Redes Inalámbricas

Carlos Varela
Luis Domínguez
Escuela Técnica Superior de Ingeniería Informática
Universidad de Valladolid
2002

Contexto de las Wireless LAN

Antes de comenzar con las redes inalámbricas deberemos plantearnos en qué contexto aparecen este tipo de redes y por qué, analizar sus características, sus ventajas y sus inconvenientes para determinados supuestos. En esta primera parte veremos los siguientes aspectos de estas redes:

- Ventajas de las WLAN
- Inconvenientes de las WLAN
- IrDA vs. RF
- Tecnologías de las Redes Inalámbricas

Ventajas de las Redes Inalámbricas

- Flexibilidad

  Dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados por el mundo Por ejemplo, para hacer esta presentación se podría haber colgado la presentación de la web y haber traído simplemente el portátil y abrirla desde Internet incluso aunque la oficina en la que estuviésemos no tuviese rosetas de acceso a la red cableada.

- Poca planificación

  Con respecto a las redes cableadas. Antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas, mientras que con una red inalámbrica sólo nos tenemos que preocupar de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red.

- Diseño

  Los receptores son bastante pequeños y pueden integrarse dentro de un dispositivo y llevarlo en un bolsillo, etc.

- Robustez

  Ante eventos inesperados que pueden ir desde un usuario que se tropieza con un cable o lo desenchufa, hasta un pequeño terremoto o algo similar. Una red cableada podría llegar a quedar completamente inutilizada, mientras que una red inalámbrica puede aguantar bastante mejor este tipo de percances inesperados

Inconvenientes de las Redes Inalámbricas

- Calidad de Servicio

  Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 10 Mbps, frente a los 100 que puede alcanzar una red normal y corriente. Por otra parte hay que tener en cuenta también la tasa de error debida a las interferencias. Esta se puede situar alrededor de 10^{-4} frente a las 10^{-10} de las redes cableadas. Esto significa que has 6 órdenes de magnitud de diferencia y eso es mucho. Estamos hablando de 1 bit erróneo cada 10.000 bits o lo que es lo mismo, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo. Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.

- Coste

  Aunque cada vez se está abaratando bastante aún sale bastante más caro. Recientemente en una revista comentaban que puede llegar a salir más barato montar una red inalámbrica de 4 ordenadores que una cableada si tenemos en cuenta costes de cablear una casa. El ejemplo era para una casa, aunque, todo hay que decirlo, estaba un poco forzado. Aún no merece la pena debido a la poca calidad de servicio, falta de estandarización y coste.

- Soluciones Propietarias

  Como la estandarización está siendo bastante lenta, ciertos fabricantes han sacado al mercado algunas soluciones propietarias que sólo funcionan en un entorno homogéneo y por lo tanto estando atado a ese fabricante. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del sistema como para la recuperación ante posibles fallos. Cualquier empresa o particular que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de enlace, etc.

- Restricciones

  Estas redes operan en un trozo del espectro radioeléctrico. Éste está muy saturado hoy día y las redes deben amoldarse a las reglas que existan dentro de cada país. Concretamente en España, así como en Francia y en Japón, existen un limitaciones en el ancho de banda a utilizar por parte de ciertos estándares.

- Seguridad

  En dos vertientes:

  - Por una parte seguridad e integridad de la información que se transmite. Este campo está bastante criticado en casi todos los estándares actuales, que, según dicen no se deben utilizar en entornos críticos cuyos en los cuales un "robo" de datos pueda ser peligroso.
  - Por otra parte este tipo de comunicación podría interferir con otras redes de comunicación (policía, bomberos, hospitales, etc.) y esto hay que tenerlo en cuenta en el diseño.

IrDA vs. RF (I)

- Infrarrojos:
  - Ventajas:
    - Emisores y receptores muy simples y baratos
    - No interfiere con otros disposivos de RF
  - Desventajas:
    - Poco Ancho de Banda
    - Necesidad de comunicación "visual"

      Esta es una desventaja importante. Por ejemplo, no se podría comunicar un pc en una sala con una impresora que esté en otra sala. Esto limita mucho las posibilidades de comunicación entre dispositivos y da un aspecto de comunicación "de juguete".
    - Habitualmente comunicaciones sólo entre 2 interlocutores

IrDA vs. RF (II)

- RadioFrecuencia
  - Ventajas:
    - Mayor área de cobertura
    - No necesita comunicación "visual" entre dispositivos
    - Mayor Ancho de Banda
  - Desventajas:

- Difícil de apantallar -> Interferencias

  No solo interferencias entre diferentes dispositivos conectados a una red, sino también entre otro tipo de dispositivos independientes que generen campos electromagnéticos, por ejemplo, microondas.

- Rango de frecuencias limitado

  Hoy día, el espectro radioeléctrico está ocupado casi al 100% así que se buscan huecos, pero como la gestión del espacio radioeléctrico es distinta en cada país, nos encontramos ante dificultades en la estandarización del espacio radioeléctrico a utilizar en una determinada tecnología.

Tecnologías de las Redes Inalámbricas

Hay múltiples tecnologías en el mercado:

- IEEE 802.11x (Wireless LAN, Wi-Fi)
- Bluetooth
- Hiperlan
- Soluciones propietarias
- Protocolos: WAP, Mobile IP, Mobile TCP

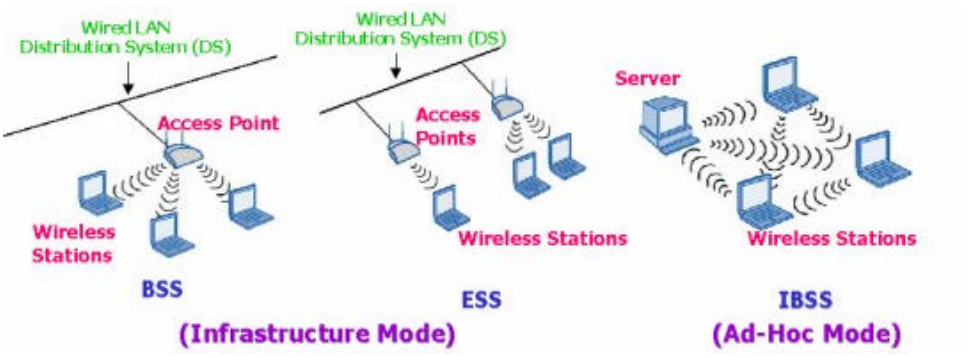
IEEE 802.11x

IEEE 802.11 comprende varios estándares:

- Definen la subcapa MAC y la física
- No son compatibles entre sí, algunos ni siquiera con ellos mismos
- Los hay de transmisión: 802.11 original (1997), 802.11b, 802.11a y 802.11g
- Extensiones al estándar 802.11a: 802.11h y 802.11i
- 802.11e, extensión para Calidad de Servicio (QoS)

Modos de operación

Hay dos modos de operación, uno ad-hoc, en el que las estaciones se comunican entre sí directamente, y otro de Infraestructura, en el que las estaciones acceden a la red a través de uno o varios puntos de acceso.



Comparación

Estándar	Tasa de transferencia	Banda de frecuencia	Precio tarjeta	Precio P. Acceso
802.11	2 Mbit/s	2.4 GHz	N/D	N/D
802.11b	11 Mbit/s	2.4 GHz	100 €	200 €
802.11a	54 Mbit/s	5 GHz	150 €	300 €
802.11g	54 Mbit/s	2.4 GHz	N/D	N/D

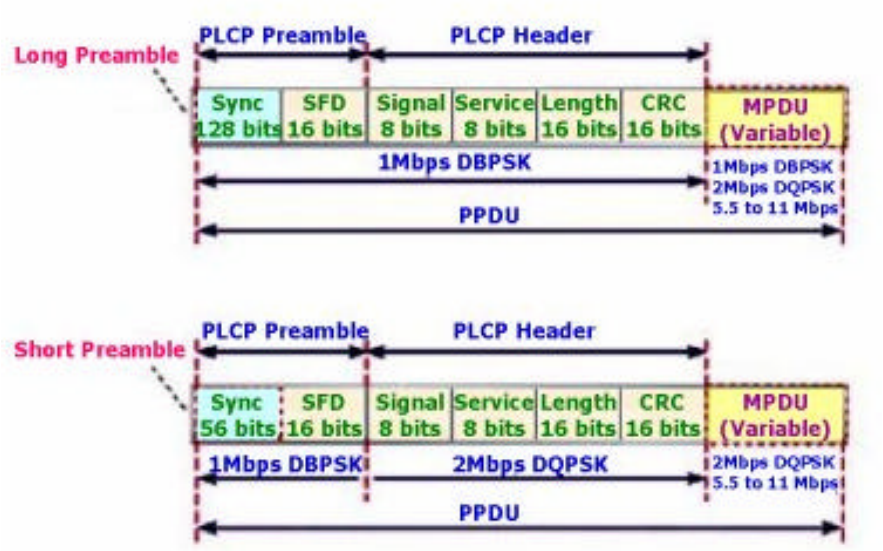
802.11

- Estándar de la IEEE, 1997
- Hasta 2Mbit/s
- 3 Especificaciones de capas físicas: 2 para radio, en la banda de los 2,4GHz y una para infrarrojos. De éstas, la de infrarrojos nunca fue implementada, y una de las de radio fue el embrión de 802.11b
- Obsoleto, pero todavía compatible con 802.11b.

802.11b

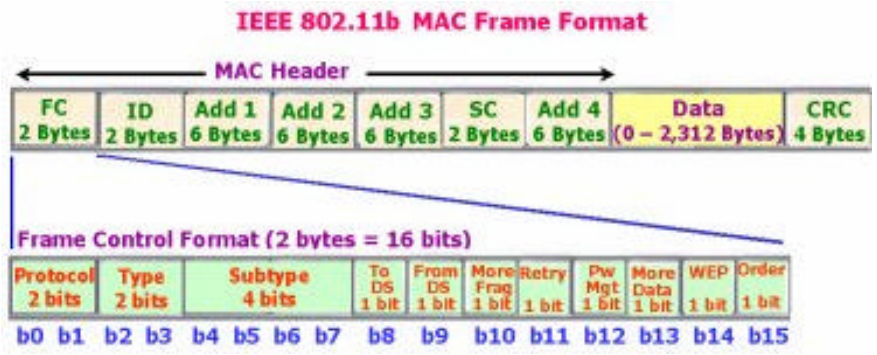
- Es el estándar más utilizado
- Se supone que alcanza 11Mbit/s, pero una tasa de transferencia más real es de unos 4Mbit/s, incluso menos, dependiendo del entorno y la distancia al punto de acceso
- CSMA/CA (Sense Multiple Access with Collision Avoidance) o RTS/CTS (Request to Send/Clear to Send), 4-Way Handshake
- Alcance de 30m en interiores

Trama Física



Preámbulo Largo: implementación obligatoria, trama normal
Preámbulo Corto: implementación optativa, para transmisión de vídeo y voz sobre IP

Trama MAC



Formato de Trama

- Frame Control (FC): versión de protocolo y tipo de trama (gestión, datos, control).
- Duration/ID (ID)
- Station ID se usa para el tipo de trama “Power-Save poll message“
- El valor de duración se usa para el cálculo del vector de reserve de red (Network Allocation Vector)
- Address fields (1-4) contienen hasta cuatro direcciones (origen, destino,

transmisión, recepción), dependiendo del campo de control de trama (bits ToDS y FromDS)

- La secuencia de control consiste en un número de fragmento y un número de trama. Se usa para representar el orden de diferentes fragmentos pertenecientes a la misma trama, y para distinguir una posible duplicación de paquetes.
- Data: la información transmitida o recibida
- CRC: campo de Control de Redundancia cíclica de 32 bits.

Formato de Control de Trama (Frame Control Format)

- Versión del Protocolo (Protocol Version) indica la versión del estándar IEEE 802.11.
- Tipo (Type) : Gestión, Control, Datos
- Subtipo (Subtype): RTS, CTS, ACK etc
- To DS se pone a 1 cuando la trama se manda a un sistema de distribución (DS)
- From DS se pone a 1 cuando la trama se recibe de un sistema de distribución (DS)
- More Fragment se pone a 1 cuando hay más fragmentos después de éste pertenecientes a la misma trama.
- Retry indica que este fragmento es una retransmisión de un fragmento previamente enviado. (Para que el receptor reconozca la transmisión duplicada de tramas)
- Power Management indica el modo de gestión de energía en el que la estación estará después de la transmisión de la trama.
- More Data indica que hay más tramas en cola hacia esta estación.
- WEP indica que el cuerpo de la trama está encriptado de acuerdo con el algoritmo WEP (wired equivalent privacy).
- Order indica que la trama se está enviando usando la clase de servicio “Estrictamente ordenado”.

802.11a

- Estándar, pero no necesariamente interoperable
- La Wireless Ethernet Compatibility Alliance (WECA) es la organización encargada de la normalización de los diferentes dispositivos que salen al mercado, de acuerdo con la especificación Wi-Fi5

- No cumple la normativa europea, al respecto de control de potencia y gestión del espectro de frecuencias
- Utiliza CSMA-CA
- Alcance a 54Mbit/s: 10 metros
- Corrección de Errores: Forward Error Correction (FEC)

802.11g

- Estándar todavía en desarrollo
- Supuestamente compatible hacia atrás con 802.11b, pero esto todavía no está garantizado
- Alto consumo

Seguridad

- Encriptación WEP (Wired Equivalence Privacy), basado en RC4
- Inseguro: periódicamente genera paquetes “débiles”, que pueden ser aprovechados para reconstruir la clave, y acceder a la red.
- Más de la mitad de las redes no lo usan
- A veces se trata como red segura (interna), cuando por definición es insegura y debería ponerse delante del firewall, y no detrás con el resto de la LAN.

Seguridad - 802.11i

Estándar adicional, todavía en desarrollo, con dos vertientes:

- Temporal Key Integrity Protocol
  - Es un RC4 reparado
  - Genera claves nuevas cada 10 Kbytes
  - Aplicable a equipamiento actual
- AES
  - Más robusto
  - No aplicable a equipamiento actual

802.11h - Para la UE

- Desarrollado por exigencia de la Unión Europea para la autorización de operación del estándar 802.11a
- Dynamic Frequency Selection, para gestión del espectro
- Transmit Power Control, para control de potencia de transmisión
- Desarrollado para desbancar a HiperLAN2, estándar impulsado por la UE

Enlaces

- www.80211-planet.com
- http://www.proxim.com/learn/library/whitepapers/wp2001-09-highspeed.html
- Seguridad :
  - http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
  - http://www.linuxsecurity.com/feature_stories/wireless-kismet.html

Bluetooth

- WPAN (Wireless Personal Area Networks), ad hoc piconets.

Podemos decir que ya no hablamos de una comunicación de algunos dispositivos con el mundo, sino que nos restringimos a un entorno reducido en el que pequeños dispositivos se comunican entre sí. Podemos estar hablando de un portatil, un reproductor mp3, una agenda electrónica, etc. comunicándose entre sí en un momento dado. Las nomenclaturas WPAN y ad hoc piconet (sobre todo esta segunda nomenclatura, ad hoc piconet o simplemente piconet) son muy utilizadas dentro del entorno Bluetooth. El término piconet concretamente se refiere a redes de área local con pequeña cobertura y sin infraestructura.

- Bluetooth es una ”Especificación abierta de una tecnología inalámbrica para redes basadas en radiofrecuencia, de bajo coste y con un único chip”.

  En 1994 Ericsson comienza unos estudios sobre la posibilidad de implementar pequeñas redes inalámbricas. Ericsson quería convertir Bluetooth en un estándar mundial, para ello inició contactos con diversas empresas. En primavera de 1998, cinco compañías (Ericsson, Intel, IBM, Nokia y Toshiba) forma el Bluetooth Consortium. Por lo tanto, no es un estándar apoyado por organismos de estandarización, pero que se prevé que se convierta en un estándar de facto.

  Bajo coste: El chip Bluetooth cuesta aprox. $5. Aunque suponemos que ese será el coste de fabricación, puesto que los dispositivos Bluetooth son bastante caros.

  Hoy en día existe el llamado SIG (Bluetooth Special Interest Group), que conforman más de 1600 compañías. Esto significa que, aunque se pregona como un estándar abierto, es necesario pertenecer a este grupo para poder fabricar dispositivos bluetooth.

Características

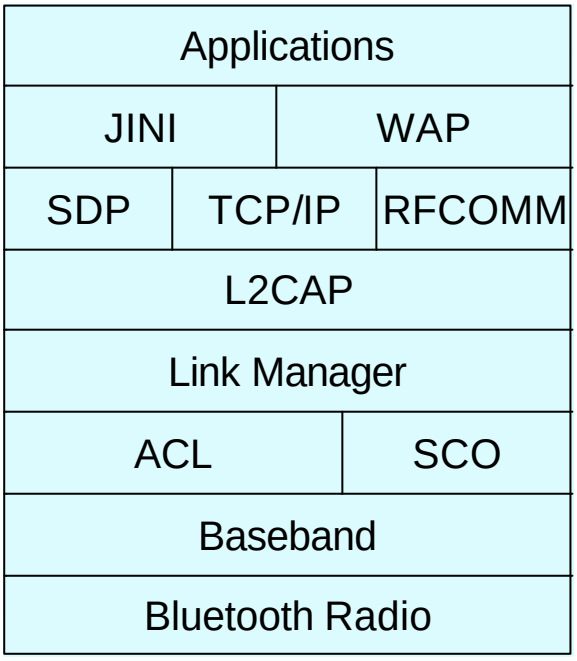
- Rango de 10 a 100 metros

Rango dependiendo de la potencia de la antena, aunque intentar comunicar dispositivos a una distancia de más de 10 metros es arriesgarse mucho, sobre todo en entornos algo críticos.

- Posibles conexiones

- 1 canal asíncrono (máx 732 + 57.6 Kbps)
  Fundamentalmente utilizado para transmisión de datos.
- 3 canales síncronos (3 x (64 x 2) Kbps)
  Fundamentalmente utilizado para servicios que requieran calidad, sobre todo para servicios de voz.
- Una combinación de canal síncrono y asíncrono (Formato de paquete DV)
  Formato de paquete DV: Cada paquete tiene una parte de voz que no lleva corrección de errores y una de datos que sí que lleva (FEC: Forward Error Correction)

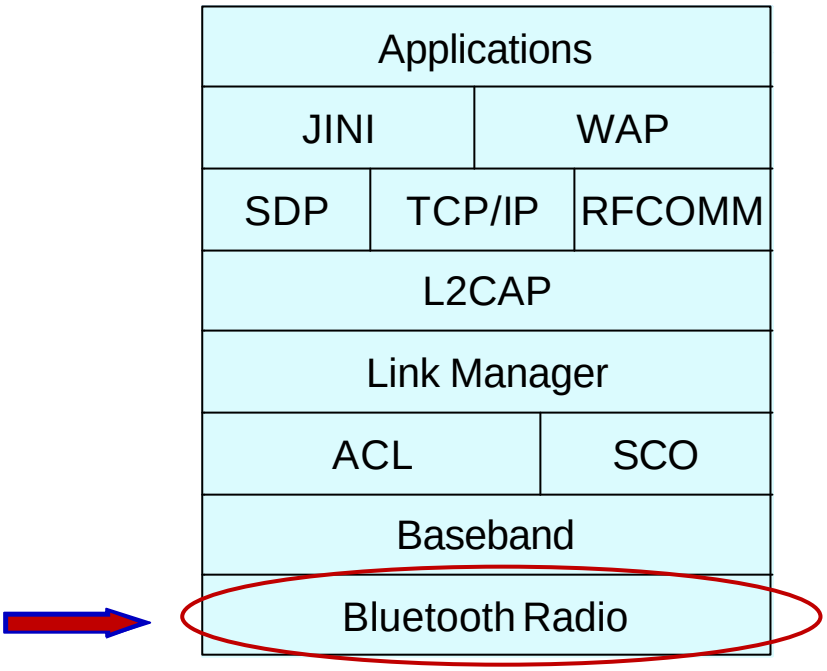
Niveles de Bluetooth



Acrónimos:
JINI: (*"Jini Is Not Initials"*) - No son iniciales - www.jini.org <http://www.jini.org>
WAP: Wireless Application Protocol
L2CAP: Logical Link Control and Adaptation Protocol
SDP: Service Discovery Protocol - Protocolo que sirve para *identificar* qué *servicios* están activos en otros dispositivos dentro de la *piconet*.
RFCOMM: Protocolo que proporciona una *emulación de puertos serie* sobre el protocolo L2CAP
ACL: Asynchronous Connection-Less

SCO: Synchronous Connection-Oriented

Bluetooth Radio

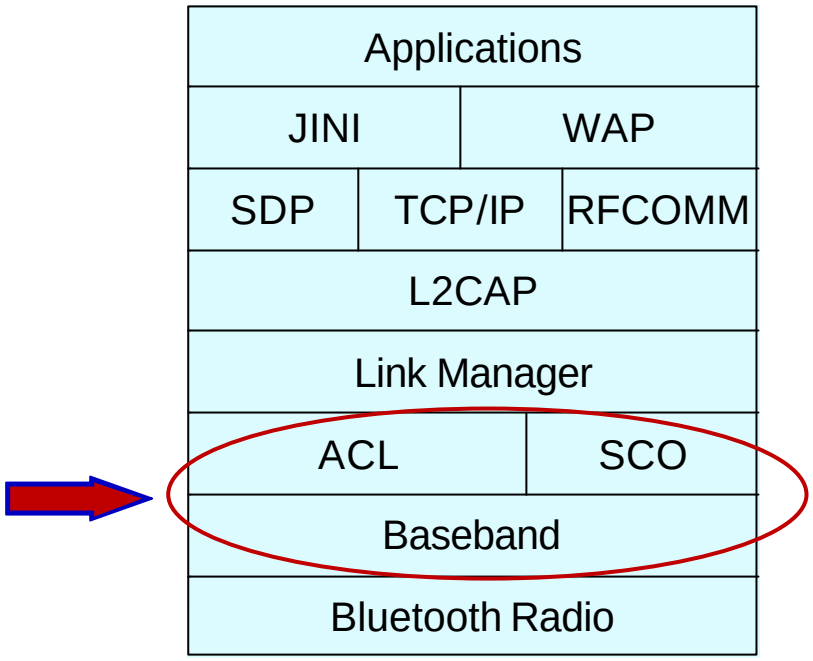


- Banda de los 2.4 GHz.

  Es la que se encarga físicamente de enviar y transmitir la información. Emite y recibe las señales eléctricas al resto de dispositivos bluetooth de la piconet.

  Francia, como curiosidad, estuvo a punto de quedarse sin la posibilidad de utilizar Bluetooth debido a que la banda de los 2.4 GHz. La utiliza el ejército francés para sus comunicaciones de radio.

Baseband (I)



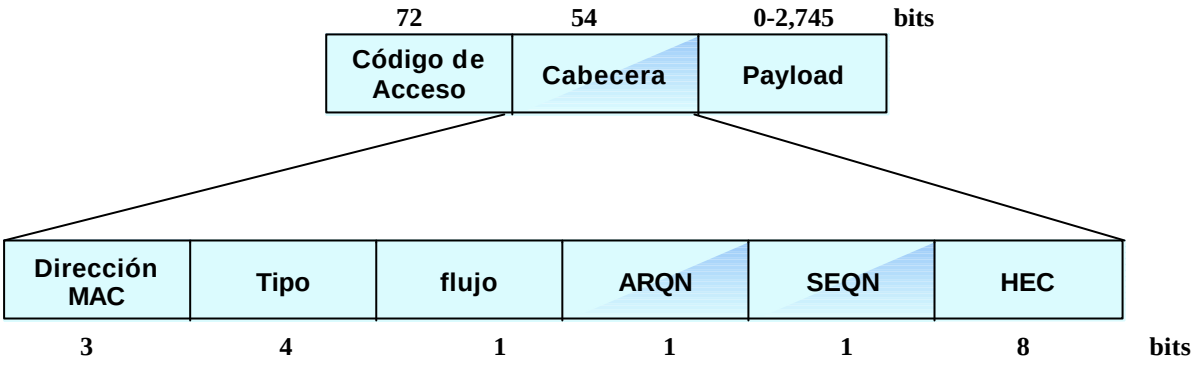
Es el nivel físico de Bluetooth.

- Uno de los dispositivos como maestro y el resto (hasta 7) como esclavos.
  - En Bluetooth se considera:
  - 2 Dispositivos compartiendo el mismo canal: Una Piconet
  - Varias piconets con algún nodo en común: Una red de dispersión (scatternet)

- Esquema de Sondeo - Selección
- Servicios:
  - Orientados a conexión (Síncronos): SCO
  - No orientados a conexión (Asíncronos): ACL

Baseband (II)

- Formato de paquete:



El codigo de acceso contiene secuencias de bits de sincronización e información sobre el control del enlace. La cabecera contien datos de control y el campo payload contiene los datos útiles además de un campo de CRC de 16 bits generado por el polinomio CRC-CCITT 210041 (octal).

La dirección de control de acceso al medio se codifica con 3 bits. En realidad se pueden conectar hasta 7 dispositivos a una piconet.

El segundo campo nos permite diferenciar entre 16 tipos de paquetes.

1 bit de control de flujo para enlaces ACL.

1 bit de confirmación de paquete recibido

1 bit para el orden de secuencia

8 bits de control de error de cabecera (Header Error Check)

- Cabecera codificada con 1/3 FEC (Forward Error Correction)

Esto significa que para codificar cada bit de la cabecera se utilizan 3 bits. Esto explica que los 18 bits del formato de la cabecera se codifiquen con 54 bits.

Link Manager

- Gestiona la configuración, el mantenimiento y la seguridad del enlace
- Proporciona servicios de autenticación, encriptación, control de energía y gestiona servicios con QoS

L2CAP

- Logical Link Control and Adaptation Layer Protocol
- Proporciona servicios con y sin conexión a los protocolos de la capa superior
- Entre otras cosas se encarga de la segmentación y reensamblado de paquetes de hasta 64KB

Seguridad (I)

La seguridad en Bluetooth es un tema bastante farragoso y, por lo que cuentan en páginas un tanto especializadas, una importante fuente de quebraderos de cabeza.

- Objetivo "Jugoso"

Los datos transmitidos por los dispositivos bluetooth son, en general, objetivos claros para posibles "espías". Esto se debe a que muchos de estos dispositivos tienen la característica de ser del tipo "agendas personales" en los que se almacena informaciones del tipo citas, contraseñas, teléfonos, direcciones... en definitiva cosas que son susceptibles de ser espiadas.
A esto debemos añadir el hecho de que utiliza radiofrecuencia, con lo que no podemos limitar el alcance de la señal y puede haber un posible "atacante" escuchando las señales emitidas por estos dispositivos.

- Técnicas incluidas en el chip
  - Autenticación mediante desafío - respuesta
  - Cifrado del flujo
  - Una clave distinta en cada sesión
- Seguridad opcional en capas superiores

Seguridad (II)

- Existen 3 posibles niveles de seguridad:
  - Modo de Seguridad 1: Sin seguridad

Es un modo NO seguro. No se realiza absolutamente ninguna tarea de seguridad

  - Modo de Seguridad 2: *Service Level Enforced Security*

Comienza a utilizar las características de seguridad en las capas más altas. Son las aplicaciones quienes deciden si quieren utilizar las características de seguridad que ofrece el protocolo.

  - Modo de Seguridad 3:*Link Level Enforced Security*

El propio protocolo establece la seguridad del sistema antes de establecer el

canal de comunicaciones y por lo tanto toda la comunicación desde ahí va cifrada. Es el nivel de mayor seguridad.

Productos

Los productos bluetooth no brillan precisamente por su asequibilidad. En principio, y aunque la tecnología ya lleva muchos años de investigación, los primeros productos comerciales “de usuario” Bluetooth se están poniendo a la venta ahora, con lo cual es posible que los precios se abaraten en un periodo no muy grande de tiempo. Los precios que damos a continuación son aproximaciones que dependen de la calidad del producto que se quiera adquirir, pero que pueden servir para darnos una idea de cómo está el mercado.

- Impresoras (400€)
- Puentes bluetooth - 802.11b (2000€)
- Manos libres móvil (250 €)
- Tarjeta de expansión para Palm (150€)
- ...

Bibliografía

- Jochen Schiller, “Mobile Communications”, Addison-Wesley
- <http://www.palowireless.com/>
- <http://www.80211-planet.com/>
- <http://www.wirelessdevnet.com/>
- <http://bluetooth.weblogs.com/>