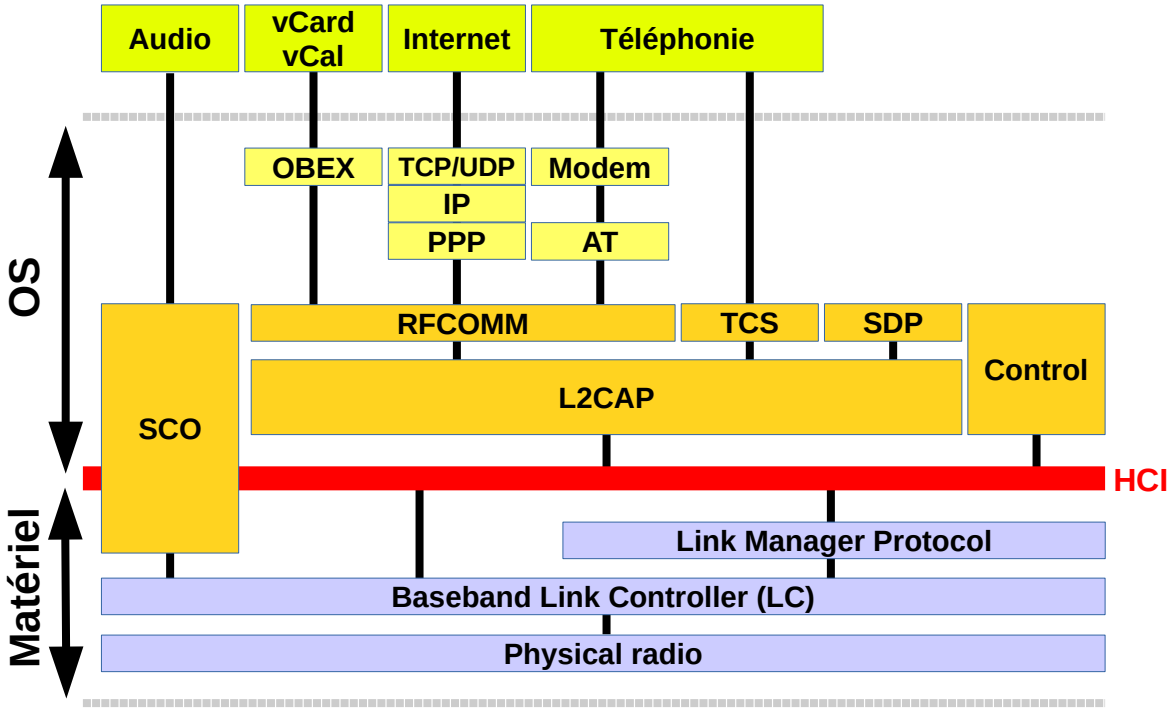
Cours Bluetooth®

Introduction



IEEE 802.15.1
Bluetooth WPAN

- OBEX : OBject EXchange – permet d'échanger des fichiers entre périphériques BT.
- RFCOMM : port série RS232 sur la couche L2CAP (utilisable par des programmes de haut niveau comme pppd, ...).
- TCS : Telephony Control Protocol Specification.
- SDP : Service Discovery Protocol – permet de découvrir les services disponibles sur un périphérique BT.
- HCI : Host Controller Interface – fournit une API universelle, indépendante du matériel.
- SCO : Synchronous Connection Oriented - port orienté audio
- L2CAP : Logical Link Control & Adaptation Protocol – segmente/réassemble les paquets, gère la QoS, multiplexe les données.
- Link Manager : gestionnaire de liaisons – authentifie, associe (appairage), gère les clés et le chiffrement, ainsi que les canaux L2CAP pour le transport des données.

Les profils (ou services)

Les profils BT peuvent être comparés à des services, disponibles sous la forme de couches logicielles standardisées pour un usage donné.

On ne peut utiliser un profil BT que s'il est présent sur les deux appareils. Exemple : pour utiliser une oreillette BT, il faut et il suffit que les deux appareils soient compatibles avec le profil HS (Head Set).

Le tableau plus loin vous présente une liste non exhaustive de profils BT.

On désigne par « **pile Bluetooth** » (ou « stack ») l'ensemble des programmes de base prenant en charge la norme côté système d'exploitation.

Sur les appareils évolutifs (ordinateurs, smartphones, ...), les piles BT sont mises à jour régulièrement via le système d'exploitation. Toutefois, la prise en charge des périphériques BT varie grandement d'un OS à un autre, voire entre versions d'un même OS. Il convient donc de bien se renseigner sur la compatibilité matériel/OS avant tout achat.

Sur d'autres appareils à usage unique (casques, enceintes, ...), ces piles sont statiques et n'ont aucun raison d'être mises à jour.

Globalement, la **modularité et l'évolutivité du BT restent toutes relatives**, car dépendantes du matériel utilisé, du logiciel utilisé, mais aussi du Bluetooth SIG (Special Interest Group), l'organisme chargé de sa normalisation.

Il existe en effet des profils BT spécifiques à des fabricants de matériels, donc inexploitables sur des appareils tiers, ou exploitables en mode dégradé, comme par exemple un casque hi-fi qui ne donnera son plein potentiel qu'avec la clé BT du fabricant, et donnera un résultat sonore potable mais minimaliste avec toute autre clé.

À noter enfin que contrairement à la croyance populaire, **le BT n'est pas une technologie dédiée uniquement aux réseaux sans-fil** : le principe des profils BT est également utilisé dans des périphériques USB et infrarouges.

Les normes (historique)

1998	1.0	
1999	1.0b	premier téléphone BT
	1.1	correction de bugs + ajout de l'information de la puissance du signal (RSSI ou Received Signal Strength Indication).
	1.2	plus grande résistance aux interférences grâce au AFH (Adaptive Frequency Hopping) ou saut de fréquences adaptatif (on ignore les canaux déjà en cours d'utilisation).
2004	2.0 + EDR	Enhanced Data Rate - vitesse multipliée par 3. Apparition de la qualité audio CD en profil A2DP.
	2.1 + EDR	amélioration de l'appairage
2009	3.0 + HS	High-Speed – utilise l'EDR pour initialiser la connection,

		puis passage en 802.11 (donc en WiFi classique) pour le transfert des données en 24Mbit/s.
2010	4.0 + BLE	Bluetooth Low Energy
2013	4.1	Connexion d'appareils multiples sur un seul accès.
	4.2	Protocole IP sécurisé pour les objets connectés.
2016	5.x	Débit jusqu'à 2,1 Mbits/s - consommation d'énergie inchangée - rayon d'action étendu.

Classe des périphériques

Classe	Puissance	Portée
1	100 mW	100 mètres
2	2,5 mW	10 à 20 mètres
3	1 mW	Quelques mètres

Les liaisons BT

Le Bluetooth travaille sur 79 fréquences, par pas de 1 MHz, dans la bande ISM et fonctionne par sauts de fréquences (1600 sauts/s, soit un saut toutes les 625 µs).

Les liaisons BT peuvent se faire en :

- **mode synchrone** : En BT1, la vitesse de base est 432 kbits/s en bidirectionnel avec renvoi des données en cas d'erreur. À partir du BT2, en EDR (Enhanced Data Rate), le débit est triplé, si les deux appareils sont compatibles (soit 1 296 kbits/s).
- **mode asynchrone** : En BT1, le débit est de 721 kbits/s en descendant et 57,6 kbits/s en montant avec renvoi des paquets en cas d'erreur. À partir du BT2, en EDR (Enhanced Data Rate), le débit est triplé, si les deux appareils sont compatibles (soit 2163 kbits/s).

SCO (Synchronous Connection Oriented)

À noter l'existence du mode spécialisé **SCO** qui propose jusqu'à 3 canaux synchrones 64 kbits/s en montant et descendant, sans renvoi de paquets en cas d'erreur (comme l'UDP classique). Le son monocanal est coupé à 8 kHz (voix humaine) et utilise un codage de type CVSDM (Continuously Variable Slope Delta Modulation) non compressé.

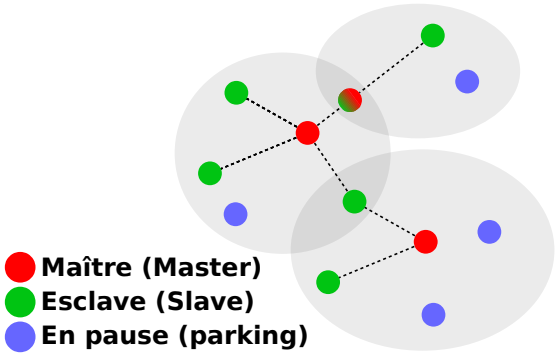
Dédié aux profils HS (oreillette) et HF (main libres), la qualité offerte est optimisée pour une conversation téléphonique, et ne sied pas à l'écoute de musique stéréo.

Pour ce dernier usage, c'est le profil A2DP (Advanced Audio Distribution Profile) qu'il faut utiliser, lequel se décompose en A2SNK (réception HiFi) et A2SRC (émission HiFi).

L'A2DP travaille par défaut en codec SBC (Sub Band Codec, imposé par la norme), mais autorise également d'autres codecs ,dont le très répandu MP3.

Les deux topologies de base

Piconet : réseau de 2 à 8 appareils BT avec un périphérique maître (le PC en général) et 1 à 7 esclaves (casque, téléphone portable, imprimante, ...). Le périphérique maître joue le rôle de concentrateur. Les périphériques esclaves voulant communiquer entre eux doivent passer par le maître.



Scatternet : réseau formé de plusieurs piconets indépendants. Un appareil (maître ou esclave) d'un premier piconet devient esclave d'un autre piconet. et devient donc la passerelle entre les deux piconets. On lève donc la limitation des 8 appareils.

Sécurité

Le BT utilise des adresses sur 2x24bits (BD-ADDR = Bluetooth Device ADDRess), les 24 premiers bits identifiant le fabricant. Comme pour les adresses MAC, il existe des logiciels dédiés permettant de forger une adresse bidon.

Le **GAP** (Generic Access Profile) de base définit trois modes de sécurité :

- **mode 1** : pas de cryptage ni d'authentification : l'appareil accepte toutes les connexions entrantes.
- **mode 2** : sécurisation au niveau applicatif (L2CAP) après établissement du canal de communication : chaque service peut ainsi être protégé de manière différente.
- **mode 3** : sécurisation au niveau de la liaison (LMP) avant établissement du canal de communication : quel que soit le service visé, il faut d'abord montrer « patte blanche ».

L'usager gère également la confiance (options **trust/untrust**) entre son appareil et les périphériques BT alentours qui viennent s'y connecter. S'il choisit de faire confiance à un appareil tiers, ce dernier aura accès à tous les services disponibles.

Au niveau service justement, on trouve encore trois niveaux de sécurité :

- **niveau 1** : nécessite une autorisation + une authentification. L'autorisation est automatique pour les périphériques de confiance, sinon l'usager doit donner manuellement l'autorisation d'accès à son appareil. L'authentification se fait par challenge/réponse entre appareils, en mono ou bi-directionnel.
- **niveau 2** : n'utilise que l'authentification
- **niveau 3** : l'accès au service est public, sans autorisation ni authentification.

Le jumelage entre appareils permet la création d'une clé de chiffrement commune, en utilisant les BD-ADDR, des nombres aléatoires, un code PIN (4 chiffres en général) statique ou dynamique, ou un mot de passe plus long. Par code PIN statique, on entend ici que certains appareils ne possèdent pas de clavier pour rentrer un code. Dès lors, ce code est enregistré en « dur » et non modifiable. On retrouve ainsi fréquemment les codes 0000 ou 1234 par défaut, ce qui n'est évidemment pas très sécurisé.

La clé de chiffrement, comme son nom l'indique, sert au chiffrement des données entre appareils jumelés.

Au final, la sécurité en BT restant sujette à caution, il est fortement conseillé :

- **de n'activer le BT qu'en cas de besoin** (donc le désactiver par défaut)
- **de cacher son équipement** (désactivation du mode découverte dans les réglages de l'appareil)
- **de rejeter immédiatement toute sollicitation inconnue**

Quelques états

- **Standby** : état par défaut quand le périphérique n'est pas connecté.
- Initialisation des connexions :
  - **Inquiry** (=demande/enquête/interrogation) : découverte active du réseau.
  - **Inquiry scan** : dispositif se mettant en écoute des messages de type **Inquiry**.
  - **Page** : connexion à un dispositif BT (nécessite de connaître l'adresse cible).
  - **Page scan** : dispositif en écoute des message de type **Page**.
- Quand un dispositif est connecté :
  - **Actif** : maître et esclave communiquent entre eux.
  - **Suspendu** : l'esclave se met en attente et ne peut plus recevoir que des messages de type SCO.
  - **Parqué** : l'esclave n'assure plus qu'une synchronisation minimale avec le maître, et se réveille à intervalles réguliers pour maintenir sa présence.
  - **Sniff** : le périphérique est en mode écoute, et alterne entre activité et économie d'énergie.

Profils BT

Le tableau suivant donne une liste de quelques profils BT qui peuvent être supportés (ou pas…) par votre PC et/ou votre smartphone. La liste n'est donc pas exhaustive.

Vous pourrez utiliser les colonnes Ordinateur/Smartphone pour y repérer les profils réellement supportés par vos appareils, en repérant l'UUID et le canal du service BT.

Profil / Rôles BT	*Désignation*	*Ordinateur*	*Smartphone*
A2SNK	**Advanded Audio Distribution – Sink (récepteur stéréo Hifi)**		
A2SRC	**Advanded Audio Distribution – Source (émetteur stéréo Hifi)**		
ACTIVESYNC	ActiveSync		
APPLE	Apple attribute		
AVRCT	Audio Video Remote Control (télécommande)		
AVRTG	Audio Video Remote Target (périphérique commandé)		
BIP	Basic Image Profile (pour envoyer, recevoir, imprimer des images ou contrôler des appareils orientés image).		
BPP	Basic Printing Profile (pour l'impression depuis un smartphone ou un PDA)		
CIP	CIP		
CTP	Cordless Telephony (passerelle de téléphone BT à réseau commuté)		
DID	DID		
DUN	Dial-Up Networking (commandes modem AT sur port série SPP)		
FAX	Fax		
FTP	**File Transfert (transfert de fichiers via OBEX)**		
GAP	**Generic Access – profil par défaut du BT qui contrôle la connexion du périphérique en unicast/broadcast**	**toujours présent par défaut**	**toujours présent par défaut**
GATT	**Generic ATTribute – profil par défaut du BT appelé après le GAP (une fois la connexion établie), pour contrôler comment sont empaquetées et envoyées les données en mode client / serveur.**	**toujours présent par défaut**	**toujours présent par défaut**
GN	GN		
HCRP	Hard Copy Cable Replacement (émulation port parallèle IEEE1284 pour l'impression depuis un PC par exemple)		
HF	**Hands-Free** (dédié automobile, permet le main-libre + le contrôle via des commandes AT : décrocher, raccrocher, rappeler, contrôler le volume, etc)		
HFAG	Hands-Free Audio Gateway		
HID	**Human Interface Device (clavier, souris, manettes, ...)**		
HOTSYNC	HotSync		
HS	**Headset** (oreillette)		

Profil / Rôles BT	*Désignation*	*Ordinateur*	*Smartphone*
HSAG	HSAG		
ISYNC	Apple iSync		
KEYB	HID keyboard		
LAN	LAN Access (PPP over SPP) - (remplacé par PAN)		
NAP	NAP		
NFTP	NFTP		
NGAGE	NGAGE		
NOKID	Nokia ID		
NSYNCML	NSYNCML		
OPUSH	**OBEX Object Push (échange de petits fichiers type vcard)**		
PALMOS	PalmOS		
PAN	Personnal Area Network (réseau ad-hoc avec émulation ethernet entre deux périphériques)		
PBAP	Phone Book Access (permet à une oreillette d'accéder au répertoire du smartphone)		
PCSUITE	Nokia PC Suite		
PRINT	Direct Printing		
SAP	SIM Access (dédié automobile pour permettre au système embarqué d'utiliser la carte SIM du smartphone)		
SEMCHLA	SEMC High Level Authentication		
SP	**Serial Port (émulation d'une liaison série RS232 pour l'échande de données)**		
SR1	Toshiba Speech Recognition SR-1		
SYNCML	SyncML Client (PIM synchronization)		
SYNCMLSERV	SYNCMLSERV		
UDITE	UDI TE		
UDIUE	UDI UE		
WIIMOTE	Wii-Mote		

Pour une liste plus complète, cf. https://www.bluetooth.com/specifications/profiles-overview.