S9 Projet Electronique
Les réseaux Zigbee, leurs applications et leurs fonctionnements.

I. Historique.

Historiquement, il existait déjà plusieurs protocoles de communication par radio fréquence (Wifi – Bluetooth) mais l'accès au réseau était complexe, le coût des objets assez élevé et l'extension à des centaines de communicants difficilement envisageable. De plus, même si la pile protocolaire était commune, les composants étaient difficilement interchangeables suivant les fabricants.

Le protocole Zigbee est donc né du besoin d'objets communicants

- De faible encombrement. *(6,7 cm² pour nos modules, miniaturisables...)*
- De faible cout.*(17 € - Xbee module Digi Int.)*
- Économe en énergie. *(de 10 à 60 mW Emission / Reception – 3µW Veille)*
- Interchangeables, quelque soit le constructeur.
- Très simples d'utilisation, en particulier lors de l'accès au réseau.
- Permettant des échanges de données sur grandes distances (*portée 100m en extérieur mais relais possibles dans le réseau)*

L'alliance Zigbee s'est alors créée (2002 25 membres, 2004 125 membres, 2012, plus de 400) et a proposé la norme Zigbee™ en 2005.

Plate-forme compatible ZigBee

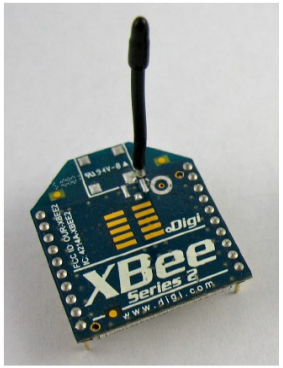
Basé sur le protocole IEEE 802.15.4™ pour ses couches PHY (gestion des transmissions radio à 868/ 915 MHz et 2,4GHz – modulation) et Médium Access Control (construction des trames, gestion des collisions) , le protocole Zigbee fournit entre autre l'infrastructure réseau permettant la mise en œuvre de réseaux maillés si besoin sécurisé.
Cette communauté industrielle regroupe aujourd'hui 400 entreprises et gère les évolutions de ce protocole par l'édition de différents Firmwares (séries 1, 2, PRO). Elle est la seule à pouvoir certifier un matériel qui sera alors interchangeable avec les autres produits certifiés portant le logo

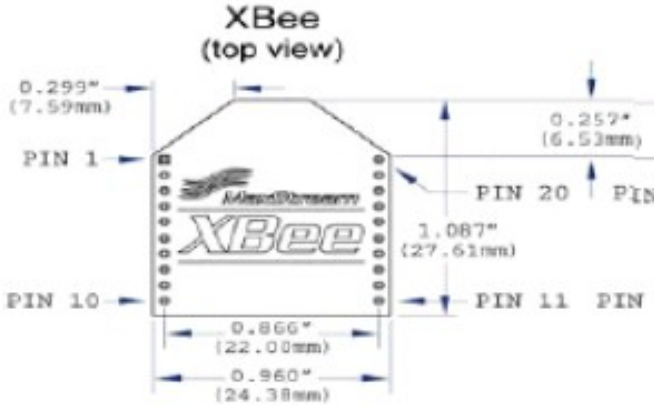
II. Applications types

- **Domotique** *Commande de lampes, chauffage, volets, etc...Cette partie dispose maintenant de modules auto alimentés.*
- **Gestion d'énergies**.*Relève de compteurs, analyse des consommations, gestion des sources autonomes,*
- **Domaine de la santé**.*Hospitalisation à domicile, suivi des données médicales*
- **Contrôle industriel** *Capteurs sans fils le long de la chaîne de production, centralisation du traitement global...*

III. Evolution des matériels :

- Brochage :





Pin Assignments for the XBee/XBee-PRO Modules
(Low-asserted signals are distinguished with a horizontal line above signal name.)

Pin #	Name	Direction	Default State	Description
1	VCC	-	-	Power supply
2	DOUT	Output	Output	UART Data Out
3	DIN / CONFIG	Input	Input	UART Data In
4	DIO12	Both	Disabled	Digital I/O 12
5	RESET	Both	Open-Collector with pull-up	Module Reset (reset pulse must be at least 200 ns)
6	RSSI PWM / DIO10	Both	Output	RX Signal Strength Indicator / Digital IO
7	DIO11	Both	Input	Digital I/O 11
8	[reserved]	-	Disabled	Do not connect
9	DTR / SLEEP_RQ/ DIO8	Both	Input	Pin Sleep Control Line or Digital IO 8
10	GND	-	-	Ground
11	DIO4	Both	Disabled	Digital I/O 4
12	CTS / DIO7	Both	Output	Clear-to-Send Flow Control or Digital I/O 7. CTS, if enabled, is an output.
13	ON / SLEEP	Output	Output	Module Status Indicator or Digital I/O 9
14	VREF	Input	-	Not used for EM250. Used for programmable secondary processor. For compatibility with other XBEE modules, we recommend connecting this pin voltage reference if Analog sampling is desired. Otherwise, connect to GND.
15	Associate / DIO5	Both	Output	Associated Indicator, Digital I/O 5
16	RTS / DIO6	Both	Input	Request-to-Send Flow Control, Digital I/O 6. RTS, if enabled, is an input.
17	AD3 / DIO3	Both	Disabled	Analog Input 3 or Digital I/O 3
18	AD2 / DIO2	Both	Disabled	Analog Input 2 or Digital I/O 2
19	AD1 / DIO1	Both	Disabled	Analog Input 1 or Digital I/O 1
20	AD0 / DIO0 / Commissioning Button	Both	Disabled	Analog Input 0, Digital IO 0, or Commissioning Button

- Séries 1 :

Uniquement pour les communications Peer to Peer. N'utilisent que le protocole 802.15.04 (pas de protocole réseau/sécurité)

- Séries 2 :

Supportent le protocole Zigbee, peuvent s'insérer dans un réseau, sous couvert d'avoir un firmware compatible.

Modems type XB24 – B (firmwares en 1.xxx) Permettent d'obtenir les commandes élémentaires et d'organiser un réseau de petite taille.

Modems type XB24-ZB (firmwares en 2.xxx) Dernière génération, permettent d'obtenir des commandes supplémentaires, utiles dans les grands réseaux.

- Séries 2 PRO :

Mêmes possibilités que les séries 2.

Puissance d'émission plus importante (jusqu'à 60 mW). Sécurisation des transmissions et des accès plus importante.

Attention, la norme européenne impose une puissance maximale de 10 mW ou 10 dBm.

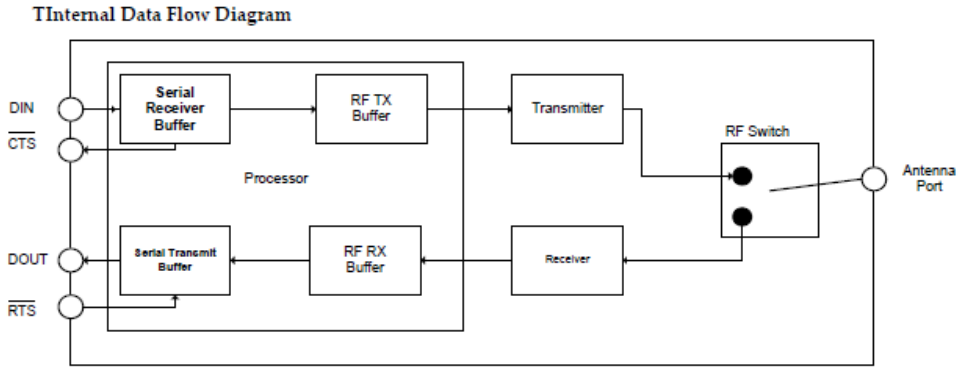
- Green Energy :

Nouvelle option de la série PRO permettant au module de fonctionner sans batterie (récupération d'énergie RF ou thermique).

IV. Détail de la pile protocolaire

1. gestion de la transmission RF – couche PHY

Des buffers sont directement intégrés dans les modules et gérés par les signaux $\overline{CTS}$/$\overline{RTS}$

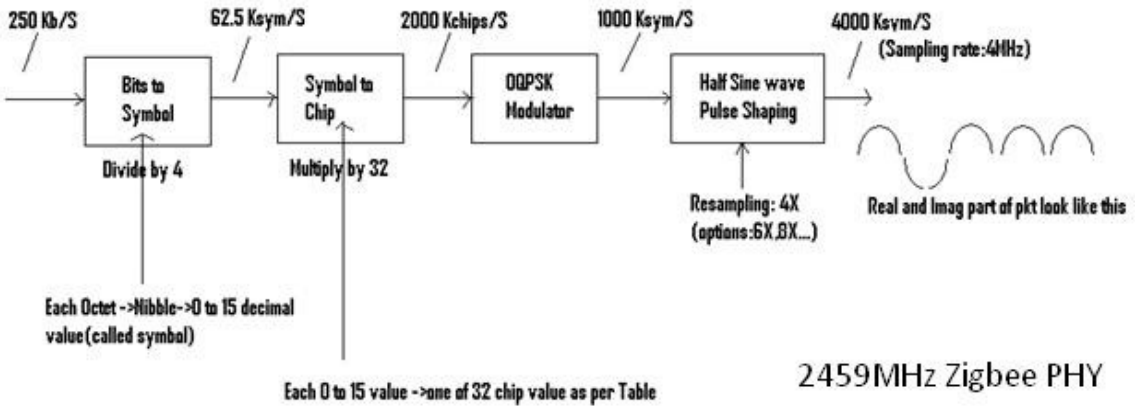


$\overline{CTS}$ est par défaut à 0 quand le module Xbee peut transmettre des données par RF, il passe à 1 quand l'espace restant dans le buffer d'entrée est de 17 octets, il repasse à 0 quand 34 octets se libèrent.

$\overline{RTS}$ doit être par défaut à 0, pour que le module Xbee puisse transmettre sur sa liaison série les données reçues par RF.

Le faire passer à 1 peut être intéressant quand le temps de traitement de l'information est long mais il faut auparavant configurer le module pour qu'il tienne compte de cette commande

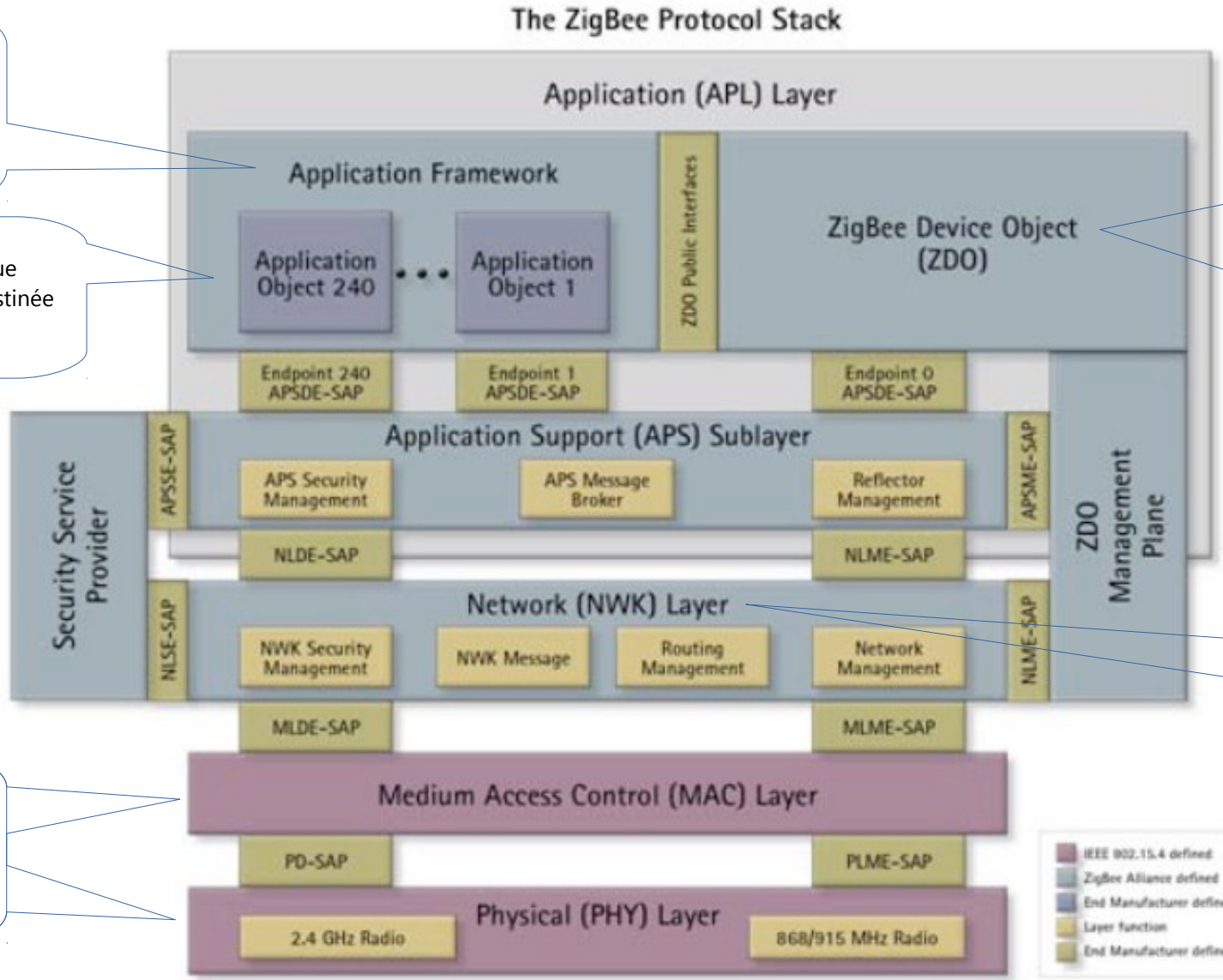
Pour information, la modulation utilisée est la QPSK :



2. Couches supérieures de la pile.

Définit un éventail de données standard suivant le type d'utilisation du module

Bloc logiciel
Qui contrôle le périphérique
En vue d'une utilisation prédestinée
Jusqu'à 240 possibilités.



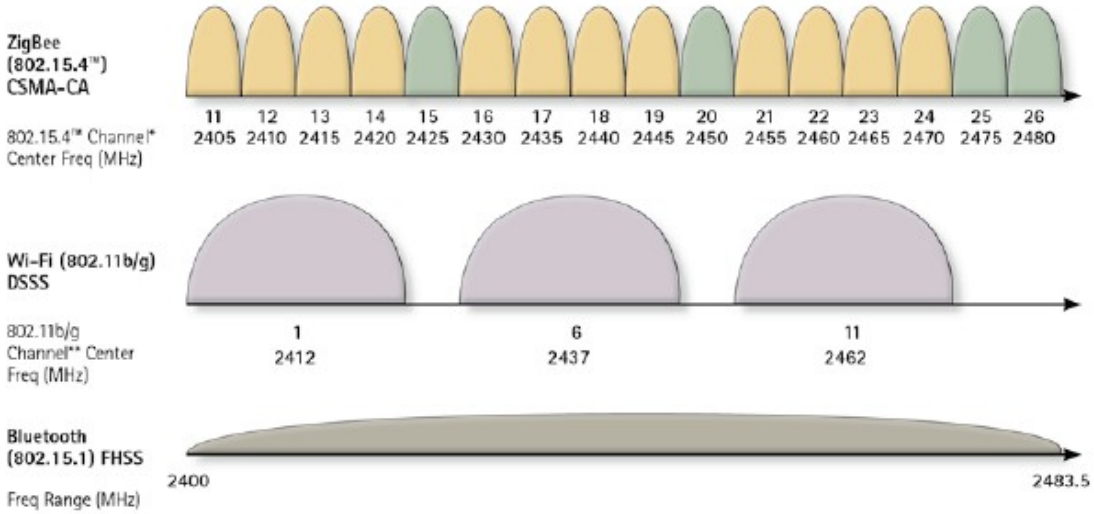
Permet de définir le rôle du périphérique dans le réseau.
Gère les réponses aux requetes de Découverte.
Gestion des commandes liées au profil
ZDO = ENDPOINT 0

Gestion du routage RF.

Norme 802.15.4

V. Avantages/ Inconvénients de cette technologie

La couche PHY gère les communications sous forme d'ondes radio à 2,4 GHz, comme la WI-FI ou le Bluetooth mais à la différence de ces deux derniers, le protocole Zigbee découpe la bande passante en 16 canaux. Les canaux privilégiés seront bien sur ceux non occupés par la Wifi.

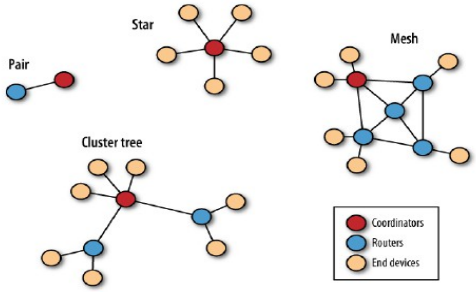


Les besoins mémoire sont beaucoup plus faibles, le nombre d'élément dans le réseau beaucoup plus important (voir chapitre suivant) mais la vitesse de transmission est beaucoup plus lente(pas de transfert de « grosses données »).

	Bluetooth	Bluetooth LE /Smart	WIFI	WIFI	WIFI (Next generation)	NFC	Zigbee	Z-Wave	ANT +
Specification	802.15.1	802.15.1	802.11g	802.11n	802.11y	NFCIP-1	802.15.4	Z-Wave alliance	ANT
Frequency	2.4 GHz	2.4 GHz	2.4 GHz	2.4GHz / 5 GHz	3.7GHz (US)	13.56 MHz	868 MHz (EU) 915MHz (US) 2.4GHz	868MHz (EU, China, India, Russia,...) 900MHz (North America, Brazil, HongKong, Australia, Japan,...)	2.4GHz
Range indoor (m)	30	10	25	50	50	0.2	30	45	10
Range max (m)	100	50	75	125	5000	0.2	1500	150	30
Data speed max	3 Mbit/s	1 Mbit/s	54 Mbit/s	540 Mbit/s	54 Mbit/s	424 kbit/s	250 kbit/s	100 kbit/s	<100kbit/s
Data speed typ.	2.1Mbit/s	270 kbit/s	25 Mbit/s	200 Mbit/s	23 Mbit/s	2.5kbit/s	150 kbit/s	40 kbit/s	20 kbit/s
Peak current	150 mA	20mA	150 mA	150 mA	-	15 mA	50 mA	20 mA	35 mA
Sleep current	5 mA	1 uA	100 µA	100 µA	-	10 µA	5 µA	2.5µA	1 µA
Battery life	Month	Year	Day	Day	-	Month/Year	Month/Year	Year	Year
Network topologies	Star	Star	Star	Star	Star	Peer to peer only	Star, Tree, Mesh	Star, Tree, Mesh	Star, Tree, Mesh
Typically :	- Headsets - Computer peripherals	- Mobile phones - Sport trackers -eHealth devices - Wireless sensors	-PC (networking) -WLAN	-same as 802.11g with improved performances -Outdoor LAN	-wireless link between hotspot	-transport ticket -secure payment -door opening	-home automation -wireless sensor networks -smart metering	-home automation	-sport trackers -eHealth devices
Official Website Link	https://www.bluetooth.org/en-us	https://www.bluetooth.org/en-us	http://www.wi-fi.org/	http://www.wi-fi.org/	http://www.wi-fi.org/	http://www.nfc-forum.org/home/	http://www.zigbee.org/	http://www.z-wave.com/	http://www.thisisant.com/

VI. Présentation du réseau et de ses intervenants.

1. Réseau minimum



Pour créer un réseau, il faut des modules présentant des fonctions distinctes :

- Un seul ***COORDINATOR***.

A sa mise sous tension le coordinateur créé le réseau sur l'adresse paramétrée par l'utilisateur et lance le scan des différents canaux de communication en testant la puissance des éventuelles émissions sur chaque fréquence et choisit le moins utilisé.

La broche 15 du module donne le statut d'association par défaut. Reliée à une LED, celle-ci clignote 1 fois par seconde quand le réseau est créé.

- Quelques ***ROUTERS***.

Une fois paramétrée la bonne adresse réseau, ces périphériques scanne les canaux pour trouver le coordinateur ayant la même adresse réseau. Ils sont alors autorisés à « rentrer » par le coordinateur. Ils peuvent ensuite dialoguer avec celui-ci mais aussi entre eux.. Ils permettent d'étendre la couverture du réseau. Ils routent dynamiquement les messages et conservent une trace des chemins routés. Ils stockent les messages à destinations des end devices qui leurs sont rattachés.

Une LED reliée à la broche 15 clignote deux fois par seconde une fois que le routeur à rejoint un réseau.

- Jusqu'à 65535 ***END DEVICE*** (adressage dynamique sur 16 bits)

Ne participent pas au routage, peuvent être mis en veille (modules mobiles, alimentés par pile)

Les périphériques doivent avant tout avoir la **même adresse réseau (PAN ID)** et le **même canal de transmission** (parametre CH lecture uniquement).

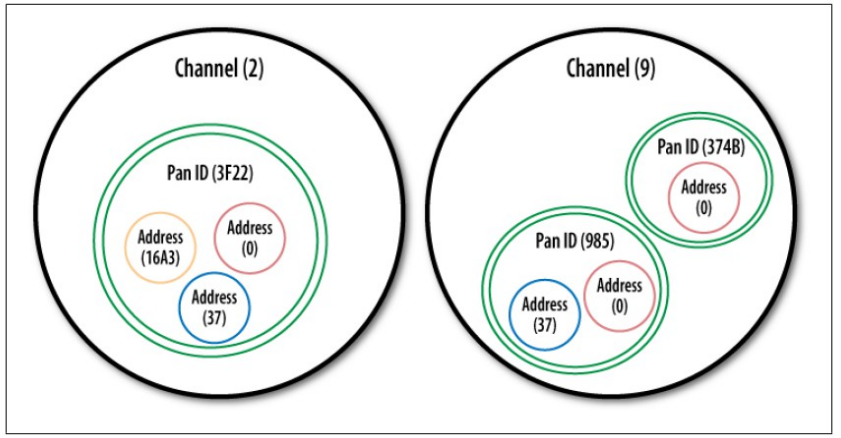
A noter que l'interchangeabilité des modules implique que les numéros de série des modules (en Hexa sur 64 bits) sont uniques. Ils constituent des paramètres d'identification des modules (SH-SL) et serviront d'adresse dans les transmissions (DH – DL) .
Cependant, le coordinateur affectera à chaque module se connectant au réseau une autre adresse dite « dynamique » sur 16 bits (MY) . Celle-ci sera réactualisée à chaque arrivée du module dans le réseau. A noter que l'adresse MY des coordinateurs est toujours 0000.
Cette adresse permet un routage plus efficace des messages mais sa connaissance n'est pas obligatoire (FFFE adresse inconnue)

Le rôle pris par le module dépend du firmware implanté à l'aide du logiciel **XCTU** (distribué par DIGI Int, gratuit mais uniquement compatible avec Windows)

Par défaut les modules portent le dernier firmware en cours pour une fonction router/end device AT à la sortie d'usine.

Ce logiciel permet aussi de lire et régler les différents paramètres du module ou d'ouvrir un terminal pour dialoguer via la liaison série avec le module ou envoyer des données à un destinataire.

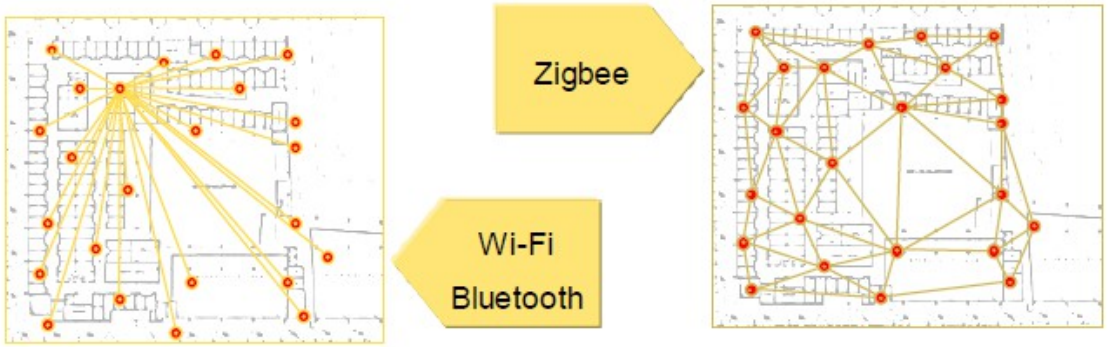
2. Organisation de l'adressage.



Les adresses de la figure ci-contre sont des adresses dynamiques.
On pourrait aussi identifier les éléments du réseau par leurs numéro de série.

3. Particularité du réseau maillé.

Réseaux mesh : maillage de routeurs interconnectés et de périphériques « ultimes », permet d'établir des communications entre deux périphériques hors de portée l'un de l'autre.



- Communications multi-sauts (« multi-hop ») : relayage des messages par les liens les plus fiables listés dans la table de routage de chaque routeur. L'algorithme de routage pour ce genre de réseau est basé sur la notion de « Distance vector » : chaque routeur qui relaie un message d'un destinataire vers un autre enregistre pour cette transmission les adresses du dernier « relayeur » et du prochain routeur vers le destinataire. Il existe d'autres algorithmes suivant le type d'échanges attendus (tous vers un ou un vers tous)

Avantages :

- Réseau évolutif et pouvant couvrir des grandes surfaces.
- Fiabilité, robustesse : découverte automatique de nouvelles routes en cas de défection d'un routeur. (réseau auto-réparable)

VII. Les deux modes de fonctionnement des modules Zigbee.

Deux grandes familles de Firmwares peuvent être implantées suivant la façon dont on veut communiquer avec les modules (paramétrages, réception des données) mais aussi suivant l'utilisation qui sera faite des données transmises (directement par l'utilisateur ou par un processeur traitant les infos).

➢ Si votre application reste simple (peu de modules dans le réseau, aucune interaction entre les systèmes reliés aux modules) , le mode Transparent/ AT Command suffira.

*Le codage utilisé pour les AT command descend des **commandes Hayes** créées pour communiquer avec les modems. Ce n'est pas un standard à proprement parler mais cette philosophie est très répandue pour le paramétrage de commandes simples.*

➢ Si au contraire votre réseau est plus complexe (nécessité de connaître précisément l'adresse de l'envoyeur, gestion à distance des paramètres, réception des échantillons logiques ou analogiques relevés sur les broches d'un module) le mode API sera plus adapté.

Le dialogue avec le module via la liaison série et l'envoi de données vers les autres modules se font sous forme de trames aux formats prédéfinis.

Celles-ci sont moins compréhensibles par l'homme mais nettement plus adaptées à un traitement « machine » :

- lecture/modifications paramètres du module.
- informations sur la bonne réception (ou non) de la demande
- adresses de l'envoyeur et des éventuels relayeurs
- cheksum

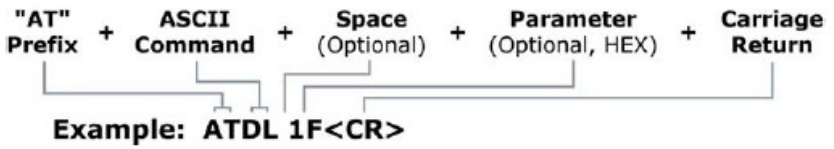
1. Principe des AT Commandes dans le mode AT Command/ Transparent.

Le module est naturellement en **mode transparent** : les données transitent « en brut » de la liaison série vers l'émetteur/recepteur RF.

On active le **mode command** en envoyant sur la liaison série la chaîne de caractères par défaut ***« +++ »*** *sans CR (paramétrage de cette chaîne via GC et CC*) , les module coupe alors son antenne et accède aux paramètres du Firmware.

Les commandes commencent par les caractères AT suivis de 2 caractères représentant le paramètre à configurer ou lire.

Le module répond sur la liaison série, soit la valeur du paramètre interrogé, soit OK pour valider un changement de valeur.



Par défaut au bout de 10s sans action sur la liaison série (paramètre CT), le module repasse ne mode transparent et rouvre son port RF.

2. Liste non exhaustive des paramètres des modules Zigbee

code	*action*	*Paramètre par défaut coordinateur*	*Paramètre par défaut Router/End device*
ID	Adresse 64 bits du réseau créé (Coordinateur) ou à rejoindre (Routeur, End Device)	0x*0*	0x*0*
CH	Canal sur lequel se font les transmissions. **Non modifiable**	0x*0B → 0x1A (channels 11-26)*	
MY	Adresse dynamique 16 bits affectée au module. Affectation aléatoire à chaque connexion.	0x0 si réseau créé. Adresse réservée au coordinateur	0xFFFE, le module n'a encore rejoint aucun réseau.
SH S**L**	Adresse 64 bits (H – 32 bits forts / L - 32 bits faibles) du module correspondant au numéro de série inscrit sur le module. **Non modifiable**		
DH **DL**	Adresse 64 bits (H – 32 bits forts / L - 32 bits faibles) du module destinataire. Commande **uniquement utile en mode AT** ou pour les envois automatiques de valeurs « captées »	0x0/ 0xFFFF :(*broadcast)* tous les membres recensés du réseau reçoivent la transmission.	0x0 / 0x0 : adresse du coordinateur.
ND	Scanne le réseau et renvoie infos de chaque module présent.		
NJ	Option gérant le temps alloué par le module à l'ouverture de la connexion pour des éventuels nouveaux entrants. (hexa * 1s)	0xFF (infini)	0xFF (infini)
JN	Paramètre le type de message automatiquement envoyé en broadcast par un nouvel arrivant dans le réseau	∅	0 : aucune identification renvoyée
P…/ D…	Paramétrage de la fonction de la broche indiquée (entrées logique, sortie logique, entrée analogique)		
RE	Retour aux paramètres par défaut du module		
NR	Reset du réseau, permet de relancer la gestion du canal de transmission et les process d'entrée sur le réseau.		
WR	Inscrit durablement les valeurs des paramètres dans la mémoire morte du module.		
CT	Gère le temps d'inactivité avant de repasser en mode transparent (valeur en décimal * 100ms)	0x64 <=> 10s *max 0x28F (FM ZB)/0x0FF (FM B)*	0x64 <=> 10s
CN	Sortie immédiate du mode commande.		

Liste de tous les paramètres des modules Xbee en annexe

3. Organisation des trames API

- Trames uniquement codées en hexa (nécessité de la table donnant les codes Ascii, calculatrice en hexa pour le cheksum)
- Toutes les transmissions attendent un acquittement. S'il n'est pas reçu, la trame est renvoyée automatiquement jusqu'à 3 fois.
- Les adresses 64 bits permettent de renseigner le champ destinataire des trames. Cependant la connaissance de l'adresse dynamique 16 bits correspondante accelère la transmission.
- Deux modes d'API disponibles : l'un sans caractères réservés (hormis 0x7E) (AP=1) l'autre avec caractères réservés (AP=2) : 0x7E (octet de départ) ; 0x7D (echap) ; 0x11 (XON) ; 0x13 (XOFF). Dans ce mode, si ces caractères doivent être utilisés pour des valeurs dans la trame il faut insérer le drapeau 0x7D suivi du résultat d'un Ou exclusif entre la valeur et 0x20.

Forme générale de la trame :

- **Byte de start** : 0x7E
- **Longueur de trame sur 2 octets** (Most significant – Least significant) : nombre d'octets de la trame qui suit, sans compter le cheksum.
- **Frame Specific Data**, dépend du type de trame utilisée (voir tableau ci dessous)
- **Cheksum** = 0xFF – l'octet de poids faible de la somme des valeurs en hexa depuis Frame Type (inclus).

API Frame Names	API ID
AT Command	0x08
AT Command - Queue Parameter Value	0x09
ZigBee Transmit Request	0x10
Explicit Addressing ZigBee Command Frame	0x11
Remote Command Request	0x17
Create Source Route	0x21
AT Command Response	0x88
Modem Status	0x8A
ZigBee Transmit Status	0x8B
ZigBee Receive Packet (AO=0)	0x90
ZigBee Explicit Rx Indicator (AO=1)	0x91
ZigBee IO Data Sample Rx Indicator	0x92
XBee Sensor Read Indicator (AO=0)	0x94
Node Identification Indicator (AO=0)	0x95
Remote Command Response	0x97
Over-the-Air Firmware Update Status	0xA0
Route Record Indicator	0xA1
Many-to-One Route Request Indicator	0xA3

Organisation des différentes trames en annexe
exemple ci dessous: trame de demande d'une valeur de paramètre.(0x08)

Frame Fields		Offset	Example	Description
Start Delimiter		0	0x7E	
Length		MSB 1	0x00	Number of bytes between the length and the checksum
		LSB 2	0x04	
Frame-specific Data	Frame Type	3	0x08	
	Frame ID	4	0x52 (R)	Identifies the UART data frame for the host to correlate with a subsequent ACK (acknowledgment). If set to 0, no response is sent.
	AT Command	5	0x4E (N)	Command Name - Two ASCII characters that identify the AT command.
		6	0x4A (J)	
	Parameter Value (optional)			If present, indicates the requested parameter value to set the given register. If no characters present, register is queried.
Checksum		7	0x0D	0xFF - the 8 bit sum of bytes from offset 3 to this byte.

The above example illustrates an AT command when querying an NJ value.

VIII. Les particularités des broches d'entrée/sortie.

Plusieurs broches des modules zigbee peuvent être configurées en Entrée ou Sortie Numérique et Entrée Analogique (max 3,3V).

Attention, certaines de ces broches permettent aussi de contrôler le fonctionnement des modules
(RSSI, Sleeep Ctrl, $\overline{CTS}$, Assoc, $\overline{RTS}$, marche)

Pour configurer ces broches, il faut faire suivre le paramètre correspondant au numéro de la broche d'un code donné dans le tableau ci dessous.

Pin Command Parameter	Description
0	Unmonitored digital input
1	Reserved for pin-specific alternate functionalities
2	Analog input, single ended (A/D pins only)
3	Digital input, monitored
4	Digital output, default low
5	Digital output, default high
6-9	Alternate functionalities, where applicable

Module Pin Names	Module Pin Numbers	Configuration Command
CD/DIO12	4	P2
PWM0/RSSIM/DIO10	6	P0
PWM/DIO11	7	P1
DIO4	11	D4
CTS/DIO7	12	D7
ASSOC/DIO5	15	D5
RTS/DIO6	16	D6
AD3/DIO3	17	D3
AD2/DIO2	18	D2
AD1/DIO1	19	DI
AD0/DIO0	20	D0

Une fois l'une ou plusieurs de ces broches paramétrées, des trames API seront automatiquement générées et envoyées au module spécifié (paramètres DH, DL). Le destinataire générera alors une trame de type 0x92 sur sa liaison série reprenant les données collectées.

- Le paramètre **IS** permet de récupérer immédiatement l'échantillon de données collectées directement sur le port série du module collecteur.
- Le paramètre **IR** dimensionne la période de prélévement et d'envoi des échantillons à l'adresse destinataire préalablement paramétrée.

  La valeur est en ms, codé en hexa (0x64 = 100ms). La valeur 0x0 désactive l'envoi périodique des données.
- Le paramètre **IC** permet d'activer la détection de changement d'état sur les entrées numériques, déclenchant ainsi l'envoi immédiat du nouvel échantillon.

Construction des masques utilisés pour la mise en forme des données collectées:

L'emplacement de chaque sortie est à 1 si utilisée, 0 sinon. Le mot binaire ainsi formé est automatiquement converti en hexa.

- 1er octet du masque digital : n/a n/a n/a D12 D11 D10 n/a n/a 2e octet du masque digital : D7 D6 D5 D4 D3 D2 D1 D0
- Octet du masque analogique : (voltage) n/a n/a n/a A3 A2 A1 A0.

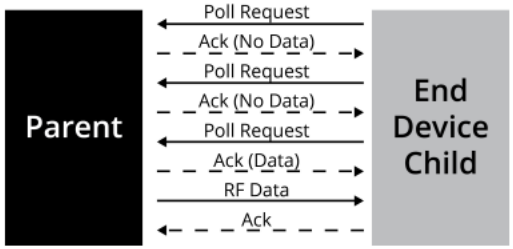
(Le bit de poids fort indique si le système de lecture de valeurs analogiques a été activé, 0 par défaut)

Les valeurs analogiques sont codées sur 10 bits, (1023 possibilités). Si la valeur est > 255, les deux octets seront donc nécessaires.

Pour reconstruire la valeur analogique correspondante, on multiplie le MSB par 0x100 (ou 256 en décimal) et on ajoute le LSB.

IX. La mise en veille des périphériques. Uniquement disponible sur les modules end devices.

La veille permet d'économiser l'énergie et donc de concevoir des systèmes autonomes (pile). Le système d'émission/réception RF est hors service. La consommation est alors de l'ordre de 60µW. Ces modules ne participent évidemment pas au routage vers d'autres modules. Ils sont liés à un module « parent » qui stockera les messages leurs étant destinés lors de la veille. (1 seul message stocké sans processeur externe).



La mise en veille ne se fait qu'à la fin de la tâche en cours (envoi / réception de données)

Le réveil prend environ 10 ms.

Si un module dormant est programmé pour envoyer des données recueillies sur ses broches d'entrée/sortie, l'envoi sera automatique à chaque réveil.

La mise en veille d'un module se gère via le paramètre **SM** et les codes suivants :

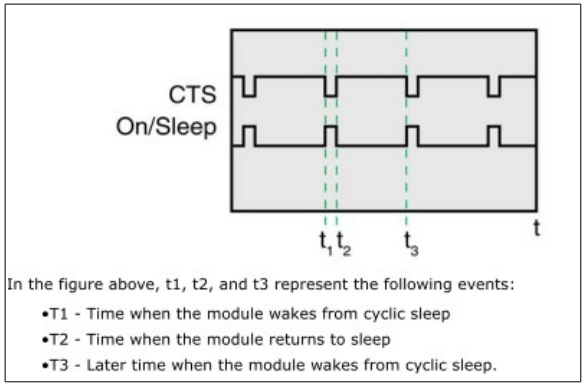
0 : par défaut : désactivé.

1 : la mise en veille est activée et dépend de l'état de la broche 9 (SLEEP_RQ)

Niveau haut : mise en veille après traitement du dernier message entrant et envoi du dernier message sortant.

Niveau bas : « réveil »

5 : Veille cyclique mais avec possibilité de réveil par la broche 9.



Lecture CTS sur broche 12. doit être configuré.
Rappel : CTS = 1 => transmission impossible

4 : veille cyclique gérée par des paramètres supplémentaires:

- Le paramètre **SP** qui gère la durée de la période de veille: Valeurs comprises entre 0x20 et 0x AF0 (soit, $*10^{-2}$ s => 320 ms à 28s).

Ce paramètre doit être réglé sur le module dormant ET sur son « parent » qui saura alors combien de temps stocker les messages.

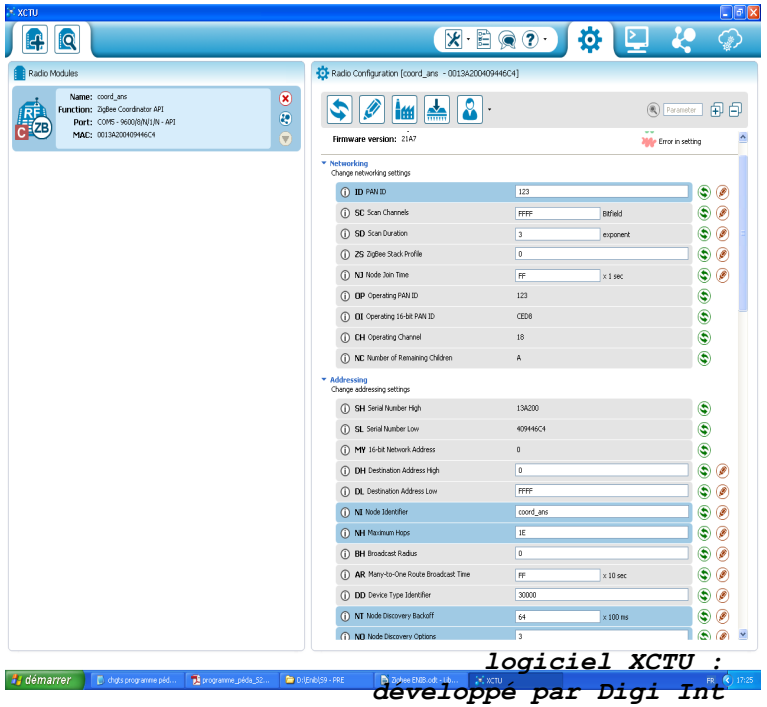
*Remarque : le temps de veille peut être rallongé via le parametre SN : nombre de périodes consécutives de veille. Ensuite on choisit l'option de reveil (SO) : à chaque fin de période ou après SN*ST périodes.*

- Le paramètre **ST** gère lui la durée minimale d'éveil après la dernière action (compteur remis à 0 après chaque reception de données).

  Valeurs de 0x1 à 0xFFFE (1ms à 65s)

X. Création d'un premier réseau de modules communicants en AT Command.

1. Premier module à paramétrer : le coordinateur.



logiciel XCTU :
développé par Digi Int
licence gratuite
ne fonctionne que sous windows
Nécessite des droits en écriture
=> travail sur D:/

- Après avoir noté le numéro de série de votre module xbee le relier via l'*usb adapter* à l'ordinateur.
- Ouvrir le **logiciel XCTU**, lancer la recherche du module sur le port série automatiquement détecté et le glisser dans la partie ***configuration***. Tous les paramètres sont alors automatiquement lus.
- Par défaut, le module est en configuration router, PAN ID 0x0.
- Choisir un PAN ID personnel, modifier le champ et sauvegarder.
- Dans le menu ***Update firmware***, choisir XB24-ZB / Zigbee Coordinateur AT

  Les versions évoluent en fonction des nouveaux firmwares créés par l'alliance Zigbee et mis à disposition par Digi Int. Le dernier en date pour ce mode de fonctionnement est le 20A7

- Passer dans l'onglet ***« terminal série »***, connecter le module. Repasser dans l'onglet de configuration.
- Modifier le paramètre PAN ID pour définir votre adresse réseau.
  Sauvegarder cette valeur (symbole crayon).
- Observer dans le terminal série la traduction en commandes Hayes de vos actions.
- Lire le nom du module par défaut (NI), le modifier pour personnaliser votre module (20 caractères ascii maximum),
- Allonger le temps d'inactivité déclenchant un retour en mode transparent et sauvegarder ces modifications.
- Vérifier que l'adresse 64 bits et non modifiable. Vérifier que les valeurs par défaut de l'adresse dynamique et l'adresse destinataire.

2. Configuration d'un premier routeur

- Prendre un deuxième module (configuration par défaut XB24-ZB / Router AT), noter son numéro de série et le relier à un 2e port USB (sans déconnecter votre coordinateur).
- Relancer la recherche de module après avoir coché le nouveau port sériée détecté, et répéter les opérations permettant de lire la configuration. Il suffit ensuite de cliquer sur l'un ou l'autre des modules pour lire/modifier leurs configs.
- Dans l'onglet ***« terminal série »*** , connecter le module.
- Entrer dans le mode Command en envoyant les caractères « +++ » (**sans <CR>**) sur la liaison série via la fenêtre **console log**, attendre 1 seconde, le module passe en mode command et répond OK.
- Grâce aux AT Command,
- Vérifier que le module est bien en configuration d'usine (routeur, PAN ID 0)
- Vérifier ses adresses 64 bits et dynamique (indication sur la non connexion de ce périphérique à un réseau.)
- Affecter un nom à ce routeur,
- Allonger le temps de sortie du mode Command.
- Entrer l'adresse réseau correspondant à celle de votre coordinateur.
- Sauvegarder ces modifications.

Le routeur va alors automatiquement demander l'autorisation au coordinateur de rentrer sur le réseau, celui ci va lui affecter une adresse dynamique et le témoin d'association de l'adaptateur USB clignote 2 fois par seconde

- Lancer un scan des éléments présents sur le réseau par ce routeur et par le coordinateur. Vérifier les données transmises.
- Modifier le paramètre NO afin de ne plus afficher les paramètres du module effectuant le scan.
- Sortir du mode *command*, vous êtes alors en mode *transparent*
- Vérifier la transmission de données d'un module vers l'autre, en utilisant les adresses par défaut puis l'adressage par direct (par adresse destinataire ou par nom).

3. Gestion des accès réseau et des transmissions multiples.

- Configurer votre coordinateur pour bloquer l'accès au réseau (paramètre NJ).
- Configurer un 2e routeur comme précédemment et tester l'entrée de celui-ci dans le réseau.
- Obtenir le statut de la tentative de connexion (paramètre JN).
- Ré-autoriser l'accès au réseau par votre coordinateur.
- Vérifier que votre réseau comprend alors 3 périphériques.
- Transmettre des messages de chacun des périphériques en broadcast ou unicast en utilisant directement le nom du module (vous vérifierez alors la mise à jour automatique des paramètres DH DL). Conclure sur les limites du mode AT.

XI. Passage en mode API

- Utiliser le logiciel XCTU pour flasher les firmwares permettant d'utiliser les transmissions en API (XB24-ZB Coordinator ou router API).
- Vérifier que la transmission de données alphanumériques par l'intermédiaire du terminal du coordinateur vers les autres modules ne fonctionne plus.

1. Interrogation des paramètres via la trame 0x08 – réponse du module via une trame0x88

Envoyer via le terminal la trame suivante sur le port série du coordinateur : **7E 00 04 08 01 4D 59 50**

7E : Octet / Byte / 8 bits de Start
La trame pèse 4 octets (00 04)
Le format de trame utilisé correspond à l'envoi/questionnement d'AT Command au module. (08)
Le code de la requête (choisi arbitrairement) est ici 01
Le paramètre demandé est MY (4D 59)
Le Cheksum vaut 0xFF – (0x08 + 0x01 + 0x4D + 0x59) = 0x50

Rque : les trames de type 08 ne transitent pas par RF.

La réponse automatiquement générée par le coordinateur et transmise sur son port série doit être : **7E 00 07 88 01 4D 59 00 00 00 D0**

La trame de réponse présente 7 octets + le cheksum
C'est une trame de type réponse à une AT Command (88)
C'est la réponse à la requête 01, qui questionnait le paramètre MY (4D 59)
La requête s'est bien exécutée (00)
Le MY du coordinateur est 00 00.
La vérification du cheksum se fait en additionnant toutes les valeurs à partir de Frame Type (0x88). L'octet de poids faible de cet somme doit valoir 0xFF.

Reprendre les opérations sur les modules routeurs pour vérifier leurs adresses dynamiques.

2. Gestion du réseau en mode API

- Vérifier qu'en générant des trames de type 08 sur les ports série des routeurs vous pouvez vérifier leurs paramètres de connexion (ID, CH, AI, JN, NO, etc).
- Faire des *reset network* coté routeurs et observer les informations transmises. Modifier éventuellement le paramètre JN.
- Utiliser la commande ND pour scanner le réseau depuis le coordinateur et observer toutes les informations récupérées.
- Utiliser le frame type 0x10 pour transmettre une donnée de votre choix en broadcast puis unicast.
  Tester les différentes combinaisons d'adresses 64bits /16bits connues/inconnues/fausses/génériques...
- Utiliser le frame type 0x17 pour modifiercertains paramètres de vos routeurs depuis le coordinateur et implanter durablement vos modifications.
- Amusez-vous !

Références :

Building Wireless Sensor Networks (A practical guide to the Zigbbe mesh networking protocol). Robert Faludi - Editions O'reilly.
Xbee/Xbee-PR ZB RF Modules datasheet march 2015

NOTES :