TESIS
IJ2002
M6
v.1

# UNIVERSIDAD CATOLICA ANDRES BELLO

## FACULTAD DE INGENIERIA

## ESCUELA DE INGENIERIA EN INFORMÁTICA

MODELO DE PUNTO DE ACCESO A REDES LAN (LAN *ACCESS POINT*)

PARA DISPOSITIVOS BLUETOOTH

**Este Jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: 20**

J U R A D O  E X A M I N A D O R

| | | |
|---|---|---|
| Firma: | Firma: | Firma: |
| Nombre: ROBERT KOENEKE | Nombre: MARIA ELENA VILLAPOL | Nombre: Wilmer Pereira |

| | |
|---|---|
| REALIZADO POR | Guillermo J. Morales Sánchez<br>Gerardo J. Rodríguez Rangel |
| PROFESOR GUIA | Dr. Wilmer E. Pereira |
| FECHA | Caracas, Octubre de 2002 |

# INDICE GENERAL

AGRADECIMIENTOS ii
DEDICATORIAS iii
INDICE GENERAL iv
INDICE DE TABLAS vii
INDICE GRAFICOS viii
RESUMEN ix
INTRODUCCION 10
PLANTEAMIENTO DEL PROBLEMA 12
OBJETIVO GENERAL. 14
OBJETIVOS ESPECIFICOS. 14
LIMITACIONES Y ALCANCES 15
JUSTIFICACION 16
CAPITULO I 20
BLUETOOTH 20
1 *Bluetooth* y el Modelo de Interconexión de Sistemas Abiertos (OSI) 21
2 Radio Frecuencia 25
2.1 Espectro Extendido 26
3 Gestor de Enlaces (LM) 27
4 Controlador de Enlaces (LC) 27
4.1 Topología de Red 29
4.2 *Slots* Temporales (*Time Slots*) 30
4.3 Tipos de Enlace. 31
4.4 Estados y modos *Bluetooth* 32
4.4.1 Estado En Espera (*Standby*) 32
4.4.2 Estado Conexión (*Connection*) 33
4.4.1.1 Sub-estado de Indagación (*Inquiry*) 33
4.4.1.2 Sub-estados de Búsqueda (*Paging*) 35
4.4.2.1 Modos de Conexión 36
5 Protocolo de gestión de enlace (LMP) 38
6 Interfaz del Controlador de host (HCI) 39
7 Protocolo de control de enlace lógico y del nivel de adaptación (L2CAP) 41
8 Protocolo para descubrir servicios (SDP) 43
9 RFCOMM 46
10 Protocolos Adoptados. 48
11 Tecnología Inalámbrica 48
11.1 *Bluetooth* e Infrarrojo 49
11.2 *Bluetooth* y *HomeRF* 51
11.3 Redes inalámbricas y *Bluetooth*. 53

11.4 Limitaciones de *Bluetooth* 56
CAPITULO II 58
METODOLOGIA 58
1 Investigación de tecnología 59
2 Estudio de Componentes 60
3 Diseño del Modelo 60
4 Codificación 60
5 Pruebas 60
CAPITULO III 61
DESARROLLO Y RESULTADOS 61
1 Investigación de Tecnología 61
2 Estudio de componentes 62
3 Diseño del Modelo 63
3.1 Descripción General del Punto de Acceso 63
3.1.1 Pila del Protocolo. 64
3.1.2 Configuraciones y Roles 65
3.1.3 Requerimientos de Usuario y Escenarios 66
3.1.4 Características básicas del Punto de Acceso 67
3.2 Aspectos de la Interfase con el Usuario 68
3.2.1 Seguridad 68
3.2.2 Modos Genéricos 71
3.2.3 Parámetros Adicionales 72
3.3 Capa de Aplicación 73
3.1 Inicialización del Servicio de Punto de Acceso a una LAN 73
3.3.2 Finalización del Servicio de Punto de Acceso a una LAN 74
3.3.3 Establecimiento de la Conexión a la LAN 74
3.3.4 Desconexión de la LAN 76
3.4 PPP 76
3.4.1 Inicialización del PPP 77
3.4.2 Finalización del PPP 77
3.4.3 Establecimiento de la Conexión PPP 78
3.4.4 Desconexión del PPP 78
3.4.5 Protocolos de Autentificación PPP 80
3.5 RFCOMM 80
3.6 Servicio de Descubrimiento 81
3.6.1 Registros del servicio de SDP 81
3.7 L2CAP 83
3.8 Gestor de Enlace (LM) 83
3.8.1 Manejo de errores 84
3.9 Control de Enlace 85

3.10 Procedimientos de la Entidad de Administración 85
3.10.1 Establecimiento del enlace 86
3.10.2 Máximo número de usuarios 87
3.11 Recomendaciones adicionales 88
4 Codificación 88
4.1 Servidor BlueLAP: 89
4.2 Cliente BlueLAP 89
4.3 Herramienta de configuración y administración 90
5 Pruebas. 91
5.1 Reconocimiento de los equipos *Bluetooth*. 91
5.2 Establecimiento del enlace inalámbrico 93
5.3 Inicialización del Punto de Acceso 95
CONCLUSIONES 104
RECOMENDACIONES 106
REFERENCIAS 107
APENDICES Tomo II
ANEXOS Tomo II

# INDICE DE TABLAS

Tabla 1 23
Capas de la pila de protocolo Bluetooth 23
Tabla 2 51
Ventajas y Desventajas de la tecnología infrarrojo 51
Tabla 3 53
Ventajas y desventajas de la tecnología HomeRF 53
Tabla 4 55
Ventajas y desventaja de la tecnología 802.11 55
Tabla 5 57
Comparación entre tecnologías inalámbricas. 57
Tabla 6 71
Tabla de requerimientos de los modos genéricos 71
Tabla 7 73
Tabla de requerimientos de la capa de aplicación 73
Tabla 8 76
Capacidades del PPP 76
Tabla 9 82
Parámetros Servicio de Descubrimiento 82
Tabla 10 84
Procedimientos LMP 84
Tabla 11 86
Procedimientos de la Entidad de Administración. 86
Tabla 12 92
Características Dispositivos Bluetooth 92
Tabla 13 93
Establecimiento de una conexión HCI. 93
Tabla 14 94
Establecimiento de una conexión L2CAP. 94
Tabla 15 95
Establecimiento de una conexión RFCOMM. 95
Tabla 16 99
Verificación de conexiones PPP e Interfases IP. 99
Tabla 17 100
Pruebas de conexión. 100

# INDICE GRAFICOS

Figura 1 Modelo OSI. 22
Figura 2 Unidades funcionales en el sistema Bluetooth. 28
Figura 3 Piconets (a)Un esclavo, (b) multi-esclavos, (c) scatternet. 29
Figura 4 Transmisión de paquetes durante los slots temporales. 31
Figura 6 Ubicación del nivel LMP en el escenario global. 38
Figura 7 Interfaz HCI. 40
Figura 8 L2CAP dentro de los diferentes niveles de Bluetooth. 41
Figura 9 Papel de L2CAP en la pila de protocolos Bluetooth 42
Figura 10 Interacción cliente-servidor. 44
Figura 11 Segmento de comunicación RFCOMM. 46
Figura 12 Estructura de Trabajo. 59
Figura 13 Pila de Protocolo. 64
Figura 14 Acceso a la LAN desde un solo terminal Bluetooth. 66
Figura 15 Acceso a la LAN desde múltiples terminales Bluetooth. 67
Figura 16 Arquitectura de seguridad para los escenarios DT-LAP. 70
Figura 16 DT utilizando la conexión del LAP. 101
Figura 17 Resumen de datos recolectados. 102
Figura 18 Cantidad de datos transmitidos en una unidad de tiempo. 102

# UNIVERSIDAD CATOLICA ANDRES BELLO
# FACULTA DE INGENIERIA
# ESCUELA DE INGENIERIA INFORMATICA

## MODELO DE PUNTO DE ACCESO A REDES LAN (LAN ACCESS POINT) PARA DISPOSITIVOS BLUETOOTH

**Trabajo Especial de Grado**

Autores: Guillermo Morales S.
Gerardo Rodríguez R.
Tutor: Dr. Wilmer Pereira G.
Fecha: Octubre, 2002

## RESUMEN

El presente Trabajo Especial de Grado, es realizado en la Universidad Católica Andrés Bello, sede Caracas, específicamente la Escuela de Ingeniería Informática. El cual tiene como objetivo la creación de un *Modelo de Punto de Acceso a Redes LAN (LAN Access Point LAP) para dispositivos Bluetooth* y un prototipo de los componentes de software basado en el modelo.

Se presenta un estudio de diferentes tecnologías de comunicación inalámbrica como lo son 802.11, *HomeRF,* Infrarrojo; se compararon con la tecnología inalámbrica *Bluetooth*, para observar sus ventajas y desventajas y así determinar si son capaces de complementarse unas a las otras, en diferentes ambientes de trabajo.

Se desarrolla un prototipo, que tiene por nombre **BlueLAP,** que funciona bajo el ambiente *Linux*, debido a las características de la pila de protocolos utilizadas, pero que puede ser accedido por cualquier dispositivo *Bluetooth* con las especificaciones adecuadas. Con este prototipo los terminales *Bluetooth* acceden a través de los servicios que provee el LAP a los diferentes recursos de la red cableada a la que se encuentre conectado el LAP

# INTRODUCCION

En la actualidad las LAN inalámbricas han ocupado un lugar importante en el mercado de las redes de área local. Las organizaciones se han dado cuenta de que las LAN inalámbricas son un complemento a las redes cableadas, para satisfacer necesidades de movilidad, traslado, redes *ad hoc* (Ver apéndice E) y cobertura de lugares difíciles de cablear.

La tecnología inalámbrica *Bluetooth* se ha convertido en una especificación global de carácter tecnológico para el establecimiento de comunicaciones inalámbricas entre dispositivos portátiles, periféricos, computadoras, etc. Esta tecnología también puede utilizarse para realizar conexiones inalámbricas y transmitir datos a redes de área local convencionales, a través de un punto de acceso, equipado con un dispositivo *Bluetooth* y conectado a la LAN.

Esto último es el objetivo del Trabajo Especial de Grado, crear un *Modelo de un Punto de Acceso a Redes LAN (LAN Access Point LAP) para dispositivos Bluetooth,* para poder cubrir las necesidades de los usuarios con los requerimientos antes planteados

Se plantean los objetivos, alcances y limitaciones del trabajo, que darán una amplia visión de los lineamientos a seguir durante la realización del mismo. El Capítulo I contiene una breve explicación del nacimiento de *Bluetooth*, así como también los conceptos y la arquitectura de los protocolos necesarios para poder

desarrollar el LAP, y finalizando con una comparación entre las diversas tecnologías existentes: 802.11, *HomeRF,* IrDA. En Capítulo II, esta enfocado a la metodología utilizada, así como también una breve descripción de las etapas involucradas en el proyecto. En el Capítulo III, se describe toda la arquitectura, características y requerimientos que debe poseer el modelo de un punto de acceso a redes LAN para dispositivos *Bluetooth*, siguiendo con los estándares utilizados por esta tecnología, y también se presentan los resultados obtenidos con la realización de este trabajo.

Y posteriormente el informe consta de las Conclusiones y Recomendaciones. Y una serie de apéndices que complementan la información de los capítulos.

# PLANTEAMIENTO DEL PROBLEMA

El acceso a la información ha tenido varias etapas, una de las más importantes fue la masificación del computador entre las personas; el que cualquier individuo con o sin conocimientos profundos de informática pudiera utilizar en casa o en la oficina un computador para realizar sus tareas y obtener mayor provecho con ello. Luego vino la comunicación, el acceso a las redes públicas por medio de los computadores, permitió el intercambio de información y con la generalización de la Internet se logró romper las barreras de la distancia para el intercambio de la información, aunado a esto la popularización de la telefonía celular permite la comunicación entre las personas en cualquier lugar y en cualquier momento. Ahora el reto es lograr que dispositivos móviles como: teléfonos móviles, PDAs, computadores portátiles, etc… permitan el acceso a toda la información ya disponible en las redes cableadas.

La tecnología *Bluetooth* creada e impulsada por un grupo de empresas líderes en telefonía móvil y computación, permite ofrecer una solución a esas necesidades de movilidad. El chip *Bluetooth* está disponible desde el año 1999, actualmente se encuentra instalado en una variedad de dispositivos como: teléfonos celulares, agendas electrónicas, PDAs, PCs, etc. Es una tecnología barata y muy poderosa, con posibilidad de acceso a redes LAN que incluyan un dispositivo *Bluetooth* desde un

punto de acceso. Por ejemplo todos los usuarios que posean el chip en un dispositivo al entrar a una LAN que pueda proveer servicio (*Bluetooth*), podrán hacer uso de Internet, servicio de mensajería, etc. Estas áreas pueden estar en la casa, lugares públicos, oficinas, etc.[1]

Este Trabajo Especial de Grado plantea el estudio de un modelo para un Punto de Acceso a Redes LAN (*LAN Access Point*) para dispositivos *Bluetooth*, que en la actualidad se encuentra en investigación y desarrollo por parte de empresas y organizaciones de todo el mundo, dado que es una necesidad poder acceder a la información y recursos que se encuentran en las redes cableadas, desde dispositivos móviles. Ej. Un estudiante trabajando en su computador portátil desde cualquier parte del *campus* universitario podría mandar a imprimir un documento y pasar recogiéndolo luego en el lugar indicado; ó el empleado que llega a su oficina e inmediatamente al entrar al área de cobertura *Bluetooth* podría tener acceso desde su PDA o su teléfono celular a la información de su Intranet desde cualquier parte de la oficina.

[1] IP Services Over Bluetooth, 1999, p. 1

## OBJETIVO GENERAL.

Desarrollar un modelo para un Punto de Acceso a Redes LAN (*LAN Access Point*) para dispositivos *Bluetooth*.

## OBJETIVOS ESPECIFICOS.

- Investigar y estudiar diferentes tecnologías de redes y comunicación:
  - Tecnología *Bluetooth*.
  - Redes LAN.
  - Protocolos de comunicación (TCP/IP, PPP etc.).
  - Transmisión inalámbrica de datos.
  - Estándares para redes (modelo OSI, IP)
- Investigar, estudiar y plantear los componentes de software necesarios para el modelo de Punto de Acceso a Redes LAN (*LAN Access Point*) para dispositivos *Bluetooth*.
- Elaborar un prototipo de los componentes de software basado en el modelo generado para un Punto de Acceso a Redes LAN para dispositivos *Bluetooth*.

## LIMITACIONES Y ALCANCES

Producto de los objetivos, los alcances de este trabajo se pueden resumir en los siguientes puntos:

- Documentación detallada sobre la tecnología *Bluetooth*; así como también investigación sobre redes LAN, protocolos de comunicación, transmisión inalámbrica de datos, estándares de redes y cualquier tecnología relacionada y necesaria para la realización del objetivo general y del documento final de trabajo .
- Análisis y evaluación de un modelo de Punto de Acceso a Redes LAN (*LAN Access Point*) para dispositivos *Bluetooth*, así como servicios recomendados que debería disponer el Punto de Acceso.
- Diseño de componentes de software, definición de infraestructura tecnológica y prototipo de los componentes de software diseñados.

Las limitaciones a tener en cuenta en el desarrollo de este trabajo especial de grado son:

- El modelo de Punto de Acceso a Redes LAN será diseñado e implementado para los dispositivos con que se cuenten en el laboratorio dispuesto para la realización de este trabajo especial de grado.
- Al no disponer de una gran cantidad de dispositivos terminales no se podrán realizar pruebas que abarquen la gran variedad de dispositivos disponibles para esta tecnología[2].

Durante la realización del Trabajo Especial de Grado surgieron otras limitaciones, como son:

- El dispositivo *Tool Kit* no soportaba ciertas funcionalidades, como por ejemplo el *Clock_offset,* que por lo tanto impedían realizar ciertas operaciones.
- No poseer en un 100 % la disponibilidad de los dispositivos, dado que otro grupo de investigación los necesitaba.

[2] En el mes de Noviembre de 2001 se realizo la entrega de dos dispositivos *Bluetooth,* uno de ellos *the Bluetooth Development Kit* y el otro *Bluetooth Aplication Tool Kit*, por parte de la empresa ERICSSON

# JUSTIFICACION

Un terminal habilitado con *Bluetooth* por si solo no tiene casi ninguna utilidad práctica, al tener una serie de dispositivos *Bluetooth* que se pueden comunicar entre si ya se obtiene cierta interoperabilidad, pero si no se puede acceder desde uno de estos dispositivos a los servicios de los que se disponen en una red se desperdicia una gran capacidad de utilización, es por esto que uno de los elementos principales a los que se debe tener acceso es a una LAN cableada y esto se logra a través de un Punto de Acceso a Redes LAN (*LAN Point Access*), donde los terminales *Bluetooth* puedan acceder a los servicios que les sean habilitados.

Estudios sobre la tecnología indican que existen una variada cantidad de aplicaciones para usuarios ó trabajo en redes con la tecnología *Bluetooth* (Albrecht, Frank y Martini, 1999)

**(1) "Escritorio sin Cables"**: Este modelo de uso de *Bluetooth* provee una manera fácil de conectar todos los periféricos del PC de escritorio sin la necesidad de usar cables para evitar el efecto "espagueti".

**(2) "El Puente a la Internet"**: Este modelo de uso de *Bluetooth* ofrece un puente entre dispositivos portátiles y una red pública (PSTN, ISDN, GSM, xDSL, LAN, etc…) vía un punto de acceso o *gateway*. Ejemplo: un teléfono celular puede ser el *gateway* entre el dispositivo *Bluetooth* y la red de telefonía celular para acceder a la Internet o a la red de telefonía.

**(3) "El Teléfono Tres-en-uno"**: Un teléfono móvil con tecnología *Bluetooth* puede funcionar en tres modos: (1) en casa trabaja como un teléfono inalámbrico conectado

a la red de telefonía publica, (2) en el trabajo funciona como un intercomunicador, (3) en cualquier otro lugar como un teléfono celular.

**(4) "Transferencia de archivos":** Muchos tipos de información pueden ser intercambiadas entre dispositivos. La información que puede ser intercambiada abarca desde pequeños objetos (como vCards entre PDAs) hasta grandes archivos entre computadores.

**(5) "Sincronización":** La sincronización es la habilidad de intercambiar y sincronizar información entre dispositivos que manejen datos de información de administración personal, entre los que se incluyen libretas telefónicas, calendarios e información de actividades.

**(6) "Acceso LAN":** Similar al puente Internet, el acceso LAN está basado en el uso de un dispositivo que actúa como un Punto de Acceso LAN (LAP) proveyendo servicios de acceso *Bluetooth* a uno o más terminales.

También Albrecht y otros mencionan los escenarios para el uso de *Bluetooth,* que pueden categorizarce de la siguiente manera:

- **Ambiente de uso en la oficina**: La tecnología y los dispositivos *Bluetooth* son usados para ayudar en servicios de comunicación y redes profesionales, Ej. Como puente entre dispositivos portátiles y un sofisticado (posiblemente cableado) *backbone* de servicios y equipos adicionales.

- **Ambiente de uso en casa**: La tecnología *Bluetooth* es usada para conectar una variedad de dispositivos diferentes sin el uso de cables, Ej. Escritorio sin cables, teléfono inalámbrico, control remoto, etc.…

- **Ambiente de uso público**: *Bluetooth* habilita a dispositivos como PDAs (*Personal Digital Assistant*) a establecer acceso a la información y los servicios en áreas públicas (Ej. Aeropuertos, Museos, Universidades, Edificios, etc.).

- **Localidades de uso independiente:** Agregadas a redes de trabajo, permite conectar dispositivos independientemente que estén fuera del área de cobertura de cualquier tipo de combinación de equipos redes.

Al ver esta cantidad de escenarios y modelos de uso, se puede deducir que la tendencia hacia la incorporación de estas tecnologías en la vida cotidiana es una necesidad, se requiere obtener y compartir información rápidamente desde cualquier punto y con cualquier dispositivo, además se necesita poder obtener recursos de las redes cableadas que ofrecen un sin fin de posibilidades. Es por esto que muchas compañías y organizaciones están investigando y desarrollando estas tecnologías.

El Punto de Acceso a Redes LAN, es el responsable de realizar la interacción entre todos los dispositivos *Bluetooth* que poseen los usuarios y las redes LAN, es decir, gracias a la realización de este modelo se podrá cubrir las necesidades actuales de información y comunicación en cualquier lugar y en cualquier momento, con tan sólo entrar en un área de servicio donde esté instalado el **Punto de Acceso a Redes LAN (*LAN Access Point*) para dispositivos *Bluetooth*.**

# CAPITULO I

# BLUETOOTH

La tecnología de transmisión de Radio Frecuencia (RF) no había sido implementada a grandes escalas, en redes inalámbricas para transmisión de datos entre dispositivos móviles, hasta hace poco tiempo, dado que las velocidades de transmisión no eran las adecuadas, problemas de seguridad y necesidades de licencia, la hacían menos competitiva en comparación con la tecnología Infrarrojo (IrDA)[3] que tiene menos tiempo pero con bastantes aplicaciones.

Por esta razón, diversos organismos internacionales se están encargando de regular los distintos espectros de frecuencias, para que aparatos iguales utilicen los mismos rangos y empleen tecnologías que les permitan trabajar de manera conjunta.

Una de las principales características de RF, es la posibilidad de transmitir a mayor distancia, pese a la existencia de obstáculos entre el emisor y el receptor. En la actualidad existen muchos dispositivos periféricos, como el ratón, el teclado, entre otros, que utilizan este tipo de transmisión, para la comunicación entre dispositivos. También existe la posibilidad de conectar cualquier máquina como: PDAs, computadoras, televisores, etc.

[3] Siglas en inglés: "Infra-red Data Asociation (IrDA)"

Para lograr evitar los problemas mencionados; con el objetivo de facilitar la conexión de todo tipo de periféricos entre sí, era necesaria la creación de un estándar global. Con la aparición de *Bluetooth* se logra tener dicho estándar.

La tecnología inalámbrica *Bluetooth*, es una especificación diseñada para permitir la comunicación "sin cables"[4] entre dispositivos móviles pequeños.

¿Por qué este nombre? La razón es que en el siglo X el rey vikingo Harald II de Dinamarca, apodado Blåtand o "diente azul" (*Bluetooth*) a causa de una enfermedad que le daba esta coloración a su dentadura, reunificó bajo su reinado numerosos pequeños reinos escandinavos, que funcionaban con reglas distintas, análogo a lo que hace la tecnología *Bluetooth*, promovida por Ericsson (Suecia) y Nokia (Finlandia), dos países escandinavos. Empresas como 3Com, Intel, IBM, Lucent, Microsoft, Motorola, Nokia o Toshiba se unieron junto a la pionera Ericsson, para formar el Grupo de Interés Especial (SIG)[5], al que actualmente ya pertenecen más de 1.600 empresas.

## 1 *Bluetooth* y el Modelo de Interconexión de Sistemas Abiertos (OSI)[6]

El modelo OSI, fue desarrollado por la Organización Internacional de Estandarización (ISO)[7] como una arquitectura para comunicaciones entre computadoras, con el objetivo de ser el marco de referencia en el desarrollo de protocolos estándares. OSI posee siete capas, como se observa en la siguiente figura:

[4] Original en inglés :"Wireless"
[5] Siglas en inglés: "Bluetooth Special Interest Group (SIG)"
[6] Siglas en ingles: "Open Systems Interconnection (OSI)"
[7] Siglas en ingles: "International Organization for Standardization (ISO) "

**(a) Capa Física**: se ocupa de la transmisión de los *bits* por el canal de comunicación; esta relacionada con las característica mecánicas, eléctricas, funcionales y de los procedimientos para acceder al medio físico.

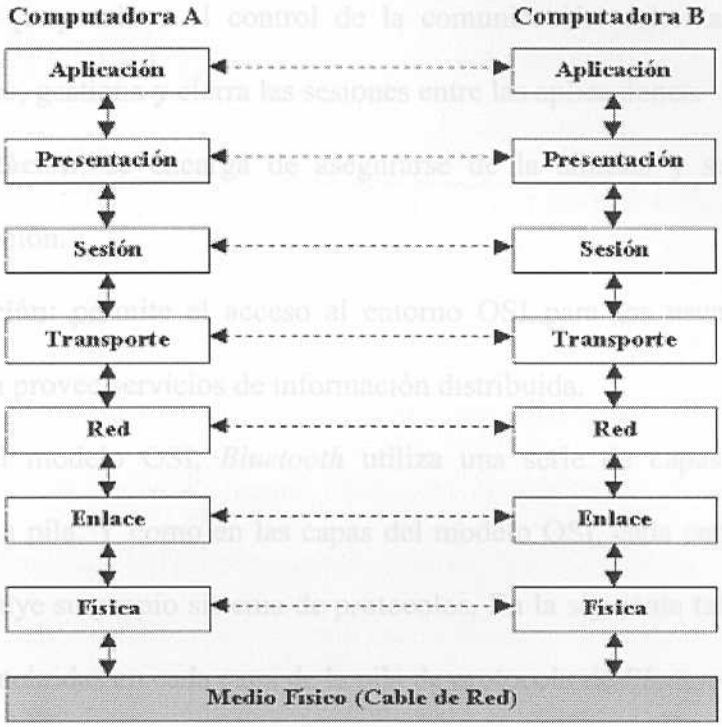


**Figura 1 Modelo OSI.** Tomado de Puigdemunt, Eduard. 2002. *Modelo OSI*. Disponible: http://www.pchardware.org/redes/redes_osi.php [Consulta: 2001, Noviembre 20]

**(b) Enlace de datos**: proporciona un servicio de transferencia de datos seguro a través del enlace físico; envía bloques de datos (tramas) realizando la sincronización, control de flujo y control de errores.

**(c) Red**: proporciona independencia a los niveles superiores con respecto a las técnicas de conmutación y de transmisión utilizadas para conectar los sistemas; se encarga de establecer, mantener y cerrar las conexiones.

**(d) Transporte**: proporciona seguridad, transferencia de datos transparente, entre los puntos finales; además proporciona procedimientos de recuperación de errores y control de flujo del origen al destino.

**(e) Sesión**: proporciona el control de la comunicación entre las aplicaciones, establece, gestiona y cierra las sesiones entre las aplicaciones.

**(f) Presentación**: se encarga de asegurarse de la síntesis y semántica de la información.

**(g) Aplicación**: permite el acceso al entorno OSI para los usuarios, así como también provee servicios de información distribuida.

Como en el modelo OSI, *Bluetooth* utiliza una serie de capas que son los protocolos de la pila. Y como en las capas del modelo OSI, cada capa de la pila de *Bluetooth* incluye su propio sistema de protocolos. En la siguiente tabla, esta la lista de protocolos incluidas en cada capa de la pila de protocolo de *Bluetooth*.

**Tabla 1**
**Capas de la pila de protocolo *Bluetooth*.**

| ***Capa del Protocolo*** | ***Protocolos*** |
|---|---|
| a. Base | a. Banda base.<br>b. Protocolo de Gestión de Enlace (LMP).<br>c. Protocolo de Control de Enlace lógico y del nivel de Adaptación. (L2CAP).<br>d. Protocolo para Descubrir Servicios (SDP). |
| b. Reemplazo del cable. | Comunicación de Radio Frecuencia (RFCOMM). |
| c. Protocolos Adoptados.(Ver Apéndice D) | a. Comunicación Móvil Infrarroja.<br>b. Protocolo de intercambio de |

| | |
|---|---|
| | Objetos.<br>c. Protocolo Punto a Punto.<br>d. Protocolo de datagrama de usuario, Protocolo de control de transmisión. Protocolo de Internet.<br>e. Ambiente para aplicaciones inalámbricas.<br>f. Protocolo para aplicaciones inalámbricas. |

Nota: Datos tomados de "*Bluetooth End to End*" (pág 150-151) por D.M Bakker y Diane Gilster, 2002, New York.

Como con el modelo OSI, significa que las capas que usa la pila de protocolo de *Bluetooth*, promueve la interoperabilidad entre las aplicaciones y el desarrollo de dispositivos con las especificaciones *Bluetooth*. No todos los dispositivos, ni las aplicaciones usan todos los protocolos que están en la pila; algunas usan partes de la pila, para cubrir un servicio necesario para una aplicación en específica.

**(a) Capa Base:** el protocolo de la capa base, provee las funciones básicas de *Bluetooth*, para la conexión de dispositivos *Bluetooth* en una *piconet*[8].

**(b) Capa de reemplazo de cable:** es una aplicación orientada a la capa del protocolo, que permite la creación de un puerto serial virtual en los dispositivos *Bluetooth*.

**(c) Protocolos adoptados:** la pila *Bluetooth* adopta muchos de los protocolos existentes, que se usan en otras comunicaciones, o en plataformas, o en tecnologías de red. *Bluetooth* incluye a estos protocolos existentes permitiendo la interoperabilidad con las aplicaciones heredadas.

[8] Ver concepto de *Piconet* en este mismo capítulo página 26.

Los protocolos que están en la capa base, reemplazo de cable, y algunos adoptados, de la pila de protocolos *Bluetooth* se encuentran explicados más adelante en este mismo capítulo.

## 2 Radio Frecuencia

El principio en que se basa la técnica de radio frecuencia es el de ondas electromagnéticas. Los campos eléctricos y magnéticos, generados por la aceleración de las cargas eléctricas, son variables en el tiempo. Dos de sus principales características son: el periodo y la amplitud.

*Bluetooth* trabaja en un espectro de radio, en la banda sin licenciar industrial, científica y medica (ISM)[9], con un rango que oscila entre los 2.4 GHz y 2.4835 GHz, pudiendo cambiar la señal hasta 1.600 veces por segundo sobre 79 canales distintos con intervalos de 1 MHz, a esta banda se le denomina "*completa*", ya que existe otra banda llamada "*reducida*", que posee las mismas características y la diferencia es que trabaja sólo en 23 canales, por ejemplo esta banda es utilizada en Francia y tiene un rango que va desde 2.4465 GHz hasta 2.4835 GHz.

La potencia de emisión se encuentra alrededor de 1 mW (0 dBm), lo que permite un radio de acción de 10 metros para los dispositivos, aunque se puede ampliar el radio de cobertura hasta los 100 metros, con la ayuda de amplificadores de 100 mW (20 dBm) de potencia. Al generar la señal se utiliza la técnica: Espectro Extendido[10].

[9] Siglas en ingles: "unlicensed Industrial, Scientific, and Medical "
[10] Original en ingles: "Spread Spectrum"

## 2.1 Espectro Extendido

Los dispositivos *Bluetooth*, envían señales de un nivel muy débil, para poder evitar la interferencia con otros sistemas. Estas señales que son enviadas a 1 milliwatt, comparado con los 3 watt o menos, que es la fuerza con que son enviadas las señales de los teléfonos celulares, es una de la causas por las cuales los dispositivos *Bluetooth* tienen un rango de acción de 10 metros. La transmisión de los dispositivos *Bluetooth* es mucho mejor, que la señal de radio, recibida desde una estación de radio local. Sin embargo la señal *Bluetooth* es transmitida en diferente frecuencia y amplitud.

Para evitar en un futuro, que la interferencia venga de otros dispositivos que compartan el mismo rango de frecuencia, como podría ser otro dispositivo *Bluetooth* transmitiendo y recibiendo, dentro del mismo rango, es por ello que *Bluetooth* utiliza la tecnología "salto de frecuencia de espectro extendido"[11]. Esto permite al dispositivo escoger aleatoriamente entre los 79 canales diferentes dentro de las frecuencias asignadas en Estados Unidos y Europa. Bajo esta tecnología, el dispositivo *Bluetooth* salta de una frecuencia a otra con una velocidad de saltos específica de acuerdo con una secuencia de código aleatoria. *Bluetooth* aplica esta tecnología a un nivel avanzado, ya que utiliza saltos de 1600 veces por segundo, permitiendo esta características la disponibilidad de alguna de las frecuencias, y el número de dispositivos que pueden ser asignados al espectro de frecuencia. Otros de los beneficios, es que permite tener mayor resistencia a la interferencia y es más segura contra las intercepciones. Lo mismo ocurre con dispositivos diferentes a los *Bluetooth*, que trabajen en la frecuencia de 2.4 GHz. Permite eliminar de una manera

[11] Original en inglés: "Frecuency-hopping Spread-spectrum"

virtual el riesgo que esos dispositivos interfieran con la transmisión *Bluetooth*, y si esto ocurriera, la interrupción duraría sólo una fracción de segundo.

En la actualidad un grupo de la IEEE 802.15 ha comenzado un proyecto de estandarización llamado 802.15.2 el cual hace una recomendación general para la coexistencia de las diferentes tecnologías dentro de las bandas no licenciadas. En este caso la banda de 2.4 GHz, y las tecnologías *Bluetooth*, 802.11, *HomeRF*, etc.

También existe una empresa llamada Mobilian, que se ha dedicado al desarrollo de una solución inalámbrica híbrida denominada *TrueRadio*, que permite la operación, en un mismo sistema, de 802.11 y *Bluetooth*, sin degradar el desempeño.

## 3 Gestor de Enlaces (LM)[12]

El gestor de enlaces es un módulo de software que se ejecuta en un microprocesador dentro de la unidad *Bluetooth* para gestionar la comunicación entre dispositivos. Cada dispositivo *Bluetooth* tiene su propio gestor de enlaces, que se encarga de descubrir a otros gestores de enlace remotos, y se comunica con ellos para gestionar el establecimiento del enlace, la autentificación, configuración y otras funciones.

## 4 Controlador de Enlaces (LC)[13]

El controlador de enlaces (LC) es un módulo de supervisión que maneja todas las funciones de la banda base de *Bluetooth* y da soporte al gestor de enlace. El controlador envía y recibe datos, solicita la identificación del dispositivo emisor, autentifica el enlace, establece el tipo de enlace (ACL o SCO), determina qué tipo de

[12] Siglas en inglés: "Link Manager (LM)"
[13] Siglas en inglés: "Link Controller (LC)"

trama utilizar en cada paquete, ordena como deben escuchar los dispositivos las transmisiones de otros dispositivos o pone a dichos dispositivos en modo retención, olfateo, estacionado, etc.

El sistema *Bluetooth* consiste en una unidad de radio, una unidad de control de enlace y una unidad para el soporte de las funciones de gestión del enlace y de interfaz del terminal (Ver Figura 2).

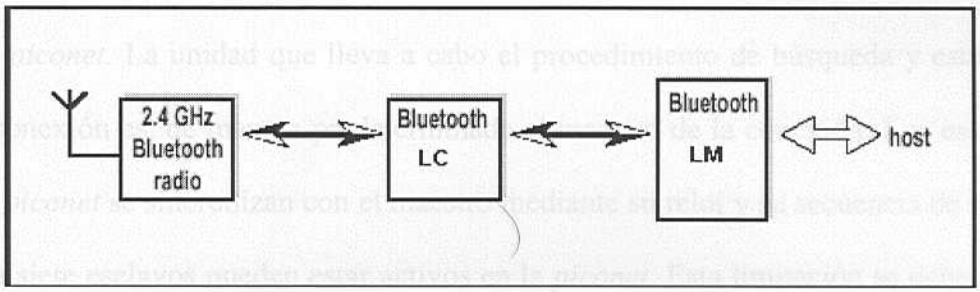


**Figura 2 Unidades funcionales en el sistema Bluetooth.** Tomado de Mc Daid, Cathal . 2000. *Routing Connections in Bluetooth*. Final Year Project, University of Limerick. Disponible: http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_lc.html [Consulta:2001, Noviembre 20]

En el *Specification of the Bluetooth System* (2001) se afirma que "puede soportar canales de datos asíncronos, hasta tres canales de voz síncronos, o un canal que simultáneamente soporte datos asíncronos y voz síncrona. Cada canal de voz soporta un canal síncrono de 64kb/s en cada dirección. El canal asíncrono puede soportar un máximo de 723.2 kb/s en asimétrico, o 433.9 kb/s en simétrico" [14](pt .B, p.41).

[14] Original en inglés: "Bluetooth can support an asynchronous data channel, up to three simultaneous synchronous voice channels, or a channel which simultaneously supports asynchronous data and synchronous voice. Each voice channel supports a 64 kb/s synchronous (voice) channel in each direction. The asynchronous channel can support maximal 723.2 kb/s asymmetric or 433.9 kb/s symmetric."

## 4.1 Topología de Red

El sistema *Bluetooth* proporciona una conexión punto a punto o multipunto (ver figura 3). En la conexión multipunto, el canal es compartido entre diferentes unidades *Bluetooth*. Cuando dos o más unidades comparten el mismo canal forman una *piconet*. Una unidad actúa como maestro de la *piconet*, mientras que las otras actúan como esclavas. El maestro es el dispositivo de una *piconet* cuyo reloj y secuencia de saltos se utilizan para sincronizar a todos los demás dispositivos, que son los esclavos en la *piconet*. La unidad que lleva a cabo el procedimiento de búsqueda y establece una conexión es, de manera predeterminada el maestro de la conexión. Los esclavos de la *piconet* se sincronizan con el maestro mediante su reloj y su secuencia de saltos. Hasta siete esclavos pueden estar activos en la *piconet*. Esta limitación se debe a que se utilizan tres bits para direccionar las unidades dentro de una *piconet*, por lo que en total se podrán direccionar ocho unidades.

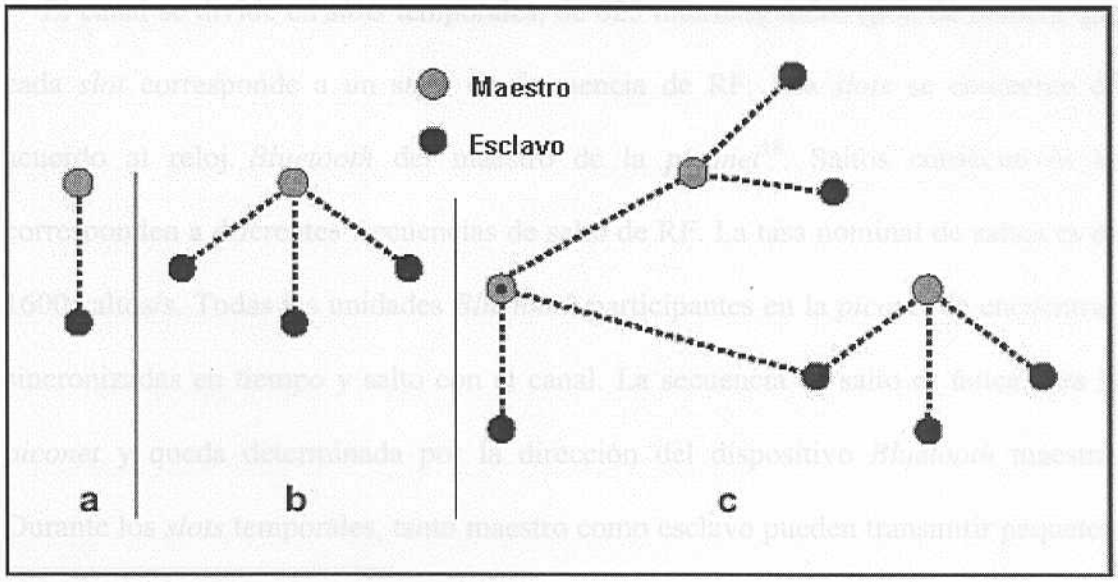


**Figura 3 Piconets (a)Un esclavo, (b) multi-esclavos, (c) scatternet.** Tomado de Mc Daid, Cathal . 2000. *Routing Connections in Bluetooth*. Final Year Project, University of Limerick. Disponible:

http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_lc.html [Consulta:2001, Noviembre 20]

Otras tantas unidades pueden permanecer inaccesibles al maestro en un estado denominado "estacionado"[15]. Las unidades esclavas estacionadas no pueden estar activas en el canal, pero permanecen sincronizadas con el maestro. Para ambos tipos de esclavas, el acceso al canal es controlado por el maestro.

Múltiples *piconets* con cobertura sobre áreas solapadas forman un *scatternet*[16]. Cada *piconet* sólo puede tener un único maestro. Sin embargo, las esclavas pueden participar en diferentes *piconets* usando una múltiplexación basada en el tiempo. Además, un maestro en una *piconet* puede ser esclavo en otra *piconet*. Las *piconets* pueden no estar sincronizados en frecuencia. Cada *piconet* tiene su propia secuencia de saltos de canal.

### 4.2 *Slots* Temporales (*Time Slots*)[17]

El canal se divide en *slots* temporales, de 625 microsegundos (μs), de manera que cada *slot* corresponde a un salto de frecuencia de RF. Los *slots* se enumeran de acuerdo al reloj *Bluetooth* del maestro de la *piconet*[18]. Saltos consecutivos se corresponden a diferentes frecuencias de salto de RF. La tasa nominal de saltos es de 1600 saltos/s. Todas las unidades *Bluetooth* participantes en la *piconet* se encuentran sincronizadas en tiempo y salto con el canal. La secuencia de salto es única para la *piconet* y queda determinada por la dirección del dispositivo *Bluetooth* maestro. Durante los *slots* temporales, tanto maestro como esclavo pueden transmitir paquetes.

[15] Original en ingles: "parked"
[16] Para mayor información ver glosario.
[17] Traducido del ingles: "Time Slots"
[18] Baseband Specification, 2001,pt B, cap. 2.2, p. 43

Se utiliza un esquema de división temporal (TDD) en el que el maestro y el esclavo transmiten alternativamente. El maestro sólo puede empezar su transmisión en *slots* con números pares, y el esclavo sólo en *slots* con números impares. El comienzo del paquete tiene que estar alineado con el comienzo del *slot*. Los paquetes transmitidos por ambos pueden ocupar hasta cinco *slots* (Ver figura 4).

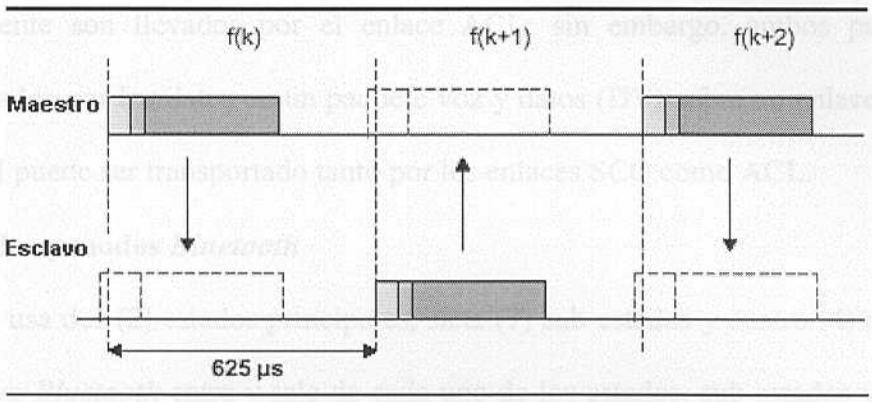


**Figura 4 Transmisión de paquetes durante los slots temporales**. Tomado de Mc Daid, Cathal . 2000. *Routing Connections in Bluetooth*. Final Year Project, University of Limerick. Disponible: http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_lc.html [Consulta: 2001, Noviembre 20]

## 4.3 Tipos de Enlace.

Se pueden establecer diferentes tipos de enlaces entre el maestro y los esclavos. Por un lado tenemos el enlace síncrono orientado a la conexión (SCO) y por el otro el enlace asíncrono sin conexión (ACL). El enlace SCO es un enlace punto a punto entre un maestro y un único esclavo en una *piconet*. El enlace ACL es un enlace multipunto entre un maestro y todos los esclavos participantes en uan *piconet*. En los *slots* no reservados para enlaces SCO, el maestro puede establecer un enlace ACL por *slot* hacia cualquier esclavo, incluyendo esclavos que ya estén comprometidos con un enlace SCO, (ver apéndice D para mayor información de los enlaces SCO y ACL). Además de los canales físicos, el sistema *Bluetooth* define los siguientes canales

lógicos: canal de control LC, control LM, canales de usuario asíncrono UA, usuario isócrono UI y usuario síncrono US. Los canales de control LC y LM son utilizados por el nivel de control de enlace y el nivel de gestión del enlace, respectivamente. El canal LC es transportado en la cabecera del paquete; el resto de canales con los datos. El canal US es transportado únicamente por el enlace SCO; los canales UA y UI normalmente son llevados por el enlace ACL; sin embargo, ambos pueden ser transportados por los datos en un paquete voz y datos (DV) sobre un enlace SCO. El canal LM puede ser transportado tanto por los enlaces SCO como ACL.

### 4.4 Estados y modos *Bluetooth*

El LC usa dos (2) estados principales, siete (7) sub-estados y cuatro (4) modos. El dispositivo *Bluetooth* entra y sale de cada uno de los estados, sub-estados y modos a través de comandos enviados desde el LM o LC, (ver figura 5).

Los estados principales son: En Espera y Conexión.

#### 4.4.1 Estado En Espera (*Standby*)[19]

Es el estado por defecto de un dispositivo *Bluetooth*. Este estado requiere de poca energía, y es usado para liberar la capacidad en la *piconet*, donde solamente puede haber siete (7) dispositivos activos al mismo tiempo. Si más de siete (7) dispositivos se encuentran en la *piconet*, al dispositivo que quiera entrar, tiene que pasar al estado de espera. En este estado sólo esta corriendo el reloj del mismo dispositivo y no tiene ninguna interacción con otro dispositivo. Todos los dispositivos permanecen en este estado hasta que el LC solicite una nueva operación, que permita salirse.

[19] Traducido del inglés: "Standby".

### 4.4.2 Estado Conexión (*Connection*)

El estado de conexión, ocurre cuando dos (2) o más dispositivos tienen una conexión activa y pueden pasar paquetes de datos en ambas direcciones.

Por defecto, los dispositivos *Bluetooth* se encuentra sin una conexión, por lo tanto tienen el estado de espera, en el cual ellos están escuchando los mensajes, a este proceso se le denomina rastrear.

El rastreo se divide en dos (2) grandes grupos: sub-estado de búsqueda y sub-estado de indagación. Estos sub-estados son para añadir o remover los dispositivos *Bluetooth* de una *piconet*. El estado de búsqueda habilita a los dispositivos *Bluetooth* para conectarse con otra unidad. El estado de indagación, cuando se habilita, se encarga de descubrir a otros dispositivos que se encuentren dentro del rango de cobertura.

#### 4.4.1.1 Sub-estado de Indagación (*Inquiry*)[20]

Los dispositivos *Bluetooth* también pueden usar tres (3) fases del sub-estado de indagación. Estas fases usan esencialmente los mismos procedimientos que las fases de búsqueda. La diferencia está en la información que es enviada entre los dispositivos. Las fases son:

**(a) Rastrear la indagación**: en esta fase, el maestro mira a los esclavos potenciales, a los cuales no se les conoce el Control de Acceso a Dispositivo (DAC)[21], necesario para crear una conexión.

[20] Traducido del ingles: "Inquiry"
[21] Siglas en ingles: "Device Access Control (DAC)"

**(b) Indagación**: en esta fase, el maestro obtiene el DAC necesario para poder establecer la conexión con el esclavo que ha respondido.

**(c) Respuesta de la indagación:** El esclavo que ha respondido con su DAC, permite comenzar el establecimiento de la conexión y el maestro entra al sub-estado de búsqueda

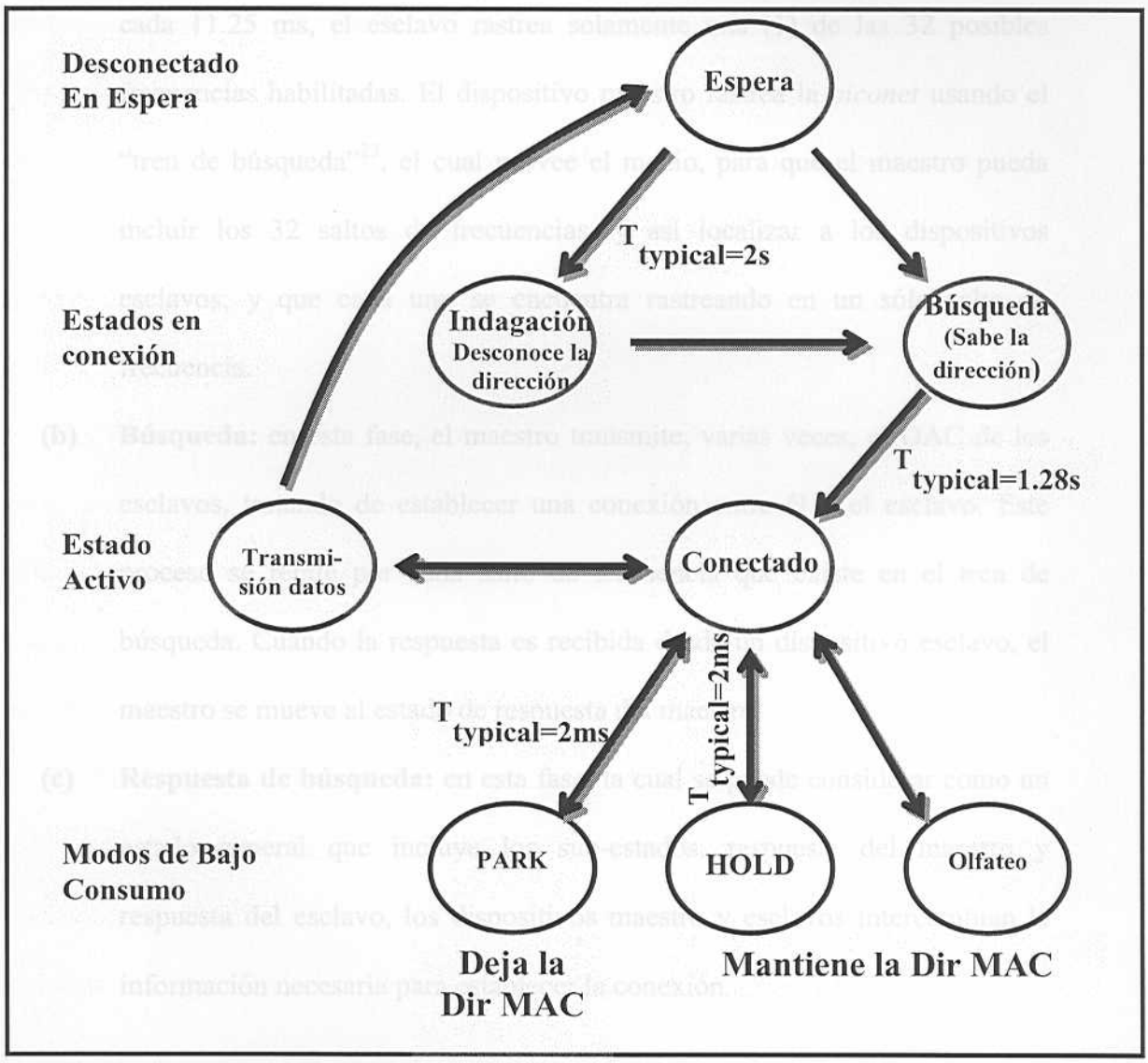


**Figura 5 Diagrama de transición entre estados.** Tomado de Mc Daid, Cathal . 2000. *Routing Connections in Bluetooth*. Final Year Project, University of Limerick. Disponible: http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_1c.html [Consulta:2002, Enero 12]

#### 4.4.1.2 Sub-estados de Búsqueda (*Paging*)[22]

*Bluetooth* usa tres (3) fases, para localizar y construir la conexión entre un maestro y un esclavo.

**(a) Rastreo de búsqueda:** en esta fase el dispositivo esclavo rastrea su DAC cada 11.25 ms, el esclavo rastrea solamente una (1) de las 32 posibles frecuencias habilitadas. El dispositivo maestro rastrea la *piconet* usando el "tren de búsqueda"[23], el cual provee el medio, para que el maestro pueda incluir los 32 saltos de frecuencias, y así localizar a los dispositivos esclavos, y que cada uno se encuentra rastreando en un sólo salto de frecuencia.

**(b) Búsqueda:** en esta fase, el maestro transmite, varias veces, el DAC de los esclavos, tratando de establecer una conexión entre él y el esclavo. Este proceso se repite por cada salto de frecuencia que existe en el tren de búsqueda. Cuando la respuesta es recibida desde un dispositivo esclavo, el maestro se mueve al estado de respuesta del maestro.

**(c) Respuesta de búsqueda:** en esta fase, la cual se puede considerar como un estado general que incluye los sub-estados: respuesta del maestro y respuesta del esclavo, los dispositivos maestro y esclavos intercambian la información necesaria para establecer la conexión.

[22] Traducido del inglés: "Paging"
[23] Original en ingles:"page train"

#### 4.4.2.1 Modos de Conexión

El estado de conexión empieza con un paquete de POLL enviado por el maestro para verificar que la unidad esclava se ha cambiado a la sincronización y a la frecuencia del canal. El esclavo puede responder con cualquier tipo de paquete. Si el esclavo no recibe el paquete de POLL o el maestro no recibe la respuesta, ambos dispositivos volverán a los sub-estados de indagación/búsqueda. Los primeros paquetes de información en el estado de conexión contienen mensajes de control que caracterizan el enlace y dan más detalles con respecto a las unidades *Bluetooth*. Las unidades poseen diferentes modos de operación en el estado de conexión: modo activo, olfateo, espera y estacionado.

**(a) Modo Activo:** la unidad participa activamente en el canal. El maestro programa su transmisión de acuerdo a las demandas de tráfico hacia y desde las diferentes esclavas. Además, soporta transmisiones regulares para mantener a las esclavas sincronizadas con el canal. Las unidades esclavas activas escuchan los *slots* en busca de paquetes desde el maestro.[24]

**(b) Modo Olfateo (*Sniff*)[25]:** es un modo para ahorrar energía en los dispositivos *Bluetooth*. Se puede reducir el ciclo de actividad para la escucha de la esclava. Si una esclava participa en un enlace ACL, tiene que escuchar en cada *slot* ACL el tráfico del maestro. Con el modo olfatear, el tiempo de *slot* en que el maestro empieza la transmisión a una esclava concreta se reduce, es decir, el maestro sólo podrá empezar

[24] Baseband Specification, 2001,pt B, cap. 10.8.1, p. 110
[25] Traducido del inglés: "Sniff"

la transmisión en *slots* de tiempo específicos, a los que se denomina *slots* de olfateo, y que se encuentran regularmente espaciados en un intervalo de *Tsniff*.[26] De esta manera la esclava empieza la escucha en los *slots* de olfateo en intentos consecutivos hasta que se recibe un paquete. Para entrar en el modo olfatear, el maestro o la esclava deben enviar un comando de olfateo a través del protocolo LM. Este mensaje contendrá el intervalo de olfateo.

**(c) Modo Espera (*Hold*)**[27]: el enlace ACL entre dos dispositivos se puede poner en modo espera durante un tiempo específico. Esto significa que la esclava no soportará paquetes ACL temporalmente. Con este modo de operación, se puede liberar capacidad para hacer otras tareas como exploración, búsqueda, pregunta o atención a otra *piconet*. Durante el modo espera, la esclava mantiene la dirección de miembro activa. Antes de entrar en el modo espera, maestro y esclavo deben ponerse de acuerdo en el tiempo en que la unidad esclava permanecerá en este modo.

**(d) Modo Estacionado (*Park*)**[28]**:** cuando una esclava no necesita participar en el canal del *piconet*, pero quiere permanecer sincronizada con el canal, puede entrar en este modo, que es de bajo consumo con una mínima actividad en la esclava, y entrega su dirección de miembro activa (AM_ADDR)[29]. En su lugar, recibe dos nuevas direcciones: dirección de miembro estacionado y dirección de petición de acceso. La esclava en modo estacionado se despierta a intervalos regulares para escuchar el canal para resincronizarse y comprobar mensajes de difusión.

[26] Baseband Specification, 2001,pt B, cap. 10.8.2, p. 111
[27] Traducido del inglés: "Hold"
[28] Traducido del inglés: "Park"
[29] Siglas en inglés: "Active Member Address (AM_ADDR)"

## 5 Protocolo de gestión de enlace (LMP)[30]

Los mensajes LMP son utilizados para configurar el enlace, seguridad y control. LMP también controla los modos de administración de energía, y los estados de conexión de una unidad *Bluetooth* dentro de una *piconet*. Los mensajes son filtrados e interpretados por el LM en el lado receptor y estos no se propagan hacia capas superiores (ver figura siguiente).

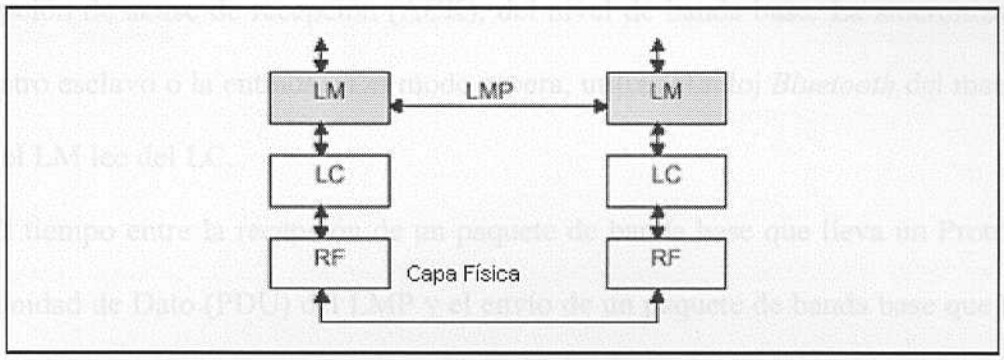


**Figura 6 Ubicación del nivel LMP en el escenario global**. Tomado de Mc Daid, Cathal . 2000. *Routing Connections in Bluetooth*. Final Year Project, University of Limerick. Disponible: http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_lmp.html [Consulta:2002, Enero 12].

Los mensajes de gestión de enlace tienen mayor prioridad que los datos de usuario. Esto significa que si el gestor del enlace necesita mandar un mensaje, éste no puede ser retrasado por el tráfico del Protocolo de Control de Enlace Lógico y Nivel de Adaptación (L2CAP)[31], aunque sí puede ser retrasado por retransmisiones de paquetes individuales de banda base.

No se tiene que reconocer explícitamente los mensajes LMP puesto que LC proporciona un enlace fiable[32]. Sin embargo, LC no garantiza ni el tiempo empleado

[30] Siglas en inglés: "Link Manager Protocol (LMP)"
[31] Siglas en ingles: "Logical Link Control and Adaptation Protocol (L2CAP)"
[32] Baseband Specification, 2001,pt C, cap. 1, p. 189

para entregar el mensaje al dispositivo remoto ni el retardo entre la entrega del mensaje al dispositivo remoto y la recepción del reconocimiento por parte del emisor.

Esto significa que se debe ser consciente de las limitaciones de los mecanismos subyacentes de LC para sincronizar los cambios de estado entre el maestro y el esclavo. El criterio para determinar cuando el maestro puede reutilizar una dirección de dispositivo tras los estados de olfatear o estacionado de un esclavo; se basa en la recepción de acuse de recepción (ACK), del nivel de banda base. La sincronización maestro esclavo o la entrada en el modo espera, utiliza el reloj *Bluetooth* del maestro, que el LM lee del LC.

El tiempo entre la recepción de un paquete de banda base que lleva un Protocolo de Unidad de Dato (PDU) del LMP y el envío de un paquete de banda base que lleve una PDU de respuesta válida, debe ser menor que el tiempo de expiración de respuesta del LMP. El valor de este tiempo es 30 segundos[33].

## 6 Interfaz del Controlador de host (HCI)[34]

Según la especificación *Bluetooth* HCI proporciona una interfaz de comandos para el controlador de banda base y el gestor de enlace. Así como también tener acceso a los registros de control y el estado del hardware. En otras palabras, esta interfaz proporciona un método uniforme para acceder a las capacidades de la banda base y el *host Bluetooth.*

[33] Baseband Specification, 2001,pt C, cap. 1, p. 190
[34] Siglas en ingles: "Host Controller Interface (HCI)"

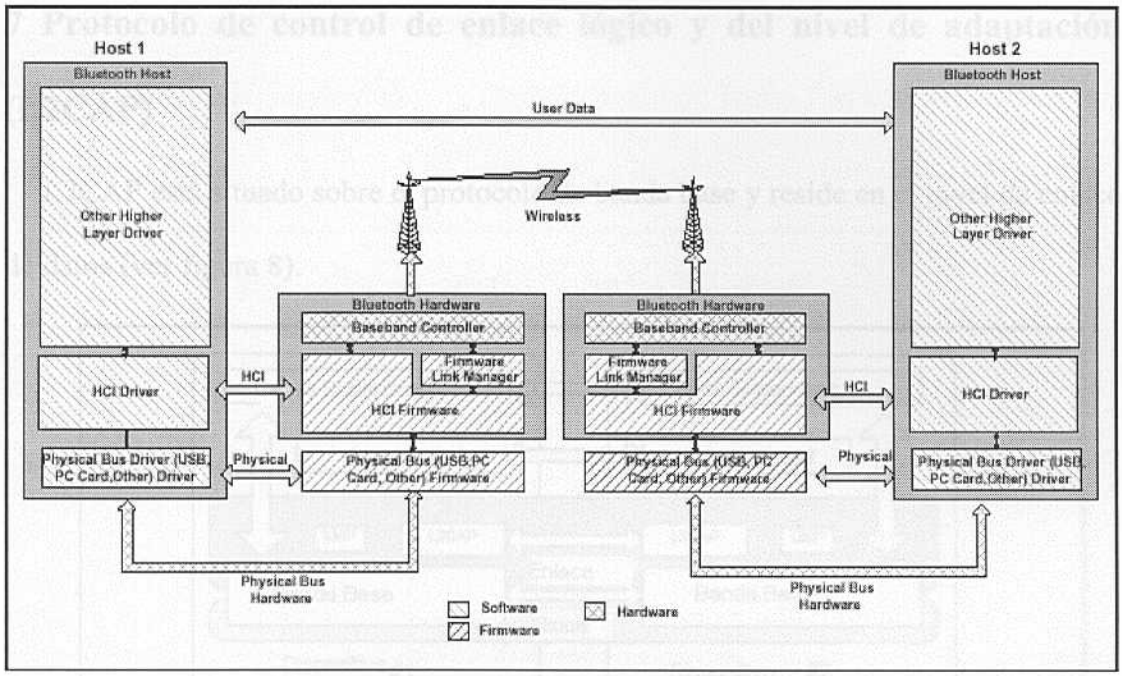


**Figura 7 Interfaz HCI.** Tomado de: Specification of the Bleutooth System , 2001, pt H1, cap. 1, p. 544

El HCI no es un componente mandatorio del módulo *Bluetooth.* Si por ejemplo el en el diseño del dispositivo el módulo esta completamente integrado, este no necesita que exista el HCI. Y en otras ocasiones si lo necesita, como por ejemplo en dispositivos PDAs cuando se le añade la chaqueta para que este pueda comunicarse con cualquier otro dispositivo *Bluetooth.*

Usar el HCI permite a una aplicación de *Bluetooth* tener acceso al hardware de *Bluetooth* sin la necesidad de saber sobre la capa de transporte u otros detalles de la puesta en práctica de hardware.

## 7 Protocolo de control de enlace lógico y del nivel de adaptación (L2CAP)

L2CAP está situado sobre el protocolo de banda base y reside en el nivel de enlace de datos (ver figura 8).

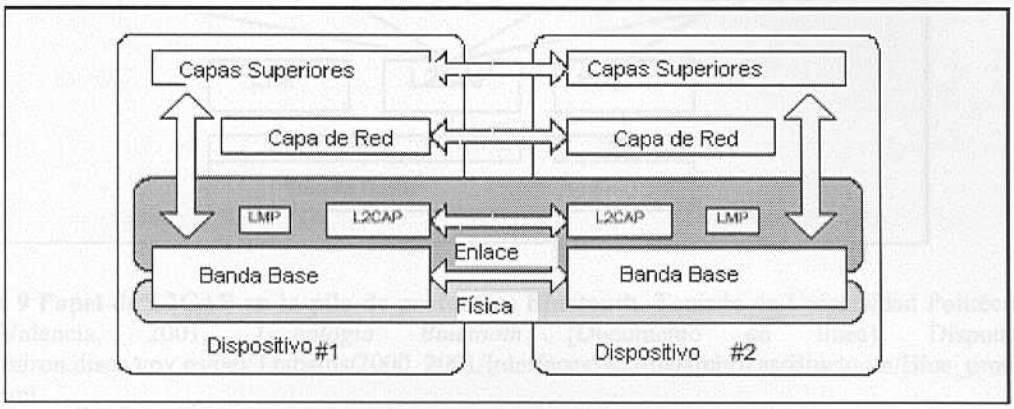


**Figura 8 L2CAP dentro de los diferentes niveles de Bluetooth.** Tomado de Universidad Politécnica de Valencia, 2001. *Tecnología Bluetooth* [Documento en línea]. Disponible :http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_l2cap.html.

Proporciona servicios de datos con conexión y sin conexión hacia protocolos de capas superiores a través de capacidades de multiplexación de protocolos, operaciones de segmentación y reensamblado, también soporta información de calidad de servicio (QoS). L2CAP permite a los protocolos y aplicaciones de alto nivel transmitir y recibir paquetes de datos L2CAP de hasta 64 kb de longitud[35].

El L2CAP solamente contempla los enlaces ACL y de momento no tiene pensado el soporte para enlaces SCO. Los requerimientos funcionales para L2CAP incluyen multiplexación de protocolos, segmentación y reensamblado (SAR).La figura 8 muestra como es el papel de L2CAP.

[35] Baseband Specification, 2001,pt D, cap. 1, p. 257

L2CAP ofrece interfaces a otros protocolos de comunicación como Protocolo de Descubrimiento de Servicio (SDP), Comunicación de Radio Frecuencia (RFCOMM) o Control Telefónico (TCS)[36]. Los canales de calidad de voz para audio y telefonía

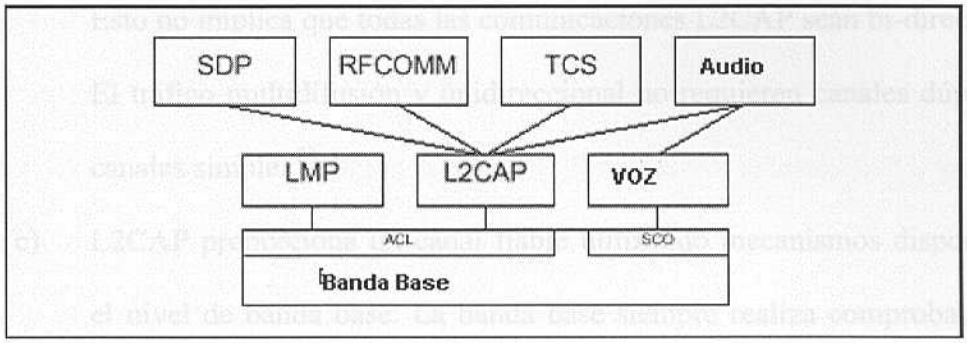


**Figura 9 Papel de L2CAP en la pila de protocolos Bluetooth.** Tomado de Universidad Politécnica de Valencia, 2001. *Tecnología Bluetooth* [Documento en línea]. Disponible :http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_l2cap.html.

suelen funcionar sobre enlaces de banda base SCO. Los requisitos de protocolo esenciales para L2CAP incluyen simplicidad y baja sobrecarga. Las implementaciones de L2CAP deben ser aplicables a dispositivos con recursos computacionales limitados. L2CAP no debería consumir excesiva energía puesto que esto provoca un descenso en la eficiencia de la radio *Bluetooth*. Los requisitos de memoria para la implementación se deberían mantener al mínimo.

El protocolo se ha diseñado bajo las siguientes consideraciones:

(a) El enlace ACL entre dos unidades se configura utilizando el LMP. La banda base proporciona una entrega ordenada de los paquete de datos, aunque

[36] Baseband Specification, 2001,pt D, cap. 1, p. 258

pueda haber tanto corrupción de paquetes como duplicados. No existirá más de un enlace ACL entre dos dispositivos[37].

(b) La banda base también proporciona canales de comunicación full dúplex. Esto no implica que todas las comunicaciones L2CAP sean bi-direccionales. El tráfico multidifusión y unidireccional no requieren canales dúplex, sino canales simplex[38].

(c) L2CAP proporciona un canal fiable utilizando mecanismos disponibles en el nivel de banda base. La banda base siempre realiza comprobaciones de integridad de datos cuando solicita o envía datos hasta que recibe un reconocimiento o finalice el tiempo. Debido a que los acuse de recepción se podrían perder, los tiempos de expiración pueden ocurrir incluso después de haber mandado correctamente los datos. El protocolo de banda base utiliza un número de secuencia de un *bit* que elimina los duplicados. Está prohibido utilizar paquetes de difusión en banda base si se requiere fiabilidad puesto que los mensajes de difusión comienzan al inicio del primer segmento del paquete L2CAP con el mismo bit de secuencia.[39]

## 8 Protocolo para descubrir servicios (SDP)[40]

SDP trata el servicio de descubrimiento de servicio específicamente para el entorno *Bluetooth*. Se encuentra optimizado por la naturaleza extremadamente dinámica de las comunicaciones *Bluetooth*. SDP se centra principalmente en el

[37] Baseband Specification, 2001,pt D, cap. 1, p. 260
[38] Baseband Specification, 2001,pt D, cap. 1, p. 260
[39] Baseband Specification, 2001,pt D, cap. 1, p. 260
[40] Siglas en ingles: "Service Discovery Protocol (SDP)"

descubrimiento de los servicios disponibles desde o a través de dispositivos *Bluetooth*. SDP no define métodos para el acceso a los servicios; una vez descubiertos los servicios con SDP, estos pueden ser accedidos de muchas maneras diferentes, dependiendo del servicio. SDP proporciona un medio para que otros protocolos se ejecuten junto con SDP, en entornos en que puede ser beneficioso. En entornos *Bluetooth*, los servicios pueden ser descubiertos usando SDP y pueden ser accedidos usando otros protocolos definidos por *Bluetooth*.

El mecanismo de descubrimiento de servicio proporciona el medio para que aplicaciones cliente descubran la existencia de servicios proporcionados por aplicaciones en los servidores, así como los atributos de estos servicios. Los atributos de un servicio incluyen el tipo o la clase del servicio y el mecanismo o información de protocolo necesarios para utilizar este servicio. En la figura 9, se puede apreciar un esquema de comunicación entre el servidor y el cliente.

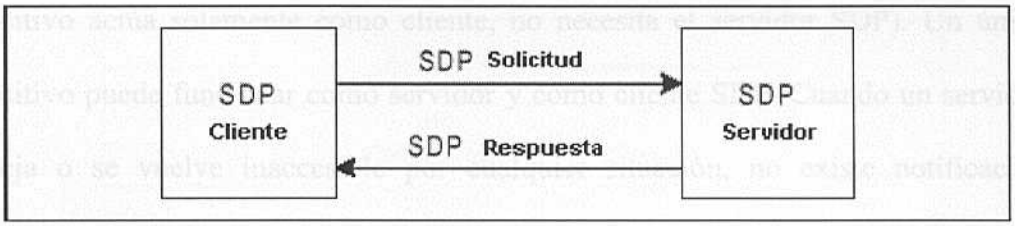


**Figura 10 Interacción cliente-servidor.** Tomado de Universidad Politécnica de Valencia, 2001. *Tecnología Bluetooth* [Documento en línea]. Disponible :http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_sdp.html.

SDP utiliza un modelo petición/respuesta donde cada transacción consiste en una petición de una PDU y otra de respuesta. En el caso en el que SDP se utilice con el Protocolo de transporte L2CAP, solamente puede estar pendiente de una petición de PDU por conexión con un servidor SDP en un instante determinado. Es decir, el

cliente debe recibir una respuesta a cada petición antes de realizar otra solicitud sobre la misma conexión L2CAP. Limitando a SDP a mandar una petición de PDU sin reconocimiento, y con esto se consigue un sencillo control de flujo[41].

SDP involucra una comunicación entre un servidor y un cliente SDP. El servidor mantiene una lista de registros de servicios que describen las características de los servicios asociados con el servidor. Cada registro de servicio contiene información acerca de un servicio único. Un cliente puede obtener información de un registro de servicio mantenido por el servidor SDP utilizando una petición SDP.

Si un cliente, o una aplicación asociada con un cliente, deciden utilizar un servicio, debe abrir una conexión por separado con el proveedor del servicio. SDP proporciona un mecanismo para descubrir los servicios y sus atributos, pero no proporciona un mecanismo para utilizar estos servicios.

Hay un máximo de un servidor SDP por cada dispositivo *Bluetooth*. (Si un dispositivo actúa solamente como cliente, no necesita el servidor SDP). Un único dispositivo puede funcionar como servidor y como cliente SDP. Cuando un servidor se aleja o se vuelve inaccesible por cualquier situación, no existe notificación explícita a través de SDP. Sin embargo, el cliente puede usar SDP para buscar servidores y averiguar que el servidor no se encuentra disponible si ya no responde a sus peticiones.

[41] Baseband Specification, 2001,pt E, cap. 2, p. 339

## 9 RFCOMM

RFCOMM es un protocolo de transporte, que proporciona las emulaciones de puertos seriales sobre el protocolo L2CAP. El protocolo se basa en el estándar de ETSI[42] TS 07.10, aunque solamente un subconjunto de este estándar es utilizado. Se ha añadido un esquema que especifica el funcionamiento del control de flujo, este esquema es usado obligatoriamente.

El protocolo soporta hasta 60 conexiones simultáneas entre dos dispositivos *Bluetooth*[43]. Aunque el número de conexiones, depende de la implementación en específico que se está realizando

Un camino de comunicación completo involucra dos aplicaciones ejecutándose sobre dispositivos diferentes (extremos de la comunicación) con un segmento de comunicación entre ellos, en la figura 9, se demuestra como es el segmento de comunicación RFCOMM.

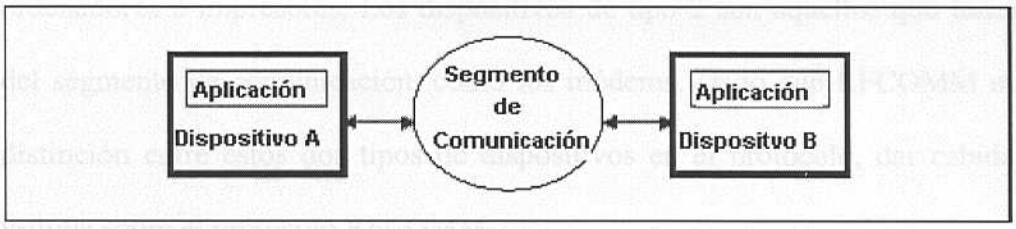


**Figura 11 Segmento de comunicación RFCOMM.** Tomado de Universidad Politécnica de Valencia, 2001. *Tecnología Bluetooth* [Documento en línea]. Disponible :http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto_sdp.html.

En este contexto, la aplicación no denota a una aplicación de usuario, sino, por ejemplo, a protocolos de nivel superior u otros servicios actuando en nombre de las aplicaciones de usuario.

[42] Siglas en ingles:"European Telecommunications Standards Institute"
[43] RFCOMM Specification, 2001,pt F:1, cap. 2.3.1, p. 397

Se pretende que RFCOMM cubra aplicaciones que hacen uso del puerto serie de los dispositivos en que residen. En una configuración simple, el segmento de comunicación es un enlace *Bluetooth* de un dispositivo a otro (conexión directa). Donde el segmento es otra red, la tecnología inalámbrica *Bluetooth* utiliza como vía entre nuestro dispositivo y el dispositivo de conexión a la red, como un módem.

A RFCOMM sólo le conciernen las conexiones entre dispositivos en el caso de conexión directa, o entre el dispositivo y un módem en el caso de una red. RFCOMM puede soportar otras configuraciones, por un lado, como módulos que se comuniquen a través de la tecnología inalámbrica de *Bluetooth*, y con una interfaz no inalámbrica por el otro lado. Estos dispositivos no son realmente módems pero ofrecen un servicio similar.

Básicamente existen dos tipos de dispositivos para los que RFCOMM debe tener cabida. Los dispositivos de tipo 1 actúan como extremos de una comunicación, como ordenadores e impresoras. Los dispositivos de tipo 2 son aquellos que forman parte del segmento de comunicación, como los módems. Dado que RFCOMM no realiza distinción entre estos dos tipos de dispositivos en el protocolo, dar cabida a tipos influye sobre el protocolo RFCOMM.

La información transferida entre dos entidades RFCOMM se ha definido para soportar dispositivos de tipo 1 y 2. Parte de la información es necesitada solamente por los dispositivos de tipo 2 mientras que otra es utilizada por ambos tipos. Como el protocolo no realiza distinción entre el tipo 1 y el 2, es tarea de los desarrolladores de RFCOMM determinar si la información pasada en el protocolo RFCOMM es útil para la implementación. Puesto que el dispositivo no es consciente del tipo de los

otros dispositivos en la comunicación, cada uno debe transmitir toda la información disponible por el protocolo.

## 10 Protocolos Adoptados.

La especificación *Bluetooth* emplea varios protocolos existentes, que se reutilizan para diferentes propósitos en los niveles superiores. Esto permite a las aplicaciones más antigua funcionen con la tecnología inalámbrica *Bluetooth* y ayuda a asegurar un correcto funcionamiento e interoperabilidad de estas aplicaciones con aplicaciones modernas diseñadas específicamente para dispositivos *Bluetooth.* Los protocolos adoptados son:

(a) Protocolo Punto a Punto (PPP)[44]

(b) Protocolo de Control de Transmisión (TCP)[45].

(c) Protocolo Internet (IP)[46].

(d) Protocolo de Datagrama de Usuario (UDP)[47].

Cada uno de estos protocolos es explicado en el apéndice C

## 11 Tecnología Inalámbrica

*Bluetooth* es una de muchas tecnologías que soportan comunicación inalámbrica, incluyendo algunas que pueden competir por el mercado inalámbrico y con la posibilidad de impedir el éxito de *Bluetooth*. Otros pueden complementar el ambiente *Bluetooth*, coexistir potencialmente y juntas trabajar bien.

[44] Siglas en inglés: "Point to Point Protocol (PPP)"
[45] Siglas en inglés: " Transmission Control Protocol (TCP)"
[46] Siglas en ingles: "Internet Protocol (IP)"
[47] Siglas en inglés: "User Datagram Protocol (UDP)"

### 11.1 *Bluetooth* e Infrarrojo

La comunicación infrarroja se realiza con una conexión óptica, la cual usa una luz infrarroja de 850 nanometros para la transmisión de voz y dato entre dispositivos. La señal necesita de una trayectoria clara y directa desde un dispositivo hasta el otro. Normalmente los dispositivos deben estar colocados cerca uno del otro y con vista entre ellos, aunque hay tecnologías que funcionan con rebotes sobre las paredes. La conexión tiene un alcance de alrededor de unos pocos metros, porque los dispositivos deben estar colocados cerca cuando intercambia información. Infrarrojo ofrece un método seguro para la transmisión. Está provisto para enlaces punto a punto entre dos dispositivos, para la transmisión de datos y sincronización de archivos.

Aunque las tecnologías *Bluetooth* e infrarrojo soportan muchas aplicaciones semejantes, cada tecnología tiene sus ventajas y desventajas. Por ejemplo en el intercambio de tarjetas electrónicas de negocio, en infrarrojo se realiza mejor. Los usuarios de infrarrojo pueden hacer el intercambio señalando desde un dispositivo a otro. El límite de rango de intercambio de datos del infrarrojo no es una limitante.

Aunque *Bluetooth* también soporta el intercambio de tarjetas *VCards,* el intercambio no es directo ni fácil. Un dispositivo *Bluetooth* primero necesita descubrir a otro dispositivo, realizar algunos procedimientos necesarios para la seguridad, servicios de acceso, y finalmente el intercambio de las tarjetas de negocio. Y el tiempo consumido en este proceso es rápido y fácil usando infrarrojo y es algo tedioso con dispositivos *Bluetooth.* (Sin embargo, una vez hecha la conexión, es rápido la transferencia de datos.)

Sin embargo *Bluetooth* no requiere de una línea de mira para la comunicación con otro dispositivo, y esto facilita la conexión con otros dispositivos en la *piconet*. Intercambiando datos con múltiples dispositivos, esto es imposible con Infrarrojo, ya que ofrece enlaces punto a punto entre dos dispositivos.

La capacidad omnidireccional de la tecnología *Bluetooth* permite la sincronización con otros dispositivos, esto ocurre automáticamente cuando los dispositivos se encuentran en un rango con otros dispositivos. La tecnología *Bluetooth* también permite que ocurra la sincronización mientras el usuario está en movimiento. Esto no puede ocurrir con Infrarrojo, lo cual requiere que ambos dispositivos permanezcan fijos en una posición para poder tomar la sincronización, aunque no necesariamente, ya existen dispositivos infrarrojos que funcionan en movimiento, por ejemplo Robots Lego.

En términos de transferencia de datos, infrarrojo proporciona una tasa de transferencia más rápida que *Bluetooth*, lo que es una gran ventaja. *Bluetooth* mueve los datos entre los dispositivos sobre los 721 Kbps, mientras que la tasa de transferencia de datos en infrarrojo es de 4Mbps.

*Bluetooth* e Infrarrojo pueden realizar conexiones inalámbricas entre dispositivos portátiles y con redes cableadas. Pero ya que *Bluetooth* no necesita la línea de mira, e hace que esto sea más fácil que con infrarrojo. Los usuarios *Bluetooth* tienen más flexibilidad en la colocación de los puntos de acceso que en los usuarios de infrarrojo. (Un punto de acceso acepta señales inalámbricas desde dispositivos portátiles mientras proveen una conexión con cable para una LAN.) También, el dispositivo

*Bluetooth* no tiene que permanecer estacionario mientras esta conectado a la LAN ( dentro de un rango de 100 metros).

*Bluetooth* e Infrarrojo permiten la conexión a internet. Y ambos trabajan bien para esas conexiones, con *Bluetooth* se tiene una pequeña ventaja en términos de la colocación del dispositivo.

Usando la tecnología infrarroja ciertamente se tiene ventajas y desventajas, que están resumidas en la tabla 2.

**Tabla 2**
**Ventajas y Desventajas de la tecnología infrarrojo**

| ***Ventajas*** | ***Desventajas*** |
|---|---|
| Velocidad. | Rango limitado. |
| Bajo consumo de poder. | Angulo de conexión limitado. |
| Seguro. | |
| No tiene interferencia de radio frecuencia. | |
| Es barato. | |

Datos tomados de "*Bluetooth End to End*" (pág 262) por D.M Bakker y Diane Gilster, 2002, New York.

Aunque son mas las ventajas que las desventajas, estas son significativas en términos de cómo ellas impactan en la usabilidad de los dispositivos Infrarrojos.

### 11.2 *Bluetooth* y *HomeRF*

*Home Radio Frecuency* (*HomeRF*), es otra tecnología inalámbrica que se usa en la banda ISM, 2.4 GHz. Esta tecnología es apoyada por un consorcio de 100 compañías miembros, muchas de los cuales se encuentran dentro del SIG de *Bluetooth*. El consorcio *HomeRF* fue creado con una especificación abierta para la industria de las comunicaciones de dispositivos digitales inalámbricos y para un ambiente de

computadoras caseras, esta es la leve diferencia con las Redes de Área Personal (PAN)[48] de *Bluetooth*.

*HomeRF* soporta la transmisión de voz y datos, usando salto de frecuencia de espectro extendido. La tasa de transferencia de datos en *HomeRF*, es de 2 hasta 10 Mbps. Una diferencia es la tasa de salto usada por los dispositivos *Bluetooth* y *HomeRF*, y la posibilidad de interferencia entre los dispositivos es leve.

*HomeRF* está basado en las especificaciones del Protocolo de Acceso Inalámbrico Compartido (SWAP)[49], la cual provee los siguientes canales para transmisión:

- Seis canales de voz, basado en el estándar de Teléfonos Inalámbricos Digital (DECT)[50].
- Un canal de datos, basado en las especificaciones 802.11 de la IEEE[51].

La tecnología de *HomeRF* ofrece precios bajos, y es alternativo a las redes inalámbricas de 802.11, porque esta no requiere de un equipo dedicado para el punto de acceso, y las conexiones son hechas punto a punto entre los dispositivos. Las conexiones *HomeRF* son buenas hasta aproximadamente 50 pies, pero no son robustas como las redes Ethernet. *HomeRF* funciona bien en ambientes hogareños, más no en los ambientes corporativos. *HomeRF* no esta previsto para dispositivos portátiles o conexiones *ad hoc* (ver definición en el apéndice E), dando a *Bluetooth* una ventaja clara en esta área.

[48] Siglas en inglés: "Personal Area Network (PAN)"
[49] Siglas en inglés: "Shared Wireles Access Protocol (SWAP)"
[50] Siglas en inglés: "Digital Enhanced Cordless Telephone (DECT)"
[51] Siglas en ingles: "Institute of Electrical and Electronics Engineers (IEEE)"

Las tecnologías *HomeRF* y *Bluetooth* pueden fácilmente coexistir y en algunos casos cada una puede complementar a la otra. Por ejemplo para crear una red viable en una casa, se podría usar *HomeRF* para conectar a todos los computadores unos con otros y con *Bluetooth* conectarse entre los periféricos y los computadores. Ya que ambos sistemas usan el salto de frecuencia, este tipo de redes locales no tendrán ningún problema de interferencia.

Claramente, *HomeRF* provee muchas ventajas para la creación de redes caseras. La tabla siguiente muestra las ventajas y desventajas *de HomeRF*.

**Tabla 3**
**Ventajas y desventajas de la tecnología *HomeRF*.**

| *Ventajas* | *Desventajas* |
|---|---|
| Velocidad. | Rango limitado. |
| Fácil de instalar. | Dificultad para integrarse con redes cableadas. |
| No requiere de un punto de acceso. | No es estable en redes como Ethernet. |
| Permite hasta 127 dispositivos por red. | Consume mucha energía, y esto no es bueno para ser usado en dispositivos portátiles. |
| Es barato. | |
| Permite múltiples redes en un mismo lugar. | |
| El uso de salto de frecuencia reduce la interferencia. | |

Datos tomados de "*Bluetooth End to End*" (pág 263) por D.M Bakker y Diane Gilster, 2002, New York.

### 11.3 Redes inalámbricas y *Bluetooth*.

El estándar 802.11 es otra opción para la conexión de redes inalámbricas, o *Wireless Fidelity* (Wi-Fi) como también es conocido. Como *Bluetooth*, esta tecnología hace uso de señales de difusión RF en la banda de frecuencia de 2.4 GHz. Esta tecnología es para el uso estricto de transmisión de datos, y no esta dirigido para señales de voz ni dar soporte telefónico. Si se puede usar para conexiones *ad-hoc*, pero básicamente es una replica de una red Ethernet sin cables.

La especificación 802.11, usa la tecnología de Espectro extendido de secuencia directa (DSSS)[52], esto difiere de la tecnología usada por *Bluetooth* que es Espectro extendido de salto de frecuencia (FHSS). DSSS tienen las señales fijas en canales de 17 MHz, opuesto a lo utilizado por *Bluetooth* que son 79 saltos de frecuencias distintos. Como resultado de usar DSSS, la especificación 802.11 permite tasas de transferencias de datos hasta 11 Mbps.

La red de 802.11 está hecha para usar un equipo de punto de acceso. Un punto de acceso es un receptor y transmisor que usan los dispositivos para poder conectarse a la red. Este punto de acceso puede añadirle un costo significativo a la red. Porque la necesidad de un punto de acceso y la configuración de una LAN, con la tecnología 802.11 pueden ser costosa. Sin embargo, esta tecnología gana significantemente en velocidad, confiabilidad y el rango de cobertura es mayor, ya que puede llegar hasta 300 pies.

La tecnología 802.11 no trabaja tan bien como *Bluetooth* para redes *ad-hoc*, porque esto requiere de instalaciones complejas. Las redes *ad-hoc* es uno de los fuertes de *Bluetooth*. Por esta razón las dos tecnologías podrían coexistir y aprovecharse una de otras, con la selección de usuarios *Bluetooth* para conectar periféricos a computadores y 802.11 para conectar el computador a una LAN de oficina.

La tecnología 802.11 también es más supcetible a las interferencias que *Bluetooth*. Por ejemplo los microondas generan la misma frecuencia de 2.4 GHz.y se ha demostrado que existe un mayor tráfico cuando dispositivos *Bluetooth* operan muy

[52] Siglas en inglés: "Direct-sequence Spread Spectrum (DSSS)"

cerca (pocos pies) del horno microondas. Claro que el problema puede ser resuelto separando al dispositivo *Bluetooth* del horno microonda cuando este esté operando. El problema con la red 802.11, es más difícil de resolver, porque la tecnología 802.11 no hace uso de los saltos de frecuencias, y esto es mucho mas vulnerable a interferencias que *Bluetooth* y *HomeRF*. Es probable que esta tecnología sea afectada por aparatos electrodomésticos y así como también por los dispositivos *Bluetooth* que operan en la banda de 2.4 GHz.

La compatibilidad es otro problema para la tecnología 802.11. Aparentemente las especificaciones de 802.11 puede interpretar diferentes especificaciones de diferentes fabricantes, por consiguiente las tarjeta de red construida por un fabricante puede no trabajar en una red 802.11 hecha por otro. Los pasos que se tienen que tomar para resolver este inconveniente son difíciles. La siguiente tabla muestra las ventajas y desventajas de la tecnología 802.11 en general, ya que existen dos estándares de 802.11, tanto el 802.11a y 802.11b.

**Tabla 4**
**Ventajas y desventaja de la tecnología 802.11**

| *Ventajas* | *Desventajas* |
|---|---|
| Velocidad. | Rango limitado. |
| Rapidez 11 Mbps. | Dificultad para integrarse con redes cableadas. |
| Conexiones confiables. | Muy costos y complejo para el uso casero. |
| Un amplio alcance. | Requiere de un punto de acceso físico. |
| Es barato. | Dificultad para configurarla y mantenerla. |
| Integración fácil con redes Ethernet | No tiene voz ni teléfono. |

Datos tomados de "*Bluetooth End to End*" (pág 265) por D.M Bakker y Diane Gilster, 2002, New York.

### 11.4 Limitaciones de *Bluetooth*

El alcance es una evidente limitación, cuando se usa esta tecnología para conectar redes LAN inalámbricas. *Bluetooth* no fue previsto inicialmente para LAN, pero son más y más los tipos de uso que se toman en consideración, hasta incluir a las LAN's. Sin embargo, las tecnologías 802.11/Wi-Fi y *HomeRF* fueron ambas diseñadas para LAN's inalámbricas, y estos estándares existentes tienen mucho más alcance que *Bluetooth*. El alcance de *HomeRF* es de 105 pies y el de 802.11 es de 300 pies, ambos significativamente mejores que los 33 pies de alcance de *Bluetooth*.

Quizás, la desventaja más grande que el alcance es la tasa de transferencia de información disponible en el ambiente *Bluetooth*. Teóricamente, la máxima tasa de transmisión de *Bluetooth* es de 1 Mbps. En la práctica, sin embargo la transmisión de información asimétrica está cerca de los 721 Kbps y en la transmisión simétrica es 432.6 Kbps.

La tasa de transmisión de IrDA es de 4 Mbps, la tasa de *HomeRF* es 10 Mbps, y la tasa de 802.11 es 11 Mbps. Está clara la desventaja de *Bluetooth* comparada con las tasas de transferencias de estas tecnologías.

La tasa de transferencia de *Bluetooth* es lo bastante rápida para muchas aplicaciones. Enviar los datos a las impresoras no necesita más de 400 o 700 Kbps y también esta tasa de transferencia es adecuada para recibir la información desde los teclados y ratones inalámbricos. Sin embargo, no es lo bastante rápido para enviar archivos largos desde un repositorio de datos a otro.

La tecnología *Bluetooth* no fue diseñada para LAN; la tecnología fue pensada para el reemplazo de cables y para crear redes *ad hoc* conectadas punto a punto (con esto

no se necesita saber la dirección de red del dispositivo). Para entrar en la LAN, la tasa de transferencia *Bluetooth* debe cambiar. Las tecnologías *HomeRF* y 802.11 escogen como van entregar la información a velocidades rápidas.

**Tabla 5**
**Comparación entre tecnologías inalámbricas.**

| *Tecnología.* | *Velocidad Máxima.* | *Alcance.* | *Tolerancia a la interferencia* | *Costo.* | *Propósito.* |
|---|---|---|---|---|---|
| *Bluetooth (RF)* | 1 Mbps | 30 pies | Media | Se quiere llegar a los 5 $, actualmente 15 $. | Reemplazo de cable. |
| IrDA | 4 Mbps | 3 pies | Ninguna. | 2 $. | Reemplazo de cable. |
| 802.11 | 11 Mbps. | 300 pies | Alta. | 100$ - 300$ | LAN´s corporativas o campus. |
| 802.15 | 1 Mbps. | 30 pies | Media | Bajo | Reemplazo de cable. |

Datos tomados de "*Bluetooth End to End*" (pág 266) por D.M Bakker y Diane Gilster, 2002, New York.

Lo que se necesita es una solución inalámbrica económica que sea cómoda y, fiable, fácil de usar y que funcione a una distancia mayor que los infrarrojos. Y *Bluetooth* es una especificación global para dispositivos de comunicaciones y redes de bajo costo y pequeño formato entre computadoras portátiles, PCs, teléfonos celulares; eliminando el uso de cables. Para más información de redes inalámbricas ver apéndice E.

# CAPITULO II

# METODOLOGIA

Para poder resolver los problemas reales, los equipos de trabajo deben incorporar una estrategia de desarrollo. Todo desarrollo del software se puede caracterizar como un bucle de resolución de problemas. En el que se encuentran cuatro etapas distintas: *status quo*, definición de los problemas, desarrollo técnico e integración de soluciones. *Status quo*, representa en el estado actual de los sucesos; la definición de problemas, identifica el problema específico a resolver; el desarrollo técnico resuelve el problema a través de la aplicación de tecnología, y la integración de soluciones ofrece los resultados. Estos son las etapas básicas en las que se divide el desarrollo de soluciones. Existen diferentes modelos de procesos para la ingeniería del software, como (a) Prototipo, (b) Espiral, (c) Reutilización, (d) Cascada, etc. La estructura utilizada para el desarrollo de este Trabajo Especial de Grado es una adaptación del Modelo Lineal Secuencial, llamado algunas veces ciclo de vida o modelo cascada, esto sugiere un enfoque secuencial, aunque el modelo usado puede hacer uso de bucles de retroalimentación, y este modelo no es estrictamente secuencial.

Aunque se usa esta adaptación, también se puede apreciar que hay una influencia de otros modelos, como por ejemplo se analizaron los riesgos de sólo poseer dos dispositivos para ser utilizados por dos grupos, esto forma parte del modelo Espiral. Con respecto al modelo de reutilización, el trabajo se basa en ciertos requerimientos

mínimos que debe poseer un punto de acceso para dispositivos *Bluetooth,* establecido por el SIG, esto es reutilización de información. Para poder apreciar mejor la estructura, es preciso ver la figura siguiente.

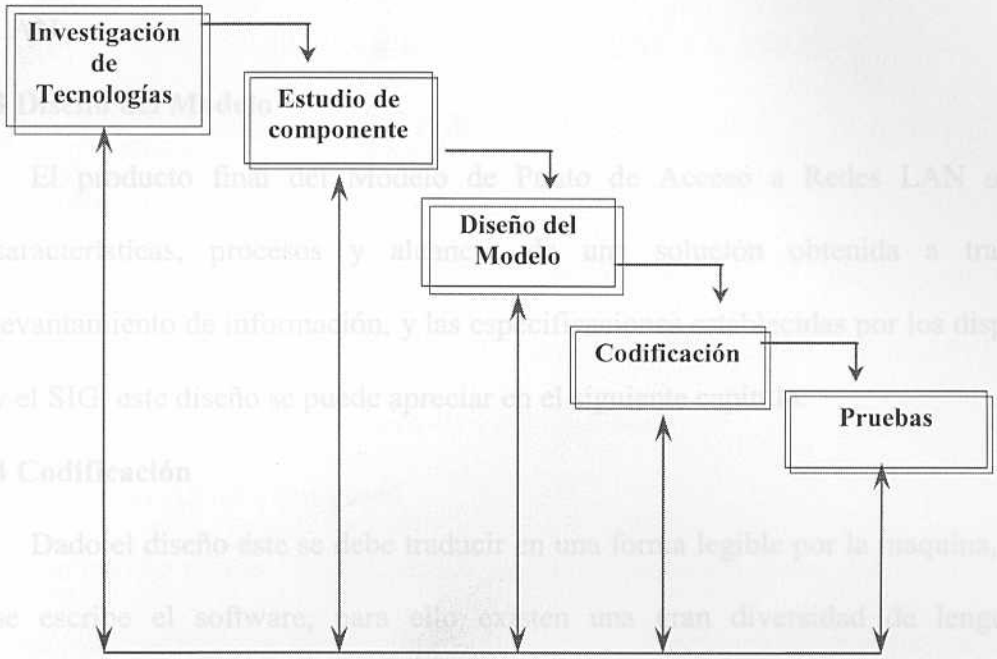


**Figura 12 Estructura de Trabajo.**

## 1 Investigación de tecnología

Es la manera de cómo obtener la información necesaria para una investigación exhaustiva sobre el trabajo a realizar; entre las fuentes de información que se pueden encontrar están: libros, revistas, foros, trabajo de grados, los perfiles y especificaciones realizado por el SIG, periódicos, *papers, etc.* Y la utilización de Internet como un medio para acceder a la información, así como también bibliotecas, etc.

**2 Estudio de Componentes**

Es la investigación sobre todos los requerimientos tanto de hardware, software, laboratorios, y equipos necesarios para la realización del modelo de Punto de Acceso LAN.

**3 Diseño del Modelo**

El producto final del Modelo de Punto de Acceso a Redes LAN serán las características, procesos y alcances de una solución obtenida a través del levantamiento de información, y las especificaciones establecidas por los dispositivos y el SIG, este diseño se puede apreciar en el siguiente capítulo.

**4 Codificación**

Dado el diseño este se debe traducir en una forma legible por la maquina, es decir se escribe el software, para ello existen una gran diversidad de lenguajes de programación.

**5 Pruebas**

Una vez que se ha generado un código, comienzan las pruebas del programa. El proceso de pruebas se centra en los procesos lógicos internos del software, asegurando que todas las sentencias se han comprobado. Realizar pruebas para la detección de errores y sentirse seguro de que se obtienen los resultados que en la realidad se obtendrían.

Por lo tanto esta estructura deja abierta la posibilidad de usar características de otros modelos para la consecución del objetivo de este Trabajo Especial de Grado.

# CAPITULO III

# DESARROLLO Y RESULTADOS

Para la realización de este Trabajo Especial de Grado se planteó una serie de objetivos, así como también se estableció una estructura de trabajo, referida en el capítulo anterior, que tiene como base el modelo de ciclo de vida llamado Cascada, para la consecución del trabajo se realizó una serie de tareas en cada una de las etapas del ciclo de vida, como se menciona a continuación:

## 1 Investigación de Tecnología

Para poder obtener la información sobre la tecnología *Bluetooth*, fue necesario la búsqueda en diversas fuentes de información, una de estas fuentes son las empresas que forman parte del SIG, ya que estas compañías son las que establecieron y rigen las especificaciones de esta tecnología. Por lo tanto se consultó y se bajó información de la pagina web http://www.ericsson.com/bluetooth, así como de otras páginas, y se obtuvo de ellas los documentos de los perfiles y especificaciones *Bluetooth*.

Se adquirieron tres libros sobre la tecnología *Bluetooth*, que complementaron la información que aparece en los perfiles y especificaciones. Se consultaron ciertos RFC (*Request For Coments*) como: 1661, 1662,1332, 0791, etc.

Así se logró tener respuestas a una serie de preguntas como las siguientes: ¿Qué es *Bluetooth?* , ¿Para qué sirve?, su topología, su funcionamiento, capacidades, comparaciones con otras tecnología (802.11, *HomeRF*, Infrarrojo), referencia con el

Modelo OSI, la seguridad en *Bluetooth,* entre otras. Todas ellas se encuentran respondidas en el capítulo I y en los apéndices.

## 2 Estudio de componentes

Al haber investigado sobre la tecnología *Bluetooth*, redes inalámbricas y ciertos modelos (OSI) y protocolos de comunicación (TCP, IP, PPP), era necesario establecer todos los requerimientos tanto de software y hardware para la realización de este trabajo. La empresa Ericsson de Venezuela donó los dos *kits Bluetooth*, indispensables para la realización del proyecto, específicamente *The Bluetooth Development Kit* y *Bluetooth Application Kit*[53].

Dado que el trabajo necesitaba la existencia de una red LAN cableada, para poder acceder a los servicios que ofrece esta red, se conformó una red *ethernet* con cuatro computadores, de la cuales dos, pertenecientes a este proyecto, se le instalaron *Linux Red Hat* 7.3, las otras dos computadoras funcionan bajo *Windows*, se usó un *Hub* marca C-Net de 8 puertos, cables, etc.

Como herramientas de desarrollo se eligió C++ y la pila de librerías *BlueZ* para dispositivos *Bluetooth* bajo *Linux*. Las razones que llevaron a escoger C++ como lenguaje de programación es que la librería *BlueZ* es para dicho lenguaje de programación, con respecto a *BlueZ,* este se eligió ya que es una de las librerías para desarrollo más completas, gratuita, se ofrece amplia ayuda en foros, existen listas de distribución para los desarrolladores que utilizan esta librería; además el propio sistema operativo *Linux* dado sus características abiertas ofrecía ciertas ventajas, tal

[53] Las especificaciones y características de estos dispositivos se encuentran en los Anexos A y B, respectivamente.

como acceso al código fuente de secciones del sistema operativo necesarios para el desarrollo.

## 3 Diseño del Modelo

Al finalizar las fases de Investigación de las Tecnologías y Estudio de los Componentes se procede al Diseño del Modelo, se determinaron los componentes de software necesarios y como debían ser implementados estos para su correcto funcionamiento e interoperabilidad según los estándares definidos por la industria.

De estos estudios surge nuestro Modelo de Punto de Acceso a Redes LAN llamado **BlueLAP**, este modelo sigue las siguientes características:

### 3.1 Descripción General del Punto de Acceso

El modelo de Punto de Acceso **BlueLAP** surge luego de realizar una ardua investigación de la tecnología *Bluetooth*, sus características y sus especificaciones. Este estudio permitió establecer cada uno de los componentes necesarios para el Punto de Acceso, estos componentes se dividen en dos grandes grupos: componentes para el DT y componentes para el LAP. Por ello a lo largo de la descripción del modelo podrán observar que siempre se exponen tanto los requerimientos para el LAP como los requerimientos para el DT.

Este Punto de Acceso fue ideado para funcionar como un componente adicional para un PC o servidor conectado a una LAN y convertirlo en un Punto de Acceso a dicha LAN y a sus recursos para los dispositivos *Bluetooth* que se encuentren en el rango de cobertura.

Este modelo expone a continuación de forma estructurada los requerimientos con los que se debe cumplir en cualquier implementación **BlueLAP** para funcionar como un Punto de Acceso compatible con cualquier dispositivo *Bluetooth*.

### 3.1.1 Pila del Protocolo.

Este modelo contempla una serie de protocolos para asegurar la interoperabilidad entre cualquier dispositivo con tecnología *Bluetooth*. La utilización de esta pila de protocolos es obligatoria para cualquier modelo de Punto de Acceso a redes LAN utilizando tecnología *Bluetooth* según las especificaciones del SIG. La siguiente figura muestra los protocolos y entidades utilizadas en este punto de acceso.

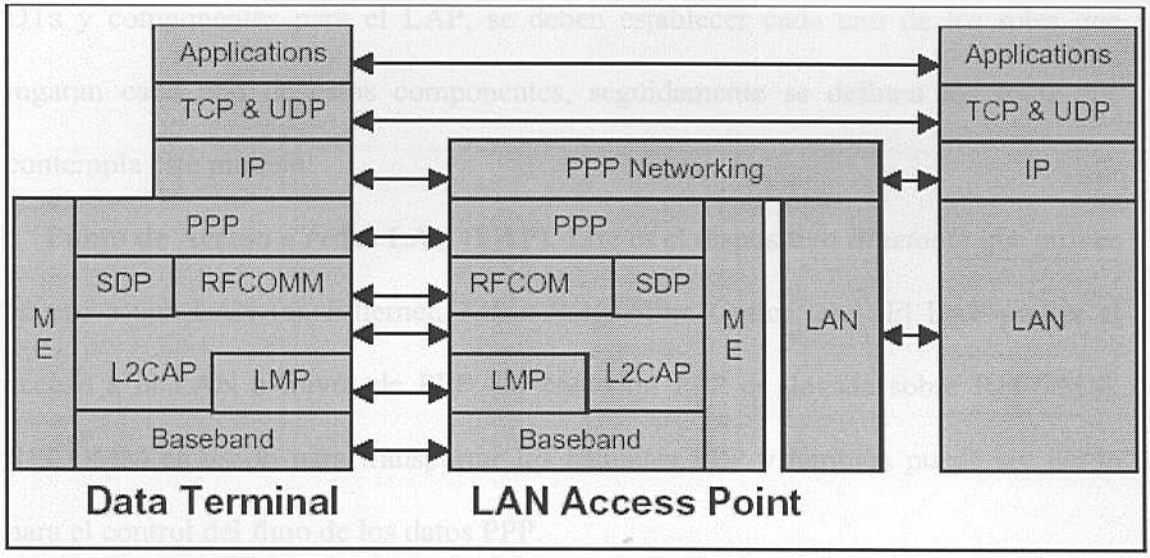


**Figura 13 Pila de Protocolo.** Tomado de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles*. [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]

PPP es el protocolo Punto-a-Punto de la IETF. PPP toma los paquetes IP desde/hacia la capa PPP y los pone dentro de la LAN. Este mecanismo no está definido en este modelo pero es una característica bien conocida de los productos de acceso remoto.

La banda base, LMP y L2CAP son las capas OSI 1 y 2 de los protocolos *Bluetooth*. RFCOMM es la adaptación del GSM TS 07.10 para *Bluetooth*. SDP es el protocolo de Descubrimiento de Servicios.

El ME es la Entidad Administradora que coordina los procedimientos durante la inicialización, configuración y conexión. Es la parte principal de la implementación, sobre la Entidad Administradora recae todo el trabajo de proporcionar el servicio del LAP a los DTs que lo requieran.

### 3.1.2 Configuraciones y Roles

Como fue explicado anteriormente este modelo contempla componentes para los DTs y componentes para el LAP, se deben establecer cada uno de los roles que jugaran cada uno de estos componentes, seguidamente se definen los roles que contempla este modelo:

**Punto de Acceso a redes LAN (LAP).** Este es el dispositivo *Bluetooth* que provee acceso a una LAN (ej. Ethernet, *Token Ring*, Fibra Óptica, etc). El LAP provee el acceso a la LAN a través de PPP. La conexión PPP es llevada sobre RFCOMM. RFCOMM es usado para transportar los paquetes PPP y también puede ser usado para el control del flujo de los datos PPP.

**Terminal de Datos (DT).** Este es el dispositivo que utiliza los servicios del LAP. Los dispositivos que típicamente actúan como terminales de datos son: *Laptops*, PCs y PDAs. Los DT son clientes PPP. Establecen una conexión PPP con un LAP para ganar acceso a una LAN.

Se asume que tanto el LAP como los DT tienen cada uno un dispositivo *Bluetooth*[54].

### 3.1.3 Requerimientos de Usuario y Escenarios

Este modelo cubre necesidades determinadas para un tipo de usuario y unos escenarios dados. Los siguientes escenarios están cubiertos por este modelo de Punto de Acceso:

(1) **Un DT utiliza un LAP** como una manera inalámbrica de conectarse a una red de área local (LAN). Una vez conectado, el DT puede operar como si se conectara a la LAN mediante una conexión de acceso telefónico a redes. El DT podrá acceder a todos los servicios provistos por la LAN. Este escenario se presenta cuando el DT debe utilizar el LAP como usuario único.

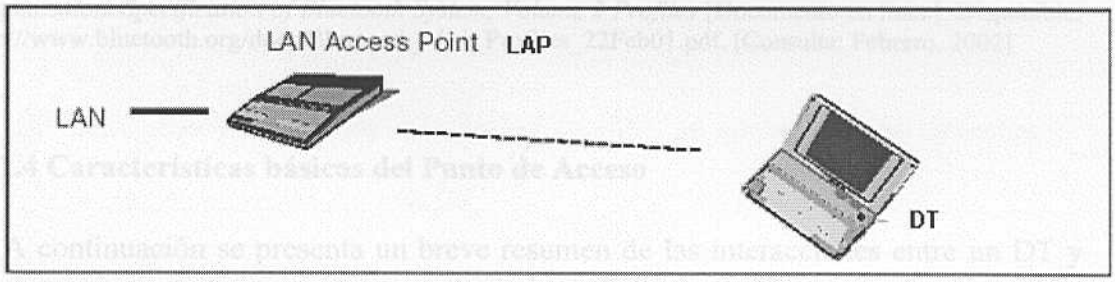


**Figura 14 Acceso a la LAN desde un solo terminal Bluetooth.** Tomado de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles* [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]

(2) **Múltiples DTs usan un LAP** como una manera inalámbrica para conectarse a una red de área local (LAN). Una vez conectado, los DTs pueden operar como si se conectarán a la LAN mediante una conexión de acceso telefónico a redes. Los DTs podrán acceder a todos los servicios

[54] Los roles de LAP y DT se pueden adoptar independientemente del dispositivo.

provistos por la LAN. Los DTs también podrán comunicarse entre si a través del LAP[55].

Las configuraciones necesarias para acceder a otras redes, por ejemplo Internet, son independientes del LAP. Una vez establecida la conexión con el LAP se podrán configurar clientes *proxy, gateways*, etc. Si fuera necesario.

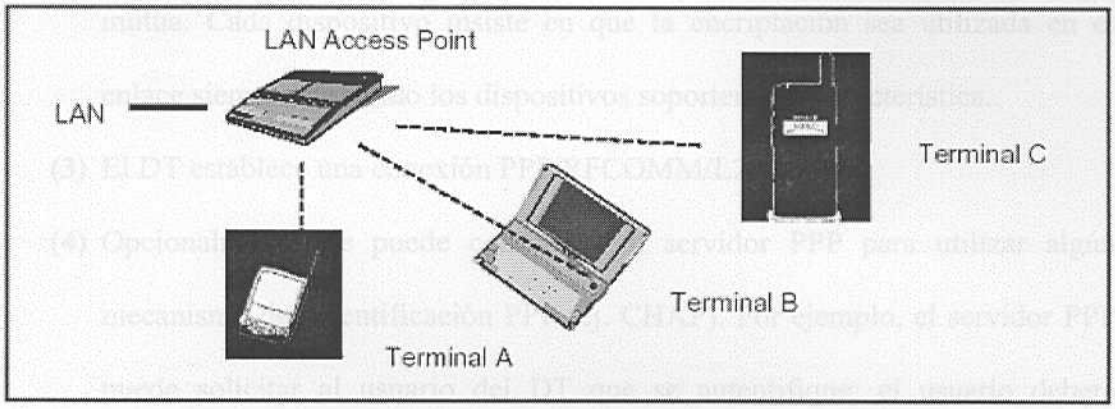


**Figura 15 Acceso a la LAN desde múltiples terminales Bluetooth.** Tomado de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles* [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]

### 3.1.4 Características básicas del Punto de Acceso

A continuación se presenta un breve resumen de las interacciones entre un DT y un LAP para iniciar el servicio de Punto de Acceso a un cliente que lo requiera. Más adelante, en este documento se detallan cada uno de los siguientes pasos:

**(1)** El primer paso es encontrar un LAP que esté dentro del rango del radio y que provea los servicios de PPP/RFCOMM/L2CAP. A la aplicación cliente en el DT se le debe indicar la dirección *Bluetooth* del LAP a conectar, si ésta no es

[55] Los DTs podrán comunicarse entre si solo si los servicios requeridos (ej. DNS) están disponibles en la LAN.

indicada, el cliente buscará dispositivos LAP en rango y conectará con el que aporte mayor disponibilidad.

(2) Si no existe el enlace físico de la banda base, entonces el DT solicita establecer el enlace con el LAP seleccionado. En este punto después del establecimiento del enlace físico, los dispositivos realizan autentificación mutua. Cada dispositivo insiste en que la encriptación sea utilizada en el enlace siempre y cuando los dispositivos soporten esta característica.

(3) El DT establece una conexión PPP/RFCOMM/L2CAP.

(4) Opcionalmente, se puede configurar el servidor PPP para utilizar algún mecanismo de autentificación PPP (ej. CHAP). Por ejemplo, el servidor PPP puede solicitar al usuario del DT que se autentifique; el usuario deberá proporcionar su nombre de usuario y contraseña. Si este mecanismo es usado y el DT falla en autentificarse, entonces el enlace PPP deberá cancelarse.

(5) Utilizando mecanismos apropiados de PPP, se negociará una dirección IP apropiada entre el LAP y el DT.

(6) El tráfico IP podrá fluir a través de la conexión PPP ahora.

(7) En cualquier momento el DT ó el LAP podrán terminar la conexión PPP.

## 3.2 Aspectos de la Interfase con el Usuario

### 3.2.1 Seguridad

Es reconocido que la seguridad en un ambiente inalámbrico es de gran importancia.

Tanto el LAP como el DT deben forzar que la encriptación esté operando en el enlace físico de la banda base mientras cualquier trafico PPP esté siendo enviado o recibido, si los dispositivos soportan las características de encriptación y autentificación. Una vez establecida la encriptación, el LAP rechazará cualquier petición de DTs que quieran desactivar la encriptación.

Adicionalmente, el emparejamiento *Bluetooth*[56] debe ocurrir como una manera de autentificación de usuarios. Un PIN o clave de enlace debe ser proporcionada, aunque se esté usando el PIN por defecto. El PIN por defecto para el acceso a LAN es un *byte* con todos los bits en 0. La falla para completar el proceso de emparejamiento prevendrá el acceso al servicio del LAP.

Se asume que el LAP puede ser físicamente localizado en un lugar donde usuarios no autorizados no puedan manipularlo o que el LAP tenga algún mecanismo de seguridad que prevenga los accesos no autorizados. Un típico DT-LAP (escenario 1 ó 2) la configuración se muestra en la figura 16.

Es importante proveer la protección básica para la transmisión *Bluetooth*. Esto requiere que la interfaz de aire sea segura así como la conexión al LAP. Por lo tanto la banda base de *Bluetooth* puede proteger el enlace con la autentificación y el cifrado. Para instalar un enlace hay que asegurar las conexiones, el LAP y DT necesitan almacenar las claves necesarias. La clave de enlace *Bluetooth* es conveniente para estos propósitos.

[56] Ver concepto en el apéndice B

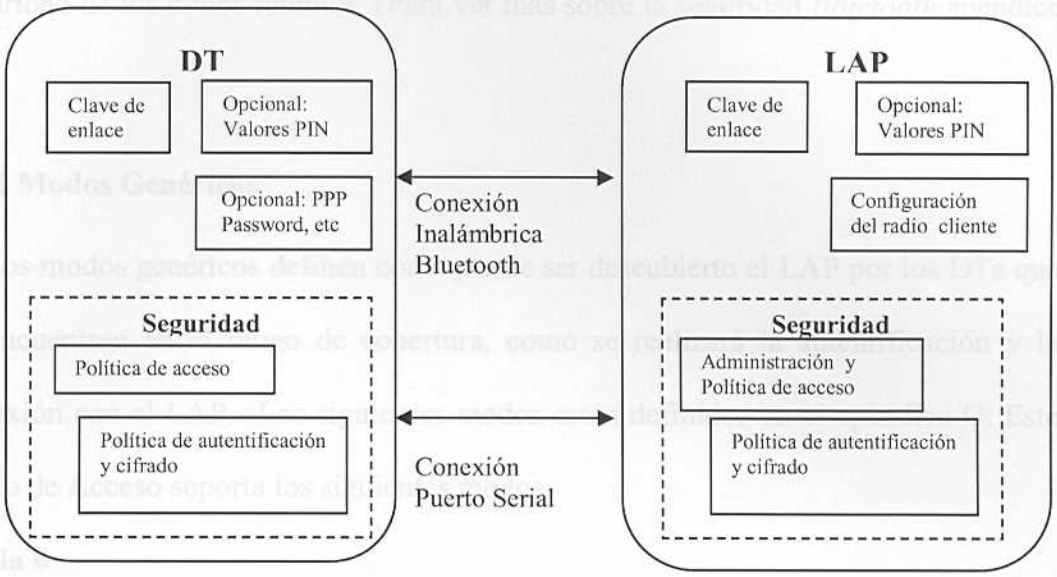


**Figura 16 Arquitectura de seguridad para los escenarios DT-LAP.** Tomado de Bluetooth SIG Security Expert Group. *Bluetooth Security White Paper,* pág 26 por Cristian Gehrmann, 2002

El LAP puede ser administrado por una interfaz de usuario *web*, el administrador del servidor donde esté instalado el LAP deberá realizar todas las configuraciones necesarias para asegurar que sólo los usuarios autorizados tengan acceso a las configuraciones del LAP. Esto es importante para asegurar que sólo los usuarios autorizados son permitidos para el cambio de las configuraciones y especialmente las configuraciones de seguridad del LAP. Por ejemplo un usuario puede ser forzado a introducir un código de acceso antes que a él o ella se le permita realizar cualquier función de administrador en el LAP. El LAP puede también ser controlado de forma remota. La administración de la seguridad de un nodo remoto es una tarea larga, pero existen diferentes soluciones. La preferencia de alguna solución depende de la estructura de la LAN. Por ejemplo SNMPv3 incluye posibilidades de administrar la

seguridad de los nodos remotos. (Para ver más sobre la seguridad *Bluetooth* apéndice F).

### 3.2.2 Modos Genéricos

Los modos genéricos definen como puede ser descubierto el LAP por los DTs que se encuentren en el rango de cobertura, como se realizará la autentificación y la conexión con el LAP. Los siguientes modos están definidos en el apéndice G. Este Punto de Acceso soporta los siguientes modos:

**Tabla 6**
**Tabla de requerimientos de los modos genéricos**

| *Modos* | *Soportado en LAP* |
|---|---|
| **Modos de Descubrimiento** | |
| Modo no-descubrible | SI |
| Modo descubrible general | SI |
| **Modos de Conectabilidad** | |
| Modo no-conectable | SI |
| Modo conectable | SI |
| **Modos de Emparejamiento** | |
| Modo no-emparejable | SI |
| Modo emparejable | SI |

Datos tomados de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles* [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]

Notas:

(1) Un uso típico del modo no-descubrible es cuando el LAP es para uso personal solamente. El DT debe recordar la identidad del LAP y nunca necesitar usar los mecanismos de búsqueda de *Bluetooth*.

(2) Un uso típico del modo descubrible general es cuando el LAP es para uso general. El DT no deberá recordar la identidad de todos los LAPs que utilice.

El DT utilizará los mecanismos de búsqueda de *Bluetooth* para descubrir los LAPs en rango.

### 3.2.3 Parámetros Adicionales

Adicionalmente a las configuraciones de los Modos Genéricos, se deben establecer la cantidad de usuarios simultáneos que pueden tener acceso al LAP. Esto como manera de poder cumplir con los escenarios establecidos para este modelo y para garantizar cotas de funcionamiento mínimos según los recursos disponibles en el LAP. Estos parámetros pueden ser configurados por el administrador del LAP:

**3.2.3.1 Máximo número de usuarios:** Según las limitaciones de recursos y capacidad de los dispositivos se puede limitar el número de usuarios simultáneos que se soporten. El administrador del LAP puede escoger el número de usuarios simultáneos a limitar[57].

- **Modo único-usuario:** Es cuando el máximo número de usuarios está configurado para permitir sólo un usuario. En este modo, tanto el DT como el LAP pueden ser el maestro de una *piconet*. El modo de usuario-único trata que un único usuario tenga acceso exclusivo al LAP[58].
- **Modo multi-usuario:** Es cuando el máximo número de usuarios está configurado para permitir más de un usuario. En este modo, el LAP debe ser

[57] A menor cantidad de usuarios simultáneos usando el radio *Bluetooth*, más ancho de banda disponible para cada uno. Un LAP puede ser restringido a un sólo usuario.

[58] Esta es una situación en donde el DT quiera conectarse al LAP y permanecer como el maestro de una *piconet* existente. Por ejemplo, un PC es el maestro de una *piconet* con conexiones a un ratón y un video proyector *Bluetooth*. El PC requiere una conexión al LAP, pero debe mantenerse como maestro de la *piconet*, entonces el LAP debe ser un esclavo de la *piconet*. Esta situación es sólo posible si el parámetro del máximo número de usuarios del LAP esta configurado en 1.

- siempre el maestro de la *piconet*. Si el DT no permite al LAP convertirse en el maestro de la *piconet*, entonces el DT no puede ganar acceso al LAP.

### 3.3 Capa de Aplicación

La Capa de Aplicación esta encargada de cumplir con los procedimientos necesarios para iniciar el servicio y configurar el LAP y que este listo para su funcionamiento. La siguiente tabla define los requerimientos que cumple este modelo en Capa de Aplicación:

**Tabla 7**
**Tabla de requerimientos de la capa de aplicación**

| *Característica* | *Soportado en LAP* | *Soportado en DT* |
|---|---|---|
| Inicialización del servicio de acceso a la LAN | SI | N/A |
| Finalización del servicio de acceso a la LAN | SI | N/A |
| Establecimiento de la conexión a la LAN | N/A | SI |
| Desconexión de la LAN | SI | SI |

Datos tomados de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles* [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]

### 3.1 Inicialización del Servicio de Punto de Acceso a una LAN

Este procedimiento inicializa la configuración del dispositivo como un LAP. Esta operación envuelve la configuración de los siguientes parámetros:

- Todos los parámetros configurables definidos anteriormente. (por ejemplo, máximo número de usuarios, modos de descubrimiento, etc.).
- Los PINs y/ó claves de enlace *Bluetooth* requeridos.

- Cualquier opción de configuración PPP apropiada (ej. Autentificación, compresión) puede ser configurada. En orden de asegurar la interoperabilidad, un LAP no debe requerir que los DTs realicen ninguna autentificación PPP, a menos que el administrador halla configurado la autentificación PPP en el servidor PPP.

El procedimiento expuesto anteriormente es el primer paso a realizar al iniciar el servicio del LAP. Cuando la inicialización esté completa, el dispositivo estará capacitado para aceptar conexiones PPP.

### 3.3.2 Finalización del Servicio de Punto de Acceso a una LAN

Este procedimiento detiene la actuación como LAP del dispositivo:

- Se finaliza el servidor PPP, se define la sección 3.4.2
- Se previene que dispositivos *Bluetooth* no autorizados accedan posteriormente eliminando las claves de enlace guardadas.

El procedimiento de finalización del servicio de Punto de Acceso se procede a realizar cuando se ha decidido detener el funcionamiento del LAP.

### 3.3.3 Establecimiento de la Conexión a la LAN

Normalmente el DT podrá iniciar el establecimiento de una conexión a la LAN:

**(1)** El primer paso es seleccionar un LAP apropiado que provea el servicio de PPP/RFCOMM. Esta selección se puede realizar de la siguiente manera:

- Se espera a que el usuario indique la dirección *Bluetooth* del dispositivo al que se quiera conectar, en caso de no ser indicada dicha dirección, el cliente

DT buscará los dispositivos de clase LAP en el rango y conectará a los dispositivos que ofrezca mayor disponibilidad. El resultado del proceso de selección debe ser un LAP que esté dentro del rango del radio y que el servicio provisto sea PPP/RFCOMM.

Los mecanismos del Servicio de Descubrimiento *Bluetooth* son utilizados para obtener la información. Este servicio de información provee toda la información requerida para crear la conexión RFCOMM.

**(2)** Opcionalmente, si se configura la solicitud de PIN en el LAP, el usuario del DT (ó la aplicación) tiene permitido proporcionar un PIN de autentificación *Bluetooth* o una clave de enlace por la aplicación. Si no se proporciona un PIN, entonces se utiliza un PIN de longitud cero.

**(3)** Opcionalmente, si se configura el servidor PPP para solicitar autentificación, el usuario del DT (o la aplicación) podría proporcionar un nombre de usuario y contraseña para la autentificación PPP. Si algún mecanismo de autentificación PPP está siendo usado y el usuario inicialmente no proporciona su nombre de usuario y contraseña, entonces deberá proporcionarlo posteriormente en el establecimiento de la conexión.

**(4)** Cuando el usuario (ó la aplicación) activen la conexión, entonces una aplicación PPP es iniciada, para intentar establecer una conexión al punto de acceso seleccionado.

Este procedimiento es utilizado por el DT que quiera establecer una conexión con la LAN a través del Punto de Acceso. Es un procedimiento estándar que debe cumplir cualquier tipo de dispositivo que desee establecer conexión con un Punto de Acceso

*Bluetooth*. Este modelo permite la interoperabilidad con clientes DT **BlueLAP** como con cualquier otro dispositivo *Bluetooth* que cumpla con las especificaciones del SIG.

### 3.3.4 Desconexión de la LAN

Tanto el LAP como el DT pueden terminar la conexión a la LAN en cualquier momento usando los procedimientos de la desconexión de PPP. Detener el funcionamiento del LAP causaría de forma inmediata la desconexión de la LAN a cualquier DT conectado en ese momento. Cancelar la conexión de un DT, automáticamente genera la desconexión PPP para ese DT en el LAP.

## 3.4 PPP

PPP puede comenzar a trabajar tan pronto el enlace RFCOMM y el puerto serial virtual respectivo se hayan establecido. El LAP exporta una interfaz de Servidor PPP. El servidor PPP utilizará este puerto serial virtual para utilizarlo como vía para iniciar la sesión PPP. Este modelo de LAP plantea un tipo de *proxy* PPP, donde los paquetes PPP son transferidos desde/hacia un Servidor PPP en algún lugar de la red.

La siguiente tabla, junto con las sub-cláusulas asociadas, definen los requerimientos mandatorios que cumple este Punto de Acceso.

**Tabla 8**
**Capacidades del PPP**

| *Procedimiento* | *Soportado en LAP* | *Soportado en DT* |
|---|---|---|
| Inicialización del PPP | SI | N/A |
| Finalización del PPP | SI | N/A |
| Establecimiento de la conexión PPP | SI | SI |
| Desconexión del PPP | SI | SI |

Datos tomados de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles* [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]

### 3.4.1 Inicialización del PPP

Sobre el LAP, la existencia de un Servidor PPP se registra en la base de datos del Servicio de Descubrimiento (ver 3.6.1).

Un dispositivo en el rol de DT no registra PPP en la base de datos del Servicio de Descubrimiento. Como sea, es posible para un dispositivo ser tanto un LAP como un DT; por lo tanto el dispositivo puede registrar PPP en la base de datos del Servicio de Descubrimiento como se definió arriba.

PPP es un protocolo orientado a paquetes, mientras que RFCOMM espera flujos de datos seriales. Por lo tanto, la capa PPP debe utilizar los mecanismos de serialización adecuados.

La inicialización del servidor PPP deberá ocurrir una vez se hallan levantado los servicios L2CAP/RFCOMM entre DT y LAP y se hallan establecido los puertos seriales virtuales tanto en el DT como en el LAP. Se utilizará algún servidor PPP que se encuentre en la LAN y la configuración de dicho servidor PPP deberá correr por cuenta del administrador de la LAN. El funcionamiento del servidor PPP es totalmente externo al LAP.

### 3.4.2 Finalización del PPP

Al detener el funcionamiento del LAP se deben detener todas las conexiones PPP que se encuentren activas. Esto se debe realizar utilizando los métodos de finalización propios de PPP.

La capa PPP deshabilita ó remueve el servicio PPP de la base de datos del Servicio de Descubrimiento (SDP).

### 3.4.3 Establecimiento de la Conexión PPP

Si no existe una sesión RFCOMM entre el LAP y el DT, entonces el dispositivo debe inicializar primero una sesión RFCOMM. El dispositivo debe obtener el canal del Servidor RFCOMM a usar desde el servicio de información (SDP) descubierto recientemente.

Usando el Protocolo de Control de Enlace (LCP), el LAP y el DT negociarán el enlace PPP.

Parte del LCP es la negociación de la Unidad Máxima de Transmisión (MTU) a usar en el enlace PPP, ver RFC 1661 para mayor información[59].

Dependiendo de las capacidades y configuraciones, el LAP podría tener múltiples sesiones PPP operando simultáneamente.

Una vez establecida la conexión PPP y negociada la dirección IP respectiva, se puede empezar a utilizar la conexión con la LAN.

### 3.4.4 Desconexión del PPP

Las siguientes razones podrían ser causas de la terminación de una conexión PPP:

**(1)** Intervención del usuario.

**(2)** Falla en la conexión RFCOMM/L2CAP. La conexión RFCOMM/L2CAP podría fallar por muchas razones. Por ejemplo, cuando el enlace de radio ha fallado o el dispositivo ha salido del rango por una cantidad excesiva de tiempo.

[59] Algunos LAPs pueden usar el proceso de negociación LCP para insistir sobre valores específicos para el MTU. Por ejemplo, un LAP con una conexión Ethernet podría desear tener un MTU apropiado, así los paquetes IP no requerirían fragmentación cuando sean transmitidos desde *Bluetooth* a Ethernet.

**(3)** Terminación por parte del LAP, si el punto de acceso no puede proveer el servicio apropiado. La razones que pueden causar esto pueden incluir: (a) detección de direcciones IP duplicadas, (b) pérdida de la conexión con la LAN, (c) pérdida de la conectividad con el servidor PPP, o (d) pérdida de la conexión con la subred IP requerida.

PPP maneja cada una de las situaciones anteriores de forma diferente. Las razones 1 y 3 resultan en una desconexión controlada en cada capa del protocolo. La razón 2 requiere un procesamiento diferente. Se podría o tratar de recuperar la conexión L2CAP/RFCOMM y en caso de no poder recuperarla terminar de forma definitivamente la conexión con el DT.

Cuando la conexión PPP es terminada, tanto por intervención del usuario como automáticamente por el LAP, entonces la capa PPP toma los siguientes pasos:

**(1)** Terminar las conexiones IPCP[60] (como se define en el RFC 1332). Esto causará que la interfaz IP sea deshabilitada.

**(2)** Terminar las conexiones LCP (como se define en el RFC 1661)

**(3)** Terminar las conexiones RFCOMM.

Cuando la conexión RFCOMM/L2CAP sea terminada de forma inesperada, la capa PPP deberá seguir los siguientes pasos:

**(1)** Terminar las conexiones IPCP (como se define en RFC 1332). Esto causará que se deshabilite la interfase IP.

**(2)** Terminar las conexiones LCP (como se define en RFC 1661).

[60] Siglas en inglés:"IP Control Protocol (IPCP)"

### 3.4.5 Protocolos de Autentificación PPP

Opcionalmente, el servidor PPP puede ser configurado para usar uno o más protocolos de autentificación PPP. Estos protocolos permiten al administrador de la red controlar el acceso a la red. El uso de estos protocolos PPP no forman parte de este diseño. Son mencionados como información solamente.

PPP soporta un variado número de protocolos de autentificación, incluyendo los siguientes:

- PPP *Challenge Handshake Authentication Protocol* (CHAP) RFC 1994.
- Microsoft PPP CHAP *Extensions* RFC 2433.
- PPP *Authentication* RFC 2433.
- PPP *Extensible Authentication Protocol* RFC 2433.

Típicamente, el usuario debe proporcionar un nombre de usuario y una contraseña en orden de ganar autorización para usar la conexión PPP. Si la autentificación falla, entonces la conexión PPP es terminada normalmente.

Los protocolos de autentificación PPP son independientes de los mecanismos de autentificación *Bluetooth*. Un administrador de red puede escoger usar cualquier combinación de mecanismos PPP y *Bluetooth*.

## 3.5 RFCOMM

Este modelo debe adoptar todos los requerimientos especificados en el apéndice H (Requerimientos de Interoperabilidad de RFCOMM).

Adicionalmente:

Como se ha definido en el *Specification of the Bluetooth System Core, RFCOMM with TS 07.10* la velocidad de la conexión RFCOMM no es configurable por el usuario. RFCOMM transmitirá los datos tan rápido como pueda. La tasa de transferencia actual puede variar, dependiendo de otro tráfico *Bluetooth* en el enlace banda base. En particular, la velocidad de conexión no será forzada artificialmente con algún valor típico de puerto serial; ej. 19200 bps.

### 3.6 Servicio de Descubrimiento

Como se mencionó en el Capítulo I (ver sección 8), el Servicio de Descubrimiento (SDP) es utilizado para dar a conocer los servicios que provee un dispositivo *Bluetooth*. Este modelo, siguiendo con las especificaciones del SIG utiliza el Servicio de Descubrimiento para dar a conocer a cualquier DT los servicios que provee el LAP. La utilización del Servicio de Descubrimiento por parte de este modelo se explica a continuación:

#### 3.6.1 Registros del servicio de SDP

Cada LAP puede proveer una Clase de Servicio para los servicios PPP/RFCOMM. Adicionalmente un dispositivo *Bluetooth* puede funcionar como LAP y como algún otro tipo de proveedor de servicios; ej. Acceso a múltiples subredes y servicios de fax.

Donde el punto de acceso provea más de un servicio PPP/RFCOMM, la selección del servicio estará basado sobre los atributos del servicio. Todos estos servicios son hechos públicos vía el SDP los DT deberán consultar la base de datos de SDP para obtener la información del los servicios disponibles.

**Tabla 9**
**Parámetros Servicio de Descubrimiento**

| *Item* | *Definición* | *Mand. /Opc.* | *Tipo* | *Valor* | *Valor por defecto* |
|---|---|---|---|---|---|
| ServiceClassIDList | | Mand. | | | |
| ServiceClass0 | UUID para "Acceso LAN usando PPP" | Mand. | UUID | Ver [61] | Ver [51] |
| ProtocolDescriptorList | | Mand. | | | |
| Protocol0 | UUID para el protocolo L2CAP | Mand. | UUID | Ver [51] | Ver [51] |
| Protocol1 | UUID para el protocolo RFCOMM | Mand. | UUID | Ver [51] | Ver [51] |
| Parameter0 | Canal del servidor | Mand. | UInt8 | Varía | Varía |
| ProfileDescriptorList | | Optc. | | | |
| Profile #0 | UUID para "Acceso LAN usando PPP" | | UUID | Ver [51] | Ver [51] |
| Parameter0 | Versión "1.00" | | UInt16 | 0x0100 | 0x0100 |
| ServiceName | Nombre desplegable | Opc. | String | Configurable | "Acceso LAN usando PPP" |
| ServiceDescription | Informacion desplegable | Opc. | String | Configurable | "Aceso LAN usando PPP" |
| ServiceAvailability | Factor de carga | Opc. | Uint8 | Dinámico | Dinámico |
| IpSubnet | Información desplegable | Opc. | String | Configurable | Configurable |

Datos tomados de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles* [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]

Los valores actuales para los IDs de los atributos universales están definidos en la especificación de Números Asignados (Ver http://www.bluetooth.org/assigned-numbers.htm).

[61] Estos valores se encuentran en: http://www.bluetooth.org/assigned-numbers.htm

- El atributo *ServiceName* es un nombre corto amigable para el servicio; ej. "Red Corporativa", "Conferencia #1", etc.
- El atributo *ServiceDescription* es una descripción más extensa sobre el servicio. Ej. "Esta red es provista para nuestros invitados. Provee acceso libre a Internet y servicios de impresión. No se requiere nombre de usuario ni contraseña".
- El atributo de *ServiceAvailability* puede ser usado en conjunción con el campo de factor de carga del CoD[62] definido para Puntos de Acceso a LANs (ver Números Asignados).

### 3.7 L2CAP

Este LAP adopta todos los requerimientos especificados en el apéndice I "Requerimientos de Interoperabilidad L2CAP".

Adicionalmente:

1.- El MTU utilizado en la capa L2CAP es determinado por el parámetro "*maximun frame size*" del RFCOMM.

### 3.8 Gestor de Enlace (LM)

Este LAP debe adoptar todos los requerimientos especificados en el apéndice J. Los requerimientos expresados en la siguiente tabla son cumplidos de forma mandatorio en este modelo:

[62] Siglas en inglés:"Class of Device CoD"

**Tabla 10**
**Procedimientos LMP**

| *Procedimiento* | *Soportado en el LAP* | *Soportado en el DT* |
|---|---|---|
| Autentificación | SI | SI |
| Emparejamiento | SI | SI |
| Encriptación | SI | SI |
| Solicitud cambio maestro/esclavo | SI | N/A |
| Realizar cambio maestro/esclavo | SI | SI |

Datos tomados de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles* [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]. Cuadro elaborado por los autores.

Adicionalmente:

- Por razones de ancho de banda, es conveniente pero no mandatario que ambos dispositivos utilicen paquetes *multi-slot*.
- Cuando el LAP es configurado en modo usuario-único (ej. El máximo número de usuarios es 1), entonces el LAP puede ser tanto el maestro o esclavo de una *piconet*.
- Cuando el LAP está configurado en modo multi-usuario (ej. El máximo número de usuarios en mayor que 1), entonces el LAP debe ser el de forma obligatoria el maestro de la *piconet*.

### 3.8.1 Manejo de errores

El LAP debe denegar el acceso al servicio PPP si el DT falla en cumplir con los siguientes requerimientos de este Punto de Acceso:

**(1)** Falla en completar el proceso de emparejamiento.

**(2)** Falla en cumplir con una solicitud de habilitar la encriptación sobre la conexión de la banda base.

(3) Falla por parte del DT en cumplir con una solicitud de realizar un cambio de maestro/esclavo. El LAP sólo puede solicitar un cambio de maestro/esclavo cuando está configurado en modo multi-usuario. En este modo el LAP debe ser el maestro de la *piconet*.

Estos errores en el proceso de establecimiento del enlace deben ser controlados de manera rigurosa, ya que pueden causar problemas en la *piconet* y fallas en los procesos de autentificación.

### 3.9 Control de Enlace

Este LAP debe adoptar todos los requerimientos especificados en el apéndice J. Adicionalmente:

1.- Los modos no-descubrible y descubrible general del LAP (ej. Cómo es usado el *InquiryScan*) están definidos en el apéndice G

2.- En orden de descubrir a los LAPs cercanos, un DT debe usar el procedimiento de Búsqueda General, se encuentran en el apéndice G.

Al tomar el rol de LAP se establece el bit de Red (#17) en el campo del CoD en los paquetes enviados. Adicionalmente, se establece su clase mayor de dispositivo a "*LAN Access Point*" tal como esta especificado en el *Bluetooth Assigned Numbers* (ver Anexo F).

### 3.10 Procedimientos de la Entidad de Administración

La Entidad de Administración debe encargarse de iniciar y controlar todos los procedimientos anteriormente mencionados. Es el vínculo entre el servidor LAP y las diferentes capas de la pila *Bluetooth*. Este modelo contempla los siguientes requerimientos para la Entidad de Administración:

**Tabla 11**
**Procedimientos de la Entidad de Administración.**

| *Procedimiento* | *Soportado en LAP* | *Soportado en DT* |
|---|---|---|
| Establecimiento del enlace | SI | SI |
| Modo multi-usuario/usuario-único | SI | N/A |

Datos tomados de Bluetooth Organization. *Specification of Bluetooth System, Volume 2 Profiles* [Documento en línea]. Disponible: http://www.bluetooth.org/docs/Bluetooth_V11_Profiles_22Feb01.pdf. [Consulta: Febrero, 2002]

### 3.10.1 Establecimiento del enlace

El establecimiento del enlace es requerido para la comunicación entre el LAP y el DT, es el origen de las interacciones entre DT y LAP. El procedimiento de establecimiento del enlace es comenzado como una consecuencia directa de las operaciones del usuario descritas en "Establecimiento de la Conexión" en la sección 3.3.3.

1. El DT realiza primero un Descubrimiento General para determinar cuales LAPs están dentro del rango del radio (ver apéndice G). Luego de haber realizado esto el DT obtiene una lista de las respuestas de los LAPs cercanos.
2. El DT ordena la lista según el campo "Factor de Carga" del CoD del Punto de Acceso. Ordenando de mayor a menor según cantidad de carga libre.
3. Si el usuario no ha indicado la dirección *Bluetooth* del dispositivo a conectar, el cliente DT podrá intentar establecer un enlace con el primer LAP de la lista. Cualquier error ó falla al establecer el enlace causará que el DT salte este LAP. El usuario del DT podrá intentar establecer enlace con el siguiente LAP en la lista.

4. Si no existen más LAPs en la lista, el DT no continuará con más procedimientos de establecimiento de enlace. El establecimiento del enlace deberá ser reiniciado.

**Indagación sin respuesta**

Si el DT no obtiene ninguna respuesta a la indagación, el DT no continuará con más procedimientos de establecimiento de enlace. El establecimiento del enlace debe ser reiniciado por el usuario.

**Búsqueda sin respuesta**

Si el LAP no responde a los intentos de búsqueda, el DT saltará este LAP.

**Emparejamiento**

Durante el establecimiento del enlace, el LAP y el DT son emparejados, lo que genera una pared de seguridad entre el LAP y el DT contra otros dispositivos.

**Errores**

Si cualquier procedimiento de LM o del Servicio de Descubrimiento falla, o si el enlace se pierde en cualquier momento del establecimiento del enlace, entonces el DT debe saltar este LAP.

Los procedimientos de la Entidad de Administración son los originarios de todos los demás procedimientos planteados en este modelo. El usuario interactúa de forma directa con la Entidad de Administración para iniciar el servicio de Punto de Acceso.

### 3.10.2 Máximo número de usuarios

Cuando el LAP ha sido configurado para permitir múltiples usuarios, entonces el LAP debe ser el maestro de la *piconet*, ver sección 2.2. En este modo, la Entidad de

Administración sobre el LAP asegura que el LAP se mantiene como maestro de la *piconet Bluetooth*.

Mientras se esté en el modo multi-usuario, el LAP debe solicitar ser el maestro de cualquier nuevo enlace físico de banda base, si, por cualquier razón, el LAP no puede mantenerse como el maestro, entonces el enlace físico debe fallar. El LMP permite a un dispositivo: (a) solicitar un cambio de maestro/esclavo, y también (b) rechazar el cumplimiento de una solicitud de realizar un cambio de maestro/esclavo.

### 3.11 Recomendaciones adicionales

Este modelo, resultante de los estudios previos y definiciones de interoperabilidad, aunque fue ideado para ser implementado como componente adicional para un PC o servidor, esto no es necesariamente una limitante. El modelo de Punto de Acceso a Redes LAN **BlueLAP** puede ser implementado en cualquier sistema de hardware y software que cumpla con los requerimientos mínimos planteados en la pila de protocolos necesarios para el modelo.

Por ser de naturaleza plural y abierta la tecnología *Bluetooth*, cualquier desarrollo que cumpla con las especificaciones mandatorias del SIG puede ser implementado en cualquier sistema y poder interconectar dispositivos de cualquier fabricante.

## 4 Codificación

Teniendo un diseño para los componentes necesarios, basados en el modelo de Punto de Acceso a Redes LAN para dispositivos *Bluetooth* y utilizando las herramientas escogidas y expuestas anteriormente, se desarrollaron los diferentes componentes de software necesarios para el funcionamiento de dicho modelo, este desarrollo arrojó los siguientes resultados:

**4.1 Servidor BlueLAP:** el servidor **BlueLAP** es el máximo resultado de la aplicación del modelo desarrollado, este servidor permite convertir un computador con un dispositivo *Bluetooth* conectado, en un Punto de Acceso a Redes LAN y proveerle a los dispositivos cliente que se encuentren en el área de cobertura acceso a sus servicios y conexión a la red cableada conectada a él.

El servidor **BlueLAP** fue desarrollado en C++ utilizando la pila de librerías **BlueZ** para dispositivos *Bluetooth* bajo *Linux*. Este desarrollo permite utilizar el servidor **BlueLAP** en cualquier distribución de *Linux* que tenga las librerías *BlueZ*. El servidor puede ofrecer servicios de Punto de Acceso a cualquier dispositivo *Bluetooth* que cumpla con las especificaciones estándar para acceder a Puntos de Acceso.

Los módulos programados para el servidor **BlueLAP** fueron:

- bluelapd.h: Contiene todas las definiciones de estructuras y funciones requeridas.
- bluelapd.c: Implementa las funciones necesarias para el funcionamiento del servidor.

**4.2 Cliente BlueLAP:** parte de la definición y diseño de un modelo de Punto de Acceso a Redes LAN es el método de utilización de dicho modelo por parte de dispositivos clientes para conectarse y obtener los servicios que provee el LAP.

Siguiendo este modelo se desarrolló un cliente **BlueLAP**, que permite a cualquier dispositivo que cuente con tecnología *Bluetooth* bajo entorno *Linux* y utilizando las librerías *BlueZ* para su funcionamiento, acceder a los servicios de un servidor **BlueLAP**.

Este cliente fue desarrollado igualmente con el lenguaje de programación C++ utilizando las librerías *BlueZ*, obteniendo los siguientes módulos:

- bluelap.h: Contiene todas las definiciones de estructuras y funciones requeridas.
- bluelap.c: Implementa las funciones necesarias para el funcionamiento del cliente.

**4.3 Herramienta de configuración y administración:** adicionalmente al desarrolló del servidor **BlueLAP**, se desarrolló una herramienta de configuración y administración del servidor. Esta herramienta permite, tanto de manera gráfica como por líneas de comando, inicializar los dispositivos *Bluetooth* a utilizar tanto por el servidor como por el cliente, configurar el servidor **BlueLAP**, iniciar y detener el servidor **BlueLAP** y monitorear las conexiones que se realizan al servidor.

Esta herramienta fue desarrollada tanto en *shell script* como en el lenguaje de programación *Perl*, con una interfaz gráfica basada en *web* que permite su utilización de forma amigable y remota. Ver Apéndice L para más información acerca de la utilización de esta herramienta.

Los módulos desarrollados para esta herramienta son:

- LAPserverconf.pl: Interfaz gráfica basada en *web* para la configuración y administración del servidor.
- startDevice_usb: Comando para inicializar un dispositivo *Bluetooth* de tipo USB para ser usado como servidor.

- startDevice_uart: Comando para inicializar un dispositivo *Bluetooth* de tipo UART para ser usado como servidor.
- startClienDevice_usb: Comando para inicializar un dispositivo *Bluetooth* de tipo USB para ser usado como cliente.
- startClienteDevice_uart: Comando para inicializar un dispositivo *Bluetooth* de tipo UART para ser usado como cliente.
- startLAPserver: Comando para iniciar un servidor **BlueLAP**.
- startLAPclient: Comando para iniciar un cliente **BlueLAP**.
- setauthon: Comando para establecer autentificación en el enlace *Bluetooth*.
- setauthoff: Comando para deshabilitar la autentificación en el enlace *Bluetooth*.
- setcrypton: Comando para establecer la encriptación en el enlace *Bluetooth*.
- setcryptoff: Comando para deshabilitar la encriptación en el enlace *Bluetooth*.

**5 Pruebas.**

Las pruebas se realizaron sistemáticamente a medida que se avanzaba en el proceso desarrollo de los componentes de software. A continuación se exponen los resultados de las pruebas en el mismo orden sistemático en que se realizaron:

**5.1 Reconocimiento de los equipos *Bluetooth*.**

Se necesitaba verificar si los dispositivos eran plenamente reconocidos y soportaban todas las características necesarias para el funcionamiento del LAP. Para realizar esto se debe leer a través de métodos de HCI la lista de características soportadas por los dispositivos, esta lista de características se encuentra en un registro

de cada uno de los dispositivos. Los resultados de estas pruebas para los dos dispositivos con los que contamos se muestran en la siguiente tabla:

**Tabla 12**
**Características Dispositivos *Bluetooth***

| Características del *Bluetooth Application Kit:* |
|---|
| Type: USB<br>BD Address: 00:80:37:13:D1:CA ACL MTU: 672:10 SCO MTU: 255:255<br>Features: 0x07 0xea 0x31 0x00<br><3-slot packets> <5-slot packets> <encryption> <RSSI><br><SCO link> <HV3 packets> <u-law log> <A-law log><br><CVSD> |
| Características del *Bluetooth Development Kit* |
| Type: UART<br>BD Address: 00:80:37:5A:02:79 ACL MTU: 672:8 SCO MTU: 64:0<br>Features: 0xff 0xf9 0x01 0x00<br><3-slot packets> <5-slot packets> <encryption> <slot offset><br><timing accuracy> <role switch> <hold mode> <sniff mode><br><park mode> <SCO link> <HV2 packets> <HV3 packets><br><u-law log> <A-law log> <CVSD> |

Al obtener estas características se determinó que el *Bluetooth Application Kit* tiene grandes diferencias con el *Bluetooth Development Kit*, dichas diferencias impusieron ciertas restricciones con las que no se tomaba en cuenta. Un ejemplo de esto se tiene al verificar que el *Bluetooth Application Kit* no posee la característica *role switch* dicha habilidad permite cambiar el rol del dispositivos según las necesidades de conexión de un momento determinado y cuya deficiencia traería como consecuencia que si por ejemplo este dispositivo fuera el maestro de una *piconet* y quisiera conectarse a un LAP también maestro de la *piconet* al no poder realizar el cambio de rol no podría conectarse al LAP.

## 5.2 Establecimiento del enlace inalámbrico

Estas pruebas se realizaron tanto a nivel de HCI como a nivel de L2CAP, estas pruebas tenían como objetivo determinar si las conexiones entre los dispositivos se realizaban de manera correcta, los resultados para estas pruebas fueron:

- **Conexión HCI:** Verificamos que la conexión a nivel de HCI se realice satisfactoriamente por medio de una herramienta (*hcidump*), con esto aseguramos que el intercambio de mensajes se cumple adecuadamente y se completa la conexión. La siguiente tabla muestra un ejemplo del proceso de establecimiento de conexión:

**Tabla 13**
**Establecimiento de una conexión HCI.**

| Dispositivo Origen | Dispositivo Destino |
|---|---|
| device: hci0 snap_len: 1028 filter: 0xffffffff<br>< HCI Command: Create Connection(0x01\|0x0005) plen 13<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Connect Complete(0x03) plen 11<br>< HCI Command: Write Link Policy Settings(0x02\|0x000d) plen 4<br>> HCI Event: Command Complete(0x0e) plen 6 | device: hci0 snap_len: 1028 filter: 0xffffffff<br>> HCI Event: Connect Request(0x04) plen 10<br>< HCI Command: Accept Connection Request(0x01\|0x0009) plen 7<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Connect Complete(0x03) plen 11<br>< HCI Command: Write Link Policy Settings(0x02\|0x000d) plen 4<br>> HCI Event: Command Complete(0x0e) plen 6<br>< HCI Command: Change Connection Packet Type(0x01\|0x000f) plen 4<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Connection Packet Type Changed(0x1d) plen 5<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Max Slots Change(0x1b) plen 3 |

- **Conexión L2CAP:** Una vez establecida la conexión HCI se necesita establecer una conexión L2CAP y comprobar que se halla realizado dicha conexión adecuada. Para esto se inició una conexión y se enviaron una serie

de datos chequeando que lleguen correctamente a través de una herramienta (*hcidump*) como lo muestra la siguiente tabla:

**Tabla 14**
**Establecimiento de una conexión L2CAP.**

| Dispositivo Origen | Dispositivo Destino |
|---|---|
| device: hci0 snap_len: 1028 filter: 0xffffffff<br>< HCI Command: Create Connection(0x01\|0x0005) plen 13<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Connect Complete(0x03) plen 11<br>< ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Connect req: psm 10 scid 0x0040<br>< HCI Command: Write Link Policy Settings(0x02\|0x000d) plen 4<br>> HCI Event: Command Complete(0x0e) plen 6<br>> ACL data: handle 0x0001 flags 0x02 dlen 16<br>L2CAP(s): Connect rsp: dcid 0x0040 scid 0x0040 result 0 status 0<br>< ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Config req: dcid 0x0040 flags 0x0000 clen 0<br>> ACL data: handle 0x0001 flags 0x02 dlen 14<br>L2CAP(s): Config rsp: scid 0x0040 flags 0x0000 result 0 clen 0<br>> ACL data: handle 0x0001 flags 0x02 dlen 16<br>L2CAP(s): Config req: dcid 0x0040 flags 0x0000 clen 4<br>MTU 2000<br>< ACL data: handle 0x0001 flags 0x02 dlen 14<br>L2CAP(s): Config rsp: scid 0x0040 flags 0x0000 result 0 clen 0<br>< ACL data: handle 0x0001 flags 0x02 dlen 672<br>< ACL data: handle 0x0001 flags 0x01 dlen 4<br>L2CAP(d): cid 0x40 len 672 [psm 10]<br>< ACL data: handle 0x0001 flags 0x02 dlen 672<br>< ACL data: handle 0x0001 flags 0x01 dlen 4<br>L2CAP(d): cid 0x40 len 672 [psm 10]<br>< ACL data: handle 0x0001 flags 0x02 dlen 672<br>< ACL data: handle 0x0001 flags 0x01 dlen 4<br>L2CAP(d): cid 0x40 len 672 [psm 10]<br>< ACL data: handle 0x0001 flags 0x02 dlen 672<br>> HCI Event: Number of Completed Packets(0x13) plen 5<br>< ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Disconn req: dcid 0x0040 scid 0x0040<br>> HCI Event: Number of Completed Packets(0x13) plen 5<br>> ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Disconn rsp: dcid 0x0040 scid | device: hci0 snap_len: 1028 filter: 0xffffffff<br>> HCI Event: Connect Request(0x04) plen 10<br>< HCI Command: Accept Connection Request(0x01\|0x0009) plen 7<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Connect Complete(0x03) plen 11<br>< HCI Command: Write Link Policy Settings(0x02\|0x000d) plen 4<br>> HCI Event: Command Complete(0x0e) plen 6<br>< HCI Command: Change Connection Packet Type(0x01\|0x000f) plen 4<br>> ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Connect req: psm 10 scid 0x0040<br>> HCI Event: Command Status(0x0f) plen 4<br>< ACL data: handle 0x0001 flags 0x02 dlen 16<br>L2CAP(s): Connect rsp: dcid 0x0040 scid 0x0040 result 0 status 0<br>> HCI Event: Connection Packet Type Changed(0x1d) plen 5<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Max Slots Change(0x1b) plen 3<br>> ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Config req: dcid 0x0040 flags 0x0000 clen 0<br>< ACL data: handle 0x0001 flags 0x02 dlen 14<br>L2CAP(s): Config rsp: scid 0x0040 flags 0x0000 result 0 clen 0<br>< ACL data: handle 0x0001 flags 0x02 dlen 16<br>L2CAP(s): Config req: dcid 0x0040 flags 0x0000 clen 4<br>MTU 2000<br>> ACL data: handle 0x0001 flags 0x02 dlen 14<br>L2CAP(s): Config rsp: scid 0x0040 flags 0x0000 result 0 clen 0<br>> ACL data: handle 0x0001 flags 0x02 dlen 676<br>L2CAP(d): cid 0x40 len 672 [psm 10]<br>> ACL data: handle 0x0001 flags 0x02 dlen 676<br>L2CAP(d): cid 0x40 len 672 [psm 10]<br>> ACL data: handle 0x0001 flags 0x02 dlen 676<br>L2CAP(d): cid 0x40 len 672 [psm 10]<br>> ACL data: handle 0x0001 flags 0x02 dlen 676<br>L2CAP(d): cid 0x40 len 672 [psm 10]<br>< ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Disconn rsp: dcid 0x0040 scid 0x0040 |

| | |
|---|---|
| 0x0040<br>< HCI Command: Disconnect(0x01\|0x0006) plen 3<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Disconn Complete(0x05) plen 4<br>> HCI Event: Command Complete(0x0e) plen 4 | > HCI Event: Number of Completed Packets(0x13) plen 5<br>> HCI Event: Disconn Complete(0x05) plen 4 |

## 5.3 Inicialización del Punto de Acceso

La inicialización del Punto de Acceso necesita que primero se establezca una conexión RFCOMM y sobre dicha conexión RFCOMM se procede con los demás procedimientos necesarios para el LAP. Un ejemplo de una conexión RFCOMM se tiene en la siguiente tabla:

**Tabla 15**
**Establecimiento de una conexión RFCOMM.**

| Dispositivo Origen | Dispositivo Destino |
|---|---|
| device: hci0 snap_len: 1028 filter: 0xffffffff<br>< HCI Command: Write Authentication Enable(0x03\|0x0020) plen 1<br>> HCI Event: Command Complete(0x0e) plen 4<br>< HCI Command: Write Encryption Mode(0x03\|0x0022) plen 1<br>> HCI Event: Command Complete(0x0e) plen 4<br>< HCI Command: Read Local Name(0x03\|0x0014) plen 0<br>> HCI Event: Command Complete(0x0e) plen 252<br>< HCI Command: Read Local Name(0x03\|0x0014) plen 0<br>> HCI Event: Command Complete(0x0e) plen 252<br>< HCI Command: Read Local Name(0x03\|0x0014) plen 0<br>> HCI Event: Command Complete(0x0e) plen 252<br>> HCI Event: Connect Request(0x04) plen 10<br>< HCI Command: Accept Connection Request(0x01\|0x0009) plen 7<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Connect Complete(0x03) plen 11<br>< HCI Command: Write Link Policy Settings(0x02\|0x000d) plen 4<br>> HCI Event: Command Complete(0x0e) plen 6<br>< HCI Command: Change Connection Packet | device: hci0 snap_len: 1028 filter: 0xffffffff<br>< HCI Command: Create Connection(0x01\|0x0005) plen 13<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Connect Complete(0x03) plen 11<br>> HCI Event: Command Status(0x0f) plen 4<br>< HCI Command: Create Connection(0x01\|0x0005) plen 13<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Connect Complete(0x03) plen 11<br>< ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Connect req: psm 3 scid 0x0040<br>< HCI Command: Write Link Policy Settings(0x02\|0x000d) plen 4<br>> HCI Event: Command Status(0x0f) plen 4<br>> HCI Event: Command Complete(0x0e) plen 6<br>> ACL data: handle 0x0001 flags 0x02 dlen 16<br>L2CAP(s): Connect rsp: dcid 0x0040 scid 0x0040 result 0 status 0<br>< ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Config req: dcid 0x0040 flags 0x0000 clen 0<br>> ACL data: handle 0x0001 flags 0x02 dlen 14<br>L2CAP(s): Config rsp: scid 0x0040 flags 0x0000 result 0 clen 0<br>> ACL data: handle 0x0001 flags 0x02 dlen 12<br>L2CAP(s): Config req: dcid 0x0040 flags 0x0000 clen 0 |

```
Type(0x01|0x000f) plen 4
> HCI Event: Command Status(0x0f) plen 4
> HCI Event: Connection Packet Type
Changed(0x1d) plen 5
> HCI Event: Command Complete(0x0e) plen 4
> ACL data: handle 0x0001 flags 0x02 dlen 12
   L2CAP(s): Connect req: psm 3 scid 0x0040
< ACL data: handle 0x0001 flags 0x02 dlen 16
   L2CAP(s): Connect rsp: dcid 0x0040 scid
0x0040 result 0 status 0
> ACL data: handle 0x0001 flags 0x02 dlen 12
   L2CAP(s): Config req: dcid 0x0040 flags
0x0000 clen 0
< ACL data: handle 0x0001 flags 0x02 dlen 14
   L2CAP(s): Config rsp: scid 0x0040 flags
0x0000 result 0 clen 0
< ACL data: handle 0x0001 flags 0x02 dlen 12
   L2CAP(s): Config req: dcid 0x0040 flags
0x0000 clen 0
> ACL data: handle 0x0001 flags 0x02 dlen 14
   L2CAP(s): Config rsp: scid 0x0040 flags
0x0000 result 0 clen 0
> ACL data: handle 0x0001 flags 0x02 dlen 8
   L2CAP(d): cid 0x40 len 4 [psm 3]
    RFCOMM(s): SABM: cr 1 dlci 0 pf 1 ilen 0
fcs 0x1c
< ACL data: handle 0x0001 flags 0x02 dlen 8
   L2CAP(d): cid 0x40 len 4 [psm 3]
    RFCOMM(s): UA: cr 1 dlci 0 pf 1 ilen 0 fcs
0xd7
> ACL data: handle 0x0001 flags 0x02 dlen 18
   L2CAP(d): cid 0x40 len 14 [psm 3]
    RFCOMM(s): PN CMD: cr 1 dlci 0 pf 0 ilen
10 fcs 0x70 mcc_len 8
     dlci 2 frame_type 0 credit_flow 0 pri 7
ack_timer 0 frame_size 667 max_retrans 0 credits
0
< ACL data: handle 0x0001 flags 0x02 dlen 18
   L2CAP(d): cid 0x40 len 14 [psm 3]
    RFCOMM(s): PN RSP: cr 0 dlci 0 pf 0 ilen
10 fcs 0xaa mcc_len 8
     dlci 2 frame_type 0 credit_flow 0 pri 7
ack_timer 0 frame_size 667 max_retrans 0 credits
0
> HCI Event: Number of Completed
Packets(0x13) plen 5
> ACL data: handle 0x0001 flags 0x02 dlen 8
   L2CAP(d): cid 0x40 len 4 [psm 3]
    RFCOMM(s): SABM: cr 1 dlci 2 pf 1 ilen 0
fcs 0x59
< ACL data: handle 0x0001 flags 0x02 dlen 8
   L2CAP(d): cid 0x40 len 4 [psm 3]
    RFCOMM(s): UA: cr 1 dlci 2 pf 1 ilen 0 fcs
```

```
< ACL data: handle 0x0001 flags 0x02 dlen 14
   L2CAP(s): Config rsp: scid 0x0040 flags
0x0000 result 0 clen 0
< ACL data: handle 0x0001 flags 0x02 dlen 8
   L2CAP(d): cid 0x40 len 4 [psm 3]
    RFCOMM(s): SABM: cr 1 dlci 0 pf 1 ilen 0
fcs 0x1c
> HCI Event: Number of Completed
Packets(0x13) plen 5
> ACL data: handle 0x0001 flags 0x02 dlen 8
   L2CAP(d): cid 0x40 len 4 [psm 3]
    RFCOMM(s): UA: cr 1 dlci 0 pf 1 ilen 0 fcs
0xd7
< ACL data: handle 0x0001 flags 0x02 dlen 18
   L2CAP(d): cid 0x40 len 14 [psm 3]
    RFCOMM(s): PN CMD: cr 1 dlci 0 pf 0 ilen
10 fcs 0x70 mcc_len 8
     dlci 2 frame_type 0 credit_flow 0 pri 7
ack_timer 0 frame_size 667 max_retrans 0 credits
0
> ACL data: handle 0x0001 flags 0x02 dlen 18
   L2CAP(d): cid 0x40 len 14 [psm 3]
    RFCOMM(s): PN RSP: cr 0 dlci 0 pf 0 ilen
10 fcs 0xaa mcc_len 8
     dlci 2 frame_type 0 credit_flow 0 pri 7
ack_timer 0 frame_size 667 max_retrans 0 credits
0
< ACL data: handle 0x0001 flags 0x02 dlen 8
   L2CAP(d): cid 0x40 len 4 [psm 3]
    RFCOMM(s): SABM: cr 1 dlci 2 pf 1 ilen 0
fcs 0x59
> ACL data: handle 0x0001 flags 0x02 dlen 8
   L2CAP(d): cid 0x40 len 4 [psm 3]
    RFCOMM(s): UA: cr 1 dlci 2 pf 1 ilen 0 fcs
0x92
< ACL data: handle 0x0001 flags 0x02 dlen 12
   L2CAP(d): cid 0x40 len 8 [psm 3]
    RFCOMM(s): MSC CMD: cr 1 dlci 0 pf 0
ilen 4 fcs 0x70 mcc_len 2
     dlci 2 fc 0 rtc 1 rtr 1 ic 0 dv 1 b1 0 b2 0 b3 0
len 0
> ACL data: handle 0x0001 flags 0x02 dlen 12
   L2CAP(d): cid 0x40 len 8 [psm 3]
    RFCOMM(s): MSC RSP: cr 0 dlci 0 pf 0 ilen
4 fcs 0xaa mcc_len 2
     dlci 2 fc 0 rtc 1 rtr 1 ic 0 dv 1 b1 0 b2 0 b3 0
len 0
> ACL data: handle 0x0001 flags 0x02 dlen 12
   L2CAP(d): cid 0x40 len 8 [psm 3]
    RFCOMM(s): MSC CMD: cr 0 dlci 0 pf 0
ilen 4 fcs 0xaa mcc_len 2
     dlci 2 fc 0 rtc 1 rtr 1 ic 0 dv 1 b1 0 b2 0 b3 0
len 0
```

```
0x92
> ACL data: handle 0x0001 flags 0x02 dlen 12
  L2CAP(d): cid 0x40 len 8 [psm 3]
    RFCOMM(s): MSC CMD: cr 1 dlci 0 pf 0
ilen 4 fcs 0x70 mcc_len 2
    dlci 2 fc 0 rtc 1 rtr 1 ic 0 dv 1 b1 0 b2 0 b3 0
len 0
< ACL data: handle 0x0001 flags 0x02 dlen 12
  L2CAP(d): cid 0x40 len 8 [psm 3]
    RFCOMM(s): MSC RSP: cr 0 dlci 0 pf 0 ilen
4 fcs 0xaa mcc_len 2
    dlci 2 fc 0 rtc 1 rtr 1 ic 0 dv 1 b1 0 b2 0 b3 0
len 0
< ACL data: handle 0x0001 flags 0x02 dlen 12
  L2CAP(d): cid 0x40 len 8 [psm 3]
    RFCOMM(s): MSC CMD: cr 0 dlci 0 pf 0
ilen 4 fcs 0xaa mcc_len 2
    dlci 2 fc 0 rtc 1 rtr 1 ic 0 dv 1 b1 0 b2 0 b3 0
len 0
> ACL data: handle 0x0001 flags 0x02 dlen 12
  L2CAP(d): cid 0x40 len 8 [psm 3]
    RFCOMM(s): MSC RSP: cr 1 dlci 0 pf 0 ilen
4 fcs 0x70 mcc_len 2
    dlci 2 fc 0 rtc 1 rtr 1 ic 0 dv 1 b1 0 b2 0 b3 0
len 0
< ACL data: handle 0x0001 flags 0x02 dlen 55
  L2CAP(d): cid 0x40 len 51 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 47
fcs 0x40
> ACL data: handle 0x0001 flags 0x02 dlen 54
  L2CAP(d): cid 0x40 len 50 [psm 3]
    RFCOMM(d): UIH: cr 1 dlci 2 pf 0 ilen 46
fcs 0x9a
< ACL data: handle 0x0001 flags 0x02 dlen 55
  L2CAP(d): cid 0x40 len 51 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 47
fcs 0x40
> ACL data: handle 0x0001 flags 0x02 dlen 55
  L2CAP(d): cid 0x40 len 51 [psm 3]
    RFCOMM(d): UIH: cr 1 dlci 2 pf 0 ilen 47
fcs 0x9a
< ACL data: handle 0x0001 flags 0x02 dlen 29
  L2CAP(d): cid 0x40 len 25 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 21
fcs 0x40
> HCI Event: Number of Completed
Packets(0x13) plen 5
> ACL data: handle 0x0001 flags 0x02 dlen 29
  L2CAP(d): cid 0x40 len 25 [psm 3]
    RFCOMM(d): UIH: cr 1 dlci 2 pf 0 ilen 21
fcs 0x9a
< ACL data: handle 0x0001 flags 0x02 dlen 25
  L2CAP(d): cid 0x40 len 21 [psm 3]
```

```
< ACL data: handle 0x0001 flags 0x02 dlen 12
  L2CAP(d): cid 0x40 len 8 [psm 3]
    RFCOMM(s): MSC RSP: cr 1 dlci 0 pf 0 ilen
4 fcs 0x70 mcc_len 2
    dlci 2 fc 0 rtc 1 rtr 1 ic 0 dv 1 b1 0 b2 0 b3 0
len 0
> HCI Event: Number of Completed
Packets(0x13) plen 5
< ACL data: handle 0x0001 flags 0x02 dlen 54
  L2CAP(d): cid 0x40 len 50 [psm 3]
    RFCOMM(d): UIH: cr 1 dlci 2 pf 0 ilen 46 fcs
0x9a
> ACL data: handle 0x0001 flags 0x02 dlen 55
  L2CAP(d): cid 0x40 len 51 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 47 fcs
0x40
< ACL data: handle 0x0001 flags 0x02 dlen 55
  L2CAP(d): cid 0x40 len 51 [psm 3]
    RFCOMM(d): UIH: cr 1 dlci 2 pf 0 ilen 47 fcs
0x9a
> ACL data: handle 0x0001 flags 0x02 dlen 55
  L2CAP(d): cid 0x40 len 51 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 47 fcs
0x40
< ACL data: handle 0x0001 flags 0x02 dlen 29
  L2CAP(d): cid 0x40 len 25 [psm 3]
    RFCOMM(d): UIH: cr 1 dlci 2 pf 0 ilen 21 fcs
0x9a
> ACL data: handle 0x0001 flags 0x02 dlen 29
  L2CAP(d): cid 0x40 len 25 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 21 fcs
0x40
> ACL data: handle 0x0001 flags 0x02 dlen 25
  L2CAP(d): cid 0x40 len 21 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 17 fcs
0x40
> ACL data: handle 0x0001 flags 0x02 dlen 23
  L2CAP(d): cid 0x40 len 19 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 15 fcs
0x40
< ACL data: handle 0x0001 flags 0x02 dlen 84
  L2CAP(d): cid 0x40 len 80 [psm 3]
    RFCOMM(d): UIH: cr 1 dlci 2 pf 0 ilen 76 fcs
0x9a
> HCI Event: Number of Completed
Packets(0x13) plen 5
> ACL data: handle 0x0001 flags 0x02 dlen 46
  L2CAP(d): cid 0x40 len 42 [psm 3]
    RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 38 fcs
0x40
```

| | |
|---|---|
| RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 17 fcs 0x40<br>< ACL data: handle 0x0001 flags 0x02 dlen 23<br>L2CAP(d): d 0x40 len 19 [psm 3]<br>RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 15 fcs 0x40<br>> ACL data: handle 0x0001 flags 0x02 dlen 84<br>L2CAP(d): cid 0x40 len 80 [psm 3]<br>RFCOMM(d): UIH: cr 1 dlci 2 pf 0 ilen 76 fcs 0x9a<br>< ACL data: handle 0x0001 flags 0x02 dlen 46<br>L2CAP(d): cid 0x40 len 42 [psm 3]<br>RFCOMM(d): UIH: cr 0 dlci 2 pf 0 ilen 38 fcs 0x40<br>< HCI Command: Read Local Name(0x03\|0x0014) plen 0<br>> HCI Event: Command Complete(0x0e) plen 252<br>< HCI Command: Read Local Name(0x03\|0x0014) plen 0<br>> HCI Event: Command Complete(0x0e) plen 252 | |

El establecimiento de la conexión RFCOMM es sólo el primer paso, para poder dar servicio de Punto de Acceso a clientes *Bluetooth* y ofrecer acceso a los recursos y servicios de la red se debe realizar una serie de pasos, como: establecimiento de enlaces PPP, asignación de interfases IP. Estos procedimientos se realizan una vez concretada la conexión RFCOMM y se utilizan herramientas del sistema operativo para comprobar cada uno de estos procedimientos, la tabla 16 muestra dichas comprobaciones.

Teniendo las conexiones PPP iniciadas y las interfaces IP funcionando, se debe tener interconexión con los recursos de la red. Para verificar esto, se pueden utilizar herramientas del sistema operativo (ping, etc…), la tabla 17 muestra las pruebas de conexión entre los dispositivos.

**Tabla 16**
**Verificación de conexiones PPP e Interfases IP.**

| **Punto de Acceso** |
|---|
| eth0 Link encap:Ethernet HWaddr 00:E0:98:1F:23:86<br>inet addr:200.84.112.155 Bcast:200.84.115.255 Mask:255.255.252.0<br>UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1<br>RX packets:1529 errors:0 dropped:0 overruns:0 frame:0<br>TX packets:5099 errors:0 dropped:0 overruns:0 carrier:0<br>collisions:3 txqueuelen:100<br>RX bytes:540662 (527.9 Kb) TX bytes:385001 (375.9 Kb)<br>Interrupt:3 Base address:0x300 |
| lo Link encap:Local Loopback<br>inet addr:127.0.0.1 Mask:255.0.0.0<br>UP LOOPBACK RUNNING MTU:16436 Metric:1<br>RX packets:208 errors:0 dropped:0 overruns:0 frame:0<br>TX packets:208 errors:0 dropped:0 overruns:0 carrier:0<br>collisions:0 txqueuelen:0<br>RX bytes:72906 (71.1 Kb) TX bytes:72906 (71.1 Kb) |
| ppp0 Link encap:Point-to-Point Protocol<br>inet addr:10.0.0.20 P-t-P:10.0.0.21 Mask:255.255.255.255<br>UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1<br>RX packets:5 errors:0 dropped:0 overruns:0 frame:0<br>TX packets:5 errors:0 dropped:0 overruns:0 carrier:0<br>collisions:0 txqueuelen:3<br>RX bytes:72 (72.0 b) TX bytes:66 (66.0 b) |
| **Cliente** |
| lo Link encap:Local Loopback<br>inet addr:127.0.0.1 Mask:255.0.0.0<br>UP LOOPBACK RUNNING MTU:16436 Metric:1<br>RX packets:238 errors:0 dropped:0 overruns:0 frame:0<br>TX packets:238 errors:0 dropped:0 overruns:0 carrier:0<br>collisions:0 txqueuelen:0<br>RX bytes:20359 (19.8 Kb) TX bytes:20359 (19.8 Kb) |
| ppp0 Link encap:Point-to-Point Protocol<br>inet addr:10.0.0.21 P-t-P:10.0.0.20 Mask:255.255.255.255<br>UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1<br>RX packets:5 errors:0 dropped:0 overruns:0 frame:0<br>TX packets:5 errors:0 dropped:0 overruns:0 carrier:0<br>collisions:0 txqueuelen:3<br>RX bytes:66 (66.0 b) TX bytes:72 (72.0 b) |

**Tabla 17**
**Pruebas de conexión.**

| ***Ping* del LAP al DT** |
|---|
| [root@dC854709B root]# ping 10.0.0.21<br>PING 10.0.0.21 (10.0.0.21) from 10.0.0.20 ppp0: 56(84) bytes of data.<br>64 bytes from 10.0.0.21: icmp_seq=1 ttl=255 time=125 ms<br>64 bytes from 10.0.0.21: icmp_seq=2 ttl=255 time=127 ms<br>64 bytes from 10.0.0.21: icmp_seq=3 ttl=255 time=148 ms<br>64 bytes from 10.0.0.21: icmp_seq=4 ttl=255 time=137 ms<br><br>--- 10.0.0.21 ping statistics ---<br>4 packets transmitted, 4 received, 0% loss, time 3032ms<br>rtt min/avg/max/mdev = 125.726/134.815/148.445/9.018 ms |
| ***Ping* del DT a la interfase PPP del LAP** |
| [root@BlueLAP root]# ping 10.0.0.20<br>PING 10.0.0.20 (10.0.0.20) from 10.0.0.21 : 56(84) bytes of data.<br>64 bytes from 10.0.0.20: icmp_seq=1 ttl=255 time=41.6 ms<br>64 bytes from 10.0.0.20: icmp_seq=2 ttl=255 time=43.2 ms<br>64 bytes from 10.0.0.20: icmp_seq=3 ttl=255 time=48.1 ms<br>64 bytes from 10.0.0.20: icmp_seq=4 ttl=255 time=53.2 ms<br><br>--- 10.0.0.20 ping statistics ---<br>4 packets transmitted, 4 received, 0% loss, time 3033ms<br>rtt min/avg/max/mdev = 41.672/46.561/53.204/4.528 ms |
| ***Ping* del DT a la interfase Ethernet del LAP** |
| [root@BlueLAP root]# ping 10.0.0.1<br>PING 10.0.0.1 (10.0.0.1) from 10.0.0.21 : 56(84) bytes of data.<br>64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=42.1 ms<br>64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=45.2 ms<br>64 bytes from 10.0.0.1: icmp_seq=3 ttl=255 time=50.4 ms<br>64 bytes from 10.0.0.1: icmp_seq=4 ttl=255 time=55.2 ms<br><br>--- 10.0.0.1 ping statistics ---<br>4 packets transmitted, 4 received, 0% loss, time 3030ms<br>rtt min/avg/max/mdev = 42.160/48.268/55.256/5.003 ms |
| ***Ping* del DT a una dirección IP en Internet** |
| [root@BlueLAP root]# ping google.com<br>PING google.com (216.239.35.100) from 10.0.0.21 : 56(84) bytes of data.<br>64 bytes from www.google.com (216.239.35.100): icmp_seq=1 ttl=44 time=430 ms<br>64 bytes from www.google.com (216.239.35.100): icmp_seq=2 ttl=44 time=437 ms<br>64 bytes from www.google.com (216.239.35.100): icmp_seq=3 ttl=44 time=442 ms<br>64 bytes from www.google.com (216.239.35.100): icmp_seq=4 ttl=44 time=412 ms |

Una vez verificada la interconexión con la LAN se puede proceder a utilizar otros recursos, como: salida a Internet, FTP, servidores de archivos, impresoras, etc… La siguiente figura muestra un ejemplo de la utilización de un DT conectado a un LAP:

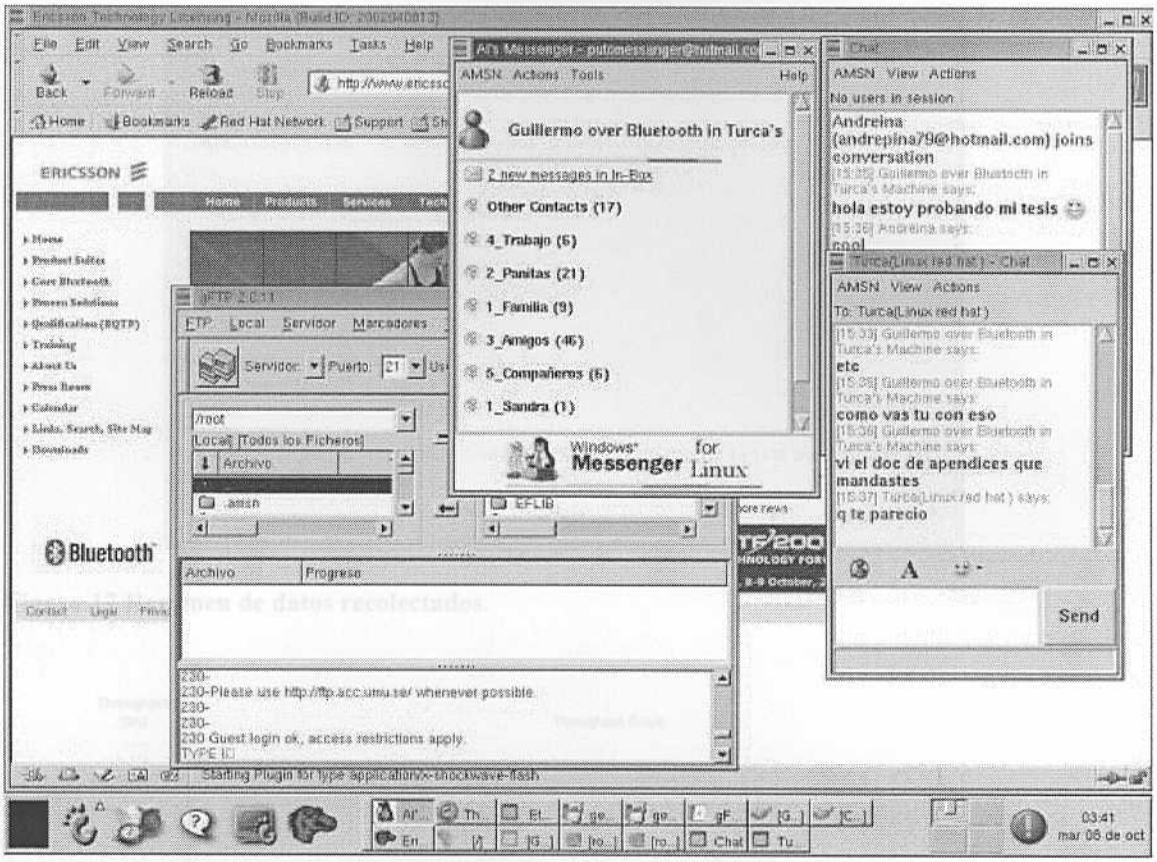


**Figura 16 DT utilizando la conexión del LAP.**

Por ultimo se utilizo un analizador de protocolos de red llamado *Ethereal* para examinar los datos que viajaban a través de la conexión *Bluetooth*, con dicha herramienta se agruparon los datos recopilados (ver figura 17), y se graficaron la cantidad de datos transmitidos en una unidad de tiempo (ver figura 18).

Estos datos recolectados con *Ethereal* permitieron comprobar tasas de transferencia, dichas tasas se encuentran dentro de los parámetros normales (~ 5 KB/seg), para los dispositivos *Bluetooth* con los que contamos para el desarrollo de este Trabajo Especial de Grado.

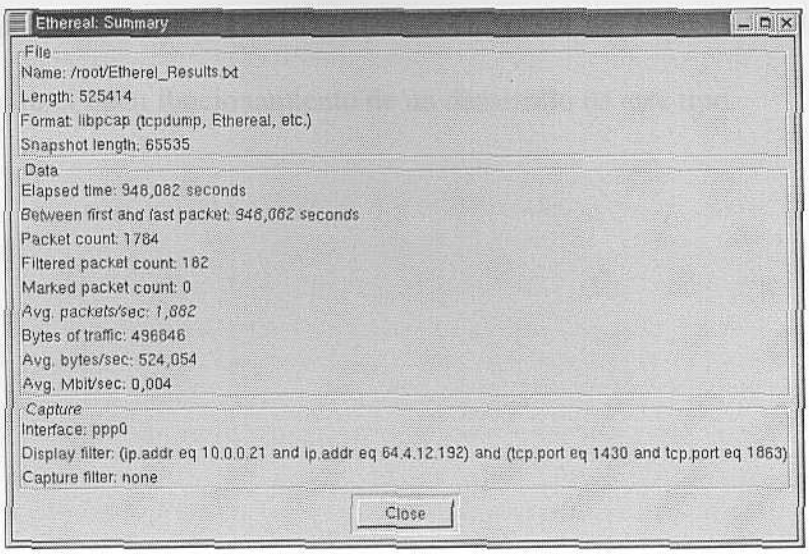


***Figura 17 Resumen de datos recolectados.***

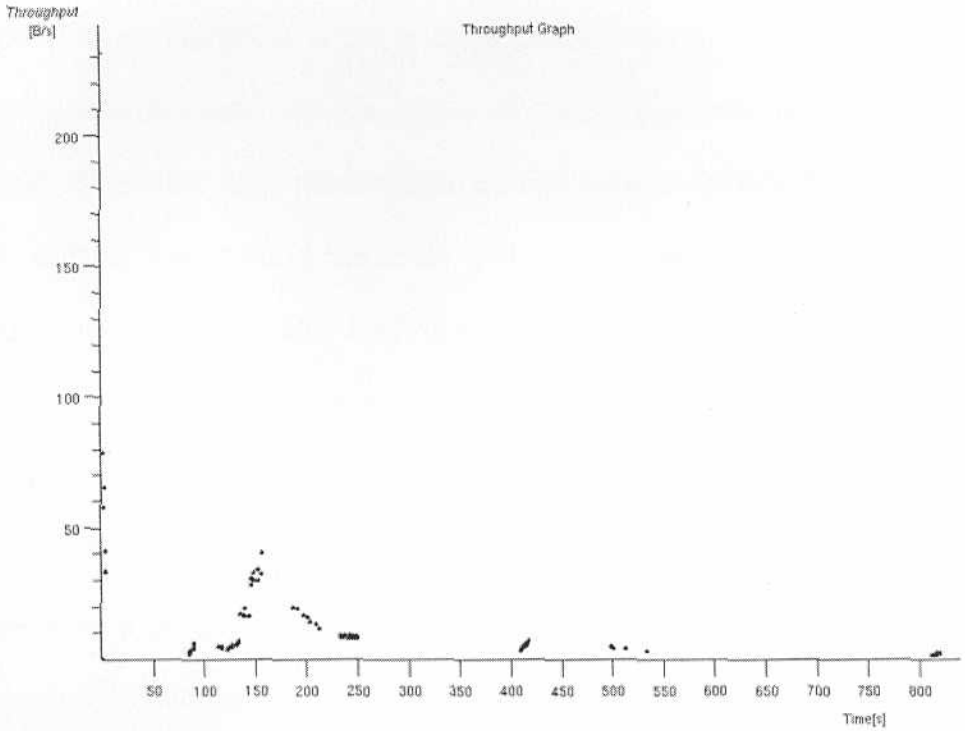


**Figura 18 Cantidad de datos transmitidos en una unidad de tiempo.**

Estas pruebas arrojaron resultados satisfactorios que nos permiten asegurar que se logro desarrollar un prototipo de Punto de Acceso a Redes LAN que cumple con los

requerimientos definidos en el modelo planteado y con las funcionalidades practicas necesarias para el buen funcionamiento de un desarrollo de este tipo.

## CONCLUSIONES

Se logró el estudio de la tecnología inalámbrica *Bluetooth*, el por qué de su creación, su estructura, las características y funcionalidades de cada una de sus partes, y su integración con la realidad que nos rodea. A su vez, este estudio permitió su comparación con otras tecnologías como son: 802.11, *HomeRF* e Infrarrojo.

En el estudio de componentes se establecieron cuales eran los componentes y requerimientos tanto de hardware y software necesarios: como: lenguaje de programación, plataforma en la que se debía trabajar, así como también los requisitos mínimos que deben tener los dos grupos de trabajo para estar en una red, la pila *Bluetooth*, el servidor LAP (desarrollado en este trabajo), el servidor PPP (provisto por el sistema operativo y utilizado por el servidor LAP), herramientas de configuración para el servidor LAP (también desarrollado en este trabajo) y los dispositivos *Bluetooth* (provistos por el fabricante Ericsson).

Se diseñó el modelo de Punto de Acceso, siguiendo los requisitos establecidos por el SIG, los dispositivos y los datos obtenidos del estudio de la tecnología *Bluetooth*. Se establecieron los escenarios en los que puede trabajar el modelo, los mecanismos de seguridad, la cantidad de usuarios permitidos, como se debe establecer el enlace, como se debe finalizar los enlaces, como debe funcionar PPP, los protocolos RFCOMM, SDP, L2CAP, el Gestor de Enlace, Control de Enlace, los procedimientos de la entidad Administradora.

# CONCLUSIONES

Se logró el estudio de la tecnología inalámbrica *Bluetooth,* el por qué de su creación, su estructura, las características y funcionalidades de cada una de sus partes, y su integración con la realidad que nos rodea. A su vez, este estudio permitió su comparación con otras tecnologías como son: 802.11, *HomeRF* e Infrarrojo.

En el estudio de componentes se establecieron cuales eran los componentes y requerimientos tanto de hardware y software necesarios; como: lenguaje de programación, plataforma en la que se debía trabajar, así como también los requisitos mínimos que debían tener los dos grupos de trabajo para estar en una red, la pila *Bluetooth*, el servidor LAP (desarrollado en este trabajo), el servidor PPP (provisto por el sistema operativo y utilizado por el servidor LAP), herramientas de configuración para el servidor LAP (también desarrollado en este trabajo) y los dispositivos *Bluetooth* (provistos por el fabricante Ericsson).

Se diseñó el modelo de Punto de Acceso, siguiendo los requisitos establecidos por el SIG, los dispositivos y los datos obtenidos del estudio de la tecnología *Bluetooth*. Se establecieron los escenarios en los que puede trabajar el modelo, los mecanismos de seguridad, la cantidad de usuarios permitidos, como se debe establecer el enlace, como se debe finalizar los enlaces, como debe funcionar PPP, los protocolos RFCOMM, SDP, L2CAP, el Gestor de Enlace, Control de Enlace, los procedimientos de la entidad Administradora.

Se desarrolló el prototipo denominado **BlueLAP**, dadas todas las especificaciones que debe cumplir el modelo, se utilizaron los lenguajes de programación *Perl* y C++. Y así cumplir con el objetivo de realizar un **Modelo de Punto de Acceso a Redes LAN (LAN Access Point) para dispositivos *Bluetooth*,** contribuyendo con una aplicación para estos dispositivos que se tienen en la escuela de Ingeniería Informática, y así poder mostrar las capacidades de esta tecnología y lo que se puede obtener de ella.

La tecnología inalámbrica *Bluetooth,* tiene grandes posibilidades de convertirse en una tecnología de mucha importancia en un futuro cercano, dadas todas las gamas de aplicaciones que tiene, y que se encuentran en desarrollo por empresas del SIG o particulares. Y es importante saber que se puede complementar con otras tecnologías inalámbricas como 802.11.

Para finalizar, se lograron los objetivos planteados en este Trabajo Especial de Grado, se realizaron estudios exhaustivos sobre las tecnologías de transmisión inalámbricas de mayor repercusión en la actualidad y se genero un documento que contiene los resultados de dichos estudios y el desarrollo planteado para un Punto de Acceso a Redes LAN para dispositivos *Bluetooth*.

# RECOMENDACIONES

Se recomienda:

- La adquisición de más dispositivos *Bluetooth,* por parte de la Escuela de Ingeniería Informática de la Universidad Católica Andrés Bello, para realizar prueba más exhaustivas del funcionamiento del prototipo desarrollado (ej. cuando existe más de un dispositivo en el área de cobertura, comprobar el funcionamiento de una *piconet,* etc).
- Realizar los clientes **BlueLAP** para otros sistemas operativos, como Windows, Mac OS y para dispositivos PDAs
- Iniciar un plan piloto de implantación de Puntos de Acceso para dispositivos *Bluetooth* en las áreas de la Universidad Católica Andrés Bello. Utilizando el prototipo resultante de este Trabajo Especial de Grado, realizando mayores pruebas para refinar el prototipo y así poder ofrecer a futuro este servicio a la comunidad universitaria.
- Fomentar la realización de trabajos de investigación usando varias tecnologías inalámbricas en conjunto, como sería el caso *Bluetooth* y 802.11, tomando en cuenta las ventajas y desventajas de cada una de ellas.
- Incentivar el desarrollo de aplicaciones innovadoras con la tecnología *Bluetooth* (ej. Robotica, domotica, etc…).

# REFERENCIAS


- Baker, D.M y Gilster, Diane, *Bluetooth End to End,* New York, Hungry Minds, Inc, 2002.
- Bluetooth Special Interest Group, "*Specification Volume 1 Specification of the Bluetooth System, Core*" version 1.1, s.l., 2001.
- Bluetooth Special Interest Group "*Specification Volume2 Specification of the Bluetooth System, Profiles"* version 1.1,s.l, 2001
- Bray, J y Sturman, C , *Connect Without Cables*, Segunda Edición, Texas, Prentice Hall, Inc, 2001
- Eco, Humberto, *Como se hace una Tesis,* Doceava Edición, España, Editorial Gedisa, s.f.
- García-Pelayo, Ramón, *Pequeño Larousse Ilustrado*, México, Ediciones Larousse, 1983.
- Informe sobre la Tecnología Bluetooth www.ldc.usb.ve/~figueira/cursos/redes2/EXPOem01/Bluetooth/contenido.htm , [Consulta: 2002, Septiembre 15]
- Kendall, Kenneth y Kendal, Julie, *Análisis y Diseño de Sistemas,* Tercera Edicion, Mexico, Prentice Hall Hispanoamericana, S.A, 1997.

- Lammle, Todd, *Cisco Certified Network Associated,* Second Edition, Alameda, SYBEX Inc, 2000.
- Modelo OSI.: http://www.pchardware.org/redes/redes_osi.php [Consulta: 2001, Noviembre 20]
- Muller, Nathan, *Tecnología Bluetooth,* Madrid, McGraw-Hill/Interamericana de España, S.A.U., 2002.
- Pressman, Roger, *Ingeniería del Software Un enfoque práctico*, Cuarta Edición, Madrid, McGraw-Hill/Interamericana de España, S.A.U., 1998.
- Stallings, William, *Comunicaciones y Redes de Computadores*, Sexta Edición, Madrid, Pearson Educación, 2000.
- Universidad Politécnica de Valencia http://miron.disca.upv.es/pei/Trabajos/2000_2001/Interfaces%20Inalambricas/Bluetooth/Blue_proto.html [Consulta: 2002, Enero 12].