



Universidad Católica de Santiago de Guayaquil

Facultad de Educación Técnica para el Desarrollo

Tesis de Grado
Previo a la Obtención del título:

Ingeniero en Telecomunicaciones

Mención en Gestión Empresarial

Tema:

“Diseño e implementación de un sistema de telecomunicaciones para información y recepción de sugerencias, aplicando la tecnología bluetooth, en la Facultad Técnica”

Realizado por:

Jorge Cortez Silva
Dennys Espín Gallardo
Fernando Espinoza Tacle
Franklin Freire Fajardo

Director de Tesis:

Ing. Washington Medina

Guayaquil – Ecuador
2010

FACULTAD DE EDUCACION TECNICA PARA EL DESARROLLO

TESIS DE GRADO

Título

“Diseño e implementación de un sistema de telecomunicaciones para información y recepción de sugerencias, aplicando la tecnología bluetooth, en la facultad técnica”

Presentada a la Facultad de Educación Técnica para el Desarrollo, Carrera de Ingeniería en Telecomunicaciones de la Universidad Católica de Santiago de Guayaquil

Por:

Jorge Cortez Silva
Fernando Espinoza Tacle

Dennys Espín Gallardo
Franklin Freire Fajardo

Para dar cumplimiento con unos de los requisitos para optar por el título de:

INGENIERO EN TELECOMUNICACIONES
Mención en Gestión Empresarial

Miembros del Tribunal

Ing. Héctor Cedeño A.
Decano de la Facultad

Ing. Pedro Tutiven López
Director de Carrera

Ing. Washington Medina M.
Director de Tesis

Dr. Kléber López Parrales
Coordinador Administrativo

Ing. Víctor del Valle Ramos
Coordinador Académico

DECLARACIÓN

Nosotros, Jorge Cortez Silva, Dennys Espín Gallardo, Fernando Espinoza Tacle, Franklin Freire Fajardo declaramos bajo juramento que la tesis aquí realizada es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y que he consultado la referencia bibliográfica que se incluyen en este documento.

Cortez Silva Jorge
0913628475

Espín Gallardo Dennys
0503117905

Espinoza Tacle Fernando
0914851803

Freire Fajardo Franklin
0921975694

Certificación

Certifico que el presente trabajo fue desarrollado por: Jorge Cortez Silva, Dennys Espín Gallardo, Fernando Espinoza Tacle, Franklin Freire Fajardo, bajo mi supervisión.

Ing. Washington Medina M.
Director de Tesis

AGRADECIMIENTO

Agradecemos a Dios por acompañarnos a lo largo de nuestro paso por la Universidad Católica Santiago de Guayaquil, por ser fortaleza en los momentos de debilidad y paz en los momentos de desespero. Por brindarnos una vida llena de aprendizajes, experiencias y sobre todo felicidad.

Les agradecemos a nuestros padres que por fruto de su esfuerzo nosotros hemos podido salir adelante en esta vida llena de obstáculos y de tropiezos, ya que ellos fueron el motor que nos impulso a continuar con nuestros estudios y luchas ante las adversidades.

Les agradecemos a nuestros maestros que se empeñaron en forjar en nosotros unas personas de bien y unos buenos elementos para el mañana, y para la vida ya que nos queda un gran camino por recorrer.

Les agradecemos a todos por estar junto a nosotros en este largo camino lleno obstáculos pero listos para seguirlos superandos.

DEDICATORIA

En este punto, solo me queda mirar atrás y ver cada uno de los pasos que di hasta llegar aquí, nunca estuve solo, por eso, a esta meta también llegaron ustedes. Quiero agradecerles infinitamente.

A Dios, que me llenó de fuerza y de paz, justamente cuando lo necesitaba. A mis padres, que desde pequeño sembraron en mí los valores que me han permitido tener una vida plena, entre ellos la disciplina, el respeto y la ansiedad por siempre aprender más, además de eso por ser siempre un refugio, un consejo y mis grandes amigos.

A mi hermana, quien con ejemplo forjó mi camino, me enseñó que cada sacrificio tiene su recompensa, me enseñaste a disfrutar los buenos momentos y a aprender de los malos.

A mis amigos Fernando, Dennys, Franklin, compañeros de curso y maestros sin ustedes aprender hubiese sido algo aburrido, gracias por aprender conmigo y por dejarme aprender de ustedes.

A mis amigos de siempre que me llenaron de aliento y me vieron seguir

Ahora, a seguir caminando y conquistar nuevas metas. Su amigo;

Jorge Cortez Silva

DEDICATORIA

Esta tesis va dedicada a las personas más especiales e importantes en mi vida; a mis padres por su gran apoyo incondicional y por enseñarme y guiarme en el camino correcto, quienes siempre estuvieron en los momentos más difíciles y erróneos de mi juventud, ayudándome y siempre respaldándome sea cual sea el motivo; también a mis abuelitos que han sido sabios maestros en mi vida, con sus grandes consejos y con todo el cariño que me han brindado; a mi hermana la cual ha estado conmigo desde siempre y me a apoyado en todo; a mi hermano el cual ha llenado mi vida de felicidad; a mi novia quien siempre me ha estado apoyando y alentando a seguir adelante en aquellos momentos que parecían ya no tener solución, con su gran fe e inspirado en ella los he podido superar.

Para ustedes; Teresa Gallardo, Fabián Espín, Dolores Gavilanes, Blanca Fuentes, Miguel Gallardo, Mayra Espín, Michael Espín, Nathaly Martínez; va dedicada esta tesis que he realizado con gran esfuerzo y sacrificio junto a mis compañeros de tesis.

Les quedo infinitamente agradecido por su gran apoyo.

Dennys Espín Gallardo

DEDICATORIA

Dedico la presente tesis y mi carrera a Dios, a mis padres Vicente Fernando Espinoza Ch. y Josefina Tacle Parra, a mi hermano, a mis abuelos, a mi familia; porque siempre me brindaron su apoyo incondicional, estuvieron en las buenas y en las malas conmigo; respetaron mis decisiones aun así creyendo que no eran las correctas, por eso le dedico todo este esfuerzo ya que es más de ellos que mío.

Les agradezco a mis compañeros, amigos de cursos, de tesis y de la vida, que cada uno con su esfuerzo y perseverancia me demostraba que si se podía así creyeran lo contrario, por todos esos momentos de felicidad y de amargura.

Gracias a todos por sus granitos de arena en lo largo de la vida.

Fernando Espinoza Tacle

DEDICATORIA

Dedicado a todos aquellos que me brindaron su apoyo y amistad durante los años de lucha en la universidad y en la elaboración de esta tesis, sin ellos no hubiera sido lo mismo:

A mis padres y mi madrina: Angela, Flavio y Maria, con su ejemplo me ayudaron a crecer, comprender y sobre a luchar por lo que se quiere.

A mis amigos: Andrés, Roberto, Christian, Dennys, Fernando, Jorge, por brindarme su amistad desinteresada.

A esa persona que siempre estuvo a mi lado dándome ánimos y apoyo incondicional, mostrando una paciencia increíble: Jennifer.

Franklin Freire Fajardo

INDICE

| | |
|---|-----|
| DECLARACIÓN | III |
| CERTIFICACION | IV |
| AGRADECIMIENTO | V |
| DEDICATORIAS | VI |
| INTRODUCCION | 1 |
| CAPITULO 1 | |
| Diseño e Implementación de un sistema de telecomunicaciones para información y recepción de sugerencias aplicando la tecnología Bluetooth, en la Facultad Técnica | |
| 1.1 Antecedentes | 2 |
| 1.2 Planteamiento del problema | 2 |
| 1.3 Justificación | 3 |
| 1.4 Hipótesis | 4 |
| 1.5 Objetivos generales | 4 |
| 1.6 Objetivos específicos | 5 |
| CAPITULO 2 | |
| ESTUDIO DE LAS TEGNOLOGÍAS BLUETOOTH | |
| 2.1. Bluetooth | 6 |
| 2.1.1 Características | 8 |
| 2.1.2 Evolución | 9 |
| 2.2 Características del enlace de radio y establecimiento de la conexión | 10 |
| 2.2.1 Procedimiento de la conexión | 10 |

| | |
|---|----|
| 2.2.2 Características del enlace de radio | 11 |
| 2.2.3 Características de la transmisión | 12 |
| 2.3 Arquitectura Bluetooth | 12 |
| 2.3.1 Capa Radio Bluetooth | 15 |
| 2.3.1.1 Banda de Frecuencia utilizada por Bluetooth | 15 |
| 2.3.1.2 Espectro Ensanchado por Salto de Frecuencia | 16 |
| 2.3.1.3 Modulación | 17 |
| 2.3.1.4 Potencia | 19 |
| 2.3.2 Capa Banda Base | 20 |
| 2.3.2.1.1 Piconet | 21 |
| 2.3.2.1.2 Scatternet | 22 |
| 2.3.2.2 Enlace Físico | 25 |
| a. Enlace Sincrónico Orientado a Conexión (SCO) | 25 |
| b. Enlace Asíncrono no Orientado a Conexión (ACL) | 26 |
| 2.3.2.3 Formato del Paquete Bluetooth | 27 |
| 2.3.2.4 Tipos de Paquetes | 34 |
| 2.3.2.5 Canales Lógicos | 36 |
| 2.3.2.6 Establecimiento de la Conexión | 37 |
| 2.3.2.7 Modos de Ahorro de Potencia | 46 |
| 2.3.3 Protocolo de Administración del Enlace LMP | 47 |
| 2.3.3.1 Emparejamiento con el Protocolo LMP | 48 |
| 2.3.3.2 Características Soportadas en el enlace | 49 |

| | | |
|-------------------------------|---|----|
| 2.3.3.3 | Requerimiento de Nombre del enlace LMP | 49 |
| 2.3.3.4 | Terminación del emparejamiento de LMP | 49 |
| 2.3.3.5 | Establecimiento de Conexión de LMP | 50 |
| 2.3.3.6 | Modos de Prueba de LMP | 50 |
| 2.3.4 | Interfaz del Controlador de Host (HCI) | 50 |
| 2.3.4.1 | Protocolo de Control y Adaptación de Enlace Lógico (L2CAP) | 51 |
| 2.3.4.2 | Canales Lógicos de L2CAP | 52 |
| 2.3.4.3 | Multiplexación de Protocolo | 52 |
| 2.3.4.4 | Segmentación y Reensamblado | 53 |
| 2.3.4.5 | Eventos de L2CAP | 54 |
| 2.3.4.6 | Formato del paquete de datos | 54 |
| 2.3.4.7 | Protocolo de Descubrimiento de Servicio SDP | 51 |
| 2.3.4.7.1 | Descripción General | 51 |
| 2.3.4.7.2 | Registros de Servicio | 56 |
| 2.3.5 | Capa RFCOMM | 56 |
| 2.3.6 | Perfiles Bluetooth | 57 |
| CAPITULO 3 | | |
| SEGURIDAD EN BLUETOOTH | | |
| 3.1 | NIVELES DE SEGURIDAD | 64 |
| 3.1.1 | Bluehacking | 67 |
| 3.1.2 | Bluesnarfing | 68 |

| | |
|---|----|
| 3.2 Seguridad con el emparejamiento de dispositivos | 68 |
| 3.3 Autenticación Bluetooth | 69 |
| 3.4 Aplicaciones de Bluetooth | 71 |
| CAPITULO 4 | |
| ESTÁNDAR IEEE | |
| 4.1 IEEE 802.15.1 | 73 |
| 4.1.1 Visión general | 74 |
| 4.2 Factores de propagación inalámbrica | 76 |
| 4.3 Atenuación y absorción de ondas | 77 |
| 4.3.1 Atenuación | 77 |
| 4.3.2 Absorción | 78 |
| 4.4 Pérdidas existentes en un radio enlace | 78 |
| 4.4.1 Pérdidas en la Trayectoria en el Espacio Libre (<i>L patch</i>) | 78 |
| 4.4.2 Desvanecimiento por Múltiple Trayectoria (<i>L fade</i>) | 79 |
| 4.4.2.1 Reflexión | 80 |
| 4.4.2.2 Penetración | 81 |
| 4.4.2.3 Difracción | 82 |
| 4.4.2.4 Dispersión | 83 |
| 4.4.2.5 Interferencia | 83 |
| 4.5 Ganancia de la antena | 84 |
| 4.5.1 Características de las antenas | 85 |
| 4.5.1.1 Diagrama de Radiación | 85 |
| 4.5.1.1.1 Antenas Omnidireccionales | 85 |

| | |
|--|-----|
| 4.5.1.1.2 Antenas Direccionales | 86 |
| 4.5.1.2 Polarización de la Antena | 87 |
| 4.5.1.3 Ancho de Banda | 87 |
| CAPITULO 5 | |
| MODELOS PARA EL CÁLCULO DEL ENLACE | |
| 5.1 Modelos para cálculos | 88 |
| 5.1.1 Modelos para el cálculo del enlace bluetooth | 88 |
| 5.1.2 Modelo que considera las pérdidas en la trayectoria y desvanecimientos | 88 |
| Multitrayectoria | |
| 5.1.3 Modelo de Atenuación Lineal por Trayectoria | 90 |
| CAPITULO 6 | |
| MUESTREO Y TABULACION | |
| 6.1 Método de muestreo | 93 |
| 6.1.1 Método Probabilístico; Muestreo Aleatorio Simple | 93 |
| 6.2 Tabulación de encuestas | 94 |
| CAPITULO 7 | |
| DISEÑO E IMPLEMENTACION DEL SISTEMA BLUESERVER | |
| 7.1 Diseño preliminar | 98 |
| 7.2 Pruebas preliminares | 100 |
| 7.3 Instalación | 104 |
| 7.3.1 Puesta del rack | 104 |
| 7.3.2 Implementación del sistema eléctrico | 106 |

| | |
|---|-----|
| 7.3.3 Implementación de la red de antenas | 108 |
| 7.3.4 Implementación del punto de red | 111 |
| 7.4 Pruebas finales | 115 |
| | |
| CAPITULO 8 | |
| JUSTIFICATIVO DE ELECCION DEL EQUIPO | |
| 8.1 Justificación de equipo | 117 |
| 8.2 F.O.D.A. | 119 |
| 8.2.1 Fortalezas | 119 |
| 8.2.2 Oportunidades | 119 |
| 8.2.3 Debilidades | 120 |
| 8.2.4 Amenazas | 120 |
| 8.3 PRESUPUESTO | 121 |
| CONCLUSIONES | 123 |
| RECOMENDACIONES | 124 |
| BIBLIOGRAFÍA | 125 |
| | |
| ANEXOS | |
| 1 Encuestas | |
| 2 Manual de Usuario BlueServer | |

ÍNDICE DE FORMULAS

| | |
|---|----|
| Ecuación 2.1 Velocidad efectiva normalizada | 24 |
| Ecuación 4.1 Atenuación | 77 |
| Ecuación 4.2 Pérdidas en la Trayectoria en el Espacio Libre | 79 |
| Ecuación 4.3 Pérdidas en la Trayectoria en el Espacio Libre (dB) | 79 |
| Ecuación 5.1 Desvanecimientos Multitrayectoria | 89 |
| Ecuación 5.2 Desvanecimientos Multitrayectoria (dBm) | 89 |
| Ecuación 5.3 Desvanecimientos Multitrayectoria (dB) | 90 |
| Ecuación 5.4 Pérdidas en la Trayectoria | 90 |
| Ecuación 5.5 Pérdidas en la Trayectoria (dB) | 90 |
| Ecuación 5.6 Atenuación Lineal por Trayectoria (interiores) | 91 |
| Ecuación 5.7 Atenuación Lineal por Trayectoria (interiores) | 91 |
| Ecuación 5.8 Atenuación Lineal por Trayectoria (interiores con muros) | 92 |
| Ecuación 5.9 Atenuación Lineal por Trayectoria (Lineal dB) | 92 |
| Ecuación 6.1 Muestreo aleatorio simple | 93 |

ÍNDICE DE FIGURAS

| | |
|--|----|
| Figura 2.1 Equipos <i>Bluetooth</i> | 7 |
| Figura 2.2 Arquitectura <i>Bluetooth</i> | 13 |
| Figura 2.3 Diagrama de comunicación de equipos Bluetooth | 16 |
| Figura 2.4 Esquema de funcionamiento FHSS | 17 |
| Figura 2.5 Esquema de transmisión en una piconet | 19 |
| Figura 2.6 Diagrama de equipos que forman una Piconet | 21 |
| Figura 2.7 Diagrama de equipos que forman una Scatternet | 23 |
| Figura 2.8 Esquema de conexión ACL | 27 |
| Figura 2.9 Diagrama de paquete Bluetooth | 28 |
| Figura 2.10 Diagrama de cabecera del paquete Bluetooth | 30 |
| Figura 2.11 Tipos de Datos en la Carga Útil | 32 |
| Figura 2.12 División de la Carga Útil para Datos | 33 |
| Figura 2.13 Cabecera de la Carga Útil para Datos | 33 |
| Figura 2.14 Diagrama de Bloques del estado Paging | 38 |
| Figura 2.15 Conexión de Dispositivos | 39 |
| Figura 2.16 Esquema de Proceso de Inquiry | 40 |
| Figura 2.17 Esquema de Proceso de Paging | 42 |
| Figura 2.18 Diagrama de Estados de Transición Bluetooth | 45 |
| Figura 2.19 Diagrama de paquete LMP | 48 |
| Figura 2.20 Diagrama de comunicación de equipos Bluetooth | 51 |
| Figura 2.21 Diagrama de segmentación de paquete L2CAP | 53 |

| | | |
|--------------------|--|-----|
| Figura 2.22 | Diagrama de paquete L2CAP | 54 |
| Figura 2.23 | Puertos emulados por <i>RFCOMM</i> | 56 |
| Figura 2.24 | Bloque de perfiles Bluetooth | 59 |
| Figura 3.1 | Proceso de autenticación Bluetooth | 70 |
| Figura 4.1 | Arquitectura IEEE 802.15 | 75 |
| Figura 4.2 | Reflexión de una señal | 81 |
| Figura 4.3 | Difracción de Señal | 82 |
| Figura 4.4 | Dispersión de Señal | 83 |
| Figura 4.5 | Diagrama de Radiación de una Antena Omnidireccional | 86 |
| Figura 4.6 | Diagrama de Radiación de una Antena Direccional | 86 |
| Figura 7.1 | Plano de cobertura de sistema BlueServer en la Facultad Técnica | 98 |
| Figura 7.2 | Visión 3D de cobertura del sistema BlueServer en la Facultad Técnica | 99 |
| Figura 7.3 | Visión 3D de cobertura del sistema BlueServer en la Facultad Técnica | 99 |
| Figura 7.4 | Configuración del equipo BlueServer mediante conexión Ethernet | 100 |
| Figura 7.5 | Configuración física de las antenas bluetooth en el HUB para prueba | 101 |
| Figura 7.6 | Configuración y activación de la función de cada antena mediante el software de administración BlueServer. | 101 |
| Figura 7.7 | Procedimiento de la creación de una campaña de envío de mensajería Bluetooth mediante el software de administración del equipo BlueServer. | 102 |
| Figura 7.8 | Verificaciones de los parámetros de la campaña creada | 102 |
| Figura 7.9 | Colocación de las antenas en campo para pruebas de potencia y ganancia. | 103 |

| | | |
|--------------------|--|-----|
| Figura 7.10 | Recepción de mensajes en los dispositivos celulares dentro de la cobertura del sistema BlueServer | 103 |
| Figura 7.11 | Determinación de sitio de ubicación del Rack para el equipo BlueServer | 104 |
| Figura 7.12 | Instalación del rack, perforación la pared y se colocó pernos ancla para el soporte por parte de nuestro compañero Fernando Espinoza | 105 |
| Figura 7.13 | Rack tipo gabinete con puerta de seguridad y ventilación instalado en la ubicación determinada dentro del cuarto de rack de la Facultad Técnica. | 105 |
| Figura 7.14 | Diagrama del sistema eléctrico instalado para equipo BlueServer | 106 |
| Figura 7.15 | Instalación del sistema eléctrico dentro del cuarto de rack de la Facultad Técnica por parte de nuestro compañero Franklin Freire | 107 |
| Figura 7.16 | Procedimiento de instalación del cableado eléctrico en su acometida | 107 |
| Figura 7.17 | Interruptor para prendido/apagado del equipo BlueServer y de antenas Bluetooth de nuestro proyecto. | 108 |
| Figura 7.18 | Diagrama de instalación de la red de antenas USB Bluetooth | 109 |
| Figura 7.19 | Extremo izquierdo donde se ubicarán 3 antenas | 110 |
| Figura 7.20 | Extremo derecho donde se ubicarán 4 antenas | 110 |
| Figura 7.21 | Antenas instaladas | 111 |
| Figura 7.22 | Diagrama punto de red | 112 |
| Figura 7.23 | Se verifica la disponibilidad del puerto en el patch panel asignado a nuestro proyecto por parte del centro de cómputo de la Universidad | 112 |

| | | |
|--------------------|--|-----|
| Figura 7.24 | Ubicación e instalación del jack en el patch panel dentro del rack de la Facultad Técnica por parte de nuestro compañero Jorge Cortez | 113 |
| Figura 7.25 | Una vez instalado el jack en el patch pannel tenemos disponible el puerto Ethernet para la conexión del patchcord | 113 |
| Figura 7.26 | Puesta de caja para punto de red y conexión directa hacia el equipo BlueServer por parte de nuestro compañero Dennys Espin | 114 |
| Figura 7.27 | Instalación completada del punto de red | 114 |
| Figura 7.28 | Caja con grupo de 4 antenas se ubicaran en la parte exterior del cuarto de rack de la Facultad Técnica en el costado derecho | 115 |
| Figura 7.29 | Caja con grupo de 3 antenas se ubicaran en la parte exterior del cuarto de rack de la Facultad Técnica en el costado izquierdo | 115 |
| Figura 7.30 | Configuración del servidor el Rack para prueba final en la parte exterior del cuarto de rack de la Facultad Técnica | 116 |
| Figura 7.31 | se verifica en el celular la recepción de la campaña creada y emitida, en la parte exterior del cuarto de rack de la Facultad Técnica | 117 |
| Figura 8.1 | Muestra de la pagina web de proveedor ZONABLU | 118 |
| Figura 8.2 | Muestra de la pagina web de proveedor BLOOZY | 118 |

ÍNDICE DE TABLAS

| | |
|--|-----|
| Tabla 2.1 Características de la tecnología Bluetooth | 9 |
| Tabla 2.2 Bandas de frecuencia y canales de <i>RF Bluetooth</i> | 15 |
| Tabla 2.3 Niveles de Emisión en Bluetooth | 19 |
| Tabla 2.4 Niveles de Potencia de Transmisión para diferentes Regiones | 20 |
| Tabla 2.5 Paquetes para Transmisión Simétrico y Asimétrico | 35 |
| Tabla 4.1 Clases de Bluetooth de <i>IEEE 802.15</i> | 76 |
| Tabla 4.2 Penetración a través de diferentes tipos de materiales | 82 |
| Tabla 8.1 Presupuesto de costo de equipo BluServer y accesorios | 121 |
| Tabla 8.2 Gastos varios y administrativos | 121 |
| Tabla 8.3 Costo de materiales y herramientas | 122 |

INTRODUCCIÓN

El contenido de esta tesis describe el estudio e implementación de un sistema que nos permitirá contar con una vía de comunicación entre las autoridades y el estudiantado dentro de la Facultad Técnica basada en la tecnología Bluetooth.

Nuestra investigación dentro del capítulo uno se basa en la problemática presentada para publicar noticias concernientes al ambiente universitario y que estas lleguen de manera oportuna a los estudiantes de nuestra facultad.

Se plantea el uso de Bluetooth, como una de las tecnologías de comunicación inalámbrica de corto alcance, gracias a que su arquitectura de protocolo y seguridades permite simplicidad en el acceso además que garantice que la información transmitida será de manera confiable; como lo detallamos dentro de los capítulos dos y tres de esta tesis. Contamos con el estándar de la IEEE 802.15 en el capítulo cuatro con las directrices de propagación y atenuación de la señal inalámbrica, así como demás factores que inciden en este estudio.

El propósito de esta tesis es suplir la necesidad antes mencionada, y el capítulo seis cuenta con cifras de un muestreo realizado en nuestra facultad. Pauta las preferencias de los encuestados y su fidelidad con la tecnología Bluetooth. Dentro del capítulo siete y ocho detallamos pruebas preliminares y el proceso llevado a cabo en la instalación e implementación del rack, antenas, sistema eléctrico; la justificación y presupuesto de este proyecto.

CAPITULO 1

Diseño e Implementación de un sistema de telecomunicaciones para información y recepción de sugerencias aplicando la tecnología Bluetooth, en la Facultad Técnica

1.1 ANTECEDENTES

La tecnología Bluetooth en los últimos años ha tenido una constante evolución debido a que se busca su utilización en distintos servicios.

Ha llegado al país únicamente por medio de los celulares para compartir información y archivos, posteriormente era una característica adicional en computadoras personales, laptops, etc. Pero siempre bajo el mismo propósito, compartir archivos entre dispositivos. Sin embargo se pueden considerar beneficios adicionales y su aplicación en distintos escenarios.

Si tomamos en cuenta las facilidades en conectividad y comunicación con otros dispositivos celulares y PDA la implementación de Bluetooth para una WPAN (Wireless Personal Area Network) en nuestra facultad resulta una manera de explotar los beneficios de una conexión inalámbrica fácil de usar.

1.2 PLANTEAMIENTO DEL PROBLEMA

La falta de acceso a la información académica, financiera y estudiantil de la universidad de manera gratuita y oportuna hoy en día es una desventaja presentada a nivel universitario y específicamente en nuestra facultad.

A menudo se celebran distintos actos y se imparten seminarios, dirigidos a los estudiantes, que no cuentan con la asistencia masiva o con el interés que se espera. Por experiencia de este grupo de trabajo sabemos que es debido a que no se difunde esa información correctamente. Como método de difusión utilizado tenemos el uso de carteleras donde encontramos volantes o también el método de boca a boca, por lo cual llegan a un sector muy pequeño de estudiantes.

Sabemos que existe un buzón de sugerencias en la facultad pero lamentablemente no cumple con su función primordial.

1.3 JUSTIFICACIÓN

Un sistema basado en la tecnología bluetooth ha sido la elegida para la implementación dentro de la Facultad Técnica gracias a que la mayoría de estudiantes están familiarizados con esta tecnología, de esta forma aprovechamos los recursos existentes y una método que no ha sido explotada ni difundida eficientemente en el país, menos aun aplicada al campo académico.

Otro beneficio importante del sistema bluetooth a implementar en la facultad es que el equipo no solo envía contenido sino que también recibe. Ésta especial característica la podemos aprovechar para recibir notas de los estudiantes con un buzón de recomendaciones, sugerencias, quejas y toda clase de notificaciones las cuales nos van a servir para saber lo que piensa el estudiantado acerca de la administración, los servicios, las instalaciones y todo lo que los rodea y así de esta forma mejorar cada día nuestra facultad.

1.4 HIPÓTESIS

Un gran porcentaje de teléfonos celulares ya están habilitados con la interfaz bluetooth. Nuestro sistema bluetooth “BlueServer” aprovecha este canal y permite transmitir contenidos, sean: datos, imágenes, videos y hasta juegos a quienes se encuentren en un radio de hasta 100 metros vía Bluetooth. Esta solución es ideal para complementar campañas educativas, informativas o de publicidad. Al utilizar bluetooth aprovechamos el poder enviar contenido informativo y los mensajes transmitidos no se facturan.

Los contenidos a enviar pueden ser de gran variedad ya que este medio de comunicación (ondas Bluetooth), permite transmitir tanto textos (tipos SMS), imágenes (fotos, dibujos), vídeos, archivos de sonido (canciones), links de accesos a páginas web e incluso programas JAVA.

El sistema “BlueServer”, hace posible la modalidad de informar a las personas como lo haría cualquier medio impreso (periódicos, revistas, etc.) con la facilidad de recibirlo en la pantalla de algún celular o notebook que posea acceso bluetooth y este dentro del área de cobertura de las antenas.

1.5 OBJETIVOS GENERALES

- Diseñar e implementar un sistema de información y recepción de sugerencias aprovechando la tecnología Bluetooth en la Facultad Técnica.

1.6 OBJETIVOS ESPECÍFICOS

- Diseñar un sistema de información aprovechando la tecnología existente.
- Mantener informada a la comunidad universitaria.
- Recepción de sugerencias para mejorar la Facultad Técnica.

CAPITULO 2

ESTUDIO DE LA TEGNOLOGÍA BLUETOOTH

2.1 BLUETOOTH

En los últimos años las redes de área local inalámbricas, *WLAN*, están ganando mucha aceptación. Van creciendo conforme aumentan sus prestaciones y se descubren nuevas aplicaciones para ellas. Las *WLAN* permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar conectados a una red determinada.

Con las *WLAN* se elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red. Un usuario dentro de una red *WLAN* puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus e incluso sobre áreas metropolitanas a velocidades de 11 *Mbps* o superiores.

Las *WLAN* ofrecen una fácil incorporación de nuevos usuarios a la red, movilidad de los usuarios, bajo costo de implementación comparado con los sistemas cableados, velocidades de transmisión aceptables y áreas de cobertura que dependen de la potencia del interfaz utilizado.

Bluetooth es una tecnología estandarizada por la *IEEE 802.15.1*, define un estándar global de comunicaciones inalámbricas de corto alcance, que posibilita la transmisión de voz y datos tanto para estaciones fijas y móviles (*PCs*, teléfonos móviles, *PDA* (Asistentes Personales Digitales), etc.).

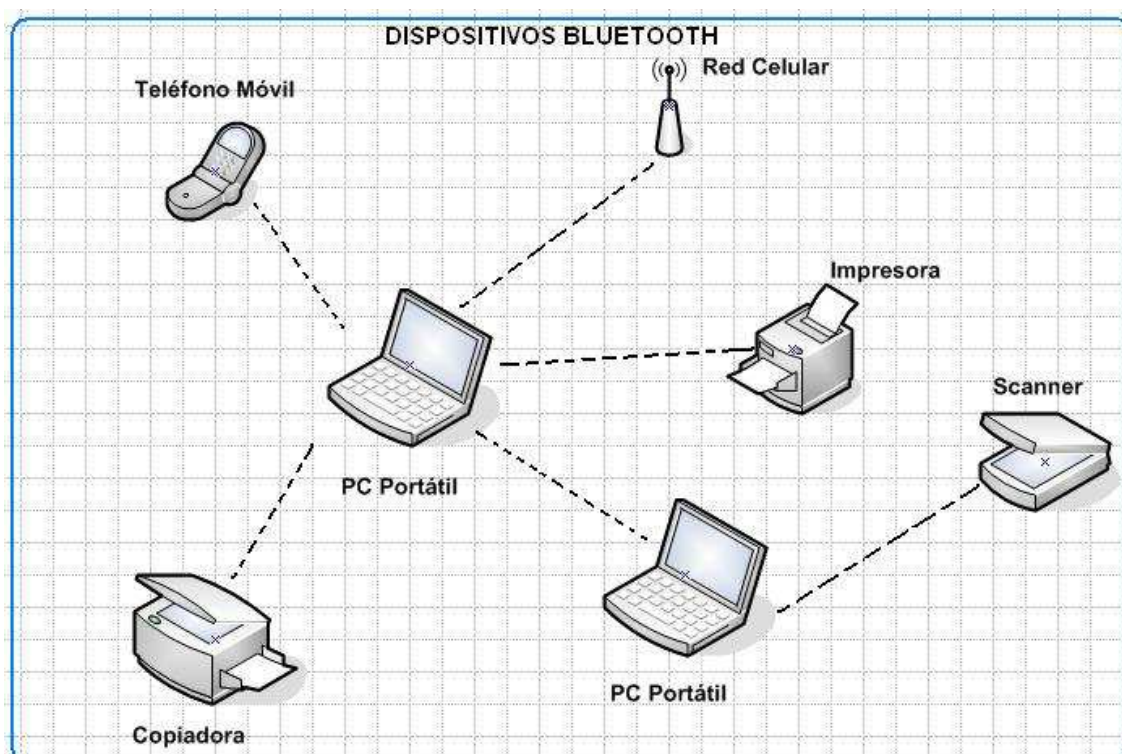


Figura 2.1 Diagrama de comunicación de equipos Bluetooth

Los objetivos que se persigue con este estándar son:

- Proporcionar comunicaciones entre equipos móviles y fijos
- Excluir cables y conectores entre éstos.
- Brindar la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre los equipos de trabajo.

2.1.1 CARACTERÍSTICAS

- La especificación de Bluetooth define un canal de comunicación de máximo 720Kb/seg con rango óptimo de 10 metros (opcionalmente 100m).
- La frecuencia de radio con la que trabaja está en el rango de 2.4 a 2.48Ghz con amplio espectro y saltos de frecuencia con posibilidad de transmitir en Full Duplex con un máximo de 1600 saltos/seg. Los saltos de frecuencia se dan entre un total de 79 frecuencias con intervalos de 1Mhz; esto permite dar seguridad y robustez.
- La potencia de salida para transmitir a una distancia máxima de 10 metros es de 0dBm (1 mW), mientras que la versión de largo alcance transmite entre -30 y 20dBm (100 mW).
- Para lograr alcanzar el objetivo de bajo consumo y bajo costo, se ideó una solución que se puede implementar en un solo chip utilizando circuitos CMOS. De esta manera, se logró crear una solución de 9x9mm y que consume aproximadamente 97% menos energía que un teléfono celular común.
- El protocolo de banda base (canales simples por línea) combina conmutación de circuitos y paquetes. Para asegurar que los paquetes no lleguen fuera de orden, los slots pueden ser reservados por paquetes síncronos, un salto diferente de señal es usado para cada paquete.
- La conmutación de circuitos puede ser asíncrono o síncrono. Tres canales de datos síncronos (voz), o un canal de datos síncrono y uno asíncrono, pueden ser soportados en un solo canal.

- Cada canal de voz puede soportar una tasa de transferencia de 64 Kb/s en cada sentido, la cual es suficientemente adecuada para la transmisión de voz. Un canal asíncrono puede transmitir como mucho 721 Kb/s en una dirección y 56 Kb/s en la dirección opuesta, sin embargo, para una conexión asíncrona es posible soportar 432,6 Kb/s en ambas direcciones si el enlace es simétrico.

| CARACTERÍSTICAS DE LA TECNOLOGÍA BLUETOOTH | |
|---|----------------------------|
| Banda de frecuencia | 2.4 GHz |
| Velocidad de transmisión | 720 Kbps |
| Alcance | < 10 m. |
| Consumo | Muy Bajo |
| Aplicaciones | Wireless Data |
| | Wireless Voice |
| | Sustitución de Cables |
| | Redes Personales |
| Características Principales | Bajo Consumo |
| | Transmisión de Voz y Datos |
| | Bajo Coste |
| | Robusto ante el ruido |
| Coste Relativo | Muy Bajo |
| Empresas Promotoras | mas 2000 |

Tabla 2.1 Características de la tecnología Bluetooth

2.1.1 EVOLUCIÓN

En 1994 *Ericsson* investigó la viabilidad de utilizar un interfaz de radio, para la interconexión de teléfonos móviles y otros accesorios, con el fin de eliminar los cables existentes entre aparatos relativamente cercanos. El estudio partía de un largo proyecto que investigaba sobre multi-comunicadores conectados a una red celular, hasta que se llegó a un enlace de radio de corto alcance.

Conforme avanzaba este proyecto, se estableció que este tipo de enlace podía ser utilizado en un gran número de aplicaciones, ya que tenía como principal virtud el estar basado en un chip de radio de bajo costo y de corto alcance.

A principios de 1998 se creó el *SIG* (*Special Interest Group*, Grupo de Interés Especial) y estuvo integrado por 5 promotores que fueron: *Ericsson*, *Nokia*, *IBM*, *Toshiba* e *Intel*. La idea era lograr un conjunto adecuado de áreas de negocio. *Bluetooth* se basó en el *SIG* y definió el estándar *IEEE 802.15.1* con el propósito principal, de establecer una interfaz aérea junto con su *software* de control, con el fin de asegurar la interoperabilidad de los equipos entre los diversos fabricantes.

“En la actualidad el *SIG* cuenta con miembros tales como *Motorola*, *3Com*, *Lucent* y *Microsoft*, el respaldo de 1900 empresas de tecnología y 2000 empleados (delegados en el Congreso convocado por el *SIG*) de otras tantas empresas que investigan productos y servicios con aplicaciones *Bluetooth*.”

2.2 CARACTERÍSTICAS DEL ENLACE DE RADIO Y ESTABLECIMIENTO DE LA CONEXIÓN

2.2.1 PROCEDIMIENTO DE LA CONEXIÓN

- Antes de que ninguna conexión sea establecida en una piconet, los dispositivos están en modo "standby".
- Cada uno busca mensajes periódicamente cada 1.28 segundos.

- Cuando un dispositivo “despierta”, escucha en un conjunto de 32 frecuencias distintas, definidas para esa unidad. El número de frecuencias varía según la región geográfica.
- El procedimiento de conexión puede ser iniciado por cualquiera de los dispositivos, y se convertirá en la estación maestra de la piconet.
- La estación maestra puede poner a las esclavas en modo "hold".
- Hay otros dos modos de ahorro de energía.
- En el modo "sniff"
- En el modo "park"

2.2.2 CARACTERÍSTICAS DEL ENLACE DE RADIO

- Bluetooth utiliza un esquema de reconocimiento rápido y saltos de frecuencia para garantizar la robustez del enlace.
- Opera en la banda de frecuencia de 2.4 GHz, libre para ISM
- Es más robusto que la mayoría de otros sistemas porque salta más rápido y usa paquetes más pequeños
- Emplea una corrección de error hacia delante (FEC, Forward Correction Error) que reduce el efecto del ruido aleatorio en enlaces de larga distancia.

2.2.3 CARACTERÍSTICAS DE LA TRANSMISIÓN

- La velocidad de los datos viene a ser de 1Mb/s.
- Utiliza un esquema de división en el tiempo para la transmisión en full-dúplex.
- El protocolo de banda base de Bluetooth es una combinación de conmutación de paquetes y de circuitos.
- Cada paquete se transmite en un salto de frecuencia distinto.
- Bluetooth puede soportar un canal de datos asíncrono.
- Los paquetes de voz no se retransmiten, ya que el método de codificación (CVSD) permite que la voz sea audible incluso con altos niveles de ruido.
- A la señal de radio, se ha añadido una expansión del espectro para facilitar la operación a niveles de potencia de más de 100mW
- La distancia nominal del enlace está comprendida entre 10 cm y 10 m, pero se puede aumentar a más de 100 m elevando la potencia de transmisión.

2.3 ARQUITECTURA BLUETOOTH

La especificación *Bluetooth* utiliza una arquitectura de protocolos que divide las diversas funciones de red en un sistema de niveles. En conjunto, permiten el intercambio transparente de información entre aplicaciones diseñadas de acuerdo con dicha especificación y fomentan la interoperabilidad entre los productos de diferentes fabricantes.

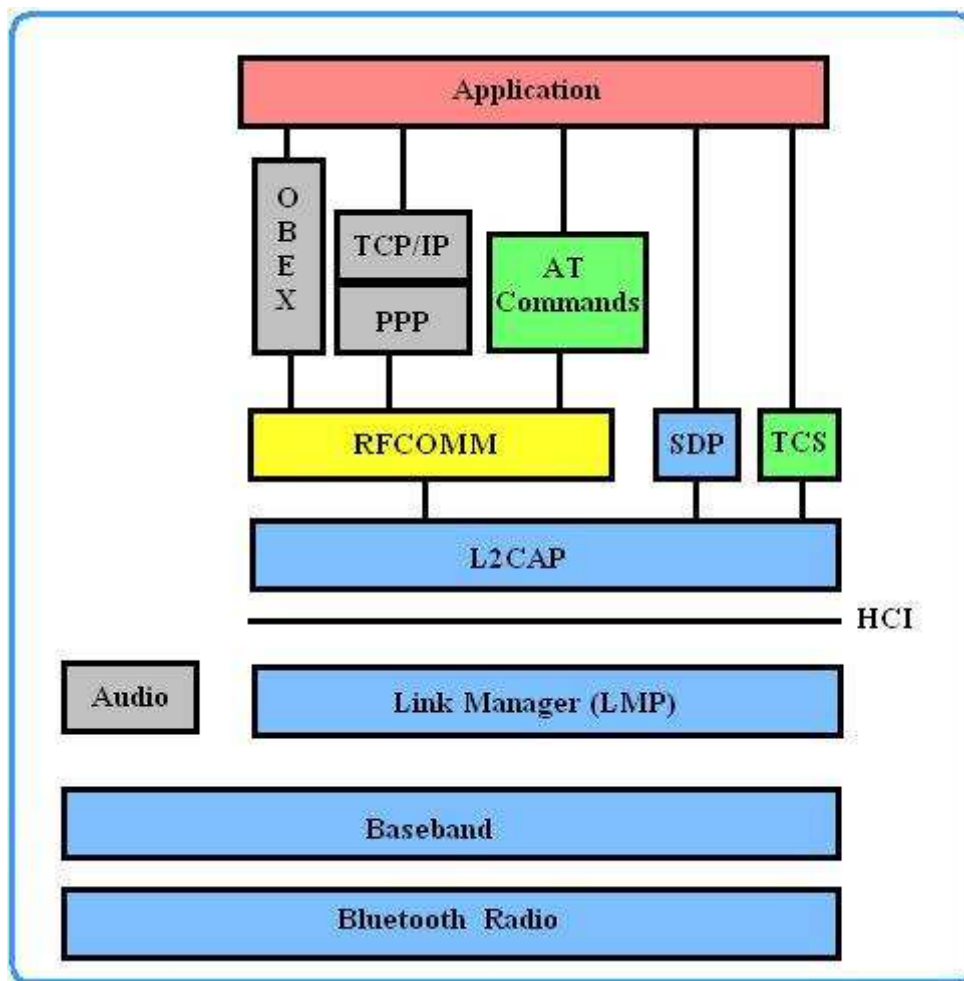


Figura 2.2 Diagrama de Capas de Arquitectura *Bluetooth*

Cada aplicación puede operar bajo una estructura de protocolos definida por cada columna como se observa en la figura 2.2, o por un conjunto de ellas. Algunas columnas son usadas sólo como soporte de la aplicación principal, como lo son el *SDP* (Protocolo de Descubrimiento de Servicio) y el *TCS* (Especificación de Control Telefónico).

La especificación es abierta, lo que permite el desarrollo de nuevos protocolos de aplicación en las capas superiores, lo cual se traduce en el desarrollo de una gran variedad de servicios por parte de los fabricantes.

Los protocolos pueden ser divididos de la siguiente forma:

- Protocolos Bluetooth Centrales (*BaseBand, LMP, L2CAP, SDP*).
- Protocolos de Reemplazo de Cable (*RFCOMM*).
- Protocolos de control de Telefonía (*TCS Binary, AT-Commands*).
- Protocolos Adaptados (*PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE*).

El llamado de núcleo de Bluetooth, ha sido implementado en su totalidad por el SIG, no obstante otros como RFCOMM y TCS-binary pese a ser desarrollados por el propio SIG, los han desarrollado siguiendo las recomendaciones de otras instituciones de telecomunicaciones, basándose en las especificaciones *ETSI-TS 07.10* y la *ITU-T Q.931*, respectivamente.

El resto de capas lógicas de sustitución de cable, de control de telefonía y de protocolos adoptados agrupan a los protocolos orientados a aplicación, permitiendo así a las diferentes aplicaciones existentes a desarrollarse en el futuro poder correr sobre el núcleo de Bluetooth. Como es una norma abierta en cuanto a los protocolos que corren sobre los protocolos específicos de transporte, se pueden hacer implementaciones que usen protocolos tan usados como FTP o HTTP por ejemplo. A partir de aquí se va a realizar una descripción detallada de los protocolos que emplea Bluetooth en su núcleo, y que constituyen la base de su funcionamiento.

2.3.1 CAPA RADIO BLUETOOTH

En este nivel se especifica detalles del interfaz aire como: bandas de frecuencia, arreglos de canales, saltos de frecuencia, esquema de modulación y niveles de potencia.

2.3.1.1 Banda de Frecuencia utilizada por Bluetooth

Para que *Bluetooth* opere globalmente, es indispensable que trabaje en una banda no licitada. La banda *ISM (Industrial, Scientific and Medical, Industrial, Científica y Médica)* de 2,45 GHz cumple con este requisito, con rangos que van de los 2.4 GHz a los 2.5 GHz, con algunas limitaciones en países como Francia, España y Japón. En la tabla 1.1 se muestra los rangos de frecuencia permitidos en diferentes regiones del mundo.

| Ubicación Geográfica | Rango Regulatorio | Canales RF |
|----------------------|---------------------|--|
| USA, Europa | 2.400 – 2.4835 GHz | $F = 2402 + K * \text{MHz}$, $K = 0, \dots, 78$ |
| España | 2.445 – 2.475 GHz | $F = 2449 + K * \text{MHz}$, $K = 0, \dots, 22$ |
| Francia | 2.4465 – 2.4835 GHz | $F = 2454 + K * \text{MHz}$, $K = 0, \dots, 22$ |

Tabla 2.2 Bandas de frecuencia y canales de RF Bluetooth

El espacio entre canales es de 1 MHz, no obstante es necesario tener unos márgenes de protección respecto al ancho de banda de trabajo, así pues, el límite superior de protección es de 2 MHz y un límite inferior es de 3,5 MHz

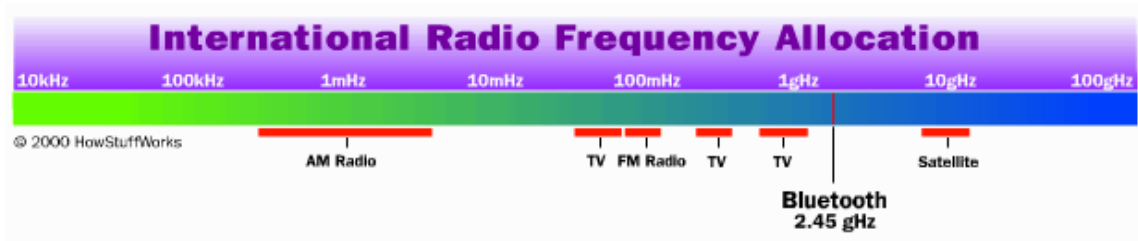


Figura 2.3 Diagrama de comunicación de equipos Bluetooth

La distancia nominal del enlace está comprendida entre 10 cm. y 10 m, pero se puede aumentar a más de 100 m elevando la potencia de transmisión. Otro aspecto importante es el consumo cuyos valores en los estados más habituales son 300uA (máx.), 30uA (standby), -50uA (hold/park).

2.3.1.2 Espectro Ensanchado por Salto de Frecuencia

Puesto que la banda *ISM* puede accesarse sin necesidad de licencia, el sistema de radio *Bluetooth* deberá estar capacitado para evitar las múltiples interferencias que se puedan producir. Éstas pueden ser evitadas utilizando un sistema de Espectro Ensanchado por Salto de Frecuencia.

Este sistema divide la banda de frecuencia en 79 canales con un ancho de banda de 1 MHz cada canal, donde, los transceptores, durante la conexión van cambiando de uno a otro canal de salto de manera pseudo-aleatoria. Con lo que se consigue que el ancho de banda instantáneo sea muy pequeño y se tenga una propagación efectiva sobre el total del ancho de banda. En la figura 2.4 se observa el esquema de

funcionamiento del sistema de (*FHSS*) Espectro Ensanchado por Salto de Frecuencia para *Bluetooth*.

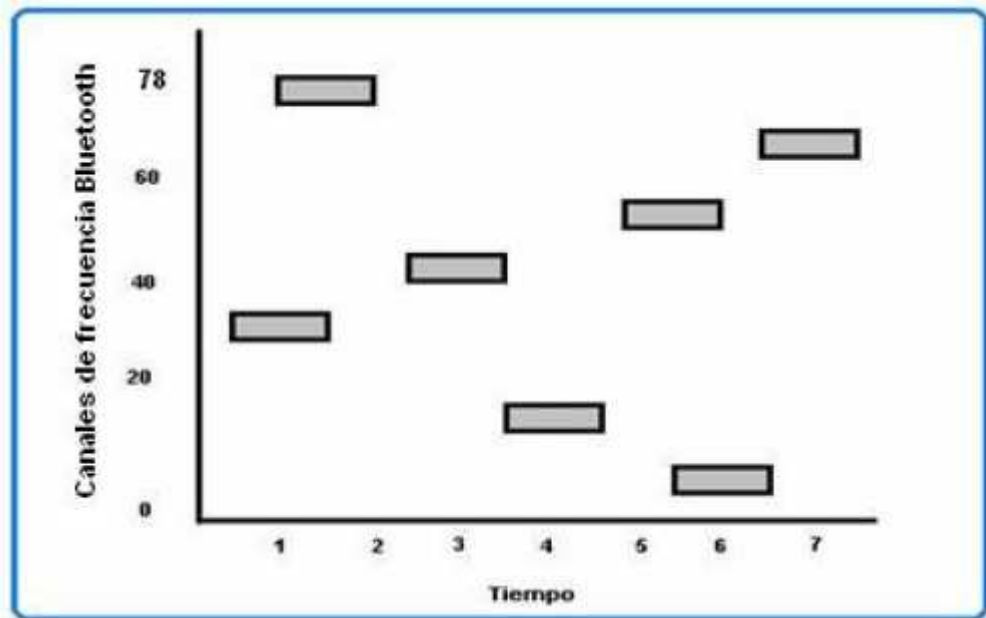


Figura 2.4 Esquema de funcionamiento FHSS

En conclusión, con el sistema *FHSS*, se pueden conseguir transceptores de banda estrecha con una gran inmunidad a las interferencias.

2.3.1.3. Modulación

En la banda de 2.4 *GHz* el ancho de banda para los sistemas *FH* está limitada en 1-*MHz*. El ancho de banda disponible es de 79 *MHz*, por lo que se dispone de 79 canales de salto en América.

Bluetooth utiliza una modulación *GFSK* (*Gaussian Frequency Shift Keying*, Modulación por Desplazamiento de Frecuencia Gausiana) con un índice de modulación $K=0.3$. En donde un “1” binario representa una desviación de frecuencia positiva, y un “0” binario representa una desviación de frecuencia negativa. La desviación máxima de frecuencia está entre 140 *KHz* y 175 *KHz*.

La elección de este esquema radica en su robustez y simplicidad de implementación del mismo. A continuación se detalla el proceso de transmisión entre dos o más dispositivos *Bluetooth* siendo uno maestro y otro esclavo, o llamado *piconet*, concepto que detallaremos mas adelante.

El canal está dividido en ranuras de tiempo, cada ranura corresponde a una frecuencia de salto y tiene una longitud de 625 *us*. Cada secuencia de salto en una *piconet* está determinada por la dirección del maestro de la *piconet*. Todos los dispositivos conectados a la *piconet* están sincronizados con el canal en salto y tiempo. En una transmisión, cada paquete debe estar alineado con el inicio de una ranura y puede tener una duración de 1, 3 o 5 ranuras de tiempo. Durante la transmisión de un paquete la frecuencia es fija. Para evitar fallas en la transmisión, el maestro inicia enviando en las ranuras de tiempo pares y los esclavos en las ranuras de tiempo impares. En la figura 2.5 se puede observar este esquema de transmisión.

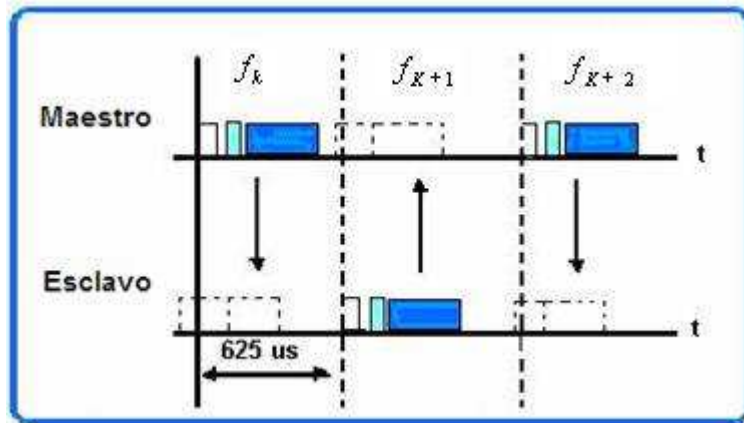


Figura 2.5 Esquema de transmisión en una piconet

2.3.1.4 Potencia

De acuerdo a las especificaciones *Bluetooth* los dispositivos de transmisión se dividen en tres grupos tal como se muestra en la tabla 2.3

| Clase de Transmisor | Potencia Máxima | Potencia Mínima | Alcance Máximo | Control de Potencia |
|---------------------|-----------------|-----------------|----------------|---------------------|
| Clase 1 | 100 mW | 1 mW | 100 m | Obligatorio |
| Clase 2 | 2.5 mW | 0.25mW | 10 m | Opcional |
| Clase 3 | 1mW | ----- | 10 cm. | ----- |

Tabla 2.3 Niveles de Emisión en *Bluetooth*

“El equipo receptor debe poseer una sensibilidad de al menos -70 dBm y la tasa de error admisible debe ser menor o igual a 0.1 %”

Los dispositivos de radio usados son de clase 2 que tienen una potencia de transmisión de 2.5 mW. La tecnología *Bluetooth* está diseñada para tener un consumo de potencia muy bajo. La tabla 2.4 representa la máxima potencia de salida permitida por regiones de acuerdo a la ubicación geográfica.

| Máxima potencia de salida | Localización Geográfica | Documento de Complacencia |
|---------------------------|-------------------------|---------------------------|
| 1000 mW | NORTE AMERICA | FCC 15.247 |
| 100 mW | EUROPA | ETS 300-328 |
| 10 mW/MHz | JAPÓN | MPT ordinance 79 |

Tabla 2.4 Niveles de Potencia de Transmisión para diferentes Regiones

2.3.2 CAPA BANDA BASE

En esta segunda capa se define el descubrimiento de dispositivos, establecimientos de conexión de una *piconet*, direccionamiento, formato de paquetes, temporización, control de potencia y comunicaciones asíncronas y síncronas entre pares.

2.3.2.1.1 Piconet

Dos o más dispositivos *Bluetooth* que comparten un mismo canal forman una *piconet*. Para regular el tráfico en el canal cada *piconet* debe tener un maestro y puede tener hasta siete esclavos activos, además pueden haber muchos más esclavos en estado *parked*². Los participantes podrían intercambiar los papeles si una unidad esclava quisiera asumir el papel de maestra. Sin embargo sólo puede haber un maestro en la *piconet* al mismo tiempo. En la figura 2.6 se puede observar una *piconet*. Si bien un maestro puede serlo de una única *piconet*, un dispositivo cualquiera puede pertenecer a varias *piconets* al mismo tiempo. Este solapamiento se denomina *scatternet* (red dispersa), aunque no se definen capacidades de ruteo por defecto entre ellas.

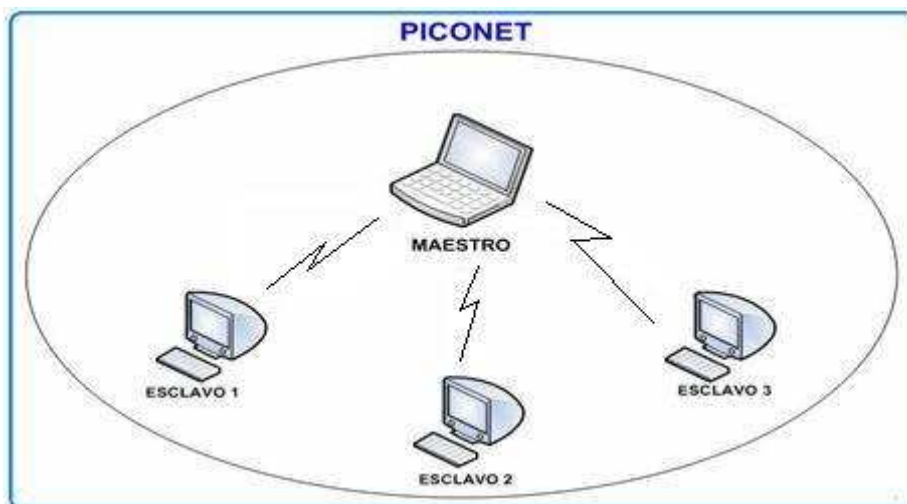


Figura 2.6 Diagrama de equipos que forman una Piconet

El uso de Bluetooth conlleva la creación de redes ad hoc entre nodos Bluetooth. La creación de enlaces requiere dos mecanismos asimétricos de rastreo. El proceso de inspección busca de forma activa dispositivos descubribles que respondan a sus peticiones. El proceso de llamada busca dispositivos que aceptan conexiones, pero a diferencia de la inspección su propósito es localizar dispositivos específicos cuyos atributos sean conocidos (de ahí la analogía con la llamada).

Los dispositivos que forman parte de una piconet comparten el canal físico y disponen de un canal físico y otro lógico entre ellos. Los modos por defecto pueden ajustarse y se pueden añadir enlaces lógicos adicionales. Un dispositivo puede pasar a operar en modo de mantenimiento (hold mode), un estado transitorio que limita la actividad en el enlace físico; también puede establecer un modo de rastreo (sniff) que define periodos de presencia y ausencia en la piconet, que pueden tener efectos en la recepción de información por broadcast no fiable. Los esclavos pueden dejarse en un estado aparcado controlado por el maestro.

2.3.2.1.2 Scatternet

Dos o más *piconets* que comparten una parte de su espacio físico de transmisión (*canal de transmisión*) forman una *scatternet*.

Las *scatternet* permiten aprovechar mejor el ancho de banda, y la velocidad efectiva individual de los usuarios es mucho mayor en la *scatternet* que si todos los usuarios estuviesen conectados a una misma *piconet*.

En la figura 2.7 se puede observar un ejemplo de una red *scatternet*

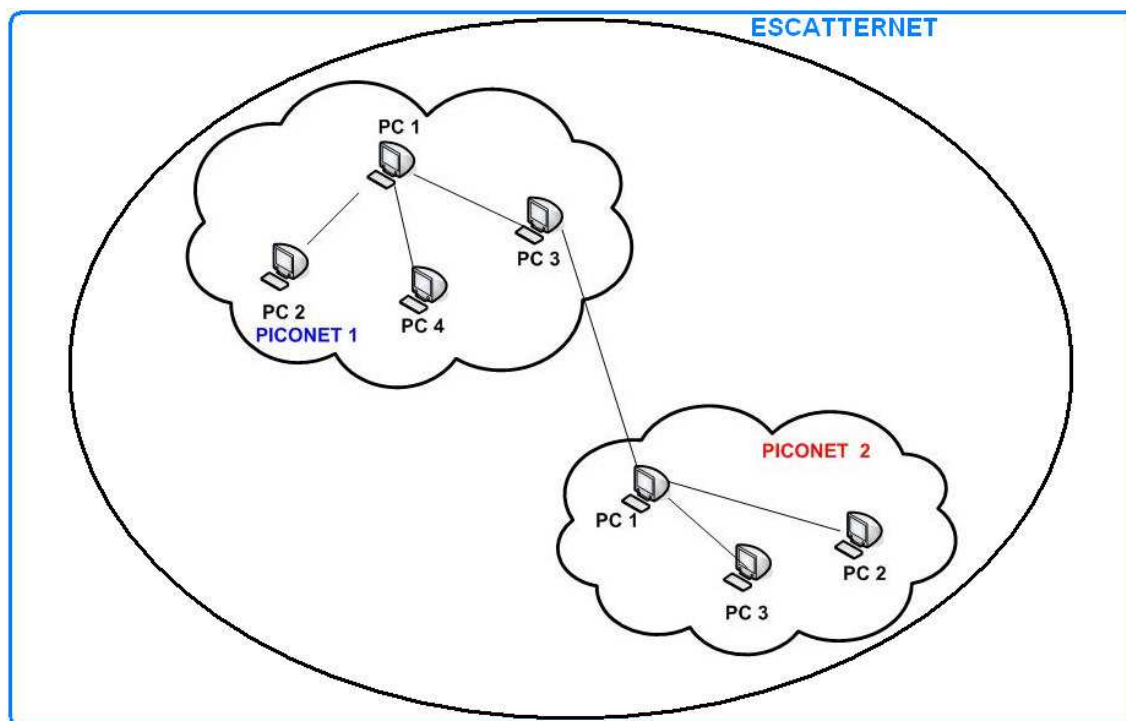


Figura 2.7 Diagrama de equipos que forman una Piconet

Las unidades que se encuentran en el mismo radio de cobertura pueden establecer potencialmente comunicaciones entre ellas. Sin embargo, sólo aquellas unidades que realmente quieran intercambiar información comparten un mismo canal creando la *piconet*. Este hecho permite que se creen varias *piconets* en áreas de cobertura superpuestas. A un grupo de *piconets* se le llama *scatternet*.

El rendimiento, en conjunto e individualmente de los usuarios de una *scatternet* es mayor que el que tiene cada usuario cuando participa en un mismo canal de 1MHz.

Además, estadísticamente se obtienen ganancias por multiplexión y rechazo de canales salto. Debido a que individualmente cada piconet tiene un salto de frecuencia diferente, diferentes piconets pueden usar simultáneamente diferentes canales de salto.

Se debe tener en cuenta que cuantas más *piconets* se añaden a la *scatternet* su velocidad efectiva disminuye poco a poco, existiendo una reducción por término medio del 10%. Sin embargo el rendimiento que finalmente se obtiene de múltiples *piconets* supera al de una simple *piconet*.

Una estimación bastante simplificada de la velocidad efectiva normalizada es:

$$TH = \left(1 - \frac{1}{79}\right)^{N-1} \quad \text{Ecuación 2.1 Velocidad Efectiva Normalizada}$$

Donde: TH = Velocidad Efectiva
N = Número de *Piconets*

La información intercambiada por una *piconet* sólo es compartida por los miembros de la *piconet*, no por toda la *scatternet*. Una unidad puede participar en distintas *piconets* por medio de *TDD* (Duplexación por división de tiempo) pero esta unidad solo puede ser maestra en una sola *piconet*.

2.3.2.2 Enlace Físico

En la especificación *Bluetooth* se han definido dos tipos de enlace que permitan soportar incluso aplicaciones multimedia:

- Enlace sincrónico orientado a conexión (*SCO*)
- Enlace asíncrono no orientado a conexión (*ACL*)

a. Enlace Sincrónico Orientado a Conexión (*SCO*)

Los enlaces *SCO* soportan conexiones simétricas, punto a punto con un ancho de banda fijo entre el maestro y un esclavo específico y conmutación de circuitos, estos enlaces se usan en conexiones de voz, estos enlaces se encuentran definidos en el canal de transmisión, reservándose dos ranuras consecutivas (envío y retorno) en intervalos fijos. La reserva de las ranuras la realiza el maestro cuando se establece la conexión entre el maestro y el esclavo. La conexión *SCO* debe establecerse explícitamente después de que se ha creado la *piconet*.

El maestro envía un mensaje de establecimiento a conexión al esclavo, usando el protocolo de gestión del enlace (*Link Management*). En una conexión *SCO* no se permiten paquetes multi-ranura es decir paquetes que ocupen 2 o más ranuras consecutivas.

En una *piconet* el maestro puede contener hasta tres enlaces *SCO* con un solo esclavo o con esclavos diferentes y el esclavo puede mantener hasta dos enlaces *SCO* si los maestros con los que se comunica son diferentes.

b. Enlace Asíncrono no Orientado a Conexión (ACL)

Los enlaces *ACL* soportan conexiones simétricas o asimétricas, punto a multipunto y con conmutación de paquetes, típicamente usadas en la transmisión de datos. Aquí, a diferencia del anterior, se necesita asegurar la entrega de datos y es utilizado para transferencia de datos sin requerimientos temporales.

Un enlace *ACL* no reserva ancho de banda, usa ranuras por demanda de 1, 3 y 5 ranuras consecutivas también usa control de errores para garantizar la entrega de los paquetes. La máxima velocidad de transmisión se obtiene enviando paquetes sin protección, de 5 ranuras, con capacidad de asignación asimétrica 721 *Kbps* en un sentido y 57,6 *Kbps* en el otro.

Ejemplo de tráfico *SCO* y *ACL* en una *piconet*:

Por defecto cuando, se establece la *piconet* la unidad maestra establece una conexión *ACL* con las unidades esclavas.

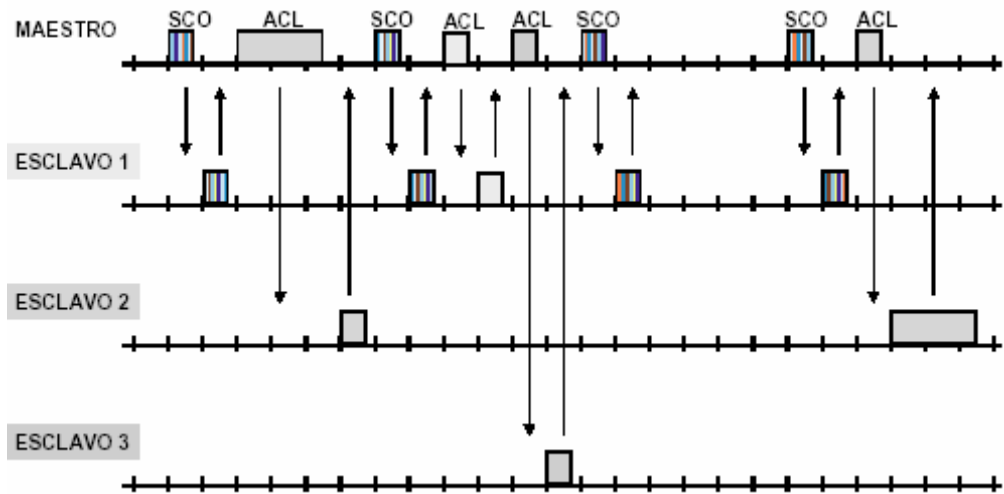


Figura 2.8 Esquema de conexión ACL

2.3.2.3 Formato del Paquete Bluetooth

En Bluetooth todos los datos que se envían a través del canal son fragmentados y enviados en paquetes. Además la información se encuentra protegida mediante códigos detectores y/o correctores de errores.

En cada ranura solo se puede enviar un paquete. El receptor los recibirá y los procesará empezando por el bit menos significativo.

Los paquetes se pueden clasificar en diferentes tipos atendiendo al número de slots (ranuras) que ocupan y dependiendo de si los enlaces son síncronos o asíncronos:

- **Enlaces asíncronos:** La tasa de transmisión máxima que se consigue se sitúa alrededor de 723 kbps. El campo de datos es de longitud variable. Hay tres tipos de paquetes según quepan en 1, 3 o 5 slots.

- **Enlaces síncronos:** El campo de datos de usuario es fijo. Este tipo de enlaces soporta full-duplex con unas tasas de transmisión mucho menores que en el caso de los enlaces asíncronos, alrededor de 64 kbps en los dos sentidos. Sólo hay paquetes que caben en 1 slot.

Los paquetes que ocupan 3 o 5 slots, son denominados multislots. Estos no utilizan saltos de frecuencia. Se envían por la misma frecuencia durante todos los slots que ocupe el paquete. Una vez finalizada la transmisión del paquete se cambia la frecuencia.

La figura 2.9, representa el formato de paquete general el cual consta de tres campos: código de acceso, cabecera y carga útil.

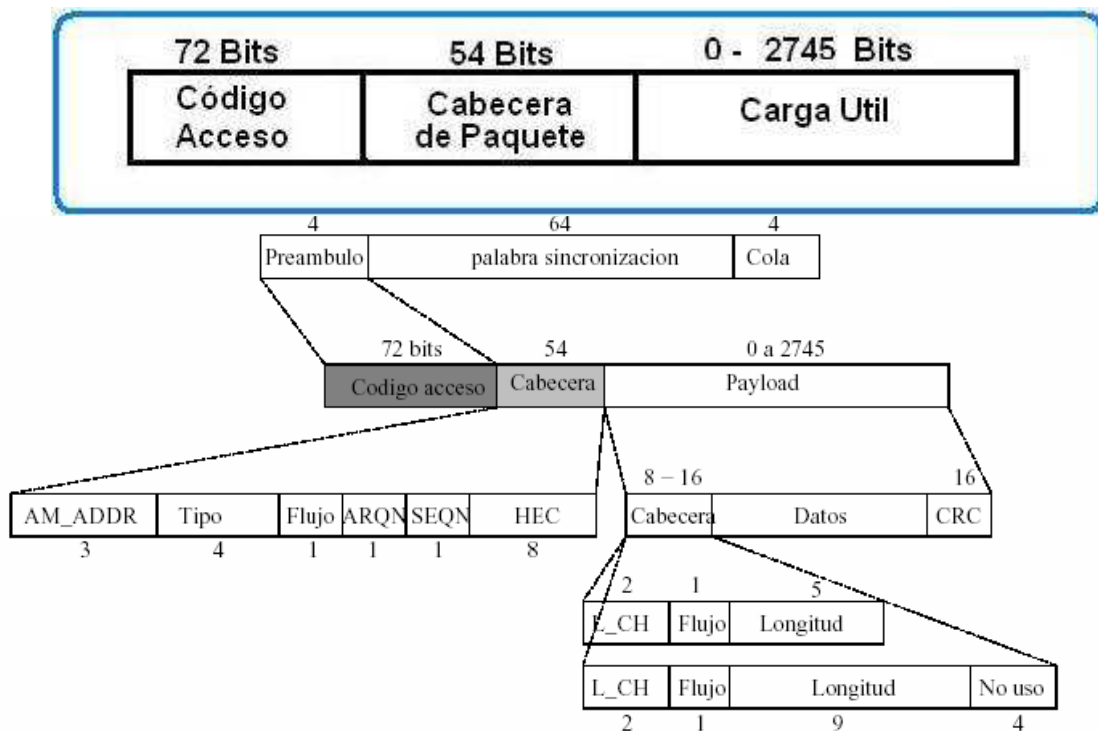


Figura 2.9 Diagrama de paquete Bluetooth

a. Código de acceso

Usado para sincronización, identificación y compensación. Todos los paquetes comunes que son enviados sobre el canal de transmisión en la *piconet* están antepuestos del mismo código de acceso.

Existen tres tipos diferentes de código de acceso:

- **Código de Acceso al Canal (CAC):** identifica una *piconet* y es incluido en todos los paquetes intercambiados dentro de la *piconet*.
- **Código de Acceso de Dispositivo (DAC):** para procedimientos de señalización especiales, *paging* (utilizado para la localización y señalización de un dispositivo), entre otros.
- **Código de Acceso de Búsqueda (IAC):** utilizado para procesos de búsqueda de dispositivos. Se llamara *(IAC) de tipo general* se usa para descubrir otros dispositivos *Bluetooth* dentro de una *piconet*, o *(IAC) dedicado* cuando se quiere descubrir dispositivos *Bluetooth* específicos.

b. Cabecera de paquete

La cabecera contiene información del control del enlace y está formada por seis campos:



Figura 2.10 Diagrama de cabecera del paquete Bluetooth

- **Dirección:** una dirección de dispositivo para distinguirlo de los demás dispositivos activos en la *piconet*. Se tienen 3 bits porque se pueden tener hasta 7 dispositivos activos en la *piconet*. El valor 000 se tiene reservado por el maestro para enviar información a todos los esclavos en la *piconet*.

Dirección *M_ADDR*: permite identificar a los esclavos que están activos dentro de una *piconet*. Si la información está dirigida a todos los esclavos entonces los 3 bits son ceros.

- **Tipo:** define el tipo de paquete enviado. Éste dependerá del enlace asociado al paquete (*SCO* o *ACL*). El campo *Tipo* también indica el número de ranuras que ocupa el paquete actual que puede ser de 1, 3 o 5 ranuras consecutivas en caso de un enlace *ACL*.

- **Flujo:** usado para el control de flujo de los paquetes sobre el enlace *ACL*, para notificar al emisor cuando el *buffer* del receptor está lleno. Si el *buffer* del receptor para el enlace *ACL* está lleno, se devuelve una señal de parada para detener la transmisión de datos (Flujo = 0), esta señal de parada sólo se aplica a paquetes *ACL*, los paquetes con información de control de enlace y *SCO* se siguen recibiendo normalmente. Cuando se vacía el *buffer* del receptor, se devuelve una señal de continuar (Flujo = 1).
- **ARQN:** usado para informar si una transferencia es exitosa o no, *ARQN* puede ser un *ACK* (*ARQN*=1) si la recepción fue exitosa, o un *NAK* (*ARQN*=0) si la recepción fue errónea, en este caso el paquete se retransmite.
- **SEQN:** permite distinguir si el paquete enviado es nuevo o es un paquete retransmitido.
- **HEC:** Código de redundancia para comprobar errores en la transmisión.

c. Carga útil

La carga útil de un paquete puede ser dividida en dos campos:

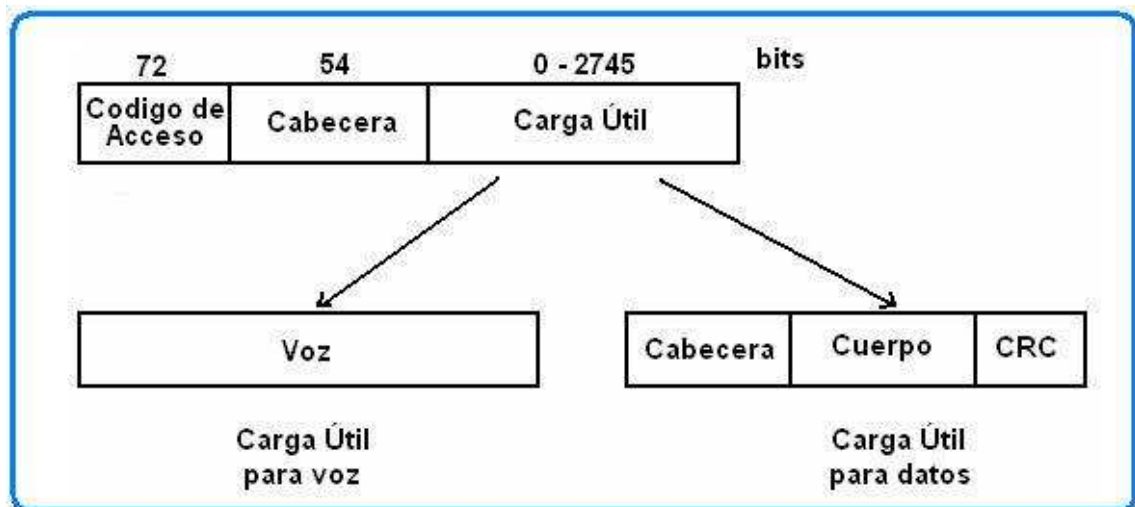


Figura 2.11 Tipos de Datos en la Carga Útil

- **Campo de Voz:** consta de una carga útil, exclusiva para la transmisión de voz. Este campo no posee una cabecera, no realiza chequeo de errores.
- **Campo de Datos:** consta de tres partes, cabecera de carga útil, datos de carga útil, y código *CRC*.

c.1) División de la Carga Útil

Como se puede observar en la figura 2.12, la carga útil destinada para el envío de datos se divide en tres campos que son cabecera, cuerpo y *CRC*.

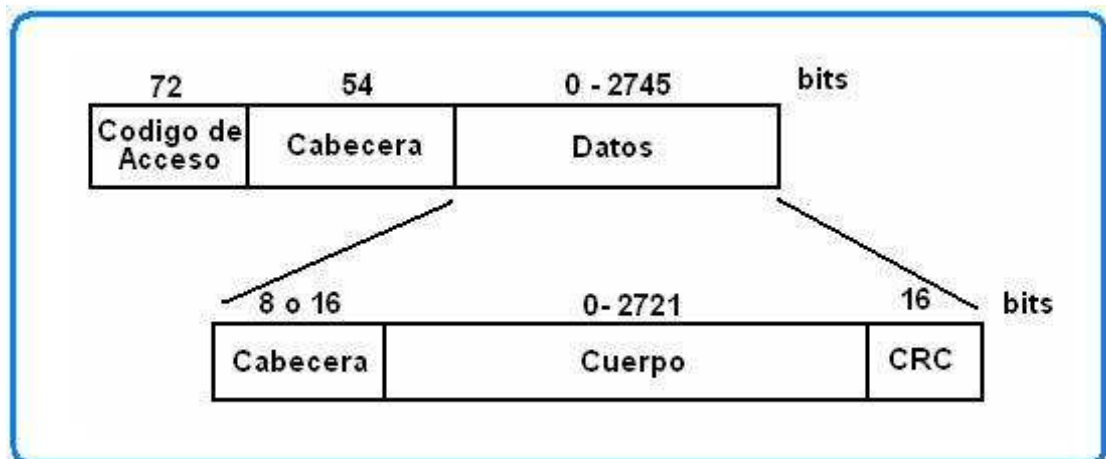


Figura 2.12 División de la Carga Útil para Datos

- **Cabecera de la Carga Útil:** consta de 8 o 16 bits dependiendo si son paquetes de una sola ranura o paquetes multi-ranura.



Figura 2.13 Cabecera de la Carga Útil para Datos

La cabecera de la carga útil consta de los siguientes campos:

- **L_CH:** consta de 2 bits y especifica el canal lógico.
- **Flujo:** campo de un 1 bit y permite realizar el control de flujo de los canales lógicos a nivel de *L2CAP*.

- **Longitud:** la longitud en bytes del cuerpo. Consta de 5 o 9 bits dependiendo si es un paquete que ocupa una sola ranura o es un paquete multi-ranura.
- **Cuerpo de la Carga Útil:** es un campo que va depender del número de bits que se van a transmitir y su longitud puede variar entre 0 y 2721 bits.
- **CRC:** es un campo de 16 bits para chequeo de errores.

2.3.2.4 Tipos de Paquetes

Los tipos de paquetes se dividen en paquetes de control y de información. Los paquetes de control son de cuatro tipos:

- **ID:** paquete de identificación. Consiste solo en el código de acceso.
- **NULL:** consiste en el código de acceso y la cabecera. Sirve para llevar información solo de control.
- **POLL:** similar al anterior; usado por el maestro para invitar a los esclavos.
- **FHS:** paquete de sincronización. Sirve para intercambiar información de identidad e información del reloj.

Los 12 códigos de paquetes restantes sirven para definir el tipo de servicio que se entrega (sincrónico o asincrónico) y el tamaño en ranuras del paquete. Los datos pueden o no ser protegidos con *FEC* (1/3 o 2/3).

Considerando la transmisión sin *FEC* se puede lograr una máxima tasa asimétrica de 723.2 Kbps con un enlace de retorno de 57.6 Kbps.

En la **tabla 2.5** se presentan algunos paquetes para transmisión sincrónica y asincrónica con sus respectivas velocidades.

| PAQUETES | | | |
|-----------------|------------------|-------------------|----------------|
| TIPO | SIMÉTRICO | ASIMÉTRICO | |
| | | ENVÍO | RETORNO |
| DM1 | 108.8 | 108.8 | 108.8 |
| DH1 | 172.8 | 172.8 | 172.8 |
| DM3 | 256.0 | 384.0 | 54.4 |
| DH3 | 384.0 | 576.0 | 86.4 |
| DM5 | 286.7 | 477.8 | 36.3 |
| DH5 | 432.8 | 721.0 | 57.6 |

Tabla 2.5 Paquetes para Transmisión Simétrico y Asimétrico

Máximas tasas de transmisión promedio en Kbps.

- **DMx**: Paquetes de largo x slots, con *FEC*
- **DHx**: Paquetes de largo x slots, sin protección

2.3.2.5 Canales Lógicos

Los canales lógicos definidos en *Bluetooth* son usados para actividades de control y para transporte de datos de usuario. Estos canales lógicos existen sobre los canales físicos *SCO* (Enlace Sincrónico Orientado a Conexión) o *ACL* (Enlace Asincrónico no Orientado a Conexión).

- **Canal de Control LC (*Link Control*)**: implementado a través de la cabecera del paquete excepto en los paquetes de identificación (*ID*) que carecen de encabezado. Se encarga de transportar información de bajo nivel tal como:
 - ✓ Caracterización de la carga útil es decir el tipo de paquete que se envía.
 - ✓ Peticiones de repetición automática
 - ✓ Control de flujo.
- **Canal de Control LM (*Link Manager*)**: transporta información de control para la administración del enlace entre el maestro y uno o más esclavos.

Este canal lógico es transportado en la carga útil y puede estar presente en enlaces *SCO* o *ACL* soportando tráfico *LMP* (Protocolo de Administración del Enlace)

- **Canal de Usuario UA (*User Asynchronous*):** transporta datos asíncronos de usuario. Generalmente es transportado en un enlace *ACL*.
- **Canal de usuario UI (*User Isochronous*):** se encarga de transportar datos isócronos de usuario. Estos datos se caracterizan porque la información de temporización está incluida en la cadena de datos. Los datos isócronos necesitan temporización de forma precisa como es el caso de enviar audio comprimido sobre un enlace *ACL*.
- **Canal de Usuario US (*User Synchronous*):** transporta datos de usuario síncronos y están presentes sobre enlaces físicos *SCO*.

2.3.2.6 Establecimiento de la Conexión

Para el establecimiento de una conexión en *Bluetooth* los dispositivos pueden estar en ciertos estados como son:

- **Inquiry:** el estado de *Inquiry* es un estado de búsqueda que es utilizado para descubrir otros dispositivos.

- **Scan:** cuando un dispositivo *Bluetooth* está en modo *STANDBY* (dormida), periódicamente escucha el canal, esperando a ser descubiertos por otros dispositivos.
- **Paging:** este estado es también llamado como un estado de paginación o localización. Es utilizado, generalmente, luego del estado *Inquiry* para establecer las conexiones.

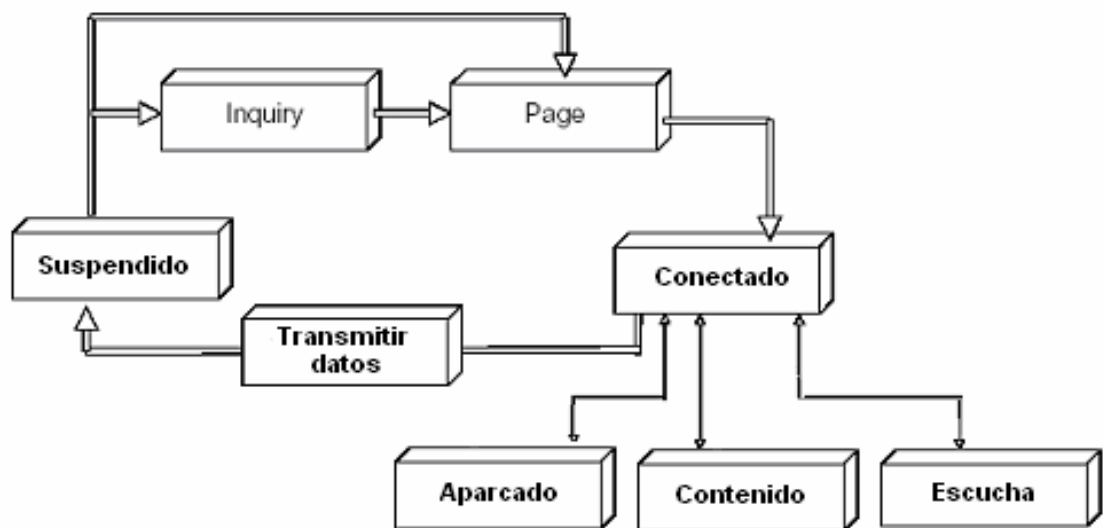


Figura 2.14 Diagrama de Bloques del estado Paging

a. Conexión entre dos dispositivos:



Figura 2.15 Conexión de Dispositivos

En una conexión de dispositivos *Bluetooth*, estos dispositivos pueden estar en diferentes estados como son: estado *Inquiry*, *Scan*, *Paging*. Dependiendo del estado de cada dispositivo la conexión se la puede realizar utilizando los siguientes procedimientos.

a.1. Inquiry

Durante el procedimiento *Inquiry* el nodo fuente invita al nodo destino con un mensaje *inquiry*, luego de escuchar el mensaje de invitación el nodo destino responde la invitación aceptando la comunicación.

La información que envía en el mensaje el nodo fuente es un paquete de *ID* (paquete de identificación) con un código *IAC* (Código de Acceso de Búsqueda).

El paquete *ID* es un paquete que no tiene cabecera ni carga útil y el código *IAC* es un código común para todos los dispositivos *Bluetooth*.

Si el destino recibe el mensaje *Inquiry* responde con un paquete *FHS* (Paquete de Sincronización) que contiene la dirección del dispositivo e información del reloj. Para evitar colisiones, los destinos difieren sus respuestas utilizando un temporizador de *backoff*.

La fuente captura información básica enviada por el destino y esta información es utilizada para hacer el *paging* con el dispositivo destino seleccionado.

A continuación en la figura 2.16 se muestra el proceso de *Inquiry*:

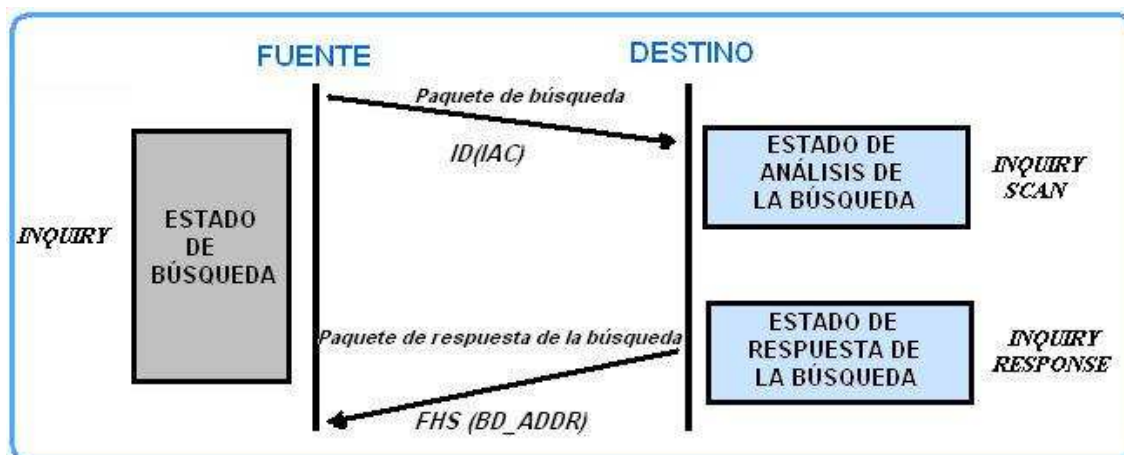


Figura 2.16 Esquema de Proceso de *Inquiry*

Pasos para el procedimiento del *Inquiry*:

- La fuente envía los paquetes de *inquiry*, que llevan la información de identificación y un código de acceso común.
- El destino que recibe los paquetes de *inquiry*, debe estar en el estado *Scan Inquiry*, en el que está atento a recibir los paquetes de *Inquiry*.
- El destino entra al estado de respuesta de la búsqueda o también llamado *Inquiry Response*, en el cual manda una contestación al mensaje de *Inquiry* enviado por la fuente.
- Una vez que el nodo destino responde a un *Inquiry*, se mueve al estado *Page Scan*

a.2. Paging

La fuente envía un mensaje de *paging* que es único al destino. El destino contesta inmediatamente sin necesidad de esperar un periodo de *backoff*.

Para establecer una conexión es necesario conocer la dirección del dispositivo *Bluetooth (BD_ADDR)*.

Esta dirección es también utilizada para el cálculo de la secuencia de salto del *paging* (*page frequency- hopping sequence*), con el cual se contacta al dispositivo durante el *paging*.

El paquete que envía la fuente es un paquete *ID* (Paquete de Identificación) al cual se le ha añadido un Código de Acceso del Dispositivo (*DAC*) este código de acceso del dispositivo contiene una parte de la dirección del dispositivo (*BDADDR*).

Luego de recibir la respuesta al *paging*, la fuente se convierte en el maestro y el destino en esclavo de la nueva *piconet*.

A continuación se representa en la figura 2.17 el procedimiento del *paging*:

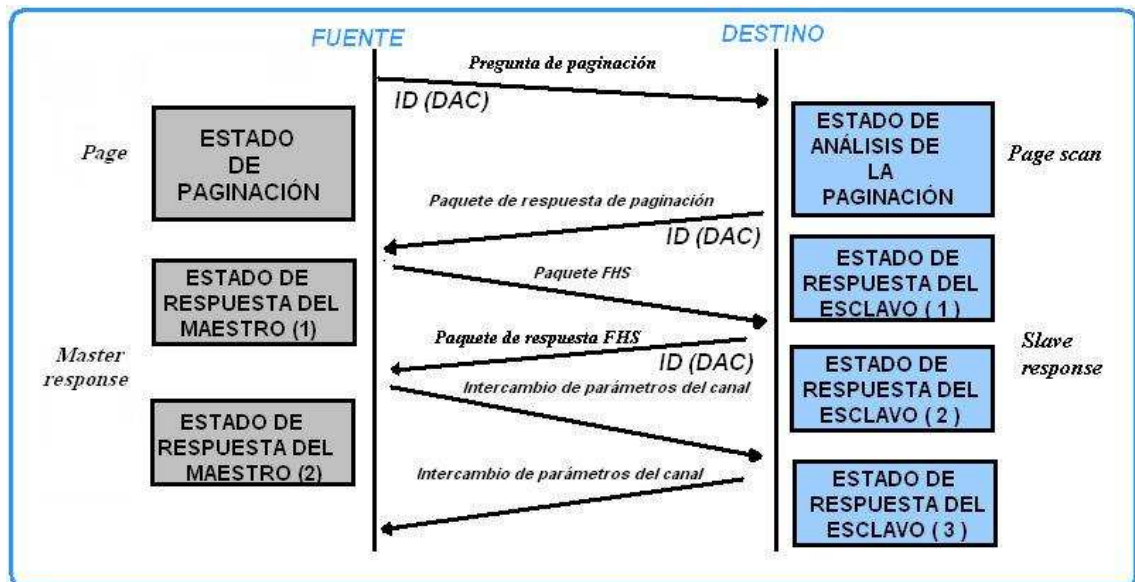


Figura 2.17 Esquema de Proceso de *Paging*
Fuente:

Procedimiento de *paging*:

- La fuente que se encuentra en el estado de *Paging* envía un *page* al destino, que contiene un paquete de Identificación (*ID*) pero esta vez con un Código de Acceso del Dispositivo.
- El destino que se encuentra en el estado de *Page Scan3* recibe el *page*.
- El destino manda una contestación a la fuente que se encuentra en el estado de *Master Response*. Esta contestación contienen un paquete idéntico al recibido (*ID*).
- La fuente que está en el estado de *Master Response* manda un paquete de sincronización (*FHS*) al destino. Este paquete de sincronización contiene la dirección del dispositivo *Bluetooth* fuente y el valor de su reloj de tiempo real *Bluetooth*.
- El destino que se encuentra en el estado *Slave Response* manda una segunda contestación a la fuente, confirmando la recepción del paquete de Sincronización (*FHS*). Esta respuesta es el mismo paquete de identificación con el mismo Código de Acceso del dispositivo.

- La fuente y el destino que se encuentran en los estados *Master Response* y *Slave Response* respectivamente, intercambian los parámetros de sincronización del Canal. El destino empieza a utilizar la secuencia de salto definida por el maestro.

El maestro puede continuar realizando invitaciones a otros dispositivos.

a.3. Admisión de un nuevo esclavo

Los pasos para la admisión de un nuevo esclavo son relativamente complejos. El maestro podría tomar una de las siguientes opciones:

- Empezar a descubrir nuevos nodos e invitarlos a unirse a la *piconet*.
- Esperar a ser descubierto por otros nodos, permaneciendo en un estado *Scan*.

En ambos casos, la comunicación en la *piconet* debe suspenderse durante el proceso de *Inquiry* y *Paging*. El retardo involucrado en la admisión de un nuevo nodo puede ser grande, especialmente si el maestro no pasa al estado de *Inquiry* o *Scan* frecuentemente; esto provoca una degradación en la capacidad de la *piconet*.

La operación de una *piconet* puede entenderse en base a “dos estados de operación” principales que se definen durante el establecimiento de una conexión.

- **Standby:** estado en el que se encuentra una unidad *Bluetooth* por defecto, es un estado de bajo consumo de potencia en el cual solo el reloj local está activo. Los dispositivos que se encuentran en este estado periódicamente entran al estado *Inquiry Scan*.
- **Connection:** en este estado una estación *Bluetooth* puede estar conectada a una *piconet* ya sea como esclavo o como maestro.

Todos los procedimientos se pueden combinar en un solo diagrama de estados, el mismo que se muestra en la figura 2.18.

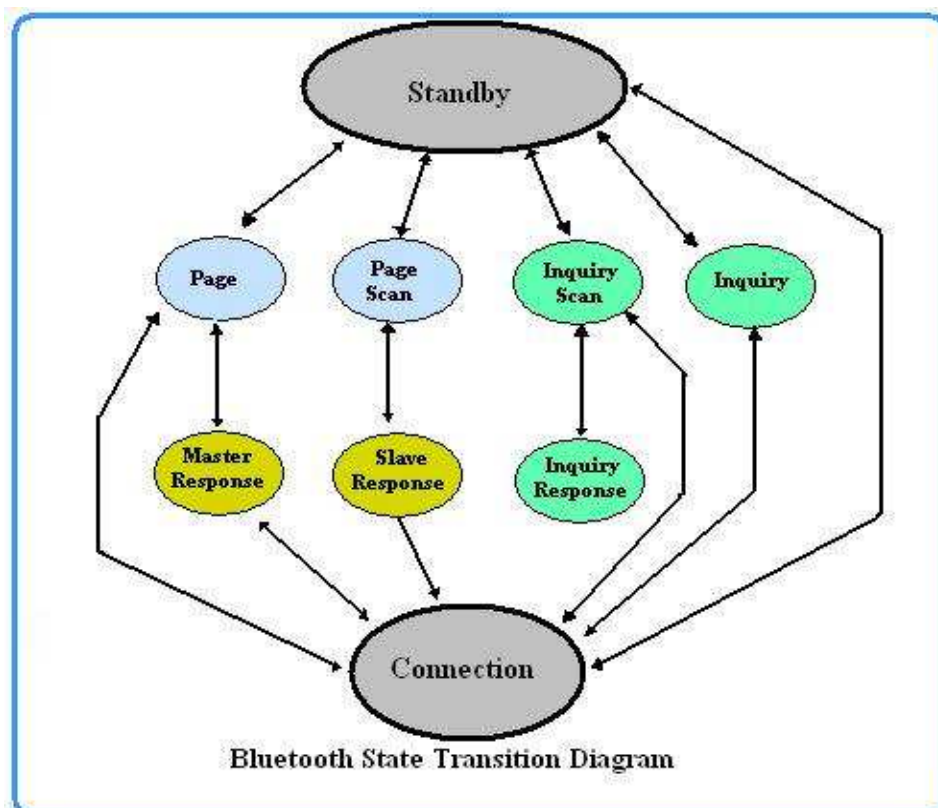


Figura 2.18 Diagrama de Estados de Transición *Bluetooth*
Fuente:

2.3.2.7 Modos de Ahorro de Potencia

Bluetooth es un estándar que permite un ahorro considerable de energía no solo por la baja potencia que utiliza cada dispositivo sino también por la manera como éstos establecen una conexión.

Una unidad en modo *SCAN* se activa durante un pequeño periodo de tiempo de 10 [ms] para reducir el consumo de potencia mientras está en modo “*STANDBY*”.

El modo *PAGE* necesita un consumo mayor de energía debido a que lleva el peso de la incerteza de frecuencia y tiempo. Se prefiere esta configuración debido a que el modo *PAGE* es más infrecuente que el modo *STANDBY*. También para ahorrar energía, las unidades *Bluetooth* que detectan un paquete que no está dirigido hacia ellas siguen en estado *STANDBY*.

Además el esquema *FH* (Salto de Frecuencia) es robusto en términos de sincronización por lo que no es necesario que se estén constantemente enviando señales de temporización, lo que también reduce el consumo de energía. *Bluetooth* además define una serie de técnicas para ahorrar energía:

- **MODO *HOLD***: el maestro puede ordenar al esclavo quedarse en modo *HOLD*. Durante este periodo no hay comunicación posible entre esclavo y maestro. Cuando el periodo expira el esclavo vuelve al canal y permanece sincronizado.

- **MODO *PARK*:** el esclavo también puede ser puesto en modo *PARK*. En este caso el esclavo entra a un ciclo de trabajo en donde los intervalos de escucha del maestro son más largos.
- **MODO *SNIFF*:** el esclavo no escucha todas las ranuras de tiempo, sino que solo escucha algunas. Para entrar al modo *SNIFF*, el esclavo y maestro deben acordar en qué ranuras el esclavo pondrá atención al canal.

2.3.3 PROTOCOLO DE ADMINISTRACIÓN DEL ENLACE *LMP*

El protocolo *LMP* se usa para establecer y controlar un enlace. Las señales son interpretadas y filtradas por el protocolo *LMP* en el lado del receptor, y no se propagan a las capas superiores.

Los mensajes *LMP* son usados para el inicio, seguridad y control del enlace. Estos mensajes de administración del enlace tienen una prioridad mayor que los datos del usuario.

El mensaje *LMP* se transmite siempre en tan sólo un slot y posee mayor prioridad que los datos del usuario y no se propaga a capas superiores. Posee tres campos importantes:

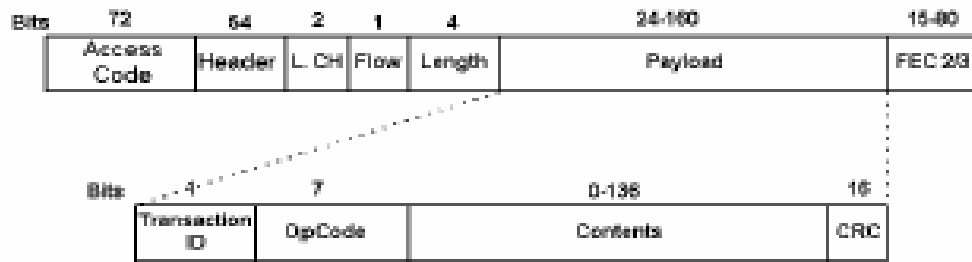


Figura 2.19 Diagrama de paquete LMP

Fuente:

1. **El identificador de transacción:** Nos indica si la PDU que se gestiona pertenece al maestro o al esclavo.
2. **Código de operación:** Es un código de 7 bits que nos permite identificar los diferentes tipos de PDUs.
3. **Campo Content:** contendrá información específica de la aplicación.

2.3.3.1 Emparejamiento con el Protocolo LMP

Si en el momento de iniciar el emparejamiento dos dispositivos *Bluetooth* no tienen una clave de enlace común, entonces se crea una clave de inicialización denominada *Kinit* basada en un número *PIN*, un número aleatorio y una dirección del dispositivo *Bluetooth* (*BD_ADDR*).

Para el procedimiento de emparejamiento existen cinco posibilidades:

- Contestador acepta el procedimiento “emparejamiento”
- Contestador tiene un número *PIN*.

- Contestador rechaza el procedimiento “emparejamiento”
- Creación de una clave de enlace.
- Intentos repetidos

2.3.3.2 Características Soportadas en el enlace

La radiocomunicación *Bluetooth* y el controlador de enlace pueden soportar solo una parte de los tipos de paquetes y características descritas en las especificaciones de Banda Base y Radio de *Bluetooth*. Las características soportadas pueden ser requeridas en cualquier momento, siguiendo un procedimiento exitoso de búsqueda en banda base. Cuando se hace un requerimiento, éste debe ser compatible con las características soportadas del otro dispositivo.

2.3.3.3 Requerimiento de Nombre del enlace LMP

El protocolo *LMP* soporta requerimiento de nombre a otro dispositivo *Bluetooth*, y es un nombre de usuario-amigo asociado al dispositivo.

2.3.3.4 Terminación del emparejamiento de LMP

La conexión entre dos dispositivos *Bluetooth* puede ser terminada en cualquier momento por el dispositivo maestro o por el dispositivo esclavo.

2.3.3.5 Establecimiento de Conexión de LMP

Después del procedimiento de búsqueda, el dispositivo maestro debe invitar al dispositivo esclavo.

2.3.3.6 Modos de Prueba de LMP

Este protocolo tiene *PDU*s para soportar diferentes modos de prueba *Bluetooth*, los cuales se usan para certificaciones y pruebas de cumplimiento de banda base y radio *Bluetooth*.

2.3.4 INTERFAZ DEL CONTROLADOR DE HOST (HCI)

Permite acceder al estado y los registros de control del aparato, además de proporcionar un método uniforme de acceder a todas las funciones de la banda base *Bluetooth*.

La sección *HCI* tiene dos funciones en la especificación *Bluetooth*:

- Definir las bases de una interfaz física para un módulo externo *Bluetooth*.
- Definir las funciones de control necesarias para todas las implementaciones *Bluetooth*.

El computador recibe notificaciones asincrónicas de eventos *HCI* independientemente de que capa de transporte se usa. Los eventos *HCI* son usados para notificar al computador cuando algo ocurre. Al descubrir éste, que ha ocurrido un evento, analizará un paquete recibido para determinar qué tipo de evento *HCI* se tiene.

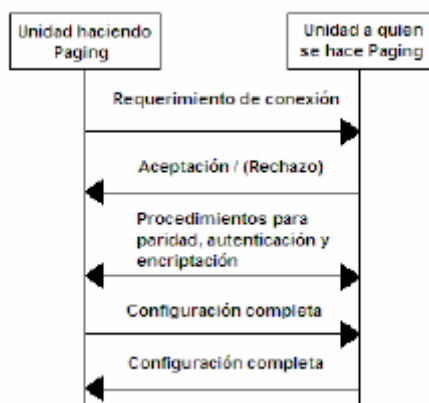


Figura 2.20 Diagrama de comunicación de equipos Bluetooth
Fuente: Proyecto de Tesis

1.1.2.5 Protocolo de Control y Adaptación de Enlace Lógico (*L2CAP*)

L2CAP se encuentra sobre el protocolo de gestión de enlace (*LMP*) y reside en la capa de enlace de datos. *L2CAP* permite a protocolos de niveles superiores y a aplicaciones, la transmisión y recepción de paquetes de datos *L2CAP* de hasta 64Kbytes, con capacidad de multiplexación de protocolo, segmentación y reensamble, y abstracción de grupos.

Para cumplir sus funciones, *L2CAP* espera que la banda base suministre paquetes de datos en los dos sentidos al mismo tiempo, realice el chequeo de integridad de los datos y que reenvíe los datos hasta que hayan sido reconocidos satisfactoriamente.

Las capas superiores que se comunican con *L2CAP* son por ejemplo el protocolo de descubrimiento de servicio (*SDP*), el *RFCOMM* y el control de telefonía (*TCS*).

2.3.4.1 Canales Lógicos de L2CAP

L2CAP está basado en el concepto de canales. Se asocia un identificador de canal, *CID*, a cada uno de los puntos finales de un canal *L2CAP*. Los *CIDs* están divididos en dos grupos, uno con identificadores reservados para funciones *L2CAP* y otro con identificadores libres para implementaciones particulares. Los canales de datos orientados a la conexión representan una conexión entre dos dispositivos, donde un *CID* identifica cada punto final del canal. Los canales no orientados a la conexión limitan el flujo de datos a una sola dirección. La señalización de canal es un ejemplo de un canal reservado. Este canal es usado para crear y establecer canales de datos orientados a la conexión y para negociar cambios en las características de esos canales.

2.3.4.2 Multiplexación de Protocolo

L2CAP soporta Multiplexación de Protocolo, ya que el protocolo de banda base no soporta ningún campo "*TYPE*" que identifica al protocolo de capa superior como protocolos de descubriendo de servicio *SDP*, *RFCOMM* y control de telefonía.

2.3.4.3 Segmentación y Reensamblado

Los paquetes de datos definidos por el protocolo banda base están limitados en tamaño. Los paquetes grandes *L2CAP* deben ser segmentados en varios paquetes más pequeños antes de transmitirse y luego deben ser enviados a la gestión de enlace.

En el receptor los paquetes pequeños recibidos de la banda base son reensamblados en paquetes *L2CAP* más grandes. Varios paquetes banda base recibidos pueden ser reensamblados en un solo paquete *L2CAP* seguido de un simple chequeo de integridad.

La segmentación y reensamblado de paquetes, es necesaria para soportar protocolos con paquetes grandes, que los soportados por la banda base, la figura 2.21 muestra la segmentación *L2CAP*.

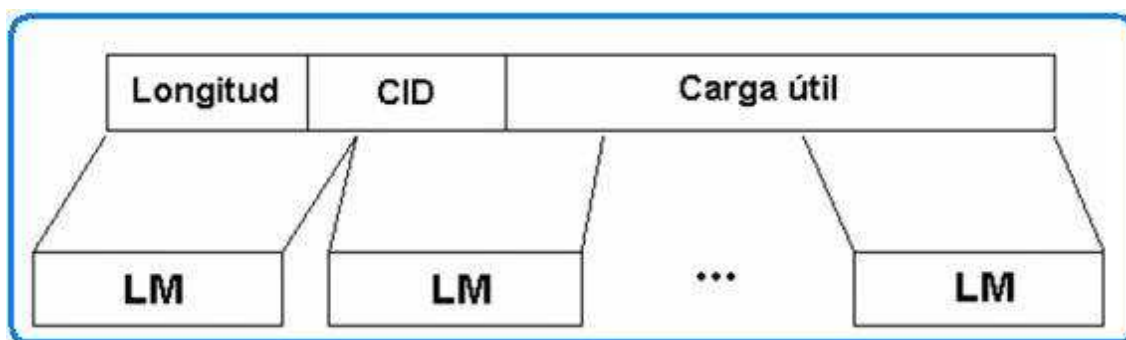


Figura 2.21 Diagrama de segmentación de paquete L2CAP
Fuente:

2.3.4.4 Eventos de L2CAP

Todos los mensajes que entran en la capa *L2CAP*, son llamados eventos. Los eventos se encuentran divididos en cinco categorías: indicaciones y confirmaciones de capas inferiores, peticiones de señal y respuestas de capas *L2CAP*, datos de capas *L2CAP*, peticiones y respuestas de capas superiores, y eventos causados por expiraciones de tiempo.

2.3.4.5 Formato del paquete de datos

L2CAP está basado en paquetes pero sigue un modelo de comunicación basado en canales. Como se puede observar en la figura 2.22, los paquetes de canal orientado a la conexión están divididos en tres campos: longitud de la información, identificador de canal, e información.

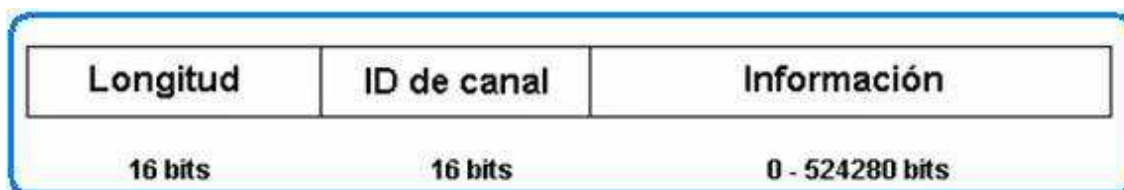


Figura 2.22 Diagrama de paquete *L2CAP*

Fuente: Proyecto de Tesis

Los paquetes de canal de datos no orientados a conexión son iguales a los paquetes orientados a conexión pero adicionalmente incluyen un campo con información multiplexada de protocolo.

2.3.4.6 Protocolo de Descubrimiento de Servicio SDP

El protocolo de descubrimiento de servicio, brinda a las aplicaciones recursos para descubrir qué servicios están disponibles y determinar las características de dichos servicios.

2.3.4.6.1 Descripción General

El *SDP* ofrece a los clientes la facilidad de averiguar sobre servicios que sean requeridos, basándose en la clase de servicio o propiedades específicas de estos servicios.

Los dispositivos *Bluetooth* que usan el *SDP* pueden ser vistos como un servidor y un cliente. El servidor posee los servicios y el cliente es quien desea acceder a ellos. En el *SDP* esto es posible ya que el cliente envía una petición al servidor y el servidor responde con un mensaje. El *SDP* solamente soporta el descubrimiento del servicio, no la llamada del servicio.

2.3.4.6.2 Registros de Servicio

Los registros de servicio contienen propiedades que describen un servicio determinado. Cada propiedad de un registro de servicio consta de dos partes, un identificador de propiedad y un valor de propiedad.

El identificador de propiedades es un número único de 16 bits que distingue cada propiedad de servicio de otro dentro de un registro. El valor de propiedad es un campo de longitud variable que contiene la información.

2.3.4.7 Capa RFCOMM

El protocolo *RFCOMM* brinda emulación de puertos seriales sobre el protocolo *L2CAP*, éste soporta hasta 60 puertos emulados simultáneamente. Dos unidades *Bluetooth* que usen *RFCOMM* en su comunicación pueden abrir varios puertos seriales emulados, los cuales son multiplexados entre sí, la figura 2.23 muestra el esquema de emulación para varios puertos seriales.

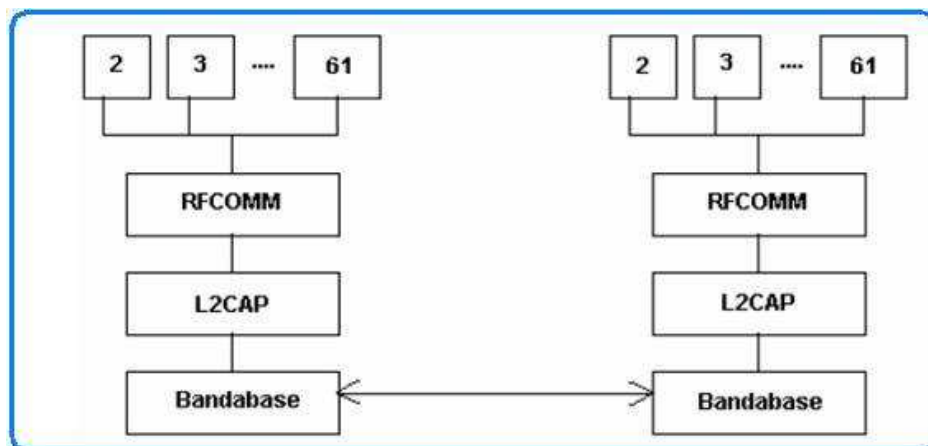


Figura 2.23 Puertos emulados por *RFCOMM*

Muchas aplicaciones hacen uso de puertos seriales. El *RFCOMM* está orientado a hacer más flexibles estos dispositivos, soportando una fácil adaptación de comunicaciones seriales utilizando *Bluetooth*. Un ejemplo de una aplicación de comunicación serial es el protocolo punto-a-punto (*PPP*). El *RFCOMM* tiene construido un esquema para emular el cable que se utiliza en una transmisión serial de datos y usa a *L2CAP* para cumplir con el control de flujo requerido por alguna estación.

2.3.5 PERFILES BLUETOOTH

Son un conjunto de mensajes y procedimientos de la especificación Bluetooth para una situación de uso concreta del equipo. Los perfiles se encuentran asociados con las aplicaciones. Los perfiles permiten que no sea necesario implementar en un determinado dispositivo toda la pila de protocolos, sólo la parte que va a necesitar. Si el dispositivo tiene muy poca memoria y/o capacidad de procesamiento e implementamos en él toda la pila de protocolos con la carga de proceso y espacio que ello implica puede que provoquemos que el dispositivo sea totalmente ineficiente para la comunicación, por ejemplo ratones, auriculares.

Además de la ventaja anterior el concepto de perfil se utiliza para asegurar la interoperabilidad entre varias unidades Bluetooth que cumplan los mismos perfiles. Cada dispositivo Bluetooth tiene al menos un perfil, es decir, una aplicación para la cual se puede utilizar el dispositivo.

Cuando dos dispositivos deben ínter operar, es decir, comunicarse entre ellos, deben tener un perfil compartido. Si por ejemplo quiere transferir un archivo desde un ordenador preparado para Bluetooth a otro, ambos ordenadores deben admitir el perfil de transferencia de archivos.

Los perfiles especifican cómo utilizar el conjunto de protocolos *Bluetooth* para implementar una solución que trabaje sin problemas con otras marcas. En cada uno se establecen opciones y parámetros, además de detallar cómo usar los distintos procedimientos de los diversos estándares que se encuentren implicados.

Todos los dispositivos Bluetooth deben soportar el perfil de acceso genérico (Generic Access Profile) como mínimo. Este perfil en particular define el descubrimiento o hallazgo de dispositivos, procedimientos de conexión y procedimientos para varios niveles de seguridad. También se describen algunos requerimientos de interfaz al usuario. Otro perfil universal, aunque no es requerido, es el perfil de acceso a descubrimiento de servicios (Service Discovery Access Profile), el cual define los protocolos y parámetros asociados requeridos para acceder a los perfiles. Un número de perfiles han sido definidos incluyendo TCS, RFCOMM y OBEX. Algunos de estos requieren la implementación de otros, y todos ellos requieren la implementación de perfiles genéricos.

En la figura 2.24 se observa la estructura de los perfiles Bluetooth.

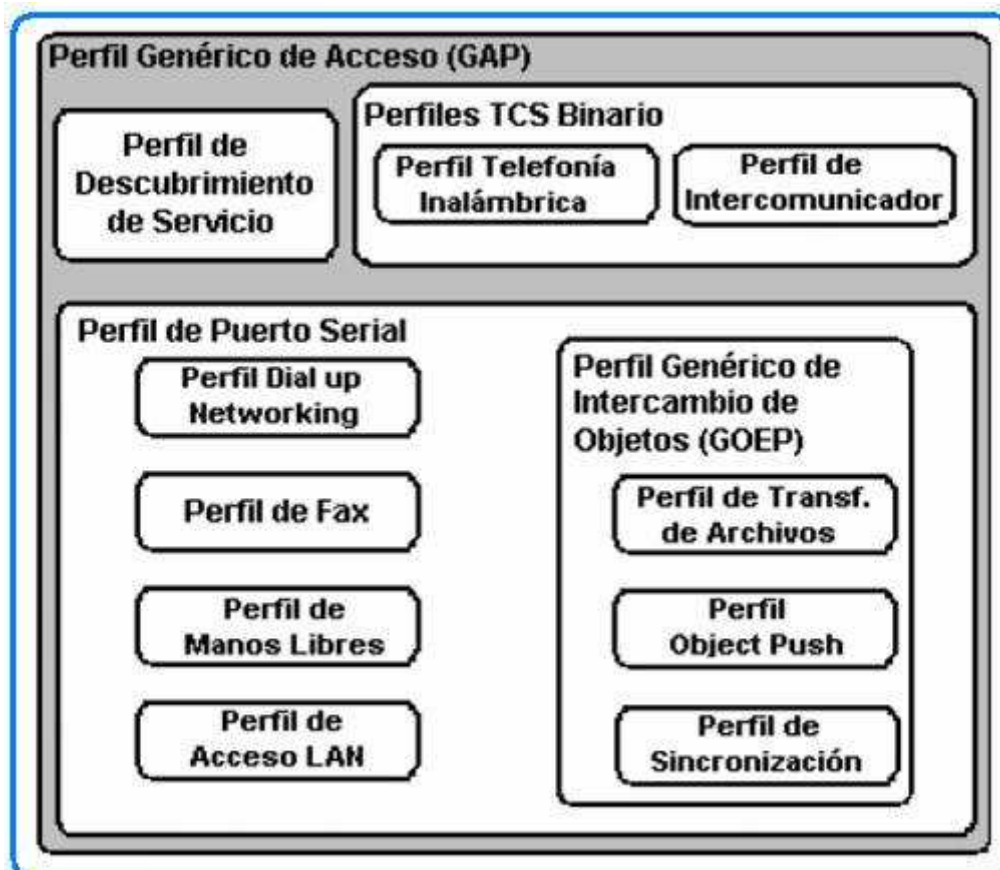


Figura 2.24 Bloque de perfiles Bluetooth
Fuente:

A continuación se hace una breve descripción de algunos de los perfiles *Bluetooth*:

- **Perfil Genérico de Acceso**

Este perfil define los procedimientos generales para el descubrimiento y establecimiento de conexión entre dispositivos Bluetooth. El GAP maneja el descubrimiento y establecimiento entre unidades que no están conectadas y asegura que cualquier par de unidades Bluetooth, sin importar su fabricante o aplicación, puedan intercambiar información a través de Bluetooth.

Para descubrir qué tipo de aplicaciones soportan las unidades. También define aspectos relacionados con los niveles de seguridad

- **Perfil Genérico de Intercambio de Objetos *GOEP***

Este perfil define como los dispositivos Bluetooth deben soportar los modelos de intercambio de objetos, incluyendo el perfil de transferencia de archivos, el de carga de objetos y el de sincronización. Los dispositivos más comunes que usan este perfil son las agendas electrónicas, PDAs y teléfonos móviles. El *GOEP* es dependiente del perfil de puerto serial.

- **Perfil de transferencia de objetos**

Este ofrece la capacidad de transferir un objeto de un dispositivo Bluetooth a otro

- **Perfil de Puerto Serial (SPP)**

El Serial Port Profile (SPP) define los requerimientos específicos para posibilitar la emulación del puerto serie en los dispositivos Bluetooth usando el protocolo RFCOMM entre parejas de dispositivos *Bluetooth* similares.

- **Perfil de Acceso a una LAN (LAP)**

El perfil de acceso a LAN define cómo pueden acceder dispositivos de una *piconet* a los servicios de una LAN como que estuviera conectado a un cable mediante el protocolo punto-a-punto, *PPP* sobre *RFCOMM*, los dispositivos que utilizan la tecnología inalámbrica Bluetooth. De esta manera pueden crearse puntos de acceso inalámbricos.

- **Perfil de Aplicación de Descubrimiento de Servicio (SDAP)**

Este define las características y los procedimientos que un dispositivo Bluetooth usa para descubrir los servicios registrados en otros dispositivos de Bluetooth y para recuperar cualquier información disponible deseada pertinente a estos servicios. El SDAP es dependiente del Perfil Genérico de Acceso GAP.

- **Perfil de Telefonía Inalámbrica**

Este perfil define como un teléfono móvil puede ser usado para acceder a un servicio de telefonía de red fija a través de una estación base. Es usado para telefonía inalámbrica de hogares u oficinas pequeñas. El perfil incluye llamadas a través de una estación base, haciendo llamadas de intercomunicación directa entre dos terminales y accediendo adicionalmente a redes externas. Es usado por dispositivos que implementan el llamado “teléfono 3-en-1”.

- **Perfil de Manos Libres**

Este perfil define los requerimientos, para dispositivos Bluetooth, necesarios para soportar el uso de manos libres. En este caso el dispositivo puede ser usado como unidad de audio inalámbrico de entrada/salida. El perfil soporta comunicación segura y no segura.

- **Perfil *Dial-up Networking***

Este perfil define los protocolos y procedimientos que deben ser usados por dispositivos que implementen el uso del modelo llamado Puente *Internet*. Este perfil es aplicado cuando un teléfono celular es usado como un *modem* inalámbrico.

- **Perfil de *Fax***

El perfil Fax Profile define los requerimientos necesarios para que los dispositivos Bluetooth adquieran soporte de transferencia de Fax. Permitirá que teléfonos Bluetooth puedan enviar y recibir faxes. El *software* de *fax* opera directamente sobre *RFCOMM*.

- **Perfil de Intercomunicador**

El Intercom Profile (IP) define los requerimientos necesarios por parte de los dispositivos Bluetooth para soportar comunicaciones entre parejas de teléfonos con soporte Bluetooth. Estos requerimientos son expresados en términos de servicios para el usuario final. El enlace directo es establecido usando señalización de telefonía sobre *Bluetooth*. Popularmente, este perfil se conoce con el nombre de "Walkie-Talkie".

- **Perfil *Object Push***

Este perfil define protocolos y procedimientos usados en el modelo *object push*. En el modelo *object push* hay procedimientos para introducir en el *inbox*, sacar e intercambiar objetos con otro dispositivo *Bluetooth*.

- **Perfil de Sincronización**

Define protocolos y procedimientos usados en el modelo de sincronización. Éste usa el *GOEP*, el modelo soporta intercambios de información personal, como por ejemplo para sincronizar agendas telefónicas, calendario, mensajes y notas de información de diferentes dispositivos.

CAPITULO 3

SEGURIDAD EN BLUETOOTH

3.1 NIVELES DE SEGURIDAD

La seguridad de Bluetooth es un tema importante y a la vez pendiente en la mayoría de los dispositivos. Un gran parte de los productos en el mercado sufren la interceptación de comunicaciones. No obstante las grandes compañías del sector de las telecomunicaciones y productoras de este tipo de equipos están tomando medidas tanto a nivel de hardware como software.

Para asegurar la protección de la información se ha definido un nivel básico de encriptación, incluido en el diseño del *chip* de radio para proveer seguridad en equipos que carezcan de capacidad de procesamiento, las principales medidas de seguridad son:

- Una rutina de pregunta-respuesta, para autenticación
- Una corriente cifrada de datos, para encriptación
- Generación de una clave de sesión (que puede ser cambiada durante la conexión)

Tres entidades son utilizadas en los algoritmos de seguridad: la dirección de la unidad *Bluetooth*, que es una entidad pública; una clave de usuario privada, como una entidad secreta; y un número aleatorio, que es diferente en cada nueva transacción.

La dirección *Bluetooth* se puede obtener a través de un procedimiento de consulta. La clave privada se deriva durante la inicialización y no es revelada posteriormente. El número aleatorio se genera en un proceso pseudo-aleatorio en cada unidad *Bluetooth*.

La especificación *Bluetooth* detalla tres modos de seguridad bajo los que el protocolo puede operar.

- **Modo1: Sin seguridad.** Todos los mecanismos de seguridad (autenticación y cifrado) están deshabilitados. Además el dispositivo se sitúa en un modo en el cual, permite que todos los dispositivos *Bluetooth* se conecten a él.
- **Modo2: Seguridad a Nivel de Servicio.** Este modo permite un acceso más flexible. Este modo es el más apropiado para ejecutar varias aplicaciones en paralelo con diferentes requerimientos de seguridad. Este modo de seguridad es impuesto después del establecimiento del canal.

- **Modo3: Seguridad a Nivel de Enlace.** El dispositivo instala procedimientos de seguridad antes del establecimiento del canal. Los dispositivos *Bluetooth* solo pueden estar en un solo modo de seguridad en un momento determinado. Un dispositivo que opere en modo 3 no podrá autenticarse ante otros dispositivos de forma selectiva, sino que tratará de autenticarse ante todos los dispositivos que intenten comunicarse con él.

Existe la posibilidad de acceder a un servicio con diferentes accesos de dispositivo:

- **Dispositivo de Confianza:** Tienen acceso sin restricción a los servicios.
- **Dispositivos de NO Confianza:** Tienen un acceso limitado

Catalogados a tres niveles de seguridad

- **Servicios Abiertos:** A los cuales puede acceder cualquier dispositivo.
- **Servicios de Sólo Autenticación:** A los cuales puede acceder cualquier dispositivo que se haya autenticado, puesto que habrá demostrado que comparte una clave de enlace con el proveedor del servicio
- **Servicios de Autenticación y Autorización:** a los cuales sólo tendrán acceso aquellos dispositivos que sean de confianza (y así estarán marcados en la base de datos del servidor).

Actualmente han aparecido dos fenómenos que han comprometido la seguridad de los dispositivos más en concreto de los móviles Bluetooth:

- Bluehacking
- Bluesnarfing

3.1.1 BLUEHACKING

Este sistema se basa principalmente en enviar mensajes con texto, a cualquier equipo Bluetooth sin permiso ni paging con el mismo. La consecuencia es la aparición de lo que ya se ha denominado Blue-Spam, tan odiado ya en el correo de los PCs. Su funcionamiento es el siguiente:

1. Este paso consiste en la creación de un contacto ficticio en la agenda del teléfono.
2. Se inicia el terminal móvil en busca de nuevos móviles en el área próxima.
3. Una vez localizado se le envía el contacto ficticio.

La causa de esta vulnerabilidad es que los terminales Bluetooth se encuentran siempre en disposición de descubrir e iniciar una conexión con cualquier dispositivo que desee conectarse. La solución es apagar la conectividad Bluetooth cuando no se utilice y tan sólo conectarla cuando se desea conectar con un dispositivo conocido.

Este caso el efecto producido por este hacking es mínimo pero si se piensa en el nivel actual de spam en el correo electrónico puede ser un aspecto de seguridad a tener en cuenta.

3.1.2 BLUESNARFING

El Bluesnarfing es algo más complicado de realizar y sus consecuencias no tan inocentes, y que ha provocado que empresas como Nokia deba haber realizado modificaciones en sus diseños de software. El problema es el mismo que en el anterior caso, la vulnerabilidad de que el teléfono se encuentre en modo “visible”, es decir disponible para interactuar con otros dispositivos. En este caso ya no se mandan “inocentes” mensajes sino que se actúa directamente a la funcionalidad de los equipos atacados, robando datos de la agenda, fechas y citas del calendario, y en algunos casos se inicia la navegación por Internet o la clonación del teléfono con los perjuicios económicos que lleva esta práctica sobre el terminal afectado.

3.2 SEGURIDAD CON EL EMPAREJAMIENTO DE DISPOSITIVOS

Al inicio de una comunicación entre dispositivos *Bluetooth* la comunicación entre éstos está protegida, motivo por el que todos los dispositivos pueden comunicarse. Un nodo *Bluetooth* puede solicitar autenticación para realizar un determinado servicio.

Para la autenticación es necesario un código *PIN*. El código *PIN* tiene una longitud de hasta 16 caracteres *ASCII*. Para que los dispositivos se comuniquen se debe ingresar en ambos lados el mismo código *PIN*.

Una vez que el usuario ha introducido el *PIN* adecuado ambos dispositivos generan una clave de enlace. Una vez generada, la clave se puede almacenar en el propio dispositivo o en un dispositivo de almacenamiento externo. La siguiente vez que se comuniquen ambos nodos se utilizará la misma clave.

El procedimiento descrito hasta este punto se denomina emparejamiento. Es importante recordar que si la clave de enlace se pierde en alguno de los dispositivos involucrados se debe volver a ejecutar el procedimiento de emparejamiento.

No existe ninguna limitación en los códigos *PIN* a excepción de su longitud.

3.3 AUTENTICACIÓN BLUETOOTH

Los dispositivos *Bluetooth* se autentican siguiendo el esquema “*challengeresponse*”, desafío-respuesta. A continuación en la figura 3.1 se puede observar el procedimiento de autenticación.

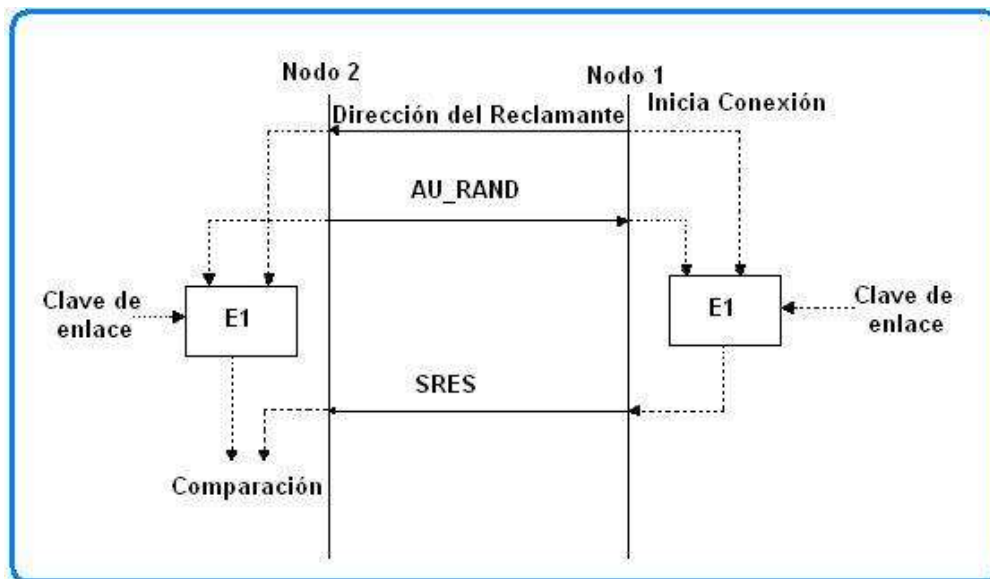


Figura 3.1 Proceso de autenticación *Bluetooth*

Pasos para la autenticación Bluetooth:

- El nodo 1 inicia la conexión transfiere su dirección de 48 bits (*BD_ADDR*) al nodo 2, esta dirección es única e identifica al dispositivo.
- En respuesta el otro nodo 2 le transfiere un “desafío” aleatorio de 128 bits (*AU RAND*) al nodo 1 que inició la conexión.
- El nodo 2 usa el algoritmo E1 para generar el “response” de autenticación, usando como parámetros la dirección del que inició la conexión, *BD_ADDR*, la clave de enlace, *Kab*, y el desafío. El nodo 1 realiza la misma operación.
- El nodo 1 que inició la conexión le devuelve el “response”, *SRES*, al otro nodo.

- El nodo 2 compara el *SRES* del demandante con el que él ha calculado.
- Si los valores de los 32 bits de los *SRES* son idénticos, el verificador establece la conexión.

3.4 APLICACIONES DE BLUETOOTH

En la actualidad se encuentra una gran cantidad de dispositivos *Bluetooth* que ofrecen aplicaciones muy variadas, permitiendo cambiar radicalmente la forma como los usuarios interactúan con los dispositivos que se encuentran relativamente cerca.

Dentro de las aplicaciones se mencionan las siguientes:

- **Transferencia de archivos:** permite la transferencia de archivos sean estos: documentos en *Word*, imágenes, presentaciones en *Power Point*, etc. Además ofrece la posibilidad de ver el contenido de las carpetas existentes en otros dispositivos.
- **Conexión a Internet:** permite tener acceso inalámbrico a Internet mediante un teléfono móvil el cual actúa como si fuera una línea telefónica fija.
- **Escritorio Inalámbrico:** permite reemplazar todos los dispositivos que utilizan cables permitiendo una comunicación vía radio. Utilizando desde un

teclado inalámbrico hasta incluso utilizar un disco duro portátil que emplee esta tecnología para comunicarse.

- **Acceso inalámbrico a LAN:** a través de esta aplicación un grupo de dispositivos *Bluetooth* podrían conectarse a la red de Área Local a través de los llamados *LAP* (Puntos de Acceso *LAN*) y compartir los recursos
- **Sincronización Automática:** este servicio permite sincronizar automáticamente y de manera continua la Información de Administración Personal (*PIM*) con otros dispositivos *Bluetooth*; la información que se actualiza es la concerniente a calendario, lista de direcciones y teléfonos, mensajes y notas.
- **Dispositivo Manos Libres Inalámbrico:** el dispositivo manos libres puede conectarse de manera inalámbrica al teléfono móvil, al ordenador portátil u otro móvil, con el fin de actuar como un dispositivo remoto con entrada y salida de audio.

CAPITULO 4

ESTÁNDAR IEEE

4.1 IEEE 802.15.1 (Bluetooth)

Los principales objetivos que se pretende conseguir con esta norma son la movilidad y la flexibilidad, los cuales vienen a ser fuertes argumentos a favor de la implementación de una Red Local Inalámbrica, en cualquier ambiente:

- Movilidad
- Simplicidad y rapidez en la instalación
- Flexibilidad en la instalación
- Costo de propiedad reducido
- Escalabilidad

Bluetooth es una especificación que define redes de área personal inalámbricas (wireless personal area network, WPAN). Está desarrollada por Bluetooth SIG y, a partir de su versión 1.1, sus niveles más bajos (en concreto, el nivel físico y el control de acceso al medio) se formalizan también en el estándar IEEE 802.15.1. En 2007, la versión más reciente es la 2.1, publicada en julio del mismo año (la revisión actual de IEEE 802.15.1 se aprobó en 2005).

Los estándares que desarrolla definen redes tipo PAN o HAN, centradas en las cortas distancias. Al igual que Bluetooth o ZigBee, el grupo de estándares 802.15 permite que dispositivos portátiles como PC, PDAs, teléfonos, pagers, sensores y actuadores utilizados en domótica, entre otros, puedan comunicarse e interoperar. Debido a que Bluetooth no puede coexistir con una red inalámbrica 802.11.x, se definió este estándar para permitir la interoperabilidad de las redes inalámbricas LAN con las redes tipo PAN o HAN.

4.1.1 Visión general

La especificación principal de Bluetooth (denominada core) define el nivel físico (PHY) y el control de acceso al medio (MAC) de una red inalámbrica de área personal. Este tipo de redes tienen por cometido la transferencia de información en distancias cortas entre un grupo privado de dispositivos. A diferencia de las LAN inalámbricas, están diseñadas para no requerir infraestructura alguna, o muy poca. Aún más, su comunicación no debería trascender más allá de los límites de la red privada.

El objetivo es lograr redes ad hoc simples de bajo coste y consumo. Para ello, Bluetooth define un espacio de operación personal (personal operating space) omnidireccional en el seno del cual se permite la movilidad de los dispositivos.

Se definen tres tipos de dispositivos con diferentes rangos de acción: las clases 1 (cien metros), 2 (diez) y 3 (uno).

El estándar realiza la formalización de estas ideas y se concibe como una solución para evitar el uso de cableado en las comunicaciones. La especificación principal define el sistema básico, pero su diseño potencia la flexibilidad. Por ello, hay multitud de opciones, definidas por los perfiles Bluetooth en especificaciones complementarias.

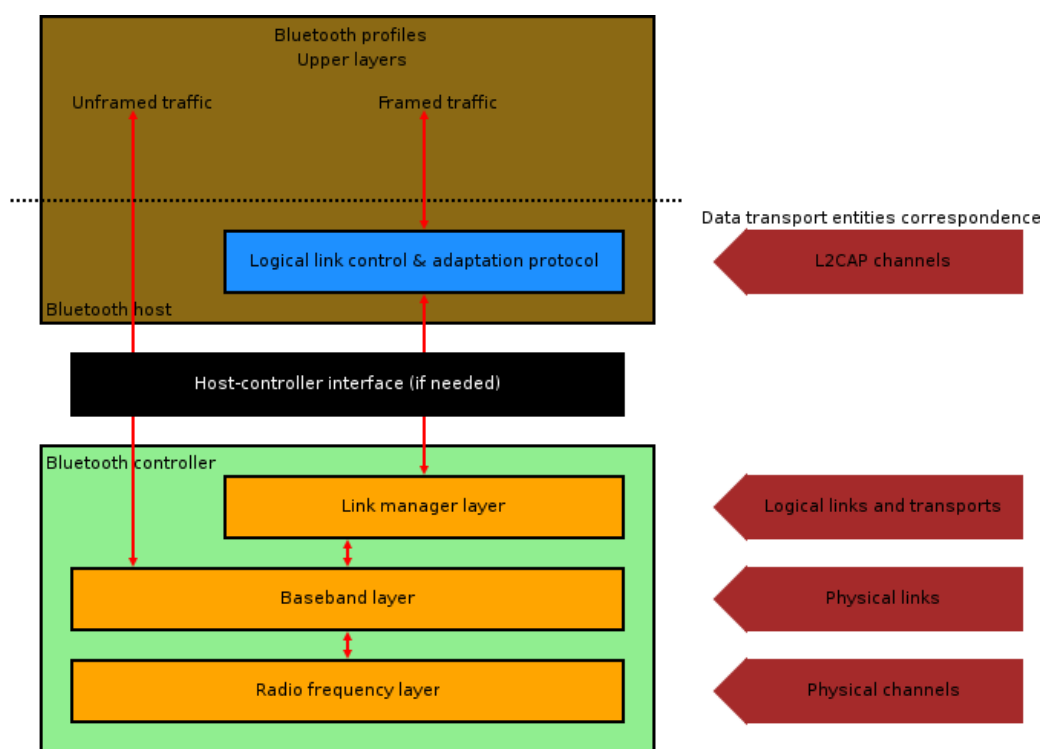


Figura 4.1 Arquitectura IEEE 802.15

Fuente: Documentos IEEE

El nivel de radiofrecuencia (RF) está formado por el transceptor físico y sus componentes asociados. Utiliza la banda ISM de uso no regulado a 2,4 GHz, lo que facilita la consecución de calidad en la señal y la compatibilidad entre transceptores.

| Clase | Potencia máxima permitida (mW) | Potencia máxima permitida (dBm) | Rango (aproximado) |
|----------------|---|--|-------------------------------|
| Clase 1 | 100 mW | 20 dBm | ~100 metros |
| Clase 2 | 2.5 mW | 4 dBm | ~25 metros |
| Clase 3 | 1 mW | 0 dBm | ~1 metro |

Tabla 4.1 Clases de Bluetooth de *IEEE 802.15*

4.2 FACTORES DE PROPAGACIÓN INALÁMBRICA

Son varios los factores a considerar a la hora de diseñar un sistema inalámbrico, algunos de los aspectos a tener en cuenta son los siguientes:

- Cobertura
- Rendimiento
- Interferencia

Entre los diferentes factores que afectan a la cobertura y rendimiento de un sistema inalámbrico se puede mencionar los siguientes:

4.3 ATENUACIÓN Y ABSORCIÓN DE ONDAS

El espacio libre puede ser considerado como el vacío y no se consideran pérdidas. Cuando las ondas electromagnéticas se encuentran en el vacío, se llegan a dispersar y se reduce la intensidad de potencia a lo que es llamado atenuación. La atenuación se presenta tanto en el espacio libre como en la atmósfera terrestre. La atmósfera terrestre no se le considera vacío debido a que contiene partículas que pueden absorber la energía electromagnética y a este tipo de reducción de potencia se le llama pérdida por absorción la cual no se presenta cuando las ondas viajan afuera de la atmósfera terrestre

4.3.1 ATENUACIÓN

La reducción de la intensidad de potencia con la distancia equivale a una pérdida de potencia y se suele llamar atenuación de la onda electromagnética. La atenuación de la onda se expresa en general en función del logaritmo de la relación de intensidades de potencia (pérdida en dB), la definición matemática de la atenuación es:

$$\gamma_a = 10 \log \frac{P_1}{P_2} \quad \text{Ecuación 4.1}$$

La reducción de la intensidad de potencia debida a la propagación en el espacio no libre se llama absorción.

4.3.2 ABSORCIÓN

Las ondas de radio que viajan por la atmósfera terrestre son atenuadas o debilitadas mediante la transferencia de energía a este medio. Entre los diferentes materiales que pueden absorber las ondas electromagnéticas se puede mencionar los siguientes: rocas, ladrillos, concreto, madera, árboles y otros materiales.

La absorción de onda por la atmósfera es análoga a una pérdida de potencia $I R^2$. Una vez absorbida la energía de onda ésta se pierde, y causa una atenuación en las intensidades de campo eléctrico, campo magnético, y una reducción en intensidad de potencia.

4.4 PÉRDIDAS EXISTENTES EN UN RADIO ENLACE

4.4.1 Pérdidas en la Trayectoria en el Espacio Libre (*L patch*)

Se define como la pérdida incurrida por una onda electromagnética al propagarse en línea recta a través del vacío, sin energías de absorción o reflexión debidas a objetos cercanos. Estas pérdidas dependen de la frecuencia, y aumentan con la distancia.

La ecuación para determinar estas pérdidas es la siguiente:

$$L_{\text{patch}} = \left(\frac{4\pi \cdot R}{\lambda} \right)^2 = \left(\frac{4\pi \cdot f \cdot R}{c} \right)^2 \quad \text{Ecuación 4.2}$$

Donde:

Patch L = pérdidas en la trayectoria en espacio libre (adimensional)

R = distancia máxima entre dispositivos (metros)

f = frecuencia (hertz)

λ = longitud de onda (metros)

c = velocidad de la luz en el espacio libre (3*10⁸ m/s)

Al pasar a dB se obtiene

$$L_{p(dB)} = 10 * \log \left(\frac{4\pi \cdot f \cdot R}{c} \right)^2$$

$$L_{p(dB)} = 20 * \log \left(\frac{4\pi \cdot f \cdot R}{c} \right)$$

$$L_{p(dB)} = 20 * \log \left(\frac{4\pi}{c} \right) + 20 * \log f + 20 * \log R \quad \text{Ecuación 4.3}$$

4.4.2 Desvanecimiento por Múltiple Trayectoria (*L fade*)

En esencia el desvanecimiento por multitrayectoria es un factor ficticio que se incluye en la ecuación del cálculo de potencia de recepción (ecuación 1.6), para tener en cuenta las características no ideales y menos predecibles de la propagación de las ondas de radio.

Estas reflexiones multitrayectoria de la onda transmitida se deben a obstáculos naturales o a objetos que actúan como dispersores, entre estos se puede citar: muebles, ventanas, paredes, puertas metálicas, etc. Pequeñas variaciones en la distancia entre emisor y receptor, del orden de una cuarta parte de la longitud de onda por ejemplo, pueden causar grandes cambios en la amplitud o en la fase de la señal.

Estas características de desvanecimientos son propias del área donde se quiera implementar la red inalámbrica, estos desvanecimientos alteran las pérdidas en la trayectoria en espacio libre, y por lo general, son perjudiciales para la eficiencia general del sistema.

Cuando la señal electromagnética se propaga por una estancia es afectada por múltiples fenómenos debido a los diferentes tipos de obstáculos que debe atravesar o en los cuales es reflejado. Es por tanto imprescindible tener en cuenta estos fenómenos, que causan atenuaciones y desvanecimientos de la señal original, a la hora de diseñar un enlace inalámbrico en ambientes internos.

4.4.2.1 Reflexión

Cuando una onda electromagnética que se propaga por el aire incide contra un objeto de grandes dimensiones en comparación con la longitud de onda se dice que ocurre reflexión.

La consecuencia de este fenómeno es que la señal puede ser absorbida, reflejada o a su vez una combinación de ambas. Esta reacción depende principalmente de:

- Propiedades de la señal, como orientación, ángulo de incidencia y longitud de onda.
- Propiedades físicas del obstáculo, como su geometría, textura y composición.

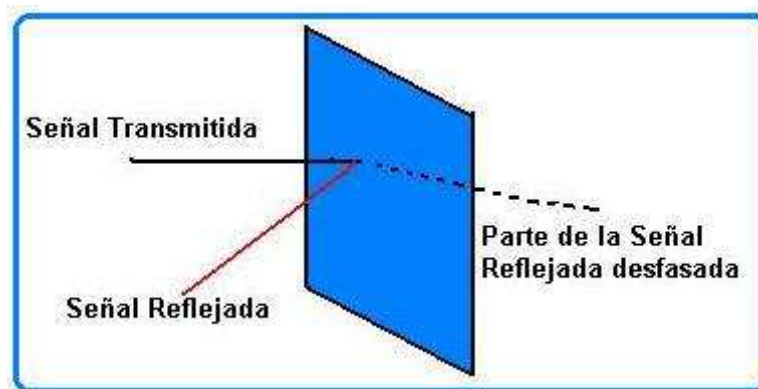


Figura 4.2 Reflexión de una señal
Fuente: Documentos IEEE

4.4.2.2 Penetración

La penetración es la capacidad de transmisión de una señal cuando ésta se encuentra en su camino con un obstáculo, cuando una señal penetra un obstáculo experimenta una pérdida, la cual será función del tipo de objeto.

En la tabla 4.2 se encuentran las pérdidas de penetración predecibles dependiendo del material.

| Tipo de obstáculo | Pérdida (dB) |
|--|--------------|
| Espacio abierto | 0 |
| Ventana metálica (tintado no metálico) | 3 |
| Ventana metálica (tintado metálico) | 5 - 8 |
| Muros finos | 5 - 8 |
| Muros medios de madera | 10 |
| Muros gruesos | 15-20 |
| Muros muy gruesos | 20-25 |
| Suelo/Techo grueso | 15-20 |
| Suelo/Techo muy grueso | 20-25 |

Tabla 4.2 Penetración a través de diferentes tipos de materiales

4.4.2.3 Difracción

La difracción ocurre cuando los obstáculos son impenetrables por las ondas de radio, el resultado de este fenómeno son ondas secundarias alrededor y detrás del obstáculo. La señal difractada depende de la geometría del objeto así como la amplitud, fase y polarización de la onda incidente en el punto de difracción.



Figura 4.3 Difracción de Señal
Fuente: Documentos IEEE

4.4.2.4 *Dispersión*

Cuando una señal transmitida se encuentra en el camino con objetos cuyas dimensiones son pequeñas con relación a la longitud de onda ocurre una dispersión.

El resultado es que el frente de onda se rompe o se dispersa en múltiples direcciones.

La dispersión en la práctica es provocada por:

- Señales de tráfico, focos.
- Conductos para los servicios eléctricos
- Estructuras de hierro forjado y tuberías.

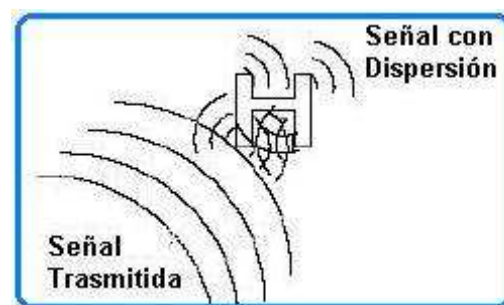


Figura 4.4 Dispersión de Señal
Fuente: Documentos IEEE

4.4.2.5 *Interferencia*

Las interferencias de radio frecuencia son uno de los asuntos más importantes a tener en cuenta para el éxito en el diseño, operación y mantenimiento de sistemas inalámbricos.

La señal de interferencia se caracteriza por ser una señal de naturaleza similar a la deseada, la misma que perturba a la señal que se desea transmitir. Se produce interferencia eléctrica cuando las señales de información de una fuente producen frecuencias que caen fuera de su ancho de banda asignado, e interfieren con otras señales de otra fuente.

“Las fuentes potenciales de interferencia de este tipo son numerosas: materiales metálicos, aislamientos, pinturas de plomo, etc. y pueden reducir la calidad de la señal radioeléctrica.”

Existen otros dispositivos que utilizan la misma banda de frecuencia que también pueden ser fuente de interferencias como hornos microondas y ciertos teléfonos inalámbricos.

4.5 GANANCIA DE LA ANTENA

La ganancia de la antena es la relación entre la intensidad de potencia radiada por la antena en una dirección específica y la intensidad de potencia radiada por una antena isotrópica alimentada con la misma potencia.

La mayoría de fabricantes especifica la ganancia de la antena en dBi (decibelios isotrópicos).

Cada antena posee una ganancia diferente, la cual depende; de los materiales de elaboración, método de propagación (omnidireccionales o direccionales), es por eso que es necesario definir las características importantes de las antenas.

4.5.1 Características de las antenas

4.5.1.1 Diagrama de Radiación

El diagrama de radiación o lóbulo de radiación es la forma como se propaga la onda electromagnética. De acuerdo al diagrama de radiación existen dos tipos básicos de antenas que son; omnidireccionales y direccionales.

4.5.1.1.1 Antenas Omnidireccionales

Una antena omnidireccional es aquella diseñada para proveer un patrón de radiación de 360°. Propagan la señal de *RF* en todas las direcciones en el plano horizontal aunque tienen un rango limitado en el plano vertical. Son las más comunes en *WLAN* y se utilizan cuando se requiere dotar en un plano cobertura en todas las direcciones. Proporcionan la cobertura más amplia dentro de edificios, pudiendo formar celdas circulares mínimamente solapadas a lo largo del edificio.

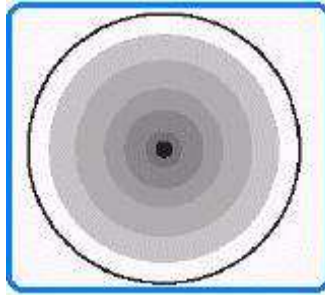


Figura 4.5 Diagrama de Radiación de una Antena Omnidireccional
Fuente: Documentos IEEE

4.5.1.1.2 Antenas Direccionales

Las antenas direccionales son aquellas que han sido concebidas y construidas para que la mayor parte de la energía sea radiada en una dirección en concreto. Puede darse el caso en que se desee emitir en varias direcciones, pero siempre que se este hablando de un número de direcciones determinado donde se encontrarán el lóbulo principal y los secundarios. Existen diferentes tipos de antena direccionales, cada una con una forma y estilo determinado, incluyendo *yagis*, antenas *patch* y parabólicas.

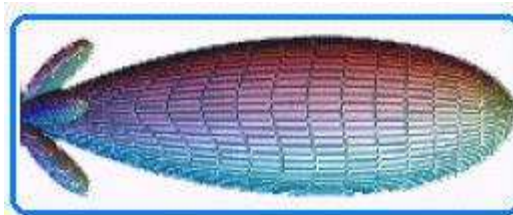


Figura 4.6 Diagrama de Radiación de una Antena Direccional
Fuente: Documentos IEEE

4.5.1.2 Polarización de la Antena

La polarización de una antena se refiere sólo a la orientación del campo eléctrico radiado desde ésta. Una antena puede polarizarse en forma lineal (en general, polarizada horizontal o vertical), en forma elíptica o circular.

Si una antena irradia una onda electromagnética polarizada verticalmente perpendicular al suelo, la antena se encuentra polarizada verticalmente; si la antena irradia una onda electromagnética polarizada horizontalmente paralela al suelo, se dice que la antena está polarizada horizontalmente.

4.5.1.3 Ancho de Banda

El ancho de banda de la antena se define como el rango de frecuencias sobre las cuales la operación de la antena es "satisfactoria". Esto, por lo general, se toma entre los puntos de media potencia, pero a veces se refiere a las variaciones en la impedancia de entrada de la antena.

En *WLANs* las antenas tienen que estar sintonizadas para la banda de 2.4 GHz (802.11b/g) o 5 GHz (802.11a). Una antena funcionará de modo eficiente sólo si su ancho de banda está dentro de las frecuencias de radio utilizadas.

CAPITULO 5

MODELOS PARA EL CÁLCULO DEL ENLACE

5.1 MODELOS PARA CALCULOS

El cálculo del enlace consiste en calcular la potencia de recepción tomando en cuenta los diferentes obstáculos y dispositivos que pueden interferir con la señal transmitida y compararla con la sensibilidad del dispositivo, para determinar si estos cumplen con los requerimientos de cobertura del sistema inalámbrico.

5.1.1 Modelos para el cálculo del enlace bluetooth

Para el cálculo del enlace *Bluetooth* se consideró modelos para ambientes internos, ya que la implementación y las pruebas de los prototipos se las realizó en este tipo de entornos. A continuación se presentan los modelos analizados:

5.1.2 Modelo que considera las Pérdidas en la Trayectoria y Desvanecimientos

Multitrayectoria

En este modelo la señal está sujeta a pérdidas en la trayectoria (*L_{patch}*) y desvanecimientos multitrayectoria (*L_{fade}*) debido a la presencia de obstáculos.

Para el cálculo de la potencia que se espera recibir en el receptor se debe considerar además las ganancias de las antenas tanto transmisora como receptora, dando como resultado la siguiente expresión:

$$P_{RX} [mW] = \frac{P_{TX} [mW] \cdot G_{TX} \cdot G_{RX}}{L_{patch} \cdot L_{fade}} \quad \text{Ecuación 5.1}$$

Donde:

- $P_{RX} [mW]$ = Potencia de recepción
- $P_{TX} [mW]$ = Potencia de transmisión
- G_{TX} = Ganancia de la antena transmisora
- G_{RX} = Ganancia de la antena receptora
- L_{patch} = Pérdidas en la trayectoria
- L_{fade} = Desvanecimientos por multitrayectoria

Si se transforma la ecuación 1.5 a dB se tiene:

$$P_{RX} [dBm] = P_{TX} [dBm] + G_{TX} [dB] + G_{RX} [dB] - L_{patch} [dB] - L_{fade} [dB] \quad \text{Ecuación 5.2}$$

Las antenas utilizadas en la banda *ISM* no permiten antenas de alta directividad por lo que se usan antenas *omnidireccionales* con ganancia unitaria, con lo cual la ecuación 1.6 queda de la siguiente forma:

$$P_{RX} [dB] = P_{TX} [dBm] - L_{path} [dB] - L_{fade} [dB] \quad \text{Ecuación 5.3}$$

Las pérdidas por trayectoria se asumen a través de estimaciones de la siguiente forma:

$$L_{path} = 20 \log\left(\frac{4 \cdot \pi \cdot R}{\lambda}\right) \approx 40 + 20 \log(R) \quad R \leq 8.5[m]$$

$$L_{path} = 36 \log\left(\frac{4 \cdot \pi \cdot R}{\lambda}\right) - 46.7 [dB] \approx 25.3 + 36 \log(R) \quad R > 8.5[m] \quad \text{Ecuación 5.4}$$

“Las pérdidas por desvanecimientos (fade L) se asumen de 8[dB], se asume este valor ya que se estima una confiabilidad del sistema igual al 90%”. Los desvanecimientos más profundos serán absorbidos por la diversidad de frecuencia del canal y causarán solo interrupciones ocasionales.

Entonces la ecuación para el cálculo del enlace para *Bluetooth* es la siguiente:

$$P_{RX} [dB] = P_{TX} [dBm] - L_{path} [dB] - 8 [dB] \quad \text{Ecuación 5.5}$$

5.1.3 Modelo de Atenuación Lineal por Trayectoria

Este modelo es realmente sencillo en cuanto a su parte de aplicación teórica, pues la parte real de mediciones por pérdidas por trayectoria tienen un gran peso. Andelman

lo propuso en el 2004 como un modelo a utilizarse cuando el transmisor y el receptor se encuentran en el mismo piso.

Este modelo de pérdidas por trayectoria lineal toma en cuenta trayectorias para interiores a partir de la potencia radiada, estas pérdidas están dadas por las pérdidas en el modelo del espacio libre, más el factor lineal que se obtiene experimentalmente.

La ecuación que describe las pérdidas en este modelo es la siguiente:

$$L = L_{FS} + a * d \quad \text{Ecuación 5.6}$$

Donde:

L_{FS} = Pérdidas en el espacio libre

a = Coeficiente de atenuación lineal

d = distancia entre el transmisor y el receptor

“El coeficiente de atenuación lineal para un ambiente de oficinas es $a=0.47$ [dB/m]”

Introduciendo la ecuación 1.4 en la ecuación 1.11 se tiene la siguiente ecuación:

$$L = 20 * \log\left(\frac{4\pi * f}{c}\right) + 20 * \log(d) + a * d \quad \text{Ecuación 5.7}$$

Para una frecuencia $f=2.4 \text{ GHz}$, la velocidad de la luz $C = 3 * 10^8 \text{ m/s}$ y el coeficiente de atenuación lineal $a = 0.47$ se tiene:

$$L = 40.1 + 20 * \log(d) + 0.47 * d \quad \text{Ecuación 5.8}$$

Tomando en cuenta que se usan antenas *omnidireccionales* con ganancia unitaria y las pérdidas totales la ecuación para el cálculo del enlace para *Bluetooth* es la siguiente:

$$P_{RX} [\text{dBm}] = P_{TX} [\text{dBm}] - 20 * \log(d) [\text{dB}] - 0.47 * d [\text{dB}] - 40.1 [\text{dB}] \quad \text{Ecuación 5.9}$$

CAPITULO 6

MUESTREO Y TABULACION

6.1 METODO DE MUESTREO

6.1.1 Método Probabilístico; Muestreo Aleatorio Simple

Muestra

- N** ?
Z 95% - 1.96 margen de confiabilidad o número de unidades de desviación estándar
S 677 Alumnos - po - todos los alumnos
E 125 Alumnos - error de estimación, esperamos que no sea mayor de 125 alumnos
N 552 Alumnos - tamaño de población

$$n = \frac{S^2}{\frac{\epsilon^2}{Z^2} + \frac{S^2}{N}}$$

Ecuacion 6.1 Muestreo aleatorio simple

$$n = \frac{(677)^2}{\frac{(125)^2}{(1.96)^2} + \frac{(677)^2}{552}}$$
$$n = \frac{458329}{\frac{15625}{3,8416} + \frac{458329}{552}}$$
$$n = \frac{458329}{4067,32 + 830,31}$$
$$n = \frac{458329}{4897,62}$$

$$n = 93.58 \neq 94$$

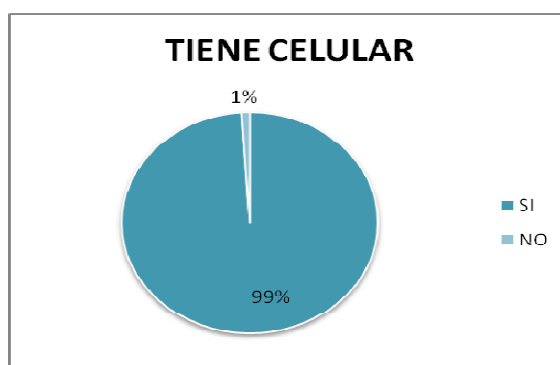
6.2 TABULACION DE ENCUESTAS

Se escogió a 94 alumnos de la Facultad Técnica al azar según los resultados obtenidos en el cálculo de la muestra para verificar la efectividad y aceptación de esta tecnología.

A continuación se muestra los resultados de las encuestas que están en el **ANEXO 1**.

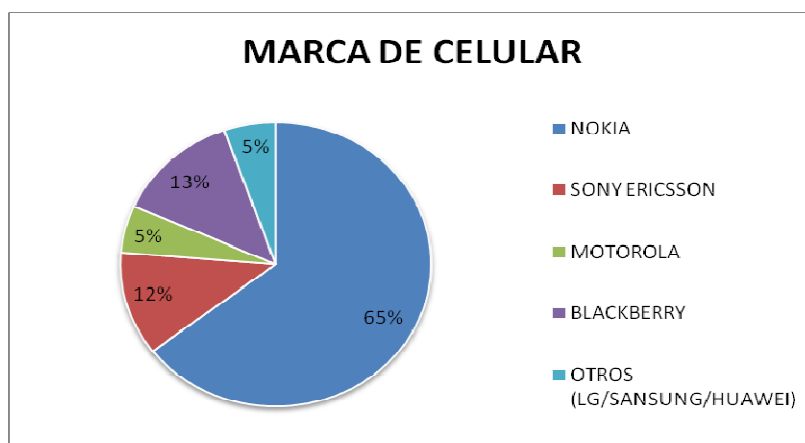
1) Dispone usted de un teléfono celular

| | |
|----|----|
| SI | 93 |
| NO | 1 |



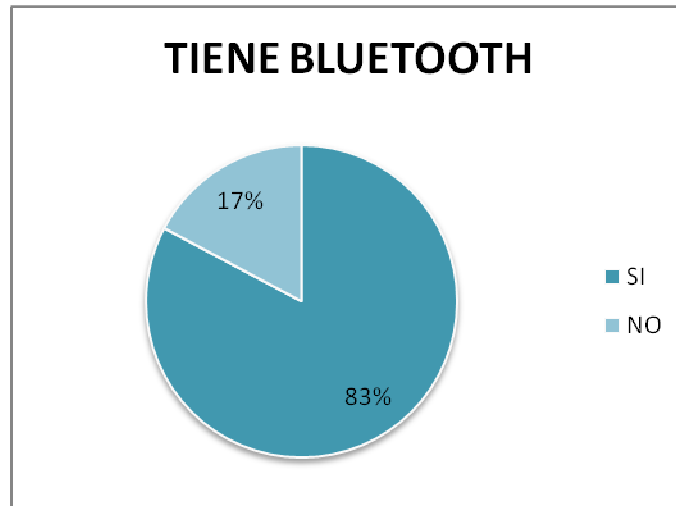
2) Que marca de teléfono usa?

| | |
|---------------------------|----|
| NOKIA | 60 |
| SONY ERICSSON | 11 |
| MOTOROLA | 5 |
| BLACKBERRY | 12 |
| OTROS (LG/SANSUNG/HUAWEI) | 5 |



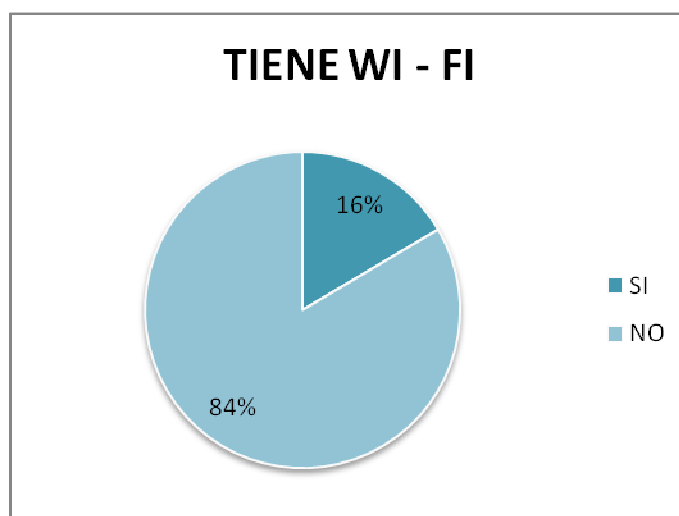
3) Tiene bluetooth?

| | |
|----|----|
| SI | 77 |
| NO | 16 |



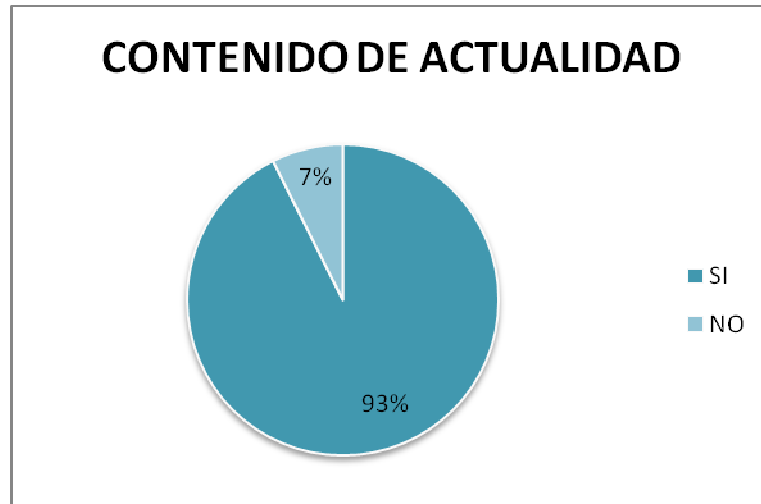
4) Tiene WI - FI?

| | |
|----|----|
| SI | 14 |
| NO | 71 |



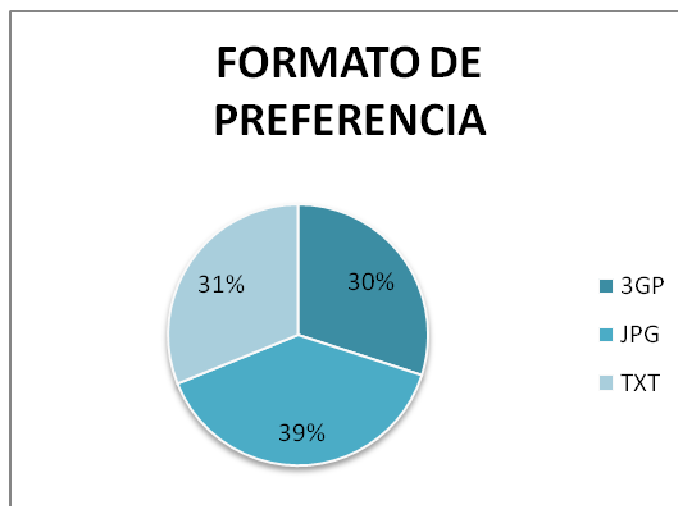
5) Le gustaría recibir contenido de actualidad a su teléfono?

| | |
|----|----|
| SI | 75 |
| NO | 6 |



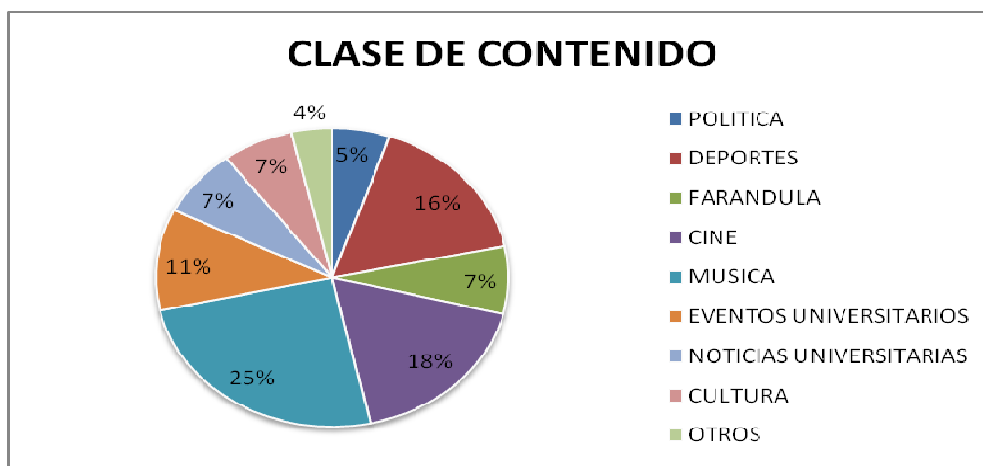
6) En que formato le gustaría recibir?

| | |
|-----|----|
| 3GP | 27 |
| JPG | 35 |
| TXT | 28 |



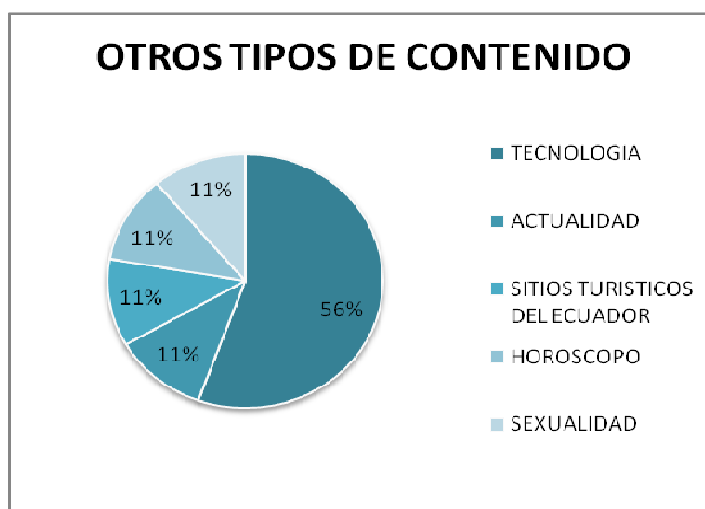
7) Que clase de contenido le gustaría recibir?

| | |
|-------------------------|----|
| POLITICA | 13 |
| DEPORTES | 40 |
| FARANDULA | 18 |
| CINE | 43 |
| MUSICA | 61 |
| EVENTOS UNIVERSITARIOS | 27 |
| NOTICIAS UNIVERSITARIAS | 18 |
| CULTURA | 16 |
| OTROS | 9 |



OTROS:

| | |
|-------------------------------|---|
| TECNOLOGIA | 5 |
| ACTUALIDAD | 1 |
| SITIOS TURISTICOS DEL ECUADOR | 1 |
| HOROSCOPO | 1 |
| SEXUALIDAD | 1 |



DISEÑO E IMPLEMENTACIÓN DEL SISTEMA BLUESERVER

7.1 DISEÑO PRELIMINAR

A continuación se muestra en la figura 7.1, 7.2 y 7.3; la posición de las antenas las cuales fueron ubicadas en este lugar por las siguientes razones:

- La distancia entre el servidor bluetooth y las antenas no puede superar los 7 metros aproximadamente, ya que el medio de conexión entre estos dispositivos es cable USB.

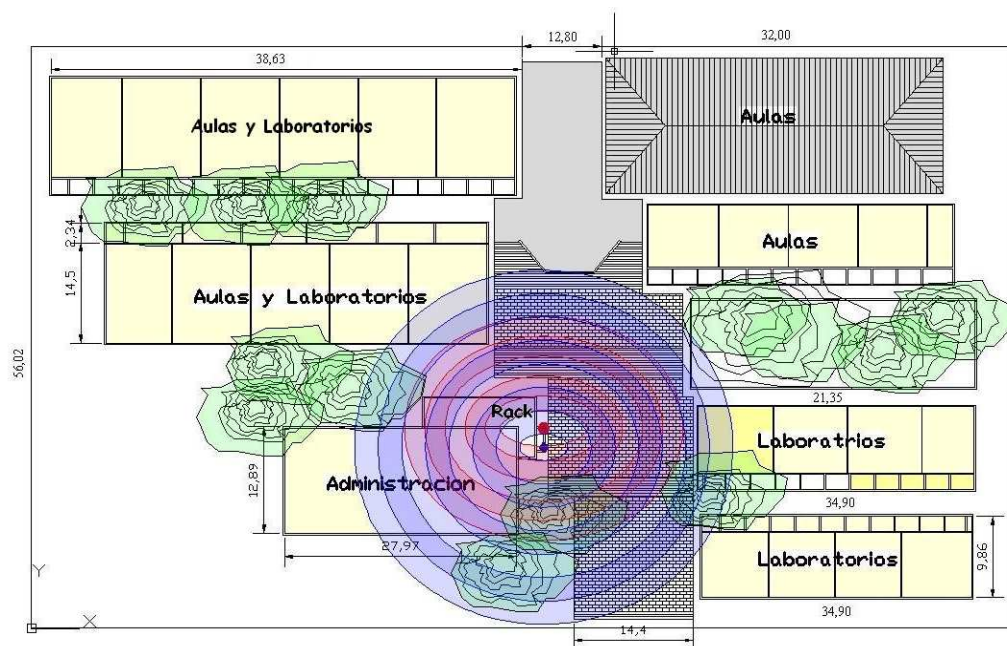


Figura 7.1 Plano de cobertura de sistema BlueServer en la Facultad Técnica
Fuente: Proyecto de Tesis.

- En esta área donde se han colocado las antenas es donde se encuentra la mayor afluencia de alumnado ya que se encuentra en el centro de la facultad; por lo tanto como el gráfico representa tenemos gran cobertura hacia todos los sectores.



Figura 7.2 Visión 3D de cobertura del sistema BlueServer en la Facultad Técnica
Fuente: Proyecto de Tesis



Figura 7.3 Visión 3D de cobertura del sistema BlueServer en la Facultad Técnica
Fuente: Proyecto de Tesis

- De la misma forma otro punto a favor de la ubicación de los equipos que en ese lugar se encuentra el Rack de la facultad el mismo que está diseñado y acondicionado para albergar equipos de tecnología el cual posee un sistema puesta a tierra y aclimatación adecuada para los equipos.

7.2 PRUEBAS PRELIMINARES

En la figura 7.4 se presenta la prueba de los equipos; en la figura 7.5 la configuración del mismo; además del funcionamiento en las antenas.

- Una vez a la llegada de los equipos se procedió a la pruebas domesticas de los mismos como se lo muestra en la figura 7.4.

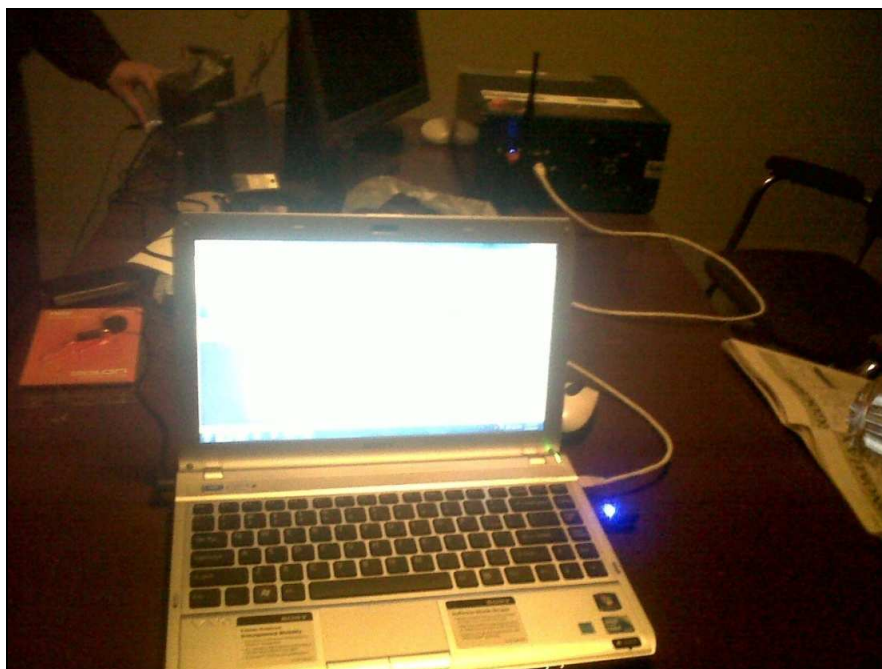


Figura 7.4 Configuración del equipo BlueServer mediante conexión Ethernet.
Fuente: Proyecto de Tesis



Figura 7.5 Configuración física de las antenas bluetooth en el HUB para prueba.
Fuente: Proyecto de Tesis

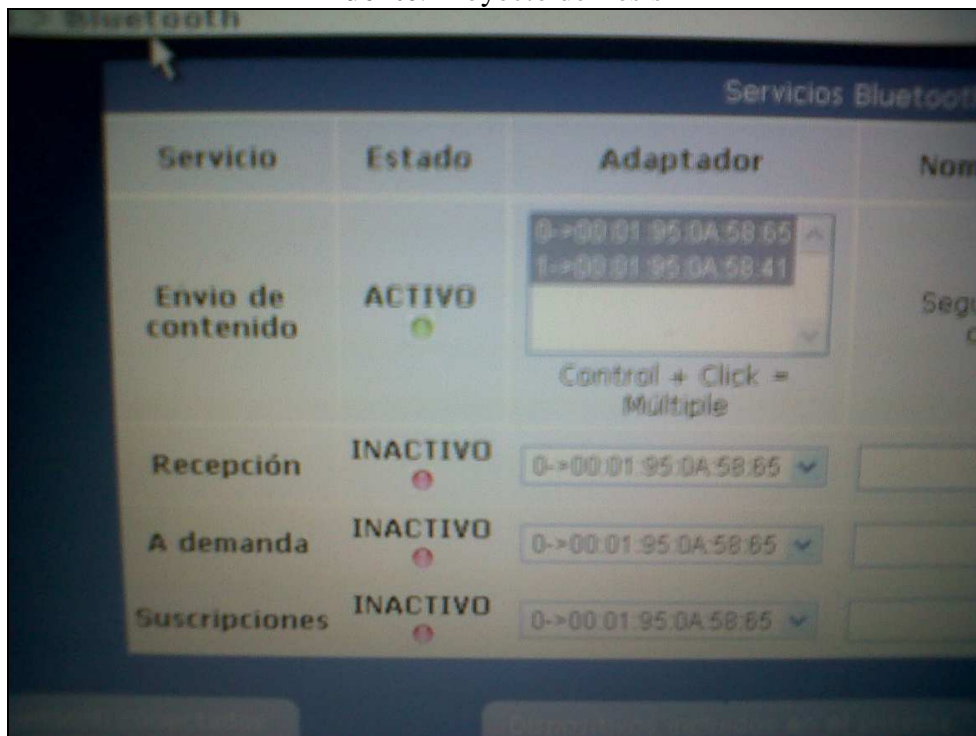


Figura 7.6 Configuración y activación de la función de cada antena mediante el software de administración BlueServer.
Fuente: Proyecto de Tesis

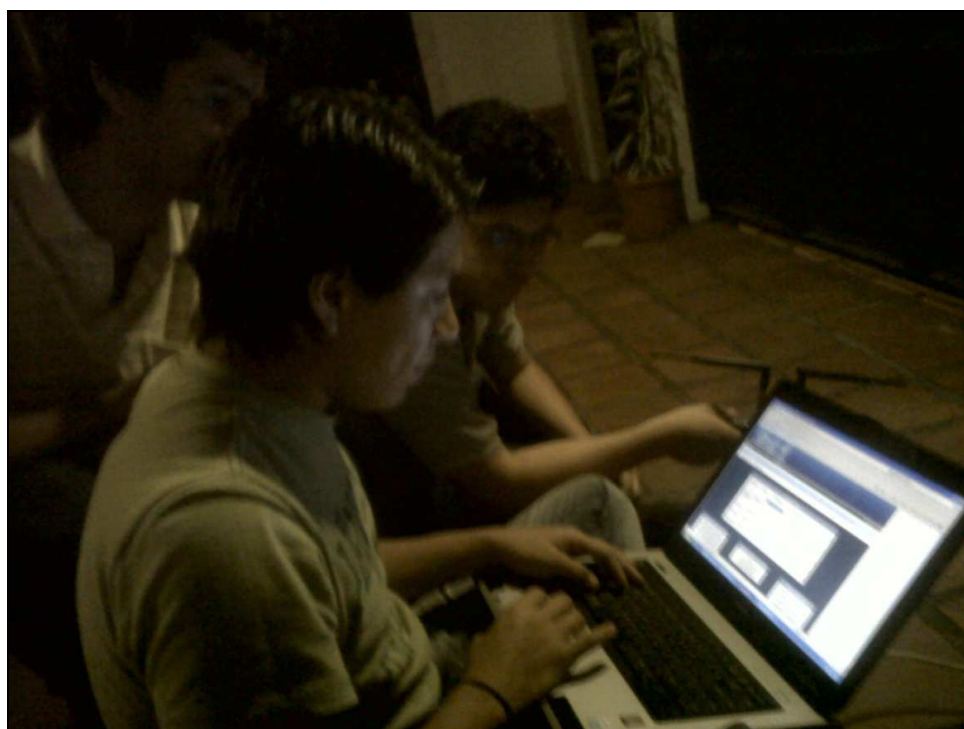


Figura 7.7 Procedimiento de la creación de una campaña de envío de mensajería Bluetooth mediante el software de administración del equipo BlueServer.

Fuente: Proyecto de Tesis



Figura 7.8 Verificaciones de los parámetros de la campaña creada.

Fuente: Proyecto de Tesis



Figura 7.9 Colocación de las antenas en campo para pruebas de potencia y ganancia.
Fuente: Proyecto de Tesis



Figura 7.10 Recepción de mensajes en los dispositivos celulares dentro de la cobertura del sistema BlueServer
Fuente: Proyecto de Tesis

7.3 INSTALACION

7.3.1 Puesta del rack

En la figura 7.11 Se presenta el lugar específico de la colocación del Rack para el equipo BlueServer dentro del cuarto de rack de la Facultad Técnica.

Se procedió a instalar un Rack tipo gabinete para que no interfiera con el Rack ya instalado; en el mismo ira el BlueServer.

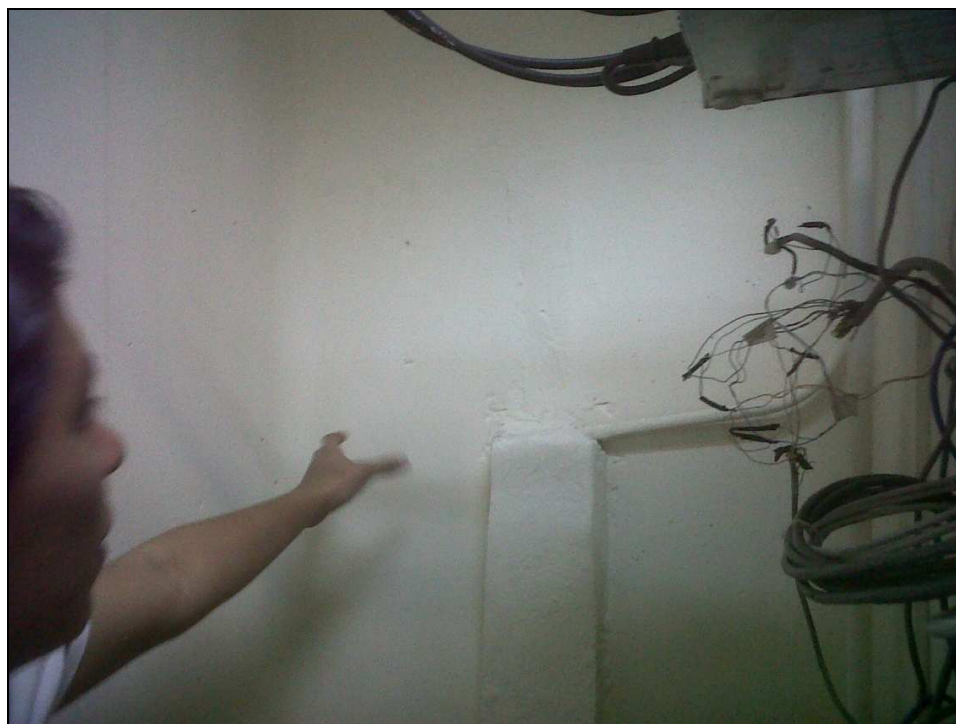


Figura 7.11 Determinación de sitio de ubicación del Rack para el equipo BlueServer
Fuente: Proyecto de Tesis



Figura 7.12 Instalación del rack, perforación la pared y se colocó pernos ancla para el soporte por parte de nuestro compañero Fernando Espinoza.

Fuente: Proyecto de Tesis

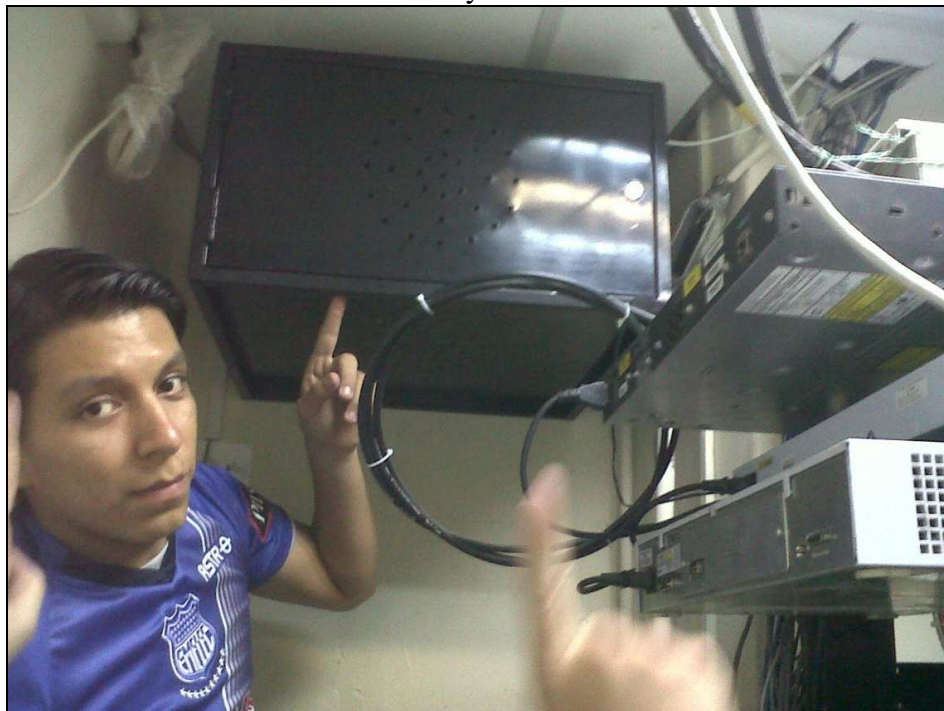


Figura 7.13 Rack tipo gabinete con puerta de seguridad y ventilación instalado en la ubicación determinada dentro del cuarto de rack de la Facultad Técnica.

Fuente: Proyecto de Tesis

7.3.2 Implementación del sistema eléctrico

En la figura 7.14 se muestra el diseño del sistema eléctrico implementado en el proyecto de tesis.

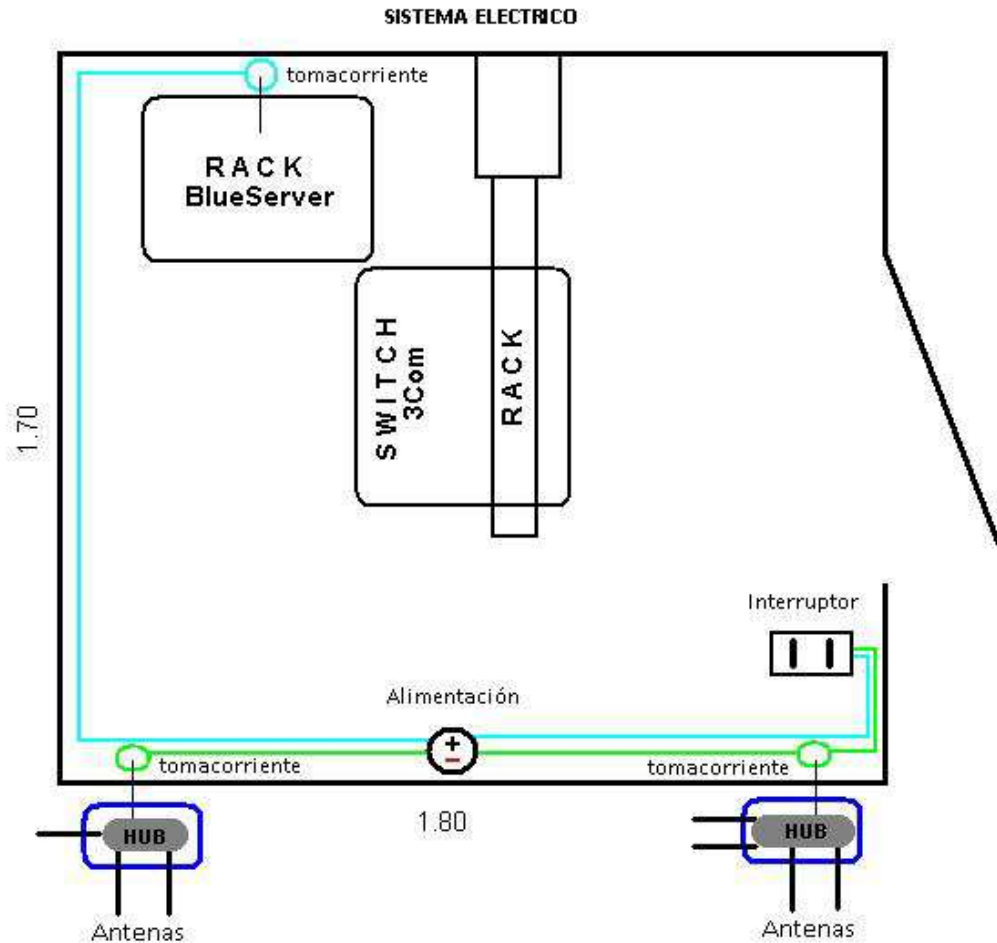


Figura 7.14 Diagrama del sistema eléctrico instalado para equipo BlueServer

Fuente: Proyecto de Tesis



Figura 7.15 Instalación del sistema eléctrico dentro del cuarto de rack de la Facultad Técnica por parte de nuestro compañero Franklin Freire.

Fuente: Proyecto de Tesis



Figura 7.16 Procedimiento de instalación del cableado eléctrico en su acometida

Fuente: Proyecto de Tesis



Figura 7.17 Interruptor para prendido/apagado del equipo BlueServer y de antenas Bluetooth de nuestro proyecto.

Fuente: Proyecto de Tesis

7.3.3 Implementación de la red de antenas

En la figura 7.18 se aprecia el esquema de instalación de la red de antenas Bluetooth ubicadas dentro del cuarto de rack de la Facultad Técnica conformada en total por 7 antenas. Esta red consiste en dos cables USB de cerca de 3 metros de largo cada uno que recorren el tramo desde el puerto USB del equipo BlueServer ubicado dentro de su rack tipo gabinete hacia el exterior del cuarto donde encontramos los HUBs USB en los cuales están conectadas directamente las antenas USB Bluetooth. Son las encargadas de dar cobertura a la facultad en un perímetro de 30 metros aproximadamente.

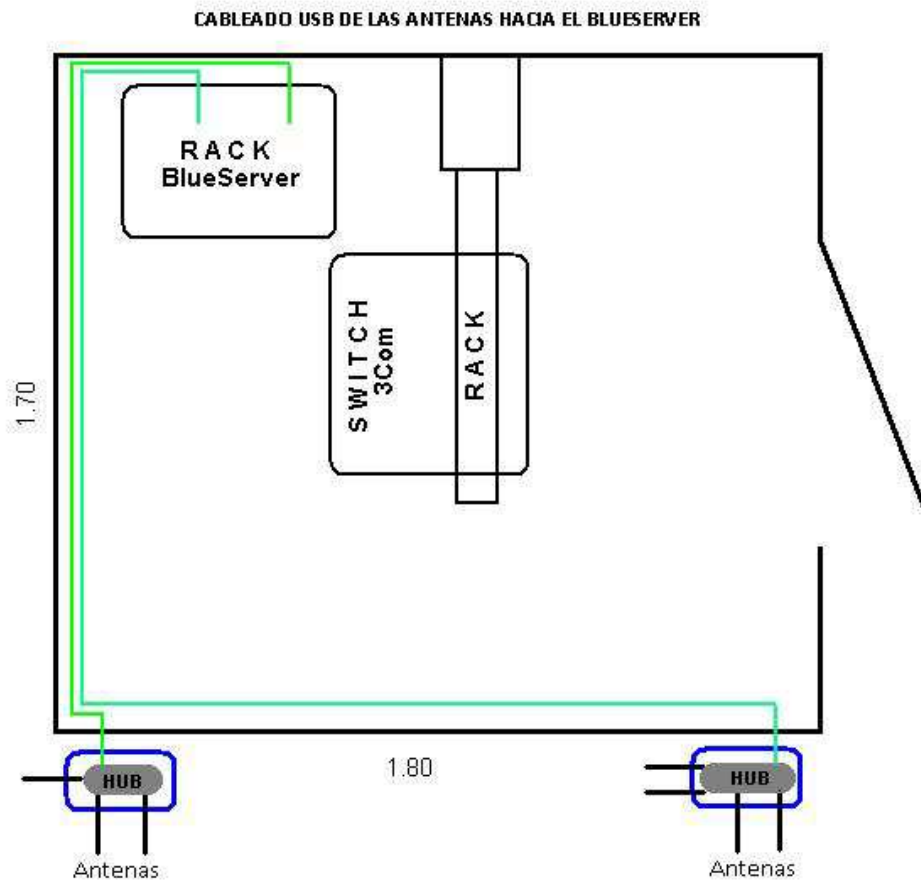


Figura 7.18 Diagrama de instalación de la red de antenas USB Bluetooth.
Fuente: Proyecto de Tesis

La ubicación de las antenas será en el exterior del cuarto de rack de la Facultad Técnica, para evitar que estén a la intemperie y su contacto directo con el medio ambiente y con agentes naturales que puedan producir el deterioro físico de las antenas USB Bluetooth se procede a instalarlas dentro de dos compartimientos por grupos de 3 y 4 antenas respectivamente.

En la figura 7.19 y 7.20 se está realizando la perforación para la colocación de los compartimientos con las antenas bluetooth en cada extremo superior de la cara posterior del Rack, las antenas son omnidireccionales.

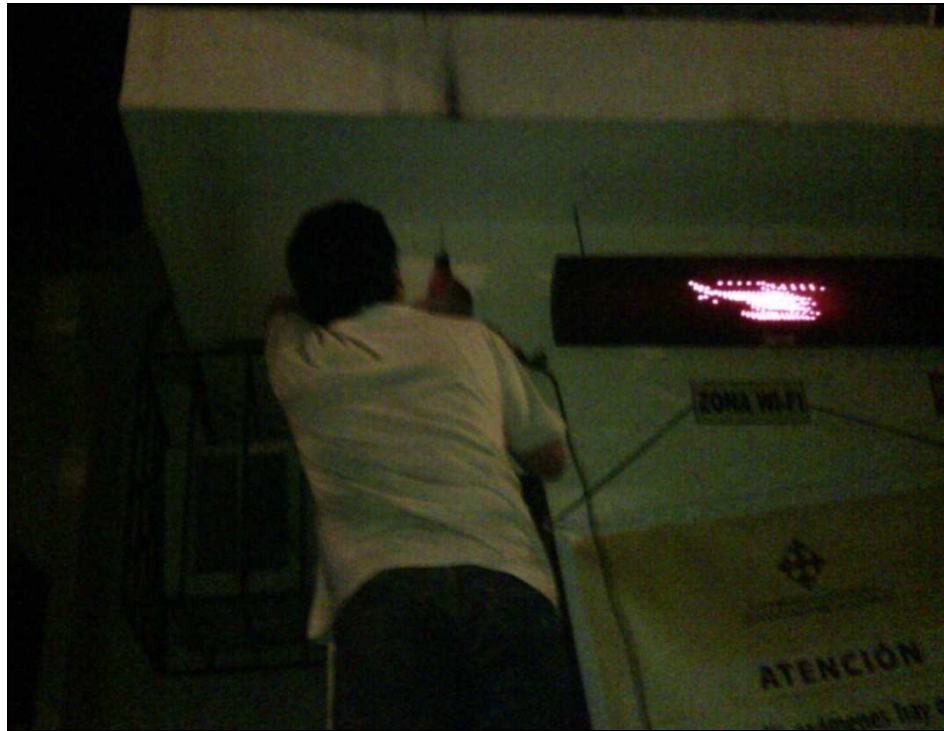


Figura 7.19 Extremo izquierdo donde se ubicaran 3 antenas
Fuente: Proyecto de Tesis



Figura 7.20 Extremo derecho donde se ubicaran 4 antenas.
Fuente: Proyecto de Tesis



Figura 7.21 Antenas instaladas
Fuente: Proyecto de Tesis

7.3.4 Implementación del punto de red

Se procedió a solicitar al centro de Computo una dirección IP para así cualquier persona que desee pueda acceder de forma remota al equipo. De la misma forma se solicito la disponibilidad de un puerto en el switch para dicha conexión.

La dirección IP y el puerto fueron las siguientes:

Puerto # 5 en el switch 3Com.

| | |
|-------------------|---------------|
| Dirección IP | 172.16.9.66 |
| Mascara de subred | 255.255.255.0 |
| Gateway | 172.16.9.202 |
| Servidor DNS | 172.16.1.230 |

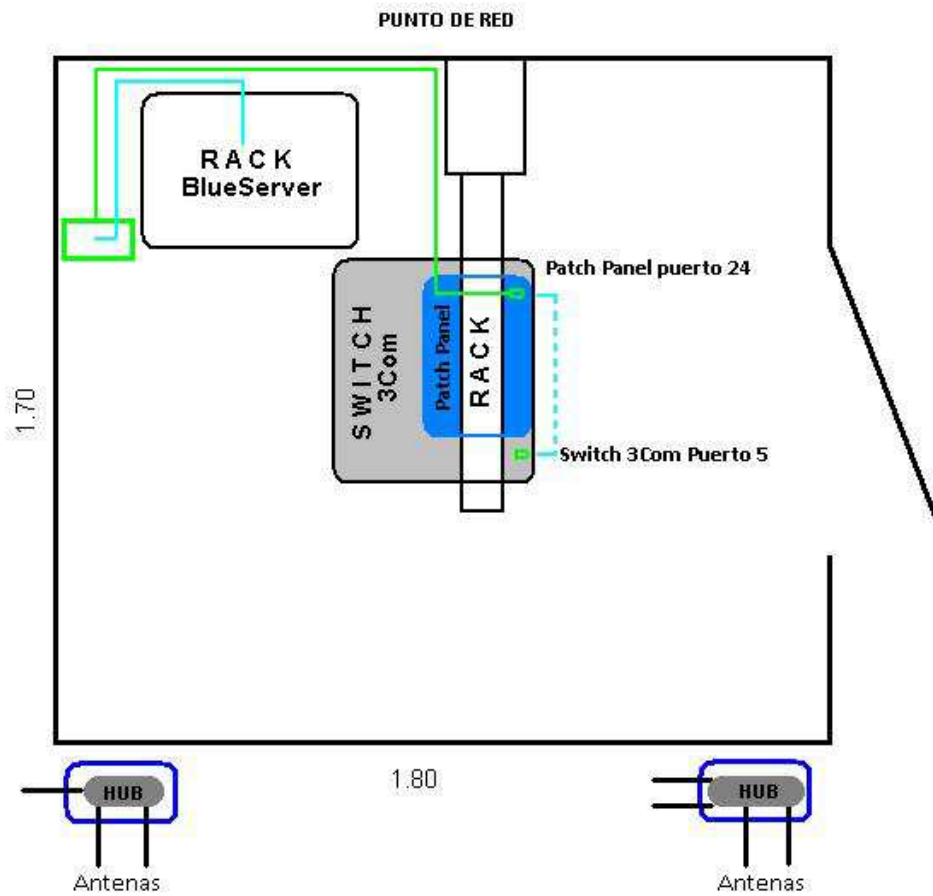


Figura 7.22 Diagrama punto de red
Fuente: Proyecto de Tesis



Figura 7.23 Se verifica la disponibilidad del puerto en el patch panel asignado a nuestro proyecto por parte del centro de cómputo de la universidad.
Fuente: Proyecto de Tesis



Figura 7.24 Ubicación e instalación del jack en el patch panel dentro del rack de la Facultad Técnica por parte de nuestro compañero Jorge Cortez

Fuente: Proyecto de Tesis



Figura 7.25 Una vez instalado el jack en el patch panel tenemos disponible el puerto Ethernet para la conexión del patchcord.

Fuente: Proyecto de Tesis



Figura 7.26 Puesta de caja para punto de red y conexión directa hacia el equipo BlueServer por parte de nuestro compañero Dennys Espin.
Fuente: Proyecto de Tesis



Figura 7.27 Instalación completada del punto de red
Fuente: Proyecto de Tesis

7.4 PRUEBAS FINALES

En las figuras 7.28 y 7.29 se está realizando la colocación de las antenas en una caja hermética diseñada para colocar equipos delicados a la intemperie.



Figura 7.28 Caja con grupo de 4 antenas se ubicaran en la parte exterior del cuarto de rack de la Facultad Técnica en el costado derecho.

Fuente: Proyecto de Tesis



Figura 7.29 Caja con grupo de 3 antenas se ubicaran en la parte exterior del cuarto de rack de la Facultad Técnica en el costado izquierdo

Fuente: Proyecto de Tesis

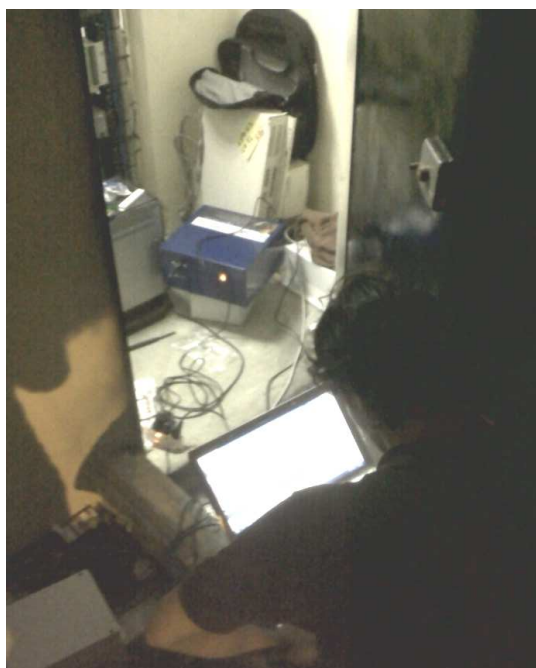


Figura 7.30 Configuración del servidor el Rack para prueba final en la parte exterior del cuarto de rack de la Facultad Técnica
Fuente: Proyecto de Tesis

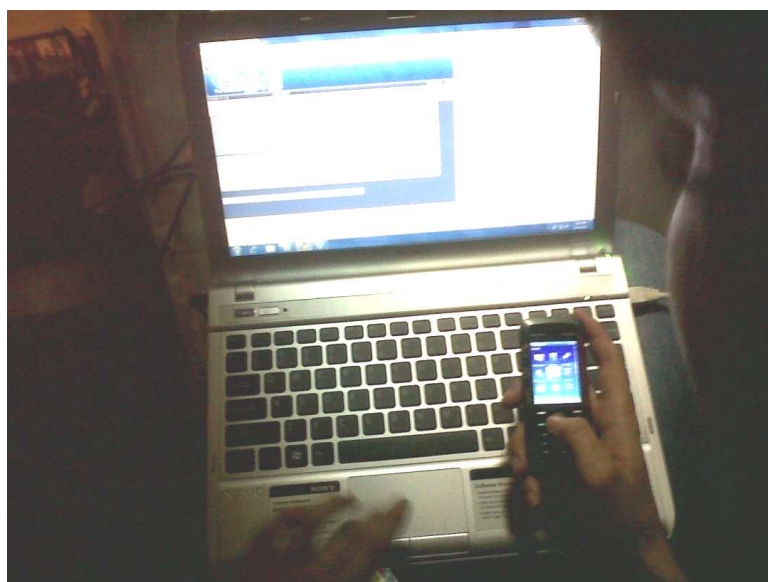


Figura 7.31 se verifica en el celular la recepción de la campaña creada y emitida, en la parte exterior del cuarto de rack de la Facultad Técnica
Fuente: Proyecto de Tesis

CAPITULO 8

JUSTIFICATIVO DE ELECCION DEL EQUIPO

8.1 JUSTIFICACIÓN DE EQUIPO

El proyecto que hemos implementado utilizando el equipo BlueServer cuenta con grandes beneficios y ventajas por sobre otros equipos similares.

Esto radica en las características del equipo que contamos; ya que nos brinda tráfico de información de dos vías, es decir tanto de envío como de recepción.

Además también existe la posibilidad de agregar tecnología 3G para tener acceso remoto de administración al equipo.

También la implementación de VPN (Virtual Private Network) con el proveedor para actualizaciones de software en caso de ser necesario. Si se toma en cuenta una expansión de antenas para ampliar zona de cobertura, por medio de la VPN se puede tener monitoreo continuo y soporte técnico 24 horas al día por parte del proveedor.

Además contamos dentro del software de administración del equipo BlueServer la posibilidad de realizar reportes y estadísticas del uso del equipo, pues cuenta con una base de datos que alberga los registros de todas las transacciones realizadas por las antenas configuradas para el envío y recepción de información.

Detallamos dos páginas de proveedores de este tipo de tecnología, pero solo se limitan en envío de mensajería bluetooth.



Figura 8.1 Muestra de la pagina web de proveedor ZONABLU

Fuente: <http://www.zonablu.es/default.aspx>



Figura 8.2 Muestra de la pagina web de proveedor BLOOZY

Fuente: <http://www.bluetoothmarketing.com/products.php>

8.2 F.O.D.A.

8.2.1 FORTALEZAS

- Tecnología inalámbrica que permite conectar dispositivos entre sí.
- Su tamaño tan pequeño y bajo consumo de potencia, lo hacen ideal para implementarlos en dispositivos móviles como, por ejemplo: teléfonos móviles, PDAs, ordenadores portátiles, teclados, mouse, mandos a distancia, cámaras fotográficas, impresoras, lectura de los contadores del hogar, además de un largo etcétera.
- Tecnología muy barata de fabricar y que las comunicaciones que se establecen entre los diferentes dispositivos son gratuitas.
- Más de 2000 empresas en todo el mundo implementan esta tecnología en sus dispositivos.

8.2.2 OPORTUNIDADES

- Por ser una tecnología barata y de corto alcance se la podría implementar en hogares y oficinas pequeñas.
- Posibilidad de tener varios dispositivos conectados a un dispositivo Bluetooth, y de esta manera eliminar la telaraña de cables.

8.2.3 DEBILIDADES

- La distancia de comunicación entre dos dispositivos debe ser menor a 10 m.
- La transmisión de datos es menor a 1Mbps (721 Kbps)

8.2.4 AMENAZAS

- Vulnerable a los ataques de hackers.
- Si no se aplican los niveles de seguridad apropiados, toda nuestra información se podría filtrar.
- Se pueden intervenir las conversaciones basadas en tecnología Bluetooth, por medio del uso de Audífonos de Manos Libres.

8.3 PRESUPUESTO

Procederemos a detallar los gastos que involucraron la implementación del proyecto.

A continuación en la tabla 8.1 tenemos los gastos que se incurrieron para la compra del equipo BlueServer, así como de las antenas USB Bluetooth y accesorios.

| DESCRIPCION | CANTIDAD | PRECIO | TOTAL |
|-------------------------------|----------|--------|-------|
| BlueServer | 1 | 1500 | 1500 |
| Antenas adicionales bluetooth | 7 | 220 | 1540 |
| HUB USB 7 puertos | 1 | 60 | 60 |
| HUB USB 10 puertos | 1 | 110 | 110 |
| TOTAL | | | 3210 |

Tabla 8.1 Presupuesto de costo de equipo BluServer y accesorios

En la tabla 8.2 desglosamos los gastos de importación de equipo a través del Courier, así como también gastos de impuestos y mano de obra de la implementación.

| DESCRIPCION | CANTIDAD | PRECIO | TOTAL |
|--------------------------------|----------|--------|--------|
| Envío de dinero (Wester Union) | 1 | 128.4 | 128.4 |
| Envío de equipos (Fedex) | 1 | 400 | 400 |
| impuestos aduaneros | 1 | 520 | 520 |
| Mano de Obra | 1 | 1300 | 1300 |
| TOTAL | | | 2348.4 |

Tabla 8.2 Gastos varios y administrativos

Los materiales y herramientas usadas para la instalación del sistema BlueServer se encuentran en la tabla 8.3 con sus respectivos costos.

| DESCRIPCION | CANTIDAD | PRECIO | TOTAL |
|----------------------------------|----------|--------|---------------|
| Caja para instalaciones externas | 2 | 30 | 60 |
| Rack de pared tipo gabinete | 1 | 160 | 160 |
| Estaño | 1 | 1.4 | 1.4 |
| Canaleta | 1 | 3 | 3 |
| Jack, caja, faceplate | 1 | 25 | 25 |
| Jack universal para patch panel | 1 | 15 | 15 |
| Patch cord | 1 | 10 | 10 |
| Broca 10mm | 1 | 4.65 | 4.65 |
| Broca 6mm | 1 | 3.10 | 3.10 |
| Broca 8mm cemento | 1 | 3.50 | 3.50 |
| Broca 8mm metal | 1 | 6.50 | 6.50 |
| Rollo cable #16 | 1 | 50 | 50 |
| Tomacorriente Simple | 3 | 2.50 | 7.50 |
| Enchufe | 3 | 1.80 | 5.40 |
| Enchufe reforzado | 1 | 3,75 | 3,75 |
| Tomacorriente Polarizado | 1 | 3.90 | 3.90 |
| Interruptor | 1 | 2.25 | 2.25 |
| Sierra | 1 | 15 | 15 |
| Cinta doble faz | 1 | 2 | 2 |
| Cinta doble | 1 | 2.35 | 2.35 |
| Tornillos y tacos | 12 | 0.50 | 6 |
| Pernos ancla | 6 | 1.12 | 6,72 |
| Arandela de presion (funda) | 2 | 0.40 | 0.80 |
| Arandela plana (funda) | 3 | 0.95 | 2,85 |
| conector USB (macho) | 2 | 1 | 2 |
| conector USB (hembra) | 2 | 1 | 2 |
| Amarras (funda 50) | 1 | 7 | 7 |
| Silicona | 1 | 15 | 15 |
| Pistola para silicona | 1 | 9 | 9 |
| Rollo de cable UTP CAT5 | 2 | 60 | 120 |
| Cable USB | 2 | 15 | 30 |
| Otros | 1 | 150 | 150 |
| TOTAL | | | 735.67 |

Tabla 8.3 Costo de materiales y herramientas

CONCLUSIONES

- Se diseñó e implementó un sistema de telecomunicaciones de información basado en la tecnología bluetooth, tomando en cuenta la infraestructura presente en la universidad.
- Se crearon diferentes campañas (grupo de mensajes) en el equipo BlueServer con contenido de importancia para la comunidad estudiantil de la facultad.
- Los dispositivos celulares, PDA's y notebooks que se encontraban dentro de la cobertura del sistema BlueServer recibieron el contenido pre cargado dentro de las campanas configuradas en el equipo BlueServer.
- Los dispositivos celulares de marca iPhone cuenta con restricciones con el uso del protocolo bluetooth que ya es de conocimiento público, pues no permite el paging de ningún otro dispositivo bluetooth para transferencia de información.
- Los dispositivos celulares de marca Blackberry cuenta con restricciones con el uso del protocolo bluetooth, pues a nivel de seguridades maneja encriptación y cifrado que no permite el paging de equipo BlueServer.
- Se receptaron con éxito las sugerencias dadas por los estudiantes que poseen cualquier tipo de teléfonos móviles via bluetooth hacia equipo BlueServer.

RECOMENDACIONES

- El equipo BlueServer ubicado en el cuarto de equipos, en su propio rack, deben contar con una temperatura recomendada para los equipos de tecnología menor a 20°C.
- Las campañas de mensajería bluetooth deben ser actualizadas en su contenido periódicamente para brindar información oportuna al estudiantado.
- Las antenas como los cables pertenecientes a las instalaciones realizadas deben ser revisados periódicamente para evitar deterioro y malfuncionamiento del sistema BlueServer.
- Para futura expansión de zona de cobertura bluetooth adquirir antenas USB Bluetooth con las mismas características técnicas usadas además de el mismo proceso de instalación en caso de estar ubicadas en el exterior.
- Revisar y depurar periódicamente buzón de sugerencia receptadas y base de datos de equipo BlueServer que contiene registros de transacciones realizadas.

8.6 BIBLIOGRAFÍA

BLUETOOTH, VISIÓN GENERAL DE UNA RED INALÁMBRICA

Universidad de Valencia – Ingeniería en Informática

COMUNICACIONES INALÁMBRICAS. UN ENFOQUE APLICADO.

Roldán Martínez, David

Editorial: RA-MA Editorial

Año edición 2004

IEEE 802.15 ESTÁNDAR

Copyright ©2010 IEEE-SA

Contact IEEE-SA

(webmaster@standards.ieee.org)

TECNOLOGÍA BLUETOOTH

Natham J. Muller - 2002

BLUETOOTH SECURITY

Christian Gehrman, Joakim Persson, Ben Smeets

Edición 2004

WIRELESS MULTIMEDIA

a guide to the IEEE 802.15.3 standard

James P. K. Gilb - 2004

<http://www.bluetooth.org/>

<http://www.bluetooth.com/>

<http://www.bluetooth.net/>

<http://www.bluezona.com/>

<http://es.wikipedia.org/wiki/Bluetooth>

<http://spanish.bluetooth.com/bluetooth/>