TESIS
II2002
M6
v.2

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMATICA

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

Universidad Católica Andrés Bello
BIBLIOTECA
Caracas

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

INDICE APENDICES

INDICE APENDICES 1
INDICE ANEXOS 2
APENDICE A 3
ACRONIMOS 3
APENDICE B 7
TERMINOLOGIA BLUETOOTH 7
APENDICE C 15
PROTOCOLOS ADOPTADOS. 15
APENDICE D 20
ENLACES FISICOS 20
APENDICE E 23
REDES LAN INALAMBRICAS. 23
APENDICE F 31
SEGURIDAD *BLUETOOTH* 31
APÉNDICE G 50
MODOS 50
APENDICE H 55
REQUERIMIENTOS DE INTEROPERABILIDAD DE RFCOMM. 55
APENDICE I 58
REQUERIMIENTOS DE INTEROPERABILIDAD DE L2CAP. 58
APENDICE J 60
REQUERIMIENTO DE INTEROPERABILIDAD DEL GESTOR DE ENLACE (LM) 60
APENDICE K 61
REQUERIMIENTOS DE INTEROPERABILIDAD DEL CONTROL DE ENLACE (LC). 61
APENDICE L 63
CONFIGURANDO Y TRABAJANDO CON BLUELAP 63

INDICE ANEXOS

ANEXO A *Bluetooth Application Tool Kit*

ANEXO B *Bluetooth Development Kit*

ANEXO C *Wi-Fi (*802.11b) *and Bluetooth*

ANEXO D *Enabling Wi-Fi and Bluetooth Coexistence without compromise*

ANEXO E 2.*4 GHz and 5 GHz WLAN: Competing or Complementary?*

ANEXO F *Bluetooth Assigned Numbers*

APENDICE A

ACRONIMOS

Acrónimo	Término en Inglés	Término en Español
ACK	Acknowledge	Confirmar
ACL	Asynchronous Connectionless	Asíncrono sin conexión
ACO	Auyhenticated Ciphering Offset	Desplazamiento de cifrado autentificado
AM_ADDR	Active Member Address	Dirección de miembro activo.
AP	Access Point	Punto de acceso
API	Application Programming Interface	Interfaz de programación de aplicaciones
ARQ	Automatic Repeat Request	Solicitud de repetición automática
AS	Autonomous System	Sistema autónomo
BB	Baseband	Banda Base
BD_ADDR	Bluetooth Device Address	Dirección de dispositivo Bluetooth
BER	Bit Error Rate	Tasa de errores de bit
BT	Bandwidth Time	Tiempo de ancho de banda
CAC	Channel Access Code	Código de acceso a canal
CHAP	Challenge Handshake Authentication	Protocolo de autentificación por negociación de desafió
CID	Channel Identifier	Identificador de canal
CoD	Class of Device	Clase de dispositivo
CRC	Cyclic Redundancy Check	Comprobación de redundancia cíclica
DAC	Device Access Code	Código de acceso a dispositivo
DCE	Data Communication Equipment	Equipo de comunicación de datos
DevA	Data Terminal A	Dispositivo Terminal A
DevB	Data Terminal B	Dispositivo Terminal B
DIAC	Dedicated Inquiry Access Code	Código de acceso de indagación dedicada
DLCI	Data Link Connection Identifier	Identificador de la conexión de transmisión de datos
DT	Data Terminal	Dispositivo Terminal
DTC	Digital Traffic Channel	Canal digital de trafico
DTE	Data Terminal Equipment	Equipo terminal de datos
EIA	Electronic Industries Alliance	Alianza de la industria

		electrónica
ETSI	European Telecommunications Standards Institute	Instituto europeo de estándares de telecomunicaciones
FDMA	Frequency Division Multiple Access	Acceso múltiple por división de frecuencia
FEC	Forward Error Correction	Corrección directa de errores
GAP	Generis Access Profile	Perfil de acceso genérico
Gbps	Gigabits per second	Gigabits por segundo
GIAC	General Inquiry Access Code	Código de acceso de indagación general
HCI	Host Controller Interface	Interfaz controladora de host
HDLC	High-level Data-link Control	Control de alto nivel de enlace de datos
IAC	Inquiry Access Code	Código de acceso de indagación
IEC	International Electrotchnical Comisión	Comisión Electrotécnica internacional
IEEE	Institute of Electronic and Electrical Engineers	Instituto de ingenieros eléctricos y electrónicos
IETF	Internet Engineering Task Force	Grupo especial de ingeniería Internet
IP	Internet Protocol	Protocolo Internet
IPX	Internetwork Packet eXchange	Intercambio de paquetes Inter- red
IrDA	Infrared Data Association	Asociación de datos por infrarrojo
ISM	Industrial, Scientific, Medical	Industriales, científicas, médicas
ITU	International Telecommunication Union	Unión internacional de telecomunicaciones
L2CAP	Logical Link Control Adaptation Protocol	Protocolo de adaptación y control del enlace lógico
LAN	Local Area Network	Red de área local
LAP	LAN Access Point	Punto de acceso a LAN
LC	Link Controller	Controlador de enlace
LCP	Link Control Protocol	Protocolo de control de enlace
LIAC	Limited Inquiry Access Code	Código de acceso de indagación limitada
LLC	Logical Link Control	Control de enlace lógico
LM	Link Manager	Gestor de enlace

LMP	Link Management Protocol	Protocolo de gestión de enlace
M_ADDR	Medium Access Control Address	Dirección de control de acceso al medio físico
MAC	Medium Access Control	Control de acceso al medio físico
ME	Management Entity	Entidad de Administradora
MTU	Maximum Transmisión Unit	Unidad de transmisión máxima
NCP	Network Control Protocol	Protocolo de control de red
PAN	Personal Area Network	Red de área personal
PDA	Personal Digital Assistant	Asistente digital personal
PDU	Protocol Data Unit	Unidad de datos de protocolo
PIN	Personal Identification Number	Número de identificación personal
PM_ADDR	Parked Member Ardes	Dirección de miembro estacionado
PPP	Point-to-Point Protocol	Protocolo punto a punto
PSM	Protocol /Service Multiplexer	Multiplexor de protocolos/servicios
QoS	Quality of Service	Calidad de servicio
RAND	Random number	Número aleatorio
RAS	Remote Access Server	Servidor de acceso remoto
RF	Radio Frequency	Radio frecuencia
RFC	Request For Comments	Solicitud de comentarios
RFCOMM	Radio Frequecy Communication	Comunicación por radio frecuencia
SAP	Service Access Points	Puntos de acceso de servicio
SAR	Segmentation and Reassembly	Segmentación y reconstrucción
SCO	Synchronous Connection Oriented	Síncrono orientado a conexión
SD	Service Discovery	Descubrimiento de servicios
SDAP	Service Discovery Application Profile	Perfil de aplicación de descubrimiento de servicios
SDP	Service Discovery Protocol	Protocolo de descubrimiento de servicio
SIG	Special Interest Group	Grupo de interés especial
TCP/IP	Transmisión Control Protocol/Internet Protocol	Protocolo de control de transmisión/ Protocolo Internet

TCP/UDP	Transmisión Control Protocol/User Datagram Protocol	Protocolo de control de transmisión/Protocolo de datagramas de usuario
TDD	Time Division Duplex	Duplex por división de tiempo
TDM	Time Division Multiplexing	Multiplexación por división de tiempo
TDMA	Time Division Multiple Access	Acceso múltiple por división de tiempo
UA	User Asynchronous	Usuario asíncrono
UAP	Upper Address Part	Parte superior de la dirección
UART	Universal Asynchronous Receiver-Transmitter	Transmisor-Receptor asíncrono universal
UC	User Control	Control de usuario
UDP	User Datagram Protocol	Protocolo de datagramas de usuario
UI	User Interface; User Isochronous	Interfaz de usuario; Usuario isócrono
UIAC	Unlimited Inquiry Access Code	Código de acceso de indagación ilimitada
UUID	Universally Unique Identifier	Identificador universal unívoco
WAE	Wireless Application Environment	Entorno inalámbrico de aplicación
WAN	Wide Area Network	Red de área extensa

APENDICE B

TERMINOLOGIA BLUETOOTH

Autentificación: es el proceso de verificar la identidad de un dispositivo en el otro extremo del enlace. Esto se consigue mediante un procedimiento de autentificación basado en la clave de enlace almacenada o mediante el emparejamiento (introducción de un PIN).

Autorización: es concederle a un dispositivo *Bluetooth* en específico acceso a un servicio específico. Puede estar basada en una confirmación del usuario o en la existencia de una relación de confianza.

Banda base: describe las especificaciones de la parte de procesamiento digital de la señal del hardware de *Bluetooth*; específicamente, se refiere al controlador de enlace, que implementa los protocolos de banda base y otras rutinas de enlace de bajo nivel. El término de banda base se refiere al nivel físico del protocolo *Bluetooth,* que gestiona los enlaces y canales físicos. La especificación Banda base define dos enlaces: síncrono orientado a conexión (SCO) y asíncrono sin conexión (ACL).

***Bluetooth*:** es la especificación de enlace de comunicación inalámbrica que opera en la banda ISM de 2.4 GHz, utilizando espectro expandido de salto de frecuencia.

Permite la comunicación de voz en tiempo real y datos entre *hosts Bluetooth*. El protocolo de enlace está basado en *time slots*.

Bonding: es un procedimiento que crea una relación entre dos dispositivos *Bluetooth* basándose en una clave de enlace común. Esta clave se crea e intercambia durante el procedimiento de acoplamiento y es almacenada por ambos dispositivos *Bluetooth* para su uso en futuras autentificaciones.

Búsqueda (*Paging*): es un procedimiento que implica la transmisión de una serie de mensajes con el objetivo de establecer un enlace de comunicaciones con una unidad activa situada dentro del área de cobertura. Si una unidad remota responde a la operación de búsqueda, se establece una conexión.

Clase de dispositivo (CoD): es un parámetro utilizado durante el procedimiento de descubrimiento de dispositivos. Este parámetro es suministrado por el dispositivo remoto, e indica que tipo de dispositivo es y que tipo de servicios soporta.

***Clock Offset*:** es la diferencia entre el reloj esclavo y el maestro, cuyo valor se incluye en la carga útil del paquete de sincronización de saltos de frecuencia.

Conexión: es la fase de la comunicación entre dispositivos mediante la cual se procede al establecimiento de una conexión entre las unidades. La fase de conexión tiene lugar después de completar la fase de establecimiento del enlace.

Descubrimiento: es un término utilizado para describir los protocolos y mecanismos por los cuales un dispositivo conectado a la red o un servicio de software toma conciencia de la red a la que están conectados y descubren que servicios de red están disponibles.

Descubrimiento de dispositivo: es el mecanismo para solicitar y recibir la dirección *Bluetooth,* el reloj, la clase de dispositivo, el modo de exploración de búsqueda utilizado y los nombres de los dispositivos.

Descubrimiento de nombres: es un procedimiento que proporciona al dispositivo iniciador el nombre de dispositivo de otros dispositivos conectables.

Descubrimiento de servicios: es la capacidad de descubrir las funcionalidades ofrecidas por los dispositivos conectados.

Dirección MAC: es la dirección de control de acceso al medio físico que se emplea para distinguir a las diferentes unidades que participan en una *piconet.*

Dispositivo de confianza: es un dispositivo *Bluetooth*, el cual ha sido previamente autentificado y al que se le ha concedido acceso a otro dispositivo, basado en su clave de nivel de enlace.

Dispositivo desconocido: es un dispositivo que no está actualmente conectado con un dispositivo local y con el cual no se ha emparejado anteriormente. A estas unidades también se les llama dispositivos nuevos.

Dispositivo de desconfianza: es un dispositivo *Bluetooth* que es desconocido para otro dispositivo; puede requerir autorización basada en algún tipo de interacción del usuario antes de que se le pueda conceder el acceso.

Emparejamiento (*Pairing*): es un proceso de inicialización por el que dos dispositivos que se estén comunicando por vez primera crean una clave de enlace común que se utilizará para las autentificaciones siguientes.

Esclavo: una unidad dentro de una *piconet* que está sincronizada con el maestro a través de su reloj y secuencia de saltos. Hasta siete esclavos pueden estar relacionados con un maestro de esta forma dentro de una *piconet*.

Espectro Extendido (*Spread Spectrum*): consiste en expandir la información de la señal sobre un ancho de banda mayor, y con ello dificultar las interferencias y su posible intercepción.

Equipo Terminal de circuito de datos (DCE): en una estación de datos, es el equipo que proporciona la conversión de señales y la codificación entre el equipo terminal de datos (DTE) y la línea. El DCE puede ser un equipo independiente, una parte integrada en el DTE o en un equipo intermedio. El DCE puede realizar otras funciones que normalmente se realizan en el extremo de la red de la línea.

Equipo Terminal de Datos (DTE): equipo consistente en instrumentos finales digitales que convierten la información del usuario en señales de datos para transmisión, o reconvierten las señales de datos recibidas en información de usuario.

Exploración de búsqueda (*Page scan*): es el proceso por el cual un dispositivo escucha para detectar mensajes de búsqueda que contengan su propio (DAC).

Gestor de Enlace (*Link Manager* LM): es el software que se encarga de realizar el establecimiento del enlace, la autentificación, la configuración del enlace, etc. Proporciona servicios como: control de cifrado, control de potencia y la implementación de las capacidades QoS. También gestiona el paso de los dispositivos entre los diferentes modos de operación.

Grupo de Interés Especial (SIG): son los miembros fundadores y otras compañías que se adoptaron a este proyecto y dieron forma al SIG de *Bluetooth*, el cual lleva a cabo todas las directrices y decisiones sobre la tecnología *Bluetooth*.

HCI (*Host Controller Interface*): es una interfaz de comando que permite gestionar la banda base de un dispositivo *Bluetooth*, la cual provee un método de acceso uniforme para las capacidades de la banda base de *Bluetooth*.

Indagación (*Inquiry*): es un procedimiento por el que una unidad transmite mensajes destinados a descubrir a las otras unidades que puedan estar activas dentro del área de cobertura.

IP (Protocolo Internet): es el protocolo que distribuye los datagramas a través de diferentes redes TCP/IP mediante enrutadores que procesan los paquetes que viajan desde un sistema autónomo a hasta otro.

ISM: son las bandas que no requieren una licencia de operador. La tecnología *Bluetooth*, opera en la banda que está sobre los 2.4 GHz.

L2CAP: es un protocolo *Bluetooth* que está en el nivel de enlace de datos (nivel 2) del modelo de referencia OSI y proporciona servicios de datos orientados a la conexión y no conexión a los protocolos de nivel superior con capacidad de multiplexación de protocolos, y funcionalidad de segmentación. L2CAP permite a las aplicaciones y protocolos de mayor nivel transmitir y recibir paquetes de datos L2CAP de hasta 64 Kbps de longitud.

Maestro: es el dispositivo de una *piconet* cuyo reloj y secuencia de saltos se utilizan para sincronizar a todos los otros dispositivos, los esclavos de la *piconet*. La unidad

que realiza el procedimiento de búsqueda y establece la conexión es, de forma predeterminada el maestro de la conexión.

Multiplexación de protocolos: es una función que es realizada en el nivel de protocolo L2CAP. Este nivel debe soportar la multiplexación de protocolos porque el protocolo de banda base no admite un campo "tipo" que permita identificar el protocolo de nivel superior que está siendo multiplexado por encima.

Nombre de dispositivo *Bluetooth*: es el nombre del dispositivo, tiene una longitud máxima de 248 bytes.

PAN (Red de área personal): es un concepto de red en el que todos los dispositivos utilizados en la vida diaria de una persona se comunican y trabajan conjuntamente, compartiendo la información y los servicios entre todos los dispositivos.

Pasarela (*Gateway*): es una estación base que emplea la tecnología inalámbrica *Bluetooth* y que está conectada a una red externa.

PDU: es un término genérico para referirse a los paquetes de datos de cabecera utilizados en cualquier nivel de una pila de protocolos.

Piconet: es un conjunto de unidades que comparten un canal común. Pueden soportar hasta ocho dispositivos interconectados en una misma *piconet*, pudiendo haber un maestro y siete esclavos.

PIN: el PIN *Bluetooth*, se utiliza para autentificar a dos dispositivos que no hayan previamente intercambiado una clave de enlace. Intercambiando el PIN, los dispositivos establecen una relación de confianza.

PPP: es un mecanismo ampliamente utilizado para proporcionar acceso a redes. PPP proporciona autentificación, cifrado, compresión de datos y soporte para múltiples

protocolos. PPP sobre RFCOMM proporciona acceso a redes LAN para dispositivos *Bluetooth.*

Procedimiento de Indagación (*Inquiry Procedure*): este procedimiento permite a un dispositivo descubrir otros dispositivos que se encuentran dentro del rango de cobertura y determinar las direcciones y relojes de dichos dispositivos, luego se usa el procedimiento de búsqueda para establecer la conexión.

QoS (*Quality of Service):* en la señalización L2CAP, se puede solicitar un rendimiento garantizado para una aplicación durante el establecimiento de la conexión. En una solicitud de configuración de QoS, pueden especificarse parámetros tales como variación del retardo, ancho de banda pico, etc. Si no se especifica ninguna opción QoS en la solicitud, se asume un servicio no garantizado.

RFCOMM: es un protocolo de transporte simple con provisiones adicionales para emular los nueve circuitos de los puertos serie RS-232 sobre el protocolo L2CAP. Este protocolo de emulación de cable serie está basado en la recomendación ETSI TS 07.10.

RS-232: es la definición de un estándar establecida por la EIA, de la interfaz de la comunicación serial, conectores, etc.

Scatternet: son dos o más *piconets* situadas en la misma área, con o sin comunicación inter-*piconet.*

SDP: el perfil de descubrimiento de servicios describe el protocolo utilizado por las aplicaciones para descubrir que servicios tienen a su disposición y para determinar las características de dichos servicios.

TCP: proporciona una conexión fiable entre dispositivos en el nivel de transporte, utilizando IP en el nivel de red.

UART: es un dispositivo que convierte las señales de datos paralelas en señales de datos seriales, para la transmisión sobre servicios de comunicación serial, o convierte señales seriales en señales paralelas para ser usado por computadora su otros dispositivos.

UDP: es un protocolo que transfiere mensajes individuales a IP para su transmisión a través de la red según un esquema no garantizado.

Unidad Máxima de Transmisión (MTU): es el tamaño máximo en *bytes* del paquete, que se puede transmitir a través de un enlace.

vCalendar: es un formato para información de planificación y calendario.

vCard: es un formato para información de carácter personal como la que aparecería en una tarjeta de visita.

APENDICE C

PROTOCOLOS ADOPTADOS.

1. Protocolo Punto a Punto (PPP).

Fue desarrollado por el Comité para la Ingeniería en Internet (IETF)[1] en 1993, este estándar define como los datos son trasmitidos sobre un enlace serial punto a punto. Dichos enlaces proveen operación bidireccional *full duplex* y asume que los paquetes serán entregados en orden. PPP tiene tres componentes:

(1) Un mecanismo para poder encapsular datagramas multiprotocolo y manejar la detección de errores.

(2) Un protocolo de enlace (LCP)[2] para poder establecer, configurar y probar la conexión de datos.

(3) Una familia de protocolos de control de red (NCPs)[3] para establecer y configurar los distintos protocolos de nivel de red, en este caso es para IP se utiliza IPCP[4].

También proporciona la verificación de autentificación, suma de verificación (CRC), en cada *frame*.

[1] Siglas en inglés: "Internet Engineering Task Force (IETF)"
[2] Siglas en inglés: "Link Control Protocol (LCP)"
[3] Siglas en inglés: "Network Control Protocols (NCPs)"
[4] Siglas en ingles: "Internet Protocol Control Protocol (IPCP)"

1.1 Protocolo IPCP.

Opcionalmente el LAP, puede configurarse para dar soporte al protocolo IP. El uso de este protocolo de PPP no forma parte de este perfil. Es mencionado en este informe con propósitos informativos. Si es soportado, el protocolo IPCP se debe apoyar en el RFC 1332.

En las siguientes sub-secciones se muestra información referente a IPCP. En ellos se describe brevemente ciertos aspectos de IPCP (para más detalles ver RFC 1332).

1.1.1 Conexión IPCP.

IPCP sólo comienza a trabajar después de que ocurre lo siguiente:(a) La conexión PPP a sido establecida usando LCP, (b) El usuario ha sido autentificado.

El protocolo IPCP negocia ciertos parámetros entre el LAP y el DT. Una vez que se ha establecido la conexión, y una vez que se ha negociado una dirección IP conveniente, la interfaz IP es habilitada.

1.1.2 Asignación de la dirección IP.

El DT requiere de una dirección IP para poder operar dentro de una LAN. Actualmente PPP permite tres posibilidades de implantación:

1.- La opción IPCP es utilizada para especificar una dirección IP pre-configurada. Si esta dirección IP no es permitida en la LAN, entonces el establecimiento del enlace IPCP no es permitido.

2.- La opción IPCP es para solicitar un configuración IP conveniente desde un servidor PPP.

3.- La opción de IPCP IP móvil es usada para solicitudes específicas de configuraciones IP. Cuando el dispositivo se mueve entre puntos de acceso en la misma LAN.

2. Arquitectura de Protocolos TCP/IP.

Es el resultado de la investigación y desarrollo llevados a cabo en la red experimental de conmutación de paquetes ARPANET, financiada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA)[5].

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren distintos niveles del modelo OSI. Los dos protocolos más importantes son el Protocolo de Control de Transmisión (TCP)[6] y el Protocolo de Internet (IP). La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

(a) Física: define la interfaz física entre el dispositivo de transmisión de datos. Se encarga de la especificación de las características del medio de transmisión, la naturaleza de las señales, la velocidad de datos, etc.

(b) Acceso a la red: es el responsable del intercambio de datos entre el sistema final y la red a la cual se ésta conectado. Puede utilizar diversos estándares para la conmutación de paquetes como ATM, *Frame Relay*, etc.

(c) Internet: es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos

[5] Siglas en inglés: "Defense Advanced Research Projects Agency (DARPA)"
[6] Siglas en inglés: "Transmission Control Protocol (TCP)"

correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

(d) **Transporte**: coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

(e) **Aplicación:** contiene la lógica necesaria para posibilitar las distintas aplicaciones de usuario.

3. Protocolo Internet (IP)

El protocolo IP transporta datagramas entre diferentes redes a través de enrutadores que procesan paquetes desde un sistema autónomo (AS)[7] a otro. Cada dispositivo en el AS tiene una dirección IP exclusiva. El protocolo IP añade su propia cabecera y una suma de comprobación, para asegurarse de que los datos son encaminados correctamente. Este proceso es ayudado por la presencia de mensajes de actualización de encaminamiento, que mantienen las tablas de direcciones actualizadas en cada enrutador. Se utilizan varios tipos de mensajes de actualización, dependiendo del conjunto de subredes incluidas en un dominio de gestión. Las tablas de enrutamiento enumeran los diversos nodos de las subredes, así como los caminos entre los nodos. Si el paquete de datos es demasiado grande para que lo acepte el nodo destino, el nivel superior TCP lo segmentará en paquetes más pequeños.

[7] Siglas en ingles: "Autonomous System (AS)"

4. Protocolo de Control de Transmisión (TCP)

TCP es un protocolo fiable extremo a extremo, orientado a la conexión, que encaja en una jerarquía de niveles de protocolos que soporta aplicaciones multirred. TCP envía los datos que se le entregan en forma de datagramas IP o paquetes al proceso apropiado en el *host* receptor. TCP define los procedimientos para fragmentar los datos en paquetes, recomponerlos en el orden correcto para reconstruir los datos originales en el extremo receptor y emitir peticiones de retransmisión para sustituir los paquetes perdidos o dañados. Como los paquetes suelen tomar rutas diferentes hacia su destino a través de internet, llegan en momentos distintos y sin ninguna secuencia. Todos los paquetes se almacenan temporalmente hasta que llegan los últimos, para poder ponerlos en orden correcto. Si un paquete llega dañado, se descarta y se reenvía otro en respuesta a una petición de retransmisión.

5. Protocolo de Datagrama de Usuario (UDP)

Es un protocolo que permite mandar paquetes a través de la red, no es confiable, es decir no garantiza que los paquetes lleguen en el mismo orden que fueron enviados, y no garantiza que los paquetes lleguen a su destino. Es usado para hacer transmisiones de pequeñas cantidades de datos, para búsquedas sencillas (donde se espera la respuesta en un lapso de tiempo corto). Lo usan algunos algoritmos de compresión de información (audio y video) y aplicaciones que tienen rutinas propias para la comprobación de errores en la recepción y envíos de paquetes.

APENDICE D

ENLACES FISICOS

El protocolo *Bluetooth* utiliza una combinación de conmutación de circuitos y de paquetes.

1 Conmutación de circuitos.

Se usa por ejemplo en redes telefónicas públicas y es la base de res privadas implementadas con líneas dedicadas. La técnica de conmutación de circuitos se desarrolló para tráfico de voz aunque también puede gestionar tráfico de datos.

En la conmutación de circuitos se establece un canal de comunicación dedicado entre dos estaciones. Se reservan recursos de transmisión y de conmutación de la red para su uso exclusivo en el circuito durante la conexión. Esta es transparente, una vez establecida parece como si los dispositivos estuviesen directamente conectados. La conmutación de circuitos puede ser aplicada a redes inalámbricas al igual que ha redes cableadas.

2 Conmutación de paquetes.

En la conmutación de paquetes, una estación realiza la transmisión de los datos en base a pequeños bloques llamados paquetes, cada uno de los cuales contiene una parte de los datos de usuario además de información de control necesaria para el adecuado funcionamiento de la red.

Un elemento clave distintivo de las redes de conmutación de paquetes lo constituye el hecho de que el funcionamiento interno puede basarse en datagramas o en circuitos virtuales internos se define una ruta entre dos puntos de

comunicación finales, de modo que todos los paquetes para dicho circuito virtual siguen el mismo camino. Por su parte, en el caso de los datagramas internos, cada paquete se trata de forma independiente, por lo que los paquetes con el mismo destino pueden seguir rutas diferentes.

La función de encaminamiento de una red de conmutación de paquetes trata de encontrar la ruta de mínimo costo a través de la red. Los algoritmos de encaminamiento adaptable se fundamentan generalmente en el intercambio entre nodos de información relativas a las condiciones de tráfico.

3 Tipos de enlace.

Los dispositivos *Bluetooth* utilizan dos enlaces, el orientado a la conexión y el sin conexión.

3.1 Enlace SCO.

El enlace SCO es un enlace simétrico punto a punto entre el maestro y uno o más esclavos específicos. El enlace SCO suele soportar información ligada al tiempo, como conversaciones de voz. Como el enlace de SCO reserva *slots*, se le considera una conexión de conmutación de circuitos entre el maestro y el esclavo. El maestro establece el enlace SCO enviado un mensaje de establecimiento vía el protocolo gestión de enlace. Este mensaje tiene los parámetros de tiempo y especifica los *slots* reservados.

El maestro puede soportar hasta tres enlaces SCO al mismo esclavo o a diferentes esclavos en una *piconet*. Un esclavo puede soportar hasta tres enlaces SCO del mismo maestro, o dos enlaces SCO si estos se originaron de maestros

diferentes. Como los paquetes transportados por enlaces SCO contienen información sensible desde el punto de vista temporal, nunca se retransmiten si hay errores.

El maestro envía paquetes al esclavo por los enlaces SCO a intervalos regulares, contados en *slots*, en los *slots* reservados para la comunicación. Al esclavo siempre se le permite responder con un paquete en la siguiente franja esclavo/maestro, a menos que la franja maestro/esclavo anterior estuviera dirigida a un esclavo diferente. Si el esclavo no detecta su propia dirección en la cabecera del paquete, todavía se le permite devolver un paquete en el *slots* reservado.

3.2 Enlace ACL.

En los *slots* no reservados para enlaces SCO, el maestro puede intercambiar paquetes con cualquier esclavo por cada *slots*. El enlace ACL ofrece una comunicación de conmutación de paquetes entre el maestro y todos los esclavos activos que participan en la *piconet*. El enlace ACL soporta tanto servicios asíncronos e isócronos pero entre un maestro y un esclavo sólo puede haber activo un enlace ACL. Para la mayor parte de los paquetes ACL, se aplica la retransmisión de paquetes para asegurar la integridad de los datos.

Se permite que un esclavo devuelva un paquete ACL en el *slots* esclavo/maestro sólo si el maestro se ha dirigido a él en el *slots* esclavo/maestro precedente. Si el esclavo no detecta su propia dirección en la cabecera del paquete, no se le permite transmitir. A los paquetes ACL que no están dirigidos a un esclavo específico se les considera paquetes de difusión dirigidos a todos los esclavos. Sino hay datos que enviar a través del enlace ACL y no se requiere sondeo, no tiene lugar ninguna transmisión.

APENDICE E

REDES LAN INALAMBRICAS.

Las LAN inalámbricas son un complemento a las redes cableadas a fin de satisfacer necesidades de movilidad, traslado, trabajo en red *ad-hoc* y cobertura de lugares difíciles de cablear. Estas redes eran poco usadas debido al alto precio, baja velocidad de transmisión, seguridad, etc.

1 Aplicaciones

Se pueden conseguir cuatro grandes aplicaciones: ampliación de redes LAN, interconexión de edificios, acceso nómada y redes *ad-hoc*.

1.1 Ampliación de redes LAN

Una red LAN inalámbrica evita los costos de la instalación del cableado y facilita el traslado y otras modificaciones en la estructura de red, pero ésto no ha evitado el uso de redes LAN cableadas. Sin embargo, una LAN inalámbrica se puede ver como otra alternativa a las redes LAN cableadas, y puede tener múltiples entornos, como serían las fábricas, almacenes, centros comerciales, construcciones históricas donde se evitaría tener que colocar el cableado y así dañar la infraestructura. En estos casos, una LAN inalámbrica ofrece una mejor alternativa. En la mayoría de las situaciones ya se tiene una LAN cableada con servidores y algunas estaciones de trabajo estacionarias. Un caso sería una fábrica, que puede tener una oficina independiente de la fábrica, pero debe estar interconectada a ella con propósitos de trabajo de red. Por lo tanto en muchas

oportunidades una LAN inalámbrica esta conectada con una LAN cableada y a ésto se le denomina ampliación o extensión de redes LAN.

En la figura 1 se muestra una configuración sencilla de una LAN inalámbrica típica en muchos ambientes. Existe una LAN cableada, como una Ethernet, que conecta a varios servidores, estaciones de trabajo y uno o más puentes o dispositivos de encaminamiento para comunicar con otras redes. También existe un módulo de control (CM) que funciona como interfaz con la LAN inalámbrica. El módulo de control incluye funciones de los puentes o de los dispositivos de encaminamiento para conectar a la LAN inalámbrica con la cableada. Además se incluye algún tipo de lógica de control de acceso, para regular la entrada a los sistemas finales.

Algunos de los dispositivos finales son independientes, como estaciones de trabajo y servidores; además los Hub u otros módulos de usuario (UM) que controlan varias estaciones fuera de una LAN cableada pueden también formar parte de la LAN inalámbrica.

La configuración de la figura 1 se denomina LAN inalámbrica de celda única, ya que todos los sistemas finales inalámbricos se encuentran en el dominio de un único módulo de control.

Otra configuración común, se sugiera la de la figura 2, es una LAN inalámbrica de celdas múltiples. En este caso existen varios módulos de control interconectados por una LAN cableada. Cada módulo de control da servicios a varios sistemas finales inalámbricos dentro de su rango de transmisión: por ejemplo, con una LAN de infrarrojos la transmisión está limitada a una sola

habitación, por lo que se necesita una celda en cada habitación de un edificio de oficina con soporte inalámbrico.

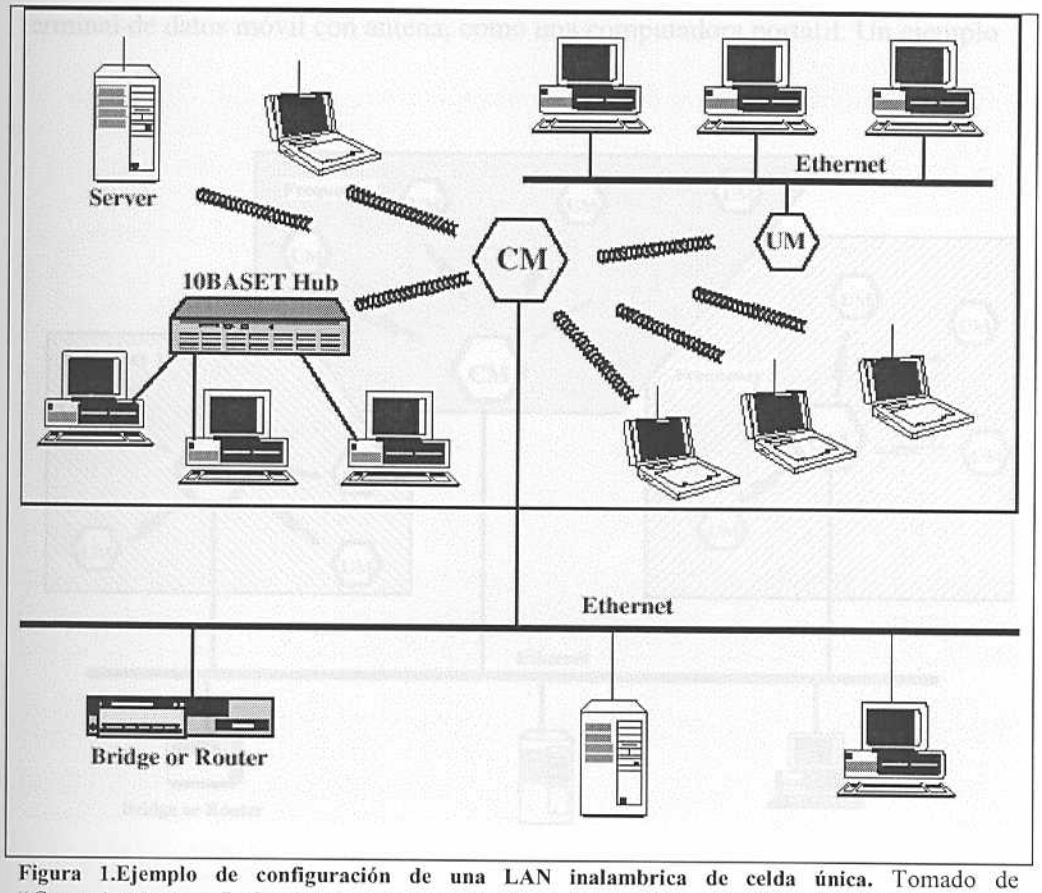


Figura 1.Ejemplo de configuración de una LAN inalambrica de celda única. Tomado de *"Comunicaciones y Redes de Computadores"* (pág 422) por William, S. 2000, Madrid.

1.2 Interconexión de edificios.

Otro uso de las LAN de tecnología inalámbrica es la conexión de redes LAN situadas en edificios vecinos, sean LAN cableadas o inalámbricas. En este caso se usa un enlace no guiado entre dos edificios. Los dispositivos así conectados son generalmente puentes o dispositivos de encaminamiento. Este enlace punto a punto no es en sí mismo una LAN, pero es usual la inclusión de esta aplicación en el contexto de redes LAN inalámbricas.

1.3 Acceso nómada.

El acceso nómada permite un enlace no guiado entre un Hub de LAN y un terminal de datos móvil con antena, como una computadora portátil. Un ejemplo

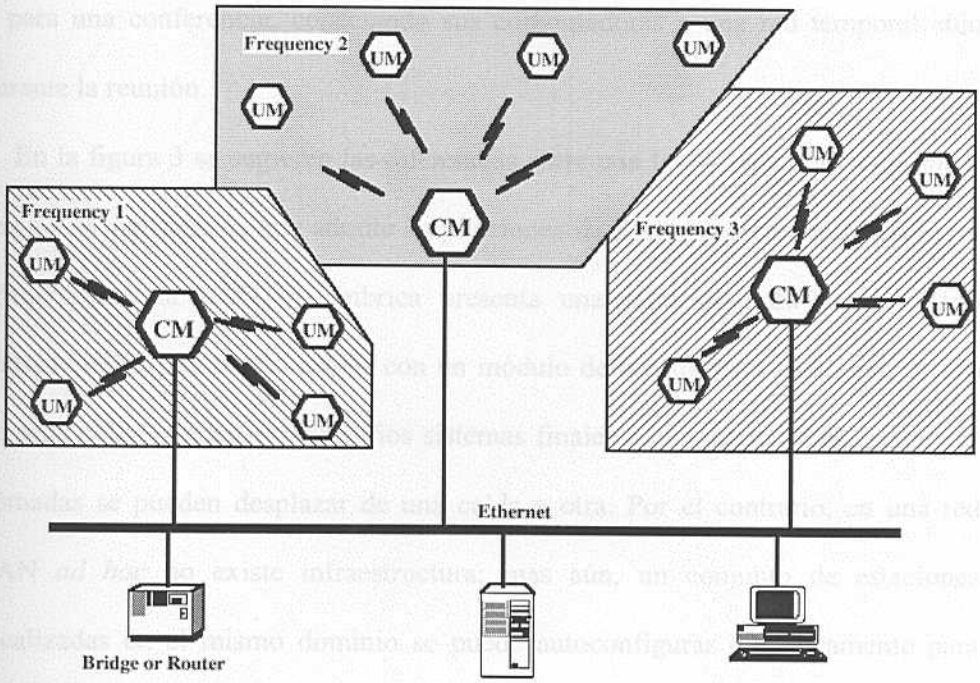


Figura 2.Ejemplo de configuración de una LAN inalámbrica de celda única. Tomado de "*Comunicaciones y Redes de Computadores*" (pág 422) por William, S. 2000, Madrid.

de este tipo de conexiones es posibilitar a un empleado que vuelve de viaje, el poder transferir los datos desde la portátil a un servidor de la oficina. El acceso nómada resulta útil también en un entorno amplio como es un campus universitario o en un centro financiero lejos de un grupo de edificios. En ambos casos los usuarios se pueden desplazar con sus computadoras portátiles y pueden desear conectarse con los servidores de una LAN inalámbrica desde distintos lugares.

1.4 Trabajo en red ad hoc.

Una red *ad-hoc* es una red igual a igual (sin servidor central) establecida temporalmente para satisfacer alguna necesidad inmediata. Por ejemplo, un grupo de empleados, cada uno con su computadora, pueden ir a una reunión de negocios o para una conferencia, conectando sus computadoras a una red temporal sólo durante la reunión.

En la figura 3 se sugieren las diferencias entre una LAN inalámbrica *ad hoc* y una LAN inalámbrica que admite ampliaciones de LAN y acceso nómada. En el primer caso, la LAN inalámbrica presenta una infraestructura estacionaria consistente en una o más celdas con un módulo de control para cada una; dentro de cada celda pueden existir varios sistemas finales estacionarios. Las estaciones nómadas se pueden desplazar de una celda a otra. Por el contrario, en una red LAN *ad hoc* no existe infraestructura; mas aún, un conjunto de estaciones localizadas en el mismo dominio se puede autoconfigurar dinámicamente para formar una red temporal.

2 Requisitos de las LAN inalámbricas.

Una LAN inalámbrica debe cumplir los mismos requisitos típicos de cualquier otra red LAN, incluyendo alta capacidad, cobertura de pequeñas distancias, conectividad total de las estaciones conectadas y capacidad de difusión. Además existe un conjunto de necesidades específicas para entornos de LAN inalámbricas. Entre las más importantes se encuentran las siguientes:

- **Rendimiento:** el protocolo de control de acceso al medio debería hacer un uso tan eficiente como fuera posible del medio no guiado para maximizar la capacidad.

- **Numero de nodos:** las LAN inalámbricas pueden necesitar dar soporte a cientos nodos mediante el uso de varias celdas.

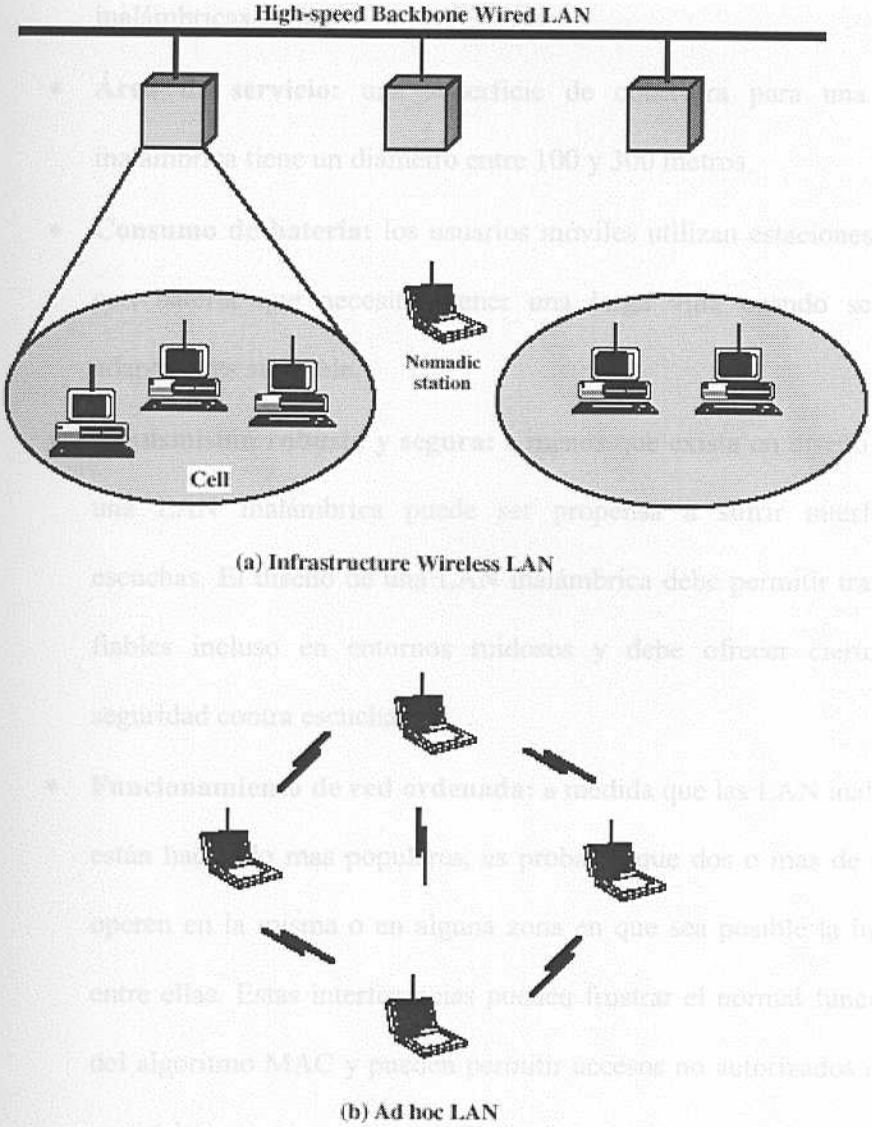


Figura 3.Configuraciones de redes LAN inalámbricas. Tomado de "*Comunicaciones y Redes de Computadores*" (pág 424) por William, S. 2000, Madrid.

- **Conexión a la LAN troncal:** en la mayoría de los casos es necesaria la interconexión con estaciones situadas en una LAN troncal cableada. En el caso de LAN inalámbrica con infraestructura, esto se consigue fácilmente

a través del uso de módulos de control que conectan con ambos tipos de LAN. Puede ser necesario dar soporte a usuarios móviles y redes inalámbricas *ad hoc*.

- **Área de servicio:** una superficie de cobertura para una red LAN inalámbrica tiene un diámetro entre 100 y 300 metros.
- **Consumo de batería:** los usuarios móviles utilizan estaciones de trabajo con batería que necesitan tener una larga vida cuando se usan con adaptadores sin cable.
- **Transmisión robusta y segura:** a menos que exista un diseño apropiado, una LAN inalámbrica puede ser propensa a sufrir interferencias y escuchas. El diseño de una LAN inalámbrica debe permitir transmisiones fiables incluso en entornos ruidosos y debe ofrecer cierto nivel de seguridad contra escuchas.
- **Funcionamiento de red ordenada:** a medida que las LAN inalámbrica se están haciendo mas populares, es probable que dos o mas de estas redes operen en la misma o en alguna zona en que sea posible la interferencia entre ellas. Estas interferencias pueden frustrar el normal funcionamiento del algoritmo MAC y pueden permitir accesos no autorizados a una LAN particular.
- **Funcionamiento sin licencia:** los usuarios podrían preferir adquirir y trabajar sobre LAN inalámbrica que no precisan de una licencia para la banda de frecuencia usada por la red.
- **Sin intervención nómada:** el protocolo MAC usado en LAN inalámbrica debería permitir a las estaciones móviles desplazarse de una celda a otra.

- **Configuración dinámica:** los aspectos de direccionamiento MAC y de gestión de red de la LAN deberían permitir la inserción, eliminación y traslado dinámicos y automáticos de sistemas finales sin afectar a otros usuarios.

APENDICE F

SEGURIDAD *BLUETOOTH*

En las especificaciones de *Bluetooth* se define los diferentes niveles de seguridad para los dispositivos *Bluetooth* y para sus servicios. Las especificaciones *Bluetooth* incluye las características de seguridad que se tienen que implementar en los enlaces, y esto también indica como trabaja la seguridad de *Bluetooth*.

Los perfiles describen como son los modelos de usuario a implementar. Este define las características de cada protocolo, que son mandatorias para un perfil en específico. Esto también define los parámetros para cada protocolo. Los perfiles *Bluetooth* piensan en disminuir los problemas del riesgo de la interoperabilidad sobre los productos desarrollados por diferentes empresas.

En varias especificaciones de los perfiles usan diferentes partes de la pila de protocolo, necesarias para soportar funcionalidades específicas. El perfil de acceso directo GAP, perfil en el cual se basan los demás, define los requerimientos que se usan comúnmente para el transporte y aplicación de los perfiles.

El GAP define tres modos diferentes de seguridad.

1 Modo 1 No seguro.

En el modo 1 de seguridad, el dispositivo no esta seguro. En este modo, el dispositivo nunca inicia un procedimiento de seguridad. Ejemplo de transferencia de datos sin seguridad, es el intercambio de las tarjetas de negocios y calendarios.

2 Modo 2 Seguridad en los niveles de servicios.

La seguridad en el modo 2, el dispositivo no inicia ningún procedimiento de seguridad hasta que se ha enviado la petición de establecer el canal o se ha iniciado el procedimiento de establecer el canal. La seguridad en este caso toma posición por encima del nivel L2CAP, estas son las capas altas de la pila de protocolo. Estos permiten mayor versatibilidad para correr aplicaciones paralelas con diferentes requerimientos de seguridad.

En el modo 2, de acuerdo al GAP, el dispositivo debe clasificar los requerimientos para diferentes servicios (por ejemplo, transferencia de archivo, conexión por dial-up), haciendo uso de al menos uno de los siguientes atributos:

- **Autentificación**: permite a un dispositivo *Bluetooth* verificar la identidad de otro dispositivo antes de permitir el establecimiento de la conexión.
- **Cifrar**: Asegura la integridad de los datos transmitidos, encriptando sistemáticamente cada paquete de datos transmitido al otro dispositivo.
- **Autorización:** le permite a un dispositivo concederle el acceso a un servicio en específico.

3 Modo 3 Seguridad en el nivel de enlace

La seguridad en el modo 3, el dispositivo inicia los procedimientos de seguridad antes de establecer el enlace, en el nivel de establecimiento del enlace (capas bajas de la pila). El enlace de seguridad es más fácil de implementar que el modo 2 de seguridad. Los procedimientos que incluye este nivel de seguridad, se pueden incluir en lo siguiente:

- Crear y usar claves.
- Autentificación de dispositivos.
- Encriptación de paquetes.

Las claves de enlace son usadas para iniciar la autentificación. O, si la clave del enlace aun no ha sido creada, el procedimiento de emparejamiento toma lugar, el cual crea una clave. Una clave de encriptación es usada para los procesos de encriptación.

La autentificación es el proceso de identificar la identidad del dispositivo con el cual se quiere establecer la conexión. La encriptación es el proceso de codificar la información para la transmisión entre dispositivos, asegurando la integridad.

4 La seguridad en la pila de protocolos de *Bluetooth*.

Bluetooth hace cumplir diferentes protocolos de seguridad en diferentes niveles de la pila de *Bluetooth*. Cuando el dispositivo esta en modo 2 de seguridad, el protocolo se cumple en la capas altas de la pila. En el modo 3 de seguridad, los protocolos se cumplen en las capas bajas, en el nivel de enlace. Cada modo de seguridad usa una parte de la pila de protocolo que da soporte a los procedimientos específicos de seguridad requeridos, como lo indica la figura siguiente.

4.1 Protocolo del nivel de enlace.

El modo 3 de seguridad hace cumplir la encriptación y autentificación. El protocolo de seguridad está definido en las especificaciones de *Bluetooth*, hace uso de cuatro elementos para la autentificación y encriptación de la información:

- Dirección del dispositivo *Bluetooth* (BD_ADDR)[8]: dirección de 48 bits, y es única para cada dispositivo *Bluetooth*.

[8] Siglas en ingles: "Bluetooth device address"

- Clave privada de enlace: es un número aleatorio de 128 bits, con el propósito de ser usado para la autentificación.

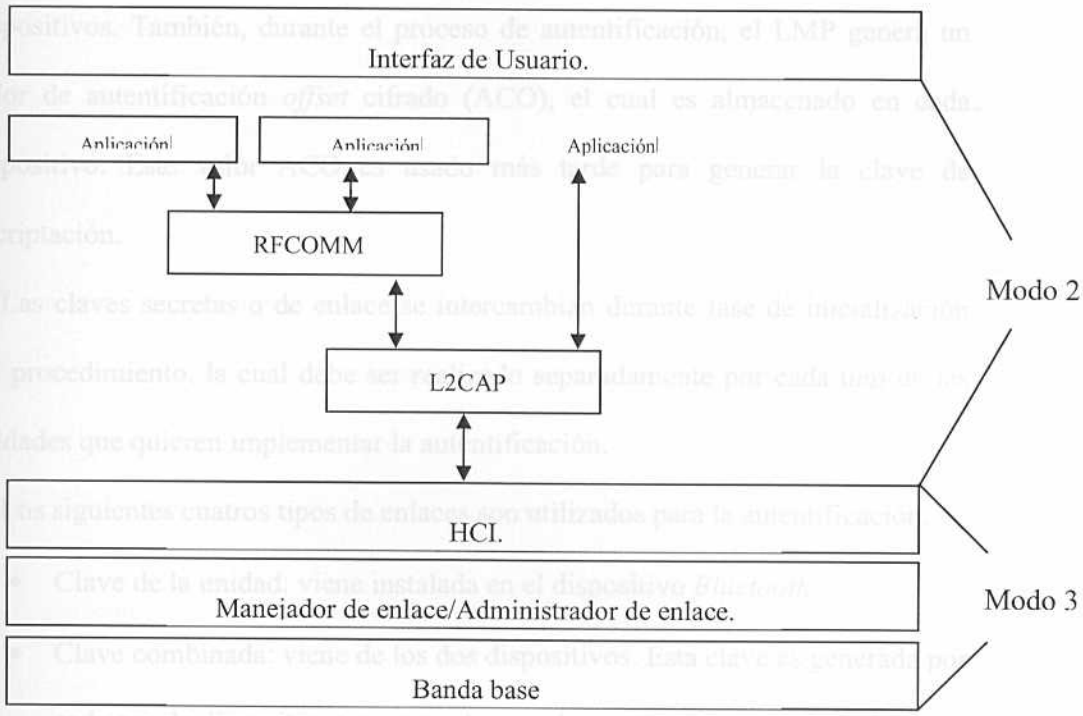


Figura 4. Pila de protocolos. Tomado de "*Bluetooth End to End*" (pág 265) por D.M Bakker y Diane Gilster, 2002, New York.

- Clave privada de encriptación de 8-128 bits, usada para encriptar la información.
- Numero random (RAND): cambiando frecuentemente, es de 128 bits, es un número semi-aleatorio o aleatorio, y es creado por el mismo dispositivo *Bluetooth*.

4.1.1 Protocolos de autentificación.

La autentificación es en LMP, y que verifica la identidad de un dispositivo remoto antes de establecer la conexión. Una segunda parte del protocolo es de dar

respuesta a una estrategia en la cual un dispositivo impone al otro, que determine que es el correcto, compartiendo una clave secreta, requerida para establecer la conexión. Si la autentificación es exitosa, el enlace es establecido entre los dispositivos. También, durante el proceso de autentificación, el LMP genera un valor de autentificación *offset* cifrado (ACO), el cual es almacenado en cada dispositivo. Este valor ACO es usado más tarde para generar la clave de encriptación.

Las claves secretas o de enlace se intercambian durante fase de inicialización del procedimiento, la cual debe ser realizado separadamente por cada uno de las unidades que quieren implementar la autentificación.

Los siguientes cuatros tipos de enlaces son utilizados para la autentificación:

- Clave de la unidad: viene instalada en el dispositivo *Bluetooth*.
- Clave combinada: viene de los dos dispositivos. Esta clave es generada por cada par de dispositivos y es usada cuando se necesita más seguridad.
- Clave maestra: es usada cuando el dispositivo maestro quiere transmitir a todos los dispositivos inmediatamente. Sobrescribiendo la clave del enlace actual por la sesión actual.
- Clave de inicio: es usada en el proceso de inicio y para proteger los parámetros de inicialización cuando se transmiten.

Todas las claves de enlace son un número aleatorio de 128 bits y pueden ser permanentes o semipermanentes.

Vista general de como se permite el procedimiento de autentificación:

(1) Las unidades envían al solicitante (dispositivo remoto) el numero aleatorio (RAND) para ser autentificado.

(2) El verificador y el que solicita el uso de la función de autentificación (esto esta fuera de las especificaciones *Bluetooth*) con el RAND, la BD_ADDR del solicitante, y la clave de enlace actual para producir una respuesta.

(3) El solicitante envía una respuesta al verificador.

(4) Si la unidad esta verificando y determina que las respuestas coinciden, la autentificación es exitosa.

Porque cada aplicación puede indicar a cual unidad puede autentificar, la unidad maestra obliga a no ser verificador. Algunas aplicaciones sólo requieren de un camino de autentificación en vez de que sea en ambos sentidos. La siguiente figura muestra el diagrama de flujo de la autentificación.

Procedimiento de Emparejamiento.

Si no existe una clave de enlace, el procedimiento de emparejamiento es usado para autentificar a dos dispositivos, basado en los códigos de seguridad de *Bluetooth*, y a esto se le denomina PIN. Posteriormente una clave de enlace común es creada. El usuario no tiene que memorizar el PIN, porque este es usado sólo una vez para crear la clave de enlace. Si se borrara la clave de enlace, y el emparejamiento se debe repetir, el usuario puede entrar con otro PIN. Sin embargo, algunos dispositivos pueden tener un PIN asignado, en la cual la interacción con el usuario no es requerida.

El procedimiento de emparejamiento puede usarse para una sola conexión segura, o esta puede ser la base para crear una conexión confiable ente los dispositivos.

Las especificaciones del GAP definen dos modos de emparejamiento:

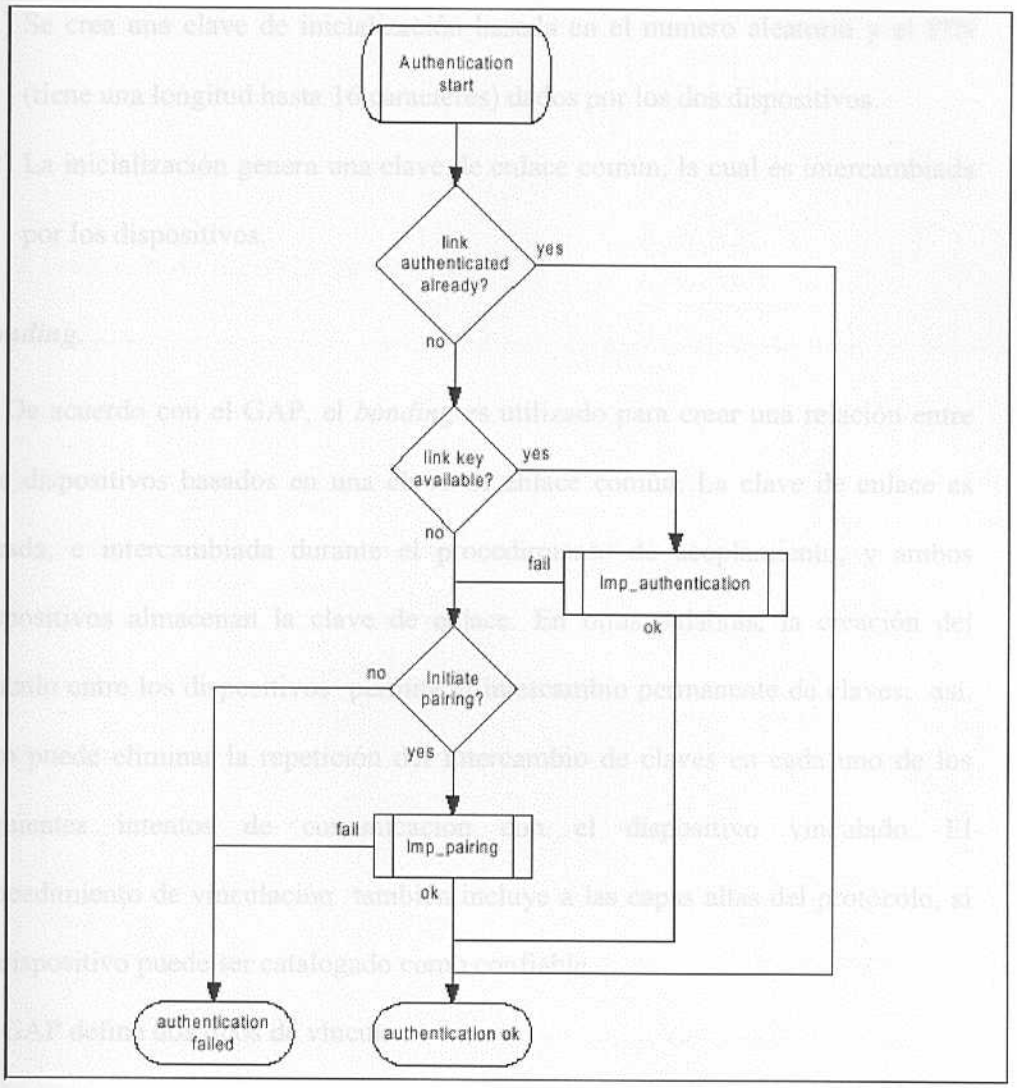


Figura 5. Diagrama de Flujo para el procedimiento de autentificación. Tomado de "*Especification of the BLuetooth System Profiles" parte* K1, pág 35, 2001.

emparejamiento y no emparejamiento. En el modo de emparejamiento el dispositivo acepta el inicio del emparejamiento del dispositivo remoto. En el otro modo, no se acepta el emparejamiento cuando es iniciado por el dispositivo remoto.

Los protocolos de emparejamiento trabajan como se explica a continuación:

(1) Se crea una clave de inicialización basada en el numero aleatorio y el PIN (tiene una longitud hasta 16 caracteres) dados por los dos dispositivos.

(2) La inicialización genera una clave de enlace común, la cual es intercambiada por los dispositivos.

Bonding.

De acuerdo con el GAP, el *bonding* es utilizado para crear una relación entre dos dispositivos basados en una clave de enlace común. La clave de enlace es creada, e intercambiada durante el procedimiento de acoplamiento, y ambos dispositivos almacenan la clave de enlace. En otras palabras, la creación del vínculo entre los dispositivos permite el intercambio permanente de claves; así, esto puede eliminar la repetición del intercambio de claves en cada uno de los siguientes intentos de comunicación con el dispositivo vinculado. El procedimiento de vinculación también incluye a las capas altas del protocolo, si el dispositivo puede ser catalogado como confiable.

El GAP define dos tipos de vínculos:

- Vinculación dedicada: ocurre cuando dos dispositivos sólo quieren crear e intercambiar una clave de enlace común.
- Vinculación general: en el proceso de establecer el enlace, realizado por ambos dispositivos bajo unas condiciones especificas, la cual es seguido del proceso de inicialización de las capas superiores, esto es opcional (estableciendo un conexión confiable).

De acuerdo con las especificaciones, el proceso de vinculación realiza la primera autentificación cuando se crea la clave de enlace y la almacena para ser usada en un futuro. El emparejamiento, como en el LMP-emparejamiento, es el

procedimiento que autentifica a dos dispositivos utilizando el PIN pero también crea una clave de enlace común que es usada como la base para una relación confiable o una conexión segura simple.

4.1.2 Protocolo de encriptación.

La encriptación es un proceso de codificar la información de usuarios para protegerla en el contenido de los paquetes y asegurar la integridad durante la conexión. La autentificación permite tomar lugar antes de que se pueda implementar la encriptación. La encriptación depende la clave de encriptación, la cual proviene de la clave de enlace actual (intercambiada durante la autentificación). Cada vez que se necesita el cifrado, el servicio de cifrado de LMP cambia automáticamente la clave de cifrado. Construyendo la clave de autentificación y la clave de cifrado por entidades distintas, esto significa que los dispositivos *Bluetooth* pueden hacer uso de una clave de cifrado corta sin debilitar al proceso de autentificación.

La clave de cifrado puede tener un tamaño que varia desde los 8 hasta 128 bits; por lo tanto el tamaño de la clave de cifrado usada entre los dispositivos debe ser negociado. Tanto el maestro o el esclavo pueden proponer o rechazar el tamaño de la clave sugerida por el otro dispositivo.

En algunos lugares de las especificaciones de *Bluetooth* los límites son negociados. Sin embargo, cada dispositivo tiene definido el tamaño máximo de la clave. También, cada aplicación define el tamaño mínimo aceptable de la clave. Si otro participante falla en la negociación del tamaño de la clave para satisfacer los requerimientos mínimos, la aplicación detiene la negociación y los dispositivos no

pueden usar el cifrado. Esto es un requisito necesario porque existe la posibilidad de que un dispositivo malicioso quiera forzar el cifrado y así hacer daño.

Para realizar el procedimiento de cifrado se siguen los siguientes pasos:

(1) La autentificación establecida entre dos dispositivos es exitosa.

(2) La clave de cifrado es negociada entre los dispositivos, y proviene de la clave de enlace.

(3) Después que se llegue a un acuerdo en el tamaño de la clave, la clave de cifrado es creada.

(4) Si la clave de enlace usada es semipermanente, sólo las transmisiones punto a punto son cifradas, las multidifusiones no necesitan el cifrado. Si la clave del maestro es usada, todas las transmisiones pueden cifrar, dependiendo del modo de cifrado.

(5) El cifrado es implementado sistemáticamente para usarse en la transmisión de datos.

4.2 Protocolos del nivel de servicio.

Si el procedimiento de seguridad es iniciado o no, depende de los requerimientos de seguridad solicitados por el canal o el servicio. En otras palabras, sin un dispositivo solicita un canal de otro dispositivo que requiere la autentificación y cifrado, la petición del dispositivo debe proveer la información necesaria. Similarmente, si un dispositivo solicita el acceso de un servicio de otro dispositivo, se debe aplicar los procedimientos apropiados de seguridad.

En el modo de seguridad 2, el dispositivo no puede iniciar ningún procedimiento de seguridad antes que cualquier dispositivo tenga la solicitud del

canal, o el mismo dispositivo inicia la solicitud del canal. Esto se cumple en la capa L2CAP y por encima de ella.

4.2.1 Autentificación y autorización.

Dos conceptos claves en la seguridad de *Bluetooth* son la autentificación y autorización.

De acuerdo al GAP, un dispositivo en el modo 2 podría clasificar los servicios de requerimientos de seguridad como los siguientes:

- Requerir sólo autentificación.
- Requerir autentificación y autorización.
- No se requiere ni autentificación ni autorización, los servicios están habilitados a todos los dispositivos.

4.2.2 Designación de la seguridad a los niveles del dispositivo.

Diferentes niveles de seguridad pueden ser definidos para los dispositivos y servicios. Esta característica proveerá de una futura flexibilidad para la arquitectura de seguridad, habilitando a un dispositivo a tener el acceso a todos diferentes servicios basado en la seguridad asignada al otro dispositivo.

De acuerdo a la especificación de *Bluetooth*, los dispositivos pueden diseñarse de la siguiente manera:

- Confiable: un dispositivo confiable, puede dar acceso ilimitado a todos los servicios de otro dispositivo. Un dispositivo puede ser designado como confiable después que el emparejamiento o vinculación ha ocurrido. Los servicios que puede tener permitido son: transferencia de archivo, sincronización, red de marcado manual.

- Desconfiable: un dispositivo es desconfiable si sólo tiene acceso limitado a servicios o le puede ser negado los servicios.
- Desconocido: un dispositivo desconocido es un dispositivo *Bluetooth* el cual no tiene información (como nombre, dirección, *passkey*) habilitada. Esto es esencial para un dispositivo desconfiables.

4.2.3 Designación de seguridad de los niveles de servicio.

Para los servicios, los requerimientos para la autorización, autentificación y cifrado se asignan por separado. Los requerimientos específicos para el acceso del GAP permiten definir tres niveles de seguridad:

- Requiere de autorización: este nivel de seguridad también requiere de autentificaron en orden para verificar que dispositivo remoto es, de hecho, el solicitante puede ser. Después del proceso de autorización, sólo a los dispositivos confiables se le concede el acceso a los servicios automáticamente. Sin embargo, porque un dispositivo desconfiable no puede crear conexiones fijas, esto puede conceder acceso a los servicios sobre una base limitada.
- Requiere autentificación: sólo el dispositivo remoto necesitan ser autentificados antes de que la aplicación se conecte.
- Requiere de cifrado: el enlace debe cambiar el modo de cifrado antes de conceder el acceso al servicio solicitado.

5 Puntos fuertes de la seguridad *Bluetooth*.

Dos criterios para medir la fuerza de los sistemas de seguridad son la usabilidad y flexibilidad. Un sistema debe ser flexible para acomodar las varias

un bajo nivel de seguridad. En las conexiones existentes, las configuraciones de seguridad alta pueden sobrescribir la configuración de baja seguridad.

6 Limitaciones de la seguridad de *Bluetooth*.

Si en situaciones normales y redes *ad hoc*, muchas de las redes son victimas de ataques realizados por terceros. En las áreas en la cual la computación puede defenderse, se muestra en las siguientes categorías:

- Acceso: la información se perdió y esta en manos de un tercero.
- Integridad: no se autoriza en intercambio de información.
- Negación de servicio: el acceso a la red es bloqueado por terceros.

En términos de la integridad de los datos y el acceso, las redes *Bluetooth* son vulnerables en las siguientes áreas:

- Entrar y almacenar el PIN: el código del PIN puede usarse en combinación con otras variables para generar las claves de cifrado y enlace. Para realizar esto, los usuarios tienen que introducir los cuatro dígitos y transmitirla a cada uno de los otros usuarios. El hecho de que esta transmisión es hecha en el aire hace que sea vulnerable. Ambos usuarios finales necesitan introducir este número para iniciar una conexión segura, ellos pueden querer guardar la información del PIN en ambos dispositivos, para evitar en varias ocasiones la introducción del número para cada intento de conexión o ellos quieren usarlo para recordar fácilmente el número. Si se pierde o es robado el dispositivo, almacenar el número puede ser un problema. También es fácil recordar y descubrir los números por terceros. Ambas situaciones plantean un riesgo de la integridad de los datos que están siendo transmitidos.

- Usando la clave de enlace: la autentificación y cifrado están basado en la clave de enlace, y sólo las unidades participantes en la conexión pueden compartir la clave de enlace. Sin embargo, la clave de enlace puede basarse en la clave de un dispositivo, la cual nunca cambia. Si el dispositivo A y B se comunican basándose en la clave de A y luego se comunica con C usando la clave de A, entonces el dispositivo B puede usar la clave de A para descifrar la comunicación entre A y C porque B sabe la clave de A. Para hacer esto B tiene que falsificar la BD_ADDR para calcular la clave de cifrado.
- Dirección del dispositivo *Bluetooth*: cada unidad tiene una dirección de dispositivo única que lo distingue de los demás. La misma unicidad de las direcciones, sin embargo esto es vulnerable. Después que la dirección es asociada a una persona, la persona puede ser rastreada, y monitorear sus actividades, por lo tanto robarse la dirección del dispositivo.

Las redes *Bluetooth* también pueden ser vulnerable a los ataques de negación de servicio, porque todos los dispositivos de una red *ad hoc* dependen de los otros para retransmitir los mensajes y porque toda la información transmitida en el aire. Los usuarios no autorizados pueden intentar congestionar la red y esto evita el flujo de la información entre las unidades. También, porque las unidades *Bluetooth* confían en el poder de la batería para su operación, un intruso puede intentar incrementar el consumo de poder en la unidad y terminar con la vida útil de la misma.

Varios de los problemas aun se pueden solucionar con los procedimientos de seguridad, particularmente si se quiere expandir a una red de área amplia. El

concepto original de *Bluetooth* era para redes de área personal, no para redes de área amplia. Para redes de área personal, en el cual el rango de cobertura es de 10 metros, la seguridad es deseable pero no necesariamente esencial.

7 Protección de un dispositivo *Bluetooth*.

En la actual arquitectura, se tiene muchas maneras de proteger el dispositivo *Bluetooth* de amenazas de seguridad. Los usuarios que necesitan transmitir una información sensitiva pueden invocar a un modo de seguridad más riguroso. Esto significa que utilizando el modo 2 de seguridad y requiriendo la autentificación, cifrado y autorización cuando un dispositivo se comunica con otro.

Los usuarios pueden crear una relación confiable entre unos dispositivos seleccionados. Este camino, cuando los datos son transmitidos, debe asegurar a los usuarios que sólo un dispositivo confiable tiene permitido recibir la información.

Cuando se crea una red *ad hoc* sobre los dispositivos, manteniendo una red pequeña y un área segura, por ejemplo en un cuarto de conferencias, se provee protección para que terceros usuarios no tengan acceso. El rango de cobertura de *Bluetooth* es sólo de 10 metros, y muchos de los *hackers* prefieren estar alejados de sus victimas.

También se puede proteger los datos usando claves específicas para cifrar el tráfico. Por ejemplo, cuando se usa una clave combinada con cada esclavo en la red. Por lo tanto, cuando un esclavo envía una información a otro esclavo debe pasar por el dispositivo maestro. En este sentido, la unidad maestro tiene mayor control sobre el origen y destino de los datos.

Requerir la autentificación en ambos sentidos, es otro medio de protección de la información (pero no del dispositivo). En esta situación, ambos dispositivos deben introducir su clave secreta, así como verificar que la información de la clave recibida es la correcta. La autentificación mutua disminuye la probabilidad de que dispositivos desconocidos puedan establecer una conexión.

Los usuarios de mecanismos para seleccionar los PINs que sean fáciles de recordar y cortos. Mientras mas largo sea el número, es mas único, y menos probable que sea descubierto por terceros.

8 Aplicación de la seguridad *Bluetooth*.

El área de la seguridad sigue siendo sobre la cual los desarrolladores deben poner mayor énfasis para ganar la aceptación de los mercados. Claro, la gran preocupación en todas las comunicaciones inalámbricas. Sin embargo, porque la autentificación es de dispositivos y no de usuarios, existe la posibilidad de tener brechas de seguridad.

Por ejemplo, si se usa un teléfono celular *Bluetooth* para llamar a un amigo que tiene su teléfono celular *Bluetooth*, el proceso de autentificación utiliza una clave secreta de cifrado para saber cuales son los participantes en la conexión. Porque se quiere mantener una conversación segura, se usa la clave secreta del amigo. Un día más tarde, otro amigo llama y usted usa la clave secreta otra vez. El amigo ahora tiene la otra clave, y usa una dirección de dispositivo falsa (comúnmente 0000) y el método de cifrado estándar, ahora puede escuchar las conversaciones del otro teléfono celular o disfrazarse como el otro teléfono.

8.1 Comunicaciones seguras con *Bluetooth*

En la mayoría de los casos, y especialmente los que incluyen los usuarios de la tecnología *Bluetooth* en las WPAN, las características de seguridad de *Bluetooth* proveen los niveles de seguridad requerido. La seguridad de *Bluetooth* tiene sus debilidades.

Las aplicaciones en las cuales no es probable la seguridad, se incluyen:

- Los dispositivos periféricos *Bluetooth* para computadoras, como el ratón, impresoras, teclados, escáner.
- Acceder a los correos electrónicos, desde un teléfono móvil o PDA conectado vía *Bluetooth* con un enlace a una computadora portátil.
- Encontrar una impresora conveniente en el lobby del hotel, o en el salón de conferencias e imprimir un documento desde tu computadora portátil, sin la necesidad de tener un cable. De la misma manera encontrar fax y otros dispositivos.

8.2 Realizar acuerdos con *ad hoc*

Cuando se crea una red *ad hoc* en un lugar de la oficina como en el cuarto de conferencia, dos métodos son permitidos para asegurar la conexión, de modo que nadie que este afuera de la sala de conferencia puede escuchar la reunión. El primer método, el maestro crea una clave combinada para cifrar los datos y enviarlos entre los dispositivos. En este método el maestro crea la clave combinada con cada uno de los dispositivos esclavos en la red *ad hoc*, lo cual permite enviar cualquier información de un esclavo a todos los demás pasando por el maestro.

El segundo método de la seguridad de redes *ad hoc* es usar la clave del maestro, lo cual permite a todos los dispositivos en la red usar la misma clave de cifrado de información y transmitirla por la red, sin la necesidad de que lo retransmita el maestro. Además de estos dos métodos, las redes *ad hoc* deben protegerse usando programas de aplicación de niveles.

APÉNDICE G

MODOS

1 Modo de descubrimiento.

Los dispositivos *Bluetooth* pueden estar en el modo descubrible o en el modo no descubrible. Hay dos modos descubrible: limitado y general.

(1) Modo Descubrible Limitado: se pone así mismo en estado disponible (para los otros dispositivos) solamente durante un período de tiempo limitado, mientras se dan unas determinadas condiciones temporales o para un suceso determinado. El dispositivo se pone en estado disponible pasando periódicamente a un estado de búsqueda, en el que comprueba la aparición de ciertos tipos de códigos de indagación. En tales ocasiones, puede responder a otro dispositivo *Bluetooth* que realice una indagación limitada utilizando un código especial denominado código de acceso de indagación limitada (LIAC, *Limited Inquiry Access Code*).

(2) Modo Descubrible General: cuando un dispositivo se encuentra en este modo, esta disponible continuamente y puede responder a otro dispositivo *Bluetooth* que realice una indagación general utilizando otro código especial llamado código de acceso de indagación general (GIAC, *General Inquiry Access Code*). Sin embargo, un dispositivo puede estar solamente en un modo descubrible cada vez: o limitado o general. Incluso cuando un

dispositivo *Bluetooth* sea descubrible, puede ser incapaz de responder a una indagación debido a otras actividades de banda base que se estén produciendo en ese momento.

Cuando un dispositivo *Bluetooth* está en modo no descubrible, no responde a ninguna indagación.

2 Modo de conectividad.

Con respecto a la búsqueda, un dispositivo *Bluetooth* puede estar tanto en modo conectable como en modo no conectable. La búsqueda es un procedimiento que implica la transmisión de una serie de mensajes con el objetivo de configurar un enlace de comunicación con una unidad activa situada dentro del área de cobertura. Cuando un dispositivo *Bluetooth* esta en modo conectable, se coloca así mismo en un estado de búsqueda. Si recibe un mensaje de búsqueda, puede responder. Cuando un dispositivo *Bluetooth* está en modo no conectable, no llega a entrar en el estado de exploración de búsqueda. Como no puede recibir mensajes de búsqueda, no los puede responder.

3 Modo de Emparejamiento.

El emparejamiento es un procedimiento de inicialización por el cual dos dispositivos que se están comunicando por primera vez crean una clave de enlace común que será utilizada para poder realizar la autentificación. Para la primera conexión, el emparejamiento requiere que el usuario introduzca un código de seguridad *Bluetooth* o PIN. Los dispositivos *Bluetooth* deben estar o en modo de emparejamiento o modo no emparejamiento. Cuando está en modo de

emparejamiento, acepta el emparejamiento iniciado por el dispositivo remoto, mientras que el otro modo no lo acepta.

4 Procedimientos del modo de inactividad

Hay varios procedimientos del modo de inactividad que pueden ser iniciados por un dispositivo *Bluetooth* y dirigidos a otro dispositivo *Bluetooth* remoto.

Tabla 1
Procedimientos del modo inactivo.

	Procedimiento	*Soportado*
1	Indagación General	C1
2	Indagación Limitada	C1
3	Descubrimiento de Nombres	O
4	Descubrimiento de dispositivos	O
5	*Bonding* (Ver Apéndice F)	O

C1: Si la iniciación del *Bonding* es soportada, al menos un procedimiento de indagación es obligatorio, de otra manera es opcional.

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

4.1 Indagación General

El procedimiento de indagación general proporciona al dispositivo *Bluetooth* demandante la dirección de dispositivo *Bluetooth*, el reloj, la clase de dispositivo y el modo de exploración de búsqueda de los dispositivos descubribles generales. Aquellos dispositivos que se en encuentren dentro del radio de acción del dispositivo iniciador pueden configurarse para realizar exploraciones con el fin de detectar mensajes de indagación con el código de acceso de indagación general

(GIAC). Todos los dispositivos en el modo descubrible general son descubiertos mediante el procedimiento de indagación general

4.2 Indagación Limitada

El procedimiento de indagación limitada proporciona al dispositivo iniciador la dirección del dispositivo *Bluetooth*, el reloj, la clase de dispositivo y el modo de exploración de búsqueda de los dispositivos que se encuentren en el modo descubrible limitado. Aquellos dispositivos que se encuentren dentro del radio de acción del dispositivo iniciador pueden configurarse para realizar exploraciones con el fin de detectar mensajes de indagación con el código LIAC, además del GIAC. Ya que no esta garantizado que el dispositivo descubrible realice exploraciones para detectar los mensajes LIAC, el dispositivo iniciador puede elegir entre el procedimiento de indagación general o limitada.

4.3 Descubrimiento de Nombres

El objetivo es proporcionar al dispositivo iniciador el nombre de otros dispositivos con los que pueda conectarse, es decir, los dispositivos que se encuentran en el radio de acción que vayan a responder a los mensajes de búsqueda. El descubrimiento es un procedimiento que permite obtener el nombre de los dispositivos *Bluetooth* accesibles, que se basa en dirigir las solicitudes a dispositivos *Bluetooth* conocidos, para los cuales está disponible la dirección de dispositivo.

Un procedimiento relacionado es la solicitud de nombre, que también se utiliza para obtener los nombres de dispositivo de las unidades *Bluetooth* accesibles. No es necesario que se realice un establecimiento completo del enlace para obtener el

nombre del otro dispositivo. En este procedimiento el dispositivo iniciador utiliza el código de acceso a dispositivo de la unidad remota, que habrá sido obtenido de antemano mediante un procedimiento de indagación.

4.4 Descubrimiento de dispositivo

El propósito es darle al dispositivo iniciador la dirección, el reloj, la clase de dispositivo, el modo de operación de búsqueda y el nombre de dispositivo de las unidades *Bluetooth* descubribles. Durante el procedimiento, se realiza una indagación general o limitada, seguida por un descubrimiento de nombre dirigido hacia alguno o todos los dispositivos que respondan la indagación.

APENDICE H

REQUERIMIENTOS DE INTEROPERABILIDAD DE RFCOMM.

En esta sección se describe los requerimientos del RFCOMM, que deben conformar las unidades con el perfil del puerto serial.

Tabla 2
Capacidades de RFCOMM

Procedimiento	*Capacidad de iniciar*		*Capacidad de responder*	
	Dev A	**Dev B**	**Dev A**	**Dev B**
Iniciar sesión de RFCOMM	SI[1]	NO[1]	NO[1]	SI[1]
Terminar sesión de RFCOMM	SI	SI	SI	SI
Establecer DLC	SI	NO[1]	NO[1]	SI
Desconectar DLC	SI	SI	SI	SI
Control de señales RS232	C[1]	C[1]	SI	SI
Transferencia de información	SI	SI	N/A[1]	N/A[1]
Evaluar comandos	NO	NO	SI	SI
Control de flujo agregado	SI[2]	SI[2]	SI	SI
Indicación del estatus de la línea remota	NO	SI	SI	SI
negociación de los parámetros DLC	NO	SI	SI	SI
negociación del puerto remoto	NO	SI	SI	SI

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

SI[1]: Capacidad de tener más de una sesión RFCOMM operando concurrentemente, esto es opcional en el protocolo RFCOMM. Aunque se puede animar a dar soporte a la concurrencia, donde tenga sentido hacerlo, las

especificaciones del SIG no lo hacen mandatorio, pero este modelo de Punto de Acceso contempla sesiones RFCOMM concurrentes en los dispositivos.

NO[1]: Con la ejecución de los roles definidos en el modelo, esta capacidad no se usará.

N/A[1]: La información transferida no es reconocida en el protocolo RFCOMM.

SI[2]: Con los mecanismo de control de flujo para utilizar (por DLC, agregado, o ambos) en esta implementación. Algunos de los procedimientos serán comentados en las secciones futuras.

1 Señales de Control RS232

Concuerda con TS 07.10, todos los dispositivos requieren enviar información dentro de todos los cambios de señales en el RS232, con el comando de estatus del MODEM.

Sin embargo, desde que se puede usar RFCOMM con la capa de adaptación, implementando algún tipo de API (no solamente el puerto serial virtual), ésto es opcional para el uso del control de señales RS232, excepto el control de flujo (la señal RTR en TS 07.10). Esta señal puede rastrear en RTS/CTS o XON/XOFF u otro mecanismo del API, la cual es implementada en esta edición.

Nota Informativa: para proveer la interoperabilidad entre los dispositivos, actualmente se usan todos los controles de señal RS232, y los dispositivos que no lo usan, el tipo anterior de implementación es necesario para el sistema de estados de señales apropiados en API/conectores para los valores por defecto convenientes, dependiendo del estado del RFCOMM. La implantación básica no confía en recibir ningún control de información RS232 del par de dispositivos. La dependencia en el estado DLC RFCOMM puede significar que el DSR/DTR así

como DCD se fija en el mayor nivel cuando el DLC RFCOMM se ha establecido, y que las señales del mismo se fijan al bajo nivel, si corresponden al cierre del DLC por alguna razón.

2 Indicación del estatus de la línea remota.

Se requiere para informar a otro dispositivo de algún cambio en la línea de estatus del RS232 con el comando de indicación del estatus de la línea remota. Si el dispositivo local retrasa la información desde el puerto serial física (o equivalente) donde tramas con errores pueden ocurrir.

3 Negociación del puerto remoto.

El Dev A puede informar al Dev B de los ajustes del RS232 con el comando de negociación del puerto remoto, directamente antes del establecimiento del DLC. Hay requerimientos para hacer si el API para RFCOMM, expone los ajuste en la capa de adaptación.(ejemplo velocidad , paridad)

El Dev B permite enviar el comando de negociación del puerto remoto.

Nota informativa: la información transportada en el procedimiento de negociación del puerto remoto, espera ser útil sólo en los dispositivos tipo II (con el puerto serial físico) o si al establecer el paso de la data, se hace la interfaz de emulación del puerto serial por alguna razón.

APENDICE I

REQUERIMIENTOS DE INTEROPERABILIDAD DE L2CAP.

La siguiente tabla junto con las sub-cláusulas que le siguen establecen los requerimientos mandatorios, que cumple el modelo de Punto de Acceso.

Tabla 3
Procedimientos L2CAP

	Procedimiento	*Soportado en DevA/DevB*
1	Tipos de canal.	
	Canal orientado a la conexión.	SI
	Canal sin conexión	NO
2	Señalización.	
	Establecimiento de conexión.	SI
	Configuración.	SI
	Terminar conexión.	SI
	Echo.	SI
	Comando de Rechazo.	SI
3	Opciones del parámetro de configuración.	
	Unidad de transmisión Máxima.	SI
	Flush Timeout	SI
	Calidad de servicio.	NO

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

1 Tipos de canal.

En este perfil, sólo los canales orientados a conexión pueden usarse. Eso implica que la difusión no se utilizara en este perfil.

En el campo PSM del paquete de búsqueda de conexión, el valor para el RFCOMM definido en el documento de Asignación de Números, es 0x0003[9].

2 Señalización.

Sólo el Dev A puede publicar la búsqueda de la conexión en L2CAP con la ejecución de este perfil. Con la excepción del perfil del puerto serial, que no impone ninguna restricción adicional o la señalización en L2CAP.

3 Opciones de configuración.

Se describe en esta sección el uso de las opciones de configuración del perfil del puerto serial.

3.1 Unidad de transmisión máxima.

En este perfil no se impone ninguna restricción en el tamaño de la MTU además de las restricciones del estado en L2CAP.

3.2 *Flush Timeout.*

La data del puerto serial es transportada sobre el canal L2CAP confiable. El valor del *Flush timeout* puede ser fijado con el valor por defecto 0xffff.

3.3 Calidad de servicio.

La negociación de la calidad de servicio es opcional en este perfil. Recomendación: se podría intentar implementar mantener un límite superior de 500 milisegundos, en el estado latente incurrido cuando regresa desde el modo de bajo poder al modo activo.

[9] Ver el valor en el documento de Asignación de Números.

APENDICE J

REQUERIMIENTO DE INTEROPERABILIDAD DEL GESTOR DE ENLACE (LM)

1 Descripción general de la capacidad

En adición, a los requerimientos que son soportados por el mismo Manejador de Enlace, en los estados de procedimientos, este perfil también requiere soporte para el cifrado en ambos dispositivos.

2 Error de comportamiento.

Si una unidad quiere usar las características mandatorias, y la otra unidad responde que no lo soporta, la unidad iniciadora puede enviar un *LMP_detach*, para destacar la razón de no soportar la característica LMP.

Una unidad puede manejar el rechazo de la solicitud, como una característica adicional.

3 Política de enlace.

Estos son los roles que no son fijos maestro-esclavo para la ejecución de este perfil.

Este perfil no tiene ningún estado que requiera el uso del modo de bajo poder, o cuando se hace uso de ellos. El LM de cada uno decide y solicita como deber ser visto apropiadamente, dentro de las limitaciones de requerimiento que se indicaron en la sección de calidad de servicio.

APENDICE K

REQUERIMIENTOS DE INTEROPERABILIDAD DEL CONTROL DE ENLACE (LC).

1 Descripción General de las capacidades.

La siguiente tabla lista todas las capacidades en el nivel de LC, y los requerimientos extras agregados a las especificaciones de la banda base.

Tabla 4
Capacidades banda base/LC

	Capacidades	Soportado en el DevA	Soportado en el DevB
1.	Indagación		SI
2.	Exploración Indagación	SI	
3.	Búsqueda		SI
4.	Exploración Búsqueda		
A	Tipo R0	SI	
B	Tipo R1	SI	
C	Tipo R2	SI	
5	Tipos de paquetes		
A	Paquete ID		
B	Paquete NULL		
C	Paquete POLL		
D	Paquete FHS		
E	Paquete DM1		
F	Paquete DH1		
G	Paquete DM3		
H	Paquete DH3		
I	Paquete DM5		
J	Paquete DH5		
K	Paquete AUX	SI	SI
L	Paquete HV1		
M	Paquete HV2		
N	Paquete HV3		
O	Paquete DV		

6.	Capacidades Inter.-piconet		

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

2 Investigación.

Cuando la investigación es invocada por el DevA, este puede usar el procedimiento de Investigación General, ver apéndice G.

3 Exploración Investigación.

Para explorar, al menos, el GIAC debe ser usado, acordado para uno de los modos de descubrimiento definidos anteriormente. Que es el de sólo permitir el uso del modo Descubrimiento Limitado, si es apropiado para la aplicación(es) que se encuentran en el DevB.

4 Búsqueda.

Sólo DevA hace búsqueda, el paso de la búsqueda puede saltarse en DevA cuando está lista la conexión de banda base entre DevA y DevB (En tal caso la conexión puede estar fijada como el resultado de las búsquedas previas de DevB.)

5 Error de Comportamiento.

La mayoría de las características en el nivel LC tienen que ser activadas por los procedimientos LMP, así que la mayoría de los errores serán capturados por esa capa. Como sea, existen algunos procedimientos LC que son independientes de la capa LMP, por ejemplo búsqueda o investigación. Un uso erróneo de las características dificulta o a veces imposibilita que se detecten. Esto no está definido mecánicamente para detectar o prevenir tales usos incorrectos

APENDICE L

CONFIGURANDO Y TRABAJANDO CON BLUELAP

BlueLAP puede ser configurado y puesto a funcionar de dos maneras, la primera por medio de líneas de comando para ser utilizados por la consola si no se dispone de entorno gráfico y la segunda manera es a través de una herramienta gráfica basada en web, que permite configurar y poner en marcha el LAP.

Estos métodos se describen con mayor detalle a continuación:

1 Líneas de comando: Como se mencionó anteriormente se dispone de líneas de comando para cónsola en caso de no encontrarse en un entorno gráfico, para la fácil configuración y puesta en marcha del LAP **BlueLAP**, a continuación se listan los comandos, su finalidad y su utilización:

- **startDevice_usb:** Este comando permite levantar un dispositivo *Bluetooth* de tipo USB para ser utilizado como LAP, se utiliza de la siguiente manera:

  <root># cd /BlueLAP_DIR/

  <root># ./startDevice_usb

  Donde: BlueLAP_DIR es el directorio donde se ha instalado

  BlueLAP.

- **startDevice_uart:** Este comando permite levantar un dispositivo *Bluetooth* de tipo UART para ser utilizado como LAP, se utiliza de la siguiente manera:

  <root># cd /BlueLAP_DIR/

  <root># ./startDevice_uart

  Donde: BlueLAP_DIR es el directorio donde se ha instalado BlueLAP.

- **startLAPserver:** Inicia el servidor LAP, según las configuraciones establecidas en el archivo de configuración ubicado en "/BlueLAP_DIR/conf/rfcommd.conf". Se utiliza de la siguiente manera:

  <root># cd /BlueLAP_DIR/

  <root># ./startLAPserver

  Donde: BlueLAP_DIR es el directorio donde se ha instalado **BlueLAP**.

- **startClientDevice_usb:** Levanta un dispositivo *Bluetooth* de tipo USB para ser utilizado como cliente, tiene la siguiente sintaxis:

  <root># cd /BlueLAP_DIR/

  <root># ./startClientDevice_usb

  Donde: BlueLAP_DIR es el directorio donde se ha instalado **BlueLAP**.

- **startClientDevice_uart** Levanta un dispositivo *Bluetooth* de tipo UART para ser utilizado como cliente, tiene la siguiente sintaxis:

<root># cd /BlueLAP_DIR/

<root># ./startClientDevice_uart

Donde: BlueLAP_DIR es el directorio donde se ha instalado **BlueLAP**.

- **startLAPclient:** Inicia el cliente DT para conectarse al LAP, según las configuraciones establecidas en el archivo de configuración ubicado en "/BlueLAP_DIR/conf/rfcommdClient.conf". Se utiliza de la siguiente manera:

  <root># cd /BlueLAP_DIR/

  <root># ./startLAPclient

  Donde: BlueLAP_DIR es el directorio donde se ha instalado **BlueLAP**.

Nota: Se debe disponer de permisos de *root* para poder ejecutar estos comandos.

2 **LAPserverconf:** Tal como se mencionó anteriormente se puede disponer de una herramienta basada en web para ser utilizada en entorno gráfico ó ejecutarla en el servidor y accederla desde estaciones remotas a través de HTTP. Esta herramienta se llama **LAPserverconf** (ver figura 6), permite configurar, ejecutar el servidor **BlueLAP** y visualizar las conexiones de clientes DTs.

Para poder hacer uso de esta herramienta se debe disponer de un servidor web *Apache* con módulo *Perl* en el servidor donde se encuentre el **BlueLAP** y haber instalado y configurado *cgiwrap* para que permita ejecutar scripts en modo *root*.

Para acceder a esta herramienta debe utilizar el siguiente URL en su navegador:

http://<SERVIDORLAP>/cgi-bin/cgiwrap/root/<BLUELAP>/LAPserverconf.pl

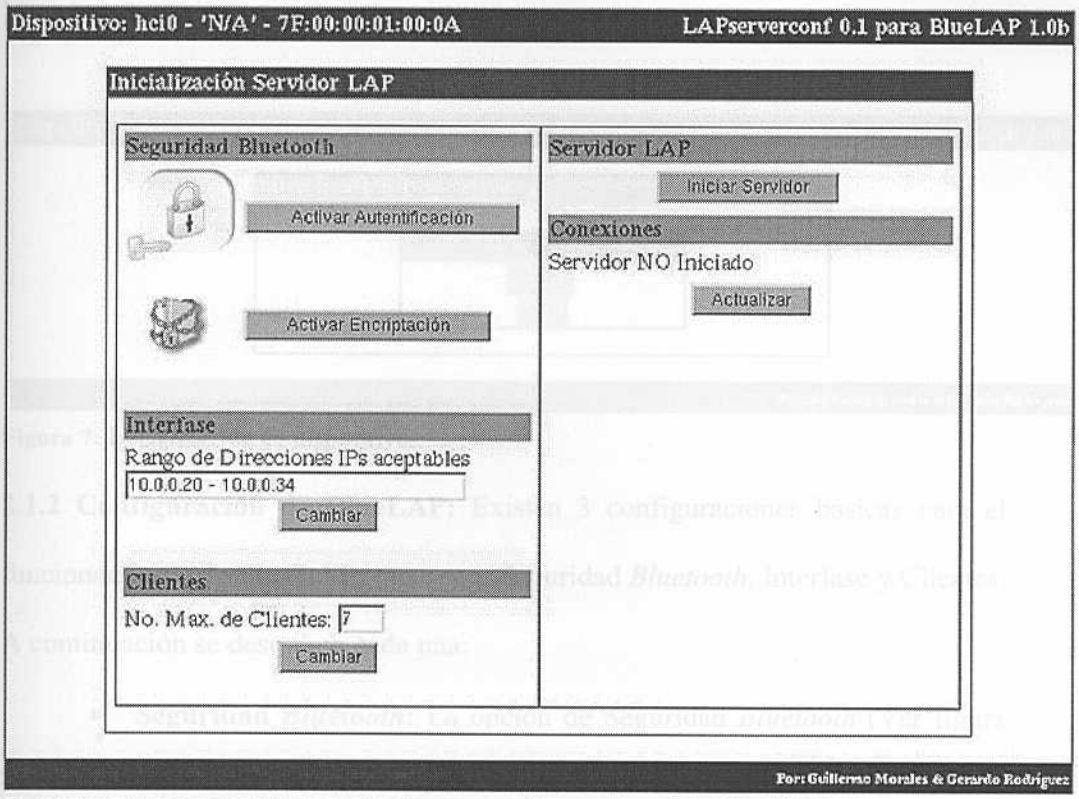


Figura 6: LAPserverconf, herramienta para configurar el servidor BlueLAP.

Donde: *<SERVIDORLAP>* es la dirección IP ó el nombre del servidor donde se encuentre el **BlueLAP** y *<BLUELAP>* es el directorio donde se instalo la herramienta gráfica.

Nota: La autentificación de usuarios que deseen acceder a LAPserverconf deberá ser manejada y configurada por el administrador del servidor.

2.1 Utilización de LAPserverconf

2.2.1 Inicialización del dispositivo: Si el dispositivo *Bluetooth* a ser utilizado como LAP no ha sido inicializado, se presentará la pantalla de la figura 7, esta pantalla nos permitirá inicializar el dispositivo, tanto USB como UART. Una vez

iniciado el dispositivo se puede proseguir con las configuraciones y puesta en marcha con el servidor LAP.

Para inicializar el dispositivo, simplemente presione el botón del tipo de dispositivo que desea inicializar.

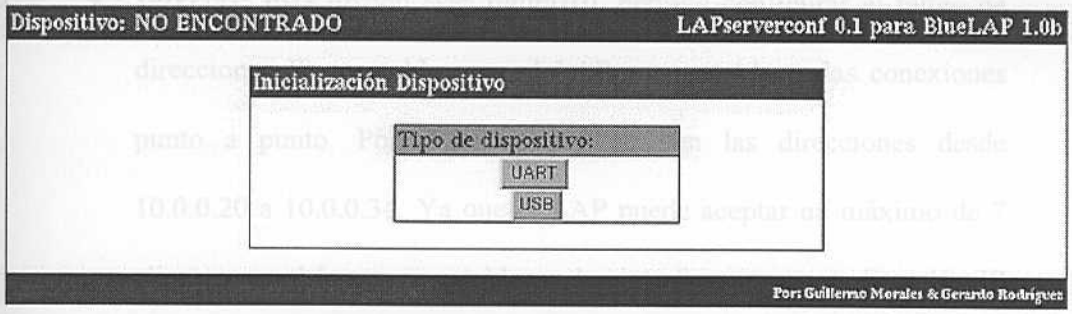


Figura 7: Inicialización de dispositivos.

2.1.2 Configuración de BlueLAP: Existen 3 configuraciones básicas para el funcionamiento de **BlueLAP**, estas son: Seguridad *Bluetooth*, Interfase y Clientes. A continuación se describen cada una:

- **Seguridad *Bluetooth*:** La opción de Seguridad *Bluetooth* (Ver figura 8), Permite activar ó desactivar las características de autentificación y encriptación del enlace *Bluetooth*. Para activar ó desactivar alguna de estas características sólo tiene que presionar el botón indicado para tal acción. La figura 9 muestra como se identifican en pantalla los diferentes estados de dichas características.

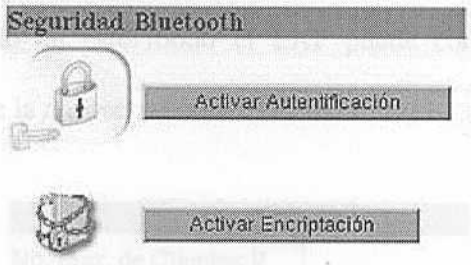


Figura 8: Opciones de seguridad.

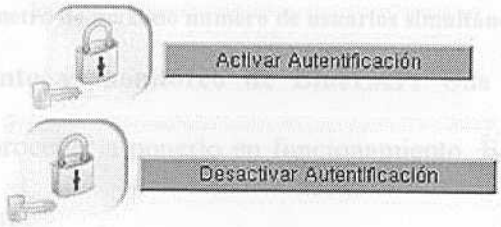


Figura 9: Estados de las opciones.

- **Interfaz:** Esta opción (ver figura10), permite configurar el rango de direcciones IP aceptables por el LAP para establecer las conexiones punto a punto. Por defecto se establecen las direcciones desde 10.0.0.20 a 10.0.0.34. Ya que el LAP puede aceptar un máximo de 7 clientes simultáneos, se establecen las interfases con una dirección IP origen y una destino que estén dentro del rango especificado en esta opción, empezando desde la primera dirección libre para el origen y la siguiente para el destino, y así sucesivamente.

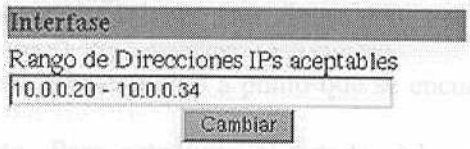


Figura 10: Parámetro de rango de direcciones IP aceptables por el servidor.

- **Clientes**: Aquí (ver figura 11), se puede establecer el parámetro de máximo número de usuarios del LAP. Por defecto este parámetro viene configurado con el máximo número de usuarios posibles (7 usuarios). El número mínimo de usuarios permitido es uno (1), al estar configurado en este modo el LAP puede comportarse tanto como maestro de la *piconet* ó como esclavo.

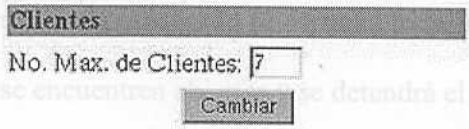


Figura 11: Parámetro de máximo numero de usuarios simultáneos en el servidor.

2.1.3 Funcionamiento y monitoreo de BlueLAP: Una vez configurado el servidor, se puede proceder a ponerlo en funcionamiento. Esto se puede realizar de la siguiente manera:

- **Iniciar Servidor:** En el apartado "Servidor LAP" (Ver figura 12), se encuentra el botón "Iniciar Servidor", al presionar dicho botón se iniciará el servidor **BlueLAP** y pasará al estado de espera de conexiones.

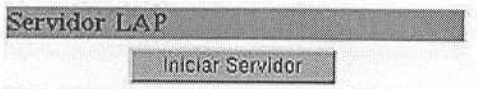


Figura 12: Iniciar servidor LAP.

- **Monitorear Conexiones:** Al iniciar el servidor se podrá disponer de un monitor de conexiones (ver figura 13), que ofrecerá información sobre las conexiones punto a punto que se encuentren funcionando en el momento. Para actualizar el estado del monitor sólo tiene que presionar el botón "Actualizar".

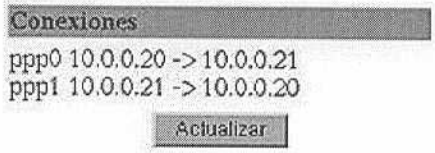


Figura13: Estado de las conexiones en el servidor LAP.

- **Detener Servidor:** Para detener el funcionamiento del servidor **BlueLAP**, debe presionar el botón "Detener Servidor" (ver figura 13), una vez presionado este botón se cerrarán todas las conexiones punto a punto que se encuentren abiertas y se detendrá el servidor LAP.

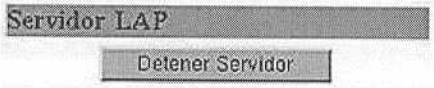


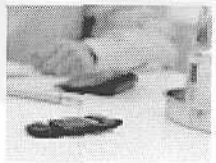
Figura 13: Detener servidor LAP.

Cliente BlueLAP: Para conectarse al servidor **BlueLAP** puede hacerlo con cualquier cliente DT que cumpla con las especificaciones *Bluetooth* para Puntos de Acceso a Redes LAN. Adicionalmente **BlueLAP** ofrece un cliente para conectarse al servidor **BlueLAP**. Para utilizar ese cliente, primero debe inicializar el dispositivo tipo Cliente, con las líneas de comando anteriormente especificadas y luego utilizar la línea de comando para iniciar el cliente LAP.

ANEXO A

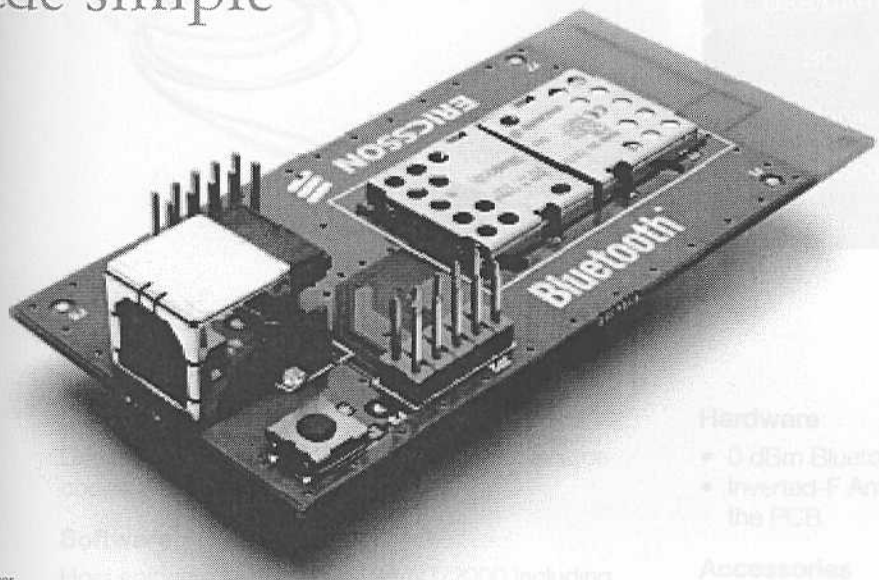
Bluetooth Application Tool Kit

ERICSSON



Bluetooth Application Tool Kit

Development made simple



- Small
- Low Power
- Low Cost

Accelerate time to market

The tool kit has been designed by Ericsson to enable adopters of the Bluetooth wireless technology to accelerate development of Bluetooth products.

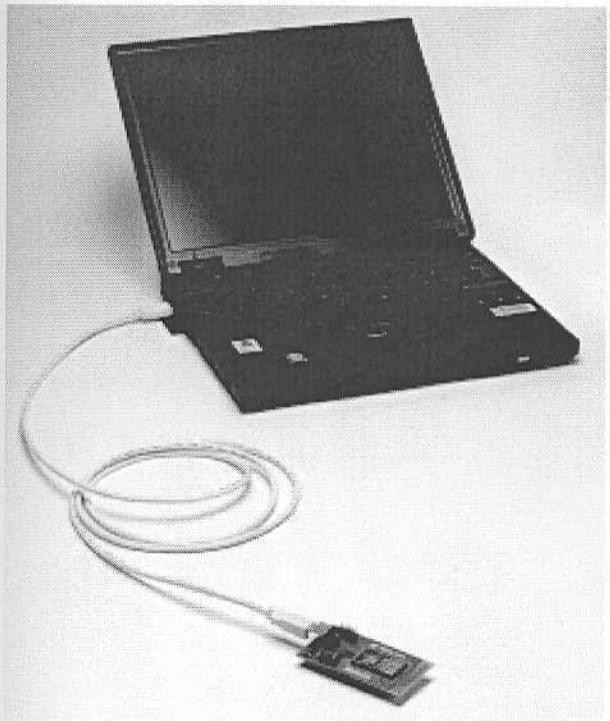
Easy Development

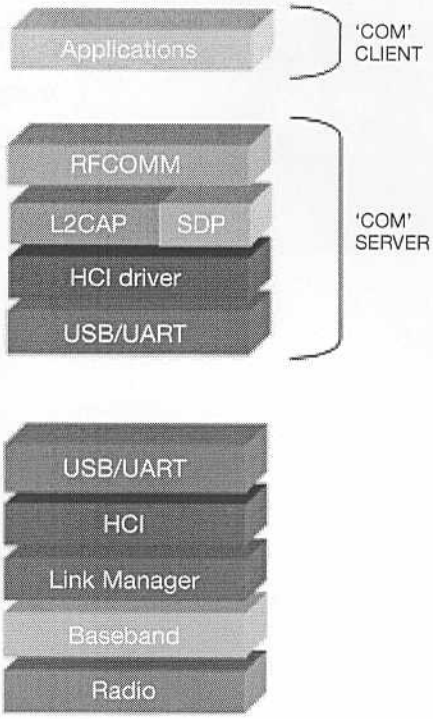
The USB connection between the host computer and the board ensures ease of use and full Bluetooth speed. Applications use a well-defined API providing access to the different layers of the protocol stack. No external power supply required.

Typical Applications

Several typical applications are included, e.g. Chat and File Transfer. Both executable images and source code. A Bluetooth neighborhood software is also included that makes it possible to detect other active Bluetooth devices within the radio range.

Bluetooth™





www.pyramid.se

Documentation

User's Manual, Technical Documentation: Source codes, API descriptions.

Software

Host software for Windows 98/NT/2000 including the following Bluetooth protocol layers: HCI, L2CAP, RFCOMM and SDP. The stack is delivered as an executable COM Server.

The following typical applications are provided: Chat, File Transfer and Bluetooth Neighborhood. These applications are implemented as COM Clients and delivered in both executable and C++ source code form.

You can order the Bluetooth Application Tool Kit on registering with Sigma ComTec, the distributor of the kit, at:

http://www.comtec.sigma.se

Hardware

- 0 dBm Bluetooth Module
- Inverted-F Antenna integrated into the PCB

Accessories

- USB Cable, type A to type B
- UART Cable, D-sub to D-sub
- D-sub to pin header converter cable

Interfaces

- USB
- UART
- External Power Connectors

Dimensions

- 80 x 40 x 15 mm

SIGMA

Sigma ComTec AB
Kristian IV:s väg 3
Box 853
SE-301 18 Halmstad
SWEDEN
info@comtec.sigma.se
http://www.comtec.sigma.se

The BLUETOOTH trademarks are owned by their proprietor and used by Ericsson under license.

*Third party brands and names are the property of their respective owners.

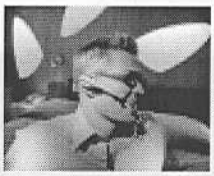
© Ericsson Technology Licensing AB, 2001.
Product specifications are subject to change without prior notice.

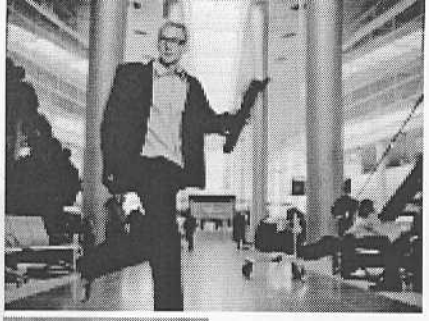
Ericsson Technology Licensing AB, SE-221 83 Lund, Sweden.
Printed in March 2001, LZT 108 4038/1
www.ericsson.com/bluetooth

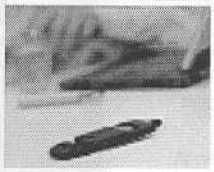
ANEXO B

Bluetooth Development Kit

ERICSSON

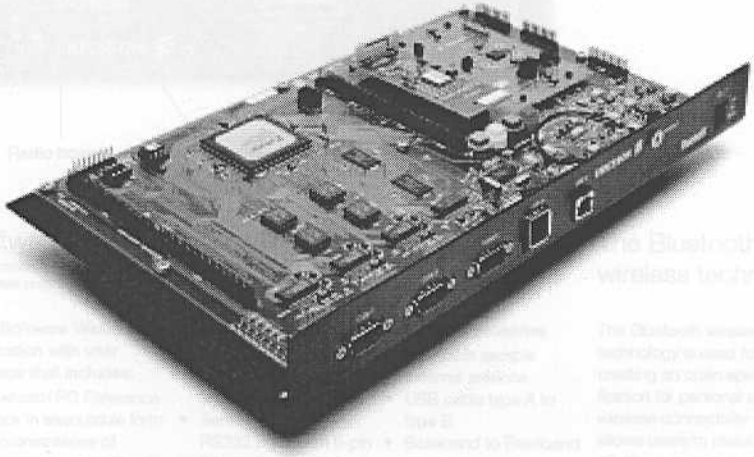






Bluetooth™ Development Kit

Faster launching of Bluetooth products



Quicker production

The Bluetooth Development Kit from Ericsson has been designed to enable early adopters of the wireless technology to quickly and easily accelerate the time to market of Bluetooth products and applications.

Seamless integration

It provides a complete and flexible design environment within which engineers can seamlessly integrate the new open wireless specification into a range of digital devices for volume production.

Demonstrates core features

The kit's exceptional quality and scaleable architecture demonstrate the core features of the Bluetooth wireless technology, thereby allowing developers to create an integrated application board for prototype products.

Meets immediate needs

The Bluetooth Developers Kit is designed to meet the needs of first-time Bluetooth developers and users.

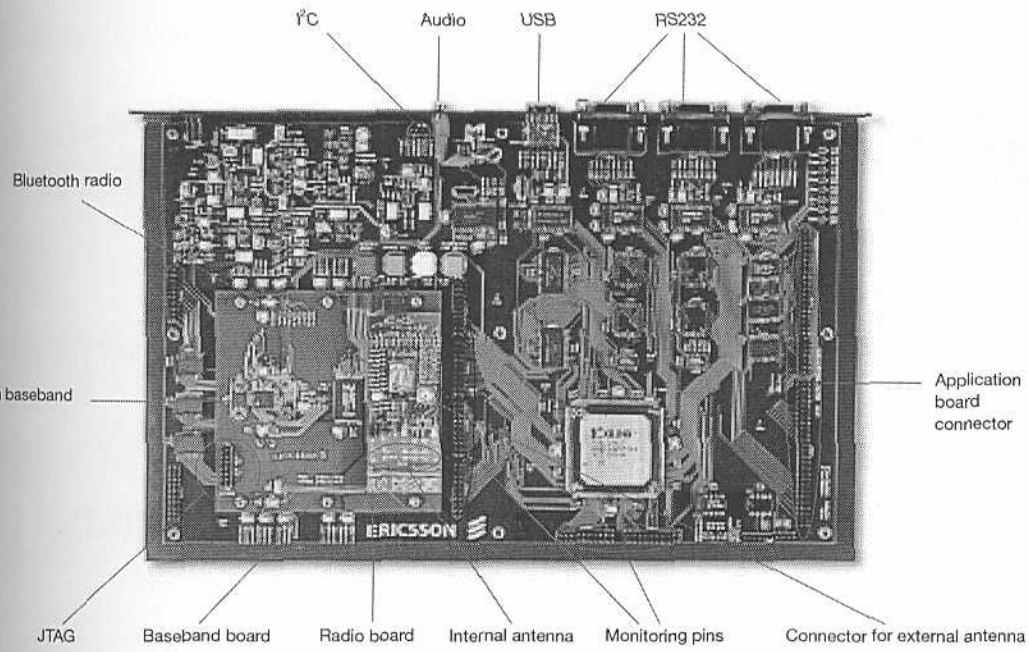
For embedded applications

The Bluetooth Development Kit is aimed at embedded application development and enables execution of code in both RAM and Flash.

Blue Unit approved

The Bluetooth Development Kit from Ericsson has been approved as a Blue Unit by the Bluetooth SIG. Blue Units are used in the Bluetooth Qualification Process. Test your product against the Bluetooth Development Kit and save valuable development time.

Bluetooth™



Documentation

Bluetooth Specifications
- Core
- Profiles

Firmware documentation
- HCI Functional Specification
- HCI UART Transport Layer
- HCI USB Transport Layer
- Message Sequence Charts
- VHDL Code

Hardware documentation
- Radio and Antenna Board Documentation
- Motherboard Documentation
- Baseband Board Documentation

Comprehensive data sheets
- Baseband Controller
- Bluetooth Module
- Bluetooth Radio Module

Introduction Slides
- Architecture
- Profiles
- Qualification
- Radio and Baseband
- Security
- Software
- Bluetooth Building Blocks

EDBK documentation
- Contents
- Documentation Overview
- Getting Started
- Introduction to Antennae
- Technical Documentation
- Technical Tutorial
- Bluetooth Developers Kit FAQs
- Bluetooth Qualification

Bluetooth PC Reference Stack is a reference porting of Bluetooth Host Stack, which is a qualified pre-tested component with the covered functionality of: HCI-Driver, L2CAP, RFCOMM and SDP.

Software

(one license for development purposes only)

Host Software Win32 C++ application with user interface that includes:
- Bluetooth PC Reference Stack in executable form
- Demonstrations of voice/data applications
- Bit-error rate (BER) test software
- Baseband to Baseband connection support software
- Application Wizard for host application development
- Application Wizard Demo
- HCI scripting tool and sample scripts
- Support for both USB & UART
- Packet Builder utility for displaying user entered packet details
- LMP (Link Manager Protocol) signaling trace

Baseband Target Firmware
- Basic test firmware that allows all the interfaces to be tested.
- Ericsson's Link Layer and Host Control Interface firmware that handles the Bluetooth radio packet protocol and provides an interface to the controlling host computer.

Hardware

Interfaces
- Radio: 0 dBm board with internal or external antenna connectors
- Serial Ports: Three RS232 ports with 9-pin 90 degree D-type female connectors
- Audio: Pin header for a typical handset
- Universal Serial Bus: One USB female
- CIF (Common Interface) for improved interoperability tests
- I²C: One 4-way pin connector
- Status LEDs
- General-purpose input/output
- JTAG Debug port for ARM CPU
- On/Off/Reset switch

Application Board Interface
- Application Board connector (20-bit address, 16-bit data, Control, Linear PCM)

Included accessories
- Bluetooth sample external antenna
- USB cable type A to type B
- Baseband to Baseband cable
- Serial cable (female to female)
- RS232 cable 9 pin, female to female
- RS232 loopback plugs, 3 pcs
- LIC (Lump-In-Cord) Power Cube 100—240 VAC to 12 VDC
- Power Cable Plugs (UK, Australia, USA/Canada, Europe)
- Ericsson Handset and Assembly Kit

Mechanical

Approximate weight: 500 grams
Dimensions (mm): Motherboard: 300x190, Baseband board: 105x105, Radio Module board 90x35.

The Bluetooth wireless technology

The Bluetooth wireless technology is used for creating an open specification for personal area wireless connectivity. It allows users to make effortless, instant connections between a wide range of communication devices. Based on a radio link, facilitating fast and secure transmission of both voice and data, Bluetooth devices operate in a globally available frequency band giving worldwide compatability.
The Bluetooth wireless technology is the global specification for wireless connectivity.

The Bluetooth Development Kit is distributed by:

The BLUETOOTH trademarks are owned by their proprietor and used by Ericsson under license.

Third party brands and names are the property of their respective owners.

© Ericsson Technology Licensing AB, 2001
Product specifications are subject to change without prior notice.

Ericsson Technology Licensing AB, SE-221 83 Lund, Sweden.
Printed in March 2001, LZT 108 2637 R2
http://www.ericsson.com/bluetooth

ANEXO C

Wi Fi (802.11b) *and Bluetooth*

Wi-Fi™ (802.11b) and Bluetooth™:

An Examination of Coexistence Approaches

Abstract

This paper analyzes different approaches to resolving the interference problems between the Wi-Fi™ and Bluetooth™ wireless technologies. This analysis explores the strengths and weaknesses of these interference mitigation approaches, and goes on to explain what is necessary for achieving satisfactory combination performance and true "Coexistence without Compromise"™. The contents are based on Mobilian Corporation's coexistence research and development work, including a thorough analysis of the problems and various experiments to understand the interference issue.

In investigating different approaches to interference mitigation, this paper gives technical data and uses common wireless technology terms. The information presented is targeted to readers who have a basic understanding of wireless networking. We recommend that readers without this understanding read Mobilian's first white paper: *Wi-Fi (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem (www.mobilian.com)*.

April 11, 2001

Disclaimer and Copyright

Windows Hardware Engineering Conference

Author's Disclaimer and Copyright: *Mobilian™, TrueRadio™, Sim-OP™, TrueConnectivity™, and Coexistence without Compromise™ are all trademarks of Mobilian Corporation.*

WinHEC Sponsors' Disclaimer: *The contents of this document have not been authored or confirmed by Microsoft or the WinHEC conference co-sponsors (hereinafter "WinHEC Sponsors"). Accordingly, the information contained in this document does not necessarily represent the views of the WinHEC Sponsors and the WinHEC Sponsors cannot make any representation concerning its accuracy. THE WinHEC SPONSORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS INFORMATION.*

Microsoft, DirectX, MS-DOS, Win32, Win64, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Other product and company names mentioned herein may be the trademarks of their respective owners.

Table of Contents

1.0 Executive Summary 3
2.0 Background 4
2.1 Technical Background 5
2.1.1 Bluetooth™ Wireless Personal Area Networking (WPAN) 5
2.1.2 802.11b Wireless Local Area Networking (Wi-Fi™) 6
2.1.3 Wi-Fi™ / Bluetooth™ Interaction and Interference 6
3.0 Interference Mitigation Approaches 8
3.1 Collocation without Coexistence Mechanism 9
3.1.1 Overview 9
3.1.2 Analysis 9
3.2 Driver-level (Modal) Switching Between Wi-Fi and Bluetooth 10
3.2.1 Overview 10
3.2.2 Analysis – Dual-mode Radio Switching 11
3.2.2.1 Dual-mode Radio Switching 11
3.2.2.2 Leaving the Network without Signaling 12
3.2.2.3 Leaving the Network with Signaling 12
3.2.3 Analysis – Driver-level Switching 12
3.2.3.1 Throughput and Time-delay Concerns 12
3.2.3.2 Impacts of Bluetooth Polling Activities 14
3.3 Adaptive Hopping 14
3.3.1 Overview 14
3.3.2 Analysis 15
3.3.2.1 Adaptive Hopping as Optional Profile (Operational Mode) 15
3.3.2.2 Adaptive Hopper Must Accurately Sense and Respond to Interferers 15
3.3.2.2.1 Bluetooth™ Difficulty in Detecting Wi-Fi™ Signal 16
3.3.2.2.2 Congested Wireless Environments are Particularly Troublesome 17
3.3.2.3 Adjacent-Channel Noise 19
3.3.2.4 Number of Channels 19
3.4 MAC-level Switching 19
3.4.1 Overview 19
3.4.2 Analysis 19
3.5 Simultaneous Operation 20
3.5.1 Overview 20
3.5.2 Analysis 22
4.0 Summary 22
5.0 Appendix 1 – In-band versus Out-of-band Noise 24
5.1 Signals and Noise 24
5.1.1 Types of Noise 24
5.2 Bluetooth and Wi-Fi Interference Cases 26
6.0 Appendix 2 – Path Loss Models Employed 28
References ....Error! Bookmark not defined.

Table of Figures

Figure 1 – Performance Hierarchy of Coexistence Approaches for Collocated Wi-Fi & Bluetooth 9
Figure 2 – Geometry of Measurement and Simulation Environment 10
Figure 3 – Measurement of Wi-Fi Throughput in the Presence of Collocated Bluetooth 10
Figure 4 – Conceptual Wireless System Diagram 11
Figure 5 – Basic Geometry of Bluetooth and Wi-Fi Penetrated Corporation 17
Figure 6 – Likely Location of Two Adaptive Hoppers 18
Figure 7 – Simultaneous Operation Covers Entire Conceptual Wireless System Diagram 21
Figure 8 – Ganymede Chariot Graph of Mobilian Corporation's TrueRadio™ Demonstration 22
Figure 9 – Mobilian's TrueRadio™ Performance in Collocated Scenario 23
Figure 10 – In-Band versus Out-Of-Band Noise 25
Figure 11 – White Noise and Colored Noise are Very Different 25
Figure 12 – Typical Transmit Mask 26
Figure 13 – Path Loss as a Function of Distance, Indoor, 2.4-GHz ISM Band 28

© 2001 Mobilian Corporation. All rights reserved.

Executive Summary

Wireless markets, from wide area networks, to local and personal area networks, are widely expected to be the significant market of the 21st Century. Investment capital is flowing to wireless companies worldwide, and market forecasts consistently project hundreds of millions of installed units. With this expansion comes increased opportunity for market innovation, and consequently, wireless penetration into the core fabric of our everyday lives.

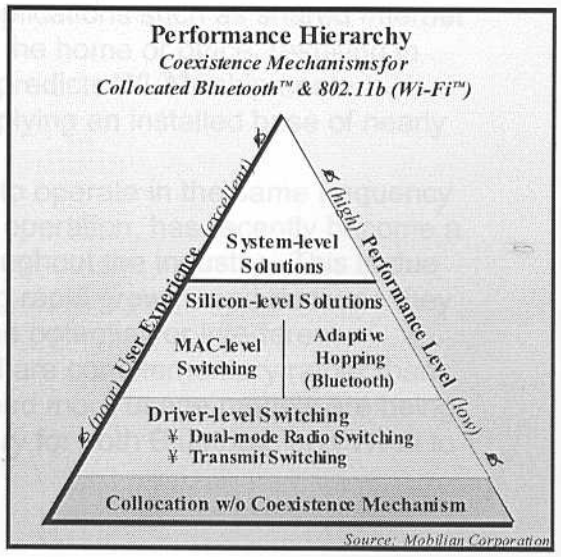
This growth is spurred by increasing demand for maximum convenience and immediate access to desired information. It is facilitated by an unlicensed frequency spectrum, providing unlimited, free access to whomever wishes to build a wireless device capable of complying with regulatory standards. These forces are working together to create traffic and device density in the unlicensed frequencies, and consequently opportunities for interference between the protocols using those frequencies.

As these trends develop, the need for multiple wireless devices operating at the same time will increase, resulting in still greater potential for interference. That is why "simultaneous operation" is becoming an important topic of discussion in today's market.

Simultaneous operation is the ability of different, fully standards-compliant wireless systems to operate simultaneously in any scenario, while experiencing minimal or no degradation in performance. This definition includes wireless devices that can give the user outstanding performance without a list of operational caveats. The device should "just work," regardless of other devices within its operating environment.

Wireless local area networking (WLAN) and wireless personal area networking (WPAN) are two networks in particular for which simultaneous operation is growing in importance. WLAN / WPAN simultaneous operation will occur more and more frequently as users begin completing everyday tasks such as copying or printing a file from their WLAN PC while using a WPAN-enabled mouse, keyboard, and speakers. Its frequency will continue to grow as personal communication devices and synchronization activities with PCs and networks grow, and it will gain even more importance as distributed applications take off – "the next big thing in software" – and WPAN devices must coexist with massive amounts of WLAN activity.

In all these scenarios, users will appreciate being able to use whatever wireless devices surround them, when they want to, and how they want to. Users will demand unhindered simultaneous operation and will resist adopting wireless devices as long as there are operational problems or perceived concerns.



© 2001 Mobilian Corporation. All rights reserved.

With this certainty facing the market today, regulatory bodies, standards bodies, and industry participants are begun several approaches to achieving simultaneous operation, including:

1. Simple collocation (combo-card reference designs);
2. Approaches in the host software (driver-level switching and dual-mode radios)
3. Approaches in the MAC layer (MAC-level switching and adaptive hopping); and
4. System-level solutions covering the entire wireless sub-system, and incorporating the best aspects of many different approaches.

Each technique's strengths and weaknesses are explored in depth in the following pages. In summary, based on exploration and assessment of each technique's interference management ability, true, sustainable simultaneous operation can only be achieved by taking a system-level approach across the entire wireless sub-system. This allows the simultaneous operation solution to selectively use the best aspects of all the techniques, and therefore manage interference extremely well. This is the approach Mobilian Corporation has employed with its first product, TrueRadio™.

Background

The 2.4 GHz Industrial, Scientific, and Medical (ISM) band is poised for strong growth. Fueling this growth are two emerging wireless technologies: WPAN and WLAN. The WPAN category is led by a short-range wireless technology called Bluetooth™. Designed principally for cable replacement applications, most Bluetooth implementations support a range of roughly 10 meters, and throughput up to 721 Kbps for data or isochronous voice transmission. Bluetooth is ideal for applications such as wireless headsets, wireless synchronization of PDAs with PCs, and wireless PC peripherals such as printers, keyboards, or mice. Cahners In-Stat predicts shipments for Bluetooth devices will reach 800 million units annually by 2004 [CIS00a].

In the WLAN category, several technologies are competing for dominance; however, based on current market momentum, it appears that Wi-Fi™ (IEEE 802.11b) will prevail. Wi-Fi offers throughput up to 11 Mbps and covers a range of approximately 100 meters. With WLANs, applications such as shared Internet access, e-mail, and file sharing can be done in the home or office, resulting in new levels of freedom and flexibility. Cahners predicts WLAN shipments exceeding 38 million units annually in 2004, implying an installed base of nearly 95 million systems [CIS00b] by the same year.

"Coexistence," the ability for multiple protocols to operate in the same frequency band without significant degradation to either's operation, has recently become a significant topic of analysis and discussion throughout the industry. This is due to several factors. Both protocols are expecting rapid growth, and because they both operate in the 2.4 GHz frequency band, the potential for interference between them is high. Also, WPAN and WLAN are complementary rather than competing technologies. Consequently, more and more usage models are being discovered in which it is desirable and necessary for both Bluetooth and Wi-Fi to operate simultaneously and in close proximity.

© 2001 Mobilian Corporation. All rights reserved.

Technical Background

This section provides some high-level background on several key characteristics of the Bluetooth and Wi-Fi protocols. A deep understanding of these characteristics is necessary to fully investigate the merits of various approaches, but this high-level overview will provide a basic understanding. Further explanation of the two protocols' technical characteristics is provided in Mobilian's first white paper, *Wi-Fi (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem* www.mobilian.com/whitepaper_frame.htm [MBLN01].

Bluetooth™ Wireless Personal Area Networking (WPAN)

Bluetooth is a WPAN protocol designed as a cable-replacement technology - low cost, modest speed, and short range (<10 meters). Bluetooth can support piconets of up to eight active devices, with a maximum of three synchronous-connection-oriented (SCO) links. SCO links are voice-oriented and designed to support real-time, isochronous applications such as cordless telephony or headsets. Bluetooth also supports asynchronous connection links (ACLs) used to exchange data in non-time-critical applications. The majority of Bluetooth devices transmit at a power level of 1 mW (0 dBm). The Bluetooth physical (or PHY) layer uses the frequency-hopping spread spectrum (FHSS) technique. Bluetooth hops at a rate of 1600 hops/sec and uses Gaussian frequency shift keying (GFSK) modulation.

When the Bluetooth technology establishes communication, it forms small networks, or piconets, of Bluetooth-enabled devices. Piconet topology consists of a single master and up to seven active slaves. In a single piconet environment, there can be only one Bluetooth device transmitting in any single time slot at any one time. Therefore, the master Bluetooth node of the piconet controls the piconet through a series of transmissions. When the master has information to transmit to the slaves, it does so. Otherwise, the master is constantly polling the slaves and listening for their responses[1]. In short, for a slave to transmit data, it first must be "asked" to do so. The slave's responses can be either NULL for no information to transmit, or they can begin transmitting if they have information to transmit. This piconet management scheme avoids interference within the piconet and is standard for any device carrying the Bluetooth certification (i.e., complying with the Bluetooth specification). Understanding some aspects of the different approaches to interference mitigation, requires further investigation of the master/slave polling mentioned above. Due to the extremely rapid nature of the polling activity (hundreds of microseconds), the Bluetooth media access controller (MAC) controls the function at the MAC-level and thus, the data transferred in the process is not

[1] The Bluetooth specification does not dictate how often a master should poll a slave, nor does it provide for any preemptive transmission from the slave to inform the master that it has data to transmit; therefore, to maximize Bluetooth throughput, many typical current design practices call for the master to poll the slaves during every available transmit time slot (800 polls / second) while in an active piconet.

© 2001 Mobilian Corporation. All rights reserved.

made available at the driver or host level. This will prove to be very significant, as is explained in later sections.

802.11b Wireless Local Area Networking (Wi-Fi™)

Like wired Ethernet, Wi-Fi supports true multipoint networking with such data types as broadcast, multicast, and unicast packets. Although standard practice is approximately one access point (AP) to every 10-20 stations (STA), the MAC address built into every device allows for a virtually unlimited number of devices to be active in a given network. These devices contend for access to the airwaves using a scheme called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The Wi-Fi physical layer uses direct-sequence spread spectrum (DSSS) at four different data rates using various modulation techniques to communicate. The transmit power level can vary, but is typically between 30 and 100 mW (+15 to 20 dBm).

Wi-Fi™ / Bluetooth™ Interaction and Interference

Bluetooth and Wi-Fi share the same unlicensed 2.4 GHz ISM band that extends from 2.4 to 2.4835 GHz under US FCC regulations. This frequency band is free of tariffs under the ISM band rules defined in FCC Part 15.247 [FCC15.247]. However, systems in this band must operate under certain constraints that are supposed to enable multiple systems to coexist in time and place. FCC Part 15.247 specifies that a system can use one of two methods to transmit in this band: FHSS or DHSS.

FHSS is a technique in which a device transmits an energy burst in a narrow frequency band for a limited time before it hops to another. This hopping process is repeated rapidly across the entire frequency band in a pseudo-random fashion. DSSS is a technique in which a device communicates by distributing its energy across a defined set of contiguous frequency bands without hopping.

Bluetooth is an FHSS technology with frequency channels 1 MHz in width and a hop rate of 1600 hops per second. Bluetooth dwells 625 μsec in every frequency channel. In the United States and most of the world, Bluetooth uses 79 different 1 MHz frequency channels of the available 83.5 MHz in the 2.4 GHz ISM band. Wi-Fi uses DSSS with a 22 MHz passband, and communicates with throughput up to 11 Mbps. A Wi-Fi system can use any of eleven[2] 22-MHz wide sub-channels across the available 83.5 MHz of the 2.4 GHz frequency band. Because Bluetooth hops on 79 of the available 83.5 1-MHz channels, and Wi-Fi occupies 22 1-MHz channels within its passband, sharing between the two technologies is inevitable. Two wireless systems using the same frequency band will have a high propensity to interfere with each other.

[2] The 11 sub-channels available under US regulation allow for multiple variations of locations for 3 simultaneously operating Wi-Fi networks and associated passbands. A Wi-Fi passband typically spans a 22-MHz channel; therefore the 83.5 MHz available within the 2.4 GHz band can support three simultaneously operating, overlapping Wi-Fi networks (83.5 MHz - (3*22 MHz) = 17.5 MHz). Geographies outside of the US may support more or fewer than 11 selectable sub-channels.

© 2001 Mobilian Corporation. All rights reserved.

In October of 2000, Mobilian Corporation published a white paper that explored this interference in great detail. The white paper, *Wi-Fi (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem,* received wide acceptance by the industry as the definitive treatment of this issue. This current paper, on the other hand, builds on the previous work and therefore assumes a certain level of understanding of the coexistence issues.
However, for the basis of this paper, it is important to establish that Wi-Fi performance generally suffers more from Bluetooth activity than vice versa. The reasons for this are explained in great detail in the aforementioned white paper, but in summary, there are two main reasons:

1) First, the Wi-Fi MAC is an adaptation of the wired Ethernet MAC, and therefore uses carrier-sense before transmission (also known as "listen before talk"). Unlike wired Ethernet, the Wi-Fi MAC cannot detect collision, so Wi-Fi dictates that every received packet is acknowledged by an "acknowledgement" (ACK). If a station or access point transmits a packet and does not receive an ACK from its target recipient, it assumes a collision with another Wi-Fi transmission has occurred. To avoid additional Wi-Fi collisions, the station uses an exponential back-off algorithm (i.e., pauses a few micro-seconds) and transmits again. By using this mechanism among others, wired and wireless Ethernet work very efficiently in a homogenous environment. However, in an unpredictable and highly interference prone Bluetooth/Wi-Fi environment, this mechanism, and its associated back-off algorithms, result in repeated error correction without corresponding interference improvement, ultimately resulting in reduced Wi-Fi throughput.
2) Second, the Wi-Fi protocol does not typically move from its 22 MHz passband[3]. This renders it highly susceptible to collision with Bluetooth. Roughly, the probability that a standard Wi-Fi 1500 byte transmission will collide with a simultaneous Bluetooth transmission is 55%. This results from the fact that Wi-Fi requires approximately 1 to 1.5 milli-seconds to receive a 1500 byte packet at 11 Mbps. This allows Bluetooth to hop approximately 2 times (625 μsec per hop / 1.5 milli-seconds). Each hop has a 1 in 79 chance of hitting a given channel, therefore 2 hops have a 2 in 79, or ~ 1/40, chance of hitting a given channel. With 22 channels occupied by the Wi-Fi network, this raises the probability to ~ 22/40 or ~ 55%.

This performance degradation occurs at any one of three levels in descending order of severity.

1) The most pronounced negative effect occurs when a Bluetooth device is collocated with a Wi-Fi device, as is the case in a combination card or notebook PC with both Wi-Fi and Bluetooth functionality.
2) The effects are slightly less severe when the transmitting Bluetooth device is located within the same piconet as a collocated Bluetooth

[3] Wi-Fi does have "channel agility" functionality; however, it is seldom used and even if it is employed, due to its relatively slow movement between channels, it is practically ineffective in avoiding the extremely rapid BT hopping pattern.

© 2001 Mobilian Corporation. All rights reserved.

and typically within 1 to 1_ meters from the collocated Bluetooth/Wi-Fi device.

3) The least severe effects occur when the interfering Bluetooth is outside the collocated Bluetooth's piconet and more than 2 meters from the collocated device.

Additional factors can either improve or worsen the negative effects outlined above. One the most important is in-band and out-of-band communication of the two protocols[4]. Table 1 below gives an overview of the different scenarios and their relative severity.

		Bluetooth Tx		Bluetooth Rx	
		In-band	Out-of-band	In-band	Out-of-band
Wi-Fi™	Tx	No Conflict	No Conflict	Strong Interference	Moderate Interference
802.11b	Rx	Strong Interference	Moderate Interference	Strong[5] Interference	Moderate Interference

Source: Mobilian Corporation

Table 1: The Interference Cases for Bluetooth and Wi-Fi[5]

Interference Mitigation Approaches

As a result of the potentially negative impacts of collocated Wi-Fi and Bluetooth devices, many companies have begun researching and developing solutions for coexistence. Potential approaches include:

- Simple device collocation with no coexistence mechanisms;
- Restricted or adaptive band hopping for Bluetooth devices;
- Switching between the two protocols; and
- System-level approaches covering the entire wireless sub-system and many of the above techniques.

[4] In-band refers to simultaneous operation in the same frequency channel. Out-of-band refers to simultaneous operation in two separate channels. This is further explained in the first white paper and in the appendix of this white paper, "6.0 Appendix – In-band versus Out-of-band Noise". This appendix is an excerpt from Mobilian's first white paper.

[5] Collocated receivers is not an interference issue. However, simultaneous reception implies some degree of simultaneous transmission by external wireless systems. In the case of collocated 802.11b and Bluetooth systems, transmissions (which the collocated Bluetooth is trying to receive) from nearby Bluetooth nodes (located within 2 meters), can significantly affect 802.11b's ability to receive.

© 2001 Mobilian Corporation. All rights reserved.

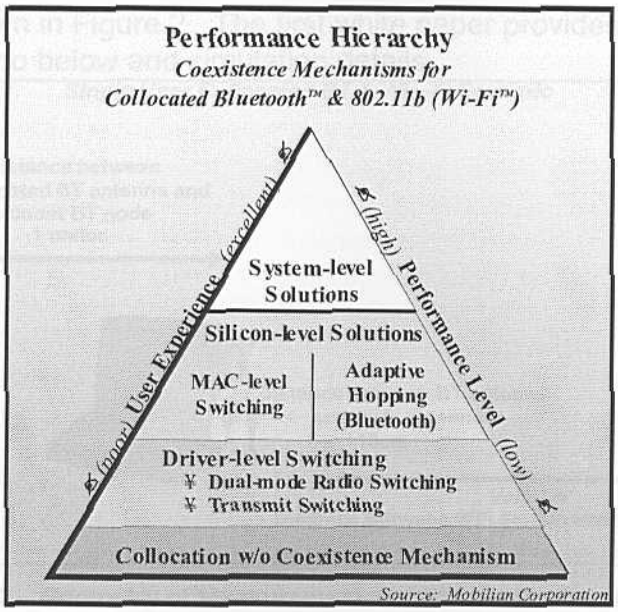


Figure 1 – Performance Hierarchy of Coexistence Approaches for Collocated Wi-Fi & Bluetooth

Each of these approaches is explored in the following pages and can be categorized into the performance and user experience hierarchy shown in Figure 1. The performance hierarchy could change dependent on the operating characteristics of the particular environment. In some scenarios, MAC-level switching may manage interference more effectively than adaptive hopping, and vice versa. The same can be said of driver-level switching and its various implementations. However, system-level solutions, providing simultaneous operation through a combination of the most appropriate aspects of each technique, will most consistently appear at the pinnacle of both performance, and user experience.

Collocation without Coexistence Mechanism

Overview

This approach simply entails collocating the two wireless devices in a single form factor without any attempt to avoid the potential interference (e.g., PC NIC reference design).

Analysis

Collocating Bluetooth and Wi-Fi without using any coexistence mitigation techniques increases the likelihood of significant interference. The coexistence issues associated with it are fundamental to the interference problem, which we have explored extensively in our first white paper. Performance is likely to be significantly degraded for both protocols in this scenario. Figure 3 shows both measured and simulated effects of this approach in the single-user network

© 2001 Mobilian Corporation. All rights reserved.

configuration shown in Figure 2. The first white paper provides extensive details of both the scenario below and simulation details.

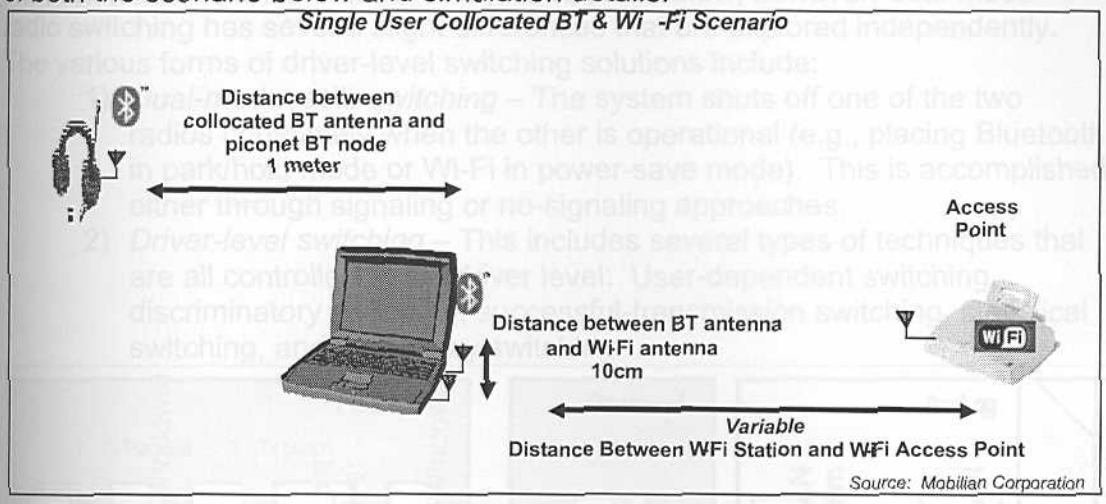


Figure 2 – Geometry of Measurement and Simulation Environment

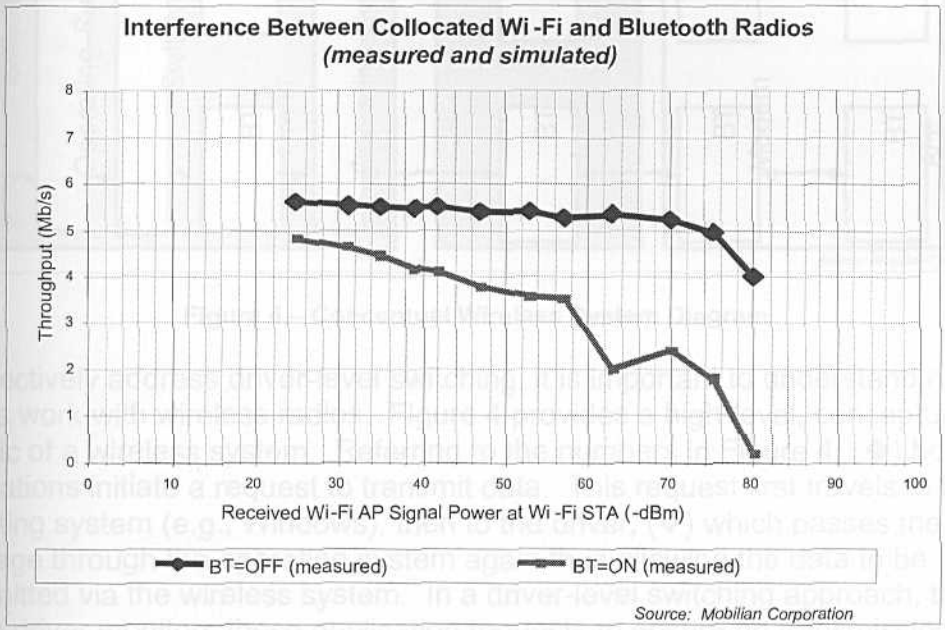


Figure 3 – Measurement of Wi-Fi Throughput in the Presence of Collocated Bluetooth

Driver-level (Modal) Switching Between Wi-Fi and Bluetooth

Overview

Driver-level switching is a time-division approach, essentially dividing the operational periods for each radio, and has many possible implementations.

© 2001 Mobilian Corporation. All rights reserved.

Each different driver-level implementation generally adheres to the characteristics described in the analysis section below; however, dual-mode radio switching has several slight differences that are explored independently. The various forms of driver-level switching solutions include:

1) *Dual-mode radio switching* – The system shuts off one of the two radios completely when the other is operational (e.g., placing Bluetooth in park/hold mode or Wi-Fi in power-save mode). This is accomplished either through signaling or no-signaling approaches.
2) *Driver-level switching* – This includes several types of techniques that are all controlled at the driver level: User-dependent switching, discriminatory switching, successful-transmission switching, statistical switching, and time-delay switching.

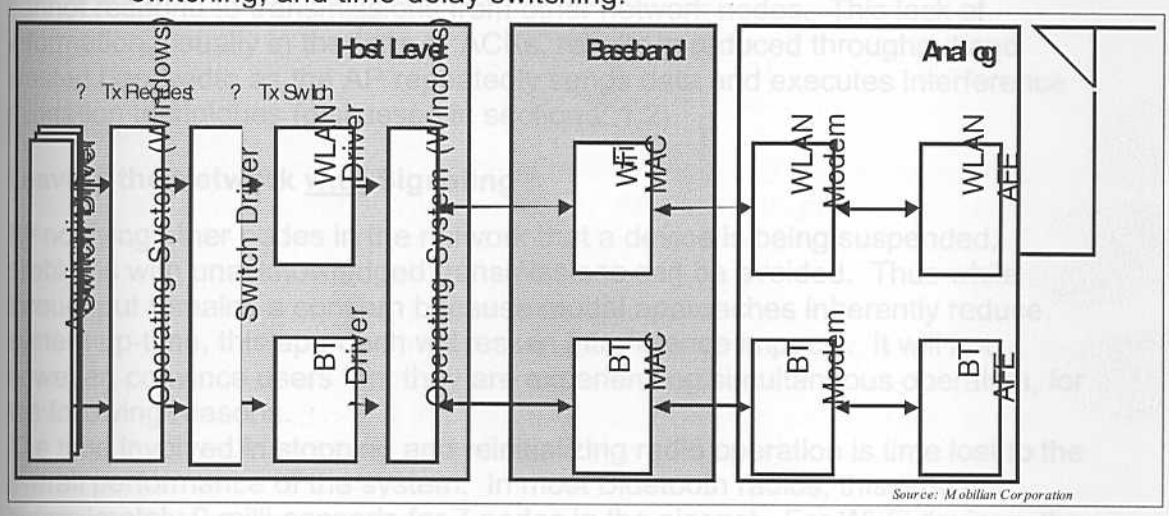


Figure 4 – Conceptual Wireless System Diagram

To effectively address driver-level switching, it is important to understand how drivers work with wireless radios. Figure 4 provides a high-level, conceptual graphic of a wireless system. Referring to the numbers in Figure 4, (◆) host applications initiate a request to transmit data. This request first travels to the operating system (e.g., Windows), then to the driver, (❖) which passes the message through the operating system again thus allowing the data to be transmitted via the wireless system. In a driver-level switching approach, the switch driver monitors these application requests to ensure no transmission collides with another.

Analysis – Dual-mode Radio Switching

Dual-mode Radio Switching

A dual-mode radio switching approach involves shutting one of the two radios off completely when the other is operating (e.g., placing Bluetooth in park/hold mode or Wi-Fi in power-save mode). The radios are never operating simultaneously, and therefore never attempting to simultaneously receive or transmit. This

© 2001 Mobilian Corporation. All rights reserved.

approach avoids interference from Bluetooth polling, an important technical difficulty with other driver-level switching approaches explained in section 3.2.3.2. Dual-mode radio switching can be accomplished either by simply stopping operation of one of the radios with no indication to other devices in the network, or by first signaling that one device is about to be suspended and then stopping operations.

Leaving the Network without Signaling

In a normal operating scenario, radios do not go into these "sleep" modes commonly used for saving power, unless they are not actively participating in the network. When a radio is suspended without signaling to other partner devices, it cannot respond to transmissions from other network nodes. This lack of information, usually in the form of ACKs, results in reduced throughput and wasted bandwidth as the AP repeatedly sends data and executes interference mitigation techniques (discussed in section 2.1.2).

Leaving the Network with Signaling

By notifying other nodes in the network that a device is being suspended, problems with unacknowledged transmissions can be avoided. Thus while throughput remains a concern because modal approaches inherently reduce system up-time, this approach will lessen interference impacts. It will not, however, convince users that they are experiencing simultaneous operation, for the following reasons.

The time involved in stopping and reinitializing radio operation is time lost to the overall performance of the system. In most Bluetooth radios, this time is approximately 9 milli-seconds for 7 nodes in the piconet. For Wi-Fi devices, the amount of time varies according the network configuration, but is generally very short (1-3 milli-seconds). While this is certainly not onerous, the cumulative impact of repeated cycles and associated time delays could easily be noticeable to the end-user.

Neither of these solutions, signaling or no signaling, will manage Bluetooth synchronous-connection-oriented links (SCO), or voice links. Bluetooth SCO links are very timing-sensitive and cannot be interrupted by Wi-Fi activity under this approach. This could potentially lead to poor user experiences when the user is attempting to talk on a Bluetooth headset and simultaneously search for files on the server or intranet using Wi-Fi.

Analysis – Driver-level Switching

Throughput and Time-delay Concerns

An intuitive problem with all modal (on/off) switching is the impact to the protocols' throughput. If a radio is suspended, it is not transmitting or receiving, and therefore the potential throughput is degraded. While this can be significant, it varies according to the differences in implementation. Therefore, we do not

© 2001 Mobilian Corporation. All rights reserved.

address the issue here. Rather, we investigate the more important aspects of the overall approach.

Because driver-level transmit switching occurs at the driver level, and because the transaction time for a driver-level switch to occur is unreliable and lengthy, avoiding collisions with incoming packets is very difficult. The resulting transmission of one protocol during reception of the other causes loss of received packets, interference, and potential user difficulties. This is caused by the driver's dependence on the host operating system, which is generally non-deterministic in its response time (i.e., non-real-time).

Reception of a standard 1500 byte Wi-Fi packet takes approximately 1 to 1.5 milli-seconds. The time required for information to transmit from the baseband to the driver – such as "there is a packet being received – do not transmit" – and for the corresponding driver activity to complete, can be anywhere from 100 micro-seconds to 2 or 3 seconds, or even longer. This is caused by the variable latency inherent in non-deterministic (non-real-time) host operating systems such as Windows, Linux, and Unix.

Host operating systems have variable latency because of the many background activities occurring during normal operation. As the interrupt from the baseband is received by the operating system, it is queued behind other interrupts and requests from other functions. This queue could range from very short to very long in terms of time required for the operating system to process the baseband interrupt. Because of this varied latency, when the operating system processes the request and passes it to the driver, the driver is not able to gauge a proper response. It doesn't "know" if the baseband request was sent 1 micro-second ago, 1 milli-second ago, or 1 second ago. This represents a huge gulf of missing information to Wi-Fi and Bluetooth, which both operate in micro-second intervals. For this reason, basebands do not currently perform this activity and a driver-level approach will potentially transmit at the same time the wireless system is receiving. As we illustrated before in Table 1 and again in Table 2 below, this scenario, one radio transmitting while the other is receiving, causes significant interference.

© 2001 Mobilian Corporation. All rights reserved.

		Bluetooth Tx		Bluetooth Rx	
		In-band	Out-of-band	In-band	Out-of-band
Wi-Fi™ 802.11b	Tx	No Conflict	No Conflict	Strong Interference	Moderate Interference
	Rx	Strong Interference	Moderate Interference	Strong[6] Interference	Moderate Interference

Source: Mobilian Corporation

Table 2: The Interference Cases for Bluetooth and Wi-Fi[6]

Impacts of Bluetooth Polling Activities

As we indicated in our discussion of Bluetooth polling functionality in Section 2.1.1, in most implementations of Bluetooth, in an active piconet, the master Bluetooth node will continuously poll the slaves. "Continuously" means in every available transmit slot or 800 times per second (1 slot request for information, 1 slot opportunity to respond).

As also explained, polling activities are controlled at the Bluetooth MAC layer and don't reach the driver-level; therefore, polling activities cannot be controlled / switched by the driver. Again, this creates significant interference, because Bluetooth will be continuously transmitting while Wi-Fi is attempting to receive. The effect of Bluetooth polling activities on Wi-Fi performance generates significant interference roughly equivalent to that in collocated Wi-Fi and BT radios with no coexistence mechanism as in Figure 3.

Adaptive Hopping

Overview

Recently (11/13/00), a group of companies petitioned the FCC requesting the initial report and order (R&O) for Wideband Frequency Hopping (WBFH), also known as ET Docket 99-231, be amended or reconsidered to allow Bluetooth to hop across as few as 15 1-MHz channels in the 2.4 GHz ISM band. This frequency-division approach, known as adaptive hopping, would theoretically allow modified Bluetooth devices to operate simultaneously with Wi-Fi devices by dividing the frequency band: Bluetooth would operate in one section, and Wi-Fi another, non-overlapping section. This technique is currently permissible under FCC regulations for radios operating under at or below –1.3 dBm of transmit power. The regulation must be changed, however, to allow the typical class 1, 2, and 3 Bluetooth devices to operate in this mode. This represents a significant change to the ISM band rules and requires much more explanation than allowed by the scope of this paper. However, we have provided a brief overview of several important aspects of this petition and the adaptive hopping approach.

[6] See footnote 5.

© 2001 Mobilian Corporation. All rights reserved.

Analysis

Adaptive hopping will provide a viable and important solution to 802.11b and Bluetooth coexistence, provided it is quickly ratified through the appropriate regulatory processes, and its recommended implementation of its intelligent adaptive hopping algorithms is well thought out. The timeliness of the regulatory process is primarily a function of the integrity of the adaptive hopping petition. If it adequately addresses the potential issues discussed in the following sections, the process should be relatively quick. However, if the petition's implementation recommendations are ambiguous, and do not adequately address the issues below, the regulatory process will likely be protracted while these important details are resolved. Regardless of the ratification timing, when passed, Bluetooth adaptive hopping will provide an excellent coexistence solution in environments with two or fewer Bluetooth piconets and no overlapping Wi-Fi networks.

Adaptive Hopping as Optional Profile (Operational Mode)

Bluetooth specification 1.0 and 1.1 do not require adaptive hopping functionality and therefore use all 79 available 1-MHz hop channels. This, of course, creates interference for any closely located Wi-Fi network, and is the core of the issue addressed by adaptive hopping. Over the next year, Cahners In-Stat estimates approximately 30 million Bluetooth devices will come to market, all theoretically under Bluetooth specification 1.1. Given that future Bluetooth devices will need to communicate with these legacy devices, the adaptive hopping petition is likely to be passed as an optional function or profile. Therefore, Bluetooth developers will not be required to include the adaptive hopping profile and may choose to eliminate it to get to market faster or optimize their product cost.

The complication arises from the fact that, when it comes to hop pattern, Bluetooth piconets must operate at the lowest common denominator. Thus, a Bluetooth device with the optional adaptive hopping functionality will be forced to bypass the mechanism and use all 79 channels if there is even one unmodified Bluetooth device in its piconet. Furthermore, since the majority of current and foreseeable Bluetooth implementations will perform the hop selection in the hardware, it will be very difficult to retroactively modify them for adaptive hopping. Accomplishing the modification would probably require a new spin or release of the Bluetooth device hardware.

This series of timing issues represents a significant consideration for adaptive hopping's universal effectiveness as a coexistence solution. There are other, more technical considerations that must also be addressed for adaptive hopping to achieve its full potential.

Adaptive Hopper Must Accurately Sense and Respond to Interferers

It appears that adaptive hopping Bluetooth devices will move into adaptive hopping mode based on one or more of several possible interference detection mechanisms. The petition does not currently specify which approach will be

© 2001 Mobilian Corporation. All rights reserved.

recommended in the Bluetooth profile, but four of the many possible technical approaches are:

1) The Bluetooth device gradually adapts its normal operation hop pattern based on observed packet loss;
2) The Bluetooth device detects and assesses received signal strength across its wireless environment before commencing operation;
3) The Bluetooth device transmits a "test" pattern of packets across the entire spectrum, observes the ratio of lost packets across available channels and locates its adapted piconet in the least active or interference-prone channel; and
4) The Bluetooth device is collocated with a Wi-Fi device, and can receive the Wi-Fi passband location from the Wi-Fi device, so it simply avoids operating within the Wi-Fi passband.

Given that under the current petition the adaptive hopping Bluetooth device must reassess its restricted mode every 30 seconds, all of these approaches will eventually result in low interference operating scenarios. However, with the exception of the last, they all have the potential to exacerbate interference problems under certain conditions.

Bluetooth™ Difficulty in Detecting Wi-Fi™ Signal

If the Bluetooth device is attempting to modify its normal 79 MHz hop pattern based on observed packet failure rates, it could create significant interference for a closely located Wi-Fi device, but have difficulty detecting interference to its own signal, and therefore not move into adaptive mode. This is caused by a combination of factors, including Wi-Fi transmit power, the distance between the Bluetooth and Wi-Fi devices, and the Bluetooth receive filter.

Consider the following scenario using the path loss model from A. Kamerman's 1999 work[7]. A Wi-Fi AP and station are transmitting at +15 dBm and are separated by approximately 15 meters, resulting in received signal strength of – 52.5 dBm at either device. If a 0 dBm Bluetooth piconet is within 5 meters of either Wi-Fi device, it will create debilitating interference for the Wi-Fi network but will not sense interference to its own signal until it is within approximately 1.3 meters of the Wi-Fi transmitter (AP or station).

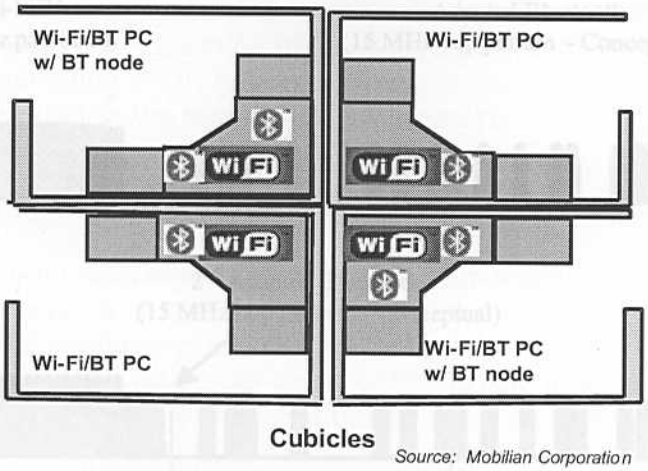
This occurs because, with 5 meters separation between the Bluetooth and Wi-Fi device, the Bluetooth signal reaches the Wi-Fi device at approximately – 54 dBm, resulting in an intolerable signal-to-noise ratio. On the other hand, the Bluetooth receive filter's noise reduction effects on the Wi-Fi signal allow the Bluetooth piconet to continue operating without significant error rates, even when it is within ~ 1.3 meters of the +15 dBm Wi-Fi transmitter. The Bluetooth receive filter reduces the Wi-Fi signal by 13 dB; therefore, at 1 meter from the Wi-Fi transmitter, the +15 dBm transmission is perceived by the Bluetooth as – 38 dBm[8]. At ~ 1.3 meters, the perceived Wi-Fi signal (noise) reaches approximately – 40 dBm, and the Bluetooth device suffers increased packet error rates and can modify its hop pattern. This creates significant opportunities for continued interference, particularly in wireless corporate scenarios with multiple networks, as depicted in Figure 5.

[7] Please see Appendix 2 for explanation of the path loss models employed.

[8] + 15 dBm – 40 dB – 13 dB = – 38 dBm

© 2001 Mobilian Corporation. All rights reserved.

While multiple network environments are not commonplace in today's market, Figure 5 shows a very likely corporate environment in which multiple Wi-Fi networks and Bluetooth piconets will likely arise[9]. In this scenario, enterprise cubicles are configured back-to-back with Wi-Fi/Bluetooth-enabled PCs in each corner, and with each user having an active or potentially active Bluetooth piconet with their PDA/cell phone or Bluetooth enabled peripherals.



Source: Mobilian Corporation

Figure 5 – Basic Geometry of Bluetooth and Wi-Fi Penetrated Corporation

Congested Wireless Environments are Particularly Troublesome

In a congested wireless environment, a newly introduced adaptive hopping Bluetooth device could have difficulty identifying the optimal location for its piconet. This is particularly relevant in situations where an existing adapted Bluetooth piconet already exists.

As mentioned earlier, interference to Bluetooth is greatest when the collocated Bluetooth radio is receiving while the Wi-Fi is transmitting, although this is not usually the case. In a typical wireless network usage scenario, a Wi-Fi station, such as a desktop or laptop PC, receives far more information from the access point (AP) than it transmits. This is known as an asymmetric usage model and is widely accepted as the dominant usage scenario for many networks.

Network asymmetry lessens the likelihood of interference from Wi-Fi to the Bluetooth because it is more likely that the Bluetooth is being subjected to a non-interfering, attenuated signal from the Wi-Fi AP rather than a relatively strong signal from the closely located Wi-Fi station. The Wi-Fi station transmits infrequently, and generally in the form of relatively short ACKs (less than 0.2 milli-seconds). This generates an interesting dichotomy wherein the adaptive hopper is likely to "choose" to operate directly in a Wi-Fi passband if there is already a BT adaptive hopping network in the environment. We explore this

[9] Figure 5 shows a potential corporate deployment/configuration of Wi-Fi and Bluetooth, developed in collaboration with a leading PC OEM. The Wi-Fi stations communicate with an Access Point (AP). The Wi-Fi stations are also equipped with Bluetooth radios communicating with another Bluetooth node (potentially a headset, PDA, etc.) Additional Bluetooth piconets can be active in adjacent cubicles.

© 2001 Mobilian Corporation. All rights reserved.

complication using the corporate environment in Figure 5, and considering the Bluetooth adaptive hopping mechanisms of detecting received signal strength and the transmission of test packets.

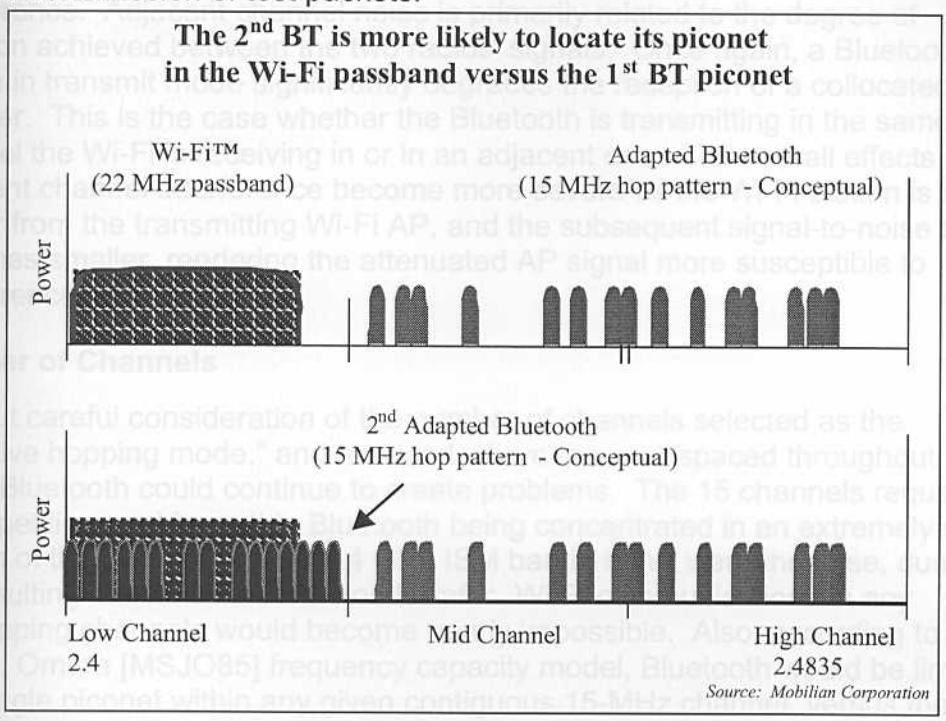


Figure 6 – Likely Location of Two Adaptive Hoppers

If the Bluetooth uses a test packet mechanism, the Bluetooth radio transmits any number of packets across the entire spectrum and gauges the most attractive channel based on the number of lost packets in each. According to testing of actual Wi-Fi networks and statistical calculation of Bluetooth hopping patterns, 0.06% of Bluetooth test packets would be lost in the Wi-Fi passband versus 1.27% in the occupied Bluetooth piconet band, thus leading the Bluetooth to locate its adapted piconet within the Wi-Fi passband, creating catastrophic interference. This has to do with common network operational characteristics such as percentage of time each network is in operating, length of transmissions, and interferer signal strength. Calculations yield similar results if the Bluetooth uses received signal strength indicators. Further details regarding these calculations are available from Mobilian Corporation.

While this example illustrates an environment with a single Wi-Fi network and two Bluetooth piconets, in future corporate environments, this could easily grow to multiple Bluetooth piconets and Wi-Fi networks, making the problem worse.

© 2001 Mobilian Corporation. All rights reserved.

Adjacent-Channel Noise [10]

Adaptive hopping does not adequately address adjacent channel, or out-of-band, interference. Adjacent channel noise is primarily related to the degree of isolation achieved between the two radios' signals. Once again, a Bluetooth device in transmit mode significantly degrades the reception of a collocated Wi-Fi receiver. This is the case whether the Bluetooth is transmitting in the same channel the Wi-Fi is receiving in or in an adjacent one. The overall effects of adjacent channel interference become more severe as the Wi-Fi station is moved further from the transmitting Wi-Fi AP, and the subsequent signal-to-noise ratio becomes smaller, rendering the attenuated AP signal more susceptible to interference.

Number of Channels

Without careful consideration of the number of channels selected as the "adaptive hopping mode," and how and where they are spaced throughout the band, Bluetooth could continue to create problems. The 15 channels requested in the petition could result in Bluetooth being concentrated in an extremely small portion of the 83.5 MHz-wide 2.4 GHz ISM band. If this were the case, due to the resulting concentrated Bluetooth traffic, Wi-Fi communications in any overlapping channels would become nearly impossible. Also, according to the Simon, Omura [MSJO85] frequency capacity model, Bluetooth would be limited to a single piconet within any given contiguous 15-MHz channel, versus the 8-10 piconet capacity under current regulations.

MAC-level Switching

Overview

MAC-level switching describes switching functionality at the baseband level. The solution is either integrated into the two protocols' basebands or in a self-contained module that communicates with both basebands and provides switching functionality "remotely." Mobilian presented this "remote" MAC-level functionality as a proposed coexistence mechanism at the November 2000 meeting of the IEEE 802.15.2 task group. The proposal, dubbed MEHTA, was very well received and will be voted on as a recommended best practice in the coming months.

Analysis

MAC-level switching is performed in the baseband and basically performs the same functionality as driver-level switching, but at a much faster rate and with predictable latency. Consequently, it is able to mitigate many of the interference factors that driver-level switching cannot. MAC-level switching does not suffer

[10] For further explanation of adjacent-channel noise, and in-band and out-of-band noise, please see the appendix.

© 2001 Mobilian Corporation. All rights reserved.

from transmitting signals into incoming receptions, Bluetooth polling, or operating system latency. However, like many of the previous approaches, it is susceptible to adjacent-channel interference and therefore does suffer some degradation. Also, a MAC-level approach will have a long development cycle time relative to a driver-level switching approach, and is pertinent only in systems employing both technologies in a very small, if not integrated, area. Such systems also typically have long development cycles.

Simultaneous Operation

Overview

Simultaneous operation is the ability for different, fully standards-compliant wireless systems to operate simultaneously in a collocated scenario while experiencing minimal or no performance degradation. Simultaneous operation also refers to devices able to offer the user outstanding performance without a list of operational caveats. The device should "just work," regardless of other devices within its operating environment.

Simultaneous operation of Wi-Fi and Bluetooth will occur more and more frequently as users begin completing everyday tasks such as copying or printing a file from their Wi-Fi PC while using a Bluetooth-enabled mouse and keyboard. Its frequency will continue to grow as personal communication devices and synchronization activities with PCs and networks grow, and it will gain even more importance as distributed applications take off – "the next big thing in software" – and Bluetooth devices must coexist with massive amounts of Wi-Fi network activity.

In all these scenarios, users will appreciate being able to use whatever wireless devices surround them, when they want to and how they want to. Users will demand "Coexistence without Compromise"™, and will resist adopting wireless devices as long as there are operational difficulties or perceived concerns.

© 2001 Mobilian Corporation. All rights reserved.

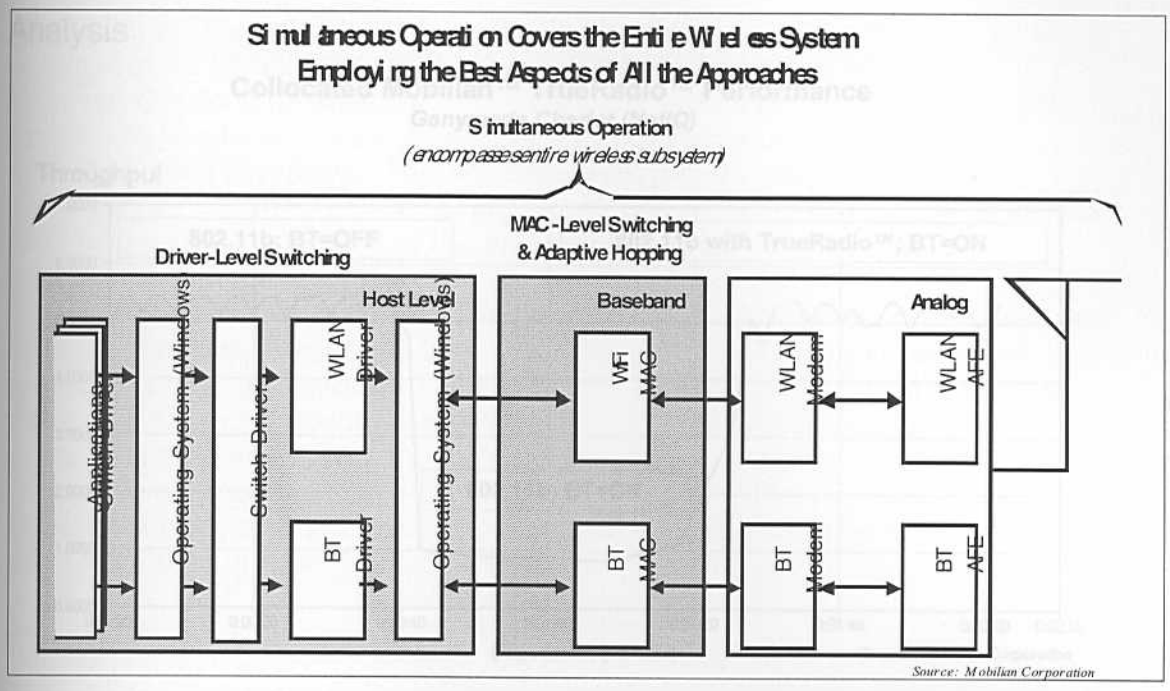


Figure 7 – Simultaneous Operation Covers Entire Conceptual Wireless System Diagram

We believe that true, sustainable simultaneous operation can only be achieved by taking a system-level approach encompassing the entire wireless sub-system. This design methodology allows the solution to selectively use the best aspects of each technique or techniques, depending on its environment and the required usage models.

For example, a driver-level switching technique may generate the best user experience in a low bandwidth synchronization scenario, while MAC-level switching will manage interference much more effectively for SCO traffic, or when a user has wireless peripherals such as speakers or a keyboard. Further, in future environments of distributed computing / applications, a system-level approach may be required to effectively allow SCO traffic while manipulating server-side office productivity applications.

Mobilian Corporation developed its first product, TrueRadio™, using a system-level methodology, and will continue development under this methodology with subsequent, multi-standard radio products.

© 2001 Mobilian Corporation. All rights reserved.

Analysis

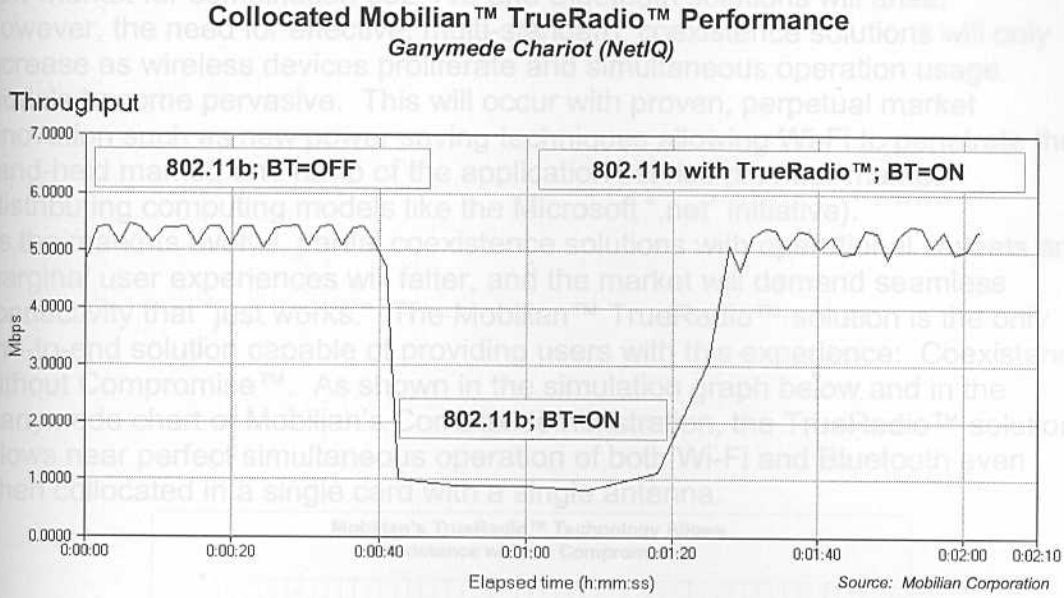


Figure 8 – Ganymede Chariot Graph of Mobilian Corporation's TrueRadio™ Demonstration

Mobilian Corporation's TrueRadio™ technology allows simultaneous operation by using technical enhancements across every aspect of the wireless sub-system, from antenna to application. It incorporates many of the best characteristics of the techniques described above, as well as other advanced technology not addressed here. By doing so, it is able to provide fully-standards-compliant Wi-Fi and Bluetooth radios capable of seamless, transparent operation under virtually any scenario, all without compromise to the end-user. Additionally, because of the high degree of integration in the Mobilian™ TrueRadio™ solution, the expected cost of the solution is substantially less than simple collocation of two chipsets or independent cards.
Mobilian demonstrated[11] its TrueRadio™ technology under NDA at Comdex 2000 with very successful results and excellent market response. The TrueRadio™ technology eliminated virtually all interference as shown by the Ganymede[12] chart in Figure 8.

Summary

The market is rapidly moving toward resolving the coexistence concerns surrounding Wi-Fi and Bluetooth. The variety of approaches discussed in this paper will likely address the issue prior to it ever affecting the end-user.

[11] The technology demonstration used a notebook computer with collocated Bluetooth and Wi-Fi radios. The Wi-Fi AP antenna was covered in attenuating material simulating an office environment with forty-five feet between the STA and AP with 8 cubicle walls. The partner Bluetooth node was located 1 meter away.

[12] Ganymede Chariot software is used by WECA in the Wi-Fi certification process. It measures the throughput for wireless LAN systems by monitoring and calculating the time required to transmit a 1MB file from the AP to the STA. Ganymede was recently acquired by NetIQ.

© 2001 Mobilian Corporation. All rights reserved.

Consequently, market forecasts for Bluetooth and Wi-Fi will remain strong, and a new market for combination 802.11b and Bluetooth solutions will arise. However, the need for effective, multi-standard, coexistence solutions will only increase as wireless devices proliferate and simultaneous operation usage models become pervasive. This will occur with proven, perpetual market innovation such as new power saving techniques allowing Wi-Fi to penetrate the hand-held market, and ramp of the application service provider market (distributing computing models like the Microsoft ".net" initiative).
As the markets evolve, partial coexistence solutions with operational caveats and marginal user experiences will falter, and the market will demand seamless connectivity that "just works." The Mobilian™ TrueRadio™ solution is the only end-to-end solution capable of providing users with this experience: Coexistence without Compromise™. As shown in the simulation graph below and in the Ganymede chart of Mobilian's Comdex demonstration, the TrueRadio™ solution allows near perfect simultaneous operation of both Wi-Fi and Bluetooth even when collocated in a single card with a single antenna.

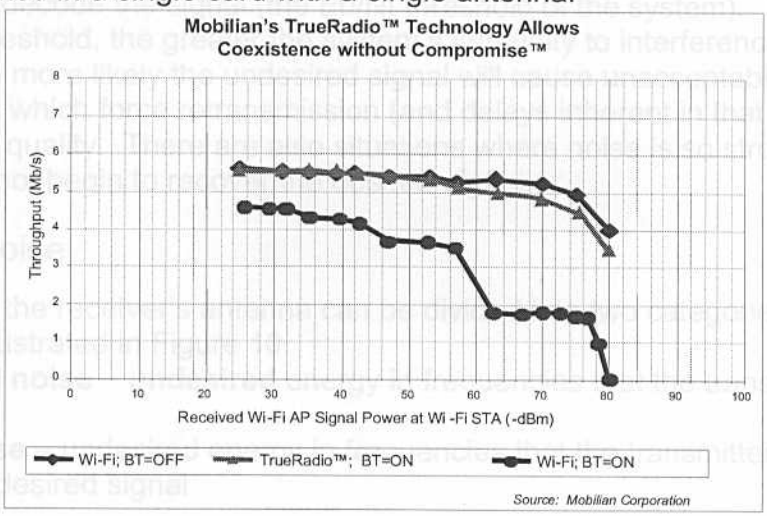


Figure 9 – Mobilian's TrueRadio™ Performance in Collocated Scenario

© 2001 Mobilian Corporation. All rights reserved.

Appendix 1 – In-band versus Out-of-band Noise

Signals and Noise

Every wireless communication system, by definition, consists of at least two nodes. At any given time, one node transmits (a transmitter) and the other receives (a receiver)[13]. Successful system operation depends on the receiver's ability to separate a desired signal from an undesired signal. This depends on the ratio between the energy of desired signal and the total noise (interference) at the receiver's antenna. This ratio is referred to as Eb/Nt (energy per bit over total noise) or SNR (signal-to-noise ratio). The receiver's job is to maximize the ability to decode desired signals while minimizing the ability to allow undesired signals (noise) to interfere. One of the most important characteristics of a communication system is the minimum SNR at which the receiver can still successfully decode the signal (the Eb/Nt threshold of the system). The lower the Eb/Nt threshold, the greater the system's immunity to interference. The lower the SNR, the more likely the undesired signal will cause unacceptable errors in data packets which force retransmission (and delays inherent in that process), or impact voice quality. There are also situations where noise is so strong that the receiver cannot begin to recover the desired signal.

Types of Noise

The noise at the receiver's antenna can be divided into two categories defined below and illustrated in Figure 10.

Out-of-band noise – undesired energy in frequencies that the transmitter does not use; and

In-band noise – undesired energy in frequencies that the transmitter used to transmit the desired signal

[13] Both 802.11 and Bluetooth stations transmit or receive (half duplex systems); there are other systems where a station transmits and receives at the same time (full duplex systems); the discussion bellow applies to both type of systems.

© 2001 Mobilian Corporation. All rights reserved.

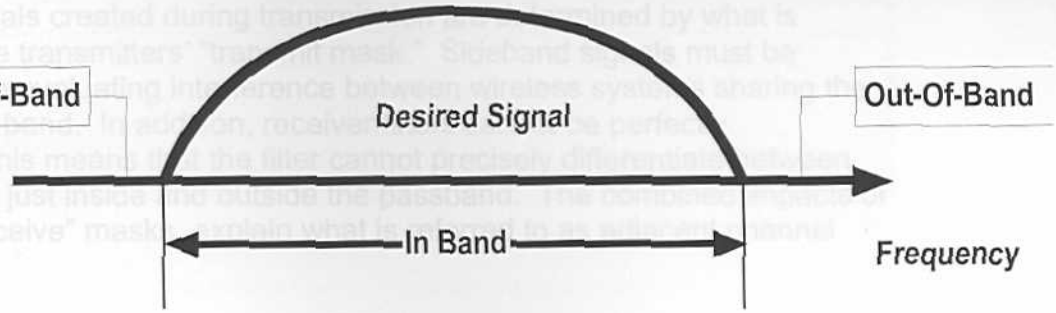


Figure 10 – In-Band versus Out-Of-Band Noise

Both in-band and out-of-band noise can degrade a wireless communications system's performance. Out-of-band noise can usually be filtered out because the energy in the system's frequency band does not carry any useful information. In-band noise, is much more problematic.

Noise can be further categorized as either "white" or "colored." White noise is a collection of energies transmitted from many different sources without any coordination between them. This energy is typically distributed evenly across the frequency band and does not have any deterministic behavior over time or frequency. Colored noise is transmitted from intentional radiators and has a specific behavior in time and frequency. Figure 11 * MERGEFORMAT illustrates the difference between white and colored noise.

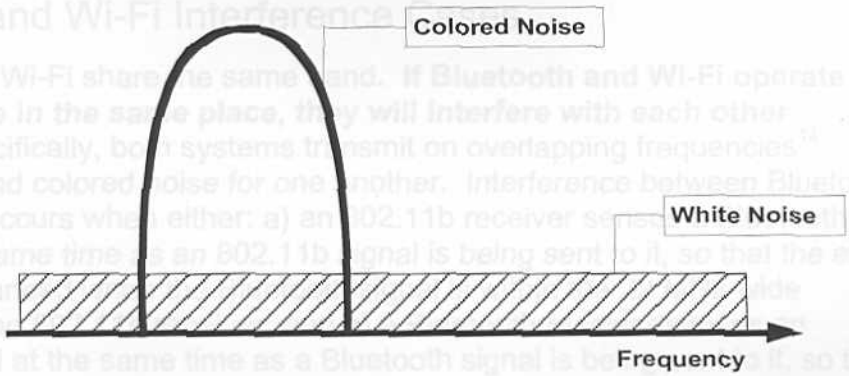


Figure 11 – White Noise and Colored Noise are Very Different

Most wireless communication systems assume that the only type of in-band noise is white noise. Other intentional radiators are assumed to transmit out-of-band. Receiver designs with their associated filtering techniques are optimized around these assumptions. Unfortunately, in a case where two intentional radiators such as Bluetooth and Wi-Fi both share the same frequency band, receivers must also address the case of in-band, colored noise.

Every transmitter is supposed to transmit only within a limited bandwidth; however, this is not physically possible without injecting noise into adjacent frequencies (sideband signals), as shown in Figure 12. The amount and nature

© 2001 Mobilian Corporation. All rights reserved.

of sideband signals created during transmission are determined by what is referred to as the transmitters' "transmit mask." Sideband signals must be considered when evaluating interference between wireless systems sharing the same frequency band. In addition, receiver filters cannot be perfectly "rectangular." This means that the filter cannot precisely differentiate between signal and noise just inside and outside the passband. The combined impacts of transmit and "receive" masks, explain what is referred to as adjacent channel interference.

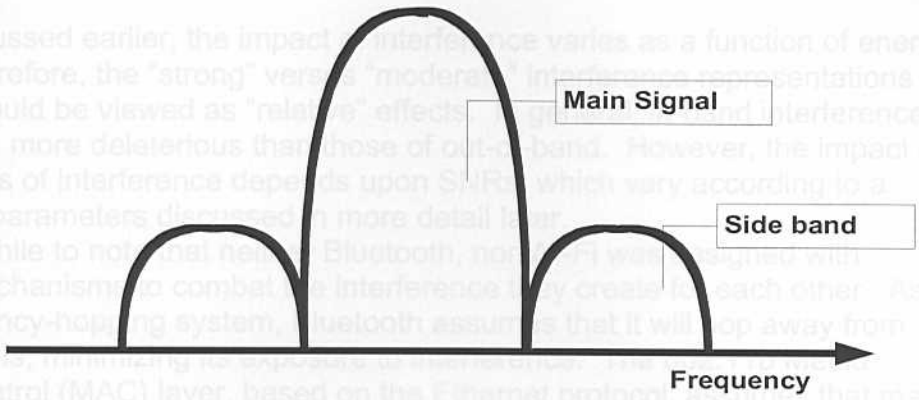


Figure 12 – Typical Transmit Mask

Bluetooth and Wi-Fi Interference Cases

Bluetooth and Wi-Fi share the same band. **If Bluetooth and Wi-Fi operate at the same time in the same place, they will interfere with each other (collide).** Specifically, both systems transmit on overlapping frequencies[14], creating in-band colored noise for one another. Interference between Bluetooth and 802.11b occurs when either: a) an 802.11b receiver senses a Bluetooth signal at the same time as an 802.11b signal is being sent to it, so that the effect is most pronounced when the Bluetooth signal is within the 22 MHz-wide passband of the 802.11b receiver; and b) a Bluetooth receiver senses an 802.11b signal at the same time as a Bluetooth signal is being sent to it, so that the effect is most pronounced when the 802.11b signal is within the passband of the Bluetooth receiver. These time-frequency collisions are summarized in the following table:

[14] We also need to take into account the sidebands of each transmission.

© 2001 Mobilian Corporation. All rights reserved.

		Bluetooth Tx		Bluetooth Rx	
		In-band	Out-of-band	In-band	Out-of-band
Wi-Fi™	Tx	No Conflict	No Conflict	Strong Interference	Moderate Interference
802.11b	Rx	Strong Interference	Moderate Interference	Strong[15] Interference	Moderate Interference

Source: Mobilian Corporation

Table 3: The Interference Cases for Bluetooth and Wi-Fi[15]

As we discussed earlier, the impact of interference varies as a function of energy ratios. Therefore, the "strong" verses "moderate" interference representations in Table 3 should be viewed as "relative" effects. In general, in-band interference impacts are more deleterious than those of out-of-band. However, the impact of both classes of interference depends upon SNRs, which vary according to a number of parameters discussed in more detail later.

It is worthwhile to note that neither Bluetooth, nor Wi-Fi was designed with specific mechanisms to combat the interference they create for each other. As a fast, frequency-hopping system, Bluetooth assumes that it will hop away from bad channels, minimizing its exposure to interference. The 802.11b Media Access Control (MAC) layer, based on the Ethernet protocol, assumes that many stations share the same medium, and if a transmission fails it is because two Wi-Fi stations tried to transmit at the same time. Later, we will discuss how this assumption drives system behavior that actually worsens the impact of interference from Bluetooth.

[15] See Footnote 5.

© 2001 Mobilian Corporation. All rights reserved.

Appendix 2 – Path Loss Models Employed

The idea of proximity is critical for this analysis. Since radio-frequency signals expand outward from the antenna in roughly spherical waves, the signal strength decreases rapidly with the distance from the transmitting antenna. This path-loss profile is proportional to the reciprocal of the squared distance from the antenna at short ranges, and attenuates more sharply in indoor environments at a distance of a few meters from the antenna, as reflection effects become apparent. The following path-loss models (Lp in dB) will be used [Kam99]:

$$Lp = -40.0 - 20\log(d), \text{ when } d <= 8 \text{ meters}$$

$$Lp = -58.5 - 33\log(d/8), \text{ when } d > 8 \text{ meters}$$

Using these empirical models, the loss profile can be plotted vs. distance as shown in Figure 13. A communication system must overcome this path loss using a combination of transmission power and receiver sensitivity to meet a desired signal-to-noise or signal-to-interference ratio criterion, which in turn translates into a probability of error. If the received signal strength is not adequate to overcome either noise or interference, unacceptable packet errors result and system throughput and latency will deteriorate.

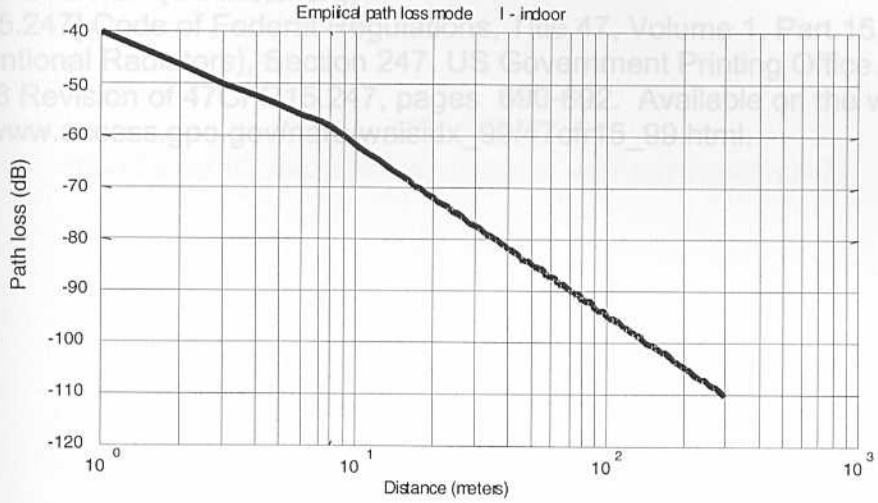


Figure 13 – Path Loss as a Function of Distance, Indoor, 2.4-GHz ISM Band

References

[CIS00a] Cahners In-Stat, *Bluetooth 2000 – To Enable the Star Trek Generation*, July 2000

[CIS00b] Cahners In-Stat, based on preliminary data to be published in December 2000

[MBLN01] Mobilian Corporation, *Wi-Fi™ (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem*, November 2000

[NGFM00] Nada Golmie and F. Mouveraux, *WPAN Coexistence Performance Evaluation: MAC Simulation Environment and Preliminary Results*. IEEE 802.15-00/066r0, March 2000.

© 2001 Mobilian Corporation. All rights reserved.

[SS00] S. Shellhammer, *Packet Error Rate of an IEEE 802.11 WLAN in the Presence of Bluetooth*. IEEE 802.15-00/133r0, May 2000.
[GE98] G. Ennis, *Impact of Bluetooth on 802.11 Direct Sequence*. IEEE 802.11-98/319, September 1998.
[JZ98] J. Zyren, *Extension of Bluetooth and 802.11 Direct Sequence Model*. IEEE 802.11-98/378, November 1998.
[JZ99a] J. Zyren, *Reliability of IEEE 802.11 Hi Rate DSSS WLANs in a High Density Bluetooth Environment*. Bluetooth '99, June 8, 1999.
[JZ99b] J. Zyren, *Reliability of IEEE 802.11 WLANs in Presence of Bluetooth Radios*. IEEE 802.15-99/073r0, September 1999.
[BT99] Specification of the Bluetooth System, version 1.0B, December 1, 1999.
[Kam99] A. Kamerman, "*Coexistence between Bluetooth and IEEE 802.11 CCK Solutions to Avoid Mutual Interferenc,e*" Lucent Technologies Bell Laboratories, Jan. 1999, also available as IEEE 802.11-00/162, July 2000.
[MSJO85] M.K. Simon, J. Omura, R. Scholtz, and K. Levitt, *Spread Spectrum Communications Vol. I, II, III*. Rockville, MD. Computer Science Press, 1985.
[ETSI99] ETR0230002 V0.2.0 (1999-04) Broadband Radio Access Networks (BRAN); High Performance Radio Local Area Networks (HIPERLAN) Type 2; System Overview (www.etsi.org)
[FCC15.247] Code of Federal Regulations, Title 47, Volume 1, Part 15, Subpart C (Intentional Radiators), Section 247. US Government Printing Office. October 1, 1998 Revision of 47CFR15.247, pages 690-692. Available on the web at: http://www.access.gpo.gov/nara/waisidx_99/47cfr15_99.html.

© 2001 Mobilian Corporation. All rights reserved.

ANEXO D

Wi-Fi and BLuetooth Coexistence without compromise

Wi-Fi™ (802.11b) and Bluetooth™:

An Examination of Coexistence Approaches

Mobilian Corporation

7431 NW Evergreen Parkway, Suite 220

Hillsboro, Oregon 97124

(503) 681-8600

www.mobilian.com

Abstract

This paper analyzes different approaches to resolving the interference problems between the Wi-Fi™ and Bluetooth™ wireless technologies. This analysis explores the strengths and weaknesses of these interference mitigation approaches, and goes on to explain what is necessary for achieving satisfactory combination performance and true "Coexistence without Compromise"™. The contents are based on Mobilian Corporation's coexistence research and development work, including a thorough analysis of the problems and various experiments to understand the interference issue.

In investigating different approaches to interference mitigation, this paper gives technical data and uses common wireless technology terms. The information presented is targeted to readers who have a basic understanding of wireless networking. We recommend that readers without this understanding read Mobilian's first white paper: *Wi-Fi (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem (www.mobilian.com)*.

Mobilian™, TrueRadio™, Sim-OP™, TrueConnectivity™, and Coexistence without Compromise™ are all trademarks of Mobilian Corporation. All other trademarks are the property of their respective owners.

©2001 Mobilian Corporation. All rights reserved.

Table of Contents

1.0 Executive Summary **4**

2.0 Background **5**

2.1 Technical Background 5

2.1.1 Bluetooth™ Wireless Personal Area Networking (WPAN) 5

2.1.2 802.11b Wireless Local Area Networking (Wi-Fi™) 6

2.1.3 Wi-Fi™ / Bluetooth™ Interaction and Interference 6

3.0 Interference Mitigation Approaches **8**

3.1 Collocation without Coexistence Mechanism 9

3.1.1 Overview 9

3.1.2 Analysis 9

3.2 Driver-level (Modal) Switching Between Wi-Fi and Bluetooth 10

3.2.1 Overview 10

3.2.2 Analysis – Dual-mode Radio Switching 11

3.2.2.1 Dual-mode Radio Switching 11

3.2.2.2 Leaving the Network without Signaling 11

3.2.2.3 Leaving the Network with Signaling 11

3.2.3 Analysis – Driver-level Switching 12

3.2.3.1 Throughput and Time-delay Concerns 12

3.2.3.2 Impacts of Bluetooth Polling Activities 13

3.3 Adaptive Hopping 13

3.3.1 Overview 13

3.3.2 Analysis 13

3.3.2.1 Adaptive Hopping as Optional Profile (Operational Mode) 14

3.3.2.2 Adaptive Hopper Must Accurately Sense and Respond to Interferers 14

3.3.2.2.1 Bluetooth™ Difficulty in Detecting Wi-Fi™ Signal 14

3.3.2.2.2 Congested Wireless Environments are Particularly Troublesome 15

3.3.2.3 Adjacent-Channel Noise 17

3.3.2.4 Number of Channels 17

3.4 MAC-level Switching 17

3.4.1 Overview 17

3.4.2 Analysis 17

3.5 Simultaneous Operation 17

3.5.1 Overview 17

©2001 Mobilian Corporation. All rights reserved.

3.5.2 Analysis 19
4.0 Summary **19**
5.0 Appendix 1 – In-band versus Out-of-band Noise **21**
5.1 Signals and Noise 21
5.1.1 Types of Noise 21
5.2 Bluetooth and Wi-Fi Interference Cases 23
6.0 Appendix 2 – Path Loss Models Employed **24**
References **25**

Table of Figures

Figure 1 – Performance Hierarchy of Coexistence Approaches for Collocated Wi-Fi & Bluetooth 8
Figure 2 – Geometry of Measurement and Simulation Environment 9
Figure 3 – Measurement of Wi-Fi Throughput in the Presence of Collocated Bluetooth 10
Figure 4 – Conceptual Wireless System Diagram 11
Figure 5 – Basic Geometry of Bluetooth and Wi-Fi Penetrated Corporation 15
Figure 6 – Likely Location of Two Adaptive Hoppers 16
Figure 7 – Simultaneous Operation Covers Entire Conceptual Wireless System Diagram 18
Figure 8 – Ganymede Chariot Graph of Mobilian Corporation's TrueRadio™ Demonstration 19
Figure 9 – Mobilian's TrueRadio™ Performance in Collocated Scenario 20
Figure 10 – In-Band versus Out-Of-Band Noise 21
Figure 11 – White Noise and Colored Noise are Very Different 22
Figure 12 – Typical Transmit Mask 22
Figure 13 – Path Loss as a Function of Distance, Indoor, 2.4-GHz ISM Band 24

© 2001 Mobilian Corporation. All rights reserved.

1.0 Executive Summary

Wireless markets, from wide area networks, to local and personal area networks, are widely expected to be the significant market of the 21st Century. Investment capital is flowing to wireless companies worldwide, and market forecasts consistently project hundreds of millions of installed units. With this expansion comes increased opportunity for market innovation, and consequently, wireless penetration into the core fabric of our everyday lives.

This growth is spurred by increasing demand for maximum convenience and immediate access to desired information. It is facilitated by an unlicensed frequency spectrum, providing unlimited, free access to whomever wishes to build a wireless device capable of complying with regulatory standards. These forces are working together to create traffic and device density in the unlicensed frequencies, and consequently opportunities for interference between the protocols using those frequencies.

As these trends develop, the need for multiple wireless devices operating at the same time will increase, resulting in still greater potential for interference. That is why "simultaneous operation" is becoming an important topic of discussion in today's market.

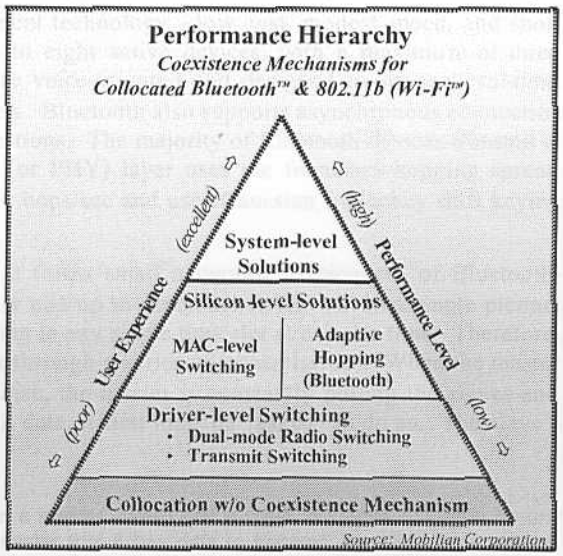
Simultaneous operation is the ability of different, fully standards-compliant wireless systems to operate simultaneously in any scenario, while experiencing minimal or no degradation in performance. This definition includes wireless devices that can give the user outstanding performance without a list of operational caveats. The device should "just work," regardless of other devices within its operating environment.

Wireless local area networking (WLAN) and wireless personal area networking (WPAN) are two networks in particular for which simultaneous operation is growing in importance. WLAN / WPAN simultaneous operation will occur more and more frequently as users begin completing everyday tasks such as copying or printing a file from their WLAN PC while using a WPAN-enabled mouse and keyboard. Its frequency will continue to grow as personal communication devices and synchronization activities with PCs and networks grow, and it will gain even more importance as distributed applications take off – "the next big thing in software" – and WPAN devices must coexist with massive amounts of WLAN activity.

In all these scenarios, users will appreciate being able to use whatever wireless devices surround them, when they want to, and how they want to. Users will demand unhindered simultaneous operation and will resist adopting wireless devices as long as there are operational problems or perceived concerns.

With this certainty facing the market today, regulatory bodies, standards bodies, and industry participants are begun several approaches to achieving simultaneous operation, including:

1) Simple collocation (combo-card reference designs);
2) Approaches in the host software (driver-level switching and dual-mode radios)
3) Approaches in the MAC layer (MAC-level switching and adaptive hopping); and
4) System-level solutions covering the entire wireless sub-system, and incorporating the best aspects of many different approaches.



Each technique's strengths and weaknesses are explored in depth in the following pages. In summary, based on exploration and assessment of each technique's interference management ability, true, sustainable simultaneous operation can only be achieved by taking a system-level approach across the entire wireless sub-system. This allows the simultaneous operation solution to selectively use the best aspects of all the techniques, and therefore manage interference extremely well. This is the approach Mobilian Corporation has employed with its first product, TrueRadio™.

© 2001 Mobilian Corporation. All rights reserved.

2.0 Background

The 2.4 GHz Industrial, Scientific, and Medical (ISM) band is poised for strong growth. Fueling this growth are two emerging wireless technologies: WPAN and WLAN. The WPAN category is led by a short-range wireless technology called Bluetooth™. Designed principally for cable replacement applications, most Bluetooth implementations support a range of roughly 10 meters, and throughput up to 721 Kbps for data or isochronous voice transmission. Bluetooth is ideal for applications such as wireless headsets, wireless synchronization of PDAs with PCs, and wireless PC peripherals such as printers, keyboards, or mice. Cahners In-Stat predicts shipments for Bluetooth devices will reach 800 million units annually by 2004 [CIS00a].

In the WLAN category, several technologies are competing for dominance; however, based on current market momentum, it appears that Wi-Fi™ (IEEE 802.11b) will prevail. Wi-Fi offers throughput up to 11 Mbps and covers a range of approximately 100 meters. With WLANs, applications such as shared Internet access, e-mail, and file sharing can be done in the home or office, resulting in new levels of freedom and flexibility. Cahners predicts WLAN shipments exceeding 38 million units annually in 2004, implying an installed base of nearly 95 million systems [CIS00b] by the same year.

"Coexistence," the ability for multiple protocols to operate in the same frequency band without significant degradation to either's operation, has recently become a significant topic of analysis and discussion throughout the industry. This is due to several factors. Both protocols are expecting rapid growth, and because they both operate in the 2.4 GHz frequency band, the potential for interference between them is high. Also, WPAN and WLAN are complementary rather than competing technologies. Consequently, more and more usage models are being discovered in which it is desirable and necessary for both Bluetooth and Wi-Fi to operate simultaneously and in close proximity.

2.1 Technical Background

This section provides some high-level background on several key characteristics of the Bluetooth and Wi-Fi protocols. A deep understanding of these characteristics is necessary to fully investigate the merits of various approaches, but this high-level overview will provide a basic understanding. Further explanation of the two protocols' technical characteristics is provided in Mobilian's first white paper, *Wi-Fi (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem* www.mobilian.com/whitepaper_frame.htm [MBLN01].

2.1.1 Bluetooth™ Wireless Personal Area Networking (WPAN)

Bluetooth is a WPAN protocol designed as a cable-replacement technology - low cost, modest speed, and short range (<10 meters). Bluetooth can support piconets of up to eight active devices, with a maximum of three synchronous-connection-oriented (SCO) links. SCO links are voice-oriented and designed to support real-time, isochronous applications such as cordless telephony or headsets. Bluetooth also supports asynchronous connection links (ACLs) used to exchange data in non-time-critical applications. The majority of Bluetooth devices transmit at a power level of 1 mW (0 dBm). The Bluetooth physical (or PHY) layer uses the frequency-hopping spread spectrum (FHSS) technique. Bluetooth hops at a rate of 1600 hops/sec and uses Gaussian frequency shift keying (GFSK) modulation.

When the Bluetooth technology establishes communication, it forms small networks, or piconets, of Bluetooth-enabled devices. Piconet topology consists of a single master and up to seven active slaves. In a single piconet environment, there can be only one Bluetooth device transmitting in any single time slot at any one time. Therefore, the master Bluetooth node of the piconet controls the piconet through a series of transmissions. When the master has information to transmit to the slaves, it does so. Otherwise, the master is constantly polling the slaves and listening for their responses[1]. In short, for a slave to transmit data, it first must be "asked" to do so. The slave's

[1] The Bluetooth specification does not dictate how often a master should poll a slave, nor does it provide for any preemptive transmission from the slave to inform the master that it has data to transmit; therefore, to maximize Bluetooth throughput, many typical current design practices call for the master to poll the slaves during every available transmit time slot (800 polls / second) while in an active piconet.

© 2001 Mobilian Corporation. All rights reserved.

responses can be either NULL for no information to transmit, or they can begin transmitting if they have information to transmit. This piconet management scheme avoids interference within the piconet and is standard for any device carrying the Bluetooth certification (i.e., complying with the Bluetooth specification).

Understanding some aspects of the different approaches to interference mitigation, requires further investigation of the master/slave polling mentioned above. Due to the extremely rapid nature of the polling activity (hundreds of microseconds), the Bluetooth media access controller (MAC) controls the function at the MAC-level and thus, the data transferred in the process is not made available at the driver or host level. This will prove to be very significant, as is explained in later sections.

2.1.2 802.11b Wireless Local Area Networking (Wi-Fi™)

Like wired Ethernet, Wi-Fi supports true multipoint networking with such data types as broadcast, multicast, and unicast packets. Although standard practice is approximately one access point (AP) to every 10-20 stations (STA), the MAC address built into every device allows for a virtually unlimited number of devices to be active in a given network. These devices contend for access to the airwaves using a scheme called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). The Wi-Fi physical layer uses direct-sequence spread spectrum (DSSS) at four different data rates using various modulation techniques to communicate. The transmit power level can vary, but is typically between 30 and 100 mW (+15 to 20 dBm).

2.1.3 Wi-Fi™ / Bluetooth™ Interaction and Interference

Bluetooth and Wi-Fi share the same unlicensed 2.4 GHz ISM band that extends from 2.4 to 2.4835 GHz under US FCC regulations. This frequency band is free of tariffs under the ISM band rules defined in FCC Part 15.247 [FCC15.247]. However, systems in this band must operate under certain constraints that are supposed to enable multiple systems to coexist in time and place. FCC Part 15.247 specifies that a system can use one of two methods to transmit in this band: FHSS or DHSS.

FHSS is a technique in which a device transmits an energy burst in a narrow frequency band for a limited time before it hops to another. This hopping process is repeated rapidly across the entire frequency band in a pseudo-random fashion. DSSS is a technique in which a device communicates by distributing its energy across a defined set of contiguous frequency bands without hopping.

Bluetooth is an FHSS technology with frequency channels 1 MHz in width and a hop rate of 1600 hops per second. Bluetooth dwells 625 µsec in every frequency channel. In the United States and most of the world, Bluetooth uses 79 different 1 MHz frequency channels of the available 83.5 MHz in the 2.4 GHz ISM band.

Wi-Fi uses DSSS with a 22 MHz passband, and communicates with throughput up to 11 Mbps. A Wi-Fi system can use any of eleven[2] 22-MHz wide sub-channels across the available 83.5 MHz of the 2.4 GHz frequency band. Because Bluetooth hops on 79 of the available 83.5 1-MHz channels, and Wi-Fi occupies 22 1-MHz channels within its passband, sharing between the two technologies is inevitable. Two wireless systems using the same frequency band will have a high propensity to interfere with each other.

In October of 2000, Mobilian Corporation published a white paper that explored this interference in great detail. The white paper, *Wi-Fi (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem,* received wide acceptance by the industry as the definitive treatment of this issue. This current paper, on the other hand, builds on the previous work and therefore assumes a certain level of understanding of the coexistence issues.

However, for the basis of this paper, it is important to establish that Wi-Fi performance generally suffers more from Bluetooth activity than vice versa. The reasons for this are explained in great detail in the aforementioned white paper, but in summary, there are two main reasons:

---

[2] The 11 sub-channels available under US regulation allow for multiple variations of locations for 3 simultaneously operating Wi-Fi networks and associated passbands. A Wi-Fi passband typically spans a 22-MHz channel; therefore the 83.5 MHz available within the 2.4 GHz band can support three simultaneously operating, overlapping Wi-Fi networks (83.5 MHz - (3*22 MHz) = 17.5 MHz). Geographies outside of the US may support more or fewer than 11 selectable sub-channels.

©2001 Mobilian Corporation. All rights reserved.

1) First, the Wi-Fi MAC is an adaptation of the wired Ethernet MAC, and therefore uses carrier-sense before transmission (also known as "listen before talk"). Unlike wired Ethernet, the Wi-Fi MAC cannot detect collision, so Wi-Fi dictates that every received packet is acknowledged by an "acknowledgement" (ACK). If a station or access point transmits a packet and does not receive an ACK from its target recipient, it assumes a collision with another Wi-Fi transmission has occurred. To avoid additional Wi-Fi collisions, the station uses an exponential back-off algorithm (i.e., pauses a few micro-seconds) and transmits again.

   By using this mechanism among others, wired and wireless Ethernet work very efficiently in a homogenous environment. However, in an unpredictable and highly interference prone Bluetooth/Wi-Fi environment, this mechanism, and its associated back-off algorithms, result in repeated error correction without corresponding interference improvement, ultimately resulting in reduced Wi-Fi throughput.

2) Second, the Wi-Fi protocol does not typically move from its 22 MHz passband[3]. This renders it highly susceptible to collision with Bluetooth. Roughly, the probability that a standard Wi-Fi 1500 byte transmission will collide with a simultaneous Bluetooth transmission is 55%. This results from the fact that Wi-Fi requires approximately 1 to 1.5 milli-seconds to receive a 1500 byte packet at 11 Mbps. This allows Bluetooth to hop approximately 2 times (625 µsec per hop / 1.5 milli-seconds). Each hop has a 1 in 79 chance of hitting a given channel, therefore 2 hops have a 2 in 79, or ~ 1/40, chance of hitting a given channel. With 22 channels occupied by the Wi-Fi network, this raises the probability to ~ 22/40 or ~ 55%.

This performance degradation occurs at any one of three levels in descending order of severity.

1) The most pronounced negative effect occurs when a Bluetooth device is collocated with a Wi-Fi device, as is the case in a combination card or notebook PC with both Wi-Fi and Bluetooth functionality.

2) The effects are slightly less severe when the transmitting Bluetooth device is located within the same piconet as a collocated Bluetooth and typically within 1 to 1½ meters from the collocated Bluetooth/Wi-Fi device.

3) The least severe effects occur when the interfering Bluetooth is outside the collocated Bluetooth's piconet and more than 2 meters from the collocated device.

Additional factors can either improve or worsen the negative effects outlined above. One the most important is in-band and out-of-band communication of the two protocols[4]. Table 1 below gives an overview of the different scenarios and their relative severity.

---

[3] Wi-Fi does have "channel agility" functionality; however, it is seldom used and even if it is employed, due to its relatively slow movement between channels, it is practically ineffective in avoiding the extremely rapid BT hopping pattern.

[4] In-band refers to simultaneous operation in the same frequency channel. Out-of-band refers to simultaneous operation in two separate channels. This is further explained in the first white paper and in the appendix of this white paper, "6.0 Appendix – In-band versus Out-of-band Noise". This appendix is an excerpt from Mobilian's first white paper.

©2001 Mobilian Corporation. All rights reserved.

		Bluetooth Tx		Bluetooth Rx	
		In-band	Out-of-band	In-band	Out-of-band
Wi-Fi™	Tx	No Conflict	No Conflict	Strong Interference	Moderate Interference
802.11b	Rx	Strong Interference	Moderate Interference	Strong[5] Interference	Moderate Interference

Source: Mobilian Corporation

Table 1: The Interference Cases for Bluetooth and Wi-Fi[5]

3.0 Interference Mitigation Approaches

As a result of the potentially negative impacts of collocated Wi-Fi and Bluetooth devices, many companies have begun researching and developing solutions for coexistence. Potential approaches include:

- Simple device collocation with no coexistence mechanisms;
- Restricted or adaptive band hopping for Bluetooth devices;
- Switching between the two protocols; and
- System-level approaches covering the entire wireless sub-system and many of the above techniques.

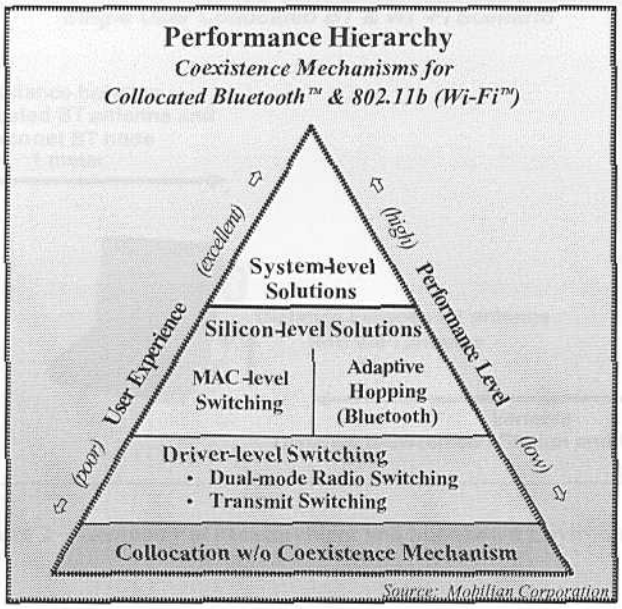


Figure 1 – Performance Hierarchy of Coexistence Approaches for Collocated Wi-Fi & Bluetooth

Each of these approaches is explored in the following pages and can be categorized into the performance and user experience hierarchy shown in Figure 1. The performance hierarchy could change dependent on the operating

[5] Collocated receivers is not an interference issue. However, simultaneous reception implies some degree of simultaneous transmission by external wireless systems. In the case of collocated 802.11b and Bluetooth systems, transmissions (which the collocated Bluetooth is trying to receive) from nearby Bluetooth nodes (located within 2 meters), can significantly affect 802.11b's ability to receive.

© 2001 Mobilian Corporation. All rights reserved.

characteristics of the particular environment. In some scenarios, MAC-level switching may manage interference more effectively than adaptive hopping, and vice versa. The same can be said of driver-level switching and its various implementations. However, system-level solutions, providing simultaneous operation through a combination of the most appropriate aspects of each technique, will most consistently appear at the pinnacle of both performance, and user experience.

3.1 Collocation without Coexistence Mechanism

3.1.1 Overview

This approach simply entails collocating the two wireless devices in a single form factor without any attempt to avoid the potential interference (e.g., PC NIC reference design).

3.1.2 Analysis

Collocating Bluetooth and Wi-Fi without using any coexistence mitigation techniques increases the likelihood of significant interference. The coexistence issues associated with it are fundamental to the interference problem, which we have explored extensively in our first white paper. Performance is likely to be significantly degraded for both protocols in this scenario. Figure 3 shows both measured and simulated effects of this approach in the single-user network configuration shown in Figure 2. The first white paper provides extensive details of both the scenario below and simulation details.

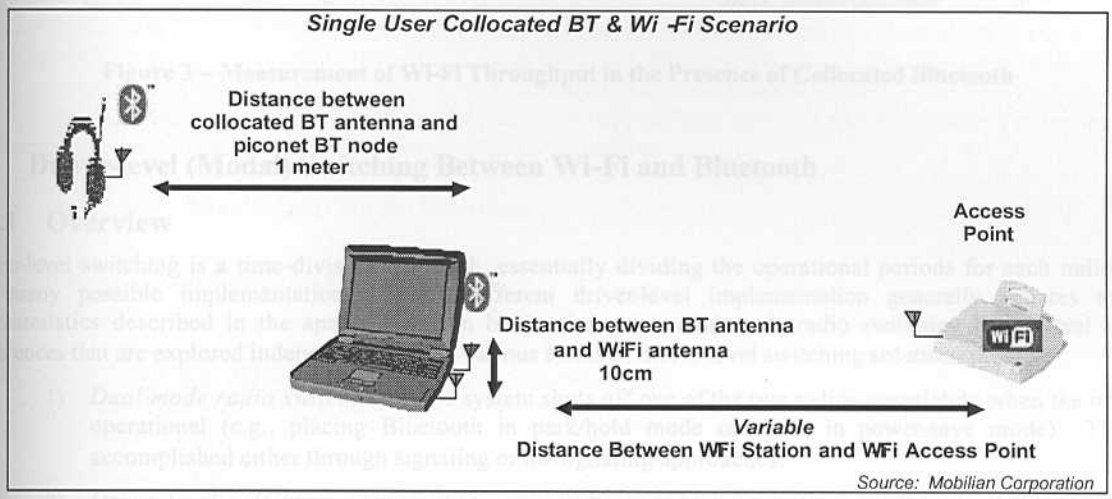


Figure 2 – Geometry of Measurement and Simulation Environment

©2001 Mobilian Corporation. All rights reserved.

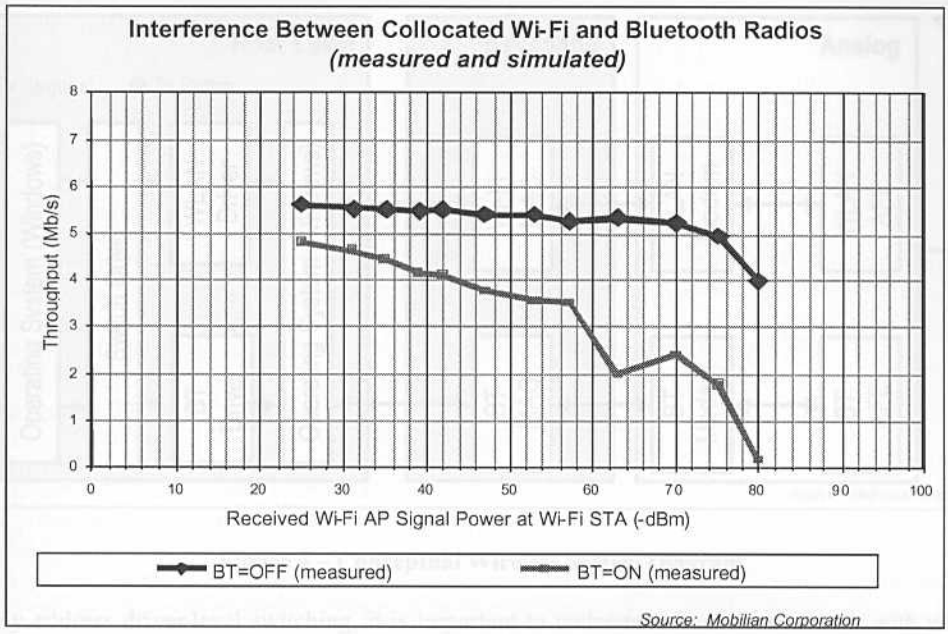


Figure 3 – Measurement of Wi-Fi Throughput in the Presence of Collocated Bluetooth

3.2 Driver-level (Modal) Switching Between Wi-Fi and Bluetooth

3.2.1 Overview

Driver-level switching is a time-division approach, essentially dividing the operational periods for each radio, and has many possible implementations. Each different driver-level implementation generally adheres to the characteristics described in the analysis section below; however, dual-mode radio switching has several slight differences that are explored independently. The various forms of driver-level switching solutions include:

1) *Dual-mode radio switching* – The system shuts off one of the two radios completely when the other is operational (e.g., placing Bluetooth in park/hold mode or Wi-Fi in power-save mode). This is accomplished either through signaling or no-signaling approaches.
2) *Driver-level switching* – This includes several types of techniques that are all controlled at the driver level: User-dependent switching, discriminatory switching, successful-transmission switching, statistical switching, and time-delay switching.

© 2001 Mobilian Corporation. All rights reserved.

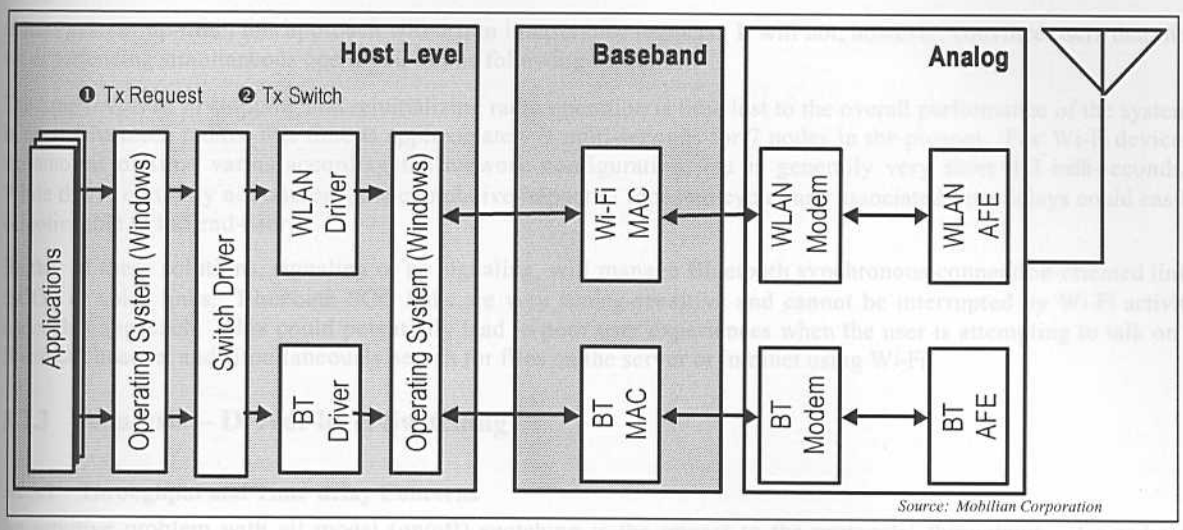


Figure 4 – Conceptual Wireless System Diagram

To effectively address driver-level switching, it is important to understand how drivers work with wireless radios. Figure 4 provides a high-level, conceptual graphic of a wireless system. Referring to the numbers in Figure 4, (❶) host applications initiate a request to transmit data. This request first travels to the operating system (e.g., Windows), then to the driver, (❷) which passes the message through the operating system again thus allowing the data to be transmitted via the wireless system. In a driver-level switching approach, the switch driver monitors these application requests to ensure no transmission collides with another.

3.2.2 Analysis – Dual-mode Radio Switching

3.2.2.1 Dual-mode Radio Switching

A dual-mode radio switching approach involves shutting one of the two radios off completely when the other is operating (e.g., placing Bluetooth in park/hold mode or Wi-Fi in power-save mode). The radios are never operating simultaneously, and therefore never attempting to simultaneously receive or transmit. This approach avoids interference from Bluetooth polling, an important technical difficulty with other driver-level switching approaches explained in section 3.2.3.2.

Dual-mode radio switching can be accomplished either by simply stopping operation of one of the radios with no indication to other devices in the network, or by first signaling that one device is about to be suspended and then stopping operations.

3.2.2.2 Leaving the Network <u>without</u> Signaling

In a normal operating scenario, radios do not go into these "sleep" modes commonly used for saving power, unless they are not actively participating in the network. When a radio is suspended without signaling to other partner devices, it cannot respond to transmissions from other network nodes. This lack of information, usually in the form of ACKs, results in reduced throughput and wasted bandwidth as the AP repeatedly sends data and executes interference mitigation techniques (discussed in section 2.1.2).

3.2.2.3 Leaving the Network <u>with</u> Signaling

By notifying other nodes in the network that a device is being suspended, problems with unacknowledged transmissions can be avoided. Thus while throughput remains a concern because modal approaches inherently

©2001 Mobilian Corporation. All rights reserved.

reduce system up-time, this approach will lessen interference impacts. It will not, however, convince users that they are experiencing simultaneous operation, for the following reasons.

The time involved in stopping and reinitializing radio operation is time lost to the overall performance of the system. In most Bluetooth radios, this time is approximately 9 milli-seconds for 7 nodes in the piconet. For Wi-Fi devices, the amount of time varies according the network configuration, but is generally very short (1-3 milli-seconds). While this is certainly not onerous, the cumulative impact of repeated cycles and associated time delays could easily be noticeable to the end-user.

Neither of these solutions, signaling or no signaling, will manage Bluetooth synchronous-connection-oriented links (SCO), or voice links. Bluetooth SCO links are very timing-sensitive and cannot be interrupted by Wi-Fi activity under this approach. This could potentially lead to poor user experiences when the user is attempting to talk on a Bluetooth headset and simultaneously search for files on the server or intranet using Wi-Fi.

3.2.3 Analysis – Driver-level Switching

3.2.3.1 Throughput and Time-delay Concerns

An intuitive problem with all modal (on/off) switching is the impact to the protocols' throughput. If a radio is suspended, it is not transmitting or receiving, and therefore the potential throughput is degraded. While this can be significant, it varies according to the differences in implementation. Therefore, we do not address the issue here. Rather, we investigate the more important aspects of the overall approach.

Because driver-level transmit switching occurs at the driver level, and because the transaction time for a driver-level switch to occur is unreliable and lengthy, avoiding collisions with incoming packets is very difficult. The resulting transmission of one protocol during reception of the other causes loss of received packets, interference, and potential user difficulties. This is caused by the driver's dependence on the host operating system, which is generally non-deterministic in its response time (i.e., non-real-time).

Reception of a standard 1500 byte Wi-Fi packet takes approximately 1 to 1.5 milli-seconds. The time required for information to transmit from the baseband to the driver – such as "there is a packet being received – do not transmit" – and for the corresponding driver activity to complete, can be anywhere from 100 micro-seconds to 2 or 3 seconds, or even longer. This is caused by the variable latency inherent in non-deterministic (non-real-time) host operating systems such as Windows, Linux, and Unix.

Host operating systems have variable latency because of the many background activities occurring during normal operation. As the interrupt from the baseband is received by the operating system, it is queued behind other interrupts and requests from other functions. This queue could range from very short to very long in terms of time required for the operating system to process the baseband interrupt. Because of this varied latency, when the operating system processes the request and passes it to the driver, the driver is not able to gauge a proper response. It doesn't "know" if the baseband request was sent 1 micro-second ago, 1 milli-second ago, or 1 second ago. This represents a huge gulf of missing information to Wi-Fi and Bluetooth, which both operate in micro-second intervals.

For this reason, basebands do not currently perform this activity and a driver-level approach will potentially transmit at the same time the wireless system is receiving. As we illustrated before in Table 1 and again in Table 2 below, this scenario, one radio transmitting while the other is receiving, causes significant interference.

© 2001 Mobilian Corporation. All rights reserved.

		Bluetooth Tx		Bluetooth Rx	
		In-band	Out-of-band	In-band	Out-of-band
Wi-Fi™	Tx	No Conflict	No Conflict	Strong Interference	Moderate Interference
802.11b	Rx	Strong Interference	Moderate Interference	Strong[6] Interference	Moderate Interference

Source: Mobilian Corporation

Table 2: The Interference Cases for Bluetooth and Wi-Fi[6]

3.2.3.2 Impacts of Bluetooth Polling Activities

As we indicated in our discussion of Bluetooth polling functionality in Section 2.1.1, in most implementations of Bluetooth, in an active piconet, the master Bluetooth node will continuously poll the slaves. "Continuously" means in every available transmit slot or 800 times per second (1 slot request for information, 1 slot opportunity to respond).

As also explained, polling activities are controlled at the Bluetooth MAC layer and don't reach the driver-level; therefore, polling activities cannot be controlled / switched by the driver. Again, this creates significant interference, because Bluetooth will be continuously transmitting while Wi-Fi is attempting to receive. The effect of Bluetooth polling activities on Wi-Fi performance generates significant interference roughly equivalent to that in collocated Wi-Fi and BT radios with no coexistence mechanism as in Figure 3.

3.3 Adaptive Hopping

3.3.1 Overview

Recently (11/13/00), a group of companies petitioned the FCC requesting the initial report and order (R&O) for Wideband Frequency Hopping (WBFH), also known as ET Docket 99-231, be amended or reconsidered to allow Bluetooth to hop across as few as 15 1-MHz channels in the 2.4 GHz ISM band. This frequency-division approach, known as adaptive hopping, would theoretically allow modified Bluetooth devices to operate simultaneously with Wi-Fi devices by dividing the frequency band: Bluetooth would operate in one section, and Wi-Fi another, non-overlapping section. This technique is currently permissible under FCC regulations for radios operating under at or below –1.3 dBm of transmit power. The regulation must be changed, however, to allow the typical class 1, 2, and 3 Bluetooth devices to operate in this mode. This represents a significant change to the ISM band rules and requires much more explanation than allowed by the scope of this paper. However, we have provided a brief overview of several important aspects of this petition and the adaptive hopping approach.

3.3.2 Analysis

Adaptive hopping will provide a viable and important solution to 802.11b and Bluetooth coexistence, provided it is quickly ratified through the appropriate regulatory processes, and its recommended implementation of its intelligent adaptive hopping algorithms is well thought out. The timeliness of the regulatory process is primarily a function of the integrity of the adaptive hopping petition. If it adequately addresses the potential issues discussed in the following sections, the process should be relatively quick. However, if the petition's implementation recommendations are ambiguous, and do not adequately address the issues below, the regulatory process will likely be protracted while these important details are resolved. Regardless of the ratification timing, when passed, Bluetooth adaptive hopping will provide an excellent coexistence solution in environments with two or fewer Bluetooth piconets and no overlapping Wi-Fi networks.

---

[6] See footnote 5.

© 2001 Mobilian Corporation. All rights reserved.

3.3.2.1 Adaptive Hopping as Optional Profile (Operational Mode)

Bluetooth specification 1.0 and 1.1 do not require adaptive hopping functionality and therefore use all 79 available 1-MHz hop channels. This, of course, creates interference for any closely located Wi-Fi network, and is the core of the issue addressed by adaptive hopping. Over the next year, Cahners In-Stat estimates approximately 30 million Bluetooth devices will come to market, all theoretically under Bluetooth specification 1.1. Given that future Bluetooth devices will need to communicate with these legacy devices, the adaptive hopping petition is likely to be passed as an optional function or profile. Therefore, Bluetooth developers will not be required to include the adaptive hopping profile and may choose to eliminate it to get to market faster or optimize their product cost.

The complication arises from the fact that, when it comes to hop pattern, Bluetooth piconets must operate at the lowest common denominator. Thus, a Bluetooth device with the optional adaptive hopping functionality will be forced to bypass the mechanism and use all 79 channels if there is even one unmodified Bluetooth device in its piconet. Furthermore, since the majority of current and foreseeable Bluetooth implementations will perform the hop selection in the hardware, it will be very difficult to retroactively modify them for adaptive hopping. Accomplishing the modification would probably require a new spin or release of the Bluetooth device hardware.

This series of timing issues represents a significant consideration for adaptive hopping's universal effectiveness as a coexistence solution. There are other, more technical considerations that must also be addressed for adaptive hopping to achieve its full potential.

3.3.2.2 Adaptive Hopper Must Accurately Sense and Respond to Interferers

It appears that adaptive hopping Bluetooth devices will move into adaptive hopping mode based on one or more of several possible interference detection mechanisms. The petition does not currently specify which approach will be recommended in the Bluetooth profile, but four of the many possible technical approaches are:

1) The Bluetooth device gradually adapts its normal operation hop pattern based on observed packet loss;
2) The Bluetooth device detects and assesses received signal strength across its wireless environment before commencing operation;
3) The Bluetooth device transmits a "test" pattern of packets across the entire spectrum, observes the ratio of lost packets across available channels and locates its adapted piconet in the least active or interference-prone channel; and
4) The Bluetooth device is collocated with a Wi-Fi device, and can receive the Wi-Fi passband location from the Wi-Fi device, so it simply avoids operating within the Wi-Fi passband.

Given that under the current petition the adaptive hopping Bluetooth device must reassess its restricted mode every 30 seconds, all of these approaches will eventually result in low interference operating scenarios. However, with the exception of the last, they all have the potential to exacerbate interference problems under certain conditions.

3.3.2.2.1 Bluetooth™ Difficulty in Detecting Wi-Fi™ Signal

If the Bluetooth device is attempting to modify its normal 79 MHz hop pattern based on observed packet failure rates, it could create significant interference for a closely located Wi-Fi device, but have difficulty detecting interference to its own signal, and therefore not move into adaptive mode. This is caused by a combination of factors, including Wi-Fi transmit power, the distance between the Bluetooth and Wi-Fi devices, and the Bluetooth receive filter.

Consider the following scenario using the path loss model from A. Kamerman's 1999 work[7]. A Wi-Fi AP and station are transmitting at +15 dBm and are separated by approximately 15 meters, resulting in received signal strength of – 52.5 dBm at either device. If a 0 dBm Bluetooth piconet is within 5 meters of either Wi-Fi device, it will create debilitating interference for the Wi-Fi network but will not sense interference to its own signal until it is within approximately 1.3 meters of the Wi-Fi transmitter (AP or station).

[7] Please see Appendix 2 for explanation of the path loss models employed.

© 2001 Mobilian Corporation. All rights reserved.

This occurs because, with 5 meters separation between the Bluetooth and Wi-Fi device, the Bluetooth signal reaches the Wi-Fi device at approximately – 54 dBm, resulting in an intolerable signal-to-noise ratio. On the other hand, the Bluetooth receive filter's noise reduction effects on the Wi-Fi signal allow the Bluetooth piconet to continue operating without significant error rates, even when it is within ~ 1.3 meters of the +15 dBm Wi-Fi transmitter. The Bluetooth receive filter reduces the Wi-Fi signal by 13 dB; therefore, at 1 meter from the Wi-Fi transmitter, the +15 dBm transmission is perceived by the Bluetooth as – 38 dBm[8]. At ~ 1.3 meters, the perceived Wi-Fi signal (noise) reaches approximately – 40 dBm, and the Bluetooth device suffers increased packet error rates and can modify its hop pattern. This creates significant opportunities for continued interference, particularly in wireless corporate scenarios with multiple networks, as depicted in Figure 5.

While multiple network environments are not commonplace in today's market, Figure 5 shows a very likely corporate environment in which multiple Wi-Fi networks and Bluetooth piconets will likely arise[9]. In this scenario, enterprise cubicles are configured back-to-back with Wi-Fi/Bluetooth-enabled PCs in each corner, and with each user having an active or potentially active Bluetooth piconet with their PDA/cell phone or Bluetooth enabled peripherals.

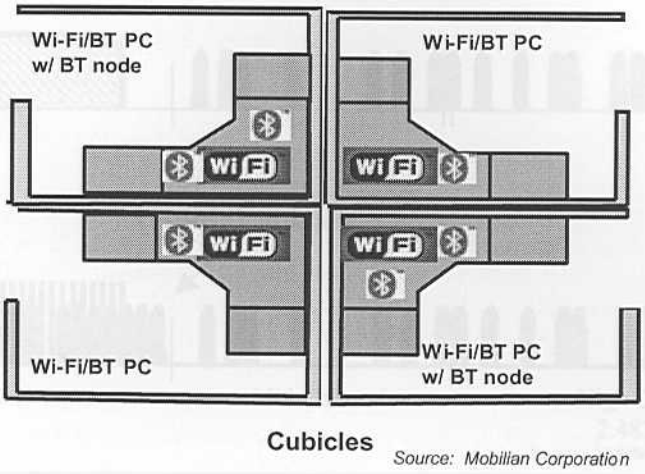


Figure 5 – Basic Geometry of Bluetooth and Wi-Fi Penetrated Corporation

3.3.2.2.2 *Congested Wireless Environments are Particularly Troublesome*

In a congested wireless environment, a newly introduced adaptive hopping Bluetooth device could have difficulty identifying the optimal location for its piconet. This is particularly relevant in situations where an existing adapted Bluetooth piconet already exists.

As mentioned earlier, interference to Bluetooth is greatest when the collocated Bluetooth radio is receiving while the Wi-Fi is transmitting, although this is not usually the case. In a typical wireless network usage scenario, a Wi-Fi station, such as a desktop or laptop PC, receives far more information from the access point (AP) than it transmits. This is known as an asymmetric usage model and is widely accepted as the dominant usage scenario for many networks.

---

[8] + 15 dBm – 40 dB – 13 dB = – 38 dBm

[9] Figure 5 shows a potential corporate deployment/configuration of Wi-Fi and Bluetooth, developed in collaboration with a leading PC OEM. The Wi-Fi stations communicate with an Access Point (AP). The Wi-Fi stations are also equipped with Bluetooth radios communicating with another Bluetooth node (potentially a headset, PDA, etc.) Additional Bluetooth piconets can be active in adjacent cubicles.

© 2001 Mobilian Corporation. All rights reserved.

Network asymmetry lessens the likelihood of interference from Wi-Fi to the Bluetooth because it is more likely that the Bluetooth is being subjected to a non-interfering, attenuated signal from the Wi-Fi AP rather than a relatively strong signal from the closely located Wi-Fi station. The Wi-Fi station transmits infrequently, and generally in the form of relatively short ACKs (less than 0.2 milli-seconds). This generates an interesting dichotomy wherein the adaptive hopper is likely to "choose" to operate directly in a Wi-Fi passband if there is already a BT adaptive hopping network in the environment. We explore this complication using the corporate environment in Figure 5, and considering the Bluetooth adaptive hopping mechanisms of detecting received signal strength and the transmission of test packets.

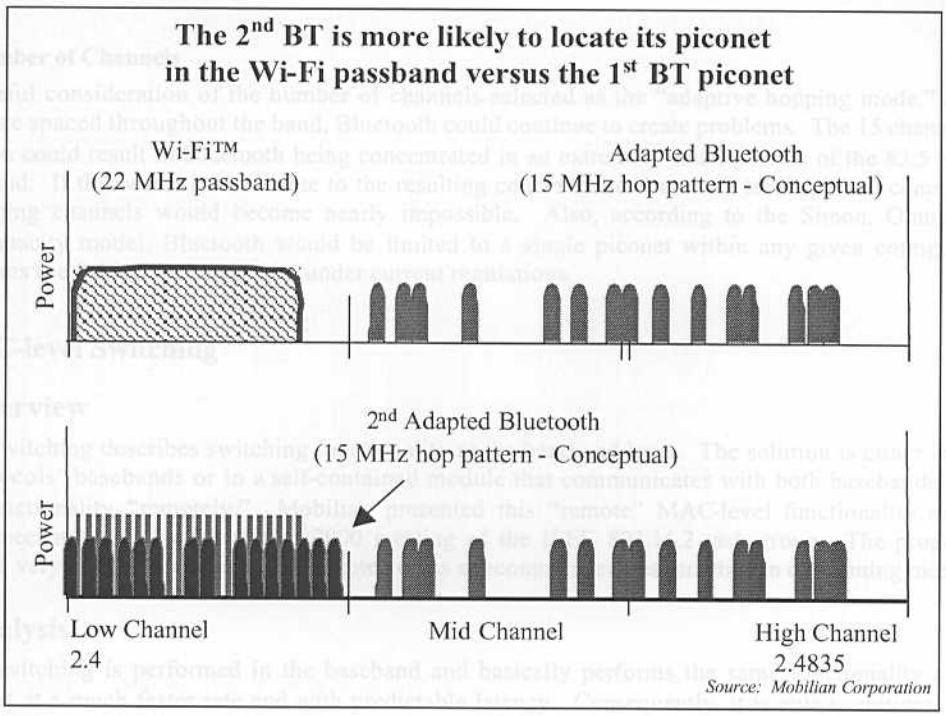


Figure 6 – Likely Location of Two Adaptive Hoppers

If the Bluetooth uses a test packet mechanism, the Bluetooth radio transmits any number of packets across the entire spectrum and gauges the most attractive channel based on the number of lost packets in each. According to testing of actual Wi-Fi networks and statistical calculation of Bluetooth hopping patterns, 0.06% of Bluetooth test packets would be lost in the Wi-Fi passband versus 1.27% in the occupied Bluetooth piconet band, thus leading the Bluetooth to locate its adapted piconet within the Wi-Fi passband, creating catastrophic interference. This has to do with common network operational characteristics such as percentage of time each network is in operating, length of transmissions, and interferer signal strength. Calculations yield similar results if the Bluetooth uses received signal strength indicators. Further details regarding these calculations are available from Mobilian Corporation.

While this example illustrates an environment with a single Wi-Fi network and two Bluetooth piconets, in future corporate environments, this could easily grow to multiple Bluetooth piconets and Wi-Fi networks, making the problem worse.

© 2001 Mobilian Corporation. All rights reserved.

3.3.2.3 Adjacent-Channel Noise[10]

Adaptive hopping does not adequately address adjacent channel, or out-of-band, interference. Adjacent channel noise is primarily related to the degree of isolation achieved between the two radios' signals. Once again, a Bluetooth device in transmit mode significantly degrades the reception of a collocated Wi-Fi receiver. This is the case whether the Bluetooth is transmitting in the same channel the Wi-Fi is receiving in or in an adjacent one. The overall effects of adjacent channel interference become more severe as the Wi-Fi station is moved further from the transmitting Wi-Fi AP, and the subsequent signal-to-noise ratio becomes smaller, rendering the attenuated AP signal more susceptible to interference.

3.3.2.4 Number of Channels

Without careful consideration of the number of channels selected as the "adaptive hopping mode," and how and where they are spaced throughout the band, Bluetooth could continue to create problems. The 15 channels requested in the petition could result in Bluetooth being concentrated in an extremely small portion of the 83.5 MHz-wide 2.4 GHz ISM band. If this were the case, due to the resulting concentrated Bluetooth traffic, Wi-Fi communications in any overlapping channels would become nearly impossible. Also, according to the Simon, Omura [MSJO85] frequency capacity model, Bluetooth would be limited to a single piconet within any given contiguous 15-MHz channel, versus the 8-10 piconet capacity under current regulations.

3.4 MAC-level Switching

3.4.1 Overview

MAC-level switching describes switching functionality at the baseband level. The solution is either integrated into the two protocols' basebands or in a self-contained module that communicates with both basebands and provides switching functionality "remotely." Mobilian presented this "remote" MAC-level functionality as a proposed coexistence mechanism at the November 2000 meeting of the IEEE 802.15.2 task group. The proposal, dubbed MEHTA, was very well received and will be voted on as a recommended best practice in the coming months.

3.4.2 Analysis

MAC-level switching is performed in the baseband and basically performs the same functionality as driver-level switching, but at a much faster rate and with predictable latency. Consequently, it is able to mitigate many of the interference factors that driver-level switching cannot. MAC-level switching does not suffer from transmitting signals into incoming receptions, Bluetooth polling, or operating system latency. However, like many of the previous approaches, it is susceptible to adjacent-channel interference and therefore does suffer some degradation. Also, a MAC-level approach will have a long development cycle time relative to a driver-level switching approach, and is pertinent only in systems employing both technologies in a very small, if not integrated, area. Such systems also typically have long development cycles.

3.5 Simultaneous Operation

3.5.1 Overview

Simultaneous operation is the ability for different, fully standards-compliant wireless systems to operate simultaneously in a collocated scenario while experiencing minimal or no performance degradation. Simultaneous operation also refers to devices able to offer the user outstanding performance without a list of operational caveats. The device should "just work," regardless of other devices within its operating environment.

Simultaneous operation of Wi-Fi and Bluetooth will occur more and more frequently as users begin completing everyday tasks such as copying or printing a file from their Wi-Fi PC while using a Bluetooth-enabled mouse and

[10] For further explanation of adjacent-channel noise, and in-band and out-of-band noise, please see the appendix.

© 2001 Mobilian Corporation. All rights reserved.

keyboard. Its frequency will continue to grow as personal communication devices and synchronization activities with PCs and networks grow, and it will gain even more importance as distributed applications take off – "the next big thing in software" – and Bluetooth devices must coexist with massive amounts of Wi-Fi network activity.

In all these scenarios, users will appreciate being able to use whatever wireless devices surround them, when they want to and how they want to. Users will demand "Coexistence without Compromise"™, and will resist adopting wireless devices as long as there are operational difficulties or perceived concerns.

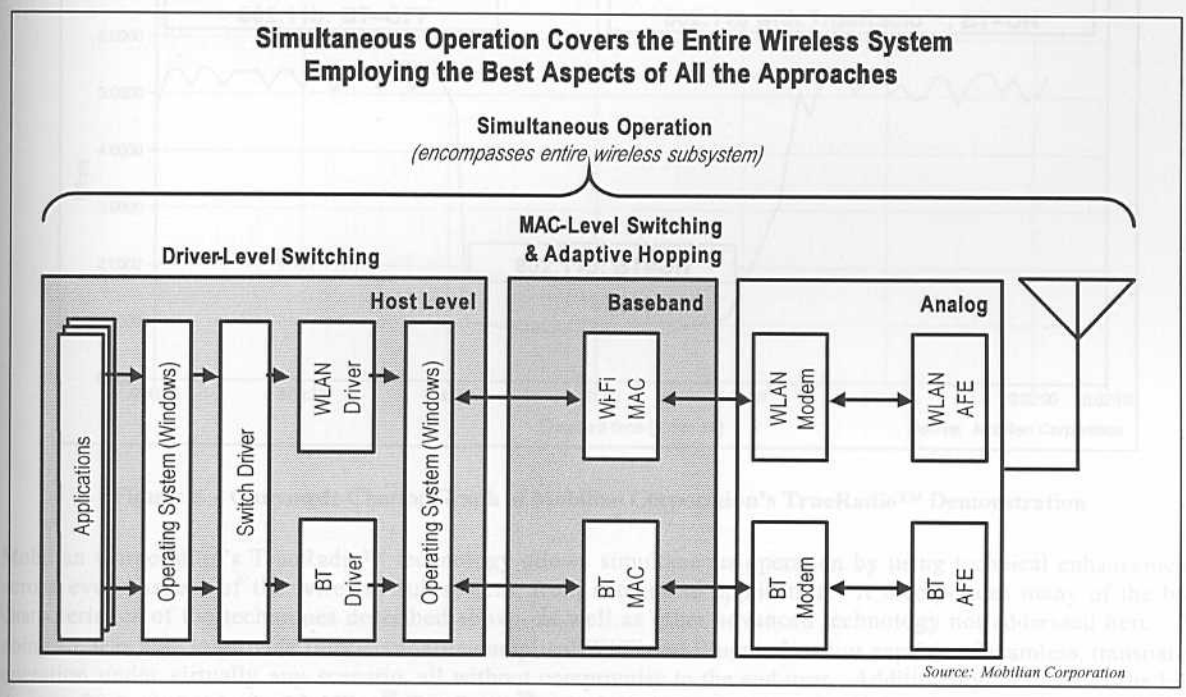


Figure 7 – Simultaneous Operation Covers Entire Conceptual Wireless System Diagram

We believe that true, sustainable simultaneous operation can only be achieved by taking a system-level approach encompassing the entire wireless sub-system. This design methodology allows the solution to selectively use the best aspects of each technique or techniques, depending on its environment and the required usage models.

For example, a driver-level switching technique may generate the best user experience in a low bandwidth synchronization scenario, while MAC-level switching will manage interference much more effectively for SCO traffic, or when a user has wireless peripherals such as speakers or a keyboard. Further, in future environments of distributed computing / applications, a system-level approach may be required to effectively allow SCO traffic while manipulating server-side office productivity applications.

Mobilian Corporation developed its first product, TrueRadio™, using a system-level methodology, and will continue development under this methodology with subsequent, multi-standard radio products.

©2001 Mobilian Corporation. All rights reserved.

3.5.2 Analysis

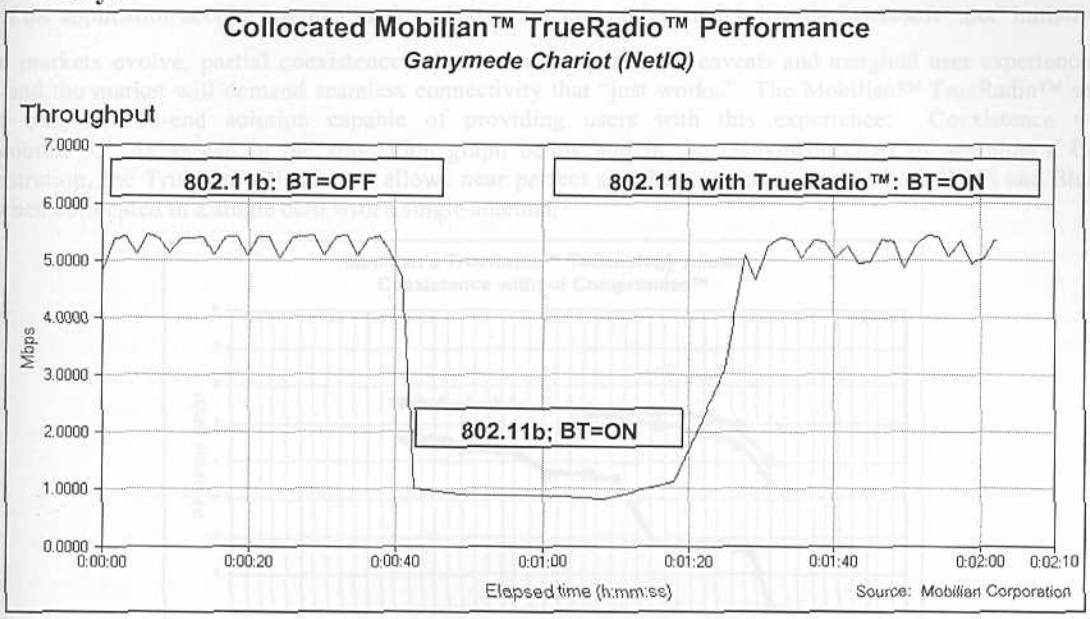


Figure 8 – Ganymede Chariot Graph of Mobilian Corporation's TrueRadio™ Demonstration

Mobilian Corporation's TrueRadio™ technology allows simultaneous operation by using technical enhancements across every aspect of the wireless sub-system, from antenna to application. It incorporates many of the best characteristics of the techniques described above, as well as other advanced technology not addressed here. By doing so, it is able to provide fully-standards-compliant Wi-Fi and Bluetooth radios capable of seamless, transparent operation under virtually any scenario, all without compromise to the end-user. Additionally, because of the high degree of integration in the Mobilian™ TrueRadio™ solution, the expected cost of the solution is substantially less than simple collocation of two chipsets or independent cards.

Mobilian demonstrated[11] its TrueRadio™ technology under NDA at Comdex 2000 with very successful results and excellent market response. The TrueRadio™ technology eliminated virtually all interference as shown by the Ganymede[12] chart in Figure 8.

4.0 Summary

The market is rapidly moving toward resolving the coexistence concerns surrounding Wi-Fi and Bluetooth. The variety of approaches discussed in this paper will likely address the issue prior to it ever affecting the end-user. Consequently, market forecasts for Bluetooth and Wi-Fi will remain strong, and a new market for combination 802.11b and Bluetooth solutions will arise.

However, the need for effective, multi-standard, coexistence solutions will only increase as wireless devices proliferate and simultaneous operation usage models become pervasive. This will occur with proven, perpetual

---

[11] The technology demonstration used a notebook computer with collocated Bluetooth and Wi-Fi radios. The Wi-Fi AP antenna was covered in attenuating material simulating an office environment with forty-five feet between the STA and AP with 8 cubicle walls. The partner Bluetooth node was located 1 meter away.

[12] Ganymede Chariot software is used by WECA in the Wi-Fi certification process. It measures the throughput for wireless LAN systems by monitoring and calculating the time required to transmit a 1MB file from the AP to the STA. Ganymede was recently acquired by NetIQ.

© 2001 Mobilian Corporation. All rights reserved.

market innovation such as new power saving techniques allowing Wi-Fi to penetrate the hand-held market, and ramp of the application service provider market (distributing computing models like the Microsoft ".net" initiative).

As the markets evolve, partial coexistence solutions with operational caveats and marginal user experiences will falter, and the market will demand seamless connectivity that "just works." The Mobilian™ TrueRadio™ solution is the only end-to-end solution capable of providing users with this experience: Coexistence without Compromise™. As shown in the simulation graph below and in the Ganymede chart of Mobilian's Comdex demonstration, the TrueRadio™ solution allows near perfect simultaneous operation of both Wi-Fi and Bluetooth even when collocated in a single card with a single antenna.

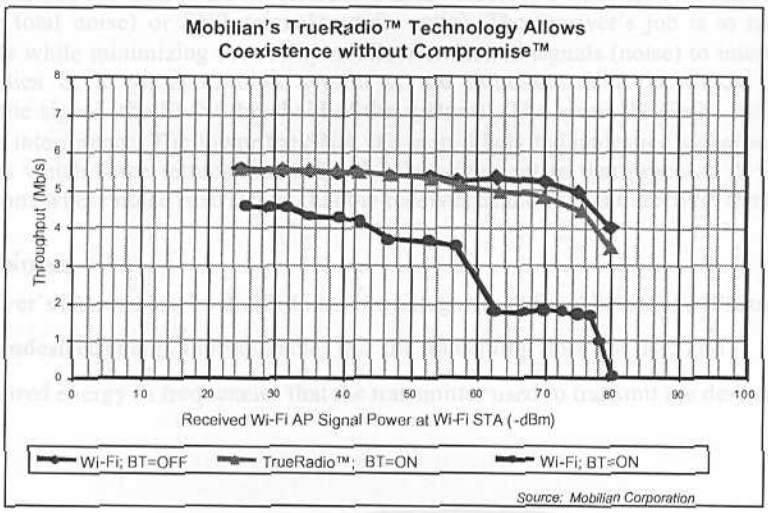


Figure 9 – Mobilian's TrueRadio™ Performance in Collocated Scenario

© 2001 Mobilian Corporation. All rights reserved.

5.0 Appendix 1 – In-band versus Out-of-band Noise

5.1 Signals and Noise

Every wireless communication system, by definition, consists of at least two nodes. At any given time, one node transmits (a transmitter) and the other receives (a receiver)[13]. Successful system operation depends on the receiver's ability to separate a desired signal from an undesired signal. This depends on the ratio between the energy of desired signal and the total noise (interference) at the receiver's antenna. This ratio is referred to as Eb/Nt (energy per bit over total noise) or SNR (signal-to-noise ratio). The receiver's job is to maximize the ability to decode desired signals while minimizing the ability to allow undesired signals (noise) to interfere. One of the most important characteristics of a communication system is the minimum SNR at which the receiver can still successfully decode the signal (the Eb/Nt threshold of the system). The lower the Eb/Nt threshold, the greater the system's immunity to interference. The lower the SNR, the more likely the undesired signal will cause unacceptable errors in data packets which force retransmission (and delays inherent in that process), or impact voice quality. There are also situations where noise is so strong that the receiver cannot begin to recover the desired signal.

5.1.1 Types of Noise

The noise at the receiver's antenna can be divided into two categories defined below and illustrated in Figure 10.

Out-of-band noise – undesired energy in frequencies that the transmitter does not use; and

In-band noise – undesired energy in frequencies that the transmitter used to transmit the desired signal

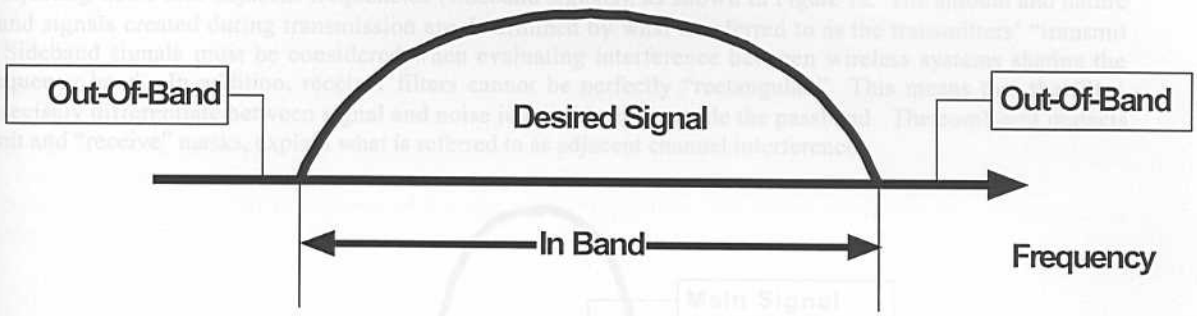


Figure 10 – In-Band versus Out-Of-Band Noise

Both in-band and out-of-band noise can degrade a wireless communications system's performance. Out-of-band noise can usually be filtered out because the energy in the system's frequency band does not carry any useful information. In-band noise, is much more problematic.

Noise can be further categorized as either "white" or "colored." White noise is a collection of energies transmitted from many different sources without any coordination between them. This energy is typically distributed evenly across the frequency band and does not have any deterministic behavior over time or frequency. Colored noise is

[13] Both 802.11 and Bluetooth stations transmit or receive (half duplex systems); there are other systems where a station transmits and receives at the same time (full duplex systems); the discussion bellow applies to both type of systems.

© 2001 Mobilian Corporation. All rights reserved.

transmitted from intentional radiators and has a specific behavior in time and frequency. Figure 11 illustrates the difference between white and colored noise.

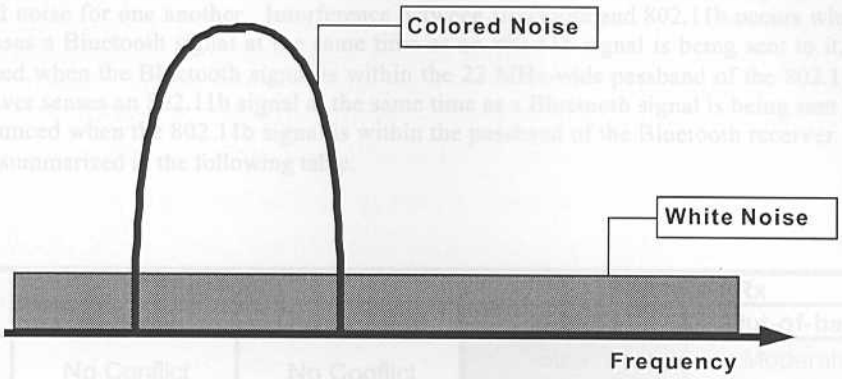


Figure 11 – White Noise and Colored Noise are Very Different

Most wireless communication systems assume that the only type of in-band noise is white noise. Other intentional radiators are assumed to transmit out-of-band. Receiver designs with their associated filtering techniques are optimized around these assumptions. Unfortunately, in a case where two intentional radiators such as Bluetooth and Wi-Fi both share the same frequency band, receivers must also address the case of in-band, colored noise.

Every transmitter is supposed to transmit only within a limited bandwidth; however, this is not physically possible without injecting noise into adjacent frequencies (sideband signals), as shown in Figure 12. The amount and nature of sideband signals created during transmission are determined by what is referred to as the transmitters' "transmit mask." Sideband signals must be considered when evaluating interference between wireless systems sharing the same frequency band. In addition, receiver filters cannot be perfectly "rectangular." This means that the filter cannot precisely differentiate between signal and noise just inside and outside the passband. The combined impacts of transmit and "receive" masks, explain what is referred to as adjacent channel interference.

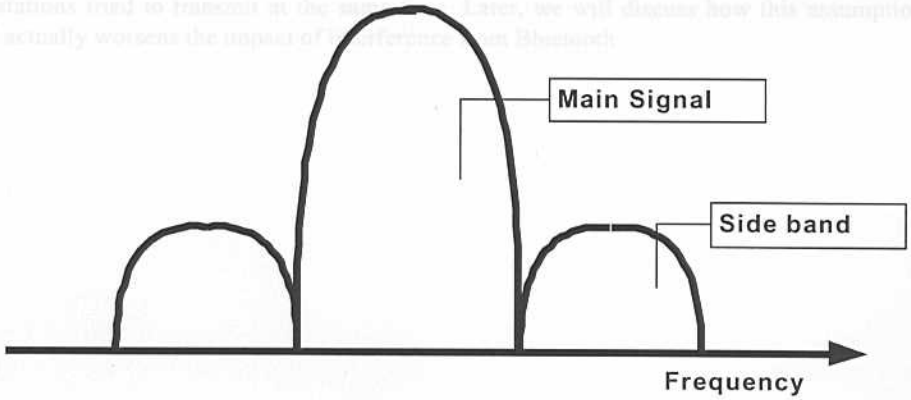


Figure 12 – Typical Transmit Mask

© 2001 Mobilian Corporation. All rights reserved.

5.2 Bluetooth and Wi-Fi Interference Cases

Bluetooth and Wi-Fi share the same band. **If Bluetooth and Wi-Fi operate at the same time in the same place, they will interfere with each other (collide).** Specifically, both systems transmit on overlapping frequencies[14], creating in-band colored noise for one another. Interference between Bluetooth and 802.11b occurs when either: a) an 802.11b receiver senses a Bluetooth signal at the same time as an 802.11b signal is being sent to it, so that the effect is most pronounced when the Bluetooth signal is within the 22 MHz-wide passband of the 802.11b receiver; and b) a Bluetooth receiver senses an 802.11b signal at the same time as a Bluetooth signal is being sent to it, so that the effect is most pronounced when the 802.11b signal is within the passband of the Bluetooth receiver. These time-frequency collisions are summarized in the following table:

		Bluetooth Tx		Bluetooth Rx	
		In-band	Out-of-band	In-band	Out-of-band
Wi-Fi™	Tx	No Conflict	No Conflict	Strong Interference	Moderate Interference
802.11b	Rx	Strong Interference	Moderate Interference	Strong[15] Interference	Moderate Interference

Source: Mobilian Corporation

Table 3: The Interference Cases for Bluetooth and Wi-Fi[15]

As we discussed earlier, the impact of interference varies as a function of energy ratios. Therefore, the "strong" verses "moderate" interference representations in Table 3 should be viewed as "relative" effects. In general, in-band interference impacts are more deleterious than those of out-of-band. However, the impact of both classes of interference depends upon SNRs, which vary according to a number of parameters discussed in more detail later.

It is worthwhile to note that neither Bluetooth, nor Wi-Fi was designed with specific mechanisms to combat the interference they create for each other. As a fast, frequency-hopping system, Bluetooth assumes that it will hop away from bad channels, minimizing its exposure to interference. The 802.11b Media Access Control (MAC) layer, based on the Ethernet protocol, assumes that many stations share the same medium, and if a transmission fails it is because two Wi-Fi stations tried to transmit at the same time. Later, we will discuss how this assumption drives system behavior that actually worsens the impact of interference from Bluetooth.

[14] We also need to take into account the sidebands of each transmission.

[15] See Footnote 5.

© 2001 Mobilian Corporation. All rights reserved.

6.0 Appendix 2 – Path Loss Models Employed

The idea of proximity is critical for this analysis. Since radio-frequency signals expand outward from the antenna in roughly spherical waves, the signal strength decreases rapidly with the distance from the transmitting antenna. This path-loss profile is proportional to the reciprocal of the squared distance from the antenna at short ranges, and attenuates more sharply in indoor environments at a distance of a few meters from the antenna, as reflection effects become apparent. The following path-loss models (Lp in dB) will be used [Kam99]:

$$Lp = -40.0 - 20\log(d), \text{ when } d <= 8 \text{ meters}$$

$$Lp = -58.5 - 33\log(d/8), \text{ when } d > 8 \text{ meters}$$

Using these empirical models, the loss profile can be plotted vs. distance as shown in Figure 13. A communication system must overcome this path loss using a combination of transmission power and receiver sensitivity to meet a desired signal-to-noise or signal-to-interference ratio criterion, which in turn translates into a probability of error. If the received signal strength is not adequate to overcome either noise or interference, unacceptable packet errors result and system throughput and latency will deteriorate.

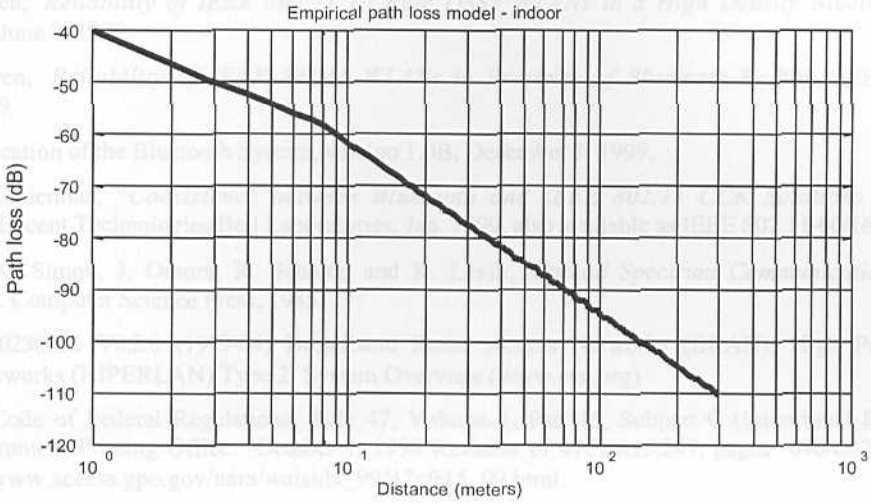


Figure 13 – Path Loss as a Function of Distance, Indoor, 2.4-GHz ISM Band

© 2001 Mobilian Corporation. All rights reserved.

References

[CIS00a] Cahners In-Stat, *Bluetooth 2000 – To Enable the Star Trek Generation*, July 2000

[CIS00b] Cahners In-Stat, based on preliminary data to be published in December 2000

[MBLN01] Mobilian Corporation, *Wi-Fi™ (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem*, November 2000

[NGFM00] Nada Golmie and F. Mouveraux, *WPAN Coexistence Performance Evaluation: MAC Simulation Environment and Preliminary Results*. IEEE 802.15-00/066r0, March 2000.

[SS00] S. Shellhammer, *Packet Error Rate of an IEEE 802.11 WLAN in the Presence of Bluetooth*. IEEE 802.15-00/133r0, May 2000.

[GE98] G. Ennis, *Impact of Bluetooth on 802.11 Direct Sequence*. IEEE 802.11-98/319, September 1998.

[JZ98] J. Zyren, *Extension of Bluetooth and 802.11 Direct Sequence Model*. IEEE 802.11-98/378, November 1998.

[JZ99a] J. Zyren, *Reliability of IEEE 802.11 Hi Rate DSSS WLANs in a High Density Bluetooth Environment*. Bluetooth '99, June 8, 1999.

[JZ99b] J. Zyren, *Reliability of IEEE 802.11 WLANs in Presence of Bluetooth Radios.* IEEE 802.15-99/073r0, September 1999.

[BT99] Specification of the Bluetooth System, version 1.0B, December 1, 1999.

[Kam99] A. Kamerman, "*Coexistence between Bluetooth and IEEE 802.11 CCK Solutions to Avoid Mutual Interferenc,e*" Lucent Technologies Bell Laboratories, Jan. 1999, also available as IEEE 802.11-00/162, July 2000.

[MSJO85] M.K. Simon, J. Omura, R. Scholtz, and K. Levitt, *Spread Spectrum Communications Vol. I, II, III*. Rockville, MD. Computer Science Press, 1985.

[ETSI99] ETR0230002 V0.2.0 (1999-04) Broadband Radio Access Networks (BRAN); High Performance Radio Local Area Networks (HIPERLAN) Type 2; System Overview (www.etsi.org)

[FCC15.247] Code of Federal Regulations, Title 47, Volume 1, Part 15, Subpart C (Intentional Radiators), Section 247. US Government Printing Office. October 1, 1998 Revision of 47CFR15.247, pages 690-692. Available on the web at: http://www.access.gpo.gov/nara/waisidx_99/47cfr15_99.html.

© 2001 Mobilian Corporation. All rights reserved.

ANEXO E

2.4 GHz and 5 GHz WLAN: Competing or Complementary?

mobilian.

2.4 GHz and 5 GHz WLAN: Competing or Complementary?

Wi-Fi™ and 802.11a are not a one-for-one trade off. They are complementary technologies and will coexist in future enterprise environments.

Mobilian Corporation

7431 NW Evergreen Parkway, Suite 220

Hillsboro, Oregon 97124

(503) 681-8600

www.mobilian.com

Abstract

With the 1999 introduction of Wi-Fi™ (IEEE-802.11b), the 2.4 GHz wireless local area network (WLAN) standard, the WLAN market finally began to experience the exciting growth levels that many have expected for so long. Now, with 802.11g speed enhancements to Wi-Fi, and 5 GHz solutions on the horizon—both promising new levels of throughput and benefits—users must be able to make an educated choice between deploying 2.4 GHz-only networks (Wi-Fi + 802.11g), 5 GHz-only networks, or a combination of both. This paper focuses on helping current and potential WLAN technology users in the enterprise segment evaluate the different technologies. In this paper, we provide an objective assessment of the different technologies according to appropriate market and business considerations, performance capabilities, deployment considerations, and technical characteristics.

Mobilian™, TrueRadio™, Sim-OP™, TrueConnectivity™, and Coexistence without Compromise™ are all trademarks of Mobilian Corporation. All other trademarks are the property of their respective owners.

Published: 5/1/2001

©2001 Mobilian Corporation. All rights reserved.

Table of Contents

Abstract		1
Table of Contents		2
Executive Summary		3
1	Wireless LAN Market – Background	4
2	Interference Concerns	5
2.1	Interference in the 2.4 GHz ISM Band	5
3	Throughput	6
3.1	Throughput – Wi-Fi	6
3.2	Throughput – 802.11gOFDM & 802.11gPBCC	7
3.3	Throughput – 802.11a	7
3.4	Throughput Conclusion	7
4	Signal Range (Decipherable)	7
5	Power Considerations, Relative to Data Rate and Signal Range	9
6	Global Spectrum Unification	9
6.1	2.4 GHz – Wi-Fi, 802.11gOFDM, & 802.11gPBCC	9
6.2	5 GHz – 802.11a	10
7	Unlicensed Available Spectrum and Spectral Efficiency	10
7.1	2.4 GHz – Wi-Fi, 802.11gOFDM, & 802.11gPBCC	10
7.2	5 GHz – 802.11a	11
7.3	Conclusion – Available Spectrum and Spectral Efficiency	12
8	Network Costs and Deployment	12
8.1	Cost of Network Interface Cards (NICs)	12
8.2	Cost and Number of Access Points	13
8.3	Cost of Support – Certified Interoperability (Wi-Fi)	13
9	Overall Conclusions	14
Appendix A—Comparison of radio wave propagation at 2.4 and 5 GHz frequencies		15
Appendix B—WLAN Throughput Calculations		16
References		17

©2001 Mobilian Corporation. All rights reserved.

Executive Summary

As the WLAN market begins to achieve momentum, several technologies are vying for market awareness and unit volume dominance: Wi-Fi and its IEEE-802.11g speed extension, and IEEE-802.11a. Although there are many more WLAN technologies and standards worldwide, this paper assesses the benefits and considerations of only these two, as we believe, based on market momentum, they will be more widely deployed than other standards.

First, allow us to establish our credibility. Mobilian Corporation is currently bringing a product to market in the 2.4 GHz space that integrates Wi-Fi and Bluetooth™ in a single chipset[1]. We are also developing a system-level 5 GHz, 802.11a-compliant product. Therefore, we consider ourselves supporters of both WLAN technologies, and believe we can provide an unbiased, comparative assessment.

Each technology has major points of differentiation, but neither is a clear "winner" based solely on operational criteria. Likewise, the two technologies are not a simple "copy / paste" for each other. Companies with existing Wi-Fi/802.11b networks cannot simply deploy a new 802.11a network on the Wi-Fi access points (APs), and expect to have similar coverage with 802.11a's 54 Megabits per second (Mbps) data rate. The physics and operational characteristics simply don't work that way.

Also, the two technologies are not mutually exclusive, and will likely never become so. In fact, given their different operating characteristics, many usage models would benefit greatly from a dual standard deployment model. Wi-Fi's range and sustainable 11 Mbps data rate could be complemented with 802.11a's space-concentrated, 54 Mbps data rate. Or, instead of a "big bang" deployment of new 802.11a infrastructure and clients, an incremental deployment could be used, saving dollars and increasing the return on investment in Wi-Fi.

The standards have very different value propositions, which touch on different end-user values by segments, usage models, applications, and existing WLAN equipment. There is no "Executive Summary" of the possible deployments for every situation. However, we believe the enterprise market will likely have deployments of both technologies for a good number of years, and the home will likely deploy Wi-Fi for internet sharing and voice, and a higher bandwidth standard for video sharing.

The remainder of this paper examines the technologies' differences. In Table 1, we provide a summary of several key differences, but we recommend reading the paper in its entirety to fully understand the key differentiators and reap the most benefit from WLAN installations.

Table 1: Key Differences Between Wi-Fi, 802.11g, and 802.11a

Standard	Modulation & Coding[2]	Spectrum Unification	Available Spectrum	Data Rate[3]	Throughput	Range[4] & Corresponding Data Rate
Wi-Fi	DSSS / CCK	Yes	83.5 MHz	11 Mbps	5-7 Mbps	100 m[4] @ 11 Mbps
$802.11g_{OFDM}$	OFDM	Yes	83.5 MHz	24 Mbps[3]	10-11 Mbps	100 m[4] @ 12 Mbps
$802.11g_{PBCC}$	DSSS / PBCC	Yes	83.5 MHz	22 Mbps	10-11 Mbps	100 m[4] @ 11 Mbps
802.11a	OFDM	No	300 MHz	54 Mbps	31 Mbps	50 m[4] @ 9 Mbps

[1] More information on Mobilian's first product, TrueRadio™, can be found on Mobilian's web site at www.mobilian.com.

[2] Modulation & Coding (acronyms)—DSSS CCK – Direct Sequence Spread Spectrum using Complementary Code Keying; DSSS PBCC – DSSS using Packet Binary Convolutional Code; OFDM – Orthogonal Frequency Division Multiplexing.

[3] Data Rate—See Appendix B—WLAN Throughput Calculations. Both 802.11a and $802.11g_{OFDM}$ are capable of 54 Mbps throughput. $802.11g_{OFDM}$ is shown at 24 Mbps to compare to 802.11_{PBCC}. $802.11g_{OFDM}$ & $802.11g_{PBCC}$ chipsets are still unapproved under FCC rule 15.247 as of publishing of this white paper.

[4] Range and Corresponding Data Rate—Assumes constant operational variables for all standards: Common receiver sensitivity, 16 dBm transmitter (40 mW), "light office" path loss model, and similar end-point data rates to Wi-Fi (11 Mbps for Wi-Fi & $802.11g_{PBCC}$; 12 Mbps for $802.11g_{OFDM}$ and 9 Mbps for 802.11a). See Appendix A—Comparison of radio wave propagation at 2.4 and 5 GHz frequencies for further discussion.

©2001 Mobilian Corporation. All rights reserved.

1 Wireless LAN Market- Background

The wireless local area network (WLAN) market is in the early stages of what appears to be mass adoption. In a recent Gartner Group survey of midsize and large businesses, 50 percent expect WLANs to be deployed at a minimum of one of their company's locations in the next two years [GG01]. This rapid adoption makes the WLAN market very attractive to many companies who have historically viewed it as too specialized and small to be meaningful. With the ratification of the 11 Mbps 802.11b standard (Wi-Fi) in the second half of 1999, guaranteed interoperability and declining cost points became a reality, and traditional tier 1 networking players such as Cisco, Lucent, 3COM, Intel, and Texas Instruments entered the WLAN market. This was in addition to existing players such as Symbol, Intermec, and Intersil (Harris Semiconductor at the time). As the market has entered this latest phase, the competitive environment has grown in intensity, driving rapid innovation and subsequent benefits in costs and performance.

The WLAN market is comprised of several competing technologies, each with different operating characteristics such as modulation type, data throughput, frequency band, and transmit power. These WLAN[5] standards include:

- HomeRF and HomeRF 2.0 (Wide-band Frequency Hopping (WBFH));
- IEEE-802.11FH/DS (1997);
- Wi-Fi (IEEE-802.11b 1999);
- IEEE-802.11gOFDM (Wi-Fi speed extension proposal);
- IEEE-802.11gPBCC (Wi-Fi speed extension proposal);
- MMAC (HiSWANa)
- HiperLAN/2; and
- IEEE-802.11a.

Two of these WLAN technologies are expected to be dominant over the next five years: Wi-Fi (and its 802.11g extension), and 802.11a. A third, whose future is still somewhat uncertain, is HiperLAN/2.

Both 802.11b and 802.11a were proposed and ratified out of the US-based Institute of Electrical and Electronic Engineers (IEEE), but use different unlicensed frequency bands. The Wi-Fi standard can achieve raw data rates of 11Mbps, has a range of about 100 meters, and uses the Industrial, Scientific, and Medical (ISM) band between 2.4000 – 2.4835 GHz.

The 802.11a standard uses the Unlicensed National Information Infrastructure (U-NII) and ISM bands in the United States, can achieve raw data rates of up to 54 Mbps for short distances, and has a range of about 50 meters at a data rate comparable to Wi-Fi (about 9-12 Mbps). The 5 GHz "band" is actually a conglomerate of several bands: 5.150 – 5.250, 5.250 – 5.350, 5.470 – 5.725, and 5.725 – 5.875.

The adoption and market ramp of these two technologies is difficult to forecast. Based on multiple analysts' market forecasts Wi-Fi's market momentum and its 802.11g speed extensions will likely carry it to unit volume dominance for the next 3-4 years. Furthermore, Wi-Fi's popularity will continue to drive down costs, and Wi-Fi certified interoperability testing will continue to be a catalyst for widespread adoption.

IEEE-802.11a will first see product samples this year (2001), but will not begin to have a meaningful ramp until late 2002 to mid-2003. This is caused by many factors, including its "cutting edge" status as a new and leading technology. (This will be attractive to a small segment of buyers, primarily home and SOHO, but will not appeal to the more risk-averse enterprise segments, or the more mainstream mass markets.) Also, with only one, or possibly two, products sampling in 2001, it is unlikely that any interoperability program will be ratified or viable.

The real question though, is how corporate IT Managers, small business owners, and home users choose between one or the other—Wi-Fi and its 802.11g speed extensions, or 5 GHz—or adopt a mixed environment. In the rest of this paper, we address the issues relevant to making this decision, and provide meaningful comparisons of the technologies' different characteristics.

[5] Many industry participants consider Bluetooth a WLAN technology. This is not consistent with the Bluetooth SIG's opinion, however, which defines it as a "cable replacement" and wireless personal area network technology. Mobilian agrees with the Bluetooth SIG for this reason, and for other technical reasons, which limit Bluetooth's ability to function effectively as a WLAN.

©2001 Mobilian Corporation. All rights reserved.

2 Interference Concerns

A common concern to all unlicensed bands is interference between the devices using the spectrum. This is absolutely a valid concern, and has historically affected all the unlicensed bands: 49 MHz, 330 MHz, 900 MHz, 2.4 GHz, etc. The life cycle of the devices using an unlicensed band generally follows a four-step process based on technical innovation, from a sparse device population to many devices sharing the spectrum:

Phase 1: The band is used primarily by scientific or military systems, not by commercial devices.

Phase 2: The first commercial devices capable of using the band enter the market and are very expensive because corresponding development costs are very high.

Phase 3: Relatively common devices begin using the spectrum because technical innovation has decreased development costs, thus lowering price points.

Phase 4: The technology that uses the band becomes available to many devices, driving prices down, device count up, and increasing the potential for interference.

Based on these historical precedents, we strongly believe that there will never be an unlicensed band that is indefinitely interference-free. Given the cost of licensed spectrum, free spectrum is, and always will be, very attractive. Therefore, the claim that a technology utilizes "un-crowded spectrum" is not a relevant buying consideration, especially when evaluating 2.4 and 5 GHz WLAN technology. This is not a decision that should be driven by moving from one band to the next with each technical innovation—that could become very expensive. Instead, it's a decision that should be driven by how suitable the solution is to the user's technical needs. Technical and market innovation will address, and in large part have already addressed, any valid interference concerns.

Furthermore, even today, both the 2.4 GHz and the 5 GHz bands are subject to overcrowding and interference, and are used by many devices outside WLAN. Table 2 below provides an overview of some of the devices and systems that use each band.

Table 2: Summary of Systems Using the 2.4 and 5 GHz Unlicensed Bands

Band	Wireless LAN Systems	Other Communication Systems	Non-Communication Systems
2.4GHz	- HomeRF	- Bluetooth	- Microwave ovens
2.400–2.4835	- HomeRF 2.0 (WBFH) - Wi-Fi (802.11b)	- Proprietary cordless phones - 802.11 FHSS (1997) - 802.11 DSSS (1997) - Proprietary vertical applications - WLL (shared internet access)	- Microwave lighting
5GHz	- 802.11a (US)	- Mobile satellite systems (MSS)	- Radar systems
5.150–5.350	- HiperLAN1 (Europe) - HiperLAN2 (Europe) - HiSWAN (Japan)	- Earth exploration satellite systems (ESSS) - Short range wireless systems - Radio Location	
5.470–5.725	- HiperLAN1 (Europe) - HiperLAN2 (Europe)	- Electronic News Gathering - Proprietary vertical applications	
5.725–5.875	- 802.11a (US)	- WLL (shared internet access)	- Microwave ovens (future – upper band)

2.1 Interference in the 2.4 GHz ISM Band

Interference in the 2.4 GHz ISM band is no longer a valid concern; however, at the beginning of the year 2000, there was good reason for concern. This was driven primarily by the potential interference created between Wi-Fi and Bluetooth. Since then, multiple companies have researched the issue and have concluded that if the two technologies are separated by 2 meters or more, there is no significant interference. They also concluded, however, that there is interference when the two are located within 2 meters, and that it can be severe when the two technologies are collocated (as in a combination

©2001 Mobilian Corporation. All rights reserved.

NIC). However, this should NOT be an issue when considering whether or not to deploy 2.4 GHz solutions. There are many solutions to the interference issue coming to market this year… long before any significant problems arise[6].

These solutions range from modifying the Bluetooth standard so its hop pattern can adapt to the presence of a Wi-Fi network, to recommended best practices and associated technologies from the IEEE and the Bluetooth SIG, to technology solutions requiring no changes to the standards, but that allow unhindered simultaneous operation of collocated Wi-Fi and Bluetooth.

Mobilian Corporation examines both the causes of interference between Wi-Fi and Bluetooth, and the various approaches to its resolution, in two white papers located on the Mobilian web site at www.mobilian.com.

3 Throughput

An important purchasing consideration for any networking technology is the amount of bandwidth, data rate, or throughput, it provides to each network user, and how well that throughput can support the applications running on the network.

For clarity purposes, data rate means the amount of data able to be sent from one node on the wireless network to another, within a given timeframe—usually seconds (11 megabits per sec = 11 Mbps). Furthermore, the difference between data rate and throughput is the amount of raw bits that travel from one node to another, in comparison to the bits representing the message content. This difference is determined by a number of factors including the latency inherent in the PHY components of the radio, the overhead and acknowledgement information that accompany every transmission, and pauses between transmissions. A comparison table of the wireless networks at hand and several wired benchmarks is shown in Table 3.

Table 3: Network Technologies Throughput Comparison

Technology	Data Rate	Actual Throughput[7]	Shared Among Users?	Estimated Time to Download 100 MB file (Actual Throughput)
56.6 Kbps Modem	56.6 Kbps	56.6 Kbps	No	4 hours
10/100 Ethernet	100 Mbps	100 Mbps	Yes	8 seconds
T1 line	1.536 Mbps	1.536 Mbps	Yes	8 minutes 41 seconds
Wi-Fi	11 Mbps	5-7 Mbps	Yes	2 minutes 8 seconds
802.11gOFDM	24 Mbps	10-11 Mbps	Yes	1 minute 13 seconds
802.11gPBCC	22 Mbps	10-11 Mbps	Yes	1 minute 14 seconds
802.11a	54 Mbps	31 Mbps	Yes	26 seconds

3.1 Throughput– Wi-Fi

Wi-Fi offers an 11 Mbps data rate, which translates into approximately 5-7 Mbps of actual message throughput. This amount is shared among all network users who are using it at *precisely* the same time, and is managed through a CSMA/CA technique modeled on its Ethernet wired equivalent. As most network traffic is bursty, and only a few users are on the network simultaneously, Wi-Fi network users generally experience very good connectivity speeds. In addition, there are several potential speed increases in store for Wi-Fi, which will come from the IEEE 802.11 Task Group g.

---

[6] In the past year, Mobilian has helped to define the market's awareness of, first, the coexistence issue, and second, the potential solutions. These topics have been covered extensively in the press, and very specifically in two Mobilian white papers. Both white papers are available on Mobilian's web site at www.mobilian.com.

1. *Wi-Fi™ (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem*—An overview of the two technologies and why there can be a problem between them.
2. *Coexistence Approaches for Wi-Fi (802.11b) and Bluetooth*—A treatment of potential techniques to resolve the issue. This white paper was recently awarded the first ever "Technical Excellence Award" at the Spring Microsoft Windows™ Hardware Engineering Conference (WinHEC) in recognition of Mobilian's "contribution to advancing the computing platform."

[7] See Appendix B—WLAN Throughput Calculations.

©2001 Mobilian Corporation. All rights reserved.

3.2 Throughput– 802.11g$_{OFDM}$ & 802.11g$_{PBCC}$

The IEEE Task Group g (802.11g) is charged to develop a new PHY extension to enhance the performance and possible applications of Wi-Fi compatible networks by increasing the achievable data rate. The IEEE is currently considering two proposals for adoption: 802.11 Packet Bnary Convolutional Code (802.11gPBCC), and 802.11 Orthogonal Frequency Division Multiplexing (802.11gOFDM).

Neither technique has been approved for use in the US under FCC Rule 15.247, but the FCC will likely modify the rule to allow whichever technique is recommended. The proposal process has been an arduous one because of the high stakes involved for all participants, but is expected to end prior to the third quarter of 2001. If the task group does not reach a recommendation by this time, the point may be moot, as emerging availability of 802.11a products and applications may erode the 802.11g value proposition.

Using OFDM and 64-Quadrature Amplitude Modulation (QAM), 802.11gOFDM will provide data rate levels equal to those provided by 802.11a OFDM technologies. However, because 802.11gOFDM is required to be backward compatible with Wi-Fi, it is burdened by bits of Wi-Fi's overhead, such as header information. For this reason, it will not likely achieve parity with the data rates possible with 802.11a. For comparison purposes in this paper, we show 802.11gOFDM's data rate at 24 Mbps, roughly equal to that of 802.11PBCC.

The 802.11PBCC technique is defined within the current 802.11b specification, but has not obtained FCC equipment authorization at the speed levels proposed by 802.11gPBCC. The 802.11gPBCC technology uses the same basic technology as Wi-Fi, but modifies the modulation scheme and the FEC slightly to achieve 22 Mbps data rate.

Both 802.11g proposals will continue to use Ethernet-like management techniques common to all 802.11 standards (including 802.11a), and will therefore efficiently share the increased throughput among all users.

3.3 Throughput– 802.11a

The IEEE-802.11a standard is based on OFDM modulation and will theoretically achieve a 54 Mbps data rate, or approximately 31 Mbps of throughput for a single network (see Appendix B—WLAN Throughput Calculations). This easily supports several simultaneous occurrences of streaming video. Additionally, 802.11a nodes share bandwidth efficiently using the same CSMA/CA techniques used in Wi-Fi systems, thus allowing a large number of users access to high wireless data rates.

3.4 Throughput Conclusion

While Wi-Fi provides plenty of throughput for the majority of common office applications in fairly dense user environments, 802.11a and Wi-Fi extensions under IEEE Task Group 802.11g will provide higher throughput, and subsequently support more bandwidth-intensive applications and larger user populations.

Quality of Service (QoS = voice) enhancements to the 802.11 MAC under development within IEEE task group e will enhance the ability of Wi-Fi, 802.11g, and 802.11a to deliver new types of time-critical data, in addition to their traditional data packets. The IEEE 802.11e Task Group recommendations will become commonly available to both the 2.4 GHz and 5 GHz solutions simultaneously, and most subsequently released 802.11 networks will then be able to support them. The higher bandwidth 802.11g and 802.11a standards will support QoS more effectively than Wi-Fi—not only because of higher bandwidth, but also because more unlicensed spectrum will be available to 5 GHz radios. This would allow 5 GHz networks to allocate a certain number of networks to voice only, and others to data. The number of potential simultaneous operating networks is covered in section 7.

4 Signal Range (Decipherable)

While the theories of electromagnetic wave propagation are outside the scope of this paper, the decipherable signal range of every wireless system is governed by the following variables:

1) RF power transmit level – power at which the signal is transmitted;

©2001 Mobilian Corporation. All rights reserved.

2) Required Es/N_0 – Signal energy required to recover the transmitted symbol[8] compared to the environmental noise (Because symbols are shorter at greater throughput levels, they require more energy in the symbol to recover it for the same error rate. This is one reason a WLAN system's throughput decreases as the distance between the AP and STA grows.);
3) Environment – The physical characteristics of the radio's environmental surroundings affect the path loss; and
4) Signal Propagation – Physics of the radio spectrum and frequency in which the radio operates.

One of the most fundamental and significant differences between communication systems operating at 2.4 and 5 GHz is the achievable communication range between the AP and the station, and the corresponding service coverage area. Assuming common environments and system operating parameters, systems operating in the 2.4 GHz frequency band offer roughly double the range of those operating in the 5 GHz band, again holding power and throughput constant. This doubled-range is explained by radio wave propagation physics, which dictate that, all other things being equal, a higher frequency signal will have a lesser range than a lower frequency signal [RAP01].

For simplicity's sake, consider one 802.11a AP compared to one Wi-Fi AP. In a typical cubicle office environment, a 15 dBm Wi-Fi AP's transmission and reception will cover a circular area with a radius of approximately 100 meters[9], with an 11 Mbps data rate. This translates into a coverage area of approximately 31,420 square meters (π*100m^2) at 11 Mbps. Assuming the RF transmit power and E_s/N_0 are held constant (i.e., same link budget), an 802.11a AP's coverage equates to a circular area with a radius of roughly 50 meters[10] for comparable data rate (9 Mbps), equaling a coverage area of approximately 7,850 square meters (see Figure 1) [RAP01, JCS01, DUR01].

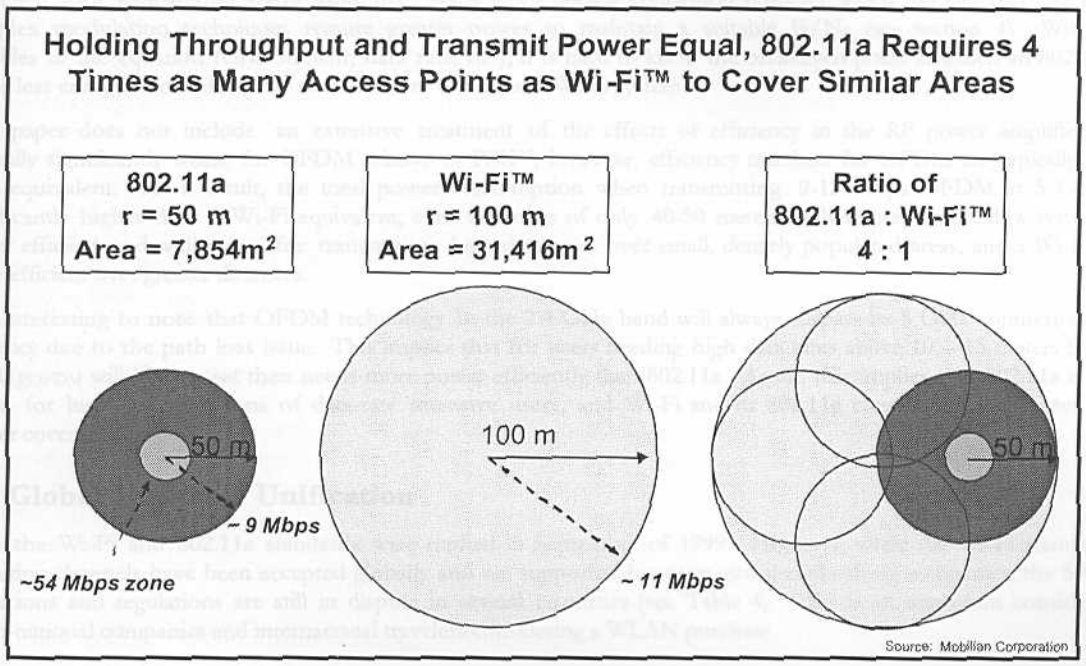


Figure 1: Coverage Comparison of Wi-Fi and 802.11a

Because of this fundamental difference in signal wave propagation, it is clear that to achieve similar coverage areas, greater numbers of 802.11a APs must be used. Consider the right-most circle in Figure 1. Four 802.11a APs are needed to cover

[8] A "symbol" is the technical wireless term for the information contained in the message. A 16 QAM symbol contains 4 bits; a 64 QAM symbol contains 6 bits.

[9] This assumes an open office environment and uses the A. Kamerman path loss model [Kam99].

[10] [RAP01, JCS01, DUR01] This assumes a conservative 5 GHz path loss. Mobilian research identified various potential 5 GHz path loss models showing decreased range compared to 2.4 GHz solutions of 45%, 50% and 75%. See Appendix A—Comparison of radio wave propagation at 2.4 and 5 GHz frequencies, for further explanation.

©2001 Mobilian Corporation. All rights reserved.

the same 30,400 meters squared that one Wi-Fi AP can cover. To reiterate, this increased number of 802.11a APs provides a comparable data rate to Wi-Fi (~9 Mbps) across the entire area, not 802.11a's highest data rate, 54 Mbps.

This is the result of a combined effect. Because the E_S/N_0 threshold and corresponding BER are more stringent for higher data rate transmit schemes, and because energy dissipates as a signal moves away from the transmitter, the further the receiver is from the transmitter, the more difficult it becomes to decipher a message. IEEE-802.11a provides high data rate (36-54 Mbps) levels close to the AP—within about 10-15 meters—making it attractive for dense user environments that also require high throughput, but its data rates are closer to 9-12 Mbps at ranges over 30-40 meters.

5 Power Considerations, Relative Data Rate and Signal Range

The previous sections discussed the fact that 802.11a systems are able to achieve about 50% of the range of 2.4 GHz systems, holding operational variables constant (RF transmit power, receiver sensitivity, etc.), and requiring a data rate approximately equal to Wi-Fi's 11 Mbps (9-12 Mbps). This limitation in range is caused by the more severe path loss of the 5 GHz spectrum, and the stringent E_S/N_0 requirements of 802.11a's higher data rate modulation techniques. However, by increasing power, 802.11a systems can achieve data rates similar to Wi-Fi (9-12 Mbps) at ranges approaching those of 2.4 GHz systems. This requires an increase of approximately 4 times the RF transmit power of an equivalent 2.4 GHz system, or from 40mW to approximately 200 mW[11], and will likely have a negative impact on battery life.

It is a common conclusion that at very close ranges (less than 30-45 feet in a light office environment), an 802.11a station will spend less time in transmit mode due to its high data rates, and therefore expend less energy than a Wi-Fi station burdened with similar data traffic amounts. This is an unclear conclusion however, given the fact that 802.11a's more complex modulation techniques require greater power to maintain a suitable E_S/N_0 (see section 4). With multiple variables in the equation (environment, data rate, etc.), it is hard to know the breakeven point at which an 802.11a system burns less energy transmitting the same amount of data as a Wi-Fi system.

This paper does not include an extensive treatment of the effects of efficiency in the RF power amplifier, which is generally significantly worse for OFDM relative to PSK[12]; however, efficiency numbers for OFDM are typically 1/3 of the PSK equivalent. As a result, the total power consumption when transmitting 9-12 Mbps OFDM at 5 GHz can be significantly higher than a Wi-Fi equivalent, even at ranges of only 40-50 meters. Therefore, an 802.11a system is more power efficient and well suited for transmitting high data rates over small, densely populated areas, and a Wi-Fi system is more efficient over greater distances.

It is interesting to note that OFDM technology in the 2.4 GHz band will always surpass its 5 GHz counterpart in power efficiency due to the path loss issue. This implies that for users needing high data rates above 10 – 15 meters from an AP, $802.11g_{OFDM}$ will likely meet their needs more power efficiently than 802.11a. Again, this implies that 802.11a is most well suited for high concentrations of data-rate intensive users, and Wi-Fi and its 802.11g counterparts are better suited for greater coverage areas.

6 Global Spectrum Unification

Both the Wi-Fi and 802.11a standards were ratified in September of 1999. However, while the Wi-Fi standard and its operating channels have been accepted globally and are supported by many global networking companies, the 5 GHz band allocations and regulations are still in dispute in several countries (see Table 4). This is an important consideration for multi-national companies and international travelers considering a WLAN purchase.

6.1 2.4 GHz – Wi-Fi, $802.11g_{OFDM}$, & $802.11g_{PBCC}$

Wi-Fi and its 802.11g speed enhancements operate in the 2.4 GHz ISM band located from 2.400 – 2.4835 GHz. Largely due to the powerful global efforts of the Bluetooth SIG and the IEEE, this unlicensed band is unified in most of the

[11] 5 GHz U-NII spectrum regulations limit transmit power in each band (see Table 4). The lower bands, in which WLANs operate, are authorized to 200mW between 5.25 and 5.35 GHz, and 40mW between 5.15 and 5.25 GHz.

[12] The peak power for OFDM systems can be much higher than the average power because many independent carriers are summed together in an OFDM system. This forces the RF power amplifier to run at a much less efficient operating point than for PSK systems such as Wi-Fi and $802.11g_{PBCC}$.

©2001 Mobilian Corporation. All rights reserved.

world. This means that devices using the 2.4 GHz spectrum, and complying with regulatory standards[13] will be legal to operate throughout the most of the world.

6.2 5 GHz – 802.11a

In the US, the IEEE-802.11a standard can legally operate in the 5.150–5.350 GHz band, and the 5.725–5.825 GHz band. Outside the US, these bands are allocated to primary users and technologies other than WLAN. Additionally, the bands are not unlicensed worldwide, and have different operational requirements. For example, the 5.470–5.725 band is not allowed for unlicensed use in the US, but is available in Europe, and conversely, the 5.725–5.825 band is available in the US but not in Europe or Japan (see Table 4). While this is not a problem for solutions contained within a single country, multi-national companies and individuals who travel internationally would be required to maintain different networks in different countries.

Table 4: 5 GHz Worldwide Spectrum Allocation and Authorized Transmit Power

5 GHz Frequency Band (GHz)	USA & Canada	Europe	France	Spain	Japan
5.150 - 5.250	40 mW	200 mW	200 mW	200 mW	200 mW
5.250 - 5.350	200 mW	200 mW	200 mW	200 mW	
5.470 - 5.725		1 W			
5.725 - 5.875	1 W				

Source: Mobilian Corporation

There are several efforts underway to unify the 5 GHz bands globally, but due to the various agencies and groups with technologies operating in the band already, it is unlikely that the band, and consequently technologies using the band, will be unified until the World Radio Conference (WRC) in 2003. Even then this harmonization is not assured, as other users of the bands will lobby for allocations to their own technologies.

The WRC will evaluate the different primary and secondary users and their proposals for common usage, and will issue a recommendation on the final worldwide band allocations and usage models. This recommendation specifies rules by international treaty and includes legal power levels, modulation techniques, and technology. In rare cases, countries have been known to deviate from the WRC guidelines, but this is not expected in these bands.

7 Unlicensed Available Spectrum and Spectral Efficiency

Wi-Fi, 802.11g, and 802.11a networks all use network passbands that cannot overlap, thus limiting the number of simultaneously operating networks to the number of available channels within the unlicensed spectrum, divided by the width of the passband. As the number of WLAN users increases and the bandwidth requirements of applications grow, more WLAN infrastructure must be deployed to support the users, and available throughput must increase. Therefore, the amount of unlicensed spectrum available, and the efficiency with which the standard uses the spectrum, are important considerations.

7.1 2.4 GHz – Wi-Fi, 802.11g_{OFDM}, & 802.11g_{BCC}

The 2.4 GHz 802.11 standards all require a passband approximately 22 MHz wide for one operating network. Using direct sequence spread spectrum modulation (DSSS), Wi-Fi provides an 11 Mbps data rate to the network users. Thus, the 2.4 GHz band's 83.5 MHz will support three non-overlapping, simultaneously operating Wi-Fi networks (66/83.5), and roughly 33 Mbps of data rate (11 Mbps * 3 networks) to be shared among common users across the coverage area (see Figure 2).

This has been proven to adequately distribute sufficient bandwidth to support the majority of applications across many environments, including the relatively dense "cube farms" of large corporations. In today's environment, common Wi-Fi

[13] While the 2.4 GHz spectral boundaries are common, the regulatory rules are not. For example, 802.11g_{OFDM} and 802.11g_{BCC} are currently illegal in the United States, but both are legal in Europe. Bluetooth with 1 MHz channels is legal in almost all relevant countries.

©2001 Mobilian Corporation. All rights reserved.

networks support applications such as Microsoft Office, email, server downloads, and FTP applications, by literally dozens of users per AP. Additionally, as user densities increase, Wi-Fi AP transmit power can be decreased, effectively increasing the number of networks within a given area, and therefore increasing the total capacity.

When 802.11g solutions begin entering the market, the available bandwidth provided by Wi-Fi will increase substantially, while maintaining relatively low cost points due to the small incremental development that will be required to produce 802.11g solutions. This will likely provide sufficient throughput for highly data-intensive programs such as computer-aided design / manufacturing, large databases, streaming video, etc.

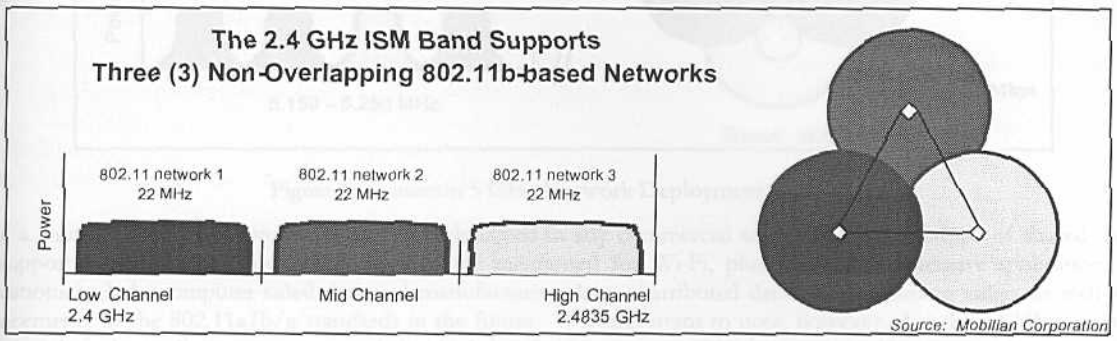


Figure 2: Three 802.11b-based Networks in the 2.4 GHz Band

Wi-Fi throughput levels will support QoS enhancements under the IEEE 802.11e Task Group, although at the expense of a dedicated network or reduced throughput for the existing network. The 802.11e's recommendations will also apply to both 802.11g and 802.11a, which will support the resulting QoS much more effectively.

7.2 5 GHz – 802.11a

The 802.11a standard requires a 16.6 MHz passband for one operating network. The modulation technique allowed in 5 GHz (OFDM) is more efficient than the spread spectrum techniques Wi-Fi uses (more bits/second/hertz), and provides up to 54 Mbps of data rate to network users. For the US-based 802.11a standard, the 5 GHz unlicensed band covers 300 MHz of spectrum and therefore supports twelve (12) non-overlapping, simultaneously operating networks, as shown in Figure 3.

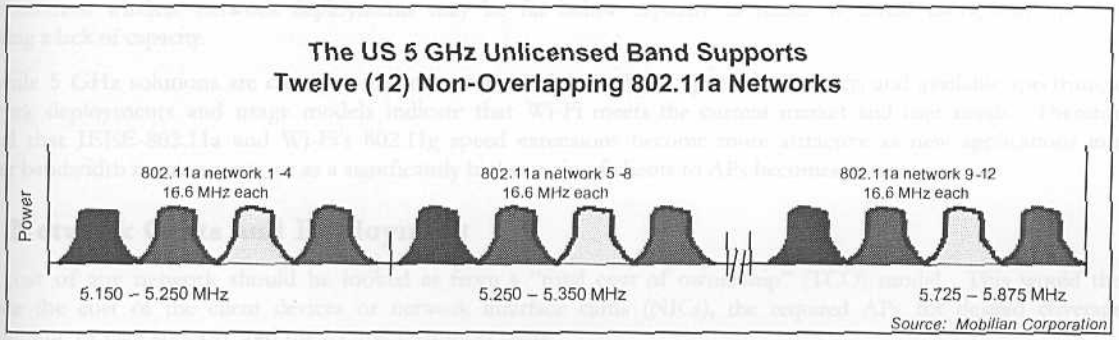


Figure 3: Twelve 802.11a Networks in the US 5 GHz Band

Sources often cite the figure "648 Mbps of total data rate to distribute across 12 networks (54 Mbps * 12 networks)." However, it is more likely that common network deployments will support 4 simultaneously operating networks in a single area, providing a 216 Mbps data rate (54 Mbps * 4 networks), only within the relatively small range at which 54 Mbps is actually attainable (see Figure 4). Further from the AP, a station's attainable data rate decreases. This issue is addressed in more detail in section 4.

©2001 Mobilian Corporation. All rights reserved.

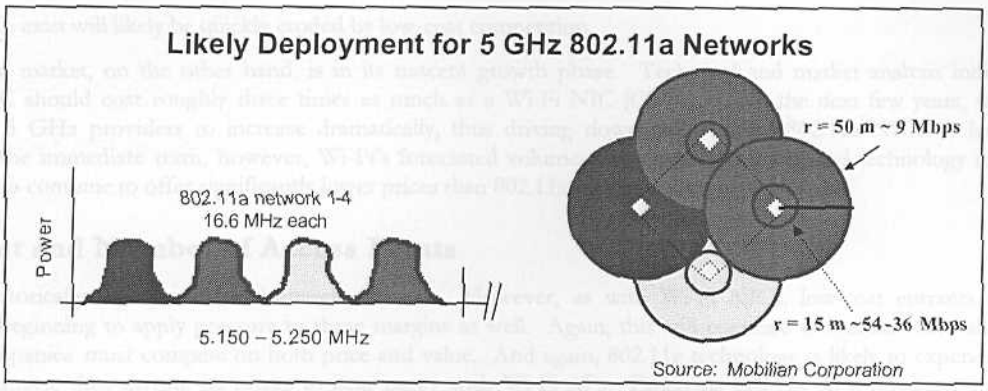


Figure 4: Common 5 GHz Network Deployment Topology

While a four-AP, 5 GHz network has not been deployed in any commercial environment, 216 Mbps of shared data rate will support all the office productivity applications mentioned for Wi-Fi, plus highly data-intensive applications. Such applications include computer-aided design / manufacturing, large distributed databases, streaming video, as well as QoS enhancements to the 802.11a/b/g standards in the future. It is important to note, however, that the 54 Mbps data rate is within a relatively small coverage area, and that high bandwidth users outside that area would require either more APs for increased coverage, or be subject to reduced throughput.

7.3 Conclusion– Available Spectrum and Spectral Effency

The 5 GHz unlicensed band provides over three times as much spectrum as the 2.4 GHz band, and 802.11a provides almost five times the data rate of currently available Wi-Fi solutions. This leads to a vast difference in the number of networks that may be deployed in a single area (12 to 3), and the corresponding data rate amount. However, a few considerations must be taken into account.

First, according to many Wi-Fi installations, an 11 Mbps data rate seems to be sufficient for today's office environment and common network applications, leading one to doubt the urgency of higher bandwidth. Second, although both Wi-Fi and 802.11a can support 20 to 30 users in both theory and recommended practice [LU01], market data shows that the penetration of APs to clients is very low: one AP to every seven clients is the average [CIS00b; VDC01]. This indicates that common wireless network deployments may be far below capacity in terms of actual users, and therefore not suffering a lack of capacity.

So while 5 GHz solutions are clearly dominant in terms of throughput, spectral efficiency, and available spectrum, current network deployments and usage models indicate that Wi-Fi meets the current market and user needs. Therefore, it is logical that IEEE-802.11a and Wi-Fi's 802.11g speed extensions become more attractive as new applications introduce higher bandwidth requirements, or as a significantly higher ratio of clients to APs becomes common.

8 Network Costs and Deployment

The cost of any network should be looked at from a "total cost of ownership" (TCO) model. This would therefore include the cost of the client devices or network interface cards (NICs), the required APs for desired coverage area, throughput, or user support, and the technical support costs.

8.1 Cost of Network Interface Cards (NICs)

The cost of network interface cards (NICs) for Wi-Fi and 802.11a solutions is currently a topic of heated debate in the industry. Wi-Fi technologies are experiencing significant downward pricing pressure from companies that have exported assembly to low-cost OEM nations. As with any competitive market, this will drive the marginal gain to equilibrium with marginal cost, and eventually companies that cannot effectively compete will exit the market. Meanwhile, the customers will benefit enormously as more features are built into every card at similar or declining costs. This same market dynamic will likely hold true for 802.11g solutions since the core technology enhancement is only slightly more expensive than existing Wi-Fi technology, and will be produced by the same companies currently producing the Wi-Fi chipsets. What

©2001 Mobilian Corporation. All rights reserved.

premiums do exist will likely be quickly eroded by low-cost competition.

The 802.11a market, on the other hand, is in its nascent growth phase. Technical and market analysis indicates that an 802.11a NIC should cost roughly three times as much as a Wi-Fi NIC [CI00c]. Over the next few years, we expect the number of 5 GHz providers to increase dramatically, thus driving down the cost for 802.11a NICs to levels closer to Wi-Fi. In the immediate term, however, Wi-Fi's forecasted volumes, IC integration levels, and technology maturity levels will allow it to continue to offer significantly lower prices than 802.11a.

8.2 Cost and Number of Access Points

APs are historically high-priced, high-margin devices. However, as with Wi-Fi NICs, low-cost entrants to the Wi-Fi market are beginning to apply pressure to these margins as well. Again, this will continue to increase the value to the end user, as companies must compete on both price and value. And again, 802.11g technology is likely to experience the same market dynamics, thus driving its prices to near parity with Wi-Fi APs. Emerging 802.11a APs, however, are likely to be generally more expensive than Wi-Fi and 802.11g APs.

A more important aspect of AP cost however, is the number of APs needed to cover similar areas. Because 802.11a APs operate in the 5 GHz unlicensed bands, the physics of radio wave propagation become a significant factor, and an 802.11a AP will cover only about a fourth of the area covered by a Wi-Fi AP. Referring back to Figure 1, this means that in order to cover similar sized areas, with all factors being equal including throughput, four 802.11a APs are required for every one Wi-Fi AP.

This not only presents a problem with potential deployment costs, but if there is an existing Wi-Fi network, it becomes readily apparent that a simple overlay of 802.11a APs will not suffice, as only a quarter of the current users will receive the 802.11a service, and a much smaller number will receive the 54 Mbps date rate (see Figure 4). There are ways to address this issue, but not without either increasing the 802.11a APs or changing the operating parameters of the pre-existing Wi-Fi network.

Of course, in some instances 802.11a's restricted range can be an attractive feature. The primary driver is very high-bandwidth requirements in a very dense user environment. A trading floor with multiple networks, or tightly packed PCs running graphics -intensive applications might be good examples of this type of scenario.

Deployment of more than three networks in a confined area is another example of where reduced range would be attractive. As shown in Figure 2, only three simultaneously operating Wi-Fi networks can overlap without causing interference to each other. Outdated Wi-Fi APs do not have adjustable transmit power, thus representing a capacity ceiling for any area smaller than Wi-Fi's 100m radius coverage. New Wi-Fi APs allow the user to scale transmit power and thus reduce the coverage footprint thereby avoiding this potential problem; but it remains a fact that the 2.4 GHz band can only support three overlapping, simultaneously operating Wi-Fi networks. The 5 GHz band, on the other hand, can support up to 12 overlapping 802.11a networks, providing for a large amount of potential throughput in a very small area. However, at this time we do not believe there is a common example of where this amount of throughput would be applicable.

8.3 Cost of Support- Certified Interoperability (Wi-Fi)

One key cost component often overlooked when deploying new technology is the cost of technical support. While many companies are not able to track the cost of a technician trouble ticket, this is a tangible component of the total cost of ownership of any piece of technology, and should be a consideration in deployment of any new technology.

In terms of managing the potential support costs for deploying a wireless LAN, one of the possibilities is clearly superior: Wi-Fi. The key differentiator between Wi-Fi and all other past and future wireless LAN technologies is the Wi-Fi brand itself. This is far more than a simple brand, because it is in fact a rigorous certification process that guarantees interoperability with other Wi-Fi certified products [WECA01].

As mentioned in section 1, the guaranteed interoperability of Wi-Fi certified products was highly instrumental in launching the overall WLAN market. Up to the point of Wi-Fi's ratification and implementation, IT managers were reluctant to adopt WLAN technologies for fear of them becoming obsolete, and because of the associated overhead support costs of configuring multiple vendors' solutions for interoperability.

Because this proved to be so critical to Wi-Fi, both 802.11g and 802.11a technologies are currently being evaluated for

©2001 Mobilian Corporation. All rights reserved.

similar certification processes. This is a time-consuming process, but it is likely to be approved and implemented in less than 12 to 18 months from the publication date of this paper. For this reason, it is likely that initial support costs for deploying these technologies will be high relative to Wi-Fi based solutions.

9 Overall Conclusions

As more and more companies adopt WLANs, the resulting benefits become easier to quantify. According to Gartner publications, the economic benefits of WLANs can add up to as much as $16,000 in savings per user compared with wired alternatives [TEC01]. Given that Wi-Fi is the most widely deployed WLAN standard, this tangible cost benefit is likely due in large part to its growing adoption as a mainstream, horizontal application—and the market shows no signs of slowing.

Wi-Fi's 11 Mbps data rate provides a good user experience in the majority of existing wireless networks, and with speed extensions fom 802.11g and 802.11a on the horizon, WLANs will be able to provide bandwidth and capacity for continued user growth and new generations of applications.

The value of both 802.11g and 802.11a is very clear. Wi-Fi's 802.11g-speed extension will provide the necessary data rate speed enhancement to allow current Wi-Fi users to deploy QoS and other high-bandwidth applications, while maintaining backward compatibility with Wi-Fi. And as 802.11a matures, it will provide greater overall capacity for bandwidth-intensive, smaller coverage areas.

Based on these clear value propositions, we expect to see mixed-standard enterprise environments in which both 802.11a and Wi-Fi-based technologies coexist. High-density, high-bandwidth common areas will be served by 802.11a—lunchrooms, conference rooms, team rooms, etc.—and lower-density, greater coverage areas will be served by Wi-Fi-based technologies (Wi-Fi and 802.11g).

A mixed-standard environment implies that client devices should be able to roam between 802.11a and Wi-Fi networks. We believe that as greater numbers of competitors enter the 5 GHz market, 802.11a prices will come down, and dual-mode clients and APs will become prevalent. These dual-mode devices will allow IT departments to benefit from the higher-capacity, higher-bandwidth 802.11a networks, while continuing to leverage the basic throughput, lower cost, and lower risk of Wi-Fi-based networks.

©2001 Mobilian Corporation. All rights reserved.

Appendix A—Comparison of radio wave propagation at 2.4 and 5 GHz frequencies

While the propagation characteristics of the 5GHz band has not been studied as extensively as the cellular and PCS bands, there is still an adequate body of analysis and measurements that can be drawn from to create useful path loss models.

The physics principle of free space propagation found in Theodore S. Rappaport's "Wireless Communications: Principles & Practice" states that as an electromagnetic wave's length (λ) grows shorter (i.e., higher frequency), the path loss of that wave increases according to a square law relationship [RAP01]. Also from electromagnetic wave propagation theory, the path loss increases proportionally with the square of the distance between transmitter and receiver in free space. Since 5 GHz radios operate a at little over 2 times the frequency of 2.4 GHz radios, it can be shown that the same link budget can only be sustained over about half the distance as a comparable 2.4 GHz system. This is represented by the equation below and Figure 5.

$\ell_x = K(d^N/\lambda_x^2)$ [often expressed in decibels as $\ell_{x\,(db)} = K_L + 10N \log_{10}(d) + 20 \log_{10}(f_x)$]

OR $d = [\,(\ell_x * \lambda^2)/K\,]^{1/N}$

Where:
ℓ_x = path loss
$_x$ = frequency band or standard ("a" for 802.11a or "b" for Wi-Fi and 802.1.1g)
K = constant
K_L = constant for loss in dB = 32.44 when f is in MHz and d is in kilometers
d = distance
N = attenuation factor: N=2 for free space; N>2 in most practical environments
λ = wavelength
f = frequency = c/λ
c = speed of light = 3×10^8 meters/second (free space)

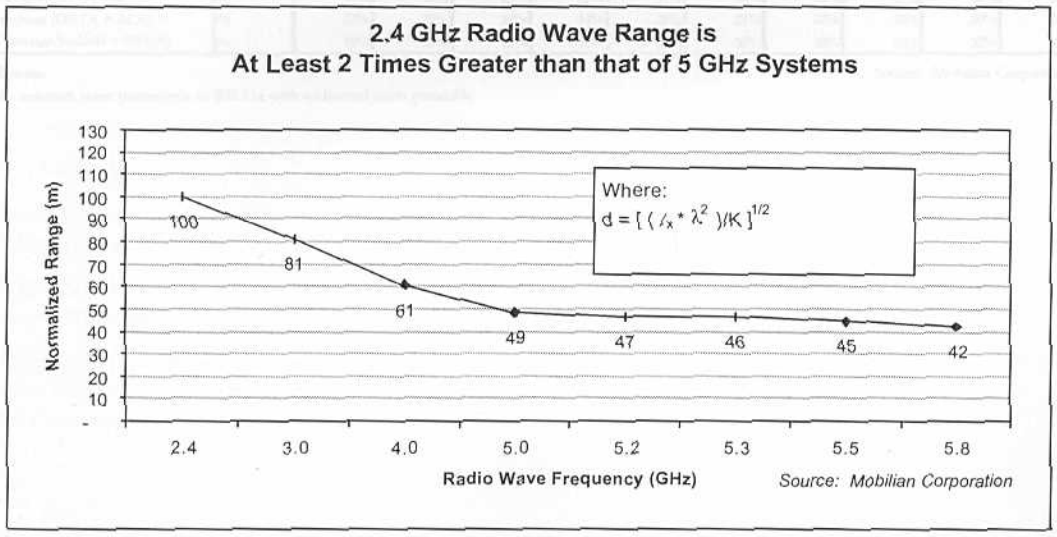


Figure 5: Comparative Free Space Path Loss Between 2.4 and 5 GHz Systems

Rappaport and Durgin's IEEE study of 5 GHz indoor path loss in urban homes [JCS01, DUR01] has been used primarily in this paper with slight modifications; it is an empirical model that is an extension of the free space path loss given above that simplifies to:

$L_a = 57 + 34 \log_{10}(d)$

Where d is in meters and the 5.x GHz band is assumed.

©2001 Mobilian Corporation. All rights reserved.

Appendix B—WLAN Throughput Calculations

The wireless LAN data rate numbers used throughout this paper refer to data rate at the top of the MAC, and use the overhead and throughput calculations shown in the table below.

Table 5: Throughput Calculation by Standard

	Units	Wi-Fi™, 11 Mbps, long preamble		Wi-Fi™, 11 Mbps, short preamble		802.11a		802.11g OFDM*		802.11g PBCC	
		slow ACK	*fast ACK*	*slow ACK*	*fast ACK*	*slow ACK*	*Fast ACK*	*slow ACK*	*Fast ACK*	*slow ACK*	*fast ACK*
CW min		31	31	31	31	15	15	31	31	31	31
SIFS	micro sec	10	10	10	10	16	16	10	10	10	10
Slot duration	micro sec	20	20	20	20	9	9	20	20	20	20
DIFS	micro sec	50	50	50	50	34	34	50	50	50	50
Average Backoff Duration	micro sec	360	360	360	360	102	102	360	360	360	360
DATA MPDU Rate	Mbps	11	11	11	11	54	54	24	24	22	22
DATA MPDU Payload size	B	1500	1500	1500	1500	1500	1500	1500	1500	1500	1500
DATA MPDU Overhead	B	28	28	28	28	28	28	28	28	28	28
DATA PPDU Overhead	micro sec	192	192	96	96	20	20	116	116	96	96
DATA PPDU Duration	micro sec	1303	1303	1207	1207	246	246	625	625	652	652
SIFS	micro sec	10	10	10	10	16	16	10	10	10	10
ACK MPDU Rate	Mpbs	2	11	2	11	24	54	2	11	2	22
ACK MPDU Length	B	14	14	14	14	14	14	14	14	14	14
ACK PPDU Overhead	micro sec	192	192	96	96	20	20	96	96	96	96
ACK PPDU Duration		248	202	152	106	25	22	152	106	152	101
Backoff + DATA + SIFS + ACK duration	micro sec	1921	1875	1729	1683	389	386	1147	1102	1174	1123
Effective throughput	Mbps	6.25	6.40	6.94	7.13	30.89	31.09	10.46	10.89	10.22	10.69
Through put as % of DATA PHY rate	%	57%	58%	63%	65%	57%	58%	44%	45%	46%	49%
MPDU+PPDU overhead (DATA + ACK) %	%	22%	23%	14%	14%	21%	21%	22%	23%	20%	21%
Backoff overhead (average backoff + SIFS)%	%	19%	20%	21%	22%	30%	30%	32%	34%	32%	33%

Assumed no collisions

*802.11g OFDM - assumes same parameters as 802.11a with additional short preamble

Source: Mobilian Corporation

©2001 Mobilian Corporation. All rights reserved.

mobilian

References

[CIS00a] Cahners In-Stat, Bluetooth 2000 – To Enable the Star Trek Generation, July 2000

[CIS00b] Cahners In-Stat, 2000 Enterprise Wireless LAN Update, February 2001

[CI00c] Cahners In-Stat, Wild On Wireless Networking: WLAN Market Young, Energetic and Growing, April 2001

[VDC01] 2000 Wireless LAN Survey, Venture Development Corporation, November 2000

[GG01] *WLAN: Even Superman Can't Dodge This Bullet*, Bob Egan, Gartner Group Mobile and Wireless Symposium, San Diego, March 2001

[MBLN01] Mobilian Corporation, *Wi-Fi™ (802.11b) and Bluetooth Simultaneous Operation: Characterizing the Problem*, November 2000

[MBLN02] Mobilian Corporation, *Coexistence Approaches for Wi-Fi (802.11b) and Bluetooth*, January 2001

[RAP01] Theodore S. Rappaport, *Wireless Communications, Principles & Practices*, 1996

[DUR01] G. Durgin, T. S. Rappaport, H. Xu, *"Measurements and Models for Radio Path Loss and Penetration Loss in and Around Homes and Trees at 5.85 GHz,"* IEEE Transactions on Communications, Vol. 46, No. 11, November 1998, pp. 1484-1496.

[WECA01] Wireless Ethernet Compatibility Alliance (WECA), *Wi-Fi System Interoperability Test Plan v1.0a*, March 28, 2000

[LU01] Orinoco AS-1000 solutions support documentation, April 17th, 2001
http://www.wavelan.com/template.html?section=m82&envelope=109&page=2054

[JCS01] John C. Stein, *Indoor Radio WLAN Performance Part II: Range Performance in a Dense Office Environment*, Harris Semiconductor (Intersil)

[IEEE802.11] International Standard ISO/IEC 8802-11 IEEE P802.11

[IEEE802.11b] IEEE Std 802.11b-1999 (Supplement to ANSI/IEEE Std 802.11, 1999 Edition)

[IEEE802.11a] IEEE Std 802.11a-1999 (Supplement to IEEE Std 802.11-1999)

[TEC01] *When wireless is the most cost-effective solution*, Veronica Combs, TecRepublic, Dec 2000.

[BT11] Bluetooth Specification 1.1

[Kam99] A. Kamerman, "*Coexistence between Bluetooth and IEEE 802.11 CCK Solutions to Avoid Mutual Interferenc,e*" Lucent Technologies Bell Laboratories, Jan. 1999, also available as IEEE 802.11-00/162, July 2000.

[ETSI99] ETR0230002 V0.2.0 (1999-04) Broadband Radio Access Networks (BRAN); High Performance Radio Local Area Networks (HIPERLAN) Type 2; System Overview (www.etsi.org)

[FCC15.247] Code of Federal Regulations, Title 47, Volume 1, Part 15, Subpart C (Intentional Radiators), Section 247. US Government Printing Office. October 1, 1998 Revision of 47CFR15.247, pages 690-692. Available on the web at: http://www.access.gpo.gov/nara/waisidx_99/47cfr15_99.html.

©2001 Mobilian Corporation. All rights reserved.

ANEXO F

Bluetooth Assigned Numbers

Bluetooth Assigned Numbers

This is a living document that lists assigned numbers, codes and identifiers in the Bluetooth standard

Bluetooth™

Version 1.1
February 22 2001

Revision History

The Revision History is shown in on page 29.

Contributors

The persons who contributed to this specification are listed on page 29.

Web Site

This document can also be found on the Bluetooth website:
http://www.bluetooth.org/assigned-numbers.htm

Disclaimer and Copyright Notice

The copyright in these specifications is owned by the Promoter Members of Bluetooth SIG, Inc. ("Bluetooth SIG"). Use of these specifications and any related intellectual property (collectively, the "Specification"), is governed by the Promoters Membership Agreement among the Promoter Members and Bluetooth SIG (the "Promoters Agreement"), certain membership agreements between Bluetooth SIG and its Adopter and Associate Members (the "Membership Agreements") and the Bluetooth Specification Early Adopters Agreements ("1.2 Early Adopters Agreements") among Early Adopter members of the unincorporated Bluetooth special interest group and the Promoter Members (the "Early Adopters Agreement"). Certain rights and obligations of the Promoter Members under the Early Adopters Agreements have been assigned to Bluetooth SIG by the Promoter Members.

Use of the Specification by anyone who is not a member of Bluetooth SIG or a party to an Early Adopters Agreement (each such person or party, a "Member"), is prohibited. The legal rights and obligations of each Member are governed by their applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Specification not in compliance with the terms of the applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement is prohibited and any such prohibited use may result in termination of the applicable Membership Agreement or Early Adopters Agreement and other liability permitted by the applicable agreement or by aplicable law to Bluetooth SIG or any of its members for patent, copyright and/or trademark infringement.

THE SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR REASONABLE SKILL OR CARE, OR ANY WARRANTY ARISING OUT OF ANY COURSE OF DEALING, USAGE, TRADE PRACTICE, PROPOSAL, SPECIFICATION OR SAMPLE.

Each Member hereby acknowledges that products equipped with the Bluetooth™ technology ("Bluetooth™ Products") may be subject to various regulatory controls under the laws and regulations of various governments worldwide. Such laws and regulatory controls may govern, among other things, the combination, operation, use, implementation and distribution of Bluetooth™ Products. Examples of such laws and regulatory controls include, but are not limited to, airline regulatory controls, telecommunications regulations, technology transfer controls and health and safety regulations. Each Member is solely responsible for the compliance by their Bluetooth™ Products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their Bluetooth™ Products related to such regulations within the applicable jurisdictions. Each Member acknowledges that nothing in the Specification provides any information or assistance in connection with securing such compliance, authorizations or licenses. NOTHING IN THE SPECIFICATION CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS.

ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE SPECIFICATION IS EXPRESSLY DISCLAIMED. BY USE OF THE SPECIFICATION, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST BLUETOOTH SIG AND ITS PROMOTER MEMBERS RELATED TO USE OF THE SPECIFICATION.

Bluetooth SIG reserves the right to adopt any changes or alterations to the Specification as it deems necessary or appropriate and to adopt a process for adding new Bluetooth™ profiles after the release of the Specification.

Copyright © 1999, 2000, 2001

3Com Corporation,
Agere Systems, Inc.,
Ericsson Technology Licensing, AB,
IBM Corporation,
Intel Corporation,
Microsoft Corporation,
Motorola, Inc.,
Nokia Mobile Phones,
Toshiba Corporation

*Third-party brands and names are the property of their respective owners.

Bluetooth™

CONTENTS

1 Bluetooth Baseband 4
1.1 The General- and Device-Specific Inquiry Access Codes (DIACs) 4
1.2 The Class of Device/Service field 4
1.2.1 Major Service Classes 5
1.2.2 Major Device Classes 6
1.2.3 The Minor Device Class field 6
1.2.4 Minor Device Class field - Computer Major Class 7
1.2.5 Minor Device Class field - Phone Major Class 7
1.2.6 Minor Device Class field - LAN Access Point Major Class 8
1.2.7 Minor Device Class field - Audio Major Class 8
2 Link Manager Protocol (LMP) 10
2.1 The Link Manger Version parameter 10
2.2 The LMP_Compid parameter codes 10
3 Logical Link Control and Adaptation Protocol (L2CAP) 11
3.1 Channel Identifiers 11
3.2 Protocol and Service Multiplexor (PSM) 11
4 Service Discovery Protocol (SDP) 12
4.1 Universally Unique Identifier (UUID) short forms 12
4.2 Base Universally Unique Identifier (UUID) 12
4.3 Protocols 14
4.4 Service classes 14
4.5 Attribute Identifier codes 15
4.6 Protocol Parameters 16
4.7 Host Operating Environment Identifiers 18
4.7.1 ClientExecutableURL substitution strings 19
4.7.2 IconURL substitution strings 20
5 References 21
6 Terms and Abbreviations 22
7 List of Figures 23
8 List of Tables 24

Bluetooth™

CONTENTS

1 Bluetooth Baseband 4

1.1 The General- and Device-Specific Inquiry Access Codes (DIACs) 4

1.2 The Class of Device/Service field 4

1.2.1 Major Service Classes 5

1.2.2 Major Device Classes 6

1.2.3 The Minor Device Class field 6

1.2.4 Minor Device Class field - Computer Major Class 7

1.2.5 Minor Device Class field - Phone Major Class 7

1.2.6 Minor Device Class field - LAN Access Point Major Class 8

1.2.7 Minor Device Class field - Audio Major Class 9

2 Link Manager Protocol (LMP) 10

2.1 The Link Manger Version parameter 10

2.2 The LMP_CompId parameter codes 10

3 Logical Link Control and Adaptation Protocol (L2CAP) 11

3.1 Channel Identifiers 11

3.2 Protocol and Service Multiplexor (PSM) 11

4 Service Discovery Protocol (SDP) 12

4.1 Universally Unique Identifier (UUID) short forms 12

4.2 Base Universally Unique Identifier (UUID) 12

4.3 Protocols 13

4.4 Service classes 14

4.5 Attribute Identifier codes 15

4.6 Protocol Parameters 16

4.7 Host Operating Environment Identifiers 16

4.7.1 ClientExecutableURL substitution strings 16

4.7.2 IconURL substitution strings 20

5 References 21

6 Terms and Abbreviations 22

7 List of Figures 23

8 List of Tables 24

1 BLUETOOTH BASEBAND

1.1 THE GENERAL- AND DEVICE-SPECIFIC INQUIRY ACCESS CODES (DIACS)

The Inquiry Access Code is the first level of filtering when finding Bluetooth devices and services. The main purpose of defining multiple IACs is to limit the number of responses that are received when scanning devices within range.

X	LAP value	Usage
0	0x9E8B33	General/Unlimited Inquiry Access Code (GIAC)
1	0x9E8B00	Limited Dedicated Inquiry Access Code (LIAC)
2-63	0x9E8B01-0x9E8B32, 0x9E8B34-0x9E8B3F	RESERVED FOR FUTURE USE

Table 1.1: The Inquiry Access Codes

The Limited Inquiry Access Code (LIAC) is only intended to be used for limited time periods in scenarios where both sides have been explicitly caused to enter this state, usually by user action. For further explanation of the use of the LIAC, please refer to the Generic Access Profile [7].

In contrast it is allowed to be continuously scanning for the General Inquiry Access Code (GIAC) and respond whenever inquired.

1.2 THE CLASS OF DEVICE/SERVICE FIELD

The Class of Device/Service (CoD) field has a variable format. The format is indicated using the 'Format Type field' within the CoD. The length of the Format Type field is variable and ends with two bits different from '11'. The version field starts at the least significant bit of the CoD and may extend upwards.

Figure 1.1: General format of Class of Device/Service

In the 'format #1' of the CoD (Format Type field = 00), 11 bits are assigned as a bit-mask (multiple bits can be set) each bit corresponding to a high level generic category of service class. Currently 7 categories are defined. These

1 BLUETOOTH BASEBAND

1.1 THE GENERAL- AND DEVICE-SPECIFIC INQUIRY ACCESS CODES (DIACS)

The Inquiry Access Code is the first level of filtering when finding Bluetooth devices and services. The main purpose of defining multiple IACs is to limit the number of responses that are received when scanning devices within range.

#	LAP value	Usage
0	0x9E8B33	General/Unlimited Inquiry Access Code (GIAC)
1	0x9E8B00	Limited Dedicated Inquiry Access Code (LIAC)
2-63	0x9E8B01-0x9E8B32, 0x9E8B34-0x9E8B3F	RESERVED FOR FUTURE USE

Table 1.1: The Inquiry Access Codes

The Limited Inquiry Access Code (LIAC) is only intended to be used for limited time periods in scenarios where both sides have been explicitly caused to enter this state, usually by user action. For further explanation of the use of the LIAC, please refer to the Generic Access Profile [7].

In contrast it is allowed to be continuously scanning for the General Inquiry Access Code (GIAC) and respond whenever inquired.

1.2 THE CLASS OF DEVICE/SERVICE FIELD

The Class of Device/Service (CoD) field has a variable format. The format is indicated using the 'Format Type field' within the CoD. The length of the Format Type field is variable and ends with two bits different from '11'. The version field starts at the least significant bit of the CoD and may extend upwards.

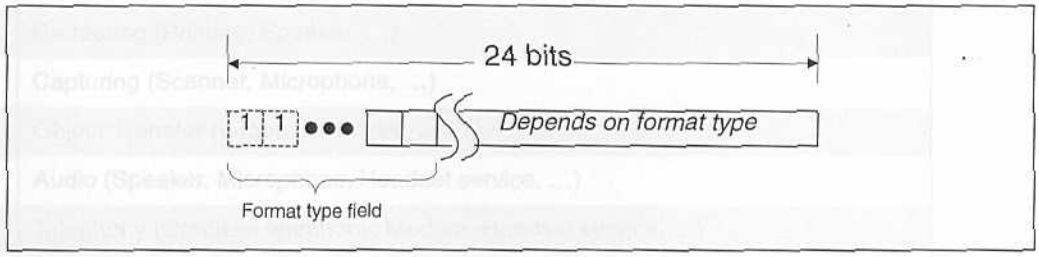


Figure 1.1: General format of Class of Device/Service

In the 'format #1' of the CoD (Format Type field = 00), 11 bits are assigned as a bit-mask (multiple bits can be set) each bit corresponding to a high level generic category of service class. Currently 7 categories are defined. These

are primarily of a 'public service' nature. The remaining 11 bits are used to indicate device type category and other device-specific characteristics.

Any reserved but otherwise unassigned bits, such as in the Major Service Class field, should be set to 0.

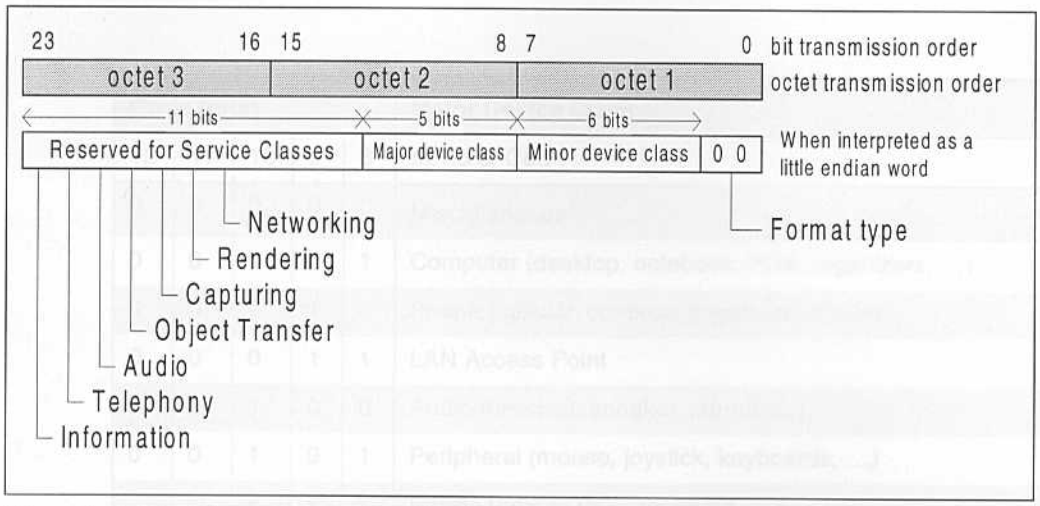


Figure 1.2: The Class of Device/Service field (format type 1). Note the order in which the octets are sent on the air and stored in memory.

1.2.1 Major Service Classes

Bit no	Major Service Class
13	Limited Discoverable Mode[1]
14	(reserved)
15	(reserved)
16	(reserved)
17	Networking (LAN, Ad hoc, ...)
18	Rendering (Printing, Speaker, ...)
19	Capturing (Scanner, Microphone, ...)
20	Object Transfer (v-Inbox, v-Folder, ...)
21	Audio (Speaker, Microphone, Headset service, ...)
22	Telephony (Cordless telephony, Modem, Headset service, ...)
23	Information (WEB-server, WAP-server, ...)

Table 1.2: Major Service Classes

1. As defined in [7]

1.2.2 Major Device Classes

The Major Class segment is the highest level of granularity for defining a Bluetooth Device. The main function of a device is used to determine the major class grouping. There are 32 different possible major classes. The assignment of this Major Class field is defined in Table 1.3.

Code (bits)					Major Device Class
12	11	10	9	8	bit no of CoD
0	0	0	0	0	Miscellaneous[1]
0	0	0	0	1	Computer (desktop, notebook, PDA, organizers, ...)
0	0	0	1	0	Phone (cellular, cordless, payphone, modem, ...)
0	0	0	1	1	LAN Access Point
0	0	1	0	0	Audio (headset, speaker, stereo, ...)
0	0	1	0	1	Peripheral (mouse, joystick, keyboards, ...)
x	x	x	x	x	Range 0x06 to 0x1E reserved
1	1	1	1	1	Unclassified, specific device code not assigned

Table 1.3: Major Device Classes

1. Used where a more specific Major Device Class code is not suited (but only as specified in this document. Devices that do not have a major class code assigned can use the all-1 code until 'classified')

1.2.3 The Minor Device Class field

The 'Minor Device Class field' (bits 7 to 1 in the CoD), are to be interpreted only in the context of the Major Device Class (but independent of the Service Class field). Thus the meaning of the bits may change, depending on the value of the 'Major Device Class field'. When the Minor Device Class field indicates a device class, then the primary device class should be reported, e.g. a cellular phone that can also work as a cordless handset should use 'Cellular' in the minor device class field.

1.2.4 Minor Device Class field - Computer Major Class

Code (bits)						Minor Device Class
7	6	5	4	3	2	bit no of CoD
0	0	0	0	0	0	Unclassified, code for device not assigned
0	0	0	0	0	1	Desktop workstation
0	0	0	0	1	0	Server-class computer
0	0	0	0	1	1	Laptop
0	0	0	1	0	0	Handheld PC/PDA (clam shell)
0	0	0	1	0	1	Palm sized PC/PDA
x	x	x	x	x	x	Range 0x06-0x7F reserved

Table 1.4: Sub Device Class field for the 'Computer' Major Class

1.2.5 Minor Device Class field - Phone Major Class

Code (bits)						Minor Device Class
7	6	5	4	3	2	bit no of CoD
0	0	0	0	0	0	Unclassified, code not assigned
0	0	0	0	0	1	Cellular
0	0	0	0	1	0	Cordless
0	0	0	0	1	1	Smart phone
0	0	0	1	0	0	Wired modem or voice gateway
x	x	x	x	x	x	Range 0x05-0x7F reserved

Table 1.5: Sub Device Classes for the 'Phone' Major Class

1.2.6 Minor Device Class field - LAN Access Point Major Class

Code (bits)			Minor Device Class
7	6	5	bit no of CoD
0	0	0	Fully available
0	0	1	1-17% utilized
0	1	0	17 - 33% utilized
0	1	1	33 - 50% utilized
1	0	0	50 - 67% utilized
1	0	1	67 - 83% utilized
1	1	0	83 - 99% utilized
1	1	1	No Service Available[1]

Table 1.6: The LAN Access Point Load Factor field

1. "Device is fully utilized and cannot accept additional connections at this time, please retry later"

The exact loading formula is not standardized. It is up to each LAN Access Point implementation to determine what internal conditions to report as a utilization percentage. The only requirement is that the number reflects an ever-increasing utilization of communication resources within the box. As a recommendation, a client that locates multiple LAN Access Points should attempt to connect to the one reporting the lowest load.

Code (bits)			Minor Device Class
4	3	2	bit no of CoD
0	0	0	Unclassified (use this value if no other apply)
x	x	x	range 0x01-0x0F reserved

Table 1.7: Reserved sub-field for the LAN Access Point

1.2.7 Minor Device Class field - Audio Major Class

Code (bits)						Minor Device Class
7	6	5	4	3	2	bit no of CoD
0	0	0	0	0	0	Unclassified, code not assigned
0	0	0	0	0	1	Device conforms to the Headset profile [9]
x	x	x	x	x	x	Range 0x02-0x7F reserved

Table 1.8: Sub Device Classes for the 'Audio' Major Class

2 LINK MANAGER PROTOCOL (LMP)

2.1 THE LINK MANGER VERSION PARAMETER

Parameter name	Assigned values	
VersNr	0	Bluetooth LMP 1.0, [2]
	1	Bluetooth LMP 1.1
	2-255	(reserved)

Table 2.1: The LMP Version Parameter Values

2.2 THE LMP_COMPID PARAMETER CODES

This is the parameter used in the LMP Version procedure. All companies that create a unique implementation of the Link Manager shall have their own LMP_COMPID.

Code	Company
0	Ericsson Mobile Communications
1	Nokia Mobile Phones
2	Intel Corp.
3	IBM Corp.
4	Toshiba Corp.
5	3Com
6	Microsoft
7	Lucent
8	Motorola
9	Infineon Technologies AG
10	Cambridge Silicon Radio
11	Silicon Wave
12	Digianswer
13 - 65534	(reserved)
65535	For use in internal and interoperability tests before a Company ID has been assigned. May not be used in products.

Table 2.2: The LMP_CompId parameter codes

3 LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL (L2CAP)

Please see Section 4.3 for assigned PSM values.

3.1 CHANNEL IDENTIFIERS

Destination CID	Protocol/usage	Reference
0x0000	Illegal, should not be used	[3]
0x0001	L2CAP signalling channel	[3]
0x0002	L2CA connection less data	[3]
0x0003 - 0x003F	(reserved)	

Table 3.1: Pre-defined L2CAP Channel Identifiers

3.2 PROTOCOL AND SERVICE MULTIPLEXOR (PSM)

Protocol	PSM	Reference
SDP	0x0001	[4]
RFCOMM	0x0003	[5]
TCS-BIN	0x0005	[6]
TCS-BIN-CORDLESS	0x0007	[6]

Table 3.2: Assigned Protocol and Service Multiplexor values (PSM)

4 SERVICE DISCOVERY PROTOCOL (SDP)

4.1 UNIVERSALLY UNIQUE IDENTIFIER (UUID) SHORT FORMS

The Bluetooth Service Discovery Protocol (SDP) specification defines a way to represent a range of UUIDs (which are nominally 128-bits) in a shorter form. A *reserved* range of 2^{32} values can be represented using 32-bits (denoted uuid32). Of these, a sub-range of 2^{16} values can be represented using only 16-bits (denoted uuid16). Any value in the 2^{32} range that is not assigned in this document is reserved pending future revisions of this document. In other words, no value in this range may be used except as specified in this or future revisions of this document. UUID values outside of this range can be allocated as described in [19] for any purpose the allocater desires.

4.2 BASE UNIVERSALLY UNIQUE IDENTIFIER (UUID)

The Base UUID is used for calculating 128-bit UUIDs from 'short UUIDs' (uuid16 and uuid32) as described in the SDP Specification [4].

Mnemonic	UUID
BASE_UUID	00000000-0000-1000-8000-00805F9B34FB

4.3 PROTOCOLS

Mnemonic	UUID	Name	Ref.
SDP	uuid16: *0x0001*[1]	sdp.bt	[4]
RFCOMM	uuid16: *0x0003*	com.bt	[5]
TCS-BIN	uuid16: *0x0005*	tcs.bt	[6]
L2CAP	uuid16: *0x0100*		[3]
IP	uuid16: *0x0009*		
UDP	uuid16: *0x0002*		
TCP	uuid16: *0x0004*		
TCS-AT	uuid16: *0x0006*	modem	
OBEX	uuid16: *0x0008*	obex	
FTP	uuid16: *0x000A*	ftp	
HTTP	uuid16: *0x000C*	http	
WSP	uuid16: *0x000E*	wsp	

Table 4.1: Protocol Universally Unique Identifiers and Names

1. 'Short UUID'

4.4 SERVICE CLASSES

Mnemonic	UUID	Profile[1]	AbstractName
ServiceDiscoveryServerServiceClassID	uuid16: *0x1000*		
BrowseGroupDescriptorServiceClassID	uuid16: *0x1001*		
PublicBrowseGroup	uuid16: *0x1002*		
SerialPort	uuid16: *0x1101*	[7]	serial.bt
LANAccessUsingPPP	uuid16: *0x1102*		
DialupNetworking	uuid16: *0x1103*	[13]	
IrMCSync	uuid16: *0x1104*	[17]	
OBEXObjectPush	uuid16: *0x1105*	[16]	
OBEXFileTransfer	uuid16: *0x1106*	[15]	
IrMCSyncCommand	uuid16: *0x1107*	[17]	
Headset	uuid16: *0x1108*	[7]	headset
CordlessTelephony	uuid16: *0x1109*	[10]	
Intercom	uuid16: *0x1110*	[11]	
Fax	uuid16: *0x1111*	[12]	
HeadsetAudioGateway	uuid16: 0x1112	[7]	
WAP	uuid16: 0x1113	[20]	
WAP_CLIENT	uuid16: 0x1114	[20]	
PnPInformation	uuid16: *0x1200*		
GenericNetworking	uuid16: *0x1201*	n/a	
GenericFileTransfer	uuid16: *0x1202*	n/a	
GenericAudio	uuid16: *0x1203*	n/a	
GenericTelephony	uuid16: *0x1204*	n/a	

Table 4.2: Service Class Identifiers and Names

1. If the specified Service Class directly and exactly implies a certain Profile, the Profile is indicated here (i.e. for concrete Service Classes). Leave empty for abstract Service Classes.

The Profile column in Table 4.2 indicates which Service Class identifiers that also directly corresponds to a Bluetooth Profile. It is not allowed to use the Service Class UUID unless the service complies with the specified Profile. These UUIDs might also appear as Profile Identifiers in the BluetoothProfileDescriptorList attribute.

4.5 ATTRIBUTE IDENTIFIER CODES

Mnemonic	Attribute ID	Reference
ServiceRecordHandle	0x0000	[4] *Bluetooth Service Discovery Protocol (SDP)*, Bluetooth SIG
ServiceClassIDList	0x0001	
ServiceRecordState	0x0002	
ServiceID	0x0003	
ProtocolDescriptorList	0x0004	
BrowseGroupList	0x0005	
LanguageBaseAttributeIDList	0x0006	
ServiceInfoTimeToLive	0x0007	
ServiceAvailability	0x0008	
BluetoothProfileDescriptorList	0x0009	
DocumentationURL	0x000A	
ClientExecutableURL	0x000B	
Icon10	0x000C	
IconURL	0x000D	
Reserved	0x000E-0x01FF	
ServiceName	0x0000 + b[1]	
ServiceDescription	0x0001 + b	
ProviderName	0x0002 + b	
VersionNumberList	0x0200	
ServiceDatabaseState	0x0201	
GroupID	0x0200	
Remote audio volume control	0x0302[2]	[7]
External network	0x0301	[10]
Service Version	0x0300	
Supported Data Stores List	0x0301	[17]
Supported Formats List	0x0303	[16]

Table 4.3: Attribute Identifiers

Mnemonic	Attribute ID	Reference
Fax Class 1 Support	0x0302	[12]
Fax Class 2.0 Support	0x0303	
Fax Class 2 Support	0x0304	
Audio Feedback Support	0x0305	
NetworkAddress	0x0306	[20]
WAPGateWay	0x0307	[20]
HomePageURL	0x0308	[20]
WAPStackType	0x0309	[20]

Table 4.3: Attribute Identifiers

1. 'b' in this table represents a base offset as given by the LanguageBaseAttributeIDList attribute. For the primary language, 'b' must be equal to 0x0100 as described in the SDP specification.
2. Items in *italic* are tentative values in this version of the document.

4.6 PROTOCOL PARAMETERS

Protocol	Parameter mnemonic	Index
L2CAP	PSM	1
TCP or UDP	Port	1
RFCOMM	Channel	1

Table 4.4: Protocol Parameters

4.7 HOST OPERATING ENVIRONMENT IDENTIFIERS

4.7.1 ClientExecutableURL substitution strings

The operating environment identifier strings have the following format[1]:

```
<cpu_type>-<manufacturer>-[<kernel>-]<os>[<version>][-<object_format>]
```

1. It is based on a format used by the GNU AutoConfig tools

The general rule is that is that a new identifier should only be defined as required to differentiate incompatible operating environments concerning an executable file image. That is, for example different <version>-tags should not be used for compatible versions of the same operating system.

Currently defined tags:

CPU-Type ID	Description
alpha	Digital Alpha* compatible
arm	ARM* core or compatible
i86	Any Intel* 80x86-family compatible CPU
i960	Intel* i960 compatible
jvm	Java Virtual Machine*
mips	MIPS MIPS* compatible
ppc	IBM/Motorola PowerPC* compatible
sh3	Hitachi SH-3* compatible
sh4	Hitachi SH-4* compatible
sparc	Sun Sparc* compatible
Kernel ID	**Description**
chorus, linux, javaos, os9, qnx, vxworks	
<os>	An 'OS identifier' as listed below, might appear in the <kernel> field when the requested OS platform is Java based.
OS+Version-Identifiers	
amigaos, beos4.5, ejava, epocc, epoce, epocq, epocs, gnu, jre1.1, jre1.2, macos, macosx, os2, os9, palmos, pjava, pjava1.1, photon, plan9, qnx, rtjava, win95, win98, win2000, wince, winnt4	
Object Format Identifiers[1]	
aout, bout, coff, elf, jar	
Manufacturer Identifiers	
amiga*, apple*, be*, ericsson*, ibm*, intel*, lucent*, microsoft*, microware*, motorola*, nokia*, palm*, psion*, qnx*, sun*, symbian*, toshiba*, unknown[2]	

1. Only applicable when the object format is not otherwise uniquely implied by the identifier string.
2. Use when no other applies.

For Linux, the 'manufacturer' field may be used to indicate Linux distribution if so required (in which case <version> indicates the version of the distribution). Otherwise use 'unknown'.

Linux Distribution Identifiers
caldera, debian, dlx, doslinux, linuxpro, linuxware, mandrake, mklinux, redhat, slackware, stampede, suse, turbolinux, yggdrasil

Example Operating Environment Identifier Strings		
i86-microsoft-win32	ppc-apple-macos	i86-redhat-linux-gnu6
i86-microsoft-win98	m68k-apple-macos	ppc-mklinux-linux-gnu
i86-microsoft-winnt4	ppc-apple-macosx	
alpha-microsoft-winnt4	i86-apple-macosx	
i86-microsoft-win2000	m68k-amiga-amigaos	
	ppc-amiga-amigaos	
i86-be-beos4.5	jvm-sun-jre1.2	
ppc-be-beos4.5	jvm-sun-pjava1.1	
arm-symbian-epoc3	jvm-sun-ejava	
i86-unknown-linux-gnu	m68k-palm-palmos-coff	
sh3-microsoft-wince	ppc-ibm-vxworks-pjava1.2	
arm-microsoft-wince	sparc-sun-javaos-jre1.2	

4.7.2 IconURL substitution strings

The IconURL operating environment identifier strings have the following general format:

<horizontal_pixels>x<vertical_pixels>x<color_depth>[m].<file_format>

The optional tag 'm' indicates monochrome or grayscale. The host is free to try to match/request any graphics file format as indicated by a <file_format> tag, however at a minimum files conforming to the Portable Network Graphic standard [18] should be made available at the resulting URL (indicated by <file_format>=png)[2].

File format tag	Description
png	Portable Network Graphics [18]
gif	Graphics Interchange File format
bmp	Windows bitmap

Currently defined IconURL Icon format identifier strings:

Example Icon format Identifier Strings	
32x32x8.png	256 color 32 by 32 icon (or 255 colors + transparent)
16x16x8.png	
16x16x1m.png	Black and white (or monochrome + transparent)
10x10x2m.png	4 gray-scales

2. The use of PNG, and whether a subset of PNG should be required, is currently pending further investigation.

5 REFERENCES

[1] *Bluetooth Baseband Specification*, Bluetooth SIG

[2] *Bluetooth Link Manager Specification,* Bluetooth SIG

[3] *Logical Link Control and Adaptation Protocol Specification*, Bluetooth SIG

[4] *Bluetooth Service Discovery Protocol (SDP)*, Bluetooth SIG

[5] *RFCOMM with TS 07.10,* Bluetooth SIG

[6] *Bluetooth Telephony Control Specification / TCS Binary*, Bluetooth SIG

[7] *Generic Access Profile*, Bluetooth SIG

[8] *Serial Port Profile*, Bluetooth SIG

[9] *Headset Profile*, Bluetooth SIG

[10] *Cordless Telephony Profile*, Bluetooth SIG

[11] *Intercom Profile*, Bluetooth SIG

[12] *Fax Profile*, Bluetooth SIG

[13] *Dial-up Networking Profile*, Bluetooth SIG

[14] *IrDA Interoperability*, Bluetooth SIG

[15] *File Transfer Profile*, Bluetooth SIG

[16] *Object Push Profile*, Bluetooth SIG

[17] *Synchronization Profile*, Bluetooth SIG

[18] *Portable Network Graphics (PNG),* http://www.w3.org/Graphics/PNG

[19] *UUIDs and GUIDs*, P. J. Leach et al, http://www.ietf.org/internet-drafts/draft-leach-uuids-guids-01.txt

[20] *Interoperability Requirements for Bluetooth as a WAP*, Bluetooth SIG

6 TERMS AND ABBREVIATIONS

LMP	Link Management Protocol
L2CA	Logical Link Control and Adaptation, protocol multiplexer layer for Bluetooth
MTU	Maximum Transmission Unit
SAP	Service Access Points
Baseband	Baseband Protocol
Service Discovery	The ability to discover the capability of connecting devices or hosts.
PnP	Plug and Play
SAR	Segmentation and Reassembly
IP	Internet Protocol
IrDA	InfraRed Data Association
PPP	Point-to-Point Protocol
IETF	Internet Engineering Task Force
RFC	Request For Comments

7 LIST OF FIGURES

Figure 1.1: General format of Class of Device/Service 4
Figure 1.2: The Class of Device/Service field (format type 1) 5

8 LIST OF TABLES

Table 1.1: The Inquiry Access Codes 4
Table 1.2: Major Service Classes 5
Table 1.3: Major Device Classes 6
Table 1.4: Sub Device Class field for the 'Computer' Major Class 7
Table 1.5: Sub Device Classes for the 'Phone' Major Class 7
Table 1.6: The LAN Access Point Load Factor field 8
Table 1.7: Reserved sub-field for the LAN Access Point 8
Table 1.8: Sub Device Classes for the 'Audio' Major Class 9
Table 2.1: The LMP Version Parameter Values 10
Table 2.2: The LMP_CompId parameter codes 10
Table 3.1: Pre-defined L2CAP Channel Identifiers 11
Table 3.2: Assigned Protocol and Service Multiplexor values (PSM) 11
Table 4.1: Protocol Universally Unique Identifiers and Names 13
Table 4.2: Service Class Identifiers and Names 14
Table 4.3: Attribute Identifiers 15
Table 4.4: Protocol Parameters 16

REVISION HISTORY

Rev	Date	Comments
1.0 draft	July 5th 1999	• Renamed some of the service class mnemonics. Added a bit to indicate if a node is in Limited Discoverable Mode (useful in a reply to GIAC). • Updated after review. Added the IAC LAP codes. • Minor editoral and clarifications, including section "Universally Unique Identifier (UUID) short forms".
1.0B	Dec 1st 1999	• Revised from a linguistic point of view. • Errata items previously published on the web has been included. These corrections and clarifications are marked with correction bars.
1.1	Dec 1st 2000	*In order to keep this section more up-to-date, it has been removed from the Core Specification and is now a separate "living" document available on the member website.* • Errata items previously published on the web have been included. These corrections and clarifications are marked with correction bars.

CONTRIBUTERS

Johannes Elg (owner)	Ericsson Mobile Communications AB
Numerous SIG members contributed directly or indirectly to this revision	