Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE IMPLEMENTACIÓN DE UNA RED INALÁMBRICA BLUETOOTH, HACIENDO ÉNFASIS EN LA SEGURIDAD DE LA MISMA

Diego Antonio de León Paredes

Asesorado por el Ing. MsEE. PhD. Enrique Edmundo Ruiz Carballo

Guatemala, marzo de 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE IMPLEMENTACIÓN DE UNA RED INALÁMBRICA BLUETOOTH, HACIENDO ÉNFASIS EN LA SEGURIDAD DE LA MISMA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR:

DIEGO ANTONIO DE LEÓN PAREDES

ASESORADO POR EL ING. MSEE. PHD. ENRIQUE EDMUNDO RUIZ CARBALLO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, MARZO DE 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patrícia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Francisco Javier Gonzáles López
EXAMINADOR	Inga. Ingrid Salomé de Loukota
EXAMINADOR	Ing. Jose Anibal Silva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la Ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE IMPLEMENTACIÓN DE UNA RED INALÁMBRICA BLUETOOTH, HACIENDO ÉNFASIS EN LA SEGURIDAD DE LA MISMA,

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 9 de mayo de 2005.

Diego Antonio de León Paredes

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 19 de febrero 2007.

Ingeniero
Coordinador Area de Electrotècnia
Escuela de Ingenierìa Mecànica Elèctrica

Estimado Ingeniero:

Por este medio le informo que he revisado el trabajo de graduación titulado: **DISEÑO DE IMPLEMENTACIÒN DE UNA RED INALÀMBRICA BLUETOOTH, HACIENDO ÈNFASIS EN LA SEGURIDAD DE LA MISMA**, elaborado por el estudiante Diego Antonio de Leòn Paredes.

El mencionado trabajo llena los requisitos para dar mi aprobación, e indicarle que el autor y mi persona somos responsables por el contenido y conclusiones de la misma.

Atentamente,

Ing Enrique Edmundo Ruiz Carballo
ASESOR

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 28 de febrero 2007.

Señor Director
Ing. Mario Renato Escobedo Martìnez
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: **DISEÑO DE IMPLEMENTACIÒN DE UNA RED INALÀMBRICA BLUETOOTH, HACIENDO ÈNFASIS EN LA SEGURIDAD DE LA MISMA, des**arrollado por el estudiante; Diego Antonio de Leòn Paredes, por considerar que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador Area de Electrònica

JCSP/sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

El Director de la Escuela de Ingenierìa Mecànica Elèctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Area, al trabajo de Graduación del estudiante; Diego Antonio de Leòn Paredes titulado: **DISEÑO DE IMPLEMENTACIÒN DE UNA RED INALÀMBRICA BLUETOOH, HACIENDO ÈNFASIS EN LA SEGURIDAD DE LA MISMA,** procede a la autorización del mismo.

Ing. Mario Renato Escobedo Martìnez
DIRECTOR

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
DE GUATEMALA

GUATEMALA, 5 DE MARZO 2,007.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG. 069.2007

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **DISEÑO DE IMPLEMENTACIÓN DE UNA RED INALÁMBRICA BLUETOOTH, HACIENDO ÉNFASIS EN LA SEGURIDAD DE LA MISMA,** presentado por el estudiante universitario **Diego Antonio de León Paredes,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

Guatemala, marzo de 2007

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

/gdech

ACTO QUE DEDICO A

Dios	Por permitirme cumplir esta meta de mi vida que solo con su bendición y ayuda es posible realizarla.
La Virgen del Rosario	Por cuidarme e interceder por mí en todo este largo camino.
Mis padres	Diego de Leon y Antonieta Paredes de de Leon, por su esfuerzo, ayuda y sobre todo por su ejemplo dado durante toda mi vida, este logro es para ustedes.
Mis hermanos:	Mary, Francisco y Roberto, por afinidad, Enrique, Hugo, Kibonge y Loren, porque fueron apoyo fundamental y moral en toda mi vida.
Mis abuelos	Catalina Escobar de Paredes, (Q.E.P.D.), Mary Eleonora Valdez Lopez (Q.E.P.D.) Jose de Jesús Paredes Rodríguez, y Francisco de Leon, gracias por siempre.
Todos mis sobrinos:	Muy Especialmente a Pablo Esteban, Andrea Maria Y Jose Pablo, por recordarme lo alegre que se puede disfrutar la vida cada día.

Todos mis tíos y primos	Gracias por ser parte de mi vida, muy especialmente a Hilda Paredes y Raúl Flores, por seguir siendo ejemplo de admiración en todos los aspectos de mi vida.
Mi nana	Adriana Martínez, nunca olvidare que tu apoyo y enseñanzas en el principio de mi vida han marcado mucho de lo que me sirve a diario.
Mis amigos	Cercanos a mi hogar, Universidad y Laborales, la vida continua y los caminos en un momento se dividen, pero los recuerdos grabados con ustedes siempre vivirán, gracias a todos.

AGRADECIMIENTOS A

Quetzaltenango	Tierra en donde mis ojos se abrieron por primera vez, y me dejo ver la belleza reflejada en todos sus aspectos.
La Universidad de San Carlos de Guatemala	Casa de estudios que me abrió las puertas para contribuir con mi trabajo en el desarrollo de mi país.
La Facultad de Ingeniería	Lugar que día con día, libro con libro, me enseñó no sólo a ser un profesional de la ingeniería, sino que me enseñó a ser una mejor persona, y saber que un profesional no se hace solo con el estudio.
Corporación Papelco S.A.	Por permitirme realizar este trabajo de graduación, además de conocer a personas que el día de hoy son grandes amigos y ejemplos a seguir en la vida.
STG de Guatemala	Porque me ha dado el apoyo profesional y académico, cuando lo he necesitado
Mi asesor	Ing. Enrique Ruiz, infinitamente gracias por el apoyo, asesoria y amistad brindada hacia mi.

Los profesionales

Ing. Ingrid de Loukota, Ing. Francisco Gonzáles, gracias por transmitirme sus conocimientos, además de brindarme su amistad como persona.

Mis amigos

Ana Lucía, Carlos Marroquin, Yonjairo Orellana, Jorge Mario Gutierrez, Nancy, Henry, Tito, Cinthya Hernandez, Marvin, Mario Gonzales, Roger Letona, Carlos Alvarez, Rogelio, Jose Carlos, Ana Molina, Karen Tohon, Luis Velasquez, Jesús Martinez, Luis Rios, Hans, Mariela, Alberto, Juan Alvarado, Pamela Vega, Xavier, Luis Puac, Carlos Narcizo, Eduardo, Justo, Evelyn, Michelle, Gaby, Sergio, Rene, Vanesa, Jose Aragon, Mario Ramos, Luis Lavagnino, Edgar Estrada, Wilfredo, Mauricio Calle, Karen Ubeda, Gustavo Ruiz, Yuli, Sandy, Andrea, Leslie Franco, Gregorio, Jorge Martinez, Eddy, Mariana, Luigy, Gary, Hector, Karla, Carolina Revolorio, Raquel, Gladis, Soledad, Jeannette, Luis Pedro, Marla, Oscar, Marlon, Ana Cecilia, Manola, Lucky, Nubia, Alejandro, Kelvin, Mayte, Marvin, Meme, Patty, Romeo, Ronaldo, Mario Merida, Walter, Wendy, Edith, Jeackeline, y a los que olvide sin querer, por que la amistad que me dan, es una aliento y alegría en base a las experiencias compartidas, muchas gracias muchachos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ACl	Conexión simétrica o asimétrica punto a multipunto sin ancho de banda prefijado, entre un maestro y uno o más esclavos activos
802.11	El protocolo IEEE 802.11 es un estándar de protocolo de comunicaciones de la IEEE que define el uso de los dos niveles más bajos de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN. En general, los protocolos de la rama 802.x definen la tecnología de redes de área local.
Ancho de Banda	Cantidad de bits que pueden viajar por un medio de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información. Se mide en millones de bits por segundo (Mbps) y las velocidades típicas hoy en día varían de 10 Mbps a 100 Mbps
Canal	Medio por el cual se realiza una transferencia de información de un lado a otro.
Capa	Distintos niveles de estructura de paquete o de enlace utilizados en los protocolos.

Enlace	Comunicación punto a punto entre una unidad maestra y una unidad esclava.
LAN	Red de área Local
Paquetes	Datos enviados en un canal y que tiene una forma que consta de tres campos los cuales son: Código de Acceso, Cabecera y Carga Útil
SCO	El enlace SCO es una conexión simétrica punto-a-punto entre el maestro y un esclavo específico.
Sincronización	Proceso mediante el cual se transmiten datos, actualizando la información existente.
Inalámbrica	Modo de tecnología de comunicación en la que no se utilizan cables, sino una frecuencia en particular para la transmisión de información.
Networking	Estar trabajando varios usuarios a la vez en una red
Encapsulamiento	El encapsulamiento es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear.
Paging	Llevar un mensaje a alguien desconocido y este al detectarle envía una respuesta de aceptación.
Claimant	Dispositivo que interactúa al momento de obtener

	una petición de envío de información.
Encriptar	Encriptar es el proceso mediante el cual la información es codificada de tal manera que no pueda ser interpretada fácilmente.
Topología	Disposición física de los nodos de una red
Servidor	Una computadora que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes o Host's
Access Point	Este aparato va pegado a la red física (alambrada) y emite señal 802.11 b/g para vincular otros equipos inalámbricos. (No. Parte: WAP54G) los modelos más comunes funcionan en la banda de 2.4 Ghz
Nodo o Host	Parte Fundamental de una red, que interactúa con otros de su misma característica para formar cualquier forma de topologías de red existentes.
Swich	Un switch es un dispositivo de red que es capaz de buscar y seleccionar el camino correcto para enviar una serie de datos a su próximo destino.
Dirección IP	Es la identificación de una máquina en concreto dentro de la red a la que pertenece.

RESUMEN

La seguridad en una empresa cada día es más importante derivado que es a través de ella que gira todo el movimiento de la misma, es por ello que no solo la confidencialidad de los clientes están ligados a la misma, sino también la importancia de toda la información que gira entorno a la economía y personal de la empresa es de vital importancia también, por tal razón en cuanto a sido el avance de la tecnología, ya que contar en la actualidad con redes inalámbricas, lo cual permiten a los trabajadores que cuenten con computadoras móviles para trasladarse de un lugar a otro dentro de un radio determinado y estar conectados a la base de datos, y poder así realizar cada una de las operaciones diarias que su trabajo lo exige.

Es por ello que haciendo el estudio correspondiente de cómo implementar una red inalámbrica, utilizando la tecnología Bluetooth nos damos cuenta de que si no tomamos las debidas precauciones esta puede ser vulnerable a cualquier persona externa que con malas intenciones pueda sustraer información valiosa de la empresa y hacer uso indebido de la misma, provocando realmente resultados lamentables en donde el impacto puede ser realmente desastroso.

La tecnología inalámbrica Bluetooth contiene tres niveles de seguridad, los cuales nos permiten elegir de acuerdo a las necesidades que tengamos, el nivel de restricción de acceso a los recursos que serán compartidos, en el caso de una red de área local ubicada en una empresa es muy recomendable utilizar el nivel de seguridad mas alto y así realmente estar tranquilos de que nadie que no este autorizado va a hacer mal uso de la misma.

OBJETIVOS

- **General**

Realizar el diseño de implementación de una red inalámbrica Bluetooth, haciendo énfasis en la seguridad de la misma, para cualquier empresa implementándola tenga seguridad en la Base de Datos que manejan.

- **Específicos**

1. Conocer el funcionamiento de una red inalámbrica Bluetooth

2. Tener los conceptos necesarios para Implementar este tipo de Red y los elementos que la componen.

3. Determinar cada uno de los niveles de seguridad existentes en la tecnología Bluetooth

4. Analizar los modos de Acceso a la Red.

5. Diseñar una red inalámbrica con fines de implementación en una empresa guatemalteca dedicada al comercio

INTRODUCCIÓN

Las comunicaciones en la actualidad van en evolución constante, tal ejemplo es el caso de las redes inalámbricas ya que éstas están en un constante incremento, cuando es momento de tomar la decisión de montar una red para usos laborales. La seguridad en la red debe ser eficiente ante los ataques de los “piratas” que pretendan sustraer, modificar o atacar de alguna otra manera, ya que por ser inalámbrica opera en la banda libre entre 2.4 y 5 Ghz de frecuencia, este rango es universal y actualmente muchos dispositivos se están fabricando con esta tecnología.

Una división de redes inalámbricas la encontramos en la tecnología Bluettoth, algo que no es muy común utilizarlo para una red con fines laborales, pero si muy funcional cuando en una empresa queremos centralizar redes pequeñas dentro de la Lan, hace que la seguridad sea fundamental y así poder utilizar esta tecnología, estableciendo comunicación con los demás elementos de red que no se están comunicando vía inalámbrica.

Analizando la comunicación basándonos en esta tecnología, no podemos dejarnos de sorprender lo cuan insegura puede resultar y ver como esto se refleja en la posible fuga de información en la empresa. Por tal motivo hacemos énfasis en cada uno de los niveles de seguridad que podemos utilizar para tener completamente la certeza de que nadie que este autorizado en la misma pueda acceder a ella.

1. DESCRIPCIÓN GENERAL DE LA TECNOLOGÍA INALÁMBRICA BLUETOOTH

La tecnología inalámbrica Bluetooth nos brinda una forma de remplazar cables y enlaces infrarrojos que interconectan dispositivos por un enlace de radio universal de corto alcance, que nos permite la creación de radio LANs.

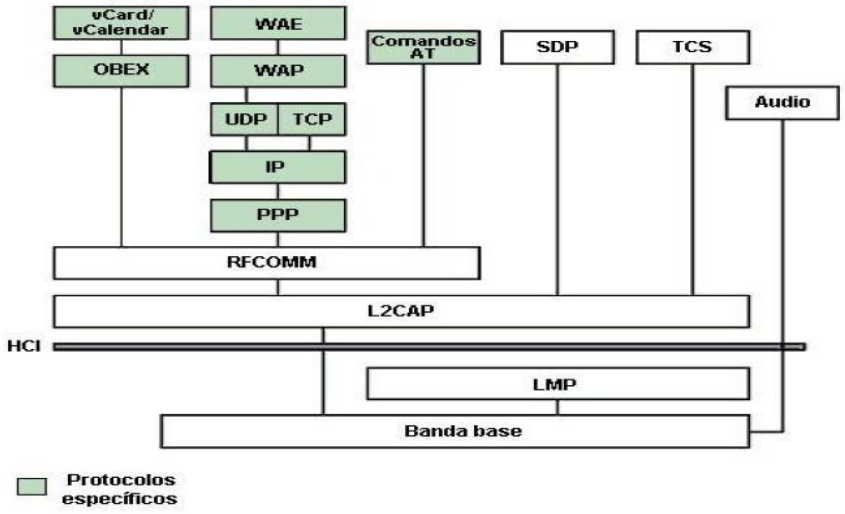
El nombre Bluetooth viene de un rey danés llamado Harald Blaatand (en inglés “Bluetooth”) quien vivió entre los años 940 y 981 y quien controló a Noruega y Dinamarca. En el año de 1998 en el mes de febrero, se fundó el ***Bluetooth Special Interest Group*** (SIG), creado con el fin de ofrecer soporte para la nueva tecnología. Actualmente, más de mil compañías lo integran y trabajan conjuntamente por un estándar abierto para el concepto Bluetooth.

Bluetooth es un sistema de radio que opera en la banda de frecuencia libre de 2.4 GHz, esta banda de frecuencia está disponible en la mayor parte del mundo, y nuestro país se encuentra en uno de ellos.

Bluetooth utiliza 79 canales de radio frecuencia con un ancho de banda de 1 MHz cada uno y una rata máxima de símbolos de 1 MSímbolo/s. Después de que cada paquete es enviado en una determinada frecuencia de transmisión, ésta cambia a otra de las 79 frecuencias. El rango típico de operación de Bluetooth es menor a 10 m, sin embargo se pueden alcanzar distancias de hasta 100 m con el uso de amplificadores, y actualmente varios dispositivos sin necesidad de amplificadores alcanzan los 100 metros, entre ellos la telefonía celular y dispositivos de red.

Como se puede observar en la figura 1, la comunicación sobre Bluetooth se divide en varias capas. A continuación se presenta una breve descripción de algunas de ellas.

Figura 1. Stack de Protocolos Bluetooth.



La capa de comunicación más baja es llamada **banda base**. Esta capa implementa el canal físico real. Esta realiza una secuencia aleatoria de saltos a través de 79 frecuencias de radio diferentes. Los paquetes son enviados sobre el canal físico, donde cada uno es enviado en una frecuencia de salto diferente. La Banda Base es la encargada de controlar la sincronización de las unidades Bluetooth y la secuencia de saltos en frecuencia, además tiene la responsabilidad de la información para el control de enlace a bajo nivel como el reconocimiento, control de flujo y caracterización de carga útil además que soporta dos tipos de enlace: síncrono orientado a la conexión (SCO), para datos y asíncrono no orientado a la conexión (ACL), principalmente para audio.

Los dos pueden ser multiplexados para usar el mismo enlace RF.

Los enlaces SCO soportan tráfico de voz en tiempo real usando ancho de banda reservado.

1.1 Protocolos utilizados

1.1.1 El *Link Manager Protocol* (LMP)

Protocolo de Gestión de Enlace es el encargado de la autenticación, encriptación, control y configuración del enlace. El LMP es también el encargado del manejo de los modos y consumo de potencia, además soporta los procedimientos necesarios para establecer un enlace SCO.

1.1.2 El *Host Controller Interface* (HCI)

Interfaz del Controlador de Enlace brinda un método de interfaz uniforme para acceder a los recursos de hardware de Bluetooth. Éste contiene una interfaz de comando para el controlador banda base y la gestión de enlace y para acceder al hardware.

1.1.3 El *Logical Link Control and Adaptation* Protocol (L2CAP)

Protocolo de *Control* y Adaptación de Enlace Lógico, corresponde a la capa de enlace de datos. Ésta da servicios de datos orientados y no orientados a la conexión a capas superiores. El fin primordial del L2CAP es multiplexar los *Protocol*os de capas superiores para poder enviar varios *Protocol*os sobre un canal b*and*a base. Con el fin de manipular paquetes de capas superiores más gr*and*es que el máximo tamaño del paquete b*and*a base, L2CAP los segmenta en varios paquetes b*and*a base. La capa L2CAP del receptor reensambla los paquetes b*and*a base en paquetes más gr*and*es para la capa superior. La conexión L2CAP también permite el intercambio de información referente a la calidad de la conexión, maneja grupos, de tal manera que varios dispositivos pueden comunicarse entre sí.

1.1.4 El *Service Discovery Protocol* (SDP)

Protocolo de Descubrimiento de Servicio define cómo actúa una aplicación de un cliente Bluetooth para descubrir servicios disponibles de servidores Bluetooth, como también de proporcionar un método para determinar las características de dichos servicios.

1.1.5 RFCOMM

Ofrece emulación de puertos seriales sobre el *Protocolo* L2CAP. RFCOMM emula señales de control y datos RS-232 sobre la banda base Bluetooth. Éste ofrece capacidades de transporte a servicios de capas superiores (por ejemplo OBEX) que usan una línea serial como mecanismo de transporte.

RFCOMM soporta dos tipos de comunicación, directa entre dispositivos actuando como *endpoints* y dispositivo-modem-dispositivo, además tiene un esquema para emulación de *null modem.*

1.1.6 El Control de telefonía binario (TCS binario)

Es un protocolo que define la señalización de control de llamadas, para el establecimiento y liberación de una conversación o una llamada de datos entre unidades Bluetooth. Además, éste ofrece funcionalidad para intercambiar información de señalización no relacionada con el progreso de llamadas. La capa de audio es una capa especial, usada únicamente para enviar audio sobre Bluetooth. Las transmisiones de audio pueden ser ejecutadas entre una o más unidades usando muchos modelos diferentes. Los datos de audio no pasan a través de la capa L2CAP, pero sí directamente después de abrir un enlace y un establecimiento directo entre dos unidades Bluetooth.

1.2 Protocolos específicos

1.2.1 *Control* de telefonía – com*and*os AT

Bluetooth soporta un número de com*and*os AT para el *Control* de telefonía a través de emulación de puerto serial (RFCOMM).

1.2.2 Protocolo Punto-a-Punto (PPP)

El PPP es un protocolo orientado a paquetes y por lo tanto debe usar su mecanismo serial para convertir un torrente de paquetes de datos en una corriente de datos seriales. Este protocolo corre sobre RFCOMM para lograr las conexiones punto-a-punto.

1.2.3 Protocolos UDP/TCP – IP

Los estándares UDP/TCP e IP permiten a las unidades Bluetooth conectarse, por ejemplo a Internet, a través de otras unidades conectadas. Por lo tanto, la unidad puede actuar como un puente para Internet. La configuración TCP/IP/PPP está disponible como un transporte para WAP.

1.2.4 Wireless Aplication Protocol (WAP) o *protocol*o de aplicación inalámbrica

WAP es una especificación de protocolo inalámbrica que trabaja con una amplia variedad de tecnologías de red inalámbricas conectando dispositivos móviles a Internet. Bluetooth puede ser usado como portador para ofrecer el transporte de datos entre el cliente WAP y su servidor de WAP adyacente. Además, las capacidades de red de Bluetooth dan a un cliente WAP posibilidades únicas en cuanto a movilidad comparado con otros portadores WAP. Un ejemplo de WAP sobre Bluetooth sería un almacén que transmite ofertas especiales a un cliente WAP cuando éste entra en el rango de cobertura.

1.2.5 Protocolo OBEX

OBEX es un protocolo opcional de nivel de aplicación diseñado para permitir a las unidades Bluetooth soportar comunicación infrarroja para intercambiar una gran variedad de datos y comandos. Éste usa un modelo cliente-servidor y es independiente del mecanismo de transporte y del API (Application Program Interface) de transporte. OBEX usa RFCOMM como principal capa de transporte.

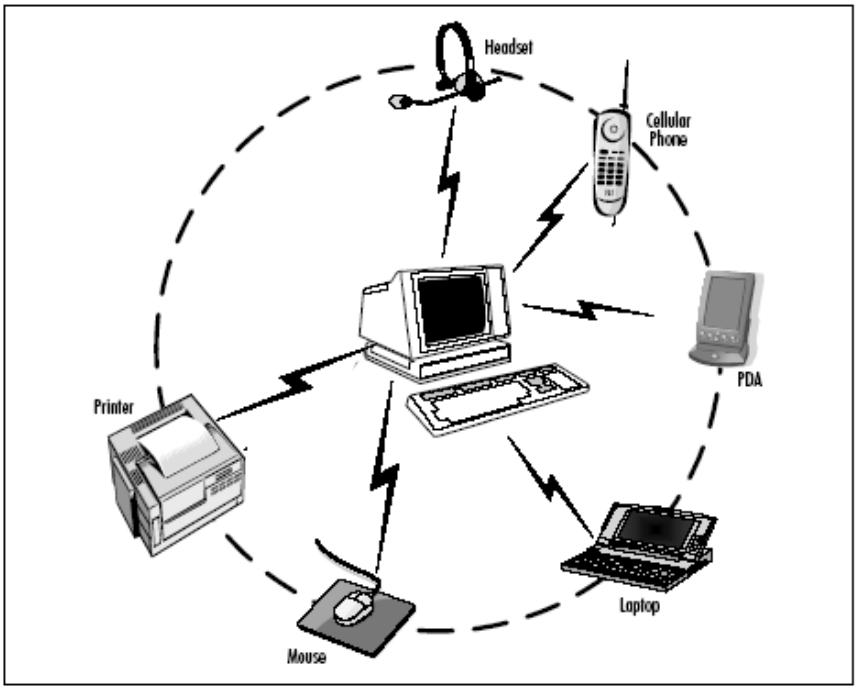
1.3 Banda base

1.3.1 Descripción general

La tecnología Bluetooth soporta un canal de datos asíncrono de hasta tres canales de voz de una manera simultanea, y es el principal responsable del manejo de los canales entre si. El canal asíncrono puede soportar comunicación simétrica y asimétrica. En la comunicación asimétrica pueden ser enviados 723.3 kb/s desde el servidor y 57.6 kb/s hacia el servidor, mientras que en la comunicación simétrica pueden ser enviados 433 kb/s en cualquiera de las dos direcciones.

Bluetooth brinda conexión punto-a-punto o conexión punto-a-multipunto. Dos o más unidades compartiendo el mismo canal forman una piconet. Cada piconet debe tener un maestro y puede tener hasta siete esclavos activos, además pueden haber muchos más esclavos en estado *parked*. Estos esclavos no están activos en el canal sin embargo están sincronizados con el maestro con el fin de asegurar una rápida iniciación de comunicación. La interconexión de varias *piconets* forma una *scatternet*. En la figura 2 se puede observar una piconet donde el PC actúa como maestro y los otros dispositivos son conectados como esclavos.

Figura 2. Piconet.



Fuente: Jennifer Bray. Bluetooth Application Developer's Guide. Pág. 3 Chapter 1

1.3.2 Enlace físico

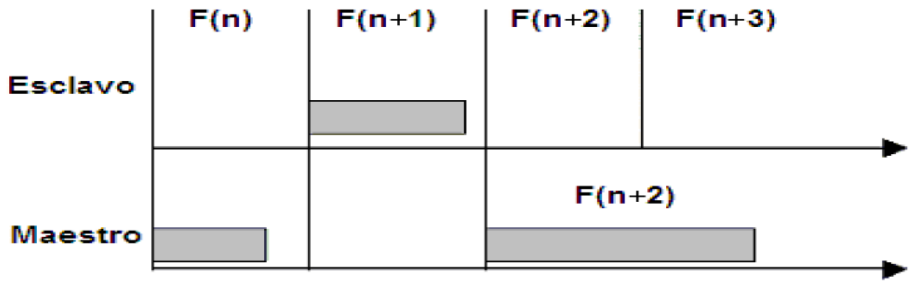
La comunicación sobre Bluetooth es perfecta para enlaces SCO o enlaces ACL. El enlace SCO es una conexión simétrica punto-a-punto entre el maestro y un esclavo específico. Para que esta comunicación pueda ser eficaz, el enlace SCO reserva slots en intervalos regulares en la iniciación, es por esto que puede considerarse como una conexión de conmutación de circuitos. El enlace ACL es un enlace punto-a-multipunto entre el maestro y uno o más esclavos activos en la piconet. Este enlace de comunicación es un tipo de conexión de conmutación de paquetes.

El maestro puede enviar mensajes broadcast (de difusión) a todos los esclavos conectados dej*and*o vacía la dirección del paquete, así todos los esclavos podrán leerán el paquete.

1.3.3 Canal físico

El canal físico contiene 79 frecuencias de radio diferentes, las cuales son accedidas de acuerdo a una secuencia de saltos aleatoria. La rata de saltos estándar es de 1600 saltos/s. El canal está dividido en *timeslots* (ranuras de tiempo), en donde cada *slot* (ranura) corresponde a una frecuencia de salto y tiene una longitud de 625 us. Todos los dispositivos conectados a la piconet están sincronizados con el canal en salto y tiempo. Cada secuencia de salto en una piconet está determinada por la dirección del maestro de la piconet. En una transmisión, cada paquete debe estar alineado con el inicio de un slot y puede tener una duración de hasta cinco *timeslots*. Durante la transmisión de un paquete la frecuencia siempre es fija. Para evitar fallas en la transmisión, el maestro inicia enviando en los *timeslots* pares y los esclavos en los *timeslots* impares. En la figura 3 se puede observar este esquema de transmisión.

Figura 3. Transmisión en una Piconet.



1.3.4 Paquetes

Los datos enviados sobre el canal de la piconet son convertidos en paquetes, éstos son enviados y el receptor los recibe iniciando por el BIT menos significativo. Como se observa en la figura 4, el formato de paquete general consta de tres campos: código de acceso, cabecera y carga útil.

Figura 4. Forma general de un paquete.

Fuente. Specification of the Bluetooth System Pág.47

1.3.4.1 Código de acceso *Access Code*

Es usado para sincronización e identificación. Todos los paquetes comunes que son enviados sobre el canal de la piconet están precedidos del mismo código de acceso al canal. Existen tres tipos diferentes de código de acceso:

- **Código de acceso al canal:** Para identificar los paquetes sobre el canal de la *piconet*.

- **Código de acceso de dispositivo:** Para procedimientos de señalización especiales, *paging* (servicio para transferencia de señalización o información en un sentido), entre otros.

- **Código de acceso de búsqueda (IAC)**: Llamado IAC general cuando se quiere descubrir a otras unidades Bluetooth dentro del rango, o IAC dedicado cuando se desea descubrir unidades de un tipo específico.

1.3.4.2 Cabecera de paquete *Header*

Como se observa en la figura 5, la cabecera de paquete esta comprendido por seis campos:

- **Dirección:** una dirección de dispositivo para distinguirlo de los demás dispositivos activos en la piconet.

- **Tipo**: define qué tipo de paquete es enviado.

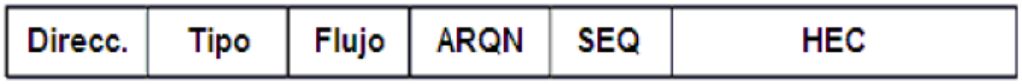
- **Flujo**: el BIT de control de flujo es usado para notificar al emisor cuándo el buffer del receptor está lleno (similar a una bandera).

- **ARQN:** *Acknowledge Receive Data* o reconocimiento de datos recibidos.

- **SEQN:** *Sequential Numbering* o numeración secuencial para ordenar los datos sobre el canal.

- **HEC:** chequeo de redundancia cíclica de cabecera.

Figura 5. Cabecera de paquete.



1.3.4.3 Carga útil *Payload*

Esta puede ser dividida en dos campos:

- **Campo de voz**: consta de datos de voz de longitud fija y existe en paquetes de alta calidad de voz y paquetes combinados de datos-voz

.

- **Campo de datos** consta de tres partes, cabecera de carga útil, datos de carga útil, y código CRC.

1.3.5 Corrección de errores

En una comunicación Bluetooth existen varios esquemas diferentes de corrección de errores:

- En la cabecera, cada BIT es repetido tres veces.

- En la carga útil es utilizado un esquema de código *Hamming*. Los bits de información se agrupan en secuencias de 10 bits, éstos son enviados como 15 bits y el algoritmo corrige todos los errores de un BIT y detecta los errores de dos bits.

- Para asegurar una recepción correcta, todos los paquetes de datos son retransmitidos hasta que el emisor reciba una confirmación. La confirmación es enviada en la cabecera de los paquetes retornados.

- Los paquetes *broadcast* son paquetes transmitidos desde el maestro a todos los esclavos. Para incrementar la posibilidad de recibir correctamente un paquete, cada BIT en el paquete es repetido un número fijo de veces.

- El chequeo de redundancia cíclica (CRC) se usa para detectar errores en la cabecera.

- Para asegurar que no desaparezcan paquetes completos, Bluetooth usa números de secuencia.

1.3.6 Transmisión/Recepción

El maestro de la *piconet* empieza enviando en *timeslots* pares y el esclavo en los impares. Solamente el último esclavo direccionado está autorizado para enviar en el *timeslot* de los esclavos. Esto no causa problemas ya que el maestro siempre está inicializando todas las conexiones y transmisiones nuevas. Los paquetes pueden ser más grandes que un *timeslot*,

debido a esto el maestro puede continuar enviando en los *timeslots* impares y viceversa. El sistema de reloj del maestro es quien hace la función de sincronización de toda la *piconet*. El maestro nunca ajusta su sistema de reloj durante la existencia de una *piconet*, son los esclavos quienes adaptan sus relojes con un *offset* de tiempo con el fin de igualarse con el reloj del maestro. Este *offset* es actualizado cada vez que es recibido un paquete desde el maestro.

1.3.7 Control de canal

El control de canal describe cómo se establece el canal de una *piconet* y cómo las unidades pueden ser adicionadas o liberadas en la *piconet*. La dirección del maestro determina la secuencia de saltos y el código de acceso al canal. La fase de la piconet está determinada por el sistema de reloj del maestro. Por definición, la unidad Bluetooth que inicia la conexión representa al maestro.

En Bluetooth, la capa de control de enlace se divide en dos estados principales: st*andby* y conexión. Además existen siete sub-estados: *page, page scan, inquiry* (búsqueda), *inquiry scan*, respuesta de maestro, respuesta de esclavo y respuesta a *inquiry*. Los sub-estados son usados para agregar nuevos esclavos a una *piconet*. Para moverse de un estado a otro se usan comandos de capas más altas o señales internas.

En la tecnología Bluetooth se define un procedimiento de búsqueda que se usa en aplicaciones donde la dirección del dispositivo de destino es

desconocida para la fuente. Esto puede ser usado para descubrir qué otras unidades Bluetooth están dentro del rango. Durante un sub-estado de inquiry o búsqueda, la unidad de descubrimiento recoge la dirección del dispositivo y el reloj de todas las unidades que respondan al mensaje de búsqueda, entonces la unidad puede iniciar una conexión con alguna de las unidades descubiertas. El mensaje de búsqueda difundido por la fuente no contiene información de ella, sin embargo, puede indicar qué clase de dispositivos deberían responder. Una unidad que permita ser descubierta, regularmente entra en un sub-estado de *inquiry scan* para responder a los mensajes de búsqueda.

Existen dos formas de detectar otras unidades. La primera, detecta todas las otras unidades en el rango de cobertura, y la segunda, detecta un tipo específico de unidades. Los esclavos que se encuentran en el sub-estado de *page scan*, escuchan esperando su propio código de acceso de dispositivo. El maestro en el sub-estado *page*, activa y conecta a un esclavo. El maestro trata de capturar al esclavo transmitiendo repetidamente el código de acceso de dispositivo en diferentes canales de salto. Debido a que los relojes del maestro y del esclavo no están sincronizados, el maestro no sabe exactamente cuándo y en qué frecuencia de salto se activará el esclavo.

Después de haber recibido su propio código de acceso de dispositivo, el esclavo transmite un mensaje de respuesta. Este mensaje de respuesta es simplemente el código de acceso de dispositivo del esclavo. Cuando el maestro ha recibido este paquete, envía un paquete de control con información acerca de su reloj, dirección, clase de dispositivo, etc. El esclavo responde con un nuevo mensaje donde envía su dirección. Si el maestro no obtiene esta respuesta en un determinado tiempo, él reenvía el paquete de control. Si el esclavo excede el tiempo de espera, entonces retorna al sub-estado de *page*

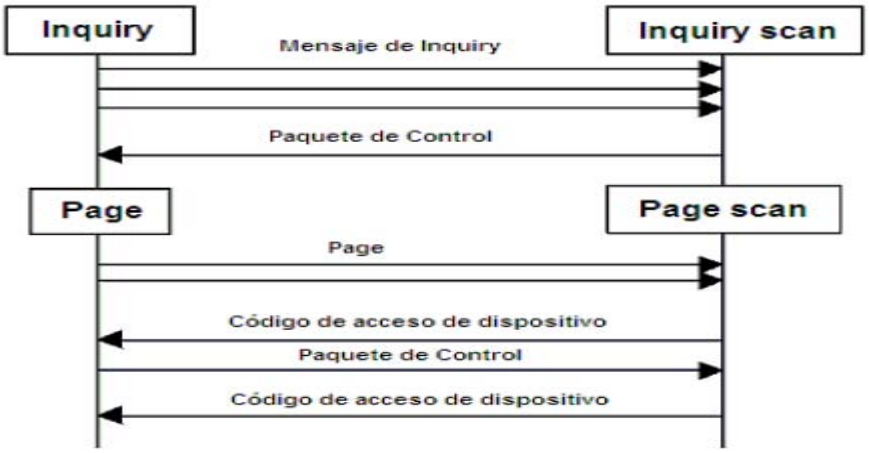
scan. Si es el maestro quien lo excede, entonces retorna al sub-estado de page e informa a las capas superiores.

Cuando se establece la conexión, la comunicación inicia con un paquete de sondeo desde el maestro hacia el esclavo. Como respuesta se envía un nuevo paquete de sondeo y de esta forma se verifica que la secuencia de salto y la sincronización sean correctas.

Cada *transceiver* receptor-transmisor Bluetooth tiene una única dirección de dispositivo de 48 bits asignada, la cual está dividida en tres campos: campo LAP, campo UAP y campo NAP. Los campos LAP y UAP forman la parte significativa del código de acceso.

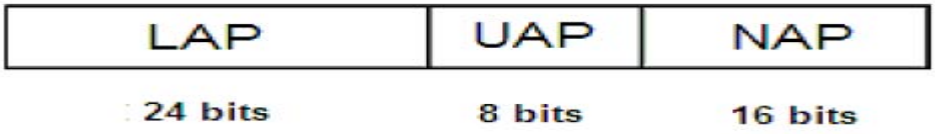
La figura 6 muestra la inicialización de la comunicación sobre el nivel banda base.

Figura 6. Iniciación de comunicación sobre el nivel de b*and*a base.



En la figura 7 se puede observar el formato de la dirección para un dispositivo Bluetooth. La dirección del dispositivo es conocida públicamente y puede ser obtenida a través de una rutina *inquiry*.

Figura 7. Dirección de dispositivos Bluetooth.



1.4 Protocolo de gestión de enlace (LMP)

En el Protocolo de gestión de enlace, LMP, se usan mensajes asociados con el establecimiento, seguridad y control. Los mensajes son enviados en la carga útil y no en los mensajes de datos de L2CAP. Los mensajes LMP son separados de los demás por medio de un valor reservado en uno de los campos de la cabecera de carga útil. Todos los mensajes LMP son filtrados e interpretados por la capa LMP del receptor, esto significa que ningún mensaje es enviado a capas superiores.

Los mensajes LMP tienen mayor prioridad que los datos de usuario, esto significa que si la gestión de enlace necesita enviar un mensaje, éste no debe ser retrasado por otro tráfico. Solamente las retransmisiones de los paquetes del nivel de banda base pueden retrasar los mensajes LMP. Además, éstos no necesitan rutinas de reconocimiento ya que la capa banda base asegura un enlace confiable. El protocolo de gestión enlace soporta mensajes para:

- Autenticación
- Paridad
- Temporización y sincronización
- Versión y características
- Encriptación
- *Switch* para desempeño como maestro o esclavo
- Petición de nombre
- Desconexión
- Modo *hold*: el maestro ordena al esclavo entrar en este estado para ahorro de potencia.
- Modo *sniff*: para envío de mensajes en *timeslots* específicos.
- Modo *park*: para que el esclavo permanezca inactivo pero sincronizado en la *piconet*.
- Enlaces SCO
- Control de paquetes *multi-slot*
- Supervisión de enlace

1.4.1 Establecimiento de conexión

Después del procedimiento paging, el maestro debe encuestar al esclavo enviando paquetes de sondeo. El otro lado recibe este mensaje y lo acepta o rechaza, si es aceptado, la comunicación incluyendo las capas superiores están disponibles (ver figura 8)

Figura 8. Establecimiento de la conexión

1.5 Protocolo de control y adaptación de enlace lógico (L2CAP)

L2CAP es encontrado sobre el protocolo de gestión de enlace (LMP) y esta ubicado 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 64 kilobytes, con capacidad de multiplexación de

protocolo, operación de segmentación y reensamble, y abstracción de grupos. Para poder funcionar efectivamente, L2CAP espera que la banda base suministre paquetes de datos en *full duplex*, que 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 podríamos tenerlas como ejemplo el protocolo de descubrimiento de servicio (SDP), el RFCOMM y el control de telefonía (TCS).

1.5.1 Canales

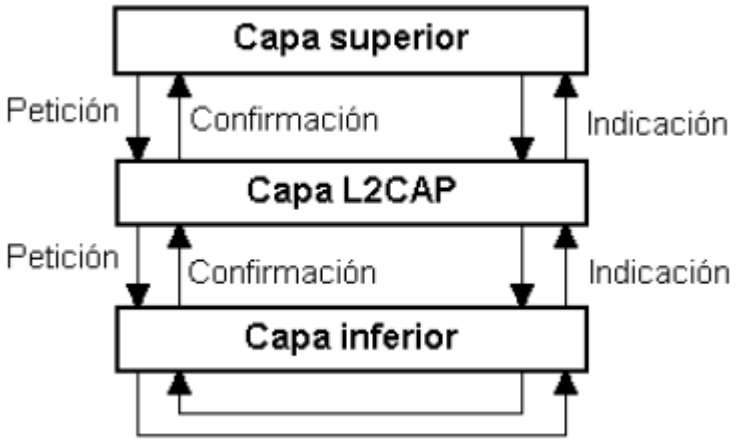
L2CAP está basado en el concepto de canales. A cada unidad de los canales *endpoints* de un canal L2CAP es asociado un identificador de canal, CID, Los cuales están divididos en dos grupos, uno con identificadores reservados para funciones L2CAP y otro con identificadores libres para implementaciones particulares. Los canales de datos orientados a la conexión representan una conexión entre dos dispositivos, donde un CID identifica cada *endpoint* del canal.

Los canales no orientados a la conexión limitan el flujo de datos a una sola dirección. 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.

1.5.2 Operaciones entre capas

Las implementaciones L2CAP deben transferir datos entre protocolos de capas superiores e inferiores. Cada implementación debe soportar un grupo de comandos de señalización, además, debe ser capaz de aceptar ciertos tipos de eventos de capas inferiores y generar eventos para capas superiores. En la figura 9 se muestra esta arquitectura.

Figura 9. Arquitectura L2CAP.

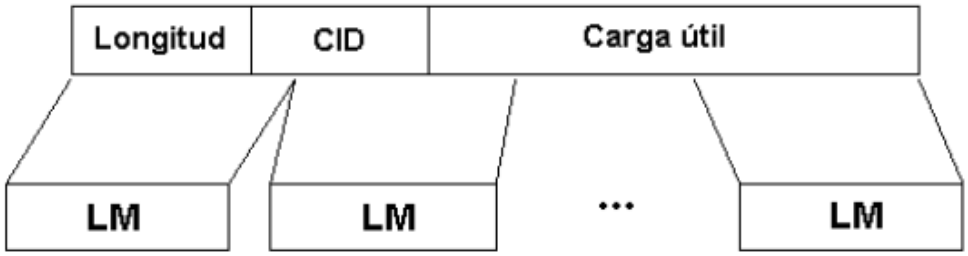


1.5.3 Segmentación y reensamblado

Todo paquete de dato está limitado en tamaño y son definidos por el protocolo de banda base. Los paquetes L2CAP grandes deben ser segmentados en varios paquetes banda base más pequeños antes de

transmitirse y luego deben ser enviados a la gestión de enlace. En el receptor los pequeños paquetes 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, SAR, funcionalmente es absolutamente necesaria para soportar protocolos usando paquetes más grandes que los soportados por la banda base. La figura 10 nos enseña la segmentación L2CAP.

Figura 10. Segmentación L2CAP.



1.5.4 Eventos

Todos los mensajes y *timeouts* 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.

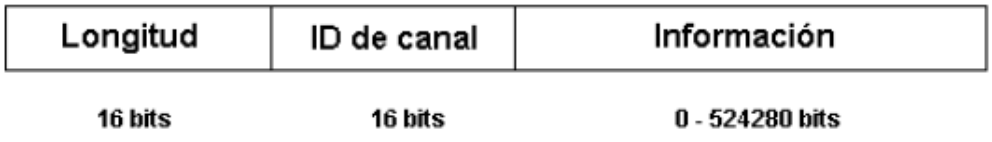
1.5.5 Acciones

Todos los mensajes y *timeouts* enviados desde la capa L2CAP son llamados acciones (en el lado del receptor estas acciones son llamadas eventos). Las acciones se encuentran divididas en cinco categorías: peticiones y respuestas a capas inferiores, peticiones y respuestas a capas L2CAP, datos a capas L2CAP, indicaciones a capas superiores y configuración de *timers*.

1.5.6 Formato del paquete de datos

L2CAP está basado en paquetes pero sigue un modelo de comunicación basado en canales. Un canal representa un flujo de datos entre entidades L2CAP en dispositivos remotos. Los canales pueden ser o no orientados a la conexión. Como se observa en la figura 11, los paquetes de canal orientado a la conexión están divididos en tres campos: longitud de la información, identificador de canal e información.

Figura 11. Paquete L2CAP



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

1.5.7 Calidad de servicio (QoS)

La capa L2CAP transporta la información de calidad de servicio a través de los canales y brinda control de admisión para evitar que canales adicionales violen contratos de calidad de servicio existentes

Antes de que un esclavo con grandes peticiones sea conectado a una piconet, el esclavo trata de obtener una garantía a sus demandas. Puede solicitar una determinada rata de transmisión, tamaño del buffer de tráfico, ancho de banda, tiempo de recuperación de datos, etc. Por lo tanto, antes de que el maestro conecte a un nuevo esclavo o actualice la configuración de calidad, debe chequear si posee *timeslots* y otros recursos libres.

1.6 Protocolo de descubrimiento de servicio (SDP)

Este protocolo brinda a las aplicaciones recursos para descubrir qué servicios están disponibles y determinar las características de dichos servicios.

1.6.1 Descripción General

Un servicio es una entidad que puede brindar información, ejecutar una acción o controlar un recurso a nombre de otra entidad.

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. Para hacer más fácil la búsqueda, el SDP la habilita sin un previo conocimiento de las características específicas de los servicios. Las unidades Bluetooth que usan el SDP pueden ser vistas 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.

1.6.2 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 propiedad 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.

1.6.3 El protocolo SDP

El protocolo de descubrimiento de servicio (SDP) usa un modelo petición/respuesta.

1.6.3.1 Petición de búsqueda de servicio

Se genera por el cliente para localizar registros de servicio que concuerden con un patrón de búsqueda dado como parámetro. Aquí el servidor examina los registros en su base de datos y responde con una respuesta a búsqueda de servicio.

1.6.3.2 Respuesta a búsqueda de servicio

Se genera por el servidor después de recibir una petición de búsqueda de servicio válida.

1.6.3.3 Petición de propiedad de servicio

Una vez el cliente ya ha recibido los servicios deseados, puede obtener mayor información de uno de ellos dando como parámetros el registro de servicio y una lista de propiedades deseadas.

1.6.3.4 Respuesta a propiedad de servicio

El SDP genera una respuesta a una petición de propiedad de servicio. Ésta contiene una lista de propiedades del registro requerido.

1.6.3.5 Petición de búsqueda y propiedad de servicio

Se suministran un patrón de servicio con servicios deseados y una lista de propiedades deseadas que concuerden con la búsqueda.

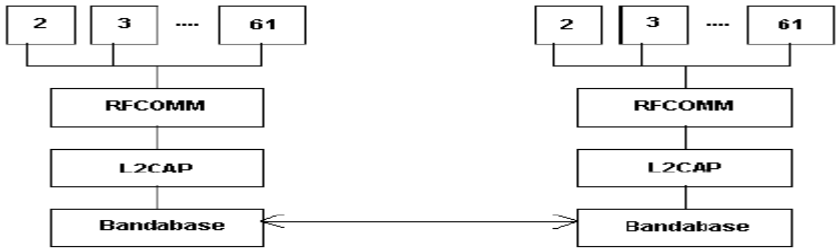
1.6.3.6 Respuesta de búsqueda y propiedad de servicio

Como resultado se puede obtener una lista de servicios que concuerden con un patrón dado y las propiedades deseadas de estos servicios.

1.7 RFCOMM

El protocolo RFCOMM brinda emulación de puertos seriales sobre el protocolo L2CAP. La capa RFCOMM es una simple capa de transporte provista adicionalmente de emulación de circuitos de puerto serial RS232. El protocolo RFCOMM 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 12 muestra el esquema de emulación para varios puertos seriales.

Figura 12. Varios puertos seriales emulados mediante RFCOMM



Muchas aplicaciones hacen uso de puertos seriales. El RFCOMM está orientado a hacer más flexibles estos dispositivos, soportando fácil adaptación de comunicación Bluetooth. Un ejemplo de una aplicación de comunicación serial es el protocolo Punto-a-Punto (PPP). El RFCOMM tiene construido un esquema para emulación de *null modem* y usa a L2CAP para cumplir con el control de flujo requerido por alguna aplicación.

1.8 Perfiles Bluetooth

El estándar Bluetooth fue creado para ser usado por un gran número de fabricantes e implementado en áreas ilimitadas. Para asegurar que todos los dispositivos que usen Bluetooth sean compatibles entre sí son necesarios esquemas estándar de comunicación en las principales áreas. Para evitar diferentes interpretaciones del estándar Bluetooth acerca de cómo un tipo específico de aplicación debería ser implementado, el *Bluetooth Special Interest Group* (SIG), ha definido modelos de usuario y perfiles de protocolo. Un perfil define una selección de mensajes y procedimientos de las especificaciones Bluetooth y ofrece una descripción clara de la interfaz de aire para servicios

específicos. Un perfil puede ser descrito como una “rebanada” completa del snack de protocolo.

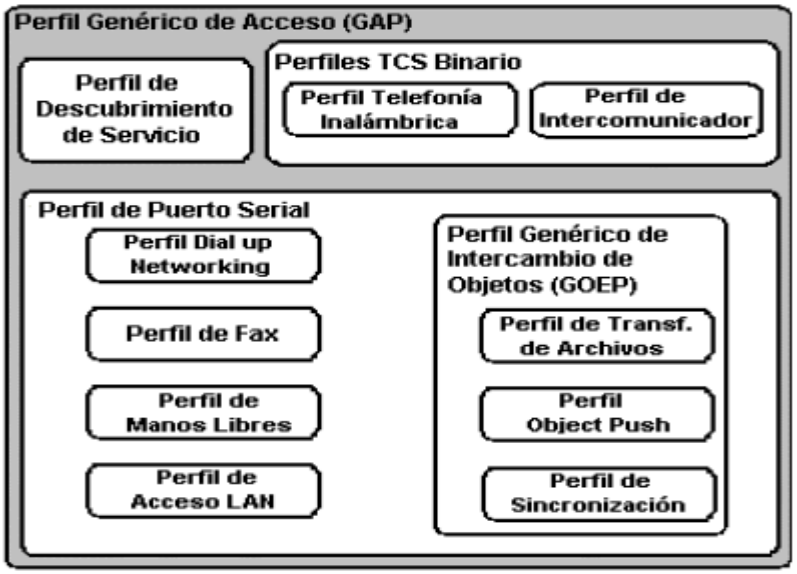
Existen cuatro perfiles generales definidos, en los cuales están basados directamente algunos de los modelos de usuario más importantes y sus perfiles.

Estos cuatro modelos son:

- Perfil Genérico de Acceso (GAP)
- Perfil de Puerto Serial
- Perfil de Aplicación de Descubrimiento de Servicio (SDAP)
- Perfil Genérico de Intercambio de Objetos (GOEP)

A continuación se hace una breve descripción de estos y algunos otros perfiles Bluetooth. La figura 13 muestra el esquema de los perfiles Bluetooth. En ella se puede observar la jerarquía de los perfiles, como por ejemplo que todos los perfiles están contenidos en el Perfil Genérico de Acceso (GAP).

Figura 13. Los Perfiles Bluetooth



1.8.1 Perfil Genérico de Acceso (GAP)

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 aplicación, puedan intercambiar información a través de Bluetooth para descubrir qué tipo de aplicaciones soportan las unidades.

1.8.2 Perfil de puerto serial

Este perfil define los requerimientos para dispositivos Bluetooth, necesarios para establecer una conexión de cable serial emulada usando RFCOMM entre dos dispositivos similares. Este perfil solamente requiere soporte para paquetes de un *slot*. Esto significa que pueden ser usadas ratas de datos de hasta 128 kbps. El soporte para ratas más altas es opcional.

RFCOMM es usado para transportar los datos de usuario, señales de control de *modem* y comandos de configuración. El perfil de puerto serial es dependiente del GAP.

1.8.3 Perfil de aplicación de descubrimiento de servicio (SDAP)

Este perfil define los protocolos y procedimientos para una aplicación en un dispositivo Bluetooth donde se desea descubrir y recuperar información relacionada con servicios localizados en otros dispositivos. El SDAP es dependiente del GAP.

1.8.4 Perfil genérico de intercambio de objetos (GOEP)

Este perfil define protocolos y procedimientos usados por aplicaciones para ofrecer características de intercambio de objetos. Los usos pueden ser, por ejemplo, sincronización, transferencia de archivos o modelo O*bject Push*.

Los dispositivos más comunes que usan este modelo son agendas electrónicas, PDAs, teléfonos celulares y teléfonos móviles. El GOEP es dependiente del perfil de puerto serial.

1.8.5 Perfil de telefonía inalámbrica

Este perfil define cómo 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.

1.8.6 Perfil de intercomunicador

Este perfil define usos de teléfonos móviles los cuales establecen enlaces de conversación directa entre dos dispositivos. El enlace directo es establecido usando señalización de telefonía sobre Bluetooth.

Los teléfonos móviles que usan enlaces directos funcionan como *walkie-talkies.*

1.8.7 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.

1.8.8 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 o *modem* es usado como un *modem* inalámbrico.

1.8.9 Perfil de fax

Este perfil define los protocolos y procedimientos que deben ser usados por dispositivos que implementen el uso de fax. En el perfil un teléfono celular puede ser usado como un fax inalámbrico.

1.8.10 Perfil de acceso LAN

Este perfil define el acceso a una red de área local LAN, usando el protocolo Punto-a-Punto, PPP, sobre RFCOMM. PPP es ampliamente usado para lograr acceder a redes soportando varios protocolos de red. El perfil soporta acceso LAN para un dispositivo Bluetooth sencillo, acceso LAN para varios dispositivos Bluetooth y PC-a-PC (usando interconexión PPP con emulación de cable serial).

1.8.11 Perfil O*bject Push*

Este perfil define protocolos y procedimientos usados en el modelo O*bject Push*. Este perfil usa el GOEP. En el modelo O*bject Push* hay procedimientos para introducir en el *inbox*, sacar e intercambiar objetos con otro dispositivo Bluetooth.

1.8.12 Perfil de transferencia de archivos

Este perfil define protocolos y procedimientos usados en el modelo de transferencia de archivos. El perfil usa el GOEP. En el modelo de transferencia de archivos hay procedimientos para chequear un grupo de objetos de otro dispositivo Bluetooth, transferir objetos entre dos dispositivos y manipular objetos de otro dispositivo. Los objetos podrían ser archivos o fólderes de un grupo de objetos tal como un sistema de archivos.

1.8.13 Perfil de sincronización

Este perfil define protocolos y procedimientos usados en el modelo de sincronización. Éste usa el GOEP. El modelo soporta intercambios de información, por ejemplo para sincronizar calendarios de diferentes dispositivo.

2. CONCEPTOS PARA LA IMPLEMENTACIÓN DE UNA RED DE ÁREA PERSONAL BLUETOOTH

Varias de las especificaciones Bluetooth son definidos escenarios en los cuales son necesarios para el desarrollo de la tecnología entes mencionada. Antes de conocer este tipo de escenarios es necesario saber el concepto de lo que es una *Piconet* y lo que es una *Scatternet* luego podemos citar los escenarios entre los que esta el perfil de área personal o perfil PAN (*Personal Area Networking Profile*). Este perfil brinda capacidades de red a estos dispositivos para lo cual utiliza un tipo de encapsulamiento de red BNEP (*Bluetooth Network Encapsulacion Protocol*). Este es de gran importancia derivado de que este encapsula los paquetes provenientes de varios protocolos de red y estos son transportados directamente a través de la capa L2CAP de Bluetooth, haciendo posible que esta red funcione.

2.1 *Piconet y Scatternet*

Una red *Piconet* es una red que esta compuesta por un dispositivo maestro y dispositivos esclavo, en la *piconet* únicamente los esclavos son conectados con el maestro y es el que determina la secuencia de saltos en una *Piconet*. Una *Piconet* es ejemplificada como se muestra en la figura 14.

Figura 14. Composición de una Piconet.

Fuente: Presentación Red Inalámbrica Bluetooth. Ricardo Maya. Universidad del valle

En una P*iconet* cuando uno de los esclavos interactúa con otra *Piconet* se forma lo que es una *Scatternet*.

Figura 15. Composición de una Scatternet.

Fuente: Presentación Red Inalámbrica Bluetooth. Ricardo Maya. Universidad del valle

2.2 Protocolo de encapsulamiento de red BNEP

El protocolo de encapsulamiento de red de Bluetooth encapsula los paquetes de los protocolos de red más utilizados, para ser transportados sobre la capa L2CAP.

BNEP requiere además un formato de encapsulamiento que optimice los bits de cabecera de tal manera que se ofrezca un manejo eficiente del ancho de banda.

Entre varias observaciones que debemos de tener muy encuentra en cuanto a este protocolo podemos ver las siguientes

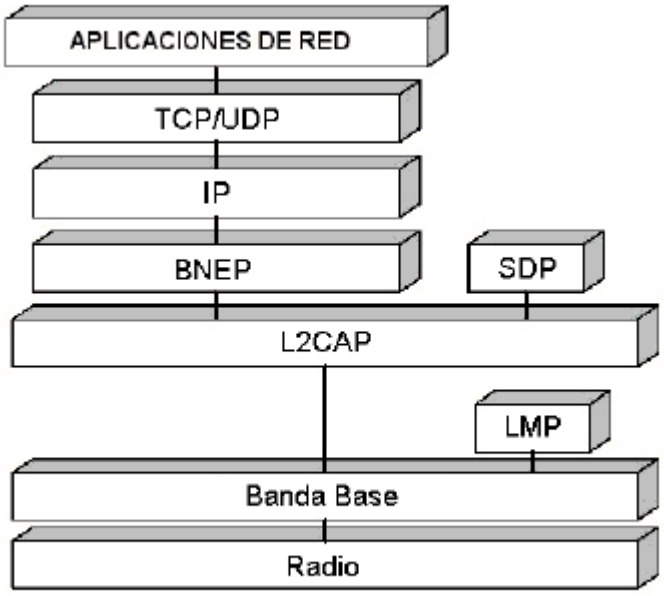
- Este Protocolo se implementa a través de canales L2CAP orientados a la conexión, BNEP especifica una unidad máxima de Transmisión (MTU) para L2CAP de 1691 bytes, esta fue seleccionada basándose en el paquete de carga útil de una *ethernet* (1500 bytes más 15 bytes de encabezado de BNEP y otros de extensión). 1691=5*339 (Tamaño de un DH5) – 4 (encabezado de L2CAP).

- Bluetooth se considera un medio de transmisión de un nivel OSI en una *ethernet*.

- Deben Aplicarse las reglas de conectividad y las topologías definidas por el Estándar lEEE 802.3

A continuación la figura 16 nos muestra donde esta ubicado el protocolo BNEP dentro de los demás protocolos de la Red Bluetooth

Figura 16. Ubicación de protocolo BNEP.



2.2.1 Orden de los *bytes* y valores numéricos

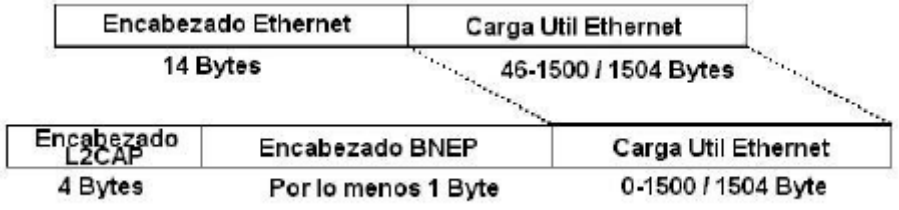
Los campos que contienen múltiples *bytes* (bits) se muestran con los *bytes* (bits) más significativos hacia la izquierda y los menos significativos hacia la derecha. Los *bytes* de los encabezados de BNEP se disponen en el formato estándar de red *Big Endian*, en donde los *bytes* más significativos se transmiten antes que los menos significativos. El *byte* cero es el más significativo. La numeración se esta denotando en forma hexadecimal.

2.2.2 Encapsulamiento de paquetes

La figura 17 nos muestra la manera como BNEP remueve los encabezados de un paquete *ethernet* y los reemplaza por un encabezado BNEP. El paquete resultante (carga útil de *ethernet* y el encabezado de BNEP) es encapsulado en un paquete L2CAP y enviado sobre Bluetooth.

BNEP es usado para transportar sobre Bluetooth tanto paquetes de datos como paquetes de control, de esta manera brinda a los dispositivos Bluetooth capacidades de red similares a las ofrecidas por *ethernet*.

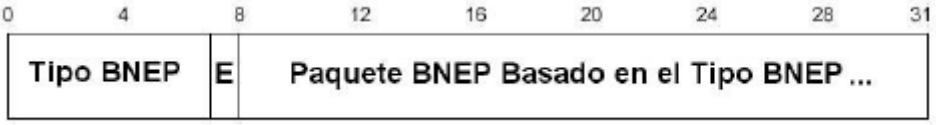
Figura 17. Encapsulamiento de un paquete *ethernet* en uno L2CAP.



2.2.3 Formato de los encabezados BNEP

Todos los encabezados de BNEP siguen la forma que aparece en la figura 18

Figura 18. Formato de encabezados BNEP.



El tipo BNEP tiene un tamaño de 7 bits y es el que identifica el tipo de encabezado BNEP que contiene el paquete.

La que se denomina con la letra (E) es la bandera de extensión, y esta es la indica si existe uno o más encabezados de extensión entre el encabezado de BNEP y la carga útil.

Y por último esta el Paquete BNEP y este depende del valor que se haya consignado en el campo del Tipo de BNEP

2.3 Tipos de paquetes

2.3.1 Tipo de paquete *BNEP_GENERAL_ETHERNET*

El paquete general de ethernet para BNEP se debe usar para transportar paquetes ethernet desde y hacia redes Bluetooth. Como lo podemos ver en la figura 19 el paquete está conformado por una dirección origen, una dirección destino y el tipo de protocolo de red contenido en la carga útil.

Cualquiera de las direcciones ya sea origen o destino puede corresponder a una dirección ethernet IEEE, si el origen o destino es un dispositivo IEEE y no un dispositivo Bluetooth

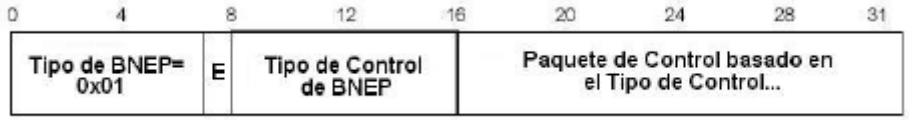
Figura 19. Formato de encabezado para un paquete BNEP_GENERAL_ETHERNET.

2.3.2 Tipo de paquete *BNEP_CONTROL*

El paquete de control de BNEP es utilizado para intercambiar información de control. En este tipo de paquete, toda la información de control está contenida en el encabezado del *BNEP_CONTROL* de tal manera que el campo de carga útil no contiene información alguna. Por el momento hay siete tipos de paquetes de control BNEP. El tipo de paquete de control es definido por el valor que se consigne en el campo tipo de control de BNEP; no se entra en detalle sobre cada tipo de paquete de control ya que esto no está dentro de los alcances del trabajo de graduación.

La figura 20 nos muestra el formato para el encabezado de un paquete *BNEP_CONTROL***.**

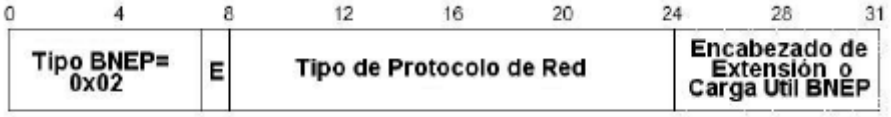
Figura 20. Formato de encabezado para un paquete *BNEP_CONTROL.*



2.3.3 Tipo de paquete *BNEP_COMPRESSED_ETHERNET*

El paquete ethernet comprimido de BNEP se usa para transportar paquetes ethernet hacia o desde dispositivos que tienen una conexión directa al nivel de la capa L2CAP usando BNEP. Debido a la existencia de una conexión L2CAP entre los dos dispositivos Bluetooth no es necesario incluir dentro del paquete las direcciones de origen y destino. La figura 21 muestra el formato de un paquete *BNEP_COMPRESSED_ETHERNET***.**

Figura 21. Formato de encabezado para un paquete *BNEP_ COMPRESSED_ETHERNET*.

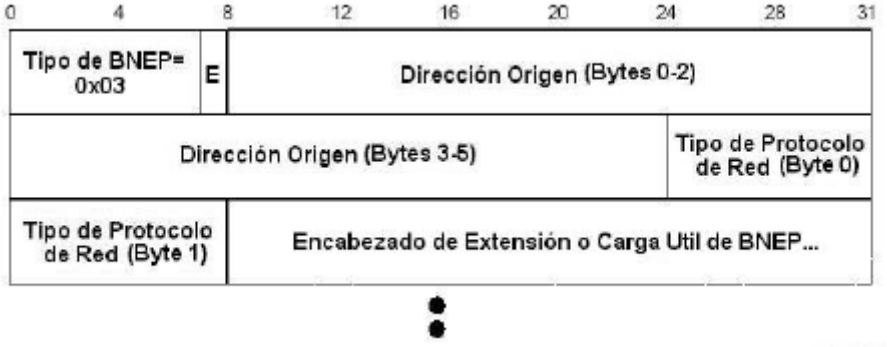


2.3.4 Tipo de paquete *BNEP_COMPRESSED_ETHERNET_SOURCE_ONLY*

Este paquete ethernet comprimido se usa para transportar paquetes ethernet hacia un dispositivo el cual siempre será el destino final para todos los paquetes.

Por esta razón los dispositivos no necesitan incluir la dirección destino en los paquetes siendo esta la misma dirección correspondiente al canal L2CAP sobre el cual se envían los paquetes.

Figura 22. Formato de encabezado para un paquete *BNEP_COMPRESSED_ETHERNET_SOURCE_ONLY*.



2.3.5 Tipo de paquete *BNEP_COMPRESSED_ETHERNET_DEST_ONLY*

Este paquete comprimido ethernet es usado para transportar paquetes desde un dispositivo el cual es la fuente del paquete. De esta manera los

dispositivos no necesitan incluir la dirección de la fuente del paquete, ya que esta fuente puede determinarse a partir de la conexión L2CAP.

Figura 23. Formato de encabezado para un paquete *BNEP_COMPRESSED_ETHERNET_DEST_ONLY.*

2.4 Perfil de red de área personal *Pan Profile*

El perfil PAN (*Personal Area Networking Profile*) describe cómo usar el protocolo BNEP para brindar capacidades de red a los dispositivos Bluetooth. El perfil PAN presenta los siguientes requerimientos funcionales:

- Define una red IP Ad-Hoc, dinámica y personal
- Debe ser independiente del sistema operativo, lenguaje y dispositivo
- Brinda soporte para los protocolos de red más comunes como IPv4 e IPv6.

- Brinda soporte para puntos de acceso en donde la red puede ser una LAN corporativa, GSM u otro tipo de red de datos.

- Debe acomodarse a los recursos reducidos disponibles en los dispositivos pequeños respecto a memoria, capacidad de procesamiento y uso de interfaces.

2.4.1 Consideraciones

.

La primera consideración que debemos tomar en cuenta es que el perfil PAN debe soportar IPv4 e IPv6. Los otros Protocolos pueden estar o no habilitados.

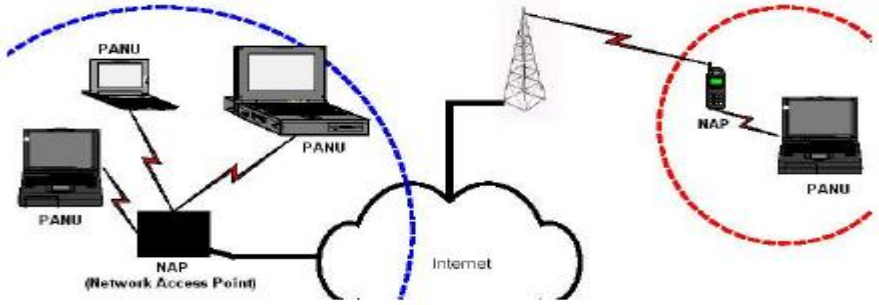
La segunda consideración que debemos tomar es que en una red generalizada, la trayectoria del tráfico originado desde un dispositivo hacia otro puede estar conformada por uno o varios medios de transporte, por ejemplo, Bluetooth, ethernet, etc.

Son tres escenarios propuestos para el perfil PAN**:** Puntos de acceso a una red *(Network Access Points)***,** Grupo de red Ad-Hoc *(Group Ad-Hoc Networks)* y PANU-PANU *(PAN User)***.** Cada uno de estos escenarios define el funcionamiento y el servicio que deben asumir los dispositivos involucrados en una de estas arquitecturas.

2.4.2 Puntos de acceso a una red (NAP)

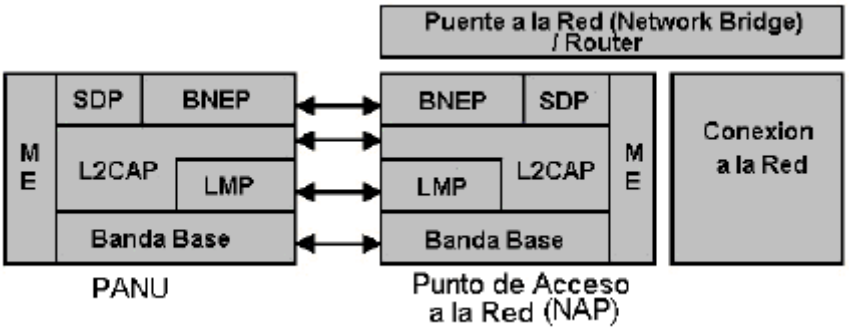
Un punto de acceso a una red **(NAP)** corresponde a una unidad que contiene uno o más dispositivos Bluetooth y actúa como puente, *proxy* o enrutador, entre una red Bluetooth y otro tipo de tecnología de red (*ethernet*, GSM, ISDN, h*ome* PNA, cable *módem* y celular).

Figura 24. Puntos de acceso a la red.



Para la Fase I del perfil PAN, el dispositivo que soporta el servicio **NAP** *(Network Access Point)* debe cumplir con las características de un Puente ethernet para soportar de esta manera los servicios de red. El dispositivo NAP distribuye los paquetes ethernet entre los dispositivos Bluetooth conectados o PAN *Users* (PANU). Los NAP pueden requerir características adicionales en los casos en que el puente sea hacia otro tipo de redes, por ejemplo GPRS. La figura 23 muestra la interacción de las capas de protocolo del modelo Bluetooth para el rol NAP.

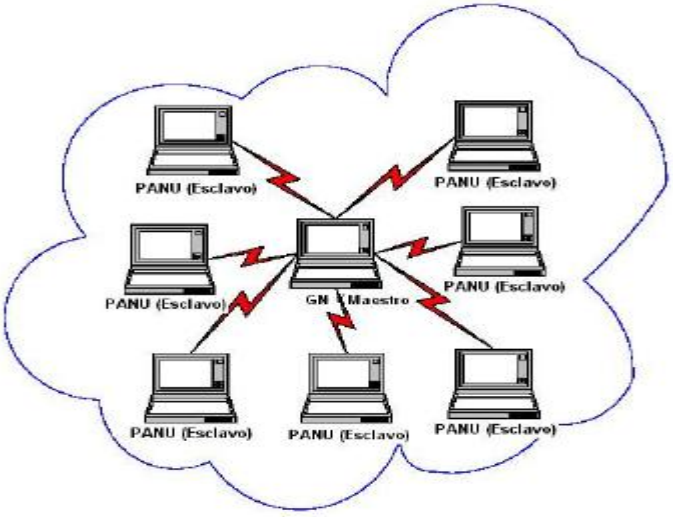
Figura 25. Rol NAP



2.4.3 Grupo de red Ad-Hoc

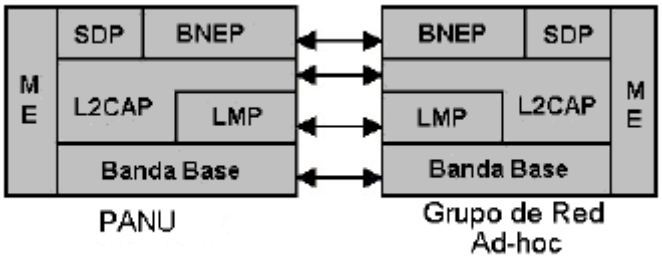
El Perfil PAN, especifica el escenario para una red personal Ad-Hoc el cual consiste en una simple P*iconet* con conexiones entre dos o más dispositivos Bluetooth. Un maestro y un máximo de siete esclavos conforman esta red. El límite de siete esclavos se debe al esquema activo de direccionamiento de Bluetooth. La figura 24 es un esquema para una red Ad-Hoc.

Figura 26. Esquema para un grupo de red Ad-Hoc.



Un grupo de red Ad-Hoc se establece para que un conjunto de dispositivos conforme una red temporal e intercambien información. El dispositivo cuyo rol es *GN (Group Ad-Hoc Network)* soporta el servicio GN**.** La figura 25 ilustra a nivel de las capas de protocolo un enlace entre un GN y un PANU.

Figura 27. Estack para un enlace en una red Ad-Hoc.



2.4.4 PANU – PANU

En este escenario se establece una conexión punto a punto entre dos usuarios de PAN (PANU), permitiéndose así una comunicación directa entre ellos. El PANU es el dispositivo Bluetooth que usa los servicios NAP o GN. El PANU asume el rol de cliente de los roles NAP o GN.

2.5 Hardware y productos Bluetooth

Después de comprender la tecnología Bluetooth se procedió a realizar una búsqueda en el mercado, para saber cuales eran los productos más

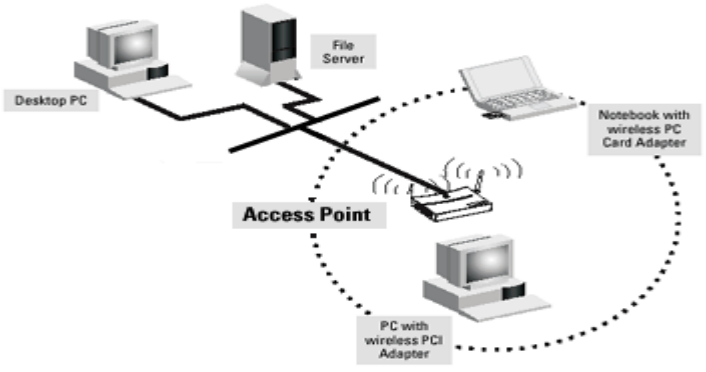
aconsejables y más actualizados hasta la fecha, para poder montar una LAN, se necesitan tres componentes, *Access Point* (Puntos de Acceso), adaptadores para PC de escritorio, *Firewalls*.

2.5.1 *Access Point*

El *Access Point* es un aparato fundamental para la puesta de nuestra LAN, este puede enlazar hasta 7 dispositivos que manejen la tecnología Bluetooth, este hace la función de s*wich* en una red cableada de categoría 5; la manera en que funciona un interruptor es que este registra la dirección del IP de los computadores que se han conectado. Cuando este recibe un mensaje, este solamente lo envía al recibidor originario. Los interruptores cortan tráfico de transmisiones innecesarias y le dejar tener una red de alto desempeño a un bajo costo.

La manera que funciona un *Access Point* se muestra en la figura 26

Figura 28. Funcionamiento de un A*ccess Point*.



Fuente: http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/topologias.htm

Entre los *Access Point* mas aconsejables que existen en el mercado son presentados a continuación:

- **Punto de acceso BlueTake BT300:** el punto de acceso BT300 de BlueTake, es una nueva solución de conectividad inalámbrica multiusuario que le permitirá acceder de forma remota a los contenidos de Internet o los de su una red corporativa. El BT300 le proporciona un acceso fácil y rápido a Internet a aquellos dispositivos remotos equipados con Bluetooth como PCs de escritorio, portátil, PDAs e incluso *SmartPhones*, simplemente conectándolo a su red mediante la conexión tipo RJ-45 a través de un *switch* o un *Hub*, y así poder disfrutar y compartir con hasta 7 usuarios la conexión desde cualquier punto de la casa u oficina, dentro del radio de cobertura del equipo (hasta 100mts.).

Figura 29. BlueTake BT300.

Las especificaciones técnicas se especifican en la tabla I.

Tabla I. Especificaciones técnicas del Bluetake BT300.

Max.Velocidad Transmisión	Hasta 1Mbps
Rango de frecuencia	2,4 - 2,483 Ghz
Potencia de transmisión	Clase 1 (100 mw)
Alcance Máximo	Hasta 100mts en espacio abierto
Sistema de transmisión	FHSS *(Frecuency Hoppong Spread Spectrum)*
Interface	10/100 *Base-T ethernet* port, RS-232 port
Protocolos soportados	*Static* IP, DHCP, PPPoE, Conexión Multipunto
Sistemas operativos soportados	Win 98SE, Me, 2000, XP
Medidas	203x130x40mm
Peso	234 grs

- **Punto de acceso Bluetooth D-*Link* DBT-900AP:** este punto de acceso es una nueva solución para la conexión inalámbrica de múltiples usuarios y dispositivos de una red Bluetooth. Permite a los usuarios móviles usar dispositivos equipados con la tecnología Bluetooth para establecer conexiones inalámbricas con una red local (LAN) y con Internet.

  El punto de acceso DBT-900AP, en conformidad con ethernet Bluetooth v1.1 e IEEE 802.3u, proporciona acceso inalámbrico a los servicios de una LAN ethernet y a los de Internet/Intranet por medio de una serie de dispositivos Bluetooth. Con el DBT-900AP los usuarios móviles pueden conectarse sin esperas cuando se encuentren dentro de un área de red

Bluetooth. Este punto de acceso Bluetooth a LAN soporta dispositivos con tecnología inalámbrica Bluetooth, que incorpora inteligencia integrada para ofrecer seguridad y una fácil instalación. El DBT-900AP soporta la tecnología punta Bluetooth perfil PAN.

El DBT-900AP opera en las numerosas frecuencias de radio de uso público que no han sido asignadas. Ofrece conectividad inalámbrica Bluetooth a los dispositivos con ethernet y a los sistemas TCP/IP de alta velocidad, así como comunicación con redes locales y con Internet sin el coste de operación (p. ej., tarifa telefónica) que supondría pasar a través de una compañía de telefonía móvil.

A través de la interfaz LAN del DBT-900AP los usuarios Bluetooth pueden acceder a servicios de información de una red de área local (LAN), correo electrónico, transferencia de ficheros, navegación web y sincronización. Las impresoras, los escáneres y los dispositivos de almacenamiento que estén conectados a una red ethernet pueden, también, ser compartidos por los usuarios Bluetooth.

Figura 30. Access Point D-*Link* DBT-900AP.

Las especificaciones técnicas se especifican en la Tabla II

Tabla II. Especificaciones técnicas del Access Point D-*Link* DBT-900AP.

Max.Velocidad Transmisión	autosensibles 10/100 Mbps
Rango de frecuencia	2,4 - 2,483 Ghz
Potencia de transmisión	Clase 1 (100 mw)
Alcance Máximo	hasta 100mts en espacio abierto
Sistema de transmisión	FHSS (*Frecuency Hoppong Spread Spectrum*)
Interface	10/100 *Base-T ethernet* port, RS-232 port
Protocolos soportados	DHCP
Sistemas operativos soportados	Win 98SE, Me, 2000, XP

2.5.2 Adaptadores para PC

Es necesario que para el montaje de nuestra LAN, tomar en cuenta el dispositivo que nos va a enlazar a los demás ordenadores entre si, para eso presentamos dos posibles opciones a tomar

- **USB BlueTake BT007si V1.2 Clase 1:** el adaptador para puerto USB Bluetooth de BlueTake BT007Si proporciona a tu PC las capacidades de conexión Bluetooth más avanzadas del momento, gracias a la

compatibilidad con la V1.2 de la norma Bluetooth y al gran número de perfiles soportados como; "*Human Interface Device* (HID)" , "*Advance Audio Distribution Profile* (A2DP)", *and* "*Basic Image Profile* (BIP)" para conexión con teclados y ratones Bluetooth, auriculares Stereo, auriculares telefónicos para VOIP, envío de imágenes desde teléfono móvil, conexión a redes inalámbricas Bluetooth y un largo etc.. Todo ello dentro del radio de alcance máximo de 100 mts. que nos ofrece la potencia de su transmisor.

Su *software* de control y gestión Bluetooth, BlueSoleil de IVT Corp., compatible con SP2 de Windows XP, proporciona un *interface* gráfico sencillo y fácil de utilizar que le permite poder gestionar y controlar sus conexiones Bluetooth con total comodidad.

Figura 31. USB BlueTake BT007si V1.2 clase 1.

Las especificaciones técnicas se muestran en la tabla III

Tabla III. Especificaciones técnicas del USB BlueTake BT007 V1.2 Clase 1

Max. Velocidad Transmisión	1 Mbps
Rango de frecuencia	2,4 ~ 2.483GHz
Potencia de transmisión	Clase 1 (100 mw)
Alcance máximo	Hasta 100mts en espacio abierto
Sistema de transmisión	FHSS (*Frecuency Hoppong Spread Spectrum*)
Interface	Usb v1.1
Energía de la Salida del Rf	DBm 13 (típico)
Sistemas operativos	Win 98SE, Me, 2000, XP
Perfiles soportados	Perfil Del Receptor de cabeza Perfil Del Puerto Serial Dial Encima Del Perfil Del Establecimiento de una red Perfil De la Transferencia De Archivo Perfil Del Dispositivo Del Interfaz Humano Perfil Del Reemplazo Del Cable Del *Hardcopy* Perfil Del Empuje Del Objeto Perfil De la Sincronización El LAN tiene acceso al perfil (solamente disponible en Windows) Perfil del FAX (solamente disponible en Windows) Perfil personal del establecimiento de una red del área (solamente disponible

Perfiles soportados	en Windows) Perfil audio avanzado de la distribución (solamente disponible en Windows) Perfil básico de la proyección de imagen (solamente disponible en Windows)

2.6 Software para el *host*

El *software* para el *host* Bluetooth corresponde a las capas del *stack* de protocolos y utilidades Bluetooth implementadas en software e instaladas en el *host*. Un *host* puede ser cualquier sistema microprocesador programable (PCs, teléfonos celulares, *mouse*, impresoras, teclados, sensores inalámbricos, etc.), capaz de ejecutar las líneas de código correspondientes al *stack* de protocolos para el *host.*

Son muchos los *stacks* de protocolos Bluetooth disponibles para el *host*, implementados en diversos lenguajes de programación y sobre distintas plataformas, siendo también muchas las empresas interesadas en su desarrollo. Independientemente de la plataforma o el lenguaje de programación, estos se basan en de la especificaciones del sistema Bluetooth.

El *host* y el *hardware* Bluetooth se comunican a través del HCI (*Host Controller Interface*) o Interfaz Controladora de *Host*. El *firmware* HCI implementa los Com*and*os HCI para el hardware Bluetooth teniendo acceso a

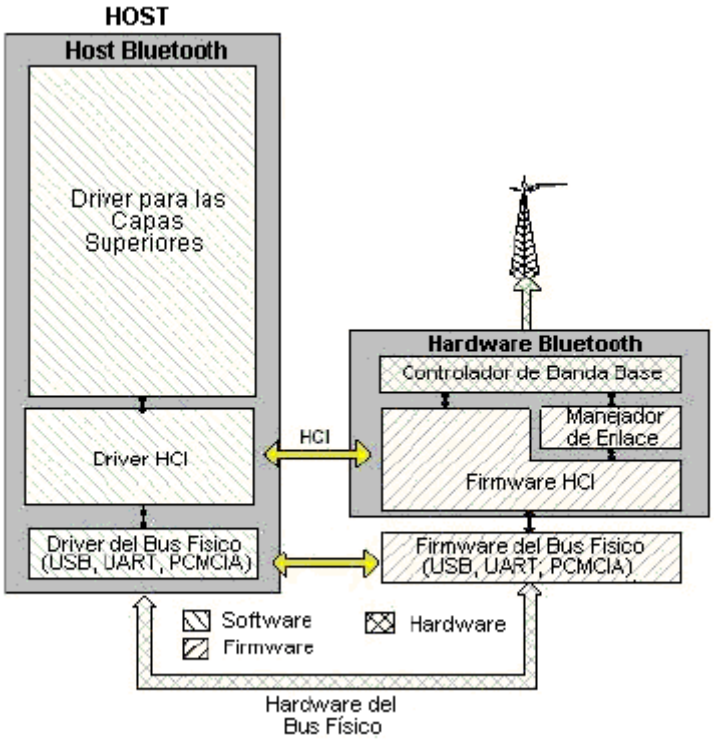
los comandos de b*and*a base, manejador de enlace, registros de estatus del hardware, registros de control y registros de eventos.

Muchas capas pueden existir entre el *driver* HCI ubicado en el *host* y el *firmware* HCI ubicado en el hardware Bluetooth. Estas capas intermedias, se encargan del control y transporte de datos a través de un medio físico (un bus físico ya sea USB, *PC Card*, RS232, u otro), para que se establezca una comunicación transparente entre el *driver* HCI y el *firmware* HCI, permitiendo el intercambio de datos y comandos entre estos dos.

El *host* recibirá notificaciones asíncronas de los eventos HCI independientemente de la capa de control de transporte del *host* que se esté usando. Los eventos HCI son usados para notificar al *host* cuando algo ocurre.

La figura 30 describe esquemáticamente la implementación del *stack* de Protocolos Bluetooth al nivel de *software, firmware* y *hardware*, especificando su ubicación ya sea en el *host* o en el hardware Bluetooth.

Figura 32. Stack de *Protocol*os Bluetooth



3. NIVELES DE SEGURIDAD

La tecnología Bluetooth esta designada para soportar varias conectividades derivado a las características asociadas a su funcionamiento como a través de un método invisible de comunicación ante el ojo Humano, es por esto que nos preguntamos, cuando es cu*and*o debemos determinar si el ambiente es seguro o no?, y nos damos cuenta que cualquiera que cuente con un dispositivo de conexión Bluetooth, puede ser capaz de ingresar a una red personal aun sin que nos enteráramos.

Esto puede ser alarmante por dos razones, la primera, porque la disponibilidad de conexión de varios dispositivos a la vez es limitada, y la segunda, porque se considera la más importante que por ser de un acceso público, nuestra data y nuestros servicios pueden tener problemas, ya que se puede acceder a nuestra data y modificarla o bien maliciosamente transmitir un virus a través de la red interna de la empresa.

Es necesario tomar en cuenta la seguridad que conlleva montar una base de datos en una empresa, para fines comerciales; la importancia que esto representa tanto para seguridad de cada uno de los clientes de la empresa como para la misma, ya que solo personal autorizado por la empresa debe ser capaz de acceder a esta información, tanto a nivel de usuario como a nivel de administrador de la red que se esta montando.

El host es el elemento importante en llevar cada uno de los perfiles de seguridad, que en este caso podría ser un servidor de dominio dedicado específicamente a esa labor, tomando el papel del administrador de la

seguridad, este tendrá como tareas diversas responsabilidades entre las cuales podemos mencionar las siguientes:

a. Configuraciones de seguridad
b. Verificar pines o claves de entrada
c. Verificar los perfiles de seguridad del usuario
d. Dar una respuesta valida y verdadera al dispositivo entrante según sea el pin y el perfil asignado a ese usuario.

La seguridad interna de este administrador de seguridad es configurado por el usuario según sea el software que se este utilizando para la realización del mismo. Como se explicara en el transcurso de este capitulo el mas recomendable nivel de seguridad cuando queremos montar una base de datos es el nivel número 2, ya que con este podemos elegir el tipo de seguridad y los accesos a los cuales podrán ingresar los usuarios del sistema.

En nuestro caso al querer montar una red inalámbrica basándonos en la tecnología Bluetooth, para poder acceder a ella debemos tomar en cuenta ciertas especificaciones como son: los modos de detección, los modos de conexión y los modos de apareamiento en donde estos se rigen en tres niveles de seguridad que regirán nuestra red, los cuales son presentados a continuación.

3.1 Modos de detección

Cuando queremos realizar una detección de un dispositivo que estemos utilizando para conectar una PC a la red Bluetooth este deberá estar

en el modo de “no detección” o en modo de “detección”, el dispositivo solo debe de estar en un modo a la vez.

Cabe hacer la aclaración que cuando un dispositivo esta en modo de “no detección” este no responderá a un descubrimiento realizado por el *Access Point*.

Cuando un dispositivo fue colocado en modo de “detección” y en nuestra red haya una respuesta de descubrimiento limitada por parte de nuestro *Access Point*, aunque nuestro dispositivo este en modo de descubrimiento este no encontrara respuesta derivado de las limitantes con que cuenta la señal de descubrimiento.

3.1.1 Modo “no detección”

Esto ocurre c*uand*o el dispositivo esta en modo “no detección” este nunca podrá entrar al estado de *INQUIRÍ _ RESPONSE*, este no es mas que un enlace efectuado entre el *Access Point* y el dispositivo.

3.1.2 Modo de detección limitada

El modo de detección limitada estaría usado por dispositivos que necesiten ser detectados por un periodo de tiempo, con determinadas condiciones en un evento específico. El propósito de este descubrimiento es que tenga un acceso limitado.

Un dispositivo en este modo no estaría por mas tiempo que el que se le especifico.

3.1.3 Modo de descubrimiento general

Este modo de detección debería de ser usado en dispositivos que necesiten estar en modo de descubrimiento constante sin ningún tipo de restricción de tiempo. El propósito de este descubrimiento es obtener una respuesta cuando se hace un descubrimiento general.

Las condiciones para que este tipo de descubrimiento se cumplan es que el dispositivo debería de entrar en el estado *INQUIRY_SCAN*, por lo menos mas de una vez en 2.56 segundos que es el tiempo que se estipula entre cada uno de las respuestas del *INQUIRY_SCAN.*

3.2 Modos de conexión

Cuando nos referimos a modo de *"paging"*, nos referimos al procedimiento que utilizamos para establecer un enlace físico de conexiones asíncronas, en un nivel de banda base, el cual consiste en la acción de iniciar y examinar la respuesta del dispositivo que se quiere conectar. Esto nos da a entender que cuando un dispositivo esta en el modo "No-Conexión" este no responderá al "*paging*", y cu*and*o este en el modo "Conexión" este si responderá al modo de "*paging"*.

3.2.1 Modo “no-conexión”

Este modo hace referencia que cuando el dispositivo esta en modo “no-conexión” este nunca podrá ingresar al modo *PAGE_SCAN*, que es el estado de banda base en donde el dispositivo esta listo para entrar al modo “*paging*”.

3.2.2 Modo “conexión”

Cuando un dispositivo esta en el modo de “Conexión” este esta entrando constantemente al estado de *PAGE_SCAN.*

3.3 Modos de apareamiento

Referente al modo “*pairing*” o modo de apareamiento, el dispositivo Bluetooth deberá estar en modo “*Pairable”* o *“Non-Pairable*”. En el modo *“Pairable”* el dispositivo Bluetooth acepta el intercambio de una estructura iniciada por un dispositivo remoto, y en el modo *“Non-Pairable”* el dispositivo no hace nada.

3.3.1 Modo de “no-apareamiento”

Cuando un dispositivo esta en el modo “*no-pairing”* este deberá responder al procedimiento del *“Link Manager Protocol”* en estado de no aceptar hasta que se cambie de estado.

3.3.2 Modo de “apareamiento”

Cuando un dispositivo esta en el modo *“pairing”* este deberá responder al procedimiento del *“Link Manager Protocol”* en estado de aceptar hasta que se cambie de estado.

3.4 Aspectos o niveles de seguridad

Bluetooth tiene tienes varios niveles de seguridad. Cada dispositivo puede operar en un solo modo a la vez. Cada uno de estos niveles debe pasar por un proceso de autenticación a excepción del nivel 1 de seguridad.

3.4.1 Autenticación

El proceso de autenticación describe como el procedimiento del *LMP-conectión* y el *LMP-Pairing,* son usados cu*and*o una autenticación es iniciada

por un dispositivo dependiendo de las distintas combinaciones que se puedan tener o mas bien dicho, dependiendo de en que modo se encuentren los dos modos tanto el de apareamiento como el conexión. Cabe mencionar que por este proceso solo se ejecuta en los niveles 2 y 3 de seguridad.

Este también es un procedimiento en el cual es una forma de esquema "*challenge-response*". Dos dispositivos interactúan entre si para que se verifiquen entre ellos. Este protocolo responde únicamente si los dispositivos dan como valida y certificada si estos se intercambian la clave entre ellos.

Para mantener la seguridad a nivel de enlace, los parámetros utilizados son:

a) La dirección del dispositivo Bluetooth (*BD_ADDR*).

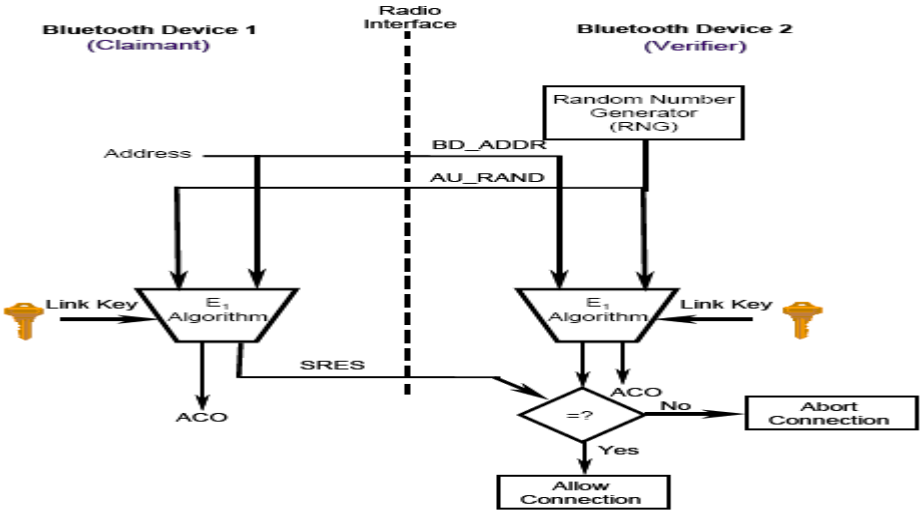
b) La clave de usuario privado autenticación.

c) La clave de usuario privado de cifrado.

d) Un número aleatorio (*RAND*).

La figura 31 nos verifica el proceso de autenticación.

Figura 33. Proceso de autenticación.



Fuente: Les Owens. Wireless Security. Special Publication Section 4-9

A continuación explicaremos cada uno de los procesos:

a. El transmisor del dispositivo 1 llamado "*claimant*", es el dispositivo que esta queriendo ingresar a la red este trasmite sus 48 bits de direccionamiento para que pueda ser verificado.

b. El segundo dispositivo que en este caso seria el receptor también llamado "*verifier*", genera y transmite 128 bits aleatorios hacia el "*claimant"*.

c. El "*verifier*" usa el algoritmo E_1, el cual es el que verifica el modo de conexión y de apareamiento y así poder dar la una respuesta de autenticación *utilizando* la dirección, la clave, y verificar lo que se esta ingresando. El "*claimant*" ejecuta la misma operación.

d. El “*claimant*” regresa la respuesta de señal procesada (SRES), al “*verifier*”.

e. El “*verifier*” compara la SRES del “*claimant*” con la respuesta procesada por el.

f. Si los 32 bits de respuesta SRES son iguales, el “*verifier*” continuara con el proceso de conexión.

Si la autenticación falla, este entrará en un tiempo de espera hasta que otra vez el proceso vuelva a activarse. Este intervalo de tiempo crece exponencialmente para prevenir que alguien no deseado pueda intentar acceder mediante el método de prueba y error ingresando diferentes claves. Sin embargo, es importante tomar en cuenta que esto no provee una seguridad enorme ante personas que con el equipo adecuado puedan rastrear la clave con algún método u equipo electrónico.

En el siguiente capítulo se estudiara detenidamente cada uno de los procesos antes mencionados en los cuales se basa la autenticación.

3.4.2 Nivel de seguridad 1

Es también llamado modo no seguro, porque el dispositivo no inicia ningún proceso de seguridad, en este modo inseguro, la funcionalidad de la seguridad, cu*and*o decimos esto nos referimos al modo de autenticación y encriptación es completamente salteado por parte del dispositivo.

En efecto cuando el dispositivo se encuentra en este modo se dice que esta en modo “promiscuos”, que el cual quiere decir que cuando se encuentra bajo este modo cualquier dispositivo puede conectarse a el. Este modo de seguridad es proveído a dispositivos con aplicaciones en la cual la seguridad no es requerida.

3.4.3 Nivel de seguridad 2

También llamado Seguridad Impuesta a Nivel de Servicio; este proceso de seguridad se inicia después de haber logrado un establecimiento con el nivel “*Logical Link Control and Adaptation* Protocol” (L2CAP), L2CAP reside en el enlace de datos y provee una conexión orientada a los servicios de las capas altas. Con este modo de seguridad, la seguridad principal, controla los accesos y servicios de cada uno de los dispositivos que estén conectados. Este tipo de seguridad esta realizando un testeo cada cierto tiempo para verificar el tipo de acceso que se tiene así como también las interfaces que se tienen con otros protocolos y con los demás usuarios. Variando las políticas de seguridad y los niveles verdaderos de restricción podemos definir las aplicaciones y los accesos que podemos controlar en un dispositivo de una forma paralela. De esta manera podemos acceder a un servicio sin afectar las restricciones de otro dispositivo. Obviamente en este nivel de seguridad, la autorización es introducida, en términos generales si un dispositivo X se da o no todo el acceso a un servicio Y.

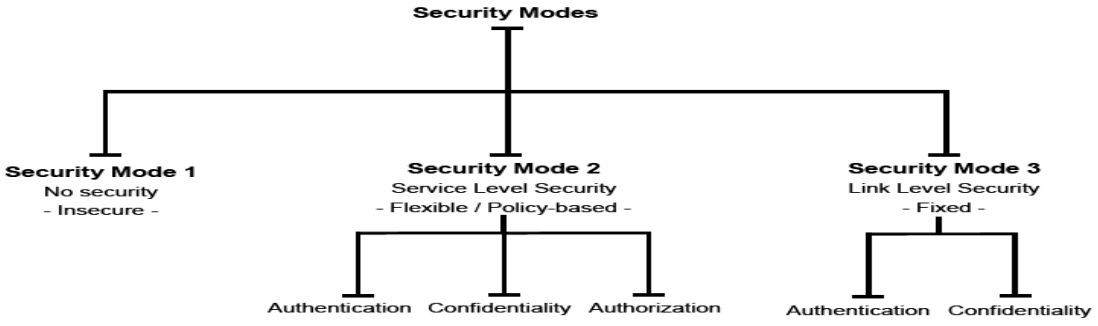
3.4.4 Nivel de seguridad 3

Llamado también, Seguridad Impuesta a Nivel de Enlace, este inicia el proceso de seguridad antes de que el canal haya sido establecido. Este es un mecanismo de seguridad y este no esta enterado de cualquier aplicación de capas de seguridad ya existentes. Este modo de seguridad soporta la autenticación y la encriptación, que veremos en el próximo capitulo.

Estas especificaciones o procedimientos de seguridad están basados en una clave secreta que es compartida por un par de dispositivos. Para generar esta clave, el proceso de apareamiento es usado cuando dos dispositivos se intentan comunicar por primera vez. La diferencia de este nivel de seguridad con el anterior es que este nivel es fijo, osease que la seguridad impuesta no es variable como si lo podemos hacer en el nivel de seguridad número 2.

A continuación la figura 32 nos demuestra en un diagrama como están basados cada uno de los niveles anteriormente descritos.

Figura 34. Fisonomía de modos de Seguridad Bluetooth.



Fuente: Wireless Security, Special Publication, Les Owens, Section 4-8

Como se mencionó al inicio del capítulo, para los fines personales de la empresa debemos escoger entre un nivel 2 y un nivel 3, siendo el más aconsejable el nivel dos ya que podemos restringir el acceso a través de la asignación de perfiles a cada uno de los usuarios que deseen ingresar al sistema. En el siguiente capitulo analizaremos cada una de estas políticas que rigen los niveles 2 y 3.

4. MODOS DE ACCESO A LA RED

En si, en el momento en que nosotros queremos acceder a la red inalámbrica, como se describió en el capitulo anterior nos damos cuenta que hay tres maneras o modos de seguridad para poder ingresar a la red, que son los niveles de seguridad 1, 2 y 3 respectivamente, si hacemos un recordatorio y basándonos en las políticas de seguridad que rigen cada uno de estos modos, vemos que en el modo o nivel de seguridad de categoría dos, involucramos tres tipos de aspectos, la Autenticación, la Encriptación y la Autorización; de la misma manera nos damos cuenta que el nivel de seguridad tipo 3 solo requiere lo que es la Autorización y la Encriptación y el nivel numero 1 no requiere ninguna de estas dos formas.

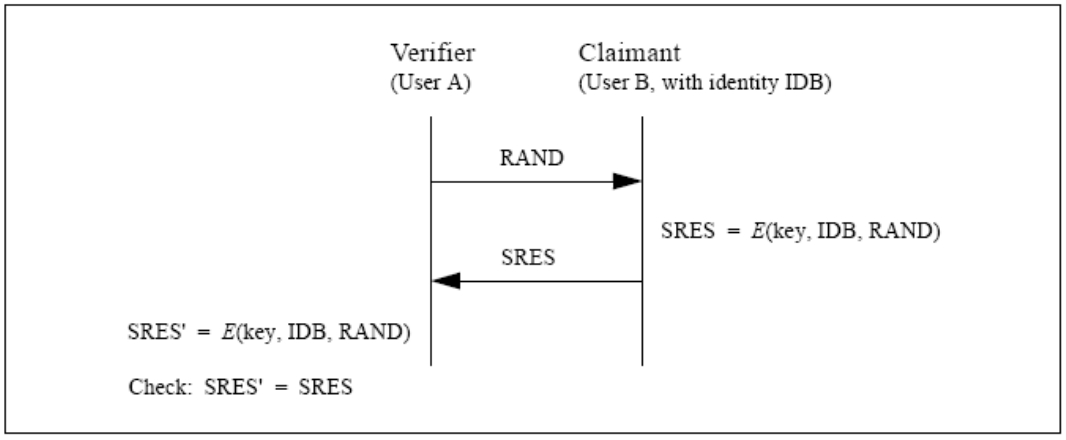
A continuación detallamos cada una de ellas.

4.1 Autenticación

El método de autenticación esta basado en el esquema de especificaciones de banda base el cual trata la manera de verificar una llave de enlace entre 2 protocolos proporcionados entre un dispositivo y otro y ver si esta corresponde a cada uno de los dos para poder realizar la comunicación, la manera en que se realiza esto es que el dispositivo 1 envía un bit verificador de paridad y luego un código aleatorio en el cual va incluida una llave de enlace que al momento de llegar al dispositivo dos este hace la respectiva verificación y determina si la clave es la misma o no. Este método esta hecho básicamente para la prevención del ataque de reflexión, este tipo de ataque no tiene forma

alguna y consiste básicamente si un dispositivo externo puede simular un código aleatorio pero si no posee la llave de enlace no podrá conectarse al dispositivo, aunque este tipo de ataque es considerado altamente destructivo.

Figura 35. Respuesta para dos sistemas actu*and*o bajo este método de autenticación.



Fuente: Specification of the Bluetooth System, Version 1.1 Página 169

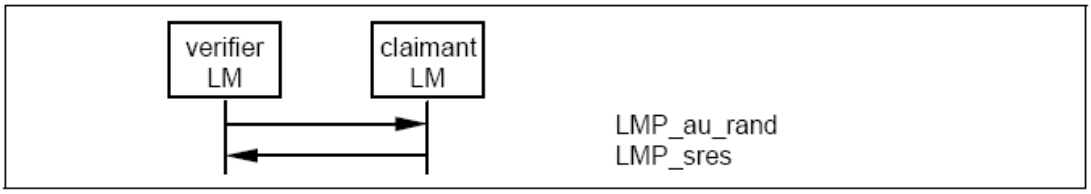
Este procedimiento ya fue explicado en el capitulo anterior y es por ello que no nos vamos a detener en ello para continuar con el proceso de autenticación.

Después de pasar por el proceso anterior pueden suceder dos opciones, cuando el c*laimant* contiene la llave de enlace y cuando este no la tenga.

4.1.1 Cu*and*o el *claimant* contiene la llave de enlace

Cuando el *claimant* contenga la llave de enlace con el verificador (dispositivo o usuario “a”) este enviara una respuesta al *claimant*, conteniendo un tipo de respuesta satisfactoria, si esta respuesta no fuera de carácter satisfactorio se interrumpe la conexión y fuerza al usuario a intentar de nuevo.

Figura 36. Tipo de autenticación cu*and*o la llave de enlace es correcta.



.

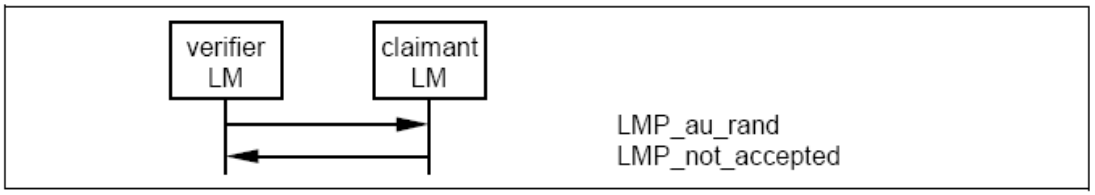
Fuente: Specification of the Bluetooth System, Version 1.1 Página 194

Cabe Mencionar que luego de que el *claimant* recibe una respuesta satisfactoria, este vuelve a repetir el proceso como una segunda confirmación antes de empezar el proceso de autenticación. Si se diera el caso de que la respuesta y la segunda confirmación chocan entre si, se forma una colisión y fuerza a los dispositivos a comenzar de nuevo este proceso.

4.1.2 Cu*and*o el *claimant* no contiene la llave de enlace

Cuando el *claimant* no contiene asociada una llave de enlace o esta es errónea el verificador automáticamente enviara una señal de respuesta denegando el acceso.

Figura 37. Tipo de autenticación cu*and*o la llave de enlace no es correcta.



Fuente: Specification of the Bluetooth System, Version 1.1 Página 194.

4.1.3 Repetidos intentos

Cuando un proceso de autenticación falla es necesario tomar un relativo tiempo de espera para poder intentar nuevamente el proceso de autenticación ya que si no el dispositivo se bloqueara por un tiempo no muy prolongado, esto se hace con la finalidad de proteger la seguridad integra de la red ante posibles tipos de ataques por estar intentando conectarse a la misma.

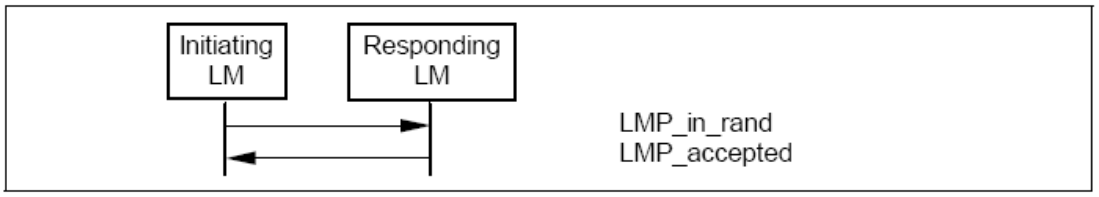
4.1.4 Modo *pairing*

Cuando dos dispositivos tienen una llave de enlace en común y esta llave es inicializada basándose en el código aleatorio en donde se envía la llave inicial. Esta llave es creada en los dispositivos, y finalmente se logra una comunicación en común; el proceso del p*airing* comienza cuando un dispositivo comienza a enviar la instrucción *LMP_au_rand*. Este dispositivo es llamado "*Initiating LM"* o *"Initiator"* y el otro dispositivo es llamado "*responding LM*" o "responder".

4.1.5 Cu*and*o el "responder" acepta el apareamiento o "*pairing*"

El "*initiator*" envía la instrucción *LMP_au_rand*; y se activa cu*and*o recibe la respuesta *LMP_accepted*. El dispositivo que inicia la secuencia calcula la llave inicial basándose en la dirección que le proporciona el "responder" y el procedimiento continua con la creación de la llave de enlace.

Figura 38. Diagrama cuando el *pairing* es aceptado.



Fuente: Specification of the Bluetooth System, Version 1.1 Página 196.

4.1.6 Cu*and*o el "responder" no acepta el apareamiento o "pairing"

Si el "responder" rechaza el apareamiento este envía una instrucción *LMP_Not_accepted* justificando el rechazo en base a que no era correcta la instrucción enviada anteriormente en *LMP_au_rand.*

Figura 39. Diagrama cu*and*o el *pairing* no es aceptado.

Fuente: CORE, Specification of the Bluetooth System, Version 1.1 Página 197.

4.1.7 Creación de la llave de enlace

Cuando la llave inicial es calculada por el código aleatorio en la unidad que inicia el proceso se procede a crear la llave de enlace. Esta llave es la que se usara para la autenticación de dos dispositivos que van a estar en constante intercomunicación entre ellos, hasta que esta llave sea cambiada. La llave creada en el proceso de apareamiento será aplicada bajo las siguientes reglas

- Si un dispositivo inicial envía una llave, y otros dispositivos envían otro conjunto de llaves, la única llave en común será la llave de enlace, que será única.

- Si solo existe un dispositivo, la llave que este envíe será considerada como la llave maestra.

- Si existen varios dispositivos y envían un conjunto de llaves, entonces se generara una clave en común entre ellos que será considerada la maestra para todos.

Figura 40. Diagrama de la creación de una llave de enlace.

Fuente: CORE, Specification of the Bluetooth System, Version 1.1 Página 197.

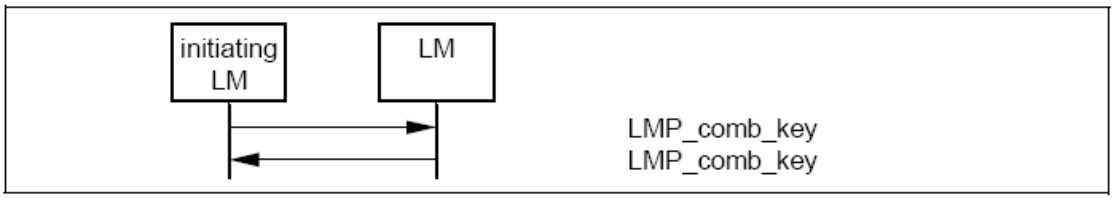
4.1.8 Repetidos intentos

Después de haber creado la autenticación, la llave de enlace falla derivado de varias causas, como se explicó anteriormente, los dispositivos se bloquean por un tiempo no muy largo, esto se hace con la finalidad de proteger la seguridad integra de la red ante posibles tipos de ataques por estar intentando conectarse a la misma.

4.1.9 Cambio de una llave maestra

Si la llave de enlace es derivada o proveniente de varias llaves de enlace brindadas por varios dispositivos la llave de enlace puede ser cambiada para generar una llave maestra que será común para cada uno de los dispositivos. El procedimiento será que cada una de las unidades en cuestión; iran siendo reconocidas una por una según el orden en el cual estas estén cambiando su llave de enlace. El contenido de este conjunto de llaves va a estar protegido con la llave que tendrán en común.

Figura 41. Diagrama del cambio satisfactorio de una llave maestra.



Fuente: CORE. Specification of the Bluetooth System, Version 1.1 Página 198.

Si el cambio de llave maestra en cada uno de los dispositivos es satisfactorio la nueva llave maestra es la que se establecerá quedando relegada la llave maestra contenida por cada uno de los dispositivos que conformaban el conjunto de llaves enviadas. Esta nueva llave será utilizada por estos dispositivos hasta que la llave maestra sea cambiada por cuestiones de seguridad; esta nueva llave será común para todos los dispositivos.

4.1.10 Cambio de una llave común

Una llave común puede ser considerada una llave de enlace temporal, ya que esta puede ser cambiada de una manera temporal, y este tipo de cambio es únicamente valido para una sesión. Haciendo este tipo de cambio es necesario que una llave de enlace en una *Piconet* soporte el proceso de encriptación del cual hablaremos mas adelante.

4.1.11 Hacer de una llave común una llave semi-permanente

Cuando un dispositivo maestro, osease el dispositivo que es considerado el primario, o el que empieza a intentar conectarse, empieza con la creación de una llave maestra, este genera un código aleatorio "*rand*" y envía al dispositivo esclavo la instrucción *LMP_temp_rand*, después de haber cambiado una llave en común por esta llave de enlace maestra, puede considerarse una llave de enlace semi-permanente; si el proceso de encriptación es usado en este enlace, y luego de haberse completado este proceso tendrá una señal de alto para luego comenzar con la encriptación llamada por el dispositivo maestro en este caso. El proceso de encriptación será tocado en el siguiente inciso.

Figura 42. Diagrama del cambio de una llave de enlace a una llave de enlace tipo semi-permanente.

Fuente: CORE, Specification of the Bluetooth System, Version 1.1 Página 199.

4.2 Encriptación

Cuando el proceso de autenticación haya sido satisfactorio se debe de usar la encriptación, como lo hemos dejado señalado este proceso de autenticación se utiliza solo cuando se ejecutan ya sea el nivel de seguridad número dos o número tres.

Si en algún dado caso en nuestra *Piconet* existiere un maestro y varios esclavos, en este caso se deben de usar los mismos parámetros de encriptación con la llave maestra que se genere con cada uno de los dispositivos que formen un conjunto y estos a la vez generen una llave de enlace maestra en común para ese grupo.

La encriptación no es más que crear una mascara para que los paquetes de información no puedan ser descifrados sino es por algún dispositivo que este manejando este mismo código de encriptación que para este caso debe ser un dispositivo que este manejando la misma lógica Bluetooth.

La siguiente figura muestra la tabla de Unidades de Protocolos de Datos se presenta a continuación mostrando cual es el contenido que lleva cada instrucción,

Figura 43. Las PDU (Unidades de Protocolos de Datos), y su contenido que puede tener en la encriptación.

M/O	PDU	Contents
O	LMP_encryption_mode_req	encryption mode
O	LMP_encryption_key_size_req	key size
O	LMP_start_encryption_req	random number
O	LMP_stop_encryption_req	-

Fuente: Specification of the Bluetooth System, Version 1.1 Página 201.

4.2.1 Modo de encriptación

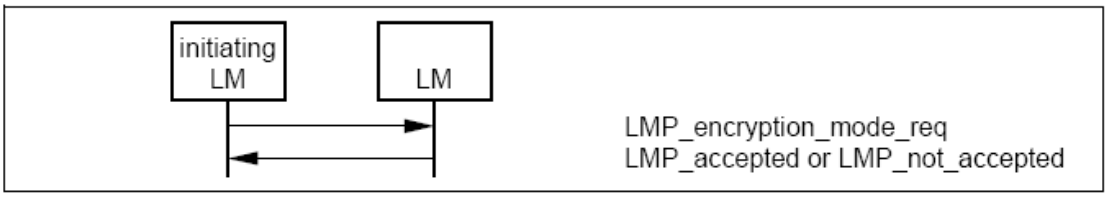
Lo que se realiza primero es que el Maestro y el esclavo deben estar coordinados si usaran o no la encriptación y si la encriptación solo será aplicada en paquetes con destino Punto a Punto o si la encriptación será aplicada al inicio de los paquetes punto a punto. Si el maestro y el esclavo están coordinados para usar el modo de encriptación el maestro continúa obteniendo con más detalle toda la información de la encriptación.

La iniciación de los dispositivos LM finaliza la transmisión del paquete ACL (*Asynchronous Connection-Less*) con la información proveniente del L2CAP, cuando para la transmisión del L2CAP, se envía la instrucción *LMP_encryption_mode_req*. Si el cambio en el modo de encriptación es

aceptado entonces el otro dispositivo finaliza la transmisión del paquete ACL (*Asynchronous Connection-Less*) con la información proveniente del L2CAP, cuando para la transmisión del L2CAP, se responde la instrucción *LMP_accepted*.

La transmisión L2CAP es re-habilitada cu*and*o la encriptación o desencriptacion esta completada, esto ocurre al termino de una secuencia de tipo 14, 15 o 16, estas secuencias se explicaran a continuación en adición a la secuencia 13.

Figura 44. Negociación que existe entre los dispositivos LM para el modo de encriptación.



Fuente: Specification of the Bluetooth System, Version 1.1 Página 201

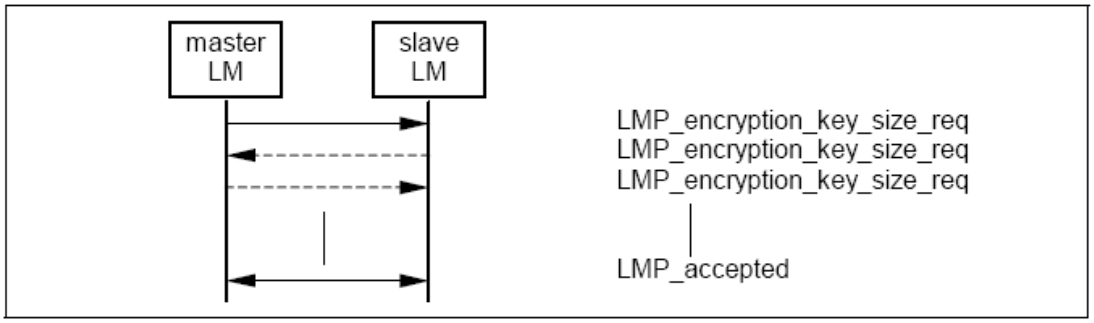
4.2.2 Tamaño de la llave de encriptación

El siguiente paso es determinar el ancho de la llave de encriptación, para poder realizar esto el maestro envía una instrucción *LMP_encriptyon_key_size_req* incluyendo en esta un tamaño de llave sugerida de un tamaño de longitud L siempre y cuando la unidad esclavo soporte este tamaño de longitud, si esto se cumple el esclavo enviara una instrucción de LMP_accepted y este usara el tamaño de la llave sugerida por el maestro.

Si ambas condiciones de envío y el tamaño de la llave sugerida por parte del maestro, entonces el esclavo envía de regreso la instrucción *LMP_encriptyon_key_size_req* sugiriendo el tamaño de la misma. El largo del valor sugerido por el esclavo debe ser menor al valor sugerido por el maestro anteriormente para que entonces la condición de aceptación se pueda cumplir, al haber enviado esta sugerencia el esclavo el maestro hace una evaluación de la misma y determina si cumple esta condición y envía la instrucción de respuesta *LMP_accepted.*

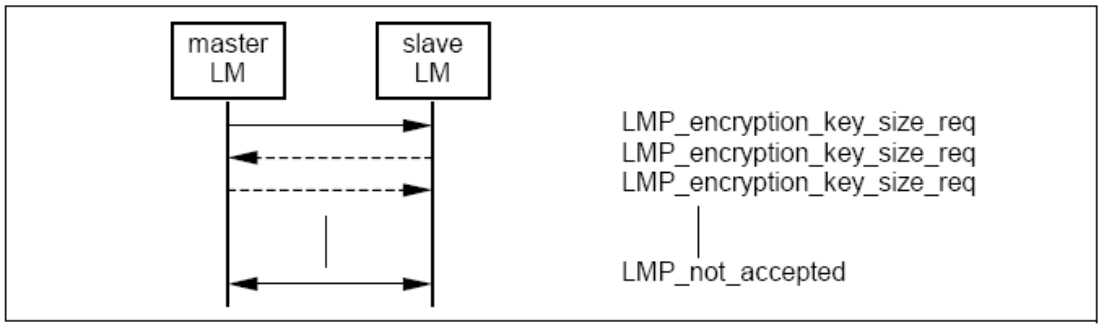
De ser necesario este tipo de procedimiento es repetido hasta que el tamaño de la llave sea aceptado por los dos. Después de haber encontrado un tamaño en la llave común para ambos empieza el proceso de encriptación. Si por algún motivo después de seguir por varios intentos y no se logra un acuerdo entre maestro y esclavo cada unidad se pone en estado de bloque por un momento basándose en la razón de que los valores de los parámetros no son soportados entre si y estas no lograran una comunicación.

Figura 45. Negociación que existe entre los dispositivos LM para el tamaño de la llave de encriptación.



Fuente: Specification of the Bluetooth System, Version 1.1 Página 202

Figura 46. Secuencia 14: Negociación fallida entre los dispositivos LM para el tamaño de la llave de encriptación.



Fuente: Specification of the Bluetooth System, Version 1.1 Página 202

4.2.3 Comenzando la encriptación

Finalmente el proceso de encriptación es iniciado, a esto se le conoce como la secuencia 15, el maestro tiene en la salida y genera un número aleatorio para la clave maestra que va a ser la llave común. Como se dijo el numero aleatorio debe ser el mismo para todos los esclavos si es que existiesen mas de uno y si estos van a iniciar y soportar el proceso de encriptación, entonces el dispositivo maestro envía la instrucción *LMP_star_encriptyon_req*, y en esta incluye el numero aleatorio generado, el esclavo calcula su llave y si esta es correcta envía la instrucción de *LMP_accepted* y comienza el proceso de encriptación.

Figura 47. Secuencia 15: Comienzo de la encriptación.

Fuente: Specification of the Bluetooth System, Version 1.1 Página 203

El proceso de Encriptación consiste en tres etapas:

- El maestro debe ser configurado para transmitir paquetes no encriptados, pero para recibir paquetes encriptados.

- El esclavo es configurado para transmitir y recibir paquetes encriptados.

- El maestro es configurado para transmitir y recibir paquetes encriptados.

Entre el paso 1 y el Paso 2, la transmisión maestro-esclavo es posible. Esto es cuando la instrucción *LMP_start_encriptyon* es transmitida.

El paso 2 es ejecutado cuando el esclavo recibe ese mensaje. Entre el paso 2 y el paso 3, la transmisión esclavo-maestro es posible. Esto es

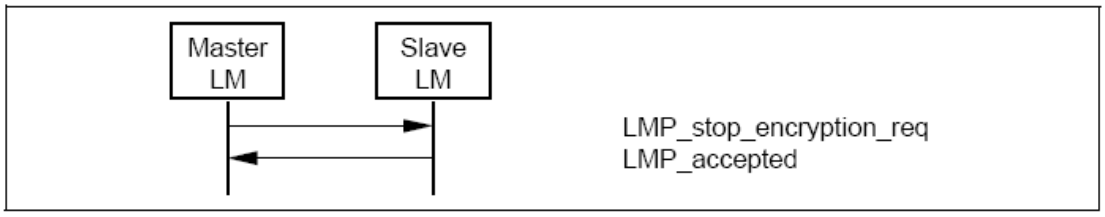
cuando la instrucción *LMP_accepted* es transmitida. El paso 3 es ejecutado cu*and*o el maestro recibe este mensaje.

4.2.4 Terminando la Encriptación

A esto se le conoce como la secuencia 16, si una de las unidades, ya sea el maestro o el esclavo desea terminar el proceso de la encriptación entonces este debe enviar la instrucción *LMP_star_encriptyon_req* con el parámetro de encriptación en modo igual a 0, que significa "*no encriptyon*", entonces el otro dispositivo responderá con la instrucción *LMP_accepted o LMP_not_acepted* como fue descrito en el apartado 4.2.1.

Si la instrucción es *LMP_accepted* entonces el proceso de encriptación se para por el maestro ya que envía la instrucción y el esclavo responde con la instrucción *LMP_accepted.*

Figura 48. Secuencia 16: Finalizando la encriptación.



Fuente: Specification of the Bluetooth System, Version 1.1 Página 203

Para parar la encriptación, es similar el procedimiento que hay que realizar, con el procedimiento de la inicialización de la encriptación, este se presenta a continuación en tres etapas:

- El maestro es configurado para transmitir paquetes encriptados, pero recibe paquetes no encriptados.

- El esclavo es configurado para transmitir y recibir paquetes no encriptados.

- El maestro es configurado para transmitir y recibir paquetes no encriptados.

Entre el paso 1 y 2, la transmisión del maestro al esclavo, es posible. Esto es cuando la instrucción *LMP_stop_encriptyon* es transmitida. El paso 2 es ejecutado cuando el esclavo recibe este mensaje. Entre el paso 2 y 3, la transmisión del esclavo al maestro es posible. Esto es cuando la instrucción *LMP_accepted* es transmitida. El paso 3 es ejecutado cuando el maestro recibe este mensaje.

4.2.5 Cambio en el modo de encriptación, llave o el número aleatorio

Si la llave de encriptación ó el numero aleatorio de encriptación necesitan ser cambiados, o si el modo de encriptación necesita ser cambiado, lo que se debe de hacer primero es parar el proceso de encriptación y entonces reiniciar con los nuevos parámetros, de acuerdo a lo anteriormente desarrollado en el modo de encriptación.

4.3 Autorización

En adición a los tres niveles de seguridad, la tecnología Bluetooth contiene dos niveles de verdad y tres niveles de servicio de seguridad. Los niveles de verdad como se menciono anteriormente son dos, el denominado "verdadero" y el denominado "no verdadero". El nivel "verdadero" es aquel que después de haber tenido exitosamente una conexión entre dos dispositivos mediante los procedimientos anteriores previamente explicados, estos tienen acceso completo entre ellos. El modo "no verdadero" es aquel con el cual los dispositivos después de haber tenido una conexión tienen un acceso limitado entre ellos.

A nivel de servicio, se han definido 3 niveles, los cuales son independientes de que nivel se seguridad se va a utilizar, y son tomados en cuenta después de haber definido cual es el mas idóneo a usar en ese momento.

Estos niveles de seguridad de servicio están definidos de la siguiente manera:

- **Nivel de Servicio 1:** Este servicio se utiliza en base al tipo de conexión con autenticación y autorización. El acceso es automático cuando los dos dispositivos están en modo "verdadero". Los dispositivos que están en modo "no verdadero" deben tener una autorización manual.

- **Nivel de Servicio 2:** Este servicio solo se utiliza en base al tipo de conexión requiriendo autenticación solamente. El tipo de acceso de

este tipo ocurre únicamente después de haber ocurrido el proceso de autenticación.

- **Nivel de Servicio 3:** Este tipo se utiliza en base a cualquier tipo de conexión. El acceso esta garantizado para cualquier dispositivo.

Asociados con estos niveles la seguridad de cada uno de estos dispositivos es restringido dependiendo el acceso al servicio que se requiera, cada vez que se requiera una autenticación, el proceso de autorización es requerido, de igual manera cuando es requerida la autenticación y la encriptación dependiendo que tipo de acceso se requiera, la autorización juega un papel importante antes de que se ejecuten los dos procesos

La arquitectura Bluetooth esta por definir políticas de seguridad de las cuales en las cuales busca que las conexiones entre dispositivos sean seguras en cualquier camino, aun cuando los dispositivos hayan tenido una conexión tipo nivel 1.

Es importante entender que el protocolo Bluetooth, puede autenticar a nivel de dispositivos no a nivel de usuario. Esto no quiere decir que no pueda conectar dispositivos controlados desde una interfaz de usuario

5. DISEÑO DE LA RED

Después de tener claro el funcionamiento de una red implementando tecnología Bluetooth, se procede a diseñar qué tipo de topología de red vamos a utilizar antes de implementarla.

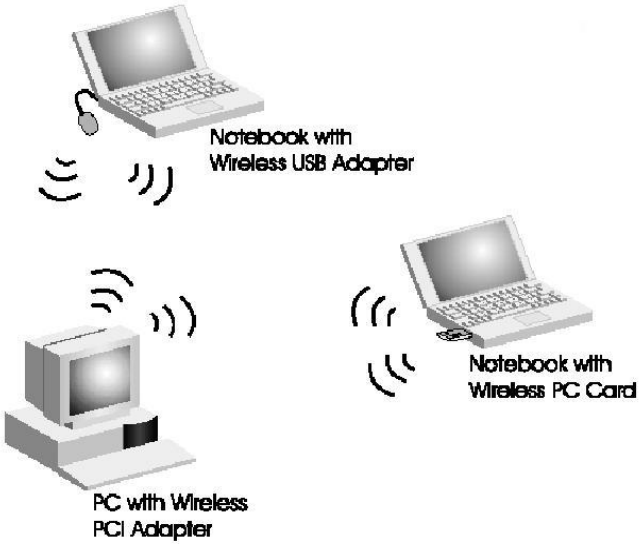
Topologías de red

Las redes LAN inalámbricas se construyen utilizando dos topologías básicas, las cuales las definiremos con los términos "infraestructura" y "Ad Hoc". Estos términos están relacionados, esencialmente, con las mismas distinciones básicas de topología.

5.1.2 Topología Ad-Hoc

En una topología Ad-Hoc, los propios dispositivos inalámbricos crean la red LAN y no existe ningún controlador central ni puntos de acceso. Cada dispositivo se comunica directamente con los demás dispositivos de la red, en lugar de pasar por un controlador central. Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas Ad-Hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

Figura 49. Topología Ad-Hoc.



Fuente: http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/topologias.htm

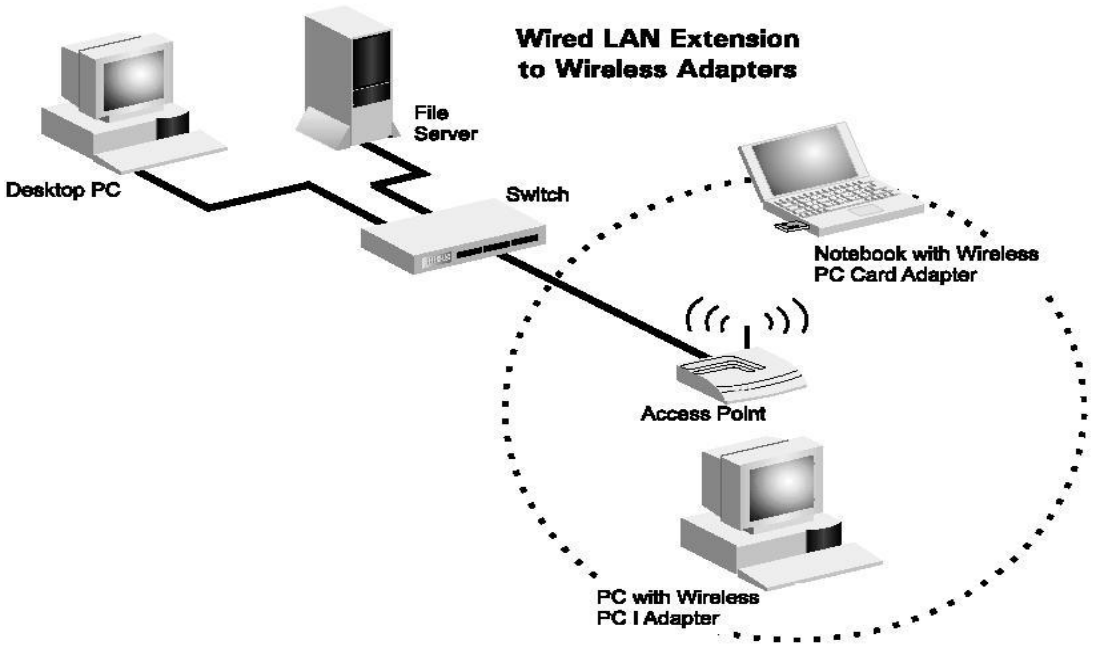
Del modo Ad-Hoc se puede decir que no tiene punto de acceso. En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red Ad-Hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

5.1.3 Topología infraestructura

Una topología de infraestructura es aquella que extiende una red LAN con cable existente para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso une la red

LAN inalámbrica y la red LAN con cable y sirve de controlador central de la red LAN inalámbrica. El punto de acceso coordina la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que se utilice y del producto. En la modalidad de infraestructura, puede haber varios puntos de acceso para dar cobertura a una zona grande o un único punto de acceso para una zona pequeña, ya sea un hogar o un edificio pequeño.

Figura 50. Topología infraestructura



Fuente: http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/topologias.htm

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red. La estación sólo puede transmitir o recibir tramas en la red después de que haya finalizado la asociación.

En la modalidad de infraestructura, todo el tráfico de red procedente de las estaciones inalámbricas pasa por un punto de acceso para poder llegar a su destino en la red LAN con cable o inalámbrica.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada. Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción

correcta, representan la parte del protocolo que evita las colisiones. Observe que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

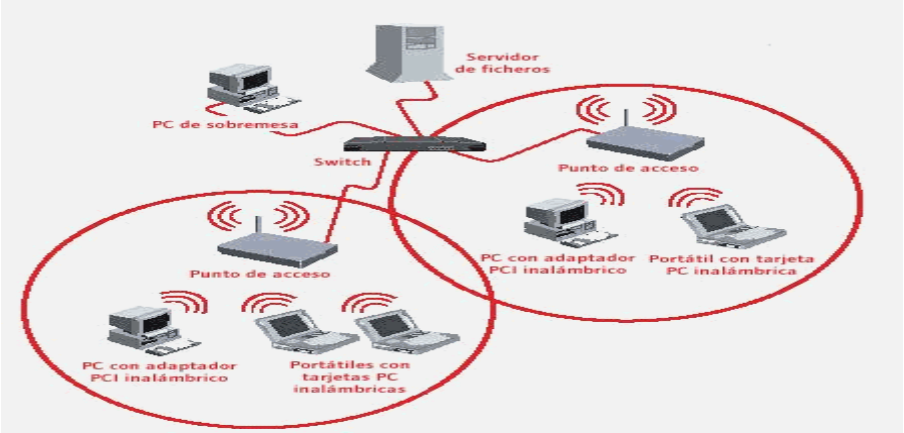
El proceso de movilidad de un punto de acceso a otro no está completamente definido en el estándar. Sin embargo, la señalización y el sondeo que se utilizan para buscar puntos de acceso y un proceso de reasociación que permite a la estación asociarse a un punto de acceso diferente, junto con protocolos específicos de otros fabricantes entre puntos de acceso, proporcionan una transición fluida.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

Unas de las utilidades más interesantes de esta tecnología inalámbrica, es la posibilidad de realizar *Roaming* entre los APs de la empresa, con lo que al

igual que la tecnología celular, no perdemos cobertura y podemos movernos desde el campo de cobertura de un AP a otro sin problemas, para ello debemos configurar los APs para que trabajen en distintos canales de frecuencia para que no se produzcan problemas de funcionamiento en las zonas donde existe cobertura de más de un AP.

Figura 51. Topología infraestructura con *roaming*.



Fuente: http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/topologias.htm

5.2 Diseño área de servidores

Ya conociendo los dos tipos de topologías que pueden tener una red inalámbrica, nos damos a la tarea de hacer el diseño físico de donde serán alojado nuestro servidor de datos y nuestro *swich* principal.

Derivado de que es una red pequeña la que queremos implementar y es un solo servidor de data y un *swich* principal en donde tendrás las siguientes características que se presentan a continuación.

5.2.1 Características del servidor

Existen varios tipo de servidores en el mercado, por comodidad, confiabilidad y soporte, escogimos el servidor de marca Hewlett-Packard y modelo DL140G3 que se muestra en la figura de abajo con su respectiva tabla de especificaciones

Figura 52. Forma física del servidor HP-DL140G3

Fuente: http://h10010.www1.hp.com/wwpc/es/es/sm/WF06a/781-783-380983-380983-12083395-12567054.html

Tabla IV. Especificaciones técnicas del servidor

Procesador, sistema operativo y memoria

Procesador	Procesador Intel® Xeon® Dual-Core 5160 (3 GHz, bus frontal (FSB) a 1333 MHz); Procesador Intel® Xeon® Dual-Core 5150 (2,66 GHz, FSB a 1333 MHz); Procesador Intel® Xeon® 5148 Dual-Core (2,4 GHz, FSB a 1333 MHz, voltaje medio); Procesador Intel® Xeon® Dual-Core 5110 (1,60 GHz, FSB a 1066 MHz); Procesador Intel® Xeon® Dual-Core 5080 (3,73 GHz, FSB a 1066 MHz); Procesador Intel® Xeon® Dual-Core 5060 (3,20 GHz, FSB a 1066 MHz); Procesador Intel® Xeon® Dual-Core 5050 (3 GHz, FSB a 667 MHz)
Características que facilitan el mantenimiento	Acceso a todos los componentes del sistema sin necesidad de utilizar herramientas para facilitar las tareas de mantenimiento en el bastidor
Peso, métrico	15,87 Kg
Chipset	*Chipset* Intel® 5000X
Tipo de memoria	DIMMs PC2-5300 con memoria intermedia completa (DDR2-667)
Ranuras de memoria	8 ranuras
Memoria máxima	16 GB
Ampliación de memoria	Máximo de 16 GB

Unidades internas

Almacenamiento masivo interno	SATA de 1 TB sin conexión en caliente; SATA de 1,5 TB de conexión en caliente; 293,6 GB SAS de conexión en caliente
Compartimentos para unidades internas	SATA sin conexión en caliente: hasta 2 unidades SATA de 3,5" sin conexión en caliente; SATA/SAS con conexión en caliente: hasta 2 unidades SATA/SAS de 3,5" con conexión en caliente
Unidad de disco flexible	Sólo a través de USB
Unidades ópticas	Unidad de DVD-ROM IDE (ATAPI) de 8x, plana (opcional); Unidad de CD-ROM IDE (ATAPI) de 24x (opcional); Unidad de DVD-ROM IDE (ATAPI) de 8x, plana (opcional); Unidad de CD-ROM IDE (ATAPI) de 24x (opcional)

Características del sistema

Chasis	Bastidor de 1U
Características de alimentación	650 W
Puerto de E/S	Red RJ-45 (*ethernet*) - 2 puertos para tarjetas de red 10/100/1000 (más 1 dedicado para gestión remota HP
Sistemas operativos compatibles	*Microsoft® Windows® 2000 Server (32 bits); Microsoft® Windows® 2000 Advanced Server (32 bits); Microsoft® Windows® 2003 y Microsoft® Windows® 2003/R2 Standard Edition (32 bits); Microsoft® Windows® 2003 y Microsoft® Windows® 2003/R2 Enterprise Edition (32*

	bits); Microsoft® Windows® 2003 y Microsoft® Windows® 2003/R2 Web Edition (32 bits); Microsoft® Windows® 2003 y Microsoft® Windows® 2003/R2 for Extended Systems Standard Edition (64 bits); Microsoft® Windows® 2003 y Microsoft® Windows® 2003/R2 for Extended Systems Enterprise Edition (64 bits); Red Hat Linux AS/ES/WS 3.0 y 4.0 (32 y 64 bits); SUSE Linux 9 (32 y 64 bits); SUSE Linux 10 (32 y 64 bits)
Características de capacidad de gestión	Gestión remota HP ProLiant Lights Out 100i de serie
Gestión de seguridad	Contraseña de encendido; Contraseña de configuración

Adicionalmente en esta área debe permanecer a una temperatura relativamente fría, pues derivado del tipo de funcionamiento que estos tipos de equipos juegan en nuestra red, deben permanecer las 24 horas del día en constante funcionamiento, es por tal razón que despiden cierto calor y por las condiciones del área que se les designo, se encierra el calor muy rápidamente.

5.3 Diseño del nodo maestro y esclavo de la piconet

Luego de realizar la instalación del servidor, se necesita establecer un punto de partida, el cual será nuestro Nodo Maestro, llamaremos en este caso al LAN s*wich* que va directamente conectado mediante un *patch cord* UTP categoría 5 debidamente crimpado en ambos extremos del mismo con conectores RJ45 fabricados para ese propósito, que cumpla los estándares de conectividad entre un LAN s*wich* y una *ethernet*, este lo instalaremos en una posición del r*ack* debajo del ya instalado servidor.

5.3.2 Características del *swich* (nodo maestro)

Este tipo de *swich*, con características especiales cumple con las características necesarias de conectividad y velocidad de 1 Gb/s en puertos específicos para la comunicarse a través de esta conexión con la *ethernet* del servidor y los demás puertos que no tengan velocidad de 1 Gb/s deben manejar velocidades de 10/100 Mb/s para conectarse con otras interfaces *ethernet.*

5.3.3 Características del *Access Point* (nodo esclavo)

Luego de haber montado y conectado de una manera satisfactoria el nodo maestro, comenzamos a determinar la ubicación del nodo esclavo, que en este caso llamaremos al *Access Point* el cual basándonos en las características

descritas con cada uno de los ejemplificados en el Capitulo 2, decidimos utilizar la opción del Bluetake BT30.

Del puerto 1 del LAN *swich* debe de haber conectividad mediante un cable UTP categoría 5 debidamente crimpado en un extremo, en el otro extremo del cable debidamente colocado para este propósito, de una manera estética y ordenada hasta el punto donde será colocado el *Access Point*, será terminado en un dado tipo j*ack* para conectores RJ45, que este a su vez montado en una placa especial para el mismo, ya teniendo de una manera correcta este tipo de conexión, procedemos a colocar un *patch cord* UTP categoría 5 debidamente crimpado en ambos extremos del mismo con conectores RJ45 fabricados para ese propósito, que cumpla los estándares de conectividad, entre el dado ya instalado y la entrada *ethernet* del *Access Point*.

5.4 Estableciendo normas de seguridad de la empresa

Cuando nos referimos a normas de seguridad, nos damos cuenta que todos los recursos de la empresa esta involucrada en la misma, estableciendo dos divisiones, vistas desde el punto tecnológico y el punto de vista humano.

5.4.1 Seguridad vista desde el punto de vista tecnológico.

Dentro del punto de vista de la seguridad tecnológica; es necesario considerar elementos que pongan las bases mínimas a seguir en materia de configuración y administración de la tecnología. Por ejemplo, establecer que los

servidores con información crítica de la empresa no deben prestar servicio de estaciones de trabajo a los empleados.

5.4.2 Seguridad vista desde el punto de vista humano

Otras personas ven a la seguridad como un problema únicamente humano. Es importante definir primero la conducta considerada adecuada para el tratamiento de la información y de los recursos utilizados. Por lo tanto, sin el apoyo de la Administración, el programa de seguridad no consigue dirigir las acciones necesarias para modificar la cultura de seguridad actual. El resultado es un programa de seguridad sin el nivel de cultura deseado y la falta de monitoreo más apropiado al orientar empleados, proveedores, clientes y socios. Sin embargo, no se debe dejar de lado los temas tecnológicos y su sofisticación, una vez que también son determinantes para la implementación de soluciones de seguridad adecuadas y eficientes.

Un ejemplo común es solicitar a los usuarios el cambio de su contraseña o *password* constantemente y que ésta deba tener una complejidad adecuada para la información manejada.

5.4.3 Elaboración de la política

Para establecer una política de seguridad debemos de tener en cuenta cuales son las exigencias que se van a presentar y las etapas que serán necesarias para elaborarlas.

5.4.3.1 Exigencias de la política

La política es elaborada tomando como base la cultura de la organización y el conocimiento especializado de seguridad de los profesionales involucrados con su aplicación y comprometimiento.

Es importante considerar que para la elaboración de una política de seguridad institucional se deben de cumplirse varios aspectos, entre los cuales figuran las personas encargadas de establecer las mismas, la elaboración del documento donde contiene las mismas, y por ultimo la publicación e información a toda la empresa de lo que se establecieron.

Parte importante que debe de contener el documento que se cree por las personas que lo elaboren es que deben expresarse las preocupaciones de la administración, donde se establecen normas para la gestión de seguridad de la información, que contengan:

- La definición de la propia política,
- Una declaración de la administración que apoye los principios establecidos y una explicación de las exigencias de conformidad con relación a:
    - Legislación y cláusulas contractuales;
    - Educación y formación en seguridad de la información;

- Prevención contra amenazas (virus, troyanos, *hackers*, incendio, intemperies, etc.)

- Debe contener también la atribución de las responsabilidades de las personas involucradas donde queden claros los roles de cada uno, en la gestión de los procesos y de la seguridad.

- No olvidar de que toda documentación ya existente sobre cómo realizar las tareas debe ser analizada con relación a los principios de seguridad de la información, para aprovechar al máximo las prácticas actuales, evaluar y agregar seguridad a esas tareas.

5.4.3.2 Etapas necesarias para la elaboración de la política

Elaborar una política es un proceso que exige tiempo e información. Es necesario conocer cómo se estructura la organización y cómo son dirigidos en la actualidad sus procesos. A partir de este reconocimiento, se evalúa el nivel de seguridad existente para poder después detectar los puntos a analizar para que esté en conformidad con los estándares de seguridad.

Tendremos en cuanta que existirán varias etapas para esta elaboración, entre ellas mencionamos las siguientes

- **Objetivos:** aquí determinaremos los objetivos que pretendemos con la elaboración de esta política.

- **Entrevista:** con estas se interrogara tanto a los administradores como a todos los usuarios existentes en la compañía y con ello se lograra identificar las necesidades de seguridad existentes en la organización.

- **Investigación y análisis de documentos:** en este proceso se investiga y se analizan que los documentos existen en la empresa y que tengan relación con seguridad para la reducción de riesgos, con el fin de analizar y darle continuidad a los mismos o bien actualizarlos.

- **Reuniones de política:** en este tipo de reuniones realizadas por el personal a cargo de la elaboración de las políticas, se tratara exclusivamente del levantado de la documentación y de las normas que se tomaran en torno a la seguridad de la empresa.

- **Glosario de la política:** al momento de redactar las normas y políticas, todo el mundo debe entender al 100% de que se esta hablando, es por tal razón que debe de existir un glosario para todos tengan el mismo nivel de comprensión y se capte de mejor manera el mensaje.

- **Responsabilidades y penalidades:** debe estar bien claro que cada elemento humano de la empresa es responsable de cada activo fijo asignado a él, por lo tanto deberán existir hojas de responsabilidad donde se especifique el activo y la penalización si se comprueba que fue dañado intencionalmente o no se tuvo el cuidado respectivo, aquí también se estipulan normas de confidencialidad de la información a terceras personas que puedan hacer mal uso de la misma.

5.5 Configuración de la red

Ya definida la configuración de la red en topología tipo estrella procedemos a la configuración que van a tener nuestros servidores y que configuración van a tener nuestros *host* de operación.

5.5.1 Configuración de los servidores

Tendremos dos servidores, cada uno de los dos los tendremos funcion*and*o con diferentes sistemas operativos, derivado de los distintos usos que le vamos a dar, en el servidor uno tendremos el sistema operativo *Linux Red Hat 7.3*, destinado a la parte de servidor DHCP., y en el servidor dos tendremos instalado el sistema operativo *Windows 2003 Server* con *SQL 2000 Server Service Pack 4*, en donde tendremos alojada la data de la empresa y archivos comunes compartidos para la empresa

5.5.1.1 Configuración del servidor uno

En Este servidor tendremos alojados nuestro servicio de DHCP *(Dynamic Host Configuration Protocol)*, este asigna direcciones IP a los *hosts* de la red, además que permite una administración simplificada, y funciona bien para todas los tamaños de red LAN. DHCP cuenta con mayores prestaciones y configuraciones automáticas que no demandan mucha administración por parte del usuario.

DHCP provee las siguientes configuraciones:

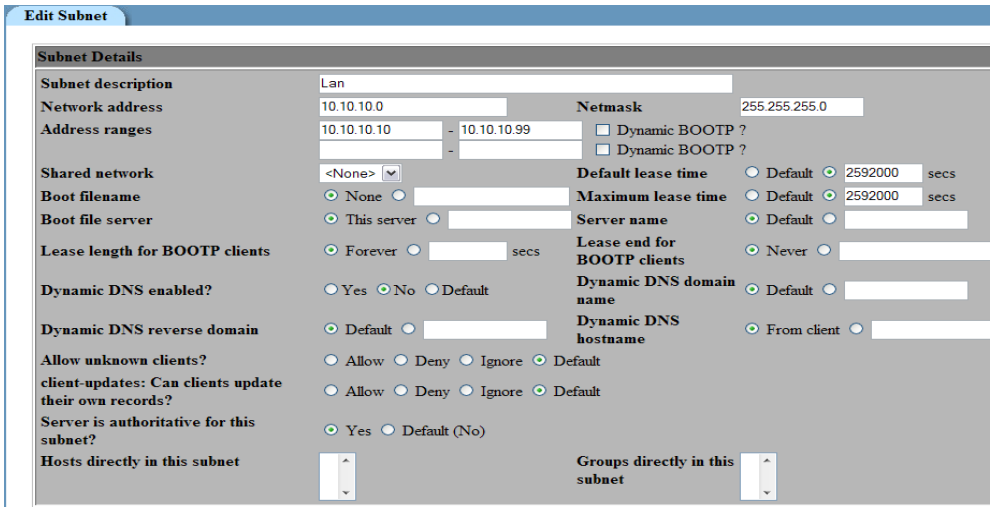
- Dirección IP
- Máscara de red
- Nombre de dominio
- *Default Gateway* (router)
- DNS
- WINS
- Entre otros

En la figura 52 se muestra la interfaz grafica del servicio de DHCP en el servidor de Linux

Figura 53. Servidor DHCP.

Ingresando al servicio de DHCP, procedemos a colocar la configuración que le dará a cada uno de los *Host* que se quieran conectar a este servicio. La figura 53 nos muestra como debe de llenarse cada uno de los campos de configuración escogidos para nuestro fin y que nuestro servicio DHCP quede funcionando de manera exitosa

Figura 54. Campos de servidor DHCP.



Ya que hemos completado esta información verificamos que nuestro archivo de configuración haya sido guardado con lo necesario para que el servicio funcione correctamente, tal como se muestra en la figura 54.

Figura 55. Archivo se configuración DHCP.

Con esta configuración nuestro servicio DHCP se pone a andar y listo para configurar a los *Host* invitados que se quieran conectar a nuestra LAN.

5.5.1.2 Configuración del servidor dos

En Este servidor tendremos alojado nuestra base de datos en *SQL 2000 Server Service Pack 4, Microsoft SQL Server 2000* es la versión del sistema de gestión de bases de datos relacionales (SGBDR) que aprovecha la sólida base establecida por su predecesor *SQL Server 6.5. Y 7. SQL Server 2000* es el SGBDR ideal para un amplio espectro de clientes corporativos y fabricantes independientes de software (ISV). Las necesidades y requisitos del cliente han dado lugar a innovaciones significativas en *SQL Server versión 2000,* entre las que se incluyen la facilidad de uso, escalabilidad y fiabilidad, y almacenamiento de datos.

Entre las más importantes innovaciones de *Microsoft SQL Server 2000* cabe citar:

- Primera base de datos que soporta la configuración automática y la auto-optimización.

- Primera base de datos con un servidor OLAP integrado.

- Primera base de datos con los servicios de transformación de datos (*Data Transformation Services*, DTS) integrados.

- El *Data Warehousing Framework* constituye el primer planteamiento de amplia cobertura, para la resolución de los problemas que plantea la utilización de metadatos.

- La primera base de datos que ofrece administración multiservidor para un gran número de servidores.

- Una gran variedad de opciones de duplicación de cualquier base de datos.

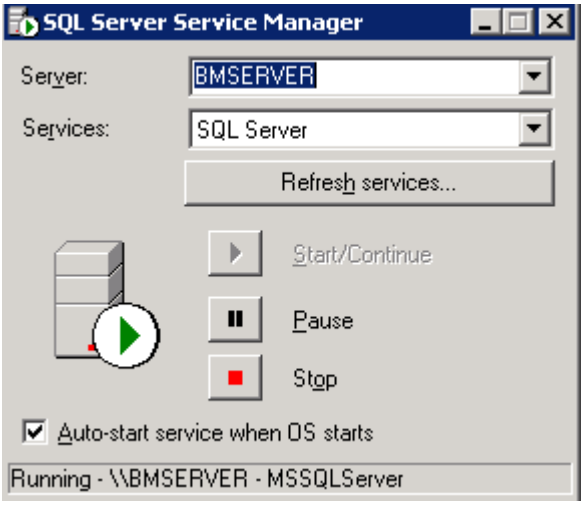
- La mejor integración con la familia *Windows NT Server, Microsoft Office y BackOffice®.*

- Acceso universal a los datos (*Universal Data Access*), la estrategia de Microsoft para permitir el acceso de alto rendimiento a una gran cantidad de fuentes de información.1

[1] Texto tomado de http://www.sqlmax.com/sql7.asp

En la figura 55 se ve que nuestro servicio de SQL este ejecutándose correctamente.

Figura 56. Servicio SQL en ejecución.



Ya seguros tanto que nuestro servidor uno y nuestro servidor dos, están ejecutándose correctamente podemos entrar a la configuración de los *host* que serán los que se conectaran a estos servidores.

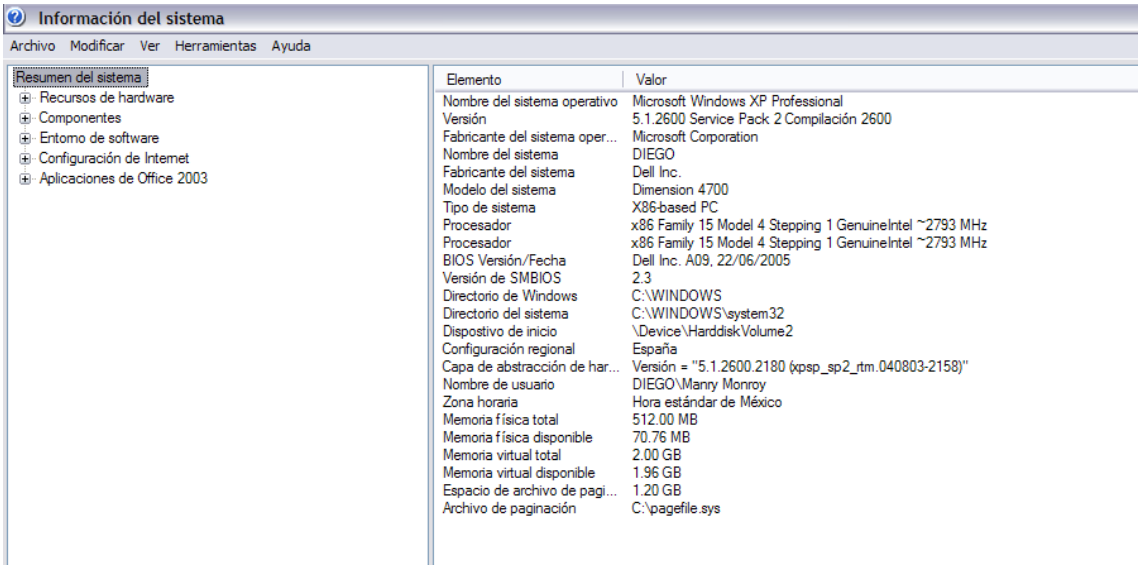
5.5.2 Configuración de los h*ost*

Cada uno de los host que serán los invitados a esta red, deben estar funcionando correctamente el sistema operativo y debidamente configurada la conexión de red para que esta adquiera automáticamente la configuración proporcionada por el servidor DHCP.

5.5.2.1 Sistema operativo

Cada uno de los *host* invitados tendrán instalados como sistema operativo *WinXp* con *Service Pack* y cada una de las actualizaciones publicadas en http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=es. La figura 56 nos muestra las características generales que tiene un *host*, en donde nos indica que tipo de sistema operativo, que versión, etc.

Figura 57. Características del sistema operativo instalado en el *host*.



5.5.3 Configuración conexión de red

Luego de tener nuestro sistema operativo funcionando correctamente, y luego de haber instalado el software provisto por el fabricante del

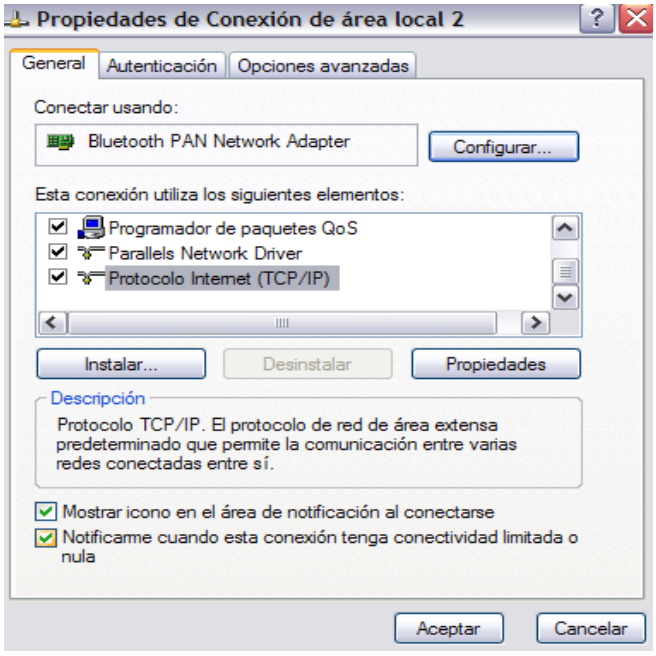
adaptador que elegimos, se nos creara una conexión de red, que por default nos aparecerá como desconectada.

En la figura 57 nos muestra las distintas conexiones de red que puede tener nuestro *host*, en donde se resalta la conexión de área local 2 que es la que corresponde en este caso a nuestro adaptador Bluetooth.

Figura 58. Conexiones de red existentes.

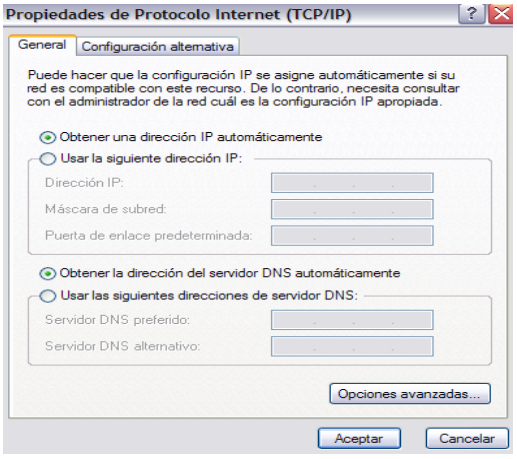
Ya posicionados en nuestra conexión de área local, entramos a las propiedades de la misma y configuramos el protocolo TCP/IP. En la figura 58 nos muestra las propiedades de la conexión en donde esta resaltado el protocolo que debemos de configurar.

Figura 59. Propiedades de conexión de área local asignada al adaptador Bluetooth.



Debemos verificar que el protocolo de Internet TCP/IP debe estar configurado para que obtenga la dirección IP automáticamente como se muestra en la figura 59

Figura 60. Configuración del *Protocol*o TCP/IP.



Ya con esta configuración nos aseguramos de que cuando tengamos una conexión a nuestro s*erver* DHCP, obtendremos una dirección IP, para que nuestro *host* sea identificado en nuestra red y poder hacer uso de la misma.

5.6 Configuración del nodo maestro y esclavo

5.6.1 Configuración del nodo maestro

Como lo vimos con anterioridad el nodo maestro esta compuesto por un LAN s*wich*, el cual para esta ocasión escogimos el s*wich Linksys* SRW224G4 , *24-port* 10/100 + *4-Port Gigabit Switch*, el cual es completamente configurable de dos maneras, en base a una conexión directa con un cable serial y configurable desde una sesión en *Hiperterminal*, o de una manera mas sencilla, con un *cross-over* conectado directamente de la computadora al *swich*, mediante una sesión de cualquier navegador de Internet.

A continuación describiremos los pasos de configuración que seguiremos para la configuración de nuestro nodo maestro.

- Iniciamos una sesión en nuestro explorador y tecleamos 192.168.0.1 que es la dirección IP por defecto que trae el *swich*.

En la figura de abajo podemos apreciar la instrucción anterior

Figura 61. Dirección de destino en un explorador *web.*

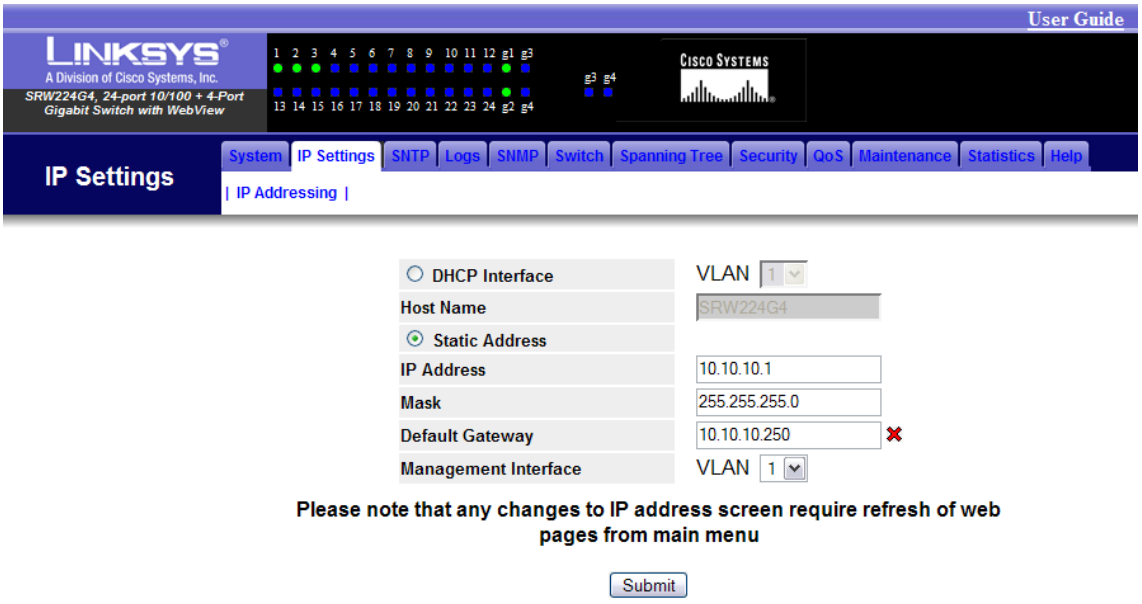
- Ya dentro de la página de bienvenida, colocamos el *user* que trae por defecto (admin.) y la contraseña por defecto esta en blanco, y le damos OK.

En la figura de abajo podemos apreciar la instrucción anterior

Figura 62. Página de bienvenida del LAN *swich*.

- Luego se procede a colocar un IP fijo de los que tenemos reservados en nuestra configuración del servidor DHCP como se muestra en la figura 63

Figura 63. Configuración IP del LAN *swich*.



Después de realizar esta configuración ya esta listo y configurado de una manera estándar y funcional para que cualquiera que se quiera conectar a cada uno de sus puertos interactúe sobre esa LAN.

5.6.2 Configuración del nodo esclavo

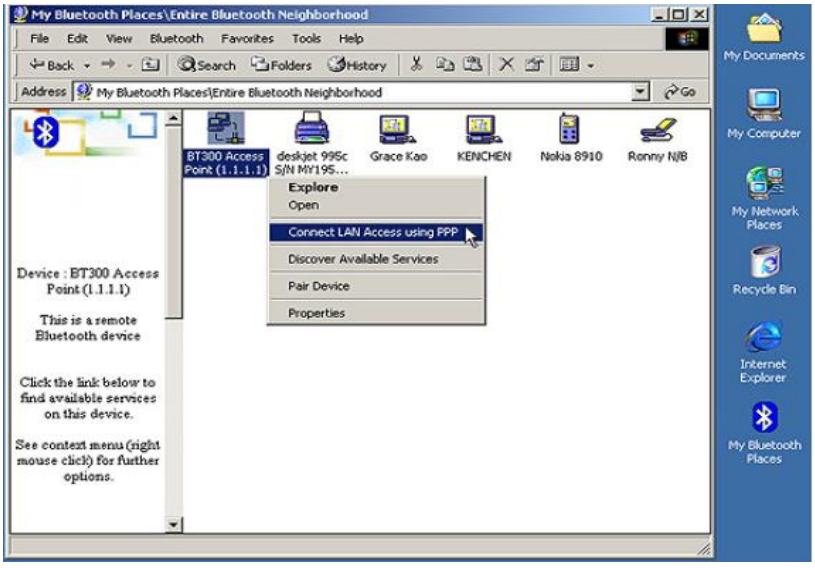
Como lo vimos con anterioridad el nodo esclavo esta compuesto por un *Access Point*, el cual nos estará irradiando la potencia necesaria para la

respectiva conexión, el cual para esta ocasión escogimos el *Access Point* Bluetake BT300, en cualquier h*ost* podemos configurarlo, en este caso lo configuraremos desde el s*erver* 1, con un nivel de seguridad alto (Nivel 3). Ya con el sistema operativo funcionando correctamente y con el software propio del adaptador configurado completamente y en modo de detección, el *Access Point* se configura de la siguiente manera.

- Ingresamos al *software* propio del *Access Point* previamente instalado que sirve para configurar el *Access Point*, allí nos aparecerá el dispositivo Bluetake 300

- Damos clic derecho en nuestro dispositivo Bluetake BT300, en el menú que se nos despliega damos clic donde dice Conectarme a la LAN Usando PPP, tal como se muestra en la figura de abajo.

Figura 64. Conexión con el A*ccess Point*.

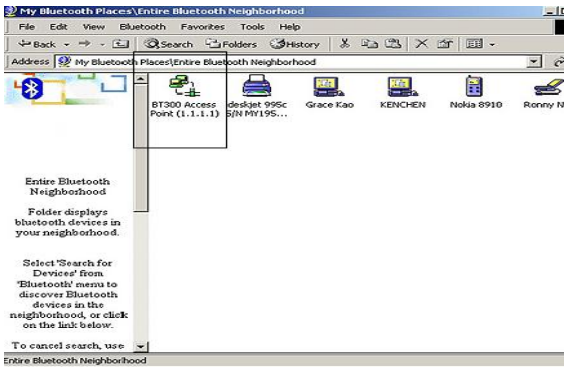


- Luego de haber realizado la acción anterior nos aparecerá una ventanita en donde por primera vez dejamos el nombre del usuario y contraseña en blanco, tal como se muestra en la figura 65.

Figura 65. Ingreso de usuario y contraseña.

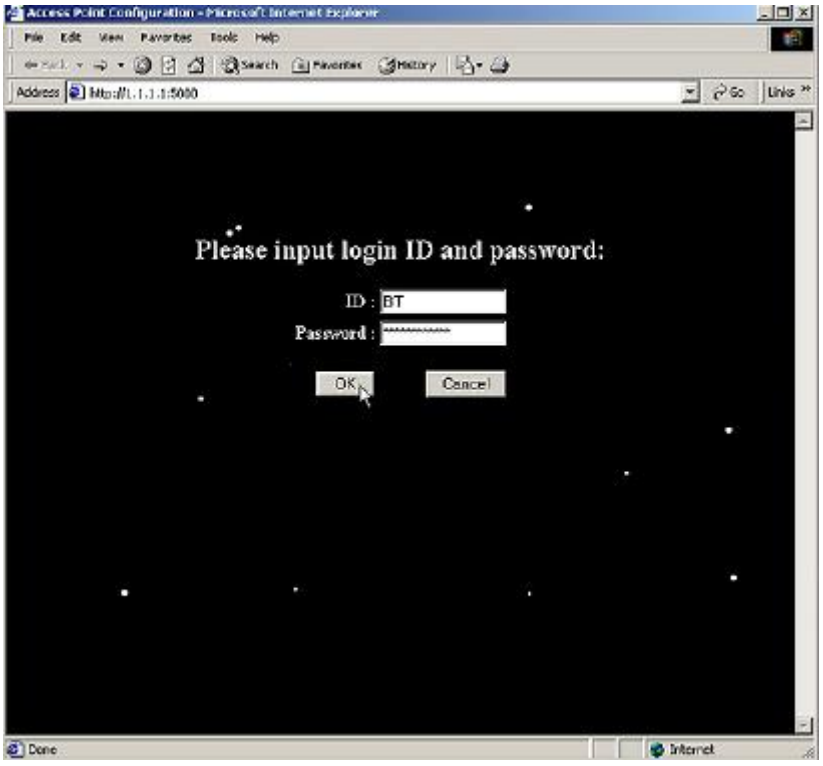
- Cuando la computadora se conecte al Bluetake BT300 satisfactoriamente, el icono que identifica al BT300 se pondrá en Verde con la dirección 1.1.1.1, tal como se aprecia en la figura de abajo.

Figura 66. Conexión Establecida con el Access *Point*.



- Luego de haber completado los pasos anteriores abrimos una sesión de nuestro explorador y tecleamos lo siguiente http://1.1.1.1:5000. Esta es la ruta para poder configurar cada una de las opciones del *Access Point*, por defecto tendremos como ID:BT y como contraseña *access_point*. Este paso lo podemos apreciar establecida en la figura 67.

Figura 67. Pantalla de inicio para configuración del A*ccess Point*.



- Luego de haber tenido una conexión satisfactoria, ya nos encontramos adentro del BT300 y podemos configurar las diferentes opciones que se presentan, en este caso configuraremos la seguridad, el IP que le vamos a asignar a este dispositivo, tal como se muestra en la figura de abajo.

Figura 68. Configuración IP del *Access Point*

Como se puede apreciar en la parte de arriba donde dice PIN *Code*, estableceremos la contraseña única que debe de ser de total confidencialidad para quien se quiera conectar a la red.

Ya estableciendo todas estas configuraciones descritas paso por paso a cada uno de los dispositivos que tenemos en nuestra red, podemos asegurarnos una conectividad segura y eficiente, en base a todos los estándares de seguridad y conectividad que requiere la empresa.

CONCLUSIONES

1. Una red inalámbrica Bluetooth basa su funcionamiento en una banda que esta disponible para su uso de manera gratuita, esta ubicada en la frecuencia de las 2.4 Ghz., la cual utiliza 79 canales con un ancho de banda de 1 MHz. Brindando así una transmisión punto a punto de un dispositivo transmisor/receptor a otro con las mismas características teniendo un alcance de hasta 100 metros.

2. Con base a cuantos elementos de una red deseamos conectar, podemos determinar qué tipo de red es la que deseamos implementar, ya sea una red sencilla tipo *Piconett* o una más compleja que formaría una *Scatternet*, además de tener muy en cuenta la operabilidad, ancho de banda y número de elementos conectados a la vez.

3. La seguridad es muy importante cuando nos disponemos a implementar una red de este tipo, es por eso que contamos con tres niveles de seguridad:
   - Nivel de Seguridad 1: Este nivel no es nada confiable ni recomendable, ya que no tiene ningún tipo de restricción ante un dispositivo de conexión entrante.
   - Nivel se Seguridad 2: Este es un nivel 50% confiable, confiable en el sentido de que si existen restricciones de por medio pero no tan severas como podrían ser.
   - Nivel de Seguridad 3: Este es un nivel bastante confiable, ya que no solo cuenta con políticas de restricción sino que los datos enviados

no pueden ser vulnerables tan fácilmente, ya que existe encriptación entre el enlace de un punto a otro. Y a nivel de LAN en una empresa este es el nivel más recomendable.

4. Cuando pretendemos acceder a una red tenemos varias formas de hacerlo de acuerdo al nivel de seguridad que vayamos a implementar, en nuestro caso como fue implementada a un nivel de seguridad tipo 3, encontraremos de acuerdo a las características de este nivel con que podremos acceder media vez la información haya sido autorizada, encriptada y autenticada.

5. El montar una red de este tipo no es tan complicado como parece, pero a la vez no es tan sencillo también, se debe de tener ciertos cuidados ante la información a compartir, basándonos en una política de seguridad en la empresa, vemos que la planificación, el acceso y las posibles penalizaciones ante la violación de las mismas, forman pieza clave y fundamenta, además de que el recurso humano a cargo de la administración debe de estar capacitado a nivel de configuración en varios escenarios de sistema operativo a utilizar por parte de la empresa, si todo esto se cumple a cabalidad, estamos seguros de que no cualquiera podrá usar de manera indebida los recursos compartidos en la LAN.

RECOMENDACIONES

1. Es aconsejable determinar el número de dispositivos externos funcionando en la frecuencia de los 2.4 GHz, cuando nos referimos a externos nos referimos a que puedan existir redes o dispositivos de tecnología inalámbrica que utilicen esta frecuencia, ya que con base a esto debe ser planeada la capacidad, potencia y alcance de los dispositivos que integraran parte de la red inalámbrica Bluetooth que se esta montando, para no tener algún inconveniente de comunicación en nuestra red.

2. Es necesario y fundamental no sobrecargar un solo *Access Point* con varios dispositivos a la vez, si fuera el caso necesario, hacer un análisis del crecimiento de usuarios y de esta manera ir agregando más puntos de acceso, para tener balanceada la carga de transferencia de información.

3. Con base al tipo de información que se maneje, es recomendable utilizar el nivel de seguridad más alto, por la importancia del giro de negocio empresarial, asegurando así la exactitud, fiabilidad, y seguridad en toda la información que involucra cada uno de los departamentos que conforman la empresa.

4. Es importante que cada uno de los usuarios pertenecientes a esa red, aprendan de memoria la contraseña de la red, y que este consiente que esta no debe ser compartida a ninguna persona ajena a la empresa, o bien si es perteneciente a la empresa pero que no cuente con derechos o autorizaciones para acceder a la red, mediante el uso de esta tecnología.

5. Los encargados de la administración de la red, deben ser personas íntegras y comprometidas en su trabajo respetando las políticas de seguridad creadas para fines de seguridad de la empresa.

BIBLIOGRAFÍA

1. Kammer, David. *Bluetooth Aplication Developer's Guide*. Edición I. Estados Unidos: *Syngress Publishing*, 2002. 561 pp.

2. *Specification of the Bluetooth System "PROFILES". versión 1.1*. *Bluetooth Corporation*, febrero 22 del 2001. 452 pp.

3. Karygiannis, Tom. *Wireless Network Security*. Publicación Especial 800-48. Estados Unidos. 104 pp.

4. *Specification of the Bluetooth System "CORE". versión 1.1. Bluetooth Corporation*, febrero 22 del 2001. 1084 pp.

5. Sweeney, Dennos. *Bluetooth Tutoria,* Virginia, junio 14 del 2000. 46 pp.

6. *Website Bluetooth*, http://www.Bluetooth.com : junio 2005

7. *Website* Revista Red, http://www.red.com.mx : julio 2005

8. *Website* Bluetooth, http://www.Bluetooth.org : julio 2005

9. *Website* Bluetooth, http://www.redes.upv.es/ter/tema%206/Presentaci%C3%B3n%20(1xhoja).pdf. : julio 2005

10. *Website* Zona Bluetooth. http://www.zonaBluetooth.com :agosto 2005

11. *Website* Ericsson. http://www.ericsson.com/bluetoot : noviembre 2005

12. *Website* BlueZ. http:/www.bluez.sourceforge.net : febrero 2006

13. *Website* HP. www.hp.com/rnd/library/pdf/understa*nd*ingBluetooth.pdf marzo 2006

14. *Website* Osmosis. www.osmosislatina.com/conectividad/Bluetooth.htm : marzo 2006

15. *Website* Bluetake. http://www.geekzone.co.nz: marzo 2006

16. *Website* D-Link. http://www.dLink.com : marzo 2006

17. *Website* GSML*and*ia. http://gsmlandia.com/instructions.php?id_instruction=7 : marzo 2006

18. *Website* HP. http://www.hp.com : enero 2007

19. *Website* Servidores DNS. http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/topologias.htm : enero 2007