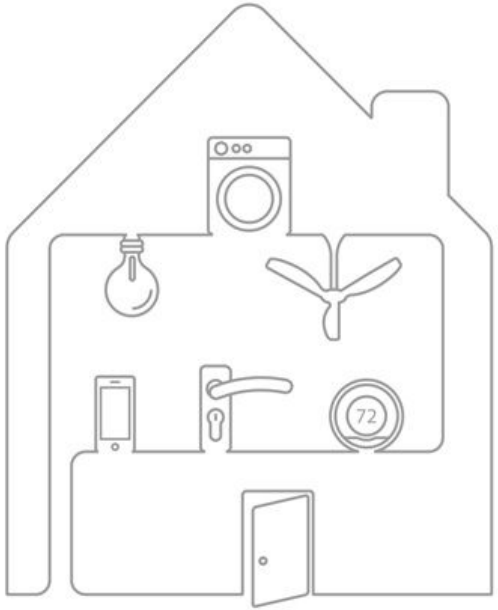


THREAD

Un protocole pour les gouverner tous ?

Pierre Piron, Léo Legron, Quentin Brunet

Protocole THREAD

Proposition d'un standard de communication open-source pour l'IoT

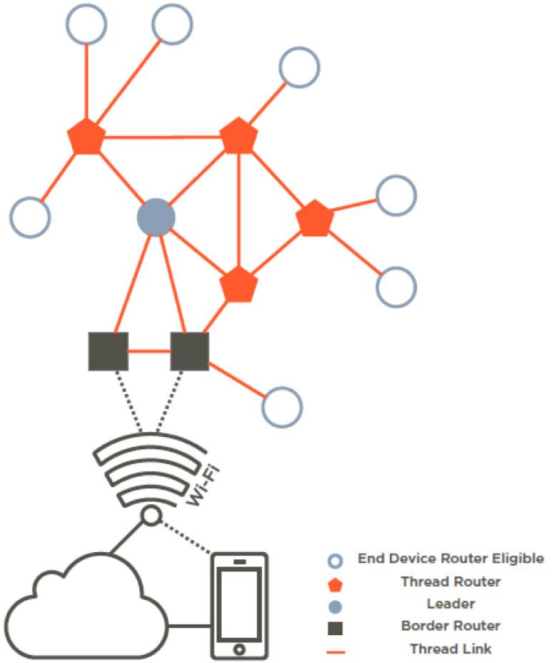
Device to Device, sans-fil, fiable et à faible consommation

Repose sur la technologie 6LoWPAN (utilise l'IPv6) elle-même basée sur le protocole 802.15.4-2006

Spécialement conçu pour la maison connectée, de quelques appareils à plus de 250 sur un seul réseau (PAN*)

Communique avec Internet sans médiateur

Coûts peu élevés



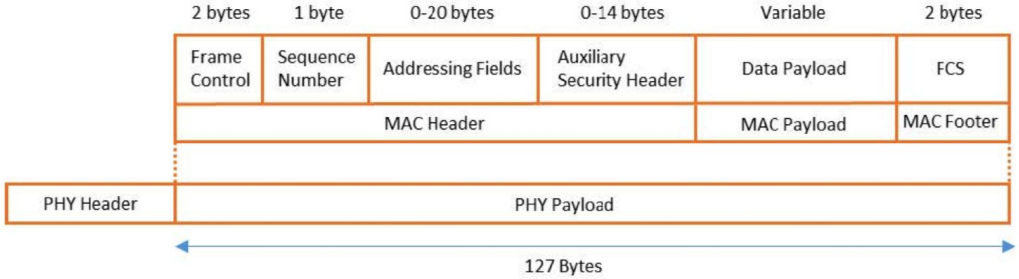
*PAN : Personal Area Network

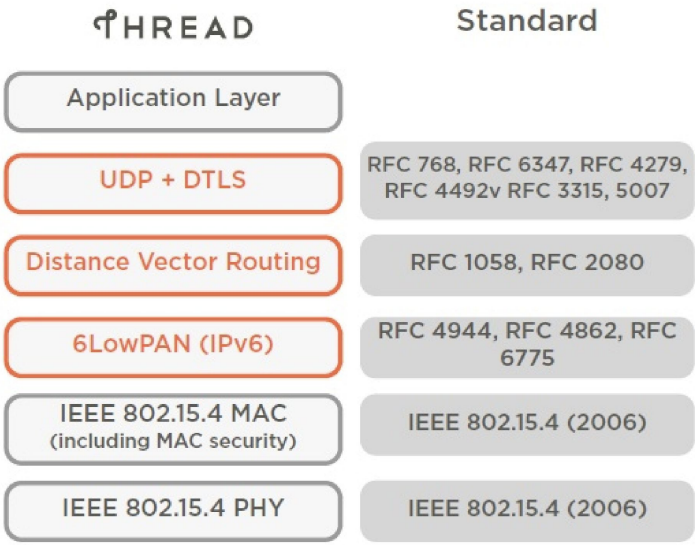
Couche Physique (PHY)

Basé sur IEEE* 802.15.4

Contient l'émetteur/récepteur radio (RF)

Communique à 250 kbps sur une la bande 2.4 GHz





*IEEE : Institute of Electrical and Electronics Engineers

Initiation de la communication (1/2)

Thread définit plusieurs types de noeuds à travers 2 grandes catégories :

- FFD (Full Function Device) appelé FTD (Full Thread Device) pour Thread
  - Routeur (qui peut-être simple routeur, Thread Leader ou Border Router)
  - REED (Router Eligible End Device)
  - FED (Full End Device)
- RFD (Reduced Function Device) appelé MTD (Minimal Thread Device) pour Thread
  - MED (Minimal End Device)
  - SED (Sleepy End Device)

Message MLE (Mesh Link Establishment)

- Propage les informations du réseau (leader data, network data, etc)
- Découvre les appareils voisins, la qualité des liens avec eux et établit de nouveaux liens

Initiation de la communication (2/2)

Scan actif du réseau pour trouver des réseaux 802.15.4

- Diffusion d'une balise sur chaque canal
- Réponse des routeurs et REEDs avec une balise contenant leur ID PAN et ID XPAN
- Décision de création d'un réseau ou d'adhérence à un réseau existant

Procédure

- Parent Request : requête multicast d'un parent
- Parent Response : réponse unicast de chaque parent éligible (routeur et REED)
- Child Id Request : requête unicast pour établir une relation Parent/Child
- Child Id Response : réponse unicast pour confirmer la relation

Topologie d'un réseau (1/2)

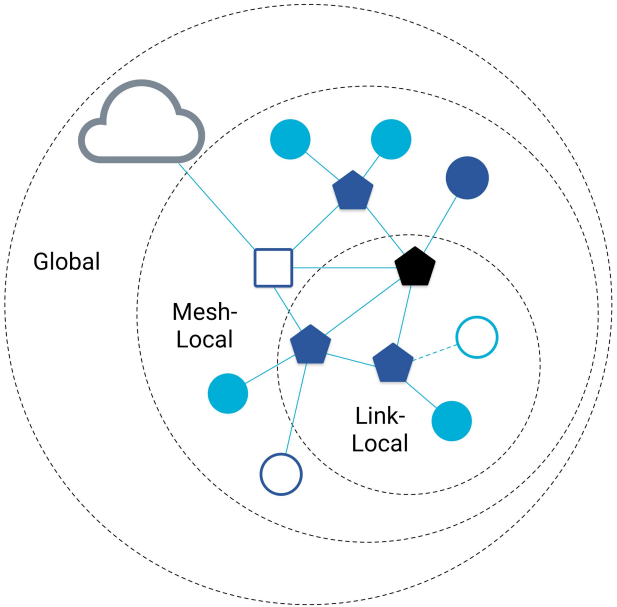
Thread est par défaut un **réseau maillé (mesh)** dynamique. Cependant, s'il n'est constitué que d'un seul routeur, alors il se comporte comme un réseau en étoile.

Distance Vector Routing : trouver le chemin critique (bi-dir)

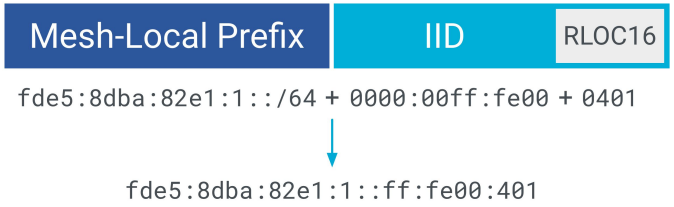
RLOC (Routing Locator) :

Exemple : 0000:00ff:fe00:***RLOC16***

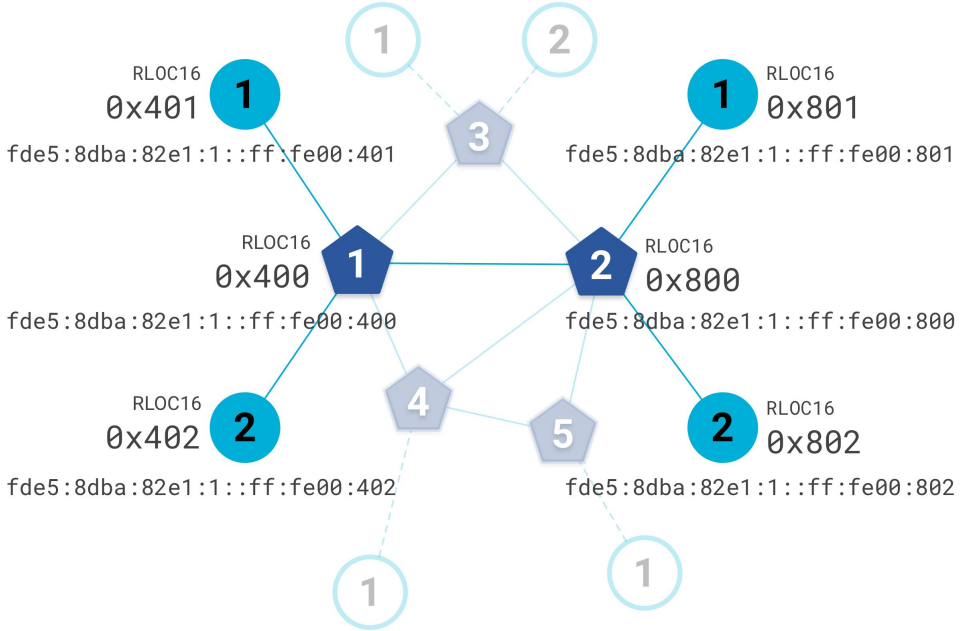
RLOC = 64 derniers bits d'une adresse IPv6



Topologie d'un réseau (2/2)



⚠️ Attention : Comme le RLOC dépend de la position du noeud dans la topologie, il peut changer.



Débit, consommation, portée, compromis ?

La portée est **faible**, suffisante pour couvrir une maison de taille normale (environ 40 mètres).

Chaque périphérique peut fonctionner pendant plusieurs années avec deux piles AA via un mode veille intelligent.

Suivant leur rôle, les devices push/pull à des rythmes différents. Les end devices sont 99% en veille et ne se réveillent que très ponctuellement, consommant ainsi un minimum d'énergie.

Compromis / Optimisations :

- Taille max des messages très faible (127 Bytes) pour limiter le taux d'erreur (BER — *the Bit Error Rate*)
- End Devices souvent "éteint"
- Mécanisme de compression des HEADERS de chaque paquet envoyé (par 6LoWPAN)

Sécurisation du réseau (1/2)

Pourquoi sécuriser ?

- Pour éviter la panne
- Pour prévenir les attaques OTAs (Over The Air)
- Pour prévenir les attaques par internet

Comment sécuriser ?

- Utilisation d'une clef de chiffrement des adresses MAC, partagée sur le réseau (standard IEEE 802.15.4-2006)
- Communication entre noeuds avec handshake, ack et retries
- Chaque noeud cache son IP et son adresse MAC
- DTLS (Data Transport Layer Security) avec les borders routers

Sécurisation du réseau (2/2)

What's (already) in the box ?

Avec Thread, un certain nombre de dispositifs préventifs sont déjà en place :

- Pas de SPOF* dans un réseau maillé, si un routeur tombe, les autres prennent la relève
- Si un appareil redémarre, il peut se reconnecter seul (data du réseau stockées en mémoire : PAN ID, informations d'adressage)
- Rejoindre un réseau nécessite d'y être autorisé par un "commissioning router"

Par ailleurs, la couche MAC de la norme 802.11 définit une méthode dite CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) utilisée par Thread et différente de CSMA/CD (with Collision Detection).

*SPOF : Single Point Of Failure

Démonstration 💻✨

Sources 

- https://openthread.io
- https://www.silabs.com/documents/public/user-guides/ug103-11-appdevfundamentals-thread.pdf
- https://www.threadgroup.org/Portals/0/documents/support/ThreadOverview_633_2.pdf
- https://standards.ieee.org/standard/802_15_4-2006.html

Merci de nous avoir écouté.

Des questions ? 🤗