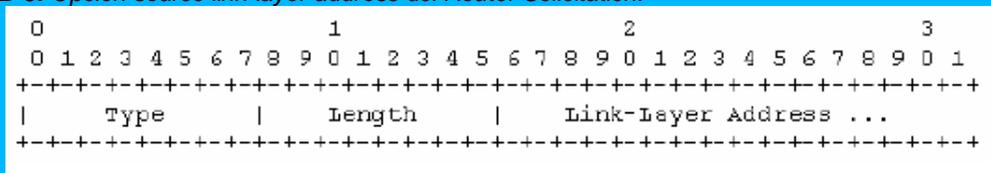
- **Type:** 1 byte.
- **Code:** 1 byte.
- **Checksum:** 2 bytes.
- **Reserved:** 4 bytes.

- **Campos Variables:**

- **Options:**
  - *Source link-layer address*

### 2.1.1. Source link-layer address

*Figura B-3: Opción source link-layer address del Router Solicitation.*



**Type:** 1 byte.

**Length:** 1 byte.

**Link-Layer Address:** 6 bytes (para IEEE 802). [IPv6-ETHER].

TAMAÑO MÍNIMO: 48 bytes = 40 de cabecera IPv6 + 8 de cabecera ICMPv6.

TAMAÑO MÁXIMO: 56 bytes = 40 de cabecera IPv6 + 8 de cabecera ICMPv6 + 8 de opciones.

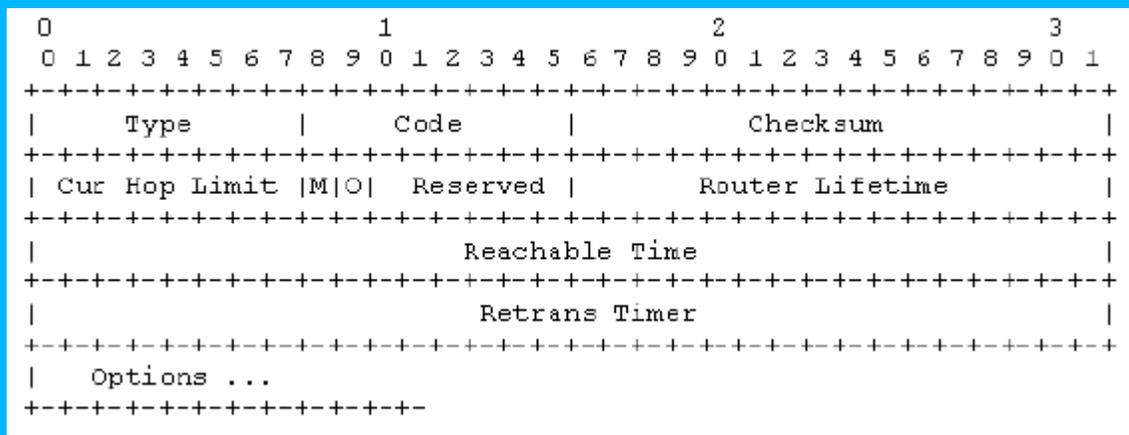
## 2.2. ROUTER ADVERTISEMENT

- **Campos Fijos**

- **Type:** 1 byte.
- **Code:** 1 byte.
- **Checksum:** 2 bytes.
- **Cur Hop Limit:** 1 byte.
- **M:** 1 bit.
- **O:** 1 bit.
- **Reserved:** 6 bits.
- **Router Lifetime:** 2 bytes.

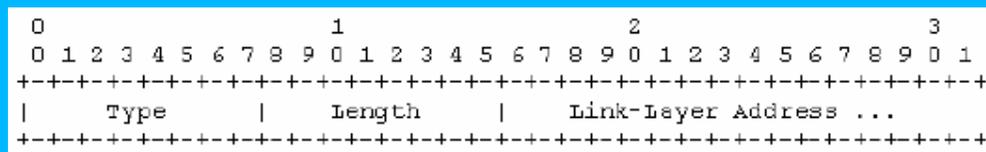
- **Reachable Time:** 4 bytes.
  - **Retrans Timer:** 4 bytes.
- **Campos Variables**
    - **Options:**
      - *Source link-layer address*
      - *MTU*
      - *Prefix Information*

**Figura B-4 :** Mensaje de Router Advertisement.



### 2.2.1. Source link-layer address

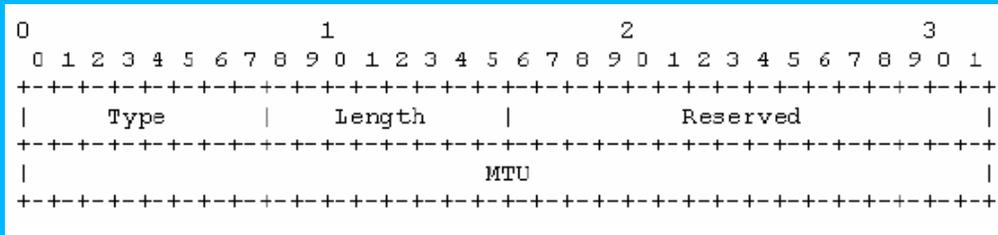
**Figura B-5:** Opción Source Link-layer Address del Router Advertisement.



- Type:** 1 byte.
- Length:** 1 byte.
- Link-Layer Address:** 6 bytes (para IEEE 802). [IPv6-ETHER].

### 2.2.2. MTU

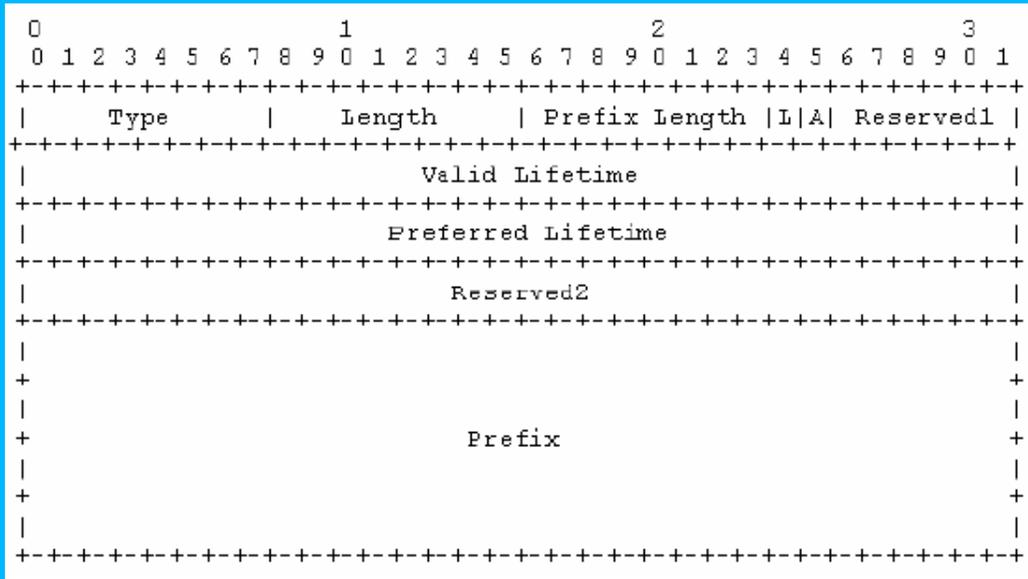
Figura B-6: Opción MTU del Router Advertisement.



**Type:** 1 byte.  
**Length:** 1 byte.  
**Reserved:** 2 bytes.  
**MTU:** 4 bytes.

### 2.2.3. Prefix information

Figura B-7: Opción Prefix Information del Router Advertisement.

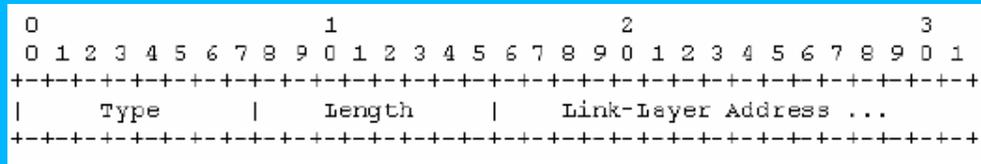


**Type:** 1 byte.  
**Length:** 1 byte.  
**Prefix Length:** 1 byte.  
**L:** 1 bit.  
**A:** 1 bit.  
**Reserved1:** 6 bits.  
**Valid Lifetime:** 4 bytes.  
**Preferred Lifetime:** 4 bytes.  
**Reserved2:** 4 bytes.



### 2.3.1. Source link-layer address

Figura B-9: Opción Source link-layer address del Neighbor solicitation.



**Type:** 1 byte.

**Length:** 1 byte.

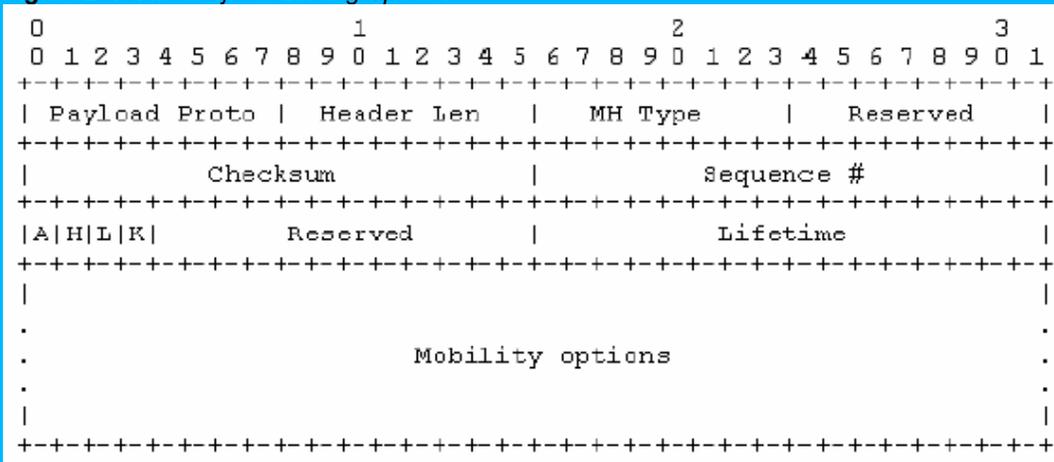
**Link-Layer Address:** 6 bytes (para IEEE 802). [IPv6-ETHER].

TAMAÑO MÍNIMO: 64 bytes 40 de cabecera IPv6 + 24 de cabecera ICMPv6.

TAMAÑO MÁXIMO: 72 bytes 40 de cabecera IPv6 + 24 de cabecera ICMPv6 + 8 de opciones.

### 2.4. BINDING UPDATE

Figura B-10: Mensaje de Binding Update.



- **Campos Fijos**
  - **Payload Proto:** 1 byte.
  - **Header Len:** 1 byte.
  - **MH Type:** 1 byte.
  - **Reserved:** 1 byte.
  - **Checksum:** 2 bytes.
  - **Sequence #:** 2 bytes.
  - **A:** 1 bit.
  - **H:** 1 bit.

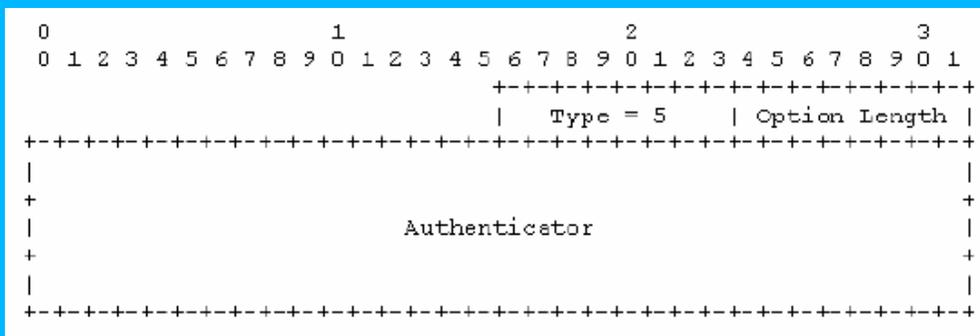
- **L:** 1 bit.
- **K:** 1 bit.
- **Reserved:** 12 bits.
- **Lifetime:** 2 bytes.

- **Campos Variables**

- **Mobility Options:**
  - *Binding Authorization Data*
  - *Nonce Indices*
  - *Alternate Care-of Address*

### 2.4.1. Binding authorization data

*Figura B-11: Mobility option: Binding Authorization Data del Binding Update*

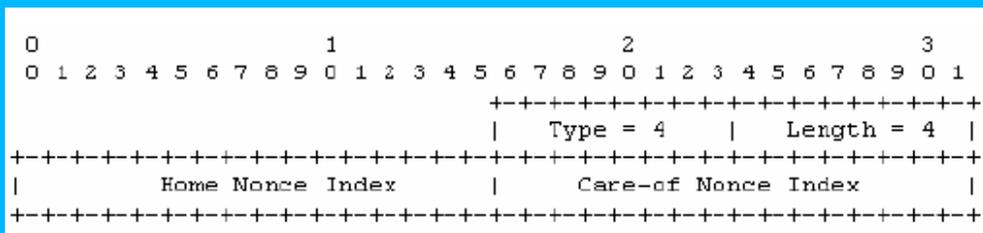


**Type:** 1 byte.  
**Option Length:** 1 byte.  
**Authenticator:** 12 bytes.  
(+2 bytes de padding)

### 2.4.2. Nonce indices

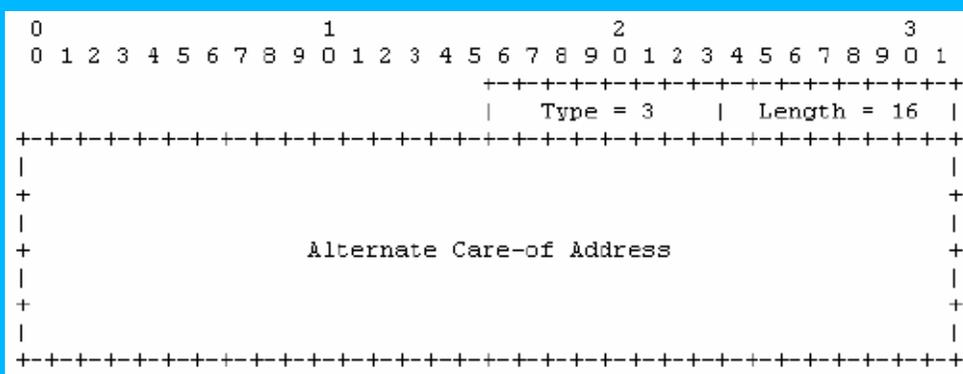
**Type:** 1 byte.  
**Length:** 1 byte.  
**Home Nonce Index:** 2 bytes.  
**Care-of Nonce Index:** 2 bytes.  
(+2 bytes de padding)

Figura B-12: Mobility option: Nonce Indices del Binding Update.



### 2.4.3. Alternate care-of address

Figura B-13: Mobility Option: Alternate Care-of Address del Binding Update.



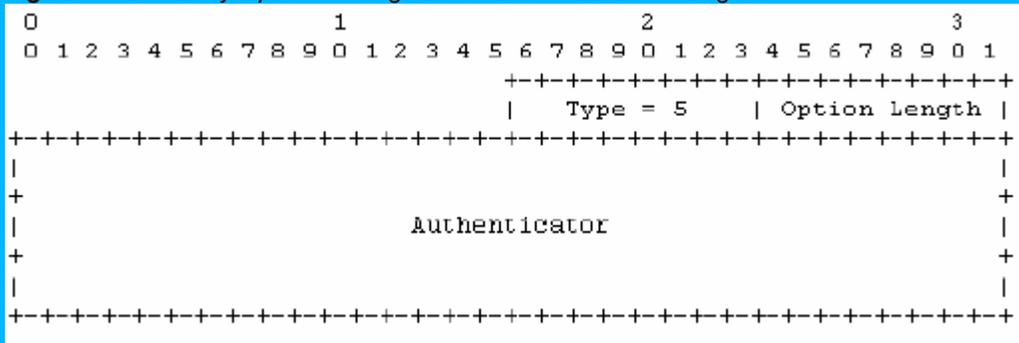
**Type:** 1 byte.  
**Length:** 1 byte.  
**Alternate Care-of Address:** 16 bytes.  
 (+2 de padding)

**TAMAÑO MÍNIMO:** 56 bytes 40 de cabecera IPv6 + 12 de cabecera de movilidad (sin contar mobility options) + 4 de padding que son necesarios cuando no hay mobility options.

**TAMAÑO MÁXIMO:** 96 bytes 40 de cabecera IPv6 + 12 de cabecera de movilidad + 44 de opciones.

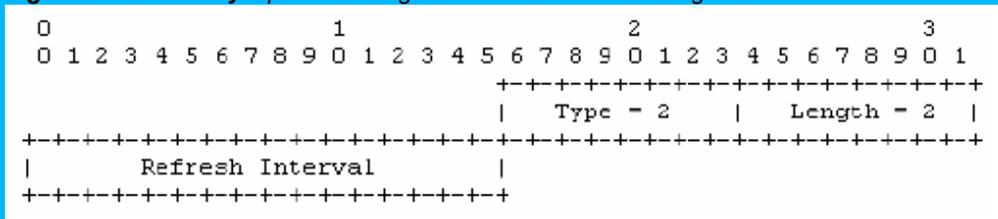


**Figura B-15:** Mobility Option: Binding Authorization Data del Binding Ack.



**2.5.2. Binding refresh advice**

**Figura B-16:** Mobility Option: Binding Refresh Advice del Binding Ack.



- Type:** 1 byte.
- Length:** 1 byte.
- Refresh Interval:** 2 bytes.  
(+ 2 bytes de padding)

**TAMAÑO MÍNIMO:** 56 bytes 40 de cabecera IPv6 + 12 de cabecera de movilidad + 4 de padding que son necesarios cuando no hay mobility options.

**TAMAÑO MÁXIMO:** 72 bytes 40 de cabecera IPv6 + 12 de cabecera de movilidad + 20 de opciones.

### 3. HIERARCHICAL MOBILE IPv6 – HMIPv6

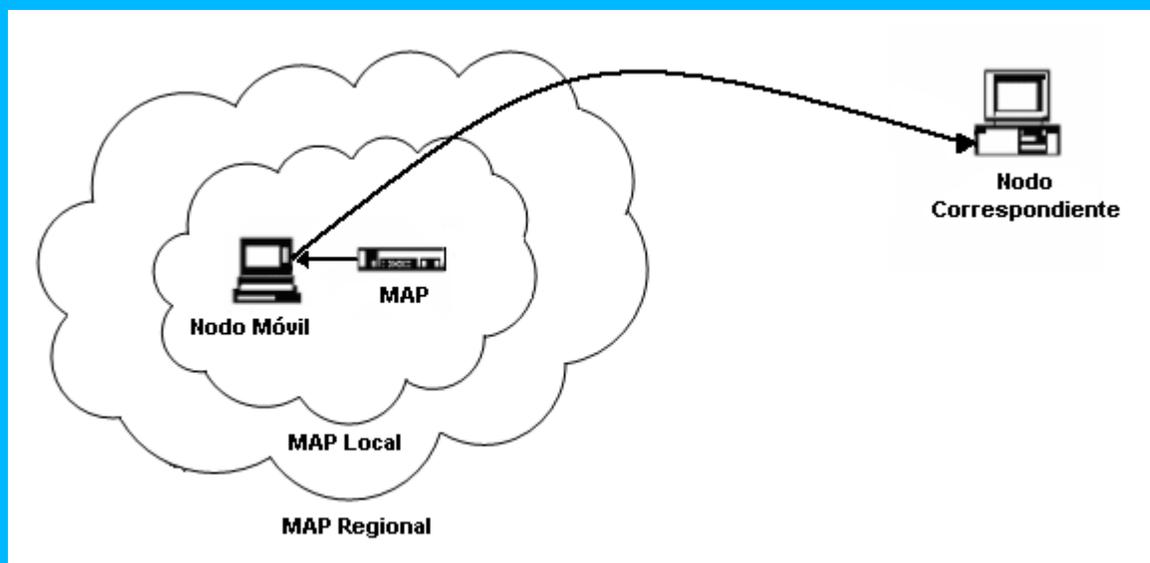
El protocolo Mobile IPv6 jerárquico es una nueva propuesta basada en Mobile IPv6 desarrollada para reducir la cantidad de señalización requerida y mejorar la velocidad de los traspasos en las conexiones móviles. HMIPv6 es una propuesta del Internet Engineering Task Force (IETF), creada al observar que MIPv6 define todos los medios para manejar la movilidad globalmente (macromovilidad), pero no trata por separado la movilidad local (micro-movilidad). Por tanto, se hace un uso ineficaz de recursos en el caso de haber movilidad local.

HMIPv6 agrega otro nivel a lo establecido en MIPv6, que separa los dos tipos de movilidad (local y global). En HMIPv6 la movilidad global es manejada por los mecanismos establecidos en MIPv6, mientras que los traspasos locales se manejan localmente.

En HMIPv6, se crea un nuevo nivel de jerarquía con la creación de un nodo denominado MAP, que hace la función del HA pero localmente, el MAP se puede situar donde quiera dentro del nivel más bajo de la jerarquía que se establece. Y cuando un nodo móvil cambia de AR sin salir del dominio MAP, no tendrá que notificárselo al HA, únicamente al MAP, consiguiendo disminuir el tráfico entre MN y HA, esta es la ventaja más importante del HMIPv6. Se puede decir que, HMIPv6 es más eficiente que MIPv6 simple ya que logra separar la movilidad global de la local y aplica el tipo de traspaso adecuado para cada caso.

La siguiente gráfica representa el escenario de trabajo que se establece con el uso de MIPv6 Jerárquico cuando un nodo móvil quiere mantener una comunicación con un nodo remoto:

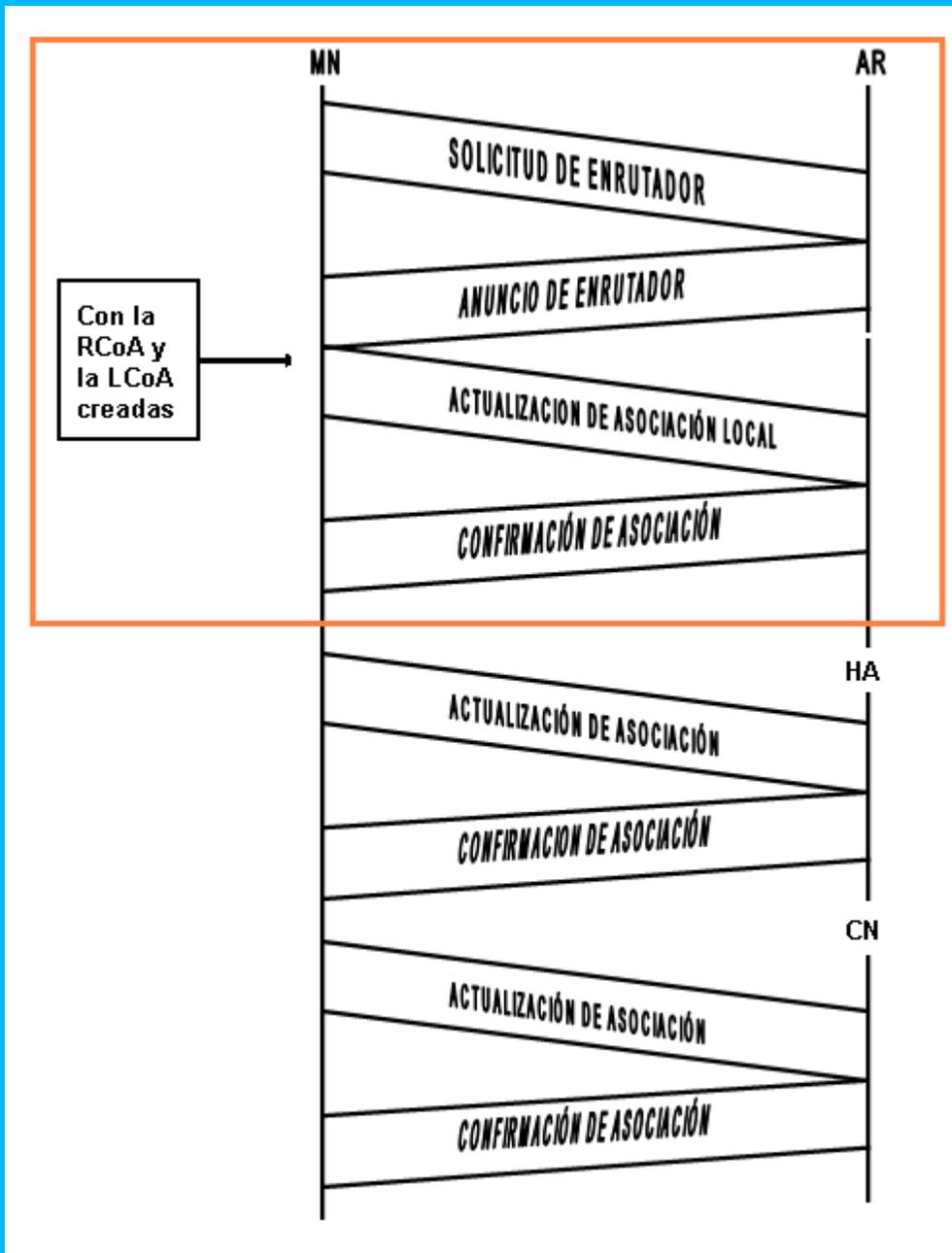
*Figura B-17: Escenario HMIPv6*



A continuación se puede observar el diálogo de localización que se establece entre el nodo móvil y la red, usando MIPv6 jerárquico, la parte de diálogo contenido en el recuadro

aranja es el intercambio de mensajes que se cursa cuando el nodo móvil se cambia de AR pero sin salir del dominio MAP en que se encuentra, en caso de que el traspaso fuera tanto de AR como de dominio MAP, el nodo tendría que notificarlo haciendo un binding al HA también, es decir, cursar todo el diálogo que se expone a continuación:

Figura B-17: Dialogo en MIP Jerárquico



#### 4. FAST MOBILE IPv6 - FMIPv6

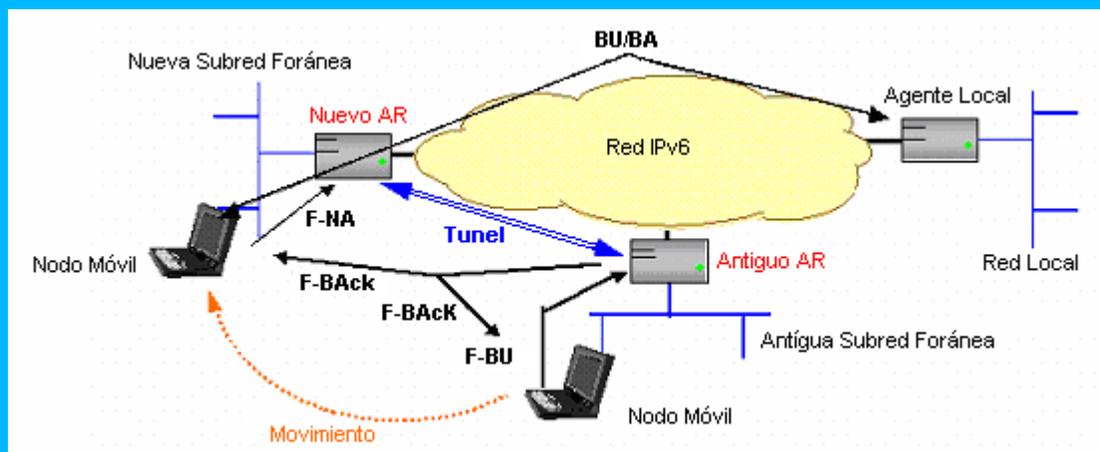
Para esta extensión de MIPv6, existen dos tipos de escenarios: FMIPv6 predictivo y FMIPv6 reactivo. El objetivo principal del mecanismo de “traspasos rápidos” sobre MIPv6, es la elección y configuración de una nueva CoA, antes de que el nodo móvil entre en una nueva subred IP, de manera que, cuando se produzca la conexión al nuevo AR esté disponible para usar la nueva CoA. La solución básica que aporta el Fast MIPv6 es la minimización del *handover latency*, que es el tiempo en que el nodo móvil permanece sin enviar ni recibir tráfico desde que se desconecta de un AR hasta que establece conexión con un nuevo AR.

Lo más importante es configurar una dirección temporal (CoA) nueva antes de que el nodo se desconecte de su antiguo AR (oldAR), entonces, cuando el nodo móvil haya establecido una conexión con el nuevo AR (newAR) puede continuar sus comunicaciones con la nueva dirección, ya conocida. Si este registro anticipado de CoA fallara, siempre se podría recurrir a un proceso de traspaso “tradicional”.

El establecimiento de la nueva CoA antes del movimiento de un nodo móvil implica la predicción del movimiento que realizará el nodo. Esta predicción se puede hacer a través de los mensajes intercambiados en la capa física o simplemente por la información relevante contenido en la capa 2 (medida del nivel de señal, etc.). El objetivo de este mecanismo es realizar el traspaso a nivel de red (IP) antes de finalizar el traspaso a nivel de enlace (capa 2),

En el siguiente gráfico se puede apreciar el escenario y el tráfico de localización establecido para Fast Mobile IPv6:

**Figura B-18:** Es cenario FMIPv6



En la fase inicial del traspaso, tanto para FMIPv6 con escenario predictivo como para FMIPv6 con escenario reactivo, el nodo móvil debe enviar a su antiguo AR (oldAR) un mensaje llamado “Routers Solicitation for Proxy”, en este mensaje el nodo móvil debe indicar la dirección de la capa de enlace (Link Layer Address) o bien el identificador del punto de acceso al que se quiere mover. El AR antiguo (oldAR) responderá con un “Proxy Router Advertisement” que se empleará para generar la nueva CoA.

En la segunda fase del traspaso, es cuando se diferencia el comportamiento del nodo móvil en predictivo o reactivo. Si es predictivo, una vez completada la fase de obtención de CoA, el nodo móvil envía un mensajes fase binding update al oldAR para actualizar la CoA y espera a recibir un Fast binding Acknowledge antes de desconectarse de su oldAR, es cuando se establece el túnel bidireccional entre el AR nuevo (newAR) y el antiguo (oldAR). Si es reactivo, antes de hacer el binding, el nodo móvil con la CoA generada, se desconecta de su red y se engancha al nuevo punto de acceso. Y una vez conectado al nuevo AR, es cuando hará el binding y completará la tercera y última fase.

La última fase del traspaso es el reenrutamiento de los paquetes desde el oldAR al newAR y es igual para los dos posibles escenarios (predictivo o reactivo).

Todo este proceso se puede entender mejor a partir de las siguientes gráficas:

**Figura B-19:** Diálogo en Fast MIPv6 con escenario predictivo

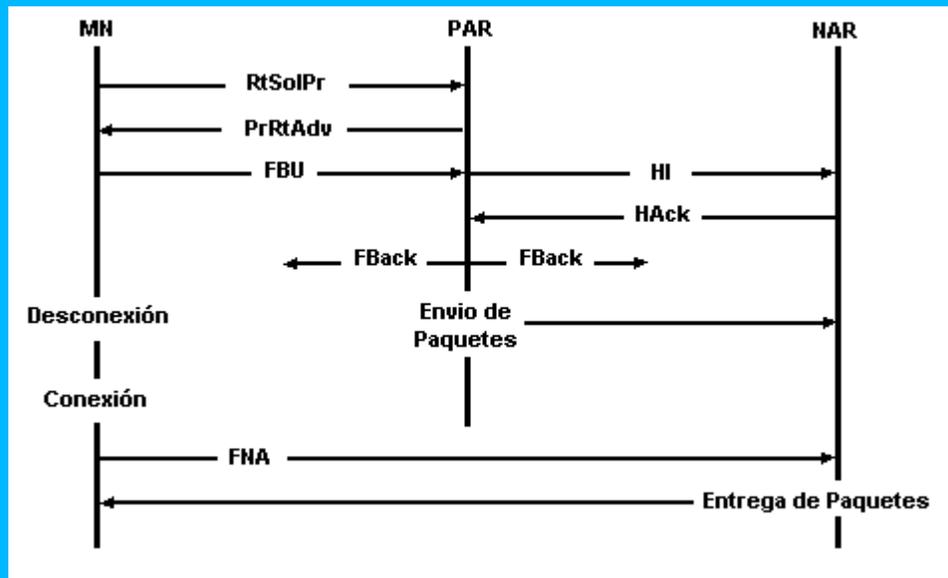
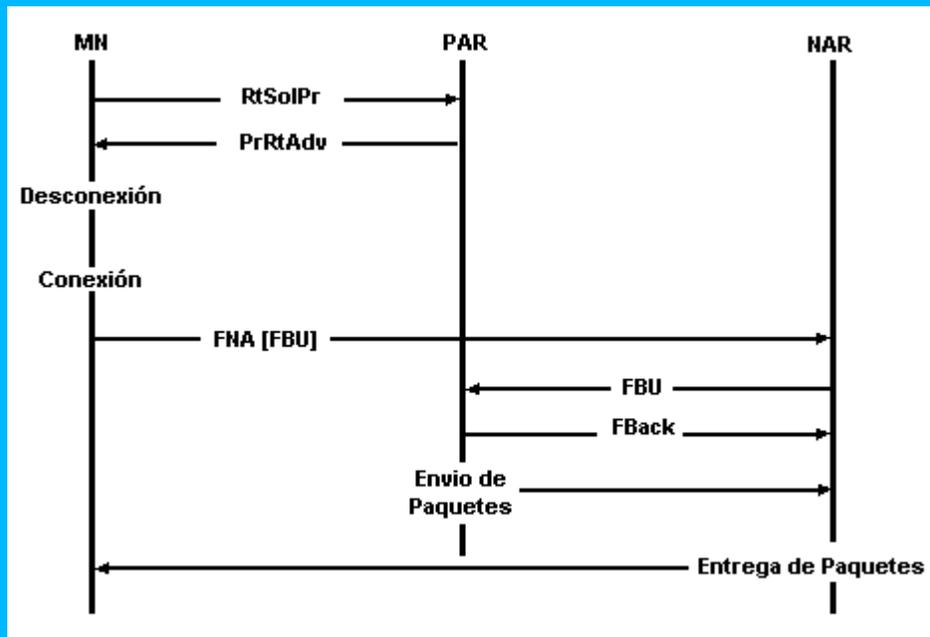


Figura B-20: Diálogo en Fast MIPv6 con escenario reactivo



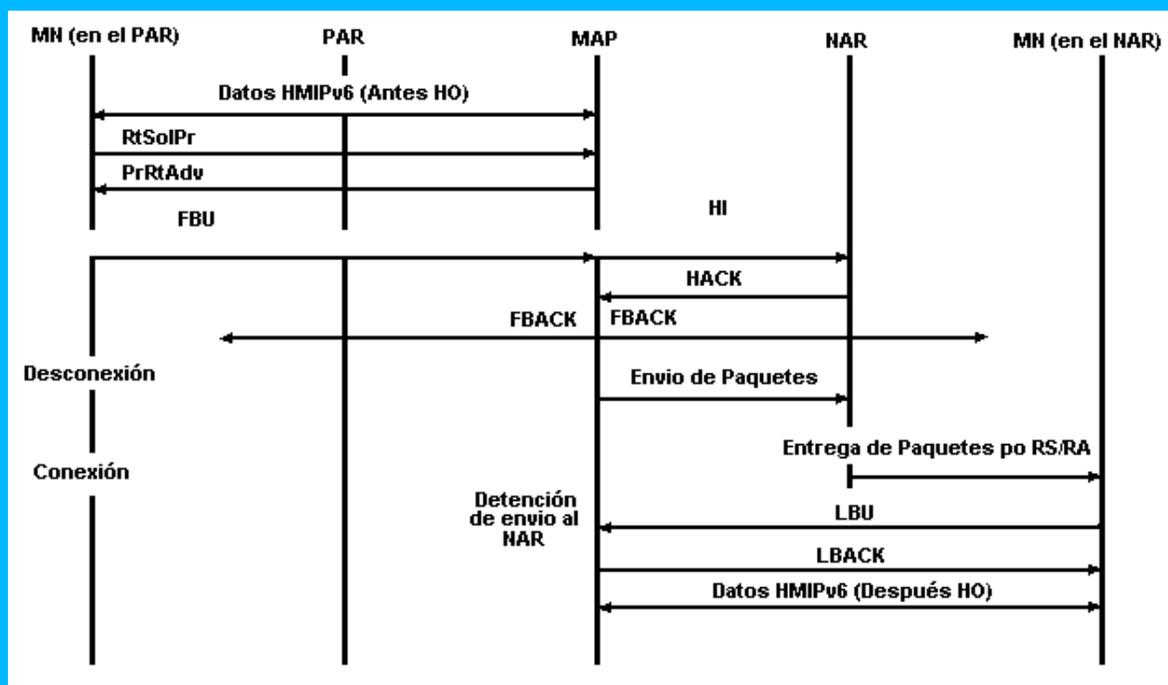
### 5. FAST HANDOVER FOR HIERARCHICAL MIPv6 – HMIPv6

Todas las ventajas que suman individualmente las dos extensiones de MIPv6 explicadas anteriormente, pueden verse incrementadas si se combinan entre sí, es decir, aplicar el traspaso rápido (Fast handover) sobre una red MIPv6 con arquitectura jerárquica.

El beneficio más importante de combinar FMIPv6 y HMIPv6 es la disminución del “*handover latency*” (tiempo que permanece el terminal sin poder enviar ni recibir tráfico, debido a que está intercambiando mensajes de localización con la red para actualizar su posición). Esta reducción se consigue aplicando el mecanismo de traspaso FMIPv6 pero en lugar de enviar los mensajes al Home Agent, se envían al MAP. Esta es una gran ventaja que, a efectos de mensajes enviados y recibidos por el terminal, no es apreciable pues se intercambian el mismo número de mensajes que si se aplica únicamente FMIPv6. La ventaja conseguida es en el tiempo.

En F-HMIPv6 el túnel para el Fast handover se establece entre el MAP y el NewAR, en lugar de ser entre el OldAR y el NewAR. En F-HMIPv6, se reutilizan los mismos mensajes de localización que en FMIPv6: RrSolPr, PrRtAdv, FBU, FBACk pero todos entre terminal y MAP. En el siguiente gráfico se puede observar el diálogo establecido entre nodo móvil y MAP y entre MAP y NewAR en este tipo de traspaso:

Figura B-21: Dialogo en Fast HMIPv6



## 6. TRASPASO HMIPv6 CON BINDING AL MAP, HA Y CN

- En este caso el MN envía 4 mensajes:
  - *Router Solicitation*: entre 48 y 56 bytes.
  - *Local Binding Update*: entre 56 y 96 bytes
  - *Binding Update*: entre 56 y 96 bytes cada uno. (2)
- En este caso el MN recibe 4 mensajes:
  - *Router Advertisement*: entre 56 y 128 bytes.
  - *Binding Acknowledge*: entre 56 y 72 bytes cada uno. (3)

### 6.1. ROUTER SOLICITATION

Mensaje de 48 a 56 bytes de longitud.

El formato y tamaño de este mensaje está explicado en la sección 2.1. de este mismo documento.

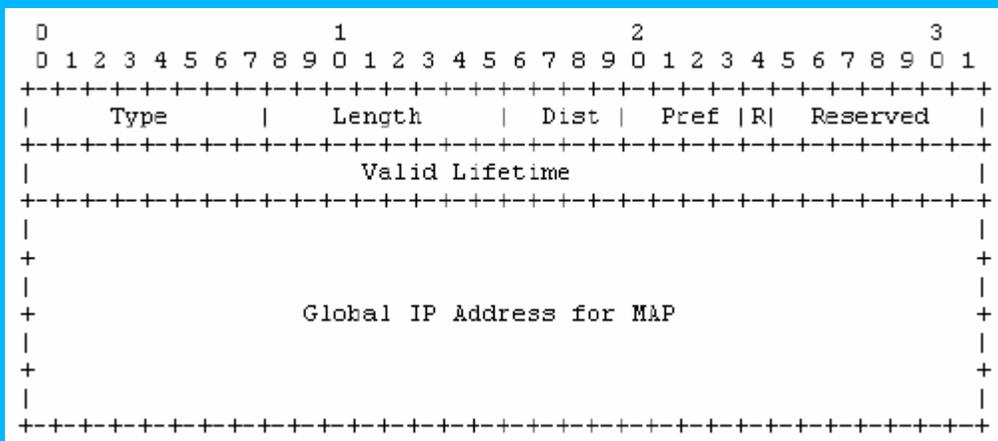
### 6.2. ROUTER ADVERTISEMENT

Este mensaje está explicado en la sección 2.2. de este mismo documento. La única diferencia a resaltar es la existencia de una opción que en diálogo de MIPv6 no se requiere: Map Option

#### 6.2.1. MAP Option

Con está opción el MN puede formar la dirección RCoA.

**Figura B-22** : MAP option del Router Advertisement.



**Type:** 1 byte.  
**Length:** 1 byte.  
**Dist:** 4 bits.  
**Pref:** 4 bits.  
**R:** 1 bit.  
**Reserved:** 7 bits.  
**Valid Lifetime:** 4 bytes.  
**Global IP Address for MAP:** 16 bytes.

Todas las demás opciones explicadas con anterioridad se mantienen iguales:

- "Source link-layer address" : 8 bytes
- "MTU" : 8 bytes
- "Prefix Information": 32 bytes.
- TAMAÑO MÍNIMO: 56 bytes = 40 de cabecera IPv6 + 16 de cabecera ICMPv6.
- TAMAÑO MÁXIMO: 128 bytes = 40 de cabecera IPv6 + 16 de cabecera ICMPv6 + 72 de opciones.

### 6.3. LOCAL BINDING UPDATE

Mensaje de 56 a 96 bytes de longitud.

Este mensaje tiene una ligera diferencia con el binding update que se hace con el HA o con el CN, es el bit M que nos indica si este mensaje forma parte de una MAP Registration, por lo demás es exactamente igual al Binding Update anteriormente explicado en la sección 2.4. del presente documento.

### 6.4. BINDING UPDATE

Mensaje de 56 a 96 bytes de longitud.

El formato y tamaño de este mensaje está explicado en la sección 2.4. de este mismo documento.

### 6.5. BINDING ACKNOWLEDGE

Mensaje de 56 a 72 bytes de longitud.

El formato y tamaño de este mensaje está explicado en la sección 2.5 de este mismo documento.

### 7. TRASPASO HMIPV6 CON BINDING AL MAP

#### 7.1. INTERCAMBIO DE MENSAJES DESDE EL MN SIN CAMBIO DE DOMINIO MAP

Cuando un MN se mueve dentro de un dominio MAP pero sin salirse, el HA no tiene porque enterarse de la posición exacta del nodo. De manera que el intercambio de mensajes que se genera llega solamente al MAP que es el único nodo que ha de conocer la posición exacta del MN en cada momento. Por tanto, el intercambio de mensajes cuando no se produce un cambio de MAP es el que está seleccionado en el recuadro naranja. Y el formato y tamaño de los mensajes está explicado con detenimiento en páginas anteriores del presente documento.

- En este caso el MN envía 2 mensajes:
  - *Router Solicitation*: entre 48 y 56 bytes.
  - *Local Binding Update*: entre 56 y 96 bytes.
- En este caso el MN recibe 2 mensajes:
  - *Router Advertisement*: entre 56 y 128 bytes.
  - *Binding Acknowledge*: entre 56 y 72 bytes.

## 8. TRASPASO CON FMIPV6

### 8.1. ESCENARIO PREDICTIVO

- En este caso el MN envía tres mensajes:
  - *Router Solicitation for Proxy Advertisement (RtSolPr)*: entre 48 y 72 bytes.
  - *Fast Binding Update (FBU)*: entre 52 y 92 bytes.
  - *Fast Neighbor Advertisement (FNA)*: entre 48 y 68 bytes.
- En este caso el MN recibe dos mensajes:
  - *Proxy Router Advertisement (PrRtAdv)*: entre 48 y 144 bytes.
  - *Fast Binding Acknowledge*: entre 52 y 72 bytes.

Además de estos mensajes, se envían entre PAR y NAR los siguientes mensajes:

- Desde PAR a NAR:
  - *Handover Initiate (HI)*: entre 48 y 100 bytes.
  - *Fast Binding Acknowledge*: entre 52 y 72 bytes.
- Desde NAR a PAR:
  - *Handover Acknowledge*: entre 48 y 68 bytes.

### 8.2. ESCENARIO REACTIVO

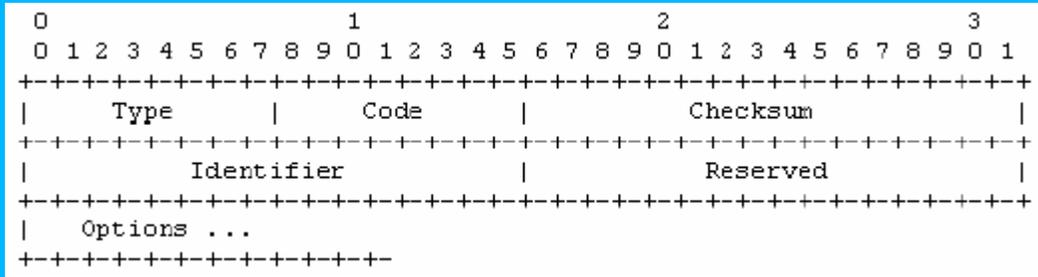
- En este caso el MN envía dos mensajes:
  - *Router Solicitation for Proxy Advertisement (RtSolPr)* : entre 48 y 72 bytes.
  - *Fast Neighbor Advertisement (FNA)*: entre 48 y 68 bytes.
- En este caso el MN recibe un mensaje:
  - *Proxy Router Advertisement (PrRtAdv)*: entre 48 y 144 bytes.

Además de estos mensajes, se envían entre PAR y NAR los siguientes mensajes:

- Desde PAR a NAR:
  - *Fast Neighbor Advertisement (FNA)*: entre 48 y 68 bytes.
  - *Fast Binding Acknowledge*: entre 52 y 72 bytes.
- Desde NAR a PAR:
  - *Fast Binding Update (FBU)*: entre 52 y 92 bytes.

8.2.1. Router solicitation for proxy advertisement (RtSolPr)

Figura B-23: Mensajes Router Solicitation for Proxy Advertisement.



• **Campos Fijos**

**Type:** 1 byte.

**Code:** 1 byte.

**Checksum:** 2 bytes.

**Identifier:** 2 bytes.

**Reserved:** 2 bytes.

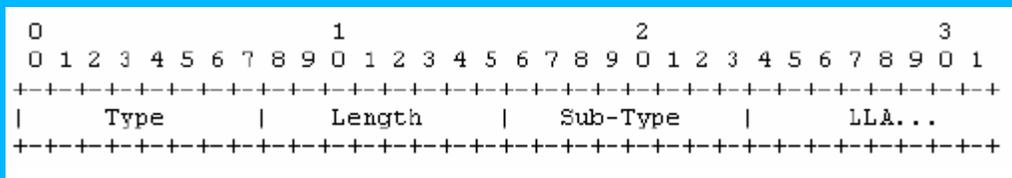
• **Campos Variables**

**Options:**

- Source Link-Layer Address.
- New Attachment Point Link-Layer Address.

Con el siguiente formato y tamaño las dos opciones:

Figura B-23: Formato del campo Options.



**Type:** 1 byte.

**Length:** 1 byte.

**Sub-Type:** 1 byte.

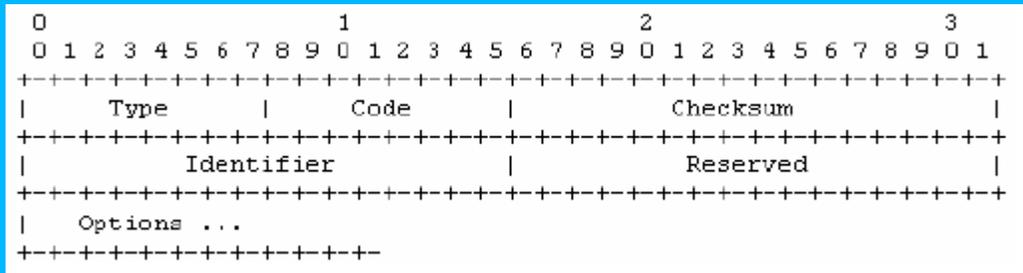
**Link-Layer Address:** 6 bytes (para IEEE 802). [IPv6-ETHER]. (+9 bytes de padding).

TAMAÑO MÍNIMO: 48 bytes = 40 de cabecera IPv6 + 8 de cabecera ICMPv6.

TAMAÑO MÁXIMO: 72 bytes = 40 de cabecera IPv6 + 8 de cabecera ICMPv6 + 24 de opciones.

### 8.2.2. Proxy router advertisement (PrRtAdv)

Figura B-24 : Mensajes Proxy Router Advertisement.



- **Campos Fijos**

- **Type:** 1 byte.
- **Code:** 1 byte.
- **Checksum:** 2 bytes.
- **Identifier:** 2 bytes.
- **Reserved:** 2 bytes.

- **Campos Variables**

- **Options:**
  - *New Router's IP Address.*
  - *New CoA Option.*

Con el siguiente formato y tamaño las dos opciones:

Figura B-25: Formato del campo Options.

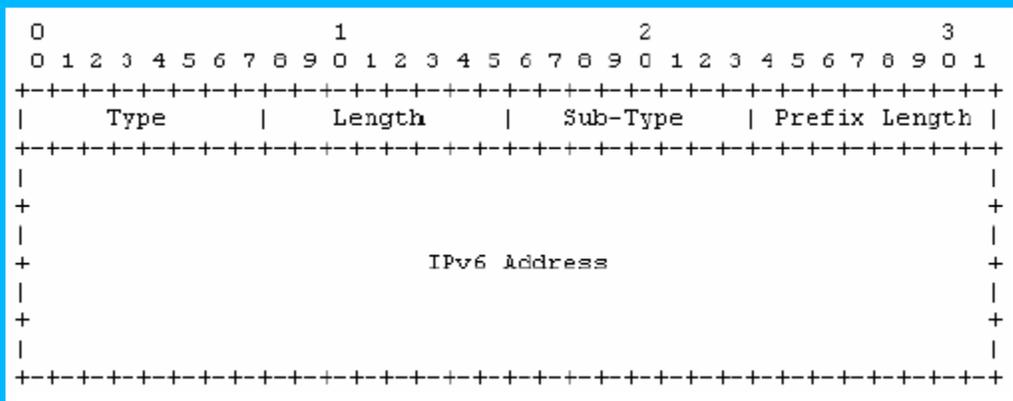
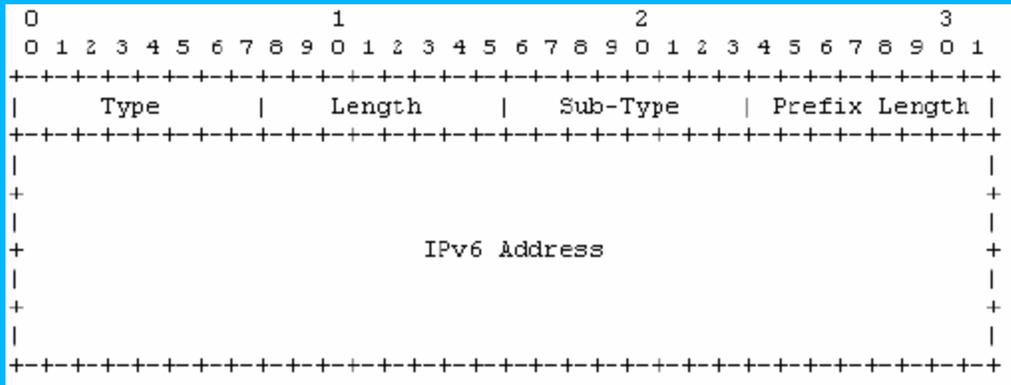






Figura B-29: Mobility Options del Fast Binding Update.



**Type:** 1 byte.

**Length:** 1 byte.

**Sub-type:** 1 byte.

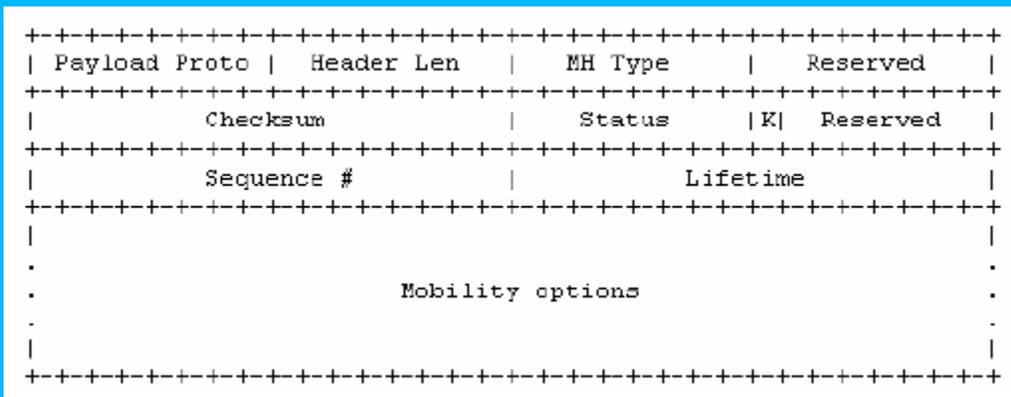
**Prefix Length:** 1 byte.

**IPv6 Address:** 16 bytes.

- TAMAÑO MÍNIMO: 52 bytes 40 cabecera IPv6 + 12 de cabecera de movilidad.
- TAMAÑO MÁXIMO: 92 bytes = 40 de cabecera IPv6 + 12 de cabecera de movilidad + 40 de Mobility Options.

#### 8.4. FAST BINDING ACKNOWLEDGE (FBAck)

Figura B-30: Mensajes Fast Binding Acknowledge.



- **Campos Fijos**

**Payload Proto:** 1 byte.

**Header Len:** 1 byte.

**MH Type:** 1 byte.  
**Reserved:** 1 byte.  
**Checksum:** 2 bytes.  
**Status:** 1 byte.  
**K:** 1 bit.  
**Reserved:** 7 bits.  
**Sequence #:** 2 bytes.  
**Lifetime:** 2 bytes.

- **Campos Variables**

**Mobility Options:**

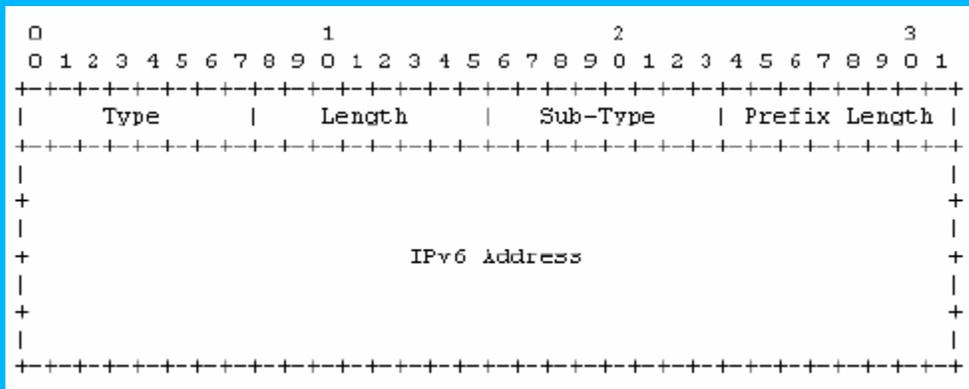
- *Alternate Care-of Address.*

**8.4.1. Alternate care-of address**

**Type:** 1 byte.  
**Length:** 1 byte.  
**Sub-type:** 1 byte.  
**Prefix Length:** 1 byte.  
**Ipv6 Address:** 16 bytes.

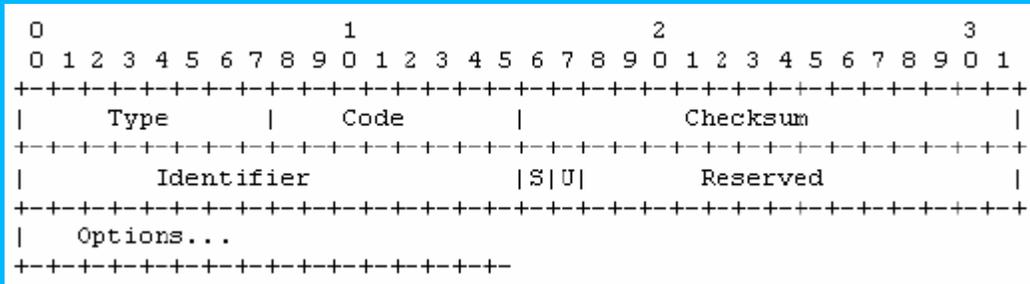
**TAMAÑO MÍNIMO:** 52 bytes 40 cabecera IPv6 + 12 de cabecera de movilidad.  
**TAMAÑO MÁXIMO:** 72 bytes 40 de cabecera IPv6 + 12 de cabecera de movilidad + 20 de Mobility Options.

*Figura B-31: Alternate Care-of Address del Binding Ack.*



### 8.5. HANDOVER INITIATE (HI)

Figura B-32: Mensaje Handover Initiate.



- **Campos Fijos**

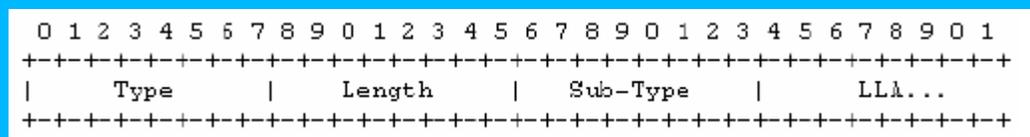
- Type:** 1 byte.
- Code:** 1 byte.
- Checksum:** 2 bytes.
- Identifier:** 2 bytes.
- S:** 1 bit.
- U:** 1 bit.
- Reserved:** 14 bits.

- **Campos Variables**

- Options:**
  - Link-layer Address of MN:

#### 8.5.1. Link-layer address of mn

Figura B-33: Link-layer Address of MN del Handover Initiate.



- Type:** 1 byte.
- Length:** 1 byte.
- Sub-Type:** 1 byte.
- Link-Layer Address:** 6 bytes (para IEEE 802). [IPv6 ETHER] (+9 bytes de padding).







### 9. TRASPASO CON F-HMIPv6

- En este caso el MN envía tres mensajes:
  - Router Solicitation for Proxy Advertisement (RtSolPr) entre 48 y 72 bytes.
  - Fast Binding Update (FBU) entre 52 y 92 bytes.
  - Local Binding Update entre 56 y 96 bytes.
  
- En este caso el MN recibe tres mensajes:
  - Proxy Router Advertisement (PrRtAdv) entre 48 y 144 bytes.
  - Fast Binding Acknowledgment (FBAck) entre 52 y 72 bytes.
  - Local Binding Acknowledgment (LBAck) entre 56 a 72 bytes.

Además de estos mensajes, se envían entre MAP y NAR los siguientes mensajes:

- Desde MAP a NAR:
  - Handover Initiate (HI) entre 48 y 100 bytes.
  
- Desde NAR a MAP:
  - Handover Acknowledgment (Hack) entre 48 y 68 bytes.

Todos los mensajes que intervienen en el traspaso con el protocolo F-HMIPv6, están explicados con anterioridad en este documento, ya que son exactamente los mismos que intervienen en FMIPv6 y HMIPv6.

## **ANEXO C:**

### **ESTANDARIZACION RELACIONADA CON MOVILIDAD**

### 1. INTRODUCCION

Diversos organismos y foros de estandarización están trabajando en aspectos relacionados con la movilidad en las telecomunicaciones. Organizaciones históricamente conocidas por sus normas para comunicaciones no móviles, como IEEE o IETF, o como OMA, se unen a entidades tradicionalmente ligadas a la estandarización de las tecnologías móviles, como ETSI y su proyecto 3GPP. Los distintos grupos colaboran, desarrollando cada uno la parte del sistema que es su especialidad. Por ejemplo, el servicio PoC sobre redes UMTS o GSM se basa en documentos de 3GPP, OMA e IETF.

En este documento anexo se explora la actividad de estandarización de los diferentes grupos de normalización, desde el punto de vista de la evolución de las redes móviles actuales y su confluencia con las redes fijas de datos y con otros tipos de accesos inalámbricos.

### 2. TIPOS DE ORGANISMOS DE ESTANDARIZACION

Debido al gran crecimiento y evolución de las redes móviles, han surgido nuevas organizaciones en esta industria tales, como alianzas, consorcios y forums; las cuales se encargan de proponer estándares y definir nuevas tecnologías.

Estas organizaciones se pueden dividir en tres categorías: *alianzas de tecnología, organizaciones de estándares y asociaciones de la industria.*

#### 2.1. ALIANZAS DE TECNOLOGÍA

Está formada para introducir al mercado una tecnología o protocolo específico y proveer interoperabilidad y certificación de productos de diferentes compañías que utilizan esa tecnología o protocolo.

Por nombrar algunos ejemplos de este tipo de organizaciones están: Bluetooth SIG; HiperLAN1, HiperLAN Alliance e HiperLAN2 Global Forum; HomeRF; El HRFWG; OFDM; WLI forum; WECA.

Cada uno especifica su frecuencia de trabajo, cobertura, aplicaciones específicas en entre otras características particulares a cada tecnología.

#### 2.2. ORGANIZACIONES DE ESTÁNDARES

Este tipo de organizaciones crean, definen y proponen estándares internacionales oficiales abiertos a la industria a través de un proceso abierto a todas las compañías.

Entre las más representativas se tiene: La IEEE (Institute of Electrical and Electronics Engineers) y La ETSI (European Telecommunications Standards Institute).

#### 2.3. ASOCIACIONES DE LA INDUSTRIA

Estas organizaciones son creadas para promover el crecimiento de la industria a través de educación y promoción, proveyendo información objetiva sobre la industria en general, tecnologías, tendencias, organizaciones, oportunidades independientemente de la tecnología. La organización más importante en esta categoría es la WLANA (Wireless LAN Association) cuya misión es ayudar y fomentar el crecimiento de la industria a través de la educación que puede ser caracterizada por asociaciones industriales y comerciales.

Organizaciones como éstas promueven la competencia y avances tecnológicos lo cual significa mejores soluciones para los usuarios de redes inalámbricas e incrementar el crecimiento de la industria. La fuerza del mercado decidirá el valor de cada organización.

### 3. ESTADO DE LA ESTANDARIZACIÓN RELACIONADA CON MOVILIDAD

#### 3.1. 3GPP

3GPP (3rd Generation Partnership Project) es el principal foro de estandarización de un sistema móvil 3G. No tiene entidad legal, es un proyecto común de sus socios, y esta formado por ETSI en Europa, ATIS en EE.UU., ARIB y TTC en Japón, TTA en Corea y CCSA en China.

3GPP representa un acuerdo de colaboración entre organismos de estandarización y otras entidades relacionadas para producir las especificaciones técnicas relativas a:

- Un sistema 3G basado en una red troncal GSM/MAP evolucionada y en el acceso radio UTRA.
- La evolución del acceso radio GSM/GPRS/EDGE.

Las tres primeras releases de 3GPP fueron:

1. *LA RELEASE 99*, que, en su modo FDD, es la base de las redes 3G hoy en servicio ("3", NTT DoCoMo) y que está en fase de despliegue en Europa.
2. *LA RELEASE 4*, que presenta una nueva interfaz radio desarrollada por el socio chino (CCSA), el modo TD-SCDMA, el cual es similar al modo TDD de la Release 99 pero con diferente tasa de chip: 1,28 Mchip/s frente a 3,84 Mchip/s. En la red troncal se introduce la separación de los planos de señalización y usuario y el concepto *media gateway*. Desde el punto de vista de usuario, puede considerarse que esta release introduce cambios menores, ya que un terminal release 4 no gozará de servicios o capacidades muy diferentes a las de otro de la release 99.
3. *LA RELEASE 5*, que introduce IMS (IP Multimedia Subsystem) y HSDPA (High Speed Downlink Packet Access). IMS permite soportar múltiples flujos multimedia con diferentes QoS, y utiliza el dominio de paquetes y el protocolo SIP para el control de sesión. HSDPA introduce en la red de acceso radio un nuevo canal descendente, compartido y de alta velocidad.

La introducción del nuevo acceso radio UTRAN no supuso el fin de la evolución de GSM. En la Release 99, EDGE supone un salto cuantitativo en cuanto a tasa de bit en la interfaz aire (hasta 384 kbit/s). La Release 4 introduce el concepto GERAN, en el que se conserva la interfaz aire GSM/GPRS/EDGE, pero que en la red de acceso radio la interfaz lu de UTRAN reemplaza a las interfaces A/Gb y se introduce el concepto de portadora radio (RAB).

De este modo, el estándar 3GPP define una red troncal (basada en MAP), dos posibilidades para la red radio (GERAN y UTRAN) y un conjunto de servicios independientes, en principio, de las redes de transporte.

4. *LA RELEASE 6*, es la última producida por 3GPP, por lo cual se describe con más detalle a continuación.

- **3GPP release 6**

Entre las múltiples mejoras y extensiones de la Release 6 sobresalen las siguientes:

- **El servicio MBMS (Multimedia Broadcast/Multicast Service)**

Es la funcionalidad más significativa de la Release 6. MBMS es un servicio de transporte, independiente de la aplicación, con un uso de recursos óptimo: en la interfaz radio los datos se transmiten una sola vez por canal común para todos los suscriptores de la célula, y en la red se utiliza una sola portadora. Se estandariza tanto para accesos radio UTRAN como GERAN. MBMS permitirá servicios de *streaming* y de descarga de archivos, localizados geográficamente, con control sobre la QoS y sobre la facturación. La recepción no está garantizada por la red de acceso; si es necesaria, deberá llevarse a cabo en las capas superiores. El modo broadcast es una transmisión unidireccional punto a multipunto a todos los usuarios del área de servicio. En lo que respecta al modo *multicast*, su diferencia está en que la transmisión se realiza solo para los usuarios suscritos a un grupo multicast, y permite tarificación y facturación. La implementación de MBMS requiere nueva funcionalidad en GGSN, SGSN, UTRAN, GERAN y UE, así como una nueva entidad funcional, el *Broadcast Multicast Service Centre* (BM-SC), que proporciona las funciones MBMS.

En el plano de transporte, MBMS envía datagramas IP multicast desde la interfaz Gi (punto de entrada a la red) al terminal con una calidad de servicio especificada. En el plano de control, MBMS gestiona la activación del servicio, la autorización, el control de sesión y la gestión de recursos. La interfaz Gmb es el punto de entrada a la red para el plano de control.

Las modificaciones en la interfaz aire de UTRAN (Um) se han reducido en lo posible. No se introduce un nuevo canal físico o de transporte, aunque a nivel lógico son necesarios dos nuevos canales descendentes:

- a. El canal MBMS point-to-multipoint Control Channel (MCCH).
- b. El canal MBMS point-to-multipoint Traffic Channel (MTCH).

Ambos utilizan el canal de transporte FACH, que a su vez se envía sobre el canal físico S-CCPCH. No se especifican canales ascendentes de control. Si es necesario un canal de retorno, las capas superiores deberán establecerlo a través del RACH o DCH.

- **El IMS (IP Multimedia Subsystem) Fase 2**

Parte de la funcionalidad original de IMS no fue completada a tiempo para ser incluida en la Release 5; se pueden destacar, por ejemplo, la gestión de grupos y los servicios de conferencia y mensajería. Por otra parte, se va a dedicar el esfuerzo necesario para la migración de los desarrollos de IMS basados en IPv4 a IPv6.

- **La interoperabilidad WLAN-3GPP**

Seis escenarios han sido considerados en el estudio previo (3GPP TR 22.934), desde el caso mas complejo, que consiste en la movilidad total con traspasos WLAN-celular, hasta el caso mas simple, en el cual el usuario recibe una factura conjunta de los dos sistemas.

En el segundo de los escenarios, cuando se accede mediante WLAN, se realiza la autenticación, autorización y facturación a través de la red 3GPP, pero el acceso a Internet es proporcionado por el operador de WLAN.

El tercer escenario permite, además, acceder a través de WLAN a los servicios 3GPP de la red de paquetes proporcionados por el operador 3GPP, por ejemplo, MMS e IMS, que normalmente no están disponibles por Internet.

- **La aplicación Push to talk over Cellular (PoC)**

Es una aplicación equivalente a las comunicaciones semiduplex de tipo “*walkie-talkie*”. Esta siendo estandarizada en OMA, pero utilizara el subsistema IMS de las redes 3GPP.

- **El nuevo canal FDD Enhanced Uplink (EDCH)**

Se introduce un nuevo canal basado en el canal ascendente dedicado DCH, con técnicas ya probadas en HSDPA: scheduling en el Nodo B, corrección de errores con Hybrid-ARQ y tamaño de TTI (transmisión Time Interval) reducidos. Estas mejoras redundan en un menor retardo en la transmisión de paquetes y un incremento en la capacidad de la red.

- **La introducción de Flexible Layer One (FLO) para GERAN**

FLO introduce el concepto de transporte, utilizado en UTRAN, en la capa física de GERAN. Con FLO, esta capa ofrece canales de transporte a la subcapa MAC. En un principio se definen solo canales de transporte dedicados (DCH) para un solo MS, y se utilizan solo los canales físicos DBPSCH. Cada canal de transporte tiene un flujo de datos con parámetros de QoS determinados, y varios canales pueden multiplexarse sobre un subcanal físico. También se introducen los conceptos de formato de transporte (TF), análogos a los empleados en la definición de los canales físicos de UMTS. Este modo de operación permite mayor flexibilidad en la adjudicación de recursos, así como la alineación de las capas 2 y superiores de la interfaz radio de GERAN con UTRAN.

### 3.2. OMA

OMA (Open Mobile Alliance) es un organismo de estandarización creado en junio de 2002, orientado a estandarizar servicios y aplicaciones móviles de manera independiente a la tecnología de transporte y acceso. Participan los principales operadores móviles, fabricantes de equipos de red y terminales, proveedores de servicios y contenidos, y compañías de tecnologías de la información de todo el mundo. OMA consolida e integra diversos grupos: WAP Forum, Location Interoperability Forum (LIF), SyncML Initiative, MMS-IOP (Multimedia Messaging Interoperability Process), Wireless Village, Mobile Gaming Interoperability Forum (MGIF) y el Mobile Wireless Internet Forum (MWIF).

El objetivo último y principal de OMA es garantizar la interoperabilidad extremo a extremo de los servicios móviles, para lo cual OMA se centra en la especificación de una arquitectura de servicios con interfaces abiertas e independiente de la tecnología de redes móviles y sus plataformas. Para proporcionar esta interoperabilidad extremo a extremo, los principios de OMA son los siguientes:

- Proporcionar productos y servicios basados en estándares abiertos.
- Disponer de una arquitectura y unas tecnologías que posibiliten servicios independientes del sistema operativo, de las tecnologías de acceso y de las plataformas de red.
- Disponer de una capa de aplicación independiente de las capas de transporte. De forma simplista se puede decir que la colaboración con 3GPP y 3GPP2 se realiza en los siguientes términos:
  - La estandarización de la red radio y la red troncal es tarea de 3GPP y 3GPP2.
  - La estandarización de aplicaciones es tarea de OMA.
- Proporcionar una interoperabilidad de servicios de manera transparente al usuario, pudiendo emplear diferentes tecnologías y modos de acceso.

OMA dedica considerables esfuerzos a especificar pruebas de interoperabilidad extremo a extremo y promueve eventos de pruebas (IOT) de las tecnologías que desarrolla. En particular, el servicio MMS, que en las primeras implementaciones resultaba decepcionante por las incompatibilidades entre redes o entre terminales, ha sido afinado por OMA estableciendo unas bases y requisitos mínimos de funcionamiento.

Además de las actividades de interoperabilidad, OMA trabaja en las siguientes áreas de especificación de servicios:

- *MULTIMEDIA MESSAGING SERVICE (MMS)*. OMA continúa con las actividades de estandarización del servicio de mensajería multimedia con el objetivo de hacer converger los estándares especificados en 3GPP y 3GPP2. Dichas especificaciones y las baterías de pruebas desarrolladas en OMA se han seleccionado como base de los requisitos que el Global Certification Forum exigirá para certificar los terminales que incorporen clientes MMS.
- *DEVICE MANAGEMENT & CLIENT PROVISIONING*. OMA continúa la actividad que comenzó en SyncML con el fin de especificar protocolos y mecanismos que permitan la gestión (local o remota) de los terminales móviles y su provisión de parámetros de acceso a servicios.
- *DIGITAL RIGHTS MANAGEMENT (DRM)*. OMA especifica un mecanismo por el cual los contenidos quedan asociados a unos derechos de uso y a un usuario en concreto, de manera que el usuario no puede distribuir libremente los contenidos protegidos.
- *MOBILE BROADCAST SERVICES (MBS)*. Se refiere a un amplio rango de servicios basados en comunicación "uno a muchos" que permite ofrecer servicios de difusión (por ejemplo, radio y TV digital) en el entorno móvil, que previsiblemente pueden crear nuevas oportunidades de negocio para los proveedores de servicio. Estos servicios se basarán en las tecnologías de broadcast y multicast digital existentes, como DVA-T/H,

DAB y 3GPP/MBMS, y hará uso de canales de transmisión de alta velocidad que se espera permitan ofrecer contenidos de difusión a bajo coste.

- *PUSH TO TALK OVER CELLULAR (POC)*. Se trata de un servicio de comunicación semiduplex tecnológicamente muy similar al de voz sobre IP, que permite a los usuarios establecer comunicaciones inmediatas con uno o mas interlocutores con un modelo de operación similar al de un "walkie talkie", simplemente presionando un botón en sus terminales móviles.
- *CONTENT SCREENING*. Se encuentra en una fase temprana de desarrollo y su objetivo es analizar y clasificar el contenido (en apropiado, no apropiado o malicioso) antes de hacerlo disponible al usuario, posibilitando el "control parental" de acceso a determinados contenidos y evitando la exposición a posibles virus, correo basura o ataques externos.
- *PRESENCIA Y DISPONIBILIDAD*. Permite que otras aplicaciones y servicios intercambien información sobre el estado, capacidades y localización de los usuarios y sus terminales de manera dinámica.
- *INSTANT MESSAGING*. Proporciona un conjunto universal de especificaciones para mensajería instantánea y servicios basados en información de presencia que se utilizan para intercambiar mensajes e información de presencia entre dispositivos móviles, servicios móviles y servicios de mensajería instantánea típicos de Internet (por ejemplo, MSN Messenger, IRC, etc.).
- *STANDARD TRANSCODING INTERFACE*. OMA esta especificando una interfaz estándar hacia plataformas de transcodificación que pueda ser utilizada por diversos servicios (navegación, mensajería, descarga de tonos, etc.), para adaptar el contenido a entregar al receptor en función de las capacidades y características de su terminal.
- *USER AGENT PROFILE*. Define el flujo extremo a extremo del perfil del agente de usuario entre el dispositivo y el servidor a través de los puntos de red intermedios, asegurando que la información de las capacidades del dispositivo este disponible para las partes que la necesiten. Permitiendo, por tanto, que se pueda garantizar que el usuario receptor recibe el contenido de manera inteligible para el, de acuerdo a sus capacidades y a las características de entorno.
- *BROWSING*. OMA ha seleccionado un subconjunto del entorno XHTML típico del ámbito de Internet fijo (XHTML-Mobile Profile) que incluye un soporte mínimo de hojas de estilo y ECMAScript.
- *MOBILE LOCATION PROTOCOL (MLP)*. Se trata de un protocolo a nivel de aplicación que permite obtener la posición de los dispositivos móviles (terminales móviles, PDAs, etc.) de manera independiente a la tecnología de red subyacente. MLP sirve de interfaz entre el servidor de localización y el cliente de servicios de localización y define el conjunto básico de operaciones que debe ser capaz de soportar el servidor de localización.
- *EXECUTION POLICY ENFORCEMENT MANAGEMENT (EPEM)*. Describe un mecanismo para especificar las condiciones en que se pueden ejecutar otros servicios, definiendo perfiles de políticas de acceso y ejecución, convirtiéndose en un

entorno de ejecución controlado, complementando la iniciativa Parlay que define unas interfaces que permiten acceso a una determinada funcionalidad.

- *MOBILE WEB SERVICES*. OMA no aspira a desarrollar nuevas especificaciones que compitan con las existentes, sino a unificar dichos estándares y describir como aplicar la tecnología web services en su arquitectura de servicios móviles.
- *MOBILE COMMERCE AND CHARGING*. Proporciona estándares para transacciones comerciales seguras desde el móvil, también conocido como m-commerce, cubriendo las áreas de cargo, cobro y pago en la transacción electrónica. OMA ha establecido, hasta el momento, acuerdos con MPF, Mobey Forum y PayCircle y pretende ampliar su abanico de colaboración en este campo a Liberty Alliance Project, MeT, OASIS y Parlay, entre otros.

Hay que indicar finalmente, que OMA pone a disposición pública su plan de trabajo, detallando sus actividades de estandarización en servicios, su evolución y sus expectativas de progreso. Dicho plan de trabajo puede encontrarse en el sitio web oficial de OMA.

### 3.3. 3GPP2

De forma similar a como se estableció 3GPP (3rd Generation Partnership Project) para la estandarización de GSM y UMTS, la estandarización de los sistemas cdma2000 se realiza a través de un proyecto de colaboración, sin entidad legal, que han establecido cinco organismos de estandarización:

1. ARIB, Association of Radio Industries and Businesses (Japón).
2. CCSA, China Communications Standards Association (China).
3. TIA, Telecommunications Industry Association (EE.UU.).
4. TTA, Telecommunications Technology Association (Corea).
5. TTC, Telecommunications Technology Committee (Japón).

También cuenta con dos representantes del mercado:

1. The CDMA Development Group (CDG).
2. IPv6 Forum.

El trabajo de preparación de las especificaciones técnicas se divide entre cuatro TSGs (Technical Specification Groups):

1. TSG-A (Access Network Interfaces).
2. TSG-C (cdma2000).
3. TSG-S (Services and Systems Aspects).

### 4. TSG-X (Core Networks).

3GPP2 ha ido produciendo distintas versiones de las distintas modalidades del estándar (1xRTT, 3xRTT, 1xEV-DO y 1xEV-DV), que están disponibles para su descarga gratuita en el portal del proyecto ([www.3gpp2.org](http://www.3gpp2.org)).

### 3.4. IEEE 802

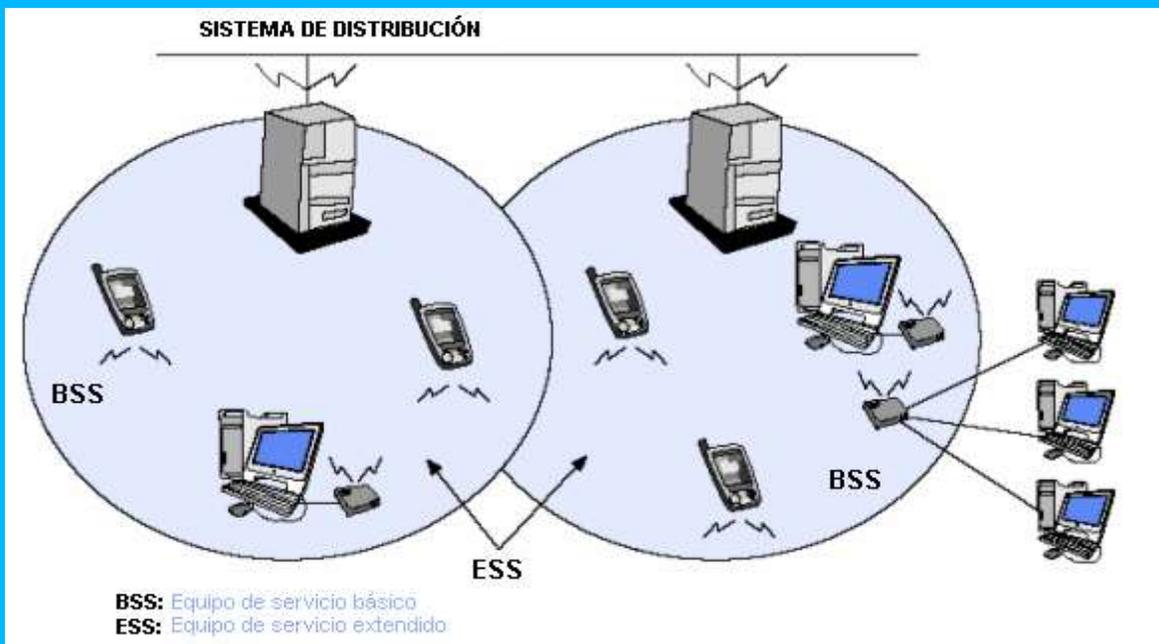
El IEEE 802 LAN/MAN Standards Committee desarrolla estándares para redes de área local (LAN) y metropolitana (MAN), fundamentalmente para las capas más bajas del modelo OSI. Los más conocidos son la familia 802.3 (Ethernet), Token Ring, y, más recientemente, Wireless LAN. La IEEE se organiza en grupos de trabajo (WGs) y sus miembros son personas individuales, no compañías.

#### 3.4.1. El estándar IEEE 802.11

Una red inalámbrica 802.11 está basada en una arquitectura celular en la que el sistema se divide en células llamadas BSS (Basic Service Set). Cada célula está controlada por una estación base llamada AP (Access Point). Un sistema puede constar de una o varias células; en el caso pluricelular los diferentes AP se conectan entre sí mediante un backbone llamado DS (Distribution System), típicamente Ethernet, aunque en algunos casos también puede ser inalámbrico (ver la Figura C-1).

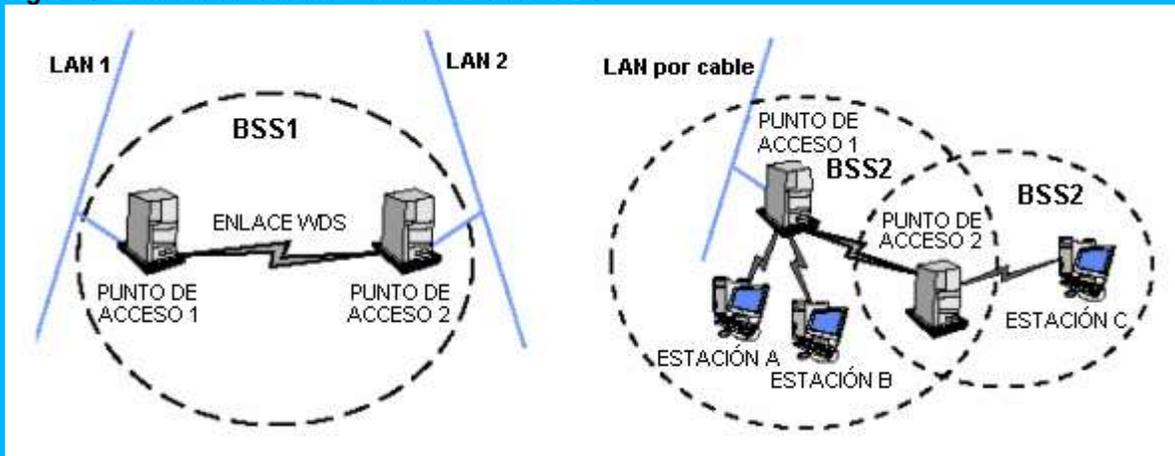
Todo este conjunto de células interconectadas se ve como una única red desde los protocolos de las capas superiores, y se llama ESS (*Extended Service Set*). Cada ESS tiene un identificador conocido como SSID, que debe ser el mismo en todos los AP del ESS.

**Figura C-1:** Topología de una red IEEE 802.11



El protocolo 802.11 puede utilizarse para soportar la conexión inalámbrica de puntos de acceso, de forma que el sistema de distribución se vuelve inalámbrico. Esta opción recibe el nombre de WDS (Wireless Distribution System). Los AP que soportan WDS pueden actuar con dos funciones: bridge inalámbrico o repetidor (ver la Figura C-2).

**Figura C-2:** Modos de funcionamiento de APs con WDS



### 3.4.2. Capas IEEE 802.11

El protocolo 802.11 define (como cualquier 802.x) la capa física y la capa MAC, suponiendo que por encima hay una capa LLC 802.2 (ver la Figura 3. 5).

Hay distintas posibilidades para la capa física dependiendo del tipo de red (a, b, g, h), e incluso distintas opciones dentro del mismo tipo. Actualmente el tipo más común es el 802.11b, cuyas características de la capa física son:

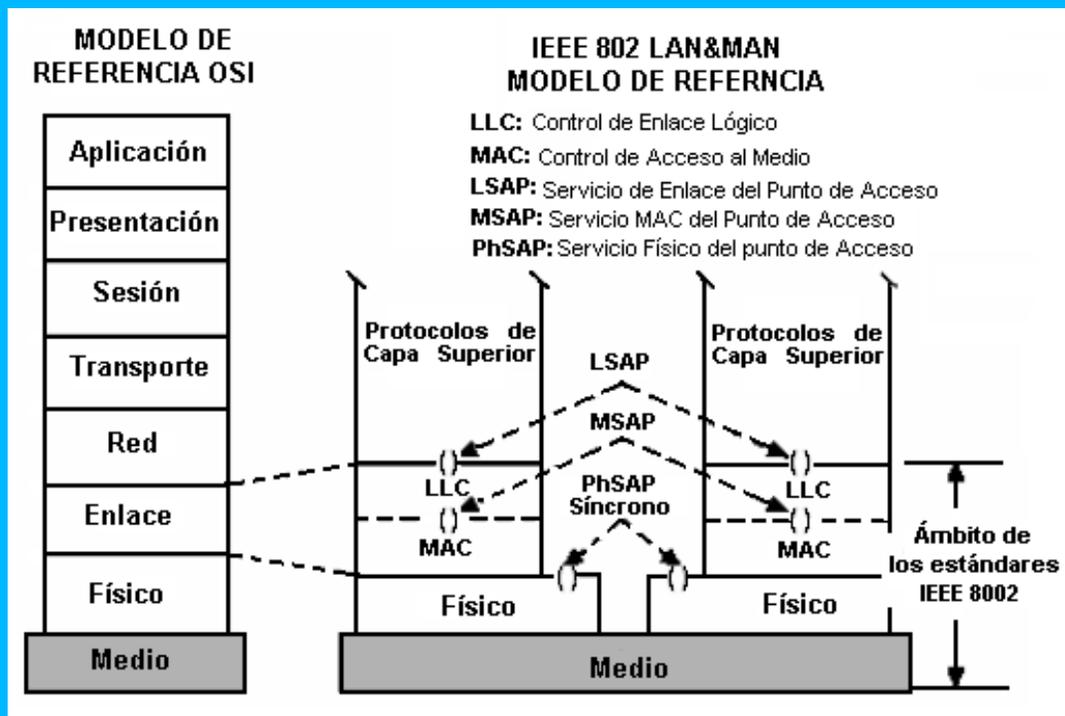
- La banda de frecuencia de 2,4 GHz.
- El DSSS (Direct Sequence Spread Spectrum).
- La codificación CCK (para las velocidades de 5,5 y 11 Mbit/s).

La capa MAC, además de la funcionalidad típica de estas capas, realiza funciones que normalmente se implementan en capas superiores: fragmentación, retransmisión de paquetes, y asentimientos (ACKs). Esto es así debido a las características de los enlaces radio, con errores altos, que aconsejan un tamaño pequeño de los paquetes, pero debiéndose preservar desde el punto de vista de las capas superiores los paquetes de 1.518 bytes típicos de Ethernet.

El método de acceso es CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), similar al popular CSMA/CD pero que no detecta colisiones, dado que:

- Se evita la necesidad de emitir y escuchar al mismo tiempo, ya que encarece mucho los productos radio.
- Existe el problema de "hidden station", en el que dos estaciones, que no se escuchan entre ellas, colisionan al acceder al AP que escucha a las dos. Para su resolución se prevé el mecanismo denominado RTS/CTS.

Figura C-3: Pila de protocolos de las redes IEEE 802



El estándar 802.11 ha dado pie a la explosión de las redes de área local inalámbricas, denominadas comúnmente WLAN o WiFi. La primera versión del estándar se publicó en 1997, resultado de dos grupos de trabajo, MAC (acceso al medio) y PHY (capa física). Posteriormente, IEEE 802.11 ha producido mejoras sucesivas encaminadas a aumentar la velocidad, adaptar la norma a nuevas bandas de frecuencia, e introducir calidad de servicio y mecanismos de seguridad o de gestión de recursos. Estas mejoras se reflejan en las revisiones del estándar (802.11a, 802.11b, etc.). Por ejemplo, la revisión 802.11b aumenta la velocidad de los iniciales 2 Mbit/s a 11 Mbit/s, y es el formato más extendido de WLAN.

La variante 802.11a, en la banda de frecuencia de 5 GHz, no ha alcanzado la misma popularidad al utilizar una banda que en algunas regiones no está liberada. La gran mayoría de los terminales WLAN utilizan la revisión 802.11b. Este estándar no especifica funcionalidades características de una red móvil como son traspasos, gestión de movilidad, gestión de recursos radio, autenticación, etc. Solamente las capas más bajas están especificadas, por lo que estas funcionalidades, si existen, son propietarias y rara vez interoperables. Por esta razón, el trabajo de los grupos 802.11i y 802.11k resulta particularmente interesante como evolución de las WLAN actuales hacia redes que permitan traspasos y condiciones de seguridad comparables a las redes móviles.

### 3.5. REDES DE AREA PERSONAL INALAMBRICAS

Se trata de redes que permiten la interconexión de dispositivos en el área que rodea a la persona o al dispositivo, con un alcance máximo que se estima en torno a los diez metros. Se soportan tasas binarias variables, que comprenden desde decenas de kilobit por segundo hasta centenares de megabit por segundo (WPAN de nueva generación). La potencia de transmisión que emplean es muy baja (típicamente 1 mW), aunque actualmente también se contempla la utilización de dispositivos de mayor potencia. Operan en bandas de espectro que no precisan licencia, toda vez que su coordinación resultaría prácticamente inviable.

Los principales estándares actuales para este tipo de redes son Bluetooth, HomeRF (abandonado) y Zigbee.

#### 3.5.1. El estándar IEEE 802.15

Las redes inalámbricas de área personal (WPANs) permiten comunicar entre sí teléfonos móviles, PDAs, PCs y otros aparatos a distancias cortas, de algunos metros. Bluetooth es la tecnología más conocida y disponible en todo tipo de equipos. Aunque fue desarrollada por un grupo de compañías, 802.15 ha adaptado y convertido Bluetooth en un estándar (IEEE 802.15.1) y desarrollado una nueva norma, IEEE 802.15.3 (denominada Zigbee), con mayores tasas de bit (hasta 55 Mbit/s) y menor consumo. Futuros desarrollos basados en técnicas UWB (Ultra Wide Band) apuntan a tasas de 100 Mbit/s o superiores, que permitirán vídeo y aplicaciones multimedia.

- **Redes bluetooth**

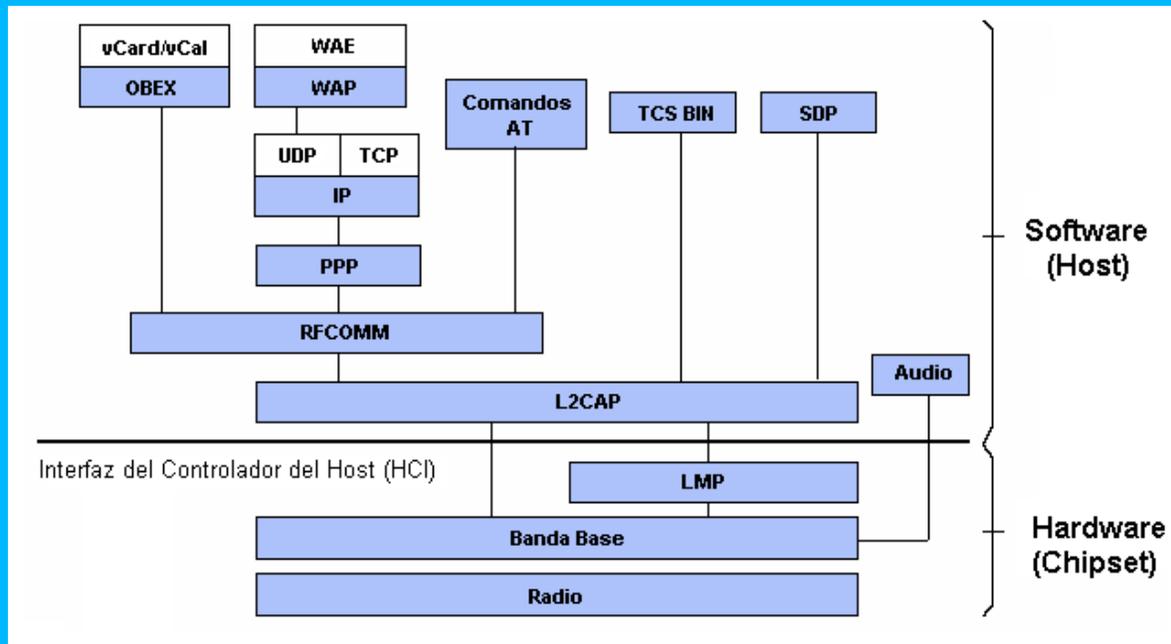
Es el tipo de red de área personal más extendido. Tiene su origen en una iniciativa que en 1994 lanza Ericsson para estudiar un sistema de comunicación inalámbrica entre teléfonos y sus accesorios. Debe su nombre a Harald Bluetooth, un rey vikingo que unió pacíficamente los pueblos de Dinamarca y Noruega. Sus principales características son:

- Opera en la banda de 2,4 GHz con una tasa binaria de 720 kbit/s.
- Utiliza salto en frecuencia (Frequency Hopping, FH), que divide el espectro disponible en 79 canales. Los transceptores saltan de un canal a otro siguiendo una secuencia pseudoaleatoria determinada por el nodo maestro con una tasa de 1.600 saltos por segundo.
- Utiliza modulación GFSK (modulación FM con un filtrado gaussiano).
- Dispone de duplexación en el tiempo TDD.
- Soporta hasta ocho dispositivos en una picorred (un maestro y siete esclavos). Los dispositivos de una picorred están sincronizados en tiempo y en frecuencia. El maestro es el dispositivo que inicia la conexión y marca la sincronización, mientras que los esclavos son los dispositivos con los que se conecta el maestro. Una vez establecida la conexión, se pueden intercambiar los roles maestro-esclavo.
- Las picorredes pueden combinarse para formar lo que se denominan “*scatternets*”

- La potencia de transmisión esta comprendida entre 0 dBm (dispositivos de clase 3) y 20 dBm (dispositivos de clase 1).
- El control de potencia es obligatorio para los dispositivos de clase 1, y opcional para el resto.

Las especificaciones de Bluetooth se desarrollan a través de Bluetooth SIG, que es una asociación comercial compuesta por empresas líderes en telecomunicaciones, computación y redes (como Ericsson, Intel, Nokia o Motorola, entre otros). Estas especificaciones comprenden tanto la descripción del hardware y los protocolos como la definición de un marco para aplicaciones. Constan de dos volúmenes: Núcleo (Core) y Perfiles (Profiles). Actualmente esta disponible la versión 1.2, que incorpora, entre otras mejoras, medidas para combatir las interferencias entre redes Bluetooth y redes WLAN que operan en la misma banda. La torre de protocolos de Bluetooth se representa en la *Figura C-4*.

*FiguraC-4: Torre de protocolos de Bluetooth*



Lo más reseñable es la separación entre los protocolos implementados directamente en el hardware y aquellos otros implementados vía software. Entre ambos se define una interfaz (HCI, Host Controller Interface) para la comunicación entre ambos niveles. Es también reseñable que además de los protocolos propios de Bluetooth (como el SDP, Service Discovery Protocol, para el descubrimiento de servicios disponibles), se incluyen otros estándares, como puedan ser los propios del conjunto de protocolos TCP/IP (UDP, TCP, IP y PPP).

En estos momentos hay millones de dispositivos que incorporan Bluetooth para soportar la conectividad inalámbrica, desde teléfonos móviles a impresoras, ratones y teclados inalámbricos, PDAs, auriculares, etc.

### • Redes Zigbee

El estándar Zigbee proporciona servicios similares a los de Bluetooth, pero orientados a la interconexión de dispositivos autónomos, como puedan ser sistemas de medida o de control. Por ello, ha predominado en su diseño el bajo consumo de energía y la capacidad para formar redes de mayor tamaño que en Bluetooth, a costa, eso sí, de soportar tasas binarias menores. Zigbee es el nombre adoptado por una alianza comercial para promocionar la adopción del estándar IEEE 802.15.4 (de forma similar a como actúa la WiFi Alliance respecto de los estándares 802.11x). Sus principales características técnicas son:

- Sus tasas binarias de 250 kbit/s y 20 kbit/s.
- Su topología en estrella, con posibilidad de peer to peer.
- Dispone de 255 dispositivos por red.
- Dispone de acceso al canal CSMA/CA.
- Su bajo consumo de potencia.
- Su alcance de 10 metros.
- Su banda de operación dual: 2,4 GHz y 868/915 MHz.

Un escenario típico de aplicación de una red Zigbee es el que se representa en la *Figura C-5*.

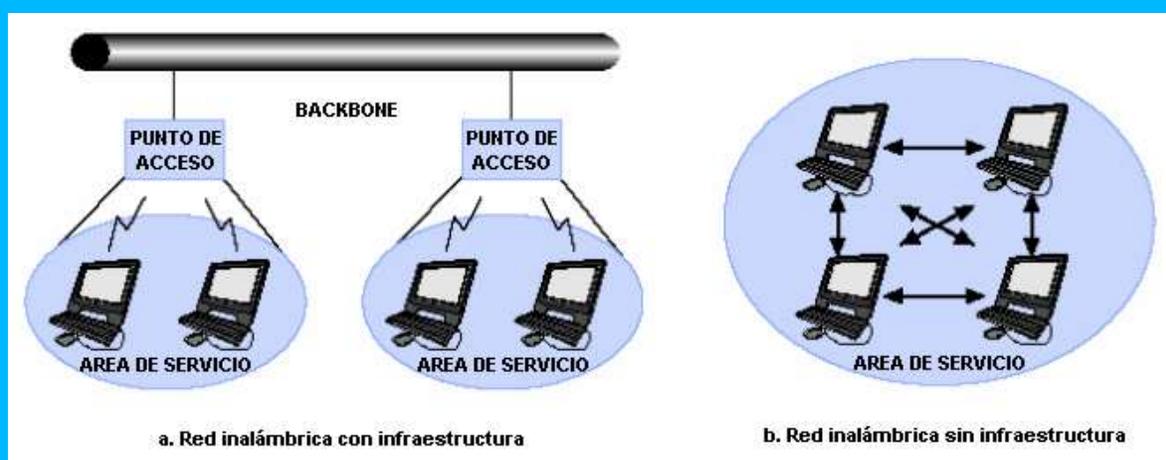
*Figura C-5: Escenario de aplicación de Zigbee*



### 3.6. REDES AD-HOC

Una red móvil ad-hoc (MANET, Mobile Ad-hoc Network), consiste en una colección de terminales o nodos inalámbricos que dinámicamente pueden conectarse entre sí, en cualquier lugar y en cualquier instante de tiempo, sin necesidad de utilizar la infraestructura de red preexistente en la zona. Se trata de un sistema autónomo en el que los servidores móviles, conectados por enlaces inalámbricos, pueden moverse libremente y actuar simultáneamente como enrutadores (o routers). En principio, una red ad-hoc puede crearse sobre la infraestructura de transporte que proporcione una red de área personal, local o metropolitana. En la Figura 3. 7 se muestra un ejemplo de redes inalámbricas con y sin infraestructura de red.

Figura C-6: Redes inalámbricas con y sin infraestructura



Las principales características de las redes ad-hoc son:

- **LOS TERMINALES AUTONOMOS.** En MANET cada terminal es un nodo autónomo, pudiendo funcionar a la vez como servidor, con su capacidad de procesamiento, y como enrutador (router).
- **SU FUNCIONAMIENTO DISTRIBUIDO.** Al no existir una infraestructura de red por debajo que sustente, centralice y controle las operaciones de red, el control y la gestión de la red se va a distribuir entre los terminales que la forman. De este modo los terminales que forman parte de una red ad-hoc deben colaborar entre ellos.
- **EL ENRUTAMIENTO MULTISALTO.** Existen dos tipos básicos de algoritmos de enrutamiento en redes ad-hoc: multisalto y monosalto. Una red MANET monosalto es más sencilla desde el punto de vista de arquitectura e implementación; en cambio, cuenta con una menor funcionalidad y aplicabilidad.
- **LA TOPOLOGIA DINAMICA DE LA RED.** Como los nodos del sistema son terminales móviles, la topología puede variar de un instante a otro de manera impredecible. Las redes MANET deben adaptarse en cada instante de tiempo al

tráfico de los nodos de red móviles, así como a las condiciones de propagación y los patrones de movilidad. Los terminales móviles que constituyen la red ad-hoc establecen dinámicamente el enrutamiento de las conexiones entre ellos mientras se van desplazando de un lugar a otro.

- **LA CAPACIDAD DE ENLACE FLUCTUANTE.** Las altas tasas binarias de error que se pueden producir en una conexión inalámbrica podrían agravarse en una red ad-hoc, pues cada enlace extremo a extremo puede compartirse por diferentes sesiones. El canal de transmisión siempre se encuentra condicionado por los niveles de ruido, atenuación e interferencia que concurren en cada instante de tiempo y en cada lugar.
- **LOS TERMINALES MOVILES LIGEROS.** En la mayoría de los casos los nodos de las redes ad-hoc son dispositivos móviles con menor capacidad de procesamiento, pequeña capacidad de memoria y batería de baja capacidad. Estos dispositivos precisan algoritmos y mecanismos optimizados para la realización de las funciones computacionales y de comunicación.

El concepto de las redes ad-hoc tiene una creciente utilidad en aquellos entornos donde la infraestructura de comunicaciones es muy escasa, o no existe, o resulta muy costosa o inconveniente de desplegar y utilizar. Este tipo de redes permite a los dispositivos móviles mantener conexiones con la red así como facilitar la conexión y desconexión de dispositivos en el sistema.

**Tabla C-1:** Aplicaciones de las redes ad-hoc

<b>APLICACIONES MILITARES</b>	Estas redes se vienen utilizando en el campo militar desde los años 70, pues cuentan con la ventaja de poder mantener una red de información entre los soldados, los vehículos militares y los centros.
<b>SECTOR COMERCIAL</b>	Las redes ad-hoc también pueden ser útiles en operaciones de emergencia, rescate y salvamento. Estas actividades tienen lugar en entornos donde no existe infraestructura de comunicaciones, o la que existe está dañada y no puede ser utilizada. Otros escenarios de aplicación comercial pueden ser las comunicaciones entre barcos.
<b>A NIVEL LOCAL</b>	Las redes ad-hoc permiten crear de forma autónoma una red multimedia esporádica formada por computadores personales y otros terminales móviles para difundir y compartir información entre los participantes de una conferencia o entre los asistentes a un curso por ejemplo. Entornos similares donde las redes ad-hoc tendrán una gran variedad de aplicaciones y servicios serán las residencias de particulares, los estadios de fútbol, puertos marítimos, cafeterías, etc.
<b>REDES DE AREA PERSONAL (Personal Area Network - PAN)</b>	Una MANET de corto alcance puede simplificar la intercomunicación entre distintos dispositivos móviles (como una PDA, un computador portátil y un teléfono móvil.)

Como se puede ver en la *Tabla C-1*, son muchas y muy atractivas las aplicaciones de las redes ad-hoc. Sin embargo existen ciertos aspectos que exigen ser estudiados cuidadosamente antes de que las redes ad-hoc puedan extenderse y comercializarse a gran escala. Los principales retos a los que se enfrentan hoy en día las redes ad-hoc son los siguientes:

- *EL ENRUTAMIENTO DE PAQUETES*. El constante cambio de la topología de red exige que el enrutamiento de los paquetes intercambiados entre dos nodos de la red sea un aspecto crítico. además, debe tenerse en cuenta que la ruta entre dos nodos puede incluir múltiples saltos, lo que complica aun más la comunicación.
- *SU SEGURIDAD Y FIABILIDAD*. Al tratarse de redes distribuidas en distintos terminales, debe prestarse especial atención a los distintos esquemas de autenticación y gestión de claves.
- *LA CALIDAD DE SERVICIO*. Otro reto importante será poder proporcionar diferentes niveles de calidad de servicio en un entorno en constante cambio.
- *EL INTERFUNCIONAMIENTO CON LAS REDES FIJAS*. además de la comunicación interna dentro de la red ad-hoc, en la mayoría de los casos también se espera disponer de la interconexión entre la red ad-hoc y la red fija (principalmente basada en IP).
- *EL CONSUMO DE POTENCIA*. Para las tareas relacionadas con la comunicación dentro de las redes ad-hoc debe pensarse en mecanismos optimizados para reducir al máximo el consumo de potencia en los terminales ligeros.

El nicho de mercado de las redes ad-hoc esta garantizado si los retos aquí expuestos se superan satisfactoriamente, ya que el campo de aplicaciones en un futuro inmediato es muy amplio.

### 3.7. REDES DE ÁREA METROPOLITANA

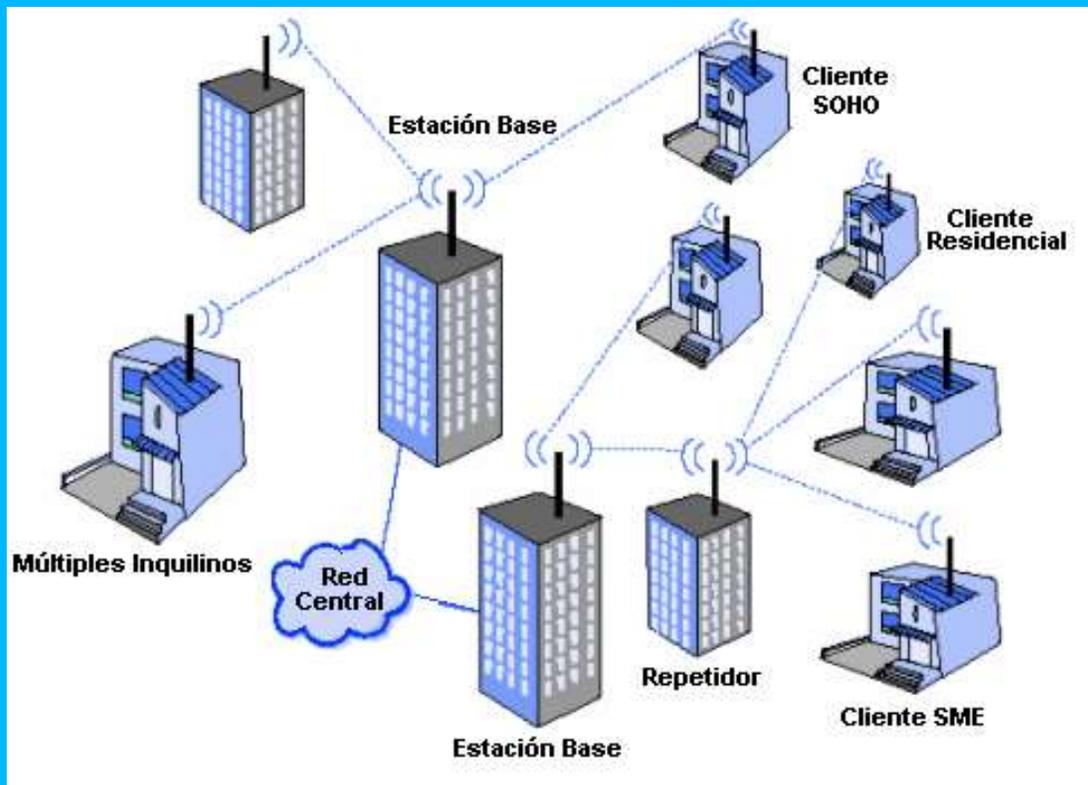
El instituto IEEE-SA (Institute of Electrical and Electronics Engineers - Standards Association) constituyó el grupo de trabajo IEEE 802.16 para especificar la interfaz aire de las redes inalámbricas de área metropolitana (wireless MAN).

#### 3.7.1. El estandar IEEE 802.16

El estándar se publicó el 8 de abril de 2002. Existe una nueva versión, denominada 802.16-2004, que actualiza las anteriores versiones 802.16, 802.16a y 802.16c. IEEE 802.16 engloba la conexión de la “última milla”, o “primera milla” según se quiera, en las redes metropolitanas de área local inalámbricas. El objetivo final es proporcionar acceso a la red desde los hogares, las pequeñas empresas, los centros comerciales, etc., como una alternativa a las conexiones tradicionales por cable. Pretende cubrir el hueco existente en el mercado entre las redes de área local inalámbricas (WLAN) y las redes móviles mucho más extensas (WAN).

El estándar 802.16 soporta una arquitectura punto a multipunto en la banda de 10 a 66 GHz, alcanzando tasas binarias de hasta 120 Mbit/s. A esas frecuencias la transmisión debe realizarse con visión directa, por lo que los tejados de los edificios resultan ser el emplazamiento óptimo para la ubicación de las estaciones base y de abonado. La estación base se conecta a la red troncal (ya sea a la red telefónica pública o a Internet) y transmite por la interfaz radio, alcanzando distancias de hasta 50 Km, por lo cual puede cubrir un gran número de estaciones de abonados, posiblemente cientos ( Figura C-7).

*Figura C-7: Visión de una red de área metropolitana*



La capa de control de acceso al medio (MAC) de 802.16 soporta muchas especificaciones diferentes de capa física, para bandas de frecuencia reguladas y sin regular (con y sin licencia). La capa MAC de 802.16 en cada estación base distribuye dinámicamente el ancho de banda disponible en los enlaces ascendente y descendente entre las estaciones de abonado mediante acceso múltiple por división en el tiempo (TDMA). Esta es una mejora importante respecto a la capa MAC de 802.11, que utiliza mecanismos de sensibilidad de canal, lo que no suele ofrecer un control efectivo del ancho de banda en el enlace radio.

Para poder dar acceso al servicio en situaciones donde no hay visión directa entre el transmisor y el receptor a más baja frecuencia, IEEE publicó en enero de 2003 el estándar 802.16a, que soporta una arquitectura en forma de malla. 802.16a opera en las frecuencias con y sin licencia entre 2 y 11 GHz, utilizando la técnica de multiplexación ortogonal en frecuencia (Orthogonal Frequency Division Multiplexing, OFDM), de modo similar a 802.11a y 802.11g.

## ANEXO C: ESTANDARIZACION RELACIONADA CON MOVILIDAD

El siguiente paso del grupo de trabajo 802.16 ha consistido en añadir portabilidad y movilidad al estándar. En marzo de 2002 el grupo de trabajo comenzó el grupo de estudio 802.16e sobre acceso inalámbrico de banda ancha en entornos móviles (Mobile Broadband Wireless Access, BWA). Este grupo de estudio dirige diferentes temas relativos a la movilidad, incluyendo la conectividad desde los vehículos en movimiento que se encuentran dentro de la cobertura de una estación base.

**Tabla C-2: Comparativa entre 802.16 y 802.11**

	802.11	802.16	DIFERENCIAS
<b>ALCANCE</b>	Por debajo de los 90 metros (deben añadirse nuevos puntos de acceso para extender la cobertura)	Hasta 48 kilómetros. El tamaño típico de la celda es de 6 a 9 kilómetros.	La capacidad física de los sistemas 802.16 tolera un mayor nivel de reflexión multirayecto, dispersión del retardo gracias a la implementación de una FFT de 256 en vez de la FFT de 64 de los sistemas 802.11
<b>COBERTURA</b>	Optimizado para máximas prestaciones en interiores, corto alcance.	Máximas prestaciones en entornos exteriores sin visión directa (NLOS). Soporta de forma estándar las nuevas técnicas avanzadas de antena.	Los sistemas 802.16 tienen una ganancia de sistema total superior, consiguiendo mayor penetración a través de obstáculos a distancias mayores.
<b>ESCALABILIDAD</b>	Destinado a aplicaciones tipo LAN, se puede escalar de uno a decenas de usuarios, con un usuario por cada dispositivo (CPE). Los tamaños de canal son fijos (200 MHz)	Diseñados para soportar eficientemente de uno a centenares de dispositivos, con un número ilimitado de usuarios para cada dispositivo. Los tamaños de canal son flexibles de 1.5 MHz a 20MHz.	El protocolo de acceso al medio (MAC) de los sistemas 802.11 usa un protocolo CSMA/CA, mientras que el correspondiente para los sistemas 802.16 usa TDMA dinámico.  Los sistemas 802.11 pueden usarse únicamente en las bandas de frecuencia no reguladas (no sujetas a licencia). Sin embargo los sistemas 802.16 pueden usarse en cualquier frecuencia disponible, pues la existencia de canales múltiples permite un despliegue de tipo celular.
<b>TASA BINARIA</b>	2,7 bits/s por Hz de pico. Hasta 54 Mbit/s en un canal de 20 MHz.	5 bit/s por Hz de pico. Hasta 100 Mbit/s en un canal de 20 MHz.	Se obtiene un uso más eficiente del espectro en los sistemas 802.16 gracias al empleo de modulaciones de orden superior a la corrección de errores flexibles.
<b>CALIDAD DE SERVICIO (QoS)</b>	Sin soporte de mecanismos de calidad de servicio.	Mecanismos de QoS implementados en la capa de acceso al medio (MAC). Provisión de voz/video y niveles de servicio diferenciados	Los sistemas 802.11: utilizan MAC basados en mecanismos de contención (CSMA/CA), que es básicamente Ethernet inalámbrico.  Los sistemas 802.16: utilizan un MAC basado en TDMA dinámico con asignación de recursos bajo demanda.

También el estándar 802.20 especifica una nueva interfaz aire para acceso de banda ancha inalámbrica. Al igual que 802.16, este estándar pretende rivalizar con DSL y las conexiones por cable tradicionales (que ofrecen velocidades de 1 Mbit/s y superiores) en el ámbito de las redes metropolitanas.

Aunque a priori parecen estándares muy similares, existen algunas diferencias importantes entre ellos. La primera es que el 802.16e estudia la incorporación de la movilidad en las bandas de frecuencias entre 2 y 6 GHz con licencia, mientras que el estándar 802.20 abarca la operación del sistema en las bandas con licencia por debajo de los 3,5 GHz. Otra diferencia más importante aún es que la especificación del estándar 802.16e se basa en un estándar ya existente, el 802.16a. Sin embargo, el 802.20 empieza desde cero. Esto significa que con una alta probabilidad los productos basados en 802.16e estarán en el mercado antes que las soluciones basadas en 802.20.

En cuanto a la aplicabilidad, el estándar 802.16e está más dirigido hacia los usuarios móviles que se desplazan caminando dentro del área de cobertura de la estación base, mientras que el 802.20 espera ofrecer altas tasas binarias de transmisión de datos también a usuarios móviles que viajen a velocidades de hasta 250 Km/h. Se trataría de una alternativa para ofrecer estos servicios en trenes de alta velocidad, por ejemplo. Como se aprecia, también existe un cierto solape entre ambos estándares.

Para finalizar esta sección se incluye la *Tabla 3. 1*, en la que se presenta una comparativa entre los estándares IEEE 802.16 (WMAN) e IEEE 802.11 (WLAN).

Las redes de área metropolitana (WMAN) se plantean como una alternativa a los accesos ADSL o de cable para empresas, fundamentalmente. Permiten un despliegue más rápido, económico y flexible. El grupo 802.16 ha producido un estándar de capa MAC que permite tasas de hasta 70 Mbit/s, funcionando sobre una capa física con múltiples variantes de frecuencia, desde 2 a 66 GHz. La revisión 802.16a se conoce popularmente como WiMax, y tiene equipos ya disponibles comercialmente.

### **3.7.2. EL estandar IEEE 802.20**

El grupo IEEE 802.20, de reciente creación, parte del concepto de área metropolitana al que añade movilidad. Especificara, al igual que IEEE 802.16, las capas de acceso al medio y física en bandas de frecuencia inferiores a 3,5 GHz, con un objetivo de tasas superiores a 1 Mbit/s y una movilidad de hasta 250 Km/h.

### **3.7.3. EL estandar IEEE 802.21**

El grupo IEEE 802.21 estudia técnicas para permitir traspasos entre redes heterogéneas (IEEE 802.11/802.16/802.20 y UMTS o GPRS). El objetivo es un estándar que definirá mecanismos independientes del acceso al medio (capa 2). Estos mecanismos permitirán optimizar la detección y selección de los puntos de acceso y los traspasos, procesos que en todo caso son gestionados por entidades de las capas superiores.

### 3.8. SEGURIDAD

La seguridad en las redes inalámbricas presenta una problemática especial debido a varios factores, como son:

- Que el usuario no puede estar seguro de que el punto de acceso al que se conecta pertenezca realmente a la organización que opera el hot spot.
- Podría tratarse de un punto de acceso falso instalado en las proximidades con propósitos fraudulentos.
- Que al utilizarse radio, la comunicación puede estar siendo escuchada por un tercero que disponga de un receptor adecuado.

Estos factores hacen que la seguridad sea un elemento muy importante, que hoy por hoy no está bien resuelto en muchas redes. La seguridad se subdivide en dos aspectos, denominados:

**AUTENTICACION.** Se debe permitir que el usuario esté seguro del punto de acceso al que se conecta y que el sistema identifique al usuario sin comprometer la seguridad futura. Por ejemplo, no sería admisible radiar una palabra de paso sin cifrar, pues alguien que estuviera escuchando tendría desde ese momento libre acceso al sistema.

**PRIVACIDAD.** Los datos intercambiados no deben ser interpretados por terceros que los escuchen.

El estándar IEEE 802.11 incorpora desde el principio un campo en la capa MAC para indicar si se utilizaba cifrado (WEP) o no. WEP (Wired Equivalent Privacy) es un mecanismo que trata de aportar seguridad (autenticación y privacidad) limitada de una forma simple. Este mecanismo presenta debilidades importantes, como son:

- Que el punto de acceso no se autentica ante el cliente.
- Que un tercero puede escuchar la respuesta cifrada y tratar de descubrir la clave compartida en un sistema informático. Las claves originales de WEP son excesivamente cortas, aunque hoy en día muchos fabricantes suministran equipos que permiten utilizar claves más largas.

En definitiva, la seguridad aportada por WEP es escasa e inadecuada para muchos propósitos. Para remediar esto, muchos sistemas acuden a la especificación IEEE 802.1x, que indica como ejecutar EAP (Extensible Authentication Protocol), que es esencialmente un protocolo de transporte que puede ser usado con distintos tipos de autenticaciones, conocidas como métodos EAP, sobre una capa de enlace.

Quizá uno de los mejores métodos de seguridad disponible hoy en día es el uso de VPN IPSec para acceder a la red local de la empresa desde un hot spot, usando un enlace esencialmente inseguro pero una capa de red segura tal como IPSec. Este enfoque sigue requiriendo software específico en los clientes y un terminador de túneles en la empresa (o en la red del ISP), pero no involucra a los hot spots, que son de los que realmente se es cliente esporádico, y, por tanto, difícilmente se tendrá instalado software adecuado a sus características.

### 4. ORGANIZACIONES DE ESTÁNDARES

#### 4.1. IETF

IETF (Internet Engineering Task Force) se define como un grupo de individuos dedicados a la evolución de las tecnologías de Internet. No tiene miembros ni cuotas, cualquier persona puede participar en sus reuniones. El producto de IETF son estándares, denominados RFC (Request For Comments), que recogen especificaciones relacionadas con Internet. Por ejemplo, IP, TCP, SMTP, PPP y ARP aparecieron como RFCs. De ellos, los denominados Internet Standards forman el subgrupo de documentos esenciales para el funcionamiento de Internet.

Actualmente, la orientación hacia arquitecturas “*todo IP*” a que se tiende en el mundo de la telefonía móvil trae consigo la reutilización de protocolos IETF. En particular, SIP (Session Initiation Protocol) es la base del subsistema IP multimedia (IMS) de 3GPP. Además, existen casi cien referencias a RFCs o internetdrafts en las especificaciones 3GPP, entre las que destacan las siguientes:

- *DIAMETER*. Es un protocolo que proporciona un marco de autenticación, autorización y registro de uso (Authentication, Authorization and Accounting, AAA) para aplicaciones de acceso a redes, movilidad en redes IP y roaming. Diameter es compatible con Radius. Se compone de una especificación base mas una serie de especificaciones dependientes de la aplicación. Diameter se utilizara en las redes móviles 3GPP para autenticación en IMS, charging de IMS prepago e interacción con WLAN.
- *SIP (Session Initiation Protocol)*. Es un protocolo de señalización de la capa de aplicación que permite crear y gestionar sesiones con uno o más participantes. Estas sesiones pueden ser llamadas de voz, multimedia, streaming, etc. SIP se basa en los nodos denominados servidores proxy para enrutar, gestionar la autenticación y autorización, y proveer los servicios. En 3GPP, SIP se ha adaptado ligeramente y es la base del subsistema IMS. además del protocolo básico, multiples RFCs e internetdrafts de IETF que extienden las funcionalidades de SIP se utilizan en 3GPP, principalmente para los servicios de presencia IMS.
- *EAP (Extensible Authentication Protocol)*. Define un marco de autenticación directamente sobre capas de enlace, WLAN por ejemplo, sin necesitar IP. Diameter se implementa sobre EAP para permitir la autenticación en una red 3GPP a través de un acceso WLAN.

#### 4.2. UIT

La UIT (Unión Internacional de Telecomunicaciones) forma parte de la red de organizaciones internacionales de las Naciones Unidas. Establecida en 1865 para facilitar el desarrollo internacional del telégrafo, su funcionamiento se basa en la cooperación entre el sector privado y los estados: sus miembros son gobiernos, organismos reguladores, fabricantes y operadores. Las comunicaciones móviles de tercera generación reciben en la UIT el nombre de IMT-2000. Las actividades de la UIT en IMT-2000 abarcan

la normalización internacional, que incluye el espectro de radiofrecuencias y la especificación de la red de acceso radio y troncal, la tarificación y facturación, y los estudios sobre aspectos de reglamentación y política. IMT-2000 cubre tanto comunicaciones móviles terrestres como por satélite.

Desde el punto de vista del acceso, IMT-2000 es un intento de armonización a escala mundial, con el resultado de una familia de sistemas de acceso radio. El proyecto IMT-2000 fue un estímulo importante para el desarrollo de sistemas 3G, ya que diferentes organismos de estandarización regionales enviaron a la UIT propuestas que luego fueron desarrolladas en detalle en distintos foros.

Dentro de la UIT, los accesos radio IMT-2000 se normalizan en la recomendación UIT M.1457. Aprobada en el año 2000, la UIT ha producido sucesivas revisiones para incluir la funcionalidad que los foros de estandarización han añadido a sus especificaciones. La M.1457 no especifica los accesos radio en detalle, esto sería imposible en un solo documento. En su lugar proporciona una lista de referencias a las especificaciones originales.

200

Los grupos UIT involucrados en IMT-2000 son los siguientes:

- **EL GRUPO DE DESARROLLO DE LAS TELECOMUNICACIONES (UIT-D).** Se encarga de realizar estudios y actividades, así como de prestar asistencia directa para fomentar la implementación de las IMT-2000 en los países en desarrollo.
- **EL GRUPO DE RADIOCOMUNICACIONES (UIT-R).** El grupo de trabajo WP8F del UIT-R se encarga del espectro de radiofrecuencias considerado en su conjunto y de los aspectos de radiocomunicaciones de las tecnologías englobadas en IMT-2000 y los sistemas posteriores. Adicionalmente, el grupo de trabajo WP8A se ocupa de los sistemas móviles anteriores a IMT-2000, y el grupo WP8D de los servicios móviles por satélite. Adicionalmente, el grupo WP8F ha comenzado a estudiar las posibilidades tecnológicas para sistemas posteriores a 3G.
- **EL GRUPO DE NORMALIZACION DE LAS TELECOMUNICACIONES (UIT-T).** La Comisión de Estudio Especial del UIT-T sobre las tecnologías IMT-2000 y sistemas posteriores estudia los aspectos de red, lo que incluye la Internet inalámbrica, la convergencia de las redes móviles y fijas, la gestión de la movilidad, las funciones de servicios móviles multimedia, y la interoperabilidad. además, se encarga de introducir mejoras en las recomendaciones vigentes del UIT-T sobre las IMT-2000. Por otro lado, recientemente se ha creado un grupo específico (focus group) sobre NGN (Next Generation Networks) en dicho sector, que concentrara sus actividades en esta materia hasta que concluya la reorganización de la UIT.
- **EL GRUPO DE INVESTIGACION Y ANALISIS.** La Unidad de Estrategias y Política de la Secretaria General de la UIT realiza investigaciones, efectúa análisis y prepara estadísticas sobre las telecomunicaciones consideradas en su conjunto. Una de sus principales esferas de actividad esta representada por las comunicaciones móviles, lo que incluye las IMT-2000 (3G).

Otra actividad de la UIT, de gran impacto en los sistemas móviles, es la coordinación en la asignación de frecuencias en las World Radio Conferences (WRC).

### 4.3. ETSI

El Instituto Europeo de Estándares de Telecomunicación (ETSI, European Telecommunications Standards Institute) es una organización independiente y oficialmente responsable en Europa de la estandarización en los campos de las tecnologías de la información y las comunicaciones; sus miembros son fabricantes, operadores y administraciones de todo el mundo. Los desarrollos sobre radiocomunicaciones en ETSI incluyen éxitos como DECT, TETRA y GSM, responsabilidad este último durante varios años del comité SMG para finalmente pasar el testigo al proyecto 3GPP del que ETSI es socio.

TISPAN es el grupo de ETSI dedicado a la estandarización de servicios y redes fijas, en particular en lo que se refiere a la evolución de redes de circuitos a redes de paquetes. Además, TISPAN es responsable de la convergencia de redes en ETSI y es el grupo que centraliza el trabajo en NGN (Next Generation Networks). Una de las tecnologías estudiadas para las NGN es el subsistema IMS estandarizado por 3GPP. IMS tiene como requisito en 3GPP la independencia de la red de transporte; es decir, un operador podría ofrecer servicios a sus suscriptores independientemente de cómo estos hayan obtenido su acceso a una red IP (UMTS, WLAN o línea fija). Un sistema diseñado de esta forma es atractivo para los operadores de red fija, y TISPAN y 3GPP han comenzado a analizar los aspectos prácticos de la teórica viabilidad del IMS 3GPP para este entorno. Algunos de los aspectos que necesitan clarificarse son las diferentes definiciones de las clases de servicio entre las redes fijas y móviles, la necesidad de la tarjeta SIM o equivalente, los codecs o el soporte a IPv4. La colaboración entre IETF y 3GPP, las redes fijas y las móviles, se repite ahora con TISPAN.

### 5. LA ESTANDARIZACIÓN A MEDIO PLAZO

Parte del éxito de los sistemas móviles, como es el caso del GSM, se debe a la existencia de un estándar ampliamente aceptado. Actualmente están implicados varios foros y entidades de estandarización en el desarrollo de la 3G y su evolución. Cada uno aporta un fragmento al sistema para ofrecer al usuario servicios interoperables sobre un abanico de redes de acceso.

Las dos grandes revoluciones de las telecomunicaciones, el servicio móvil e Internet, se tienden la mano. Como no podía ser de otro modo, esto se plasma, en primer lugar, en las normas y estándares que definen los sistemas. Los protocolos desarrollados por IETF, enfocados a Internet, se retoman y adaptan en las redes IMS para móviles. IMS permitirá a los operadores prestar servicios clásicos de circuitos sobre redes de paquetes, llevando a una red troncal “todo IP”. Y cerrando el bucle, los operadores de telefonía fija podrán reutilizar esta tecnología.

En el acceso radio se produce una fragmentación, el usuario dispondrá de diversas redes de acceso (una red GSM/GPRS/EDGE evolucionada, una red IMT-2000 y un acceso WLAN). Los organismos de estandarización continúan mejorando las tecnologías, para hacerlas transparentes e interoperables, y aumentar así la velocidad y la capacidad. La colaboración entre los grupos de IEEE 802 y 3GPP/3GPP2 conducirá a la posibilidad de realizar traspasos de forma transparente entre redes tecnológicamente tan dispares como WLAN y UTRAN.

La interoperabilidad de los equipos y los servicios es uno de los mayores retos a que se enfrentan las comunicaciones móviles. En este sentido, OMA responde a una necesidad claramente identificada por los operadores móviles y ocupa un espacio que antes estaba vacío.

**ANEXO D:**

**ANALISIS FINANCIERO DE LAS PROPUESTAS DE  
DISEÑO**

### 1. INTRODUCCION.

El presente anexo pretende detallar el estudio financiero de las diferentes opciones de diseño propuestas en el Capítulo 5. La marca de los dispositivos que se relacionan a continuación son sugeridos por motivo de que han sido recomendados por empresas que ya han implementado los sistemas de movilidad y pueden dar fe de su adecuado desempeño, además sus fabricantes poseen una amplia trayectoria a nivel mundial en la fabricación y distribución de dispositivos para la implementación de redes a nivel cableado e inalámbrico como es el caso de CISCO y división LINKSYS en fabrica y distribución de dispositivos para redes inalámbricas.

No obstante, la Universidad del Cauca en el momento que decida implementar una de las propuestas expuestas, posee la flexibilidad de adoptar cualquier proveedor en la adquisición de los dispositivos.

Por otro lado el estudio financiero se ha realizado en forma sectorizada y/o por facultades aprovechando la modularidad que los diseños nos brindan, luego entonces cada facultad puede en forma independiente iniciar su sistema de servicios inalámbricos sin que tenga que depender de el resto de sectores.

## 2. ESTUDIO FINANCIERO DE LA PROPUESTA No. 1

La propuesta numero uno, como el capitulo 5 lo expone consiste en la distribución de NAs en las diferentes facultades, cuidándose de que los niveles de radiación de los mismos no sobrepasen los limites de cada una de las edificaciones; este confinamiento de las células de radiación busca cubrir solo exclusivamente áreas específicas de cada una de las facultades con el fin de cumplir con un parámetro de seguridad frente a usuarios no deseados.

- FACULTAD CIENCIAS DE LA SALUD**

*TABLA D- 1: Costo Total Facultad de Salud*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	7	\$ 210.000	\$ 1'470.000
POW OVER ETHERNET	7	\$ 110.000	\$ 770.000
Puntos de red	8	\$ 200.000	\$ 1'600.000
PC	1	\$ 1'000.000	\$ 1'000.000
WS-C2950-12Cat 2950	1	\$ 1'400.000	\$ 1'400.000
PROTECTOR des ELEC	7	\$ 60.000	\$ 420.000
<b>COSTO TOTAL FACULTAD CIENCIAS DE LA SALUD</b>			<b>\$ 6'660.000</b>

- SECTOR TULCAN**

*TABLA D- 2: Costo Total Sector Tulcán*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	1	\$ 210.000	\$ 210.000
POW OVER ETHERNET	1	\$ 110.000	\$ 110.000
Puntos red	1	\$ 200.000	\$ 200.000
PC	1	\$ 1'000.000	\$ 1'000.000
ANTENA 120ª HG2414SP-120	1	\$ 357.000	\$ 357.000
REPETIDOR.	1	\$ 210.000	\$ 210.000
Pigtail	1	\$ 90.000	\$ 90.000
PROTECTOR des ELEC	2	\$ 60.000	\$ 120.000
<b>COSTO TOTAL SECTOR TULCAN</b>			<b>\$ 2'297.000</b>

• **SECTOR INGENIERIAS**

*TABLA D- 3: Costo Total Sector Ingenierías*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	4	\$ 210.000	\$ 840.000
POW OVER ETHERNET	4	\$ 110.000	\$ 440.000
Puntos red.	5	\$ 200.000	\$ 1'000.000
PC	2	\$ 1'000.000	\$ 2'000.000
WS-C2950-12Cat 2950	1	\$ 1'400.000	\$ 1'400.000
ANTENA HG2414SP-120	1	\$ 357.000	\$ 357.000
PIGTAIL	1	\$ 90.000	\$ 90.000
PROTECTOR des ELEC	4	\$ 60.000	\$ 240.000
<b>COSTO TOTAL SECTOR INGENIERIAS</b>			<b>\$ 6'367.000</b>

• **SECTOR EDUCACION**

*TABLA D- 4: Costo Total Sector Educación*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	2	\$ 210.000	\$ 420.000
POW OVER ETHERNET	2	\$ 110.000	\$ 220.000
Puntos red	3	\$ 200.000	\$ 600.000
PC	2	\$ 1'000.000	\$ 2'000.000
WS-C2950-12Cat 2950	1	\$ 1'400.000	\$ 1'400.000
PROTECTOR des ELEC	2	\$ 60.000	\$ 120.000
<b>COSTO TOTAL SECTOR EDUCACION</b>			<b>\$ 4'760.000</b>

• **MUSEO NATURAL**

*TABLA D- 5: Costo Total Museo Natural*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	3	\$ 210.000	\$ 630.000
POW OVER ETHERNET	3	\$ 110.000	\$ 330.000
Puntos red.	4	\$ 200.000	\$ 800.000
PC	1	\$ 1'000.000	\$ 1'000.000
WS-C2950-12Cat 2950	1	\$ 1'400.000	\$ 1'400.000
PROTECTOR des ELEC	3	\$ 60.000	\$ 180.000
<b>COSTO TOTAL MUSEO NATURAL</b>			<b>\$ 4'340.000</b>

## ANEXO D: ANALISIS FINANCIERO DE LAS PROPUESTAS DE DISEÑO

- **ZONA CENTRICA: CARMEN S/DOMINGO ARTES VICERRECTORIA DE CULTURA Y BIENESTAR**

**TABLA D-6:** Costo Total Zona Céntrica

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	6	\$ 210.000	\$ 1'260.000
POW OVER ETHERNET	6	\$ 110.000	\$ 660.000
Puntos red	9	\$ 200.000	\$ 1'800.000
PC	4	\$ 1'000.000	\$ 4'000.000
WS-C2950-12Cat 2950	3	\$ 1'400.000	\$ 4'200.000
PROTECTOR des ELEC	6	\$ 60.000	\$ 360.000
<b>COSTO TOTAL ZONA CENTRICA</b>			<b>\$12'280.000</b>

- **SECTOR LAS GUACAS**

**TABLA D- 7:** Costo Total Sector Las Guacas

DESCRIPCION	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	2	\$ 210.000	\$ 420.000
POW OVER ETHERNET	2	\$ 110.000	\$ 220.000
Puntos red.	2	\$ 200.000	\$ 400.000
PC	2	\$ 1'000.000	\$ 2'000.000
PROTECTOR des ELEC	2	\$ 60.000	\$ 180.000
<b>COSTO TOTAL SECTOR LAS GUACAS</b>			<b>\$ 3'220.000</b>

- **RELACION DEL VALOR TOTAL DE LA PROPUESTA No 1**

**TABLA D- 8:** Relación del Valor Total de la Propuesta No. 1

SECTOR	VALOR
MEDICINA	\$ 6'660.000
TULCAN	\$ 2'297.000
INGENIERIAS	\$ 6'367.000
EDUCACION	\$ 4'760.000
MUSEO NATURAL	\$ 4'340.000
ZONA CENTRICA: EL CARMEN, S/DOMINGO, ARTES, CASA CALDAS.	\$ 12'280.000
LAS GUACAS	\$ 3'220.000
<b>VALOR TOTAL</b>	<b>\$ 39'924.000</b>

### 3. ESTUDIO FINANCIERO DE LA PROPUESTA No. 2

En esta propuesta se busca interconectar radioeléctricamente las diferentes celdas que ya han sido propuestas en la opción número uno, para ello el uso de antenas de diferente tipo y el uso de sectores particulares cobra importancia en pro de conseguir este objetivo.

- FACULTAD CIENCIAS DE LA SALUD**

**TABLA D- 9:** Costo Total Facultad Ciencias de la Salud

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	7	\$ 210.000	\$ 1'470.000
POW OVER ETHERNET	7	\$ 110.000	\$ 770.000
Puntos de red	8	\$ 200.000	\$ 1'600.000
PC	1	\$ 1'000.000	\$ 1'000.000
WS-C2950-12Cat 2950	1	\$ 1'400.000	\$ 1'400.000
ANTENAHG2412U	1	\$ 140.000	\$ 140.000
PIGTAIL	1	\$ 90.000	\$ 90.000
PROTECTOR des ELEC	7	\$ 60.000	\$ 420.000
<b>COSTO TOTAL FACULTAD CIENCIAS DE LA SALUD</b>			<b>\$ 6'890.000</b>

- SECTOR TULCAN**

**TABLA D- 10:** Costo Total Sector Tulcán

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
AP	1	\$ 210.000	\$ 210.000
POW OVER ETHERNET	1	\$ 110.000	\$ 110.000
Puntos red	1	\$ 200.000	\$ 200.000
PC	1	\$ 1'000.000	\$ 1'000.000
ANTENA HG2412U	2	\$ 140.000	\$ 280.000
REPETIDOR.	1	\$ 210.000	\$ 210.000
Pigtail	2	\$ 90.000	\$ 180.000
PROTECTOR des ELEC	2	\$ 60.000	\$ 120.000
<b>COSTO TOTAL SECTOR TULCAN</b>			<b>\$ 2'310.000</b>

• **SECTOR INGENIERIAS**

*TABLA D- 11: Costo Total Sector Ingenierías*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	4	\$ 210.000	\$ 840.000
POW OVER ETHERNET	4	\$ 110.000	\$ 440.000
Puntos red.	5	\$ 200.000	\$ 1'000.000
PC	2	\$ 1'000.000	\$ 2'000.000
WS-C2950-12Cat 2950	1	\$ 1'400.000	\$ 1'400.000
ANTENA HG2414SP-120	1	\$ 357.000	\$ 357.000
PIGTAIL	1	\$ 90.000	\$ 90.000
PROTECTOR des ELEC	4	\$ 60.000	\$ 240.000
<b>COSTO TOTAL SECTOR INGENIERIAS</b>			<b>\$ 6'367.000</b>

• **SECTOR EDUCACION**

*TABLA D- 12: Costo Total Sector Educación*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	6	\$ 210.000	\$ 1'260.000
POW OVER ETHERNET	6	\$ 110.000	\$ 660.000
Puntos red	7	\$ 200.000	\$ 1'400.000
PC	3	\$ 1'000.000	\$ 3'000.000
WS-C2950-12Cat 2950	1	\$ 1'400.000	\$ 1'400.000
ANTENA HG2412U	2	\$ 140.000	\$ 280.000
ANTENA HG2414SP-120	1	\$ 357.000	\$ 357.000
ANTENA HG2414P-NF	1	\$ 80.000	\$ 80.000
PIGTAIL	4	\$ 90.000	\$ 360.000
PROTECTOR des ELEC	6	\$ 60.000	\$ 360.000
<b>COSTO TOTAL SECTOR EDUCACION</b>			<b>\$ 6'457.000</b>

• **MUSEO NATURAL**

*TABLA D- 13: Costo Total Museo Natural*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	4	\$ 210.000	\$ 840.000
POW OVER ETHERNET	3	\$ 110.000	\$ 330.000
Puntos red.	4	\$ 200.000	\$ 800.000
PC	1	\$ 1'000.000	\$ 1'000.000
WS-C2950-12Cat 2950	1	\$ 1'400.000	\$ 1'400.000
ANTENA HG2414SP-120	1	\$ 357.000	\$ 357.000
PIGTAIL	1	\$ 90.000	\$ 90.000
PROTECTOR des ELEC	4	\$ 60.000	\$ 240.000
<b>COSTO TOTAL MUSEO NATURAL</b>			<b>\$ 5'057.000</b>

• **ZONA CENTRICA: CARMEN S/DOMINGO ARTES VICERRECTORIA DE CULTURA Y BIENESTAR**

*TABLA D- 14: Costo Total Zona Céntrica*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
*WRT54G	9	\$ 210.000	\$ 1'890.000
POW OVER ETHERNET	9	\$ 110.000	\$ 990.000
Puntos red	12	\$ 200.000	\$ 2'400.000
PC	4	\$ 1'000.000	\$ 4'000.000
WS-C2950-12Cat 2950	3	\$ 1'400.000	\$ 4'200.000
ANTENA HG2414SP-120	1	\$ 357.000	\$ 357.000
ANTENA HG2409PCR	1	\$ 62.000	\$ 62.000
ANTENA HG2415P-180	1	\$ 1'000.000	\$ 1'000.000
PIGTAIL.	3	\$ 90.000	\$ 270.000
PROTECTOR des ELEC	9	\$ 60.000	\$ 540.000
<b>COSTO TOTAL ZONA CENTRICA</b>			<b>\$15'709.000</b>

• **SECTOR LAS GUACAS**

*TABLA D- 15: Costo Total Sector Las Guacas*

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRT54G	2	\$ 210.000	\$ 420.000
POW OVER ETHERNET	2	\$ 110.000	\$ 220.000
Puntos red.	2	\$ 200.000	\$ 400.000
PC	2	\$ 1'000.000	\$ 2'000.000
PROTECTOR des ELEC	2	\$ 60.000	\$ 120.000
<b>COSTO TOTAL LAS GUACAS</b>			<b>\$ 3'160.000</b>

• **EDIFICIOS PARTICULARES**

**TABLA D- 16:** Costo Total Edificios Particulares

DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
WRE54G	2	\$ 210.000	\$ 420.000
Puntos de red	3	\$ 200.000	\$ 600.000
ANTENA HG2414HSP-090	1	\$ 300.000	\$ 300.000
ANTENA HG2414P-NF	1	\$ 80.000	\$ 80.000
PIGTAIL	2	\$ 90.000	\$ 180.000
PROTECTOR des ELEC	2	\$ 60.000	\$ 120.000
<b>COSTO TOTAL EDIFICIOS PARTICULARES</b>			<b>\$ 1'700.000</b>

• **RELACION DEL VALOR TOTAL DE LA PROPUESTA No. 2**

**TABLA D- 17:** Relación del Valor Total de la Propuesta No. 2

SECTOR	VALOR
MEDICINA	\$ 6'890.000
TULCAN	\$ 2'310.000
INGENIERIAS	\$ 6'367.000
EDUCACION	\$ 6'457.000
MUSEO NATURAL	\$ 5'057.000
ZONA CENTRICA: EL CARMEN, S/DOMINGO, ARTES, CASA CALDAS.	\$ 15'709.000
LAS GUACAS	\$ 3'160.000
EDIFICIOS PARTICULARES	\$ 1'700.000
<b>VALOR TOTAL</b>	<b>\$47'650.000</b>

## **ANEXO E**

**SERVICIOS PRESTADOS SOBRE LAS REDES MOVILES.**

## **1. INTRODUCCION.**

El presente documento da una visión general sobre la evolución de los diferentes sistemas celulares y las arquitecturas de movilidad la compatibilidad entre si y su legislación de operación en loas diferentes partes del mundo.

### 2. REGLAS Y PROTOCOLOS

#### 2.1. ARQUITECTURA Y PROTOCOLOS PARA SERVICIOS SOBRE REDES GPRS Y UMTS

Los Servicios de Valor Agregado (SVA) se definen en la Ley de la Ordenación de las Telecomunicaciones como:

"Servicios de telecomunicación que, no siendo servicios de difusión y utilizando como soporte servicios portadores o servicios finales de telecomunicación, añaden otras facilidades al servicio soporte, o satisfacen nuevas necesidades específicas de telecomunicaciones como, entre otras, acceder a información almacenada, enviar información, o realizar el tratamiento, depósito y recuperación de información".

Como se puede ver, este enfoque de los SVA está centrado en los servicios de telecomunicación ofrecidos por las operadoras. La aparición de las nuevas redes de datos GPRS y UMTS, permite a los usuarios disponer de una amplia gama de servicios que no son exclusivamente de telecomunicación y que no son proporcionados únicamente por los operadores de redes móviles.

Los servicios que los operadores de redes GSM proporcionan actualmente son primordialmente servicios conversacionales, aunque existen otros de menor importancia. Estos servicios conversacionales permiten a los usuarios de las redes móviles, realizar llamadas a usuarios de otras redes móviles y/o fijas. Se dividen en:

- **Llamadas y facilidades de llamadas**

Existe un gran número de facilidades y servicios vocales: desvío de llamadas, visualización de la identidad del llamante, restricciones de llamadas, etc.

- **Redes privadas virtuales**

Servicio que permite disponer de la funcionalidad típica de centralita (planes privados de numeración, restricciones de llamadas, etc.) desde los terminales móviles y/o fijos, sin necesidad de disponer de equipos adicionales en las instalaciones de los abonados al servicio.

- **Servicios de datos**

Pueden ser:

- **SERVICIOS DE MENSAJERÍA:** Estos servicios permiten el envío de mensajes de texto entre terminales móviles, y entre terminales y la red: SMS, USSD, Chat, envío de SMS desde aplicaciones externas a la red móvil, etc.
- **SERVICIOS PORTADORES DE DATOS:** Servicios que proporcionan un canal de datos a utilizar por aplicaciones informáticas: acceso a Intranet de empresas, acceso a Internet, etc.

Todos estos servicios, tanto básicos como de valor agregado, poseen dos características comunes: el operador de red proporciona el servicio completo y el usuario debe proporcionar la información del servicio a utilizar, antes de acceder a él. Esta última característica permite que el servicio se controle desde un único punto: el de acceso.

Las arquitecturas para el desarrollo de SVA pueden, bien estar soportadas por este modelo, implementando servicios en los nodos de acceso (centrales digitales o MSC), o bien por un modelo de delegación, como por ejemplo el modelo de la Red Inteligente (RI).

Adicionalmente, la provisión de nuevos servicios de Internet a los que se podrá acceder a través de GPRS y UMTS, se están introduciendo nuevos requisitos para las arquitecturas de servicio, haciendo que el esquema de RI ya no sea adecuado para el nuevo entorno de red. Estos servicios pueden clasificarse en:

- **Servicios que resultan de la evolución de los actuales**

Los servicios de comunicaciones actuales se están adaptando a las nuevas arquitecturas de datos y redes de transmisión. Conservan los dos rasgos básicos vistos anteriormente: serán proporcionados en su integridad por el operador y dispondrán de un único punto de control.

- **Servicios de internet**

Estos servicios poseen características diferentes a las descritas anteriormente: el operador de red no tiene por qué dar el servicio completo (contemplando la posibilidad de que lo que quiere consumir el usuario y la lógica del servicio, o al menos una parte de ella, estén fuera de la red del operador) y el usuario no tiene por qué dar a priori la información del servicio que va a utilizar (el usuario va accediendo a diferentes niveles de servicio, en cada nivel puede decidir qué bienes o servicios desea consumir, es decir, el entorno de decisión es dinámico).

Estas características condicionarán las arquitecturas y protocolos para la realización de servicios de valor agregado, ya que la lógica del servicio estará distribuida parte en la red del operador móvil y parte fuera de ella. Aparecen, por tanto, los siguientes factores de complejidad, que es necesario considerar por su importancia:

- La dificultad que tiene el control tanto de la conectividad como de los servicios entre los terminales y usuarios con alta movilidad.
- La alta diversidad tecnológica y administrativa, hace que la provisión de servicios y de "service level agreements" requiera una cooperación entre operadores, así como entre tecnologías de red diferentes.
- Las nuevas redes requieren mecanismos para la interoperación de inteligencia "dentro" y "fuera" de la red.
- La gestión de calidad y la facturación de los servicios requiere mecanismos muy diferentes entre las redes de paquetes y las redes de conmutación de voz.
- La provisión de nuevos servicios de Internet que resulten de la migración de los ya establecidos por la segunda generación, donde, o el operador controla el servicio

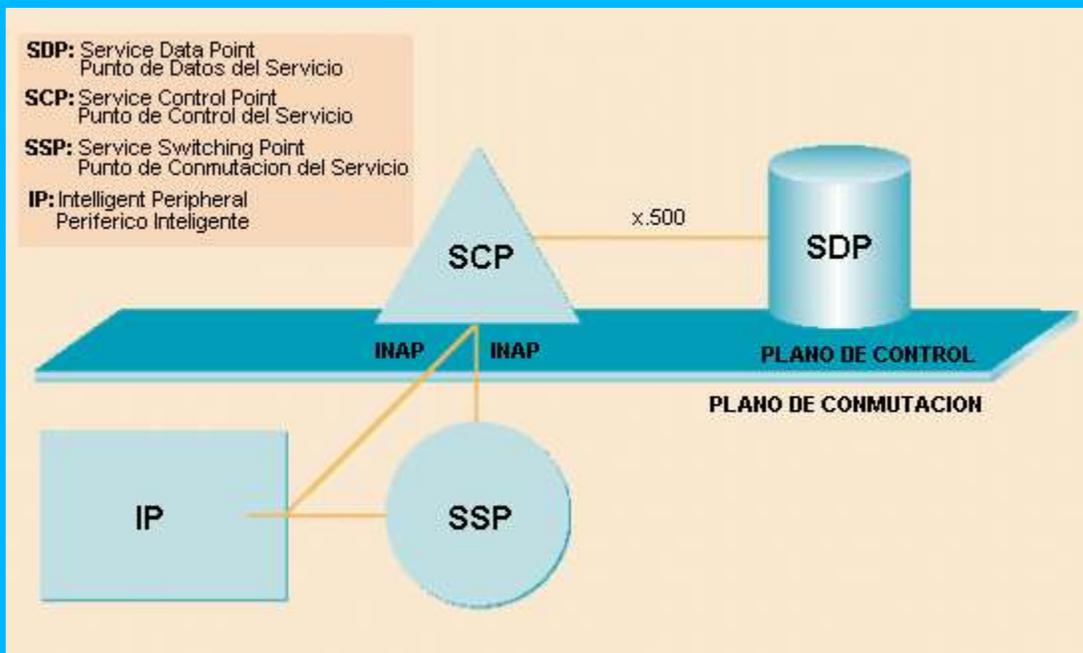
desde un único punto (el acceso), o como Servicios de Internet donde el entorno de decisión es dinámico para el usuario y ofrece mayor flexibilidad a los proveedores de servicios.

Bajo estas condiciones las arquitecturas y protocolos sobre los que los operadores móviles buscan apoyarse para la prestación de SVA son:

### 2.1.1. La arquitectura de RI (Red Inteligente)

La arquitectura de RI es actualmente un estándar de la ITU-T, que define un modelo de elementos y relaciones que permite la prestación de SVA; donde la idea que subyace en la RI es separar el control de servicios, de la función de conmutación, con el fin de crear una arquitectura de servicios más fácil de gestionar y más eficiente en la creación de nuevos servicios; especificando dos niveles: el plano de control y el de conmutación. Cada uno con elementos específicos para el establecimiento gestión y control de llamada. La *Figura E-1* muestra la Arquitectura de Red Inteligente.

*Figura E-1: La Arquitectura de RI*



### 2.1.2. La arquitectura de CAMEL

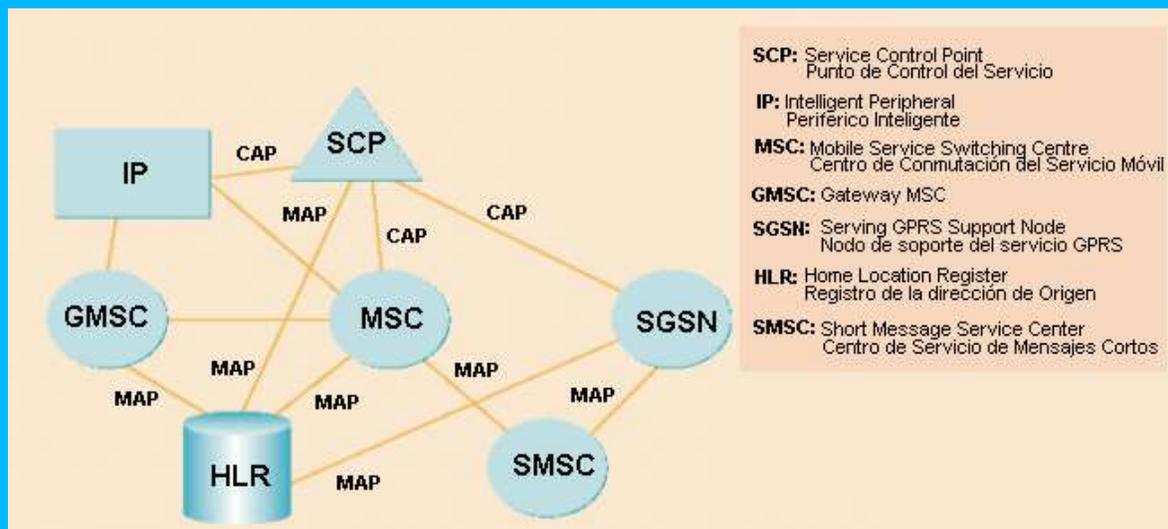
La estandarización de GSM comenzó cuando todavía no se había empezado a estandarizar la RI. Inicialmente GSM fue ideado siguiendo el modelo de RDSI, es decir, se estandarizaron los mismos servicios suplementarios y no la arquitectura de servicios.

Cuando nacieron los estándares de la RI pronto se vio el potencial de aplicarlos a las redes móviles, sin embargo resultó que la arquitectura de la RI se podía aplicar trivialmente a las redes móviles por el efecto roaming. El roaming hace que un usuario puede estar conectado a otra red diferente de la que tiene su suscripción, y en la que, por tanto, se encuentran sus datos y se ejecutan sus servicios.

El efecto roaming y los requerimientos particulares de la movilidad se abordaron mediante la Customized Applications for Mobile network Enhanced Logic (CAMEL), definido por la ETSI, el cual describe una arquitectura similar a la de la RI, pero aplicada a redes móviles.

En resumen CAMEL ofrece una gran riqueza de posibilidades para asociar SVA a la gestión de movilidad. CAMEL permite al operador trasplantar los servicios clásicos de la RI al entorno de red móvil, pero además permite prestar nuevos servicios que son propios de los terminales móviles. La *Figura E-2* muestra los elementos de red de la Arquitectura de Camel.

*Figura E-2: Elementos de Red de CAMEL*



### 2.1.3. El estándar MOBILE IP

Un aspecto crítico en la convergencia entre las comunicaciones móviles y los servicios de datos, es la posibilidad de ofrecer movilidad a servicios basados en IP, de manera transparente para los protocolos de la capa superior. Mobile IPv4 es un estándar propuesto por IETF para resolver este problema, permitiendo al nodo móvil la posibilidad de usar dos direcciones IP: una dirección fija de la red a la que pertenece (home address) y una dirección "de visita" que varía en función del punto de red donde se conecte cada vez (care-of address).

Son tres los mecanismos sustanciales que articulan el modo de operación en Mobile IPv4:

1. *EL DESCUBRIMIENTO DE LA CARE-OF ADDRESS*: Con este procedimiento, el nodo móvil obtiene la que será su care-of address durante su estancia en una red en la que un Foreign Agent gestiona las direcciones IP de los nodos visitantes.
2. *EL REGISTRO DE LA CARE-OF ADDRESS*: Una vez que el nodo móvil ha obtenido una care-of address, su Home Agent debe conocerla. El proceso comienza cuando el nodo móvil envía una petición de registro con la información de la care-of address. Cuando el Home Agent recibe esta petición, añade la información necesaria a su tabla de enrutamiento y responde al Foreign Agent aceptando la petición.
3. *EL TUNELAJE HACIA LA CARE-OF ADDRESS*: Cuando el Home Agent acepta la petición, comienza a asociar la dirección de red propia del nodo móvil con la dirección care-of address. El mantenimiento de esta asociación está temporizado y el mecanismo de tunelaje, por defecto, es encapsular IP sobre IP. Asimismo, el Home Agent (origen del túnel) inserta una nueva cabecera IP (cabecera de túnel) delante de la cabecera IP de cualquier paquete dirigido a la home address del nodo móvil.

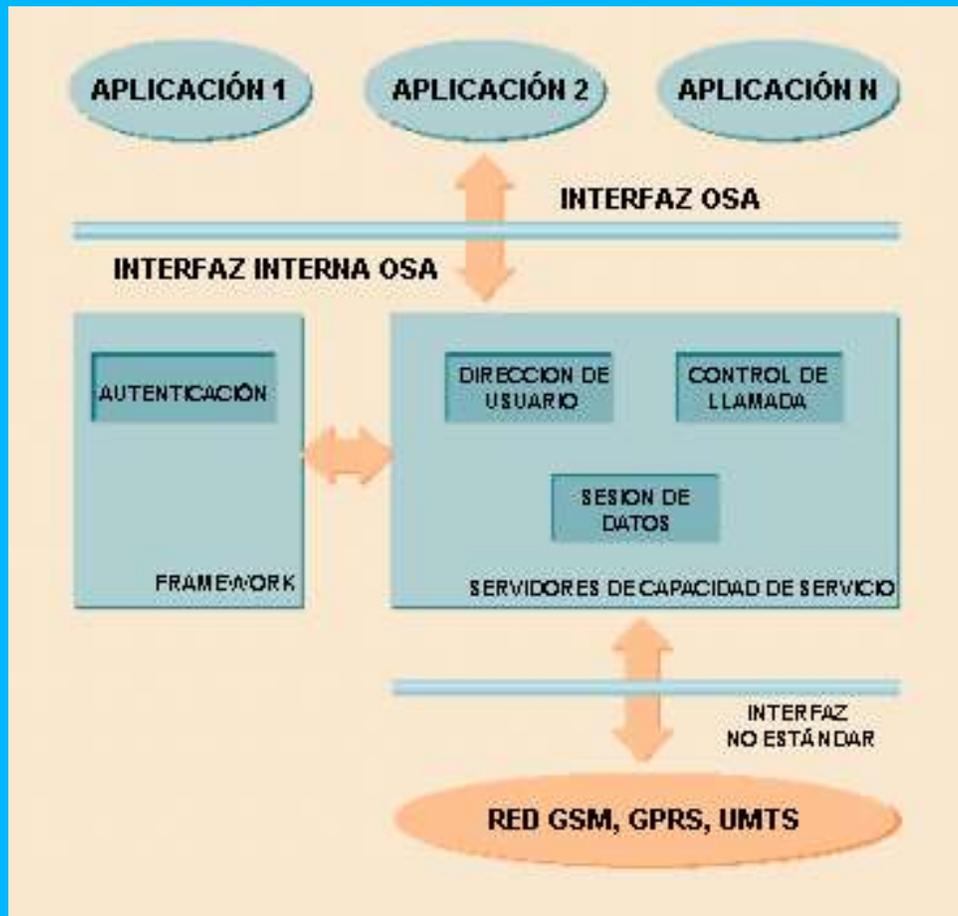
En la prestación de los SVA, el hecho de que un terminal móvil conserve su dirección IP, cuando esté realizando roaming entre las redes de los operadores, facilita enormemente la implementación de los SVA basados en la identidad IP del usuario. Sin embargo, hay que tener en cuenta que:

- El proceso de Mobile IPv4 es costoso desde el punto de vista de la red, por lo que las implementaciones reales posiblemente pasarán por activar el modo "Mobile IP" únicamente cuando sea necesario.
- No todas las redes dispondrán de Mobile IPv4, por lo que será necesario seguir considerando los casos en que la IP es dinámica, lo cual produce interrupciones del servicio.
- Las situaciones en las cuales es necesario aplicar Mobile IPv4 pueden ser excepcionales, ya que el roaming no se produce de manera frecuente y pocos servicios son tan críticos que no puedan ser interrumpidos.

### **2.1.4. La arquitectura de OSA**

Las especificaciones de UMTS han introducido una nueva dimensión de complejidad para la que CAMEL no resulta adecuado. Contrario a la red GSM, que es predominantemente una red de voz conmutada, la red UMTS es una red de integración total de comunicaciones de voz y datos, basada completamente en el transporte y enrutamiento de paquetes, en busca de la convergencia definitiva de Internet, la red de telefonía, la red móvil, la red de difusión de televisión y radio. El modelo de provisión de servicios de CAMEL resultó demasiado restrictivo para este entorno generalizado. La *Figura E-3* muestra la Arquitectura de OSA.

Figura E-3: Arquitectura de OSA



Por tanto, los organismos de estandarización decidieron generalizar los conceptos de RI y CAMEL, con la creación de una plataforma "abierto" de servicios que permite la provisión de éstos a través de tecnologías y administraciones diferentes, fue así que se creó la Open Service Architecture (OSA). OSA es un estándar del 3GPP que define una arquitectura que permite al operador de red y a las aplicaciones de terceras partes utilizar la funcionalidad de la red móvil, a través de una interfaz abierta y estandarizada. Es decir, es una forma de publicar las facilidades de la red móvil UMTS para que puedan ser fácilmente utilizadas, ocultando las características y problemáticas de implementación de los distintos proveedores de redes de telecomunicación.

La arquitectura de OSA define tres niveles en la frontera con el operador de red:

1. **EL NIVEL DE APLICACIONES**, que es el espacio de las aplicaciones que implementan los SVA. Estas aplicaciones son las que utilizarán la interfaz OSA para acceder a los recursos de la red móvil. Las aplicaciones pueden ser propias del operador de red o de terceros.

2. *EL NIVEL DE SERVICIOS BÁSICOS O "FRAMEWORK"*: Es el espacio de las aplicaciones básicas necesarias para establecer el entorno apropiado para utilizar las facilidades de red. Algunos ejemplos son: autenticación, búsqueda de capacidades de servicio, etc.
3. *EL NIVEL DE SERVIDORES DE CAPACIDADES DE SERVICIO (SCS)*: Es el espacio de las aplicaciones donde se proporciona una interfaz OSA sobre las funciones de red del operador móvil.

Este último nivel ofrece facilidades para: Control de llamadas, Sesión de datos, Localización de usuario de red, Estatus de usuario; Capacidades de Terminal y Transferencia de Mensajes.

La definición que se hace de OSA por 3GPP es bastante abstracta. Sin embargo, se ha encontrado apoyo para su implementación en dos iniciativas industriales: Las interfaces Parlay y JAIN.

- **La interfaz PARLAY**

Parlay fue la respuesta a uno de los problemas clave para los operadores: que es el de proporcionar SVA y mantener "service level agreements" en un entorno mucho más complejo que la red tradicional de telefonía. Es la definición de una interfaz estandarizada y abierta, para permitir el acceso a los recursos de las redes de los operadores a aplicaciones que no tienen por qué residir en el dominio del operador.

La interfaz de Parlay está descrita en UML y CORBA IDL. Esta interfaz, además de permitir el acceso a los servicios de la red del operador de telecomunicaciones, define unos servicios para asegurar que el acceso a los recursos se realice de forma controlada y sólo a aquellas zonas que permita el operador de red.

Algunas de las aplicaciones típicas que podrían realizarse utilizando Parlay son:

- Los centros inteligentes y distribuidos de atención al cliente. Parlay permite a un "call center" o centro de llamadas tratar sus propias llamadas, en lugar de confiar en los servicios del operador.
- Un uso generalizado de Parlay es realizar llamadas gratuitas al centro de atención al cliente a través de una página Web (servicio "clic-to-dial").
- Los servicios Business to Business. Por ejemplo, los centros de traducción simultánea distribuidos utilizan Parlay para redirigir las llamadas entrantes al traductor disponible y relevante.
- Los SVA o de llamadas, tanto para redes GSM como para voz sobre IP.
- El hecho de disponer de una interfaz estandarizada, con un alto grado de seguridad, para acceder a los recursos de las redes de los operadores de

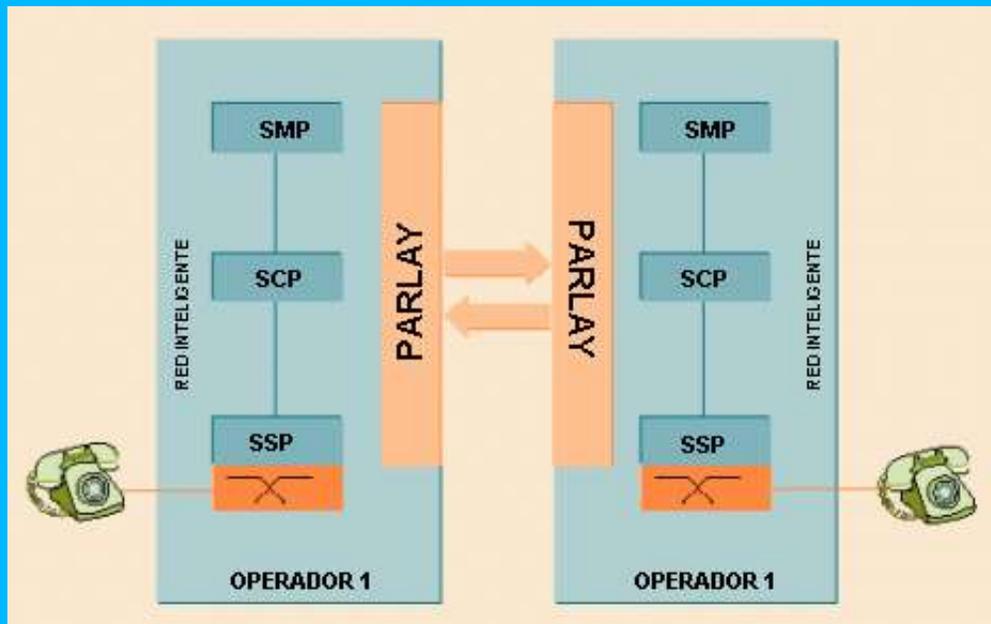
telecomunicaciones, permite que Parlay sea útil para solucionar los problemas de interconexión entre redes de distintos operadores.

- Las aplicaciones de control de flota, en las que empresas como centrales de taxis o transporte público pueden disponer de información de localización de vehículos a través de la interfaz Parlay.

Es necesario aclarar que CAMEL también permite realizar este tipo de servicios, bajo el supuesto de que ambas redes disponen de estos protocolos y de que existe un acuerdo entre los operadores.

El entorno de Parlay es más seguro y controlable por los operadores, por lo que el acuerdo a alcanzar puede ser menos estricto. La *Figura E- 4* muestra la comunicación entre redes a través de Parlay.

**Figura E-4:** Comunicación entre redes a través de Parlay



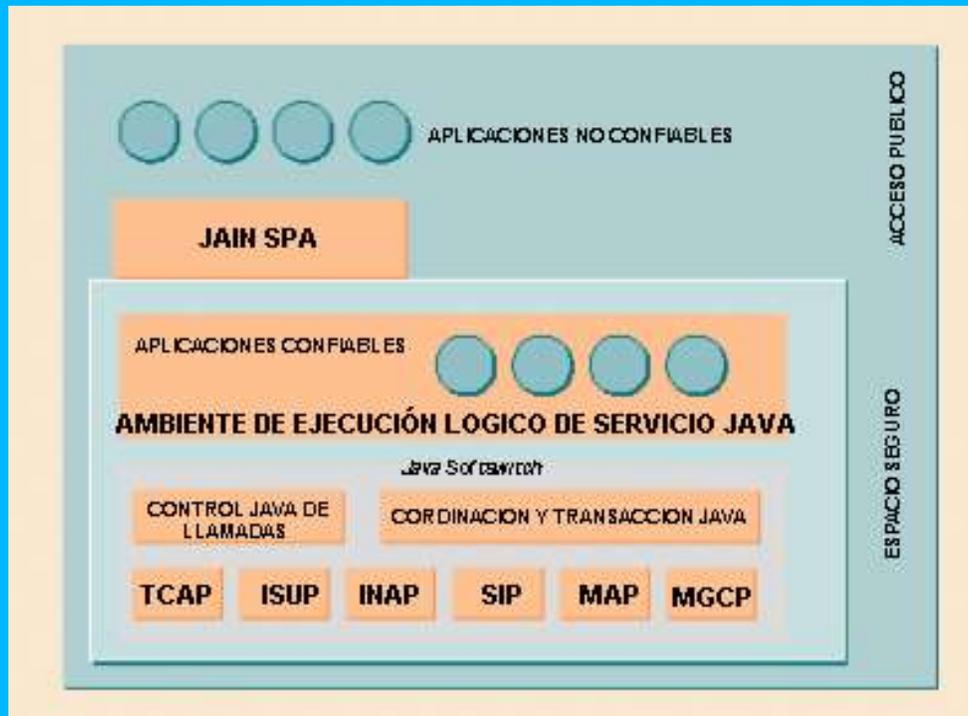
- **La interfaz JAIN**

Java Applications for Intelligent Networks (JAIN) fue una iniciativa de la comunidad de desarrolladores de Java (Java Developer Community) de la compañía Sun, para definir unas interfaces en Java mediante las cuales se pudiera utilizar todos los protocolos habituales en telefonía y voz sobre IP. La *Figura E- 5* muestra la Arquitectura de Jain.

En la interfaz de JAIN se definen niveles de entorno de ejecución de aplicaciones de los operadores que utilicen las interfaces Java, para la prestación de SVA (Java Service Logic

Execution Environment), que es una abstracción del modelo de control de llamada (Java Call Control) de nivel de interfaces de señalización de red (Basic interfaces) que proporciona acceso a las capacidades de señalización de los operadores de red. Puede proporcionar interfaces de SS7, tales como TCAP, ISUP, INAP y MAP, e interfaces del entorno de voz sobre IP, tales como H323, SIP. Y JAIN Service Provider Access (SPA). Interfaz de acceso a las funciones de red de aplicaciones que necesiten niveles de seguridad y control de acceso específicos.

**FiguraE- 5:** Arquitectura de JAIN



Puede parecer que JAIN y Parlay tienen muchos puntos en común, sin embargo existen algunas diferencias importantes entre ambas interfaces:

- Parlay define una interfaz entre la inteligencia "dentro" y "al margen" de la red. Sin embargo, JAIN pretende, fundamentalmente, aprovechar el entorno de desarrollo Java para la creación de servicios de RI.
- Parlay sólo define la interfaz, no implementaciones. En cambio, JAIN está orientado a producir librerías y APIs.
- JAIN define el entorno de ejecución de las aplicaciones.
- Parlay está pensada para que aplicaciones de terceros utilicen las funciones de los operadores de red, por lo que el marco de seguridad es importante. Sin embargo, JAIN originalmente se limitaba al dominio del operador.

### 2.2. LOS SERVICIOS DE LAS REDES 3G

La motivación principal para iniciar la especificación de OSA ha sido el deseo de crear nuevos servicios que representarán el valor agregado de los servicios de 3G. Comparando los servicios actuales de RI con las redes 3G móviles, se pueden reconocer cuatro categorías:

1. Servicios que tienen sentido tanto en la red fija como en la red 3G, por ejemplo, el desvío o bloqueo de llamadas.
2. Servicios de red fija que no tienen sentido en redes 3G, por ejemplo, "call forward on busy" no es relevante para los servicios de datos en los cuales el usuario siempre está conectado y no existe la noción de estar "ocupado".
3. Servicios de red fija que deben ser reimplementados para tener sentido en redes 3G, por ejemplo, todos los servicios de facturación deben ser adaptados para un entorno en que se factura la comunicación por volumen, no por tiempo de conexión.
4. Los nuevos servicios 3G que no existían anteriormente en las redes fijas.

Es evidente que el modelo de negocio de UMTS dependerá, en gran parte, de la última categoría de servicios. Esta categoría determinará el valor agregado de las redes 3G. ETSI ha introducido el concepto de Virtual Home Environment (VHE), que define la personalización y presencia virtual de UMTS.

En sus documentos ETSI define el VHE como un concepto con dos componentes claves:

1. **LA PERSONALIZACIÓN:** VHE permite un alto grado de personalización de servicios, lo cual quiere decir que los servicios se ejecutan a partir de perfiles personales. Estos perfiles personales determinan dónde, cuándo y cómo un usuario quiere recibir sus llamadas, definiendo éstas el 'look and feel' (la interfaz de usuario) del servicio. Los perfiles deben ser modificables desde cualquier localidad y los que se gestionan dentro del terminal (o USIM) deben ser recuperables ante pérdidas de conexión, batería o robo del terminal (es decir, tienen backup en red).
2. **EL ACCESO UNIVERSAL:** VHE permite el acceso a todos los servicios de la Home Network desde cualquier red visitada, incluso si la red visitada no soporta dichos servicios. Esta condición es muy significativa y tiene un impacto importante sobre la arquitectura de VHE. Además, VHE también permite al usuario utilizar servicios locales en la red visitada, incluso si no tiene suscripción para estos servicios en la Home Network.

Desde el punto de vista del usuario, la diferencia entre el usuario particular y corporativo es muy significativa para la definición del VHE, ya que estos grupos tienen requisitos muy diferentes, de modo que:

- Para usuarios corporativos, VHE será considerado una extensión de su VPN y su Intranet.

- Para particulares, VHE será una extensión del PC y del teléfono (móvil o fijo). El operador tendrá que implementar un conjunto de servicios concretos que proporcionen el concepto VHE según los requisitos del usuario. La implementación del VHE tendrá tres dimensiones:

1. *LA CONECTIVIDAD:* El acceso universal al VPN o la Intranet de empresas implica no sólo una cobertura universal, sino también que el operador tendrá que asegurar niveles de seguridad y Quality of Service (QoS).
2. *LOS SVA:* La gestión de perfiles personales y la mensajería unificada implica un control de servicios 'inteligentes' a través de operadores. El VHE requiere entonces la implantación de CAMEL y de acuerdos entre operadores para dejar el control de servicios a la Home Network.
3. *LA FACTURACIÓN:* El concepto del VHE implica una alta movilidad de usuarios y, por tanto, de servicios que tendrán que facturarse entre operadores.

### 3. ESTANDARIZACIÓN DE LOS SISTEMAS CELULARES DE TERCERA GENERACIÓN

#### 3.1. IMT – 2000

La tercera generación de comunicaciones móviles agrupa varios sistemas como son: UMTS, cdma2000 y UWC-136, que han sido desarrollados por los foros 3GPP, 3GPP2 y UWCC, respectivamente, todos como familia del IMT-2000.

Los grandes objetivos del IMT-2000 son:

- Reserva de una porción de espectro común en todo el mundo, tanto para sistemas terrestres como de satélite.
- Uso de terminales móviles, con capacidad de itinerancia mundial y capacidad para acceder a servicios multimedia.
- Maximizar la compatibilidad de las interfaces radio para poder operar en distintos entornos.
- Alta velocidad de transmisión de datos, con capacidad para soportar tanto conmutación de circuitos como de paquetes.
- Los Sistemas multimedia.
- Capacidad de soportar servicios simétricos y asimétricos en todos los entornos de operación.
- Compatibilidad de servicios dentro de IMT-2000 con la red fija.
- Favorecer la normalización de un entorno de creación de servicios que pueda ser utilizado por los operadores para definir sus propios servicios.
- Eficiencia espectral, flexibilidad en el uso y reducción de costes, como resultado de la utilización de nuevas tecnologías.

El resultado de los trabajos de la ITU se recoge en una serie de recomendaciones, documentos de carácter general que delimitan las características que deben tener los sistemas de tercera generación.

De estas recomendaciones, probablemente la de mayor interés es la *M.1457*, que recoge un resumen de las interfaces radioeléctricas de los sistemas IMT-2000.

#### 3.1.1. Historia del IMT – 2000

Las RTTs (Radio Transmission Technologies) son elementos clave para la definición de los sistemas de tercera generación. Con un plazo que expiraba en junio de 1998, la ITU lanzó una petición formal para la presentación de RTTs candidatas a su utilización en los nuevos sistemas. Se presentaron diez propuestas: dos europeas, cuatro de EE UU, dos de Corea, una de Japón y una de China.

Excepto en dos de las propuestas (la UWC-136 americana, que se describirá posteriormente, y la DECT europea) basadas en TDMA, la técnica de acceso a radio elegida fue la DS-CDMA (Direct Spread CDMA). Las ocho propuestas elegidas se pueden dividir en tres clases distintas, basándose en las especificaciones de sistema (tasa de chip, funcionamiento síncrono / asíncrono de la estación base, modo de transmitir las secuencias de piloto) las cuales son:

1. UTRA (Europa-ETSI), W-CDMA (Japón-ARIB), WCDMA/NA (EEUU- T1P1), CDMA II (Corea-TTA) y WIMS-WCDMA (EEUU-TIA TR46.1).
2. cdma2000 (EE UU-TIA TR45.5) y CDMA I (Corea-TTA).
3. TD-SCDMA (China-CATT).

A la fase de presentación siguió otra de consenso, para la decisión sobre cuales de las candidaturas cumplían los requisitos de la 3G. Como consecuencia de esta presentación, se produjo una convergencia entre varias de las candidaturas que, a su vez, tuvo el efecto de propiciar la creación de lo que se denomina proyectos conjuntos (partnership projects). Su objetivo era el de proporcionar un foro, dentro del cual pudieran colaborar las diversas organizaciones de normalización de diferentes regiones mundiales, para la especificación de las propuestas fruto de la convergencia entre las candidaturas presentadas por dichas organizaciones.

En concreto, son dos los proyectos conjuntos que se establecieron:

1. El 3GPP (Third Generation Partnership Project) para armonizar las propuestas europeas y asiáticas.
2. El 3GPP2 (Third Generation Partnership Project 2) para armonizar las propuestas americanas y coreanas basadas en cdma2000.

Como resultado de los trabajos del OHG (Operators Harmonization Group), a finales de mayo de 1999 se alcanzó un acuerdo de armonización, el llamado G3G (Global Third Generation CDMA Approach). El objetivo era armonizar los parámetros radio tanto como fuese posible y, al mismo tiempo, permitir la conexión de los sistemas, tanto a una red troncal europea GSM MAP evolucionada como a una red troncal americana ANSI-41 evolucionada. Como consecuencia, en el marco del G3G se reconocen las siguientes interfaces radio para W-CDMA:

- FDD DS (*Direct Spread*), basada en la propuesta UTRA W-CDMA del 3GPP.
- FDD MC (*Multi Carrier*), basada en la propuesta cdma2000 del 3GPP2.
- TDD, el sistema UTRA TD/CDMA de ETSI, armonizado con el TD-SCDMA chino.

El segundo requisito, el de conectar la interfaz radio G3G a las redes europea y americana, se alcanzará modificando la estructura de protocolos de ambas redes.

En la reunión de Helsinki de 25 de octubre a 5 de noviembre de 1999, el TG 8/1 de la ITU-R aprobó la familia de sistemas IMT-2000 para la componente terrestre y que podrían

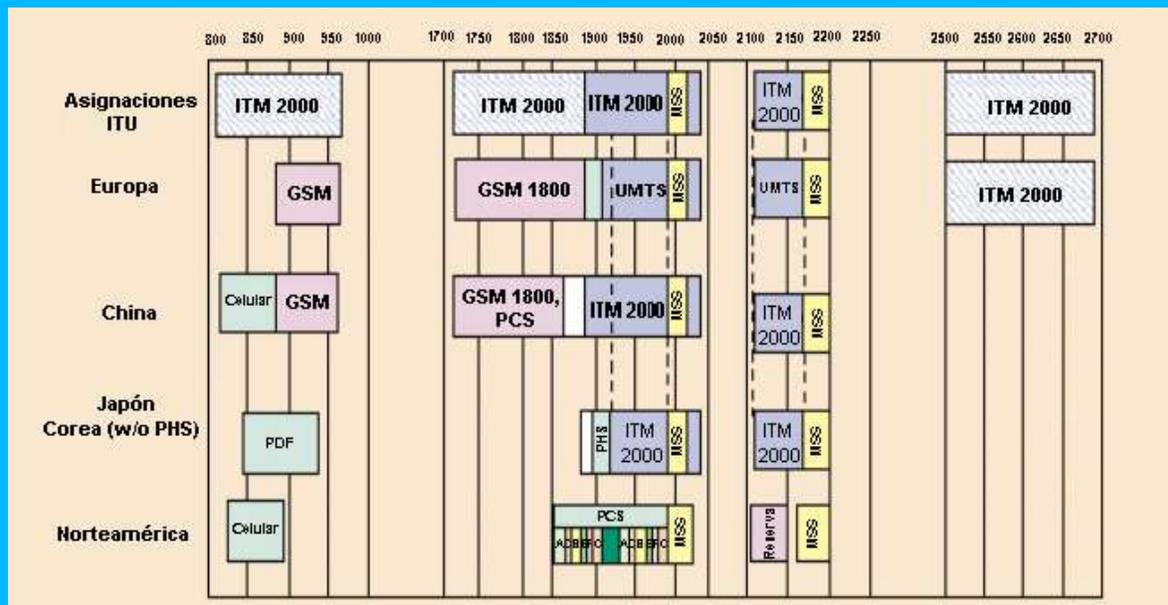
estar disponibles hacia el año 2010. La *Figura E- 6* muestra la familia de Sistemas IMT-2000.

*Figura E- 6: Familia de Sistemas IMT – 2000*

NOMBRE ITU	CONOCIDO COMO:	ORGANISMO DE ESTANDARIZACIÓN
IMT-2000 CDMA Direct Spread (DS)	UMTS-FDD UMTS W-CDMA	3GPP
IMT-2000 CDMA Multi-Carrier (MC)	cdma 2000	3GPP2
IMT-2000 CDMA TDD	UMTS-TDD UMTS	3GPP
IMT-2000 TDMA Single Carrier	UWC-136	UWCC
IMT-2000 FDMA/TDMA	DECT	ETSI

### 3.1.2. Especificaciones del espectro DE IMT-2000

*Figura E-7: Especificaciones del Espectro de IMT – 2000*

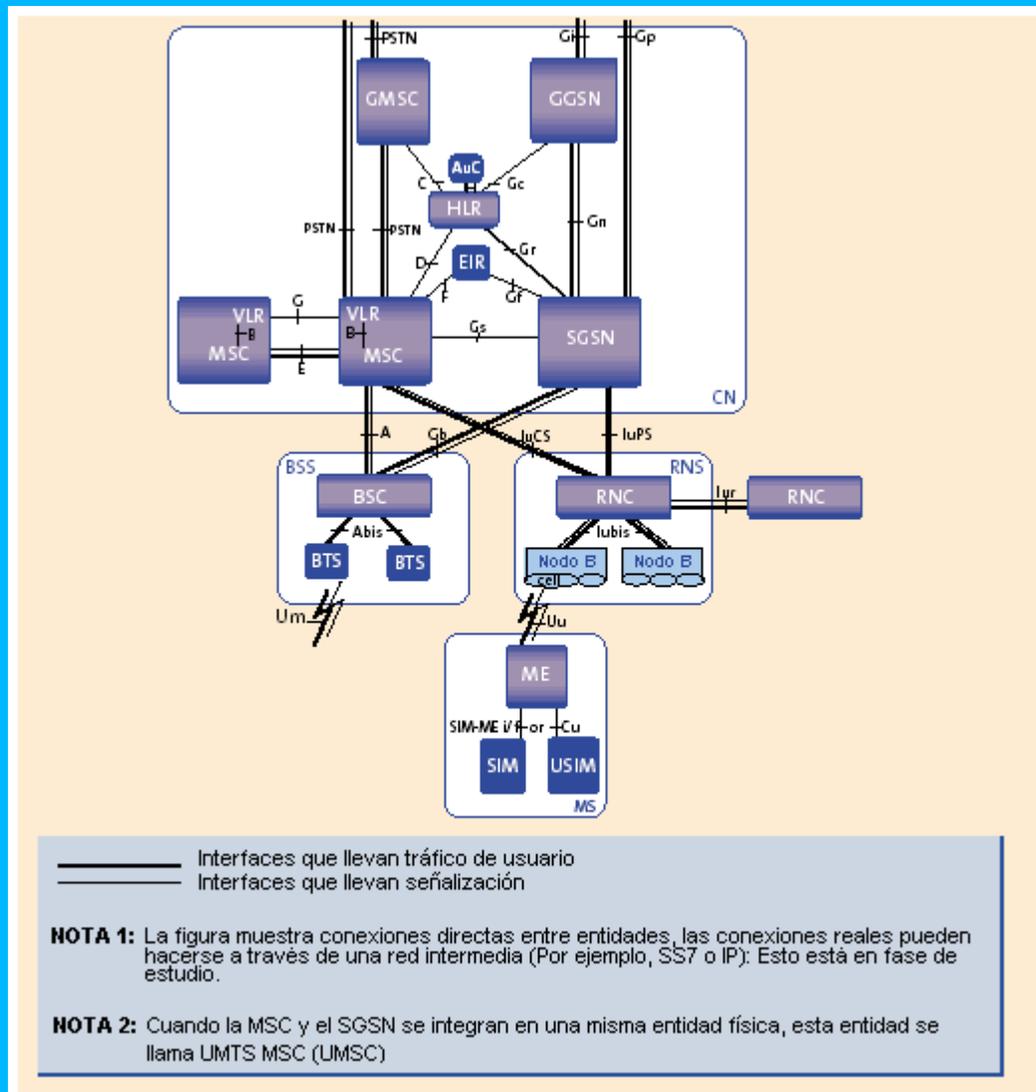


En la conferencia WRC-1992 (WRC'92) de la ITU, se recomendó la reserva de 230 MHz de espectro para IMT-2000 en las bandas 1885-2025 MHz y 2110-2200 MHz, que incluyen 1980-2010 MHz y 2170-2200 MHz para la componente satelital.

Esta banda ha sido ampliamente utilizada en la concesión de licencias de tercera generación en Europa. Sin embargo, en la mayor parte del continente americano toda esta banda está ya ocupada por los sistemas de segunda generación y en China está dedicado a aplicaciones WLL (Wireless Local Loop). Por esto, es que uno de los objetivos de IMT-2000: la reserva de una banda única en todo el mundo, no se ha alcanzado plenamente.

### 3.2. EL SISTEMA UMTS

Figura E- 8: Arquitectura del Sistema UMTS



La estandarización de una norma como el UMTS supone la definición de un extenso conjunto de especificaciones que garanticen el funcionamiento global del sistema. Al ser

un proceso gradual con continuas evoluciones y revisiones, el 3GPP se propuso proporcionar cada cierto tiempo un conjunto de normas que constituyeran de por sí el estándar. Dicho conjunto se conoce con el nombre de Release. Esta forma de trabajo permite tener un sistema funcionando, a la vez que se va mejorando y completando. La *Figura E- 8* muestra la Arquitectura de UMTS. La arquitectura de UMTS esta conformada por :

1. Red troncal o núcleo de red (Core Network, CN).
2. Red de acceso radio (Radio Access Network, RAN).
3. Terminales móviles (User Equipment, UE).

### 3.3. EL SISTEMA CDMA2000

El cdma2000 es un sistema de tercera generación que cumple los requisitos de IMT-2000. Fue desarrollado por el foro 3GPP2 como una evolución del sistema CDMA de banda estrecha (1,25 MHz) americano IS-95, también conocido como CdmaOne.

- Con el objeto de facilitar la transición, el sistema cdma2000 especifica dos soluciones: 1X y 3X, sobre portadoras de 1,25 MHz y 3,75 (3 x 1,25) MHz, respectivamente.
- Con la misma finalidad, el 3GPP2 también está normalizando los sistemas HDR (High Data Rate) como una evolución del sistema 1X. El HDR comprende el 1xEV-DO propuesto por el fabricante Qualcomm para datos en paquetes (acceso a Internet) y el 1xEV-DV propuesto por Motorola (en fase de desarrollo), que incluye servicio de voz en paquetes.
- Teniendo en cuenta la necesidad de facilitar la convergencia y dotar de flexibilidad al cdma2000, el 3GPP2 también normaliza los sistemas DS-41 y MC-MAP, que consisten en modificaciones de las especificaciones cdma2000 para que la RTT de UMTS opere sobre ANSI-41 y para que la RTT cdma2000 opere sobre GSM MAP, respectivamente, puntos importantes a considerar que los sistemas americanos están basados en una red troncal ANSI-41 y los sistemas europeos en una red troncal GSM MAP, diferencia que dificulta la itinerancia en los sistemas.

#### 3.3.1. Historia deL 3GPP Y 3GPP2

Aunque el ETSI propuso inicialmente el concepto de 3GPP como una organización global, el foro pronto anunció su interés de enfocarse, primordialmente, hacia soluciones basadas en GSM y su evolución.

Consecuentemente, el Comité Internacional del ANSI propuso la creación del 3GPP2 para promocionar la estandarización de redes troncales basadas en la norma ANSI-41 y sus RTTs asociadas. Básicamente, la idea era desarrollar el estándar cdma2000 como evolución natural del IS-95, de amplia implantación en Estados Unidos y Latinoamérica.

El 3GPP2 tuvo su lanzamiento formal en enero de 1999 en Vancouver (Canadá). En el 3GPP2 están representados TIA (EE UU), ARIB y TTC (Japón).

En cuanto a las tecnologías de acceso, estas también son CDMA, y para facilitar la evolución desde IS-95 se han propuesto dos versiones: cdma2000 RTT-1X, empleando una portadoras de 1,25 MHz (al igual que en IS-95), y cdma2000 RTT-3X, con 3 portadoras de 1,25 MHz (3,75 MHz en total).

### 3.3.2. Sistemas cruzados en CDMA2000 (ESPECIFICACIONES)

Con este término se hace referencia a los sistemas 3G que son combinación de los sistemas 3GPP y 3GPP2, empleando combinaciones de capas altas y capas bajas de protocolo de ambos sistemas. En el 3GPP2 se han estandarizado dos sistemas de este tipo:

- **los sistemas UMTS en ANSI-41 (DS-41)**  
Son sistemas que combinan la interfaz aire de UMTS con la red troncal ANSI-41. El proceso consiste en modificar la señalización de la capa 3 (Upper Layer) del cdma2000 para permitir que la interfaz aérea del sistema IMT-2000 CDMA Direct Spread (DS), es decir UMTS, pueda funcionar con los servicios de control de llamada y gestión de la movilidad de la red troncal ANSI-41. Esta combinación de capacidades se conoce abreviadamente como sistema DS-41.
- **Los sistemas CDMA2000 en GSM-MAP (MC-MAP)**  
Son sistemas que combinan la capa física, MAC (Medium Access Control), LAC (Link Access Control) y la subcapa RRC (Radio Resource Control) de cdma2000 con las capas CM (Connection Management) y MM (Mobility Management) de UMTS. El proceso consiste en modificar las capas bajas de cdma2000 para que pueda funcionar en la red troncal GSM-MAP definida por el 3GPP. Este modo de operación se conoce como Multi-Carrier (MC) usando GSM MAP, o abreviadamente MC-MAP.

### 3.3.3. Sistemas HDR EN CDMA2000

Finalmente con respecto al CDMA2000 encontramos los Sistemas HDR (High Data Rate) en cdma2000 que incluyen dos sistemas promocionados por Qualcomm y Motorola, y estandarizados por el 3GPP2 como 1xEV-DO y xEV-DV. Ambos sistemas se basan en una portadora 1X.

## 3.4. EL SISTEMA UWC-136

### 3.4.1. Historia evolución 2G IS-136 A 3G UWC-136

La UWC-136 (Universal Wireless Communications-136) es una especificación RTT de tercera generación que cumple los requisitos IMT-2000 de la ITU. La UWC-136 se elabora en la TIA TR45.3, a partir de propuestas del UWCC (Universal Wireless Communications Consortium), y se publica como un estándar americano ANS TIA/EIA-136.

En abril de 2000 se publicó lo que hoy se conoce como UWC-136, la que se concibió como una evolución hacia 3G del sistema 2G americano TDMA IS-136, que a su vez

provenía del sistema analógico AMPS EIA- 553. Entre sus características está que sigue manteniendo la filosofía de retrocompatibilidad y añade la convergencia con la evolución del GSM europeo, adoptando las tecnologías GPRS (General Packet Radio Service) y EDGE (Enhanced Data rates for GSM/Global Evolution) para los servicios de conmutación de paquetes.

Se debe tener en cuenta que el sistema IS-136, aparte de la técnica de acceso múltiple TDMA, no tiene mucho en común con GSM. Frente a los 8 usuarios (intervalos temporales) por portadora de 200 Khz. del GSM, el IS-136 soporta 3 usuarios en portadoras de 30 Khz., y en cuanto a la red troncal el IS-136 está basado en ANSI-41 frente a la GSM MAP.

La estrategia de evolución se dividió en tres fases. La primera consistió en la mejora de la calidad del sistema 2G que ya estaba en servicio, proporcionando voz y datos en circuito sobre los canales de 30 Khz. provenientes del AMPS analógico. En la segunda fase (denominada 136+) se incluye conmutación de paquetes basado en GPRS (denominada GPRS-136) sobre las portadoras de 30 Khz. En la tercera fase (denominada 136HS, 136 High Speed) se introducen portadoras de 200 Khz. (136HS Outdoor o EDGE) para alta velocidad de hasta 348 BIT/s, en entornos de alta movilidad, y portadoras de 1,6 MHz (136 HS Indoor) para muy alta velocidad, superiores a 2 Mbit/s en interiores.

En cuanto a la red troncal, esta tecnología se sigue basando en la red ANSI-41, desarrollándola para mejorar la prestación de servicios y para hacerla converger con la red GSM MAP.

#### **4.4.2. Descripción del sistema UWC-136 (estándares técnicos)**

El UWC-136 incluye los servicios del bien establecido estándar IS-136 y añade los servicios de conmutación de paquetes a alta velocidades, de 384 BIT/s, y a muy alta velocidad, de 2 Mbit/s.

Con relación a los servicios vocales se puede reseñar la introducción de un codificador vocal (vocoder) compatible con GSM para facilitar la interoperabilidad. Este codificador opera en canales de 30 Khz. con modulación 8-PSK y coexiste con los codificadores originales que operan con modulación 4-DQPSK.

El servicio de datos por conmutación de paquetes se denomina GPRS-136, empleando las capas superiores del GPRS GSM y soportándose sobre tres portadoras (136+, 136HS Outdoor y 136HS Indoor) para proporcionar velocidades que van desde 11,2 BIT/s hasta 2 Mbit/s.

La portadora 136+ (30 Khz.) soporta servicios vocales y de datos. Se especifican dos tipos de modulación: 4-DQPSK obligatoria y 8-PSK opcional. Los servicios básicos y de datos pueden funcionar con cualquiera de las modulaciones, lo que permite diferenciar el servicio y dar robustez al canal.

La portadora 136HS Outdoor (200 Khz., igual que en GSM) permite el despliegue de los servicios de datos de alta velocidad en exteriores. Se especifican dos modulaciones obligatorias: GMSK y 8-PSK. La codificación del canal y la modulación pueden variar, a fin de lograr una adaptación óptima del caudal en función de la robustez del canal.

Por último, la portadora 136HS Indoor (1,6 MHz) permite el despliegue de servicios de datos a muy alta velocidad, superiores a 2 Mbit/s en interiores. Se especifican dos modulaciones obligatorias: BOQAM (Binary Offset QAM) y QOQAM (Quaternary Offset).

La característica básica de funcionamiento del servicio de datos por conmutación de paquetes es la de ancho de banda por demanda. El ancho de banda asignado en un momento determinado es función de la combinación de servicios requerida. Permite asignar y des-asignar canales de forma incremental, según se requiera.

El ancho de banda asociado a cada servicio se ajusta a éste. Mediante la gestión dinámica del ancho de banda se obtiene una gran eficiencia espectral, así como que células de jerarquía inferior puedan "robar" ancho de banda a la red general para dar mayor capacidad en una región geográfica determinada.

### 4. ASPECTOS LEGALES Y REGULATORIOS.

No es una novedad que desde la aparición y posterior consolidación de tecnologías como la informática, telecomunicaciones y las grandes redes de información, ha existido una carencia en términos de leyes bien preparadas y enfocadas hacia este tipo de tecnología. Así, en los asuntos de legislación tecnológica la tecnología ha ido siempre más rápido que las leyes y los reguladores que las producen. Es por esto que cada vez se deban buscar mecanismos más objetivos y flexibles que sean aplicables en distintos y complejos escenarios tecnológicos, dándole así aplicación al principio de “neutralidad tecnológica”. El desarrollo y la convergencia de la tecnología cada vez hacen más palpable la necesidad de estándares internacionales y de la armonización de las regulaciones.

Debido a la creciente capacidad en términos de alcance y disponibilidad de los dispositivos móviles, cada vez exige mayor atención a aspectos como la privacidad y la seguridad de los usuarios, como veremos a continuación.

#### 4.1. USUARIOS Y PRIVACIDAD

La protección del usuario o del consumidor dentro de estas nuevas tecnologías es un tema tan trascendental que la Organización de Cooperación y Desarrollo Económico (OECD) en diciembre de 1999 publicó una guía con recomendaciones para proteger a los consumidores de comercio electrónico. Pero no es éste el único tópico que se cuestiona con respecto a las nuevas tecnologías. Son muchos los casos en que el permitir que un usuario esté disponible prácticamente en cualquier lugar y a cualquier hora tiendan a invadir su vida privada y a poner en riesgo la información que este bajo su dominio. Por lo tanto debe garantizarse el nivel de protección de la información que se recibe y/o envía a través de la misma.

#### 4.2. SEGURIDAD

Uno de los mayores desafíos que enfrentan las personas encargadas de establecer las normas es la combinación de telefonía conmutada y soluciones IP. El ETSI (European Telecommunications Standards Institute) cuenta con un grupo de trabajo que se encarga de la normalización en esta área. Esto brinda muchas oportunidades, pero también da lugar a numerosos riesgos de seguridad. La seguridad se refiere tanto a las redes como a la información personal y confidencial que se transmite a través de las mismas.

En el caso de las redes, los datos digitales que se transmiten por las redes inalámbricas son altamente vulnerables de ser copiados o modificados por un tercero. La movilidad que es una de las ventajas del Mobile Internet representa un problema en materia de seguridad, puesto que hace las redes susceptibles a interceptaciones, hacking y virus. El punto más vulnerable de la red es el punto de transferencia entre el protocolo inalámbrico al protocolo fijo.

Otro aspecto a analizar es el acceso a la señal. Así por ejemplo, con la red inalámbrica de la Universidad de los Andes un estudiante que viva cerca y que tenga alcance a la cobertura de la red, podría acceder a Internet sin necesidad de estar en la Universidad. También las redes inalámbricas dentro de edificios, igualmente pueden ser interceptadas o utilizadas para otros fines.

Actualmente, las medidas de seguridad funcionan con sistemas de encriptación como el WEP y el RADIUS (sistema de autenticación que verifica credenciales de los usuarios y permite el acceso o no al sistema), como se mencionó anteriormente el desarrollo y reconocimiento de protocolos que aumenten los niveles y/o garanticen seguridad como el 802.11g es un aspecto fundamental para la evolución del Mobile Internet.

Debido al tipo de información sensitiva y confidencial que se transmite y guarda en dispositivos móviles los mecanismos de seguridad deben aumentar. Los productores de agendas electrónicas para contrarrestar la renuencia de las compañías a darle a sus empleados agendas electrónicas como medio de trabajo debido al riesgo que corre la información que estos manejan, han incluido en sus últimas versiones lectura de huellas digitales como mecanismo de seguridad y control de acceso. Además, los dispositivos terminales son más complejos y tienen más posibilidades de ser infectados por virus o troyanos. Por lo tanto, la protección de los clientes se convirtió en la prioridad de los fabricantes, los operadores de red y los proveedores del servicio.

Al desarrollar áreas tales como el aprendizaje electrónico, la salud electrónica, el gobierno y el comercio electrónico, el desafío consiste en que la tecnología no sólo se implemente sino que también se utilice. Para esto se requiere una infraestructura de red confiable y segura, en la que los usuarios puedan confiar y que garantice la privacidad, confiabilidad e integridad de la información que se comunica.

Respondiendo a estas necesidades la Directiva Europea 2002/58 establece obligaciones para los proveedores de comunicaciones electrónicas respecto a la seguridad de sus redes; en el evento que estas redes no sean seguras deberá informar a los usuarios de la inseguridad de las redes y el riesgo que corre la información que se transmite a través de ellas. En Colombia actualmente no existe reglamentación al respecto.

Dentro de los sistemas de facturación, también se presenta un tema de seguridad de la información. Como se mencionó, este sistema de facturación debe ser convergente para que, entre otras, se garantice la seguridad y protección de la información de los usuarios.

La normalización (que a veces apoya las acciones legislativas) tiene un papel importante también en este campo. Desde el momento de su implementación, el ETSI fue el pionero en el establecimiento de normas de seguridad y participa en diversas actividades de seguridad relacionadas con la utilización de TICs.

En cuanto a la seguridad de las comunicaciones móviles, ETSI contribuye, en gran medida, al desarrollo de las comunicaciones móviles por medio de 3GPP. A lo largo de 2003, se avanzó en el tema de las especificaciones para Release 6, las cuales incluyen el apoyo para la Gestión de Derechos Digitales (DRM) y la 3G/WLAN.

En junio de 2002, el CEN y el ETSI crearon un grupo conjunto de Seguridad en Redes e Información (NIS) como respuesta al pedido de la Comisión Europea de crear una “estrategia sobre la seguridad de las redes electrónicas y una acción para implementarla fácilmente”. El informe del grupo se publicó en 2003 y contenía un trabajo de investigación sobre las normas de seguridad de los inventarios. Recomienda que la normalización mejore el acceso a comunicaciones electrónicas seguras, incluso al comercio electrónico y al intercambio de información dentro y fuera de Europa. En especial, el informe

recomienda que el trabajo optimice la interoperabilidad, de modo que se mejoren las normas y que se proteja a los usuarios domésticos y a las pequeñas y medianas empresas (PyME).

### 4.3. LEGISLACIÓN EN EL SECTOR COMUNICACIONES

La legislación en materia de comunicaciones ha venido siendo modificada de una manera eficiente desde los años 80 a nivel mundial. Dentro de esas modificaciones a la reglamentación, tres factores han sido predominantes en los países:

- Liberalización del mercado.
- Creación de reguladores independientes.
- Políticas de competencia efectivas.

#### 4.3.1. Licencias

En Europa los países ya atravesaron el proceso de adjudicación de licencias de 3G. Para tal efecto, la Comisión Europea elaboró un reporte en Junio del 2002, donde enumeró cinco principios para que los reguladores encargados de la administración y asignación de espacios en el espectro electromagnético tengan en cuenta:

- La asignación debe basarse en el concepto de mercado sostenible
- Debe permitir la introducción de nueva tecnología y/o capacidad
- Debe minimizar distorsiones
- Debe alinear las condiciones de licencias con otros niveles de regulación que permitan estabilidad financiera
- Debe dar soporte al inicio de la demanda del mercado

Las plataformas 2.5.G y 3G contienen una ventaja frente a las otras plataformas porque permiten diferenciar dentro de lo que se transmite qué corresponde a voz y qué corresponde a datos. Por eso, la facturación del Mobile Internet no tiene que estar basada en minutos, lo cual implica una ventaja para que las sumas que una compañía cobre a otra por interconexión estén basadas en costos reales y no haya lugar para abusos por parte de los operadores dueños de la infraestructura.

#### 4.3.2. Leyes relacionadas con la movilidad en Colombia

La prestación de servicios móviles en Colombia comenzó en 1994 bajo las condiciones descritas en la ley 37 de 1993 y demás normas complementarias. Estas normas determinaron la asignación de 25 MHz para cada concesionario en la banda de 850 MHz, lo cual, de acuerdo al estado de la tecnología en ese entonces era suficiente para la prestación de este tipo de servicios.

Las acciones del gobierno nacional en materia de telecomunicaciones se han enfocado en el aumento de la cobertura nacional en los servicios de telecomunicaciones, la consolidación de la liberalización del mercado y el fomento de la inversión en el sector de telecomunicaciones a fin de profundizar la penetración, modernizar la infraestructura y diversificar la oferta de servicios a los usuarios.

En desarrollo de estas acciones las normas constitucionales, artículo 75, y legales, decreto ley 1900 de 1990, decreto 741 de 1993 y el decreto 1620 de 2003, han establecido de manera expresa la competencia que le asiste al Ministerio de Comunicaciones para administrar el espectro electromagnético.

En el caso particular de la telefonía móvil celular, los artículos 13 y 14 del Decreto 741 de 1993 consagran la mencionada facultad del Ministerio y la obligatoriedad en la exigencia de autorización previa para el uso de dicho espectro.

En este orden de ideas, es importante resaltar que en el caso particular de los servicios móviles, el Espectro Electromagnético se constituye como un elemento esencial para la prestación del servicio, según lo previsto en el artículo 1 de la ley 37 de 1993.

El Decreto 2103 de 2003 establece que la adjudicación del espectro deberá hacerse a solicitud de parte, salvo cuando el Ministerio de Comunicaciones juzgue que la solicitud no tiene una base sólida o que no existe disponibilidad de frecuencias para cumplirla.

Adicionalmente, el Ministerio de Comunicaciones deberá hacer un análisis de las bandas del espectro objeto de adjudicación, con el fin de determinar el procedimiento y las condiciones que se deberán cumplir para que los actuales concesionarios ubicados en esta parte del espectro, dejen libres estas bandas y de esta forma se puedan asignar a los operadores de los servicios móviles.

#### **4.4. COMPETENCIA**

La política de competencia ha sido un factor que ha permitido el desarrollo del Internet y la telefonía móvil. En la convergencia de estas dos tecnologías será necesario que la regulación de competencia se mantenga durante todo el proceso, es decir desde la licitación de las licencias hasta la prestación del servicio.

La labor de los reguladores y de los entes gubernamentales encargados en materia de competencia, además de determinar qué compañías gozan de una posición dominante y cuáles fusiones o escisiones crean monopolios o posiciones de ventaja dentro del mercado, son:

- Garantizar la conectividad y operabilidad de los operadores, servidores y proveedores.
- Administrar el espectro electromagnético de una manera eficiente.

Determinar qué compañías gozan de una posición dominante será una labor cada vez más difícil en el contexto de la convergencia, puesto que puede ser que cierta compañía sea dominante en un sector de las comunicaciones pero no en otro, y preste servicios y/o productos en los dos. En contraste con el mercado de telefonía móvil, ahora sí se van a ver fusiones entre compañías debido a los altos costos e inversiones que requiere la

plataforma 3G. Adicionalmente, los reguladores nacionales en materia de competencia conjuntamente con la ayuda de organismos regionales e internacionales no deberán perder de vista el objetivo de la armonización de las legislaciones de competencia.

### 4.5. ACCESO

El acceso en materia de tecnología es parte importante de la competencia, especialmente en el Mobile Internet ya que los operadores se están convirtiendo en administradores de contenido e incluso están desarrollando portales de Internet para que los usuarios accedan a este contenido. Aún cuando los operadores podrían argumentar que el usuario de Mobile Internet hace una búsqueda de información específica cuando navega por Mobile Internet, los reguladores de competencia deberían asegurarse que así los operadores sean administradores del contenido o que tengan su propio portal deben garantizar al usuario el acceso libre a Internet, por ejemplo dándole la opción de links con otros portales de Internet.

### 4.6. COMPATIBILIDAD ENTRE TECNOLOGÍAS

Los servicios móviles han tenido distintos grados de evolución, y a estas etapas se les ha denominado generaciones. Los primeros teléfonos móviles pertenecían a la primera generación 1G los cuales funcionaban con tecnología análoga. Posteriormente, con la tecnología digital CDMA, TDMA, GSM y PDC vinieron los móviles de segunda generación 2G, y con la tecnología digital se empezó a implementar el envío de mensajes de texto y se dieron los primeros pasos hacia la transmisión de datos.

Actualmente, nos encontramos con la migración hacia las redes de tercera generación (3G), las cuales ofrecen mayor velocidad, transmisión de datos e información más compleja como videocomunicaciones, acceso completo a Internet, capacidad para proveer servicios a usuarios al mismo tiempo, todo esto independientemente de la localización del usuario.

Existen tres tecnologías diferentes y cinco frecuencias de bandas aprobadas para 3G con diferentes sistemas operativos entre países. Por lo tanto, para lograr la interoperabilidad de los mismos, temas como la convergencia en las interfaces y los puentes entre frecuencias deberán ser resueltos.

Comercialmente, entre los Protocolos WI-FI, la tecnología 802.11b es la que está predominando, a pesar de esto tiene un gran competidor en la Telefonía Móvil, por lo tanto es difícil saber qué tecnología predominará, puesto que cada una tiene su mercado y tipo de usuarios. Por eso, es difícil asegurar que una tecnología vaya a suplir a la otra, simplemente el mercado dará espacio para los servicios móviles dependiendo del tipo de servicio y la facilidad de acceso, de esta forma, se utilizará Internet Inalámbrico a través de portátiles, agendas electrónicas (América) y teléfonos móviles (Europa y Asia), complementando los servicios entre sí. Por ejemplo, mientras exista cobertura WI-FI se accederá a Internet a través de estos protocolos, pero cuando alguien esté fuera de esa cobertura podrá usar su teléfono móvil para acceder a Internet y para hacer llamadas telefónicas.

Como consecuencia de lo anterior, podemos concluir que las diferentes tecnologías, plataformas y dispositivos que sirven de infraestructura a la Movilidad, están llamados a complementarse en lugar de sustituirse.

## REFERENCIAS BIBLIOGRAFICAS

- [1] Blair, D., Tweedly, A., Thomas, M., Trostle, J. y M. Ramalho, "Realtime Mobile IPv6 Framework" ("Estructura de IPv6 Móvil en Tiempo real"), Trabajo en marcha.
- [2] Calhoun, P., Montenegro, G. y C. Perkins, "Mobile IP Regionalized Tunnel Management" ("Gestión de Tunelaje Sectorizado de IP Móvil"), Trabajo en marcha.
- [3] Deering, S. and R. Hinden, "Internet Protocol, Versión 6 (IPv6) Specification" ("Protocolo de Internet, Especificacion version 6 ipv6"), [RFC 2460](#), Diciembre 1998.
- [4] Koodli, R., Ed., "Fast Handovers for Mobile IPv6" ("Handovers Rápido para Ipv6 Móvil"), Trabajo en marcha.
- [5] Yavatkar, R., Pendarakis, D. and R. Guerin, "A Framework for Policy-based Admission Control" ("Marco para el Control de Admisión basado en Políticas"), [RFC 2753](#), Enero 2000.
- [6] Kempf, J., McCann, P. and P. Roberts, "IP Mobility and the CDMA Radio Access Network: Applicability Statement for Soft Handoff" ("Movilidad IP y la Red de Acceso Radio de CDMA: Declaración de la Aplicabilidad para Handoff suave"), Trabajo en marcha.
- [7] Kempf, J., Ed., "Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network" ("Descripcion del Problema: Razones para Realizar la Transferencia de Contexto entre Nodos en una Red de Acceso IP"), [RFC 3374](#), Septiembre 2002.
- [8] Trossen, D., Krishnamurthi, G., Chaskar, H. and J. Kempf, "Issues in candidate access router discovery for seamless IP-level handoffs" ("Problemas en el descubrimiento de candidatos a enrutadores de acceso para handoffs nivel IP sin interrupciones"), Trabajo en marcha.
- [9] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6" ("Soporte de la movilidad en IPv6"), [RFC 3775](#), Junio 2004.
- [10] Perkins, C., Ed., "IP Mobility Support for IPv4" ("Soporte de la movilidad para IPv6"), [RFC 3344](#), Agosto 2002.
- [11] Perkins, C., Calhoun, P. and J. Bharatia, "Mobile IPv4 Challenge/Response Extensions (revised)" ("Extensiones de Desafío/Respuesta para IPv4 Móvil (revisado)), Trabajo en marcha.
- [12] Perkins, C. and P. Calhoun, "AAA Registration Keys for Mobile IP" (Claves de Registro AAA para IP Móvil), Trabajo en marcha.
- [13] Ernst, T. and H. Lach, "Network Mobility Support Terminology" (terminología de soporte para la Movilidad en Redes), Trabajo en marcha.