

Wireless Personal Area Networks

Introduction

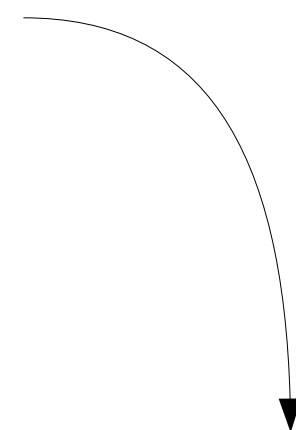
Besoins

- Remplacement des câbles par des liens sans fil et flexibilité
- Collecte de données issues de capteurs sans fil
- Suivi santé patient
- Monitoring de structures
- ...
- Autonomie énergétique
- Faible maintenance
- Faible coût



Bluetooth (IEEE 802.15.1)

Connectique sans fil



IEEE 802.15.4 / ZigBee

Réseaux de capteurs sans fil

Sommaire

1.Introduction

2.Bluetooth

3.IEEE 802.15.4 / ZigBee

4.Conclusion

Bluetooth

Origines et Objectifs

Famille des protocoles IEEE 802.15 pour les réseaux faible portée

- Remplacement des câbles par un lien sans fil pour la connexion faible distance
 - ✓ Souris, oreillette...
- Connectivité réseau
 - ✓ Synchronisation, partage d'accès...

Unification du moyen de communication entre les périphériques



Unification des royaumes du Danemark, de Suède et de Norvège au 10^e siècle



Harald la Dent Bleue

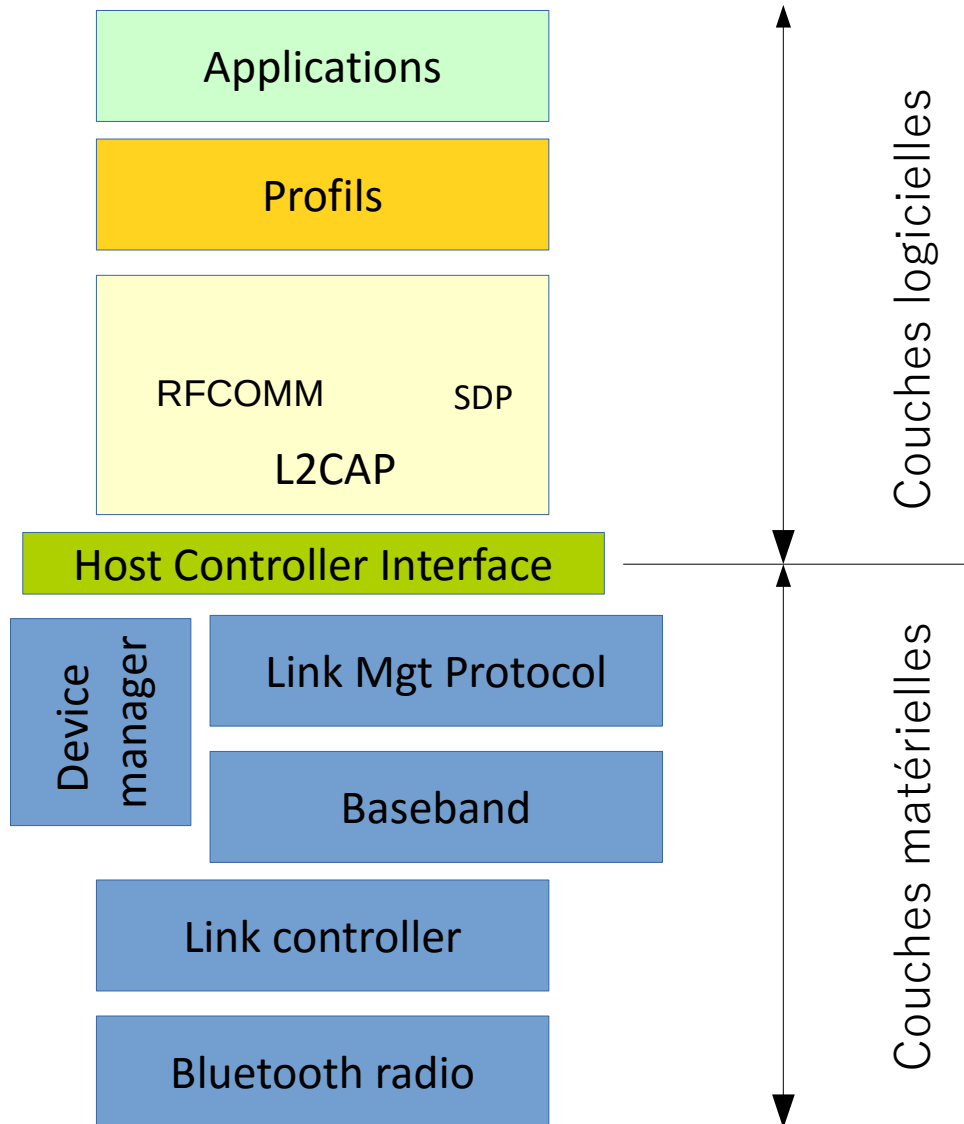
Bluetooth

Origines et objectifs

Caractéristiques

- Faibles coûts et intégration importante
- Faible portée
- Econome en énergie
- Interopérabilité totale sans intervention extérieure

Bluetooth Architecture

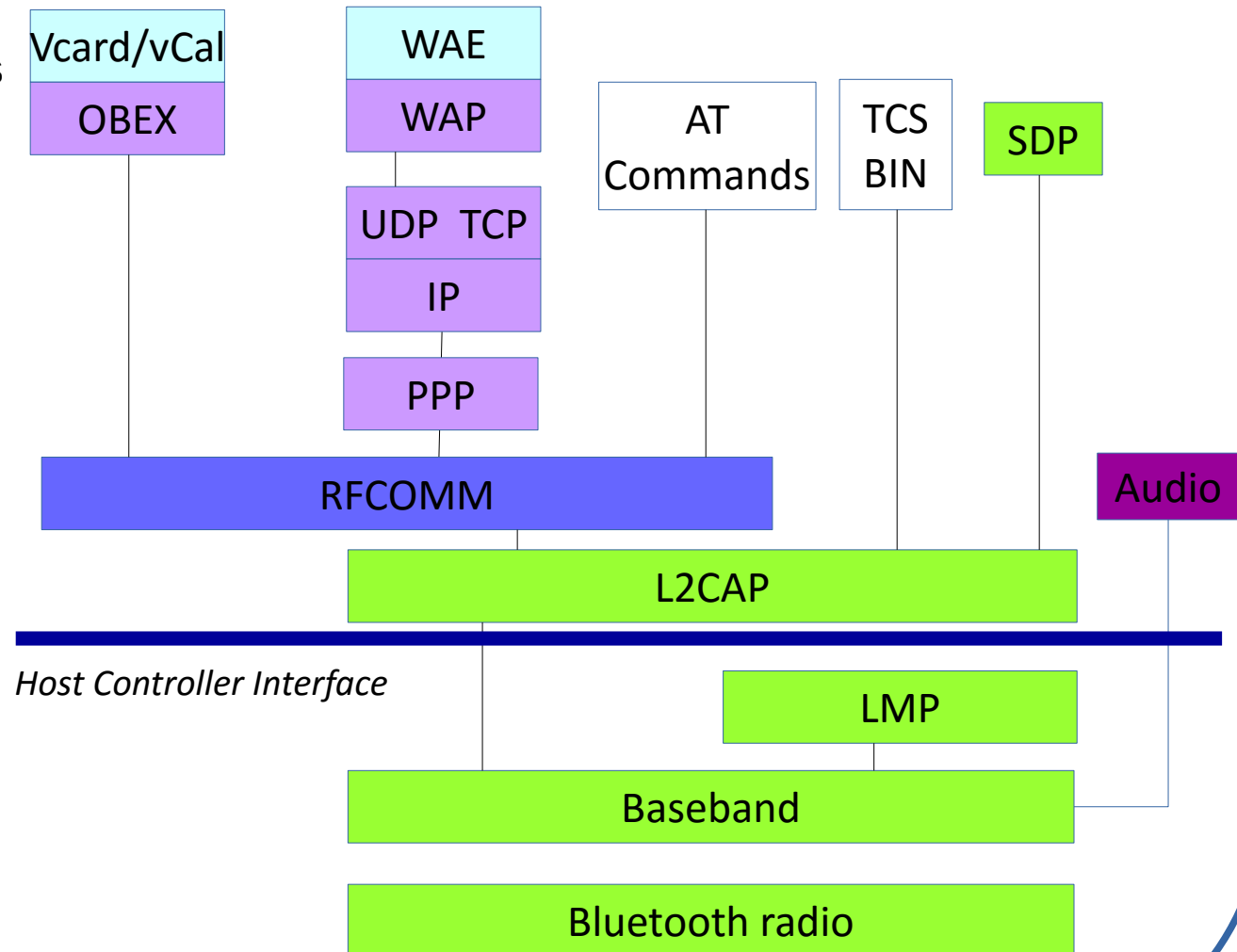


Electronique et interopérabilité

Bluetooth Architecture

Point de vue protocolaire

- Remplacement de liens variés
 - ✓ Série
 - ✓ Voix
- Formats
- Fonctionnalités réseau
- Contraintes temporelles et Qualité de Service



Bluetooth Architecture

Classification des protocoles

Bluetooth Core

Baseband

LMP

L2CAP

SDP

Cable Replacement

RFCOMM

Telephony Control

TCS Binary

AT-commands

Adopted Protocols

PPP

UDP/TCP/IP

OBEX

WAP

vCard

vCal

IrMC

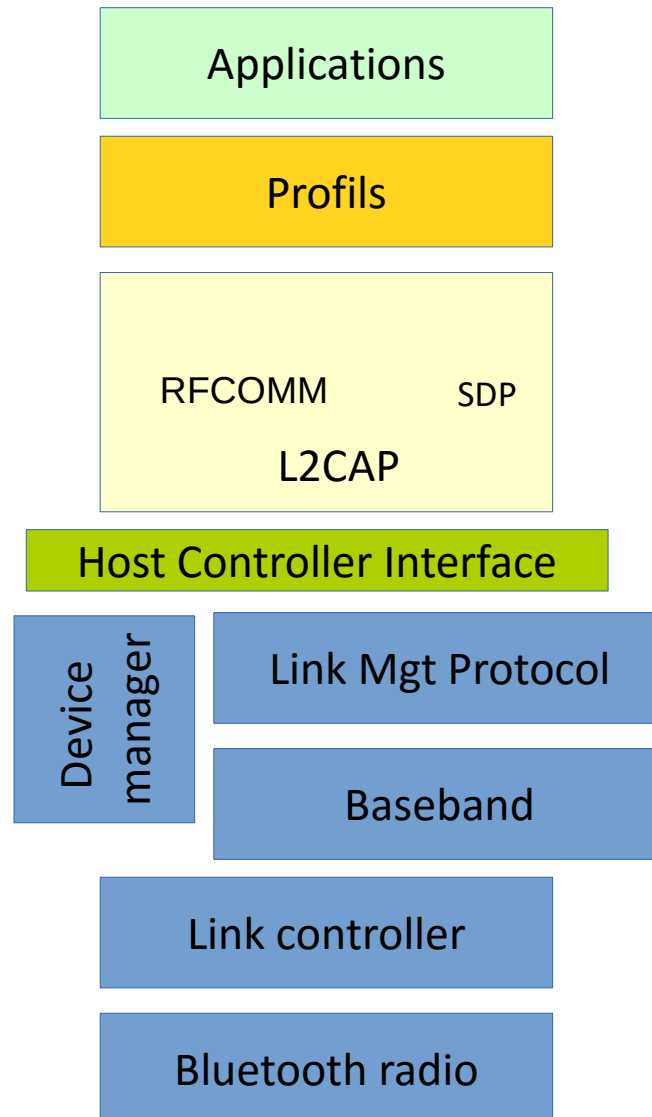
WAE

SDP : *Service Discovery Protocol*

L2CAP : *Logical Link Control and Adaptation Protocol*

LMP : *Link Management Protocol*

Bluetooth Architecture



Bluetooth

Couche physique

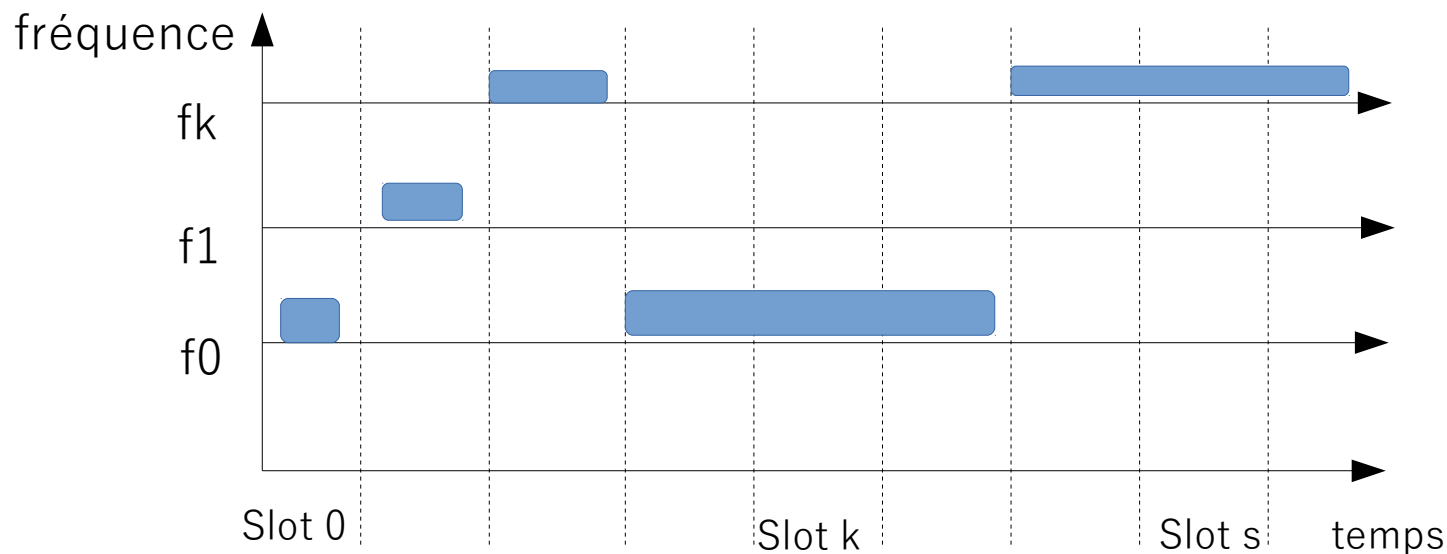
Caractéristiques

- Transmissions effectuées dans la bande ISM (*Industrial, Scientific and Medical*) 2.4GHz
 - $F_l = 2.400 \text{ GHz}$; $F_h = 2.4835 \text{ GHz}$
- Canal découpé en 79 sous-canaux
 - Espacement entre les canaux : 1MHz
- *Frequency Hopping Spread Spectrum*
 - Sauts rapides de fréquence
 - Minimisation des interférences avec d'autres technologies utilisant la même bande de fréquence
 - WiFi, 802.15.4 DSSS...
 - Séquence de saut dépendant de l'adresse du nœud-maître
 - Séquence partagée avec les autres membres du réseau pour maintenir la communication
 - Un saut toutes les 625 microsecondes \Rightarrow 1600 changements par seconde
 - Faible taille de paquets car la bande est bruitée (taux d'erreur important)

Bluetooth

Couche physique

Le FHSS à la mode Bluetooth



- Quand un nœud en a le droit, il entame la conversation sur un slot pair.
- Les réponses lui parviennent sur un slot impair
- La trame peut occuper le médium pendant 1, 3 ou 5 slots
- Le saut de fréquence se fait entre deux transmissions
- Robustesse par rapport à une occupation statique du canal
 - Evitement de brouilleur bande étroite

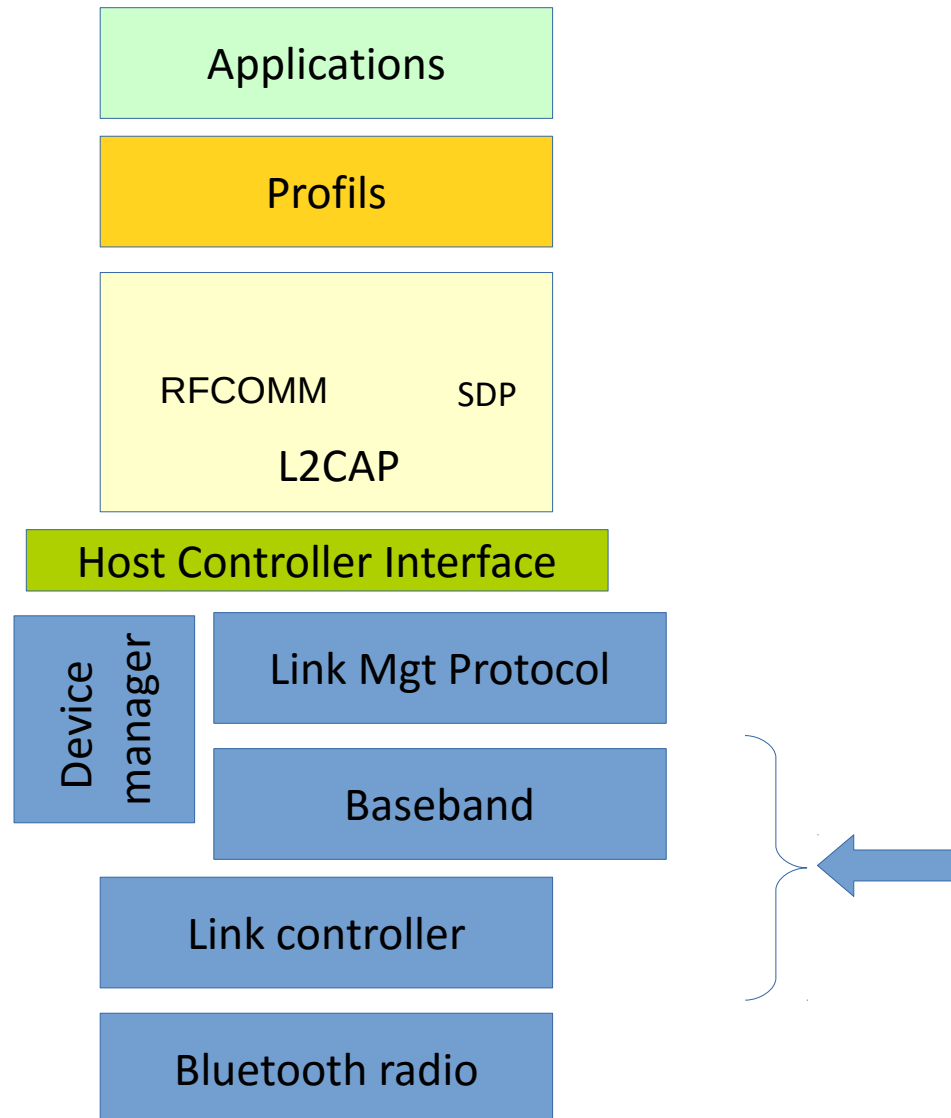
Bluetooth

Couche physique

Caractéristiques (suite)

- Classes de modules radio
 - Classe 1
 - 100mW
 - Portée : 100m
 - Classe 2
 - 2,5mW
 - Portée : 10m
 - Classe la plus répandue
 - Classe 3
 - 1mW
 - Portée : 1m

Bluetooth Architecture



Bluetooth

Bande de base et *Link Control*

Services fournis

- Création d'un lien radio entre deux nœuds
 - Etablissement de connexion
 - Synchronisation des horloges des nœuds
 - Synchronisation des séquences de saut de fréquence
- Mécanismes de correction d'erreurs
- Cryptage bas niveau
- Adressage sur 48 bits équivalent à une adresse MAC

Typologie de liens

- SCO *Synchronous Connection-Oriented*
 - Audio ou Audio+Données
 - Allocation périodique de slots temporels (temps de parole)
- ACL *Asynchronous Connection-less Link*
 - Données uniquement
 - Taille de trame variable

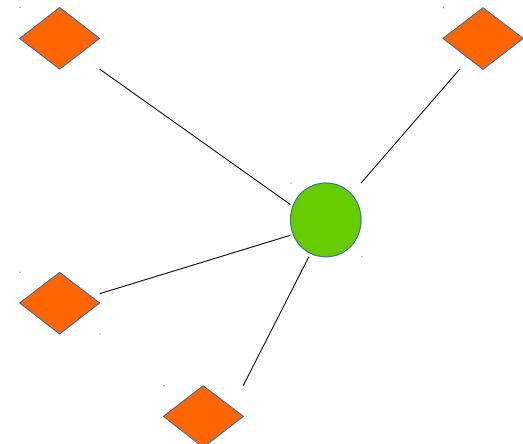
Bluetooth

Bande de base et *Link Control*

Création de liens => Création d'un réseau

Piconet

- 1 maître, n esclaves
 - ✓ Au plus 7 esclaves actifs dans le piconet
 - ✓ Possibilité d'avoir 255 esclaves passifs
- Séquence de sauts de fréquence et horloge imposées par le maître
- Emissions du maître : slots pairs
- Emissions des esclaves : slots impairs
- Temps de parole alloué par le maître
- Pas d'échange entre les esclaves



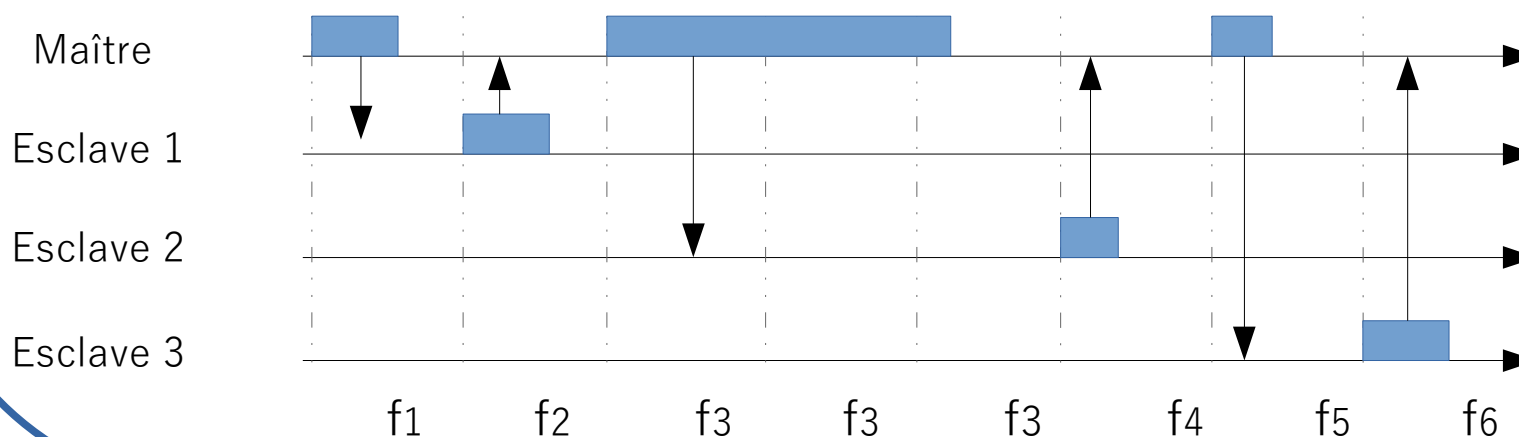
Bluetooth

Bande de base et *Link Control*

Création de liens => Création d'un réseau

Communications en *Time Division Duplex*

- Division en *slots* de 625μs
- Changement de fréquence à chaque paquet
- *Polling* des esclaves par le maître
- Un esclave ne peut parler qu'immédiatement après avoir été « pollé »
- Collisions dans un *piconet* vs Collisions entre *piconets* voisins



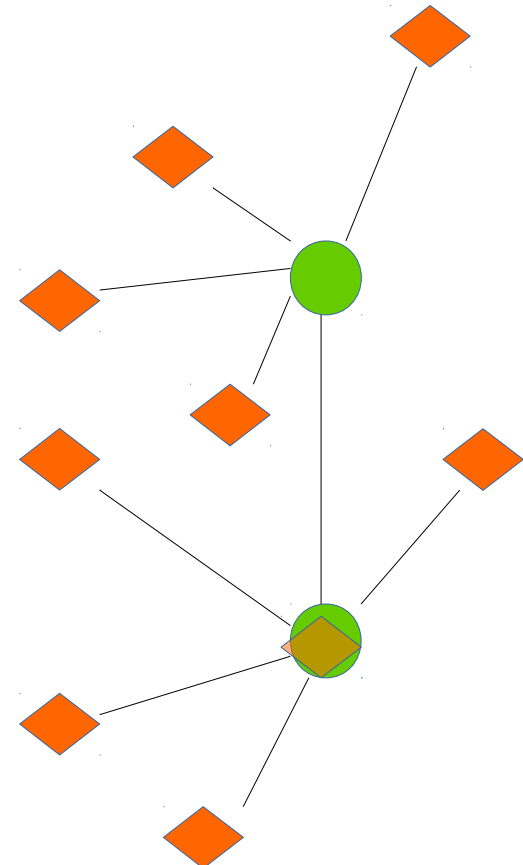
Bluetooth

Bande de base et *Link Control*

Création de liens => Création d'un réseau

Scatternet

- Combinaison de *piconets*
- Arbre d'étoiles
- Maître de niveau n, esclave de niveau n-1
- Au plus 10 *piconets*, 72 nœuds actifs
- Intersection de *piconets* : station relais



Bluetooth

Bande de base et *Link Control*

Format de paquets

- Format général



- Utilisé pour la synchronisation
- Préambule de 4 bits
- Mot de synchronisation de 64 bits
- Types :
 - DAC ou *Device Access Code*: utilisé dans la phase de *paging*
 - CAC ou *Channel Access Code* : utilisé durant la phase où les nœuds sont connectés
 - GIAC ou *Generic Inquiry Access Code* : phase d'enquête générale, identification des nœuds voisins
 - DIAC ou *Dedicated Inquiry Access Code* : recherche d'un type spécifique de voisin

Bluetooth

Bande de base et *Link Control*

Format de paquets

- Format général



18 bits utiles protégés => 54 bits

Champs :

- Adresse de l'esclave visé
- Type de paquet*
- Bit de contrôle de flux : permet d'interrompre temporairement le flux de trafic
- Bit d'accusé de réception
- Bit de numérotation
- Mot de contrôle d'intégrité des paquets

Bluetooth

Bande de base et *Link Control*

Format de paquets

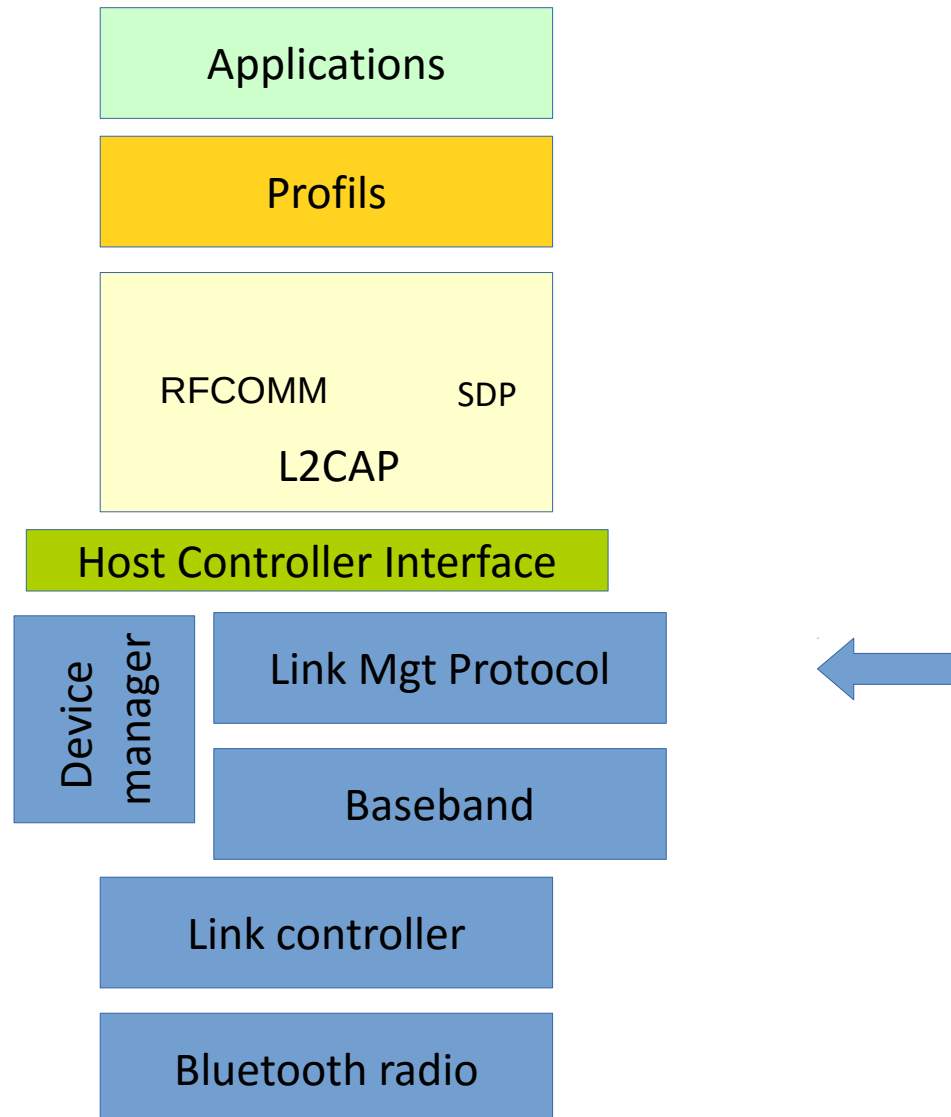
- Format général



Types de paquets

- Communs à tous types de communications
 - Paquet FHS : code d'accès, en-tête et 160bits de données
 - Paquet *Poll* : code d'accès et en-tête, acquitté
- Communications synchrones
 - *Synchronous Connection Oriented* (SCO)
 - Parfois une portion de données asynchrones avec CRC et retransmission
 - Normalement, pas de CRC ni de retransmissions
 - *Extended SCO* (eSCO)
 - CRC associé aux données, retransmissions possibles
- Communications asynchrones : *Asynchronous Connection-Less* (ACL)
 - Données utiles et CRC

Bluetooth Architecture



Bluetooth

Link Management Protocol

Services fournis

- Gestion du *piconet*
 - Ajout/suppression d'esclaves du *piconet*
 - Basculement du rôle (maître/esclave)
 - Etablissement des liaisons SCO/ACL
 - Contrôle du cycle d'activité (*duty-cycle*) de la radio
 - Contrôle des états de connexion des nœuds dans le *piconet*
 - ✓ *Hold*: permet à une station de se libérer de son *piconet* pour une durée fixe
 - ✓ *Sniff*: écoute périodique du canal pendant une durée prédéfinie
 - ✓ *Park*: station restant synchronisée avec le maître mais qui n'intervient pas ce qui lui permet de réintégrer rapidement le *piconet*
- Sécurité
 - Authentification des périphériques
 - Échange de clés

Bluetooth

Link Management Protocol

Economie d'énergie et modes des esclaves

Dépenses d'énergie

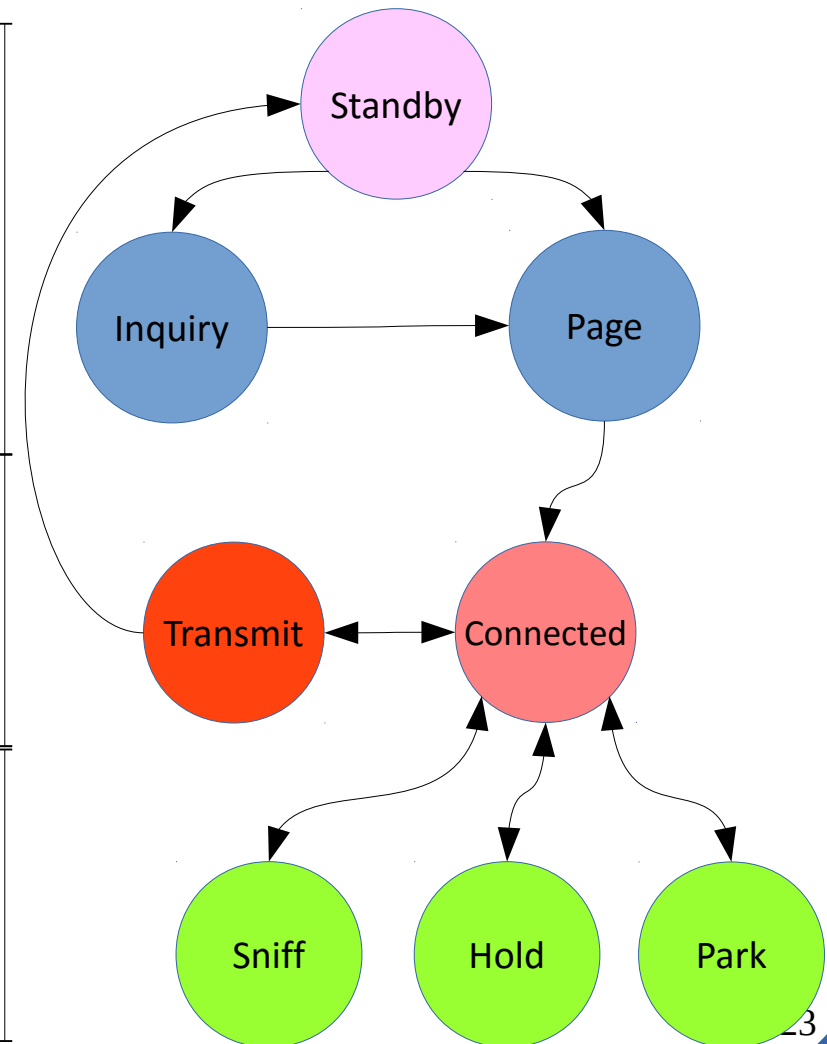
- Transmission de trames
- Réception de message
- *Idle Listening*

Etablissement de connexion

- **Sniff** : mode applicable dans un contexte de trafic périodique avec des débits faibles
- **Hold** : mode permettant d'effectuer d'autres activités (inquiry, établissement de connexion, participation à d'autres piconets...)
- **Park** : mode permettant d'avoir plus de 7 esclaves dans un piconet

Etats actifs

Modes économes en énergie

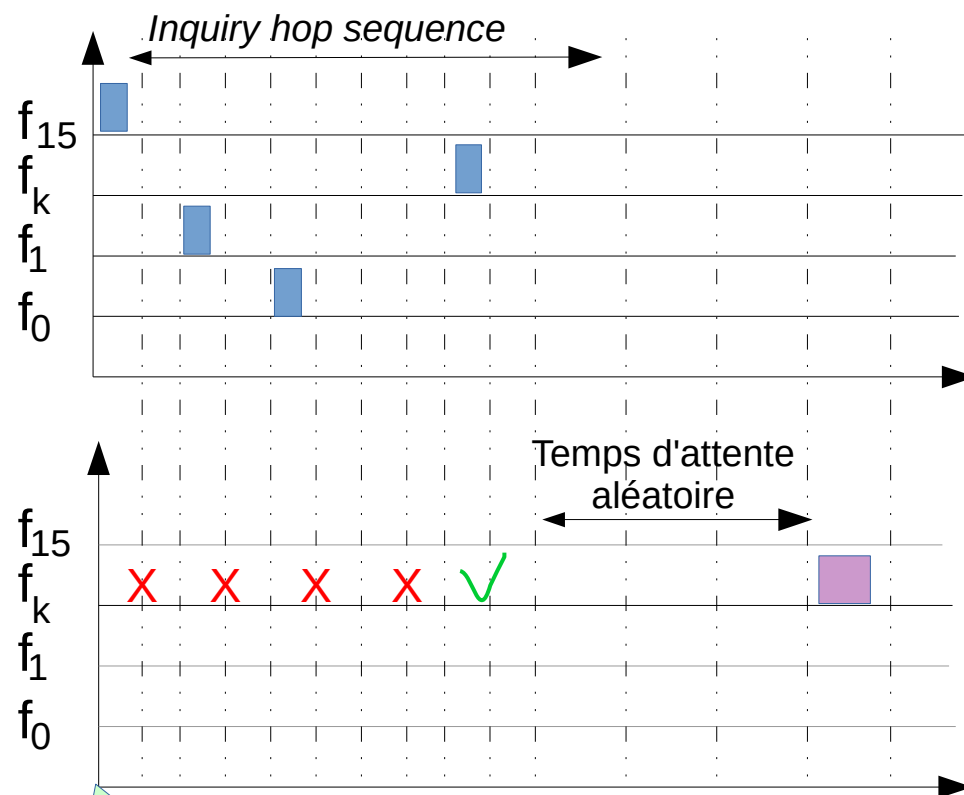


Bluetooth

Link Management Protocol

Etablissement de connexion : phase *Inquiry*

● : nœud disponible (A) ● : nœud cherchant à se connecter à des voisins (B)



- A en mode *Inquiry Scan*
 - En réception sur une fréquence dépendant de son adresse
- B transmet un train de paquets ID
 - IAC (*Inquiry Access Code*) indiquant le type de terminaux pouvant répondre
 - En général un GIAC (*General IAC*) qui permet de joindre tous les éléments
 - Pour certains éléments actifs, on peut utiliser un DIAC (*Dedicated IAC*)

Bluetooth

Link Management Protocol

Etablissement de connexion : phase *Inquiry*

● : nœud disponible (A) ● : nœud cherchant à se connecter à des voisins (B)

- Un train T1 est émis 256 fois puis un second train T2 est émis 256 fois
 - Le temps total pour émettre ces 2 trains et récupérer suffisamment de réponses est de 10,24s
 - Néanmoins, si suffisamment de réponses sont collectées avant ce délai, le train peut être interrompu
 - Côté récepteur, le temps minimum d'écoute doit durer pendant un temps suffisant pour que les 16 fréquences soient couvertes
- A la réception d'un paquet d'*Inquiry*, A émet, après un temps d'attente aléatoire, un paquet *Inquiry Response*
 - Temps d'attente décompté en slot et évitement de collisions entre les réponses
 - *Inquiry Response* : séquence de sauts (FHS), informations d'horloge nécessaires pour l'état *Page*

Bluetooth

Link Management Protocol

Etablissement de connexion : phase de *Paging*

● : nœud disponible (A) ● : nœud cherchant à se connecter à des voisins (B)

Objectifs :

- Répartir les rôles (maître-esclave)
- Synchroniser l'esclave au maître (horloge et séquence de sauts de fréquence (FHS))

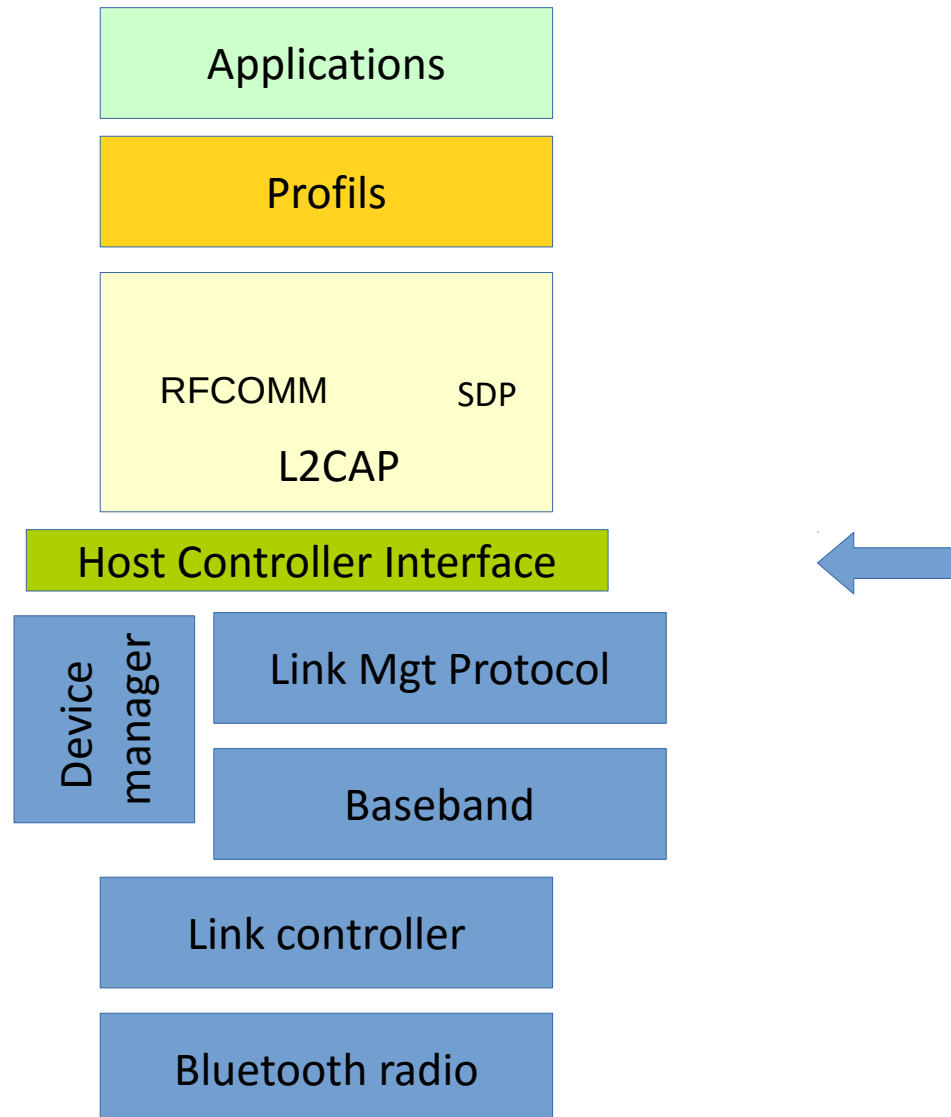
Hypothèse de départ

- B connaît la FHS de A et son horloge

Processus

- L'initiateur devient le maître => A sera esclave
- B **estime** la position actuelle dans la FHS de A.
 - Estimation => possible erreur
- B transmet le message *Page* sur une plage de fréquence choisie à partir de la fréquence estimée.
 - Plage de 32 fréquences divisée en 2 trains de 16 fréquences.
- A choisit une des fréquences dédiées au *Paging* et attend le message

Bluetooth Architecture



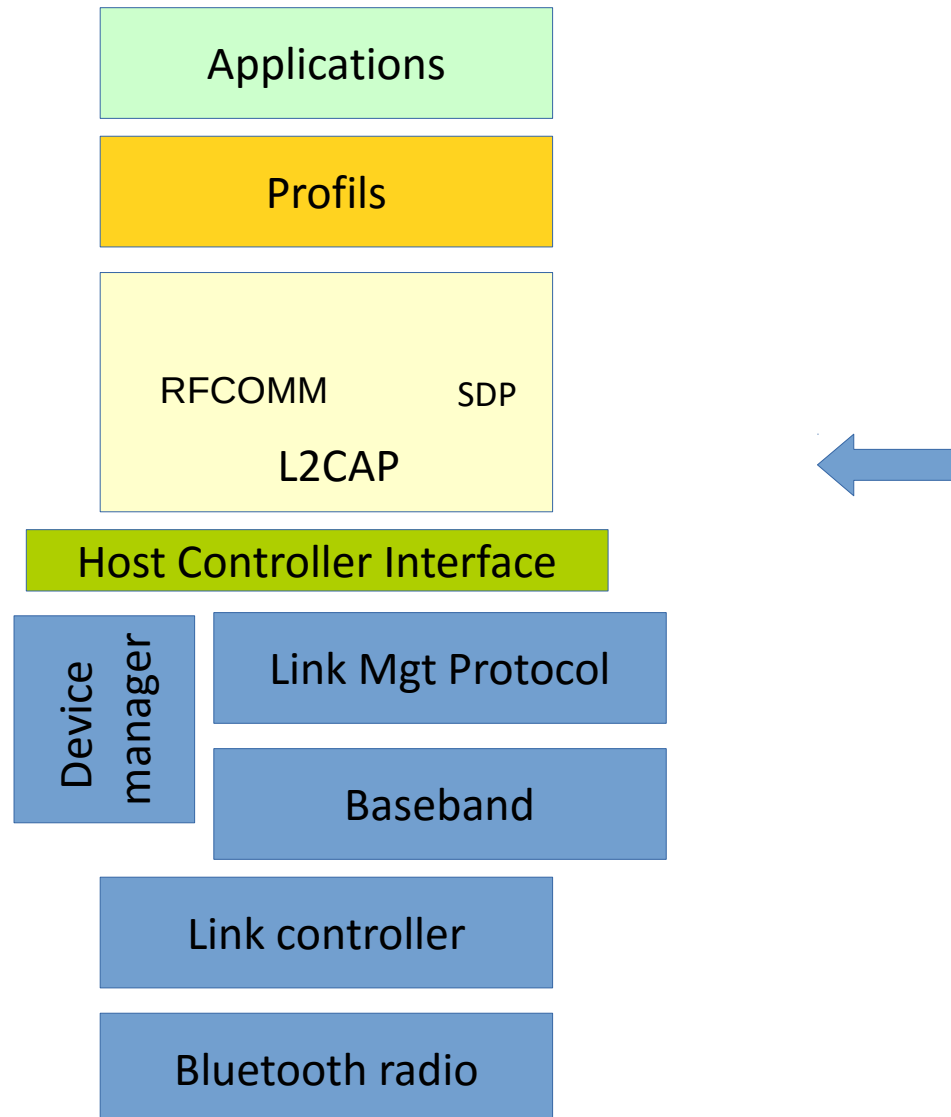
Bluetooth

Interface HCI

Host Controller Interface

- Interface entre les parties matérielles et logicielles de la pile protocolaire
- Fournit un interface de commande uniformisée à un contrôleur
 - Méthode d'accès aux fonctionnalités indépendante des détails de l'implémentation des couches basses de la pile protocolaire
- Types de commandes
 - *Link* : contrôle la création de lien avec d'autres équipements
 - *Policy* : contrôle le comportement du *Link Manager*
 - *Informational, Status* : accès aux registres du contrôleur
- Accessible via :
 - UART
 - USB
 - RS-232

Bluetooth Architecture



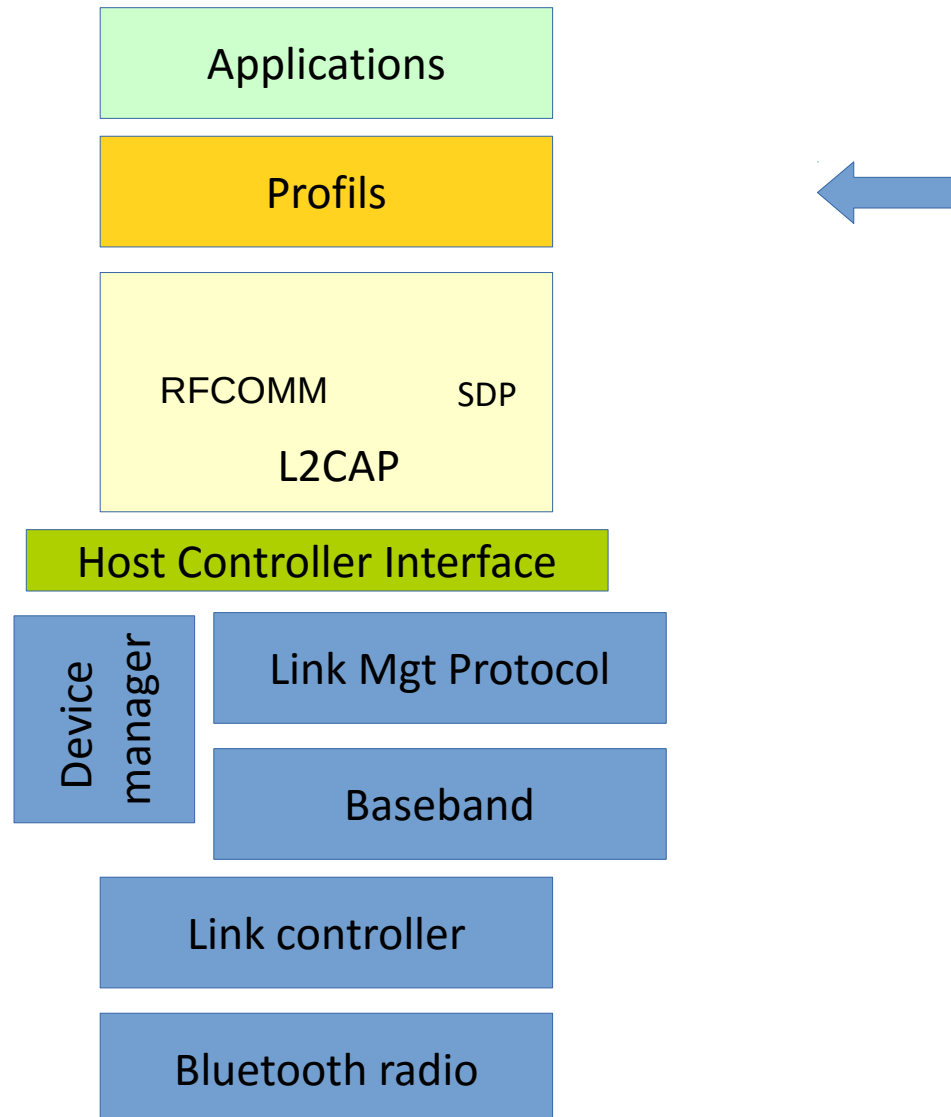
Bluetooth

Logical Link Control and Adaptation Protocol

L2CAP :

- Services de transmission de données en mode connecté et mode non connecté
 - Pas de gestion de liens SCO voix : la gestion est faite directement en bande de base
- Multiplexage des applications au-dessus des couches de transmission
 - Association des paquets aux protocoles de couches supérieures
- Adaptation : segmentation des messages (64ko) et réassemblage
- Gestion de la qualité de service (QoS)
 - $QoS = f(\text{bande passante ; délais})$
 - L2CAP vérifie avec les couches sous-jacentes que cette QoS peut être assurée

Bluetooth Architecture



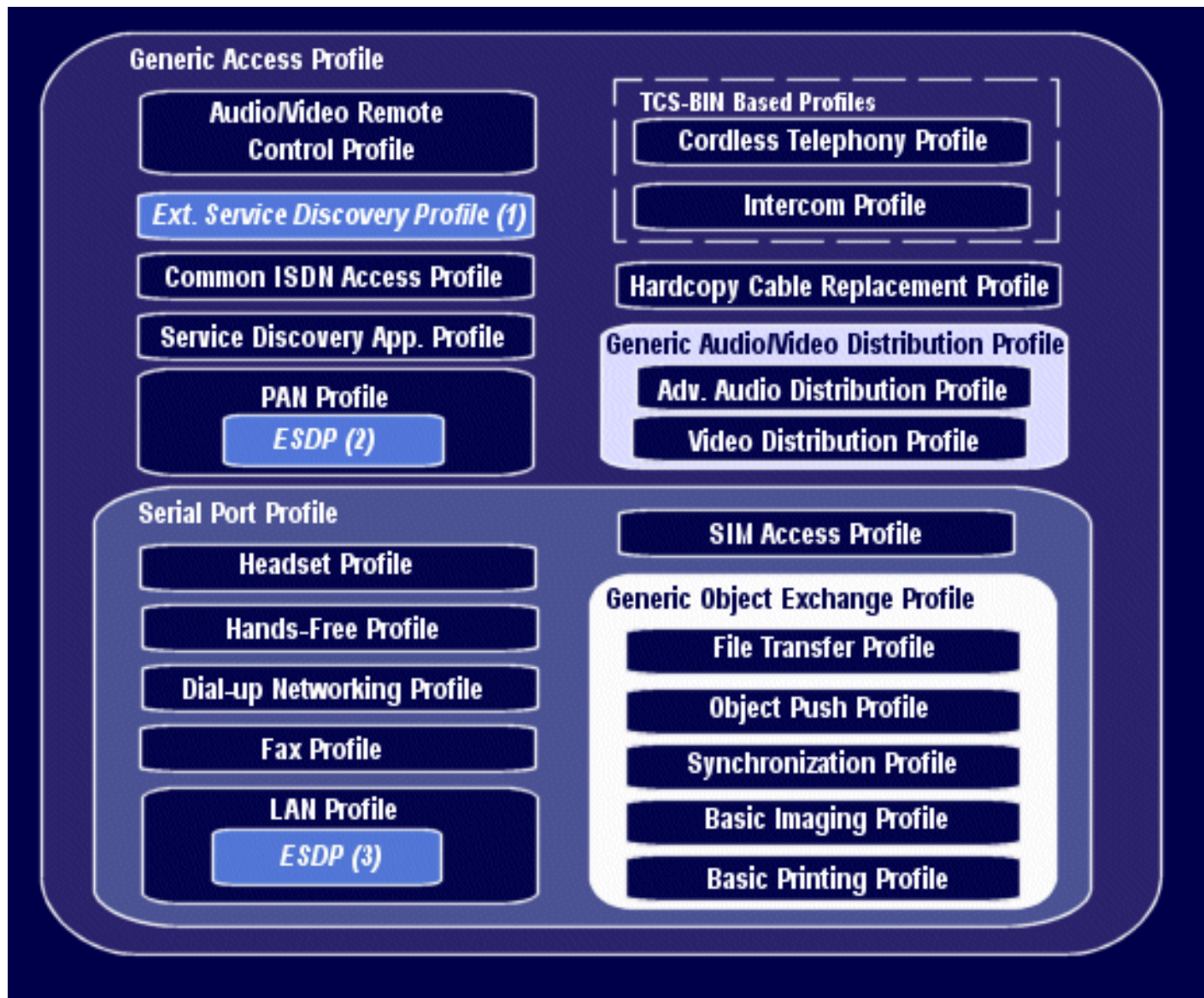
Bluetooth

Profils

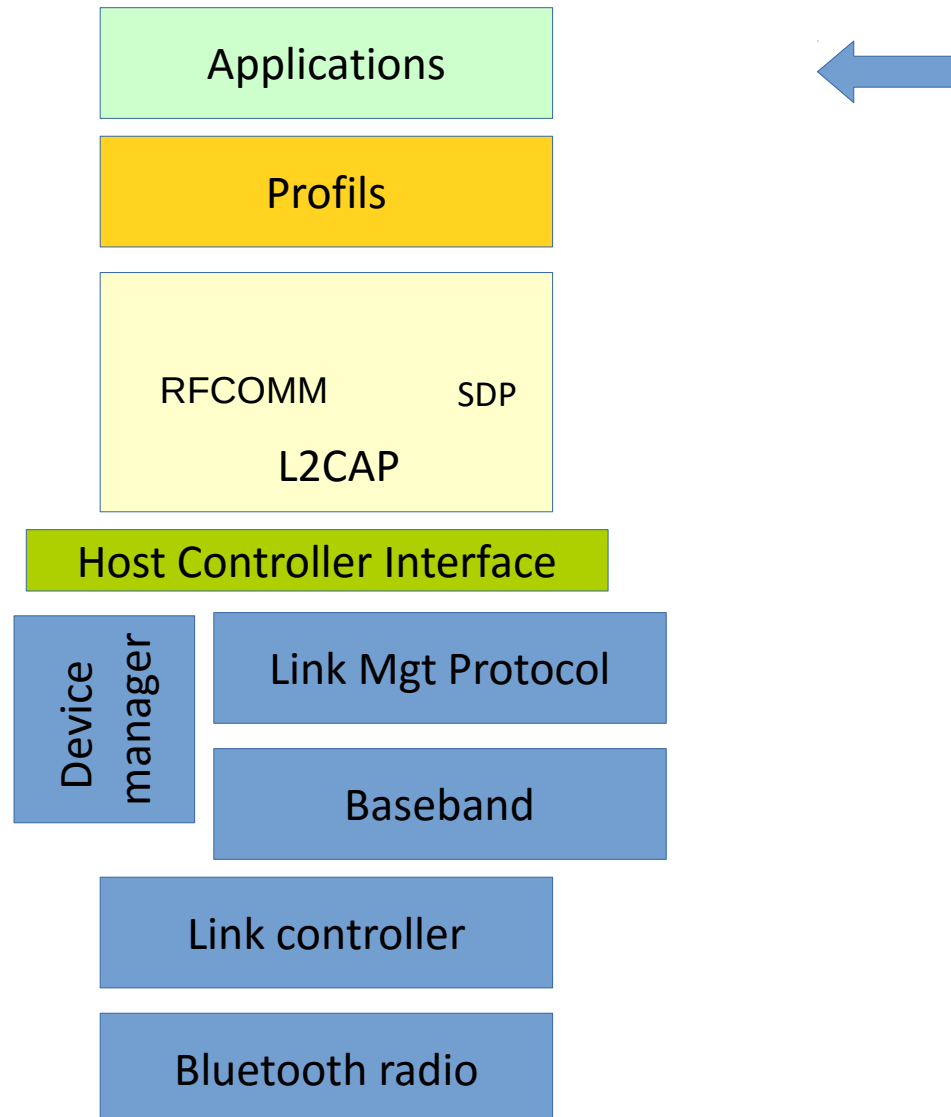
Profil Bluetooth : mode de fonctionnement de l'équipement

- Un service n'est supporté que si le profil correspondant est disponible sur tous les équipements impliqués dans la communication
- Un profil contient des informations au moins sur les points suivants
 - Les autres profils dont il dépend
 - Les interfaces à utiliser
 - Les parties de la pile Bluetooth à utiliser
- L'objectif des profils est de permettre une interopérabilité entre les équipements

Bluetooth Profiles



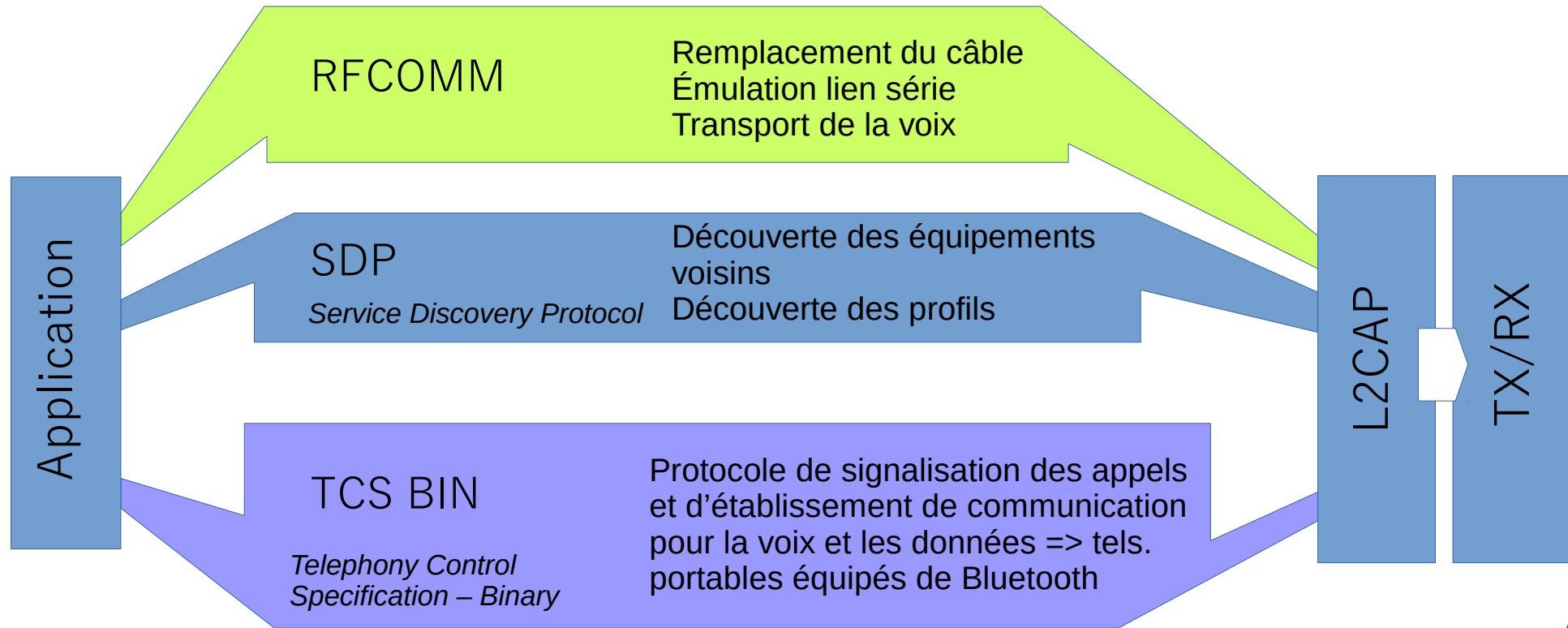
Bluetooth Architecture



Bluetooth

Couche application

Services



Bluetooth

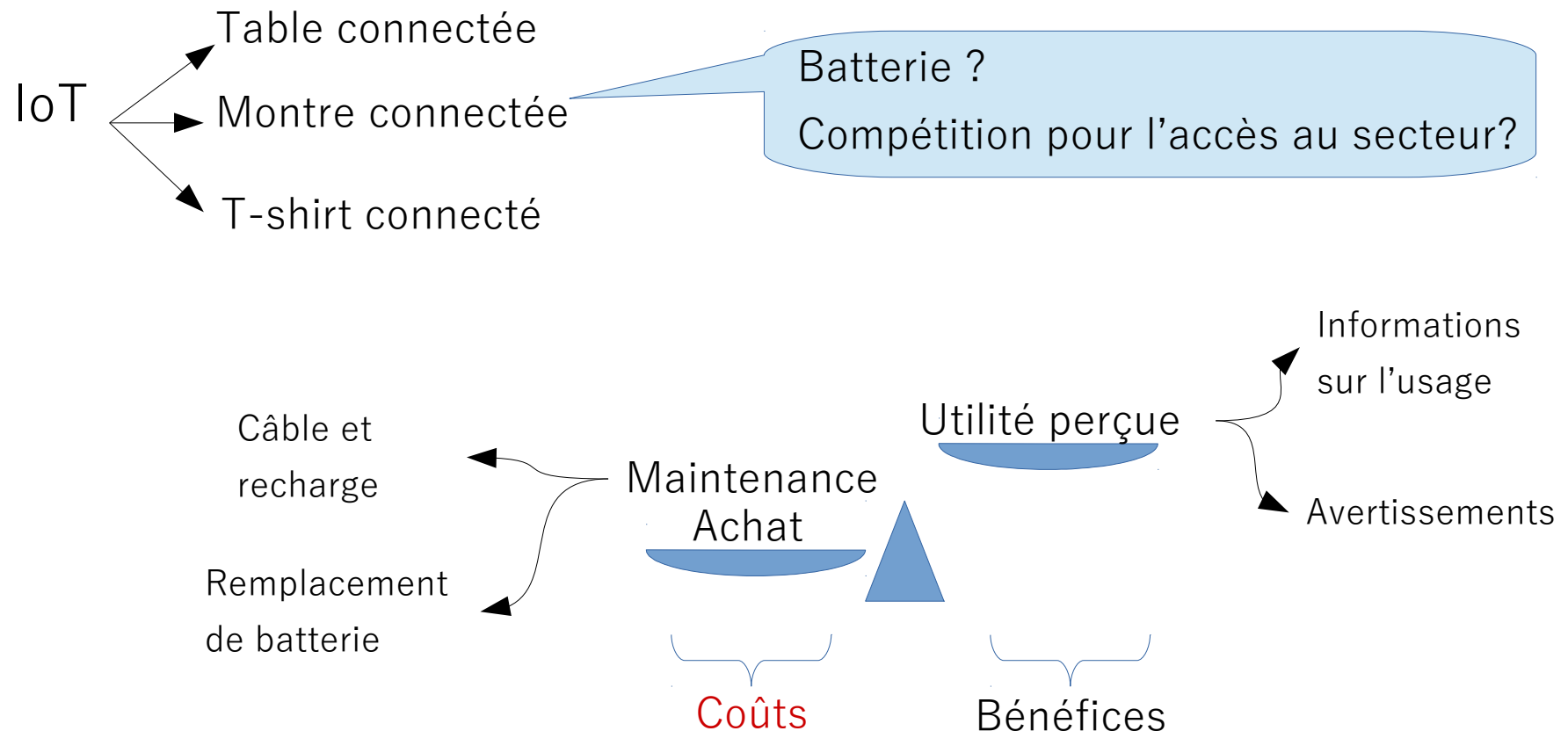
Evolutions : BLE

Bluetooth Low Energy ou Bluetooth Smart ou Version 4.0+

- Objets connectés
 - Durée de vie
 - Besoins en débit
 - Ex : *wearables* fitness, santé...
- Bluetooth Core : pile protocolaire largement adoptée par l'industrie
- Adaptation
 - Réduction de la consommation énergétique
 - Réduction du débit

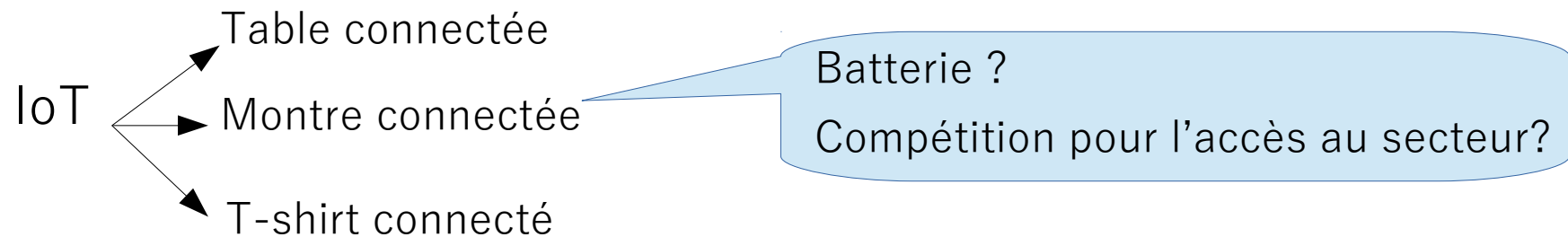
Bluetooth

Evolutions : *Backscatter*



Bluetooth

Evolutions : *Backscatter*



Signal propre



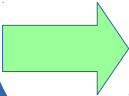
Réflexion de signaux existants

Transmission à la demande

Transmission opportuniste

Source d'énergie locale

Exploitation de signaux WiFi ambiants



« *Every smart phone is a backscatter reader : Modulated backscatter compatibility with Bluetooth 4.0 Low Energy (BLE) devices* », J. F. Ensworth, M. S. Reynolds, IEEE International Conference on RFID, 2015

A green arrow points from the left towards the citation text.

Sommaire

1.Introduction

2.Bluetooth

3.IEEE 802.15.4 / ZigBee

4.Conclusion

IEEE 802.15.4 / ZigBee

Origines et Objectifs

Besoins

- Connectivité sans fil faible portée
- Capteurs communicants
- Facteur de forme
- Énergie limitée : pile bouton...
- Maintenance minimale

Technologies disponibles

- Wi-Fi
- Bluetooth
- Infrarouge
- Solutions propriétaires et interopérabilité
- Nouveau standard ?

Couches hautes

Couches basses



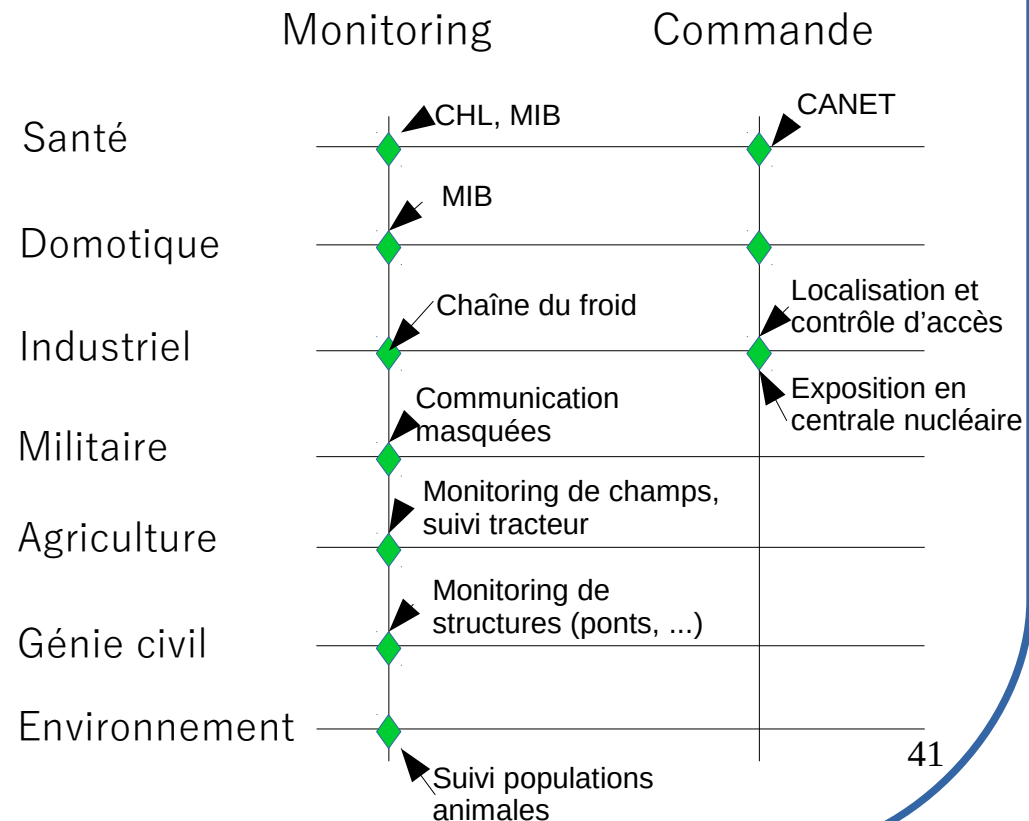
IEEE 802.15.4 / ZigBee

Origines et Objectifs

Objectifs

- Connectivité réseau faible/moyenne portée à bas débit
 - Collecte de données issues de capteurs
 - Portée : 10-30m en intérieur ; 150m en extérieur
- Autonomie énergétique
 - Maximiser durée de vie sur une pile bouton (années)
- Maintenance minimale et coût

Applications



IEEE 802.15.4 / ZigBee

Origines et Objectifs

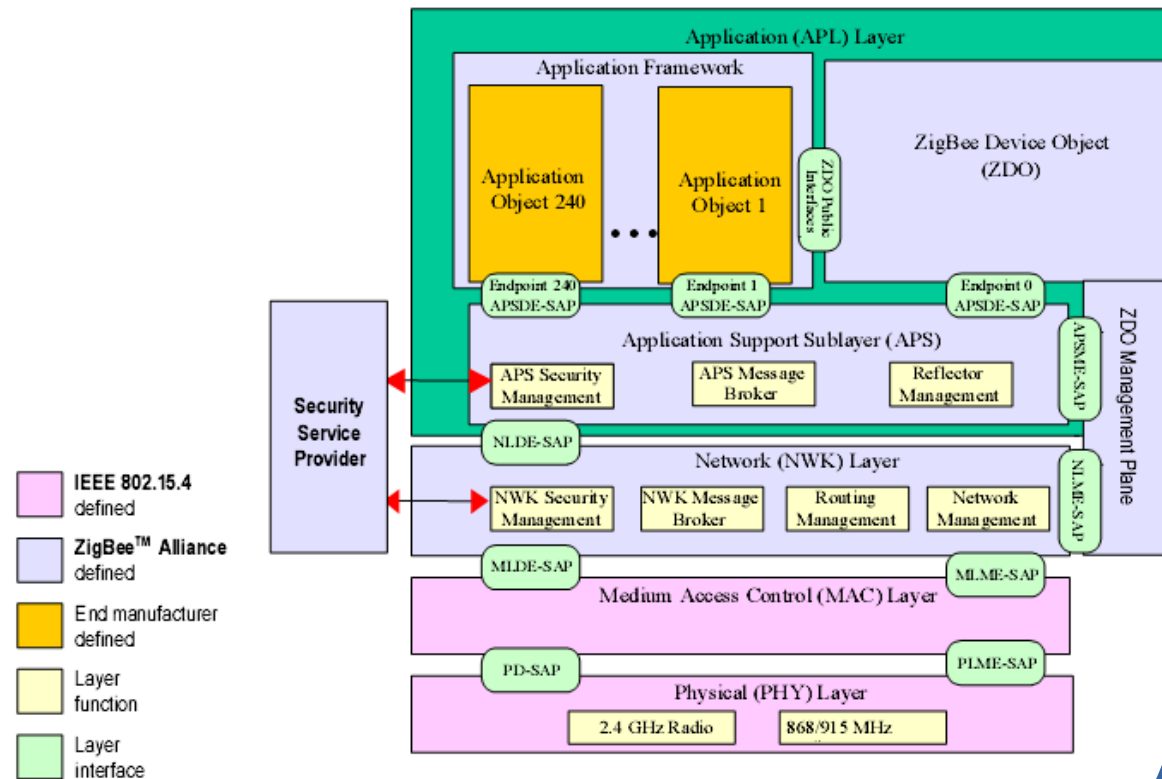
ZigBee

- Couches supérieures, de NWK à APP
- Support de différents profils applicatifs

Standard IEEE 802.15.4

- *Low-Rate Low-Power* WPAN
- Spécification couvrant les couches PHY et MAC
- *Wireless Sensor Network* et *Device Layer* de l'*Internet of Things (IoT)*

Pile protocolaire complète



IEEE 802.15.4 / ZigBee

Couche physique

Bandes de fréquence

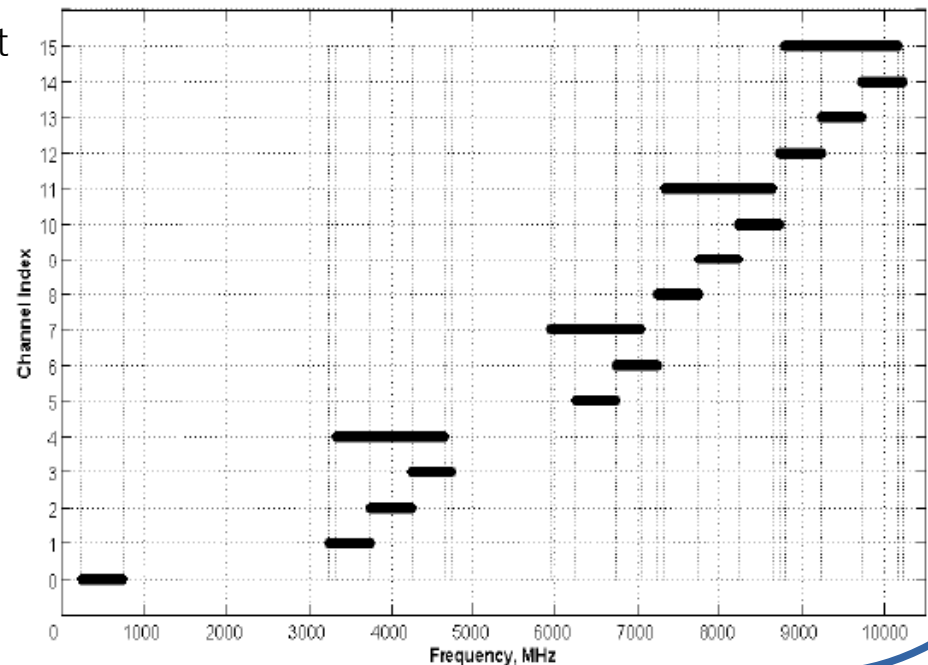
- 780MHz, 868MHz, 915MHz, 2.4GHz (ISM), 3-10GHz

Technologies courantes (portée, débit, largeur de bande, disponibilité, applications spécifiques)

- *Direct Sequence Spread Spectrum* (DSSS) : 250kb/s à 2,4GHz
- 16 Canaux de 5MHz

- *Chirp Spread Spectrum* (CSS) : 250kb/s ou 1Mb/s à 2,4GHz
- 14 Canaux de 22MHz dont 3 sans recouvrement

- *Ultra-Wide Band* (UWB) : 3-10 GHz
- 16 canaux :
 - 1 canal à 499,2MHz
 - 4 canaux entre 3 et 5GHz
 - 11 canaux entre 6 et 10GHz
- Largeur de canal 499,2MHz ou 1,3GHz



IEEE 802.15.4 / ZigBee

Couche MAC

Types de nœuds

- *Full-function Device* (FFD)
 - Peut jouer les rôles de PAN *coordinator* et de *coordinator*
- *Reduced-function Device* (RFD)
 - Nœud d'extrémité
 - Ne peut être un coordinateur
 - S'associe à un unique coordinateur
 - Ressources de calcul minimales

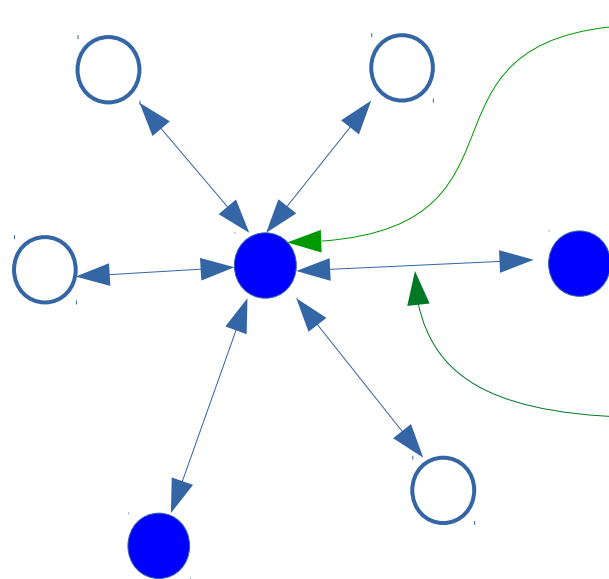


IEEE 802.15.4 / ZigBee

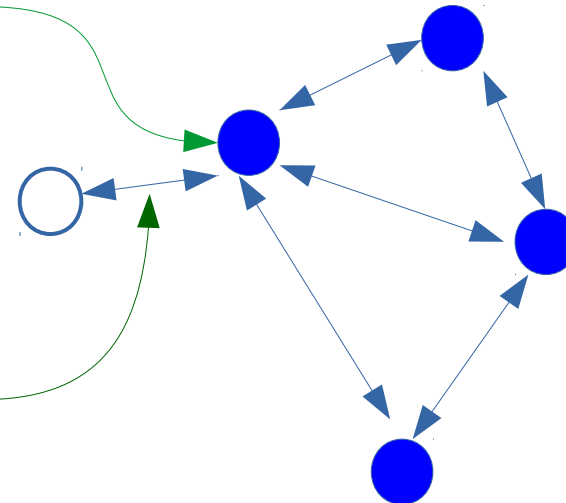
Couche MAC

Topologies

Étoile



Point-à-point



PAN coordinator

Communications

- Toutes les communications passent par le PAN-C
- Le PAN-C relaie les informations entre les nœuds

- Un lien de communication est possible dès que les nœuds sont à portée radio
- Possibilité de routage multi-sauts d'une source vers sa destination
- Peut aller vers un réseau *mesh*

IEEE 802.15.4 / ZigBee

Couche MAC

Méthodes d'accès

No-Beacon

- Le coordinateur écoute en permanence le réseau pour détecter des transmissions
 - Nécessite qu'il soit relié à une source d'énergie
- Utilisation d'une méthode d'accès de type CSMA/CA + RTS/CTS
 - Écoute du support avant d'émettre
 - Utilisation d'espaces de temps entre les trames
 - Acquiescement systématique par la station réceptrice
 - RTS/CTS pour gérer les terminaux cachés
 - Dans cette solution les stations terminales peuvent se mettre en veille périodiquement mais pas le coordinateur

IEEE 802.15.4 / ZigBee

Couche MAC

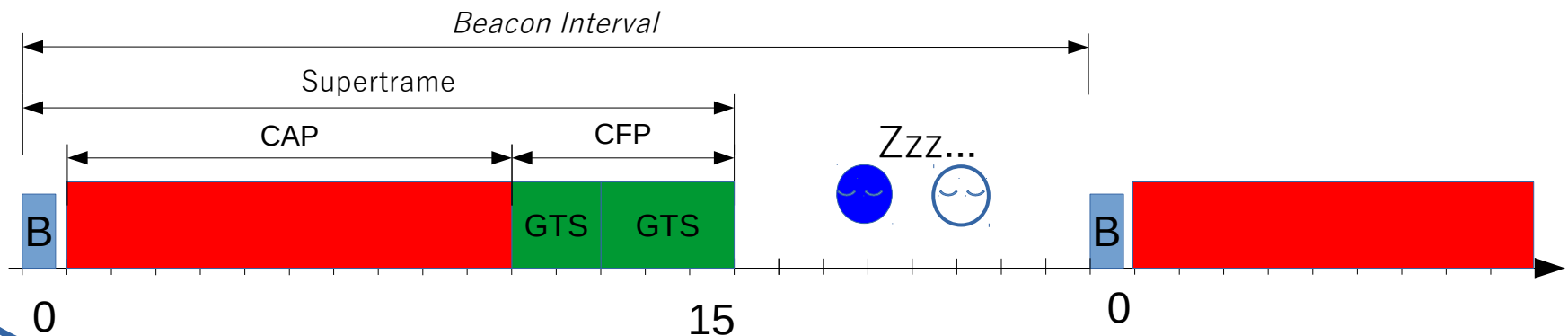
Méthodes d'accès

Beacon enabled

- Diffusion périodique de trames de signalisation (*beacon*)
 - Synchronisation
 - Allocation de ressources
- Structure temporelle
 - *Beacon Interval*
 - Supertrame de 16 slots
 - *Contention Access Period* (CAP)
 - *Contention Free Period* (CFP)
 - Sommeil et économie d'énergie

Compétition pour l'accès au médium avec CSMA/CA

Division en *Guaranteed Time Slots* (GTS), réservés chacun à un nœud

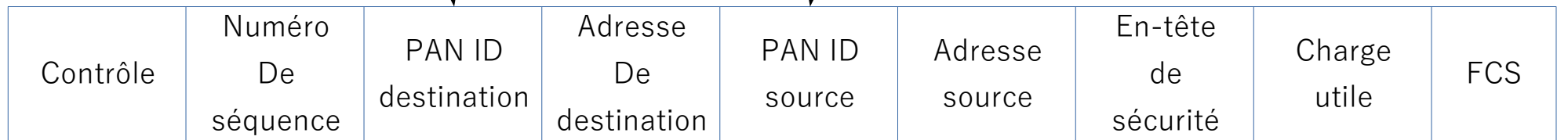


IEEE 802.15.4 / ZigBee

Couche MAC

Format et types de trames

- ID du réseau
- Peut être résumé pour des communications intra-PAN



- Type de trames
 - Beacon
 - Données
 - Commandes
- ACK/No-ACK ?
- Mode d'adressage

- EUI 64 bits
- *Short address* 16 bits

Contrôle
d'intégrité de
la trame

IEEE 802.15.4 / ZigBee

de → à →

Réseau de capteurs « non-hobbyist »

- 1 couche PHY
- 1 couche MAC compatible *mesh*
- 1 couche NWK avec routage sur *mesh*
- 1 syntaxe standardisée au niveau application

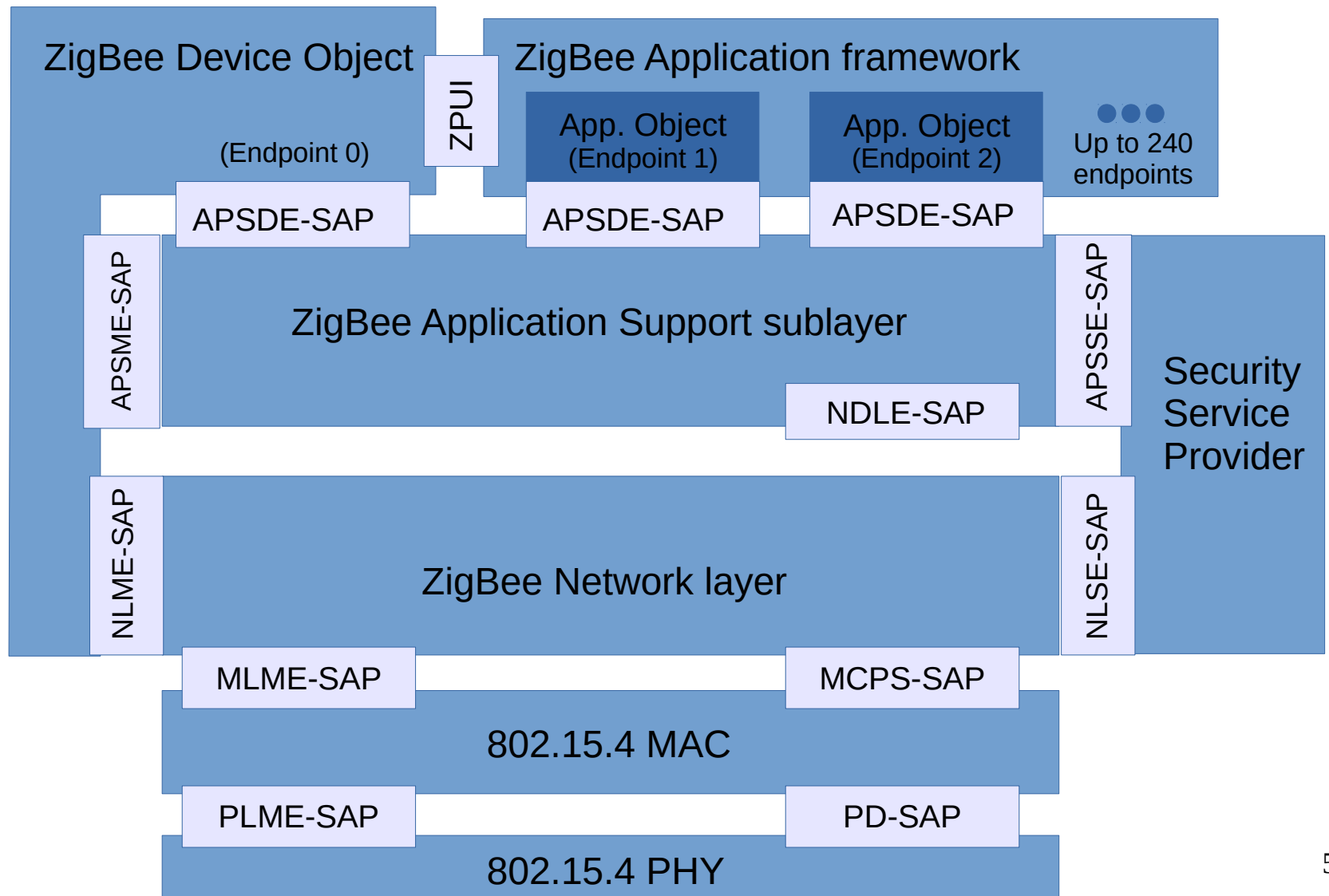
IEEE 802.15.4

ZigBee

Empilez, raccorder les *Service Access Points* et servez !

IEEE 802.15.4 / ZigBee

Architecture protocolaire



IEEE 802.15.4 / ZigBee

Couche NWK

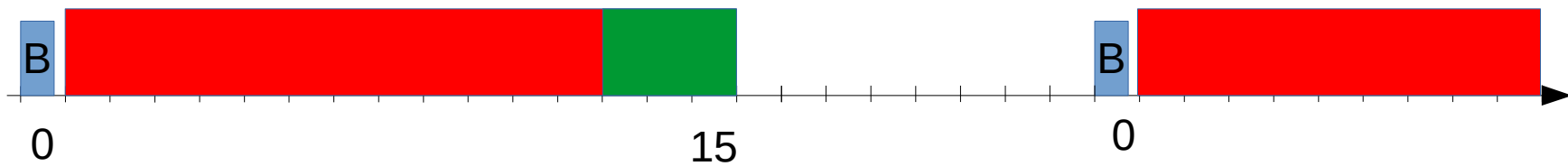
Responsabilités de la couche réseau

- Initiation du réseau
- Association ou retrait d'un nœud dans le réseau
- Découverte de route
- Mise en place de la sécurité via le module de sécurité
 - Cryptage AES (*Advanced Encryption Standard*) 128bits
 - Pas d'échange de clés
- Assignation des adresses si le nœud est un coordinateur
 - Utilise un adressage réseau sur 16 bits
 - 2^{16} nœuds supportés en théorie
 - En pratique pour des raisons d'accès au canal on estime qu'un réseau en étoile peut supporter 2000 nœuds
 - 256 sous-réseaux possibles (ou clusters)

IEEE 802.15.4 / ZigBee

Couche NWK

Création du réseau : utilisation de fonctionnalités de MAC et PHY



Démarrage d'un FFD

Scan des canaux de fréquence

Si aucun PAN détecté, prise de rôle : PAN-C

Transmission périodique de *beacons*



Démarrage d'un RFD

Scan des canaux de fréquence



Détection d'un PAN par ses *beacons*

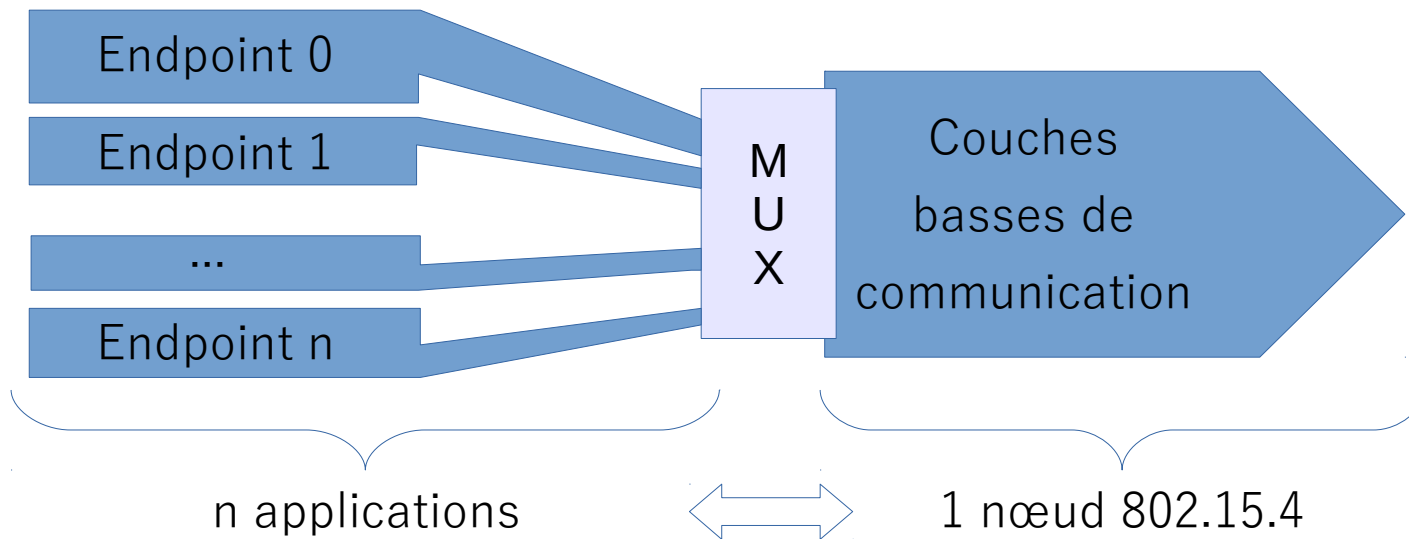
Lancement d'une procédure d'association

Échange de trames avec le FFD de rattachement

Éventuellement, demande de GTS

IEEE 802.15.4 / ZigBee

Sous-couche Application Support (APS)



Ex : un nœud ZigBee supportant
une lampe à variateur

IEEE 802.15.4 / ZigBee

Profils ZigBee

Utilisations

Domotique ou *Home Automation* (HA)

Sécurité, contrôle d'éclairage, contrôle d'accès

Immotique ou Commercial *Building Automation* (CBA)

Sécurité, contrôle d'éclairage, contrôle d'accès, relevé de compteur

Surveillance d'installation industrielle ou *Industrial Plant Monitoring* (IPM)

Gestion des biens, contrôle de processus, contrôle environnemental, gestion de l'énergie

Application des télécommunications ou *Telecommunications Applications* (TA)

Livraison d'informations dans les zones à risques, enquêtes publiques, télécommandes...

Solutions de comptage automatique ou *Automatic Metering Initiative / Smart Energy 1* (AMI ZSE1)

Gestion de la consommation d'énergie, production de relevés de consommation

Soins à domicile ou à l'hôpital ou *Personal Home and Hospital* (PHHC)

Surveillance d'un patient, surveillance de la forme physique

IEEE 802.15.4 / ZigBee

WSNs et localisation

Où est ma montre ?
Où sont mes clés ?
Où est l'employé ?
Où est le pompier ?

Localisation

- Peu gourmande en énergie
- Efficace en indoor
- Précise (sub-room level)

