

01130
8



**UNIVERSIDAD NACIONAL AUTÓNOMA DE
MÉXICO**

FACULTAD DE INGENIERÍA

REDES INALÁMBRICAS

**TESIS CON
FALLA DE ORIGEN**

T E S I S

**QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN TELECOMUNICACIONES**

P R E S E N T A N:

**CARLOS GILBERTO CALZADA RIOS
GERARDO SÁNCHEZ VÁZQUEZ**

A S E S O R:

ING. JESÚS REYES GARCIA



A



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

TESIS CON FALLA
DE
ORIGEN

Agradecimientos.

Quiero agradecer:

En lo académico y profesional...

A la Universidad Nacional Autónoma de México; por la oportunidad que me ha dado de formarme durante estos ocho años.

A la Facultad de Ingeniería; por la preparación que me ofreció y esta haciendo de mí un excelente profesionista.

A todos mis profesores; por su trabajo y esfuerzo, valores que han inculcado en mí durante todo este tiempo. En especial al Ing. Jesús Reyes García por el apoyo que me brindó durante este trabajo de tesis y por la paciencia que tuvo durante éste proceso.

En lo personal...

A mis padres Juan Carlos y Marisela; por toda una vida de esfuerzos y sacrificios brindándome siempre cariño y apoyo cuando lo he necesitado. Les agradezco infinitamente por heredarme el tesoro y valor más importante que pueda darsele a un hijo, amor.

A mi hermano Gerardo Manuel; por su amistad y compañía, por sus consejos y por todos los momentos que hemos vivido juntos, los cuales han hecho que crea más en la hermandad.

A la Familia Calzada y a la Familia Ríos; por todo el cariño que me han brindado desde niño, por que ahora son mis modelos de vida a seguir, tanto en lo profesional como en lo personal.

A la Familia Sánchez Vázquez; por el apoyo que me han brindado, por hacerme sentir parte de su familia. En especial al Ing. Gerardo Sánchez Vázquez, por su amistad y cariño, por todos los momentos maravillosos que hemos vivido juntos durante este trabajo y fuera de él, por sus consejos y total confianza. A la Lic. Angélica Rosete Vázquez por... simplemente todo lo que es y todo lo que significa para mí mmmm...=o).

A la Familia Vela Serafín, en especial a la Act. Mariana Vela Serafín; por el apoyo que me ofrecieron, amor, cariño y por todas las facturas de madurez que le pagué a la vida a raíz de que los conocí y que han hecho de mí un mejor ser humano.

Y por último pero no menos importante jajajaja..., a todos mis amigos y cuates: Gus, el Maestro (Elías), a las Chicas Superpoderosas (Verito, Odet, Güerita), Bety, Telmita, Arturito, Rulo, el Mike, Omar, los Tocayos (Toro y Móvil), el Diablito, Edson, el Choto y todos los que no menciono pero saben que los tengo en el corazón; por todos los momentos inolvidables que viví con ustedes, por fortalecerme como persona, por apoyarme, cuidarme y preocuparse por mí, por los consejos, regaños y claro por apoyarme a realizar este trabajo de tesis jajaja...

Carlos

Agradecimientos.

En lo profesional:

- ✓ Quiero agradecer a la Universidad Nacional Autónoma de México por darme la oportunidad de estudiar en la Facultad de Ingeniería, esto es por hacer de mí un excelente profesionista.
- ✓ Así mismo les agradezco a mis profesores de la carrera de Ingeniería en Telecomunicaciones por darme la educación profesional que hoy en día tengo; pero en especial le agradezco al director de esta tesis, el Ing. Jesús Reyes García por su apoyo y confianza en el desarrollo de ésta.

En lo personal:

- ✓ Durante el proceso de mi educación profesional hubieron muchas personas que me apoyaron y animaron a salir adelante, de estas personas puedo mencionar a:
- ✓ Mis padres Rosalinda Vázquez Osorio y Carlos Sánchez Maldonado, quienes con su amor, confianza, apoyo y educación, me han inculcado salir adelante a pesar de las adversidades, pues siempre estaban y siguen estando a mi lado viendo por mi bienestar.
- ✓ Mis hermanos, quienes con su ejemplo como profesionistas, me han guiado por un buen camino llevándome a ser una mejor persona, y así mismo creyendo que el amor entre hermanos si existe.
- ✓ A la familia Sánchez y Vázquez quienes día con día me siguen demostrando que la convivencia familiar si existe, por que se que puedo confiar en cada uno de los integrantes de estas grandes familias.
- ✓ A la familia Calzada Rios, quienes me han dado siempre sabios consejos para salir adelante, en especial la Profesora Marisela y el Profesor Juan Carlos. En esta familia también están Gerardo Manuel con quien he llevado una amistad muy padre y el Ing. Carlos Gilberto, quien con su amistad y ayuda hemos logrado superar una prueba más que nos puso la vida y además le agradezco esos buenos y malos momentos que hemos vivido juntos lo cual ha hecho más grande nuestra amistad.
- ✓ A todos mis amigos de la universidad y de la vida diaria como son Arturo Alcantara, Alejandro, Gustavo, Elias, Arturo Maraboto (con su levanta ...), al Rulo, el diablito (Juan), Edson, el Choto, Móvil, Verónica, Odette, Maribel, Bety, Diana Jessica (GCi), Vanessa, Selene, Arely (la ñoña), Antelma y Luis Acosta entre otros, les agradezco por su amistad y ayuda durante toda la carrera; también les agradezco esos momentos de diversión (por ejemplo esas largas tardes en el estacionamiento de la facultad) y de tristezas (sino mal lo recuerdo hay muy pocas) las cuales recuerdo como si fueran el día de ayer (mis mejores recuerdos de ellos están en Acapulco).

En general les agradezco a todas y cada una de las personas mencionadas aquí por formar parte de mi vida.

Atte.

Gerardo Sánchez Vázquez



ÍNDICE

Introducción	1
1. Tecnologías Habilitadoras	3
1.1 Códigos de línea	3
1.1.1 Sin retorno al nivel 0 (NRZ-L)	3
1.1.2 Sin retorno al nivel 0, invertido (NRZI)	3
1.1.3 Codificación Diferencial	3
1.1.4 Bipolar-AMI	4
1.1.5 Binario multinivel o Pseudotemario	4
1.1.6 Comparativa Binario Multinivel	4
1.1.7 Manchester	4
1.1.8 Manchester Diferencial	5
1.1.9 Bipolar 3 Ceros de Alta Densidad.. (HDB3)	5
1.2 Técnicas de Modulación	5
1.2.1 Amplitude Shift Keying (ASK)	6
1.2.2 Phase Shift Keying	6
1.2.3 Frequency Shift Keying	7
1.2.4 Gaussian Minimun Shift Keying GMSK	8
1.2.5 Modulación en Amplitud por Cuadratura (QAM)	8
1.2.6 Modulación OFDM	9
1.3 Técnicas de Acceso Múltiple	11
1.3.1 Frequency Division Duplexing (FDD)	11
1.3.2 Time Division Duplexing (TDD)	12
1.4 Técnicas de Acceso Múltiple al Canal	12
1.4.1 Acceso Múltiple por División de la Frecuencia FDMA	12
1.4.2 Acceso Múltiple por División del Tiempo TDMA	12
1.4.3 Híbrido FDMA/TDMA	13
1.4.4 Acceso Múltiple por División de Código CDMA	13
1.4.4.1 Capacidad de acceso múltiple	14
1.4.4.2 Espectro Esparcido (Spread Spectrum).....	15
1.4.4.3 Secuencia Directa – CDMA (DS-CDMA o DSSS)	15
1.4.4.4 Salto de Frecuencia CDMA (FH-CDMA)	17
1.4.4.5 Salto de Tiempo – CDMA (Time Hopping – CDMA)	18
1.4.4.6 Sistemas Híbridos CDMA (HS-CDMA)	19
1.5 Codificación	20
1.5.1 Códigos de Bloque Lineales	20
1.5.1.1 Detección de Errores: Síndrome	20
1.5.1.2 Distancia mínima	21
1.5.1.3 Corrección de errores	21
1.5.2 Códigos Cíclicos	22
1.5.3 Códigos Convolucionales	22
1.5.4 Características de los Principales Códigos	23
1.5.4.1 Códigos de control de redundancia cíclica	23
1.5.4.2 Código de Golay	23
1.5.4.3 Códigos Bose, Chaudhuri, y Hocquenghem (BCH)	24
1.5.4.4 Códigos Reed-Solomon (RS)	24
2. Redes de Paquetes por Radio	25
2.1. Mobitex	26
2.1.1 Descripción y Arquitectura del Sistema	26
2.1.2 Arquitectura del Protocolo	28
2.2 CDPD (Cellular Digital Packet Data)	29
2.2.1 Descripción y Arquitectura del Sistema	29
2.2.2 Arquitectura del Protocolo	31
2.2.3 Capa MAC del sistema CDPD	32
2.3 GPRS (General Packet Radio Service)	33
2.3.1 Descripción y Arquitectura del Sistema	33
2.3.2 Arquitectura del Protocolo	35

D

5.5.1.3	Protocolos que ofrecen aplicaciones extra en IrDa	107
5.5.2	Descripción y Arquitectura de la conexión en IrDA	108
6.	Redes de Radio Ad Hoc	110
6.1	Introducción a las Redes Ad Hoc	110
6.2	Características de las Redes Ad Hoc	110
6.3	Protocolos Ad Hoc	112
6.3.1	Protocolos Proactivos	112
6.3.1.1	Destination Sequenced Distance Vector Routing (DSDV)	113
6.3.1.2	Clusterhead Gateway Switch Routing (CGSR)	114
6.3.1.3	Wireless Routing Protocol (WRP)	115
6.3.2	Protocolos Reactivos	116
6.3.2.1	Ad-Hoc On-Demand Distance Vector (AODV)	116
6.3.2.1.1	Funcionamiento	117
6.3.2.1.2	Descubrimiento de Ruta	118
6.3.2.2	Dynamic Source Routing (DSR)	118
6.3.2.2.1	Funcionamiento	119
6.3.2.2.2	Descubrimiento de Ruta	119
6.3.2.3	Temporally-Ordered Routing Algorithm (TORA)	121
6.3.2.3.1	Funcionamiento	122
6.3.2.4	Associativity-Based Routing (ABR)	123
6.4	Comparación de los Protocolos	125
6.4.1	Protocolos Proactivos	125
6.4.2	Protocolos Reactivos	126
7.	Computación Móvil y Computación Esparcida (Pervasive)	127
7.1	Computación Móvil	127
7.1.1	Mecanismos y Protocolos de Descubrimiento de Servicios	128
7.1.1.1	SLP - Service Location Protocol	128
7.1.1.2	Jini	129
7.1.1.3	Universal Plug and Play (UPnP)	130
7.1.1.4	Salutation	131
7.1.2	Comparación de Técnicas de Descubrimiento de Servicios Existentes	132
7.1.3	Deficiencias en las Arquitecturas Existentes de Descubrimiento de Servicios	132
7.1.4	Técnicas de Descubrimiento de Servicios Mejoradas para Comercio Móvil	133
7.1.4.1	El Marco de Agentes Ronin	133
7.1.4.2	Proyecto XReggie	134
7.2	Computación Esparcida(Pervasive) o Ubicúa	134
7.2.1	Tipos de Redes que se despliegan para la Computación Ubicua	136
7.2.1.1	Redes de Control	136
7.2.1.1.1	Redes de Propósito General	137
7.2.1.1.2	Redes Orientadas a la Automatización de Viviendas	137
7.2.1.2	Redes Multimedia	138
8.	Estado de la Implementación de las Tecnologías	140
8.1	Comienzo de las Redes Inalámbricas en México	140
8.2	Visión de Especialistas y Empresarios Mexicanos Acerca de las Redes Inalámbricas en el País	140
8.2.1	Crecimiento y Penetración de las Redes Inalámbricas en el País	142
8.2.2	La Barrera de la Velocidad	143
8.2.3	Preocupación por la Seguridad	143
8.2.4	Cultura de Uso	144
8.3	Implementación de una Red Inalámbrica	145
8.3.2	Elección de productos	145
8.3.2.1	Productos WLAN 802.11	145
8.3.2.2	Productos Bluetooth	147
8.4	Redes Inalámbricas en México	148
8.4.1	Internet Inalámbrico con Prodigy Movil	149
8.4.2	Red GSM GPRS de Telcel	151
8.4.3	Internet Móvil desarrollado por Wireless Net Online	152
8.4.4	Internet Inalámbrico en el Área Hotelera	155

2.4 ARDIS (Advancer Radio Data Information)	37
2.4.1 Descripción y Arquitectura del Sistema	37
2.4.2 Arquitectura del Protocolo	39
2.5 Características principales de Redes Inalámbricas de Paquetes por Radio	40
3. Redes de Área Local Inalámbricas WLANs	41
3.1 HiperLAN2	42
3.1.1 Arquitectura de la Red	42
3.1.2 Arquitectura del Protocolo de HiperLAN2	43
3.1.2.1 Capa de Convergencia	44
3.1.2.2 Capa de Control de Enlace de Datos (DLC)	45
3.1.2.2.1 Subcapa de Control de Enlace de Radio (RLC)	46
3.1.2.2.2 Protocolo de Control de error (EC)	46
3.1.2.2.3 Protocolo MAC	46
3.1.2.3 Funciones de Red de Radio y Apoyo QoS	48
3.1.2.4 Capa física	48
3.2 IEEE802.11	51
3.2.1 Arquitectura de la Red WLAN IEEE 802.11	52
3.2.2 Arquitectura del Protocolo de IEEE802.11	53
3.2.2.1 Capa Física (PHY)	53
3.2.2.2 La Capa de Acceso al Medio (MAC)	55
3.2.2.2.1 Trama de IEEE802.11	55
3.2.3 Comparación entre los Estándares IEEE802.11 a, b y g	57
4. Telefonía Inalámbrica Pública o Empresarial	61
4.1 Digital European Cordless Telecommunications (DECT)	62
4.1.2 Configuración de la red y aplicaciones para el estándar DECT	62
4.1.3 Arquitectura del Protocolo del estándar DECT	63
4.1.4 Especificaciones técnicas y descripción funcional del estándar DECT	64
4.2 Personal Handy-phone System (PHS)	68
4.2.1 Arquitectura de la Red PHS	69
4.2.1.1 Asignación de Funciones	72
4.2.1.2 Interfase de Red	72
4.2.2 Arquitectura del Protocolo	73
4.2.3 Comparación entre DECT y PHS	75
5. Redes de Área Personal Inalámbricas (WPANs)	76
5.1 Grupo de Trabajo 802.15	76
5.1.1 Grupo de trabajo 1 (TG1) WPAN/Bluetooth	78
5.1.2 Grupo de trabajo 2 (TG2) – Coexistencia	78
5.1.3 Grupo de trabajo 3 – Alta tasa de transmisión en WPANs	79
5.1.4 Grupo de trabajo 4 - WPAN Baja Tasa de Transmisión	81
5.2 Estándar Bluetooth	85
5.2.1 Modelos de uso de Bluetooth	86
5.2.2 Arquitectura de la Red	87
5.2.3 Pila de Protocolos de Bluetooth	88
5.2.3.1 Capa de Radio de Bluetooth	90
5.2.3.2 Banda Base	91
5.2.3.3 Formato del Frame de Bluetooth	92
5.3 HomeRF	94
5.3.1 Arquitectura del sistema HomeRF	94
5.3.2 Arquitectura del Protocolo	96
5.3.3 Transmisión de Datos	97
5.3.4 Transmisión de Voz	98
5.4 Air5	99
5.4.1 El Chipset Air5	101
5.4.1.1 Chip Banda-Base	102
5.4.1.2 Chip RF	102
5.5 Infrared Data Association IrDA	102
5.5.1 Arquitectura del Protocolo	104
5.5.1.1 Capa Física IrPHY	104
5.5.1.2 Capa IrLAP y Capa IrLMP de IrDa	107

E

5.5.1.3	Protocolos que ofrecen aplicaciones extra en IrDa	107
5.5.2	Descripción y Arquitectura de la conexión en IrDA	108
6.	Redes de Radio Ad Hoc	110
6.1	Introducción a las Redes Ad Hoc	110
6.2	Características de las Redes Ad Hoc	110
6.3	Protocolos Ad Hoc	112
6.3.1	Protocolos Proactivos	112
6.3.1.1	Destination Sequenced Distance Vector Routing (DSDV)	113
6.3.1.2	Clusterhead Gateway Switch Routing (CGSR)	114
6.3.1.3	Wireless Routing Protocol (WRP)	115
6.3.2	Protocolos Reactivos	116
6.3.2.1	Ad-Hoc On-Demand Distance Vector (AODV)	116
6.3.2.1.1	Funcionamiento	117
6.3.2.1.2	Descubrimiento de Ruta	118
6.3.2.2	Dynamic Source Routing (DSR)	118
6.3.2.2.1	Funcionamiento	119
6.3.2.2.2	Descubrimiento de Ruta	119
6.3.2.3	Temporally-Ordered Routing Algorithm (TORA)	121
6.3.2.3.1	Funcionamiento	122
6.3.2.4	Associativity-Based Routing (ABR)	123
6.4	Comparación de los Protocolos	125
6.4.1	Protocolos Proactivos	125
6.4.2	Protocolos Reactivos	126
7.	Computación Móvil y Computación Esparcida (Pervasive)	127
7.1	Computación Móvil	127
7.1.1	Mecanismos y Protocolos de Descubrimiento de Servicios	128
7.1.1.1	SLP - Service Location Protocol	128
7.1.1.2	Jini	129
7.1.1.3	Universal Plug and Play (UPnP)	130
7.1.1.4	Salutation	131
7.1.2	Comparación de Técnicas de Descubrimiento de Servicios Existentes	132
7.1.3	Deficiencias en las Arquitecturas Existentes de Descubrimiento de Servicios	132
7.1.4	Técnicas de Descubrimiento de Servicios Mejoradas para Comercio Móvil	133
7.1.4.1	El Marco de Agentes Ronin	133
7.1.4.2	Proyecto XReggie	134
7.2	Computación Esparcida(Pervasive) o Ubicúa	134
7.2.1	Tipos de Redes que se despliegan para la Computación Ubicua	136
7.2.1.1	Redes de Control	136
7.2.1.1.1	Redes de Propósito General	137
7.2.1.1.2	Redes Orientadas a la Automatización de Viviendas	137
7.2.1.2	Redes Multimedia	138
8.	Estado de la Implementación de las Tecnologías	140
8.1	Comienzo de las Redes Inalámbricas en México	140
8.2	Visión de Especialistas y Empresarios Mexicanos Acerca de las Redes Inalámbricas en el País	140
8.2.1	Crecimiento y Penetración de las Redes Inalámbricas en el País	142
8.2.2	La Barrera de la Velocidad	143
8.2.3	Preocupación por la Seguridad	143
8.2.4	Cultura de Uso	144
8.3	Implementación de una Red Inalámbrica	145
8.3.2	Elección de productos	145
8.3.2.1	Productos WLAN 802.11	145
8.3.2.2	Productos Bluetooth	147
8.4	Redes Inalámbricas en México	148
8.4.1	Internet Inalámbrico con Prodigy Movil	149
8.4.2	Red GSM GPRS de Telcel	151
8.4.3	Internet Móvil desarrollado por Wireless Net Online	152
8.4.4	Internet Inalámbrico en el Área Hotelera	155

Conclusiones	157
Apéndice A	160
Apéndice B	167
Referencias	177

G

INTRODUCCIÓN

Es una realidad que las redes inalámbricas se han ido abriendo camino a lo largo de la evolución de las diferentes tecnologías de comunicación existentes, y sobre todo con la llegada de los sistemas móviles celulares de Tercera Generación (3G), las redes de comunicaciones móviles están entrando en una nueva fase de evolución desde la red única ubicua centrada en voz, hasta una plataforma abierta capaz de soportar un conjunto de nuevos servicios y aplicaciones. En paralelo están surgiendo nuevos desarrollos y normas para redes de usos dedicados y cobertura restringida en entornos residenciales y profesionales o para redes de corto alcance, las cuales son el objeto de análisis en esta tesis, ya que en los próximos años las tendencias modificarán el paisaje de las comunicaciones móviles, el cual estará dirigido al suministro abierto de servicios soportados por redes de acceso dedicadas a aplicaciones específicas. La importancia de estas evoluciones es que influirán en gran parte a la definición de los sistemas móviles de cuarta generación. Los estudios y avances tecnológicos más importantes requeridos para satisfacer las exigencias de los usuarios mediante la creación de estas nuevas redes se viene realizando en universidades y centros de investigación de las grandes empresas de telecomunicaciones.

Es por eso que el siguiente trabajo de tesis tiene como objetivo principal, realizar un análisis de diversas redes inalámbricas que han surgido o se han propuesto durante los últimos años, los cuales presentan diversas innovaciones tecnológicas que pueden influir en la forma en que se desarrollan diversas actividades. Así mismo en este trabajo, se realizará una comparación interna entre los diferentes estándares existentes dentro de un mismo grupo de redes inalámbricas, comparando las principales propiedades correspondiente a la capa Física (PHY), Enlace (MAC) y Red del modelo de referencia OSI además de las características generales como: eficiencia, rentabilidad, costos entre otras cosas.

El método para llevar a cabo el análisis de las redes inalámbricas fue; obteniendo información de revistas técnicas relacionadas con tecnologías inalámbricas y de páginas de Internet de las principales organizaciones y empresas que están trabajando sobre el desarrollo de estas tecnologías, obteniendo información de los principales fabricantes de equipo y de empresas suministradoras de servicios de telecomunicaciones.

Con la información recopilada se realizó una evaluación de las diferentes tipos de redes para desarrollar el temario propuesto y cumplir con el objetivo de la tesis.

Para esto en el Capítulo 1 mencionamos las diferentes tecnologías habilitadoras que ayudan a tener una comunicación entre diferentes dispositivos las cuales son necesarias conocer para introducir las características primordiales de las diferentes redes inalámbricas como son: ancho de banda, tasa de transmisión, y cualidades básicas en cualquier esquema de comunicación.

Ya en el Capítulo 2 observamos la creación y uso de las Redes de Paquetes por Radio, como son: ARDIS, CDPD, Mobitex y GPRS. Después las Redes de Área Local Inalámbricas (WLANS) son analizadas en el Capítulo 3, haciendo mención del estándar 802.11 y sus diferentes grupos de trabajo, así también el estándar de la ETSI HiperLAN2.

En el Capítulo 4 comparamos y analizamos las dos principales tecnologías de telefonía inalámbrica pública o empresarial: DECT (de Europa) y PHS (de Japón). Posteriormente las Redes Inalámbricas de Área Personal, como son, el estándar IEEE 802.15 y sus grupos de trabajo, Bluetooth, HomeRF, Air5 y el estándar que utiliza radiación infrarroja IRDA, son revisadas en el Capítulo 5.

Un concepto importante dentro de las nuevas redes es el que se desarrolló en el Capítulo 6, Red Ad Hoc. Como la tendencia es hacia el argumento de redes dependientes de la aplicación y la localización, optimizadas de acuerdo a su utilización, el usuario dependiendo de sus

necesidades y preferencias, será servido por la red más idónea o construirá su propia red (Red Ad Hoc).

En el Capítulo 7 se hace un análisis de la esencia de la computación móvil ahora conocida como computación esparcida (prevasive) las cuales crean entornos con gran densidad de dispositivos con capacidad de comunicación permanente y de análisis, por medio de computadoras que puedan integrarse exitosamente en la vida cotidiana del ser humano.

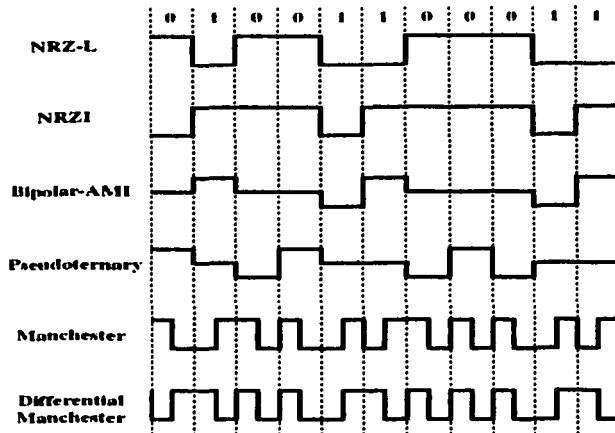
Finalmente en el Capítulo 8 analizamos el estado de implementación de las Redes Inalámbricas, comparando necesidades y requerimientos dependiendo de la aplicación que se le vaya a dar a la red; por eso mencionamos algunos dispositivos y empresas que se dedican a implementar, hacer equipos y trabajos relacionados a redes inalámbricas; además mencionamos algunas aplicaciones que ya están en servicio en México.

El resultado de este trabajo fue tener un estudio sobre las nuevas Redes Inalámbricas donde se resaltan las innovaciones tecnológicas en ellas y la problemática de su implementación, así también para que este trabajo pueda servir como referencia y base para el desarrollo de otras tesis.

1. Tecnologías Habilitadoras

1.1 Códigos de línea

Los códigos de línea son los siguientes: Sin retorno al nivel 0 (NRZ-L), Sin retorno al nivel 0 invertido (NRZI), Bipolar AMI, pseudoternario, Manchester, Manchester Diferencial y HDB3.



TESIS CON FALLA DE ORIGEN

Figura 1.1 Formatos de codificación con señales digitales

1.1.1 Sin retorno al nivel 0 (NRZ-L)

Dos tensiones diferentes para bits 0 y 1. Tensión constante durante el tiempo de bit, es decir, que no hay transición durante el bit 0, tensión positiva constante para 1. Así mismo, se tiene más a menudo la tensión negativa para 1 y positiva para 0

1.1.2 Sin retorno al nivel 0, invertido (NRZI)

Sin retorno al nivel 0 invertido en los "unos". Pulso de tensión constante durante la duración del bit. Datos codificados como presencia o ausencia de transición de señales al comienzo del tiempo de bit. Transición (bajo a alto o alto a bajo) denota un 1 binario. Si no hay transición significa un 0 binario

1.1.3 Codificación diferencial

Los datos se representan más por transiciones que por niveles por lo que es más fácil la detección de la transición que del nivel, en sistemas de transmisión complejos es más fácil perder el sentido de la polaridad si, por ejemplo, se invierten los cables.

Las ventajas e inconvenientes de los códigos NRZ son:

- Ventajas
 - Fáciles de construir
 - Usan bien el ancho de banda
- Inconvenientes
 - Componente continua
 - Falta de capacidad de sincronización
- Utilizados para grabación magnética.
- No se suelen utilizar para transmisión de señales
- Binario multinivel.
- Usa más de dos niveles.



1.1.4 Bipolar-AMI

(Inversión de marca alternada).

- "Cero" representado por ausencia de señal en la línea.
- "Uno" representado por pulso positivo o negativo.
- Los pulsos "uno" alternan en la polaridad.
- No pierde el sincronismo en tramas largas de "unos" (los "ceros" sí tienen ese problema).
- No hay componente continua neta.
- Ancho de banda inferior.
- Sencilla detección de errores.

1.1.5 Binario multinivel o Pseudoternario

Los "unos" se representan por ausencia de la señal en la línea. Los "ceros" se representan por alternancia positiva y negativa. No tiene ventajas ni inconvenientes respecto del código bipolar-AMI.

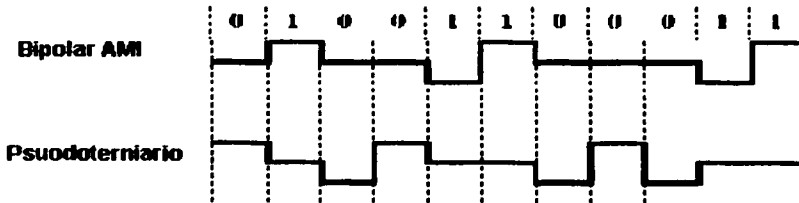


Figura 1.2 Formatos de codificación Bipolar AMI y Binario Multinivel.

1.1.6 Comparativa Binario Multinivel

No es tan eficiente como los NRZ. Cada elemento de señal sólo representa un bit. En un sistema de 3 niveles el receptor debe distinguir entre tres niveles: (+A, -A, 0). Requiere aproximadamente 3dB más de energía de señal, para la misma probabilidad de error de bit.

1.1.7 Manchester

Transición en medio de cada periodo de bit. La transición sirve como reloj y datos. Bajo hacia alto representa un 1. Alto hacia bajo representa un 0. Usado para IEEE 802.3: Ethernet (CSMA/CD).

1.1.8 Manchester Diferencial

Transición a mitad de bit, sólo para temporización. Transición al comienzo de un periodo de bit representa 0. Falta de transición al comienzo de un periodo de bit representa un 1. Es un esquema de codificación diferencial. Usado para IEEE 802.5: Token Ring.

- Ventajas e inconvenientes de los códigos bifase:
 - Inconvenientes: Hay una transición por bit, al menos, y a veces dos. La velocidad máxima de modulación es el doble de la de NRZ y requiere más ancho de banda.
 - Dentro de las ventajas tenemos los siguientes puntos: Sincronización en el medio de la duración de bit (autotemporización). No hay componente continua de directa. Existe detección de errores y hay una ausencia de transición esperada.

1.1.9 Bipolar 3 Ceros de Alta Densidad (HDB3)

High Density Bipolar 3 Zeros, está basado en el código bipolar-AMI. Las cadenas de 4 "ceros" se reemplazan por cadenas con uno o dos pulsos, causa violaciones del código AMI, así mismo no es fácil que ocurra como resultado del ruido y el receptor detecta las secuencias y las convierte en todos "0"

1.2 Técnicas de Modulación

Las técnicas de modulación digital pueden agruparse en tres grupos, dependiendo de la característica que se varíe en la señal portadora. Cuando se varía la amplitud, la técnica de modulación digital que se utiliza se conoce como **Modulación por Corrimiento en Amplitud** (ASK, por sus siglas en inglés). Si se varía la frecuencia o la fase, las técnicas empleadas serían la **Modulación por Corrimiento en Frecuencia** (FSK) o la **Modulación por Corrimiento en Fase** (PSK), respectivamente. Cualquiera que sea la técnica de modulación digital empleada, la amplitud, la frecuencia o la fase de la señal portadora podrá tomar únicamente un número finito de valores discretos.

Debido a que permite una visualización muy clara del ambiente de modulación digital que se utilice, resulta muy práctico representar una fuente discreta de señales a partir de su "**espacio de señal**" o "**constelación**". Una "constelación" es una representación geométrica de señales en un espacio de "n" dimensiones, en donde se visualizan todos los símbolos de salida posibles que puede generar un modulador. Gracias a que en una constelación cada símbolo tiene asociado un valor de magnitud y uno de fase (como sucede en una representación polar), salvo en el caso de la modulación FSK, todos los demás esquemas de modulación digital pueden representarse en un plano de dos dimensiones.

La amplitud y la fase de una señal pueden modularse simultáneamente o por separado, aunque esto resulta difícil de generar y principalmente de detectar. En vez de ello, es muy práctico separar la señal en dos componentes independientes conocidos como I (componente "**en fase**") y Q (componente "**en cuadratura**"), ambos ortogonales entre sí. Cuando nos referimos a comunicaciones digitales, es común expresar la modulación en términos de estas dos componentes, razón por la cual, la representación de una **constelación bidimensional I-Q** es particularmente útil y puede asociarse a la mayor parte de los métodos de modulación digital. En una "constelación I-Q", la componente "en fase" se proyecta en el eje de las abscisas (eje x) y la componente "en cuadratura" se proyecta en el eje de las ordenadas (eje y) de un plano cartesiano. Se dice que una señal estará "en fase" cuando su ángulo de fase sea de cero grados (situada en el eje I) y que una señal estará "en cuadratura" cuando se encuentre desfasada 90° respecto a la señal en fase (situada en el eje Q). Véase la Figura 1.3.

ERRORES CON
 FALLA DE ORIGEN

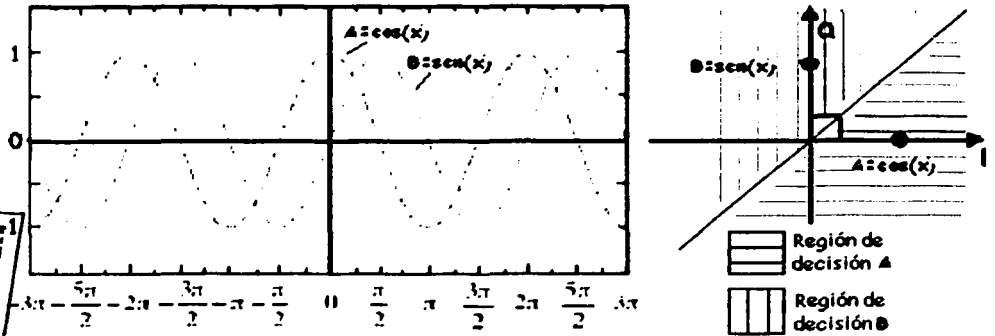


Figura 1.3 Proyección de una señal en fase (coseno) y una señal "en cuadratura" (seno) en la constelación "I-Q" con defasamiento de 90°.

En esta representación I-Q, cada señal que se mapea en una constelación tendrá asociada una posición precisa. (Esto es, un punto de coordenadas (I,Q).) Es con base en esta posición que los equipos receptores pueden determinar qué señal se transmitió. Para ello, cada señal mapeada en la constelación tiene asociada una "región de decisión". Ver Figura 1.3. Sin embargo, conforme una señal se propaga a través del canal de comunicación, ésta se verá afectada por ruido, provocando una modificación en la posición de los símbolos mapeados en la constelación. Cuando uno de estos símbolos se ubica más allá de la "región de decisión" que le corresponde, éste se confundirá con alguno de los símbolos adyacentes y, en consecuencia, provocará un error de bits.

1.2.1 Amplitude Shift Keying (ASK)

En la modulación ASK se varía la amplitud de una señal con frecuencia y fase constantes, de tal forma que en su "constelación I-Q", los símbolos mapeados se ubican a lo largo del eje I. En el caso de la modulación binaria ASK, un "0" lógico se representa por $s_1(t) = 0$, mientras que un "1" lógico se representa por $s_2(t) = A \cos(\omega_c t)$. De tratarse de modulación ASK multinivel 2, el número de símbolos mapeados en la constelación determinará el número de posibles niveles de amplitud que tome la señal ASK. La Figura 1.4(a) muestra la constelación de la modulación binaria ASK y la señal ASK para la secuencia binaria 0010110.

1.2.2 Phase Shift Keying

En la Modulación por Corrimiento en Fase (PSK), la característica que varía de la señal portadora es la fase, manteniéndose la amplitud y la frecuencia constantes. Para una modulación PSK multinivel, la señal PSK podrá contar con tantos valores distintos de fase como símbolos se tengan mapeados en la "constelación I-Q". Debido a que entre cada señal existe una diferencia de fase, cada símbolo mapeado podrá componerse de una componente "en fase" y una componente "en cuadratura". En el caso específico de la modulación binaria PSK (BPSK), un "0" lógico se representaría por $s_1(t) = A \cos(\omega_c t)$, mientras que el "1" lógico estaría representado por $s_2(t) = A \cos(\omega_c t - \delta)$. Obsérvese en la Figura 1.4(b) los diagramas de las constelaciones BPSK y QPSK, así como también la señal BPSK para la secuencia anterior.

1.2.3 Frequency Shift Keying

Para la Modulación por corrimiento de frecuencia multinivel se envía una portadora de m señales, cada una con una frecuencia distinta, donde m es igual al número de símbolos posibles, mapeados en la constelación FSK correspondiente. A diferencia de las técnicas de modulación anteriores, la constelación de un sistema de modulación FSK multinivel consiste en m ejes coordenados. Es importante señalar que una constelación FSK no presenta componentes I o Q, puesto que la característica que varía en la señal es su frecuencia.

Un "0" lógico en el esquema de modulación binaria FSK será representado por $s_1(t) = \cos(\omega_1 t)$ y un "1" lógico por $s_2(t) = \cos(\omega_2 t)$. La Figura 1.4(c) muestra la constelación FSK binaria y la señal correspondiente a esta técnica de modulación para la misma secuencia binaria que se venía utilizando.

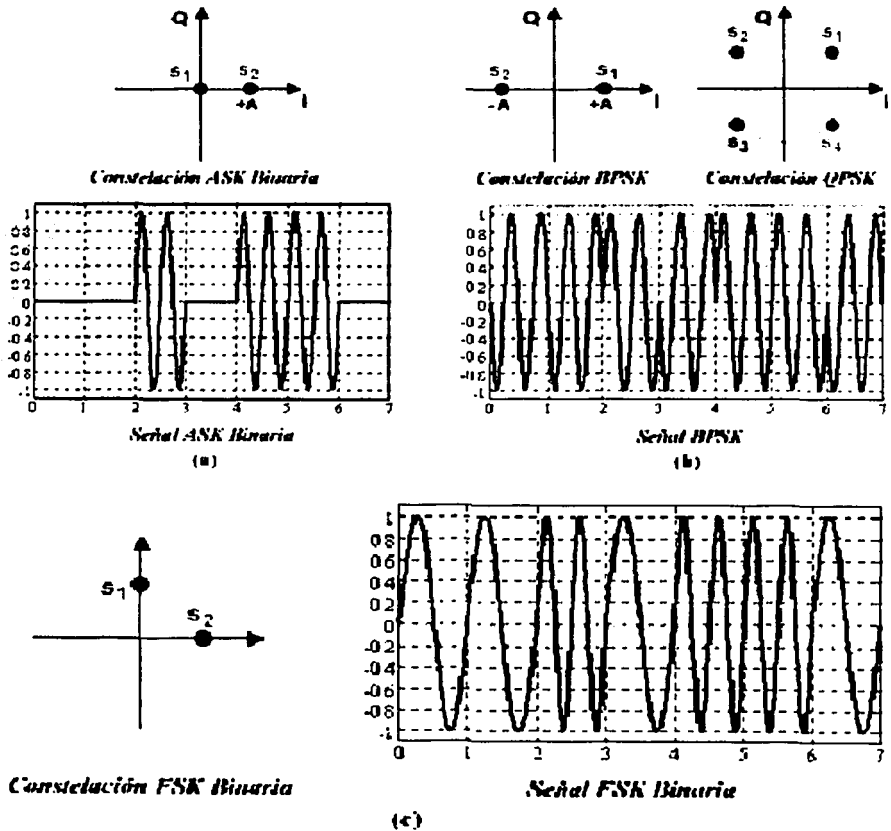


Figura 1.4 (a), (b) y (c). Señales binarias y constelaciones de las modulaciones digitales ASK, BPSK y FSK.

1.2.4 Gaussian Minimum Shift Keying GMSK

Es un método de modulación digital derivado de la modulación por desplazamiento de fase y que se utiliza en el sistema GSM de telefonía celular. Esto puede ser visualizado en un diagrama I/Q que muestra los componentes real (I) e imaginario (Q) de la señal transmitida (figura 1.5). La transmisión de un bit cero o uno se representa por el cambio de fase por incrementos de $+\pi$ o $-\pi$. Cada símbolo que se transmite representa un bit, es decir, cada cambio en la fase representa un bit.

Al usar la modulación BPSK, la distancia entre los diferentes símbolos es menor que al usar GMSK. Estas menores distancias aumentan el riesgo de una interpretación errónea de los símbolos, porque para el receptor es más difícil diferenciar entre los distintos símbolos recibidos. Bajo buenas condiciones de radio, esto no tiene mucha influencia. Bajo condiciones de radio pobres, sin embargo, adquiere más importancia. Por lo tanto, se usarán bits "extra" para agregar más codificación de corrección de errores y permitir la recuperación de la información correcta. GMSK es más eficiente sólo bajo ambientes de radio muy pobres, como es el caso de Mobitex.

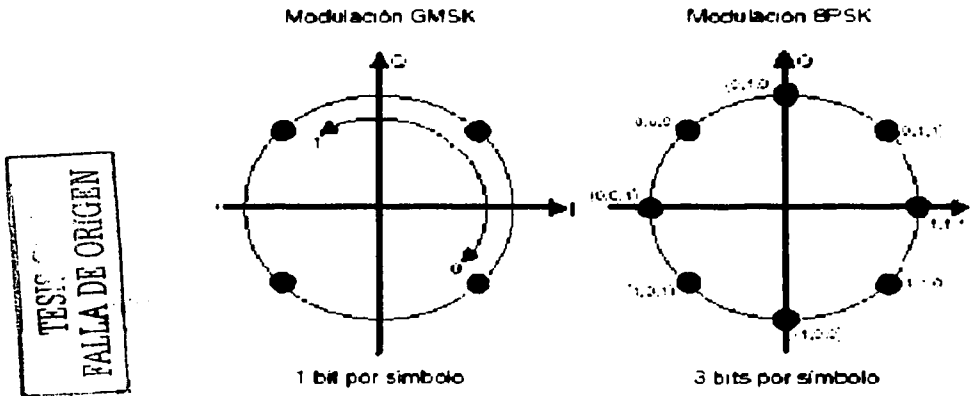


Figura 1.5 Diagrama I/Q de la modulación GMSK.

1.2.5 Modulación en Amplitud por Cuadratura (QAM)

La Modulación en Amplitud por Cuadratura (QAM, por sus siglas en inglés) es un esquema de modulación multinivel en donde se envía una de $M = 2^n$ señales, con distintas combinaciones de amplitud y fase. Utilizando múltiples niveles, tanto en la modulación en amplitud como en la modulación en fase, es posible la transmisión de grupos de bits, de manera que cada uno de estos grupos será representativo de un conjunto nivel-fase característico de la portadora de la señal, mismo que dará cabida a un símbolo. Una de las características principales de la modulación QAM es que modula la mitad de los símbolos con una frecuencia y la otra mitad con la misma frecuencia, pero desfasada 90° . El resultado de las componentes después se suma, dando lugar a la señal QAM. De esta forma, QAM permite llevar dos canales en una misma frecuencia mediante la transmisión ortogonal de uno de ellos con relación al otro. Como ya se ha dicho, la componente "en cuadratura" de esta señal corresponderá a los símbolos modulados con una frecuencia desfasada de 90° , y la componente "en fase" corresponde a los símbolos modulados sobre una portadora sin fase. Obsérvese en la Figura 1.6 las constelaciones para los esquemas de modulación 4-QAM, 16-QAM y 64-QAM. Note que para cada uno de ellos se varían los niveles de amplitud y de fase de la señal.

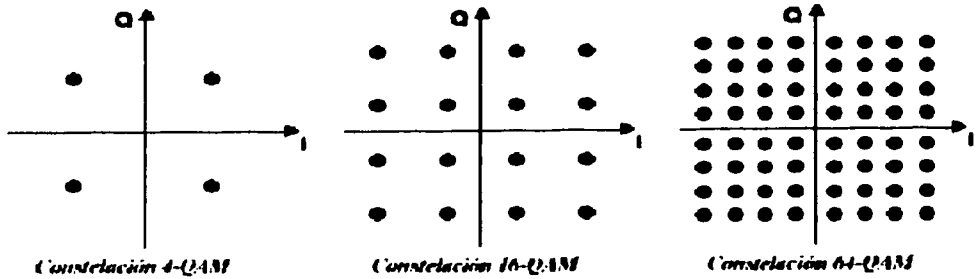


Figura 1.6 Ejemplos de constelaciones QAM.

En el caso concreto de la modulación 16-QAM, permite contar con 16 estados diferentes, mismos que estarán determinados por el número de símbolos mapeados en su constelación correspondiente. Debido a que $16 = 2^4$, cada uno de estos símbolos puede representarse mediante cuatro bits, dos de ellos correspondientes a la componente “en cuadratura” (portadora desfasada), y los dos restantes, correspondientes a la componente “en fase” (portadora con fase cero) de la señal. Puesto que existen estas dos componentes, cada una representada por dos bits en 16-QAM, es posible transmitir 4 posibles niveles de amplitud para cada componente, lo que supone que, por el efecto de la cuadratura, pueden transmitirse 16 estados.

1.2.6 Modulación OFDM

El principio de la modulación OFDM consiste en distribuir el flujo binario de información entre un gran número de portadoras de forma que cada una maneje una velocidad de datos reducida con respecto a la del flujo total. En consecuencia la duración “Tu” de los símbolos aumenta respecto al caso de modular una sola portadora, haciendo de esta forma a la señal muy robusta frente a interferencias por trayectos múltiples (ecos) ya que el retardo de éstos resulta ser muy pequeño comparado con la duración citada.

Por otra parte la separación en frecuencia entre las portadoras se hace igual al inverso de la duración “Tu” de los símbolos, con lo que la posición de las portadoras en el espectro de frecuencias (figura 1.7) coincide con los nulos del espectro de las portadoras adyacentes (condición de portadoras ortogonales). En estas condiciones se consigue mínima interferencia de intersímbolos.

Para fortalecer todavía más a la señal transmitida frente a los ecos, se amplía la duración de los símbolos añadiendo un tiempo Δ denominado “intervalo de guarda” a la duración útil Tu con lo que la duración total del símbolo pasa a ser: $T_s = \Delta + T_u$. El intervalo de guarda es una continuación cíclica de la parte útil del símbolo, el cual se inserta delante de él. En estas condiciones, si la señal se recibe por dos cambios diferentes con un retardo relativo entre ellas, siempre que este retardo no supere el intervalo de guarda, coincidirá en las dos la información contenida dentro del tiempo útil del símbolo de la señal principal.

El tiempo Δ del intervalo de guarda se mide en fracciones de la duración útil “Tu” del símbolo, disponiéndose de cuatro posibles valores: $\Delta / T_u = 1/4 \ 1/8 \ 1/16 \ 1/32$.

TESIS CON
FALLA DE ORIGEN

TESIS CON FALLA DE ORIGEN

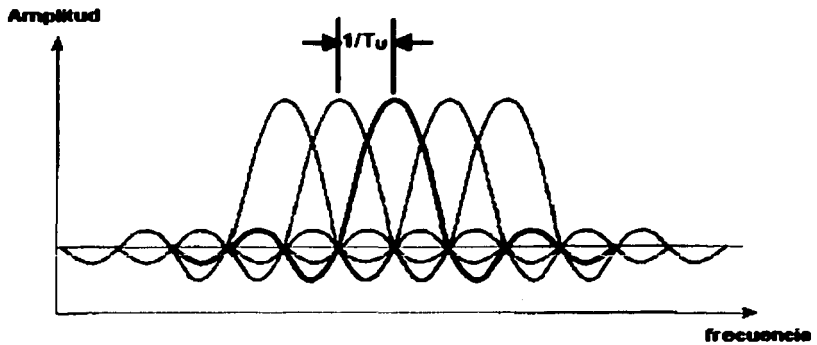


Figura 1.7 Espectro de portadoras adyacentes en la modulación OFDM.

Como los receptores ignoran la señal recibida durante el intervalo de guarda de la señal principal, el resultado es que no habrá interferencia entre símbolos. Sin embargo la inserción de este intervalo de guarda supone una pérdida en la capacidad de transmisión del canal.

En las siguientes figuras se ilustran la disposición de las portadoras en tiempo y frecuencia antes y después de la inserción del intervalo de guarda.

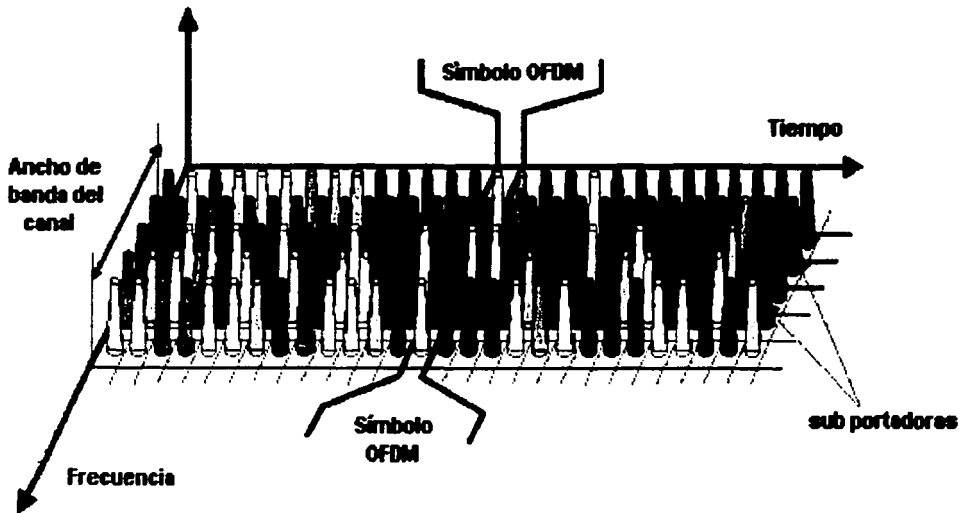


Figura 1.8 Distribución de las portadoras en el tiempo y frecuencia.

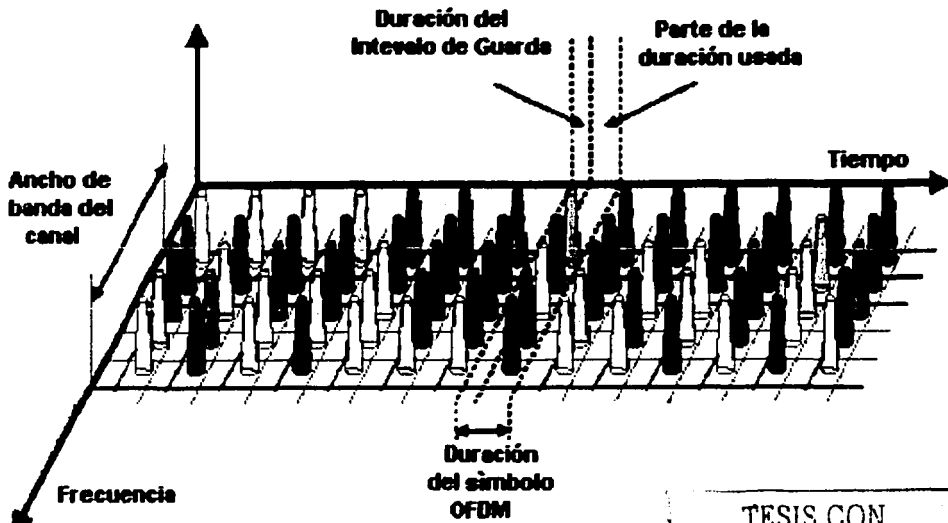


Figura 1.9 Inserción del intervalo de guarda

TESIS CON
FALLA DE ORIGEN

1.3 Técnicas de Acceso Múltiple

Los métodos de acceso múltiple permiten compartir una cantidad finita de espectro de radio entre una gran cantidad de usuarios. En las comunicaciones inalámbricas, es conveniente que el usuario móvil pueda enviar y recibir información en forma simultánea hacia y desde la estación base. A esta "simultaneidad" se la denomina "DUPLEXION" (duplexing).

Para lograr la "duplexión", existen técnicas en el dominio del tiempo y en el dominio de la frecuencia *Frequency Division Duplexing (FDD)*, *Time Division Duplexing (TDD)*.

1.3.1 Frequency Division Duplexing (FDD)

Este método provee dos frecuencias distintas para cada usuario. Dicho método requiere la presencia de un dispositivo denominado "**Duplexor**", en el aparato móvil, permitiendo la recepción y transmisión simultánea. La separación entre las frecuencias de Tx y de Rx es constante para todos los canales.



Figura 1.10(a) Método de duplexión FDD.

1.3.2 Time Division Duplexing (TDD)

Éste utiliza un canal de frecuencia por usuario y mediante el uso de ranuras de tiempo para Tx y para Rx, se da la sensación de "simultaneidad" al usuario. (Nótese que este método no es "full duplex" en estricto rigor.)



Figura 1.10(b) Método de duplexión TDD.

1.4 Técnicas de Acceso Múltiple al Canal

1.4.1 Acceso Múltiple por División de la Frecuencia FDMA

Este esquema consiste en dividir el espectro disponible en varios canales de frecuencia de manera que cada usuario utiliza a la vez dos canales para su comunicación uno para el enlace de subida (con el que transmite información hacia la red) y el otro para el enlace de bajada (con el que recibe información desde la red). Esta asignación de canales es exclusiva, de manera que los canales no pueden ser utilizados simultáneamente por más de un cliente y cada uno de estos canales está bordeado por pequeñas bandas de frecuencia que evitan traslaparse entre sí. Se asignan canales individuales a cada usuario, estos canales son asignados de acuerdo a la demanda. Una frecuencia es para Tx y otra para Rx y normalmente FDMA se combina con multiplexing FDD (ej: sistema AMPS). FDMA utiliza un filtro de RF para minimizar la interferencia con canales adyacentes. Así mismo los amplificadores de potencia no lineales, utilizados en la estación base, trabajan cercanos a la saturación por lo que la no linealidad produce ensanchamiento en frecuencia y genera intermodulación (IM). Dicha IM en RF produce interferencia en los otros canales.

1.4.2 Acceso Múltiple por División del Tiempo TDMA

Con este sistema un usuario ocupa el ancho de banda disponible total pero sólo por un corto período de tiempo. El canal de radio frecuencia se divide en intervalos de tiempo y estos son asignados periódicamente al mismo usuario; cada uno de estos intervalos es subdividido en otros dos: uno para el enlace de subida y otro para el enlace de bajada. Todos los intervalos de tiempo están bordeados por intervalos de protección.

1.4.3 Híbrido FDMA/TDMA

En un sistema TDMA el ancho de banda usado por el sistema se divide normalmente en pequeños canales de radio frecuencia, por lo que actualmente, GSM es un híbrido FDMA/TDMA, como lo son también otros sistemas de telefonía celular de segunda generación.

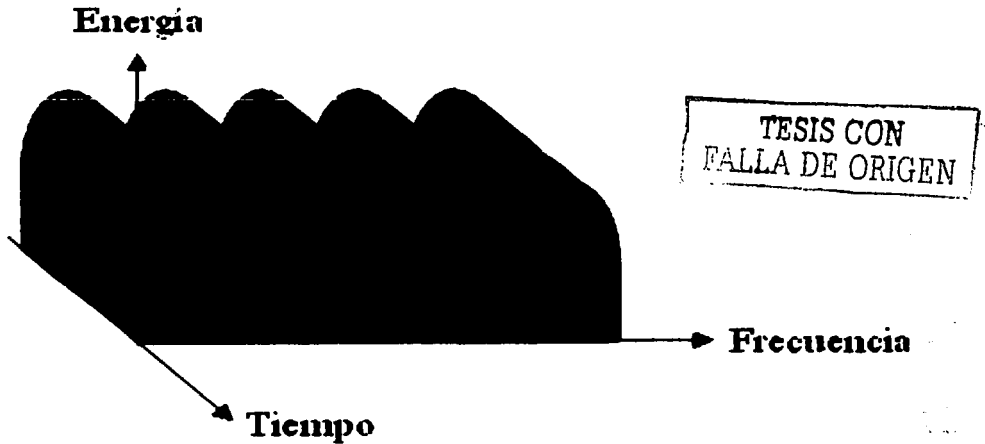


Figura 1.11 Híbrido FDMA/TDMA

1.4.4 Acceso Múltiple por División de Código CDMA

Con este esquema, todos los usuarios ocupan la misma frecuencia simultáneamente, separados por códigos especiales. A cada usuario se le asigna un código aplicado como modulación secundaria, la cual es usada para transformar la señal del usuario en una versión codificada de espectro esparcido.

El receptor emplea el mismo código esparcido para transformar la señal de espectro esparcido de vuelta al flujo de datos original del usuario.

Si la potencia de cada usuario no es controlada por la EB se obtendrá un problema cercano-lejano, éste problema aparece cuando muchos usuarios acceden al mismo canal, entonces lo que se procede a realizar es:

Se utiliza la misma frecuencia. Se combina con TDD o FDD. Si se tuviese un número infinito de códigos ortogonales, no existiría limitación en el N° de usuarios, pero, al aumentar N° de usuarios aumenta la probabilidad de error (sube el piso de ruido en forma lineal). Además, el número de códigos ortogonales no es infinito, ya que está limitado por la cantidad de bits dedicados a formar dicho código ortogonal. El problema cercano-lejano, es indeseado, por lo que se utiliza un detector de alta potencia y se compara con la deseada.

Los códigos se seleccionan de tal manera que tengan una baja correlación cruzada con otros códigos. Esto significa que correlacionando la señal de espectro esparcido recibida con el código asignado sólo es posible recuperar la señal que fue esparcida usando el mismo código, las demás señales permanecen dispersas sobre un amplio ancho de banda.

Por lo tanto, sólo el receptor que conoce el código de esparcimiento correcto puede extraer la señal original de la señal de espectro esparcido recibida. Además, como en un sistema TDMA, el

ancho de banda total disponible se puede dividir en pequeños canales de radio frecuencia. Hay diversos métodos para modular señales CDMA. Uno de ellos es la modulación DSSS (Secuencia Directa de Espectro Esparcido) En este método, la señal modulada ocupa todo el tiempo el único ancho de banda total de portadora.

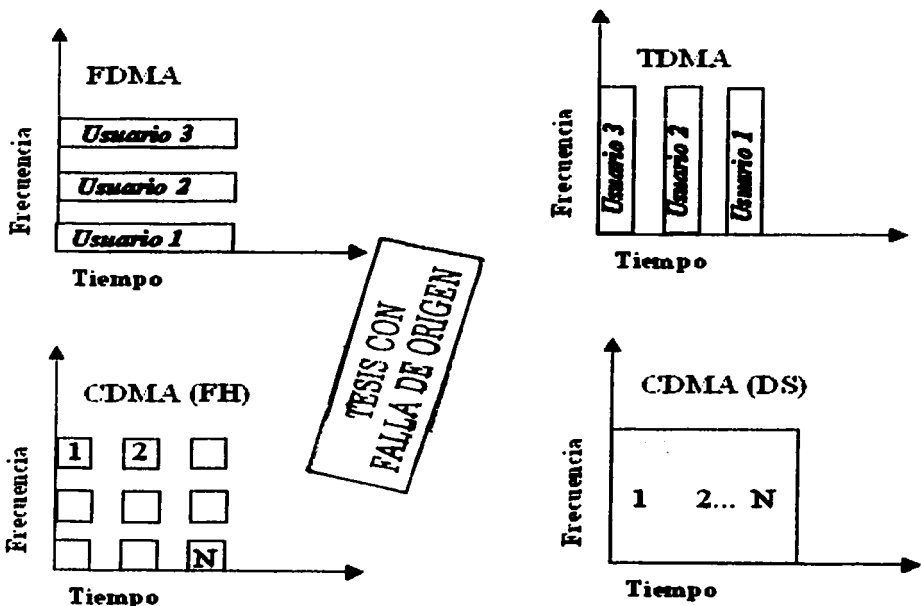
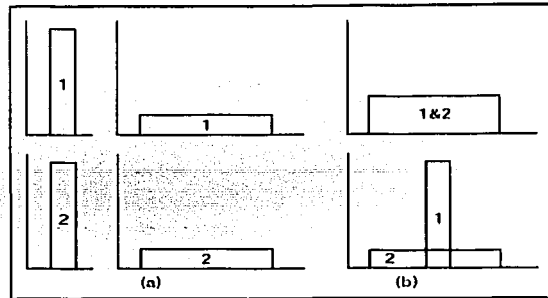


Figura 1.12 Diagramas tiempo - frecuencia de las técnicas de acceso múltiple

1.4.4.1 Capacidad de acceso múltiple

Si múltiples usuarios transmiten señales en el espectro disperso al mismo tiempo, el receptor podrá distinguir entre los usuarios dándole a cada usuario un código el cual tendrá una correlación cruzada suficientemente baja con los otros códigos. Correlacionando la señal recibida con el código de la señal de un cierto usuario, este será el único que podrá obtener dicha señal., mientras que las otras señales quedan en el espectro esparcido en un gran ancho de banda. La capacidad de acceso múltiple se muestra en la siguiente figura, en donde la figura 1.13(a) muestra a dos usuarios generando una señal de banda estrecha de datos en el espectro esparcido. En la figura 1.13(b) ambos usuarios transmiten sus señales al mismo tiempo y al recibir 1 solo la señal del usuario 1, la información de dicho usuario es recobrada.



TESIS CON
FALLA DE ORIGEN

Figura 1.13 Principio básico del acceso múltiple del espectro esparcido.

1.4.4.2 Espectro Esparcido (Spread Spectrum)

También llamada de espectro amplio, disperso o extendido, es la técnica más utilizada en LANs inalámbricas inicialmente desarrollada con el propósito de combatir las interferencias en las comunicaciones militares.

Consiste en dividir las señales informativas en distintas frecuencias que están en la banda reservada para aplicaciones generales industriales, científicas y médicas llamada banda ISM (Industrial Scientific and Medical Radio Frequency) la cual ocupa la parte del espectro que va de 902 - 928 [MHz], 2.4 - 2.484 [GHz], y 5.725 - 5.850 [GHz], frecuencias también utilizadas por hornos microondas y controles de puertas eléctricas entre otros (para estas frecuencias no es necesario licencia).

Si el receptor no está sincronizado a la frecuencia correcta, una señal del espectro esparcido se tomaría como ruido de fondo. Además, con esta técnica se reduce la interferencia con otras señales no deseadas.

A continuación pasamos a comentar los dos tipos de espectro extendido que existen:

1.4.4.3 Secuencia Directa – CDMA (DS-CDMA o DSSS)

En DS-CDMA la información de la señal se modula directamente por un tiempo discreto digital y es discretamente valorada la señal del código. La señal de datos puede ser analógica o digital. En el caso de que sea una señal digital la modulación de los datos a menudo se omite y la señal de datos es directamente multiplicada por la señal codificada y la señal que resulta modula a la portadora en banda ancha. Por esta multiplicación es que la DS-CDMA toma ese nombre.

En el diagrama de bloques de la figura 1.14 se muestra un transmisor de DS-CDMA. La señal de datos binaria modula a la portadora en RF. La portadora modulada, entonces, es modulada por una señal codificada. Esta señal codificada consiste en un número de bits codificados llamados "chips", estos pueden ser +1 o -1. Para obtener la señal deseada esparcida, la frecuencia del chip de la señal codificada debe ser mucho mayor que la frecuencia del chip de la señal de información. Para el código de modulación pueden ser usadas distintas técnicas de modulación, pero usualmente se utilizan algunas como PSK, BPSK, D-BPSK, QPSK y MSK.

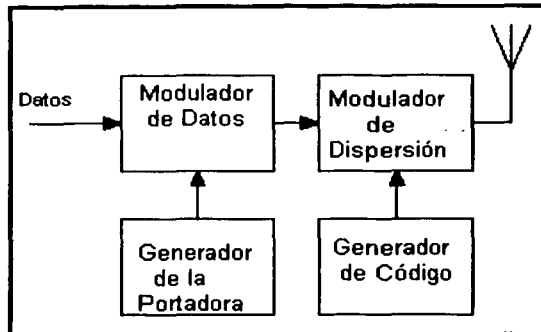


Figura 1.14 Diagrama de bloques de un transmisor DSSS.

Después de la transmisión de la señal, el receptor usa una demodulación coherente para encontrar la señal en el SS, usando un codificador de secuencia generada. Este tiene que ser capaz de recuperar la señal, el receptor no solo conocerá la secuencia del código usado con la que se esparció la señal, pero los códigos de recuperación de la señal recibida y el generador de código tendrán que estar sincronizados. La sincronización tiene que ser completada al principio de la recepción y mantenida hasta que toda la señal haya sido recibida. En el bloque de código sincronización/seguimiento es en donde se lleva a cabo el paso anterior. Después de recuperar y ver los datos de la señal modulada y después de la demodulación los datos originales, la señal original puede ser recuperada.

FALLA DE ORIGEN

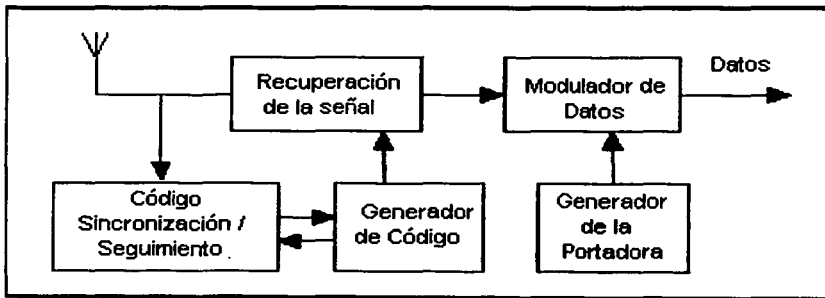


Figura 1.15 Receptor de la señal DS-SS.

Debido al efecto de los chips, el DSSS está actualmente limitado a 2 [Mb/s] en la banda de 902 [MHz] y a 10 [Mb/s] en la banda de 2.4 [GHz]. En E.E.U.U y Europa, DSSS opera en el rango 2.4 [GHz] hasta 2.4835[GHz], esto implica un total de 83.5 [MHz] que se dividen en 14 canales cada uno con 5 [MHz] de ancho de banda. Cada país utiliza determinados canales.

En topologías de red en las que haya varias celdas, ya sean sobrepuestas o adyacentes, los canales pueden operar simultáneamente sin apreciarse interferencias si la separación entre frecuencias centrales es como mínimo 30 [MHz]. Esto quiere decir que de los 83.5 [MHz] podemos obtener 3 canales independientes que pueden operar simultáneamente en una determinada zona geográfica con ausencia de interferencias.

DSSS cubre una distancia de 150 metros y se utiliza normalmente en aplicaciones punto a punto.

1.4.4.4 Salto de Frecuencia CDMA (FH-CDMA)

En el salto de frecuencia de CDMA la frecuencia de la portadora de la señal de información modulada no es constante pero esta cambiando periódicamente. Durante los intervalos de tiempo T la frecuencia de la portadora es la misma, pero después de cada intervalo de tiempo la portadora brinca o cambia a otra frecuencia. El patrón de brinco o cambio de frecuencia es decidido por el código de la señal. El conjunto de frecuencias disponibles para la portadora puede llamarse *hop-set*. La frecuencia ocupada por el sistema FH-SS (Frequency Hopping Spread Spectrum) difiere considerablemente de un sistema DS-SS (Direct Sequence Spread Spectrum). Un sistema de Secuencia Directa ocupa toda la banda de frecuencias cuando transmite, considerando también que un sistema de salto en frecuencia (FH) usa solo una pequeña parte del ancho de banda cuando este transmite. La diferencia entre las frecuencias usadas en FH-SS y DS-SS se muestra en la siguiente figura. Supongamos que un sistema FH está transmitiendo en la banda de frecuencia 2 durante el primer periodo de tiempo. Un sistema de DS transmite en el mismo periodo de tiempo esparciendo la potencia de la señal sobre toda la banda de frecuencia, entonces la potencia transmitida en la banda de frecuencia 2 será mucho menor que la del sistema FH. De cualquier manera la el sistema DS transmite en la banda de frecuencia 2 durante todos los periodos de tiempo, mientras que el sistema FH solo usa esta parte de la banda en el tiempo. En promedio ambos sistemas transmitirán la misma potencia en la banda de frecuencia.

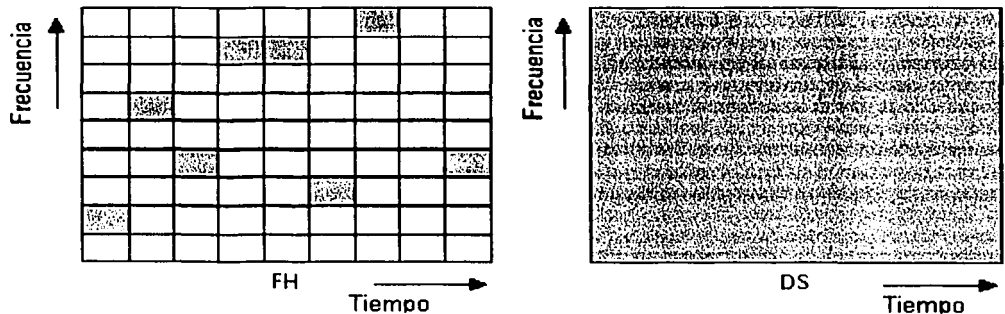


Figura 1.16 Tiempo/Frecuencia por las señales FH y DS.

En la figura 1.17 se muestra el diagrama de bloques del sistema FH-CDMA. Utilizando un sintetizador rápido de frecuencias, este es controlado por una señal codificada, la frecuencia de la portadora es convertida en la frecuencia transmitida.

El proceso inverso lo lleva a cabo el receptor. Usando una secuencia de código generado, el receptor de señales convierte la señal recibida en una señal banda base. Por lo tanto los datos son recuperados después de la demodulación. El circuito de sincronización/seguimiento (synchronization/tracking) asegura que el salto realizado por la portadora generada se sincronice con la portadora recibida, entonces, este proceso de demodulación podrá llevarse a cabo.

TESIS CON FALLA DE ORIGEN

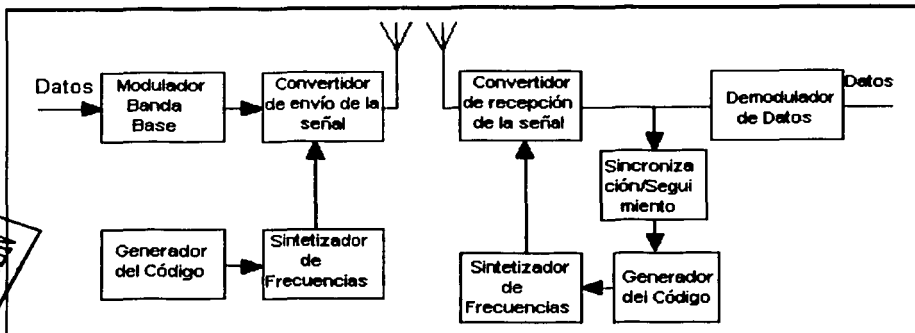


Figura 1.17 Diagrama de bloques de un transmisor y receptor FH-CDMA.

1.4.4.5 Salto de Tiempo – CDMA (Time Hopping – CDMA)

En el sistema de salto de tiempo en CDMA la señal de datos es transmitido en una ráfaga de intervalos de tiempo determinado por un código asignado al usuario. El eje del tiempo es dividido en tramas, y cada trama es dividida en M ranuras de tiempo. En cada trama el usuario transmitirá en una de las M ranuras de tiempo. Cada ranura de tiempo M es transmitida dependiendo del código de la señal asignada al usuario. Puesto que un usuario transmite todos sus datos en una sola ranura de tiempo M , en vez de utilizar todas ranuras de tiempo M , la frecuencia necesita para su transmisión aumentar en un factor M . En la figura 1.19 observamos que TH-CDMA utiliza todo el espectro de banda ancha en cortos periodos de tiempo en vez de utilizar parte de todo el espectro del tiempo. El sistema de transmisión y recepción de THSS se muestra en la figura 1.18.

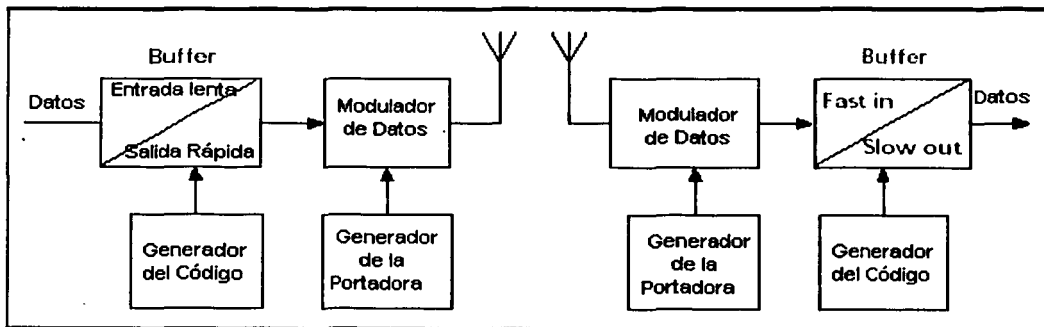
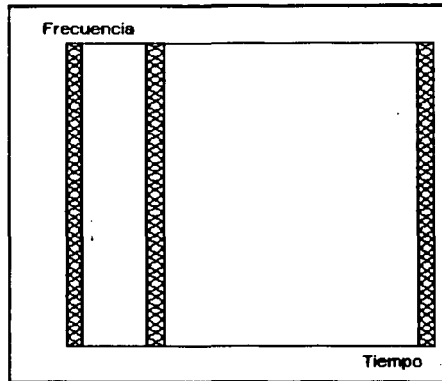


Figura 1.18 Diagrama de bloque de un transmisor y receptor de un sistema TH-CDMA.



TESIS CON FALLA DE ORIGEN

Figura 1.19 Gráfica de tiempo y frecuencia del sistema TH-CDMA.

1.4.4.6 Sistemas Híbridos CDMA (HS-CDMA)

Los sistemas híbridos CDMA emplean una combinación de dos o más de las técnicas de espectro esparcido ya mencionadas. Para combinar las técnicas de modulación básicas de espectro esparcido, se tiene cuatro híbridos posibles: DS/FH, DS/TH, FH/TH y DS/FH/TH. La idea principal de estos sistemas híbridos es combinar las ventajas de cada una de las técnicas de modulación. Si nosotros tomamos, por ejemplo, la combinación del sistema DS/FH, en este caso se podría observar la ventaja que se tiene al no ser afectado por la propiedad de multitrayectorias del sistema DS combinado con la favorable operación cercano-lejano del sistema FH. Seguramente, la desventaja yace en el aumento de la complejidad de los sistemas de transmisión y recepción, por ejemplo, tenemos la siguiente figura en donde podemos observar el diagrama de bloques de un sistema híbrido de transmisión DS/FH CDMA.

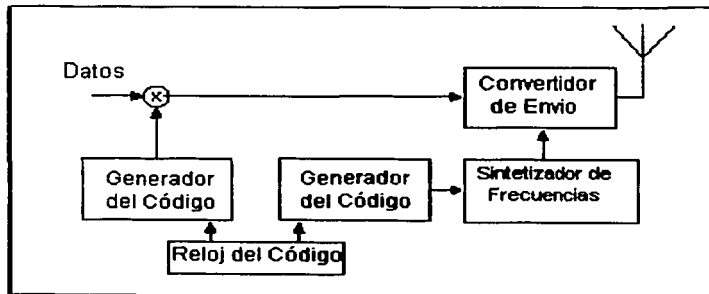


Figura 1.20 Transmisor de un sistema híbrido DS/FH.

La señal de información pasa por el primer sistema (DS) usando una señal codificada, esta es esparcida en el espectro de radiofrecuencia, la señal esparcida se modula en una portadora cuya frecuencia de salto va de acuerdo con el código de ese sistema (FH). Entonces el código del reloj se asegura de corregir la relación entre estos dos códigos.

1.5 Codificación

A medida que el control de errores ha sido de interés se utiliza la codificación en dos diferentes aproximaciones, esto es, detección de errores y corrección de errores. Los códigos usados comúnmente son muy simples y combinados usualmente con un esquema ARQ (Automatic Repeat Request).

Después estas aproximaciones requieren códigos más elaborados así que aumenta a un número seguro de errores de bits que pueden ser corregidos en la recepción. Este esquema es conocido como FORWARD ERROR CORRECTION (FEC). Las redundancias son agregadas en el mensaje por el canal de codificación en la transmisión final, para producir los datos codificados en la más alta tasa de bit, (higher bit rate). En la recepción final, el canal decodificado convenientemente trata que todo salga en los datos recibidos en orden de reestablecer el mensaje inicial. Los códigos han sido clasificados dentro de dos grupos básicos: esto es, códigos de bloque y códigos convolucionales. Estos se distinguen uno del otro por la ausencia o presencia de memoria, respectivamente. Los códigos pueden también ser clasificados como lineales o no lineales. En los códigos lineales dos palabras de código son aumentadas en aritmética modulo dos para generar una tercer palabra código.

1.5.1 Códigos de Bloque Lineales

En un código de bloque lineal (n, k) un mensaje de k -bits es codificado en una palabra código de n -bits. En consecuencia, el número de bits redundantes es $n-k$. Dado esto, un mensaje sin codificar es transmitido en una tasa z , la tasa de transmisión de el mensaje codificado es incrementado a $(n/k)z$ así que el tiempo total de transmisión puede ser guardado sin alteraciones. La relación de menor dimensión es $r = k/n$ es conocida como tasa de código y clasificada de 0 a 1. Dejando que el vector sea u de k -dimensiones el que contenga el mensaje sin codificar y que c sea un vector de n -dimensiones el que contenga el mensaje codificado. Se define a G como una matriz generadora, como: $c = u \cdot G$

Porque c contiene el mensaje sin codificar mas los bits redundantes, la matriz generadora debe ser compuesta de una matriz identidad de $k \times k$ y un coeficiente $k \times (n-k)$. Se denota la matriz de identidad como I_k y el coeficiente de la matriz como P . $G = [PM_k]$

Un código de bloque con esta representación es conocido como un código de bloque lineal sistemático. Otra importante definición es la matriz de paridad con las dimensiones $(n-k) \times n$, escrita como: $H = [I_{n-k} MP^T]$ donde I_{n-k} es una matriz identidad $(n-k) \times (n-k)$ y P^T es una matriz transpuesta de P de $(n-k) \times k$. Esto se puede demostrar con aritmética modulo 2:

$$HG^T = [I_{n-k} MP^T] \cdot \begin{bmatrix} P^T \\ I_k \end{bmatrix} = P^T + P^T = 0$$

Las matrices G y H son utilizados en las operaciones de descodificación y codificación.

1.5.1.1 Detección de Errores: Síndrome

Cuando se transmite una palabra de código c , ésta llega a la recepción final como $r = c + e$, donde e es un vector error que contiene 1's indicando la posición del error y 0's en el resto de la palabra. En la recepción final la decodificación cumple con la siguiente operación: $s = rH^T$

Conocido como síndrome de r . Esto es fácil de mostrar si $s \neq 0$ entonces los errores han sido detectados. Si $s = 0$ entonces los errores no han sido detectados (aunque ellos podrían todavía haber ocurrido). Por que $r=c+e$ y $c=uG$, entonces: $s = uGH^T + eH^T$ $s = eH^T$

Esta ecuación muestra que el síndrome depende solo sobre el error e y no sobre la palabra código

LOS CON
 DE ORIGEN

transmitida. Porque e es un vector de n -dimensiones y H^T es una matriz de $n \times (n-k)$, entonces s es un vector de $(n-k)$ dimensiones. En otras palabras hay 2^{n-k} síndromes posibles.

1.5.1.2 Distancia mínima

La distancia de Hamming $d(x,y)$ entre dos palabras código x y y es definido como un número de 1's obtenidos después de la operación or-exclusiva bit por bit entre las dos palabras código. Por lo tanto la distancia entre 1001 y 0111 es 3. El peso de Hamming $w(x)$ de una palabra código x es definido como el número de unos que tenga una palabra. En el caso anterior el peso respectivo de cada palabra es 2 y 3. De la definición de la distancia de Hamming se muestra lo siguiente:

$d(x,y) = w(x+y)$ la mínima distancia d_{\min} de un código de bloques lineal es la mas mínima distancia de Hamming entre cualquier par de vectores códigos en el código., i.e;

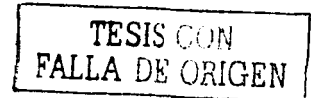
$$d_{\min} = \min\{d(x,y) : x, y \in c, x \neq y\}$$

Por consiguiente:

$$d_{\min} = \min\{w(x,y) : x, y \in c, x \neq y\}$$

Porque $z = x+y$ es otro vector código en c esto muestra que

$$d_{\min} = \min\{w(z) : z \in c, z \neq 0\} \text{ o } d_{\min} = w_{\min}$$



En otras palabras la distancia mínima es el menor peso de Hamming del vector código que contenga el mayor número de ceros en el código.

Para encontrar el peso de Hamming mínimo se cancela la palabra nula y sobre todas las otras se escoge el peso mínimo.

Distancia mínima = peso mínimo

1.5.1.3 Corrección de errores

Un código (n,k) admite 2^n vectores de código que contienen 2^k palabras de código. La mejor estrategia de decodificación es tal que sobre la recepción de cualquier vector del código, el decodificador se asocie con la palabra más cercana del código.

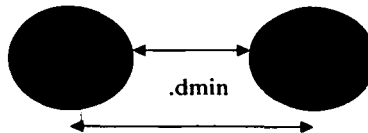


Figura 1.25. Distancia entre dos palabras código vecinas.

Definir las esferas no traslapadas con radio t alrededor de cada palabra de código de manera que dentro de cada esfera todos los vectores del código son decodificados correctamente. Porque (1) las esferas no hacen el traslape y no hacen la comparación de uno con otro y (2) la distancia entre las dos palabras de código vecinas es la mínima distancia. Esto es la distancia mínima del código: $d_{\min} \geq 2t + 1$, donde t es el número de errores que se pueden corregir en un bloque de largo.

Consecuentemente, se puede decir que un código de bloque lineal (n,k) puede corregir t errores tales que:

$$t \leq \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

1.5.2 Códigos Cíclicos

Los códigos cíclicos comprenden una clase especial de códigos de bloque lineales. Su estructura algebraica es tal que la codificación, el síndrome computarizado y, la decodificación son muy simples para implementar y para ser hecha por registros promediados variados con alguna conexión de retroalimentación. Una propiedad fundamental de este código es que cualquier variación cíclica de un vector del código en c es también un vector de código en c .

Esta sugerencia de que los elementos de cada palabra de código de longitud n puede ser tratada como los coeficientes de un polinomio de grado $(n-1)$. Haciendo que $c_i, i=0,1,\dots,n-1$, sean los elementos de una palabra de código c . El correspondiente código polinomial puede ser escrito como:

$$c(D) = c_0 + c_1 D + c_2 D^2 + \dots + c_{n-1} D^{n-1}$$

Donde D es una variable real arbitraria. Si se impone la condición que $D^n=1$, entonces la multiplicación de $c(D)$ por D corresponderá a un desplazamiento (rotación) de los elementos de $c(D)$ a la derecha. Es fácil de mostrar que si se multiplica $c(D)$ por D i veces se tendría que:

$$D^i c(D) = c_{n-i} + c_{n-i+1} D + c_{n-i+2} D^2 + \dots + c_0 D^i + c_1 D^{i+1} + c_2 D^{i+2} + \dots + c_{n-1} D^{n-1}$$

1.5.3 Códigos Convolucionales

En un bloque codificado las palabras del código son generadas básicamente bloque por bloque. Sin embargo hay aplicaciones donde los bits del mensaje vienen en forma serial y no en bloques grandes, donde el uso de un buffer puede ser indeseable. En este tipo de situaciones donde el tiempo para realizar la decodificación es reducido se aplican los códigos convolucionales. Su nombre debe a que la codificación se entiende como la convolucion entre un vector de información con la respuesta al impulso del codificador.

Los bits de redundancia en cualquier instante son una función solamente del mensaje en ese instante. En la codificación convolucional el codificador es una máquina de estados finita que acepta los bits del mensaje de manera serial. Las palabras del código generadas en cierto instante de tiempo son una función de la entrada en ese instante y del estado de la máquina.

Un codificador convolucional (n, k, m) acepta k entradas seriales, produce n salidas, y tiene una máquina con 2^m estados. Por lo tanto, si una secuencia de la información de longitud kL es codificada convolucionalmente, la palabra del código correspondiente tiene una longitud $n(L+m)$ y la tasa del código esta dada por:

$$r = \frac{kL}{n(L+m)}$$

Esto se reduce a:

$$r = \frac{k}{n}, \text{ si } L \gg m$$

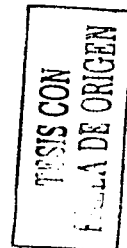
La longitud de restricción se define como el número máximo de las salidas del codificador que se pueden influenciar por un solo bit de información. Por lo tanto la longitud de restricción es dada por $n(m+1)$.



1.5.4 Características de los Principales Códigos

Códigos Hamming: Estos se han utilizado principalmente para la detección o la corrección de error en sistemas de las comunicaciones digitales y del almacenaje de datos

Parámetros	
Longitud del código	$n = 2^m - 1$
Numero de bits en el mensaje	$k = 2^m - m - 1$
Numero de bits de redundancia	$m = n - k \geq 3$
Distancia mínima	$d=3$
Capacidad para la corrección de error	$t=1$



1.5.4.1 Códigos de control de redundancia cíclica

Los códigos de control de redundancia (CRC) se utilizan principalmente para la detección de errores. El CRC puede detectar los patrones del error siguientes:

1. Despliegue de errores por longitud $\leq n-k$;
2. Despliegue de errores por longitud $= [1 - 2^{-(n-k)}] (n - k + 1)$
3. Despliegue de errores por longitud $\geq [1 - 2^{-(n-k)}] (n - k + 1)$
4. Numero de bits erróneo bits $\leq d-1$
5. Cualquier patrón del error, dado que el número de errores es impar y el polinomio generador del código presenta como número par coeficientes distintos a cero.

1.5.4.2 Código de Golay

Parámetros	
Longitud del código	$n=23$
Numero de bits en el mensaje	$k=12$
Numero de bits de redundancia	$m=11$
Distancia mínima	$d=7$
Capacidad para la corrección de error	$t=3$
	$g_1(D) = 1 + D^2 + D^4 + D^5 + D^6 + D^{10} + D^{11}$
	$g_2(D) = 1 + D + D^5 + D^6 + D^7 + D^9 + D^{11}$
	$1 + D^{23} = (1 + D)g_1(D)g_2(D)$

1.5.4.3 Códigos Bose, Chaudhuri, y Hocquenghem (BCH)

Los códigos BCH son una generalización de los códigos de Hamming para la corrección de errores múltiples

Parámetros	
Longitud del código	$n = 2^m - 1$
Numero de bits en el mensaje	$k \geq n - mt$
Numero de bits de redundancia	$m \geq 3$
Distancia mínima	$d \geq 2t + 1$
Capacidad para la corrección de error	$t < 2^{m-1}$

1.5.4.4 Códigos Reed-Salomon (RS)

Los códigos RS abarcan la subclase especial y más importante de los códigos de Q-arios BCH. El codificador para un código RS (n,k), código con m-bits símbolos agrupa la secuencia de datos binaria en bloque, cada bloque que contiene k símbolos de (km bits)

Parámetros	
Longitud del código	$n = q - 1 = 2^m - 1$
Numero de bits en el mensaje	K
Numero de bits de redundancia	$n - k = 2t$
Distancia mínima	$d = 2t + 1$

TESIS CON
FALLA DE ORIGEN

2. Redes de Paquetes por Radio

A pesar del éxito y la rápida expansión que han tenido las redes celulares en los últimos años, las redes móviles de paquetes por radio han logrado sobrevivir. Esto se debe a que dichas redes están diseñadas para conmutación de paquetes (asíncronas) en vez de la conmutación de circuitos como las redes celulares de voz (isócronas). Entonces los recursos son usados en forma más eficiente lo cual resulta en un menor costo y un mejor funcionamiento.

Las redes móviles de datos son más eficientes en cuanto a costo que las redes celulares sobre todo cuando se transmiten cantidades pequeñas de datos. Otra ventaja de las redes móviles de datos con respecto a las celulares es su capacidad de almacenar la información y poder transmitirla en forma diferida, a diferencia de los celulares, donde las terminales tienen que estar continuamente encendidas. En cambio en las redes móviles de datos los mensajes se almacenan sin importar donde se encuentre uno o con el móvil sin encender. No hay una necesidad de estar en contacto todo el tiempo.

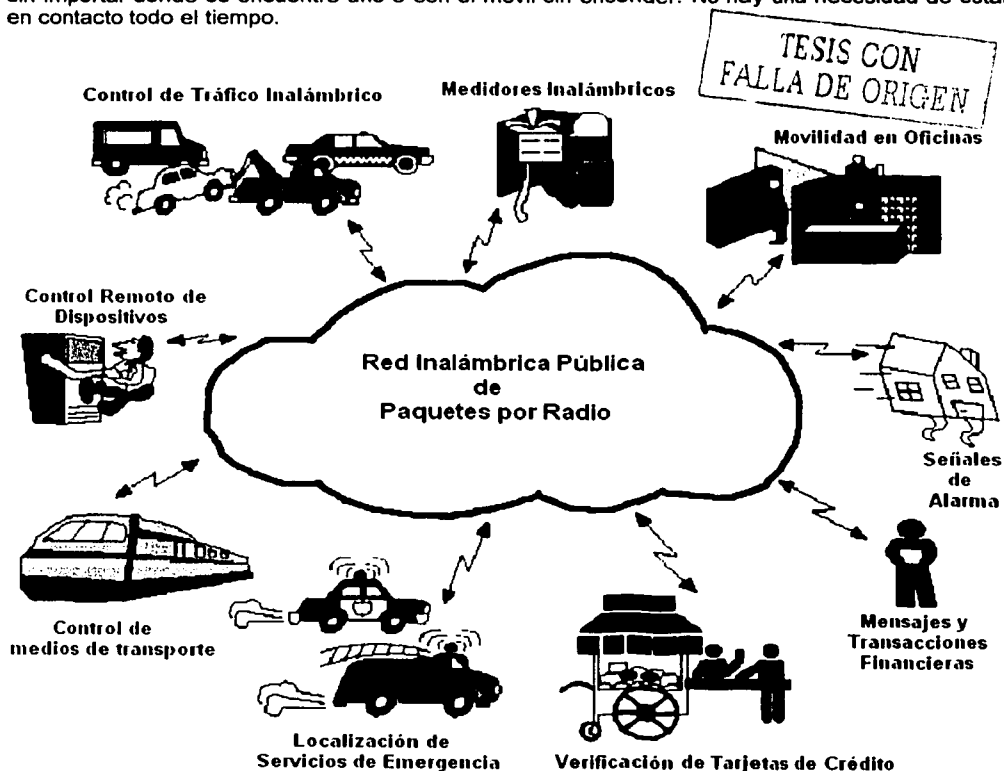


Figura 2.1 Principales aplicaciones de las redes móviles de datos.

Como se observa en la figura 2.1, las aplicaciones principales de estas redes móviles de datos son: envío de mensajes, recolección remota de datos, acceso remoto a base de datos, verificación de tarjetas de crédito, localización automática de vehículos, acceso a Internet y servicio de despacho computarizado. Otras aplicaciones posibles que no están tan desarrolladas todavía son: servicios de correos, de emergencia, de taxis o de camiones que necesiten un medio que les provea información en tiempo real acerca del estado de los vehículos y conductores, recorridos y cronogramas, y comunicación bidireccional entre conductores y despachantes.

En el mundo las redes móviles de datos más importantes son Mobitex, CDPD, GPRS y ARDIS. Las redes Mobitex y ARDIS son redes dedicadas a transmisión de datos. En cambio el CDPD utiliza las redes celulares analógicas existentes.

2.1. Mobitex

Mobitex es una tecnología que fue desarrollada por Telia, que es la PTT Sueca, como un sistema de comunicaciones privado de alarma para sus ingenieros de campo, pero luego evolucionó hacia un sistema de tipo público, habiéndose convertido en una norma mundial de facto. En Suecia la explotación comercial comenzó en 1986. Este tipo de sistema utiliza una estructura de tipo celular. En EEUU, RAM Mobile Data (RMD) opera sistemas Mobitex en 7700 ciudades y pueblos, cubriendo el 90 % de la población comercial y 11000 millas de autopistas interestatales, con roaming automático a lo largo de todas las áreas de servicio. RMD es una *joint business venture* de RAM Broadcasting Corporation y Bellsouth.

La tecnología Mobitex está instalada o se está instalando en 23 países incluyendo: Reino Unido, Francia, Suecia, Finlandia, Noruega, Bélgica, Holanda, Australia y Chile entre otros. Existe un Mobitex Operators Association (MOA) que se ocupa de revisar las especificaciones, coordinar el software y el hardware y hacer evolucionar la tecnología. Su trabajo estimula la aparición de fabricantes de terminales.

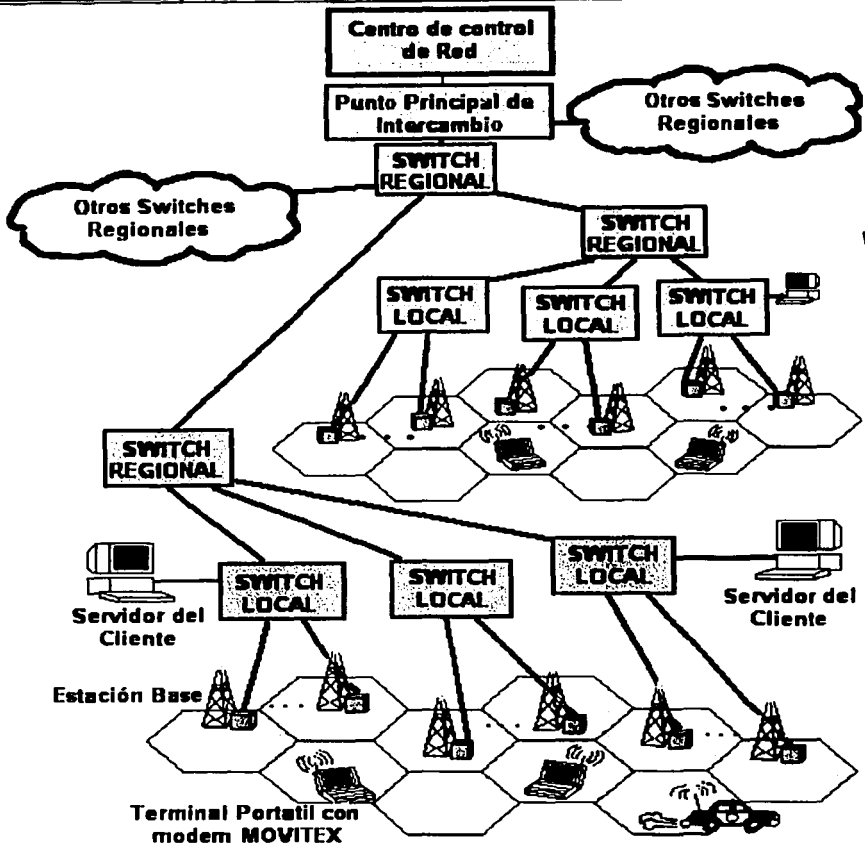
2.1.1 Descripción y Arquitectura del Sistema

El sistema MOBITEX como ya se mencionó emplea una distribución celular para proporcionar servicios de comunicación inalámbricos a un área geográfica específica. Está conformada de una estructura jerárquica que incluye seis niveles o seis nodos en la red, dependiendo del tamaño y área de cobertura.

Como se muestra en la figura 2.2, la infraestructura comprende tres tipos de nodos: las estaciones base, los switches locales y los switches regionales. La célula atendida por el mismo switch local forma un área de servicio o una subred. En cada área de servicio hay de 10 a 30 pares de frecuencias (llamados canales) los cuales están asignados al radio servicio. Todos estos canales tienen un ancho de banda de 12.5 [kHz] y soportan tasas de transferencia de datos de 8 [Kb/s].

En E.U.A. Mobitex usa la banda de 900 [MHz], para el downlink (base a móvil) emplea de 935 [MHz] a 940 [MHz] y para el uplink (móvil a base) emplea las frecuencias de 896 [MHz] a 901 [MHz]. En el resto del mundo, la mayoría de los sistemas están en la banda comprendida entre 410 [MHz] y 450 [MHz].

Las estaciones base están conectadas a los switches locales empleando las facilidades de la red telefónica local usando ya sea X.25 o HDLC. Similarmente, los switches locales están conectados a nodos de mayor nivel (switches regionales) empleando las facilidades que brinda la telefonía de larga distancia y usualmente emplea los mismos protocolos para realizar la conexión y transmisión de datos. En la cabeza de la estructura jerárquica es donde se lleva a cabo la interconexión con otras redes. Finalmente se encuentra otro elemento de la red, el Centro de Control de la Red (NCC), el cual se encarga de la administración de la red y también realiza las funciones de supervisión.



TESIS CON
 FALLA DE ORIGEN

Figura 2.2. Arquitectura del Sistema Mobitex

Una característica que vale la pena resaltar es que en las redes Mobitex, la conexión o el envío y recepción de un mensaje ocurre en el más bajo nivel posible (este no es el caso de otras redes), asegurando una respuesta rápida en tiempo y reduciendo el tráfico en la red. En otras palabras, la comunicación entre dos usuarios que se encuentre dentro de la misma célula involucra solamente la estación base de esta célula. Si los usuarios se mueven en diferentes células pertenecientes a la misma área de servicio, el envío y la recepción del mensaje ocurre en el switch local del área de servicio. Solamente en casos de movilidad, autenticación, y otros mensajes de señalización necesitan viajar más arriba de la estructura para mantener una mejor operación de la red. Además, si la conexión entre la estación base y su switch superior se llegara a perder, la estación base operaría en modo autónomo, manejando solamente la comunicación entre sus células. Otro rasgo importante de Mobitex es la posibilidad de enviar un paquete a un número de destinatarios. Para lograr eficiencia en el uso de los recursos, el remitente del mensaje no debe transmitir múltiples copias del mismo paquete, en vez de eso, solamente envía un paquete con la lista de los destinatarios deseados en el encabezado del mensaje.

2.1.2 Arquitectura del Protocolo

La arquitectura de Mobitex está asociada solamente con las tres primeras capas del modelo de referencia OSI. Además, los tres protocolos empleados por estas tres capas no están claramente mapeados con su correspondiente en el modelo OSI.

En lo que respecta a la estructura de la trama de la capa física, al principio se tiene el encabezado de la trama que es usado para establecer sincronización de las tramas y para identificar las estaciones de radio base. El campo de preámbulo incluye un patrón de sincronización que permite al receptor adquirir una sincronización de los bits y decodificar correctamente el resto de la trama. El preámbulo contiene ocho pares de unos y ceros. Cuando contiene la siguiente secuencia (1100110011001100) significa que la trama es transmitida de la estación base, y si tiene la siguiente forma (0011001100110011) es la estación móvil la que transmite la trama. En pocas palabras la capa física puede identificar si la trama viene de la estación base o de otra estación móvil.

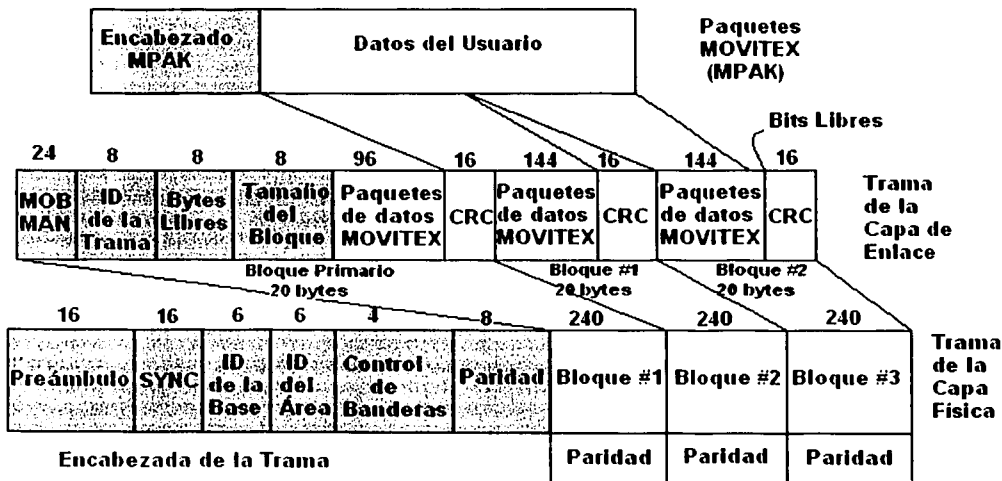


Figura 2.3. Estructura de una trama en Mobitex

El esquema de modulación empleado en Mobitex es GMSK (Gaussian Minimum Shift Keying) con un Índice de modulación de 0.5. Como se mencionó antes, el espaciado entre canales es de 12.5 [kHz] y la tasa de transmisión es de 8 [kb/s].

TESIS CON FALLA DE ORIGEN

2.2 CDPD (Cellular Digital Packet Data)

CDPD (Cellular Digital Packet Data) es un servicio de paquetes de datos para los sistemas AMPS/TDMA. CDPD es una red sobrepuesta que hace uso de la Infraestructura de las redes existentes.

Algunas características interesantes de CDPD son:

- CDPD usa la misma frecuencia y ancho de banda de canales AMPS/TDMA. Por lo tanto, la planeación celular, sitios y líneas de transmisión pueden ser compartidos con el sistema celular.
- CDPD es una especificación abierta y soporta roaming y operación similar a través de redes CDPD de otros operadores.
- CDPD provee un servicio seguro ya que incluye autenticación de los dispositivos móviles y encriptación automática de datos sobre la interfase aérea.
- CDPD optimiza el espectro ya que puede dar servicio a varios subscriptores mediante un solo canal de paquetes de datos compartido.
- Los sistemas CDPD se diseñan para aprovechar los canales desocupados de voz de la red celular analógica, tal como AMPS. Estos canales desocupados son usados para transmitir pequeños mensajes de datos y para establecer un servicio por conmutación de paquetes. Para utilizar estos canales desocupados CDPD aplica un procedimiento de saltos entre las frecuencias celulares disponibles.

2.2.1 Descripción y Arquitectura del Sistema

La naturaleza de las redes por paquetes de datos ofrece una óptima utilización de espectro ya que cientos de usuarios (hasta 800 dependiendo del tipo de tráfico) pueden estar activos, simultáneamente, en un solo canal. La tasa de transmisión de este canal es de 19.2 [Kb/s]. Una de las características del sistema CDPD es su escalabilidad. Esta escalabilidad del sistema hace posible configurar sistemas con un excelente costo-beneficio para diferente número de subscriptores en la red.

Algunas de las aplicaciones son: Acceso inalámbrico a bases de datos, E-mail, Telemetría, puntos de venta, cajeros automáticos, acceso a Internet/Intranet, transporte, localización de vehículos

La red CDPD incluye los siguientes elementos: MBDS (Mobile Data Base Station), MD-IS (Mobile Data Intermediate System), AS (Accounting Server), CAS (Customer Activation Server), Servidor de Autenticación, NMS (Network Management System).

Cada MBDS puede manejar de 1-3 canales de CDPD. Si esto no es suficiente, existe la posibilidad de incrementar la capacidad añadiendo otro MBDS a la estación base. En la configuración de red típica el MD-IS se instala en la Central y los MDBS en los sitios celulares junto con las estaciones base. Sin embargo, el máximo número de MDBS soportado por el MD-IS es mayor que la cantidad de estaciones base soportadas por la Central en una red AMPS o TDMA común.

La Interfase de aire provee el servicio a los usuarios móviles (M-ES). La capa física de esta interfase es el canal de RF provisto por el MBDS. El propósito de la red es permitir que los datos sean transmitidos hacia y recibidos desde equipos (sistemas finales) que son conectados a la red.

Una red de CDPD consiste de los siguientes elementos: Sistema Final Móvil (M-ES). Provee acceso a la red. La forma en que los subscriptores alcanzan acceso a la red es a través del M-ES. Este puede ser físicamente estacionario o móvil, pero siempre es considerado potencialmente móvil. La red CDPD asegura el direccionamiento de los datos gramas de una M-ES a otra M-ES continua, aún si su localización física cambia. La red CDPD encamina la localización de los M-ES y enruta los datos gramas del nivel de red apropiadamente. La movilidad implica que un M-ES pueda cambiar su punto de acceso a la subred según su conveniencia.

Los M-ES controlan los siguientes servicios de soporte y administración: Inicialización de transferencia de celdas, generación y cambio de claves para encriptación, transmisión full duplex o half duplex, Control de Acceso al Medio (MAC) para asegurar que las transmisiones M-ES no interfieran con las transmisiones de otras M-ESs u otros dispositivos que no sean CDPD, suministro de difusión de datos a otras M-ESs, encriptación de datos transferidos.

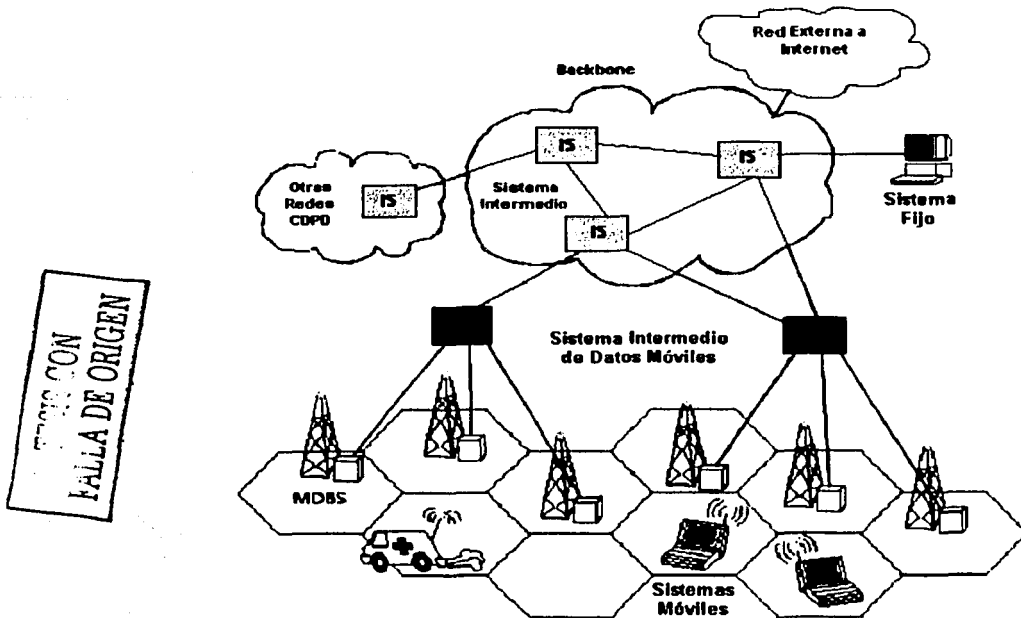


Figura 2.4. Arquitectura de una Red CDPD

Sistema Final Fijo (F-ES). Es un sistema conectado a la red de datos, típicamente es una plataforma-servidor (HOST). Las redes CDPD hacen una distinción entre sistemas finales móviles (M-ES) y Sistemas finales fijos (F-ES) con el propósito de administrar la movilidad. Estos sistemas pueden ser sistemas externos de datos tales como: bases de datos o aplicaciones internas de soporte y servicio. Los sistemas finales fijos externos son autónomos y operados fuera del control directo de la red CDPD. El uso primario de una red CDPD es para comunicación entre F-ES's y M-ES's y entre M-ES's y M-ES's.

La estación base de datos móviles (MDBS) intercambia datos entre sistemas finales móviles (M-ESs) y entre sistemas intermedios de datos móviles (MD-IS). Las MDBS manejan la comunicación a través del canal de radio y la Inter operación entre el uso de canales de voz (DMM) y la administración de recursos de radio (RRM). Al menos una MDBS es localizada en cada celda y recibe datos de una o varias M-ESs en un simple flujo de canal. Un flujo de canal es el medio que conecta los MDBS a un M-ES en un canal particular de RF. En sentido directo las transmisiones de las MDBS son recibidas por todas las M-ES's. En sentido inverso, las MDBS reciben las transmisiones de la M-ES.

El Sistema Intermedio de Datos Móviles (MD-IS) permite funciones de enrutamiento basadas en la localización actual de las M-ESs. Las MD-IS tiene la información y usan el protocolo MNLP para intercambiar información de localización de otras MD-IS.

Los sistemas intermedios (IS) implementan el nivel de red, definido en las especificaciones de CDPD. Las funciones de nivel de red son permitir que cualquier pareja de sistema final se pueda comunicarse con otro. El nivel de red encuentra un camino a través de una serie de ISs conectados hasta que el sistema final sea encontrado. Los ISs direccionan los data gramas de nivel de red al destino correcto. Los ISs deben tratar con: Cálculo de enrutamiento, fragmentación, reensamblaje, congestión.

Hay tres diferentes tipos de enlace que pueden ser configurados en una red de CDPD, como se muestra en la figura 2.5. El tipo de configuración depende de la función de los nodos o la terminación de la red a cada lado del enlace, estos enlaces son:

- Enlace A o Enlace Aéreo: conectan sistemas finales móviles MDBS.
- Enlace I o Proveedor de enlace: Conectan MD-IS a ISs y conecta proveedores de servicios de red entre ellos mismos.
- Enlace E o enlaces externos: conectan FESs a ISs.

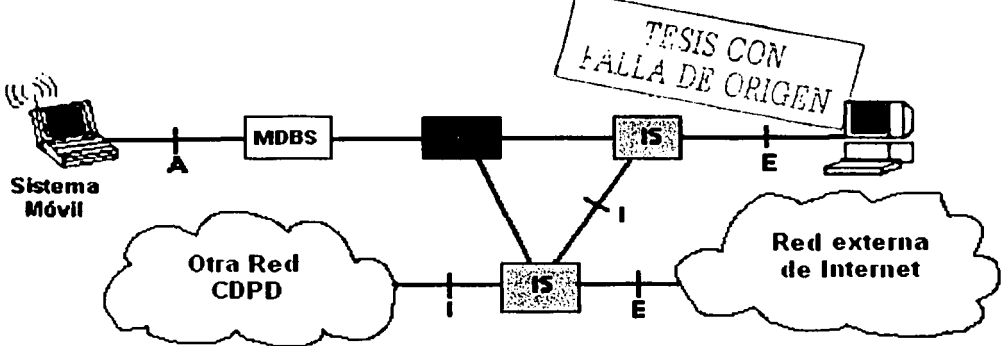


Figura 2.5. Interfaces estandarizadas con CDPD

2.2.2 Arquitectura del protocolo

La capa física de CDPD corresponde a una organización funcional la cual acepta una secuencia de bits de la capa MAC y los transforma en una forma de onda modulada para la transmisión en un canal de radio frecuencia de 30 kHz. Esto se ilustra en la figura anterior, la comunicación entre MDBS y M-ES toman un par de canales de radiofrecuencia (esta son frecuencia fijas separadas). El primer canal, llamado canal de envío (forward) pone en orden la dirección de MDBS a los M-ES's y estos son dedicados al uso de CDPS compartiendo la voz en la red celular. De cualquier manera la transmisión del canal de envío es continua si ésta es usada con CDPD. El segundo canal, llamado canal inverso o de regreso (reverse channel) pone en orden la dirección de transmisión de M-ES's al MDBS y es compartido entre todos los M-ES's con el mismo MDBS. A partir de los canales de envío e inverso (reverse), forman un canal de flujo CDPD.

La modulación empleada en un canal de radio frecuencia con CDPD es GMSK, con BTR = 50, una frecuencia mayor que la frecuencia central de la portadora representa un 1 lógico, mientras que un cero lógico se representará con una frecuencia menor a la frecuencia central de la portadora. La tasa de transmisión en ambos canales de radio frecuencia es de 19.2 [kb/s].

La arquitectura del protocolo de CDPD con interfase de aire esta ilustrada en la siguiente figura:

TESIS CON FALLA DE ORIGEN

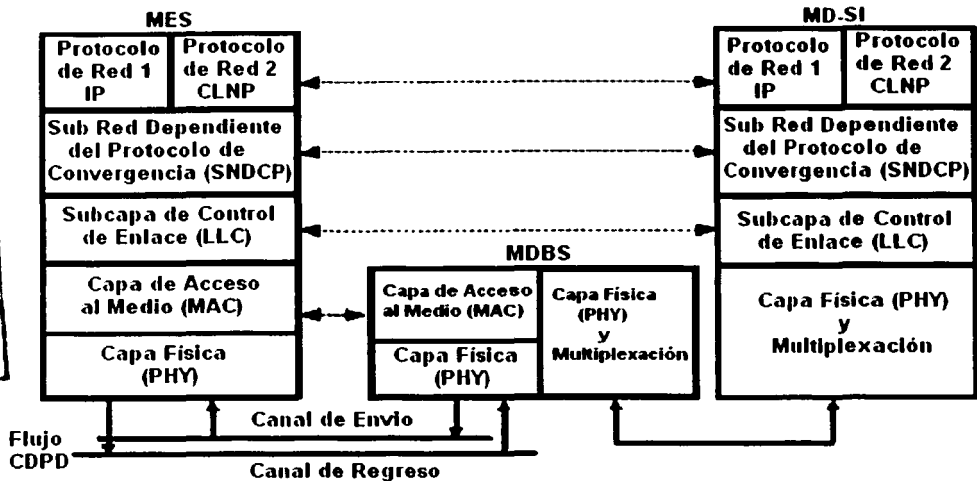


Figura 2.6. Arquitectura del protocolo CDPD.

2.2.3 Capa MAC del sistema CDPD

La capa MAC modela una organización funcional operando entre las capas físicas y el LLC. La capa MAC de un M-ES coopera con su correspondiente capa MAC dentro de un MDBS. El propósito de esta capa es transmitir información particularmente con las unidades de datos del protocolo de transferencia (LPDU's) entre entidades de igual LLC a través de la interface de aire de CDPD. Para este propósito, la capa MAC proporciona los siguientes servicios:

- Encapsula LPDU's en las estructuras de la trama para así asegurarse de delimitar el LPDU, la sincronización de la trama y transparencia de datos.
- Codifica LPDU's para protección de errores y deterioros dentro del canal móvil. Detecta y corrige errores de bits cuando recibe las tramas.
- Controla el acceso al canal compartido inverso (reverse).
- Se sincroniza con las transmisiones del canal de envío para hacer posible la recepción de datos así como también el control de la información transmitida a cada célula de CDPD.

El propósito de la capa LLC será transmitir información entre entidades de la capa de red a través de la interface de aire CDPD. El protocolo aplicado en esta capa es llamado Protocolo de Transmisión de Datos Móviles (Mobile Data Link Protocol MDLP).

Por lo tanto, se ve que la funcionalidad de un MDBS está restringida dentro de las capas físicas y de MAC. Sobre la capa MAC, un MDBS es totalmente transparente. El servicio primario ofrecido por el MDLP a la capa superior (SNDCP), es la disposición y el control de unas o más conexiones de transmisión de datos lógicas en una corriente del canal de CDPD. Sobre la capa del LLC, se tratan estas conexiones de transmisión de datos mientras que el MD-IS transporta frames individuales que se pueden utilizar para transportar mensajes hacia adelante y hacia atrás entre una o más M-ES's. Dentro de cada conexión de transmisión de datos, pueden haber uno o más flujos en la red que se acomodan a través de las instalaciones proporcionadas por el SNDCP. Las conexiones de transmisión de datos se lleva a cabo por medio de una etiqueta de dirección contenida en cada mensaje (trama). Esta etiqueta de dirección se llama el identificador temporal del equipo (TEI) y es un concepto puro de la capa LLC, es decir, es utilizada internamente por la CRCG-SVG

capa LLC y no es necesario que otras capas lo conozcan. El protocolo de convergencia dependiente de la subred (SNDPCP) deja de operar entre la capa de transmisión de datos y la capa de red. Específicamente, el SNDPCP realiza las siguientes funciones: segmentación, encriptado, multiplexación, compresión del encabezado, compresión de datos y calidad de servicio.

2.3 GPRS (General Packet Radio Service)

La primera especificación de GPRS (General Packet Radio Service) fue publicada a finales de 1997 después de que la ETSI comenzara este trabajo en 1994. El principal objetivo de GPRS es proveer a usuarios con interfaces móviles por paquetes de datos conectividad con otras redes de datos. Esta interfaz es normalmente parte de una red GSM, la cual fue originalmente diseñada para ofrecer servicios por conmutación de paquetes. Un aspecto importante que se puede mencionar acerca de GPRS, es que dicha tecnología es totalmente compatible con la arquitectura de una red GSM. Su introducción es un paso importante en la evolución de las redes actuales GSM hacia tercera generación. GPRS puede considerarse junto con CDPD y las redes AMPS como redes de datos que comparten la infraestructura de acceso en GSM. La conmutación de circuitos y los servicios de GPRS tienen que coexistir en el mismo ambiente de red sin cambios significativos en el sistema.

La tasa de transmisión de GPRS es suficiente para soportar aplicaciones como: navegar en la Web, compresión de video y utilizar el protocolo de transferencia de archivos FTP (File Transfer Protocol). La introducción de GPRS hace posible: servicios basados en conmutación de circuitos y de paquetes en una red de telefonía móvil, tiempos de registro/acceso breves, eficientar los recursos que se tienen cuando se transmite vía radio, conectividad a redes externas de datos por conmutación de paquetes que se basan en IP o X.25.

2.3.1 Descripción y Arquitectura del Sistema

Los servicios de GPRS se clasifican en dos grupo: principales:

- Servicios Punto a Punto PTP (Point-To-Point), que a su vez se dividen en cualquiera de las dos siguientes conexiones orientadas:
 - a. Servicio de Red Orientado a la Conexión Punto a Punto: PTP-CONS(Connexion Oriented Network Service), la conexión con una red IP es un ejemplo.
 - b. Servicio de Red Orientado a la Conectividad Punto-Punto PTP-CLNS (Connexionless Oriented Network Service), como ejemplo la conexión con redes de paquetes PDN(Packet Data Network) como X.25.

Los servicios PTP se aprovechan en la primera fase de GPRS

- Servicio Punto-Multipunto PTM(Point-To-Multipoint), incluye dos tipos de servicio:
 - a. Servicios Multicast (PTM-M, Point-To-Multipoint Multicast).
 - b. Servicios de Grupo (PTM-G, Point-To-Multipoint Group).

Los servicios PTM se aprovecharan como un segundo peldaño en GPRS.

Las terminales GPRS son capaces de soportar varios protocolos de red. Una Estación Móvil GPRS (MS Movil Station) puede operar en alguno de los siguientes tres modos:

- Clase A: La Estación Móvil (MS) que puede usar los dos servicios GPRS y GSM y puede además soportar sus servicios simultáneamente.
- Clase B: La Estación Móvil (MS) que puede utilizar los dos servicios, GPRS y GSM pero solo puede operar con un tipo de servicio a la vez entre GPRS o GSM.
- Clase C: La Estación Móvil que tiene acceso solo a los servicios GPRS.

Un requisito clave para estos nuevos nodos consiste en que se puedan ampliar, de manera que los operadores empiecen a ofrecer servicios de datos por paquetes a alta velocidad empleando nodos pequeños en áreas seleccionadas que sean rentables y añadir después más capacidad extra según sea necesario.

2.3.2 Arquitectura del Protocolo

A la cabeza de de la capa del protocolo pueden haber varios protocolos de red, GPRS soporta los protocolos X.25 e IP, para ser usados para aplicaciones punto a punto. Los paquetes de información son enviados a través de la de la PLMN – GPRS el cual utiliza protocolos dedicados.

Una de las características es que, sin importar los paquetes transportados se usa IP como protocolo de capa de red para el backbone GPRS. El protocolo de túnel GPRS (GTP) habilita la creación de túneles para paquetes de datos multiprotocolo a través del backbone GPRS entre nodos de soporte.

El GTP utiliza el protocolo TCP (Transmission Control Protocol) o UDP (User Datagram Protocol) dependiendo de cuando se necesite una conexión confiable (paquetes de datos X.25) y cuando no (paquetes IP).

El protocolo de convergencia dependiente de la subred (SNDCP – Subnetwork Dependent Convergence Protocol) al igual que en CDPD tiene la función de transformar unidades de datos del protocolo de capa de red de forma transparente. La introducción de nuevos protocolos de la capa de red no requiere del cambio de todas las capas de protocolos GPRS: Solo es necesario hacer cambios al SNDCP. También el SNDCP tiene la posibilidad de comprimir datos (V.42 Bis) y la compresión de encabezado (compresión de encabezado TCP-IP) para mejorar la eficiencia del canal.

El protocolo del control del enlace lógico (LLC) opera a lo largo de las interfaces Um y Gb, creando un enlace lógico entre MS y su SGSN. Las funciones del LLC comprenden encriptación, control de flujo y control de secuencia. Por lo tanto, si el protocolo LLC se usa en modo confirmado (acknowledged), provee detección y corrección de errores al transmitir; cuando el LLC se encuentra en modo no confirmado (unacknowledged), indica cuales son los errores que no se pueden corregir. El protocolo LLC es usado por el SNDCP para la transmisión de paquetes y unidades de datos en la capa de red (PDUs), por el protocolo SMS para transmitir mensajes SMS, y por la administración de movilidad de GPRS para transferir datos de control.

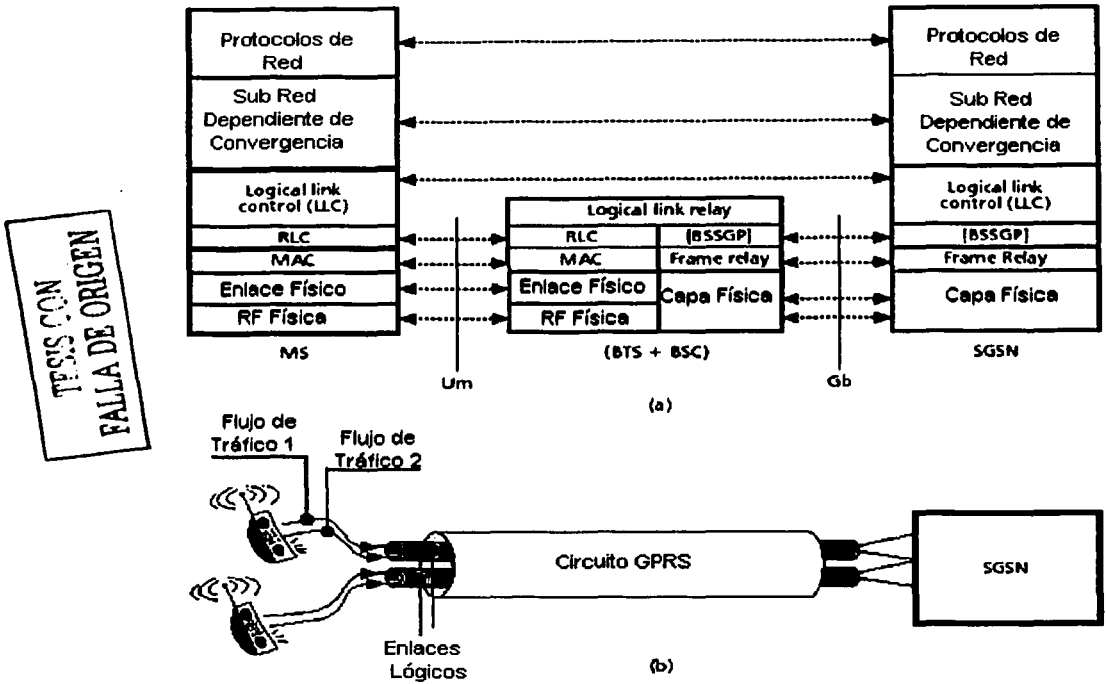
El protocolo de Control del Enlace de Radio/Control de Acceso al Medio (RLC/MAC) da servicios para la transferencia de PDUs del LLC utilizando un medio compartido entre la red y múltiples MSs. Las funciones del protocolo RLC son segmentación y reensamble de PDUs del LLC. Se puede configurar para que opere en modo confiado y no confiado, dependiendo de la calidad de servicio (QoS) que se requiera. El modo confiado, se efectúa la detección de PDUs del LLS erróneos basada en "checksum" y la retransmisión de los PDUs erróneos.

El protocolo MAC ubica los diferentes canales lógicos necesarios para compartir el medio de transmisión común por las distintas MSs. Permite a una MS utilizar distintos canales físicos pero también el multiplexado de distintas MSs sobre un canal físico como se muestra en la figura anterior (b).

La capa de enlace físico facilita un número de canales físicos a la capa RLC/MAC. Algunas de sus funciones son: procedimientos para el control de la potencia, monitoreo de la calidad de la señal del enlace de radio, entrelazado (interleaving) y la corrección de los errores enviados.

La capa inferior en la interface Um, es decir, la capa física de radiofrecuencia, es la encargada de la transmisión y recepción en la frecuencia portadora, la cual coincide con la capa de radiofrecuencia de GSM.

El servicio de GPRS se basa en el siguiente protocolo de arquitectura de red mostrada en la siguiente figura:



TESIS CON FALLA DE ORIGEN

Figura 2.9. (a) Arquitectura del protocolo de GPRS; (b) presentación esquemática del tráfico y del acoplamiento lógico que multiplexan en GPRS.

En el caso donde un móvil origina tráfico para un usuario fijo, el SGSN encapsula los paquetes de datos y los enruta al GGSN apropiado, en donde son enviados a la correcta Red de Datos por Conmutación de Paquetes PSDN(Packet Switched Data Network). Las normas específicas de enrutamiento se aplican dentro del PSDN para mandar los paquetes al usuario correspondiente. Por otro lado los paquetes que vienen, de un usuario fijo son primero dirigidos al GGSN por el PSDN, basado en la revisión de la dirección destino. El GGSN revisa el contexto del enrutamiento asociado con esta dirección destino y determina la dirección de la SGSN que sirve como enrutador hacia el MS. Subsiguiente, el paquete original de datos es encapsulado dentro de otro paquete(esteste proceso es llamado tunneling), el cual es enviado al SGSN y por último entregado a la correspondiente MS. La red backbone GPRS es una red privada IP. El direccionamiento IP usado en este backbone es seleccionado por el operador del sistema GPRS y por eso no es sabido fuera del PLMN, como se ilustró en la figura anterior.

Dentro de GPRS, existen dos diferentes esquemas de encapsulado que se usan. El primero, entre el SGSN todos los paquetes son encapsulados por medio de un protocolo de tunneling de GPRS(GTP) para habilitar el uso de diferentes protocolos de paquetes de datos, aunque estos

protocolos no los soportan todos los SGNs. El segundo, encapsulación entre la MS y la SGNs es realizado al separar la administración lógica de la conexión de los protocolos de la capa de red.

2.4 ARDIS (Avancer Radio Data Information)

Es un servicio de radio de dos vías que se basa en la tecnología RD-LAP Motorola. ARDIS es el precursor de las redes móviles de transmisión de los Estados Unidos. Ofrece un servicio bidireccional de datos. La red ARDIS se localiza en los 800 MHz de la banda de frecuencia, la técnica de acceso utilizada es FDMA y utiliza la modulación GFSK. Los canales tienen una separación de 25 [kHz] y el espacio entre los canales bidireccionales es de 45 [MHz]. ARDIS se basa en dos protocolos de interfaz de aire para su red: los MDC-4800 que proporciona servicios de 4.8 [kb/s], este protocolo está implementado en toda la red ARDIS y RD-LAP que proporciona un servicio de 19.2 [kb/s], con una tasa de transmisión útil de 8 [kb/s] y solamente algunas áreas de servicio importante han sido abarcadas con este protocolo RD-LAP.

2.4.1 Descripción y Arquitectura del Sistema

La red de ARDIS está conectada a reguladores de radio vía líneas de enlaces dedicados. ARDIS tiene cerca de 1400 estaciones base ocupando cerca de 1100 células. Los usuarios accesan al sistema con una lap top que contenga una tarjeta con terminal de radio el cual lo comunica con las estaciones base. Cada una de las estaciones base de ARDIS se comunica con uno de los radio controladores de red como se muestra en la figura 2.10.

Un radio controlador de red es una computadora especializada también llamada procesador de control de la radio frecuencia de red RF/NCP (Radio Frequency / Network Control Processor). El RF/NCP maneja los recursos de radio frecuencia incluyendo las estaciones base de radio y los datos que se envían sobre los canales de radio. Se manejan los canales de entrada y de salida usando diversas estrategias de entrega. El RF/NCP evalúa la intensidad de la señal recibida de cada dispositivo de transmisión inalámbrico en cada estación base para cada paquete de datos entrante que él detecte ("hear"). Después selecciona la mejor estación base para comunicarse con algún dispositivo inalámbrico en particular y enviará un mensaje de salida a través de esa estación base. Este proceso asegura la selección óptima de un sitio, aunque los dispositivos del suscriptor pueden moverse o estar sujetos a la presencia de ruido. El RF/NCP es un componente de la red que ayuda a manejar la capacidad del Roaming automático en la red de ARDIS. Los dispositivos inalámbricos pueden moverse automáticamente (Roaming) entre cual quiera de las frecuencias de ARDIS o en los dos protocolos (MDC-4800 o RD-LAP 19.2), o entre cualquiera de las capas de ARDIS que se han configurado para utilizarse dentro o fuera de cualquier sitio. Además, a través de las transmisiones periódicas de los "mensajes del canal de señalización" cada dispositivo inalámbrico se asegura del tener el servicio más eficiente disponible en esa área. Cada RF/NCP es conectado a una línea digital de la alta velocidad con un message switch (MS). El RF/NCP pasa la información referente a la fuente, la longitud y el destino de cada mensaje al MS, que permite a ARDIS realizar el análisis de red de la densidad del tráfico en cada sitio. El MS pasa la información al RF/NCP en relación si el dispositivo del suscriptor esta registrado a la red y si tiene derecho para acceder a los servicios de la red. Cada MS es una computadora de uso general que es el dispositivo principal de la red de ARDIS. El MS enruta los mensajes al destino apropiado, almacena la información del registro del suscriptor y realiza funciones de contabilización y de facturación. También sirve como un punto de acceso para los ordenadores centrales de los clientes, realiza la conversión de protocolo, maneja la determinación del problema y proporciona una función de monitoreo y de prueba para el sistema de administración de la red.

TESIS CON FALLA DE ORIGEN

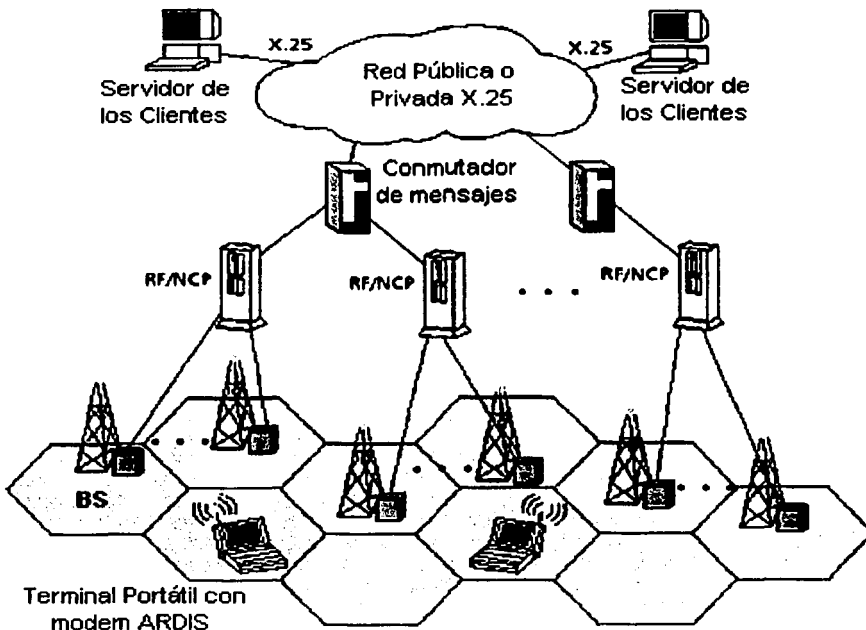


Figura 2.10. Arquitectura de la red de Ardis.

Para conectar la computadora de un cliente y un MS se usa los circuitos dedicados de X.25. La banda de frecuencia de funcionamiento es 800 [MHz] y la conexión de radiofrecuencia utiliza frecuencias que están separadas entre ellas 45 [MHz], que son utilizadas simultáneamente para formar un canal full-duplex. ARDIS se implementó inicialmente con una tasa de transmisión de 4800 bps con canales de 25 [kHz], pero esta tasa se ha aumentado a 19.2 Kbps en algunas áreas de servicio. La potencia de la estación base es aproximadamente de 40 [W], que proporciona cobertura desde 15 hasta 25 [km]. Por otra parte las terminales de radio funcionan con una potencia de 4 [W]. El área de cobertura de las estaciones bases se traslapan para aumentar la probabilidad de que la señal de una estación base alcance por lo menos una estación base. La cobertura traslapada, combinada con los niveles de potencia diseñados y la codificación error-corrección en el formato de la transmisión, asegura que ARDIS puede apoyar comunicaciones portátiles dentro y fuera de los edificios. Esta capacidad para la cobertura dentro de las construcciones es una característica importante del servicio de ARDIS. Dentro de cada célula, las terminales de radio de ARDIS tienen acceso a la red usando un método de acceso aleatorio llamado el acceso múltiple del sentido de los datos (DSMA – Data Sense Múltiple Access). Antes de cada transmisión, una terminal de radio detecta el transmisor de la estación base para determinar si un "busy bit" o "bit de ocupado" está apagado o encendido. Este bit indica si la estación base está recibiendo actualmente datos (es decir que el "busy bit" está encendido) o no (el "busy bit" está apagado). Cuando este bit está encendido, las terminales de radio no pueden transmitir y en este estado se evitan las colisiones. Por otra parte, cuando el bit de ocupado está apagado, la terminal de radio permite transmitir. Sin embargo, si dos terminales comienzan la transmisión al mismo tiempo, los paquetes colisionan por lo que se procura retransmitir utilizando otro protocolo de conexión.

2.4.2 Arquitectura del Protocolo

Los protocolos propietarios de intercambio de datos son usados para transportar datos a diferentes puntos de la interface. En el servidor del cliente (o Host), el protocolo estándar del enrutamiento del contexto (SCR) se utiliza para transportar datos entre este servidor y el MS los mensajes para la transmisión están separados en paquetes, cada con un encabezado, conteniendo como información de ruteo, el tamaño del frame.

Los mensajes del Host pueden ser uno de los siguientes tres tipos:

- Host Message Delivery Request (HR), usada por el Host para enviar mensajes a las terminales móviles.
- Host Message Delivery Request (HC), usada por el MS para confirmar que se recibió el mensaje.
- Mobile Device Message Delivery Indication (MI), utilizado por el móvil para reconocer el mensaje recibido.

Además, los tipos de mensaje extendidos del SCR se utilizan para supervisar la actividad del móvil, realizar diagnósticos del loopback, y supervisar el estado en que se encuentra.

En el extremo final de la terminal móvil, el protocolo Native Control Language (NCL) es usado como protocolo de capa de acoplamiento entre la aplicación que efectúe el cliente en su terminal móvil y el módem de radio. El protocolo de NCL proporciona un servicio orientado a transacciones particularmente conveniente para los usos sin conexión. La información se intercambia entre la terminal móvil y el módem de radio en paquetes llamados unidades de datos de servicios (SDUs – Service Data Units).

NCL provee tres tipos de SDUs:

- SDUs, que publican las instrucciones como por ejemplo "envía" y "recibe" los mensajes.
- Respuesta del estado SDUs, que son respuestas a los comandos.
- Informe de acontecimiento de SDUs, que puede ser permitido o ser inhabilitado.

Adicionalmente a los mensajes de ruteo usando los protocolos SCR y NCL, la red de ARDIS provee data TAC messaging DM conocida como ruteo punto a punto.

Con la ayuda de este protocolo, los mensajes se pueden enviar a partir de una terminal móvil a otra y así, se establece un servicio de mensajería de dos vías. Para este servicio, un anfitrión intermedio del DM se utiliza dentro de la infraestructura de ARDIS.

Entre un módem de radio y una estación base, (RD-LAP o MDC-4800) el protocolo proporciona una capa de acoplamiento y una cierta funcionalidad de la capa de red. La longitud máxima de transmisión que soporta es de 512 bytes para RD-LAP y 256 bytes para el MDC-4800. La técnica de modulación en la capa física es GFSK.

2.5 Características principales de Redes Inalámbricas de Paquetes por Radio.

En la siguiente tabla podemos observar algunas de las características principales de redes inalámbricas de paquetes por radio, en las cuales podemos confiar dependiendo de las necesidades que se tengan como consumidor, pues cada una tiene sus especificaciones técnicas como se muestra a continuación. Cabe mencionar que en este caso la banda de frecuencia utilizada es ICM.

	MOBITEX	CDPD	GPRS	ARDIS
Nº de Canales	10 - 30	1-3 p/c MDBS	20 - 40	
Tipo de Modulación	GMSK	GMSK	GMSK	GFSK
Tipo de Interfase	Aire	Aire	Aire	Aire
Tipo de Red	X.25 o HDLC	IP y X.25	IP y X.25	X.25
Banda de Frecuencia	80 - 400 - 800 y en América 900 [MHz]	900 [MHz]	900 [MHz]	800 [MHz]
Velocidad de Transmisión	8 [kb/s]	19.2 [kb/s]	160 [kb/s]	19.2 [kb/s]
Separación entre Canales	12.5 [kHz]	30 [kHz]	200 [kHz]	25 - 45 [kHz]
Técnica de Acceso Múltiple	FDMA	TDMA	TDMA/FDMA	FDMA

TESIS COY
FALLA DE ORIGEN

3. Redes de Área Local Inalámbricas WLANs

En los últimos años las redes inalámbricas (WLAN, Wireless Local Area Network) han ganado muchos adeptos y popularidad en mercados como hospitales, fabricas, bodegas, tiendas de autoservicio, tiendas departamentales, pequeños negocios y áreas académicas. Las redes inalámbricas permiten a los usuarios acceder información y recursos en tiempo real sin necesidad de estar físicamente en un sólo lugar. Con una WLAN la red por sí misma es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red y lo más importante incrementa la productividad y eficiencia en las actividades diarias de la empresa. Un usuario dentro de una red inalámbrica puede transmitir y recibir voz, datos y video dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas.

Muchos de los fabricantes de computadoras y equipos de comunicaciones como PDAs (Personal Digital Assistants), módems, microprocesadores inalámbricos, lectores de punto de venta y otros dispositivos están introduciendo aplicaciones en soporte a las comunicaciones inalámbricas. Las nuevas posibilidades que ofrecen las WLANs son permitir una fácil incorporación de nuevos usuarios a la red, ofrecen una alternativa de bajo costo a los sistemas cableados, además de la posibilidad ubicua para acceder cualquier base de datos o cualquier aplicación localizada dentro de la red. A continuación se resumen algunas de estas ventajas de las WLANs, concernientes a productividad, conveniencia y costo, en comparación con las redes inalámbricas:

- **Movilidad:** Las redes inalámbricas pueden proveer a los usuarios de una LAN acceso a la información en tiempo real en cualquier lugar dentro de un entorno. Esta movilidad incluye oportunidades de productividad y servicio que no es posible con una red alámbrica.
- **Simplicidad y rapidez en la instalación:** La instalación de una red inalámbrica puede ser tan rápida y fácil, además que puede eliminar el uso de cableado.
- **Flexibilidad en la instalación:** La tecnología inalámbrica permite a la red ir donde la alámbrica no puede ir.
- **Costo de propiedad reducido:** Mientras que la inversión inicial requerida para una red inalámbrica puede ser más alta que el costo en *hardware* de una LAN alámbrica, la inversión de toda la instalación y el costo del ciclo de vida puede ser significativamente inferior. Los beneficios y costos a largo plazo son superiores en ambientes dinámicos que requieren acciones y movimientos frecuentes.
- **Escalabilidad:** Los sistemas de WLANs pueden ser configurados en una variedad de topologías para satisfacer las necesidades de las instalaciones y aplicaciones específicas. Las configuraciones son muy fáciles de cambiar y además es muy fácil la incorporación de nuevos usuarios a la red.

Los fabricantes de WLANs migraron de la banda de 900 MHz a la banda de 2.4 GHz para mejorar la velocidad de información. Este patrón continua al abrirse el estándar IEEE 802.11a en la banda de 5 GHz operando con una velocidad de datos de hasta 54 Mbps. Esta banda de 5 GHz promete otras mejoras en velocidad permitiendo quizá algún día romper la barrera de los 100 Mbps.

Con relación al costo los equipos de WLANs han abierto nuevos mercados. Para esta tecnología, la demanda continua incrementándose, la reducción del costo en la ingeniería y eficiencia en la fabricación permitirán la reducción mas de los costos, hasta que llegue un día en que un adaptador de un cliente inalámbrico cueste lo mismo que un adaptador alámbrico.

Las redes WLANs que analizaremos en este capítulo serán las redes HiperLAN2 y 802.11 ya que ambas sean comercializado y han tenido un gran auge en el mercado de las redes LAN inalámbricas, además de que organizaciones con gran prestigio a nivel mundial son las encargadas de definir el estándar con que dichas tecnologías operan.

3.1 HiperLAN2

Se han dedicado muchos esfuerzos de investigación y normalización para concebir tecnologías apropiadas de transmisión y de redes. La Fuerza de Tareas de Ingeniería de Internet (IETF), la Unión Internacional de Telecomunicaciones (ITU) y el Foro ATM están definiendo el núcleo de la red fija. Del mismo modo está trabajando el proyecto de Redes de Acceso de Radio de Banda Ancha (BRAN) del Instituto Europeo de Normas de Telecomunicaciones (ETSI) en normas para distintos tipos de redes inalámbricas de acceso de banda ancha. Una de estas normas, que se denomina *red de radio de área local de altas prestaciones, tipo 2* (HiperLAN2) da acceso de comunicaciones de alta velocidad a distintos núcleos de la red de banda ancha y terminales en movimiento (portátiles al igual que móviles).

Antes de empezar con el trabajo de normalización sobre HiperLAN2, la ETSI desarrolló la norma HiperLAN1 para la conexión en red *ad hoc* de dispositivos portátiles. Esta norma apoya principalmente la transferencia de datos asíncrona y aplica un mecanismo de acceso múltiple – de la familia de acceso múltiple que detecta al portador (CSMA) – con la prevención de llamadas confluyentes (CA). Usando la técnica CSMA / CA para resolver emulación, comparte el modelo la capacidad de radio disponible entre usuarios activos que tratan de transmitir datos durante un periodo de tiempo superpuesto. A pesar de que HiperLAN1 da un medio de transportar servicios limitados en tiempo, no controla o garantiza la calidad de servicio QoS en el enlace inalámbrico. Por lo que se considera como un sistema de entrega de datos, *best effort*. Esto es lo que ha motivado a ETSI a desarrollar una nueva generación de normas que apoyan datos asíncronos y servicios críticos en lo que se refiere a tiempo (por ejemplo, voz y video empaquetados) que están limitados por retardos de tiempo específicos.

3.1.1 Arquitectura de la Red

HiperLAN2 depende de una topología de red celular en combinación con una capacidad de red *ad hoc*. Apoya dos modos de operación básicos: modo centralizado (CM) y modo directo (DM).

El modo de operación centralizado se aplica a la topología de red celular donde cada celda de radio es controlada por un punto de acceso (AP) que cubre una cierta área geográfica. En este modo se comunican los terminales móviles entre sí o con el núcleo de la red por medio del punto de acceso. El modo de operación centralizado es usado principalmente en aplicaciones comerciales de interior y de exterior donde el área que se ha de cubrir es más grande que una celda de radio.

El modo de operación directo se aplica a la topología de red *ad hoc* de ambientes de hogar privados y donde toda el área que sirve se cubre por una celda de radio. Las terminales móviles en una red de residente de celda única pueden intercambiar datos directamente entre sí en este modo. El punto de acceso controla la asignación de recursos de radio a las terminales móviles.

La movilidad al aire libre de HiperLAN2 es limitada, al comparar con otros sistemas celulares. Los ambientes de aplicación típicos son oficinas, hogares, salas de exposiciones, aeropuertos, estaciones de tren, etc. Por lo tanto es fácil describir la arquitectura de la red, ya que solo es necesario un Access Point (AP) y dispositivos móviles con tarjetas que sean compatibles con HiperLAN2 o solamente los dispositivos si se requiere una topología de red descentralizada (Figura 3.1).

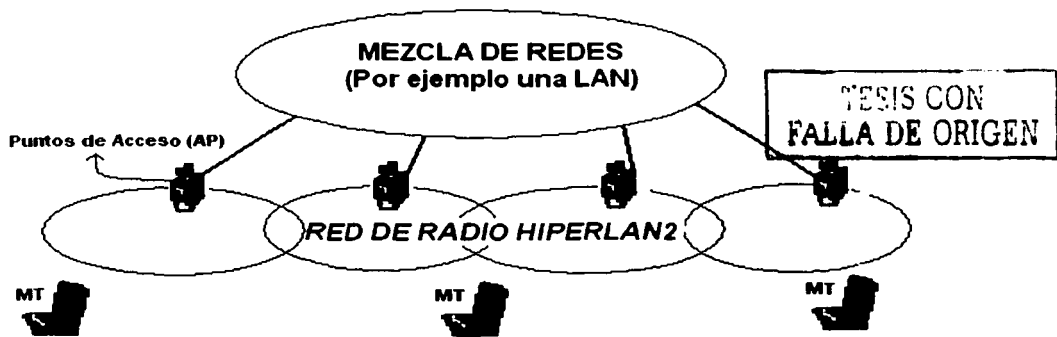


Figura 3.1 Red típica de HiperLAN2

La norma HIPERLAN/2 apoya la movilidad de terminales a velocidades de hasta 10 [m/s]. Además da un medio de manejar distintos ambientes de interferencia y propagación, con objetivo de:

- mantener el enlace de comunicaciones a bajas proporciones de señal a interferencia;
- mantener la calidad de servicio; y
- encontrar una reciprocidad apropiada entre extensión de comunicaciones y tasa de datos.

El interfaz de aire de la norma HIPERLAN2 está basado en una comunicación duplex con división en el tiempo (TDD) y acceso dinámico de multiplexación por división en el tiempo (TDMA). HIPERLAN2 es una plataforma flexible en la que se pueden basar una variedad de aplicaciones comerciales y de multimedia con velocidades de transmisión de hasta 54 [Mb/s].

3.1.2 Arquitectura del Protocolo de HiperLAN2

La norma HIPERLAN2 especifica una red acceso de radio que se puede usar con una variedad de núcleos de la red. Esto se hace posible gracias a:

- una arquitectura flexible que define las capas físicas independientes de núcleo de la red (PHY) y de control de enlace de datos (DLC); y
- un juego de capas de convergencia que facilitan el acceso a distintos núcleos de la red (Figura 3.2).

Varias capas de convergencia han sido o están siendo definidas actualmente para interoperar con:

- redes de transporte de protocolo Internet (IP) (Ethernet y el protocolo de punto a punto, PPP);
- redes basadas en modo asíncrono de transferencia (ATM);
- núcleos de la red de tercera generación; y
- redes que usan protocolos y aplicaciones IEEE 1394 (Firewire).

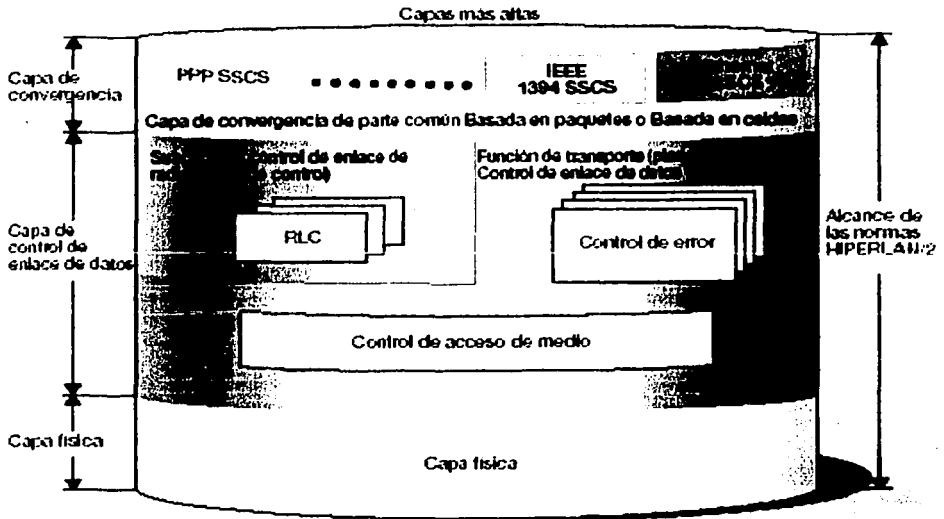


Figura 3.2 Arquitectura de los protocolos de HiperLAN2

Las unidades de datos que se transmiten dentro de estos núcleos de la red pueden diferenciarse en longitud, tipo, y contenido. Una capa de convergencia específica en HiperLAN2 segmenta unidades de datos a unidades de datos de servicio de usuario (U-SDU) de longitud fija HiperLAN2 DLC que se transmiten a su destino por medio de servicios de transporte de datos DLC y PHY.

3.1.2.1 Capa de Convergencia

La capa de convergencia (CL) tiene dos funciones principales: adapta solicitudes de servicio de capas más altas al servicio ofrecidas por el DLC, y convierte paquetes de capa más alta de longitud fija o variable a una unidad de datos de servicio de longitud fija (SDU) que se usa dentro del DLC.

La capa de convergencia traduce así los datos de entrada a distintos portadores del DLC. Por ejemplo, si suponemos que la calidad de servicio Ethernet es apoyada por medio de IEEE 802.1p, entonces la prioridad indicada en el campo de identificación adicional estipula el tipo de tráfico que se debe llevar en el paquete. La capa de convergencia traduce distintos tipos de tráfico a distintas clases y por consiguiente a distintos portadores de radio.

Hay dos tipos de capa de convergencia una capa de convergencia basada en celda, que maneja capas más altas con paquetes de longitud fija por ejemplo: núcleos de la red basados en ATM; y una capa de convergencia basada en paquetes, que maneja capas más altas con paquetes de longitud variable por ejemplo, Ethernet. Se han definido subcapas de convergencia separadas específicas a servicio (SSCS) para hacer la adaptación de servicio apropiada para Ethernet, IEEE 1394, PPP, y el sistema universal de telecomunicaciones móviles (UMTS). La Figura 3.3 describe la estructura básica de cada tipo de capa de convergencia.

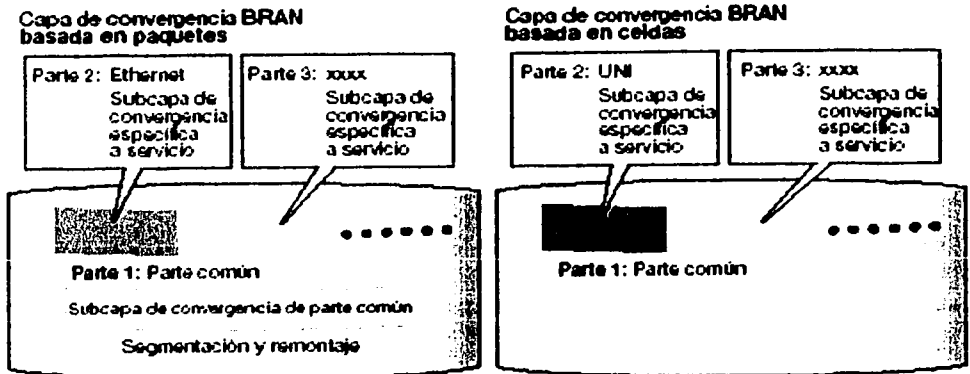


Figura 3.3. Estructura general de la capa de convergencia.

La función de relleno, segmentación y remontaje de las unidades de datos de servicio DLC de longitud fija es una característica clave que hace posible normalizar e implementar las capas DLC y PHY independientemente del núcleo de la red. La Figura 3.4. describe la traducción de unidades de datos de capa más alta hasta las ráfagas PHY.

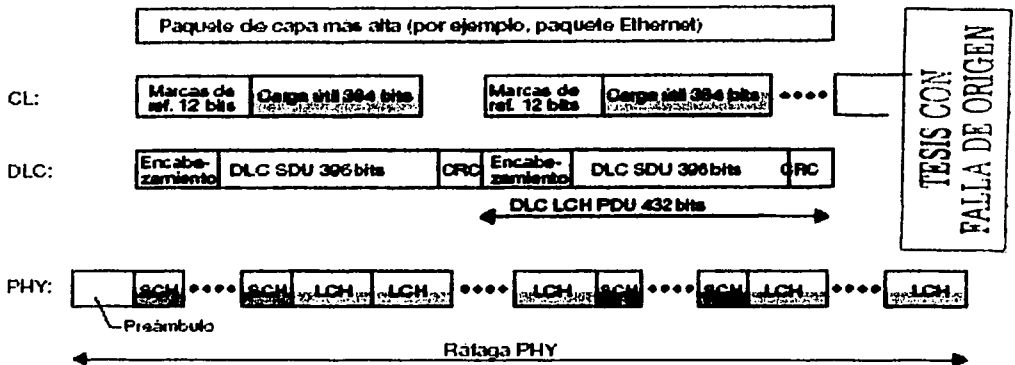


Figura 3.4. Correlación de paquetes de la capa más alta en las capas de HiperLAN2.

Para transmisión, las unidades de datos en la capa DLC son unidades de datos en paquete (PDU) de canal de transporte largo (LCH); para mensajes de control se usan PDUs de canal de transporte corto.

3.1.2.2 Capa de Control de Enlace de Datos (DLC)

La capa DLC consiste de una subcapa de control de enlace de radio (RLC), un protocolo de control de error (EC), y un protocolo MAC.

3.1.2.2.1 Subcapa de Control de Enlace de Radio (RLC)

El RLC maneja tres funciones principales de control:

1. La función de control de asociación es usada para autenticación, gestión de clave, asociación, desasociación, y encriptación.
2. La función de control de recursos de radio (RRC) gestiona el traspaso (solución genérica), selección dinámica de frecuencia, terminal móvil activo / ausente, economización de potencia, y control de potencia.
3. La función de control de conexión de usuario DLC establece y desconecta conexiones de usuario, multidifusión y difusión.

En resumen se usa el RLC para intercambiar datos en el plano de control entre un punto de acceso y un terminal móvil por ejemplo, el terminal móvil forma asociaciones con el punto de acceso por medio de señalización RLC. Después de terminar el proceso de asociación, el terminal móvil puede solicitar un canal de control dedicado para establecer portadores de radio. Los portadores de radio se refieren como conexiones DLC dentro de la especificación HiperLAN2.

La terminal móvil podría solicitar conexiones múltiples DLC, donde cada una ofrece apoyo único para calidad de servicio (QoS) como es determinado por el punto de acceso.

No es necesario que el establecimiento de la conexión resulte en una asignación inmediata de capacidad por el punto de acceso. El terminal móvil recibe en vez una dirección DLC única que corresponde a la conexión DLC.

3.1.2.2.2 Protocolo de Control de error (EC)

Los modos de operación de control de error se definen para apoyar distintos tipos de servicio:

1. El *modo confirmado* usa la retransmisión para mejorar la calidad del enlace y garantizar una transmisión de funcionamiento seguro. El modo confirmado está basado en solicitud de repetición automática (ARQ) de repetición selectiva (SR). Se puede dar un tiempo de espera bajo por medio de un mecanismo de descartar.
2. El *modo de repetición* repite las PDUs de los DLC portadores de datos (LCH PDU) para dar una transmisión bastante fiable (Figura 3.2.). No hay canal de realimentación disponible. El transmisor puede retransmitir PDUs arbitrariamente. La retransmisión de PDUs refuerza la recepción. El receptor acepta, sin embargo, sólo las PDUs cuyo número de secuencia se encuentra dentro de su ventana de aceptación. El modo de repetición es usado típicamente para la transmisión de datos de difusión.
3. El *modo no confirmado* da una comunicación de bajo tiempo de espera y poco fiable sin retransmisiones. Por lo tanto no se encuentra disponible ningún canal de realimentación.
4. Se pueden enviar datos de unidifusión usando el modo confirmado o el no confirmado., Los servicios de difusión pueden ser apoyados por el modo de repetición o por el modo no confirmado. Los servicios de multidifusión pueden ser enviados en modo no confirmado o pueden ser multiplexados a transmisiones de unidifusión existentes.

3.1.2.2.3 Protocolo MAC

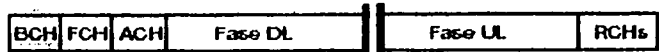
La estructura básica de trama en el interfaz de aire tiene una duración fija de 2ms y comprende campos para control de difusión, control de trama, control de realimentación de acceso, transmisión de datos en el enlace descendente y el enlace ascendente, y acceso aleatorio (Figura 3.5.). Durante la comunicación de enlace directo contiene la trama un campo de enlace directo adicional

Capítulo 3. Redes de Área Local Inalámbricas

(que no se muestra en la Figura 3.5.). La duración del control de difusión es fija, mientras que la duración de otros campos se adapta dinámicamente a la situación del tráfico.

El canal de difusión (BCH), que contiene información de control que se envía en cada trama MCA, permite principalmente el control de recursos de radio. El canal de trama (FCH) contiene una descripción exacta de la asignación de recursos dentro de la trama MAC actual. El canal de realimentación de acceso (ACH) transmite información sobre intentos anteriores de acceso aleatorio. El tráfico de enlace descendente o enlace ascendente consiste de datos a o de terminales móviles. El tráfico de conexiones múltiples a o de un terminal móvil puede ser multiplexado a un tren PDU, donde cada conexión contiene LCHs de 54 octetos para datos y SCHs de 9 octetos para mensajes de control.

HiperLAN2 apoya antenas (sectores) de haces múltiples como un medio de mejorar el presupuesto de enlace y de reducir la interferencia en la red de radio.



DL a un MT

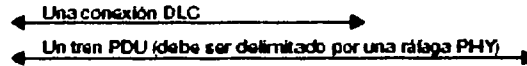


Figura 3.5 Estructura básica de trama (antena de un sector).

Cuando un terminal móvil tiene datos para transmitir a una cierta conexión DLC, debe solicitar capacidad primero enviando una solicitud de recurso (RR) al punto de acceso. La solicitud de recurso contiene el número de PDUs LCH pendientes en el terminal móvil para la conexión DLC concreta. Con base en un sistema de segmentos, la terminal móvil puede usar segmentos de emulación para enviar el mensaje RR. Al variar el número de segmentos de emulación (canales de acceso aleatorio, RCH), el punto de acceso puede reducir el retardo de acceso. Si ocurre una colisión, se envía información al terminal móvil en el ACH de la trama MAC siguiente. La terminal móvil rebaja después un número aleatorio de segmentos de acceso.

Después de haber enviado la solicitud de recurso al punto de acceso, la terminal móvil entra en un modo sin emulación donde se programa para oportunidades de transmisión (enlace ascendente y enlace descendente). La programación de recursos se lleva a cabo en el punto de acceso, un controlador centralizado permite un apoyo eficaz QoS.

El punto de acceso podría hacer una interrogación secuencial a la terminal móvil para obtener información sobre PDUs pendientes. Del mismo modo, la terminal móvil podría informar al punto de acceso sobre su estado al enviar una solicitud de recurso por medio del RCH.

3.1.2.3 Funciones de red de radio y apoyo QoS

La norma HiperLAN2 define las mediciones y la señalización que apoyan a un número de funciones de red de radio, incluyendo la selección dinámica de frecuencia, la adaptación de enlace, traspaso, antenas de haces múltiples, y control de potencia. Los algoritmos son específicos al vendedor. Las funciones apoyadas de red de radio permiten la instalación celular de sistemas HiperLAN2 con cobertura completa y altas velocidades de transmisión de datos en una variedad de ambientes. El sistema asigna frecuencias automáticamente a cada punto de acceso para comunicación la selección dinámica de frecuencia (DFS) permite que varios operadores puedan compartir el espectro disponible y evita el uso de frecuencias interferidas. La selección de frecuencia está basada en mediciones de interferencia realizadas por el punto de acceso y terminales móviles asociados. La calidad del enlace de radio, que depende del ambiente de radio, cambia con el tiempo y de conformidad con el tráfico en las celdas de radio circundantes. Para hacer frente a las variaciones se aplica un programa de adaptación de enlace: la adaptación del modo de capa física o sea, la tasa de código y el programa de modulación está basada en mediciones de calidad de enlace (Tabla 1).

La adaptación de enlace se usa en el enlace ascendente y en el enlace descendente.

El punto de acceso mide la calidad del enlace en el enlace ascendente e indica en el FCH, cuál modo PHY debe usar el terminal móvil para la comunicación de enlace ascendente. El terminal móvil mide del mismo modo la calidad en el enlace descendente y sugiere, en cada solicitud de recurso señalizada al punto de acceso, un modo PHY para comunicación de enlace descendente. El punto de acceso selecciona el modo final PHY tanto para el enlace ascendente como para el enlace descendente. El control de potencia de transmisor es apoyado en el terminal móvil (enlace ascendente) y el punto de acceso (enlace descendente). El control de potencia en el terminal móvil es usado principalmente para simplificar el diseño del receptor del punto de acceso, al evitar el control automático de ganancia. El control de potencia en el punto de acceso ha sido introducido principalmente para propósitos reguladores, para reducir la interferencia a otros sistemas en la misma banda.

HiperLAN2 apoya calidad de servicio al permitir que el punto de acceso pueda establecer y gestionar distintos portadores de radio durante la transmisión. El punto de acceso selecciona el modo apropiado de control de error (confirmado, no confirmado y repetición) inclusive regulaciones de protocolo en detalles (por ejemplo, tamaño de ventana ARQ, número de retransmisiones, descartados). La programación se realiza al nivel MAC, donde el punto de acceso determina cuántos datos y señalización de control serán enviados en la trama MAC actual. Por ejemplo, al hacer una interrogación secuencial o regularidad a un terminal móvil sobre su estado de tráfico (datos pendientes a ser retransmitidos), el punto de acceso da al portador de radio del terminal un retardo de acceso corto. El mecanismo de interrogación secuencial da un acceso rápido para servicios de tiempo real. El apoyo adicional QoS incluye adaptación de enlace funciones internas (mecanismos de admisión, congestión y derivación) para evitar situaciones de sobrecarga

3.1.2.4 Capa física

Las unidades de datos que se han de transmitir por medio de la capa física de HiperLAN2 son ráfagas de longitud variable. Cada ráfaga consiste de un preámbulo y un campo de datos. El campo de datos se compone de un tren de PDUs SCH y LCH que han de ser transmitidas o recibidas por un terminal móvil. La Multiplexación ortogonal de división de frecuencia (OFDM) ha sido seleccionada como el programa de modulación para HiperLAN2, debido a un buen comportamiento en canales muy dispersivos.

En términos de sensibilidad y comportamiento al estar sometido a una interferencia de canal a una tasa de bits de 25 [M/s], la OFDM supera en comportamiento a la modulación de portadora único por 2 a 3 dB. La modulación de portadora única no puede apoyar tasas altas de bit de forma eficaz este es un factor importante, ya que se exige que HiperLAN2 apoye tasas de bit mucho más altas. Un inconveniente con OFDM es la rebaja de potencia de amplificador, que afecta la cobertura. La

Capítulo 3. Redes de Área Local Inalámbricas

rebaja de amplificador de potencia relacionada con OFDM es de 2 a 3 dB más grande que la de una modulación de portadora única, para la máscara de espectro que se ha especificado para HiperLAN2. Sin embargo, en términos de cobertura, se compensa esta "debilidad" de OFDM por una sensibilidad más grande. El consumo de potencia en terminales móviles, que también es afectado por la rebaja de potencia de amplificador, debe ser considerado junto con: el consumo de potencia reducido en el receptor OFDM; y la relación de tráfico de enlace descendente y de enlace ascendente, que se espera que sea muy asimétrica.

Con base en estos y en otros argumentos, se prefiere la OFDM al comparar con la modulación de portador a única.

Se ha seleccionado un cuadrículado de canal de 20 [MHz] para dar un número razonable de canales en un ancho de banda de 100 [MHz], que podría ser el ancho de banda más angosto de sistema continuo que se encuentra disponible (por ejemplo, en Japón). Para evitar frecuencias mezcladas no deseadas en las implementaciones, es también de 20 [MHz] la frecuencia de muestreo (a la capacidad de una transformación Fourier rápida inversa de 64 puntos, IFFT, en el modulador).

El espaciamiento de subportador obtenido es de 312.5 [kHz]. Para facilitar la implementación de filtros y para alcanzar una supresión de canal adyacente suficiente, se usan 52 subportadoras por canal; 48 subportadoras llevan datos y 4 son pilotos que facilitan la desmodulación coherente. La duración del prefijo cíclico es de 800 [ns], lo que es suficiente para permitir un buen comportamiento en canales con una extensión de retardo de raíz cuadrada de la media de los cuadrados de por lo menos 250 [ns]. Se puede usar un prefijo opcional cíclico corto con 400 [ns] para aplicaciones de interior y de corto alcance.

Una característica clave de la capa física es que da varios modos de capa física con distintas tasas de codificación y programas de modulación, que se seleccionan por adaptación de enlace. La capa física apoya la manipulación de cambio de fase binaria y cuaternaria (BPSK, QPSK) así como la modulación de amplitud de cuadratura (16QAM) para la modulación de las subportadoras. 64QAM se puede usar además como un modo opcional.

La corrección de error hacia adelante (FEC) se realiza por un código convolucional con una tasa de 1/2 y longitud de restricción 7. Las tasas de código 9/16 y 3/4 se obtienen por medio de perforación. Los modos de capa física son elegidos de manera tal que el número de bits de potencia de codificador corresponda a un número entero de símbolos OFDM. Para acomodar bits de cola se aplica una perforación dedicada apropiada antes de perforar la secuencia de bit codificada. Se han especificado siete modos de capa física (Tabla 1).

TABLA 1. MODOS DE CAPA FISICA DE HIPERLAN/2

Modo	Modulación	Régimen de código	Régimen de código de capa física
1	BPSK	1/2	6 Mbit/s
2	BPSK	3/4	9 Mbit/s
3	QPSK	1/2	12 Mbit/s
4	QPSK	3/4	18 Mbit/s
5	16QAM	9/16	27 Mbit/s
6	16QAM	3/4	36 Mbit/s
7	64QAM	3/4	54 Mbit/s

Seis de los modos de capa física son obligatorios; 64QAM es opcional. Cada ráfaga de capa física incluye un preámbulo, del cual hay tres tipos para:

- el canal de control de difusión;
- otros canales de enlace descendente; y
- el canal de enlace ascendente y el de acceso aleatorio.

El preámbulo de las ráfagas opcionales de enlace directo es idéntico al preámbulo del enlace ascendente largo. El preámbulo en el canal de canal de control de difusión permite la sincronización de trama, el control automático de ganancia, la sincronización de frecuencia, y la estimación de canal. Por contraste, se usa el preámbulo en ráfagas de tráfico de enlace descendente sólo para la estimación de canal. Las ráfagas de tráfico de enlace ascendente y las ráfagas de acceso aleatorio permiten la estimación de canal y de frecuencia. Por lo tanto hay varios preámbulos con distintas estructuras y longitudes (Figura 3.6., Cuadro B).

CUADRO B. PREÁMBULOS DE HIPERLAN/2

Los símbolos A y B están compuestos de 16 muestras de dominio de tiempo. Los símbolos indicados con -A y -B son réplicas negativas de A y B, respectivamente.

El bloque de cuatro símbolos, A, -A, A, -A puede ser producido por un IFFT de 64 puntos de un símbolo de dominio de frecuencia con 12 subportadoras a los índices de frecuencia +/- 2, +/- 6, etc. es anexado por repetición en el dominio de tiempo. Del mismo modo se producen los símbolos B de un símbolo de dominio de frecuencia con los subportadores usados en los índices +/- 4, +/- 8, etc.

Gracias a las estructuras de dominio de tiempo de las secuencias A, -A, A, -A y B, B, B, B, es fácil distinguir los canales de control de emisión y las ráfagas de enlace ascendente. Los símbolos anexados -A y -B mejoran la estimación de temporización.

La parte C, que es incluye en cada preámbulo, está compuesto de dos símbolos de entrenamiento que usan 52 subportadores y un prefijo cíclico de 1.6 us. La parte C es usada para la estimación de canales, mientras que los símbolos cortos anteriores son usados para todos los otros propósitos, tales como la sincronización de trama, la estimación de frecuencia, etc.

Figura 3.6. Los preámbulos de HiperLAN2

Preámbulo en ráfaga de difusión



Preámbulo en ráfagas de enlace descendente



Preámbulo corto en ráfaga de enlace ascendente



Preámbulo largo en ráfaga de enlace ascendente



Dependiendo de las capacidades del receptor, éste puede elegir el punto de acceso entre dos preámbulos de enlace ascendente. Cada preámbulo es obligatorio para la terminal móvil. El comportamiento de la sincronización inicial o sea, cuando los terminales sincronizan al preámbulo BCH se caracteriza por la probabilidad de detección de avería y la probabilidad de alarma falsa. Los resultados de simulación muestran que hasta en un escenario de peor caso (relación de potencia baja de señal a ruido de 5 dB, un canal de desvanecimiento muy dispersivo con una extensión de retardo de 250 ns, y una compensación de frecuencia de 40 ppm), es de 96 % la probabilidad de una sincronización con éxito en HiperLAN2. HiperLAN2 da de esta manera un medio de sincronización rápido, eficaz y robusto.

TESIS CON FALLA DE ORIGEN

3.2 IEEE802.11

IEEE802.11 es un estándar para redes inalámbricas definido por la organización Institute of Electrical and Electronics Engineers (IEEE), instituto de investigación y desarrollo, de gran reconocimiento y prestigio, cuyos miembros pertenecen a decenas de países entre profesores y profesionales relacionados con las nuevas tecnologías.

El estándar IEEE802.11 es un estándar en continua evolución, debido a que existen cantidad de grupos de investigación, trabajando en paralelo para mejorar el estándar, a partir de las especificaciones originales.

La primera versión del estándar fue definida en 1997. Aunque el comité evaluador fue creado en 1990, muestra del gran desarrollo que ha sido la primera versión. Esta versión trata de ofrecer varias formas para poder interconectar computadoras y otros dispositivos sin la necesidad de algún tipo de cableado. Esta primera versión, visto hoy está obsoleta, pero ha marcado un principio para una tecnología prometedora.

Se nos ofrece tres alternativas en cuanto a tecnología subyacente para poder realizar nuestra red. Ofrece entre otras cosas tres capas físicas, por la cual enviaríamos los datos, infrarrojos (IR), por la banda ICM 2.4 [GHz] con técnicas de espectro ensanchado, ya sea con salto en frecuencias como por secuencia directa. Con el estándar original se consiguen velocidades hasta un máximo de 2Mbps tanto por radiofrecuencia como por infrarrojos.

Más adelante y como consecuencia de la incorporación de las investigaciones de los grupos de trabajo 11b y 11a se ha conseguido mejorar las tasas máximas de transmisión. Más concretamente con 11b se ha podido conseguir 11[Mb/s] en la banda de 2.4 [Ghz], usando técnicas de espectro ensanchado y secuencia directa, cambiando además la modulación, clave para mayores tasas de transferencia.

Por otra parte el grupo de trabajo 11a, ha conseguido acercar las redes inalámbricas a las cableadas, con una velocidad máxima de 54[Mb/s]. Mientras que el grupo de trabajo 11g, ya estipula lo relacionado a manejar velocidades máximas de de 54[Mb/s] en la banda de 2.4[GHz] compatible con el estándar 11b.

Otros grupos definidos que trabajan en una variedad de propuestas para mejorar el servicio de las redes WLANs son los grupos:

- **Grupo 11c:** Añadir soporte MAC en 802.1 para operaciones de puente para el estándar 802.11.
- **Grupo 11d:** Definir nuevos requerimientos para la capa física, como puede ser canales, secuencias de saltos y otros requerimientos para hacer funcionar 802.11 en otros países, donde no es posible implementar 802.11, puesto que no tienen 2.4 [GHz] libre o es más corta la banda de frecuencias.
- **Grupo 11e:** Mejorar el MAC del 802.11 para que pueda manejar de forma adecuada Calidad de servicio, poder tener clases de servicio y mejorar los mecanismos de seguridad y autenticación. Mejorar el PCF y DCF de manera que se mejore la eficiencia. Se aplicará a los estándares físicos a, b y g de 802.11. La finalidad es proporcionar claves de servicio con niveles gestionados de QoS para aplicaciones de datos, voz y video.
- **Grupo 11f:** Su objetivo es lograr la interoperabilidad de Puntos de Acceso (AP) dentro de una red WLAN con múltiples proveedores en el servicio. El estándar define el registro e Puntos de Acceso (AP) dentro de una red y el intercambio de información entre dichos Puntos de Acceso cuando un usuario se traslada desde un punto de acceso a otro.
- **Grupo 11h:** Mejorar la capa física (PHY) en la banda de 5 [GHz] para países europeos. Por tema de las licencias es imposible transmitir en esta banda en Europa, de ahí que estas investigaciones se centren en elaborar mecanismos de selección entre interiores y exteriores.

- **Grupo 11i:** Se refiere al objetivo más frecuente del estándar 802.11, la seguridad. Se aplicará a los estándares físicos a, b y g de 802.11 Proporciona una alternativa a la Privacidad Equivalente Cableada (WEP) con nuevos métodos de encriptación y procedimientos de autenticación.

Como ya se ha visto, hay cantidad de grupos de trabajo, hoy día trabajando en paralelo, con el objetivo común de mejorar el estándar en diversos aspectos. De ahí que se puede concluir que se trate de una especificación en continua evolución con posibilidad de adaptarse a nuevos requerimientos y demandas de usuario en un futuro.

3.2.1 Arquitectura de la Red WLAN IEEE 802.11

Una red inalámbrica de área local WLAN 802.11 consiste en una estructura que posee un conjunto básico de servicios o Basic Service Set (BSS's) compuesta de estaciones o nodos inalámbricos que son conectadas a una capa de distribución de red o DS. Cada BSS está conformado por nodos móviles o estaciones que se encuentran controlados por una Distributed Coordination Function (DCF) que determina que nodo tiene derecho a transmitir o recibir información en el medio inalámbrico de radio propagación. Las estaciones en un BSS obtienen acceso a la capa DS y por lo tanto a otros nodos inalámbricos fuera de su área de cobertura a través del AP. Una estación puede estar conectada solo a un AP en un instante dado de tiempo en la simulación.

La capa DS soporta la movilidad de los nodos mediante direccionamiento e integración de forma transparente a la computación interna de la información en las estaciones.

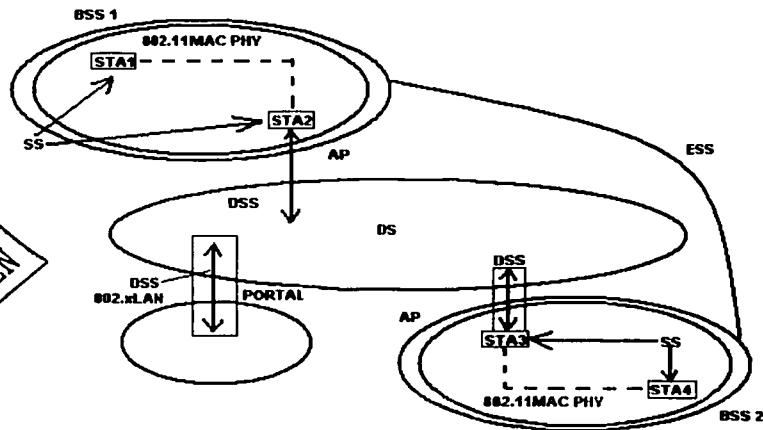


Figura 3.7 Arquitectura de la WLAN IEEE 802.11

La estación STA 1 y la estación STA 4 se pueden conectar a través del Extended Service Set (ESS) que cubre los BSS 1 y BSS 2. La comunicación entre las estaciones que componen un BSS se realiza mediante función Distributed Coordination Function DCF involucrando la capa Medium Access Layer (MAC) y la capa física (PHY). El mensaje original de STA 1 pasa por AP 1 a través STA 2 mediante el Distribution Service Set DSS y de ahí al DS en donde el enrutamiento óptimo direcciona STA 4 a través del AP 2 y de STA 3 en el BSS 2. En el caso en el que la capa DS direcciona un nodo fuera de la red inalámbrica se utiliza un protocolo en el DSS que configura un portal o servidor que sirve como interfase entre la WLAN y una LAN alámbrica.

TESIS CON
FALLA DE ORIGEN

La norma IEEE 802.11 permite el monitoreo de la portadora en forma física a través de la interferencia aérea de las ondas de forma virtual a través de la subcapa MAC. El monitoreo físico de la portadora detecta la presencia de otros usuarios WLAN IEEE 802.11 analizando todos los paquetes detectados y monitoreando la actividad del canal vía medición de la potencia relativa de la señal proveniente de otras fuentes. La prevención de las colisiones en el protocolo CSMA/CA se realiza mediante la configuración de un tiempo de backoff, si un nodo inalámbrico está listo para acceder al canal de control inicialmente censa el canal para determinar si está o no ocupado, si está ocupado espera a que se encuentre libre mediante el NAV(Network Allocation Vector) el cual se activa cuando se detectan los respectivos marcos RTS Request To Send y CTS Clear To Send de los nodos que se encuentran utilizando el canal de control; una vez que el canal se encuentra libre se determina el Distributed Coordination Function Interframe Structure (DIFS) y se procede a procesar el tiempo de backoff para evitar las colisiones con otros nodos inalámbricos, la estación espera a que el contador interno llegue a cero o en su defecto el canal de control vuelva a estar en estado de ocupación, si el timer no ha llegado a cero y el canal lo ocupa otro nodo inalámbrico, el contador regresivo se detiene, al recibir de nuevo el DIFS, el contador reinicia su marcha regresiva y cuando llega a cero envía su marco RTS. Si dos o más estaciones llegan a cero en su contador interno al mismo tiempo o en su defecto en la ventana de vulnerabilidad (Tiempo de Tx del RTS) el AP asume que ocurrió una colisión y se procede a reiniciar el proceso de acceso al canal de control dejando el CTS=0, después del envío del RTS por parte de alguno de los nodos inalámbricos.

Como ya se ha explicado, el estándar permite el uso de varios medios y técnicas para establecer conexiones. El estándar original permite usar infrarrojos, espectro expandido tanto en salto en frecuencias como secuencia directa. Todo ello con la ventaja de usar una capa de acceso al medio (MAC) común. Ello da mucha flexibilidad a los desarrolladores e investigadores, que pueden olvidarse de ciertos aspectos ya que no existe dependencia directa entre ellos.

Los estándares de IEEE802.11 son de libre distribución y cualquier persona puede ir a la página Web del IEEE y descargarlos. Estos estándares sólo definen especificaciones para las capas físicas y de acceso al medio y para nada tratan modos o tecnologías a usar para la implementación final. Esto debe permitir y facilitar la interoperabilidad entre fabricantes de dispositivos IEEE802.11 y para asegurarse de ello se ha creado una alianza denominada WECA para crear y definir procedimientos para conseguir certificados de interoperabilidad y de cumplir las especificaciones, todo dentro de un estándar llamado WiFi o también llamado "Wireless Fidelity". El nombre además es un indicativo del enfoque doméstico y muy enfocado hacia el usuario final.

3.2.2 Arquitectura del Protocolo de IEEE802.11

3.2.2.1 Capa Física (PHY)

La capa física en cualquier red define la modulación y características de señalización para la transmisión de datos en ese medio. Como ya he dicho en este estándar dos métodos de transmisión por radiofrecuencias y uno por infrarrojos ha sido definido.

Para poder transmitir para redes inalámbricas en bandas sin licencia se necesita usar técnicas de espectro ensanchado, ello está definido en los requerimientos de casi todos los países.

Las definiciones para la transmisión por radiofrecuencia en los estándares son espectro ensanchado por salto en frecuencias (FHSS) y espectro ensanchado por secuencia directa (DSSS). Ambos están definidos para trabajar en la banda de 2.4 [GHz], y DSSS además tiene una variante en la banda de los 5Ghz, que consigue mayores velocidades de transmisión.

➤ FHSS

Salto en frecuencias refiere a un sistema que periódicamente cambia las frecuencias en la que transmite. La banda entera se usa y ello contribuye a aumentar la seguridad frente a escuchas y

ayuda a suprimir ruido e interferencia. Tiene 22 patrones de saltos predefinidos usando los 79 canales de 1Mhz a un mínimo de 2.5 saltos por segundo.

Además hay importantes problemas de sincronización para que tanto transmisor como receptor salten a la vez, de ahí que se defina paquetes de sincronización.

Para la modulación FHSS usa FSK gaussiano de 2 ó 4 niveles. Las velocidades típicas conseguidas son de 1 y 2 Mbps para FHSS,

➤ DSSS

Las modulaciones usadas para DSSS son BPSK y QPSK para el estándar original y para 11b que permite conseguir 11Mbps se utiliza CCK. 1, 2, 5 y 11 para DSSS ya sea velocidad original o parte de 11b.

Además se ha definido una variante de IEEE802.11, incorporado recientemente a la especificación que permite conseguir 54Mbps en la banda de 5Ghz, con un ancho de banda de hasta 300MHz y usando una modulación OFDM.

El modo de funcionamiento es el siguiente, el sistema de radio usando DSSS trabaja en un canal fijo y preconfigurado, esto le permite obtener mayores tasas de transferencia, con la desventaja de ser más sensible a interferencia y a señales procedentes de otros dispositivos usando la misma frecuencia. De manera que es posible tener tres puntos de acceso con tres canales diferentes, sin solapar en un mismo emplazamiento, sin tener en cuenta ningún tipo de planificación. Aunque para más de tres puntos de acceso sí es necesaria cierta planificación, para poder mantener las velocidades, puesto que el solape de celdas y frecuencias tendrá un deterioro sobre el rendimiento.

Para transmitir la capa física DSSS utiliza una secuencia de Barker de 11bits, ello le permite extender los datos antes de ser transmitidos. Cada bit transmitido es modulado por la secuencia de 11bits, esto permite extender uniformemente la energía de transmisión por un ancho de banda mayor que si lo enviásemos de forma directa. Otra ventaja de la técnica es que permite reducir el efecto de las interferencias que afecten en una banda pequeña.

Pero hoy día casi todos los fabricantes optan por la versión 11b (High Rate), también basado en DSSS. Esto hace que la migración de 2Mbps a 11Mbps sea muy sencilla, puesto que el esquema de modulación subyacente es muy similar. Además se permite la coexistencia entre los sistemas permitiendo además una gradual transición entre sistemas, tal como puede ser cambiar de una Ethernet de 10Mbps a otro de 100Mbps.

Para conseguir 11Mbps, la capa física del 11b utiliza tecnología CCK para codificar los datos, ello permite obtener las velocidades de hasta 11Mbps con posibilidad de bajar a 5.5Mbps o 2-1Mbps si fuese necesario. Como en las redes cableadas un aumento de la tasa de transmisión nos permite usar muchas aplicaciones nuevas, como streaming de video/audio que el estándar anterior se quedaba corto.

También cabe mencionar, que debido a los temas de licencias, y la problemática de no poder utilizar 11a, IEEE tiene un grupo de trabajo investigando en cómo aumentar las prestaciones en la banda de 2.4Ghz. Este grupo, 11g, ya ha conseguido 22Mbps y parece ser que en un futuro próximo podrá aumentar la velocidad hasta equipararse a 11a sin tener los problemas legales de éste.

➤ INFRARROJOS.

Se soporta un estándar infrarrojo para comunicaciones inalámbricas. Se opera en la banda de 850 a 950 [nm] (300 a 428 [GHz]) con una potencia máxima de 2W. Se utiliza una modulación PPM de 4 o 16 niveles con lo que se consigue una velocidad máxima de 1-2Mbps.

Se considera que la transmisión por infrarrojos es más seguro ante escuchas, puesto que la comunicación por infrarrojos necesita línea de vista para comunicarse, no como los por

radiofrecuencias que pueden ser interceptadas sin que nadie lo sepa. Sin embargo las transmisiones por infrarrojos pueden ser afectados por cuerpos opacos y por la luz solar y los mecanismos de 802.11 por radiofrecuencia si incluyen algún que otro método para seguridad.

3.2.2.2 La Capa de Acceso al Medio (MAC)

La especificación de la capa MAC del IEEE802.11 tiene muchas similitudes con el estándar de Ethernet cableado (IEEE802.3). El protocolo del 802.11 es un esquema de protocolo conocido como detección de portadora, acceso múltiple, evitando colisiones (CSMA/CA). Este protocolo evita las colisiones, en vez de detectarlas como el algoritmo de 802.3. Es extremadamente difícil detectar colisiones en una red de transmisión de radiofrecuencias y de ahí de que se trate de evitar las colisiones. La capa MAC opera junto con la capa física muestreando la energía del medio transmisor de datos. El protocolo CSMA/CA permite opciones para que se pueda minimizar las colisiones usando tramas de transmisión RTS/CTS, datos y reconocimientos de una manera secuencial. Junto a estas tramas se suele incorporar datos de duración de los envíos con tal que asegurar que esos envíos no van a ser interrumpidas, ya que los demás nodos saben que deben estar callados durante esa duración de tiempo, todo ello además es asegurada y confirmada con reconocimientos.

Pero un problema común a cualquier WLAN es el problema de los nodos ocultos. Esto puede llegar a reducir las prestaciones en un 40% en una WLAN con alta carga. Ocurre cuando un nodo no puede escuchar transmisiones de un nodo, y trata de transmitir a un nodo que si puede escucharlas, allí se puede generar muchas colisiones. Algunas mejoras se han incorporado para evitar el problema con el uso de RTS/CTS de una manera inteligente.

Además se utiliza tiempos entre tramas para evitar colisiones, ello a parte de evitar colisiones, permite además cierto uso de clases de calidad o por lo menos de preferencia de un tráfico sobre otro, utilizando funciones de coordinación puntual y de permitir el acceso al medio de tráfico prioritario antes que a los demás.

En la tabla 2 se presentan algunos de los parámetros temporales que caracterizan el funcionamiento del protocolo de acceso CSMA/CA para cada una de las tecnologías especificadas en la norma.

	DSSS	FHSS	IR
Slot time	20 μ s	50 μ s	6 μ s
SIFS	10 μ s	28 μ s	7 μ s
DIFS	50 μ s	128 μ s	19 μ s
aCCAtime	$\leq 15 \mu$ s	27 μ s	5 μ s
MSDU _{max} size	2312 b	2312 b	2312 b
RxTxArTime	10 μ s	19 μ s	0 μ s
Phy preamble	192 b	122 b	92-112 b

Tabla 2 Parámetros Temporales del protocolo CSMA/CA

3.2.2.2.1 Trama de IEEE802.11

Las tramas MAC contienen los siguientes componentes básicos:

- una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia.
- un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama.
- un secuencia checksum (FCS) que contiene un código de redundancia CRC de 32 bits.

Las tramas MAC se pueden clasificar según tres tipos:

1. Tramas de datos.
2. Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda.
3. Tramas de gestión. Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso.

La trama, por otra parte, es muy parecida a las demás de la familia IEEE802, siendo de 48bits de longitud y con muchos campos comunes a la trama de Ethernet. A continuación se muestra un ejemplo:

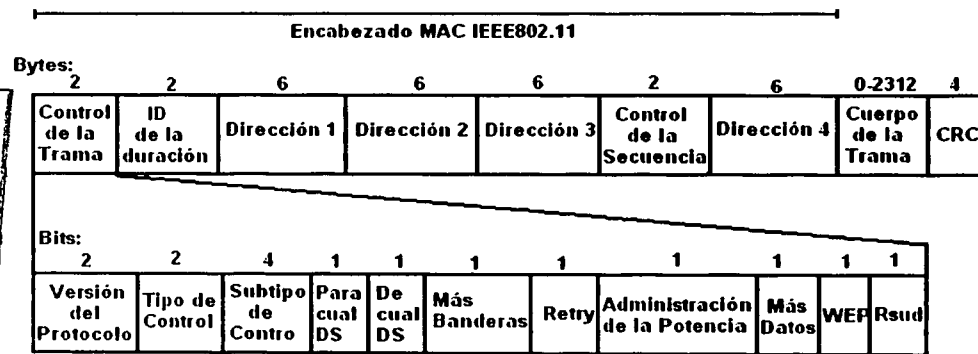


Figura 3.8. Trama MAC del IEEE802.11

Los campos que componen esta trama son:

- Campo de control. Merece examinar aparte. Lo haremos más abajo.
- Duration/ID. En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación.
- Campos address1-4. Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.
- Campo de control de secuencia. Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.
- Cuerpo de la trama. Varía según el tipo de trama que se quiere enviar.
- FCS. Contiene el checksum.

Los campos de control de trama tienen el formato siguiente:

- Versión.
- Type/Subtype. Mientras el campo tipo identifica si la trama es de datos, control o gestión, el campo subtipo nos identifica cada uno de los tipos de tramas de cada uno de estos tipos.
- ToDS/FromDS. Identifica si la trama si envía o se recibe al/del sistema de distribución. En redes ad-hoc, tanto ToDS como FromDS están a cero. El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución. Para ello situamos a uno tanto ToDS como FromDS.
- Más fragmentos. Se activa si se usa fragmentación.
- Retry. Se activa si la trama es una retransmisión.

TESIS CON FALLA DE ORIGEN

- Power Management. Se activa si la estación utiliza el modo de economía de potencia.
- More Data. Se activa si la estación tiene tramas pendientes en un punto de acceso.
- WEP. Se activa si se usa el mecanismo de autenticación y encriptado.
- Order. Se utiliza con el servicio de ordenamiento estricto, en el cual no nos detendremos.

Se puede ver lo mucho que se parece a una trama Ethernet, con algunas excepciones, por ejemplo, como incorporar 4 campos de direcciones. Esto se hace para facilitar el tráfico desde y hacia nodos al otro lado de los puntos de acceso. Además se incorpora muchos mecanismos de control para ahorro de energía, seguridad, etc.

3.2.3 Comparación entre los Estándares IEEE802.11 a,b y g

Para comprender los diferentes estándares IEEE802.11 debemos conocer los elementos que conforman una red. En la gran mayoría de las aplicaciones 802.11ba y g existen dos elementos básicos:

- AP (Access Point): este dispositivo es el punto de acceso a la LAN cableada. Es decir, es la interfase necesaria entre una red cableada y una red inalámbrica, es el traductor entre las comunicaciones de datos inalámbricas y las comunicaciones de datos cableadas.
- CPE (Customer Premise Equipment) : es el dispositivo que se instala del lado abonado o suscriptor. Así como las tradicionales placas de red que se instalan en un PC para acceder a una red LAN cableada, las Tarjetas de Red Inalámbricas dialogan con el Access Point (AP) quien hace las veces de punto de acceso a la red cableada.
- La Tarjeta de Red Inalámbrica puede ser de distintos modelos en función de la conexión necesaria a la computadora:
 - Tarjeta de Red Inalámbrica USB cuando la conexión a la computadora se realiza a través del puerto USB de la misma.
 - Tarjeta de Red Inalámbrica PCI cuando la conexión a la computadora se realiza a través de su slot interno PCI.
 - Tarjeta de Red Inalámbrica PCMCIA cuando la conexión a la computadora (comúnmente laptops o notebooks) se realiza a través de su slot PCMCIA.

En todo sistema 802.11 se establece un diálogo entre los CPE (Tarjetas de Red Inalámbricas) y el Access Point a través de una comunicación radioeléctrica a una frecuencia de 2.4 Ghz (802.11b y g) o de 5 Ghz (802.11a).

Para poder entender las características propias de los diferentes estándares que forman 802.11 en la siguiente tabla se puede comparar los tres protocolos que actualmente se comercializan dentro del estándar IEEE 802.11. Estos son el 802.11b, 802.11a y 802.11g en orden de aprobación por el IEEE:

Estándares Inalámbricos

Estándar	802.11b	802.11a	802.11g
Aprobado IEEE	Julio 1999	Julio 1999	Junio del 2003
Popularidad	Adoptado masivamente	Nueva tecnología, crecimiento bajo	Nueva tecnología, con un rápido crecimiento
Velocidad de Transmisión	Hasta 11 Mb/s	Hasta 54 Mb/s	
Costo	Barato	Relativamente caro	Relativamente barato
Frecuencia	2.4 50- 2.4835 Ghz	5.725 - 5.850 Ghz	2.4 50- 2.4835 Ghz
Cobertura	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos	Cobertura baja, unos 150 metros, con mala conectividad con obstáculos	Buena cobertura, unos 300 - 400 metros con buena conectividad con determinados obstáculos
Acceso Público	El número de Hotspots crece exponencialmente	Ninguno en este momento.	Compatible con los HotSpots actuales de 802.11b. El paso a 802.11g no es traumático para los usuarios
Compatibilidad	Compatible con 802.11g, no es compatible con 802.11a	Incompatible con 802.11b y con 802.11g	Compatible con 802.11b, no es compatible con 802.11a
Modos de datos	1, 2, 5.5, 11 Mb/s	6, 9, 12, 18, 24, 36, 48, 54 Mb/s	1, 2, 5.5, 11 Mb/s 6, 9, 12, 18, 24, 36, 48, 54 Mb/s
Modulación	DQPSK/CCK(11, 5.5 Mb/s) DQPSK(2 Mb/s) DBPSK(1 Mb/s)	BPSK (6, 9 Mb/s) QPSK (12, 18 Mb/s) 16-QAM (24, 36 Mb/s) 64-QAM (48, 54 Mb/s)	OFDM/CCK(6,9,12,18,24,36,48,54Mb/s) OFDM(6,9,12,18,24,36,48,54) DQPSK/CCK(22,33,11,5.5Mb/s) DQPSK (2 Mbps) DBPSK (1 Mbps)
Número de canales independientes	3	8	3
Rango en espacio libre (según la velocidad de transferencia de datos)	120(11Mb/s) hasta 460 metros(1Mb/s)	30(54Mb/s) hasta 300metros(6Mb/s)	100(54Mb/s) hasta 450 metros(12Mb/s)
Rango en habitaciones (según la velocidad de transferencia de datos)	30(11Mb/s) hasta 90 metros(1Mb/s)	12(54Mb/s) hasta 90metros(6Mb/s)	30(54Mb/s) hasta 90 metros(12Mb/s)
Número de usuarios admitido por punto de acceso	192	512	128
Aplicación	Datos	Multimedia	Datos y Multimedia
Características	El sistema más desarrollado hasta ahora	Ideal para entornos con gran densidad de usuarios	Reemplazara a 802.11b con una velocidad de transmisión mayor y mejor seguridad

PROBLEMAS CON FALLA DE ORIGEN

Podemos ver una gráfica con la relación entre la distancia (medida en pies, un pie = 0.3048 metros) y la velocidad de transmisión que podemos usar en cada caso. Por supuesto las distancias pueden variar dependiendo de la potencia y los [dBm] irradiados por la tarjeta de cada fabricante.

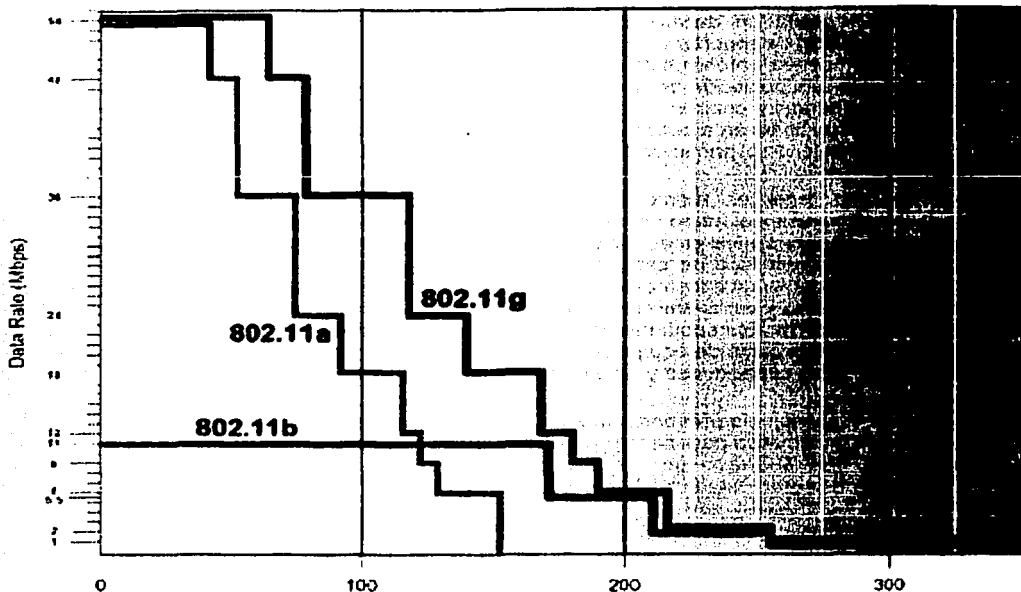


Figura 3.9 Relación entre la distancia y la velocidad de transmisión en los 3 protocolos comerciales de la IEEE802.11

Los distintos tipos de radiofrecuencia y modulación de estas tres tecnologías hacen imposible su operación en conjunto. Por ejemplo, un usuario final con una tarjeta de radio 802.11a no podrá conectarse a un access point 802.11b o 802.11g.

Como reglas generales para elegir si es mejor utilizar la tecnología 802.11a o la 802.11b, se pueden enunciar las siguientes:

Considere el uso de 802.11b si:

- Se requiere la cobertura de un espacio amplio, tal como un almacén o tienda departamental. 802.11b le proporcionará la solución menos costosa al emplear menos access points.
- Los usuarios finales se encuentran dispersos. Si hay relativamente pocos usuarios que necesiten movilidad dentro de las instalaciones, entonces 802.11b estará a la altura de los requerimientos de desempeño debido a que habrá pocos usuarios disputándose el ancho de banda total de cada access point. A menos que haya necesidades de un muy alto desempeño por cada usuario, 802.11a estaría muy sobrado para estas aplicaciones.
- Ya tiene una inversión hecha en sistemas con 802.11b.

Considere el uso de 802.11a si:

- Se necesita un desempeño muy alto. La razón principal para elegir 802.11a es la necesidad de soportar aplicaciones muy exigentes que incluyan video, voz y la transmisión de imágenes y archivos de un gran tamaño.
- Existe una población de usuarios muy densa. Lugares como laboratorios de computadora, aeropuertos y centros de convenciones necesitan dar soporte a una gran cantidad de usuarios en un área común que compiten por el mismo access point, con cada uno de ellos compartiendo el ancho de banda total.

Es importante tener en mente que la interoperabilidad entre 802.11a y b será mejorada considerablemente en el futuro cercano pues ya existen chips compatibles con 802.11a/b/g, lo que permitirá a los fabricantes crear radios que se comuniquen con 802.11a y 802.11b (además de 802.11g). Como resultado de esto, una terminal portátil con una tarjeta de radio 802.11a/b por ejemplo, detectará automáticamente cuando un access point sea 802.11a o b y se comunicará de la forma adecuada, y del mismo modo, un access point podrá trabajar con dispositivos 802.11a y dispositivos 802.11b. Es importante aclarar que esto seguramente será una tendencia en el futuro, aunque ningún fabricante de equipos con radio frecuencia cuenta actualmente con dispositivos que cuenten con estas capacidades y estén a la venta al público.

802.11b es la tecnología preponderante en este momento entre los fabricantes de dispositivos de identificación automática para ser utilizada en equipos como terminales portátiles. Las marcas más importantes han apostado por esta tecnología debido a su gran confiabilidad y apropiado desempeño en la gran mayoría de aplicaciones reales.

4. Telefonía Inalámbrica Pública o Empresarial

Hasta hace poco tiempo los sistemas de telefonía sin hilos (o teléfonos sin cordón) solo eran considerados como bienes de consumo, elementos familiares en los hogares mas o menos acomodados de la sociedad. Actualmente, debido al desarrollo de la tecnología y de la espectacular demanda de servicios de comunicaciones móviles, constituyen uno de los sistemas de comunicaciones con más atractivos para los usuarios y con un mercado potencial grande.

Los sistemas de telefonía sin hilos se pueden clasificar en generaciones que, si bien han aparecido en un corto espacio de tiempo, lo que hace que coexistan en la práctica unas con otras, están basados en diferentes tipos de tecnologías y van dirigidos a diferentes tipos de aplicaciones. Podemos distinguir tres generaciones bien diferenciadas:

- La primera generación constituye el sistema más simple de comunicaciones móviles de voz; una única estación base conectada a la terminación de la red telefónica pública, se comunica con un portátil vía radio proporcionando al usuario servicio telefónico en una determinada área de servicio. Está pensado para uso domestico exclusivamente. Las tecnologías que en esta primera generación se desarrollaron fueron CT0 y CT1 que constituyen los teléfonos sin cordón analógicos basados en un sistema de tipo monocélula/monousuario.
- La segunda generación incorpora la digitalización del trayecto radio y permite le acceso directo de la red telefónica conmutada para servicios de tipo público. La tecnología que en esta segunda generación se desarrolló fue CT2 basado en un sistema de tipo monocélula/multiusuario.
- La tercera generación permite constituir redes de telefonía móvil geográficamente dispersa, con posibilidades de aplicación en entornos de muy alta densidad de usuarios, como los edificios de oficinas, incluyendo además facilidades de red inteligente, lo que permitirá el desplazamiento de los usuarios entre diferentes sistemas y su funcionamiento con otras redes. Las tecnologías que en esta tercera generación se desarrollaron son: en primer lugar CT3, considerado como el primer sistema de telefonía sin hilos de esta generación; constituye en realidad un sistema pre-DECT ya que ambos tienen la misma base tecnológica, diferenciándose casi exclusivamente en la banda de frecuencia utilizada. Esta nueva generación surgió con la pretensión de establecer un estándar de teléfonos sin hilos digitales el cual culmino con el sistema DECT en Europa y su similar PHS en Japón.

Las aplicaciones de los sistemas sin hilos son:

- Uso residencial: Los teléfonos sin hilos de tipo residencial proporcional las mismas facilidades que los teléfonos fijos normales y además permiten a sus usuarios hacer llamadas desde cualquier punto dentro del hogar. Es la primera utilización que se le dio a estos sistemas y la más extendida en la actualidad.
- Uso público: Este servicio permite la utilización de teléfonos portátiles en la vía pública, en lugares en donde las necesidades de comunicación se han satisfecho tradicionalmente mediante la instalación de teléfonos públicos. Este tipo de servicio se asemeja al de los sistemas celulares.
- Sistemas de comunicaciones de empresa. Con este servicio las personas que trabajan en una oficina disponen de un teléfono portátil de bolsillo que proporciona todas las facilidades de una extensión normal de la central del edificio. Cada portátil tiene su propia identidad única y su posición dentro del edificio es supervisada por el sistema para poder dirigirle las llamadas entrantes. Constituyen sistemas pico celulares que permiten hacer y recibir llamadas de cualquier punto del edificio o en movimiento.

4.1 Digital European Cordless Telecommunications (DECT)

El estándar *Digital European Cordless Telecommunications* (DECT) fue inicialmente concebido a finales de 1980 como el estándar Europeo para teléfonos inalámbricos en aplicaciones domésticas y fue desarrollado a partir de CT2.

El objetivo del nuevo estándar propuesto por CEPT era mejorar la calidad de voz, aumentar la capacidad de tráfico, mejorar seguridad en las llamadas e inmunidad a la interferencia entre teléfonos inalámbricos cercanos.

El estándar DECT fue finalizado en 1992 y publicado por ETSI, organismo de estandarización sucesor de CEPT pero su alcance había evolucionado hacia 2 nuevas aplicaciones: una fue teléfonos inalámbricos para aplicaciones de negocios (PBX inalámbricas) y la otra un sistema de acceso inalámbrico para suscriptores a las redes públicas de telecomunicaciones que incluía la opción telepunto y el lazo local de abonado (RLL).

Desde 1993 DECT ha sido un estándar de facto en la Unión Europea, sin embargo, su alcance no ha terminado allí. Existe el estándar Telecomunicaciones Inalámbricas Personales (PWT) desarrollado para PCS (Servicios de Comunicación Personal) más conocido como WCPE, una iniciativa de AT&T, Motorola y Nortel que modifica la capa física de DECT para lograr compatibilidad con las regulaciones de la Federal Communications Commission (FCC) en USA.

Este alcance global y amplio soporte por parte de fabricantes ha presionado al ETSI a redefinir el acrónimo de DECT por el de *Digital Enhanced Cordless Telecommunications*.

Se estima que en 1998 solamente en Europa existían 6.5 millones de usuarios usando DECT y para el 2005 existirán aproximadamente 65 millones de unidades en uso.

DECT es un estándar de acceso digital vía radio para comunicaciones inalámbricas en una o múltiples celdas. Está basado en la tecnología de acceso TDMA que es la misma que usan los sistemas celulares conocidos pero con la diferencia que los sistemas celulares fueron diseñados para cubrir una amplia área de cobertura con baja densidad de usuarios mientras que el estándar DECT fue optimizado para cobertura local y alta densidad de usuarios.

4.1.2 Configuración de la red y aplicaciones para el estándar DECT

Las tres aplicaciones básicas que han sido difundidas comercialmente y desplegadas con éxito están en la telefonía inalámbrica residencial, sistemas inalámbricos de negocios, y la alternativa de radio para los abonados de la red pública fija, conocido como el Lazo Local de Abonado (RLL) (figura 4.1).

En el caso de *teléfono inalámbrico para el hogar*, un típico sistema DECT consiste de un microteléfono (handset) y una unidad base que se conecta a la estación radio base.

Un *sistema inalámbrico de negocios DECT* está compuesto por una red de estaciones radio base todas conectadas a la PBX a través de un interfaz de radio. Este sistema es parecido a los celulares ya que los usuarios pueden caminar dentro del área de cobertura haciendo y recibiendo llamadas. Las celdas en este caso son muy pequeñas (pico celdas) pero permiten una alta densidad de usuarios. Ejemplos típicos se tiene en los grandes edificios donde se tienen oficinas saturadas de llamadas.

Los *sistemas RLL* están caracterizados por estaciones radio base localizadas en cualquier punto en donde queremos implantar nuestra red y cada usuario es equipado con un transceptor (transmisor-receptor) DECT fijo al cual se conecta cualquier teléfono estándar, se permiten servicios de transmisión de datos, fax en grupo 3, etc. Existe un avance adicional en este campo que consiste en equipar al usuario de un teléfono inalámbrico DECT para proveerle un limitado grado de movilidad en su área local. Esta solución es llamada Generación de telefonía móvil (CTM) *Cordless Terminal Mobility*.

Como el estándar permite comunicaciones de datos, ha creado además la posibilidad de Wireless LANs (Redes de Área Local Inalámbricas), las cuales podrían compartir la capacidad con los sistemas telefónicos inalámbricos.

Una configuración típica DECT con sus diferentes ámbitos de aplicación es la que se observa en la figura 4.1. La incorporación de movilidad requiere la adición de interfaces adicionales y una base de datos y registros de movilidad.

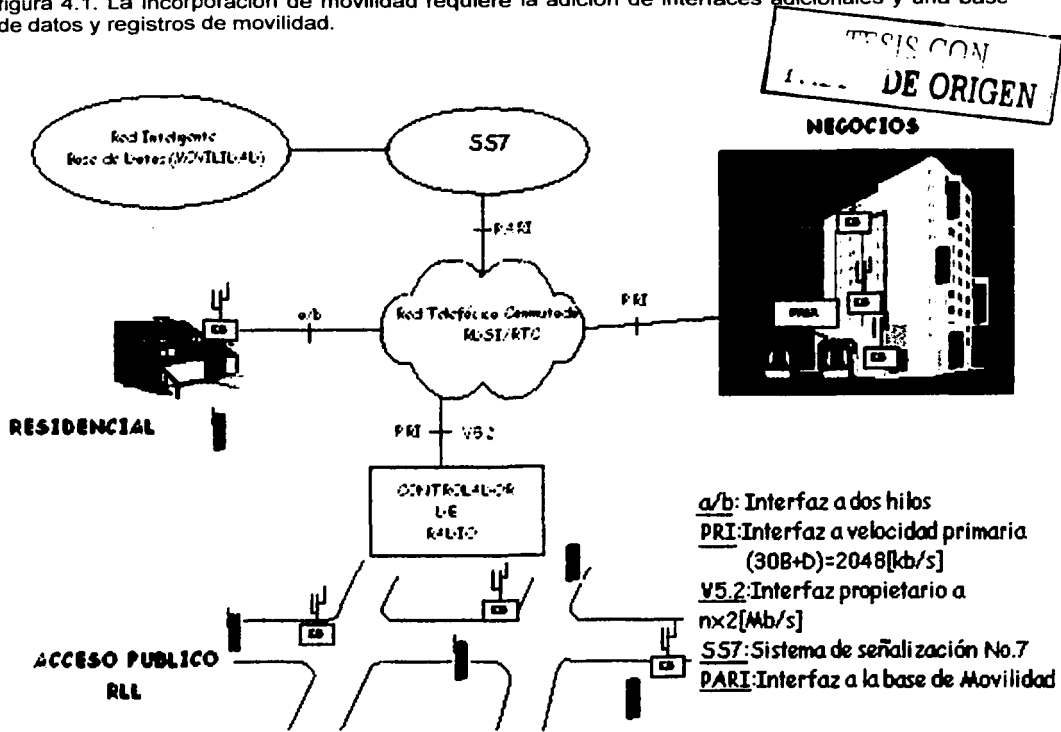


Figura 4.1 Configuración de la red DECT

4.1.3 Arquitectura del Protocolo del estándar DECT

El estándar DECT está dividido en 10 secciones, especifica 4 capas de conectividad más otras importantes funciones. Las cuatro capas corresponden aproximadamente a las capas 1, 2 y 3 del modelo de referencia OSI y son descritas a continuación:

- La *Capa Física* especifica los parámetros de radio tales como frecuencia, temporización y potencia, sincronismo de bit y ranura de tiempo, así como funcionamiento para el transmisor y receptor
- La *Capa de Control de Acceso al Medio* se emplea para el establecimiento de la conexión entre el terminal y las estaciones base. Todas las estaciones base transmiten una señal piloto que permite a los terminales seleccionar una de ellas sin que se requiera una transmisión.
- La *Capa de Control de Enlace de Datos* ofrece enlaces altamente confiables a la capa red. Además de información de señalización, ofrece una gama de servicios alternos que varían

entre la transmisión sencilla, transmisión de voz con codificación y transmisión conmutada de paquetes y de circuitos con varios niveles de protección.

- *La Capa Red* es la que se encarga de la señalización del estándar y especifica el intercambio de mensajes entre las estaciones radio base y los terminales para el establecimiento, mantenimiento y finalización de llamadas. Un grupo de servicios tal como Administración de Movilidad es muy importante ya que ofrece movilidad a los terminales a través del empleo de procedimientos de registro y verificación de los mismos.
- *La sección de Identidad y Direcciones* del estándar permite que cada pieza del equipo manufacturada bajo el estándar tenga su propia identidad. La estructura es altamente flexible y está en capacidad de trabajar con la infraestructura de un sistema huésped, por ejemplo GSM.
- *Características de Seguridad.* Cubren las rutinas para validación de terminales y estación base usando los algoritmos de criptografía.
- *La sección de Codificación de la voz y Transmisión* especifica el tipo de codificación que será empleado. DECT emplea un codec ADPCM a 32 kbps (G721 UIT-T). El control del eco también se considera y especifica que debe estar relacionado con los retardos introducidos por los sistemas de transmisión.
- *El Perfil de Acceso Público (PAP)* cubre en detalle las especificaciones de los equipos que deben ser empleados para acceso a las redes públicas y que puedan ser vistos como el nivel más elevado de estandarización dentro de DECT. La Interfaz Común (DECT-CI) puede ser empleada a discreción por el fabricante.
- *La sección de algoritmos de criptografía* del estándar especifica los detalles de los algoritmos de validación.
- Finalmente, las *Pruebas de Homologación* especifican los procedimientos de prueba que se deben realizar al equipo para cumplir con las regulaciones.

4.1.4 Especificaciones técnicas y descripción funcional del estándar DECT

DECT opera en la banda 1880-1900 MHz. Pero debido a su tendencia a la globalización en América se ha propuesto el rango de 1910- 1930 MHz para que no interfiera con el servicio PCS.

Estructura *Multi-Carrier/ Time Division Multiple Access / Time Division Duplexing (MC/TDMA/TDD)* .- Con el fin de alcanzar una densidad alta de usuarios DECT es capaz de suministrar un gran número de canales en un rango relativamente pequeño (20MHz); utiliza para ello 2 métodos: división en frecuencia y división en el tiempo.

DECT es un sistema *Multi-Portadora (MC)*, el espectro de 20 MHz se divide en 10 portadoras cada una de 1.728MHz, cada portadora a su vez se divide en 24 intervalos de tiempo usando la técnica de *Acceso Múltiple por División de Tiempo (TDMA)*, con 12 intervalos de tiempo usados para recepción y 12 para transmisión de tráfico entre las terminales y la estación base en un arreglo por *División Dúplex de Tiempo (TDD)*. Tal como se observa en la figura 4.2, debido a que un canal de voz con DECT toma un par de intervalos de tiempo y como hay 12 intervalos de tiempo por cada una de las 10 portadoras se tiene un total de 120 canales de voz disponibles para el tráfico. La duración de la trama es de 10 ms. y viaja a una velocidad de 1152 [kb/s]. Cada intervalo de tiempo tiene una capacidad útil para transportar una señal de 32 [kb/s] junto a una tasa de señalización y control de 6.4 [kb/s]. DECT por lo tanto puede ser caracterizado como un *sistema MC/TDMA/TDD*.

La estación base puede transmitir en cualquiera de los 120 canales pues cada canal dúplex funciona independientemente en cualquiera de las 10 portadoras. Además un transceptor se encuentra en capacidad de cursar hasta 12 llamadas simultáneas y se necesita un sólo transceptor por cada portadora.

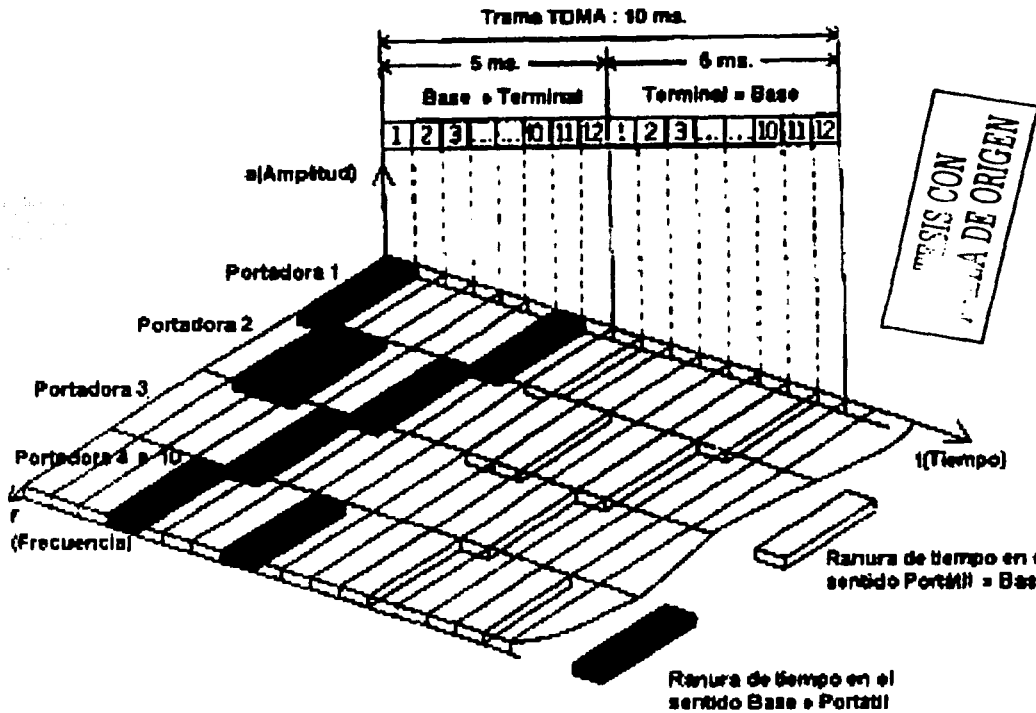


Figura 4.2. Estructura MC/TDMA/TDD en DECT

En la figura 4.3. se muestra en detalle la estructura de la trama DECT. Una trama consiste en 24 intervalos de tiempo, 12 para cada sentido y tiene una duración de 10 ms. Cada intervalo de tiempo transporta 420 bits teniendo en cuenta que los primeros 32 se utilizan con propósito de sincronización y los restantes 388 bits para el usuario y para los datos de control.

320 bits de ellos son utilizados para el transporte de la información y los restantes 68 bits para los canales de señalización, CRC y los canales "X". La duración de cada uno de los intervalos de tiempo es 52.1 ms mayor que la duración de los 420 bits transmitidos. La diferencia en tiempo corresponde al tiempo de guarda y resulta equivalente a la duración de 60 bits.

El campo A transporta los canales de señalización asociados (C) y los canales de difusión (Q). El canal "Q" facilita el servicio a la unidad de abonado de manera que repita la información correspondiente si es necesario. En cada trama se transmiten 48 bits. Los canales "Q" y "C" comparten, por tanto, un total de 4.8 [kb/s]. La capacidad se asigna bajo demanda mientras se garantice un mínimo de capacidad. Los restantes 16 bits del campo "A" se utilizan para proteger los datos con chequeo de redundancia cíclica (CRC), así la tasa neta del canal de control es 6.4 [kb/s] por usuario (incluyendo el proceso CRC) y su máxima velocidad de información de 4.8 [kb/s]. El

campo "B" se utiliza para transportar información de usuario (canal "I"). Ofrece 320 bits por ráfaga o 32 [kb/s].

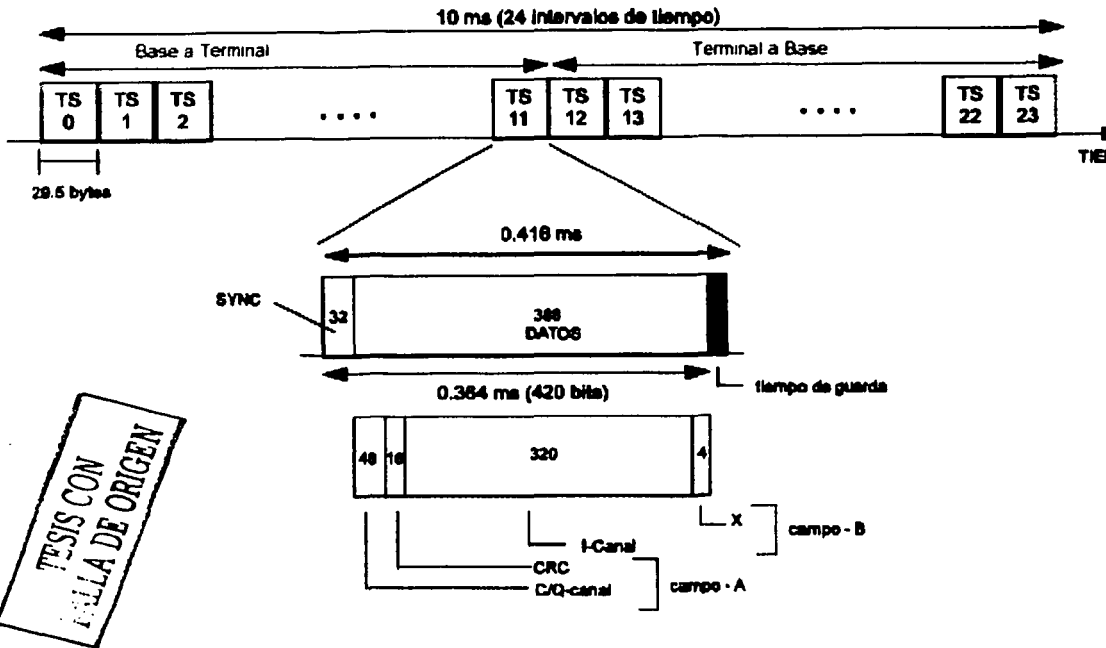


Figura 4.3. Trama DECT

Los cuatro bits "X" se determinan desde alguno de los 320 bits del canal "I". Sin embargo no es la intención proteger el canal "I" de errores de transmisión, sino detectar interferencias parciales con la ráfaga, independientemente del servicio transportado. Esta detección es de vital importancia para permitir a sistemas no sincronizados operar en la misma área geográfica.

Selección Continua Dinámica de Canales (CDSC). A diferencia de los sistemas celulares tradicionales, DECT no requiere planificación de frecuencias, únicamente la planificación de la cobertura de radio. Esta funcionalidad se logra gracias a CDSC mediante un proceso descentralizado. Cada terminal DECT tiene acceso a todos los canales de radio y selecciona el canal disponible de mejor calidad cuando una conexión es requerida. Pero la terminal está continuamente *buscando* el canal que da la mejor señal y conmuta la conexión a ese canal cuando éste es encontrado. Esta característica le permite al mismo canal (misma portadora, mismo intervalo de tiempo) ser reusado para diferentes llamadas en celdas que no se solapan.

Roaming de estaciones base. El seguimiento o roaming sólo es posible si se apoya en algún sistema externo que gestione movilidad. Es decir, la movilidad generalizada entre celdas se consigue bien porque sus estaciones base están conectadas al mismo sistema DECT, o bien por pertenecer a distintos sistemas conectados (mediante interfaz tipo A) a las centrales con software de móviles (por ejemplo, GSM). Se necesitaría tarjeta SIM en portátiles para conseguir la movilidad del usuario con terminales duales DECT-GSM.

En esta línea se están llevando a cabo tareas de definición y normalización del concepto CTM: PARI+ a partir de la tecnología DECT. Mediante CTM se consigue, apoyándose en potentes

protocolos y elementos de Red Inteligente (IN), la movilidad en la red fija sin restricciones, es decir, las comunicaciones personales. En este caso se utilizaría como interfaz a 2[Mb/s] entre la red fija y los controladores de estación base al acceso primario con facilidades de movilidad (Figura 4.1).

Transferencia continua entre canales sin interrupción (Seamless Handover). Cuando se detecta un canal de mejor calidad (enviado por la misma o por diferente estación base) la terminal conmutará a este nuevo canal. Esta capacidad de traspaso se llama Handover y el proceso es el siguiente: la terminal pide la apertura de un segundo canal, que puede ser con otra estación base, cuando ambos canales transportan la misma señal, el terminal cierra el primer canal y utiliza el que se ha establecido recientemente y señaliza al sistema. La conmutación es indetectable por el usuario por lo que se llama *seamless handover*.

Modulación. El transceptor radio DECT utiliza modulación *Gaussian Minimun Shift Keying (GMSK)* con $BT = 0.5$.

La modulación GMSK se deriva de GFSK cuando el *Índice de modulación* (b) = 0.5. El factor BT en cambio corresponde al producto (Ancho de banda del filtro gaussiano*Período de símbolo = $B*T$) ; de esta manera, el producto BT indica el ancho de banda a 3 [dB] del filtro gaussiano para la formación del pulso en relación a la tasa de bit. Mientras el espectro de GMSK llega a ser más compacto con el decremento del valor de BT , la degradación debido a la interferencia inter-símbolo (ISI) aumenta. Así por ejemplo el esquema de modulación del estándar celular GSM (GMSK con $BT = 0.3$) presentaría una mayor degradación por interferencia inter-símbolo que DECT.

Potencia. Debido al pequeño radio de cobertura, las terminales DECT son de baja potencia: la potencia máxima del transmisor es de +24 [dBm] (aproximadamente 250 [mW]) y potencia media de 10 [mW].

Codificación de voz. La codificación de voz en DECT es realizada antes de la transmisión usando un codec ADPCM Código de Modulación Diferencial Adaptativo de Pulsos (Adaptative Differential Pulse Code Modulation) a 32 [kbit/s]. Esta técnica utiliza principios de modulación Delta así como de PCM y se logra una severa reducción en la velocidad de señalización y de la banda de transmisión utilizada. El resultado de la codificación es una calidad de voz mejor a las líneas alámbricas comunes y sistemas celulares ya que la calidad de un circuito ADPCM de 32 [kb/s] es comparable a la de un circuito PCM de 64 [kb/s]. Para una llamada telefónica ordinaria se usa un solo intervalo elemental, pero existen facilidades para que una llamada use varios intervalos: por ejemplo un acceso de tasa binaria básica en ISDN 2B+D(144 [kb/s]) puede usarse hasta cinco intervalos.

Alta capacidad. La tecnología digital de radio TDMA usada en el estándar permite atender a los requerimientos de los sistemas inalámbricos de negocios con PBX donde las densidades de tráfico son altas. DECT está diseñado para soportar sobre los 10,000 [Erlangs/km²] suficiente para 50,000 a 100,000 [usuarios / km²]. Tales densidades son logradas a través del uso de pico celdas con rangos típicos de 30 a 70 metros de radio en interiores y hasta 300 metros en exteriores. Aquello implica el uso de terminales económicas y de baja potencia. Para su aplicación en RLL se puede utilizar antenas direccionales o sectoriales (en vez de omnidireccionales) y conseguir con esta disposición radios de cobertura de hasta 10 [km].

Seguridad. El estándar DECT usa técnicas de encriptado haciendo que las escuchas de radio indebidas sean virtualmente imposibles, así como autenticación en el acceso.

Terminal de usuario inalámbrico. Tiene un tamaño de bolsillo y escaso peso (aproximadamente unos 150 g.). La tecnología de radio usa transmisión discontinua, lo cual reduce el consumo de la batería. Tiempos característicos de la terminal en stanby y plena conversación son de 45 horas y 9 horas respectivamente.

4.2 Personal Handy-phone System (PHS)

Mientras en Europa se trabaja sobre el sistema DECT y su evolución, en Japón ya se está comercializando con bastante éxito un sistema de telecomunicaciones inalámbrico al que se denomina PHS (Personal Handy-phone System).

Como puede identificarse en la figura 4.4, el sistema PHS define algo más que el acceso por radio, al contrario de lo que hace DECT. Este sistema identifica también elementos de red, tales como el Servidor PHS, el HLR (Home Location Register) o registro de posición de base, el CDR (Call Detail Recorder) o base de registros de llamada, el NMS (Network Management System) o sistema de gestión de red y la BC/SDM (Billing Centre/Subscriber Data Management) o centro de explotación.

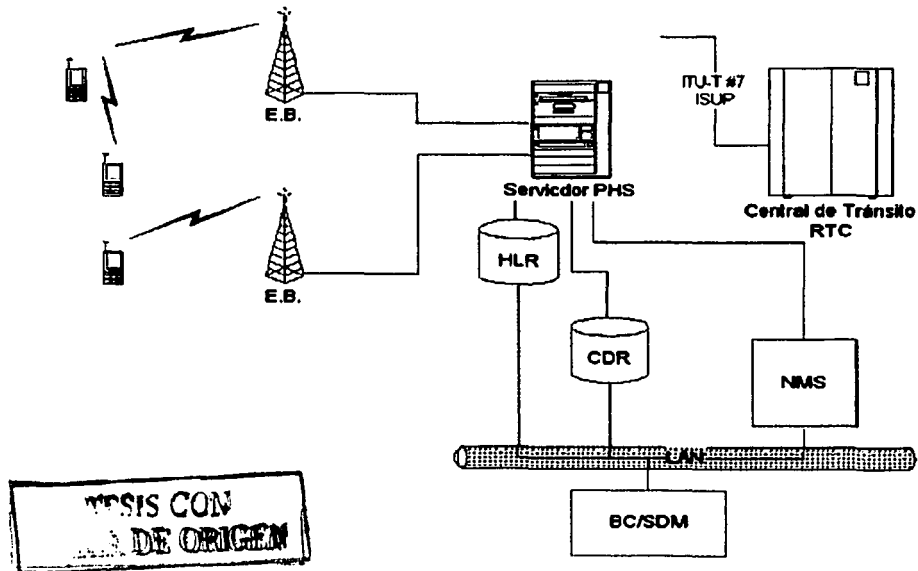


Figura 4.4 Sistema PHS

Este sistema se ha construido sobre la base de tecnologías digitales de acceso por radio y una arquitectura de red que se forma por micro células. PHS utiliza una técnica de asignación dinámica de canales, que unido a técnicas descentralizadas de control de los radiocanales los cuales permiten al operador utilizar las frecuencias de forma flexible y eficiente.

La interfase de aire está totalmente estandarizada por la Asociación de Industrias y Empresas de Radio (ARIB, Association of Radio Industries and Businesses), que es una organización japonesa encargada de estos temas. La interfase de red entre estaciones de base y la red digital está estandarizado por el Comité Técnico de Telecomunicaciones, que es el órgano japonés responsable de los estándares de red. Esta interfaz de red está basada en la RDSI modificado que permitir funciones específicas de PHS, tales como el registro, la autenticación y el handover.

Algunas de las características básicas de este sistema son las siguientes:

- Funciona en la banda de 1898 a 1918 MHz.
- Utiliza la técnica de acceso TDMA/TDD, igual que DECT.
- Alta calidad de voz gracias al uso de la modulación ADPCM (Adaptative Differential Pulse Code Modulation) a 32 kbps.
- Selección dinámica de canal; la terminal PHS decide cuando y hacia donde realiza el handover.
- No es necesario planificar frecuencias, lo que permite una instalación relativamente sencilla.
- Handover automático.

A diferencia del resto de sus competidores, permite la comunicación entre terminales sin necesidad de utilizar el resto de la red.

4.2.1 Arquitectura de la Red PHS

El sistema PHS, es un sistema de acceso inalámbrico con una arquitectura de micro células, usando la banda de frecuencias de 1.9 GHz. En la figura 4.5 se muestra el concepto general de PHS. Podemos ver en este diagrama, que lo podemos aplicar a un sistema de comunicaciones público móvil, o a un lazo local inalámbrico (Wireless Local Loop WLL), esto sustituye a los teléfonos de par de hilos para proveer a los suscriptores con servicios telefónicos, o para un PBX inalámbrico, o un teléfono sin hilos casero, o a los transmisores-receptores que permiten a las PSS comunicarse directamente con cualquier otro. Una interfase común de aire (Common Air Interface CAI) de PHS es estandarizado como RCR STD-28 por la Asociación de la Industria y Negocios de la Radio (Association of Radio Industries & Businesses ARIB). Las interfaces del Usuario-Red y Red-Red (User - Network Interface UNI & Network - Network Interface NNI) están basadas en los estándares ITU-T serie Q.

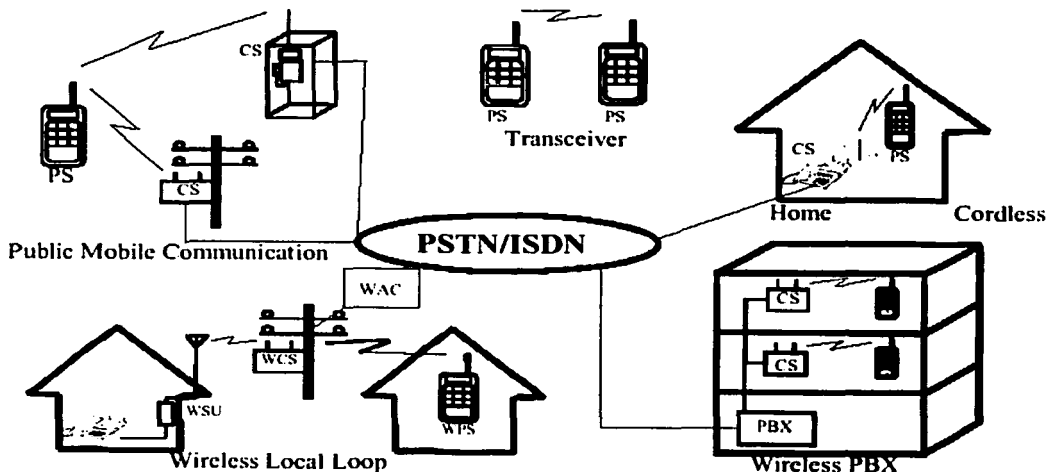


Figura 4.5 Arquitectura de una red básica de PHS



Objetivos generales de PHS. El sistema de comunicación inalámbrica de transmisión y recepción de PHS emplea una arquitectura de micro células, puede tener mayor cobertura por unidad de tráfico en donde existen sistemas de telefonía celular. PHS puede implementar alta calidad de voz equivalente a la que nos proporciona un teléfono alámbrico ya existente a través del empleo de una codificación de voz ADPCM y este puede también proveer alta velocidad de servicios de multimedia.

PHS es un sistema telefónico inalámbrico de la segunda generación propuesto como sucesor a los teléfonos inalámbricos analógicos convencionales. La telefonía inalámbrica analógica convencional se ha aplicado a los sistemas de comunicación privados en reducida escala para uso en los edificios, el hogar u oficinas. PHS no convierte simplemente a digital su sistema inalámbrico de transmisión sino también emplea un sistema inalámbrico de acceso para lograr un alto funcionamiento de tráfico. PHS maneja llamadas entrantes y salientes durante el viaje con las características del registro del handover y de la localización durante una llamada para proporcionar los servicios equivalentes a los de los sistemas existentes de telefonía portátil. Estas características permiten que PHS, funcione como un sistema de teléfono inalámbrico dentro de hogares o de oficinas para así gozar extensamente de servicios móviles públicos de comunicación al aire libre. Aunque el sistema de micro células tiene alto funcionamiento de tráfico, no es aplicable a las comunicaciones móviles de alta velocidad porque el handover es utilizado con mucha frecuencia. PHS se diseña principalmente para las comunicaciones móviles en áreas urbanas a las velocidades que se mueven las personas.

Las comunicaciones móviles convencionales requieren una red exclusiva. Aunque esta red compleja permite la comunicación mientras que viaja a una velocidad, hay mucha complejidad en el registro de la localización, como el handover entre otras características. Además, las comunicaciones móviles convencionales requieren de un sistema de señalización que se delegue para realizar complicadas operaciones de control. Por otra parte, PHS se diseña para ser utilizado y para funcionar directamente en una red RDSI, la cual acomode los teléfonos alámbricos ordinarios, puesto que PHS se considera una extensión del teléfono inalámbrico convencional para el uso casero. El registro de la localización y otras características móviles son controlados usando el sistema de señalización ordinario de RDSI. El control es puesto en ejecución por las características de una Red Inteligente (IN) incorporadas en la red. Este concepto permite establecer una red de comunicaciones móviles muy grande con una inversión inicial pequeña. Las principales características de PHS son:

- Compartir el PS (personal station) por diversas aplicaciones PHS permite comunicaciones públicas al aire libre (outdoor) y comunicaciones privadas de interior, en hogares y oficinas (indoor) con un solo CAI (Common Air Interface). La asignación dinámica del canal de PHS permite compartir una sola banda de frecuencia para una variedad de propósitos. El uso del mismo PS para muchos diversos usos no es solamente una gran ventaja para los usuarios sino que también reduce el costo de fabricación porque el número de los productos PS disminuye.
- Frecuencias compartidas entre múltiples portadoras comunes: otra característica del canal dinámico es asignar funciones permitidas por PHS donde la única banda de frecuencias puede ser compartida por varios operadores (portadoras comunes). Esta característica permite el uso altamente eficiente de frecuencias. Compartir frecuencias elimina la mala distribución del uso de estas debido a la diferencia de escala de operaciones de cada operador o a la diferencia de las áreas de servicio entre operadores. PHS emplea un sistema de tiempo completo Time Division Duplex (TDD) para facilitar la extensión de la banda de frecuencia previniendo que la demanda de tráfico en un futuro aumentará.
- Comunicaciones Multimedia: PHS emplea una codificación de voz mediante una tecnología ADPCM y puede transmitir señales vía modem de 9.8 kbps similar al sistema telefónico alámbrico. PHS también realiza la comunicación de la portadora de 32 kbps vía RDSI. Además, la comunicación de la portadora de 64 kbps está siendo estandarizada por ARIB.

1. Conmutador de paso (Transit Switch TS): Tiene las funciones de conectar y conmutar con otras redes para permitir que las comunicaciones sean realizadas a través del TS.
2. Centro de conmutación PHS (PHS Switching Center): Realiza las funciones de proceso tales como paging, conmutación móvil, y handover además de las funciones de conmutación normales.
3. Punto de Control de Servicio: Utiliza la base de datos para realizar el registro de la localización, la autenticación, y la búsqueda de la localización de la llamada que recibe el PS. El SCP está conectado con el conmutador tarifario a través del Canal de Señalización Común de la red (CCS).
4. Estación Base de las Células (Cell Station CS): Proporciona funciones de comunicaciones inalámbricas digitales a estaciones personales móviles (PS) y la interfase RDSI con la red.
5. Estaciones Personales (PS): La terminal adquirida por el suscriptor tiene la capacidad de realizar comunicaciones inalámbricas digitales con las estaciones base de las células (CS).

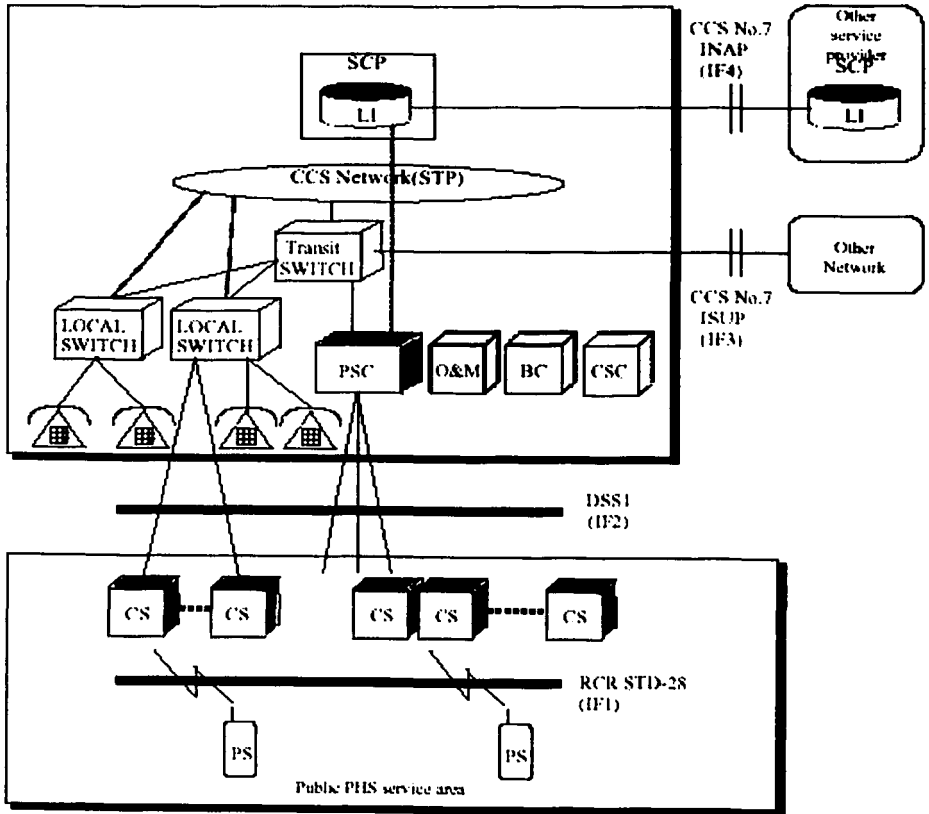


Figura 4.6 Configuración de la red PHS integrada una estructura de red inteligente PSTN / RDSI.

4.2.1.1 Asignación de Funciones

Para implementar un sistema de comunicaciones móviles se requieren funciones de conmutación particulares las cuales no fueron adquiridas por la telefonía alámbrica convencional. Lo siguiente describe estas funciones brevemente.

1. Registro de localización. El registro de localización tiene por objetivo mantener y poner al día la información constantemente la localización de las PS. El propósito de este procesamiento es informar a la base de datos de la red la localización de la estación personal móvil (PS) por adelantado, porque es necesario buscar la estación personal (PS) y avisarle cuando la llamada ha sido terminada.
2. Paging (Sistema de búsqueda de abonados): Un mensaje de la llamada entrante se envía a todas las CSs en el área de paging (de búsqueda de abonados) que tiene un código de área incluido en el PS. Entonces el mensaje de llamada entrante se envía de cada CS a su PSs.
3. Handover. Es el proceso de mantener una llamada, es decir, que el PS se mueve desde una zona de radio a otra usando una CS nueva en la zona visitada. La función del handover es particularmente importante para PHS puesto que utiliza un sistema de micro células.
4. Autenticación. Es la función de evitar que un usuario no autorizado use servicios de comunicación ilegalmente. La autenticación determina si o no un PS ha sido suscrito al servicio solicitado de comunicaciones, cuando la terminal hace una petición de conexión tal como creación de llamada, terminación de llamada, registro de localización, o handover.
5. Roaming. Es un servicio que permite a una PS de PHS obtener una conexión entrante o saliente en otra red de manera semejante como si estuviera en la red original.

4.2.1.2 Interfase de Red

La información detallada se puede enviar y recibir entre el CS y la red a través de un canal de control a un CS el cual debe de ser conectado vía RDSI. Esto proporciona funciones sofisticadas requeridas para implementar servicios de PHS, tales como registro de la localización, paging, handover, autenticación, y roaming así como los servicios suplementarios inherentes a RDSI.

En la las siguientes líneas se describen las que la interfase de RDSI provee.

1. Notificación de número de terminal. Esta función permite enviar y recibir el número de identificación del PS entre la red digital y el CSs al iniciar y terminar una llamada. Es puesta en ejecución señalando los números de PD para llamar y los elementos de información del número al que se ha llamado.
2. Terminación múltiple de llamada en la interfase. Un área de múltiples CSs se utiliza generalmente como la unidad de registro de localización para reducir la carga de tráfico de la transmisión informativa del registro de localización. Por lo tanto es necesario que un lado de la red realice el procesamiento simultáneo de llamada entrante para las múltiples interfaces de una llamada entrante.
3. D-Channel Sharing. Significa realizar la función de control de la llamada en los canales de información (B-channel) de múltiples circuitos físicos con un canal señalización (D-channel) de un solo circuito físico. Esta función reduce el costo de la instalación de CS y del grupo de CS en caso de instalar múltiples circuitos físicos al mismo CS.

4.2.2 Arquitectura del Protocolo

Los elementos representativos de la capa física PHY y la capa MAC del modelo de red que utiliza PHS se describe en los siguientes puntos:

- > Sistema de Micro Células. PHS emplea un sistema de micro células con un área de la célula limitada por la salida de transmisión del CS (Cell Station) de hasta 500 mW y la salida del PS (Personal Station) de 10 mW. El propósito del sistema de micro células es proveer de suficiente tráfico y mantenerlo funcional con pocas bandas de frecuencia aumentando la reutilización de la frecuencias. El empleo del sistema de micro células asegura la calidad de la voz equivalente a la de un sistema telefónico alámbrico usando una capacidad de canal amplia 32 kbps. El sistema de la sección inalámbrica emplea 4 canales (TDMA / TDD), y una tasa de bit física de 384 kbps. Esto asegura satisfactoriamente una calidad de transmisión sin la disposición del ecualizador automático y entonces esto puede reducir los costos de las PS y las CS.
- > Sistema de de múltiple acceso (TDMA / TDD). La trama de transmisión inalámbrica de PHS se estructura por un sistema de 4 canales TDMA. La trama es puesta en ejecución en la comunicación full duplex por el acoplamiento de bajada del CS al PS y el acoplamiento ascendente en dirección opuesta es multiplexada por el sistema de TDD. El primer canal de la trama de TDMA se utiliza como canal de control. Una frecuencia particular es asignada al canal de control de un operador público de una comunicación en particular, y el mismo canal se utiliza en todas CSs y las PSs acomodadas en la red de este operador. En el proceso de llamada de este sistema, la información de control primero se intercambia sobre el canal de control, por lo que uno de los tres canales restantes del tráfico (ranuras de tiempo) se asigna para la comunicación del usuario, entonces, cuándo uno de los canales de tráfico y el canal de frecuencia debe ser utilizado, se especifica sobre el canal de control.

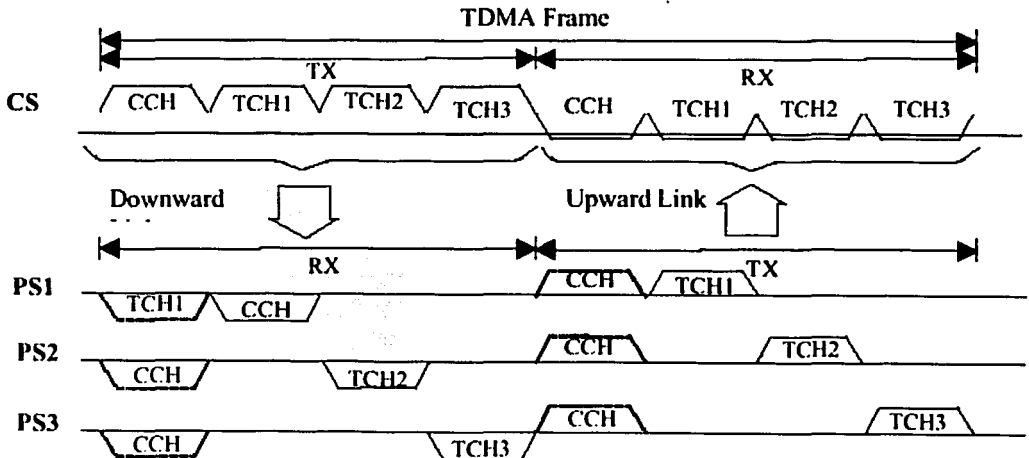
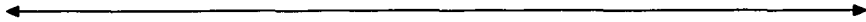


Figura 4.7 Descripción de la trama de transmisión inalámbrica PHS.

240 bits, 625 μ s



Comunicación física de la ranura (ranura de tráfico)

R	SS	PR	Palabra Única	CI	SACCH	Información	CRC	Guarda
4	2	6	16	4	16	160	16	16

Control físico de la ranura

R	SS	PR	Palabra Única	CI	Encabezado	Información	CRC	Guarda
4	2	62	32	4	42 o 70	62 o 34	16	16

Figura 4.8 Formato de la ranura de tiempo (slot-time) de PHS

- Canal de control de frecuencia fija. El control de comunicación funciona como un notificador de llamada entrante o de salida, así mismo entrega la información del abonado, y la autenticación que se requiere antes de comenzar una conversación real en el sistema de comunicación inalámbrico. En PHS, los canales de frecuencia particulares son usados exclusivamente para especificar el control de la comunicación, además las frecuencias son compartidas por todos los CSs y PSs dentro del mismo sistema. Esto permite al PS intercambiar fácilmente la información de control con la CS. Esto elimina la necesidad de buscar para una frecuencia del canal de control cada vez que el PS se mueve desde una célula a otra célula colindante. Esto alternadamente facilita el control del handover y reduce drásticamente el consumo de la batería para esperar una llamada. Compartir la misma banda de frecuencia de diversos operadores, o por diversos tipos de comunicación, ya sean privados o públicos, requiere frecuencias independientes del canal del control para ser asignada a usos particulares.
- Sistema dinámico para la asignación del canal. El canal de control señala un canal de tráfico con menor interferencia después de comprobar las condiciones del canal del tráfico de las ranuras de tiempo (slots time) y frecuencia cuando se le asigna una frecuencia a una ranura de tiempo. Así, el actual canal de tráfico con cada llamada varía la ranura de tiempo y la frecuencia. Este sistema, designa el canal dinámico del sistema, elimina la necesidad de la asignación anterior de las frecuencias usadas por el CS distinto al sistema celular ordinario, permitiendo a las frecuencias ser utilizadas muy eficientemente. Las características de este sistema no solamente es el incremento de la eficiencia sino también la flexibilidad y la capacidad de expansión en el diseño del sistema a través de una nueva célula trasladada en la célula existente para así satisfacer el aumento del tráfico demandado.

TESIS CON
 FALLA DE ORIGEN

4.2.3 Comparación entre DECT y PHS

Es importante mencionar que estas dos tecnologías fueron desarrolladas por culturas totalmente diferentes y es claro que cada una se ha ido deteniendo o ha ido evolucionando dependiendo de las necesidades de los usuarios que todavía las utilizan es por eso que una comparación exhaustiva sería muy difícil hacerla ya que las aplicaciones que se le han dado en los dos diferentes continentes han sido muy diferente, por ejemplo en Europa se utiliza más para transmisión de voz, mientras que en Japón el estándar manejan además de la voz, comunicaciones multimedia, es por eso que ARIB piensa en desarrollar el estándar para la comunicación de la portadora de 64 [kb/s] ; con esto reafirmamos lo que es bien conocido, la tecnología va evolucionando y sigue creciendo o desarrollandose, dependiendo de las necesidades que el usuario tenga y en este caso la "cultura de uso" aplica en estas dos tecnologías tan similares pero tan distintas en su uso. Es por este motivo que la tabla 4.1, menciona y compara solamente algunas de las características técnicas entre estas dos tecnologías.

	DECT	PHS
Desarrollado en:	Europa	Japón
Estandarizado por	ETSI	TTC/RCR
Acceso Multiple	TDMA/TDD	TDMA/TDD
Tasa de transmission de voz	32 [kbit/s]	32 [kbit/s]
Duración del timeslot	417 [µs]	625 [µs]
Duración de la trama	10 [ms]	5 [ms]
Codificación de voz	ADPCM G. 721	ADPCM G. 721
Frecuencia	1880-1900 [MHz]	1895-1918 [MHz]
Espacio entre portadoras	1.728 [MHz]	300[kHz]
Canales/Portadora	12	4
N° de Portadoras	10	53
Velocidad de Transmisión	1152 [kb/s]	384 [kb/s]
Técnica de Modulación	GFSK	QFSK
Potencia	10 [mW]	10 [mW]
Handover	Si	Si

Tabla 4.1. Características principales de los sistemas de telefonía sin hilos DECT yPHS.

TESIS CON
FALLA DE ORIGEN

5. Redes de Área Personal Inalámbricas (WPANs)

La tecnología inalámbrica de comunicación que utiliza radio frecuencia RF ha emergido, eso podrá permitir que los dispositivos se conecten fácilmente con poca intervención de los usuarios a través de la interfase aérea. Esta tecnología llamada Redes Inalámbricas de Área Personal (WPANs) difiere de otras tecnologías inalámbricas y alámbricas tradicionales LAN. El objetivo primordial de las WPANs en el mercado de consumo, es su utilidad en la conectividad de aparatos portátiles o de uso cotidianos. Las WPANs fueron diseñadas de tal suerte que son muy económicas, compactas en tamaño, fáciles de usar y tener muy bajo consumo de energía. Sin embargo, independientemente de la tecnología que se utilice, las WPANs ofrecen un nuevo concepto en las comunicaciones con el llamado Personal Operating Space (POS). Contrario a la infraestructura de las redes que son instaladas, el POS es un espacio de cobertura pequeña alrededor del individuo en donde la comunicación ocurre en una red de tipo Ad Hoc. El POS se conecta al usuario y tiene la capacidad de moverse junto con él. Con este dispositivo se tiene la opción de comunicarse con otros dispositivos que tengan la capacidad de comunicación POS.

Los subsistemas de comunicación que provee la capacidad en las WPANs en un dispositivo personal puede no interferir con la función primaria de dicho dispositivo o con la parte que éste tenga como función en una red, por ejemplo un asistente personal digital (PDA) con capacidades para pertenecer a las WPANs podrá verse y funcionar como un PDA común sin la necesidad de cambiar su configuración o software de uso. En general, los subsistemas de las WPANs en los dispositivos personales en donde se utilizan no afectan la forma y uso que traen dichos dispositivos ya de fabrica y además se tiene un impacto mínimo en el costo y en la potencia que consume este tipo de dispositivo.

Las WPANs manejan una cobertura típica de 10 [m] hasta algunos cientos de metros y un número limitado de dispositivos que pueden comunicarse entre sí. Las WPANs son capaces de ser creadas espontáneamente según la necesidad que tenga el usuario, requiere poca intervención del usuario para poder montar la red e interoperar con redes establecidas o que se encuentren aisladas. Las WPANs proveen modos de operación confiables y seguros, permitiendo a grupos de dispositivos personales privados conectarse fácilmente mientras que se limita la conectividad a la red a dispositivos ajenos o de poca confiabilidad.

Por ultimo, pero no menos importante, por la naturaleza de las WPANs así como las WLANs opera en una banda de frecuencias de uso libre (la banda ICM), por esta razón necesitan convivir con otras tecnologías de radio que utilizan estas mismas frecuencias.

En este capitulo se hizo una recopilación de algunas actividades representativas de las WPANs, como son:

- Estándares
- Descripción de los sistemas y protocolos utilizados en algunas tecnologías.
- Aplicaciones que se permiten en este tipo de redes, bajo las siguientes tecnologías: Los grupos de trabajo de IEEE802.15, Bluetooth, Home RF, Air 5 e IrDA.

5.1 GRUPO DE TRABAJO 802.15

En Marzo de 1998, se creó el grupo de estudio WPAN (Wireless Personal Area Networks) en la IEEE. Más tarde, en Mayo, se forma el grupo de interés especial (SIG) de Bluetooth. Un año después, en Mayo de 1999, el grupo de estudio WPAN pasa a ser IEEE 802.15, el grupo de trabajo WPAN.

A diferencia de los estándares de redes inalámbricas como IEEE 802.11b y Bluetooth, que se han venido centrando en la calidad de servicio y en la seguridad, IEEE 802.15 intenta dar respuesta a las limitaciones de complejidad, tamaño, costos y consumo de energía en las WPANs.

5. Redes de Área Personal Inalámbricas (WPANs)

El Grupo de Trabajo 802.15 de IEEE está definiendo nuevos estándares aplicables en dispositivos inalámbricos de bajo costo y corto alcance dentro de redes de área personal inalámbricas. El grupo de trabajo está intentando superar tres retos primarios: equilibrar los costos con la frecuencia utilizada y el ancho de banda, asegurar la coexistencia con otros dispositivos inalámbricos y proporcionar seguridad en entornos de roaming.

El estándar 802.15 define las especificaciones relativas al nivel físico y al de control de acceso al medio (MAC) para los dispositivos inalámbricos de una WPAN. El nivel físico transmite en uno de varios canales en el rango de los 2.4 [GHz], mientras que las especificaciones MAC definen el formato de los mensajes y el procedimiento para el establecimiento seguro de la red.

Una WPAN está formada por un grupo dinámico de no más de 255 dispositivos que se comunican entre sí en distancias no superiores a 10 m. A diferencia de las LAN inalámbricas, sólo los dispositivos situados dentro de esta limitada área participan en la red; es decir, no está definida la conexión online con dispositivos externos.

Durante el proceso de creación de la WPAN, se selecciona a uno de los dispositivos para que actúe como controlador de todas las comunicaciones que se establezcan. Para ello, el controlador difunde una señal que permite al resto de dispositivos sincronizarse entre sí, asignándoles además ranuras de tiempo, después de verificarlas. Los datos se pueden enviar a toda la WPAN usando su dirección de destino, o a un dispositivo en concreto.

En busca de una mayor flexibilidad, el grupo de trabajo 802.15 está definiendo diferentes versiones dirigidas específicamente a dispositivos con requerimientos diferentes. Así, 802.15.3 se centra en niveles físico y MAC de baja potencia y una tasa de transmisión alta (alrededor de 55 [Mb/s]), mientras que 802.15.4 soporta niveles físico y MAC de muy baja potencia y baja tasa de transmisión (alrededor de 250 [kb/s]). Es por eso, que los procesos de estandarización buscan minimizar costos, complejidad y tamaño. Estos principios básicos están presentes en los criterios de selección para la gestión de la potencia, algoritmos de seguridad y QoS. Además, las limitadas distancias de cobertura de las WPAN suponen de por sí costos y potencia de transmisión reducidos. Como los requerimientos de seguridad de las redes 802.15 son diferentes de los de las redes estáticas debido a su naturaleza dinámica, el grupo de trabajo está tratando de especificar soluciones de clave pública para autenticación e intercambio de claves. Una vez que los dispositivos han sido autenticados, cada dispositivo de la WPAN comparte claves de protección de grupo (simétricas) para encriptar los datos y garantizar su integridad. Este mecanismo de autenticación también puede utilizarse para crear una subred segura entre dos dispositivos. Otra cuestión que todavía ocupa al grupo de trabajo es la coexistencia entre diferentes dispositivos 802.15, y entre éstos con otros de distinto tipo. Se trata de asegurar la no interferencia con otros equipos basados en estándares que también utilizan las frecuencias de 2.4 [GHz].

Los dispositivos 802.15 crean redes inalámbricas de forma dinámica para proporcionar comunicaciones seguras en distancias cortas. A continuación se describe como un dispositivo es anexo a una red WPAN 802.15 y posteriormente se muestran los grupos que componen al estándar.

- Los dispositivos determinan qué dispositivo es el más indicado para actuar como servidor.
- Una vez autenticados los dispositivos por el servidor, solicitan unirse a la PAN.
- El servidor establece ranuras de tiempo para cada dispositivo y distribuye las claves de protección de la información de la WPAN.
- Los dispositivos deben transmitir los datos protegidos durante sus ranuras de tiempo.
- Opcionalmente, dos dispositivos pueden crear su propia subred segura.

5. Redes de Área Personal Inalámbricas (WPANs)

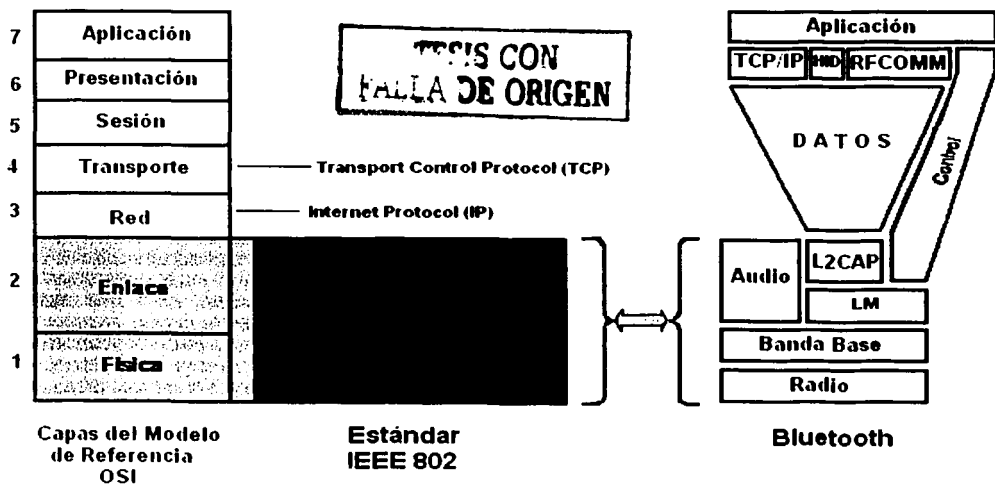
5.1.1 Grupo de trabajo 1 (TG1) WPAN/Bluetooth

El nuevo estándar de IEEE 802.15.1-2002 es un recurso adicional para los que pongan los dispositivos de Bluetooth en ejecución. Los principales puntos de 802.15.1 se muestran en el siguiente párrafo el cual nos proporciona más información:

Las capas de transporte más bajas (L2CAP, LMP, banda base, y radio) de la tecnología inalámbrica de Bluetooth son definidos. Bluetooth es una especificación de la industria para la conectividad en RF de corto alcance para los dispositivos personales móviles.

IEEE ha repasado y ha proporcionado una adaptación al estándar de Bluetooth Specification v1.1 Foundation (L2CAP, LMP, y banda base) y de la capa PHY (radio). También se especifica una cláusula SAPs el cual incluye la interfaz LLC/MAC para la norma ISO/IEC 8802-2 LLC. También se especifica un anexo normativo que proporciona un Protocol Implementation Conformance Statement (PICS).

En la Figura 5.1 se observa la compatibilidad que se ésta llevando a cabo entre las capas MAC y PHY de los estándares 802 y Bluetooth.



5.1 Figura Compatibilidad entre 802.15.1 y Bluetooth.

5.1.2 Grupo de trabajo 2 (TG2) - Coexistencia

Dentro del grupo IEEE 802.15, se ha iniciado un proyecto de estandarización llamado 802.15.2, el cual hace una recomendación general para la coexistencia dentro de las bandas no licenciadas. Este proyecto es, no obstante, sólo una recomendación, y queda por parte de los miembros de la industria la decisión de acatarla.

Las causas del problema radican en que las tecnologías en cuestión están ambas en constante desarrollo, y en un eminente peligro de extinción. La velocidad a la que se mueve el mercado de las tecnologías inalámbricas es increíble, y la competencia por ser el primero lleva a los desarrolladores a quitar importancia al problema de la coexistencia.

5. Redes de Área Personal Inalámbricas (WPANs)

Aunque el grupo de trabajo de la IEEE siempre ha tenido como una de sus primeras metas, lograr que 802.15 y 802.11 puedan coexistir, en el mundo comercial se sigue un camino distinto. El Bluetooth SIG, aparte de intentar satisfacer las especificaciones de la IEEE, debe lograr un desarrollo rápido del estándar, por la presión que tiene de todas sus compañías patrocinantes.

Lograr una coexistencia con 802.11b es complicado y largo, por los diferentes modelos de capas de 802.11 y Bluetooth. Debido al acelerado proceso de desarrollo de Bluetooth, se ha llegado a un punto en que los dispositivos que se encuentran actualmente en el mercado interfieren los unos con los otros hasta el punto de su inutilización.

Aunque los dispositivos Bluetooth lidian constantemente por el espectro de frecuencias con los dispositivos de WLANs como 802.11 y HomeRF, éstas dos tecnologías no están dirigidas a los mismos mercados. Otra tecnología que comparte algunos casos de uso con Bluetooth es IrDA, un estándar para comunicaciones vía infrarroja entre dispositivos el cual explicaremos más adelante.

5.1.3 Grupo de trabajo 3 – Alta tasa de transmisión en WPANs

El grupo de trabajo de la IEEE 802.15.3 tiene como misión primordial la creación del estándar para una red WPAN, que provea soluciones a este tipo de redes con rangos de alcance, de bajo costo, bajo consumo de potencia con el objetivo de tener aplicaciones multimedia y digitalización de imágenes. El estándar IEEE 802.15.3 también conocido como Red Inalámbrica de Área Personal mayores a los 55 Mb/s con esto proporciona alta definición en señales de video y alta fidelidad en señales de audio opera en la banda de frecuencias no licenciada de los 2.4 GHz. Es por eso la importancia de este grupo que se encargó de crear el estándar y la creación de la especificación de las capas MAC y PHY para las High-rate WPANs.

Comparado con las diferentes tecnologías de redes de área local inalámbricas, como IEEE 802.11a,b, e HiperLAN, la tecnología que maneja Redes de Área Personal de alta velocidad 802.15.3 posee rasgos específicos que son solicitados por la mayoría de los dispositivos de comunicación portátiles y por sus aplicaciones.

Algunas características del estándar IEEE 802.15.3 para redes inalámbricas de área personal de alta velocidad son las siguientes:

- Habilidad para formar conexiones Ad hoc que soporte QoS para tráfico de servicios multimedia.
- Fácil coexistencia con redes ya existentes.
- Ahorro de energía debido a que tiene un administrador avanzado de potencia.
- Bajo costo y optimización de la implementación de la capa MAC y PHY para rangos de comunicación cortos (menores a 10 m).
- Soporta tasas de transmisión altas, arriba de los 55 [Mb/s], generalmente utilizados en transmisiones donde se necesita calidad en el audio y video.

En la figura 5.2 se muestra la estructura del frame de IEEE 802.15.3, el cual consiste en un intervalo de señalización de la red, un periodo de acceso para la conexión CAP y un periodo libre para la conexión CFP reservado para garantizar las ranuras de tiempo o time slots (GTS). El límite entre la CAP y el GTS se ajusta dinámicamente.

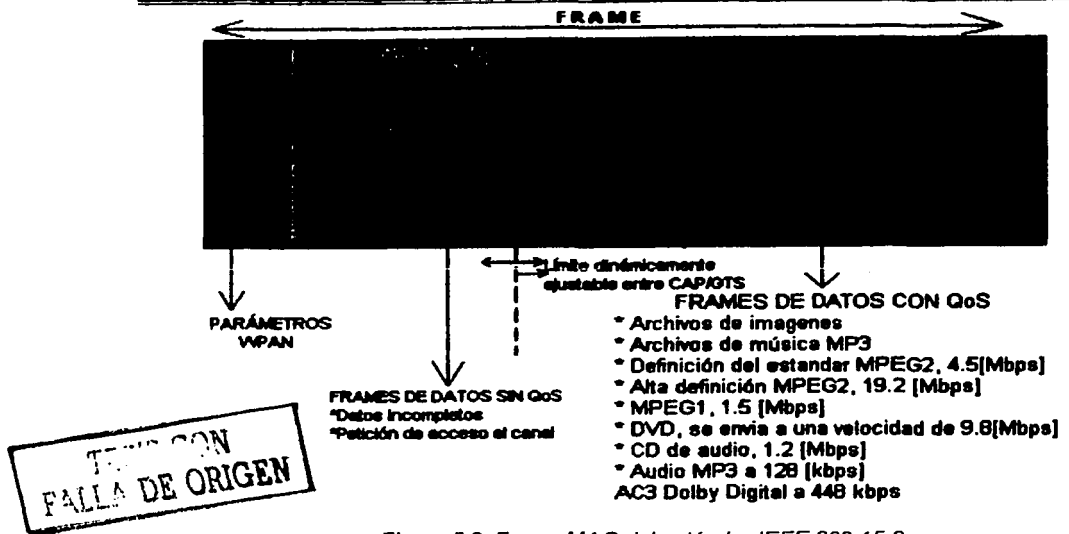


Figura 5.2. Frame MAC del estándar IEEE 802.15.3.

El intervalo de señalización de la red ISR se transmite al comienzo de cada frame, y es el encargado de transporta parámetros específicos de la WPAN, incluyendo la administración de la potencia, e información de dispositivos nuevos que quisieran unirse a la red. El periodo CAP (contention accesse period) se reserva para tramas de datos que no tengan que ver con calidad de servicio como puede ser, una pequeña cantidad de datos incompletos o solicitudes de acceso a canales requeridos por algún dispositivo en la red. El resto de la duración del frame es reservado para el GTS (guaranteed time spot), el cual transporta tramas de datos 0con disposiciones específicas de calidad de servicio. El tipo de datos transmitidos en el GTS pueden ser desde imágenes pesadas o archivos de música hasta transmisión de audio de alta calidad o de video de alta definición. Finalmente, el administrador de la potencia es uno de los distintivos principales del protocolo MAC de 802.15.3, el cual es designado para bajar la corriente que se drena mientras el dispositivo esta siendo conectado a la WPAN. En el modo de ahorro de potencia, las disposiciones de calidad de servicio siempre se mantienen.

La capa física de 802.15.3 opera en la banda de frecuencia entre los 2.4 [GHz] y los 2.4835 [GHz] y se diseño para manejar tasas de transmisión desde los 11 hasta los 55 [Mb/s]. Los sistemas de 802.15.3 utilizan la tasa de símbolo de 11 Mbaudios, como la que se utiliza en los sistemas de 802.11b. Para operar a esta tasa de símbolo se especificaron cinco formatos de modulación:

- Modulación QPSK sin codificación para transmitir a 22 [Mb/s]
- Modulación QPSK con codificación trellis
- Modulación 16-QAM para transmitir a 11 [Mb/s]
- Modulación 32-QAM para transmitir a 33 [Mb/s]
- Modulación 64-QAM para transmitir a 55 [Mb/s]

Finalmente, dependiendo de la capacidad de los dispositivos, para tasas de transmisión de 33-55 [Mb/s] que usan los esquemas de modulación 16,32, 64 QAM la información se codifica por medio de un código trellis 2D de ocho estados. Las señales de 802.15.3 utilizan un ancho de banda de 15 [MHz], las cuales toman en cuenta cuatro canales designados de subida en la banda de 2.4 [GHz].

5. Redes de Área Personal Inalámbricas (WPANs)

5.1.4 Grupo de trabajo 4 - WPAN Baja Tasa de Transmisión

En diciembre del 2000 dos grupos de estandarización, ZigBee del grupo de trabajo de Home RF, y el grupo de trabajo 15 de la IEEE 802 combinaron esfuerzos para cubrir las necesidades que se tenía de una red inalámbrica en entornos caseros y de tipo industrial, que utilizara poca potencia en los dispositivos que la conformaran y que además su implementación fuera muy económica. En diciembre del mismo año el Comité para Nuevos Estándares (NesCom) de la IEEE oficialmente sancionó un nuevo grupo de trabajo para empezar a desarrollar un estándar para Redes Inalámbricas de Área Personal de baja transmisión (LR-WPAN), el cual se llamó 802.15.4. Lo innovador de este grupo de trabajo fue que proveyó un estándar con muy poca complejidad, costo y potencia para la transmisión de datos de baja velocidad muy bajos y dispositivos portátiles o móviles. El alcance del Grupo de Trabajo 4 las especificaciones de las capas física (PHY) y de la capa de control de acceso al medio (MAC).

El estándar IEEE 802.15.4 tiene una variedad de aplicaciones como son: control y monitoreo en la industria, seguridad pública, localización de desastres naturales; monitoreo preciso en la agricultura de pesticidas, herbicidas y niveles de pH. Sin embargo una de las más grande oportunidades que tendrá IEEE 802.15.4 será la automatización y el manejo de una red en el interior de un hogar u oficina.

El proyecto IEEE 802 divide la capa de enlace LLC (Data Link Layer) en dos subcapas. La capa LLC se estandarizo en 802.2 y es común entre los estándares de 802 como el 802.3, 802.11, y 802.15.1, mientras que la subcapa MAC tiene ver más con el hardware y puede variar dependiendo de la implementación de la capa física. En la figura 5.3 se muestra como 802.15.4 entra dentro de la Organización Internacional de Estandarización ISO y se compara su conexión con el modelo de referencia OSI.

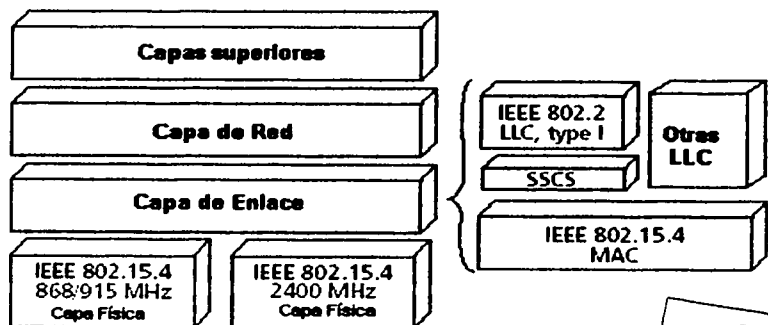


Figura 5.3. Capas de IEEE 802.15.4.

Los lineamientos de la capa MAC de 802.15.4 son asociación, reconocimiento del reparto del frame, mecanismo de acceso al canal, validación del frame, garantizar la administración de las ranuras de tiempo.

La estructura del frame de MAC es muy flexible ya que se pueden acomodar las necesidades de diferentes aplicaciones y topologías de red mientras que se este manteniendo un protocolo simple. El formato general del frame MAC se muestra en la figura. El frame MAC se le conoce también como MPDU (MAC protocol data unit), el cual se compone del encabezado MAC MHR (MAC header), unidad de datos de servicios MAC MSDU (MAC service data unit), y el MAC footer MFR. El primer campo del MHR, es el campo de control del frame, el cual indica el tipo de frame MAC cuando empieza la transmisión, especifica el formato de los campos de direcciones y CRCG-SVG

5. Redes de Área Personal Inalámbricas (WPANs)

controla el reconocimiento. Se puede decir, que el campo de control del frame especifica como es el resto del frame y que es lo que contiene.

El tamaño del campo de direcciones puede variar entre 0 y 20 bytes. Por instantes, el frame de datos puede contener información de la fuente e información del destinatario, mientras que el frame de reconocimiento que se regresa o que se responde no contenga información de la direcciones. Por otra parte, el frame de señalización puede contener solamente información de la direcciones de la fuente. Esta estructura tan flexible ayuda a incrementar la eficiencia del protocolo para seguir manteniendo los paquetes.

El tamaño del campo de información puede variar; sin embargo el tamaño del frame MAC completo, no puede exceder los 127 bytes. Los datos contenidos en el campo de información dependen del tipo de frame. La capa MAC de IEEE 802.15.4 maneja cuatro tipos diferentes de frame:

- Frame de señalización
- Frame de datos
- Frame de reconocimiento
- Frame de control de la MAC

Solo los frames de señalización y de datos contienen información enviada por capas superiores; los frame de reconocimiento y de control de la MAC se originan en la MAC y son usados para realizar comunicaciones punto a punto dentro de la misma MAC.

Otros campos del frame MAC son el número de secuencia y el frame de chequeo de secuencia FCS. El número de secuencia en el encabezado del frame MAC acopla el frame de reconocimiento con la transmisión previa. La transmisión se considera exitosa solo cuando el frame de reconocimiento contiene el mismo numero de secuencia que el frame que se transmitió previamente. El FCS ayuda a verificar la integridad del frame MAC y se utiliza un chequeo de redundancia cíclico de 16 bits 16-bits CRC (cyclic redundancy check) avalado por la ITU-T.

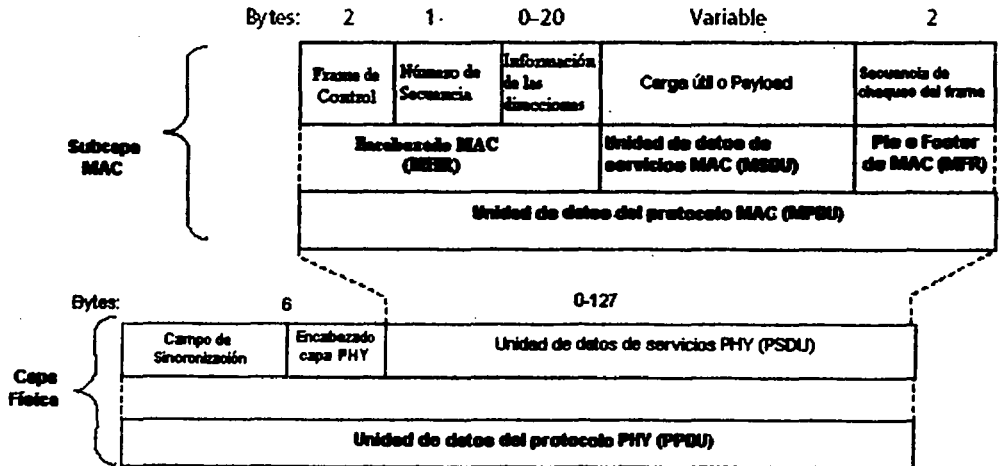


Figura 5.4. Formato general del Frame MAC.

TESIS CON
FALLA DE ORIGEN

5. Redes de Área Personal Inalámbricas (WPANs)

El estándar IEEE 802.15.4 tiene tres niveles de seguridad:

- Sin seguridad de ningún tipo (para anunciar algunas aplicaciones)
- Listas de control de acceso (seguridad sin criptografía)
- Seguridad primaria simétrica (utiliza AES-128)

Para minimizar los costos de los dispositivos que no requieran seguridad, el método principal de distribución no se especifica en el estándar pero se puede incluir in capa superiores para aplicaciones específicas.

IEEE 802.15.4 ofrece dos opciones de la capa física que se pueden combinar con la capa MAC para permitir aplicaciones de banda ancha en la red. Ambas opciones de la capa física utilizan métodos de secuencia directa de espectro esparcido (DSSS) ya que resulta muy barata su implementación. La diferencia fundamental entre las dos capas físicas es la banda de frecuencia que utilizan. La capa física 2.4 [GHz] especifica operaciones en la banda de frecuencia no licenciada de los 2.4 [GHz] (ISM), mientras que la capa física 868/915 [MHz] opera en la banda de los 869 [MHz] en Europa y en la banda ISM de los 915 [MHz] en los Estados Unidos.

Otra característica que distingue a la capa física del estándar 802.15.4 y es de gran interés para las redes y sus tipos de aplicaciones, es la velocidad de transmisión y tipo de modulación que se utiliza para lograr dicha velocidad. En la tabla 1 siguiente se hacen referencia algunas características que tienen que ver con la velocidad de transmisión y la técnica de modulación.

Capa Física	Banda de Frecuencia	Parámetros de los Datos		
		Velocidad de Bit (kb/s)	Velocidad de símbolo (kbauds)	Tipo de Modulación
868/915	868.0–868.6 MHz	20	20	BPSK
MHz PHY	902.0–928.0 MHz	40	40	BPSK
2.4 GHz PHY	2.4–2.4835 GHz	250	62.5	O-QPSK

Tabla 1. Parámetros de la Modulación.

802.15.4 maneja 27 canales de frecuencia disponibles en los tres tipos de banda, como se muestra en la figura 5.5. La capa física de los 868/915 [MHz] soporta un canal simple entre los 868.0 y los 868.6 [MHz], y diez canales entre los 902.0 y los 928.0 [MHz], con una separación de 2 [MHz]; en la banda de los 2.4 [GHz] se manejan 16 canales entres los 2.4 y los 2.4835 [MHz] con un espaciado de 5 [MHz] entre cada canal, como se muestra la figura 5.6.

Número del Canal	Frecuencia central del canal (MHz)
$k = 0$	868.3
$k = 1, 2, \dots, 10$	$906 + 2(k - 1)$
$k = 11, 12, \dots, 26$	$2405 + 5(k - 11)$

TESIS CON
FALLA DE ORIGEN

Figura 5.5. Canales de frecuencia IEEE 802.15.4.

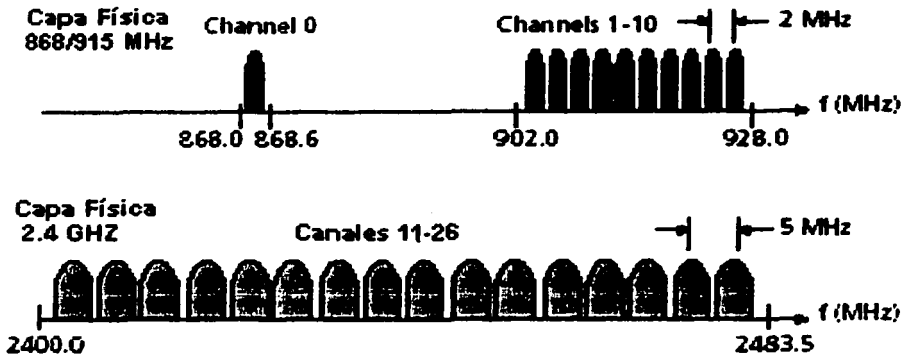


Figura 5.6. Estructura del canal IEEE 802.15.4.

Finalmente podemos observar en la figura 5.6 como 802.15 sus diferentes variantes subsisten entre sí, teniendo cada una sus propias características y observándose además la relación de las capas con cada una de las variantes.

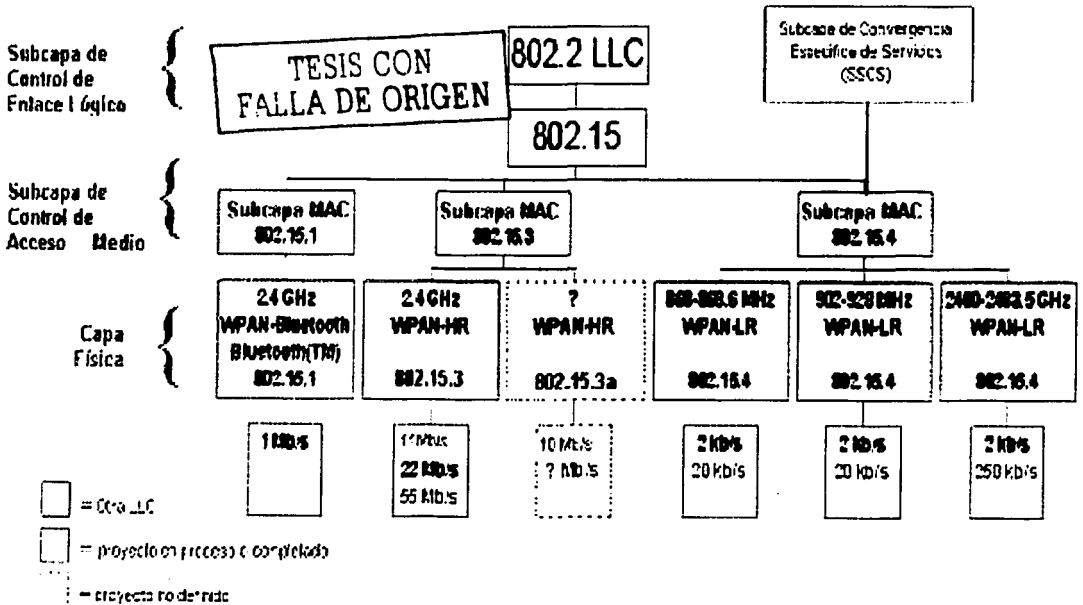


Figura 5.6. Relación entre las subcapas MAC de 802.15 y la capa física.

5. Redes de Área Personal Inalámbricas (WPANs)

5.2 Estándar Bluetooth

Bluetooth define un estándar global de comunicación inalámbrica, que posibilita la transmisión de voz y datos entre diferentes equipos mediante un enlace por radiofrecuencia. Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos
- Eliminar cables y conectores entre éstos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales

La tecnología Bluetooth comprende hardware, software y requerimientos de interoperabilidad, por lo que para su desarrollo ha sido necesaria la participación de los principales fabricantes de los sectores de las telecomunicaciones y la informática, tales como: Ericsson, Nokia, Toshiba, IBM e Intel. Posteriormente se han ido incorporando muchas más compañías, y se prevé que próximamente lo hagan también empresas de sectores tan variados como: automatización industrial, maquinaria, entretenimiento, fabricantes de juguetes, electrodomésticos, etc., con lo que en poco tiempo se nos presentará un panorama de total conectividad de nuestros aparatos tanto en casa como en el trabajo.

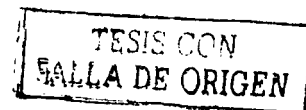
En 1994 Ericsson inició un estudio para investigar la viabilidad de una interfase vía radio, de bajo costo y bajo consumo, para la interconexión entre teléfonos móviles y otros accesorios con la intención de eliminar cables entre aparatos. El estudio partía de un largo proyecto que investigaba sobre unos multicomunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance, llamado *MC link*. Conforme éste proyecto avanzaba se fue viendo claro que éste tipo de enlace podía ser utilizado ampliamente en un gran número de aplicaciones, ya que tenía como principal virtud el que se basaba en un chip de radio relativamente económico.

A comienzos de 1997, según avanzaba el proyecto MC link, Ericsson fue despertando el interés de otros fabricantes de equipos portátiles. En seguida se vio claramente que para que el sistema tuviera éxito, un gran número de equipos deberían estar equipados con ésta tecnología. Esto fue lo que originó a principios de 1998, la creación de un grupo de interés especial (SIG), formado por 5 promotores que fueron: Ericsson, Nokia, IBM, Toshiba e Intel. La idea era lograr un conjunto adecuado de áreas de negocio, dos líderes del mercado de las telecomunicaciones, dos líderes del mercado de las PCS portátiles y un líder de la fabricación de chips. El propósito principal del consorcio fue y es, el establecer un estándar para la *interfase* aérea junto con su software de control, con el fin de asegurar la interoperabilidad de los equipos entre los diversos fabricantes.

El primer objetivo para los productos Bluetooth de primera generación eran los entornos de la gente de negocios que viaja frecuentemente. Por lo que se debería pensar en integrar el chip de radio Bluetooth en equipos como: PCS portátiles, teléfonos móviles, PDAs y auriculares. Esto originaba una serie de cuestiones previas que deberían solucionarse tales como:

- El sistema debería operar en todo el mundo.
- El emisor de radio deberá consumir poca energía, ya que debe integrarse en equipos alimentados por baterías.
- La conexión deberá soportar voz y datos, y por lo tanto aplicaciones multimedia.

Para poder operar en todo el mundo es necesaria una banda de frecuencia abierta a cualquier sistema de radio independientemente del lugar del planeta donde nos encontremos. Sólo la banda ISM (médico-científica internacional) de 2.4 [GHz] cumple con éste requisito, con rangos que van de los 2400 [MHz] a los 2500 [MHz], y solo con algunas restricciones en países como Francia, España y Japón.



5.2.1 Modelos de uso de Bluetooth

El Grupo de Interés Especial de Bluetooth (SIG) ha desarrollado la Versión 1.0 de la Especificación de Bluetooth que permite el desarrollo de servicios interactivos y aplicaciones sobre módulos de radio y protocolos de comunicación de datos. Además, el SIG ha identificado varios modelos de uso a partir de los cuales resulta sencillo descubrir cómo funcionan y se asocian los distintos protocolos de la pila de Bluetooth.

El grupo de Interés Especial de Bluetooth ha identificado modelos de uso, que se identifican con determinados perfiles y que a continuación se exponen. Los perfiles definen los protocolos y las características de protocolo que soporta cada modelo de uso en particular. Los cuatro perfiles son el perfil de acceso genérico (GAP), el perfil de puerto serie, el perfil de aplicación de descubrimiento del servicio (SDAP) y el perfil de intercambio de objetos genérico (GOEP).

Los modelos de uso nos facilitan una visión de las posibilidades que la tecnología Bluetooth nos ofrece, a continuación mostramos hacemos mención de dichos modelos.

- **Transferencia de ficheros.** Consiste en transferir objetos de datos desde un aparato (por ejemplo, una PC, un teléfono inteligente o un PDA) hacia otro.
- **Bridge de Internet.** En este modelo de uso, el teléfono móvil o el módem inalámbrico actúan como módem para el PC, proporcionando conexión a la red y capacidades de fax sin necesidad de conexiones físicas al PC.
- **Acceso a LAN.** En este modelo de uso, varias terminales de datos (DTs) usan un Punto de Acceso a la LAN (LAP) como conexión inalámbrica a la red de área local (LAN). Una vez conectados, los DTs operan como si estuvieran conectados a la LAN mediante una conexión de red. EL DT puede acceder a todos los servicios ofrecidos por la LAN.
- **Sincronización** El modelo de uso de sincronización proporciona una sincronización aparato a aparato (teléfono, PDA, ordenador, etc.) de la información personal PIM (Personal Information Management), típicamente libro de teléfonos, mensajes, notas, calendario, etc. Para transferir información de tareas, calendario y tarjetas de negocio y para su procesado por ordenadores, teléfonos celulares y PDAs que utilizan un protocolo y un formato común, se requiere sincronización.
- **Tres funciones en un teléfono.** Los handsets telefónicos construidos con este perfil se pueden conectar de tres formas diferentes:
 - Los teléfonos pueden actuar como teléfonos inalámbricos conectados a la red telefónica pública conmutada (PSTN) y pagando la cuota de una línea fija. Este escenario incluye realizar llamadas por medio de una estación base de voz, hacer llamadas directas entre dos terminales mediante la estación base y acceso a servicios suplementarios proporcionados por la red externa.
 - Los teléfonos se pueden conectar directamente con otros teléfonos con el propósito de actuar como "walkie-talkie" o una extensión del handset. En lo referente a este escenario de intercomunicación, no hay que pagar por la conexión.
 - El teléfono puede actuar como un teléfono celular conectado a la infraestructura celular, siendo necesario pagar por el uso del sistema celular.
- **Headset final.** El headset puede ser conectado inalámbricamente con el propósito de actuar como un interfaz de entrada-salida audio de un aparato remoto. El headset incrementa la libertad de movimiento del usuario mientras mantiene la privacidad de la llamada. Un ejemplo común es un escenario en el que un headset se usa con un handset celular, o con un handset inalámbrico, o con un ordenador personal, ahora bien, siempre para entrada y salida de audio.

5.2.2 Arquitectura de la Red

Si un equipo se encuentra dentro del radio de cobertura de otro, éstos pueden establecer conexión entre ellos. En principio sólo son necesarias un par de unidades con las mismas características de hardware para establecer un enlace. Dos o más unidades Bluetooth que comparten un mismo canal forman una piconet. Para regular el tráfico en el canal, una de las unidades participantes se convertirá en maestra, pero por definición, la unidad que establece la piconet asume éste papel y todos los demás serán esclavos. Los participantes podrían intercambiar los papeles si una unidad esclava quisiera asumir el papel de maestra. Sin embargo sólo puede haber un maestro en la piconet al mismo tiempo.

Cada unidad de la piconet utiliza su identidad maestra y reloj nativo para seguir en el canal de salto. Cuando se establece la conexión, se añade un ajuste de reloj a la propia frecuencia de reloj nativa de la unidad esclava para poder sincronizarse con el reloj nativo del maestro. El reloj nativo mantiene siempre constante su frecuencia, sin embargo los ajustes producidos por las unidades esclavas para sincronizarse con el maestro, sólo son válidos mientras dura la conexión.

Bluetooth maneja dos tipos de enlaces, representados en la Figura 5.7:

- **SCO (Síncrono Orientado a la Conexión):** es un enlace simétrico punto a punto entre un maestro y un solo esclavo en la Piconet. El maestro mantiene el enlace de SCO usando ranuras reservadas (tipo conmutación de circuitos). El enlace de SCO lleva principalmente información de voz. El maestro puede mantener hasta tres enlaces simultáneos de SCO mientras los esclavos pueden mantener dos o tres enlaces de SCO. Los paquetes de SCO no se retransmiten nunca. Los paquetes de SCO se usan para transmisiones de 64 [kb/s].
- **ACL (Asíncrono Sin Conexión):** es un enlace punto a multipunto entre el maestro y todos los esclavos que participan en la Piconet. En las ranuras no reservadas para los enlaces de SCO, el maestro puede establecer un enlace ACL con cualquier esclavo, inclusive el esclavo ya comprometido en un enlace SCO (tipo de conmutación de paquetes). Sólo puede existir un único enlace ACL. Para la mayoría de los paquetes de ACL, se aplica retransmisión de paquetes.



Figura 5.7 Tipos de enlaces físicos.

Como ya hemos comentado, las unidades maestras controlan el tráfico del canal, por lo que estas tienen la capacidad para reservar ranuras en los enlaces **SCO**. Para los enlaces **ACL**, se utiliza un esquema de sondeo. A un esclavo sólo se le permite enviar una ranura a un maestro cuando ésta se ha dirigido por su dirección MAC (medio de control de acceso) en el procedimiento de la ranura maestro-esclavo. Éste tipo de ranura implica un sondeo por parte del esclavo, por lo que, en un tráfico normal de paquetes, este es enviado a una urna del esclavo automáticamente. Si la información del esclavo no está disponible, el maestro puede utilizar un paquete de sondeo para

5. Redes de Área Personal Inalámbricas (WPANs)

sondear al esclavo explícitamente. Los paquetes de sondeo consisten únicamente en uno de acceso y otro de cabecera. Este esquema de sondeo central elimina las colisiones entre las transmisiones de los esclavos.

Las unidades que se encuentran en el mismo radio de cobertura pueden establecer potencialmente comunicaciones entre ellas. Sin embargo, sólo aquellas unidades que realmente quieran intercambiar información comparten un mismo canal creando la piconet. Este hecho permite que se creen varias piconets en áreas de cobertura superpuestas. A un grupo de piconets se le llama scatternet, la cual se muestra en la figura 5.8. El rendimiento, en conjunto e individualmente de los usuarios de una scatternet es mayor que el que tiene cada usuario cuando participa en un mismo canal de 1 [MHz]. Además, estadísticamente se obtienen ganancias por multiplexión y rechazo de canales. Debido a que individualmente cada piconet tiene un salto de frecuencia diferente, diferentes piconets pueden usar simultáneamente diferentes canales de salto.

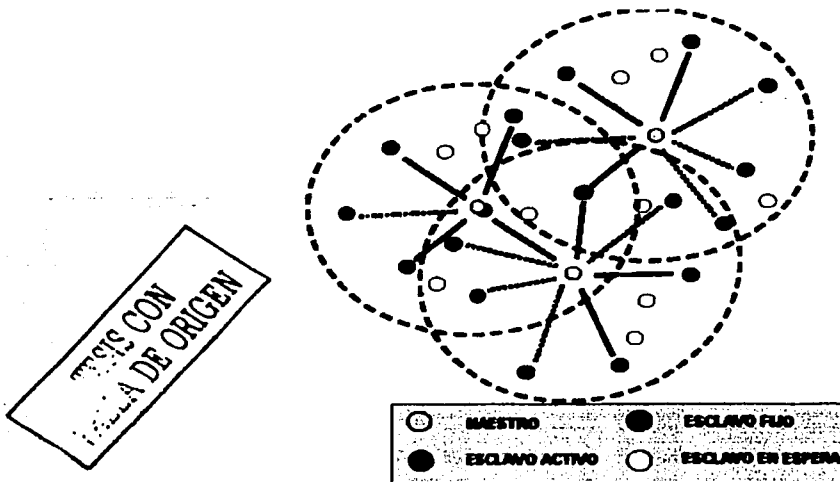


Figura 5.8 Scatternet.

5.2.3 Pila de Protocolos de Bluetooth

El objetivo final de la especificación es permitir que las aplicaciones, escritas de manera que cumplen la especificación, funcionen unas con otras. Para conseguir este funcionamiento interactivo, las aplicaciones parejas (es decir, el correspondiente cliente y servidor de la aplicación) en aparatos remotos deben funcionar sobre pilas idénticas de protocolos. La siguiente lista de protocolos es un ejemplo de una pila de protocolos (de arriba a abajo) que soporta la aplicación de intercambio de tarjetas de negocios:

vCard - OBEX - RFCOMM - L2CAP - Banda Base

Esta pila de protocolos contiene tanto un convenio para la representación de objetos internos, vCard, como protocolos de transporte 'sobre el aire', que serían el resto de la pila. Diferentes aplicaciones pueden funcionar sobre diferentes pilas de protocolos. Sin embargo, cada una de estas pilas de protocolos usa un enlace de datos y una capa física común. La figura 5.9 muestra la pila completa de protocolos de Bluetooth tal como se define en la especificación. En la parte superior de la pila están las aplicaciones que soportan los modelos de uso de Bluetooth. No todas las aplicaciones hacen uso de todos los protocolos que se muestran en la figura 5.9, sino que

5. Redes de Área Personal Inalámbricas (WPANS)

funcionan sobre uno o más cortes verticales de esta pila de protocolos. La figura 5.9 muestra la relación en la cual cada protocolo utiliza los servicios de los demás protocolos cuando hay que transferir los datos, y también las relaciones con el resto de protocolos.

TESIS CON FALLA DE ORIGEN

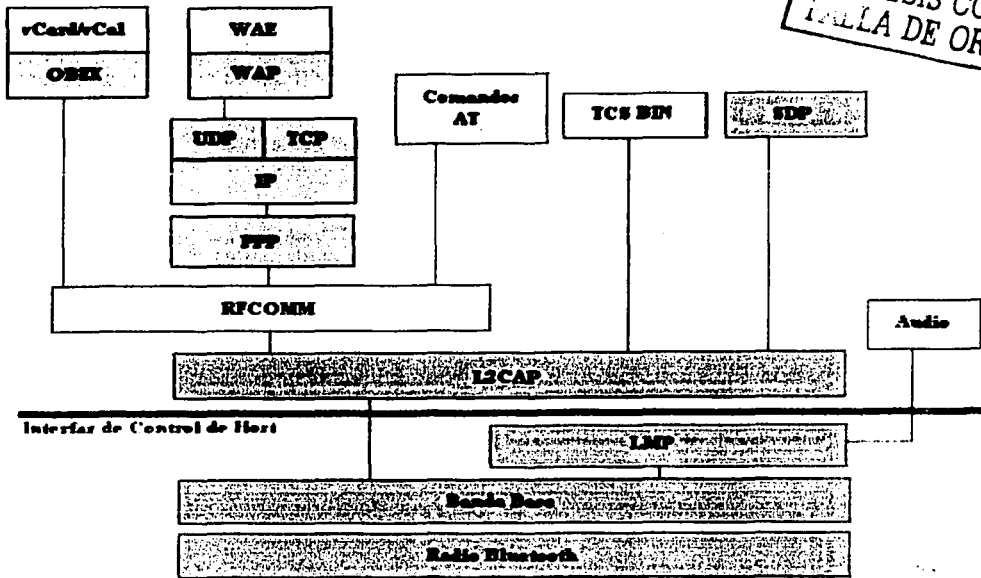


Figura 5.9 Pila de Protocolos de Bluetooth.

Como se ve en la figura 5.9, la pila completa de Bluetooth comprende protocolos específicos de Bluetooth como el LMP y el L2CAP, y protocolos no específicos de Bluetooth como el OBEX (Protocolo de Intercambio de Objetos) y el UDP (Protocolo de Datagramas de Usuario). En el diseño de la pila completa de protocolos, el principio fundamental ha sido maximizar la reutilización de los protocolos existentes para diferentes propósitos en las capas superiores. La reutilización de protocolos también ayuda a adaptar las aplicaciones existentes a trabajar con la tecnología Bluetooth y a asegurar el funcionamiento fluido y la interoperatividad de estas aplicaciones. La especificación está abierta, de modo que hace posible que los vendedores libremente implementen sus propios protocolos de aplicación sobre los protocolos específicos de Bluetooth, permitiendo así el desarrollo de un gran número de nuevas aplicaciones que fomentan el desarrollo de las capacidades de la tecnología Bluetooth.

La pila de protocolos de Bluetooth puede dividirse en cuatro capas de acuerdo a su propósito. Los protocolos que pertenecen a cada capa se distribuyen del siguiente modo:

Capa de Protocolo	Protocolos en la pila
Protocolos esenciales de Bluetooth	Banda base, LMP, L2CAP, SDP
Protocolo de reemplazamiento de cable	RFCOMM[5]
Protocolos de control de telefonía	TCS Binario, Órdenes AT
Protocolos adoptados	PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE

Tabla 2 Los protocolos y las capas en la pila de protocolos de Bluetooth.

5. Redes de Área Personal Inalámbricas (WPANs)

Además de las capas de protocolos de la tabla, la especificación también define un Interfaz Controlador del Host (HCI), que envía órdenes al controlador banda base y al administrador de enlace, y proporciona acceso al estado del hardware y a los registros de control. En la figura 5.9, el HCI se sitúa debajo de L2CAP pero esa posición no es obligatoria, ya que el HCI puede situarse encima del L2CAP.

Los protocolos esenciales de Bluetooth comprenden exclusivamente protocolos de Bluetooth desarrollados por el Bluetooth SIG. Los protocolos RFCOMM y TCS Binario han sido también desarrollados por el Bluetooth SIG pero están basados en la ETSI TS 07.10 y la recomendación ITU Q.931, respectivamente. Los protocolos esenciales de Bluetooth (más Bluetooth radio) son requeridos por la mayoría de los aparatos de Bluetooth, mientras que el resto de protocolos solo se utilizan cuando son necesarios.

Como se mencionó antes, la especificación Bluetooth está abierta, de forma que pueden adaptarse protocolos adicionales (como por ejemplo HTTP, FTP, etc.) en la parte superior de los protocolos de transporte específicos de Bluetooth o en la parte superior de los protocolos orientados a las aplicaciones mostrados en la figura 5.9.

5.2.3.1 Capa de Radio de Bluetooth

La capa radio de Bluetooth es la capa más baja definida en la especificación de Bluetooth. Define los requisitos del aparato transceptor que opera en la banda de ISM 2.4 [GHz].

El canal radio de Bluetooth utiliza espectro ensanchado mediante salto de frecuencia de 79 saltos separados 1 [MHz], comenzando en 2.402 [GHz] y terminando en 2.480 [GHz], como se muestra en la Figura 5.10. En unos pocos países (como España y Francia) esta banda de la frecuencia es (temporalmente) menor, y utilizan un sistema de 23 saltos. Para cumplir las regulaciones de banda de cada país en ambos sistemas se deja una banda de guardia en los límites superior e inferior de la banda.

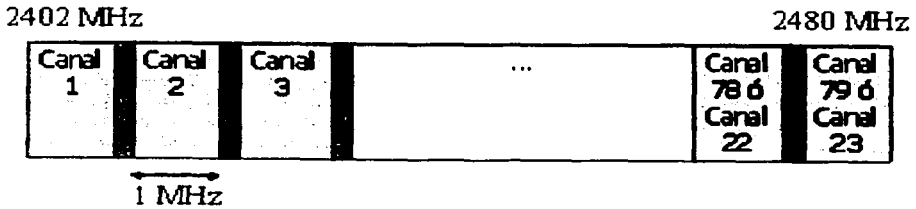


Figura 5.10 Bandas de Frecuencia.

El transmisor que se utiliza en Bluetooth tiene las siguientes características:

Clases de Potencia: cada aparato se clasifica dentro de 3 clases de potencia,

- Clase de Potencia 1: diseñada para aparatos de cobertura amplia (~100 [m]), con una potencia máxima de salida de 20 [dBm],
- Clase de Potencia 2: para aparatos de cobertura normal (~10 [m]), con una potencia máxima de salida de 4 [dBm],
- Clase del Potencia 3: para aparatos de corto alcance (~10 [cm]), con una potencia máxima de salida de 0 [dBm].

El interfaz radio de Bluetooth está basado en una antena de potencia nominal de 0 [dBm]. Cada aparato puede variar opcionalmente su potencia transmitida.

5. Redes de Área Personal Inalámbricas (WPANs)

La modulación que usa Bluetooth es GFSK (Gaussian Frequency Shift Keying, Modulación de Frecuencia Gaussiana) donde un 1 binario es representado por una desviación positiva de la frecuencia y un 0 binario por una desviación negativa de la frecuencia. El índice de la modulación debe estar entre 0.28 y 0.35.

5.2.3.2 Banda Base

La Banda Base es la capa física de Bluetooth. Maneja los canales y los enlaces físicos además de otros servicios como la corrección de errores, la selección del salto y la seguridad de Bluetooth. La capa Banda Base se encuentra encima de la capa de radio de Bluetooth en la pila de protocolos de Bluetooth. El protocolo de Banda Base funciona como un Controlador de Enlace, que trabaja con el administrador del enlace para llevar a cabo las rutinas del nivel de enlace como conexión del enlace y el control de potencia. La Banda Base controla también enlaces asíncronos y enlaces síncronos, maneja paquetes y hace paginación y búsqueda para el acceso averiguando los aparatos de Bluetooth que se encuentran dentro del área. El transceptor de Banda Base aplica un esquema de división de tiempo dúplex (TDD), de forma que alternativamente transmite y recibe. Por lo tanto, aparte de los diferentes saltos de frecuencia (división de frecuencia), el tiempo es también discreto.

Como vimos en la capa radio, Bluetooth opera en la banda ISM de 2.4 [GHz]. En México, EEUU y Europa, está disponible un ancho de banda de más o menos 83.5 [MHz] en el cual se definen 79 canales de RF espaciados 1 [MHz], dependiendo del país. En España y la Francia, está disponible una banda más pequeña con 23 canales de RF espaciados 1 [MHz]. En la Tabla 3 se especifica exactamente la distribución de los canales en cada uno de los países.

País	Rango de Frecuencia	Canales de RF	
Europa ,México y EEUU	2400-2483.5 [MHz]	$f = 2402 + k$ [MHz]	$k = 0, \dots, 78.$
Japón	2471-2497 [MHz]	$f = 2473 + k$ [MHz]	$k = 0, \dots, 22.$
España	2445-2475 [MHz]	$f = 2449 + k$ [MHz]	$k = 0, \dots, 22.$
Francia	2446.5-2.483.5 [MHz]	$f = 2454 + k$ [MHz]	$k = 0, \dots, 22.$

Tabla 3 El canal físico de Bluetooth

* Excepto España y Francia.

El canal es representado por una secuencia pseudo-aleatoria para el salto de frecuencia a través de los 79 o 23 canales de RF. La secuencia de salto es única para cada Piconet y está determinada por la dirección del aparato Bluetooth maestro. Igualmente, la fase de la secuencia de salto está determinada por el reloj Bluetooth del maestro. El canal se divide en ranuras de tiempo (slots), donde cada ranura corresponde con una frecuencia RF de salto. Saltos consecutivos corresponden a diferentes frecuencias RF de salto.

El canal se divide en ranuras de tiempo de 625 μ s., que se numeran según el reloj del maestro de la Piconet de Bluetooth.

Se usa un esquema TDD donde maestro y esclavo transmiten alternativamente. El maestro comenzará su transmisión en ranuras numeradas solo como pares, y el esclavo comenzará su transmisión en ranuras numeradas como impares sólo. El comienzo del paquete se alineará con el comienzo de la ranura.

TESIS CON
FALLA DE ORIGEN

Todas estas características mencionadas aparecen reflejadas en la Figura 5.11.

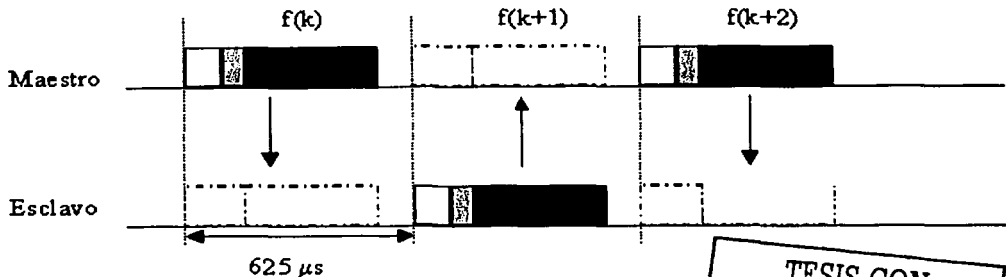


Figura 5.11 Transmisión de paquetes.

Bluetooth tiene cinco canales lógicos que pueden ser utilizados para transferir tipos diferentes de información. En el nivel de enlace se usan los canales LC (Canal de Control) y LM (Administrador del Enlace), mientras que para llevar información de usuario se usan los canales UA (Asíncrona), UI (Isosíncrona) y US (Síncrona).

Se pueden asignar cuatro tipos posibles de direcciones a unidades Bluetooth:

- **BD_ADDR**, Bluetooth Device Address, Dirección del Dispositivo Bluetooth. A cada transceptor de Bluetooth se le asigna una dirección de 48 bits única.
- **AM_ADDR**, Active Member Address, Dirección de Miembro Activo. Es un número de 3 bits. Es sólo válido cuando el esclavo está activo en el canal. También es llamada a veces la dirección de MAC de una unidad de Bluetooth.
- **PM_ADDR**, Parked Member Address, Dirección de Miembro Estacionado. Es una dirección de 8 bits que distingue a los esclavos estacionados, y es sólo válida cuando el esclavo está estacionado.
- **AR_ADDR**, Dirección de Petición de Acceso. La usa el esclavo estacionado para determinar la ranura esclavo-a-maestro en la ventana de acceso que le permite mandar mensajes de petición de acceso. Es sólo válido cuando el esclavo está estacionado y no es necesariamente única.

5.3.3.3 Formato del Frame de Bluetooth

Todos los datos en la Piconet se transmiten en paquetes. Hay trece tipos de paquetes diferentes definidos para la capa Banda Base del sistema Bluetooth. Todas las capas superiores usan estos paquetes para componer la PDU nivel superior. Los paquetes son:

- **ID, NULL, POLL, FHS, DM1**, que se definen tanto para enlaces SCO como para enlaces ACL.
- **DH1, AUX1, DM3, DH3, DM5, DH5** se definen solo para enlaces ACL.
- **HV1, HV2, HV3, DV** se definen solo para enlaces SCO.

Los paquetes tienen un formato específico, representado en la Figura 5.12. Así, cada paquete se compone de 3 entidades, el código del acceso (72 bits), el encabezado (54 bits), y la carga útil (de 0 a 2774 bits).

5. Redes de Área Personal Inalámbricas (WPANS)



Figura 5.12 Formato del Frame de Bluetooth.

Las tres entidades referidas son las siguientes:

- Código de acceso, Figura 5.13: se usa para la sincronización, la compensación del offset, la paginación y la búsqueda. Hay tres tipos diferentes de código de Acceso:
 1. Código de Acceso al Canal (CAC), identifica una única Piconet,
 2. Código de Acceso de Aparato (DAC), se usa para paginar y responder, y
 3. Código de Acceso de Búsqueda (IAC), se usa para la búsqueda.

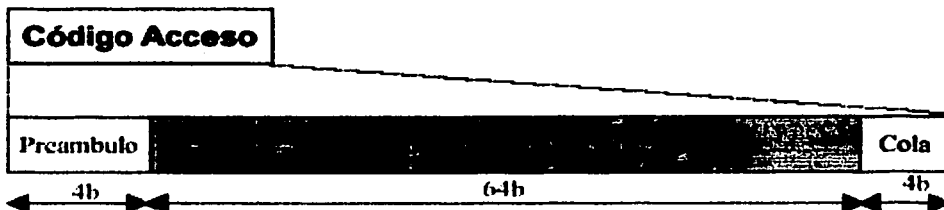


Figura 5.13 Código de Acceso del Frame de Bluetooth.

- Encabezado, Figura 5.14: contiene información para el reconocimiento de paquete, numeración de paquetes para la reordenación de paquetes fuera de orden, el control de flujo, la dirección de esclavo y control de errores de la cabecera.

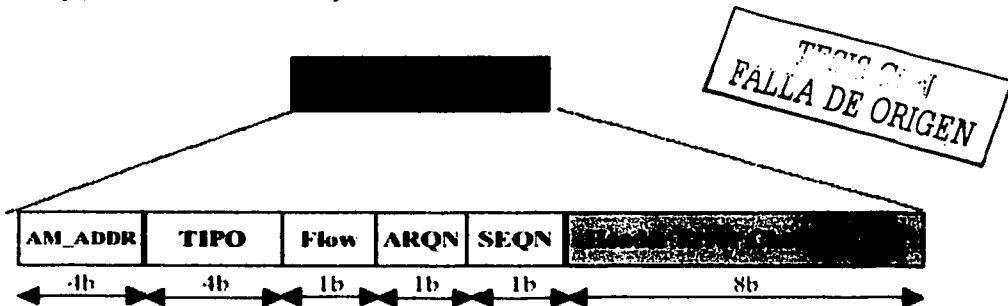


Figura 5.14 Encabezado del Frame de Bluetooth.

- Carga útil Figura 5.15 puede contener campo de voz, campo de datos o ambos. Si tiene un campo de datos, la carga útil contendrá también una cabecera de la carga útil.

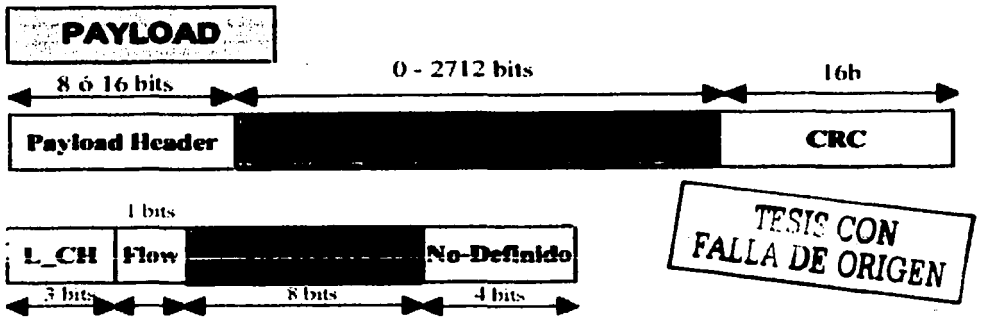


Figura 5.15. Carga Útil del Frame de Bluetooth

5.3 HomeRF

HomeRF se pensó para el mercado de las redes domésticas. Por esto, decidieron incorporar una serie de servicios. Por una parte soporta flujo de datos entre dispositivos de los denominados "streaming media", es decir de audio/video como puedan ser reproductores de video y DVD, cadenas de sonido, o Webpads. Para este servicio utiliza un tráfico con prioridades que describiremos más adelante.

Por otra parte soporta dispositivos de transmisión de voz en tiempo real, como teléfonos inalámbricos, y todo esto interaccionando con dispositivos informáticos tradicionales (PC, impresoras...). Para ello utiliza un protocolo denominado SWAP (Shared Wireless Access Protocol), que soporta TDMA (Time Division Multiple Access) para servicios de voz en tiempo real, y CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance) para servicios de datos de alta velocidad. Las empresas propietarias de HomeRF constituyen el denominado HRFWG (Home RF Working Group), y son un grupo con muchas de las empresas más importantes en el sector tecnológico.

5.3.1 Arquitectura del sistema HomeRF

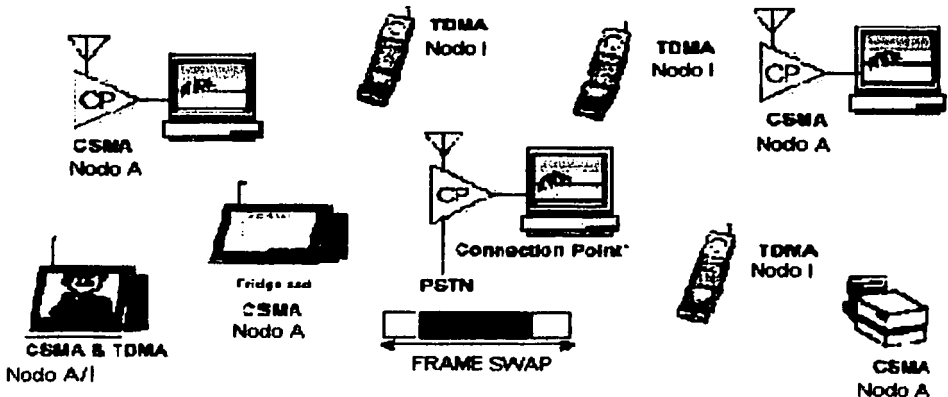


Figura 5.16 Acceso a diferentes dispositivos a la red HomeRF.

5. Redes de Área Personal Inalámbricas (WPANs)

HomeRF no admite funcionamiento ad hoc, sino que tiene una estructura predeterminada (red gestionada). Los dispositivos conectados pueden interactuar con la red de dos maneras diferentes, con Punto de Conexión o sin él. En el primer caso cada dispositivo interactúa directamente con la red. Entre tales dispositivos encontramos productos de automatización doméstica como interruptores de la luz.

El segundo caso proporciona comunicación de voz interactiva y crítica controlada por un Punto de Conexión (acceso a Internet, teléfonos inalámbricos). Este Punto de Conexión podría ser un PC que conecte con los dispositivos a través de interfaces como Universal Serial Bus (USB) una tarjeta o módem interfaz HomeRF. El Punto de Conexión también podría utilizarse para dar soporte al suministro de potencia para prolongar la vida de las pilas de los dispositivos programando el modo standby.

En cuanto a la comunicación entre los dispositivos para el intercambio de información existen dos posibilidades:

- Modo de funcionamiento: Host/Client es el utilizado en transmisión de voz, aplicaciones internet centralizadas, y en algunas aplicaciones más.
- Modo Peer to peer es el más eficiente para compartir recursos, por ejemplo un DVD o una impresora.

HomeRF soporta ambos modos simultáneamente.

La especificación HomeRF 1.0 contemplaba llegar a 1 [Mb/s] utilizando modulación 2 FSK y hasta 2 [Mb/s] utilizando 4 FSK, pero ante la ausencia de un espacio de mercado claro en precios y prestaciones, los miembros de la HomeRF presionaron el año pasado a la FCC norteamericana para que les concediera más ancho de banda en la banda espectral donde se mueven, los 2.4 [GHz].

Para la compresión de datos utiliza el algoritmo LZRW3-A. Para la encriptación de los datos utiliza el algoritmo "blowfish", un algoritmo con un trillón de códigos similar al GSM A5 pero más robusto, con una clave de 128 bits.

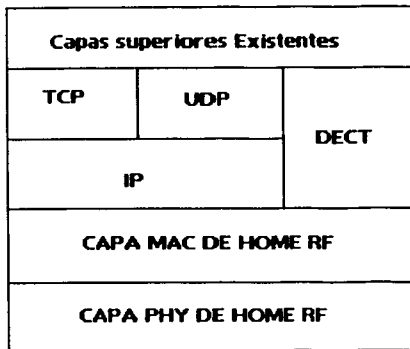
Blowfish fue creado por Bruce Schneier, autor del libro Applied Cryptography Utiliza claves de hasta 448 bits y, hasta el momento, ha resistido con éxito todos los ataques. Por ello y por su estructura se le considera uno de los algoritmos más seguros, a pesar de lo cual no se utiliza masivamente. Tal vez se deba a su relativa juventud (la del algoritmo, no la de Schneier). Su autor no ha patentado el método para que pueda ser empleado sin limitaciones.

Ha sido diseñado para ser rápido (cifra datos en modo de 32 [bit] a razón de 26 ciclos de reloj por byte). Es compacto (puede correr ocupando menos de 5 [Kb] de memoria), simple (las únicas operaciones que se utilizan son sumar, XOR, y buscar la tabla de particiones en operaciones de 32 [bits]), seguro (la longitud de la clave de Blowfish es variable y puede tener una longitud de hasta 448 bits como dije antes), y robusto (a diferencia de DES, la seguridad de Blowfish no disminuye por simples errores de programación).

El algoritmo de cifrado por bloques Blowfish, que cifra datos en bloques de 64-bits al mismo tiempo, es dividido en dos partes: claves de expansión y cifrado de datos. Las claves de expansión convierten una clave de más de 448 bits en varias subclaves que totalizan 4168 bytes. El cifrado de datos consiste en una función simple que permite 16 iteraciones. Cada iteración consiste en la permutación de una clave dependiente y una substitución de una clave y datos dependiente. Blowfish utiliza un gran número de subclaves que deben ser preprocesadas antes de cualquier proceso de cifrado o descifrado

5.3.2 Arquitectura del Protocolo

Las aplicaciones de HomeRF, referencias y mapas están existentes en las capas de red. Sin embargo, HomeRF ha modificado las tecnologías existentes para las capas física (PHY) y de transmisión de datos (MAC). En la figura 5.17 se ilustran las capas de la red de HomeRF.



TESIS CON FALLA DE ORIGEN

Figura 5.17 Capas de la Red de HomeRF

El nivel físico de HomeRF es común a todos los dispositivos. Funciona mediante emisión de ondas de radio en la banda de 2.4 [GHz] (ISM). Con un ancho de banda de entre 1 y 3.5 [MHz]. La potencia de transmisión es de 100 [mW], existiendo un modo standby de bajo consumo.

FHSS (Frequency Hopping Spread Spectrum): Utiliza espectro expandido con salto de frecuencia de 50 [saltos/seg]. Con esta técnica consigue evitar las múltiples interferencias presentes en su banda de emisión, en la que a parte de encontrarse otras tecnologías inalámbricas también hay interferencias de dispositivos como hornos de microondas u otras redes inalámbricas.

HomeRF utiliza un mecanismo de salto inteligente, el denominado "Adaptive Hopping Mechanism". Consiste en que si realiza una transmisión en un canal, y detecta interferencias en su transmisión, y luego salta, volviendo a detectar interferencias en el nuevo canal, no saltará a ninguna frecuencia comprendida en el rango entre las dos últimas empleadas, por comprender que existe un dispositivo emitiendo interferencia en esa franja.

Tiene un alcance de unos 50 metros, a lo que se corresponde la idea principal de dar cobertura en cualquier lugar dentro y alrededor de la vivienda. Puede interconectar teóricamente hasta 127 dispositivos. Como vemos en la figura 5.16, HomeRF admite 75 canales de los denominados básicos (5 [MHz]) y 15 de los denominados supercanales (1 [MHz]).

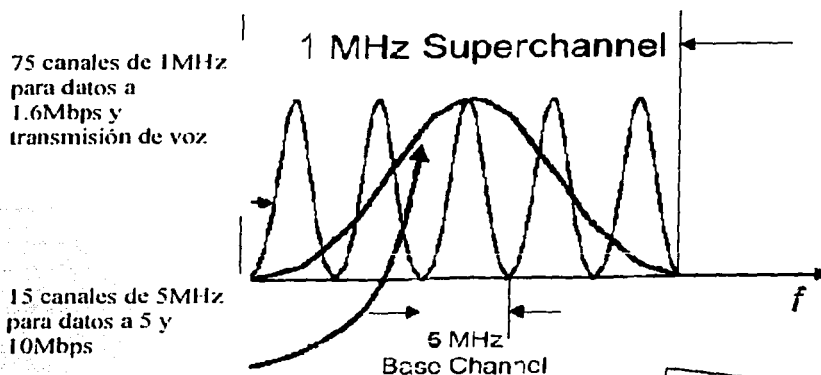


Figura 5.18 Canales de transmisión de HomeRF.

TESIS CON FALLA DE ORIGEN

El nivel MAC de HomeRF proporciona servicio para tres tipos de datos:

- Tráfico asíncrono sin conexión, usado por el tráfico TCP/IP.
- Tráfico con prioridades y con conexión, para multimedia, que usa UDP/IP.
- Tráfico isócrono, para el servicio de transmisión de voz bidireccional, con soporte para varias conexiones que utiliza también el protocolo DECT.

5.3.3 Transmisión de Datos

En la figura 5.19 vemos cómo cada trama, que puede ser de 10 ó 20 [ms] dependiendo de la presencia de datos isócronos, está mayoritariamente asignada a datos asíncronos. Dentro de éstos, los primeros paquetes enviados son los prioritarios con conexión. Se permiten hasta 8 sesiones de este tipo, correspondientes a los 8 niveles de prioridad existente.

Esta prioridad es asignada dependiendo del tipo de servicio, y los requerimientos de calidad del mismo. Si no se utiliza alguno de estos periodos, su tiempo será utilizado por los datos asíncronos. Permite aplicaciones unidireccionales (audio/video) o bidireccionales (VoIP/video phone). Para los datos asíncronos utiliza conmutación de paquetes.

El protocolo de contención actúa esencialmente como en Ethernet. Sin embargo, durante ciertos periodos (periodos libres de contención), el tiempo es reservado por dispositivos de transmisión de voz activados. Este tiempo se divide en periodos específicos pares, usados para los dos sentidos de la comunicación Full Duplex.

Cuando no hay conexiones de voz activas, este tiempo es recuperado para el uso del protocolo de contención.

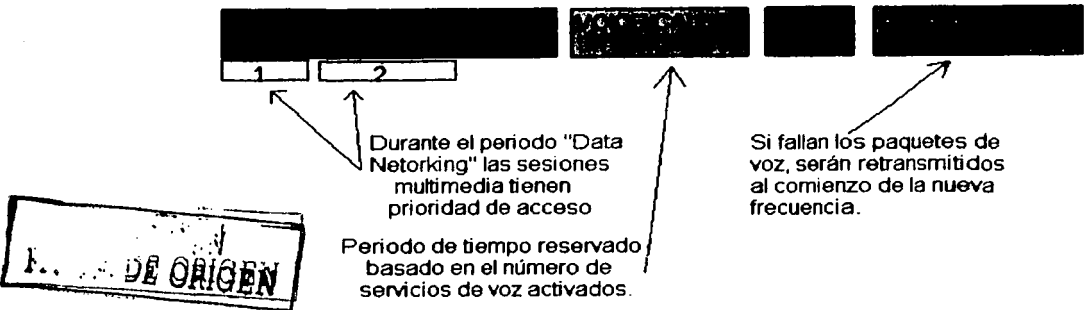


Figura 5.19. Características generales del Nivel MAC de HomeRF.

5.3.4 Transmisión de Voz

Aunque HomeRF está basado en una trama de 20 [ms] (con un salto de frecuencias por trama), cambia a una estructura de subtrama de 10 [ms] (uno por subtrama) cuando hay conexiones de servicio de voz activas. El hecho de tener una trama más corta hace que se reduzca la latencia y mejore la inmunidad a las interferencias, aspectos fundamentales en el servicio de voz. Sin embargo, el tiempo empleado en aumentar el servicio del protocolo de saltos hace que baje la tasa de transferencia, algo que importa más al servicio de transmisión de datos, que los dos factores anteriores.

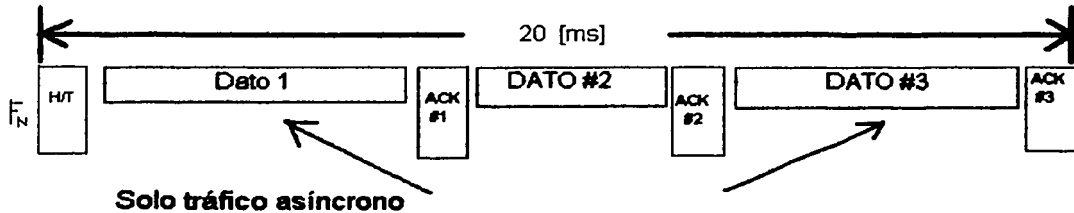


Figura 5.20 Trama sin servicio de voz activado.

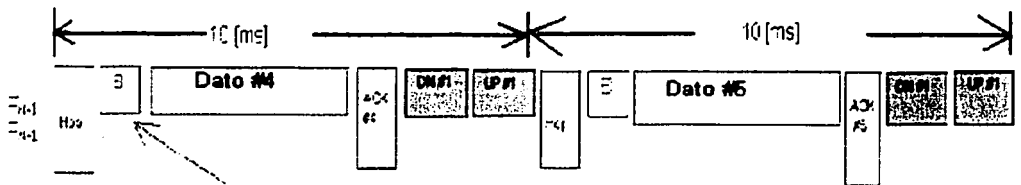


Figura 5.21. Trama con servicio de voz activado.

5. Redes de Área Personal Inalámbricas (WPANs)

En la figura 5.21 observamos que la trama es de 20 [ms] y se utiliza únicamente el protocolo de acceso basado en contención. En cambio, en la figura 5.21 se reduce el periodo de tiempo asignado a este protocolo, y se le asigna al de división de tiempo (TDMA), para el servicio de voz. Este servicio es bidireccional (Full duplex) usando TDD (Time Division Duplex). Esto explica los campos Dn#1 y Up#1.

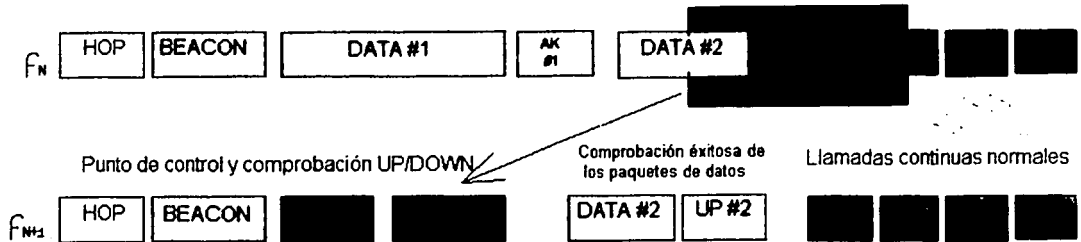


Figura 5.22 Mecanismo de retransmisión de voz.

Como vemos en esta figura 5.22, si aparece una interferencia coincidiendo en tiempo y frecuencia con los paquetes de voz, éstos serán retransmitidos en menos de 10 [ms], que es la latencia a la que se comprometen para éste servicio. Al ser retransmitidos tras el salto de frecuencia evitan las interferencias del canal anterior. Esto, sumado al mecanismo inteligente de salto anteriormente comentado, nos asegura una calidad de servicio considerable para la transmisión de voz.

Con un mecanismo de acceso basado en contención, un paquete que quiera transmitirse debe disputarse el acceso a la red con otros paquetes en su situación. Esto implica colisiones que provocan un retraso variable, y esto es lo que no se puede permitir en la transmisión de voz, y de ahí que HomeRF utilice los periodos libres de contención para el servicio de voz.

5.4 Air5

Air5 es una tecnología reciente y con un alto desarrollo en la implementación de la capa física, también está regularizada dentro de las especificaciones de la IEEE 802.11a. Utiliza el espectro de 5 [GHz], con el estándar 802.11a y la mejora en la tecnología de la capa MAC, Air5 permite servicios de multimedia, tales como vídeo, audio, y datos que se entregarán con las garantías de QoS. Con estas capacidades, una sola red inalámbrica puede distribuir servicios de multimedia a través de una casa, como se muestra en la figura 5.23.

Con un diseño mejorado de RF y técnicas de procesamiento de señales avanzadas, Air5 entrega una gran capacidad de transferencia de datos, de hasta 40 [Mb/s] en distancias reales hasta de 75 [m]. El rango es vital porque en un hogar típicamente se tiene solamente un punto de acceso responsable de distribuir la información inalámbrica a través de toda la casa.

La tecnología de red Air5 puede apoyar a una amplia gama de diversas aplicaciones las cuales se llevan a cabo sobre un solo canal libre de RF de 5 [GHz]. Mientras que las aplicaciones del usuario vienen y van todo el tiempo, la red se reconfigura automáticamente sin ninguna interrupción y así adaptarse a cualquier otra actividad que la red inicie.

TESIS CON
TALLA DE ORIGEN

5. Redes de Área Personal Inalámbricas (WPANs)

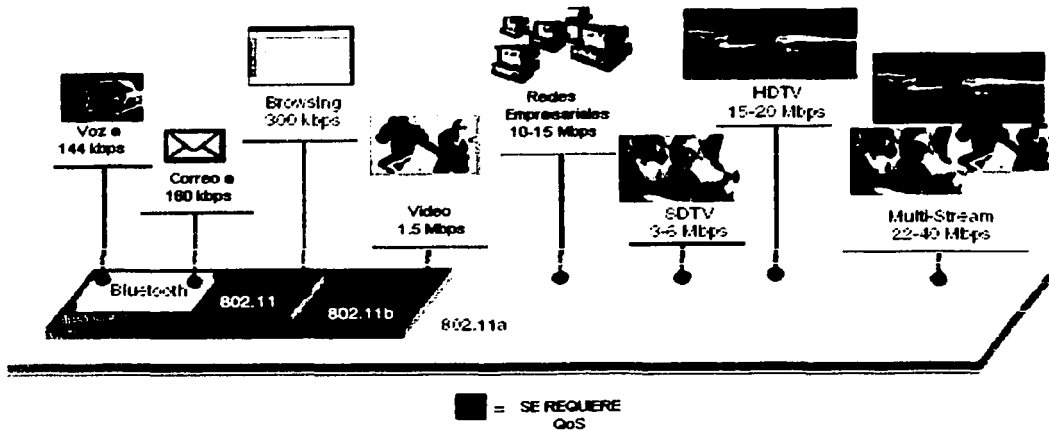


Figura 5.23 Air5 es capaz de soportar diferentes tipos de equipos y sistemas que otros similares no lo hacen.

Una sola red Air5 que funciona sobre un canal de RF de 5 [GHz] puede soportar hasta 7 altos flujos de QoS más de 64 usuarios, todos estos simultáneamente. En la tabla 4 se muestra algunos de los servicios casi ilimitados que Air5 puede soportar:

Distintos Casos	US-HDTV	DVD	SDTV	Datos	Técnica de Modulación
1	-	-	-	41.1 Mbps	64QAM 3/4
2	1	-	1	-	64QAM 3/4
3	-	1	1	1.092 Mbps	64QAM 3/4
4	1	-	1	5.543 Mbps	64QAM 3/4
5	-	3	-	-	64QAM 3/4
6	-	2	1	2.205 Mbps	64QAM 3/4
7	-	-	4	1.092 Mbps	64QAM 3/4
8	-	2	-	-	16QAM 3/4
9	-	1	1	4.430 Mbps	16QAM 3/4
10	-	-	3	-	16QAM 3/4

Tabla 4 Servicios que Air5 puede soportar.

5. Redes de Área Personal Inalámbricas (WPANs)

En la figura 5.24 se ilustran algunos usos que puedan dar a la tecnología Air5.

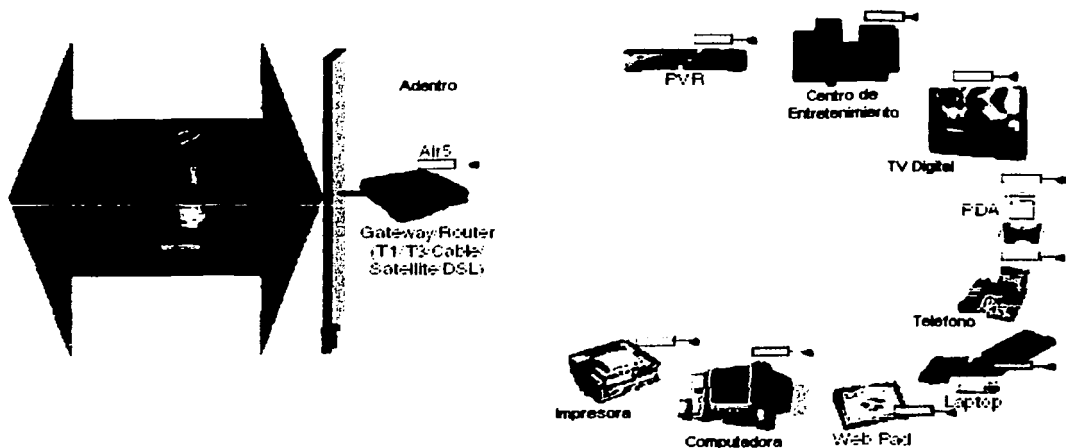


Figura 5.24. Ejemplos de aplicación de la tecnología Air 5 en el Hogar.

5.4.1 El Chipset Air5

El chipset Air5 está constituido por dos chips: el de banda base y RF. Los chips trabajan juntos para proporcionar una solución end-to-end completa, abarcando todos los elementos necesarios para enviar vídeo, audio, y datos por el aire (que es el medio de transmisión) en la banda de 5 [GHz], como se muestra en la figura 5.25.

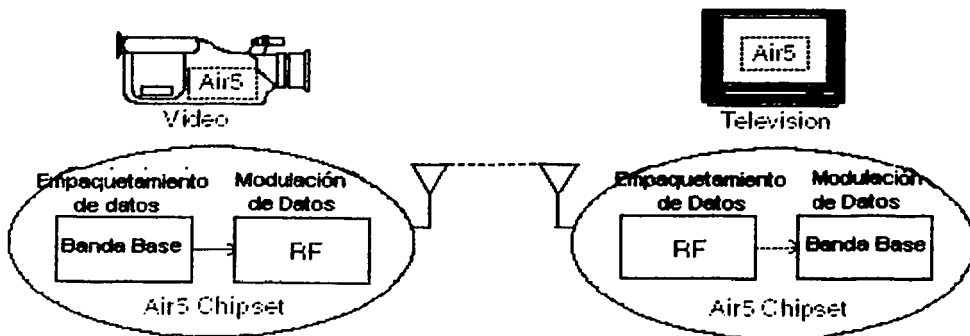


Figura 5.25 Ejemplo de una aplicación de Air 5.

5. Redes de Área Personal Inalámbricas (WPANs)

5.4.1.1 Chip Banda-Base

La chip de banda base de Air5 proporciona las funciones de la capa física (PHY) y (MAC). Éste chip empaqueta los datos de una manera que no garantiza confiabilidad, estado latente, y la entrega de los paquetes de datos. Air5 utiliza un MAC síncrono, el cual se requiere para aplicaciones de video. Utiliza una modulación TDMA y proporciona gran rendimiento en el procesamiento porque no hay colisiones, y no requiere el buffering de datos en la fuente o en el destino. Dentro del chip banda base, el encriptado utilizado es el triple-DES el cual proporciona seguridad en los datos fuerte.

5.4.1.2 Chip RF

El chip Air5 de RF contiene un modulador OFDM de alto rendimiento y un amplificador de energía (PA) para el transmisor, y un amplificador de bajo ruido (LNA) para el receptor. Éste chip también emplea un filtro on-chip y osciladores on-chip, eliminando muchos componentes externos, y los interconectan directamente con la antena. Las principales compañías están trabajando en los datos de next-generation y dispositivos de video que utilizan el chipset Air5. Se espera que estos dispositivos alcancen el mercado de consumidor a mediados del 2003.

Ahora caber mencionar las diferencias más importantes que los usuarios de redes Air5 experimentarán directamente:

Los enlaces inalámbricos de Air5 darán una mayor confiabilidad de 4 o 5 veces mejor que las típicas redes de la IEEE 802.11a lo cual es crucial para la entrega de audio y videop ininterrumpidamente.

Magis utiliza un procesamiento con un sofisticado arreglo de antenas multidireccional en el radio de los receptores para poder tener una bueno seleccionde frecuencias lo cual está fuertemente presente en enlaces inalámbricos in-door de 5 [GHz].

Magis utiliza el estándar digital del encriptado Triple-DES para su seguridad en la capa física así como otros protocolos sofisticados de la admisión y de la autenticación en la red.

5.5 Infrared Data Asociación IrDA

Infrared Data Association IrDA fue formado en junio de 1993 para desarrollar una tecnología inalámbrica de comunicaciones a través de radiación infrarroja, barata, fácil de utilizar y con un radio de funcionamiento de corto alcance. La reunión inaugural fue asistida por más de 70 compañías que reconocieron el valor de definir una sola familia donde se especificaran la comunicación de datos a través de radiación infrarroja (IR).

Antes de que IrDA existiera ya se manejaban proyectos de comunicaciones inalámbricas por medio de IR que no eran interoperables. Había el riesgo considerable de que el mercado para las comunicaciones inalámbricas por medio de IR de corto alcance se fragmentara alrededor de un cierto número de proyectos, que podrían individualmente quebrar al momento de intentar absorber todo el mercado. Para los vendedores de sistemas y periféricos impacientes por el despliegue de soluciones inalámbricas las cuales utilizarían para sus aplicaciones informáticas, la ausencia de una tecnología dominante con conectividad, represento un vacío. Sin una tecnología dominante, el riesgo de elegir la tecnología incorrecta era significativo. Así que existía un interés compartido en la generación de especificaciones comunes, esto preparo el terreno para que IrDA comenzara a trabajar. Los requerimientos originales se pueden resumir como:

- > Bajo costo al adaptarse un producto que utilizara IR
- > Tasa de transmisión mayor a 115 [kb/s]
- > Un radio de funcionamiento de 0 [m] hasta por lo menos 1 [m]
- > Un ángulo de cobertura definido por el cono de alcance de 15 a 30 grados.

5. Redes de Área Personal Inalámbricas (WPANs)

La comunicación inalámbrica por IrDA transfiere ficheros punto a punto y bidireccionales en ráfagas de alta tasa de transmisión y corta distancia, usando radiación directa por medio de LEDs con un ángulo estrecho el cual forma el cono de alcance. Las transmisiones IrDA requieren apuntar de forma relativamente cuidadosa, y son fáciles de bloquear. Por esa razón, no se puede esperar una gran distancia de recepción.

Adicionalmente, uno o ambos dispositivos pueden requerir software especial para que la comunicación pueda sincronizarse.

El estándar original de IrDA, conocido como IrDA 1.0, permitía la transferencia de datos a un velocidad de hasta 115.2 [kb/s] en un radio de acción de 1 metro y un ángulo de 15 grados. En 1996 se adoptó una extensión de este estándar, el IrDA 1.1 que permitía transferencias 35 veces superiores al IrDA 1.0. En el estándar IrDA-1.1, el máximo tamaño de datos que se pueden transmitir es de 2048 bytes y la tasa máxima de transmisión es de 4 [Mb/s].

La tabla 5 nos muestra los avances que ha tenido IrDA en términos de la introducción de las diferentes clases de productos que ponen en práctica varias mezclas de servicios que se utilizaron o que actualmente se utilizan.

FECHA APROXIMADA DE INTRODUCCIÓN	CATEGORÍA DEL DISPOSITIVO
Finales de 1994	115.2 kb/s Componentes ópticos del transmisor/receptor
Principios de 1995	115.2 kb/s Impresoras láser personales Adaptadores del puerto serial Adaptadores para impresoras
Mediados de 1995	115.2 kb/s PCs portátiles Windows '95 Impresoras portátiles de inyección de tinta
Finales de 1995	4 Mb/s transmisores/receptores ópticos
Mediados de 1996	4 Mb/s PCs portátiles 4 Mb/s dispositivos de acceso para LANs (Ethernet) Dispositivo de comunicación Nokia 9000 Windows CE 4 Mb/s Impresoras láser personales
Finales de 1997	Cámaras Digitales Teléfonos Móviles
Mediados de 1998	Plataforma Palm (Palm III) Aplicaciones de captura y repartición de información
Principios de 1999	Implementación de IrDA/Linux Estaciones portátiles Sony

Tabla 5. Categorías de los productos IrDA

La radiación infrarroja, también puede usarse para interconexiones un tanto más largas y es una posibilidad para las interconexiones en redes de área local (LAN). La distancia efectiva máxima se encuentra alrededor de los ocho kilómetros y la máxima tasa de transmisión proyectada es de 16 [Mb/s]. Dado que la IR es transmisión en línea de vista (ambos dispositivos deben poder "verse" entre sí), es sensible a la niebla y otras condiciones atmosféricas.

Como el infrarrojo, es parte del espectro de luz, no atraviesa paredes. Y como la mayor parte de los dispositivos que incorporan IrDA, tienen un radio de funcionamiento corto, esto significa que cualquier dato que sea intercambiado vía IR, ya sea a una red, a otro dispositivo o a una impresora, es seguro. IR, es más seguro que las señales de radio que pueden ser interceptadas por otros dispositivos de radio.

TECNOLOGÍA CON
FALLA DE ORIGEN

5.5.1 Arquitectura del Protocolo

A continuación describimos la arquitectura del protocolo de IrDA, los servicios proporcionados en los límites de la capa, el modelo de conexión, el modelo de información y los procesos de los dispositivos y servicios que IrDA proporciona. En la figura 5.26 la arquitectura del protocolo y muchos de los servicios de uso de IrDA.

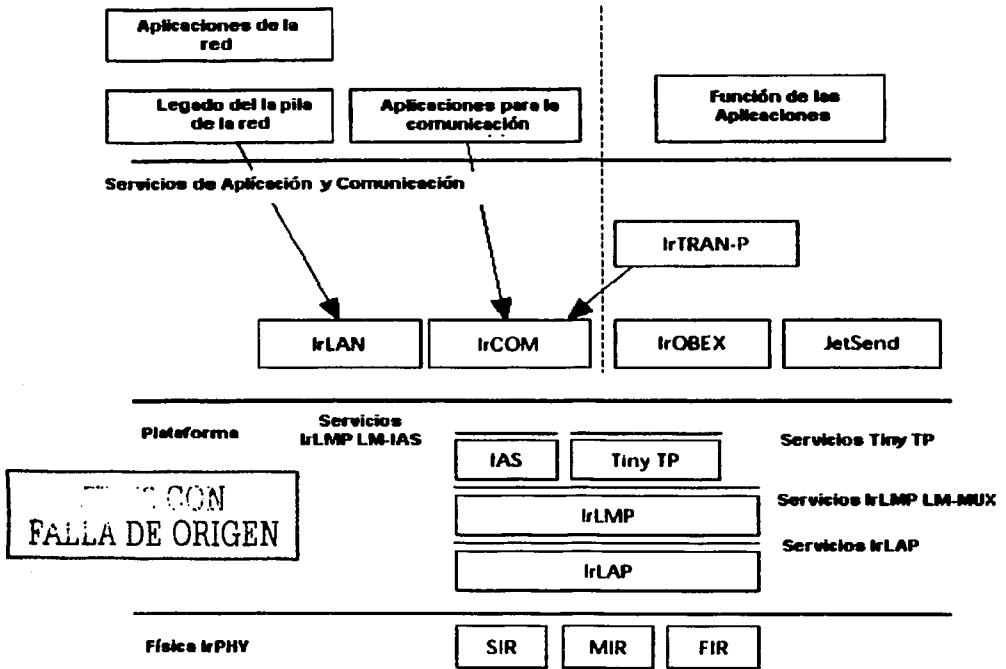


Figura 5.26. Arquitectura del protocolo IrDA.

5.5.1.1 Capa Física IrPHY

El nivel físico IrPHY (Physical Signaling Layer) especifica el formato de trama y codificación, y las características eléctricas, ópticas y físicas del enlace.

Se tienen los siguientes dispositivos:

- Dispositivos tipo serie (SIR), con velocidades de transferencia de hasta 115 [kb/s]. Normalmente están asociados a un puerto serie en los portátiles, y se pueden utilizar como puertos serie estándar.

Dentro de esta categoría podemos incluso encontrar adaptadores que convierten un puerto serie estándar en un puerto IrDA. Se conocen como *IrDA Dongles*, estos dispositivos son los más utilizados para comunicaciones con computadoras portátiles y teléfonos móviles, algunas características son las siguientes:

5. Redes de Área Personal Inalámbricas (WPANs)

- Se utiliza para negociar las opciones a 9.6 [kb/s]
- **Byte Framing:** se añaden antes y después de cada byte de datos un bit de start (0) y un bit de stop (1)
- **Packet Framing:** Se utiliza un CRC de 16 bits para la detección de errores

Byte framing UART:



Packet framing :



Figura 5.27 Trama de la capa física de SIR (Serial IrDA).

- Se utiliza un método llamado RZI, donde un 0 se codifica con un pulso independiente de entre 1.6 micro segundo y 3/16 de la longitud del bit, y un 1 se codifica con la ausencia de pulso

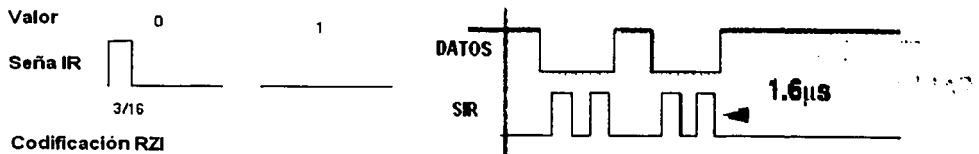


Figura 5.28 Codificación en SIR.

- **Dispositivos MIR:** Parece ser que esta en desuso. Medium Infrared. Esta orientado a transmisión entre 576 [Kb/s] y 1.152 [Mb/s]. En este caso las características de codificación y la trama cambian:
 - Un flujo de datos 'cero' se codifica con la presencia de un pulso óptico de 1/4 de la duración del intervalo de bit
 - El protocolo SDLC, con su aproximación a un bit stuffing (secuencia de escape) de inserción de cero, garantiza la ocurrencia mínima de ceros (pulsos de luz) en el flujo de datos.

TESIS CON
FALLA DE ORIGEN

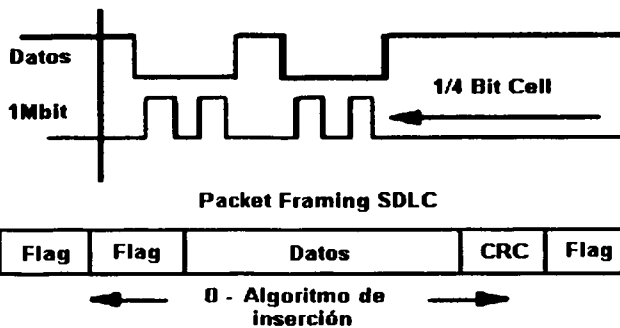


Figura 5.29 Codificación y Trama de MIR.

- Dispositivos de Alta Velocidad (FIR) de velocidades de transferencia de 4 [Mb/s]. Se utilizan para la conexión infrarroja entre equipos e impresoras en una "red infrarroja".
 - Se utiliza el método 4-PPM (4 pulse position modulation).
 - Se utiliza un CRC de 32 bits y se realiza mediante hardware.

DE ORIGEN

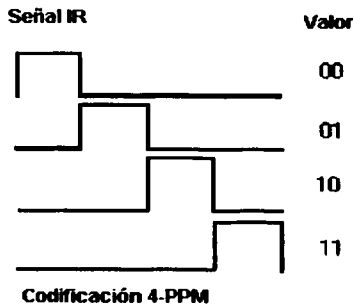


Figura 5.30 Codificación para dispositivos FIR

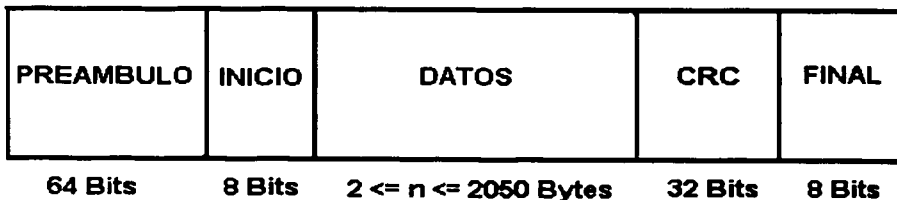


Figura 5.31 Trama para los dispositivos FIR

5. Redes de Área Personal Inalámbricas (WPANs)

- Dispositivos de Muy Alta Velocidad (VFIR) la tasa de transferencia es de 16[Mb/s].

5.5.1.2 Capa IrLAP y Capa IrLMP de IrDa

La capa de enlace se denomina **IrLAP** (link access protocol) gestiona el entramado de paquetes, proporciona un servicio seguro de comunicación entre dispositivos utilizando una conexión orientada, en caso de que esto no suceda, garantiza informar a la capa superior sobre los errores ocurridos, etc.

La capa de red se gestiona desde el **IrLMP** (link management protocol), encargándose del control de conexiones, multiplexado de éstas, registro de servicios, así como el poder integrar múltiples conexiones físicas. Puede existir la capacidad de soportar diversos dispositivos IrDA en un solo sistema, al mismo tiempo cada dispositivo es capaz de controlar hasta 16 periféricos de forma simultánea. No todos los equipos IrDA soportan conexiones múltiples, por lo que el usuario deberá cuidar que no haya más de un dispositivo conectado por infrarrojos. Esta capa consta de dos componentes:

- Multiplexador IrLMP: permite que haya múltiples clientes del servicio de red sobre una sola conexión de enlace. La comunicación a nivel de red es entre aplicaciones. Varias comunicaciones de red descansan sobre una conexión a nivel de enlace entre dos sistemas.
- IAS. Servicio de acceso a la información. Es una base de información de cada sistema para uso de las conexiones que puedan venir. Es como unas "páginas de consulta" que contienen la información asociada a los servicios o aplicaciones disponibles en un terminal.

5.5.1.3 Protocolos que ofrecen aplicaciones extra en IrDa

Existen otros protocolos que ofrecen aplicaciones extra para acceder a redes de área local, teléfonos móviles o cámaras digitales, que son:

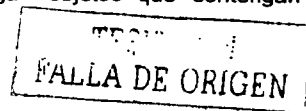
- La capa de transporte se denomina **IrTTP** (tiny transport protocol). Se encarga de controlar la fragmentación y defragmentación de paquetes, control de flujo y de conexiones, etc.

Para promover interoperabilidad entre las aplicaciones, se desarrollaron para IrDA las especificaciones para los servicios que se ofrecerían con las diferentes aplicaciones y los protocolos que estas aplicaciones soportarían. A continuación se muestran los protocolos y servicios más notables que utiliza la plataforma IrDA 1.x:

- **IrCOMM**, suministra la emulación para los puertos serial y paralelo sobre la plataforma de IrDA. Esto permite que las aplicaciones para la comunicación funcionen sobre la plataforma IrDA sin ningún cambio y también prevé el acceso inalámbrico a los módems externos.
- **IrLAN**, proporciona el acceso inalámbrico al estilo LANs de IEEE 802.

Tipos de conexiones posibles:

- Permite conectar un PC a una LAN por medio de un IrLAN Adapter.
 - Permite la comunicación de dos PCs como si estuvieran conectados como una LAN
 - Permite conectar un PC a una LAN por medio de un segunda PC ya conectada.
- **IrOBEX**, suministra el intercambio de objetos simples que contengan datos y se podría considerar el análogo de IrDA de HTTP. IrOBEX entrega objetos que contengan



5. Redes de Área Personal Inalámbricas (WPANs)

información tales como tarjetas de crédito, agendas y archivos binarios entre los dispositivos.

- **IrTRAN-P**, maneja el intercambio de imágenes entre las cámaras fotográficas digitales que se encuentren inmóviles, las impresoras de la foto, y las PC.
- **IrMC**, que define un perfil de las especificaciones relevantes de IrDA para la inclusión en teléfonos celulares. Mucho de este trabajo está siendo utilizado por la comunidad de Bluetooth. IrMC proporciona interacciones independientes con teléfonos celulares que tengan características comunes tales como sincronización de la agenda, sincronización del calendario, y acceso inalámbrico del módem. También maneja teléfonos de tercera generación conocidos como smart phones.
- **IrJetSend**, describe cómo atar el protocolo de Hewlett-Packards JetSend para la interacción de las aplicaciones de red y la plataforma de IrDA.

5.5.2 Descripción y Arquitectura de la conexión en IrDA

El modelo de la conexión de IrDA 1.x se establece sobre todo por las capas de IrLAP y de IrLMP. Hay una correspondencia de 1:1 entre los puntos de acceso de servicio (LSAPs) de la capa IrLMP LM-MUX y los puntos de acceso de servicio (TSAPs) de la capa Tiny TP. De esta manera, la capa Tiny TP no contribuye al modelo de conexión, esta capa altera simplemente las características de la entrega del canal.

Dentro de cada dispositivo de IrDA (o estación) (Figura 5.33), se acceden a los servicios de IrLAP por medio de un único punto de acceso de servicio (ISAP).

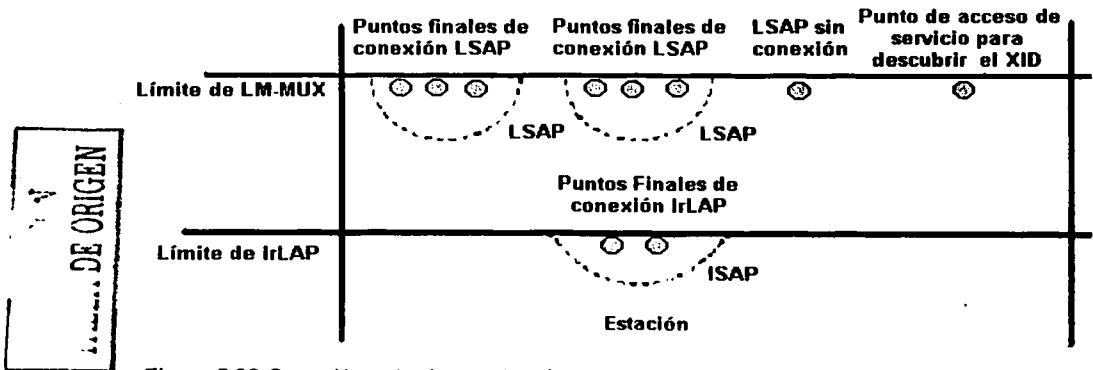


Figura 5.32 Conexión entre los puntos de acceso de servicio y los puntos finales o terminales

La arquitectura permite que múltiples puntos terminales de la capa IrLAP existan dentro del ISAP; sin embargo, el protocolo de IrLAP define en la práctica solamente una conectividad punto a punto. No hay ninguna investigación o publicaciones comerciales de IrDA que apoyen la conectividad punto-multipunto.

Sin embargo, existe una implementación comercial disponible que soporta múltiples interfaces IrLAP dando la impresión de efectuar operaciones multipunto a través de diversas situaciones independientes que se pueden dar entre la capa IrLAP y la capa IrPHY.

Asimismo, se accede a los servicios de IrLMP LM-MUX por medio de múltiples LSAPs. Típicamente, cualquier aplicación dependerá de una LSAP y, en general, apoyará las conexiones múltiples de IrLMP LM-MUX (o las conexiones Tiny TP). Así, cada LSAP puede contener varios

5. Redes de Área Personal Inalámbricas (WPANs)

puntos finales de conexión LM-MUX. Las direcciones de LSAP son formadas por la concatenación de un selector de 8-bits contenido en el LSAP y la dirección del dispositivo donde reside el LSAP.

Las conexiones de IrLAP son etiquetadas por el par (desordenado) de 32 bits de cada dirección de los dispositivos implicados en la conexión. Después del establecimiento de la conexión, una dirección temporal de la conexión de 7 bits se utiliza en los paquetes como alias para concatenar esta dirección del dispositivo. Asimismo, las conexiones de IrLMP LM-MUX son etiquetadas por el par (desordenado) de direcciones de LSAP en cada extremo de la conexión de LM-MUX. Por lo que a lo mas puede existir una sola conexión entre la LM-MUX y dos LSAPS cualquiera. Este modelo de conexión es idéntico al ofrecido por TCP/IP donde, las direcciones IP se pueden substituir por las direcciones de los dispositivo de IrDA y los números de acceso de TCP/IP se substituyen para los selectores de IrLMP LSAP.

6. Redes de Radio Ad Hoc

6.1 Introducción a las Redes Ad Hoc

En algunas ocasiones no se puede disponer o no se desea disponer, de una infraestructura de red (como podría ser una red LAN, MAN o WAN) para que nodos móviles se puedan comunicar con agentes foráneos o agentes bases. Los ejemplos más comunes del uso de esta tecnología, son la comunicación entre grupos de rescate en una situación de desastre, o la comunicación entre tropas militares, donde la infraestructura normal, no esta disponible (porque se encuentran en un área remota) o esta destruida (por ejemplo después de un terremoto). Otros ejemplos incluyen: empresarios queriendo compartir información en un aeropuerto, o una clase de estudiantes queriendo interactuar durante una lectura.

Las redes sin infraestructura, comúnmente conocidas como *redes Ad Hoc*, no poseen elementos fijos o administración centralizada de ningún tipo. Todos los nodos son capaces de moverse y conectarse dinámicamente de una manera arbitraria con otros nodos de la red, definiendo diferentes topologías que cambian velozmente.

El objetivo de las redes Ad Hoc es el de soportar comunicaciones robustas y eficientes en redes móviles inalámbricas, mediante la incorporación de funciones de encaminamiento a los nodos móviles. Tales redes deberán disponer de tecnologías multisalto, que se adapten rápida y dinámicamente a los cambios de topologías que los nodos describen, siempre teniendo en cuenta las limitaciones en los consumos de energía.

En los últimos años, los grupos de investigación de redes Ad Hoc han basado sus esfuerzos en la forma en que la ruta de un nodo, a otro nodo de la red es construida. Los protocolos desarrollados proponen básicamente dos formas de crear rutas en una red Ad Hoc:

- **Proactivamente:** Se basa en que cada nodo conozca la ruta a cualquier otro nodo de la red en el momento que quiera enviar paquetes con datos. Estos algoritmos tratan de mantener la información necesaria para el encaminamiento continuamente actualizada. Cada nodo mantiene una o más tablas con los datos para encaminar hacia cualquier otro nodo de la red. Los cambios en la topología de la red propician el envío masivo de paquetes para mantener las tablas actualizadas.
- **Reactivamente:** En éste caso se construye la ruta bajo demanda, es decir, se descubre la ruta a un nodo cualquiera cuando una estación emisora lo solicite. Este método consiste en inundar la red con paquetes de descubrimiento de ruta hasta que se encuentre el nodo en cuestión. Es decir que los protocolos basados en tablas, las rutas son creadas solo cuando se requieren. Cuando un nodo requiere una ruta hacia un destino concreto se inicia un proceso de descubrimiento de ruta. Este proceso termina cuando se encuentra un camino hacia el destino o cuando se examinan todas las alternativas y ninguna lleva al destino final. Cuando la ruta es descubierta, es necesario mantenerla (mantenimiento de ruta) hasta que el destino se vuelva inalcanzable o la ruta deje de ser necesaria

En las próximas secciones de este capítulo estudiaremos las principales características de estas redes, y profundizaremos en éstas dos corrientes, ya mencionadas, de protocolos que se desarrollan hoy en día.

6.2 Características de las Redes Ad Hoc

Una red móvil Ad Hoc consiste de un conjunto de estaciones móviles que son libres de moverse arbitrariamente. Estos nodos pueden estar ubicados en aviones, barcos, camiones, autos o pueden ser llevados por personas (pequeños dispositivos). Estas redes se caracterizan por ser sistemas

autónomos, que pueden trabajar de forma aislada, o pueden tener "puentes" o interfaces a las redes cableadas.

Una característica importante de estas redes es que trabaja como una red "stub", cuando esta conectada a una red cableada. Las redes stub transportan tráfico que es originado y/o destinado a nodos perteneciente a la red Ad Hoc, pero no permiten que el tráfico exógeno transite por esta.

Los nodos de las redes Ad Hoc están equipados con transmisores y receptores inalámbricos, que utilizan antenas omnidireccionales (broadcast) o altamente direccionables (punto a punto). Dependiendo de la posiciones de los nodos, las potencias de recepción y transmisión, e interferencias que pueden existir en un mismo canal, existe en un momento dado entre los nodos de conectividad inalámbrica en forma de grafo de características aleatorias, también llamado red *Ad Hoc*. La topología de la red Ad Hoc cambia con el tiempo a la vez que los nodos cambian su posición relativa, sus parámetros de recepción y transmisión.

Es notorio que los equipos inalámbricos instalados en los nodos de redes Ad Hoc proveen un radio de transmisión limitado. Esta limitación no permite a los nodos establecer una comunicación punto a punto con *todas* las otras estaciones de la red. Por lo cual, si dos nodos se quieren comunicar, y están fuera de su radio de alcance, deberá haber otras estaciones (pertenecientes a la red) que se comporten como routers, encaminando los paquetes salto por salto hasta el nodo destino. En la figura 6.1 vemos una red Ad Hoc compuesta de tres nodos. Las circunferencias que circunscriben a cada nodo, representan los radios de transmisión de cada uno de ellos. En este ejemplo, el nodo A desea enviarle una serie de paquetes al nodo C. Pero esto no es posible, ya que C se encuentra fuera del radio de A. Por lo que el nodo B, se convierte en un router, recibiendo los paquetes de A y encaminándolos a C.

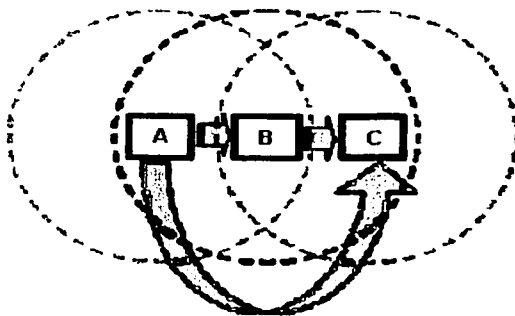


Figura 6.1. Red Ad Hoc compuesta de tres nodos móviles.

Por lo tanto, los protocolos de redes Ad Hoc deben implementar funciones de encaminamiento, que se responsabilicen de encontrar la ruta de un nodo a otro, adaptándose dinámicamente a las diferentes topologías definidas por el movimiento de los nodos que la componen. Además, estos protocolos deberán funcionar correcta e independientemente de las características y rangos de transmisión de cada nodo, y sus interrelaciones con los demás.

Podemos resumir las principales características de las redes Ad Hoc en los siguientes puntos:

- **Topología dinámica.** Los nodos se pueden mover arbitrariamente, por lo cual la topología de la red (la cual es típicamente multisalto) cambiará aleatoria y rápidamente con estos, un número impredecible de veces.
- **Ancho de banda limitado y conexiones de capacidad variable.** Las conexiones inalámbricas continuarán teniendo una capacidad inferior a sus contrapartes cableadas.

- *Operaciones con gasto de energía limitado.* Casi todos los nodos dentro de una red Ad Hoc deberán contar con sus baterías o alguna otra fuente de energía agotable para sus comunicaciones. Para estos nodos, el criterio más importante para el diseño de sus sistemas deberá ser la conservación de energía.
- *Seguridad física limitada.* Las redes móviles inalámbricas son generalmente más propensas a los riesgos físicos de seguridad que las redes cableadas. La mayor posibilidad de ataques tales como: hombre en el medio (eavesdropping), dirección de origen falsa (spoofing) y negación de servicio, deberán ser cuidadosamente considerados. Todas estas características, que muchas veces son contradictorias, hacen que el diseño de protocolos para redes móviles Ad Hoc sea bastante complejo. Por lo cual es importante definir las metas u objetivos que se han propuesto para diseñar este tipo de sistemas.

El objetivo fundamental buscado por los investigadores de redes Ad Hoc, es el desarrollo de capacidades de encaminamiento, para garantizar conexiones punto a punto, en un dominio puramente inalámbrico y móvil. También se puede destacar los siguientes objetivos dentro del desarrollo de protocolos para este tipo de redes:

- Proveer operaciones efectivas sobre un amplio rango de contextos de red. Un contexto es un conjunto de características que describen una red móvil y el ambiente que la rodea.
- Soportar los servicios tradicionales IP orientados a la desconexión.
- Reaccionar eficientemente a los cambios de topología y a las demandas de tráfico, mientras se mantiene un encaminamiento efectivo en un contexto de red móvil.

También se han propuesto objetivos considerando temas como direccionamiento, seguridad, y la interacción con las interfaces de capas menores y capas mayores.

6.3 Protocolos Ad Hoc

En los últimos años se han propuesto diversos frentes para atacar los distintos objetivos que se han propuesto anteriormente, entre ellas podemos destacar:

- Algoritmos Proactivos vs. Reactivos.
- Direccionamientos planos vs. Direccionamientos jerárquicos.
- Dentro de los Proactivos, algoritmos de Vector de Distancia vs. Algoritmos de Estado de los Enlaces.
- Algoritmos priorizan el mínimo consumo de energía vs. algoritmos que priorizan la calidad de servicios.
- Algoritmos híbridos, que conjugan las mejores características de los protocolos proactivos, con las de los reactivos.

En general, los protocolos existentes pueden ser clasificados en proactivos o reactivos. Los proactivos evalúan constantemente las rutas dentro de la red, para que cuando un paquete quiera ser enviado, el camino al destinatario ya sea conocido y pueda utilizarse inmediatamente. En cambio, los protocolos reactivos, invocan a un procedimiento de determinación de la ruta solo bajo demanda. Es decir, cuando una ruta es necesaria, un procedimiento de búsqueda global es ejecutado.

A continuación estudiaremos los algoritmos más importantes que se han desarrollado en las investigaciones sobre redes Ad Hoc.

6.3.1 Protocolos Proactivos

Los protocolos proactivos son aquellos que mantienen información de encaminamiento consistente y actualizada para cada nodo, de forma que se puedan enviar datos a cualquier otra estación de la red de forma inmediata. Estos protocolos requieren que cada nodo mantenga una o más tablas para almacenar la información de encaminamiento, y que respondan a los cambios de topología propagando actualizaciones a través de la red, de forma de mantener una visión correcta de ésta.

Existen tres formas por lo cual un nodo puede mantener una tabla de rutas actualizada y consistente. La primera alternativa es la *centralizada*, en donde un nodo computa todas las rutas y luego las distribuye a los otros nodos. El problema más importante con el encaminamiento centralizado es la complejidad requerida para proveer servicio cuando el nodo central falla y el retardo necesario para adaptarse a los cambios de topología.

La segunda opción es la *descentralizada*, en la cual cada nodo crea y mantiene su tabla de encaminamiento actualizada, mediante la información de la topología de la red. Esta alternativa es también conocida como algoritmos de *estado de los enlaces*, y funcionan permitiendo que cada nodo determine su propia conectividad (el "estado del enlace") y luego distribuya esa información, mediante el método de inundación, a todos los demás nodos de la red. Las actualizaciones de los estados de los enlaces proveen a los otros nodos con la información necesaria para determinar la topología de la red Ad Hoc, y luego poder crear la tabla de rutas. Finalmente, la tercera alternativa es la *distribuida*, en donde los nodos cooperan para establecer las rutas, sin que ninguno de ellos tenga información de cual es la topología completa de la red. Esta alternativa también es llamada algoritmos de *vector de distancia*. Estos algoritmos operan haciendo que cada nodo mantenga una tabla (por ejemplo, un vector) que da la mejor distancia conocida a cada destino de la red, y que nodo utilizar para llegar a este. Estas tablas se actualizan intercambiando información con los vecinos. La segunda y tercera alternativa son las soluciones que más se adecuan a la problemática de las redes Ad Hoc, ya que se trata de no depender de ninguna entidad centralizada. Por este motivo mencionaremos las principales características de estas dos últimas:

El algoritmo de *vector de distancia básico*, necesita muchas iteraciones para converger cuando hay una falla de alguna conexión, y pueden tener problemas de bucles en las rutas, cuando la longitud del camino hasta un nodo aumenta. Sin embargo se ha modificado levemente este algoritmo para minimizar estos problemas.

Los algoritmos de estado de los enlaces pueden comportarse de una manera más robusta cuando los enlaces entre los nodos fallan, ya que checan periódicamente las conexiones.

Los algoritmos de estado de los enlaces proveen a cada nodo un mapa de la topología de la red, por lo cual cuando un enlace falla, un camino alternativo puede ser generado rápidamente. Se han propuestos varios algoritmos eficientes de vector de distancia que cuando una conexión falla se pueda computar una ruta alternativa, pero las modificaciones a el algoritmo básico son significativas.

Un algoritmo de estado de los enlaces puro genera más tráfico que un algoritmo de vector de distancia.

Como el ancho de banda es un recurso tan limitado en este tipo de redes, es importante conocer el overhead de los algoritmos de vector de distancia y de estados de los enlaces.

6.3.1.1 Destination Sequenced Distance Vector Routing (DSDV)

El protocolo DSDV esta basado en la familia de protocolos de vector de distancia propuesta por Bellman-Ford, con las modificaciones necesarias para prevenir bucles en las rutas. Cada nodo móvil en la red mantiene una tabla de rutas, en donde se encuentran todos los destinos posibles dentro de la red, con la cantidad de saltos necesarios para llegar a cada uno de ellos. Cada entrada es marcada con un **número de secuencia**, que es asignada por el nodo destinatario. Este número de secuencia permite a los nodos móviles distinguir entre una ruta actualizada y una ruta que haya caducado, de esta manera se previene los bucles en las rutas muy largas. Las actualizaciones de las tablas de rutas son periódicamente transmitidas a través de la red, de forma de mantener la consistencia en la información de encaminamiento. Para poder aliviar la gran cantidad de tráfico potencial que este tipo de actualizaciones puede ocasionar, se utilizan dos tipos de estrategias que utilizan distintos paquetes. El primero llamado de *full dump* (o de actualización total). Este tipo de paquete transporta toda la información de encaminamiento disponible, y puede requerir unos cuantos *frames* o *tramas* de datos (unidad de transporte en la Capa de Enlace de Datos).

Durante los periodos en los cuales los nodos se mueven ocasionalmente, no se utilizan estos paquetes ya que la información de encaminamiento cambiaría mínimamente. Para estos casos se usan los paquetes llamados *incrementales*, los cuales tienen como cometido transportar solo la información de encaminamiento que haya cambiado desde le último *full dump*. Cada uno de estos paquetes incrementales deben ajustarse al tamaño estándar de un *frame* o *trama* de datos, de esta forma disminuirá el tráfico generado. Los nodos móviles mantienen una tabla adicional donde almacenan la información de encaminamiento transportada por estos paquetes. Los paquetes de actualización de información de encaminamiento, contienen los siguientes campos:

- La dirección al destino.
- La cantidad de saltos para alcanzar ese destino.
- El número de secuencia de la información recibida, con relación al destino.
- El nuevo número de secuencia, que es único para ese paquete.

Cuando un nodo móvil recibe información de encaminamiento nueva (usualmente en paquetes incrementales), es comparada con la que ya existía en la tabla de rutas. La ruta que tenga asociada el número de secuencia más reciente es la utilizada. En el caso de que dos rutas tengan el mismo número de secuencia asociado, se utilizará aquella con la "mejor" métrica elegida, de forma de optimizar el camino al destino. La métrica elegida, del nuevo paquete de actualización, es incrementada en una unidad de medida, y se almacena en la tabla. Luego, las nuevas rutas generadas son empaquetadas para ser enviadas como paquetes de actualización a sus vecinos.

La movilidad de los nodos, generalmente causa fallos y rupturas en los enlaces. Estos fallos deberán ser detectados por la Capa de Enlace del protocolo, o puede ser inferidos si no se recibe ninguna difusión de un vecino en un determinado lapso de tiempo.

A un fallo en una conexión se le asigna el valor *infinito* (cualquier valor mayor al máximo establecido para esa métrica) y un nuevo número de secuencia. Como el fallo se podría calificar de un cambio sustancial en la red, es necesario que el nodo informe inmediatamente de este hecho a sus vecinos, mediante la difusión de un paquete de actualización.

La creación de paquetes de información para notificar de un cambio en la red, es la única situación en la cual se permite que un nodo que no sea una estación destino genere un número de secuencia.

6.3.1.2 Clusterhead Gateway Switch Routing (CGSR)

El protocolo CGSR difiere del DSDV en la forma en que direcciona a sus nodos, y en el esquema de organización de la red que se emplea. En vez de un direccionamiento de red "*plano*", es decir sin jerarquías, el CGSR cuenta con un protocolo multisalto para redes de nodos móviles, que utiliza *clusters* (*agrupamientos*) para su organización, e implementa diversos esquemas de encaminamiento heurístico o deductivos.

Mediante la designación de un Head Cluster (o cabeza de grupo) (HC), se puede controlar un grupo reducido de nodos Ad Hoc, un canal de acceso, el encaminamiento, y la utilización del ancho de banda. Un algoritmo distribuido de selección es utilizado para designar un nodo como HC dentro del cluster. La desventaja de tener un esquema de este tipo, es que el tener múltiples cambios de HC afecta de manera adversa el rendimiento del protocolo, ya que los nodos pasarían ocupados en la selección del nuevo HC.

Para solucionar esto se ha desarrollado un protocolo para que los cambios de HC sean mínimos. Se lo conoce como protocolo Least Cluster Change (LCC), en donde sólo cambia si dos HC entran en su radio de transmisión, o cuando un nodo se mueve lo suficiente para estar fuera del área de cobertura de todos los HC.

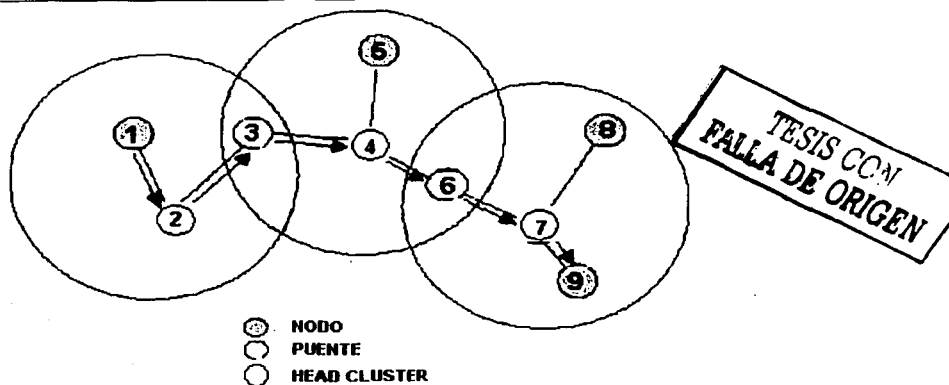


Figura 6.2. Esquema básico del protocolo CGSR. Encaminamiento del nodo 1 al nodo 9.

El protocolo CGSR utiliza el DSDV como esquema de encaminamiento subyacente, por lo cual presenta un overhead similar a este. Sin embargo, modifica el DSDV mediante el uso de un encaminamiento jerárquico HC-a-PUENTE para transportar el tráfico entre nodos de diferentes clusters. Los nodos *puente* son aquellos que se encuentran dentro del área de transmisión de dos o más HC (figura 6.2). Un paquete que es enviado por un nodo es primero encaminado al HC, para que este último lo reenvíe al puente, y este a su vez a otro Head Cluster. Este método es repetido hasta que el HC del nodo destino es alcanzado. Luego el paquete es enviado al destinatario. La figura 6.2 ilustra un ejemplo de este tipo de encaminamiento. Mediante el uso de este algoritmo, cada nodo deberá mantener una *tabla de miembros de cluster (TMB)*, con una entrada para cada estación de la red, donde se almacena el HC asociado con cada una de estas. Estas tablas son distribuidas periódicamente por cada nodo utilizando el algoritmo DSDV. Las estaciones actualizan sus tablas con la recepción de los paquetes de actualización que envían sus vecinos.

Además de la TMB, cada nodo debe mantener una *tabla de encaminamiento*, con la cual determinará el próximo salto para alcanzar el destino. Cuando se recibe un paquete, el nodo consulta su TMB y la tabla de encaminamiento para seleccionar el HC más cercano en la ruta al destinatario. Luego, el nodo deberá verificar su tabla de rutas, de forma de poder determinar el próximo salto para alcanzar el HC descubierto en el paso anterior. Luego se transmitirá el paquete a ese nodo.

6.3.1.3 Wireless Routing Protocol (WRP)

El protocolo WRP es un protocolo proactivo, que tiene el objetivo de mantener información de encaminamiento para alcanzar a todos los nodos de la red.

Por este motivo, cada nodo deberá responsabilizarse de mantener cuatro tablas:

- *Tabla de distancias.*
- *Tabla de encaminamiento.*
- *Tabla de costo de la conexión.*
- *Y una tabla con la lista de mensajes retransmitidos (MRL).*

Cada entrada de la MRL contiene el número de secuencia actualizado del mensaje, un contador de retransmisiones, un vector de flags (o banderas) (para cuando envían un ACK [4]) con una entrada para cada nodo, y una lista de las actualizaciones enviadas en los mensajes de actualización. A su vez la MRL registra todas aquellas actualizaciones que tienen que ser retransmitidas, y también aquellos nodos que enviarán un ACK cuando reciban la retransmisión. Los nodos móviles se informan de cambios en los enlaces mediante el uso de los mensajes de actualización. Estos mensajes son sólo enviados entre nodos vecinos y contienen una lista de las actualizaciones (el

nodo destino, la distancia a este, y el nodo predecesor), así como otra lista con las respuestas indicando cual nodo debería enviar un ACK cuando reciba el mensaje de actualización. Cuando un enlace entre dos nodos se pierde, estos envían un mensaje de actualización a los vecinos. Estos últimos modifican sus entradas en la tabla de distancias y verifican si existe otra ruta posible a través de otros nodos. Cualquier nuevo camino encontrado es informado a los nodos originales para que puedan actualizar sus tablas de acuerdo a los cambios en los enlaces.

Los nodos se percatan de la presencia de nodos vecinos, mediante la recepción de ACKs y otros mensajes. Por lo cual si un nodo no se está comunicando, deberá enviar periódicamente un mensaje HELLO, para asegurar la conectividad con sus vecinos. De otra forma, si un nodo no enviara estos paquetes, sus vecinos inferirían que ocurrió un fallo en la conexión, causando una falsa alarma.

Cuando un nodo recibe un paquete HELLO de una nueva estación, esta será inmediatamente incluida en la tabla de encaminamiento. A su vez el nodo receptor del paquete le enviará un mensaje con la información del su tabla de encaminamiento.

Parte de la innovación del WRP es la forma en que este protocolo previene los bucles en las rutas a los destinos.

6.3.2 Protocolos Reactivos

A diferencia del enfoque proactivo, los protocolos *reactivos* están basados en algoritmos ejecutados bajo demanda. Es decir, cuando un nodo necesita una ruta hasta otra estación presente en la red Ad Hoc, se ejecuta un proceso de descubrimiento global para encontrar la ruta hasta el destinatario. Por lo cual estos protocolos crean *rutas* solamente cuando el nodo fuente necesita enviarle un paquete al nodo final.

Esta familia de protocolos se caracteriza por ser de carácter distribuido, ya que los procesos de descubrimiento de ruta se inician en cada nodo fuente y no existe ningún tipo de entidad centralizada que pueda coordinar estos procesos.

El proceso de descubrimiento se completa cuando se encuentra la ruta hasta el nodo final, o bien, todas las combinaciones posibles de rutas se hayan examinado sin encontrar el nodo buscado. Una vez que la ruta haya sido establecida, es mantenida por un *procedimiento de mantenimiento de ruta* hasta que, el destino sea inaccesible a través de todo el camino, o que la ruta ya no sea necesaria.

6.3.2.1 Ad-Hoc On-Demand Distance Vector (AODV)

El AODV es un protocolo reactivo basado en el algoritmo proactivo DSDV, con la diferencia de que cada nodo móvil perteneciente a la red Ad Hoc, inicia una búsqueda de ruta global solo cuando necesita un camino hasta otra estación, es decir, *bajo demanda*.

El protocolo AODV presenta las siguientes características:

- Permite a los nodos móviles obtener rápidamente las rutas a nuevos destinatarios, y no requiere que las estaciones mantengan conexiones a otros nodos que no estén en funcionamiento.
- Permite la formación de grupos multicast, en donde sus miembros pueden cambiarse activamente durante la vida de la red.
- Permite a los nodos responder rápidamente a los fallos en las conexiones y a los cambios de topología, muy comunes en este tipo de red.
- Las rutas que este protocolo genera están libres de bucles.
- Mediante la resolución del problema de "conteo al infinito" característico de la familia de protocolos de Bellman-Ford, se provee de una rápida convergencia cuando la red presenta cambios en su topología.
- Cada entrada en la tabla de rutas está asociada a un número de secuencia, el cual es creado por el nodo destino o por el líder del grupo multicast.

6.3.2.1.1 Funcionamiento

Los mensajes utilizados por el protocolo AODV son los siguientes:

- **RREQ:** Pedido de ruta o *route request*.
- **RREP:** Respuesta de ruta o *route reply*.
- **RERR:** Error en la ruta o *route error*.
- **MACT:** Activación del grupo multicast o *multicast activation*.
- **GRPH:** Utilizado por grupos multicast. (Group Hello)

Mientras los nodos móviles que establezcan una comunicación posean rutas válidas para realizarla, el protocolo AODV no ejecutará ningún proceso. Pero cuando sea necesario una ruta a un nuevo destino (sea una sola estación o un grupo multicast), el nodo en cuestión deberá hacer una difusión del paquete RREQ de forma de encontrar un camino hacia ese destino. Una ruta puede ser determinada cuando el paquete RREQ alcance el nodo buscado, o cuando una estación intermedia posea una ruta actualizada al destino. La ruta encontrada se activa mediante la respuesta del paquete RREP al nodo que ejecutó el proceso de descubrimiento de ruta. Como todas las estaciones intermedias que recibieron el *pedido de ruta* almacenaron en su tabla la ruta de regreso a el nodo emisor, el paquete RREP puede ser fácilmente transmitido en su camino desde la estación destino hasta, la estación emisora.

Cada nodo monitorea el estado de las conexiones de los próximos saltos de sus rutas activas. Cuando se produce un fallo en el enlace de una ruta activa, un paquete RERR es utilizado para notificar a las estaciones la pérdida de esa conexión. Este paquete indica que destinos están en ese momento inactivos.

Los paquetes RREQ son utilizados también cuando un nodo desea unirse a un grupo multicast. Un bit configurado en el paquete RREQ indica a las estaciones que cuando reciban el paquete RREP, no sólo tendrán que configurar sus tablas de rutas, si no que también sus tablas de rutas multicast, que serán utilizadas en caso de que el nodo sea seleccionado para formar parte del árbol. Si esto sucede, el nodo y los intermediarios serán informados mediante un paquete MACT.

En los grupos multicast, el paquete GRPH es difundido periódicamente por el líder de grupo. El mensaje transporta la dirección IP del líder y del grupo multicast. Esta información es utilizada para reparar el árbol multicast en caso de que una parte de él este desconectada. Como AODV es un protocolo de encaminamiento, tiene necesariamente que lidiar con la administración de las tablas de rutas. Para cada entrada de su tabla utiliza los siguientes campos:

- Dirección del destino.
- Número de secuencia del destino.
- Contador de saltos. (Número de saltos necesarios para alcanzar el destino).
- Último contador de saltos.
- Próximo salto.
- Lista de nodos precursores.
- Tiempo de vida de la ruta.
- Banderas de encaminamiento.
- Los campos que siguen son almacenados en cada entrada de la tabla multicast:
- Dirección del grupo multicast.
- Dirección del líder del grupo multicast.
- Número de secuencia del grupo multicast.
- Próximos saltos.
- Cantidad de saltos al próximo miembro del grupo multicast.
- Cantidad de saltos al líder del grupo multicast.

6.3.2.1.2 Descubrimiento de Ruta

Cuando un nodo determina que necesita una ruta hasta otra estación y no la tiene disponible en su tabla, ejecuta el procedimiento de búsqueda de ruta, haciendo una difusión de un paquete RREQ entre sus vecinos. Un nodo no tiene una ruta disponible por dos razones, porque no conocía previamente el nodo destino, o porque poseía una ruta pero esta había expirado.

El campo *Número de Secuencia del Destino* en el paquete RREQ, es el último número de secuencia conocido para ese destino, y fue copiado de la tabla de rutas del nodo emisor del mensaje. Si no se conoce ningún número de secuencia se utiliza el cero. El campo *Número de Secuencia del Nodo Emisor* en el paquete RREQ, es su propio número de secuencia. El campo *identificador de Broadcast*, es incrementado en uno cada vez que se hace una difusión del paquete RREQ. El campo *Contador de Salto* es configurado en cero. Luego de la difusión del RREQ, el nodo espera por la respuesta de un mensaje RREP. Si este último no es recibido en un tiempo dado, el nodo origen difunde el RREQ nuevamente, hasta un máximo establecido de veces. Cada vez que se re difunde el RREQ es preciso que el nodo incremente el *identificador de Broadcast*.

Los paquetes de datos que están esperando una ruta para ser enviados a sus destinos, deberán ser almacenados temporalmente en el nodo emisor, con un manejo FIFO (Fist In First Out, el primero que entra es el primero que sale). Si el paquete RREQ es difundido el máximo de veces posibles, los datos serán borrados del almacenamiento temporal, y se enviará a las capas superiores un mensaje de DESTINO INALCANZABLE.

Cuando un nodo recibe un paquete RREQ, primero verifica si ha llegado algún otro paquete de este tipo, con la misma dirección del nodo emisor y el mismo identificador de Broadcast, dentro de un período de tiempo establecido. Si esto sucediese, el nodo descartará el nuevo paquete RREQ.

Los paquetes no descartados son procesados por los nodos, para decidir si hay que redifundirlos o para generar una respuesta RREP. Cuando una estación recibe un paquete RREQ, verifica si posee una ruta actualizada para ese destino. Si no fuera de este modo, tendría que hacer una redifusión del RREQ a través de su(s) interfase(s), pero insertando su propia dirección, en el campo *Dirección de Origen* de la cabecera del nuevo paquete. El *Número de Secuencia del Destino* tendrá que actualizarse al máximo entre el número del paquete viejo y el número que ese nodo posea en su tabla de rutas (si la entrada existe). La cantidad de saltos máximos permitidos en el paquete será reducido en uno, y el *contador de saltos* aumentado en uno.

Si en cambio, el nodo posee en su tabla una ruta actualizada para ese destino, deberá comparar su número de secuencia, con el campo *Número de Secuencia del Destino* en la cabecera del paquete RREQ. Si el número de secuencia de la tabla de rutas es menor, el nodo deberá redifundir el paquete RREQ.

El nodo generará un paquete de respuesta RREP si sucede que:

Tiene una ruta activa al destino, y el número de secuencia de esa entrada en la tabla, es mayor o igual al el número del paquete RREQ este es el nodo destino.

6.3.2.2 Dynamic Source Routing (DSR)

El protocolo DSR utiliza un método de encaminamiento en la cual el emisor de un paquete determina la secuencia completa de nodos, a través de los cuales se comunicará con el destino deseado. El emisor lista explícitamente la ruta en la cabecera del paquete, identificando el próximo salto con la dirección del nodo siguiente al que se tiene que reenviar el paquete en su camino al destinatario. Este método es conocido como *encaminamiento desde la fuente*, y ha sido utilizado en múltiples protocolos para redes cableadas, variando la forma en que se definía una ruta. Podría ser estática (sin búsqueda de ruta, se configuran antes de que la red comience a funcionar) o dinámicamente. Este protocolo ofrece importantes ventajas frente a los algoritmos proactivos en el contexto de una red Ad Hoc:

- Primero, el DSR no utiliza mensajes periódicos de actualización de las ruta, de esta forma reduce la utilización del ancho de banda, que se manifiesta de forma significativa en los períodos de poco movimiento de los nodos.
- También se economiza de mejor forma la energía consumida, ya que no se tiene la necesidad de enviar, ni de recibir actualizaciones periódicas. Por este motivo, estos protocolos utilizan diferentes estados: "en espera" y "durmiendo", y de esta forma economizan más la energía de las baterías.
- Finalmente, los protocolos de encaminamiento convencionales (cómo los de vector de distancia o estado de los enlaces) no fueron diseñados para soportar los cambios de topología característicos de las redes Ad Hoc. En un ambiente con nodos móviles funcionando como routers (por la capacidad de encaminar paquetes a través de la red) los protocolos creados deben converger rápidamente a los fallos en las conexiones (que muchas veces son ocasionados por el simple movimiento de un nodo).

6.3.2.2.1 Funcionamiento

Para enviar un paquete a otro nodo, el emisor construye una *ruta desde la fuente* en el paquete, insertando la dirección de cada estación en la red por donde la cual el paquete debe ser reenviado para llegar al receptor. Luego el emisor transmite el paquete a través de su interfase de red inalámbrica al primer nodo en la lista de direcciones. Cuando una estación recibe un paquete, y si no es el nodo destino, simplemente transmite el paquete al próximo salto. Una vez que el paquete llega a su destino final, este es pasado al software de la capa de red de ese nodo.

Cada nodo móvil que participa en la red Ad Hoc, guarda una *verificación de ruta*, en el cual almacena todos los caminos que ha "aprendido". Por lo cual, cuando un nodo envía un paquete a otra estación, el emisor verifica si posee una ruta en su tabla de verificación hacia ese destino. Si no encuentra ninguna ruta, el emisor deberá ejecutar protocolos de *descubrimiento de ruta*. Mientras espera que este proceso termine, el nodo puede continuar con sus procesos normalmente, enviando y recibiendo paquetes con otras estaciones. El nodo deberá almacenar temporalmente el paquete hasta que se encuentre la ruta, o podrá descartarlo en caso de que el destino sea inalcanzable, en donde entraran los protocolos de capas superiores para reenviar este paquete. Cada entrada en la tabla verifica si tiene asociado un período de expiración, después del cual la ruta es borrada de la verificación. Mientras un nodo esta utilizando una ruta, debe monitorear continuamente el correcto funcionamiento de ésta. Este proceso es llamado *mantenimiento de ruta*.

Cuando el mantenimiento de ruta detecta un problema con una ruta en uso, se deberá ejecutar nuevamente el proceso de descubrimiento de ruta para encontrar una nueva hasta el destino.

6.3.2.2.2 Descubrimiento de Ruta

El descubrimiento de ruta permite a cualquier nodo en una red Ad Hoc, descubrir dinámicamente un camino a cualquier otra estación de la red, mediante una conexión directa, o utilizando uno o más nodos para establecer una ruta multisalto.

Un nodo que inicia un descubrimiento de ruta, hace una difusión de un paquete RREQ (Route Request), que será recibido por todas la estaciones que se encuentran en el radio de transmisión de este. Si el paquete RREQ tiene éxito, es decir llega al nodo destino, la estación emisora recibirá un paquete RREP (Route Reply), en el cual estará la secuencia de nodos necesarios para llegar a la estación destino. Además de la dirección del nodo origen o emisor, y la dirección del nodo destino o *blanco*, el paquete RREQ contiene un registro donde acumula la secuencia de saltos que son realizados por dicho paquete mientras se propaga por la red, durante el descubrimiento de ruta. Además de estos tres campos, el paquete RREQ tiene asociado un número identificador único RId (Request Identifier), fijado por el emisor. Para detectar los paquetes duplicados que se reciben, todos los nodos de la red mantienen una tabla con los pares *<dirección del emisor, RId>*.

Cuando un nodo recibe un paquete RREQ, procesa el pedido de ruta de acuerdo de los siguientes pasos:

1. Si el par <dirección del emisor, RId> para este RREQ es visto en la tabla de los pedidos de ruta reciente, entonces se descarta el paquete y no se lo procesa.
2. Si la dirección del nodo que esta procesando el paquete, está dentro de la lista de estaciones por donde paso ese paquete, este es descartado.
3. Si la dirección del nodo blanco coincide con la dirección de la estación receptora del paquete, entonces el descubrimiento de ruta tuvo éxito y la lista de saltos almacenada en el paquete muestra la ruta hasta el nodo emisor. Por esta se envía un mensaje de RREP con la copia de la ruta.
4. Si no ocurre ninguno de los anteriores puntos, se adiciona la dirección del receptor a la lista de nodos en el paquete y se re difunde el paquete RREQ.

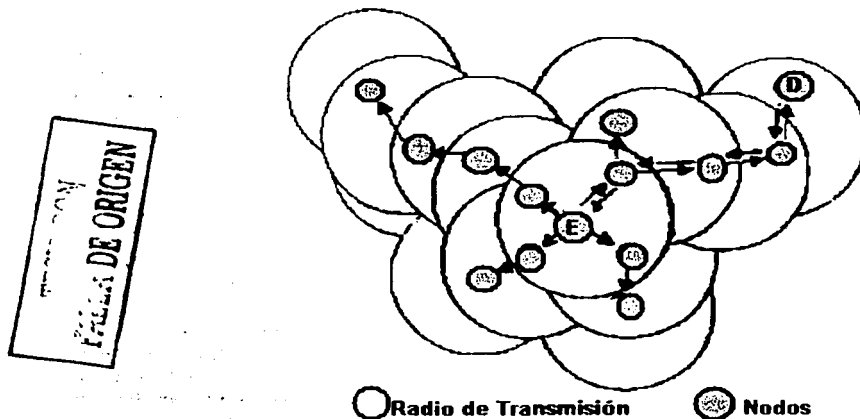


Figura 6.3. DSR. Proceso de descubrimiento de ruta.

Como hemos visto, el paquete de pedido de ruta RREQ se propaga a través de la red ad hoc hasta que alcanza el nodo destino, el cual responde al nodo fuente con un mensaje de RREP (Ver Figura 6.3). El paquete RREQ original es recibido solo por los nodos que se encuentran dentro del rango de transmisión del nodo fuente, y cada uno de ellos a su vez, re difunden este paquete siguiendo los pasos vistos anteriormente. En el caso en que un nodo no cumpliera el paso número dos en el momento que recibiese un paquete RREQ, se incurriría en un bucle en el camino al destino.

De forma de retornar el paquete RREP al nodo emisor del descubrimiento de ruta, es preciso que la estación de destino deba tener una ruta hasta éste. Recordemos que las conexiones inalámbricas no siempre son bidireccionales, por lo cual se deberá tomar con precaución este proceso. En caso de que la estación destino tenga en su chequeo una ruta hasta el emisor, se utilizaría esta para enviar el paquete RREP. En caso de que no exista esa entrada en el chequeo, deberá utilizar la ruta en reversa que esta almacenada en el paquete RREQ.

Los protocolos de encaminamiento convencionales integran los procesos de descubrimiento de ruta y de mantenimiento de esas rutas, enviando continuamente actualizaciones de la información de encaminamiento. Si el estado de un router o de una conexión cambia, las actualizaciones periódicas reflejarán eventualmente los cambios a los otros integrantes de la red, y presumiblemente se computarán nuevas rutas. Sin embargo, si se utiliza el proceso de descubrimiento de ruta, no existe ningún tipo de actualización periódica que permita relevar estos

cambios. En lugar de esto, mientras una ruta esta en uso, se ejecuta un procedimiento de *Mantenimiento de Ruta* que monitorea el estado de las rutas e informa al nodo fuente de cualquier error.

Como las redes inalámbricas son inherentemente menos confiables que las cableadas, muchas redes inalámbricas utilizan un acuse de recibo (ACK) salto por salto a nivel de capa de enlace de datos, de forma de proveer un mecanismo para detectar fallos y paquetes con errores, y poder retransmitirlos. En estas redes, el mantenimiento de las rutas puede ser fácilmente provisto, desde que en cada salto, el nodo que transmite el paquete puede verificar si esa conexión sigue funcionando. Si la capa de enlace de datos reporta un problema de transmisión que no se puede solucionar, ese nodo envía un paquete de *error de ruta (RERR)* al nodo emisor original. El paquete REER contiene las direcciones de las dos puntas de la conexión con errores: la del nodo que encontró el error, y la del nodo que no pudo ser alcanzado. Cuando un paquete RERR es recibido, la conexión con errores es removida de todas las entradas de la tabla del nodo original.

6.3.2.3 Temporally-Ordered Routing Algorithm (TORA)

Este protocolo ha sido desarrollado para adaptar sus operaciones en ambientes de redes altamente dinámicas. Fue diseñado para minimizar las reacciones frente a los cambios de topología. Un concepto clave para su diseño, es que los mensajes de control se intercambian generalmente entre un pequeño grupo de nodos. Además garantiza que las rutas generadas no tendrán bucles, y que proveerá múltiples rutas para un mismo par origen-destino.

El protocolo puede ser dividido en tres funciones básicas:

- Crear Rutas.
- Mantener Rutas.
- Y Borrar Rutas.



Para *crear una ruta* desde un nodo dado hasta otra estación, requiere el establecimiento de una secuencia de enlaces directos que conduzcan los paquetes de un nodo al otro. Esta función es iniciada solamente cuando un nodo que no posea enlaces directos, requiera una ruta a cierto destino. Por lo cual, crear rutas corresponde esencialmente a asignar direcciones a los enlaces de una red no direccionada, o en una porción de esta, creando un grafo acíclico diseccionado (DAG) orientado al nodo destino (Ver Figura 6.4).

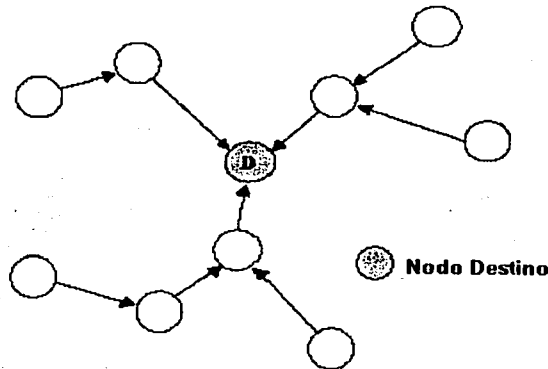


Figura 6.4. TORA. Grafo acíclico diseccionado (DAG) orientado al nodo destino.

El *mantenimiento de ruta*, se refiere a las acciones que debe llevar a cabo el protocolo para reaccionar a los cambios de topológicos de la red, de forma tal que las rutas hasta un destino dado se puedan restablecer en un tiempo finito. Es decir, que se reconstruirá el DAG en un periodo de tiempo finito.

La función de *borrado de rutas* es ejecutada cuando se detecta la partición del DAG, es decir, se pierde alguna conexión. En este caso, todos los enlaces (en la porción de red que fue particionada desde el destino) deberán ser borrados. Para poder realizar estas tres funciones, el protocolo cuenta con distintos paquetes de control: El utilizado para crear rutas: *query (QRY)*, el utilizado para crear rutas y mantenerlas: *update (UPD)*, y el utilizado para borrar rutas: *clear (CLR)*.

6.3.2.3.1 Funcionamiento

Durante las fases de creación y mantenimiento de las rutas, los nodos utilizan una métrica llamada *peso o altura* para establecer el DAG (el grafo diseccionado acíclico) orientado a la estación destino. Luego, se le asigna a cada enlace una dirección (corriente abajo o corriente arriba) basada en el peso de los dos nodos que la componen (ver Figura 6.5).

El grafo esta orientado al destino, el cual posee la menor altura de todos los nodos. Sin embargo, el nodo fuente que origino el paquete QRY no será necesariamente la estación con más altura en la red. Esto puede conducir a la situación donde múltiples rutas son posibles desde el nodo fuente al destino, pero solamente un camino es descubierto. La razón de esto, es porque la altura es inicialmente basada en la distancia en número de saltos al destino.

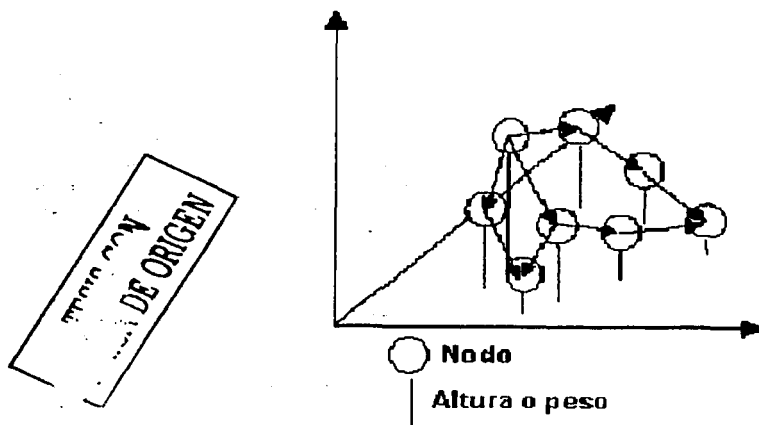
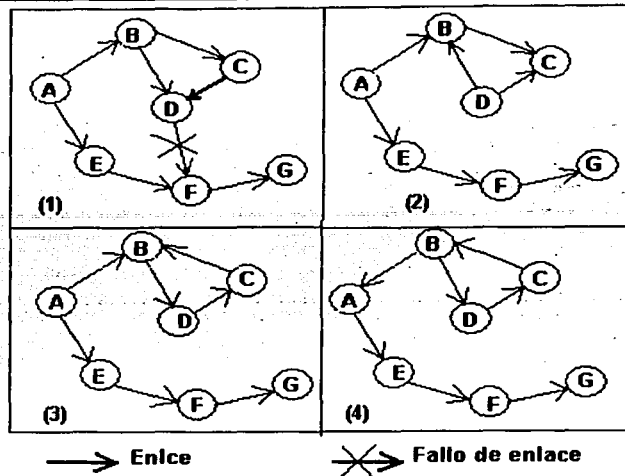


Figura 6.5. TORA. Creación de grafo en base a sus alturas.

Cuando los nodos se mueven, es muy probable que el DAG se particione, por lo cual se deberá ejecutar el algoritmo de mantenimiento, de forma de restablecer el grafo orientado a un destino dado.

Luego de un fallo en el último enlace corriente abajo (Figura 6.6(1)), un nodo generará un nuevo nivel de referencia, y luego lo difundirá a todos sus vecinos, de forma de coordinar una reacción estructurada para asimilar el fallo. Los enlaces serán redireccionados para reflejar los cambios del nuevo nivel de referencia. Esto tiene el mismo efecto que cuando se cambia la dirección de uno o más enlaces cuando un nodo no tiene conexiones corriente abajo.



TESIS CON
 FALLA DE ORIGEN

Figura 6.6. TORA. Mantenimiento de la ruta.

En resumen la idea básica es la siguiente, cuando un nodo pierde su último enlace corriente abajo (E.): se convierte en un mínimo local) como consecuencia de un fallo en la conexión, este selecciona una nueva "altura" de forma de convertirse en un máximo global, definiendo un nuevo nivel de referencia. Por regla, cualquier nuevo nivel creado, es más alto que cualquier otro existente. Como consecuencia de esta acción será necesario redireccionar los enlaces, lo cual puede causar que otros nodos también pierdan sus últimos enlaces corriente abajo. Estos nodos ejecutarán un redireccionamiento parcial, con respecto a sus vecinos que posean alturas ya asociadas con el nuevo nivel de referencia. De esta manera, el nuevo nivel de referencia es propagado desde el lugar donde fallo el enlace hacia el resto de la red. Esta propagación se extenderá solo a los nodos que hayan perdido todas las rutas hacia el destino.

6.3.2.4 Associativity-Based Routing (ABR)

El protocolo Associativity-Based Routing se caracteriza por crear rutas libres de bucles, por no generar deadlocks (o bloqueos), ni paquetes duplicados. El ABR define una nueva métrica en el área de las redes Ad Hoc, la cual es llamada *Asociación por Estabilidad*. Por lo cual, las rutas son generadas a partir del grado de asociación de estabilidad que hay entre los nodos. Cada estación difunde periódicamente un paquete, para avisar a sus vecinos que se encuentra en ese lugar. Cuando sus vecinos reciben el aviso, actualizan sus tablas de *asociación* incrementando un contador en la entrada del nodo emisor del paquete. La asociación por estabilidad, es definida por la estabilidad de los enlaces de un nodo con respecto a otra estación, a través del tiempo y del espacio. Un alto nivel de asociación por estabilidad indica poco movimiento de un nodo, mientras que un bajo nivel indica que el nodo se mueve constantemente. Los contadores de asociación son llevados a cero cuando los vecinos del nodo, o el nodo mismo se mueven fuera del área de cobertura. El objetivo fundamental del protocolo ABR es generar y mantener rutas para redes móviles Ad Hoc, que tengan un tiempo de vida más largo.

El ABR presenta tres fases en su funcionamiento:

- Descubrimiento de la ruta.
- Reconstrucción de la ruta.
- Borrado de rutas.

La fase de descubrimiento de ruta es realizada mediante la difusión de un paquete de *pedido de ruta* (BQ) y un ciclo de *espera de respuesta* (REPLY). Cuando un nodo desea encontrar otra

estación móvil en la red, deberá difundir un paquete BQ para buscar otros nodos que posean una ruta al destino. Todas las estaciones que reciben el BQ (que no son el nodo destino) añaden sus direcciones, la información de *asociación con sus vecinos* y los parámetros de QoS (calidad de servicio) a la cabecera del paquete. El nodo sucesor borra toda la información de asociación del nodo corriente arriba, y deja solo su información y la del nodo corriente abajo. De esta manera, cuando el paquete llega al destino, contendrá toda la información de asociación de los nodos que componen la ruta para llegar al destino. Por lo cual, el nodo destino podrá seleccionar la mejor ruta hasta el nodo fuente, mediante el análisis de la información de asociación de todos los nodos. Luego la estación destino envía un paquete REPLY de vuelta a el nodo fuente a través de la ruta encontrada. Las estaciones que propagan el REPLY marcan la ruta como valida, mientras todas las demás permanecen inactivas, por lo cual no existirán paquetes repetidos.

La tarea de *reconstrucción de las rutas* (RRC) consiste en un descubrimiento de ruta parcial, un borrado de las rutas invalidas, una actualización de las rutas validas, y un nuevo descubrimiento de ruta, dependiendo de cual nodo se movió. El movimiento del nodo fuente, como se muestra en la figura 6.7, requerirá un nuevo proceso de descubrimiento de ruta.

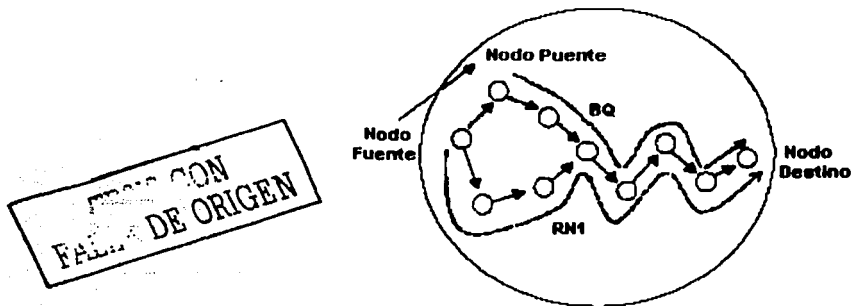


Figura 6.7. ABR. Mantenimiento de ruta cuando un nodo fuente se mueve.

EL mensaje RN[1], es una notificación utilizada para borrar las entradas de ruta asociadas con los nodos corriente abajo. Cuando es el destino el que se mueve, el nodo inmediato corriente arriba borra sus rutas y determina si el nodo es aún alcanzable mediante un *proceso de localización* (LQ[H]), donde H se refiere al contador de saltos del nodo corriente arriba hasta el destino (Figura 8). Si el nodo destino recibe el paquete LQ, entonces responde con un REPLY, con la mejor ruta parcial disponible; de otra forma, el nodo que inicio el proceso presenta un TIME OUT, por lo cual el proceso retrocede a la próxima estación corriente arriba. Para esto se envía un mensaje RN que borra la ruta inválida, e informa a ese nodo que deberá iniciar el proceso LQ. Si el proceso antes comentado, llega hasta la mitad de la ruta, entonces se discontinúa y se comienza un proceso BQ desde el nodo fuente.

Cuando una ruta ya no es necesaria, el nodo fuente inicia la difusión de un proceso de *borrado de ruta* (RD), para que los nodos que la componen actualicen sus tablas.

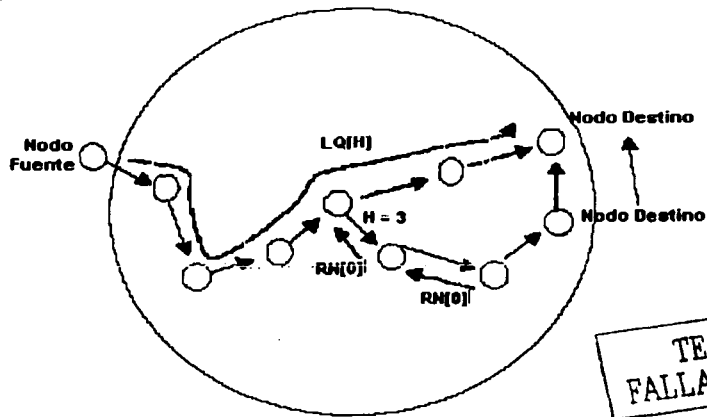


Figura 6.8. ABR. Mantenimiento de ruta para cuando el nodo destino se mueve.

6.4 Comparación de los Protocolos

6.4.1 Protocolos Proactivos

PARÁMETROS	DSDV	CGSR	WRP
Complejidad Tiempo	$O(D)$	$O(d)$	$O(h)$
Complejidad: Comunicación	$O(x = N)$	$O(x = N)$	$O(x = N)$
Direccionamiento	Plana	Jerárquica	Plana
Libre de bucles	Si	Si	Si, pero no instantaneamente
Número de tablas requerido	Dos	Dos	Cuatro
Frecuencia de transmisión de actualizaciones	Periódicamente y cuando se necesite	Periódicamente	Periódicamente y cuando se necesite
Actualizaciones transmitidas a	Vecinos	Vecinos y Cluster Head	Vecinos
Utilización número de secuencia.	Si	Si	Si
Utilización de mensajes HELLO	Si	No	Si
Nodos críticos	No	Si (Cluster Head)	No
Métricas de encabezamiento	Camino más corto	Camino más corto	Camino más corto
Capacidad de Multicast	No	No	No

Abreviaturas

N = Número de nodos en la red.

D = Diámetro de la red.

h = altura del árbol de encabezamiento.

x = número de nodos afectados en un cambio de la topología.

6.4.2 Protocolos Reactivos

PARÁMETROS	AODV	DSR	TORA	ABR
Complejidad : Tiempo (inicialización)	O (2D)	O (2d)	O (2d)	O (2d+z)
Complejidad : Tiempo (Luego de un fallo)	O(2d)	O(2d) ó 0**	O(2d)	O(l+z)
Complejidad: Comunicación (Inicialización)	O(2N)	O(2N)	O(2N)	O(N+y)
Complejidad: Comunicación (Luego de un fallo)	O(2N)	O(2N)	O(2N)	O(x+y)
Direccionamiento	Plano	Plano	Plano	Plano
Libre de bucles	SI	SI	SI	SI
Capacidad Multicast	SI	NO	NO	NO
Utilización de paquete ALIVE *	NO	NO	NO	SI
Posibilidad de Múltiples rutas	NO	SI	SI	NO
Utilización de la mejor ruta o tablas de control de tiempo	SI	NO	NO	NO
Metodología de reconfiguración de rutas.	Borrar Ruta, Notificar Fuente	Borrar Ruta, Notificar Fuente	Reparación de ruta	Búsqueda de ruta parcial
Métricas de encaminamiento.	Ruta más corta y actualizada	Ruta más corta	Ruta más corta	Asociatividad y camino más largo
Rutas mantenidas en:	Tablas de R	Chequeo de R	Tablas de R	Tablas de R

Abreviaturas:

l = Diámetro del segmento de red afectado.

y = Número total de nodos formando el camino por donde el paquete REPLY transita.

z = Diámetro del camino por donde el paquete REPLY transita.

N = Número de nodos en la red

d = Diámetro de la red.

h = altura del árbol de encaminamiento.

X = Número de nodos afectados en un cambio de la topología.

**TESIS CON
FALLA DE ORIGEN**

7. Computación Móvil y Computación Esparcida (Pervasive)

Las computadoras personales, Internet y la World-Wide Web han influido ya en muchos aspectos del mundo de los negocios y hay señales evidentes de una amplia convergencia de industrias enteras como la de los medios de comunicación, entretenimiento, electrónica de consumo, telecomunicaciones, y tecnología de la información. La siguiente ola de la revolución tecnológica nos afectará directamente y en todos los aspectos de nuestra vida cotidiana.

De forma contraria a lo que las predicciones populares decían, el siglo XXI se caracterizará menos por la colonización de la luna, las ciudades submarinas y los coches de energía nuclear (lo cual requiere inversiones enormes en infraestructura), que por las aplicaciones basadas en tecnologías de lo diminuto y por lo tanto casi invisibles como la biotecnología, la nano-tecnología y la microelectrónica, y será muy interesante ver qué sinergias se desarrollan entre estas áreas.

Durante más de 30 años la conocida ley de Moore, según la cual la funcionalidad de un procesador se duplica cada 18 meses, ha demostrado ser cierta. Una mejora similar en prestaciones se aplica también a algunos otros parámetros importantes de la tecnología. Estamos seguros ahora de que la tendencia actual continuará durante unos cuantos años más, lo que hace que toda esta área de desarrollo sea tan intrigante. Ahora parece que el futuro próximo estará caracterizado por pequeñas computadoras que se comunican de forma espontánea, que por su tamaño tan pequeño y por su bajo precio, se integrarán en casi todos los objetos cotidianos. La tecnología de la información por lo tanto se volverá ubicua e invadirá todos los aspectos de nuestras vidas.

Los teléfonos móviles con acceso a Internet y los Asistentes Digitales Personales (*Personal Digital Assistants*, PDAs) que se comunican sin cables con otros dispositivos próximos a ellos son los primeros indicios de la era *-post-PC-*venidera. Al principio, el principal objetivo es permitir el acceso a la información de cualquier tipo desde cualquier lugar y en cualquier momento, lo que evidencia los esfuerzos actuales de la industria por integrar aparatos de información móvil y utilizable en procesos de negocios basados en la Web y escenarios de comercio electrónico. Sin embargo, a largo plazo, esta continua tendencia tecnológica puede dar lugar a la fusión del la computadora con los objetos cotidianos típicos para que se vuelva literalmente invisible.

Aunque el mundo físico no se transforme en una enorme plataforma única informática interactiva tan rápidamente como algunos expertos creen, está claro que, con la creciente informatización y la conexión en red de los objetos cotidianos, nos estamos volviendo cada vez más dependientes de sistemas fiables de la tecnología de la información.

Este capítulo se dedica a la tendencia actual hacia la informatización y conexión en red de todas las cosas a menudo expresada con los términos de computación ubicua o computación pervasiva (es decir, ampliamente difundida). Aspira a proporcionar una primera noción de las técnicas, las expectativas y los antecedentes que llevan a un futuro invadido por la tecnología de la información.

7.1 Computación Móvil

La Computación móvil es un término que se refiere a varios elementos nuevos de la computación. Uno de los elementos que comprende es el de la **computación omnipresente** - que son computadoras y sensores integrados en diferentes dispositivos, electrodomésticos, herramientas, en el hogar y en lugares de trabajo y fábricas y hasta en la ropa. Otro elemento se presenta en la **comunicación continua** - un alto grado de comunicación entre dispositivos y sensores con infraestructura ubicua en una red segura con el núcleo alambrado y con aditamentos inalámbricos que se comunican con el núcleo. Debido a que el cómputo está logrando integrarse tanto en nuestras vidas y actividades, la interacción humano-computadora, como por ejemplo el diálogo hablado con las computadoras, llegará a ser muy importante.

Descubrir estos tipos de servicios en forma dinámica se está volviendo muy importante en el presente escenario. En el futuro cercano, un servicio debería seleccionarse automáticamente para un trabajo, teniendo en consideración su ubicación física, historia previa, y diversa información semántica adicional. El mecanismo de descubrimiento necesita moverse más allá de la comparación trivial de atributo o interfaz. El mecanismo de descubrimiento debería estar mucho más basado en conocimiento, y la inteligencia artificial jugará un rol importante en la selección del servicio. Para construir una arquitectura de descubrimiento de servicios eficiente es necesario enfocarnos en los siguientes puntos.

1. Eficiencia del mecanismo de descubrimiento, es decir, que tan rápido y barato puede descubrirse un servicio.
2. Confiabilidad del mecanismo de comunicaciones subyacente: si el mecanismo de comunicaciones subyacente no es confiable, entonces el protocolo tiene que ajustarse de manera acorde.
3. Administración del tiempo de vida del servicio: En un entorno dinámico, los servicios podrían estar disponibles por un período de tiempo acotado.
4. Aspectos de seguridad: usuarios maliciosos no debería ser capaces de acceder a servicios seguros.

7.1.1 Mecanismos y Protocolos de Descubrimiento de Servicios

A continuación mencionamos los protocolos de descubrimiento de servicios existentes:

- Protocolo de Ubicación de Servicios (SLP - Service Location Protocol).
- Jini, una arquitectura de descubrimiento de servicios basada en Java.
- Universal Plug and Play (UPnP), la solución de Microsoft al descubrimiento de servicios.
- Salutation, protocolo liviano de descubrimiento de servicios independiente del protocolo de red.

Tratamos de identificar algunos de los problemas inherentes asociados con las arquitecturas de descubrimiento existentes.

7.1.1.1 SLP - Service Location Protocol

El Protocolo de Ubicación de Servicios SLP (Service Location Protocol) es un producto del Grupo de Trabajo del Protocolo de Ubicación de Servicios SVRLOC (Service Location Protocol Working Group) de la Fuerza de Ingeniería de Internet IETF (Internet Engineering Task Force). Es un protocolo para descubrimiento automático de servicios para redes basadas en el Protocolo Internet. SLP es un protocolo independiente del lenguaje. De este modo la especificación del protocolo puede implementarse en cualquier lenguaje. Basa su mecanismo de descubrimiento en atributos de servicio, los cuales son en esencia formas diferentes de describir a un servicio. Puede satisfacer formas de servicios tanto de hardware como de software.

La infraestructura SLP consiste en tres tipos de agentes:

1. Agentes Usuarios
2. Agentes de Servicio
3. Agentes de Directorio

Los Agentes Usuarios adquieren vínculos de servicios para las aplicaciones de usuario final que piden los servicios. Los Agentes de Servicio son responsables de publicar los vínculos de servicio a los Agentes de Directorio haciendo así que los servicios estén disponibles a los Agentes Usuarios. El Agente de Directorio mantiene una lista de servicios publicados en una red.

SLP ofrece los siguientes servicios:

1. Obtener vínculos de servicios para los Agentes de Usuarios.
2. Mantener el directorio de servicios publicados.
3. Descubrir atributos de los servicios disponibles.
4. Descubrir Agentes de Directorio disponibles.
5. Descubrir los tipos disponibles de Agentes de Servicio.

TESIS CON
FALLA DE ORIGEN

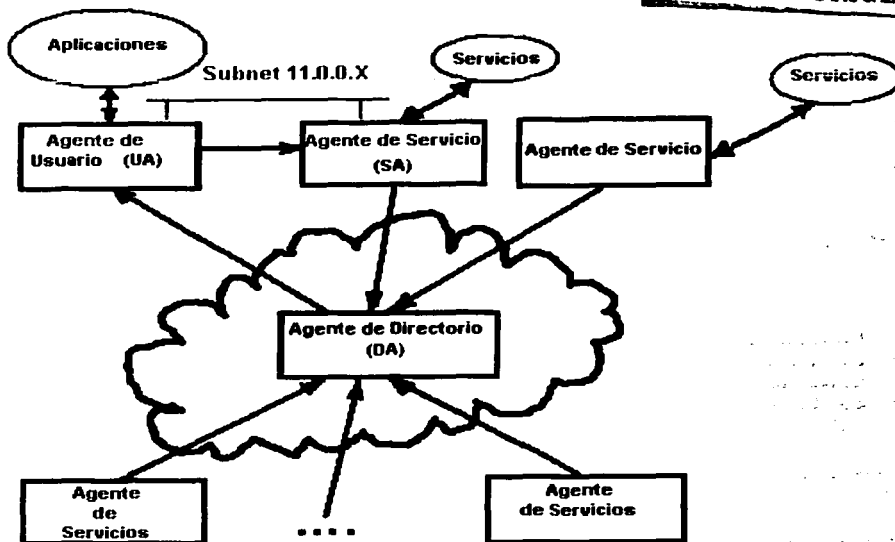


Figura 7.1 Las transacciones básicas del protocolo de Ubicación de Servicios:

Un servicio se describe por los valores de configuración de los posibles atributos para ese servicio. Por ejemplo, un servicio que permite a los usuarios descargar contenido de audio o video puede describirse como un servicio que es sin-cargo o pago-por-uso. SLP también soporta un mecanismo simple de arriendo de registro de servicios que maneja los casos donde el hardware del servicio está averiado pero el servicio continúa siendo anunciado.

7.1.1.2 Jini

Jini es una arquitectura distribuida orientada a servicios desarrollada por Sun Microsystems. Los servicios en Jini pueden representar dispositivos de hardware, programas de software, o una combinación de los dos. Una colección de servicios Jini forma una federación Jini. Los servicios Jini coordinan unos con otros dentro de la federación. El objetivo general de Jini es convertir a la red en una herramienta flexible y fácilmente administrable en la cual los clientes computacionales y humanos puedan encontrar servicios en un modo robusto y flexible. Jini esta diseñada para hacer a la red una entidad más dinámica que refleje mejor la naturaleza dinámica del grupo de trabajo al posibilitar la capacidad de agregar y quitar servicios en forma flexible.

Uno de los componentes claves de Jini es el Servicio de Búsqueda Jini JLS (Jini Lookup Service), el cual mantiene información dinámica acerca de los servicios disponibles en una federación Jini. Cada servicio debe descubrir uno o más Servicios de Búsqueda Jini antes de que pueda ingresar

en una federación. La ubicación del JLS podría conocerse de antemano, o podrían descubrirse usando *multicast*. Un JLS puede en potencia estar disponible a la red local o a otras redes remotas (por Ej. Internet). El JLS también puede asignarse para tener nombres de grupo de modo que un servicio pueda descubrir a un grupo específico en su vecindad.

Cuando un servicio Jini quiere unirse a una federación Jini, primero descubre uno o más JLS de la red local o redes remotas. El servicio entonces carga su *proxy* de servicio (es decir, un conjunto de clases Java) al JLS. Los clientes de servicio pueden usar este *proxy* para contactar al servicio original e invocar métodos del servicio. Ya que los clientes de servicio sólo interactúan con *proxies* de servicio basados en Java, esto permite que varios tipos de servicios, tanto servicios de hardware y software, sean accedidos de modo uniforme. Por ejemplo, un cliente de servicio puede invocar pedidos de impresión a un servicio de impresión PostScript aún si no tiene ningún conocimiento del lenguaje PostScript.

Un usuario que busque un servicio en una red primero envía en simultáneo (*multicast*) una consulta para encontrar el JLS en la red. Si existe un JLS, el objeto remoto correspondiente se descarga a la máquina del usuario. El usuario entonces usa el objeto para encontrar el servicio deseado. En Jini, el descubrimiento de servicios se hace por coincidencia (*matching*) de interfaz o coincidencia de atributos Java. Si el JLS contiene un servicio válido implementando la interfaz especificada por el usuario, entonces se descarga un *proxy* para ese servicio en la máquina del usuario. El *proxy* se usa de ahora en adelante para llamar a diferentes funciones ofrecidas por el servicio.

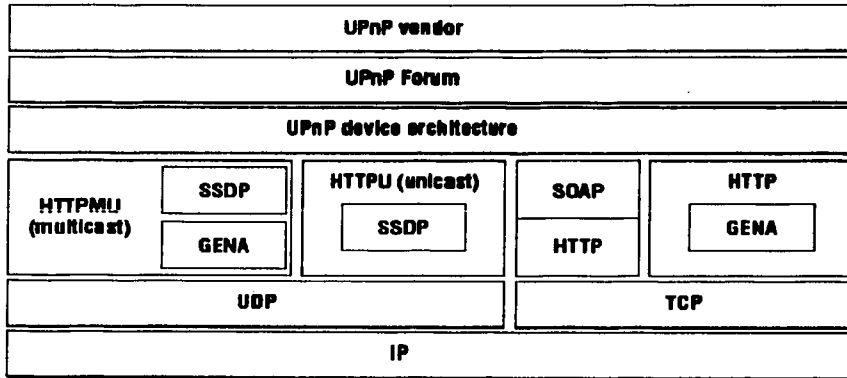
7.1.1.3 Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP), impulsado básicamente por Microsoft, es una arquitectura que evoluciona diseñada para extender el modelo original de periféricos *Plug and Play* de Microsoft a un mundo altamente dinámico de muchos dispositivos de red provistos por muchos proveedores. UPnP trabaja básicamente con conjuntos de protocolos de red de las capas más bajas (esto es, TCP/IP), implementando estándares a este nivel, figura 7.2. UPnP intenta asegurar que todos los fabricantes de dispositivos pueden adherir rápidamente al estándar propuesto sin mayores problemas. Al brindar una conjunto de protocolos de red definidos, UPnP permite que los dispositivos construyan sus propias APIs (Application Programming Interfaces) que implementen estos protocolos - en cualquier lenguaje o plataforma que ellos elijan.

UPnP usa el Protocolo Simple de Descubrimiento de Servicios SSDP (Simple Service Discovery Protocol) para descubrir servicios en redes basadas en el Protocolo Internet. SSDP puede operarse con o sin un servicio de directorio o búsqueda en la red. SSDP opera sobre los protocolos abiertos existentes, usando HTTP (HyperText Transfer Protocol) tanto sobre envío único (*unicast*) y envío múltiple (*multicast*) UDP (User Datagram Protocol). El proceso de registro envía y recibe datos en forma de hipertexto, pero tiene alguna semántica especial.

Cuando un servicio quiere unirse a la red, primero envía un mensaje de aviso (o anuncio), notificando al mundo acerca de su presencia. En el caso de aviso de envío múltiple, el servicio envía el aviso en una dirección de envío múltiple reservada. Si está presente un servicio de directorio o búsqueda, éste puede registrar tales avisos. Mientras tanto, otros servicios en la red pueden ver directamente estos avisos. El mensaje de "aviso" contiene un URL (Universal Resource Locator) que identifica el servicio publicado y un URL a un archivo que brinda una descripción del servicio publicado.

Cuando un cliente de servicios quiere descubrir un servicio, puede tanto contactar al servicio directamente a través del URL que se provee en el anuncio del servicio, o puede enviar un pedido de búsqueda de envío simultáneo (*multicast*). En el caso de descubrir un servicio a través del pedido de búsqueda de envío simultáneo, el pedido del cliente puede ser respondido por el servicio directamente o por un servicio de directorio o búsqueda. La descripción del servicio no juega ningún rol en el proceso de descubrimiento del servicio.



GENA: General Event Notification Architecture
SOAP: Simple Object Access Protocol
SSDP: Simple Service Discovery Protocol
UDPs: User datagram packets
UPnP: Universal Plug and Play

TESIS CON
FALLA DE ORIGEN

Figura 7.2 Arquitectura del Protocolo UPnP

7.1.1.4 Salutation

Salutation es un protocolo de descubrimiento de servicios y administración de sesión desarrollado por compañías líderes de la tecnología de la información. Salutation es un estándar abierto independiente de sistemas operativos, protocolos de comunicaciones y plataformas de hardware. Salutation fue creado para resolver los problemas de descubrimiento de servicios y utilización entre un amplio conjunto de dispositivos y equipos en un entorno de gran cobertura de conectividad y movilidad. La arquitectura provee aplicaciones con diferentes servicios que son escasos a través de toda la red. También contiene funciones para descubrir las capacidades de servicios remotos. Salutation brinda características para que una aplicación establezca sesiones que operen con cualquier servicio remoto.

La arquitectura Salutation define una entidad llamada Administrador Salutation SLM (Salutation Manager) que funciona como un intermediario de servicios para los servicios en la red. Las diferentes funciones de un servicio están representadas por unidades funcionales. Las Unidades Funcionales representan características esenciales de un servicio (por Ej. fax, impresora, escáner, etc.). Además, los atributos de cada Unidad Funcional se capturan en el Registro de Descripción de Unidad Funcional. Salutation define la sintaxis y semántica del Registro de Descripción de Unidad Funcional (por Ej. nombre, valor). SLM puede ser descubierto por los servicios en un número de maneras tales como:

1. Usando una tabla estática que guarda la dirección de transporte del SLM remoto.
2. Enviando una consulta de descubrimiento usando el protocolo definido por la arquitectura Salutation.
3. Preguntando la dirección de transporte del SLM remoto a través de un servidor de directorio central. Este protocolo está indefinido por la arquitectura Salutation, sin embargo, la especificación actual sugiere el uso de SLP.
4. El servicio especifica directamente la dirección de transporte del SLM remoto.

El proceso de descubrimiento de servicios puede realizarse a través de múltiples SLMs. Un SLM puede descubrir otros SLMs remotos y determinar los servicios que están registrados allí. El Descubrimiento de Servicios se lleva a cabo comparando el tipo de servicio requerido, según lo especifica el SLM local, con el tipo de servicio disponible en un SLM remoto. Se usan Llamadas a Procedimientos Remotos para transmitir el tipo de servicio requerido desde el SLM local al SLM remoto y para transmitir la respuesta desde el SLM remoto al SLM local. El SLM determina las características de todos los servicios registrados en un SLM remoto al manipular la especificación del tipo de servicio requerido. También puede determinar las características de un servicio específico registrado en un SLM remoto o la presencia de un servicio específico en un SLM remoto al comparar un conjunto específico de características.

7.1.2 Comparación de Técnicas de Descubrimiento de Servicios Existentes

Los protocolos descritos en esencia usan atributos típicos o comparación de interfaz para comparar los servicios existentes en la red. SLP asume la existencia de un mecanismo subyacente basado en el Protocolo Internet (IP) y usa UDP (User Datagram Protocol) para comunicarse. Salutation en contraste es una arquitectura independiente de protocolo de red. La presencia de un administrador de transporte en Salutation aísla el mecanismo de comunicación subyacente del administrador de salutation. De este modo se espera que salutation tenga prominencia cuando estén en función redes no basadas en el Protocolo Internet. UPnP trabaja con conjuntos de protocolos de más bajo nivel y su especificación está basada en la suposición de una red tipo Protocolo Internet por debajo.

Tanto SLP, Salutation y UPnP son protocolos independientes del lenguaje. Las especificaciones del protocolo pueden implementarse en cualquier lenguaje. Jini por otra parte es totalmente dependiente de Java para su implementación. Java es un lenguaje independiente de la plataforma lo cual hace a su vez a Jini independiente de la plataforma. En Jini, la interacción entre servicios y usuarios está definida en términos de la interfaz de un objeto, mientras que en UPnP, la interacción está definida en términos de un protocolo de red. UPnP usa un esquema de coincidencia basado en XML para descubrir servicios. Jini en cambio usa interfaces Java.

UPnP y Salutation usan en esencia *multicasting* para encontrar servicios o escuchan a pedidos de servicios para encontrar la ubicación de los servicios deseados. Jini por su parte usa un esquema centralizado donde todos los tipos de servicios se registran en un servicio de búsqueda. Los usuarios contactan al servicio de búsqueda para descubrir los servicios existentes en la red. El Protocolo de Ubicación de Servicios implementa un esquema basado en un directorio centralizado como también un esquema de envío simultáneo para descubrir servicios. Mientras que los esquemas centralizados del Protocolo de Ubicación de Servicios y Jini son más escalables, son también candidatos a tener un único punto de falla. Salutation a diferencia de Jini es un protocolo liviano y hace menos suposiciones del protocolo subyacente y recursos de computación. De este modo puede llevarse fácilmente a dispositivos de mano poco potentes. Jini en cambio, debido a su dependencia de Java requiere considerables recursos de computación para funcionar correctamente.

7.1.3 Deficiencias en las Arquitecturas Existentes de Descubrimiento de Servicios

Todas las infraestructuras y arquitecturas de descubrimiento de servicios mencionadas arriba como SLP, Jini, UPnP, y Salutation han sido desarrolladas para explorar los aspectos de descubrimiento de servicios en el contexto de sistemas distribuidos. Mientras muchas de las arquitecturas brindan una buena base para desarrollar sistemas con componentes distribuidos en redes, no solucionan de forma adecuada todos los problemas que pueden surgir en un dominio dinámico.

Algunas de las deficiencias son:

- *Falta de representación.* Los servicios en el Comercio Electrónico son heterogéneos por naturaleza. Estos servicios se definen en términos de sus funcionalidades y capacidades. Las descripciones de funcionalidad y capacidad de estos servicios son usados por los

clientes del servicio para descubrir los servicios deseados. Coincidencia de atributos es un componente muy importante para encontrar los servicios apropiados en tal entorno. Las arquitecturas de descubrimiento de servicios existentes carecen de lenguajes expresivos, representaciones y herramientas que sean buenas al representar un amplio rango de descripciones de servicios y sean buenas para razonar acerca de las funcionalidades y capacidades de los servicios. Por Ej., los protocolos de descubrimiento de servicios no usan ningún parámetro de rendimiento para los servicios existentes. Solamente están satisfechos con encontrar un servicio. No consideran si el servicio sería capaz de atender el pedido.

- *Falta de comparación inexacta.* En la arquitectura Jini, las funcionalidades y capacidades de los servicios se describen en términos de objetos Java de interfaces. Las coincidencias de capacidad de Servicios son procesados solamente a nivel objeto y a nivel sintaxis. Por ejemplo, la Búsqueda Jini genérica y otros protocolos de descubrimiento permite que un servicio cliente encuentre un servicio de impresión que soporte impresión a color, pero los protocolos no son lo suficientemente potentes para encontrar el servicio de impresión geográficamente más cercano que tenga la cola de impresión más corta. Los protocolos realizan comparación semántica exacta mientras encuentran un servicio. De esta forma ellos pierden el poder de dar una "coincidencia justa" aun si estaba disponible.

7.1.4 Técnicas de Descubrimiento de Servicios Mejoradas para Comercio Móvil

Habiendo identificado algunas de las deficiencias comunes en las técnicas de descubrimiento de servicios existentes, presentamos una breve descripción de como resolver dichas deficiencias. Uno puede mejorar el mecanismo de descubrimiento de servicios aplicando herramientas y técnicas de Inteligencia Artificial a los sistemas existentes. El proyecto XReggie se concentra en mejorar la coincidencia de atributos más allá del la comparación trivial basado en sintaxis. Con el advenimiento de redes ad-hoc y aproximaciones basados en agentes, será extremadamente necesario comunicarse entre diferentes grupos de agentes en diferentes redes quienes hablan diferentes lenguajes. En el proyecto Ronin se ha resuelto este problema y provisto una marco para dichas comunicaciones.

7.1.4.1 El Marco de Agentes Ronin

El Marco de Agentes Ronin es un desarrollo de agente distribuido basado en Jini. Ronin introduce una arquitectura híbrida, una composición de arquitectura orientada a servicios y orientada a agentes, para desplegar en sistemas distribuidos dinámicos. Entre muchas de las características distinguibles del marco, Ronin ofrece una facilidad de descripción de agente simple pero potente que permite que los agentes se encuentren unos a otros y una infraestructura que alienta el rechazo de aplicaciones de Inteligencia Artificial no Java.

En Ronin, los agentes se describen usando dos tipos de atributos: los atributos de Agente Común y los atributos de Agente de Dominio. Estos son dos conjuntos de atributos de servicio Jini que están asociados con cada agente Ronin en el Servicio de Búsqueda Jini. Los atributos de Agente Común definen las funcionalidades y capacidades genéricas de un agente de modo independiente del dominio. Los atributos de Agente de Dominio definen las funcionalidades específicas del dominio del agente. El marco define el significado semántico de cada atributo de Agente Común, pero no define el significado semántico de ningún atributo de Agente de Dominio.

La facilidad de descripción de Ronin puede mejorar la infraestructura de descubrimiento de servicios de Jini para Comercio Móvil de la siguiente forma:

1. Como todos los servicios Jini orientados a agentes, los agentes Ronin comparten un conjunto de atributos de Agente Común. Ellos pueden descubrir otros servicios basados solamente en las funcionalidades independientes del dominio de los servicios.
2. Una vez que un servicio ha descubierto a otro servicio usando la facilidad de descripción de Ronin, es posible para estos dos servicios formar una negociación de comunicaciones básica basada en los significados semánticos de los atributos de Agente Común. Por

ejemplo, si un servicio tiene conocimiento acerca del tipo del Lenguaje de Comunicación de Agente ACL (Agent Communication Language) que el otro servicio habla, pueden comenzar su conversación siguiendo el protocolo estándar ACL de negociación predefinido.

Desarrollar infraestructuras que son más "inteligentes" a menudo requiere técnicas y herramientas de IA sofisticadas, tales como motores de inferencia, sistemas de representación de conocimiento, programación con restricciones, etc. Por ejemplo, sería útil para un Servicio de Búsqueda Jini ser capaz de razonar acerca de las capacidades de sus servicios registrados, permitiendo que el JLS haga recomendaciones de búsqueda de servicios más "inteligentes".

El marco Ronin brinda un Servicio de Motor Prolog Jini JPES (Jini Prolog Engine Service). Este servicio provee servicios de motor Prolog remoto para componentes habilitados para Jini en la red. JPES provee una herramienta de programación lógica distribuida para servicios habilitados para Jini. Un Servicio de Búsqueda mejorado puede usar el JPES para razonar acerca de las capacidades de servicios y poder hacer recomendaciones más "inteligentes".

7.1.4.2 Proyecto XReggie

El proyecto XReggie investiga como Jini y sistemas similares pueden ser llevados más allá de sus simples aproximaciones de coincidencia de servicios basadas en sintaxis, agregando poder expresivo a las descripciones de servicios. XReggie agrega las facilidades para describir funcionalidades y capacidades de servicios usando XML (Extended Markup Language). XReggie permite que el descubrimiento de servicios se realice de manera más estructurada y descriptiva. En el corazón de XReggie está el Servicio de Búsqueda Jini mejorado que brinda "ubicación de servicios" para dispositivos habilitados para Jini. XReggie puede ayudar a que los clientes de servicios descubran dichos servicios de manera esencialmente sin cambios respecto de la infraestructura Búsqueda y Descubrimiento Jini. Además, permite que los servicios anuncien sus capacidades en un formato descriptivo bien estructurado usando XML. Aún más, XReggie permite que los servicios sean descubiertos usando descripciones XML.

7.2 Computación Esparcida(Pervasive) o Ubicúa

La computación ubicua o pervasive es nombrada también como Ubicomp 1, nomádica, la tercera ola en la computación o el tercer paradigma. Actualmente, debido a la evolución de la tecnología inalámbrica, así como el éxito comercial de los dispositivos de pequeñas pantallas como los teléfonos celulares y los asistentes digitales personales (PDA's), este paradigma a comenzado a surgir como una opción de implementación real.

Desde sus orígenes, la computación ubicua se concibió como una manera de incrementar el uso de las computadoras, teniendo muchas de estas disponibles, en el ambiente físico en el que nos encontramos, pero invisibles para el usuario.

Al hablar de tener muchas computadoras disponibles en el ambiente que nos rodea, no nos referimos a las computadoras tal y como las conocemos (las PC's), si no a dispositivos periféricos como impresoras, dispositivos de video, audio, etc. con procesadores de bajo poder de procesamiento y dispositivos digitales personales como PDA's, que tienen la capacidad de comunicarse con los demás, ofrecer sus servicios, procesar peticiones y llevar a cabo la función para la cual fueron construidos.

La computación ubicua se caracteriza por dos atributos principales:

- Ubicuidad. Donde las interacciones son dirigidas hacia múltiples interfaces en lugar de una sola computadora.
- Transparencia. Donde la tecnología esta tan incorporada en nuestra vida que es invisible para nosotros.

Debido a las características de este tipo de dispositivos, los cuales son la base de la computación ubicua, nos damos cuenta de que este paradigma esta fuertemente ligado a la movilidad, arquitecturas empotradas, redes inalámbricas, por lo que todas la problemáticas que estas conllevan, son heredadas en esta nueva ola de la computación.

La computación pervasiva representa el eslabón evolutivo más grande en la línea de trabajo en términos de la informatización y de la comunicación a mediados de los 70's. Existen dos eslabones primarios en esta evolución, los sistemas distribuidos y la computación móvil. Muchos problemas técnicos en la computación pervasiva corresponden a problemas ya identificados y estudiados en el comienzo de esta evolución. En muchos de los casos, existen soluciones que se aplican directamente; en otros casos, la demanda de la computación pervasiva es totalmente diferente a las nuevas soluciones que han sido buscadas.

El campo de los sistemas distribuidos surgieron de la intersección de las computadoras personales y las redes de área local LANs. Las investigaciones que siguieron a las hechas a mediados de los 70's y a lo largo de lo principios de los 90's, crearon una trama de trabajo conceptual y las bases para algoritmos que han proveído un valor muy importante en todos los trabajos en los que se involucran dos o más computadoras conectadas por una red, sin importar si es estática o móvil, alambica o inalámbrica. Existen diferentes áreas que caracterizan a la computación pervasiva: las comunicaciones remotas, la falta de tolerancia, disponibilidad, acceso remoto a la información y la seguridad. La computación pervasiva añade cuatro campos adicionales como se muestra en la Figura 7.3.

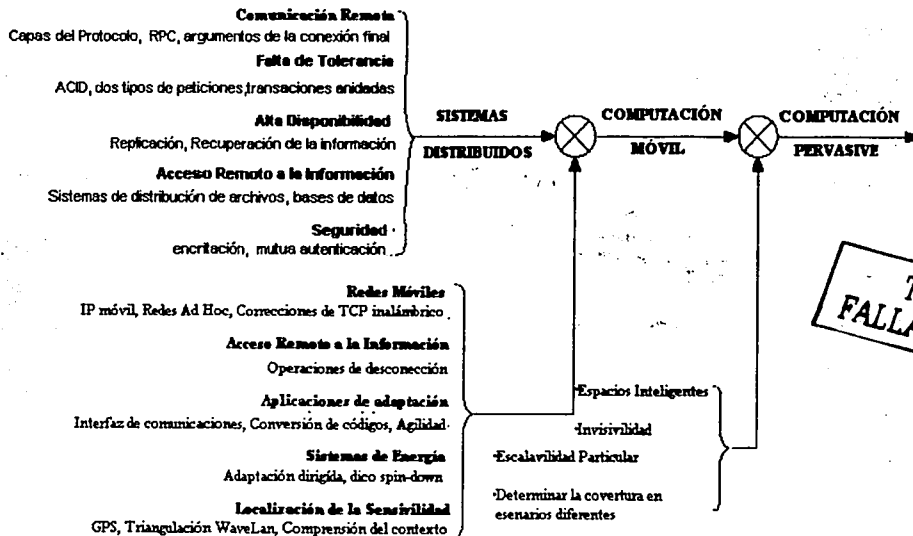


Figura 7.3 Principal Clasificación de la búsqueda de problemas en sistemas de computación pervasiva

Actualmente, la implementación de la computación ubicua, adquiere valor de importancia, debido a los avances de la tecnología, a la necesidad nomadica de transportarnos de un lugar a otro, a la posibilidad de que los dispositivos medien entre ellos, se ofrezcan servicios e intercambien información.

7.2.1 Tipos de Redes que se Despliegan para la Computación Ubicua

La existencia de la computación ubicua normalmente implica el desplegar redes de comunicación heterogéneas, debido a la gran variedad de dispositivos que se pueden conectar y al distinto tipo de información que intercambian. Dependiendo del tipo de tráfico que se quiere transmitir se ha realizado una primera clasificación del tipo de red que se necesita desplegar. Por un lado se exponen las redes de control, adecuadas para controlar cualquier tipo de dispositivo electrónico o eléctrico. A su vez las redes de control se pueden clasificar en redes de propósito general y redes orientadas a la automatización de viviendas. Las primeras se caracterizan por tener un modelo de comunicación orientado a datos, de tal forma que la comunicación de dos dispositivos se realiza estableciendo relaciones entre las variables del emisor y del receptor. En las segundas, para la comunicación entre dispositivos, se definen un conjunto de funciones concretas que especifican las operaciones que se permiten realizar.

Por otro lado se presentan las redes multimedia. Se ha utilizado la denominación de redes multimedia para designar a aquellas redes que son capaces de transmitir voz y vídeo en tiempo real. Este tipo de tráfico tiene dos requerimientos que imponen características mínimas a las redes multimedia:

- La primera restricción se plantea por la necesidad de un ancho de banda mínimo para poder transmitir.
- La segunda restricción viene impuesta porque el tráfico multimedia es isócrono. Cuando se transmite la señal de vídeo-audio digitalizada, se están enviando en cada paquete muestras de la señal. El receptor, según los paquetes, extrae las muestras y puede reconstruir la señal analógica. Para que la reconstrucción sea en tiempo real, el retardo entre dos paquetes consecutivos no puede superar un máximo. Esto obliga a que la red disponga de mecanismos que aseguren un retardo aceptable para toda la transmisión. Las redes de control y las redes multimedia muy previsiblemente van a coexistir durante bastante tiempo, dada la necesidad de transmitir diferentes tipos de información y el costo excesivo de emplear redes multimedia para realizar el control.

Existe una importante división en cuanto al medio físico utilizado que se resume en infraestructuras cableadas e inalámbricas. Por norma general las redes cableadas prefieren la línea de potencia y el par trenzado:

- La línea de potencia tiene la ventaja de que se puede aprovechar el cableado existente modificando solamente los dispositivos, lo cual abarata costos y facilita la integración en la vivienda. Sin embargo es muy sensible al ruido e interferencias. Por otro lado también existe el problema de que los parámetros de la red eléctrica (tensión y frecuencia) cambian según el país, lo cual obliga a duplicar los dispositivos o añadir adaptadores.
- El par trenzado exige tener que desplegar una nueva red, pero ofrece mejores prestaciones. Las redes de control específicas de automatización de viviendas prefieren la solución por línea de potencia, lo cual es lógico ya que es la que les permite mayor cuota de mercado.
- Las redes inalámbricas ofrecen una solución híbrida sobre las anteriores, añadiendo la ventaja de eliminar la necesidad del cableado. Este tipo de redes, que pueden enviar tanto información de control y datos, como información multimedia, se convierten en la opción necesaria de un sistema ubicuo móvil, o como la opción práctica para evitar cablear el entorno ubicuo.

7.2.1.1 Redes de Control

Son redes que se utilizan para el control de los sensores y dispositivos de recepción del entorno ubicuo. Se han identificado dos factores que condicionan el diseño de estas redes:

- La información que envían los sensores o que llega a los dispositivos de recepción no varía muy rápidamente en el tiempo.

- En un entorno pueden existir multitud de estos dispositivos. La primera condición permite crear protocolos sencillos, lo cual enlaza adecuadamente con la segunda condición, ya que el costo añadido a cada uno de los dispositivos será reducido.

7.2.1.1.1 Redes de Propósito General

Dentro de estas redes destacan EIB y LONWork. Ambas se basan en un sistema descentralizado en el que cada uno de los dispositivos conectados tiene control propio. La red se muestra como un bus lógico al cual se añaden los dispositivos. Al utilizar un medio compartido se implementan mecanismos de contienda que permitan solucionar las colisiones. Dado que utilizan un modelo de comunicación orientado a datos, para que dos variables se puedan asociar deben ser del mismo tipo. Esto obliga a que ambos protocolos hayan intentado definir una semántica de datos flexible y lo más completa posible. Esta definición de tipos de datos es la clave para conseguir interoperabilidad entre distintos fabricantes y uno de sus beneficios inmediatos es que los dispositivos puedan realizar un gran número de funciones distintas dependiendo de cómo están interconectados.

➤ EIB

El bus EIB se perfila como uno de los estándares que puede dominar el mercado europeo en los próximos años. Se encuentra muy bien posicionado, ya que está respaldado por un consorcio de grandes empresas europeas, entre ellas Siemens. Esta posición ha sido recientemente reforzada con la creación de Konnex. Konnex es una iniciativa que establece criterios de convergencia entre tres de las redes de control más destacadas de Europa: EIB, EHS y Batibus. Esta iniciativa toma como piedra angular a EIB.

El protocolo EIB permite hasta 14 400 dispositivos por red, transmitiendo a una velocidad de 9600 [bps] en par trenzado y a 2400 [bps] en red eléctrica. Dentro del campo de la investigación se están realizando progresos en el desarrollo de pasarelas con TCP/P, integración con Jini y agentes inteligentes.

➤ LONWork

LONWork es un estándar propietario perteneciente a la empresa Echelon, de mayor difusión en Norteamérica. LONWork utiliza para el intercambio de información (ya sea de control o de estado) el protocolo LonTalk. Toda la información de este protocolo está disponible para cualquier fabricante, aunque Echelon exige una tasa por cada dispositivo fabricado. Las empresas Cypress, Toshiba y Motorola comercializan un circuito integrado denominado Neuron que implementa el protocolo. Cada circuito integrado 2Neuron tiene un identificador único de 48 bits, lo cual implica que el número de dispositivos no va a ser un problema. La velocidad de transmisión es de 4000 [bps] en línea de potencia y puede alcanzar hasta 1.25 [Mbps] en par trenzado, pero bajo condiciones muy restrictivas. LONWork presenta mayor difusión en Europa de la que tiene EIB en EE.UU.

7.2.1.1.2 Redes Orientadas a la Automatización de Viviendas

Este tipo de redes se utiliza fundamentalmente en entornos residenciales. Entre estas redes resaltan X10, CeBus y SCP.

➤ X10

X10 es un protocolo de comunicación que permite controlar aparatos eléctricos a través de la instalación de red eléctrica. El estándar surgió hace 20 años como parte de los experimentos realizados por la empresa Picosystem y lleva más de quince funcionando en el ámbito comercial. Las prestaciones del protocolo son bastante limitadas debido a su sencillez. Se definen únicamente 16 comandos, y la red sólo puede constar de hasta 256 dispositivos que se conectan utilizando la red eléctrica. Aun así, gracias a que los dispositivos son baratos y sencillos de instalar es un protocolo muy extendido en Estados Unidos sobre el cual se han realizado una enorme cantidad de desarrollos. La mayoría de las instalaciones de automatización residenciales en EE.UU. utilizan

este protocolo. En la actualidad se puede encontrar como bus de control en proyectos de investigación relacionados con entornos ubicuos.

➤ **CEBus**

CEBus presenta similitudes con X10 respecto a su filosofía de diseño, pero sus prestaciones son muy superiores. CEBus permite distintos tipos de medios físicos y una mayor cantidad de dispositivos. La aportación más significativa de CEBus es el lenguaje CAL. Este es un lenguaje orientado a comandos que permite controlar dispositivos conectados a CEBus y asignar recursos. El lenguaje define un conjunto de funciones para cada uno de los dispositivos. CAL utiliza el paradigma de programación orientada a objetos. Sin embargo, los objetos CAL no se organizan en jerarquías (no existe el concepto de herencia tal como se entiende en orientación a objetos), sino que el comportamiento depende del contexto en el que se encuentre. Por ejemplo, si tenemos un objeto de control analógico, éste se puede usar tanto para representar un control de volumen, un termostato o un regulador. CEBus soporta velocidades de hasta 8000 [bps].

➤ **SCP (Simple Control Protocol)**

SCP es un protocolo abierto desarrollado por Microsoft. Presenta características tanto de una red específica como de propósito general. Es un protocolo orientado a mensajes entre dispositivos. Cada dispositivo se modela como un conjunto de propiedades, que dan información sobre el estado, un conjunto de acciones, que aportan la funcionalidad del dispositivo, y una colección de servicios, donde cada servicio es un conjunto de propiedades y acciones. Además aporta mecanismos para poder establecer relaciones entre variables, de forma que cuando cambia una variable, el cambio se propaga automáticamente a las variables que estén relacionadas con ella. Otra característica novedosa es que cada dispositivo que se añade a la red ha de registrarse. Así resulta bastante sencillo consultar qué dispositivos están disponibles en cada momento. SCP es la última apuesta de Microsoft para entrar en el campo de la automatización de viviendas. De momento SCP está en fase de desarrollo y su único medio de transmisión posible es la línea de potencia.

7.2.1.2 Redes Multimedia

Un aspecto íntimamente relacionado con la computación ubicua es lo que se podría denominar presentación ubicua. Esta consiste en poder disponer de una información multimedia en cualquiera de los dispositivos audio-visuales del entorno. Para ello se precisa una difusión inteligente y centrada en el usuario del audio y del vídeo. Un ejemplo clásico es aquel en el que la música acompaña al usuario por todas las estancias de una vivienda. Para ello el sistema requiere poder representar y controlar todos los flujos de información continua que se generen. Con la digitalización del vídeo y del audio han surgido nuevos protocolos que pretenden solucionar la interconexión de los nuevos aparatos electrónicos, tanto entre sí como con las PCs. Este esfuerzo en transmitir todas las señales con formato digital permite reducir los costos de interconexión y homogeneizar los equipos. Entre las redes multimedia existentes se destacan IEEE 1394, USB y Ethernet.

➤ **IEEE 1394 vs USB**

IEEE 1394 y USB son dos soluciones que permiten interconectar dispositivos digitales audio-visuales. USB surgió dentro del mundo de las PCs como un bus serie de alta velocidad y pretende establecerse como el estándar de comunicación entre los periféricos y la PC. IEEE 1394 ofrece mejores prestaciones y plantea una visión más general. Ambas redes presentan mecanismos para garantizar la calidad de servicio, de tal forma que los dispositivos que quieran transmitir tienen que reservar previamente una parte del ancho de banda, siendo el protocolo el encargado de decidir si se concede o no. IEEE 1394 constituye la capa física sobre la que se implementa HAVi [HAVi 1998] y aporta mayor funcionalidad en la gestión de audio y vídeo. HAVi es una iniciativa propuesta por un consorcio formado por distintas empresas del sector audiovisual que trata de potenciar la transmisión de audio y vídeo digital.

	IEEE 1394	USB
Comunicación	Serie/Paralelo	Serie
Velocidad de Transmisión	400 [Mb/s]	1.5/12/240 [Mb/s]
Conexión a Cliente	Si	Si
Alimentación	Si	Si
Número de Dispositivos por Red	64449	127
Orientado a	Dispositivos Rápidos	Periféricos Lentos
Apoyo	Sony, Apple, Compaq	Microsoft, Intel

Tabla 7.1 Comparativa de las prestaciones de la IEEE 1394 y USB. IEEE 1394 contituye la capa física sobre la que se implementa HAVi (Home Audio Visual Interoperability).

➤ **Ethernet**

Es un protocolo de área local desarrollado por la empresa Xerox Corporation en cooperación con DEC e Intel en 1976. Al basarse en un protocolo de contienda no presenta mecanismos para garantizar el ancho de banda necesario durante toda la transmisión. Sin embargo el estándar parte con una experiencia de más de veinte años de desarrollo que le han consolidado como una tecnología de alta fiabilidad y elevado rendimiento. Además se pueden destacar dos importantes ventajas:

- Al estar ampliamente soportada la interoperabilidad de Ethernet con el protocolo IP queda fácilmente resuelta la pasarela entre la red interna de los dispositivos ubicuos y la conexión a Internet.

- Permite velocidades de transmisión desde 10 a 100 [Mb/s]. Aunque su enfoque primario era transmitir datos entre computadoras, tiene las prestaciones necesarias para poder transportar tráfico multimedia. Un ejemplo de aplicación ubicua de la red Ethernet es HomePNA. Consiste en un protocolo que emplea el cableado telefónico combinado con la tecnología Ethernet para distribuir información entre las distintas habitaciones de un hogar. HomePNA actualmente puede transmitir hasta 10 [Mb/s], y se estima que la red pueda soporta hasta 100 [Mb/s]. De momento en la red se pueden conectar hasta 25 dispositivos, por lo que se hace más adecuada como *backbone* de alta velocidad.

**TESIS CON
FALLA DE ORIGEN**

8. Estado de la Implementación de las Tecnologías

8.1 Comienzo de las Redes Inalámbricas en México

El de la movilidad, omnipresencia o comunicación permanente -como quiera llamársele- ha sido la tierra prometida por la industria de tecnologías de información y comunicaciones (TIC) desde hace tiempo. Han sido innumerables los debates sobre las posibilidades de que un individuo realmente esté conectado las 24 horas del día, desde cualquier lugar, dentro de un ambiente de trabajo virtual, pero finalmente el deseo de movilidad tiene qué ver -más que con comodidad- con un tema central en estos tiempos: la productividad.

Es por ello que de las promesas de movilidad, las de las redes inalámbricas son las que han adquirido más sentido tanto para usuarios como para proveedores.

Si bien es cierto que en el último año el tema de la movilidad ha sido uno de los temas más mencionados dentro de la industria TIC -sobre todo porque ofrece un espacio para explotar el negocio de los servicios-, es preciso aclarar que la tecnología no es nueva en lo absoluto.

Es difícil precisar cuándo nacieron las redes inalámbricas, pero la mayoría de los especialistas en México coinciden en que es una tecnología muy vieja; por ejemplo, Nilsa Islas, directora de Relaciones Públicas y Mercadotecnia de Enterasys Networks en México, se remontó a 12 años atrás, mientras que Hayeth Melayes, gerente de Comercialización de Proxim, comentó que su empresa empezó a vender soluciones inalámbricas desde 1979.

Aunque existieran desde hace ya muchos años, lo cierto es que la penetración en el país comenzó a adquirir cierta fuerza hasta hace aproximadamente siete años, complementó Islas.

Las versiones sobre su antigüedad y el tiempo que estas tecnologías llevan comercializándose en México son diversas, pero podríamos decir que hace de tres a seis años comenzaron a llamar la atención de manera poderosa entre los usuarios.

Un aspecto fundamental relacionado con esta evolución, al igual que con la de cualquier otra tecnología, fue el desarrollo tecnológico para garantizar una mayor seguridad y confianza al usuario sobre la estabilidad de estas redes y de sus sistemas.

Una vez que las tecnologías se hicieron más complejas y se crearon estándares para facilitar su empleo (por ejemplo, el 802.11b en WLANs), lo que implica la integración de diversos dispositivos y servicios para lograr una solución óptima, se abre una gran oportunidad de venta de consultoría.

El sueño de un mundo móvil inalámbrico en donde la comunicación pueda darse desde cualquier lugar tiene como principio la propagación de las redes inalámbricas.

8.2 Visión de Especialistas y Empresarios Mexicanos Acerca de las Redes Inalámbricas en el País.

Más que con un mercado específico, las redes inalámbricas se relacionan mayormente con necesidades específicas y se consideran una solución ideal para compañías que requieren movilidad constante al interior de sus instalaciones. No importa si la empresa es grande o pequeña sino que realmente se justifique tener una solución inalámbrica.

Especialistas mencionan que las soluciones inalámbricas son más aptas para los trabajadores a distancia y empleados que se llevan trabajo a casa, por lo cual las redes de este tipo están más dirigidas a los espacios públicos o zonas activas, instalaciones de empresas o en los hogares de los empleados que precisan conectividad constante con la empresa.

Según explicó a la revista especializada *infochannel* Gustavo Riverón, director de Canales de Avaya México, esto es una aplicación que se está haciendo más común dentro de edificios inteligentes de empresas medianas.

Con base en la experiencia de Avaya sobre estas soluciones, el directivo aclaró que en los corporativos no es muy frecuente encontrar redes *wireless*: "Sólo en los altos niveles y en donde se están remodelando o ampliando las instalaciones".

A decir de Riverón, el mayor crecimiento, que es como se esta dando, es en hospitales, hoteles y espacios abiertos para ofrecer el servicio a los visitantes, así como en instalaciones que exigen mucha movilidad, como son las universidades y las industrias, para facilitar -por ejemplo- la localización del personal y su conexión a la red.

En el caso de Cisco Systems, Ramón Vignal, ingeniero de Sistemas de Centros de Solución Tecnológica de la subsidiaria mexicana, señaló que las instalaciones son más solicitadas por pequeñas y medianas empresas (PyME).

Por su parte, Galib Karim, director de la División de Redes Empresariales de Nortel Networks en México, agregó que las compañías ubicadas en edificios difíciles de cablear, por el tipo del material con que están construidos o por ser históricos, son clientes atractivos.

De todas las aplicaciones posibles es preciso destacar que, por lo general, las redes inalámbricas se conciben para necesidades específicas, pues normalmente una compañía no instala esta infraestructura en todo su edificio, sólo en las áreas en donde verdaderamente es aprovechada, aclaró en su oportunidad Felipe González, analista de Estrategias de Mercado en México de The Yankee Group.

Si una empresa quiere expandir su infraestructura o necesita levantar una rápidamente, la opción inalámbrica es perfecta, ejemplificó Sergio Vega, gerente de Mercadotecnia de CA en México.

Entre las ventajas que ofrece una red inalámbrica destaca la de dotar de movilidad a los usuarios sin perder contacto con la conexión a Internet; es decir, la búsqueda de productividad es el principal incentivo para adquirir estas tecnologías.

Para Riverón el costo también es una ventaja relevante, pues en las redes cableadas el costo se relaciona con la cantidad de nodos requeridos, además de que en una red alámbrica el costo del cable puede representar hasta 40% o 50% de la inversión total en la infraestructura.

En ese sentido, Ramón Vignal reveló que instalar cableado en un lugar puede ser muy costoso, ya que debe ponerse un techo o un piso falso y romper paredes; además, complementó, el precio de los cables y los dispositivos es más caro que un *access point*.

Este tipo de redes también ahorran tiempo, por prescindir de la instalación de los cables; son sencillas de montar, configurar y mantener, aseveró Genaro Ramos, director general de SMC Networks.

8.2.1 Crecimiento y Penetración de las Redes Inalámbricas en el País

Gracias a que las soluciones sin cable cumplen con la demanda de aumentar la productividad, los fabricantes de equipo y aplicaciones las promueven como “el negocio del futuro” y prácticamente se ha convertido en la promesa más fuerte en el mercado, de acuerdo con Felipe González, de The Yankee Group.

En febrero del 2001 Gartner publicó un estudio en donde predecía que las tecnologías inalámbricas se extenderían a todos los niveles: “Para las comunicaciones de rango corto los dispositivos con Bluetooth alcanzarán el mercado masivo; para el rango medio la conectividad inalámbrica en oficinas con LANs inalámbricas basadas en estándares 802.11b continuarán siendo ampliamente instaladas, y para las aplicaciones de rango amplio los paquetes de datos y servicios en teléfonos móviles (2.5G) y 3G empezarán a emerger como es el caso de GPRS”.

Asimismo, afirmó en el documento que las redes LAN inalámbricas representaron una de las pocas áreas en que las empresas estaban deseosas de invertir “y la creciente popularidad de la tecnología puede ser atribuida a la ratificación de un estándar central y el deseo de los vendedores de conformarlas”.

Más tarde, en septiembre del 2001, Gartner anunció que los embarques mundiales de redes LAN inalámbricas estaban siguiendo un ritmo que los llevaría a un crecimiento de 73% en 2002.

En aquella ocasión previó que los ingresos llegarían a casi 2,800 millones de dólares en 2003, en comparación con los 2,100 millones de dólares esperados para 2002, y predijo que el mercado continuaría experimentando un crecimiento sano hasta el 2007.

También citó el porcentaje de penetración de las redes LAN inalámbricas en la base instalada de *notebooks*, que fue del 9% en el año 2000, mientras que para 2003 llegaría a 50% y hasta un 90% en 2007.

A esos números agregó que, si bien las redes LAN inalámbricas anteriormente se compraban como complementos de las computadoras personales, ya que a finales del 2001 10% de todas las *laptops* se entregado con una red LAN incluida y aumentará a 31% en 2004, mientras que para 2007 la proporción llegará a 68%.

Los analistas de Gartner afirman que los negocios deberán utilizar redes de 802.11b en adelante. En la mayoría de los casos, los negocios estarán satisfechos con su desempeño a largo plazo y la 802.11b será la tecnología preferida para los que frecuenten puntos *hot spot*. Sin embargo las redes 802.11a, en combinación con la 802.11g, comenzarán a reemplazar las compras de las 802.11b a principios del 2004. El ancho de banda adicional será utilizado para nuevas aplicaciones como voz sobre IP y *streaming video*.

“Cuando maduren en el 2004, las redes WLAN 802.11a ofrecerán ventajas tecnológicas significativas sobre las redes 802.11b”, “Algunas de las ventajas incluyen rangos de enlace de hasta 54 [Mb/s], escasa interferencia de aparatos Bluetooth y de consumo que operan en la saturada banda de 2.4 [GHz], además de disponibilidad de hasta 13 canales en América del Norte y más en otros mercados europeos”.

De acuerdo a Gartner, más del 50% de todas las implementaciones WLAN tendrán lugar dentro de mercados verticales durante el 2004.

Al respecto, la consultora recordó que los fabricantes de computadoras personales de alto nivel ya ofrecen computadoras portátiles con adaptadores inalámbricos en conjunto y refirió que Intel acababa de anunciar su intención de incorporar capacidades de LAN inalámbrica a la próxima plataforma móvil Banias, “lo cual impulsará la integración de la red LAN inalámbrica en las nuevas computadoras portátiles”.

8.2.2 La Barrera de la Velocidad

Los beneficios suenan bien y, por ello, las promesas se han extendido, pero antes de crear demasiadas expectativas es preciso tomar en cuenta las desventajas y los retos que las redes sin cables aún deben enfrentar.

En general, los ejecutivos mexicanos advirtieron que si una compañía necesita manejar un amplio ancho de banda es más conveniente instalar una red alámbrica.

La velocidad se percibe como una limitante considerable todavía, pues la red cableada puede llegar hasta 1,000 [Mb/s] y una red inalámbrica sólo alcanza 11 [Mb/s]; por tanto, en una red inalámbrica debe tomarse en cuenta la cantidad de *access points* necesarios para dar un buen acceso (algunos fabricantes, como es el caso de Avaya, lanzarán próximamente tarjetas de 54Mbps).

No obstante esta desventaja vista por algunos especialistas, para otros -como Ramón Vignal, de Cisco- "los 11Mbps disponibles hoy en día son más que suficientes, pues muchas compañías ni siquiera los aprovechan". La cuestión es identificar las necesidades de las empresas para determinar si es necesario instalar una red inalámbrica.

Al respecto, Galib Karim, de Nortel, apuntó que para mejorar la velocidad ofrecida por las redes inalámbricas es preciso adquirir equipos más grandes, pero como éstos son más caros, resultan menos atractivos.

8.2.3 Preocupación por la Seguridad

Para Bernardo Zamora (Comactive) el principal reto a vencer es el de la seguridad, pues muchas empresas no están adoptando soluciones Wi-Fi porque el estándar actual proporciona una seguridad muy baja.

El directivo explicó que actualmente se emplea el estándar Wired Equivalent Privacy (WEP) basado en *passwords*, e informó que probablemente para el próximo año esté listo el siguiente estándar: Wi-Fi Protected Access (WPA), que es más robusto y es óptimo para las grandes empresas.

El nuevo estándar implica más esperanzas de crecimiento, para vencer el temor a la inseguridad que ha velado un tanto el desarrollo de las redes sin cables, pues a pesar del estándar WEP no hay mucha confianza, como lo demuestra el hecho de que menos de 10% de las redes inalámbricas tiene esta protección, citó Zamora.

A lo anterior el ejecutivo agregó: "En Latinoamérica el problema del sistema operativo es un reto importante, pues sólo Windows XP trae soporte nativo para Wi-Fi; las computadoras con Windows 95 no lo pueden utilizar, y Windows 98 y 2000 requieren *drivers* especiales".

En el mismo tenor, Sergio Vega (CA) alertó: "Un punto importante a considerar antes de pensar en implantar esta tecnología es la seguridad, puesto que el medio de transmisión es el aire y, por tanto, no sólo se corre una gran cantidad de riesgos sino que muchas fuentes de información de la empresa se ven expuestas a otras personas".

También Nilsa Islas (Enterasys) nombró a la seguridad como la principal preocupación: "Por eso estamos trabajando en la difusión de *firewalls*, controles de acceso y autenticación, así como en la promoción de programas integrales de seguridad en las empresas, para que su personal colabore de manera directa".

Aunque la desventaja más fuerte, desde la perspectiva de Vega, está en la facilidad de acceder a la red sin autorización, también destacó la importancia de monitorear la disponibilidad de las comunicaciones ante las posibles fallas causadas por la interferencia que hay en algunos edificios.

De acuerdo con Hayeth Melayes (Proxim), los problemas de interferencia son causados por la falta de algunos estándares pendientes en la tecnología.

8.2.4 Cultura de Uso

A pesar de las desventajas prevalecientes, las mejoras en la tecnología inalámbrica le han hecho ganar más confianza por parte de los usuarios: de acuerdo con un estudio de The Yankee Group, a finales de los 90, en una escala del uno al cinco, la seguridad tenía un valor de 4.1 en la preocupación de las empresas, mientras que el año pasado este porcentaje se redujo a 3.8.

Pero de los obstáculos presentes no sólo hay cuestiones técnicas; también está la cuestión cultural, como en toda promoción de tecnología. Quien más aludió a este punto fue Felipe González, de la misma consultora, recordando que "el mercado mexicano no es muy consumidor de estos servicios. La cafetería norteamericana Starbucks ha tenido mucho éxito con su solución inalámbrica como un servicio adicional para los clientes, aunque probablemente el resultado no sea el mismo si se implanta una solución similar en una cafetería mexicana".

Cada uno de los ejecutivos se mostró optimista -pero con mesura- y todos dijeron estar conscientes de que el camino apenas comienza a andarse, y aunque reconocen el potencial de negocio que se avecina, admiten que "el negocio inalámbrico no es el Mesías de la industria informática".

Todos aceptaron las desventajas y los retos a vencer, pero al mismo tiempo voces como la de Genaro Ramos (SMC) aclaran que las desventajas parecen más grandes cuando se comparan con las soluciones cableadas.

En respuesta a la inquietud sobre si las redes inalámbricas sustituirán en el futuro a las cableadas, la respuesta fue una sola: "Más que sustituto, son un complemento".

Gustavo Riverón (Avaya) reconoció que la red inalámbrica es un elemento que tomará más participación en el mercado, pero al mismo tiempo seguirán evolucionando las redes cableadas. Las aplicaciones inalámbricas seguirán siendo de nicho.

La opinión de Felipe González aludió a una comparación con los teléfonos inalámbricos: "No creo que haya un reemplazo de las redes cableadas; dependerá del precio y la funcionalidad, pero no es práctico y eso lo demuestra el caso de los teléfonos convencionales, los cuales conviven con los inalámbricos tanto en el hogar como en las empresas".

En Nortel Networks la venta de soluciones relacionadas con tecnología inalámbrica en el 2001 equivalían a 3% de los ingresos totales de la compañía y en este año equivalen 6%, el mercado se considerará como maduro, según sus expectativas.

Estadísticas de las Redes Inalámbricas

- Ingresos esperados por redes WLAN en 2002 a nivel mundial: 2,100 millones de dólares.
- Ingresos esperados para 2003: 2,800 millones de dólares.
- Crecimiento de los embarques mundiales de redes WLAN en 2002: 73%.
- Penetración de las redes WLAN en la base instalada de PCs en 2000: 9%
 - En 2003: 50%.
 - En 2007: 90%.
- *Laptops* que serán entregadas con una red LAN incluida en 2002: 10%.
 - En 2004: 31%.
 - En 2007: 68%.

8.3 Implementación de una Red Inalámbrica

Los parámetros básicos para el diseño de la red inalámbrica son:

- Características del recinto.
- Número de usuarios con acceso inalámbrico.
- Prestaciones necesarias de la red.
- Integración e interoperabilidad con otras redes.

Para hacer la implementación de la red además de los cuatro puntos principales anteriormente mencionados, debemos hacer un revisar tópicos adicionales como son: tecnologías que se aplicaran la cual depende directamente de las características del recinto, número de usuarios, prestaciones de la red y como se van a integrar todos los servicios.

El análisis de los diferentes tipos de redes inalámbricas se hicieron en los capítulos anteriores, es por eso que a continuación mencionaremos los fabricantes y características que algunos productos y empresas manejan en este rubro, para finalizar con algunos ejemplos de redes ya establecidas en el país o servicios que se están prestando utilizando redes inalámbricas.

8.3.2 Elección de productos

8.3.2.1 Productos WLAN 802.11

Es importante mencionar que debido a las aplicaciones que se le dan a las redes inalámbricas en México, la mayoría de los usuarios manejan redes inalámbricas de área local WLAN, específicamente 802.11b ya que esta tecnología cumple con las necesidades que actualmente las empresas en el país requieren, sobretodo de movilidad y de velocidades de transmisión razonables para aplicaciones empresariales. La tabla siguiente muestra algunas características de los equipos que manejan 802.11b. Los productos analizados fueron: Airconnect de 3COM, WL de Compaq, 2011 de Intel y Aeronet de CISCO.

Capítulo 8. Estado de la Implementación de las Tecnologías.

	3COM AirConnect	Compaq Wireless	Intel Wireless 2011	CISCO Aeronet
Distribuidor	3COM	Compaq	Intel	CISCO
Especificación	IEEE 802.11b	IEEE 802.11b	IEEE 802.11b	IEEE 802.11b
Certificación Wi-Fi	Si	Si	Si	Si
Soluciones disponibles				
Punto de Acceso	3CRWE74796B	WL410	WEAP2011EU	AIR-AP352E2C
Adaptador PC Card	3CRWE73796B	WL110	WPC2011EU	AIR-PCM352
Adaptador PCI	3CRWE777A	WL210	N.D.	AIR-PCI352
Características de Radio				
Banda de	ICM	ICM	ICM	ICM
Frecuencias				
Tipo de Señal	DSSS	DSSS	DSSS	DSSS
Tasa de transferencia				
Ajuste dinámico	Si	Si	Si	Si
11 Mbps	Si	Si	Si	Si
5.5 Mbps	Si	Si	Si	Si
2 Mbps	Si	Si	Si	Si
1 Mbps	Si	Si	Si	Si
Modo de transmisión	Half duplex	Half duplex	Half duplex	Half duplex
Acceso al medio.	CSMA/CA	CSMA/CA	CSMA/CA	CSMA/CA
Modulación				
CCK a 5.5 y 11 Mbps	Si	Si	Si	Si
DQPSK a 2 Mbps	Si	Si	Si	Si
DBPSK a 1 Mbps	Si	Si	Si	Si
Topologías				
Punto a punto	Si	Si	Si	Si
Punto de acceso	Si	Si	Si	Si
Encriptación				
WEP (40 bits)	Si	Si	Si	No
WEP (128 bits)	Si	Si	Si	Si
RC4	Si	Si	N.D.	N.D.
Software				
Punto de acceso	Site Survey Dynamic Access	Site Survey APManager	Site Survey	Site Survey
Cliente	Si	Si	Si	Si
Reglamentaciones				
Certif. FCC Clase B	Si	Si	Si	Si
CSA	Si	Si	Si	Si
Marca CE	Si	Si	Si	Si
Garantía	3 años	1 año (AP) y 3 años (PC Card y PCI)	3 años (AP) e ilimitada (PC Card)	1 año (AP) y 3 años (PC Card y PCI).
Sistemas Operativos				
Windows 9x	Si	Si	Si	Si
Windows NT 4.0	Si	Si	Si	Si
Windows 2000	Si	Si	Si	Si
Características del punto de acceso				
Interfaz de red	10BASE-T(RJ45)	10BASE-T(RJ45)	10BASE-T(RJ45)	10/100BASE-T(RJ45)
Puerto serie RS-232	Si	No	Si	Si
Nº máx. de clientes	64	N.D.	127	N.D.
Diversidad de antena	Si	Si	Si	Si
Transformador	Externo	Externo	Externo	No
Alimentación a través de línea Ethernet	Si	Si	Opcional	Si
Precios aproximado por unidad (pesos)				
Punto de acceso	12 000	10 200	12 400	11 500
Adaptador PC Card	2 500	2 300	2 600	3 800
Adaptador PCI	3 000	2 900	N.D.	4 000

8.3.2.2 Productos Bluetooth

La Tecnología Bluetake proporciona una solución basada en tecnología Bluetooth que permite integrar rápidamente soluciones innovadoras para transferencia inalámbrica de datos, reduciendo los tiempos de instalación y creando una ventaja competitiva para el usuario.

- **Adaptador para impresora Bluetooth BT200** con software de impresión incluido: FieldSoftware PrintPocketCE (para PocketPC 2002/2000 OS), dispositivo Bluetooth v1.1 , 2.4 [GHz]~2.480 [GHz] FHSS Radio de cobertura de 10 metros (en espacio abierto), Soporta sistemas operativos Windows XP/2000/ME/98SE, PocketPC 2002/2000, Palm 5.0/4.0(Software extra de impresión para las PDAs Bluetooth, la versión específica varía según el sistema operativo empleado por la PDA), velocidad de impresión de hasta 115,2[Mb/s], conector de Puerto Paralelo de 36 pines.
- **Terminal Punto de Acceso BT300** Dispositivo Bluetooth v1.1 ,2.4 [GHz]~2.483 [GHz] FHSS, 100 metros de área de cobertura (área abierta) , soporta sistemas operativos Windows XP/2000/ME/98SE , soporta el Perfil de Acceso a LAN Bluetooth , velocidad de transmisión de hasta 1[Mb/s], la interfase integra puertos RS232 y 10/100 Base-T Ethernet Port, sensibilidad: -70dBm a 0.1BER .
- **Manos libres Bluetooth BT400** 2.4 [GHz] ~ 2.480 [GHz] FHSS, dispositivo Bluetooth v1.1, 10 metros de área de cobertura (en espacio abierto), soporta el Perfil de Audifono Bluetooth, sensibilidad < -84 dBm.
- **Adaptador Bluetooth USB BT009V** Bluetooth versión 1.1, rango de 2.4 [GHz] ~ 2.483 [GHz] FHSS, acceso de datos a través del puerto USB 10 metros de alcance (área abierta), sistemas Operativos WIN98SE/ME/2000/XP, servicio de transferencia de datos, dial-up y LAN , sensibilidad < -85 dBm, velocidad de transmisión de datos 1[Mb/s].
- **Tarjeta CompactFlash BT100** Dispositivo Bluetooth v1.1, 2.4 [GHz] ~ 2.480 [GHz] FHSS , 10 metros de área de cobertura (en espacio libre), solución óptima para cualquier PDA basada en Windows CE, incluye los perfiles de Transferencia de Archivos, Conexión Telefónica a Redes y Acceso a LAN, Sensibilidad< -85 dBm , transferencia de datos de hasta 1[Mb/s].
- **Adaptador Bluetooth USB BT009S** Bluetooth versión 1.1,2.4 [GHz] ~ 2.483 [GHz] FHSS, acceso de datos a través del puerto USB , 10 metros de alcance (área abierta) , servicio de trasferencia de datos, dial-up y LAN, sistemas Operativos WIN98SE/ME/2000/XP ,sensibilidad < -85 [dBm], velocidad de transferencia de datos 1[Mb/s].
- **Dongle Bluetooth USB BT007** Con las mismas funciones que el Poke2 y el Crystal, la señal de este adaptador alcanza los 100 metros permitiendo conexiones a mayor distancia. Bluetooth versión 1.1, 2.4 [GHz]~2.483 [GHz] FHSS, acceso de datos a través del puerto USB, sistemas Operativos WIN98SE/ME/2000/XP, servicio de transferencia de datos, dial-up y LAN, sensibilidad < -85 [dBm], velocidad de transferencia de datos 1[Mb/s].

Existe una serie de controladores, para los dispositivos Bluetooth, a continuación mencionaremos sus aplicaciones, nótese que la mayoría de estos controladores son de licencia libre y todos fueron puestos a disposición en este año 2003.

- **Controladores para BLUETAKE USB (Versión: 1.3.2.7)**
 - Disponible para las series BT007, BT009S, BT009V
 - OS: Windows XP/2000/ME/98SE
 - Fecha de lanzamiento: 2003.02.18

Nota: Es necesario instalar el WinRoute Lite software para Windows 98SE/ME. Puedes bajar una versión de prueba del WinRoute Lite ó comprar la versión formal de <http://www.kerio.com/>

- **Controladores para BLUETAKE CF (Versión:1.2.2)**
 - Disponible para el BT100 (Compact Flash para PDA)
 - OS: Window CE .NET, Pocket PC 2002, Pocket PC 2003
 - Fecha de Lanzamiento: 2003.08.05

Nota: El software es libre de licencia, y puede instalarse sin ninguna restricción adicional además de las mencionadas en la página de su desarrollador. www.christersson.org.

- **PC Control - Control remoto con Bluetooth**
 - Controle la PC por medio de ondas Bluetooth desde su teléfono celular.
 - OS: Window XP/2000/98SE
 - Fecha de Lanzamiento: 2003.08.05

Nota: El software es libre de licencia, y puede instalarse sin ninguna restricción adicional además de las mencionadas en la página de su desarrollador. www.christersson.org.

- **FloAT - Sincroniza con Bluetooth**
 - Sincronize contactos e información entre su teléfono celular y su PC
 - OS: Window XP/2000/98SE
 - Fecha de Lanzamiento: 2003.08.05

Nota: El software necesita de ciertos componentes previamente instalados, los cuales puedes encontrar de forma detallada en su sitio web: www.eflame.com/fma/

- **Servidores de impresión**

Los servidores de impresión permiten a los usuarios con redes heterogéneas compartir sus impresoras desde la PC o entornos de red sin complicaciones. Se instalan rápidamente, permiten impresión simultánea en todas las redes, incluso aquellas conectadas a sistemas IBM Mainframe y AS/400.

ORIGINAL
 DE ORIGEN

Modelo	Descripción Corta	Precio de lista
AXIS 5800+ Bluetooth Print Server	Axis 5800+ PrintServer Bluetooth y Ethernet 10/100. 2 paralelos. Windows/Novell/UNIX/OS2/Mac/Web.	\$480
AXIS 5810 Bluetooth Print Server	Axis 5810 PrintServer Wireless Bluetooth y Ethernet 10/100. 1 paralelo. Windows/Novell/UNIX/OS2/Mac/Web.	\$174
AXIS 5900 802.11b Print Server	Axis 5900 PrintServer Wireless 802.11b y Ethernet 10/100. 2 paralelos. Windows/Novell/UNIX/OS2/Mac/Web.	\$373
AXIS 9010 Bluetooth AccesPoint	Axis 9010 Permite conectarse a red Ethernet / FastEthernet, Internet y sistemas con TCP/IP a usuarios móviles equipados con PDA's, teléfonos o notebooks que soporten Bluetooth.	\$426

8.4 Redes Inalámbricas en México

El mundo de la tecnología está lleno de promesas; algunas no cumplidas, otras cumplidas a medias y varias más que ya son una realidad. Seguramente entre esas promesas que se ven cada vez más cercanas y de las que se escucha hablar está el acceso a internet y las aplicaciones en cualquier lugar y a cualquier hora –el famoso anywhere, anytime– mediante la tecnología inalámbrica.

Si bien el avance se está dando en varios países, en México se concentran en casos aislados como campus universitarios, industria hotelera, y gran parte en oficinas corporativas. El sector de servicios sigue a la zaga; aún no es posible conectarse de manera inalámbrica a una red pública en muchos lugares públicos, por ejemplo, para acceder al correo electrónico o a los sistemas de una empresa. Hoy uno se tiene que conformar con los kioscos de Telmex o con alguna otra

Capítulo 8. Estado de la Implementación de las Tecnologías.

empresa con la que se contrate el servicio, cibercafés o salas ejecutivas. Es por eso que a continuación mencionaremos algunos de estos servicios y algunos de los proyectos en los que ya se está trabajando en el país.

8.4.1 Internet Inalámbrico con Prodigy Móvil

Prodigy Móvil es un servicio que provee acceso de alta velocidad inalámbrico (WiFi) a Internet en sitios públicos tales como Aeropuertos, Restaurantes, Universidades, Hoteles, Centros Comerciales, Centros de Convenciones, Hospitales, entre otros que se están sumando a la red día a día. Los sitios están diseñados con velocidad de acceso para navegar a alta velocidad. No importa si usas una computadora portátil o PDA; si es 802.11b (WiFi) se pueden bajar archivos, correo electrónico, ver un video o escuchar alguna canción.

Antenas (Access Points), instalados en el sitio público con tecnología 802.11b (WiFi), transmiten señales de radio frecuencia, a dispositivos compatibles con esta tecnología (WiFi) que se encuentren en la zona de cobertura.

La velocidad de transmisión es gobernada por la velocidad del acceso de cada sitio público.

Los sitios públicos con cobertura de Prodigy Móvil están equipados con accesos de banda ancha (Prodigy Infinitum) para satisfacer las necesidades del usuario.

La renta mensual de Prodigy Móvil incluye acceso ilimitado en los sitios públicos con cobertura. Existen tarifas preferentes para clientes que tienen algún servicio de la familia Prodigy, consulta las definiciones.

SERVICIO PRODIGY MÓVIL	RENTA MENSUAL PRODIGY MÓVIL Pesos M.N. + I.V.A
Si cuentas ya con Prodigy Infinitum	\$0 por promoción
Si cuentas ya con Prodigy DialUp: Paquete Móvil Internet	\$ 99.99
Si cuentas ya con Prodigy Turbo: Paquete Móvil Turbo	\$ 99.99
Prodigy Móvil	\$ 199.99

El servicio Prodigy Móvil incluye:

- 1 cuenta de acceso.
- 1 cuenta de correo electrónico de 25 MB.
- Espacio gratuito para página web de 10MB.

Para utilizar el servicio de Prodigy Móvil se requiere tener una PC portátil (LapTop) o un dispositivo PDA (PocketPC o equipo Palm) que tengan integrado o soporten la instalación de una tarjeta de acceso inalámbrico 802.11b (WiFi).

Para el caso de una PC portátil, la tarjeta de acceso inalámbrico se conecta a través de un puerto PCMCIA y se instala su controlador correspondiente. Para el caso de una PDA es importante tener cuidado, ya que no todos los equipos permiten la instalación de un dispositivo de acceso inalámbrico; se deberá consultar con el fabricante o distribuidor para confirmar si es posible la conexión a través de su equipo.

Los requisitos mínimos para la PC portátil son:

- Procesador: Pentium a 166 MHZ ó mayor (ó compatible)
- Espacio disponible en Disco Duro: 40 MB
- CD ROM: Drive CD-ROM 4x o mayor
- Memoria RAM: 32 MB ó mayor
- Interfase de Conexión (Hardware): Puerto PCMCIA disponible para tarjeta de red inalámbrica. Compatible con la especificación IEEE-802.11b también conocida como WiFi (Wireless Fidelity)
- Dispositivos: Adicionales: No
- Software: Navegador WEB (Internet Explorer 5 ó Netscape 4 ó superior)
- SO: Windows 98 / 98 SE / ME / 2000 .
- SO Windows Network: *Win NT 4.0
- Sistemas Operativos Macintosh: MAC 8.5, 8.6, 9.0, 9.1, 9.2 y 10

En una primera etapa, el Servicio Prodigy Móvil se proporciona en sitios públicos fijos predefinidos, como pueden ser restaurantes, hoteles, centros de convenciones, plazas comerciales, etc., de las ciudades de México, Guadalajara, Monterrey y Cancún, la lista completa se puede consultar en la página de Prodigy Móvil: www.prodigymovil.com. También se proporciona el servicio en los aeropuertos de las ciudades de México, Guadalajara, Monterrey, Los Cabos, Tijuana, Puerto Vallarta y Acapulco.

En esta primera etapa, es requisito tener una línea telefónica Telmex, sin embargo se está trabajando para proporcionar el Servicio Prodigy Móvil a través de tarjetas prepagadas similares a las tarjetas de telefonía celular o bien con cargo a tarjeta de crédito. Muy pronto se podrá disfrutar de este servicio pagándolo por estos medio.

En una segunda etapa, el Servicio Prodigy Móvil se ampliará a otras ciudades de la República Mexicana.

Prodigy Móvil de Telmex eligió a Cisco Systems como proveedor de equipos de tecnología de redes inalámbricas de área local (WLAN), así como de switcheo e infraestructura de red de servicios IP (UNINET).

Cabe señalar que diariamente se suman nuevos puntos de enlace con la intención de terminar el año con más de 300 hotspots.

Adicionalmente, el servicio de Prodigy Móvil permite la generación de Redes Privadas Virtuales (VPN) con lo que los usuarios corporativos no tendrán ningún problema para acceder de manera segura a sus redes empresariales y a aplicaciones como Intranet, correo electrónico corporativo, etc., logrando así una mayor eficiencia en el aprovechamiento de su tiempo.

Además, con Prodigy Infitum se puede adquirir el Módem Ruteador Inalámbrico, es un nuevo equipo que consiste en un módem/ruteador con capacidad para conectarse a Prodigy Infitum (ADSL) en cualquiera de las versiones actualmente comercializadas 256, 512 y 2000.

Capítulo 8. Estado de la Implementación de las Tecnologías.

La promoción de cero gastos de Instalación de Prodigy Infinitum con Módem Ruteador Inalámbrico Incluye:

IP Dinámica	Prodigy Infinitum 256	Prodigy Infinitum 512	Prodigy Infinitum 2000
Cuenta de acceso a Prodigy Infinitum, que permite acceder a través de Prodigy-Móvil de manera simultánea con Prodigy Infinitum y acceder a través de Prodigy Internet para Roaming en más de 3,500 poblaciones de México y 750 de Estados Unidos.	1 Cuenta	1 Cuenta	1 Cuenta
Cuentas de correo electrónico con capacidad de 25 Mb (con dominio prodigy.net.mx)	25	25	25
Espacio para publicación de página personal del tipo www.prodigy.net.mx/minombre .	10 MB	10 MB	10 MB
Computadoras sugeridas en Red	16	32	64
Renta Mensual	\$599	\$999	\$4599

8.4.2 Red GSM GPRS de Telcel

TELCEL, empresa líder en México introduce la tecnología GSM para sistemas de comunicación móvil, la tecnología GSM es el estándar de comunicación móvil de mayor crecimiento y el más utilizado en el mundo, el cual abarca más de 180 países y más de 780 millones de usuarios. A través de GSM se tienen los servicios más avanzados e innovadores del mundo como son tomar y enviar fotografías con tu celular, consultar tus e-mails, archivos, presentaciones, chats, juegos en línea, navegar en Internet, mira quien te habla (identificador de llamadas con foto). La conexión móvil que Telcel maneja, da opción de no solo comunicar un teléfono portátil con otro, sino utilizar dicho teléfono como modem de laptops y PDA para que los dispositivos puedan acceder a la red GSM.

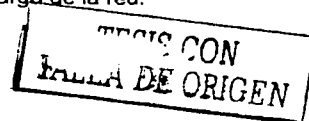
Telcel actualmente cuenta con una red GSM de generación 2.5 (La antesala de la 3ra. Generación) y es importante señalar que una de las tecnologías que utiliza para la transmisión de datos es GPRS, a través de un convenio firmado con la empresa Ericsson en el año 2000. A continuación mencionaremos algunas características que dicha aplicación esta llevando ya a la práctica, con el fin de mencionar el uso que tiene un sistema GPRS con el usuario final.

Telcel maneja diferentes tecnologías de transmisión de datos, dependiendo de las necesidades de los usuarios, como son:

CSD (Circuit Switched Data). Esta tecnología permite la transmisión de datos a velocidades de hasta 9.6 [kb/s]. Se basa en el uso de canales dedicados, por lo que la velocidad es constante durante todo el tiempo que dura una conexión. Se factura de acuerdo al tiempo de conexión y está disponible para usuarios de Amigo GSM (prepago).

HSCSD (High Speed Circuit Switched Data). Esta tecnología hace posible alcanzar velocidades de hasta 57.6 [kb/s] en la red GSM de Telcel. Funciona de forma similar a CSD sólo que la velocidad se obtiene combinando varios canales de 14.4[kb/s]. Esto hace posible recibir grandes cantidades de información, por ejemplo, imágenes y archivos de datos muy rápido. Por el momento está disponible únicamente para usuarios GSM de planes tarifarios.

GPRS (General Packet Radio Service) .Esta tecnología de transmisión de datos es característica de la red GSM y Telcel es el primer operador en México que ofrece este servicio. La tecnología GPRS transfiere datos en paquetes a alta velocidad, utilizando uno o varios canales de la red GSM. Los usuarios comparten estos canales por lo que las velocidades de transmisión varían dependiendo del número de usuarios simultáneos conectados y de la carga de la red.



Las principales ventajas de GPRS son:

- Y Siempre estás conectado (always on)
- Y Puedes recibir llamadas de voz mientras estás conectado
- Y El cobro se realiza con base en la cantidad de información enviada/recibida

A continuación presentamos algunas equivalencias para que tener una idea de cuánto cuesta el servicio.

NAVEGANDO EN WAP (CONEXIÓN MÓVIL DESDE TU TELCEL GSM)		NAVEGANDO CON UNA PDA (CONEXIÓN MÓVIL DESDE TU PDA)	
Concepto	Kb Aproximados	Concepto	Kb Aproximados
Consulta de Cartelera	10	Consulta de Saldo Bancario	21
Consulta de Restaurante	8	Consulta de Restaurante	16
Consulta de Horóscopo	7	Búsqueda en Sección amarilla	36
Búsqueda en Sección Amarilla	13	Envío de e-mail sin Archivo Adjunto	3
Envío de una e-card	14	Reenviar un e-mail	6
Leer una Noticia	10	Envío de una e-card	

Tabla 8.1 Equivalencia GPRS

*Las equivalencias son aproximadas, están basadas en consultas estándar por lo que pueden variar.

El servicio GPRS disponible únicamente para planes tarifarios Telcel GSMGPRS ya está activado en tu Telcel GSM, por lo que no necesita contratación. La tarifa es de \$0.12 +IVA por Kb o fracción.

Sin embargo, para obtener un mejor aprovechamiento y mejores precios, te recomendamos activar uno de nuestros planes GPRS.

FALTA DE ORIGEN

PAQUETE	KB INCLUIDOS	TARIFA	PRECIO POR KB ADICIONAL
Básico	1,000	\$100.00 + IVA	\$0.10 + IVA
Paquete 50	5,000	\$200.00 + IVA	\$0.05 + IVA
Paquete 100	10,000	\$300.00 + IVA	\$0.04 + IVA
Paquete 500	50,000	\$500.00 + IVA	\$0.02 + IVA

*El servicio esta disponible al momento de la contratación, pero requiere de que el equipo cuente con la capacidad GPRS o CSD

8.4.3 Internet Móvil desarrollado por Wireless Net Online

Internet Móvil es una solución desarrollada por Wireless Net Online S.A. de C.V. para proporcionar un servicio de Internet inalámbrico de alta calidad basado en la infraestructura de las compañías celulares, actualmente trabajan con la red GSM de Telcel. Online agrega optimización, contenido, e-mail, variedad de equipo y soporte técnico al sistema nativo, proporcionando a sus clientes una mejor experiencia al navegar por la red.

El servicio de Internet Móvil está basado en la infraestructura de las compañías celulares de voz, sin embargo, en su manera nativa el servicio móvil es lento y presenta problemas de conexión frecuentemente.

La tecnología GPRS permite en su forma original, una conexión a Internet desde su laptop con un throughput de entre 30 y 40 [k/s]. Mediante el Internet Móvil GPRS de Online se puede llegar hasta 160 [k/s] de throughput lo que permite correr la mayoría de las aplicaciones multimedia. El aumento de velocidad mediante la optimización de Online es de 2 a 5 veces en la mayoría de las aplicaciones. Además el Internet Móvil GPRS de Online presenta menos del 1% de falla al conectarse a una página web en comparación del entre 5 y 30 por ciento de falla en el GPRS nativo.

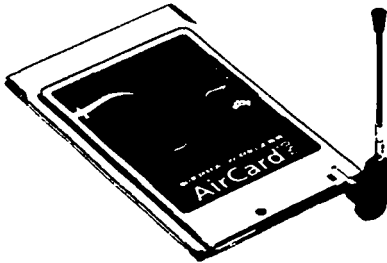
Internet Móvil de Online ofrece un buzón de email que permite hacer transferencias de archivos adjuntos a la máxima velocidad, además se permite seleccionar o eliminar los correos que quiere antes de bajarlos a su laptop o PDA.

Actualmente existe cobertura en prácticamente todo el país, incluyendo cerca de 200 poblaciones y 50 carreteras y autopistas.

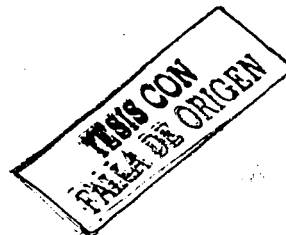
Dado que el servicio GPRS se cobra en base al tráfico de datos, mediante la tecnología de optimización de Online usted se puede ahorrar de 50 hasta un 90% de kilobytes transmitidos, además de una carga de 2 a 5 veces más rápida en las aplicaciones de Internet, esto se consigue mediante las mejoras en el protocolo de transmisión y técnicas de compresión que aplica Online. En algunos casos, el ahorro en bits transmitidos mediante esta optimización es aun más dramática. Con Esto se ve reflejado en una facturación mucho menor así como en una transmisión de aplicaciones de Internet mucho más eficiente y rápida, como se muestra en la siguiente figura.

Productos y Planes.

Aircard 750

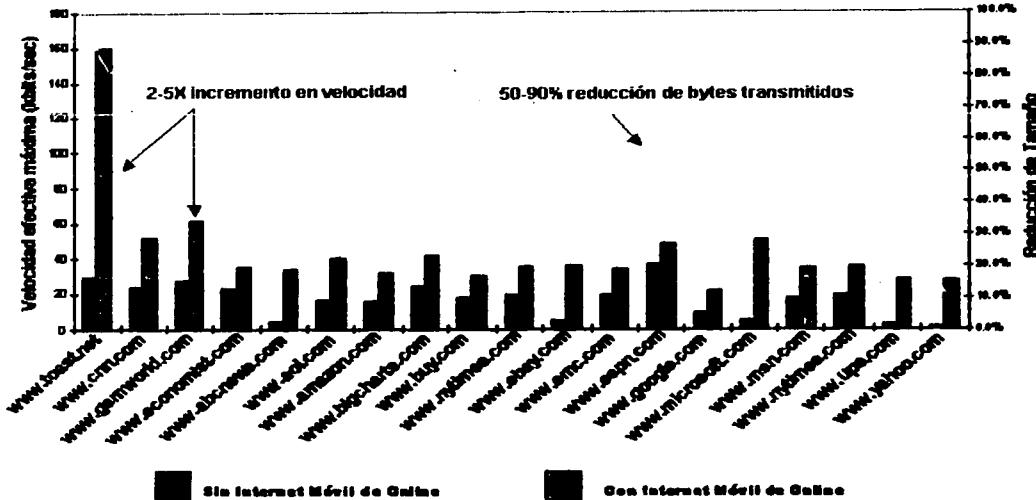


Precio: US \$ 425.00 + I.V.A.* No incluye embarque



Comparativo de Internet Móvil GPRS Nativo VS Online

FAJLA DE ORIGEN



* Tests con optimización media y hora no pico

Los planes tarifarios de Internet Móvil de Online están basados en el volumen de tráfico transmitido (entrada y salida) por el dispositivo móvil, teniendo cada uno de ellos las siguientes características:

- Tarifa fija por un máximo de kilobytes transmitidos.
- Costo por kilobyte adicional transmitido por arriba del volumen fijo contratado.
- No dependen de ningún plan de voz, por lo que los planes de Internet Móvil son independientes.
- Los planes incluyen aceleración y optimización.

Además, con Internet Móvil de Online la transmisión de paquetes de datos puede reducirse hasta 10 veces o mas en comparación con los accesos a Internet tradicionales, debido a la avanzada tecnología de optimización implementada, permitiendo adicionalmente alcanzar velocidades de navegación de más de 100[k/s].

PLAN	INCLUYE[MB]	EQUIVALENTE CON OPTIMIZACIÓN [MB]	COSTO AL MES [PESOS]	COSTO DE KBYTE EXCEDENTE [PESOS]
Lite	15	70	399	0.05
Corporativo	40	210	699	0.04
Multimedia	100	528	1199	0.04

8.4.4 Internet Inalámbrico en el Área Hotelera

El Hotel Sheraton Suites Santa Fe puede considerarse pionero y visionario en varios aspectos con respecto a las tecnologías inalámbricas, ya que fueron los primeros en la industria hotelera en México, en lanzar un servicio de acceso inalámbrico a Internet con capacidad de red pública privada (VPN).

Actualmente, los ejecutivos que llegan a hospedarse a Sheraton Suites tienen la posibilidad de acceder a Internet y archivos en sus empresas con la máxima seguridad. Lo único que tienen que hacer es conectar una tarjeta inalámbrica a su notebook, configurarla y ser reconocidos por la red en cualquier lugar del hotel: habitaciones, restaurante, jardín, bar, salones y lobby, durante todo el día, por la módica cantidad de \$150 pesos diarios. Una ganga si se toma en cuenta que una hora en el centro de negocios puede superar los \$100 pesos.

Sólo se tiene que dejar un voucher abierto por \$200 dólares, en caso de extravío de la tarjeta inalámbrica. Y si por casualidad alguien no lleva consigo una computadora portátil, puede rentarla por \$40 dólares por día.

No es necesario hacer el login cada vez que se trasladan a otro punto del edificio, ya que las 20 antenas instaladas los reconocen siempre. Esto se logra gracias a que el backbone es totalmente inalámbrico.

Antes de que existiera este servicio, si un cliente requería del acceso a Internet, debía acudir al business center del hotel y utilizar una de las máquinas que había ahí. La conexión no era la óptima: se utilizaba un enlace dial-up, el cual además se compartía con el resto de los usuarios que laboran en la empresa. Por tanto, la velocidad se veía seriamente mermada, esto nos muestra que la necesidad de conectividad a Internet de primer nivel era un punto necesario para dar un mejor servicio a los clientes de este servicio.

También existía la opción de conectarse mediante la línea telefónica de su habitación, pero la facturación de este servicio provocaba inconformidades. Como en la mayoría de los hoteles, el conmutador está programado para contabilizar el uso de los teléfonos por minuto. Pero claramente los clientes se quejaban de lo costoso que resultaba al final este servicio.

Claramente la búsqueda de opciones para prestar un servicio de calidad y, sobre todo, económico.

Una de las alternativas, además de una red inalámbrica, fue instalar cableado estructurado en las 194 habitaciones. No fue la más convincente, ya que además de resultar muy costosa requería abrir paredes para cablear el edificio; algo que definitivamente afectaría la imagen del lugar.

También está la opción del servicio On Command, un sistema de acceso a la red mediante la televisión. Si bien parece interesante, particularmente porque la TV tiene un teclado inalámbrico que llama la atención y que hasta parece un juego, no tiene el desempeño necesario. Aunque los proveedores aseguran que funciona de maravilla, sus clientes no opinan lo mismo. Entre los hoteles que tienen On Command la mayoría reportan muchos problemas. Por ejemplo, si se conectan cinco usuarios simultáneos, la señal se cae, apuntan los huéspedes que han utilizado este servicio. Además, la televisión sólo permite navegar por Internet, mas no que los huéspedes conecten sus computadoras y trabajen con ellas, que es el objetivo final.

Una vez que se tomó la decisión de poner una red inalámbrica en el hotel, no hubo muchos problemas para poder llevar a cabo la instalación ya que una de las ventajas que tiene la disposición arquitectónica del hotel es su espacio abierto. Las paredes de las habitaciones son de tablaroca, por lo que las señales no tienen dificultades para atravesarlas. Por tanto, se decidió montar una topología tipo estrella con un Central Outdoor Router (COR) como antena principal para dar servicio al lobby y al bar. Ésta se desempeña como el punto de unión entre la red inalámbrica y la red con cable UTP.

Se asignaron, además, dos Remote Outdoor Router (ROR) para cubrir los salones de eventos y el restaurante, y ocho más se colocaron estratégicamente en los pisos tres, cinco, siete y nueve. La conexión entre el COR y los ROR es de 11 [Mb/s]. Estos 10 puntos de acceso funcionan como el backbone inalámbrico y se utilizan otro 10 más pequeños como respaldo y para reforzar la señal.

La conexión a Internet llega a través de Adetel, la portadora, mediante un enlace de 512 [Kb/s] que va directamente a un ruteador Cisco 1600. Este ruteador se conecta, a su vez, con un Cisco Firewall PIX 515, que ofrece seguridad de acceso a través de VPN y separa el tráfico de la red interna y de la inalámbrica.

El siguiente punto de la ruta es un switch 3Com desde el cual sale la señal hacia los usuarios internos y una más hacia el COR de Avaya, que envía y recibe la señal del resto de las antenas. En las laptops de los visitantes se instalan tarjetas RED PCMCIA para gozar del servicio en cualquier lugar del hotel.

Para ofrecerles acceso remoto de forma segura a las redes corporativas de sus compañías se emplean capacidades VPN basadas en estándares como Internet Key Exchange (IKE)/IP Security (IPSec). Asimismo, se utiliza encriptación de 56 bits Data Encryption Standard (DES) para mantener fuera a los hackers. El cableado estructurado al interior de la red y hacia el punto de acceso fue provisto por Anixter.

Hasta ahora la inversión para ofrecer el servicio de Internet inalámbrico asciende a \$20,000 dólares aproximadamente; pero, se piensa recuperar la inversión en un tiempo estimado de año y medio a dos.

Debido a que la competencia es más aguerida cada día, se planean nuevos servicios, como el sistema USG de Nomadix. Con este equipo, ya no será necesario que un empleado del business center o de la recepción configuren cosas como las direcciones IP y DNS en la computadora para tener acceso inalámbrico a Internet, como se hace actualmente. USG brinda la capacidad plug-and-play, por lo que en un futuro bastará colocar la tarjeta inalámbrica y todas las configuraciones se harán automáticamente para que la red las reconozca.

También se podrá segmentar la velocidad que se requiera, desde 64 [kb/s] hasta 1 [Mb/s], de acuerdo con las necesidades de cada usuario. Si en un momento dado un huésped está trabajando con 64 Kbps y requiere incrementar a 512 [Kb/s] durante un corto periodo de tiempo, va a ser posible que lo haga; se le cobrará adicionalmente sólo el lapso en que ocupó la velocidad alta.

Sheraton Suites Santa Fe ha demostrado ser un innovador, al grado que los directores de sistemas de hoteles como Four Seasons, Fiesta Americana y Camino Real, entre otros, se han acercado a la gerencia de este hotel para conocer su experiencia con este proyecto. Y así no pueden quedarse atrás para cumplir la promesa del acceso en cualquier lugar y a cualquier hora.

CONCLUSIONES

Después de recabar toda la información y realizar el análisis de cada uno de los puntos correspondientes al temario propuesto en este trabajo de tesis, podemos concluir lo siguiente:

Las redes inalámbricas tienen como objetivo principal, proporcionar al usuario una gran movilidad sin perder conectividad, teniendo como atractivo fundamental, la facilidad de instalación, bajo consumo de potencia y además la tasa de transmisión que ya alcanzan en algunas aplicaciones más de 54 [Mb/s]. Por otro lado, el ahorro que supone la supresión del medio de transmisión cableado, en este sentido el objetivo fundamental es formar redes híbridas donde coexistan los dos sistemas teniendo claro que la integración con otras redes beneficiará en forma global a dicha red híbrida.

Tras estudiar las topologías de las redes inalámbricas, descubrimos el verdadero potencial de este tipo de redes. Su flexibilidad y versatilidad justifican perfectamente su existencia, ya que en situaciones muy concretas (características de edificios, situación geográfica de otras redes o terminales, necesidad de desplazamiento continuo, etc.) las redes inalámbricas son casi la única solución, y permiten además una gran variedad de configuraciones.

La discusión y comparación de cada una de las redes se desarrolló al final de cada capítulo y fue ahí donde se analizó las características principales de las diferentes tecnologías, con base en ese análisis y comparación podemos concluir, que, el implementar una red inalámbrica depende totalmente de las necesidades de conectividad, así como de la aplicación y necesidades que queramos cubrir con la red; debemos hacer un estudio minucioso de las características del recinto, el número de usuarios con acceso inalámbrico y el tipo de equipos que se utilizarán.

Así mismo en el estudio que se llevó a cabo de los diferentes tipos de redes inalámbricas y sus aplicaciones podemos mencionar que, esta área de las telecomunicaciones aún se encuentra en un proceso de desarrollo, por que las aplicaciones que tenemos disponibles en ellas son limitadas; esto se debe a que no se manejan las grandes tasas de transmisión como en las redes alámbricas, pero se prevé que en un futuro no muy lejano esto podría cambiar gracias a las distintas técnicas y avanzados protocolos de comunicación entre los dispositivos utilizados para redes inalámbricas. Ahora, otro punto muy importante es la interconectividad que se pretende tener con este tipo de redes, la cual consiste en tener siempre una comunicación entre ellas aunque se estén utilizando distintos tipos de tecnologías, por ejemplo, se va a tener la posibilidad de comunicar una WLAN y una WPAN y así mismo la WPAN estar intercomunicada con una red celular conformando así una red Ad Hoc. La ventaja de lo mencionado anteriormente, es que se contará con total libertad de movimiento, seguridad y privacidad al momento de entablar una comunicación, esto es posible, gracias al desarrollo de técnicas habilitadoras tan avanzadas, que en un futuro el transmitir información de suma importancia será tan seguro como enviarla por una red convencional alámbrica.

Como se describió existen una gran variedad de redes inalámbricas, pero nosotros creemos que las más representativas por su uso, y por las necesidades que llegan a cubrir en el ámbito de las redes inalámbricas de área local (WLANs) son, HiperLAN2 y el estándar IEEE 802.11 con sus diferentes grupos de trabajo; y con respecto a las redes de área personal (WPANs), Bluetooth y HomeRF. Es por eso que el cuadro siguiente concluye con el análisis de estas tecnologías tan importantes en el mercado mundial. Además de que son tecnologías que día con día siguen desarrollando nuevas alternativas, y que son de muy fácil acceso a todo tipo de público, es decir, que este tipo de redes pueden estar presentes desde un hogar o un edificio empresarial hasta las ya conocidas comunicaciones celulares.

Conclusiones.

	IEEE 802.11	HomeRF	Bluetooth	HiperLAN2
Características Generales y de la Capa Física				
Capacidad Nomádica	Parcialmente al ser detectado por el AP	Sólo en el área de cobertura del AP	Parcialmente al ser detectado por el AP	Parcialmente al ser detectado por el AP
Movilidad	Sí, al ser administrado por capas superiores	No	La movilidad del maestro afecta la configuración de la piconet. Puede administrarse por capas superiores	Sí, al intercambiar servicios con otras redes LAN
Administración de la Potencia	Con tendencias a permanecer activo y el AP mandan mensajes en el periodo de espera	Con tendencias a permanecer activo y el AP mandan mensajes en el periodo de espera	Con tendencias a permanecer activo	Con tendencias a permanecer activo y el AP mandan mensajes en el periodo de espera
Número de Dispositivos conectados	127	127	7 esclavos por maestro	256
Tasa de transmisión [Mb/s]	1, 2 -IEEE802.11 11-IEEE802.11b 54-IEEE802.11a 54-IEEE802.11g	1.6	1	54
Banda de frecuencia	5[GHz] para IEEE802.11a y 2.4[GHz] para los demás	2.4[GHz]	2.4[GHz]	2.4[GHz]
Seguridad	Verifica la autenticidad y utiliza WEP	Verifica la autenticidad y utiliza encriptado	Compartir la llave y encriptado	Compartir la llave y encriptado
Facilidad en la instalación	Inmediata para una topología Ad hoc	Inmediata para una topología Ad hoc		
Facilidad en el mantenimiento	Sí	Sí	Sí	Sí
Costo aproximado	Precio aceptable \$1 600	Económico entre \$110 y \$1 100	Muy económico entre \$55 y \$550	Caro
Capacidad de conexión con otras redes	Con bridge para LANs IEEE802 y con distintos routers	Con bridge para LANs IEEE802 y con distintos routers	Con bridge para LANs IEEE802 y con protocolos PPP	Funciones internas para soportar tráfico ya sea por paquetes o celular
Características de la Capa de Enlace				
Topología Inalámbrica	Ad hoc o infraestructura	Ad hoc o infraestructura con un solo AP	infraestructura	Ad hoc o infraestructura
Tipo de acceso al medio para una topología Ad hoc	Descentralizado para un tráfico asincrono y centralizado para los demás	Descentralizado para un tráfico asincrono y centralizado para los demás	Centralizado	Centralizado
Tipo de acceso al medio para una topología con infraestructura	Sólo descentralizado para tráfico asincrono	Sólo descentralizado para tráfico asincrono	Centralizado	Centralizado con elección a que un AP controle el medio
Comunicación centralizada	No	No	Sí	No, si existe comunicación directa
Comunicación con dispositivos fuera del rango de cobertura	Sí, al utilizar enrutamiento en capas superiores	Sí, al utilizar enrutamiento en capas superiores	Sí, al utilizar enrutamiento en capas superiores	Sí, al utilizar enrutamiento en capas superiores
Soluciones para problemas de nodos no detectados	Con la trama RTS y CTS	Sólo se usa un AP	Salto en frecuencia	Cada dispositivo en la red utiliza un canal de frecuencia diferente



Conclusiones.

Tráfico				
Unicast Multicast Broadcast	Unicast Multicast Broadcast: Dentro del rango de cobertura de los dispositivos	Unicast Multicast Broadcast: Dentro del rango de cobertura de los dispositivos	Unicast: Sólo entre el maestro y el esclavo Broadcast: Sólo el maestro	Unicast: Entre un par de dispositivos dentro del rango de cobertura del AP Multicast Broadcast: Entre el AP y los dispositivos
Retardo de guarda punto a punto	Entre dos dispositivos seleccionado en el área de cobertura	Entre dos dispositivos seleccionado en el área de cobertura	Sólo en una piconet con polling	Entre dos dispositivos seleccionado en el área de cobertura
Variaciones delimitadas	Entre dos dispositivos seleccionado en el área de cobertura	Entre dos dispositivos seleccionado en el área de cobertura	Entre dos dispositivos seleccionado en el área de cobertura	Entre dos dispositivos seleccionado en el área de cobertura
Perdidas de Control	Con ARQ para paquetes Unicast	Con ARQ para paquetes Unicast	Con ARQ para paquetes Unicast	Con ARQ para paquetes Unicast
Nivel de Prioridad de Usuarios	No	No	No	según en donde se establezca la conexión
Dinámicas para la Distribución de Tráfico	No hay retardos para cambios de tráfico Asíncrono. Actualización de la tabla de peticiones para cambios en el tráfico síncrono.	No hay retardos para cambios de tráfico Asíncrono. Actualización de la tabla de peticiones para cambios en el tráfico síncrono.	No hay retardos para cambios de tráfico Asíncrono.	Actualización de la tabla de peticiones para cambios en el tráfico síncrono.
Coexistencia con diferentes tipos de tráfico	Con un supertrama: Peticiones para tráfico síncrono y contención para asíncrono.	Con un supertrama: Peticiones para tráfico síncrono y contención para asíncrono.	Continuas peticiones de datos en tráfico asíncrono y síncrono. Variaciones con tráfico asíncrono para recibir un intervalo máximo de datos.	Con supertrama: Se hacen las peticiones de transmisión de datos en cualquier tipo de tráfico.

TESIS CON FALLA DE ORIGEN

APENDICE A. Seguridad de Redes Inalámbricas

La utilización del aire como medio de transmisión de datos mediante la propagación de ondas de radio ha proporcionado nuevos riesgos de seguridad. La salida de estas ondas de radio fuera del área de cobertura de la red permite la exposición de los datos a posibles intrusos que podrían obtener información sensible de la red y de la seguridad informática de la misma.

Varios son los riesgos derivados de este factor. Por ejemplo, se podría perpetrar un ataque por inserción, bien de un usuario no autorizado o por la ubicación de un punto de acceso ilegal más potente que capte las estaciones cliente en vez del punto de acceso legítimo, interceptando la red inalámbrica. También sería posible crear interferencias y una más que posible denegación de servicio con sólo introducir un dispositivo que emita ondas de radio a la misma frecuencia con la que la red este trabajando.

La posibilidad de comunicarnos entre estaciones cliente directamente, sin pasar por el punto de acceso permitiría atacar directamente a una estación cliente, generando problemas si esta estación cliente ofrece servicios TCP/IP o comparte ficheros. Existe también la posibilidad de duplicar las direcciones IP o MAC de estaciones cliente legítimas.

Los puntos de acceso están expuestos a un ataque de Fuerza bruta para averiguar los passwords, por lo que una configuración incorrecta de los mismos facilitaría la irrupción en una red inalámbrica por parte de intrusos.

A pesar de los riesgos anteriormente expuestos, existen soluciones y mecanismos de seguridad para impedir que cualquiera con los materiales suficientes pueda introducirse en una red. Unos mecanismos son seguros, otros, como el protocolo WEP fácilmente 'rompibles' por programas distribuidos gratuitamente por Internet.

A.1 Mecanismos de Seguridad

A.1.1 WEP (*Wired Equivalent Protocol*)

El protocolo WEP es un sistema de encriptación estándar propuesto por el comité 802.11, implementada en la capa MAC y soportada por la mayoría de vendedores de soluciones inalámbricas. En ningún caso es comparable con IPSec. WEP comprime y cifra los datos que se envían a través de las ondas de radio.

Con WEP, la tarjeta de red encripta el cuerpo y el CRC de cada trama 802.11 antes de la transmisión utilizando el algoritmo de encriptación RC4 proporcionado por RSA Security. La estación receptora, sea un punto de acceso o una estación cliente es la encargada de desencriptar la trama.

Como parte del proceso de encriptación, WEP prepara una estructura denominada 'seed' obtenida tras la concatenación de la llave secreta proporcionada por el usuario de la estación emisora con un vector de inicialización (IV) de 24 bits generada aleatoriamente. La estación cambia el IV para cada trama transmitida.

A continuación, WEP utiliza el 'seed' en un generador de números pseudoaleatorio que produce una llave de longitud igual al payload (cuerpo más CRC) de la trama más un valor para chequear la integridad (ICV) de 32 bits de longitud.

El ICV es un checksum que utiliza la estación receptora para recalcularla y compararla con la enviada por la estación emisora para determinar si los datos han sido manipulados durante su envío. Si la estación receptora recalcula un ICV que no concuerda con el recibido en la trama, esta queda descartada e incluso puede rechazar al emisor de la misma.

WEP especifica una llave secreta compartida de 40 o 64 bits para encriptar y desencriptar, utilizando la encriptación simétrica.

Antes de que tome lugar la transmisión, WEP combina la llave con el payload/ICV a través de un proceso XOR a nivel de bit que producirá el texto cifrado. Incluyendo el IV sin encriptar sin los primeros bytes del cuerpo de la trama.

La estación receptora utiliza el IV proporcionado junto con la llave del usuario de la estación receptora para desencriptar la parte del payload del cuerpo de la trama.

Cuando se transmiten mensajes con el mismo encabezado, por ejemplo el FROM de un correo, el principio de cada payload encriptado será el mismo si se utiliza la misma llave. Tras encriptar los datos, el principio de estas tramas será el mismo, proporcionando un patrón que puede ayudar a los intrusos a romper el algoritmo de encriptación. Esto se soluciona utilizando un IV diferente para cada trama.

La vulnerabilidad de WEP reside en la insuficiente longitud del Vector de Inicialización (IV) y lo estáticas que permanecen las llaves de cifrado, pudiendo no cambiar en mucho tiempo. Si utilizamos solamente 24 bits, WEP utilizará el mismo IV para paquetes diferentes, pudiéndose repetir a partir de un cierto tiempo de transmisión continua. Es a partir de entonces cuando un intruso puede, una vez recogido suficientes tramas, determinar incluso la llave compartida.

En cambio, 802.11 no proporciona ninguna función que soporte el intercambio de llaves entre estaciones. Como resultado, los administradores de sistemas y los usuarios utilizan las mismas llaves durante días o incluso meses. Algunos vendedores han desarrollado soluciones de llaves dinámicas distribuidas.

A pesar de todo, WEP proporciona un mínimo de seguridad para pequeños negocios o instituciones educativas, si no está deshabilitada, como se encuentra por defecto en los distintos componentes inalámbricos.

A.1.2 OSA (*Open System Authentication*)

Es otro mecanismo de autenticación definido por el estándar 802.11 para autenticar todas las peticiones que recibe. El principal problema que tiene es que no realiza ninguna comprobación de la estación cliente, además las tramas de gestión son enviadas sin encriptar, aún activando WEP, por lo tanto es un mecanismo poco fiable.

A.1.3 ACL (*Access Control List*)

Este mecanismo de seguridad es soportado por la mayoría de los productos comerciales. Utiliza; como mecanismo de autenticación, la dirección MAC de cada estación cliente, permitiendo el acceso a aquellas MAC que consten en la Lista de Control de Acceso.

A.1.4 CNAC (*Closed Network Access Control*)

Este mecanismo pretende controlar el acceso a la red inalámbrica y permitirlo solamente a aquellas estaciones cliente que conozcan el nombre de la red (SSID) actuando este como contraseña.

A.2 Diseño Recomendado

Se podrían hacer varias recomendaciones para diseñar una red inalámbrica e impedir lo máximo posible el ataque de cualquier intruso.

Como primera medida, se debe separar la red de la organización en un dominio público y otro privado. Los usuarios que proceden del dominio público (los usuarios de la red inalámbrica) pueden ser tratados como cualquier usuario de Internet (externo a la organización). Así mismo, instalar cortafuegos y mecanismos de autenticación entre la red inalámbrica y la red clásica,

situando los puntos de acceso delante del firewalls y utilizando VPN a nivel de firewalls para la encriptación del tráfico en la red inalámbrica.

Los clientes de la red inalámbrica deben acceder a la red utilizando SSH, VPN o IPsec y mecanismos de autorización, autenticación y encriptación del tráfico (SSL). Lo ideal sería aplicar un nivel de seguridad distinto según qué usuario accede a una determinada aplicación.

La utilización de VPNs nos impediría la movilidad de las estaciones cliente entre puntos de acceso, ya que estos últimos necesitarían intercambiar información sobre los usuarios conectados a ellos sin reiniciar la conexión o la aplicación en curso, cosa no soportada cuando utilizamos VPN.

Como contradicción, es recomendable no utilizar excesivas normas de seguridad por que podría reducir la rapidez y la utilidad de la red inalámbrica. La conectividad entre estaciones cliente y PA es FCFS, es decir, la primera estación cliente que accede es la primera en ser servida, además el ancho de banda es compartido, motivo por el cual nos tenemos que asegurar un número adecuado de puntos de acceso para atender a los usuarios.

También se podrían adoptar medidas extraordinarias para impedir la intrusión, como utilizar receivers (Signal Leakage Detection System) situados a lo largo del perímetro del edificio para detectar señales anómalas hacia el edificio además de utilizar estaciones de monitorización pasivas para detectar direcciones MAC no registradas o clonadas y el aumento de tramas de reautenticación.

Por último también podrían ser adoptadas medidas físicas en la construcción del edificio o en la utilización de ciertos materiales atenuantes en el perímetro exterior del edificio, debilitando lo máximo posible las señales emitidas hacia el exterior. Algunas de estas recomendaciones podrían ser, aún a riesgo de resultar extremadas:

- Utilizar cobertura metálica en las paredes exteriores.
- Vidrio aislante térmico (atenúa las señales de radiofrecuencia).
- Persianas venecianas de metal, en vez de plásticas.
- Poner dispositivos WLAN lejos de las paredes exteriores.
- Revestir los closets (rosetas) de la red con un revestimiento de aluminio.
- Utilizar pintura metálica.
- Limitar el poder de una señal cambiando la atenuación del transmisor.

A.3 Políticas de Seguridad

Aparte de las medidas que se hayan tomado en el diseño de la red inalámbrica, debemos aplicar ciertas normas y políticas de seguridad que nos ayudarían a mantener una red más segura:

- Utilizar WEP, aunque sea rompible con herramientas como AirSnort o WEPCrack, como un mínimo de seguridad.
- Utilizar mecanismos de intercambio de clave dinámica aportado por los diferentes productos comerciales hasta que el comité 802.11i, encargado de mejorar la seguridad en las redes inalámbricas, publique una revisión del estándar 802.11 con características avanzadas de seguridad, incluyendo AES (Advanced Encryption Standard) e intercambio dinámico de claves.
- Inhabilitar DHCP para la red inalámbrica. Las IPs deben ser fijas.
- Actualizar el firmware de los puntos de acceso para cubrir los posibles agujeros en las diferentes soluciones wireless.
- Proporcionar un entorno físicamente seguro a los puntos de acceso y desactivarlos cuando se pretenda un periodo de inactividad largo (ej. ausencia por vacaciones).
- Cambiar el SSID (Server Set ID) por defecto de los puntos de acceso, conocidos por todos. El SSID es una identificación configurable que permite la comunicación de los clientes con un determinado punto de acceso. Actúa como un password compartido entre la estación cliente y el punto de acceso. Ejemplos de SSID por defecto son "tsunami" para Cisco, "101" para 3Com, "Intel" para Intel.
- Inhabilitar la emisión broadcast del SSID.

- Reducir la propagación de las ondas de radio fuera del edificio.
- Utilizar IPsec, VPN, firewalls y monitorizar los accesos a los puntos de acceso.

A.4 Sistemas Detectores de Intrusos

Los sistemas detectores de intrusos, IDS, totalmente integrados en las redes clásicas cableadas, están tomando forma también en las redes inalámbricas. Sin embargo, aún son pocas las herramientas disponibles y sobretodo realmente efectivas, aunque empresas privadas están desarrollando y adaptando sus sistemas detectores de intrusos para redes inalámbricas (como ISS en su software Real Secure).

Las redes inalámbricas nos proporcionan cambios nuevos respecto a los sistemas de detección de intrusos situados en las redes clásicas cableadas.

En primer lugar, la localización de la estación de captura de tráfico debe estar instalado en la misma área de servicios WLAN que queramos monitorizar. Este punto es crítico y obtendremos muchos falsos positivos si la localización es inapropiada o la sensibilidad del agente tan elevada que puede incluso capturar tráfico procedente de otras WLANs ajenas a la nuestra.

Otro punto crítico en los sistemas detectores de intrusos para redes es la identificación de tráfico anómalo, ya que existen aplicaciones como el NetStumbler y Dstumbler que utilizan técnicas de descubrimiento de redes inalámbricas especificadas en 802.11 junto con otras propias, por lo que el agente IDS debe detectar y distinguir un tráfico de otro. Como punto positivo encontramos que ya existen patrones para distinguir a estos programas utilizados por los intrusos.

A.5 Futuros cambios: Comité 802.11i

Siendo conscientes de las debilidades del estándar 802.11 en su protocolo WEP, se formó el comité 802.11i para paliar y mejorar los aspectos de seguridad en las redes inalámbricas. Muchos son los que creen que las medidas llegan tarde, y que las soluciones propietarias se han hecho 'dueñas' en este apartado mediante los protocolos ULA (Upper Layer Protocol), aplicables a las capas más altas del modelo OSI, y no especificadas en 802.11i por no ser objetivo del estándar.

A.5.1 Los Protocolos ULA (Upper Layer Protocol)

Los protocolos ULA proporcionan intercambio de autenticación entre el cliente y un servidor de autenticación. La mayoría de los protocolos de autenticación incluyen:

- EAP-TLS (Extensible Authentication Protocol with Transport Layer Security), protocolo de autenticación basado en certificados y soportado por Windows XP. Necesita la configuración de la máquina para establecer el certificado e indicar el servidor de autenticación.
- PEAP (Protected Extensible Authentication Protocol), proporciona una autenticación basada en el password. En este caso, solamente el servidor de autenticación necesitaría un certificado.
- EAP-TTLS (EAP with Tunneled Transport Layer Security), parecido al PEAP, está implementado en algunos servidores Radius y en software diseñado para utilizarse en redes 802.11 (inalámbricas).
- LEAP (Lightweigh EAP), propiedad de Cisco y diseñado para ser portable a través de varias plataformas wireless. Basa su popularidad por ser el primero y durante mucho tiempo el único mecanismo de autenticación basado en password y proporcionar diferentes clientes según el sistema operativo.

Las medidas que el comité 802.11i esta estudiando intentará mejorar la seguridad de las redes inalámbricas. Estas medidas se publicarán a principios de este año, pero ya existen documentos que nos hablan por donde se encaminan dichas mejoras.

Los cambios se fundamentan en 3 puntos importantes, organizados en dos capas.

A un nivel más bajo, se introducen dos nuevos protocolos de encriptación sobre WEP totalmente compatibles entre sí, el protocolo TKIP (Temporal Key Integrity Protocol) y el CCMP (Counter Mode with CBC-MAC Protocol), que trataremos de explicar a continuación, junto con el estándar 802.1x para el control de acceso a red basado en puertos.

A.5.2 Estándar 802.1x

Como ya he comentado anteriormente, es un estándar de control de acceso a la red basado en puertos. Como tal, restringe el acceso a la red hasta que el usuario se ha validado.

El sistema se compone de los siguientes elementos:

- Una estación cliente.
- Un punto de acceso.
- Un servidor de Autenticación (AS).

Es este nuevo elemento, el Servidor de Autenticación, el que realiza la autenticación real de las credenciales proporcionadas por el cliente. El AS es una entidad separada situada en la zona cableada (red clásica), pero también se puede implementar en un punto de acceso. El tipo de servidor utilizado podría ser el RADIUS, u otro tipo de servidor que se crea conveniente (802.1x no especifica nada al respecto).

El estándar 802.1x introduce un nuevo concepto, el concepto de puerto habilitado/inhabilitado en el cual hasta que un cliente no se valide en el servidor no tiene acceso a los servicios ofrecidos por la red. El esquema posible de este concepto lo podemos ver a continuación:

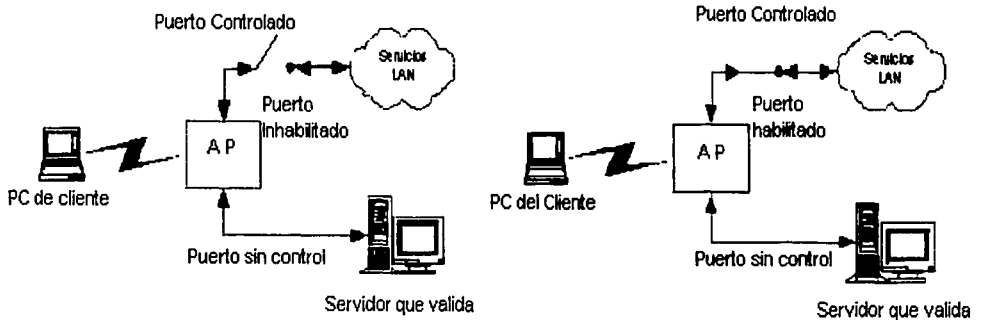


Figura A.1 Esquema puerto habilitado/inhabilitado 802.1x

En sistemas con 802.1x activado, se generarán 2 llaves, la llave de sesión (pairwise key) y la llave de grupo (groupwise key). Las llaves de grupo se comparten por todas las estaciones cliente conectadas a un mismo punto de acceso y se utilizarán para el tráfico multicast, las llaves de sesión serán únicas para cada asociación entre el cliente y el punto de acceso y se creará un puerto privado virtual entre los dos.

El estándar 802.1x mejora la seguridad proporcionando las siguientes mejoras sobre WEP:

- Modelo de seguridad con administración centralizada.
- La llave de encriptación principal es única para cada estación, por lo tanto, el tráfico de esta llave es reducido (no se repite en otros clientes).

- Existe una generación dinámica de llaves por parte del AS, sin necesidad de administrarlo manualmente.
- Se aplica una autenticación fuerte en la capa superior.

A.5.3 TKIP (Temporal Key Integrity Protocol)

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP y mantener la compatibilidad con el hardware utilizado actualmente mediante una actualización del firmware.

El protocolo TKIP está compuesto por los siguientes elementos:

- Un código de integración de mensajes (MIC), encripta el checksum incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.
- Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.
- Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIP Sequence Counter) para protegerse contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

La estructura de encriptación TKIP propuesta por 802.11i sería la siguiente:

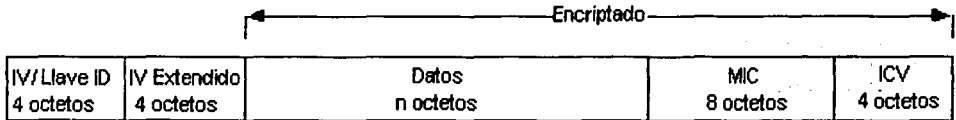


Figura 2: Estructura de encriptación TKIP

La utilización del TSC extiende la vida útil de la llave temporal y elimina la necesidad de redecodificar la llave temporal durante una sola asociación. Pueden intercambiarse 248 paquetes utilizando una sola llave temporal antes de ser rehusada.

Se combinan en dos fases la llave temporal, la dirección del emisor y el TSC para la obtención de una llave de 128 bits por paquete, dividido en una llave RC4 de 104 bits y en una IV de 24 bits para su posterior encapsulación WEP.

El MIC final se calcula sobre la dirección física origen y destino y el MSDU (MAC Service Data Unit o texto plano de los datos en la trama 802.11) después de ser segmentado por la llave MIC y el TSC.

La función MIC utiliza una función hash unidireccional, si es necesario, el MSDU se fragmenta incrementando el TSC para cada fragmento antes de la encriptación WEP.

En la descriptación se examina el TSC para asegurar que el paquete recibido tiene el valor TSC mayor que el anterior. Sino, el paquete se descartará para prevenir posibles ataques por repetición. Después de que el valor del MIC sea calculado basado en el MSDU recibido y descriptado, el valor calculado del MIC se compara con el valor recibido.

En el proceso de encapsulado TKIP se muestra a continuación:

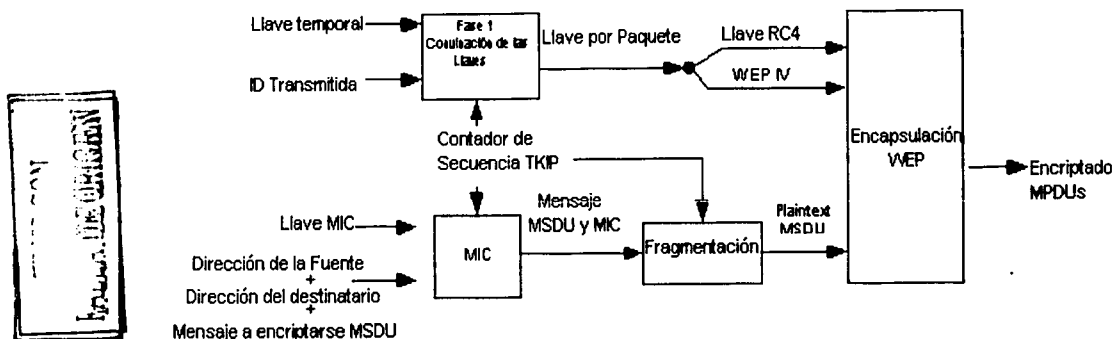


Figura 3: Proceso de encapsulación TKIP

A.5.4 CCMP (Counter Mode with CBC-MAC Protocol)

Este protocolo es complementario al TKIP y representa un nuevo método de encriptación basado en AES (Advanced Encryption Standards), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC. Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizando 802.11i.

En la siguiente figura podemos observar el formato tras la encriptación CCMP:

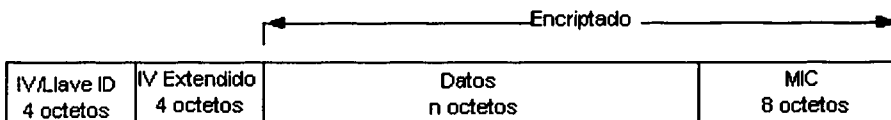


Figura 4: Estructura encriptación CCMP

CCMP utiliza un IV de 48 bits denominado Número de Paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el MIC y la encriptación de la trama.

Apéndice B. Sistema de Telefonía Móvil Digital GSM.

En 1982, cuando aparecieron los primeros servicios celulares comerciales, la CEPT (*Conference Européen des Postes et Télécommunications*) tomó la iniciativa de poner en marcha un grupo de trabajo (llamado *Groupe Spécial Mobile*) encargada de especificar un sistema de comunicaciones móviles común para Europa en la banda de 900 [MHz].

Los servicios móviles pueden asociarse más fácilmente a un abonado que a un equipo o a una terminación de línea, proporcionando lo que se conoce como servicios de comunicación personal. Se espera que el desarrollo de redes de comunicación personal con acceso radio a la red fija afecte a una proporción significativa de abonados en los próximos diez años. De entre las posibles tecnologías que podrían ser utilizadas para soportar tales servicios se ha escogido la GSM, adaptada a la banda recientemente reservada de 1800 [MHz] (1850-2200 [MHz]), constituyendo el llamado DCS 1800 (*Digital Cellular System*).

B.1.1 Servicios y Facilidades del Sistema GSM

En principio, todos los servicios disponibles en la Red Digital de Servicios Integrados (RDSI) han sido incluidos en el desarrollo de GSM. Pero debido a las restricciones de velocidad de transmisión de datos y tasa de errores, algunos de los servicios han sido desarrollados con restricciones.

B.1.1.1 Teleservicios

- La telefonía es el teleservicio más importante del sistema GSM. Permite llamadas entre la red pública (RTPC/RDSI) y la red móvil
- Soporta el servicio de fax del Grupo 3 si se dispone de los adaptadores de interfaz correspondientes.
- Ofrece un tipo de correo electrónico (E-mail) de mensajes cortos (140 bytes) que puede considerarse como un servicio de búsqueda (*paging*) alfanumérico y bidireccional. Se confirma la entrega de los mensajes, lo que constituye una ventaja importante sobre los sistemas de búsqueda.

B.1.1.2 Servicios Portadores: Para servicios de datos, soportan velocidades de transmisión que van de los 300 bits/s a los 9.6 [Kb/s].

B.1.1.3 Servicios Suplementarios: Muchos de estos servicios son equivalentes a los disponibles en la RDSI. Los principales son: llamada restringida, desvío de llamadas, identificación del abonado llamante.

B.1.1.4 Módulo de Identidad de Abonado: Una terminal GSM no tiene acceso a la red salvo si dispone de todos los datos específicos del abonado. Estos datos están incluidos en una tarjeta inteligente llamada SIM (*Subscriber Identity Module*) que debe introducirse en el terminal. La tarjeta SIM, cuyo acceso se protege con un número de identificación personal, contiene, no sólo los datos del abonado (número en la RDSI, clave personal, etc...) sino también determinada información personal, como marcación abreviada de números, lista de redes preferentes e información de las tarifas. En la tarjeta SIM también se almacenan los mensajes cortos.

B.1.1.5 Funciones de Seguridad: En el sistema GSM la protección de la información se realiza a tres niveles:

1. Autenticación por el sistema de las tarjetas SIM, para impedir el acceso a usuarios no registrados.
2. Cifrado de la transmisión para impedir escuchas no autorizadas (voz y datos).
3. Protección de la identidad del abonado.

B.1.1.6 Arquitectura Funcional e Interfases de un sistema GSM

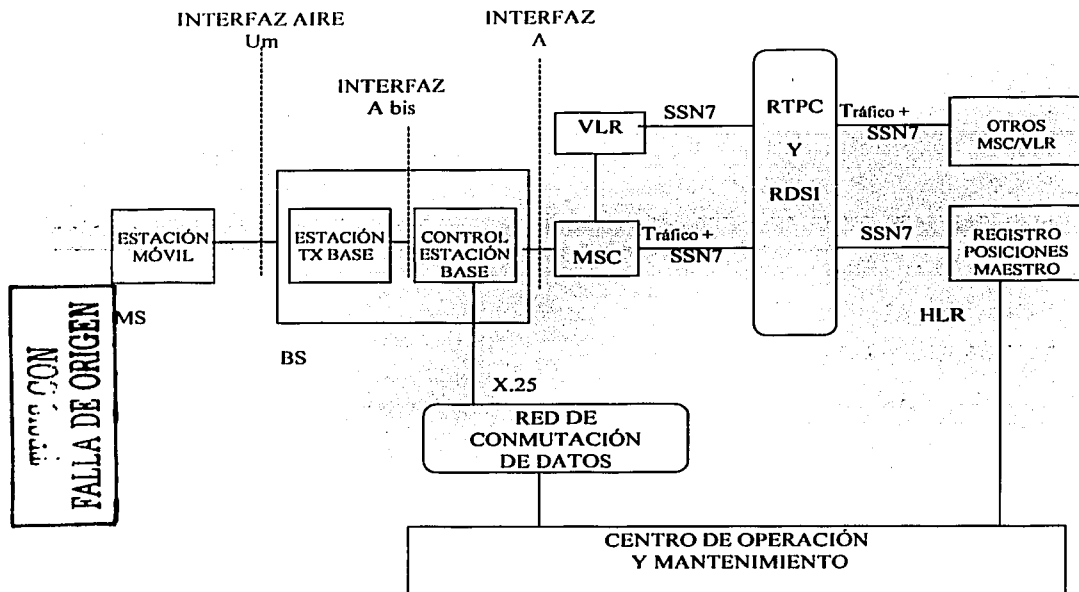


Figura 1. Aquí se muestran las principales entidades funcionales e interfaces de un sistema GSM.

El sistema de la estación comprende un controlador y un equipo transmisor-receptor desplegado en el área de cobertura. La parte del subsistema de red incluye un equipo de conmutación (MSC, *Mobile Switching Centre*) dedicado al servicio móvil, que enlaza todos los elementos del sistema, a través de líneas dedicadas, con la red pública (RTPC o RDSI).

B.1.1.6.1 Bases de Datos de la Red

Las bases de datos que se utilizan en GSM para la gestión de las funciones de movilidad de abonados y para el control de la llamada son:

- La HLR (*Home Location Register*). Almacena información de los abonados locales tal como: el perfil de servicio de cada abonado y su posición en todo momento.
- La VLR (*Visiting Location Register*). Almacena la identificación de los usuarios que se encuentran de paso por las células que dependen de un MSC.
- La EIR (*Equipment Identity Register*). Almacena los identificadores de los equipos de los abonados. Ello se utiliza para detectar el uso no autorizado de equipos de usuario, impidiéndose el acceso a la red.
- La AC (*Authentication Centre*). Almacena la clave y el algoritmo para cifrar la identidad del usuario y para cifrar la información que viaja vía radio

Las especificaciones de GSM definen funciones lógicamente separadas e interfaces para cada una de las bases de datos, permitiendo que cada función se pueda implementar en un componente de red distinto y físicamente separado.

B.1.1.6.2 Plan de Numeración

Se asigna un número internacional RDSI bien al usuario, a través de la tarjeta SIM, o bien al terminal móvil. La numeración en cada país debe ser compatible con el panel de numeración nacional correspondiente.

El número consiste en un código de país, un código intra-nacional (que básicamente identifica la red móvil destino) y el número de abonado. Fundamentalmente, el número de abonado define el encaminamiento de la llamada a través de la RTPC/RDSI hacia la MSC destino. El MSC usa el número de abonado para extraer de la HLR la información de re-encaminamiento apropiada para hacer llegar la llamada a la MSC en la que se encuentra el abonado de paso.

La información de re-encaminamiento viene especificada por el número de roaming (*roaming number*) que se obtiene de la HLR. Este número es un código temporal asignado por la VLR al usuario visitante y enviado a la HLR y tiene la misma estructura que los número RDSI de la zona en la que se encuentra el usuario.

B.1.2 Protocolo de Capa 1

B.1.2.1 Estructura de los Canales Radio

Se utiliza una estructura de acceso TDMA/FDMA. Se han estandarizado dos bandas de frecuencias:

1. 890-915 [MHz] para la dirección móvil a estación base.
2. 935-960 [MHz] para la dirección estación base a móvil.

Estas bandas se han dividido en 124 pares de portadoras separadas 200 [KHz], empezando con el par 890.2/935.2 [MHz]. Cada célula tiene asignadas un conjunto de pares, desde sólo una a un máximo de 15. El tamaño de las células varía de 1 a varios kilómetros.

Cada una de las portadoras se ha segmentado en tiempo, de acuerdo a un esquema de acceso múltiple por división en el tiempo. (TDMA), en 8 intervalos de tiempo de duración 0.577 [ms/intervalo]. Los intervalos de tiempo se numeran del 0 al 7 en la trama, cuya duración es de 4.615 [ms].

Esta misma estructura se emplea en los enlaces ascendente y descendente, pero con un desplazamiento de 2 intervalos, para que un móvil que utilice un canal físico concreto transmita y reciba en instantes de tiempo diferentes. De este modo se evita el duplexor de antena. Además, el móvil monitoriza la señal enviada desde células adyacentes para, en su caso, solicitar un cambio de célula.

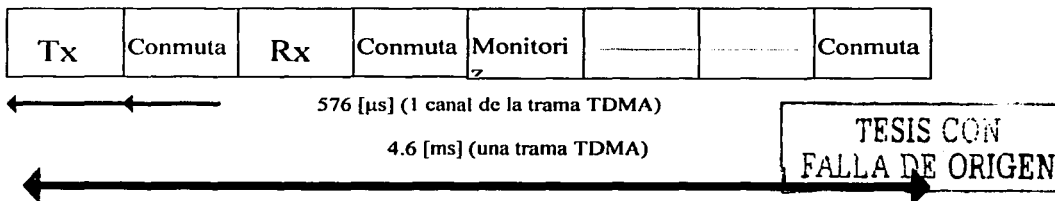


Figura 2. Trama TDMA.

La estación móvil transmite en ráfagas, cuando llega el intervalo de tiempo correspondiente, de 148 bits, más 8.25 bits de guarda para permitir pequeños desplazamientos de tiempo dentro del intervalo. La velocidad de transmisión es de $156.25 \text{ [bits]/ } 0.577 \text{ [ms]} = 270.833 \text{ [Kb/s]}$. Estos

valores numéricos son aproximados puesto que en la recomendación GSM los tiempos se dan tomando como referencia una multitrama.

La recomendación define 5 tipos de ráfagas: normal, de corrección de frecuencia, de sincronización, muda y de acceso. La estructura de la ráfaga muda es la misma que la de corrección de frecuencia. La ráfaga de tráfico de abonado consta de 148 bits con la siguiente asignación:

- 3+3 bits de encabezado-tail (Tail bits). Tienen por objeto lograr ecualización de todos los bits por igual.
- $2 \times 57 + 2$ bits de información (bits encriptados). De ellos 2×57 son información y otros dos indican si la ráfaga es de tráfico de abonado o de señalización por robo de intervalo.
- 26 bits que constituyen la secuencia de entrenamiento. Esta es secuencia conocida de bits que permite al receptor adquirir la sincronización y analizar las condiciones del canal con objeto de ajustar el ecualizador.
- Las ráfagas modulan la portadora asignada, con modulación GMSK.

B.1.2.2 Canales Físicos y canales Lógicos

Un canal físico se forma mediante la repetición periódica de un intervalo de tiempo. El flujo binario que somos capaces de transferir a través de un canal físico se puede a su vez compartir por varios canales lógicos. En definitiva estamos realizando una multiplexación de canales lógicos sobre los físicos.

En GSM se definen, fundamentalmente, dos tipos de canales lógicos: los de tráfico de abonado y los de señalización y control. Para soportar estos canales lógicos se definen dos estructuras de multitrama una de 26 tramas (con una duración de 120 ms) para los canales de tráfico y otra de 51 tramas (con una duración de 236 ms) para canales de señalización y control.

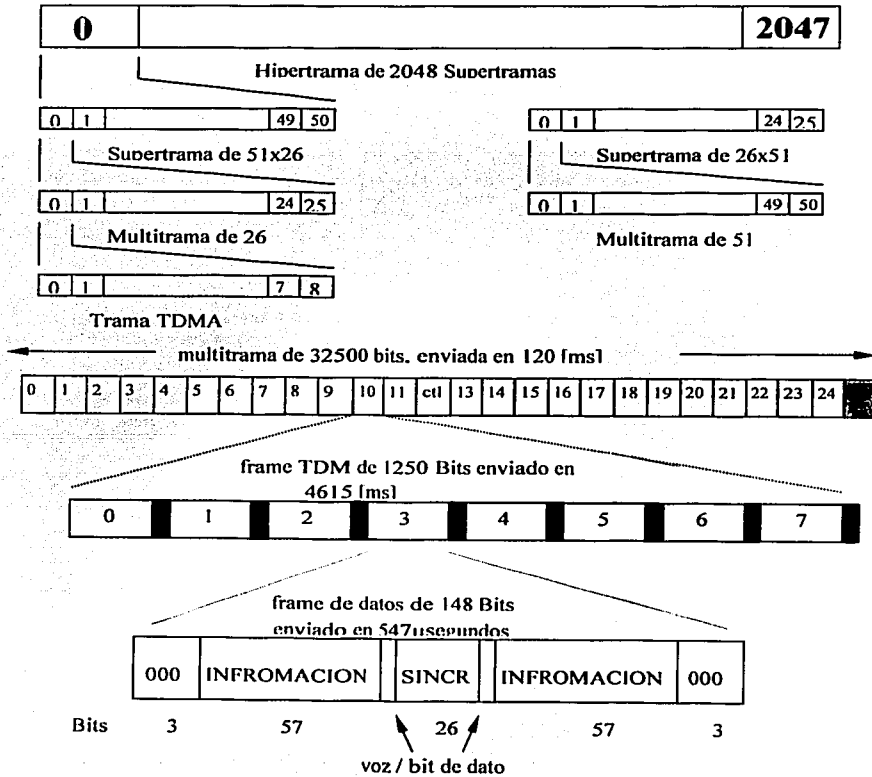


Figura 4. Jerarquía de tramas en un sistema gsm.

TESIS CON
FALLA DE ORIGEN

B.1.2.3 Multitrama de 26 Tramas

La estructura de 26 tramas soporta canales de tráfico (TCH) y sus correspondientes canales asociados de control, que pueden ser lentos (SACCH) o rápidos (FACCH).

Los TCH se han dividido en dos tipos de TCH uno de velocidad máxima y otro de velocidad mitad. Un TCH de velocidad máxima permite la transmisión de voz codificada a 13 [kb/s] o de datos a 3.6, 6 ó 12.6 [kb/s]. Un TCH de velocidad media, que se consigue usando en media una ráfaga de cada dos, permite transportar voz codificada a 6.5 [kb/s] y datos a 2.4 y 4.8 [kb/s]. Estas velocidades son las velocidades de información útil, puesto que las velocidades reales son algo mayores (22.8 [kb/s]) debido a la información de control que hay que incluir.

Los TCH de velocidad máxima se implementan sobre 24 de las 26 tramas de la multitrama, donde cada TCH ocupa el mismo intervalo de tiempo en cada trama. La trama 12 (numeradas desde la 0), se dedica a los canales SACCH, obteniéndose 8 canales SACCH, uno para cada uno de los TCH's. Los canales SACCH llevan señalización correspondiente a la información recurrente, como ajuste de potencia o de trama, medidas de calidad del canal, información de las tarifas, etc. La trama 25 está reservada para implementar los 8 SACCH adicionales requeridos para soportar los 8 canales TCH adicionales de velocidad media.

Canales de tráfico de abonado de tasa máxima



26 Tramas = 120 ms



Canales de tráfico de abonado de tasa máxima

A: Canal de señalización para los canales T
 a: Canal de señalización para los canales t



EL canal FACCH se obtiene bajo demanda mediante el robo de intervalos a un TCH. Se utiliza para el envío de mensajes urgentes como son los relativos al control del *handover* entre células. EL robo de un intervalo se indica mediante los *flags* correspondientes en la ráfaga de tráfico.

B.1.2.4 Multitrama de 51 tramas

Soporta los canales de señalización y control de tipo general como son el inicio/fin de la llamada, identificación y actualización del móvil, etc...

Los canales lógicos de que se dispone son:

- > **SDCCH.** Se utiliza para transferencia de control de la llamada, desde y hacia el móvil durante el establecimiento de la llamada. Como los canales TCH, el SDCCH tiene asociado su propio SACCH y se libera cuando la llamada ha sido establecida.
- > **BCCH.** Se utiliza en la dirección base (BS) a móvil para la difusión de información a nivel de sistema como puede ser: parámetros de sincronización, servicios disponibles e identificador de célula. Este canal está activo de forma permanente, enviando ráfagas mudas cuando no hay

información que transmitir, pues los móviles monitorizan el nivel de señal recibida de este canal para la determinación del *handover*.

- **SCH.** Se utiliza para difundir información, desde la BS al móvil, de sincronización de trama.
 - **FCCH.** Se utiliza para difundir información, desde la BS al móvil, de sincronización de portadora.
 - **CCCH.** Son un conjunto de canales lógicos que se utilizan para transferir información de señalización entre todos los móviles y la BS, por ejemplo cuando se origina una llamada o se realiza la búsqueda mediante llamada. Hay tres canales de control comunes:
- I. PCH. Lo utiliza el sistema para realizar la búsqueda de los móviles.
 - II. RACH. Lo utilizan los móviles que tratan de comunicarse con el sistema. Se utiliza un protocolo de acceso denominado ALOHA RANURADO para solicitar la adjudicación de un canal SDCCH con el que poder iniciar el establecimiento de una llamada.
 - III. AGCH. Lo usa el sistema para asignar recursos a los móviles como puede ser un SDCCH.

Deberíamos hacer nota aquí que los canales PCH y AGCH nunca son usados por el mismo sistema en el mismo instante y por tanto pueden estar implementados sobre el mismo canal lógico.

Todos los canales lógicos descritos, excepto el SDCCH, se implementan sobre el intervalo 0 de las tramas que forman la multitrama (de 51 tramas). Para ello se utiliza una frecuencia dedicada exclusivamente a tareas de control y que se asigna de forma individual a cada célula.

El SDCCH y su canal SACCH se implementan sobre un canal físico seleccionado por el operador. Dependiendo de las necesidades y criterios del operador, con los canales de señalización y control descritos en este apartado se pueden crear tres estructuras de multiplexación de canales lógicos alternativas:

- I. Un canal de difusión (BCCH) y un canal común (CCCH).
- II. Ocho canales dedicados independientes (SDCCHs).
- III. Cuatro canales de control SDCCH, un BCCH y un CCCH.

B.1.2.5 Desplazamiento de la Multitrama de 51 Tramas sobre la de 26 Tramas

Como se mencionó anteriormente, los canales de transmisión y recepción están desplazados en el tiempo de manera que el receptor dispone de cierto tiempo para sintonizarse a la nueva frecuencia. Para permitir que todos los terminales móviles puedan monitorizar los canales de control; la multitrama de 51 tramas se desliza en el tiempo respecto a la multitrama de 26 tramas. De esta forma, cada estación móvil transmite en un intervalo de tiempo y recibe en otro, de los seis restantes; tres se utilizan para conmutar en frecuencia y los otros tres se dedican a monitorización de los canales de control.

B.1.3 Protocolo de Capa 2

B.1.3.1 Estación Móvil a Estación Base

El protocolo de la capa de enlace de datos se denomina LAPD, utilizado para soportar la señalización sobre canal D en la RDSI, pero convenientemente modificado para su uso en un entorno de radio como es GSM.

Los campos son:

- CAMPO DE DIRECCIONAMIENTO. Consta de los siguientes subcampos:
 - I. Identificador del Punto de Acceso al Servicio (*Service Access Point Identifier*, SAPI). Define al destino.

Apéndice B. Sistema de Telefonía Móvil Digital GSM.

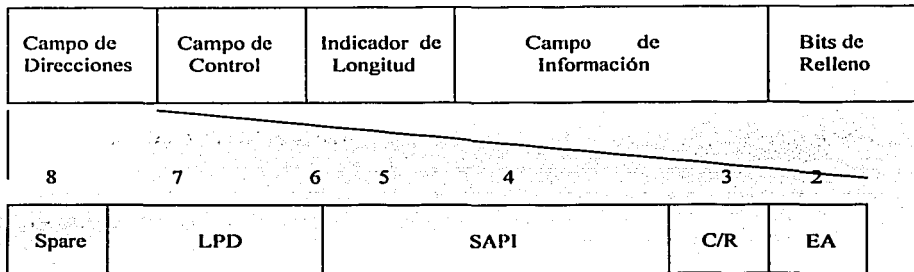
- II. Discriminador de Protocolo (*Link Protocol Discriminator, LPD*). Se usa para especificar alguna de las recomendaciones especiales de LAPDm.
 - III. C/R Indica Comando o Respuesta y su uso es el mismo que el del LAPD.
 - IV. Dirección Extendida (*Extended Address, EA*). Se utiliza para extender el campo de direccionamiento más allá de un octeto. Se debe poner a "1" el último octeto y a "0" en los demás.
 - V. El bit número 8 se ha reservado para uso futuro.
- CAMPO DE CONTROL. Soporta los números de secuencia y especifica el tipo de trama, todo ello de forma análoga a como se hace en LAPD. En LAPDm se utilizan los mismos tipos de trama que en LAPD: tramas no numeradas de información y control, tramas de transferencia de información y tramas de supervisión.
- INDICADOR DE LONGITUD. Delimita el campo de información del campo de relleno (de acuerdo a requerimientos del nivel físico).

Los campos de *flags, bit stuffing* y *campo de detección de errores*, no se utilizan en LAPDm, pues es el nivel físico el encargado de delimitar las fronteras de una trama y de detectar y corregir errores.

Estructura de la Trama

La estructura de la trama LAPDm puede verse en la siguiente figura:

FALLA DE ORIGEN



B.1.3.2 Interfaz Estación Base a Centro de Conmutación Móvil.

La interfase entre la BS y el MSC se realiza sobre un enlace de 2.048 [Mb/s] en el que los canales de voz y los de señalización comparten el medio mediante un multiplexado por división en el tiempo. Los canales lógicos de señalización son el soporte del nivel 2 de la Parte de Transferencia de Mensaje (MTP) del SSN7 del CCITT, que provee los servicios típicos de nivel 2 como son: detección de errores, control de flujo y secuencia correcta de los paquetes.

B.1.4 Protocolos de Capa 3

Las funciones atribuidas al nivel 3 en GSM no son compatibles con las que se han otorgado al nivel 3 de OSI. Los protocolos de nivel 3 en GSM se utilizan para soportar funciones tales como la gestión de los recursos de radio, de la movilidad y de la información relacionada con una llamada. En el modelo OSI estas funciones se atribuyen a niveles superiores. Por ello, se prefiere llamar al nivel 3 en GSM **Nivel de Mensaje (NM)**.

El NM está compuesto de 3 subcapas: la subcapa de gestión de los recursos de radio (*Radio Resource Management*, RR), la subcapa de gestión de la movilidad (*Mobility Management*, MM) y la subcapa de gestión de la conexión (*Connection Management*, CM).

El NM también implementa el nivel 3 del SSN7 del CCITT, tanto la parte de transferencia de mensajes (*Message Part*, MTP) como la parte de señalización para el control de la conexión, entre la BS y el MSC.

B.1.4.1 Gestión de los Recursos de Radio.

El conjunto de protocolos de nivel 3 controla el enlace entre los terminales y la red. Un terminal equipado con una tarjeta SIM, cuando se pone en funcionamiento, explora los canales de radio para encontrar el canal lógico de sincronismo y así sincronizarse. Se queda entonces en un modo semiaactivo, esperando bien el ser llamado mediante el canal de búsqueda, bien una petición para acceder a la red enviando un mensaje en el canal de acceso aleatorio. En el último caso se asigna un canal dedicado mediante el canal de acceso. El proceso de búsqueda es tal que permite al terminal estar en modo discontinuo (*stand by*), es decir la mayor parte del tiempo se encuentra en modo reposo para ahorrar energía.

B.1.4.1.1 Handover

En GSM el concepto del *handover* se ha extendido al ámbito intra-células, lo que implica que se puedan seleccionar distintos canales incluso en la misma célula.

Antes de tomar la decisión de realizar un *handover*, el controlador de la estación base acumula información sobre el tráfico y sobre la situación del enlace de radio, como la calidad (tasa de errores), la potencia transmitida, el nivel de señal recibido y la desviación en tiempo. Tanto la BS como los terminales realizan medidas de calidad. Aprovechando la estructura TDMA, el terminal mide parámetros de la señal que recibe de las células vecinas (a petición de la BS).

Los algoritmos para la decisión del *handover* se implementan en la BS, pero no están especificados en las recomendaciones del GSM. Así, cada fabricante es libre de diseñar un algoritmo exclusivo, esto es especialmente decisivo en entornos de alta densidad de tráfico con células pequeñas.

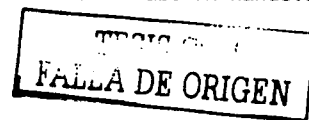
B.1.4.1.2 Control de Potencia

Las dos direcciones del enlace de radio entre el terminal y la BS están sujetas a ajustes de potencia continuas (cada 60 [ms]) en un margen de unos 26 [dB]. Este ajuste de potencia, tanto del transceptor de la BS como de la terminal se realizan bajo la supervisión del sistema de control de la BS. Esto mejora el aprovechamiento del espectro al limitar las interferencias dentro del sistema y ahorra batería.

B.1.4.1.3 Control de la Desviación en Tiempo

Como los terminales que se encuentran dentro de una misma célula se encuentran a distintas distancias de la BS (diferentes retardos de propagación), las ráfagas que ésta recibe tienen diferentes retardos. La dispersión en tiempo hace necesario un tiempo de guarda grande entre ráfagas, lo que da lugar a un bajo aprovechamiento del ancho de banda. Para minimizar este efecto en el interfaz aire, se hace un ajuste de tiempo en el terminal. Este ajuste cubre un margen de 233 [ms], que permite la corrección para células de un radio máximo de 35 Km.

La BS monitoriza la desviación en tiempo de cada terminal y lo utiliza como un criterio para realizar el *handover* y también para ayudarle a corregir su desviación antes de llevar a cabo un *handover* sincronizado.



B.1.4.1.4 Gestión de los Canales Radio

Las recomendaciones del GSM dejan una gran flexibilidad a la hora de definir una estrategia de asignación en tiempo real de canales comunes y dedicados. La petición de acceso procedente de un terminal por medio del canal de acceso aleatorio debe controlarse para evitar situaciones de bloqueo. Entre los medios disponibles, el más eficiente es el que usa el número de la Clase de Acceso. En la tarjeta SIM de cada abonado se almacena un número aleatorio del 1 al 10, si se produce una saturación, la BS puede restringir, a través del canal de difusión, el acceso a cualquier clase de abonados. Para abonados de alta prioridad (como servicios de seguridad o emergencia, personal de campo, etc...) se reservan números de clases especiales (del 11 al 15).

B.1.4.5 Gestión de la Seguridad

La autenticación se realiza pidiendo al terminal el resultado de un cálculo específico sobre un número aleatorio (RAND) que envía el sistema y comprobando después este resultado con el correcto. Este proceso de cálculo depende de hecho de una clave secreta (Ki) que es específica para cada tarjeta SIM de cada abonado. El cálculo se hace siguiendo un algoritmo de cifrado A3, que tiene la propiedad de que conociendo el resultado y una entrada (RAND), no puede deducirse prácticamente la otra entrada (Ki). La clave secreta (Ki) y el algoritmo A3 se almacenan, con protección, en la tarjeta SIM y en el HLR. El cifrado de la ráfaga de datos se logra con un segundo algoritmo de cifrado A5, que se aplica a una clave (Kc) que se escoge para cada conexión y aun número que cambia en cada ráfaga. La clave Kc se calcula en el terminal y en el HLR con un tercer algoritmo A8, similar al A3. Los algoritmos A3 y A8 no se especifican en las recomendaciones del GSM, sino que se dejan a la elección del operador.

Referencias.

➤ Capitulo 1

http://www.eveliux.com/fundatel/menu_telecom.html
<http://192.168.27.20/visita/clase5.doc>
<http://192.168.27.20/visita/clase6.doc>
<http://www.aniret.org.mx/pdf/articulos/qam.pdf>
<http://www.joseangelsanchezortiz.net/Archivos/ PresentaTelema/CodificaDatos>
http://www.uv.es/~montanan/redes/trabajos/LANs_inalambricas.doc
http://electronika2.tripod.com/info_files/modfase.htm

➤ Capitulo 2

<http://www.mobitex.org/networks/index.html>
<http://www.geocities.com/wm2001ar/CapituloIII.htm>
http://www.ericsson.com/network_operators/mobitex/about.shtml
http://www.ericsson.com/network_operators/mobitex/products.shtml
<http://atenea.udistrital.edu.co/egresados/xsepulveda/temas/tema1.html>
<http://atenea.udistrital.edu.co/egresados/xsepulveda/temas/tema2.html>
<http://www.comsoc.org/livepubs/surveys/public/3q99issue/salkintzis.html>
<http://www.comsoc.org/pubs/surveys> "Survey of Mobile Data Networks" Apostolis K. Salkintzis.

➤ Capitulo 3

Martin Johnsson, *HiperLAN/2 – The Broadband Radio Transmission Technology Operating in the 5 GHz Frequency Band*, HiperLAN/2 Global Forum, 1999
www.hiperlan2.com/presdocs/site/whitepaper.pdf

HiperLAN2 Global Forum - *Towards the WLAN Heaven - Can HiperLAN2 make it all through?*, presentado en CeBIT del 6 Abril 2001
<http://www.hiperlan2.com/presdocs/site/h2gf-pres-cebit-2001.ppt>

Fredrik Kristensen, Magnus Sandgren - *A system simulation of wireless local area networks operating in the 5 GHz band*, Master of Science Thesis de la empresa Telia Research AB, August 2001
www.hiperlan2.com/presdocs/site/rapporten039.doc

Wi-Lan, *Whitepaper – Wide-band Orthogonal Frequency Division Multiplexing*
http://www.wi-lan.com/library/whitepaper_wofdm_technical.pdf

<http://www.nd.edu/~mhaenggi/NET/wireless/hiperlan/Introduction.htm>
Vistazo general de la tecnología, y algunos recursos
<http://www.tml.hut.fi/Studies/Tik-110.300/1999/Essays/hiperlan2.html>
Trabajo de Janne Korhonen sobre HiperLAN2, de la Universidad de Helsinki

<http://www.eveliux.com/articulos/wlans.html>
<http://www.eveliux.com/articulos/estandareswlan.html>
<http://www.idg.es/comunicaciones/wireless/pdf/tec-stan-aplic04.pdf>

Referencias.

➤ Capitulo 4

<http://www.geocities.com/coaditel/DECT.htm>

http://www.phsmou.or.jp/documents/TECH_June2000.html
General Description of Public Personal Handy-phone System, Version: 01
Fecha: Abril 21, 1997.PHS MoU Classification: Unrestricted

<http://www.auladatos.movistar.com/Aula-de-Datos/Tutoriales-y-Documentacion/Introduccion-a-las-comunicaciones-moviles/3-Tipos-de-comunicaciones-moviles/#14>

➤ Capitulo 5

<http://bluetooth.ericsson.se/ebc/default.asp>
<http://www.mot.com/bluetooth/apps/index.html/>
<http://www.nokia.com/bluetooth/whatis.html/>
<http://www.gcr.tsc.upc.es/downloads%5Ccomm%5Cbluetooth.pdf>
<http://www.bluetooth.com/bluetoothguide/models/interactive.asp>
<http://www.bluetooth.com/bluetoothguide/models/internet.asp>
<http://www.bluetooth.com/bluetoothguide/models/models.asp>
http://www.bluetooth.com/bluetoothguide/models/two_in_one.asp
<http://bluetooth.ericsson.se/ebc/default.asp>
<http://www.gsmdata.com/artblue.htm>
<http://www.mot.com/bluetooth/apps/index.html>
<http://www.option.com/techno/bluetooth01.htm>
<http://www.palowireless.com/homerf/homerf1.asp>
<http://www.palowireless.com/homerf/homerf2.asp>
<http://www.palowireless.com/homerf/homerf3.asp>
<http://www.palowireless.com/homerf/homerf4.asp>
<http://www.palowireless.com/homerf/homerf5.asp>
<http://www.palowireless.com/homerf/homerf6.asp>
<http://www.palowireless.com/homerf/homerf7.asp>
<http://www.redes.upv.es/irc/trabajos/Pablol.pdf>
<http://www.magisnetworks.com/air5/>
http://www.securitytechnet.com/resource/hot-topic/homenet/IEEE_0902.pdf
http://www.magisnetworks.com/pdf/white_papers/M14077WalkThrough1stFloor.pdf
http://www.magisnetworks.com/pdf/white_papers/home_network_security.pdf
<http://lucas.linux.org.mx/Manuales-LuCAS/INTERCONEXION-IRDA/Interconexion-IRDA.pdf>

➤ Capitulo 6

BRAUNL, T.: "*Eyebot Documentation*",
<http://www.ee.uwa.edu.au/braunl/eyebot>, 2002.

CHAPARRO, D., RODRIGUEZ, R., PELEGRÍN, J.: "*Encaminamiento Ad-Hoc*",
<http://pantuflo.escet.urjc.es/ir-1-2/crpl>, 2002.

PERKINS, C. E., BELDING-ROYER, E. M., DAS S. R.: "*Mobile Ad Hoc Networking Working Group - Internet Draft*", <http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-11.txt>, 2002.

PERKINS, C. E., BHAGWAT, P.: "*Highly Dynamic Destination-Sequenced Distance-Vector Routign (DSDV) for Mobile Computers*", *Comp. Commun.*, 1994.

<http://gsyc.escet.urjc.es/~caguero/proyectos/pera/node2.html>
<http://www.ietf.org/html.charters/manet-charter.html>

Referencias.

http://www.ee.surrey.ac.uk/Personal/G.Aggelou/MANET_PUBLICATIONS.html
http://profesores.elo.utfsm.cl/~agv/ipd438/2s02/indepthStudy/bravo/informe_avance_1.pdf
<http://gsyc.escet.urjc.es/~caguero/proyectos/pera/node10.html>
<http://www.redes.upv.es/rm/transpas/t3a.pdf>

➤ Capitulo 7

Arnold, Wollrath, et al. *The Jini Specification*. Reading, MA, USA: Addison-Wesley, 1999.

Chen, Harry. "Developing a Dynamic Distributed Intelligent Agent Framework Based on the Jini Architecture." Master's thesis, University of Maryland Baltimore County, January 2000.

Chen, Harry. Jini Prolog Engine Service (JPES). <http://qentoo.cs.umbc.edu/ipes/>.

Chen, Harry. Ronin Agent Framework. <http://qentoo.cs.umbc.edu/ronin/>.

Rekesh, John. "UPnP, Jini and Salutation - A look at some popular coordination framework for future network devices." Technical Report, California Software Lab, 1999.
<http://www.cswl.com/whitepapr/tech/upnp.html>.

The Salutation Consortium Inc. Salutation Architecture Specification (Part 1), version 2.1 edition, 1999.

SLP White Paper http://playground.sun.com/srvloc/sip_white_paper.html.

Understanding E-Service: Chapter 2 of the Internet
<http://www.hp.com/e-services/understanding/chapter2/>.

University Plug and Play Device Architecture Reference Specification. Microsoft Corporation.
<http://www.acm.org/crossroads/espanol/xrds7-2/service.html>

➤ Capitulo 8

www.ca.com.mx
www.comactive.com.mx
www.enterasys.com
www.smc.com
www.yankeegroup.com
www.avaya.com/ac/common/index.jhtml
http://www.bluetake.com.mx/productos_bluetooth.htm
<http://www.axis.com.mx/precios.htm>
http://www.prodigy.com.mx/int/prod_prodigy_infi_inai.html#4
<http://www.prodigymovil.com.mx>
http://www.netmedia.info/business/articulos.php?id_sec=23&id_art=4284
<http://www.online.com.mx/movil/index.html>
www.3com.com/prod/es_LA_AMER/prodlist.jsp?tab=cat&cat=13&subcat=89

Artículos publicados en la IEEE

- IEEE Communications Surveys • <http://www.comsoc.org/pubs/surveys> • Fourth Quarter 1998 • Vol. 1 No. 1
- Dahlman, Gudmundson, Nilsson, Sköld
"UMTS/IMT-2000 Based on Wideband CDMA"
Septiembre, 1998
- Dinan, Jabbari
"Spreading Codes for Direct Sequence CDMA and Wideband CDMA Cellular Networks"
Septiembre, 1998
- J. E. Padgett, G. Günther, T. Hattori "Overview of Wireless Personal Communications"
Enero 1995
- Sklar "Rayleigh Fading Channels in Mobile Digital Communications System"
Septiembre, 1997 IEEE Signal Processing Magazine
- Flikkema "Spread Spectrum Techniques for Wireless Communication"
Mayo, 1997.
- DUBE, R.: "*Signal Stability based Adaptive Routing (SSA) for Ad-Hoc Mobile Networks*",
IEEE Pers. Commun., 1997.
- DAS, S. R., PERKINS, C. E., ROYER, E. M., MARINA, M. K.: "*Performance Comparison of Two On-demand Routing Protocols for Ad hoc Networks.*" IEEE Personal Communications Magazine special issue on Ad hoc Networking, 2001.
- Elizabeth Royer and C-K Toh "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pp. 46-55.
- Satyanarayanan, M. "Pervasive computing: vision and challenges"
Personal Communications, IEEE Volume: 8, Issue: 4, Year: Aug 2001

Páginas de organizaciones

- <http://portal.etsi.org/bran/hta/Hiperlan/hiperlan2.asp>
Página de la ETSI dedicada al estándar HiperLAN2. Se pueden descargar las especificaciones y los protocolos gratuitamente (previo "login").
- <http://www.hiperlan2.com>
HiperLAN2 Global Forum, foro dedicado a la extensión y divulgación de HiperLAN. Agrupa a múltiples empresas interesadas en dar un impulso a esta tecnología.
- <http://www.ofdm-forum.com>
Foro OFDM, dedicado a la divulgación de esta tecnología de transmisión inalámbrica
- <http://www.ero.dk>
European Radiocommunications Office (ERO), organismo europeo encargado de armonizar el uso del espectro de radiofrecuencia de los países de la Unión Europea
- <http://www.wi-lan.com/technology/main1.html>
Wi-Lan vende tecnología relacionada con OFDM, y tiene un par de artículos al respecto
- <http://standards.ieee.org/wireless/>
IEEE Wireless Standards Zone
- <http://www.hiperlan2.com/>
Hiperlan2 Global Forum
- <http://www.atheros.com/>
Atheros Communications
- <http://www.bluetooth.com/>
Bluetooth White Paper.
<http://www.bluetooth.com/developer/whitepaper/whitepaper.asp>
- www.avaya.com
- www.cisco.com/mx/
- www.nortelnetworks.com
- www.proxim.com
- www.cisco.com/en/US/products/hw/wireless/index.html