

Bluetooth et BLE : Support dans Linux

maxime.chevallier@openwide.fr

Open Wide Ingénierie

09 février 2016

1 Bluetooth

- Présentation
- Architecture logique
- Appairage
- Découverte de services

2 Bluetooth Low Energy

- Présentation
- Architecture logique
- Attributs

3 BlueZ

- Présentation
- Bluez : Kernel
- Bluez : Userspace

1 Bluetooth

- Présentation
- Architecture logique
- Appairage
- Découverte de services

2 Bluetooth Low Energy

3 BlueZ

Historique

- 1994 : Création (Ericsson)
- 1998 : SIG (Ericsson, Intel, Nokia, Toshiba)
- 1999 : v1.0
- 2004 : v2.0 : Basic Rate / Enhanced Data Rate
- 2010 : v4.0 Low Energy
- 2014 : v4.2



Logo Bluetooth

Historique

- 1994 : Création (Ericsson)
- 1998 : SIG (Ericsson, Intel, Nokia, Toshiba)
- 1999 : v1.0
- 2004 : v2.0 : Basic Rate / Enhanced Data Rate
- 2010 : v4.0 Low Energy
- 2014 : v4.2



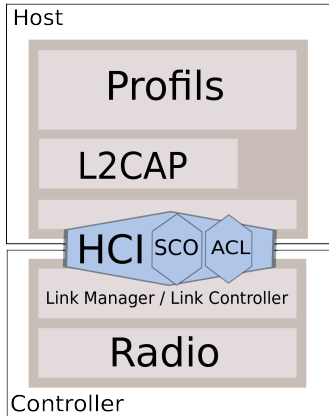
Logo Bluetooth

Historique

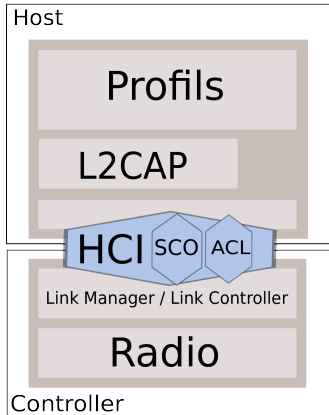
- 1994 : Création (Ericsson)
- 1998 : SIG (Ericsson, Intel, Nokia, Toshiba)
- 1999 : v1.0
- 2004 : v2.0 : Basic Rate / Enhanced Data Rate
- 2010 : v4.0 Low Energy
- 2014 : v4.2

Caractéristiques physiques

- 2.4 GHz
- Max 24Mb/s
- 79 canaux, AFH
- Conso : 1W



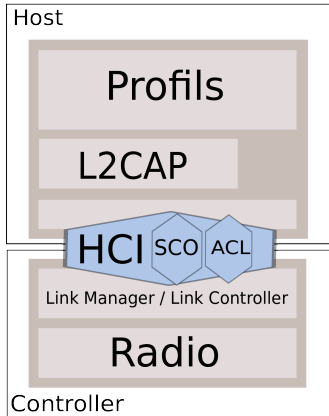
Bluetooth core



Bluetooth core

Host

- Logique Métier
- Scheduling
- Buffering



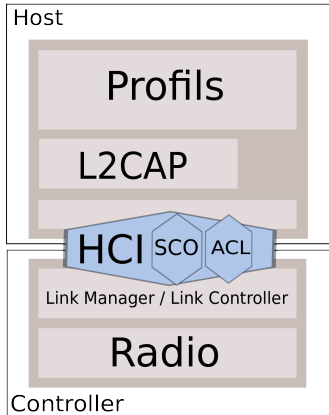
Bluetooth core

Host

- Logique Métier
- Scheduling
- Buffering

Host to Controller

- Host to Controller Interface
- Synchronous Connection-Oriented
- Asynchronous Connection-Less



Bluetooth core

Host

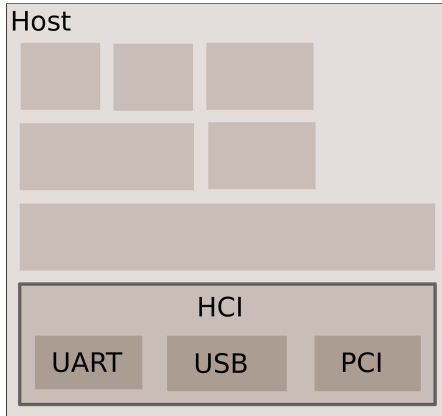
- Logique Métier
- Scheduling
- Buffering

Host to Controller

- Host to Controller Interface
- Synchronous Connection-Oriented
- Asynchronous Connection-Less

Controller

- Connexion
- Découverte



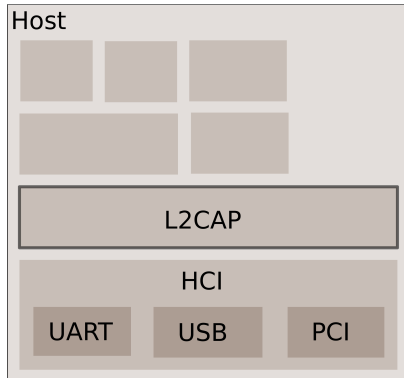
Host to Controller Interface

HCI

- Uniformisation
- Abstraction

Commandes :

- Données
- Configuration
- Évènements

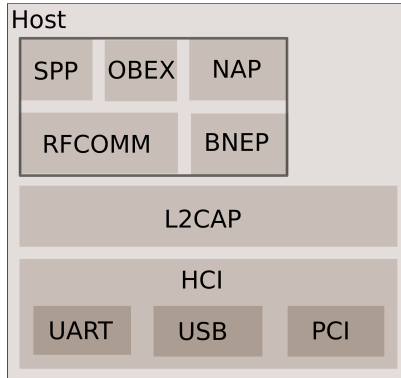


L2CAP

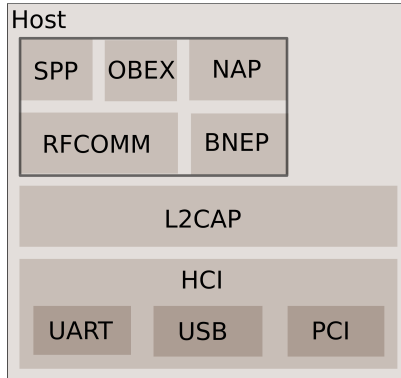
Socle pour de nombreux profils :

- Multiplexage
- Buffering
- QoS
- Scheduling

Logical Link Control and Adaptation Protocol



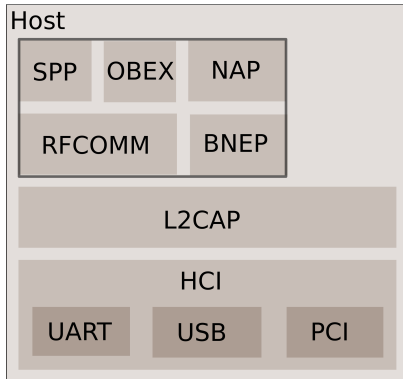
Profils



Protocoles

- RFCOMM
- BNEP
- AVCTP (controle A/V)
- AVDTP (transport A/V)

Profils



Profils

Protocoles

- RFCOMM
- BNEP
- AVCTP (controle A/V)
- AVDTP (transport A/V)

Profils

- Serial Port Profile
- Human Interface Device
- Personal Area Network
- Phone Book Access Profile

Découverte

- 1 Inquiry
- 2 Paging
- 3 Connexion

Découverte

- 1 Inquiry
- 2 Paging
- 3 Connexion

Appairage

- Connexion automatique,
- sécurisée,
- authentifiée,
- adaptée à l'appareil.

Découverte

- 1 Inquiry
- 2 Paging
- 3 Connexion



Appairage

- Connexion automatique,
- sécurisée,
- authentifiée,
- adaptée à l'appareil.

Découverte

- 1 Inquiry
- 2 Paging
- 3 Connexion



Appairage

- Connexion automatique,
- sécurisée,
- authentifiée,
- adaptée à l'appareil.



Découverte

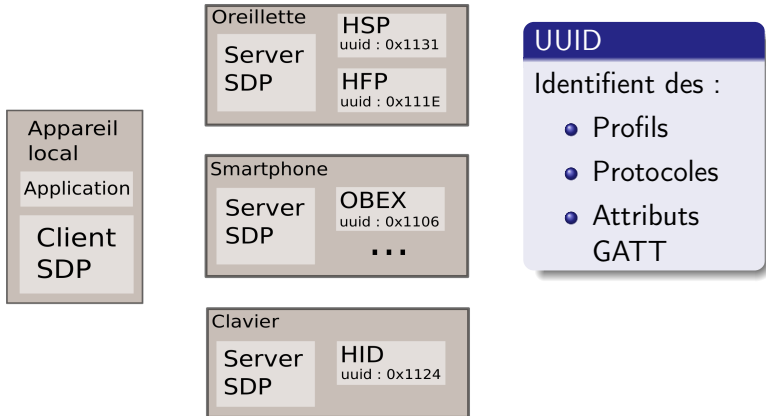
- 1 Inquiry
- 2 Paging
- 3 Connexion



Appairage

- Connexion automatique,
- sécurisée,
- authentifiée,
- adaptée à l'appareil.





Service Discovery Protocol

Liste : <https://www.bluetooth.com/specifications/assigned-numbers/service-discovery>

1 Bluetooth

2 Bluetooth Low Energy

- Présentation
- Architecture logique
- Attributs

3 BlueZ

Bluetooth Smart

- 2006 : Wibree (Nokia)
- 2010 : Bluetooth 4.0



Logos Bluetooth Low Energy

Bluetooth Smart

- 2006 : Wibree (Nokia)
- 2010 : Bluetooth 4.0



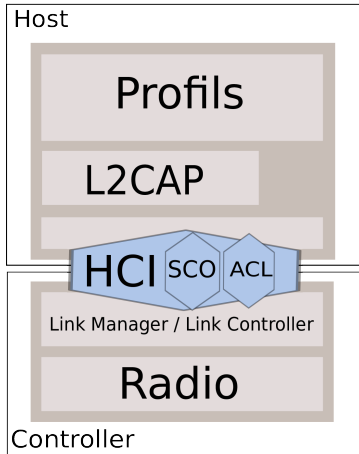
Logos Bluetooth Low Energy

Bluetooth Smart

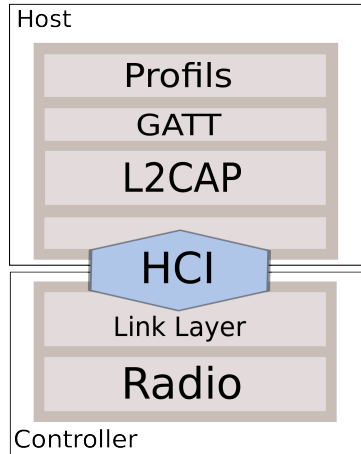
- 2006 : Wibree (Nokia)
- 2010 : Bluetooth 4.0

Caractéristiques

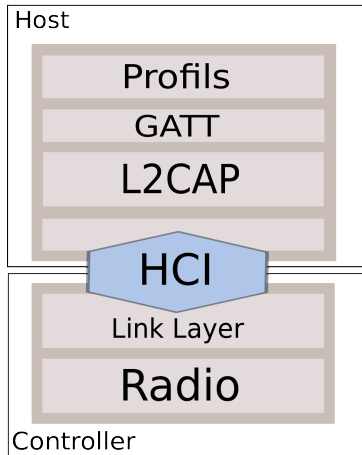
- 2.4 GHz
- 40 canaux
- 1 Mbit/s
- Conso entre 0.01W et 0.5W



Core BR/EDR



Core BLE



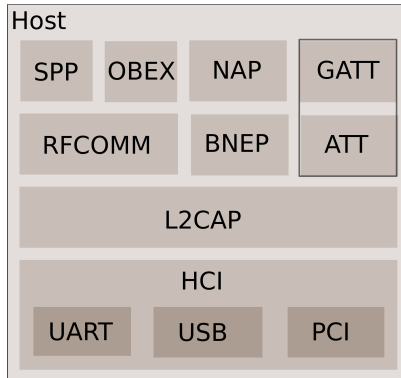
Core BLE

Link Layer

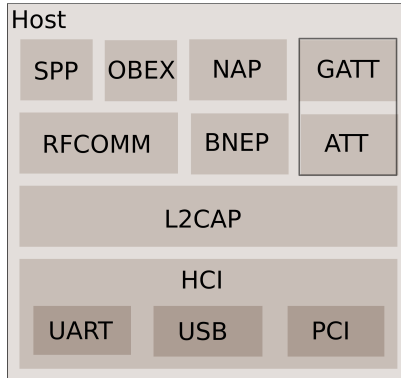
- Advertising
- Scanning
- Connected

Sécurité

- Clé côté Host
- AES 128
- Adresses :
 - Publique
 - Aléatoire



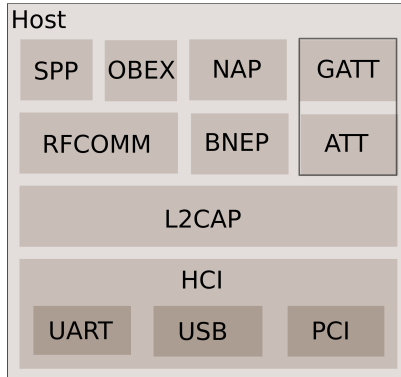
ATTrtributes / Generic ATTrtributes



ATT

- Protocole
- Transport d'attributs

ATTrIBUTES / Generic ATTrIBUTES



ATTributes / Generic ATTributes

ATT

- Protocole
- Transport d'attributs

GATT

Profil BLE

- Client
- Serveur

GATT

GATT

Attribut

- Type : UUID
- Permissions :
 - R/W
 - Encryption
 - Autorisation
- Valeur
- Handle : Adresse

GATT

Attribut

- Type : UUID
- Permissions :
 - R/W
 - Encryption
 - Autorisation
- Valeur
- Handle : Adresse

Services

GATT

Attribut

- Type : UUID
- Permissions :
 - R/W
 - Encryption
 - Autorisation
- Valeur
- Handle : Adresse

Services

Regroupe des :

Caractéristiques

GATT

Attribut

- Type : UUID
- Permissions :
 - R/W
 - Encryption
 - Autorisation
- Valeur
- Handle : Adresse

Services

Regroupe des :

Caractéristiques

- Déclaration
- Valeur

GATT

Attribut

- Type : UUID
- Permissions :
 - R/W
 - Encryption
 - Autorisation
- Valeur
- Handle : Adresse

Services

Regroupe des :

Caractéristiques

- Déclaration
- Valeur
- Et parfois :

GATT

Attribut

- Type : UUID
- Permissions :
 - R/W
 - Encryption
 - Autorisation
- Valeur
- Handle : Adresse

Services

Regroupe des :

Caractéristiques

- Déclaration
- Valeur
- Et parfois :

Descripteurs

Métadonnées sur la
caractéristique

Heart Rate Service

	Handle	UUID	Permissions	Value
Service	0x0021	SERVICE	READ	HRS
Characteristic	0x0024	CHAR	READ	NOT[0x0027]HRM
	0x0027	HRM	NONE	bpm
Descriptor	0x0028	CCCD	READ/WRITE	0x0001
Characteristic	0x002A	CHAR	READ	RD[0x002C]BSL
	0x002C	BSL	READ	<i>finger</i>

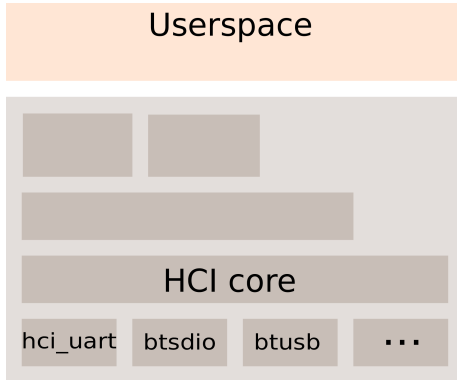
Exemple de service GATT

"Getting started with bluetooth low energy", R.Davidson, Akiba, Carles Cufi, Kevin Townsend, O'Reilly

- 1 Bluetooth
- 2 Bluetooth Low Energy
- 3 **BlueZ**
 - Présentation
 - Bluez : Kernel
 - Bluez : Userspace

BlueZ

- 2001 : Max Krasnyansky (Qualcomm)
Kernel 2.4.6
- 2004 : Marcel Holtmann (Intel)
Kernel 2.6
- 2012 : Low Energy (BlueZ 5.0)
Kernel 3.5
- 2016 : BlueZ 5.37



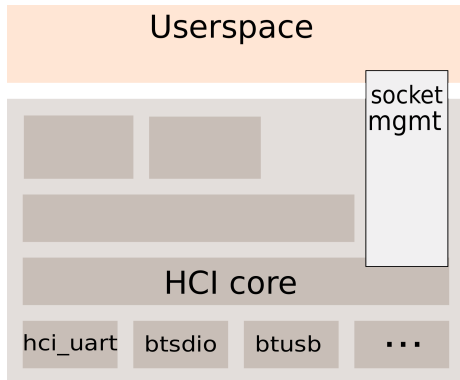
Host to Controller Interface

HCI

- Queueing
- Ordonnancement

Transport :

- USB
- UART
- PCI
- SDIO
- PCMCIA



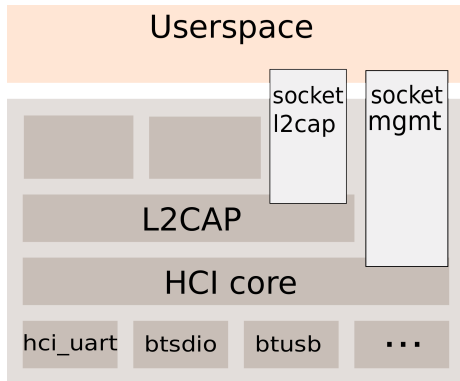
Management interface

mgmt socket

- HCI pour userspace
- Remplace hci sockets

Paramètres

```
- PF_BLUETOOTH
- BTPROTO_HCI
struct sockaddr_hci
- .hci_family = AF_BLUETOOTH
- .hci_dev = HCI_DEV_NONE
- .hci_channel = HCI_CHANNEL_CONTROL
```



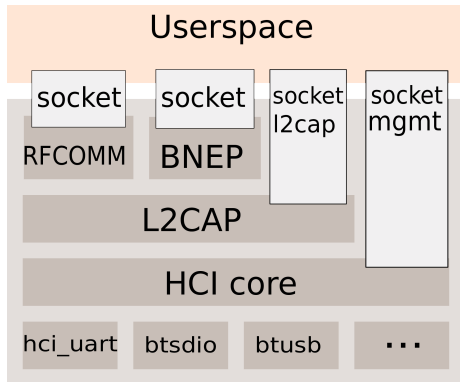
L2CAP

l2cap socket

- API Socket
- - Adresse
- - PSM

Paramètres

```
- AF_BLUETOOTH
- BTPROTO_L2CAP
struct sockaddr_l2
- .l2_family = AF_BLUETOOTH
- .l2_bdaddr = *BDADDR_ANY
- .l2_psm = htobs(0x1001);
```



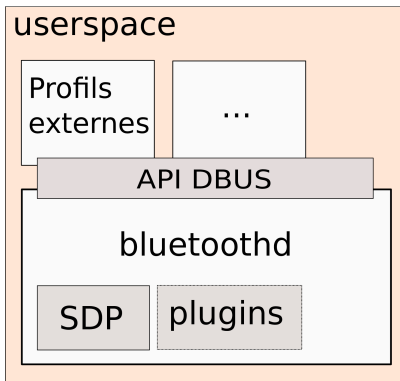
RFCOMM, BNEP, etc.

rfcomm socket

- API Socket
- - Adresse
- - Canal

Paramètres

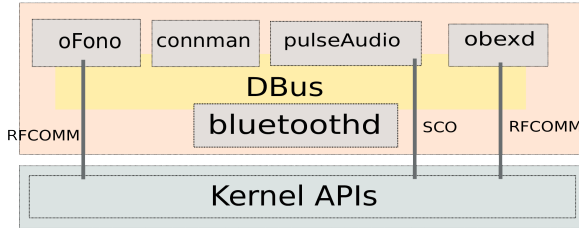
```
- AF_BLUETOOTH
- BTPROTO_RFCOMM
struct sockaddr_l2
- .rc_family = AF_BLUETOOTH
- .rc_channel = 1
- .rc_braddr = *BRADDR_ANY;
```



bluetoothd

Démon bluetoothd

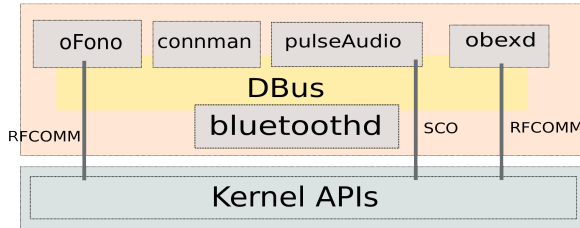
- Serveur SDP
- Gestion sockets
- Plugins
- Agents d'appairage
- API DBus



Profils Externes

oFono

- Gestion
Téléphonie
- HFP / HSP



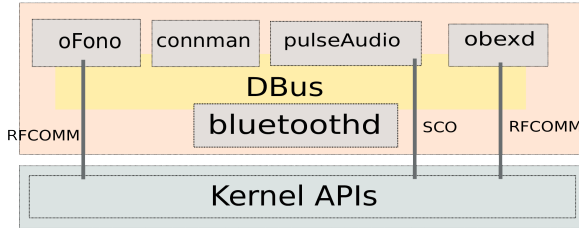
Profils Externes

oFono

- Gestion Téléphonie
- HFP / HSP

connman

- PAN (NAP)



Profils Externes

oFono

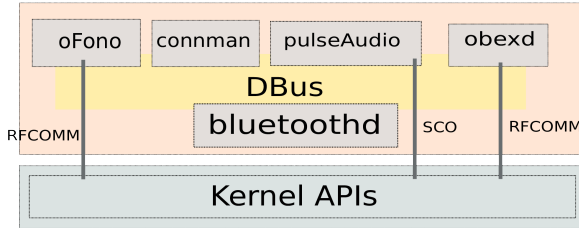
- Gestion Téléphonie
- HFP / HSP

connman

- PAN (NAP)

obexd

- OBEX, OPP



Profils Externes

oFono

- Gestion Téléphonie
- HFP / HSP

connman

- PAN (NAP)

obexd

- OBEX, OPP

pulse audio

- AD2P
- Gateway HFP

Outils

bluetoothctl

- Appairage
- SDP

Outils

bluetoothctl

- Appairage
- SDP

obexctl

- OBEX
- FTP

Outils

bluetoothctl

- Appairage
- SDP

btmgmt

- mgmt API
- Configuration

obexctl

- OBEX
- FTP

Outils

bluetoothctl

- Appairage
- SDP

btmgmt

- mgmt API
- Configuration

obexctl

- OBEX
- FTP

hcidtool / hciconfig

- HCI brut
- Configuration

Outils

hcidump

- Log HCI
- Filtrage protocoles

Outils

hcidump

- Log HCI
- Filtrage protocoles

btmon

- Log HCI
- Log bluetoothd
- Dump btsnoop (wireshark)

Outils

hcidump

- Log HCI
- Filtrage protocoles

btmon

- Log HCI
- Log bluetoothd
- Dump btsnoop (wireshark)

- **hciattach**
hci over UART

Outils

hcidump

- Log HCI
- Filtrage protocoles

btmon

- Log HCI
- Log bluetoothd
- Dump btsnoop (wireshark)

- **hciattach**
hci over UART
- **l2ping**
test L2CAP

Outils

hcidump

- Log HCI
- Filtrage protocoles

btmon

- Log HCI
- Log bluetoothd
- Dump btsnoop (wireshark)

- **hciattach**
hci over UART
- **l2ping**
test L2CAP
- **rfcomm**
gestion RFCOMM / SPP

Outils

hcidump

- Log HCI
- Filtrage protocoles

btmon

- Log HCI
- Log bluetoothd
- Dump btsnoop (wireshark)

- **hciattach**

hci over UART

- **l2ping**

test L2CAP

- **rfcomm**

gestion RFCOMM / SPP

- **sdptool**

gestion SDP

Outils GATT

btgatt-client

- Connexion GATT
- Notifications
- Découverte services

Outils GATT

btgatt-client

- Connexion GATT
- Notifications
- Découverte services

gatttool

- Connexion GATT
- Découverte services
- Remplacé par btgatt-client

Outils GATT

btgatt-client

- Connexion GATT
- Notifications
- Découverte services

gatttool

- Connexion GATT
- Découverte services
- Remplacé par btgatt-client

btgatt-server

- Test GATT
- Interactif

HCI lib

- Accès HCI
- Langage C, userspace
- Configuration précise :
 - Advertising LE
 - Commandes constructeur
- Utilisateurs avertis

Merci !

<https://github.com/minimaxwell/docs/tree/master/bluetooth/meetup>