



## **IEEE 802.15.4 & ZigBee<sup>®</sup>**

### **Profils et applications**

*S. Besson, N. Brasseur, S. Lenain, A. Donezar Ibañez*

*Evaltech - ESEO, 10 Boulevard Jeanneteau – BP 30926 - 49100 Angers - [www.eseo.fr](http://www.eseo.fr)*

- ✓ **Introduction**
- ✓ Généralités
- ✓ IEEE 802.15.4
  - ✓ PHY
  - ✓ MAC
- ✓ ZigBee
  - ✓ NWK
  - ✓ APL

ZigBee est une spécification d'un protocole haut-niveau utilisant des systèmes radio de faible puissance basés sur la norme IEEE 802.15.4 pour des réseaux sans fils de proximité (WPAN).

ZigBee est destiné aux applications RF qui nécessitent:

- Un faible débit
- Un réseau qui peut être sécurisé
- Une autonomie énergétique (à l'échelle de la durée de vie du produit). Emission de trame pour l'applicatif

L'Alliance ZigBee fournit :

- Les spécifications
- Les profils d'application
- Les tests de conformité et de certification.

## L'Alliance ZigBee:

- C'est une association à but non lucratif créée en 2002
- Elle est principalement constituée d'entreprises
- Elle a pour mission de développer des normes qui doivent « offrir plus de liberté et de flexibilité pour un monde plus intelligent et durable ». Zigbee doit donc:
  - Fournir des normes à l'échelle internationale de réseaux faible consommation axés sur les applications de surveillance, de contrôle et de capteurs
  - Permettre aux produits , à partir de ces normes, de fonctionner pendant plusieurs années sur batteries ou avec des systèmes de récupération d'énergie
  - Relier des dispositifs différents sur un seul réseau
  - Offrir une variété de fonctionnalités pour assurer la communication dans n'importe quel environnement (mesh networking...)
  - Etre simple à configurer et doit être sans maintenance pendant plusieurs années

L'Alliance ZigBee comporte plus de 375 membres.

L'Alliance est composée de trois types de membres.

- Promoteurs (13) (représentés au directoire)

**ember**

**EMERSON**

**freescale**  
semiconductor

**legrand**

**Itron**

**Kroger**

Landis  
Gyr  
manage energy better

**PHILIPS**

**Reliant**  
Energy

**Schneider**  
Electric

**ST**

**TEANDRIL**  
The Power is Yours

**TEXAS**  
INSTRUMENTS

- Participants (175)(rôles actifs sur le développement de ZigBee et droit de vote dans les groupes de travail) dont:
  - Analog Devices
  - Atmel
  - Cisco
  - Digi
  - Intel
  - Microchip
  - NXP
  - Panasonic
  - Pioneer
  - Renesas
  - Samsung
  - Siemens
  - Sony
  - Whirlpool
- Utilisateurs (Adopters) (ex: Freebox)

Pour devenir membre :

- 50000 \$US/an pour le grade promoteur
- 9500 \$US/an pour le grade participant
- 3500 \$US/an pour le grade utilisateur + frais d'administration pour les produits certifiés de 1000 \$US pour le premier produit et 500 \$US pour chaque nouveau produit.

Pour certifier un produit ZigBee:

- Il faut utiliser une plateforme conforme ZigBee (802.15.4 + pile ZigBee)
- Passer une certification du produit (application sur la plateforme)
- Etre membre.

ZigBee, basé sur la norme IEEE 802.15.4, est donc principalement dédié aux domaines d'application suivants:

- l'automatisation de bâtiment en réseau pour l'électronique grand public
- la gestion et l'efficacité énergétique
- l'automatisation industrielle
- le monitoring
- la domotique
- la santé





- ✓ Introduction
- ✓ **Généralités**
- ✓ IEEE 802.15.4
  - ✓ PHY
  - ✓ MAC
- ✓ ZigBee
  - ✓ NWK
  - ✓ APL

Zigbee est construit sur le model OSI où les couches PHY et MAC sont assurées par la norme IEEE 802.15.4 dont les caractéristiques principales sont les suivantes:

- Vitesses de transmission 250 kb/s, 100kb/s, 40 kb/s, et 20 kb/s
- Topologie peer to peer (support mesh pour ZigBee), étoile, cluster d'arbre,
- Adressage 16 bits ou 64 bits (@MAC)
- Allocation optionnelle de créneau temporel garanti (GTSS)
- Accès au canal de transmission avec évitement de collision (CSMA-CA)
- Acquittement possible de l'ensemble des transmissions
- Basse consommation
- Détection d'énergie (ED)
- Indication de qualité de connexion (LQI)

Deux types de dispositif radio peuvent communiquer sur un réseau IEEE 802.15.4 :

- FFD (Full Function Device) qui est capable de relayer des messages :
  - Il peut être désigné ou se désigner coordinateur du réseau (c'est-à-dire, le contrôleur principal du PAN (Personal Area Network))
  - Il est désigné comme coordinateur (rôle de routeur pour ZigBee)
  - Il peut effectuer le rôle d'un RFD
- RFD (Reduced Function Device) :
  - Il ne peut pas devenir coordinateur
  - Il est le dispositif de fin de réseau (rôle en ZigBee)

Un FFD peut échanger avec l'ensemble des RFDs du PAN ou avec d'autres FFDs.

Un RFD peut échanger uniquement avec un dispositif de type FFD.

## Définition:

Deux dispositifs ou plus étant dans un environnement personnel communicant (POS) et sur le même canal forment un LR-WPAN.

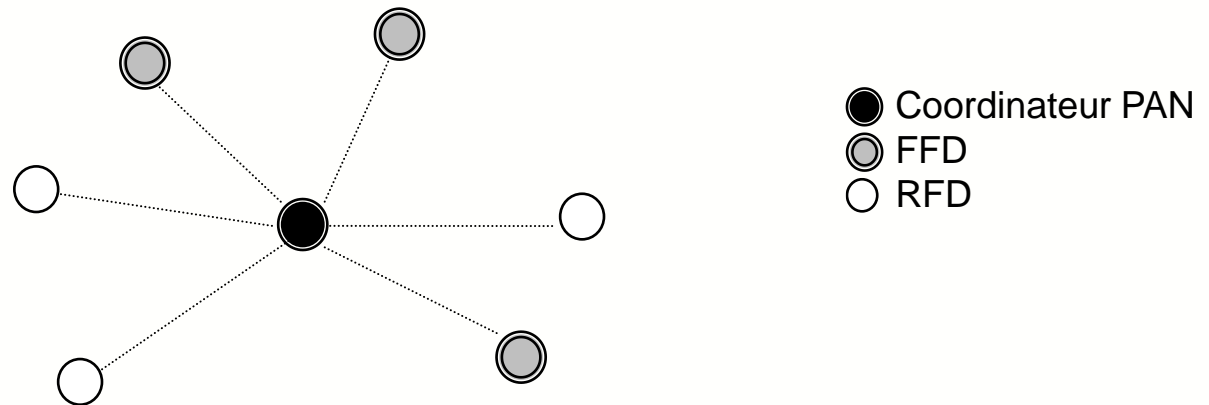
Ceci inclut donc au minimum :

- Un FFD qui joue le rôle de coordinateur du PAN
- Un end device (RFD ou FFD).

Chaque dispositif peut utiliser son adresse 64 bits pour communiquer à travers le réseau, ou une adresse courte (16 bits) peut lui être donnée par le coordinateur quand le dispositif est associé au réseau.

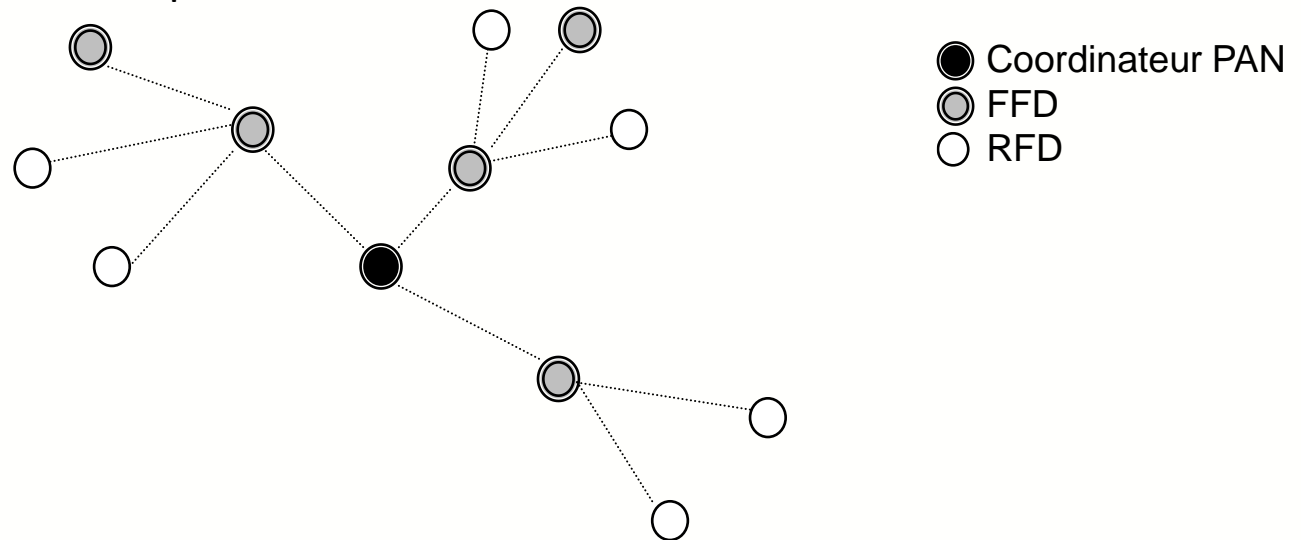
Dans ce cas, le coordinateur met à jour une table qui associe respectivement l'adresse 64 bits à l'adresse 16 bits de chacun des dispositifs radio associés au PAN.

La topologie étoile est contrôlée par un coordinateur (FFD). Les end devices (RFDs) ou les FFDs, communiquent directement avec le coordinateur.



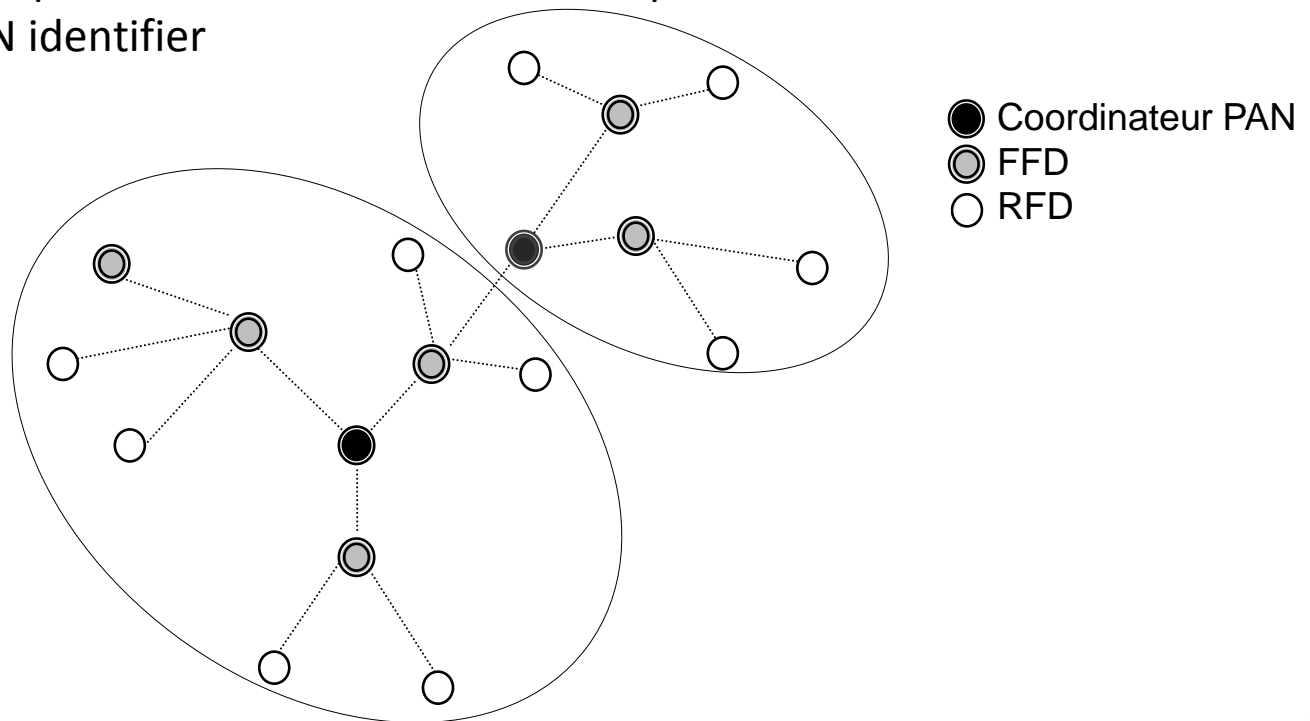
Le coordinateur initie et maintient le réseau. Il route aussi les messages. C'est une topologie simple à faible latence.

La topologie arbre (cas particulier du peer to peer) se construit autour d'un coordinateur. Celui-ci initie le réseau. Les dispositifs (FFD ou RFD) transmettent leurs messages aux routeurs (FFD) qui transmettent les données et contrôlent les messages en utilisant une stratégie de routage hiérarchique.



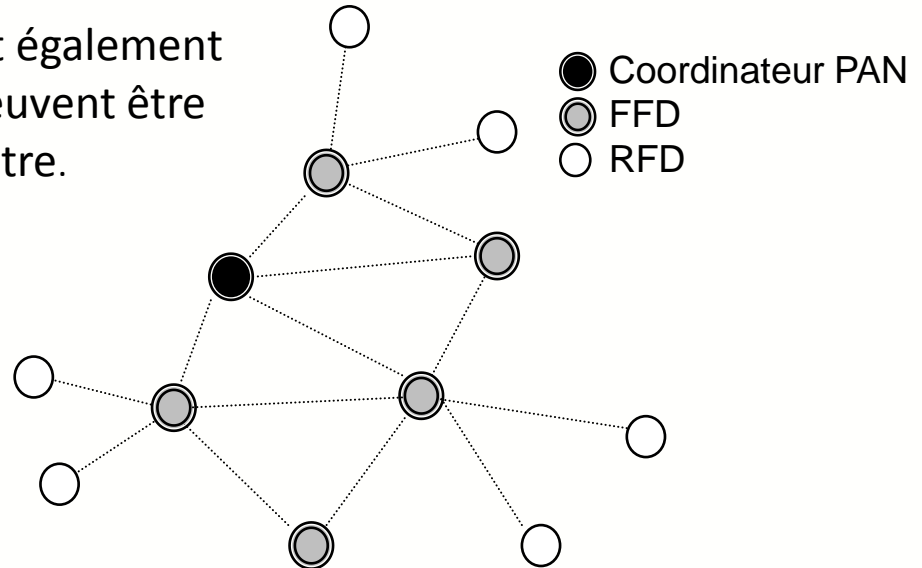
Cette topologie n'est pas toujours appropriée pour des applications à faible latence.

Dans une topologie multi-clusters tree, le premier coordinateur peut charger un FFD de devenir un coordinateur d'un nouveau cluster adjacent. Ce coordinateur monte à son tour son réseau. Son parent est le routeur le liant au premier coordinateur. Ces réseaux ont chacun leur PAN identifier



Cette topologie n'est pas toujours appropriée pour des applications à faible latence.

La topologie maillée (mesh) se construit également autour d'un coordinateur. Les messages peuvent être routés de n'importe quel dispositif à un autre.



Chaque FFD est un routeur pour les dispositifs voisins.

Choix de la meilleure route entre deux dispositifs peut être déterminé avec l'algorithme de routage AODV (Ad hoc On Demand Distance Vector):

- Les réseaux maillés permettent une communication totale peer to peer
- Avantages : permet d'avoir un réseau robuste avec une restructuration dynamique mais il n'est pas toujours approprié pour des applications sous batterie.



ZigBee est un réseau « self-forming »:

Dans un réseau mesh, le premier FFD qui démarre peut se déclarer PAN coordinateur et les autres dispositifs rejoignent le réseau en envoyant des requêtes d'association.

Zigbee est un réseau « self-healing »:

Dans un réseau mesh, il y a plus d'une route pour transmettre un message d'un dispositif à un autre. Quand la meilleure route n'est plus opérationnelle (obstacle à la transmission RF ou un défaut d'alimentation), le réseau peut sélectionner une autre itinéraire pour router le message.

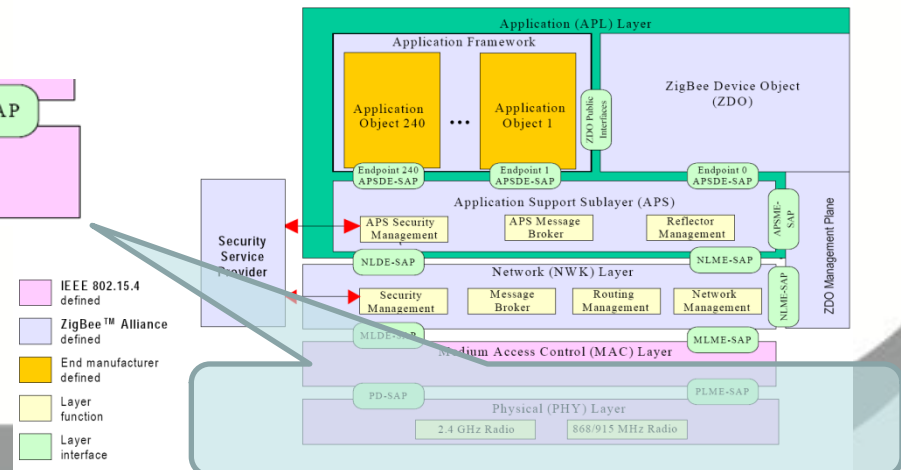
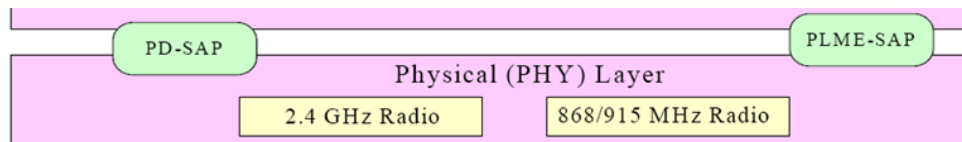
ZigBee est un réseau « ad-hoc »:

A opposer au réseau de type « infrastructure » où le point d'accès au routeur est désigné, ZigBee utilise un protocole réactif (ADOV) qui construit la table de routage lorsqu'un nœud en effectue la demande sans connaître la topologie du réseau

- ✓ Introduction
- ✓ Généralités
- ✓ **IEEE 802.15.4**
  - ✓ **PHY**
  - ✓ MAC
- ✓ ZigBee
  - ✓ NWK
  - ✓ APL

Les grandes fonctionnalités gérées par la couche physique de la norme IEEE 802.15.4 sont :

- L'activation et la désactivation du transceiver radio
- La détection d'énergie (ED)
- L'indication de qualité de connexion (LQI)
- L'évaluation d'un canal libre (CCA) pour CSMA-CA
- La sélection du canal
- La transmission et la réception de paquets à travers le medium physique



La norme IEEE802.15.4-2003 définit 27 canaux répartis sur 3 bandes de fréquence:

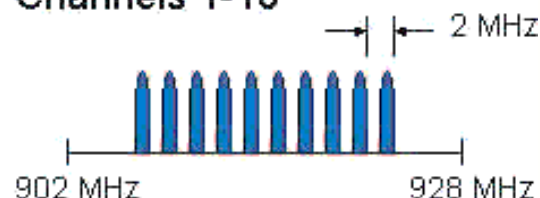
- 1 canal sur la bande 868 MHz pour l'Europe
- 10 canaux sur la bande 915 MHz pour l'Amérique du Nord
- 16 canaux sur la bande 2.450 GHz pour le monde

**868MHz/  
915MHz  
PHY**

Channel 0

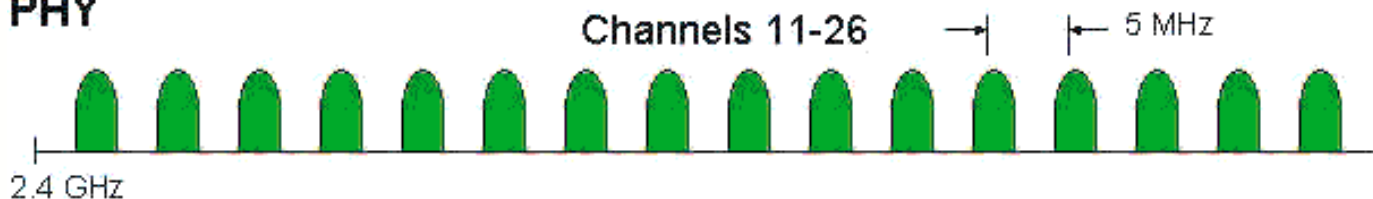


Channels 1-10



**2.4 GHz  
PHY**

Channels 11-26



Les normes IEEE802.15.4-2006 et IEEE802.15.4C-2009 offrent des débits supérieurs sur les bandes 700/800/900 MHz

Les puissances de transmission maximum autorisées sont:

Frequency band	Geographical region	Maximum conductive power/ radiated field limit	Regulatory document
2400 MHz	Japan	10 mW/MHz	ARIB STD-T66 [B22]
	Europe (except Spain and France)	100 mW EIRP or 10 mW/MHz peak power density	ETSI EN 300 328 [B26] and [B27]
	United States	1000 mW	Section 15.247 of FCC CFR47 [B29]
	Canada	1000 mW (with some limitations on installation location)	GL-36 [B32]
902–928 MHz	United States	1000 mW	Section 15.247 of FCC CFR47 [B29]
868 MHz	Europe	25 mW	ETSI EN 300 220 [B25]

## Détection d'énergie (ED) :

Cette fonctionnalité permet d'estimer l'énergie présente sur un canal donné. La valeur minimum estimable doit être au maximum 10 dB au dessus de la sensibilité du récepteur. L'étendue de mesure doit être d'au moins 40 dB avec une précision de +/- 6dB. Cette mesure est une moyenne de l'indication de force du signal reçu (RSSI) durant 8 périodes de symbole.

## Détection de porteuse (CS):

Comme la fonctionnalité précédente, la détection de porteuse permet d'évaluer la disponibilité d'un canal. Cette fonctionnalité par contre démodule le signal pour vérifier si le signal est conforme 802.15.4. Si tel est le cas, le canal est considéré occupé.

## Indicateur de qualité de connexion (LQI) :

Cette fonctionnalité permet d'estimer la force et/ou la qualité des paquets reçus.

Cette estimation utilise:

- la détection d'énergie (ED),
- une estimation du rapport signal/bruit , (« correlation value » sur les 8 premiers symboles reçus)
- Combinaison des deux méthodes

Cette mesure est faite à chaque réception de paquet et sous demande, le retour de cette information doit être un entier compris entre :

- 0x00 => la plus basse qualité de signal
- 0xFF => la plus haute qualité











Cette information doit contenir au moins 8 niveaux.

## RSSI vs LQI :

Le RSSI est une indication de force de signal reçu qui n'indique pas forcément une bonne qualité ou intégrité de ce même signal.

A l'inverse, LQI ne donne pas non plus une indication de la force du signal reçu.

### Exemple:

	RSSI	LQI
- Signal faible en présence de bruit		
- Signal faible avec absence totale de bruit		
- Signal non présent ou couvert par un fort bruit		
- Signal fort sans beaucoup de bruit		
- Signal fort saturant le récepteur		



## Evaluation de la disponibilité d'un canal (CCA) :

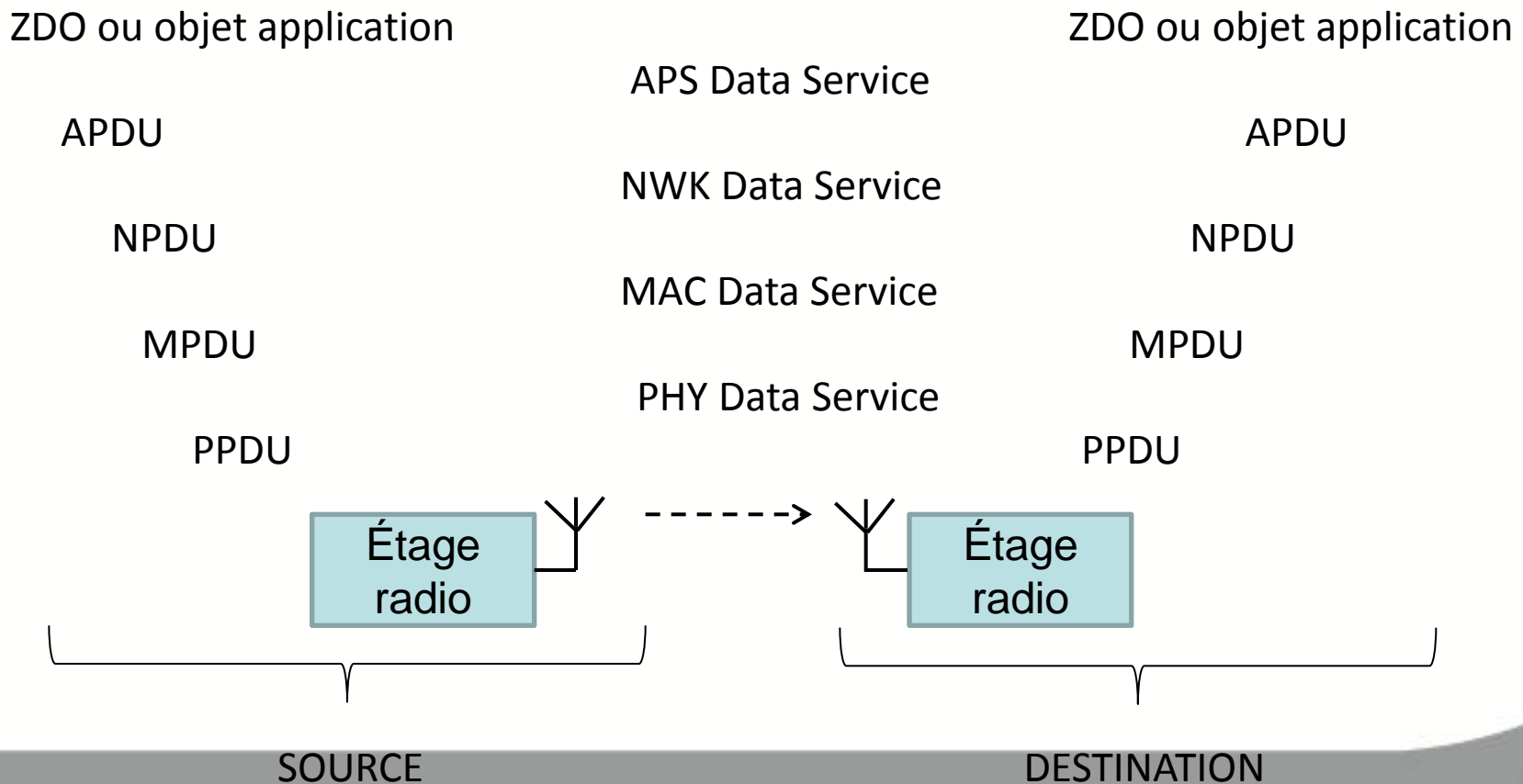
C'est la première étape du mécanisme CSMA-CA (accès multiple au medium avec détection de porteuse et évitement de collisions). Cette évaluation permet de savoir si un dispositif est déjà entrain d'émettre.

Un dispositif IEEE 802.15.4 doit pouvoir réaliser un CCA en proposant au moins un des 3 modes suivants:

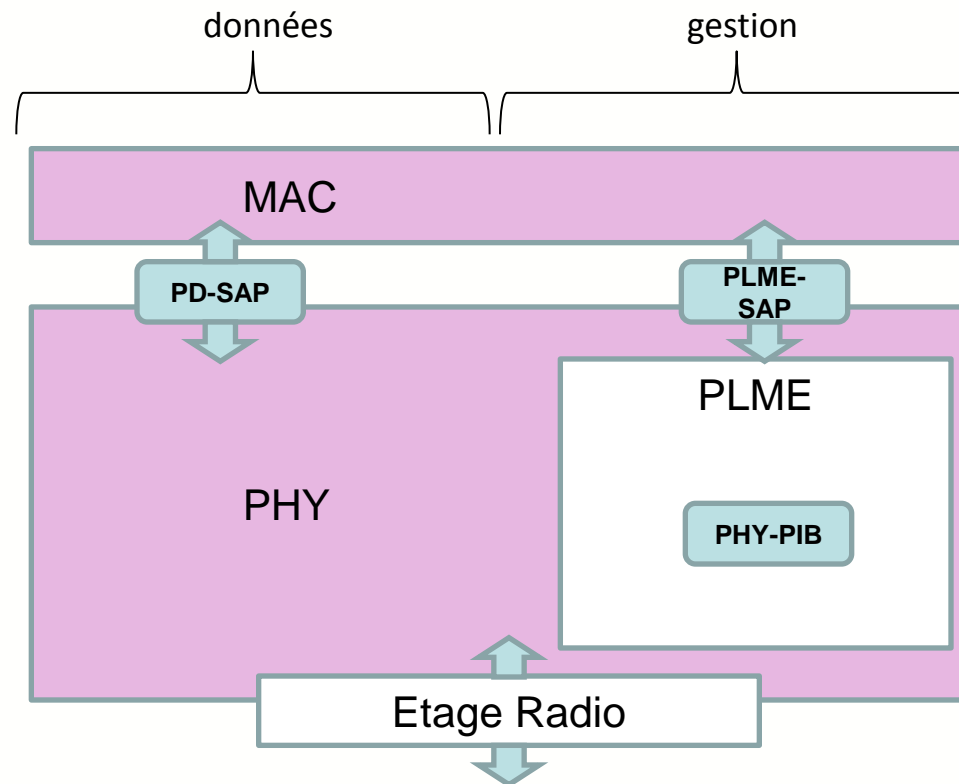
- CCA mode 1 : Energie au dessus du seuil de détection d'énergie
- CCA mode 2 : Détection de porteuse
- CCA mode 3 : Détection de porteuse et/ou au dessus du seuil de détection d'énergie

Le retour de cette fonctionnalité est canal libre ou occupé.

## Transfert de données à travers les couches:



## PHY Data Service et PHY Management Service :



La norme IEEE 802.15.4 et la spécification ZigBee utilisent le concept de primitives pour décrire les services qu'une couche fournit à la couche supérieure.

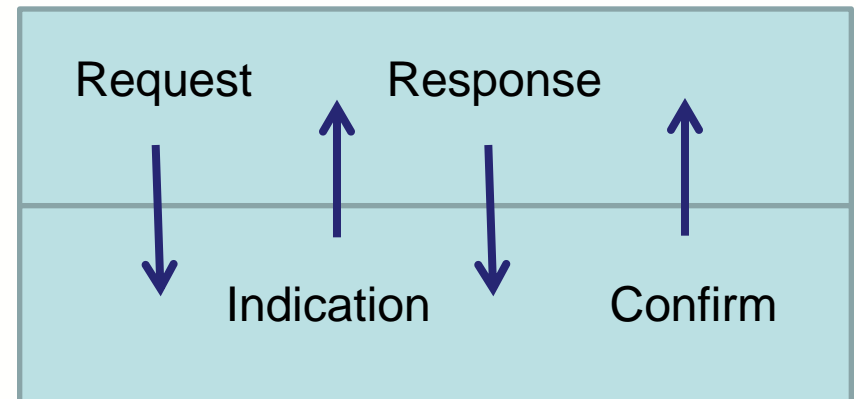
Les couches PHY, MAC et NWK fournissent des services aux couches supérieures. Ces couches partagent le même mécanisme pour le transfert d'une donnée:

Il y a quatre catégories de primitives de services:

- *<primitive>.request*
- *<primitive>.indication*
- *<primitive>.response*
- *<primitive>.confirm*

Couche N+1  
Service utilisateur

Couche N  
Service  
fournisseur



Exemple : La couche MAC souhaite que la couche PHY exécute une détection d'énergie

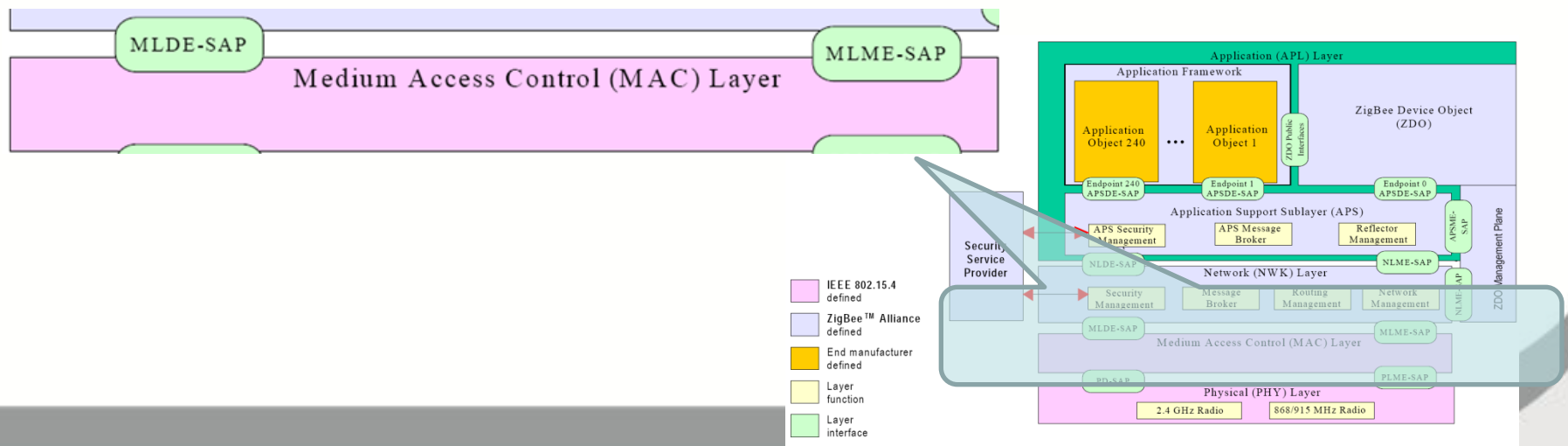
- MAC => PHY     *PLME-ED.request()*
- PHY => MAC     *PLME-ED.confirm(status, EnergyLevel)*

Name	Type	Valid range	Description
status	Enumeration	SUCCESS, TRX_OFF, or TX_ON	The result of the request to perform an ED measurement.
EnergyLevel	Integer	0x00-0xff	ED level for the current channel. If status is set to SUCCESS, this is the ED level for the current channel. Otherwise, the value of this parameter will be ignored.

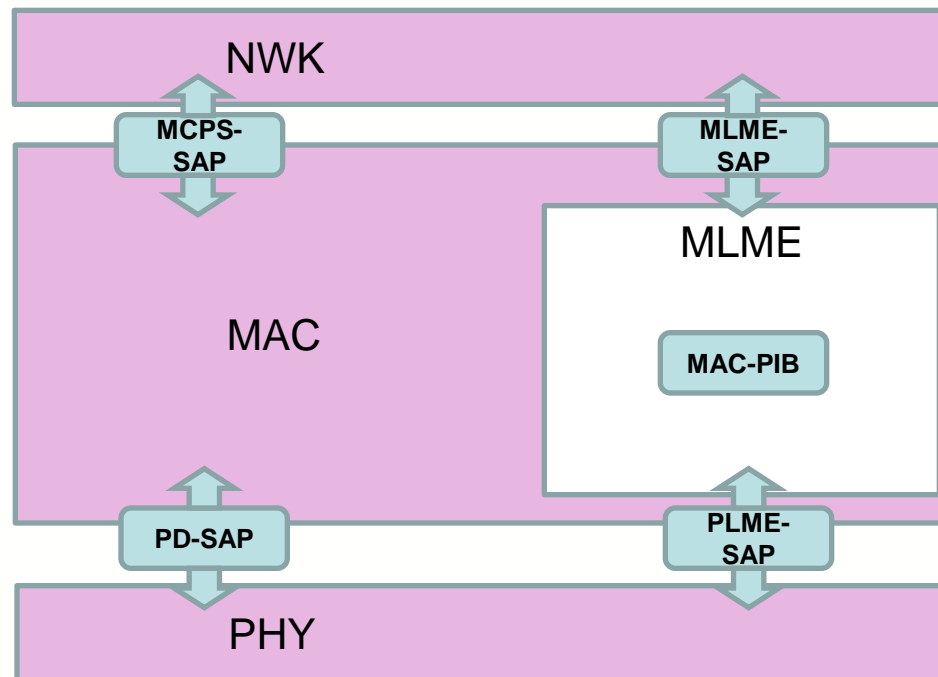
- ✓ Introduction
- ✓ Généralités
- ✓ **IEEE 802.15.4**
  - ✓ PHY
  - ✓ **MAC**
- ✓ ZigBee
  - ✓ NWK
  - ✓ APL

Les grandes fonctionnalités gérées par la couche MAC de la norme IEEE 802.15.4 sont :

- La gestion des beacons
- L'accès au canal avec le mécanisme CSMA-CA
- La gestion de la garantie d'un créneau temporel (GTS)
- La validation de trame
- L'acquittement de l'arrivée d'une trame
- L'association et la dissociation d'un dispositif

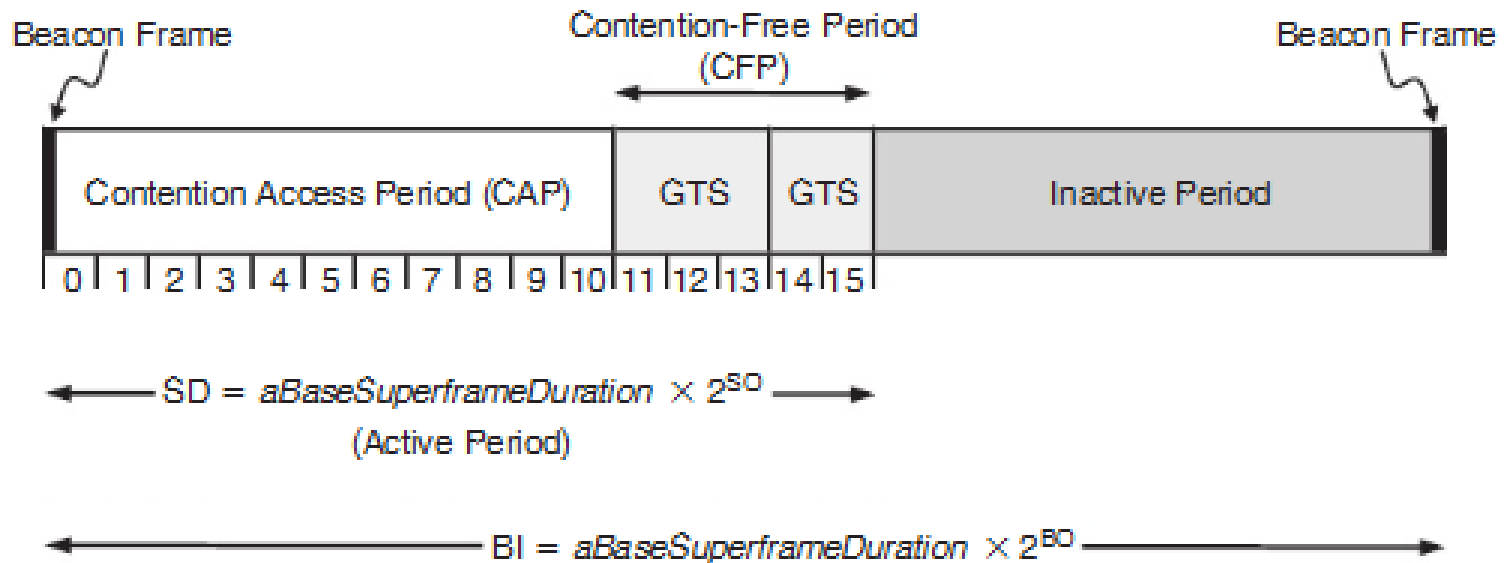


## MAC Data Service et MAC Management Service :



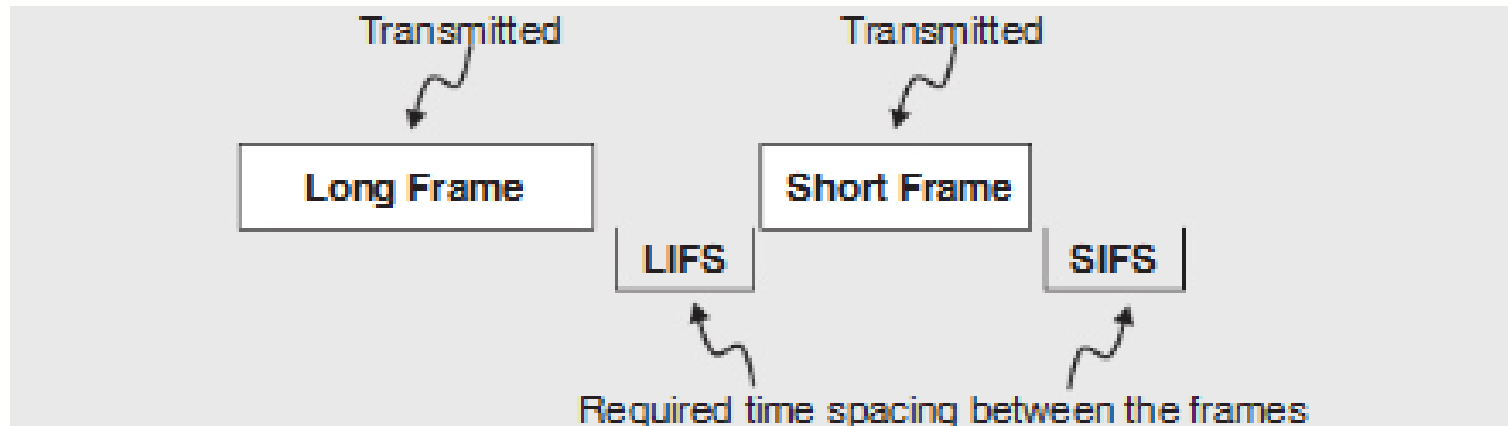
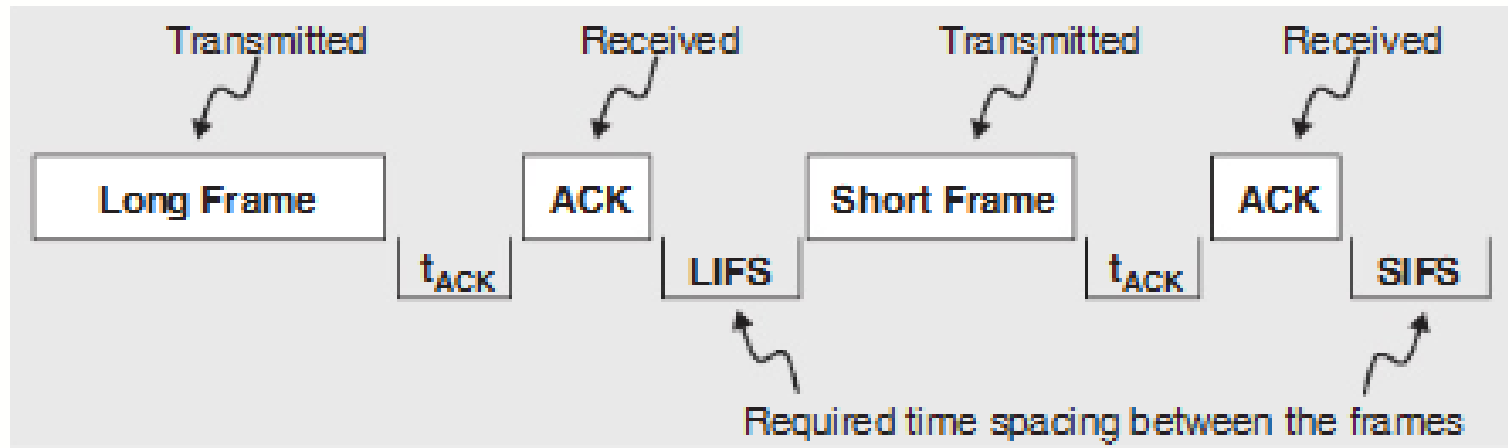


## Structure de la Super Trame



- Délimiter par deux trames MAC de type Beacon (trame balise)
- au plus 3 types de période:
  - Période active:
    - Période avec accès concurrent (CAP)
    - Période avec accès libre (CFP)
  - Période inactive

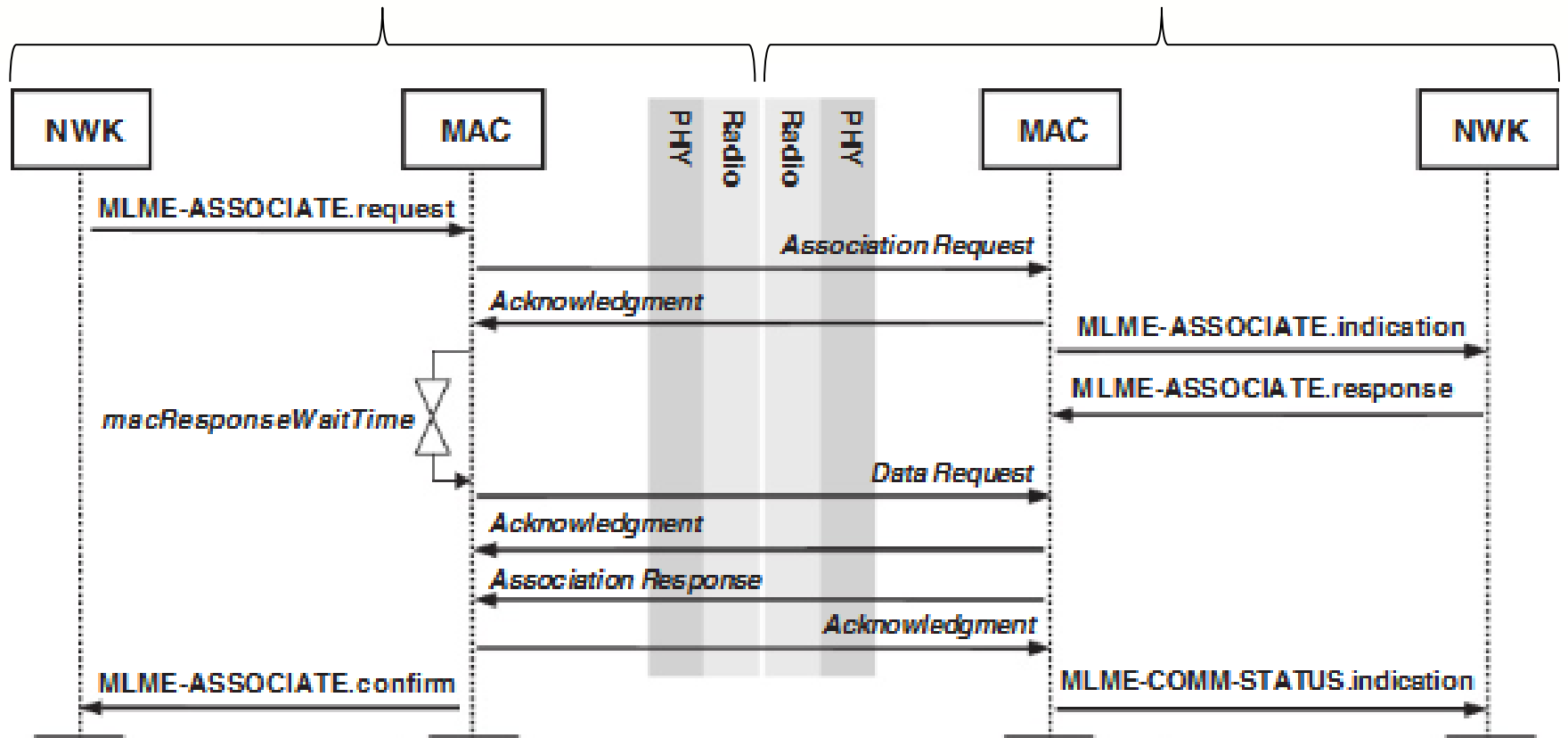
## Espacement entre les frames



## Association:

Dispositif souhaitant s'associer

Coordonateur



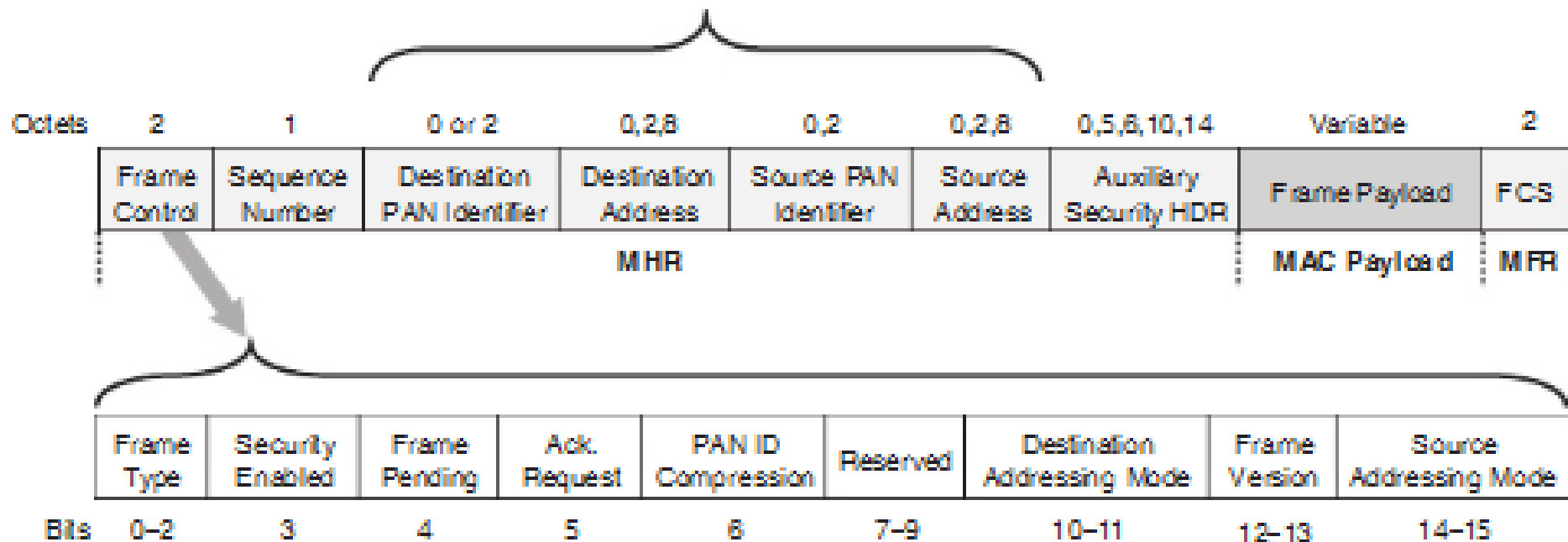
## Procédure de réalignement d'un dispositif orphelin

- Un dispositif qui était associé au réseau et qui a perdu son association est considéré comme orphelin (ce n'est pas le cas pour un dispositif qui s'est dissocié du réseau).
- Si un dispositif transmet une trame qui nécessite un acquittement et que celui-ci n'est jamais reçu, l'application peut déclarer le dispositif comme orphelin.

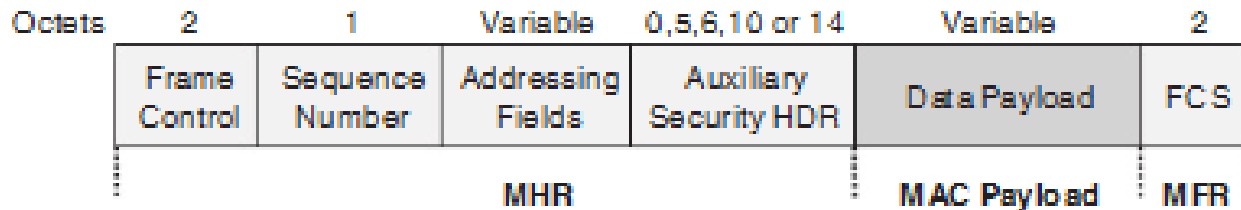
La couche réseau (NWK) a le choix entre deux procédures:

- Reset de la couche MAC et lancement d'une procédure d'association
- Lancement de la procédure de réalignement d'un dispositif orphelin.

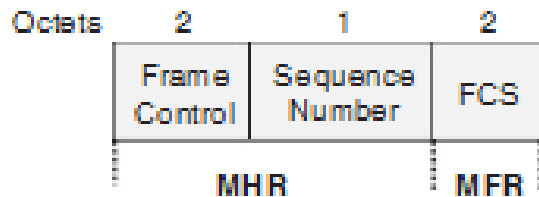
## Trame MAC générale



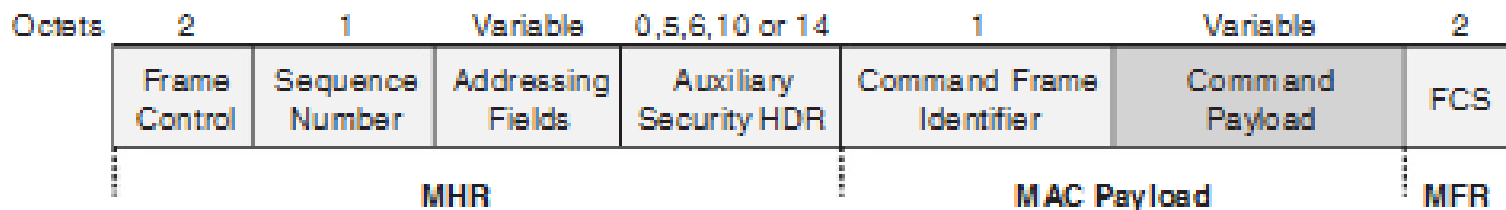
## Trame MAC de données



## Trame MAC d'acquittement



## Trame MAC de commande



## Identifiants des commandes MAC

Identifiant	Commande
0x0001	Association request
0x0002	Association response
0x0003	Disassociation notification
0x0004	Data request
0x0005	PAN ID conflict notification
0x0006	Orphan notification
0x0007	Beacon request
0x0008	Coordinator realignment
0x0009	GTS request

## Mode « Promiscuous »

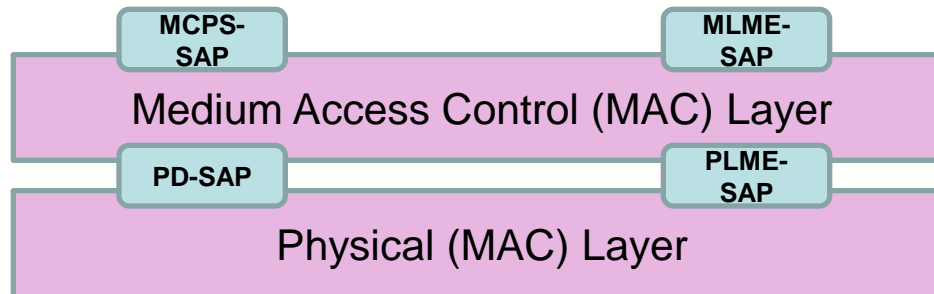
Ce mode permet de lire toutes les données reçues par un dispositif. Ce mode est utilisé pour du monitoring

*macPromiscuousMode* à TRUE



Les grandes fonctionnalités gérées par la norme IEEE 802.15.4 sont:

- La gestion des beacons
- L'accès au canal avec le mécanisme CSMA-CA
- La gestion de la garantie d'un créneau temporel (GTS)
- La validation de trame
- L'acquittement de l'arrivée d'une trame
- L'association et la dissociation



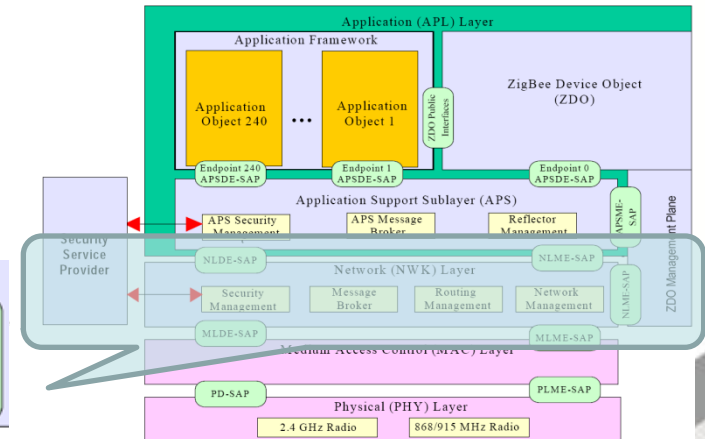
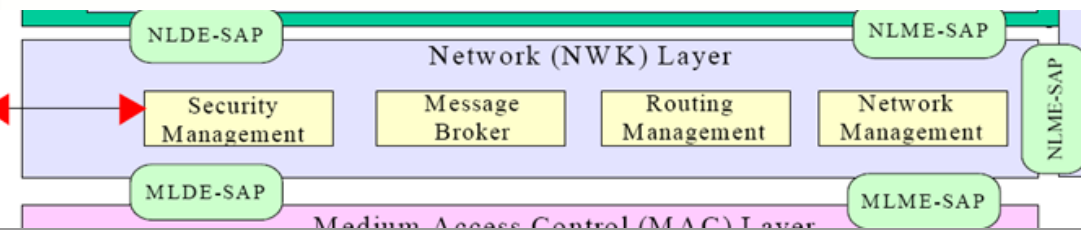
- L'activation et la désactivation du transceiver radio
- La détection d'énergie (ED)
- L'indication de qualité de connexion (LQI)
- La sélection du canal
- L'évaluation d'un canal libre (CCA)
- La transmission et la réception de paquets à travers le medium physique

- ✓ Introduction
- ✓ Généralités
- ✓ IEEE 802.15.4
  - ✓ PHY
  - ✓ MAC
- ✓ ZigBee
  - ✓ NWK
  - ✓ APL

Les grandes fonctionnalités gérées par la couche réseau de la spécification ZigBee sont :

- Démarrer un nouveau réseau
- La configuration d'un nouveau dispositif (opérer comme un coordinateur ou essayer de rejoindre un réseau existant)
- Joindre ou quitter un réseau
- Appliquer la sécurité au niveau de la couche réseau
- Router les trames\*
- Découvrir et maintenir les routes entre les dispositifs
- Découvrir les dispositifs pouvant être atteints directement
- Stocker les informations des dispositifs voisins
- Délivrer des adresses aux dispositifs rejoignant le réseau\*

\* (coordinateur Zigbee ou routeur (coordinateur 802.15.4))



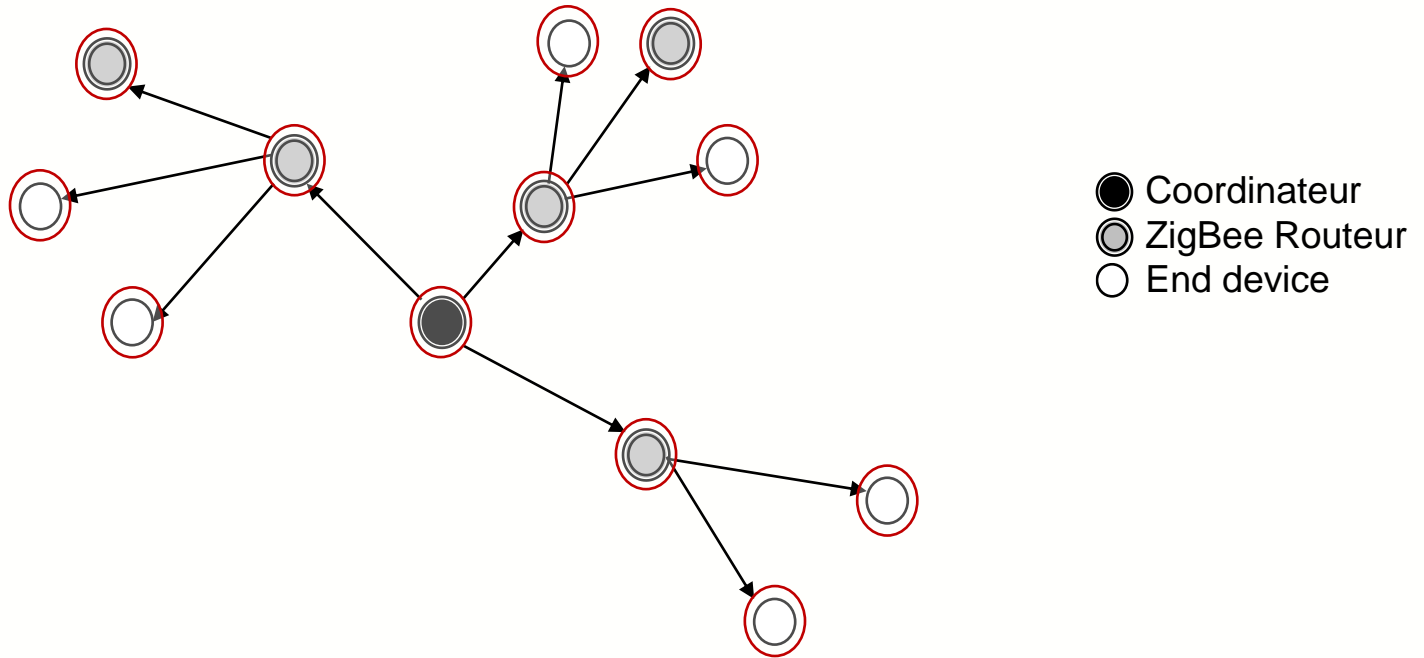
## Mécanisme de communication:

- @MAC  $\Leftrightarrow$  @NWK
- Paramètre radius : indique dans la trame le nombre de relais à effectuer

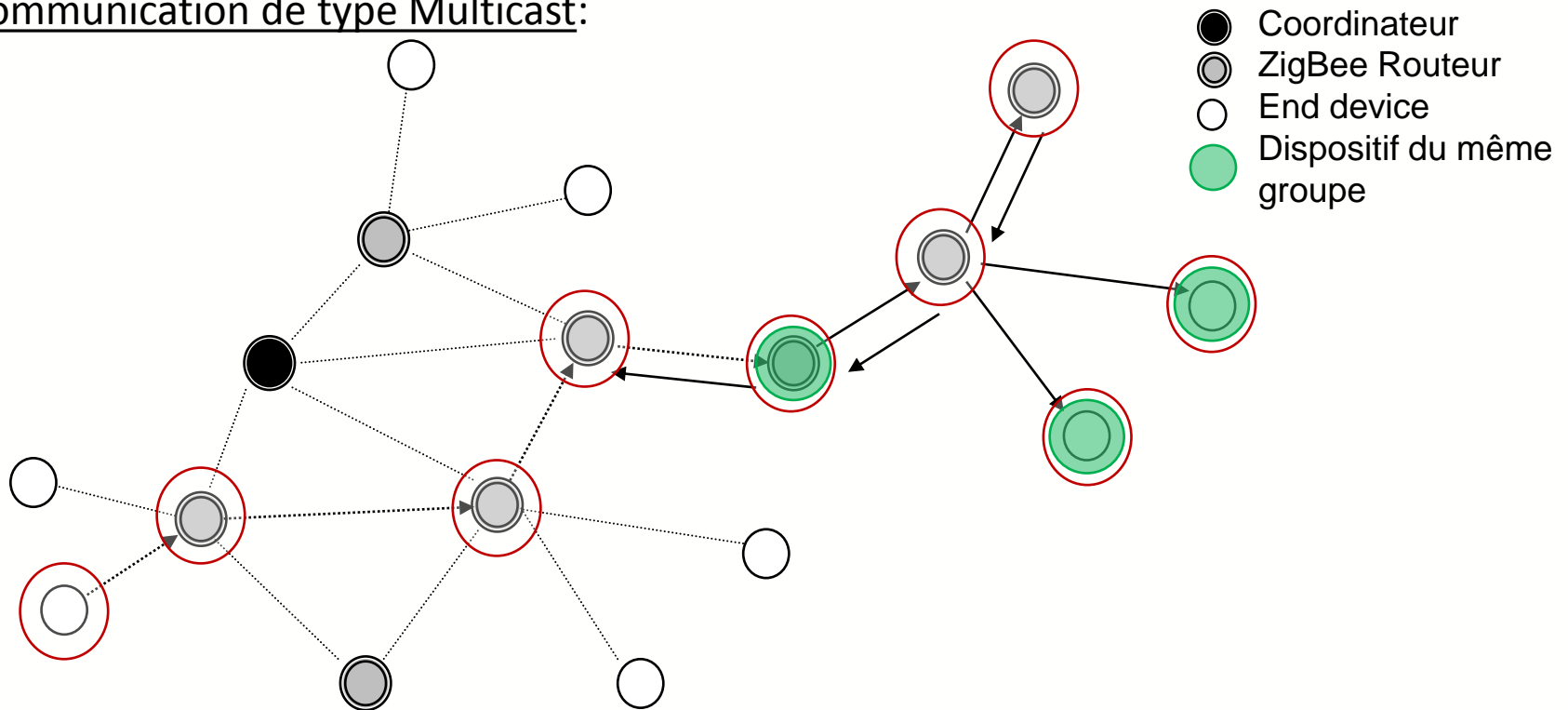
## 3 catégories de communication

- Broadcast
- Multicast
- Unicast

## Communication de type Broadcast:

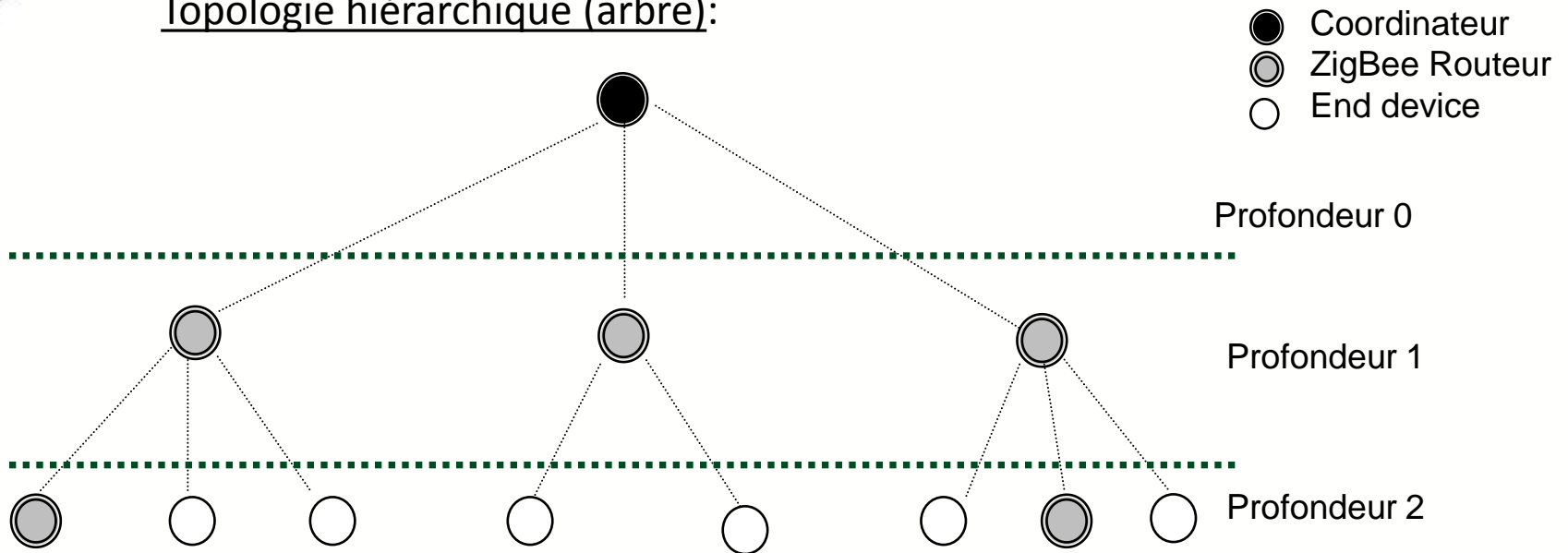


## Communication de type Multicast:



- Message à destination d'un groupe (même groupe ID)
- Braodcast à partir du premier membre du groupe

## Topologie hiérarchique (arbre):



- Adressage par défaut (profondeur et nombre maximum d'enfants)
- Distribution d'adresse(s) aux parents potentiels

## Routage:

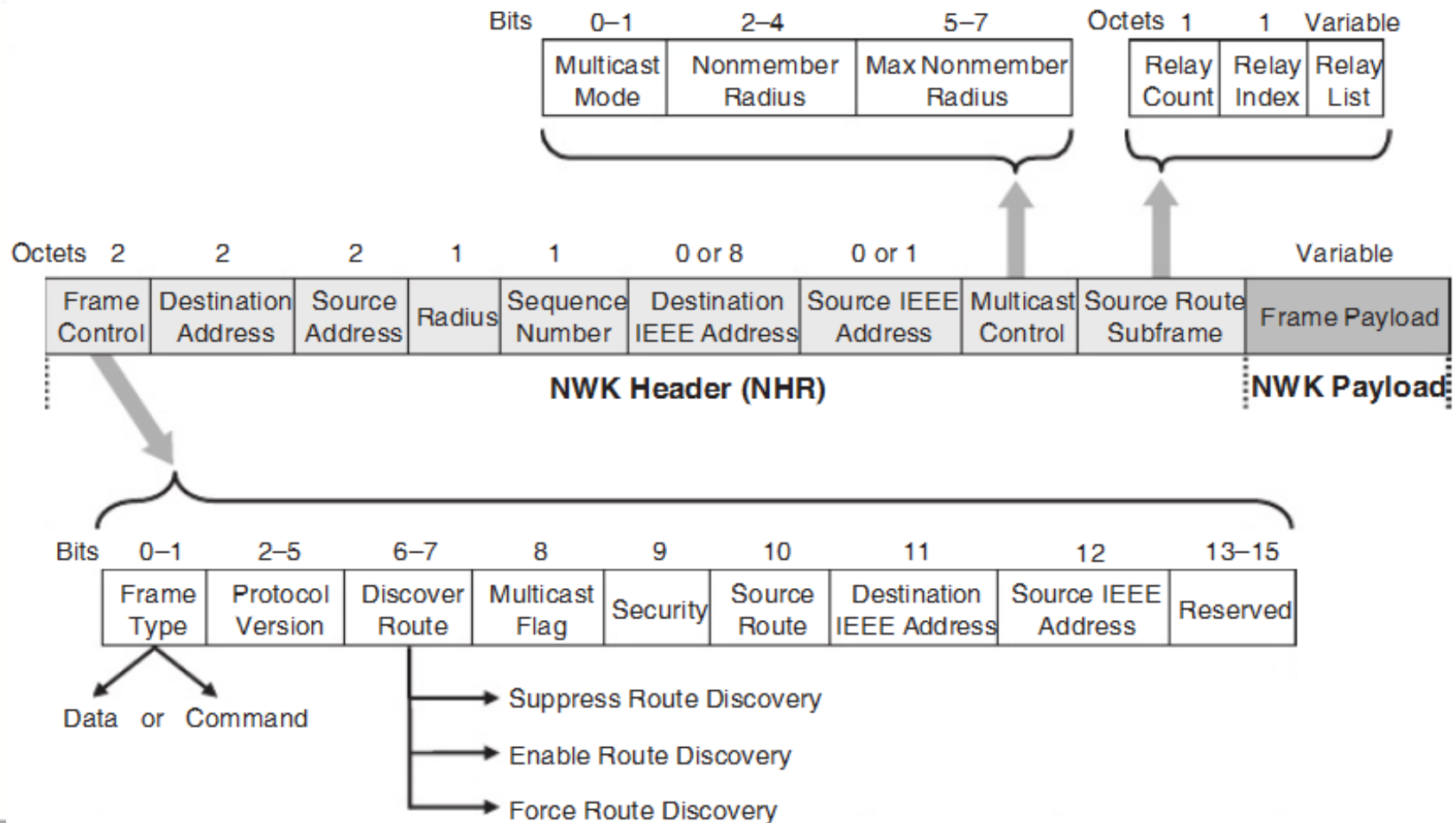
- Réaliser par le coordinateur ZigBee et les routeurs
- Un chemin est défini par:
  - Sa longueur (L) : nombre de dispositif
  - $\sum C(\text{lien}) \rightarrow$  coût entre chaque dispositif :
    - la probabilité d'un succès d'acheminement
    - $0 < C(\text{lien}) \leq 7$  (peut-être défini par une moyenne du LQI)
- Le coordinateur ZigBee et les routeurs tiennent à jour des tables de routage (@destination, .... Enregistrement de la route, @du prochain dispositif sur le chemin).
- Pour la découverte de nouvelles routes, une table de découverte de route est utilisée
- La table des voisins permet de connaître les liens entre les dispositifs du voisinage (type de dispositif, échec de transmission, LQI, lien de parenté,...)



## Structures des trames NWK

- Trame de beacon
- Trame de données
- Trame d'acquittement
- Trame de commande MAC

## Trame NWK générale

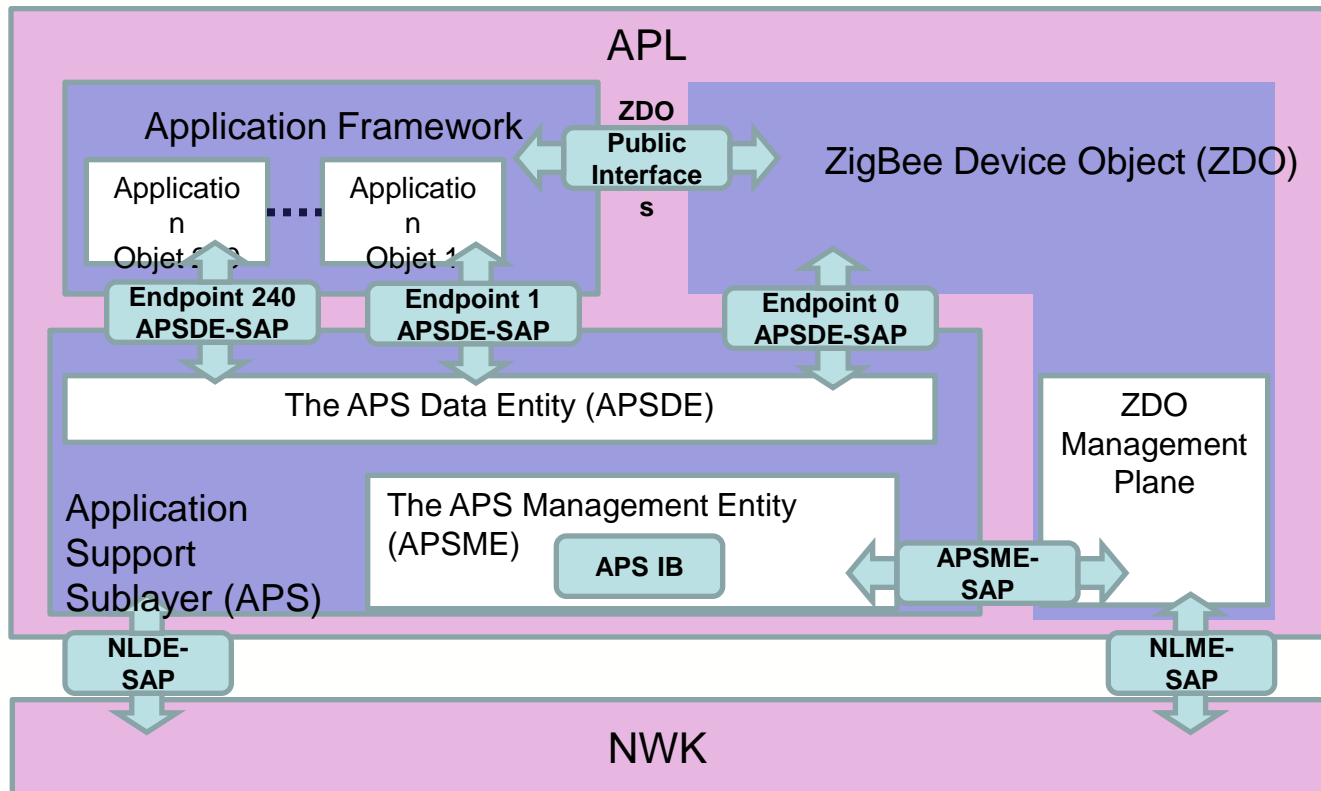


## Identifiants des commandes NWK

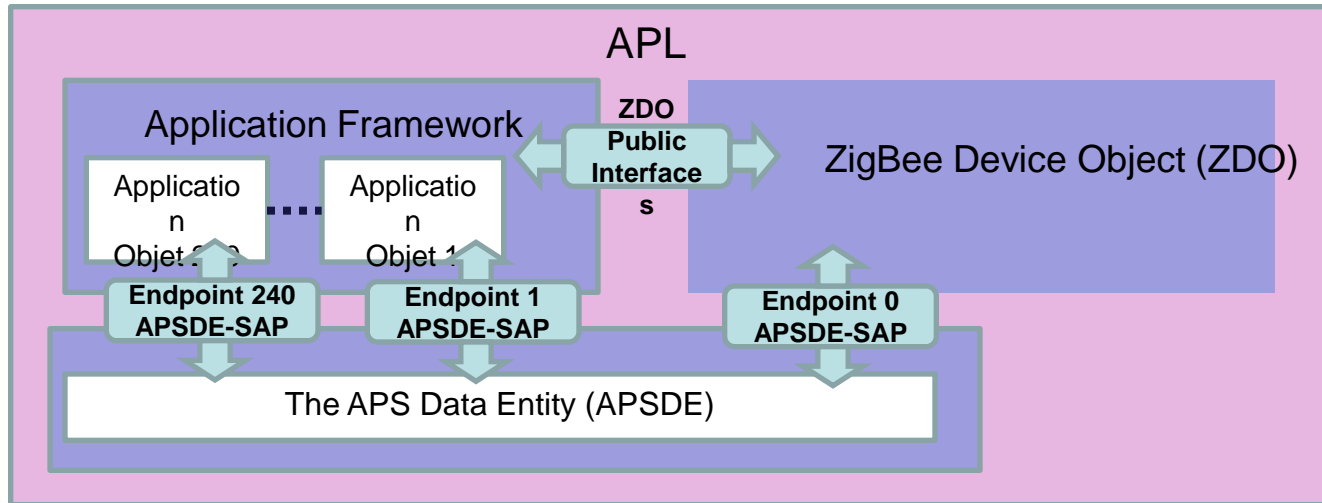
Identifiant	Commande
0x0001	Route request
0x0002	Route reply
0x0003	Route error (network status)
0x0004	Leave
0x0005	Route record
0x0006	Rejoin request
0x0007	Rejoin response
0x0008	Link status (ZigBee-Pro)
0x0009	Network report (ZigBee-Pro)
0x000A	Network update (ZigBee-Pro)

- ✓ Introduction
- ✓ Généralités
- ✓ IEEE 802.15.4
  - ✓ PHY
  - ✓ MAC
- ✓ ZigBee
  - ✓ NWK
  - ✓ APL

## Application Data Service et Application Management Service




## Application Framework



- Permet d'utiliser des profils d'application (profils ZigBee) (jusqu'à 240)
- Les profils d'application permettent l'interopérabilité entre des profils identiques utilisés par des produits de marques différentes (interrupteur et une lampe)
- L'identifiant d'un profil est délivré par l'Alliance ZigBee (entre 0x0000 et 0x7FFF, 0xC000 et 0xFFFF pour une application spécifique fabricant)
- Le nom d'un profil correspond à l'application (ex: Health Care, Consumer Electronics Remote Control CERC)

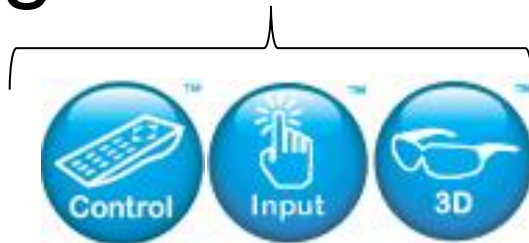
Les profils d'applications:

	RF4CE			PRO							IP		
Application Profile	ZRC	ZID	Z3S	ZLL 	ZHA <div>ZGP (optional)</div>	ZBA	ZTS	ZRS	ZHC	ZSE 1.X	ZSE 2.0		
Network	ZigBee RF4CE			ZigBee PRO							ZigBee IP (IETF based)	Alternate IP Transport	
MAC	IEEE 802.15.4 – MAC											Alternate MAC	
PHY	IEEE 802.15.4 – sub-GHz (specified per region)				IEEE 802.15.4 – 2.4 GHz (worldwide)							Alternate PHY	

## ZigBee PRO



## ZigBee RF4CE



## ZigBee IP





## Profil ZigBee RF4CE



ZigBee Remote Control est un profil permettant une communication bidirectionnelle, en réduisant les problèmes de masquage tout en augmentant la portée.



ZigBee Input Device est un profil pour les produits types claviers, souris ou fonctions similaires tout en gérant des fonctionnalités avancées comme le multi-touch.



ZigBee 3D Sync est un profil dédié aux dispositifs de visions 3D offrant plus de flexibilité sur les mouvements de l'utilisateur.

## Profiles ZigBee PRO



ZigBee Smart Energy est un profil pour les produits qui surveillent, contrôlent, informent et automatisent la livraison et l'utilisation de l'énergie et de l'eau.



ZigBee Home Automation est un profil pour les produits domotiques comme l'éclairage, les volets, les alarmes,...



ZigBee Telecom Services est un profil pour les cartes SIM actives ce qui permettrait de délivrer des informations locales, d'effectuer des paiements par mobile, des localisations en intérieur, et de l'échange pour les jeux.

## Profiles ZigBee PRO



ZigBee Retail Services est un profil pour réduire le temps lors du paiement, aider à la localisation de produits, d'offres promotionnelles...



ZigBee Bulding Automation est un profil pour les produits liés à la sécurité, à la fiabilité, au contrôle des systèmes des bâtiments



ZigBee Health Care est un profil destiné au monitoring des patients, pour les activités de fitness, localisation en temps réel...

## Profile ZigBee PRO



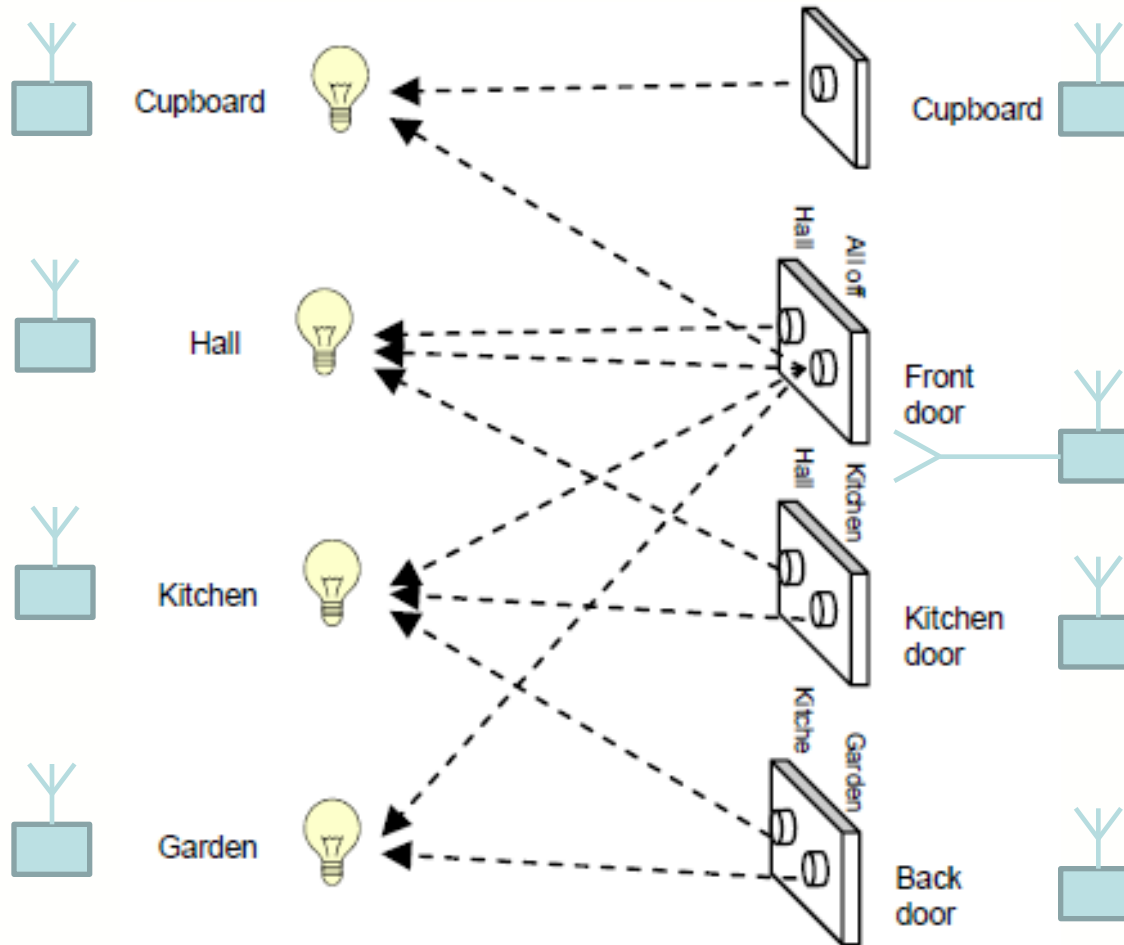
ZigBee Light Link est un nouveau standard permettant l'ajout de dispositif d'éclairage sans aucune intervention de configuration (Touchlink) (Interopérabilité avec ZHA, ZID, ZRC et ZHC),

## Profile ZigBee IP

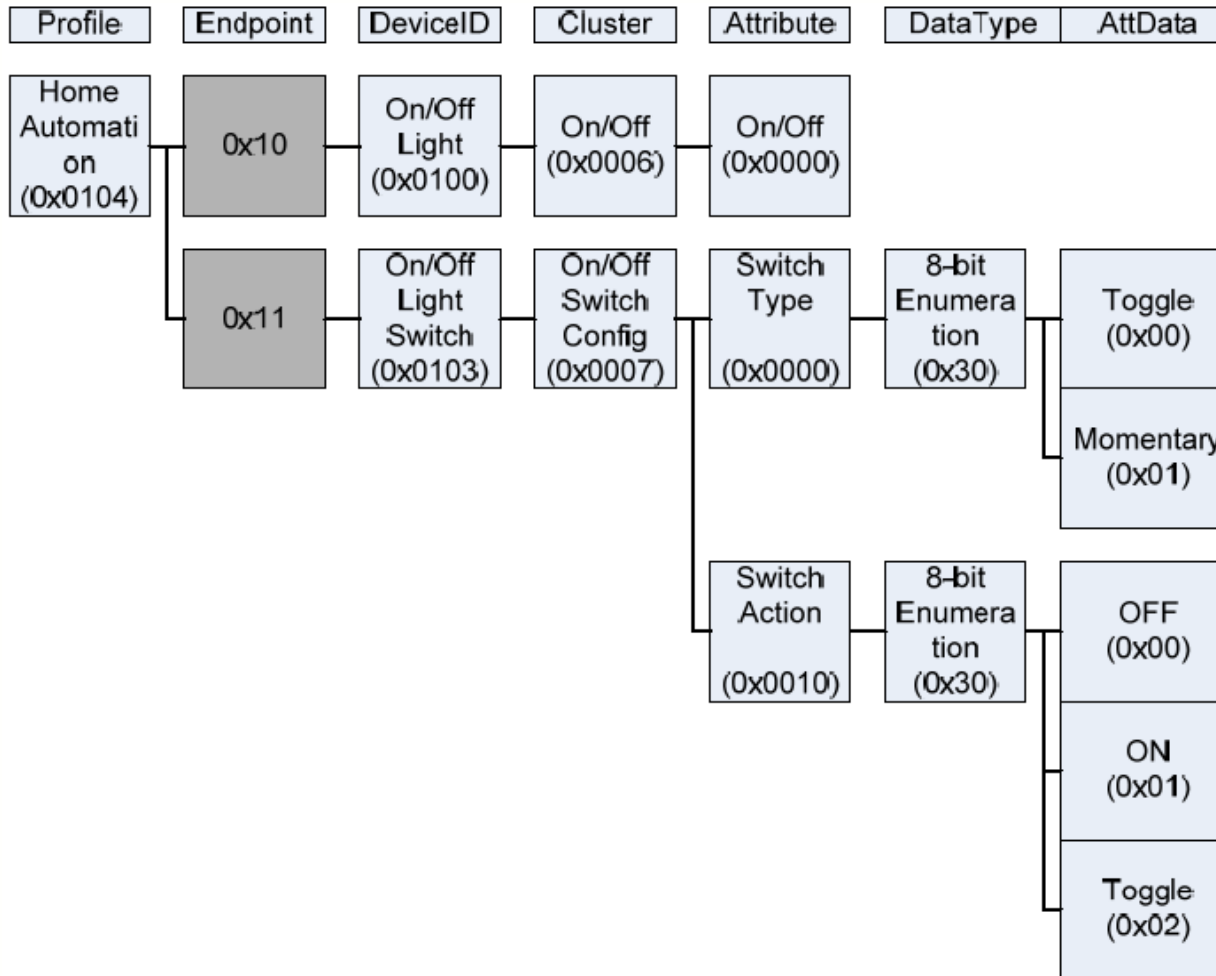


ZigBee Smart Energy est un profil qui ajoute au profil 1.X des fonctionnalités de contrôle d'installation de recharge de véhicule électrique, configuration et rechargement de firmware pour des dispositifs du réseau, contrôle de charge...

## Profil ZigBee (Application Profile) – liens logiques (binding)



## Profil ZigBee (Application Profile) – une lampe et un interrupteur



Ref:

<http://zigbee.org/>, ZigBee.org

075367r02ZB\_AFG-Home\_Automation\_Profile\_for\_Public\_Download, ZigBee.org

075366r01ZB\_AFG-ZigBee\_Cluster\_Library\_Public\_download\_version, ZigBee.org

ZigBee Wireless Networks and Transceivers, Shahin Farahani, ISBN: 978-0-7506-8393-7

[http://fr.wikipedia.org/wiki/Routage\\_AdHoc](http://fr.wikipedia.org/wiki/Routage_AdHoc)

[http://en.wikipedia.org/wiki/Phase-shift\\_keying](http://en.wikipedia.org/wiki/Phase-shift_keying)

zic04\_zcl\_api.pdf, CEL

Overview of the IEEE 802.15.4 standards family for Low Rate Wireless Personal Area Networks, N.Salman, I. Rasool, A.H.Kemp

ZigBee for Applications Developers © FlexiPanel Ltd

ZigBee, Alliance ZigBee et l'ensemble des profils sont des marques déposées.