Zigbee, domotic and open source !

Alexis Lothoré – Meetup 02/18

What will we see ?

- Zigbee : what is it ?
- Zigbee fundamentals
- Our case : the « bulb issue »
- Implementing our very own gateway : steps and feedback
- Next steps and improvements

- Zigbee : what is it ?
- Zigbee fundamentals
- Our case : the « bulb issue »
- Implementing our very own gateway : steps and feedback
- Next steps and improvements

Zigbee : what is it ?

- Radio protocol for IoT
- Goals : simplicity, low cost and low energy, scalable
- Specified by Zigbee Alliance
- EU : 868Mhz/2,4Ghz

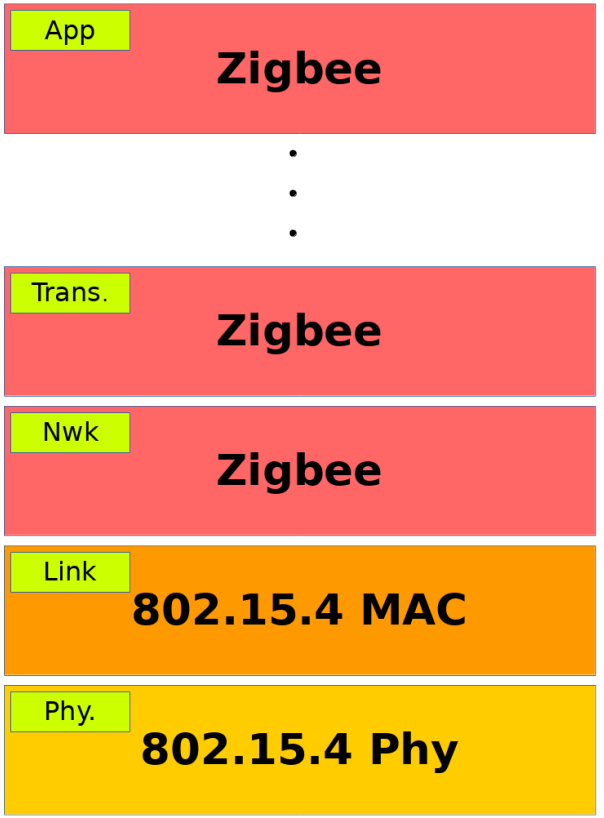
www.zigbee.org

Zigbee : what is it ?

http://www.zigbee.org/zigbeealliance/our-members/

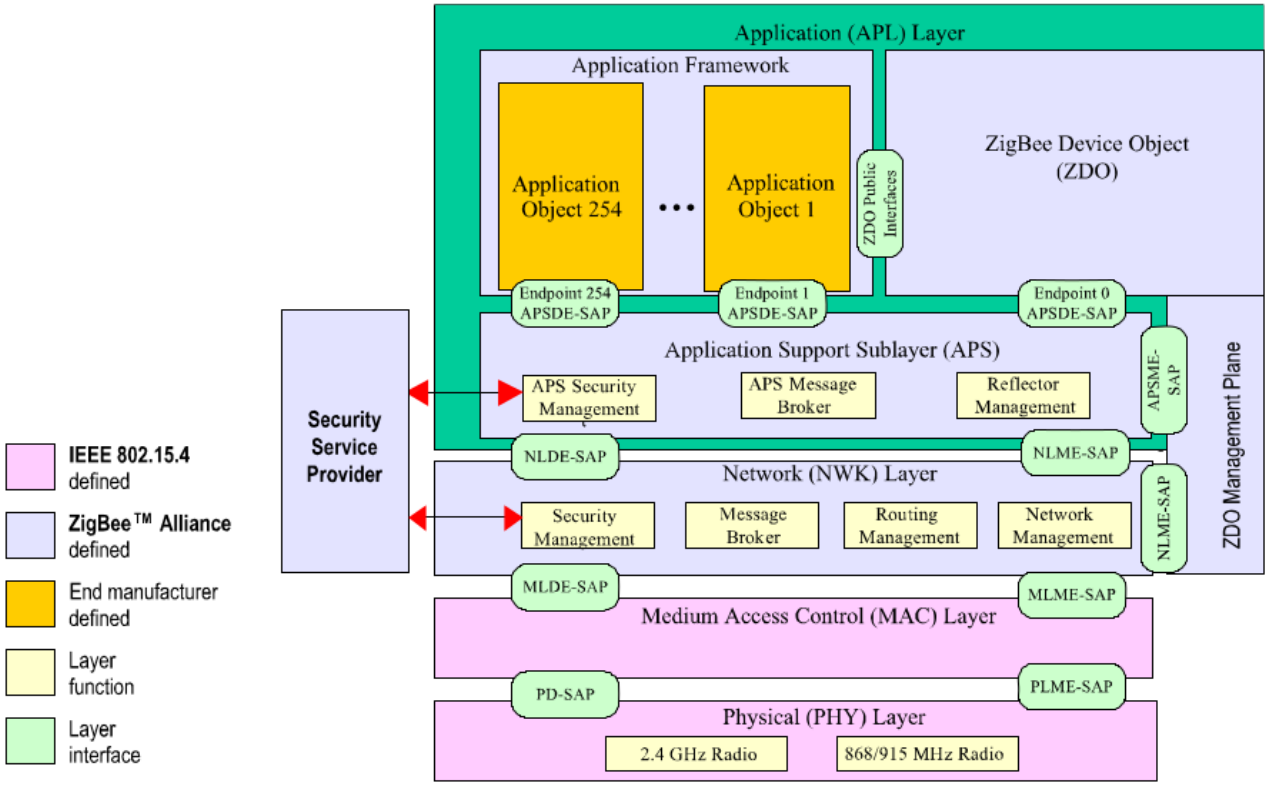
- Zigbee : what is it ?
- Zigbee fundamentals
- Our case : the « bulb issue »
- Implementing our very own gateway : steps and feedback
- Next steps and improvements

Zigbee fundamentals



=> Zigbee protocol takes multiple OSI layers in charge

Zigbee fundamentals

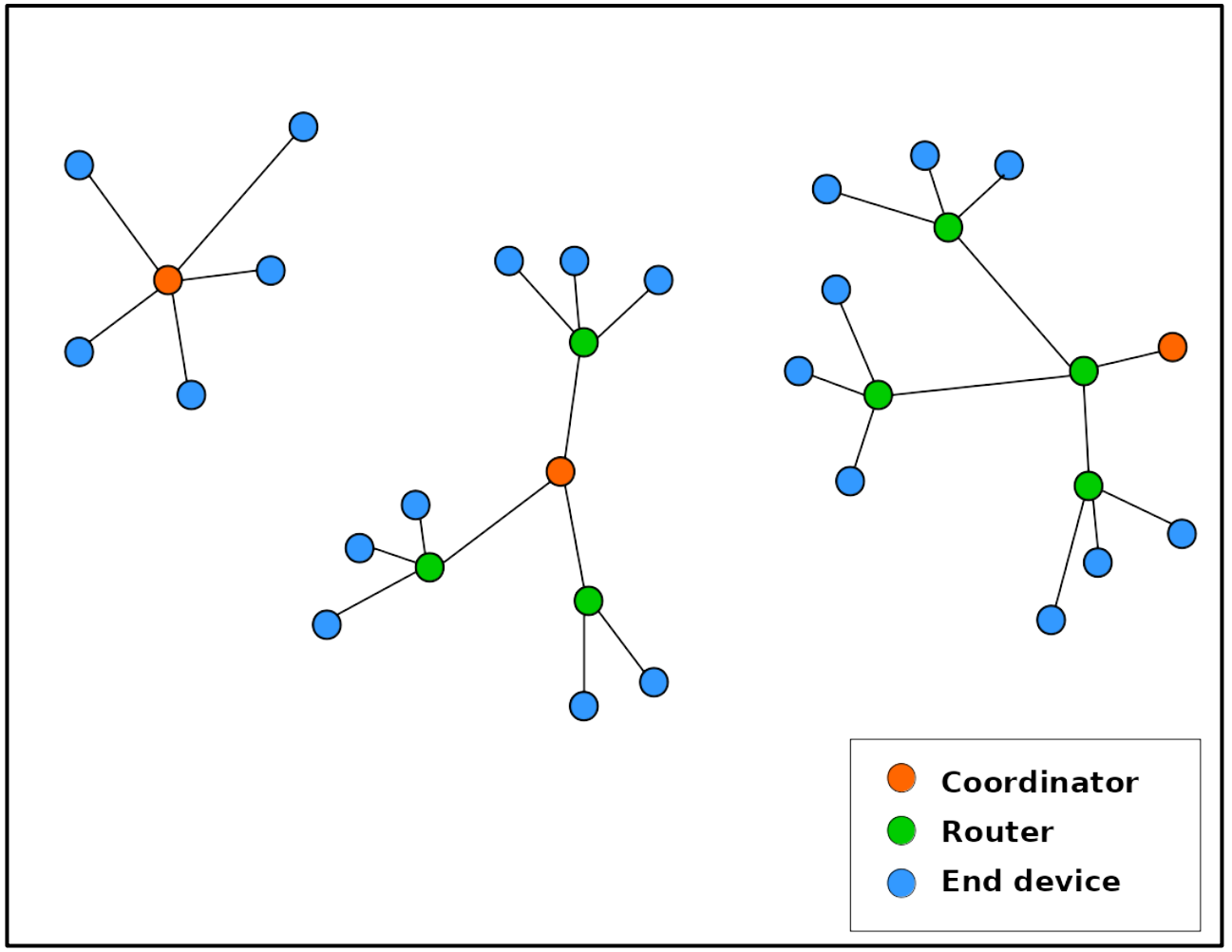


Zigbee specification

- NWK : network layer
- APS : Application Support Sublayer
- ZDO : Zigbee Device Object
- AF : Application framework

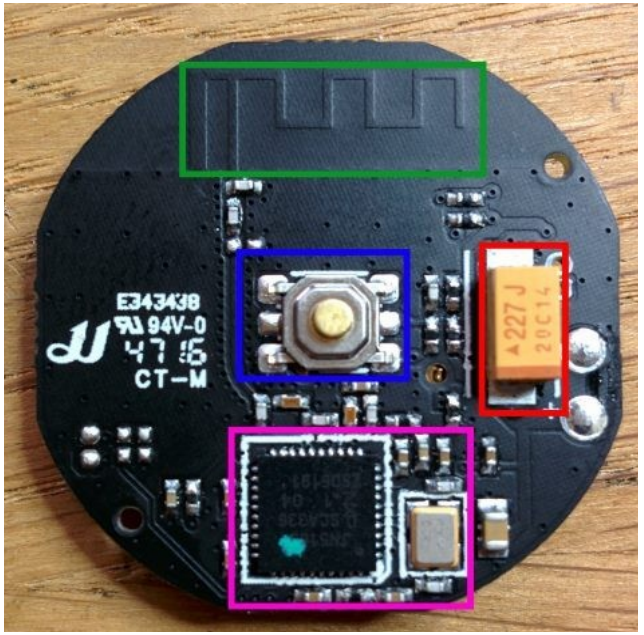
Zigbee fundamentals

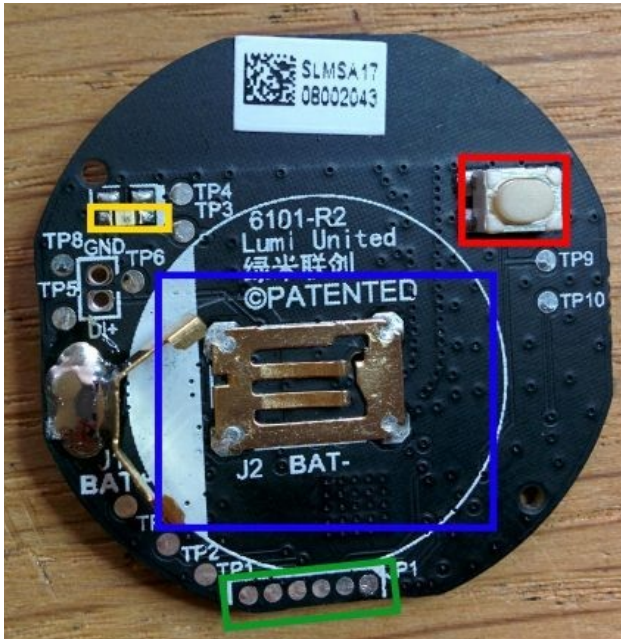
- Different network topologies



Zigbee fundamentals

- Low power nodes





https://faire-ca-soi-meme.fr/domotique/2017/04/15/test-xiaomi-mijia-6-in-1-smart-home/

Zigbee fundamentals

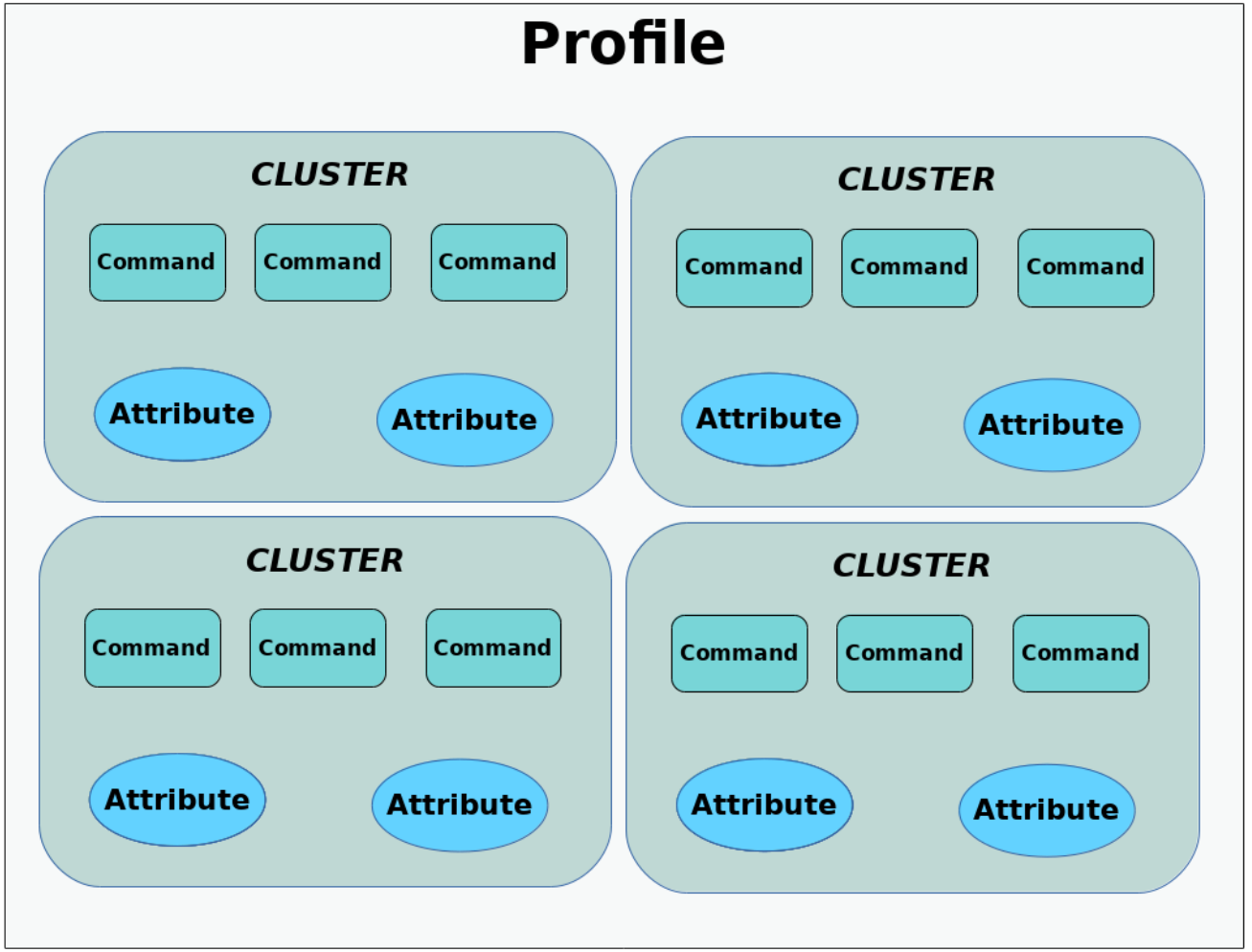
- Routing features
  - Coordinator (and possibly routers) have/has a routing table, and a route discovery table
  - Route requests/replies between nodes to establish and maintain routes : unicast, multicast, many-to-one
  - Routing based on path cost algorithm, with cost variable and estimation set by each manufacturer.
  - Can be driven from higher layers of protocol

Zigbee fundamentals

- Security
  - Based on 128 bits symmetric keys
  - Application security (link key) and/or network security (network key)
  - Key retrievement ?
    - Key transport
    - Key establishement
    - Pre-installation
  - Presence of a « Trust Center »

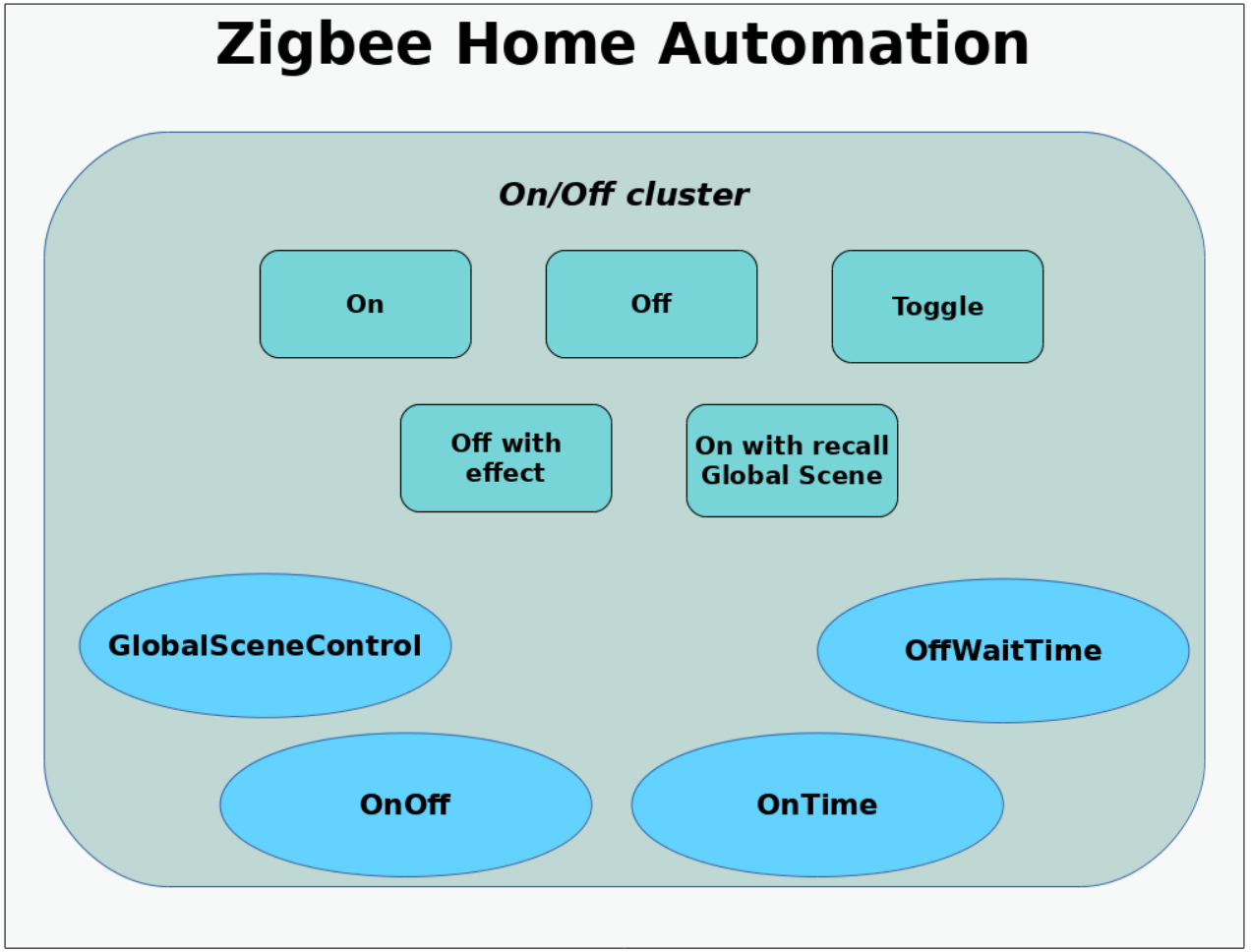
Zigbee fundamentals

- Application framework



Zigbee fundamentals

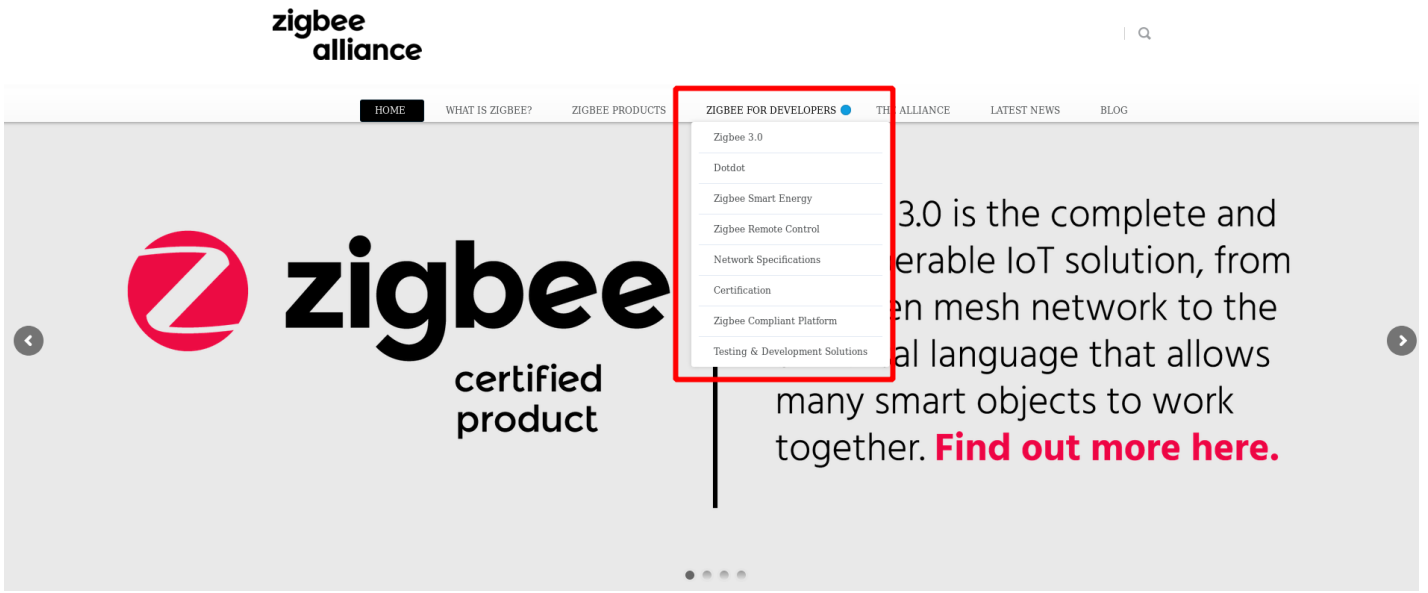
- Application framework



Sources

To Go Further :

- Zigbee specification
- Zigbee Cluster Library Specification
- Zigbee Home Automation Public Application profile



www.zigbee.org

- Zigbee : what is it ?
- Zigbee fundamentals
- Our case : the « bulb issue »
- Implementing our very own gateway : steps and feedback
- Next steps and improvements

Our case : the « bulb issue »

Goals :

- add the bulb to my domotic environment
- If successful, add different devices to it
- With a (very) low cost solution, and embedded
- Software part must be open source
- Increase skills : Zigbee learning

« So you have got a Hue lamp ? Great, now go buy a bridge and download the app ! »

Nope !

Our case : the « bulb issue »

Existing solutions

zigbee-shepherd

kappaIO

cc-znp

ZiGate

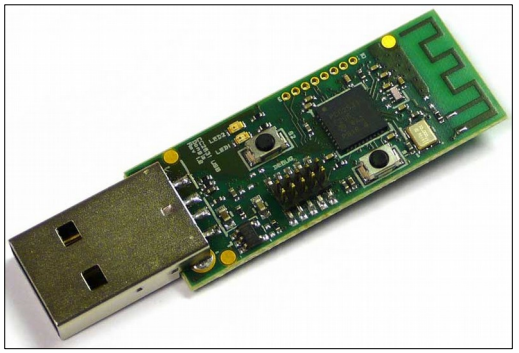
Does not totally fit my needs

- Zigbee : what is it ?
- Zigbee fundamentals
- Our case : the « bulb issue »
- Implementing our very own gateway : steps and feedback
- Next steps and improvements

Implementing our very own gateway

First step : select the hardware for
- Our gateway
- The dev tools (e.g. : sniffer)

The contenders :



www.ti.com

CC253X

VS

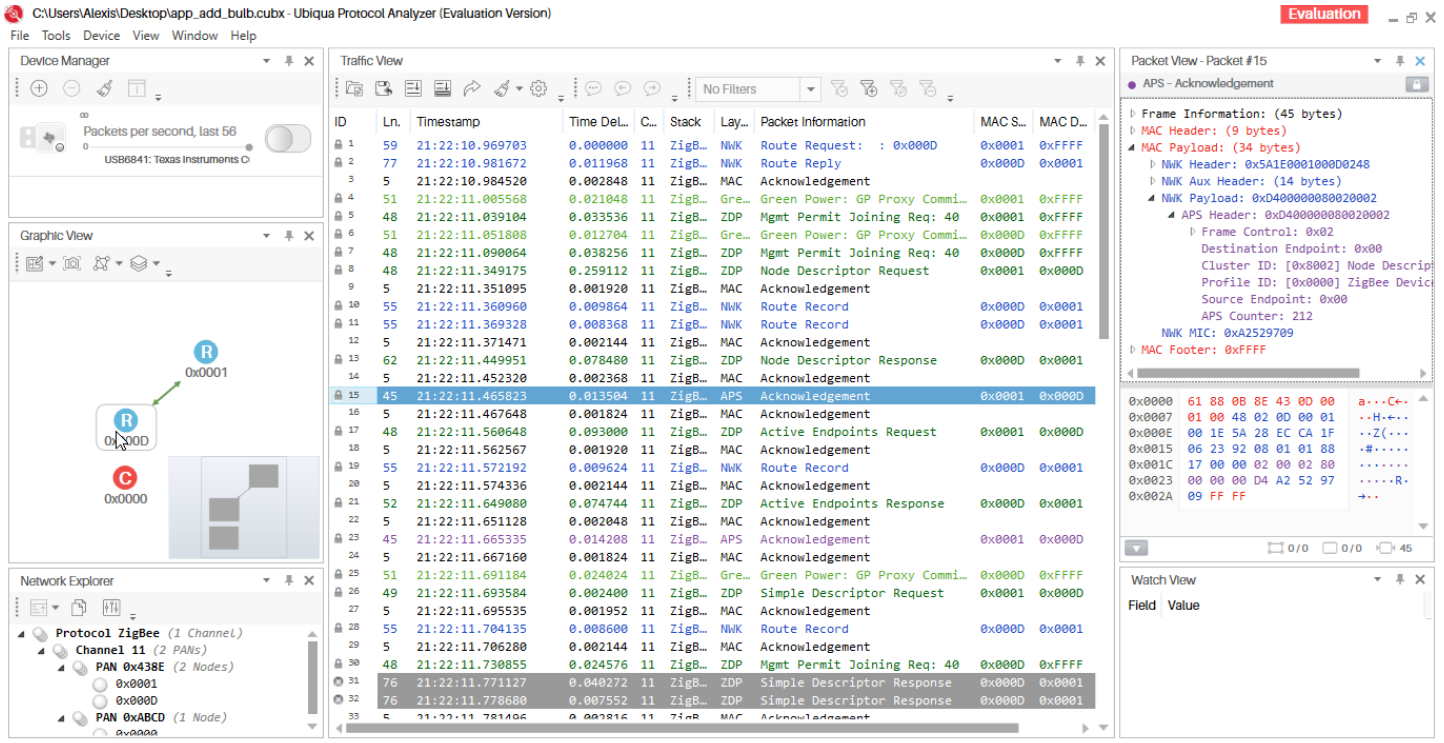
www.nxp.com

JN516x

Implementing our very own gateway

Second step : select the software for sniffing/debugging

The ultimate IoT (Zigbee) radio sniffer : Ubiqua



Implementing our very own gateway

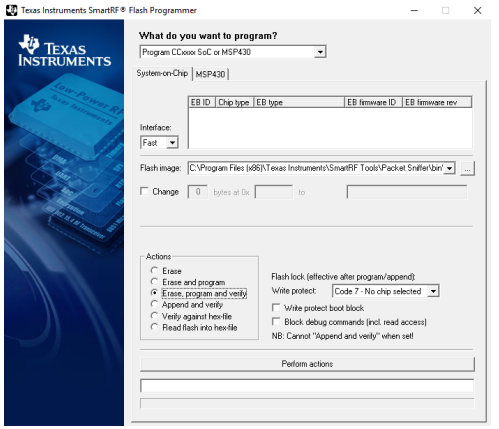
Third step : mix it !

http://www.ti.com/tool/Z-STACK

http://www.ti.com/tool/CC-DEBUGGER

sniffer_fw_cc2430.hex	12/06/2014 14:39	Fichier HEX	10 Ko
sniffer_fw_cc2530.hex	19/06/2014 10:07	Fichier HEX	9 Ko
sniffer_fw_cc2531.hex	19/06/2014 10:07	Fichier HEX	23 Ko
sniffer_fw_cc2533.hex	19/06/2014 10:07	Fichier HEX	8 Ko
sniffer_fw_cc2540.hex	19/06/2014 10:07	Fichier HEX	28 Ko
sniffer_fw_cc2540_uart.hex	12/06/2014 14:39	Fichier HEX	24 Ko
sniffer_fw_cc2540_usb.hex	19/06/2014 10:07	Fichier HEX	47 Ko
sniffer_fw_cc2544.hex	19/06/2014 10:07	Fichier HEX	26 Ko
sniffer_fw_ccxx10_usart0_alt1.hex	12/06/2014 14:39	Fichier HEX	7 Ko
sniffer_fw_ccxx10_usart1_alt2.hex	12/06/2014 14:39	Fichier HEX	7 Ko
sniffer_fw_ccxx11.hex	12/06/2014 14:39	Fichier HEX	21 Ko

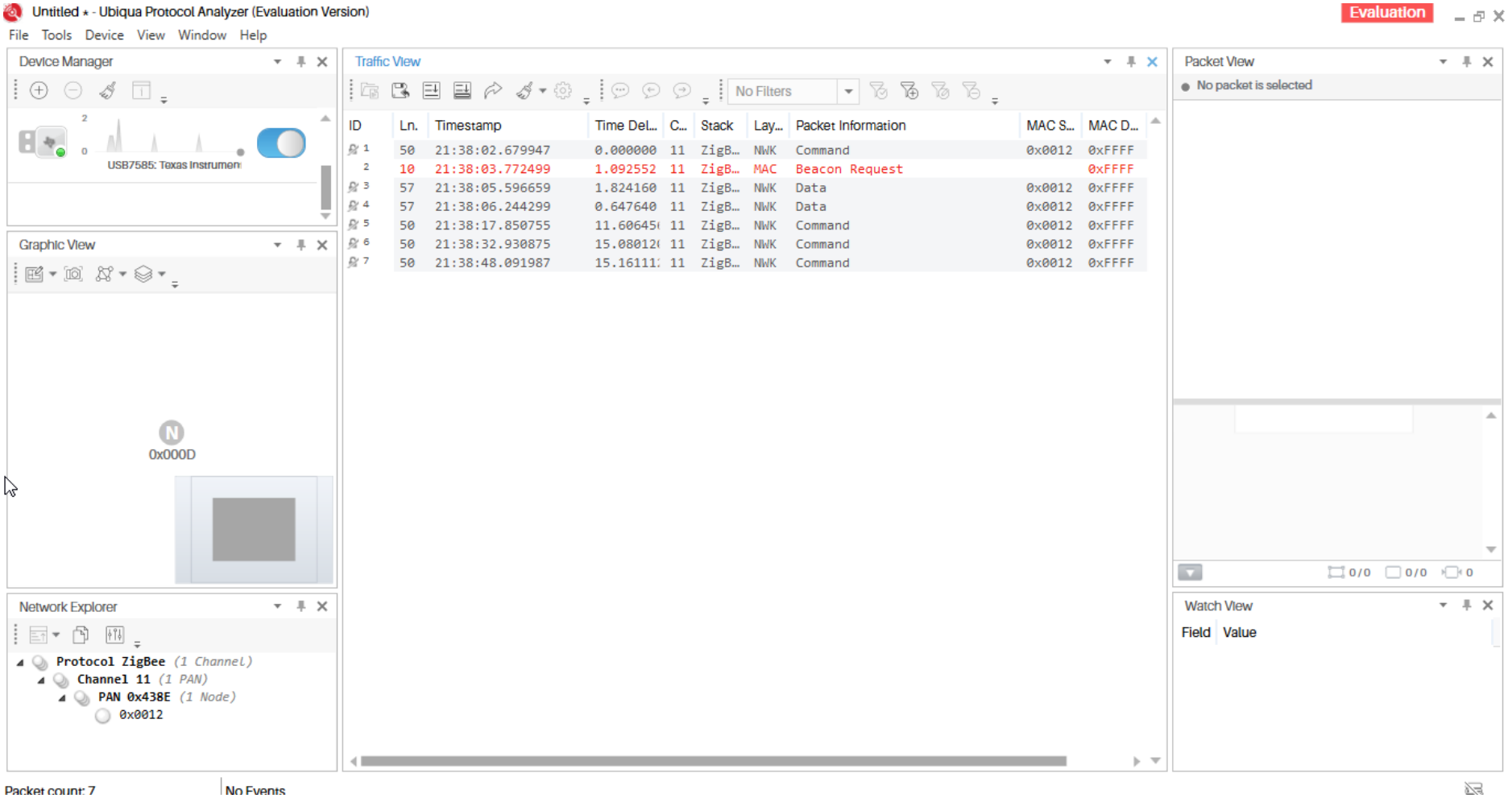
C:\\Program Files(x86)\Texas Instruments\SmartRF Tools\ Packet Sniffer\bin\general\firmware



C:\\Program Files(x86)\Texas Instruments\SmartRF Tools\ Flash Programmer\bin

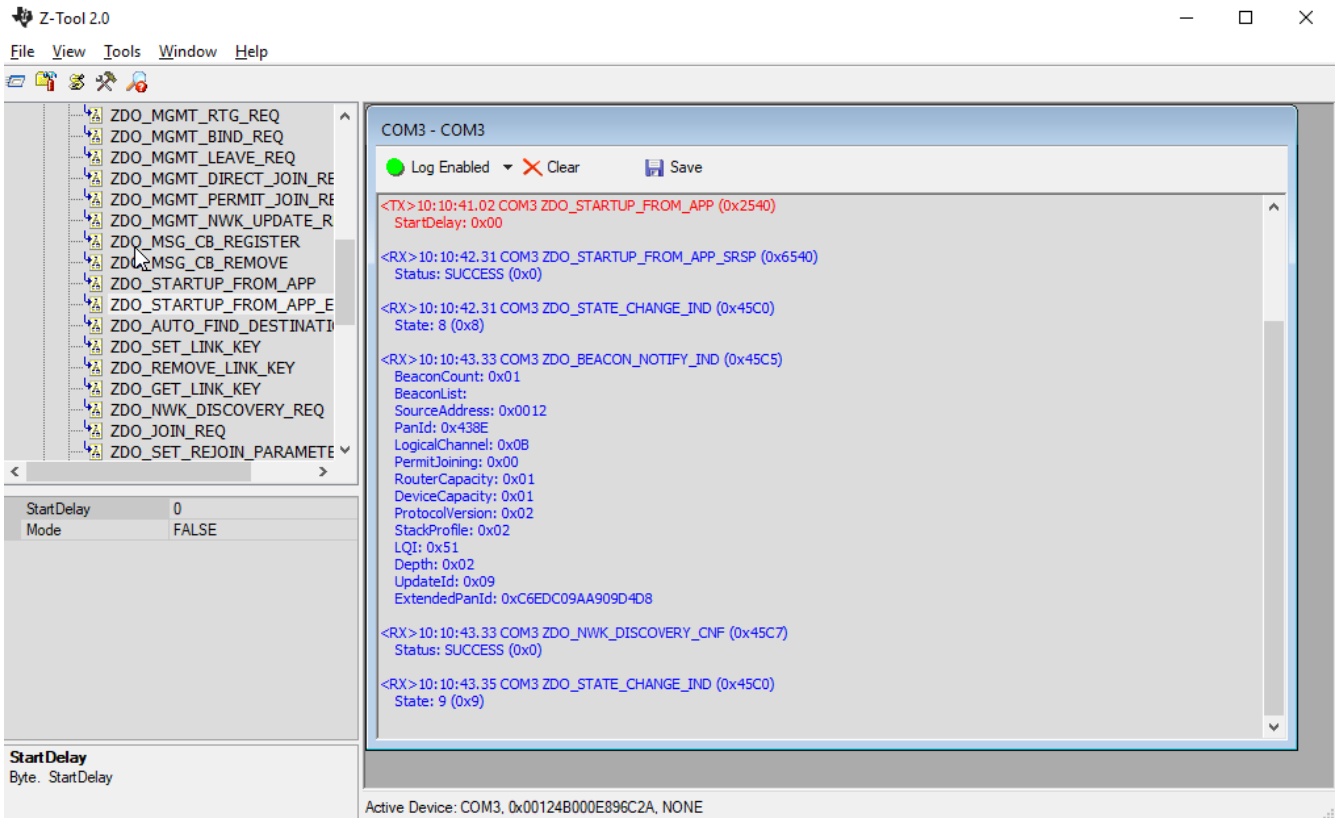
Implementing our very own gateway

Switch the bulb on !



Implementing our very own gateway

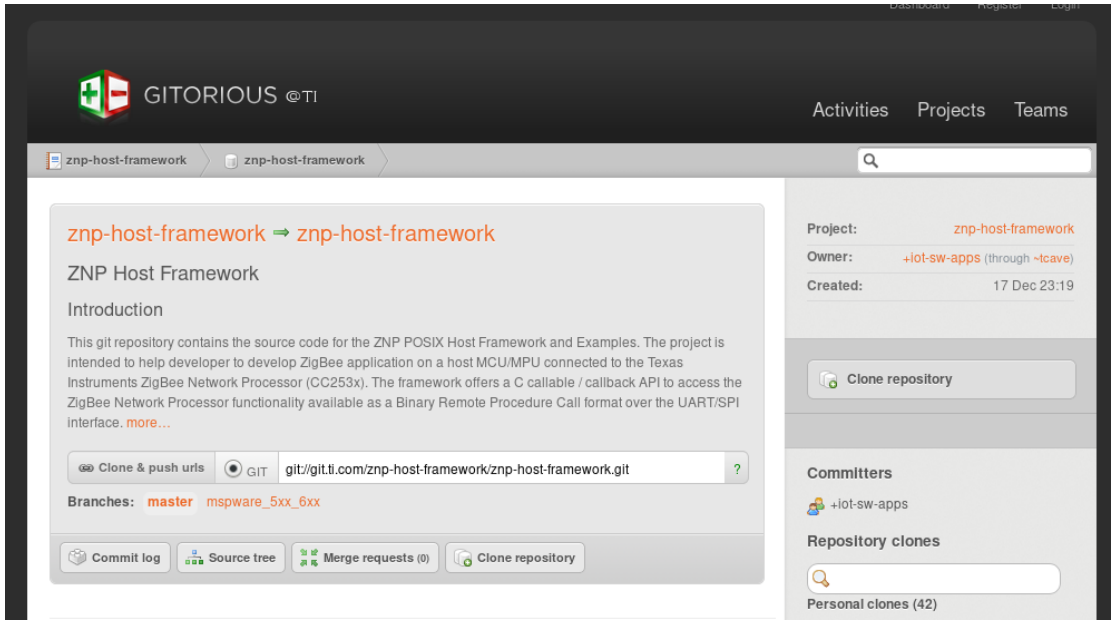
First interactions with bulb : Z-Tool and ZNP firmware



Firmware : C:\\Texas Instrument\Z-Stack 3.0.1\Projects\HomeAutomation\GenericApp\CC2531

Implementing our very own gateway

Going further : ZNP host in C



https://git.ti.com/znp-host-framework/znp-host-framework

- RPC (remote procedure call) processing : physical medium
- MT (Monitor and Test) processing : commands
  - MT_SYS
  - MT_ZDO
  - MT_AF
  - MT_UTILS
  - …
- Firmwares
- Example binaries

Implementing our very own gateway

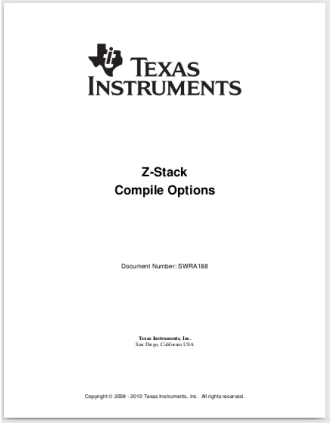
ZNP Recipe

http://www.ti.com/tool/Z-STACK

http://www.ti.com/tool/CC-DEBUGGER

GenericApp,
Home automation project

https://www.iar.com/iar-embedded-workbench/#!?device=CC2531F128&architecture=8051

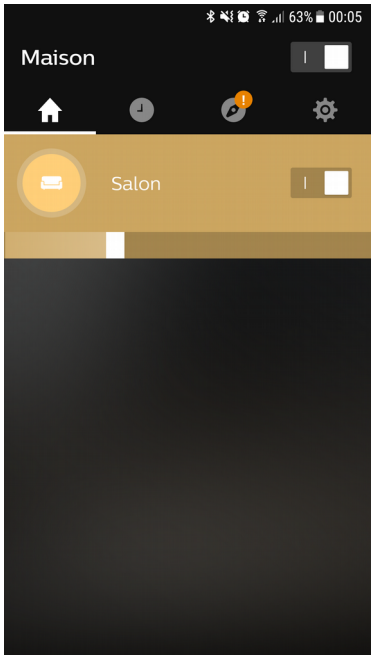


http://e2e.ti.com/cfs-file/__key/communityserver-discussions-components-files/158/4606.z_2d00_stack-compile-options.pdf

Implementing our very own gateway

Hue bridge « reverse engineering »

Hue bridge

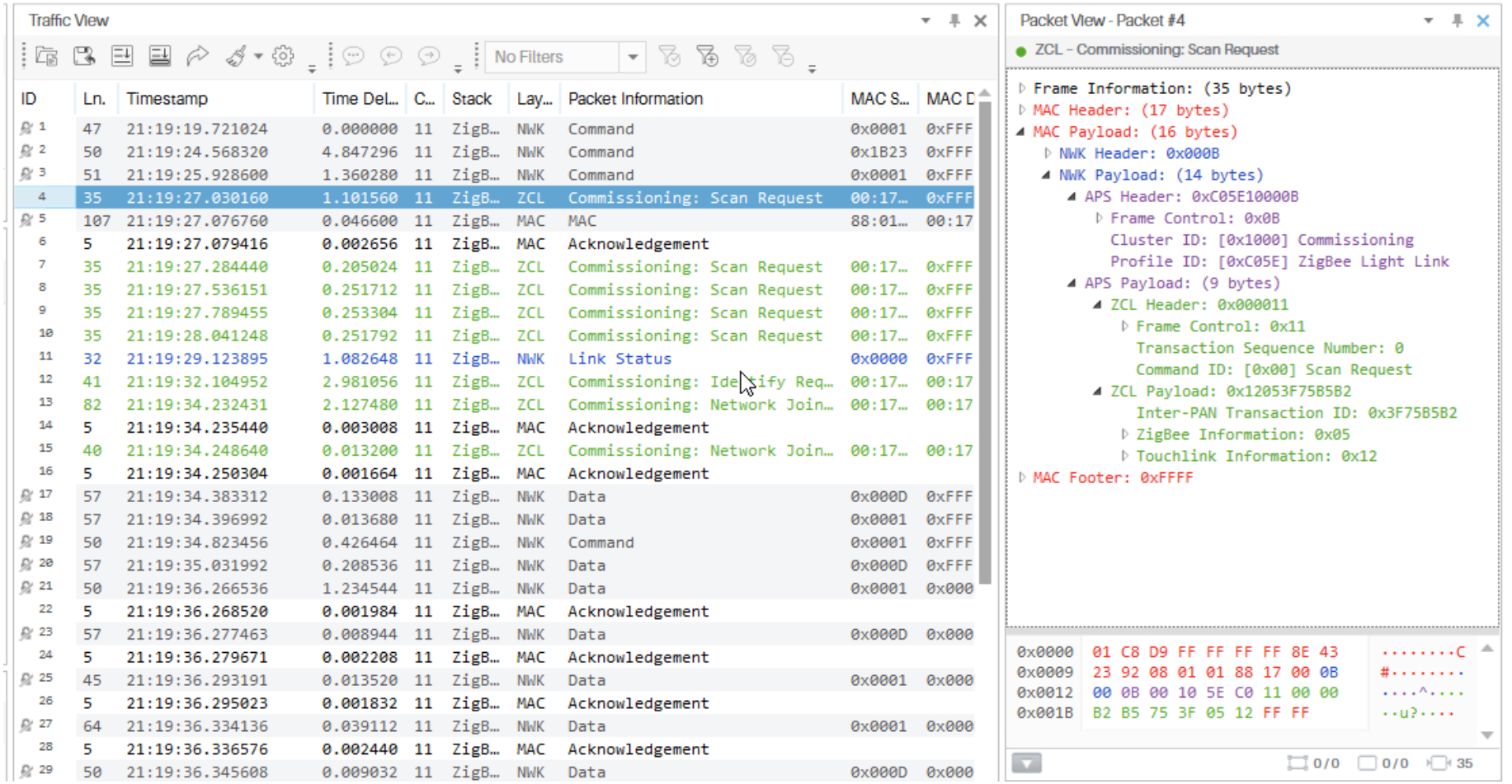


Android App

Goal : intercept trafic between Hue bridge and lamp, during a « touchlink » procedure

Implementing our very own gateway

Bulb/bridge first capture while pairing



Implementing our very own gateway

Going further in Zigbee Light Link Standard

Cluster Id	Cluster Name
0x0000	Basic
0x0003	Identify
0x0004	Groups
0x0005	Scenes
0x0006	On/Off
0x0008	Level Control
0x0300	Color Control
0x1000	Commissioning

ZLL Clusters

Implementing our very own gateway

Going further in ZLL Commissioning Cluster

	Command identifier field value	Description	Mandatory/ optional	Reference
Touchlink	0x00	Scan request	Mandatory	7.1.2.2.1
	0x02	Device information request	Mandatory	7.1.2.2.2
	0x06	Identify request	Mandatory	7.1.2.2.3
	0x07	Reset to factory new request	Mandatory	7.1.2.2.4
	0x10	Network start request	Mandatory	7.1.2.2.5
	0x12	Network join router request	Mandatory	7.1.2.2.6
	0x14	Network join end device request	Mandatory	7.1.2.2.7
	0x16	Network update request	Mandatory	7.1.2.2.8
	All other values in the range 0x00 – 0x3f	Reserved	-	-
Utility	0x41	Get group identifiers request	Mandatory[6]	7.1.2.2.9
	0x42	Get endpoint list request	Mandatory[6]	7.1.2.2.10
	All other values in the range 0x40 – 0xff	Reserved	-	-

?

	Command identifier field value	Description	Mandatory/ optional	Reference
Touchlink	0x01	Scan response	Mandatory	7.1.2.3.1
	0x03	Device information response	Mandatory	7.1.2.3.2
	0x11	Network start response	Mandatory	7.1.2.3.3
	0x13	Network join router response	Mandatory	7.1.2.3.4
	0x15	Network join end device response	Mandatory	7.1.2.3.5
	All other values in the range 0x00 – 0x3f	Reserved	-	-
Utility	0x40	Endpoint information	Mandatory[7]	7.1.2.3.6
	0x41	Get group identifiers response	Mandatory[7]	7.1.2.3.7
	0x42	Get endpoint list response	Mandatory[7]	7.1.2.3.8
	All other values in the range 0x40 – 0xff	Reserved	-	-

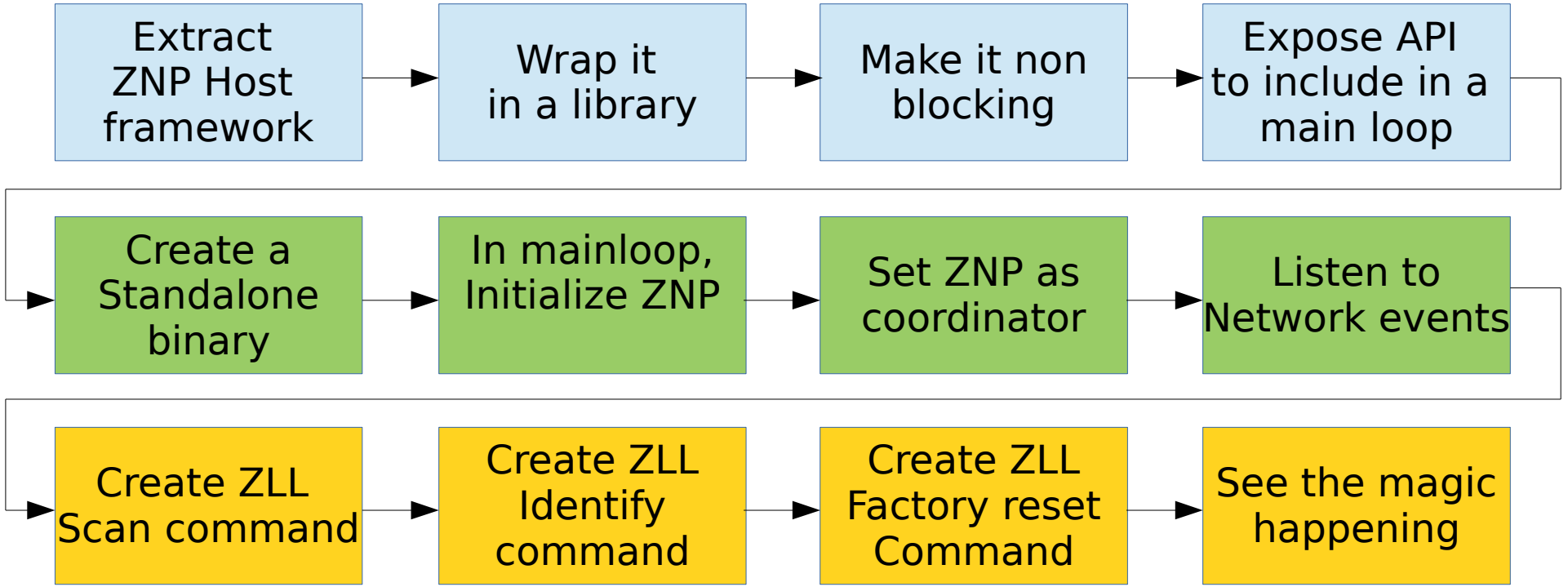
ZLL Commissioning cluster client commands

ZLL Commissioning cluster server commands

Zigbee Light Link Standard,
http://www.zigbee.org/zigbee-for-developers/applicationstandards/zigbee-light-link/

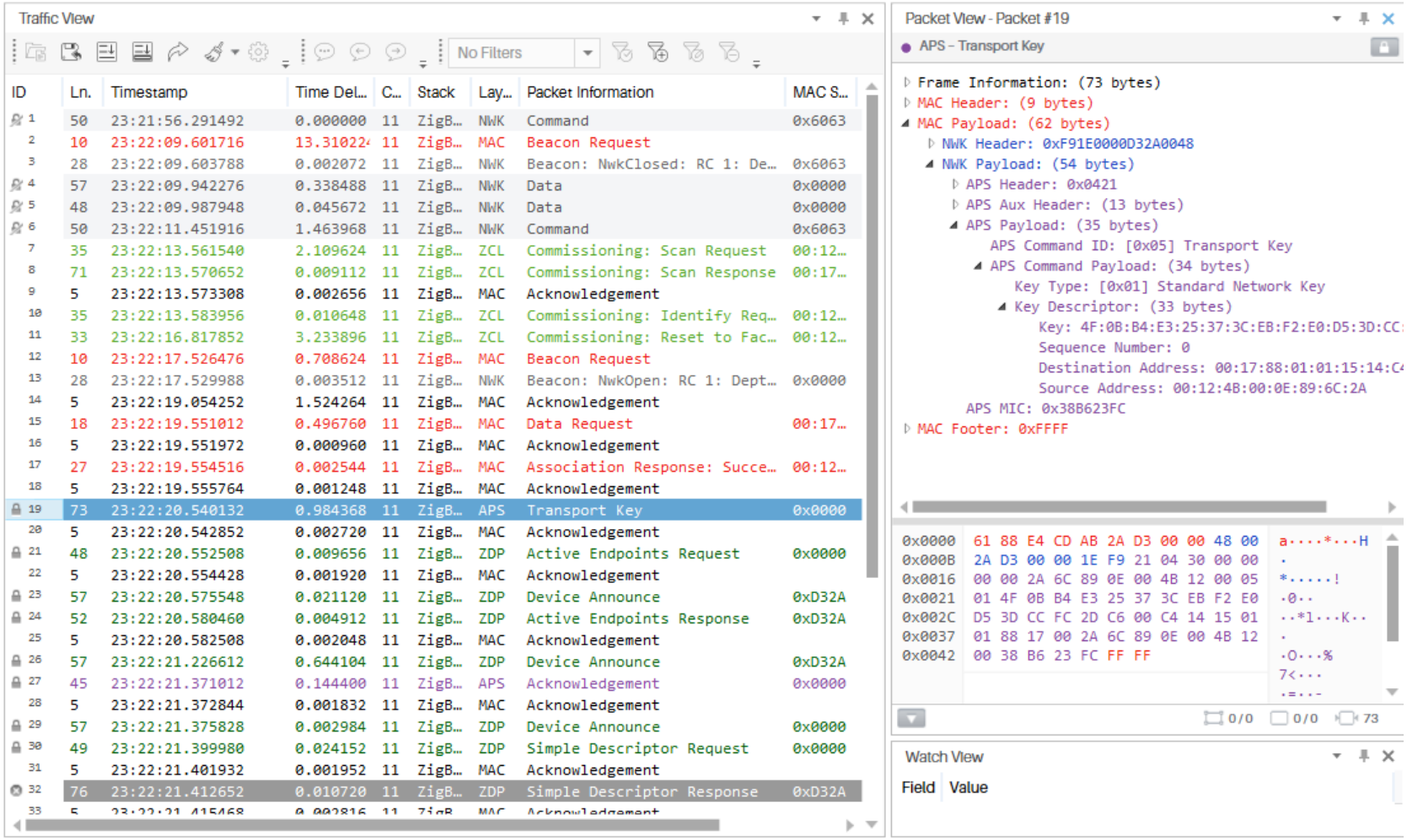
Implementing our very own gateway

Let’s start building serious things !



Implementing our very own gateway

The lamp has joined the network !



Implementing our very own gateway

Let’s play with ou newly installed device

Identifier	Name
0x00	Move to hue
0x01	Move hue
0x02	Step hue
0x03	Move to saturation
0x04	Move saturation
0x05	Step saturation
0x06	Move to hue and saturation
0x07	Move to color
0x08	Move color
0x09	Step color
0x0a	Move to color temperature

Color control cluster commands

Command Identifier Field Value	Description	M/O
0x00	Off	M
0x01	On	M
0x02	Toggle	M
0x40	Off with effect	O
0x41	On with recall global scene	O
0x42	On with timed off	O

On/Off cluster commands

Octets	1	1
Data Type	uint8	uint8
Field Name	Effect identifier	Effect variant

« Off with effects » command parameters

Implementing our very own gateway

Playing with a new device : Xiaomi smart button

Some main differences :

- Sleeping node : only up when button state changes
- Hardcoded endpoints (new profile : Zigbee Home Automation)
- Difficult to read devices properties

Procedure :

- Hard reset button
- Wait for it to join network
- Push button : report button state visible
- On/Off cluster again !

Xiaomi Smart Button

Implementing our very own gateway

Playing with a new device : Xiaomi room sensor

Procedure :

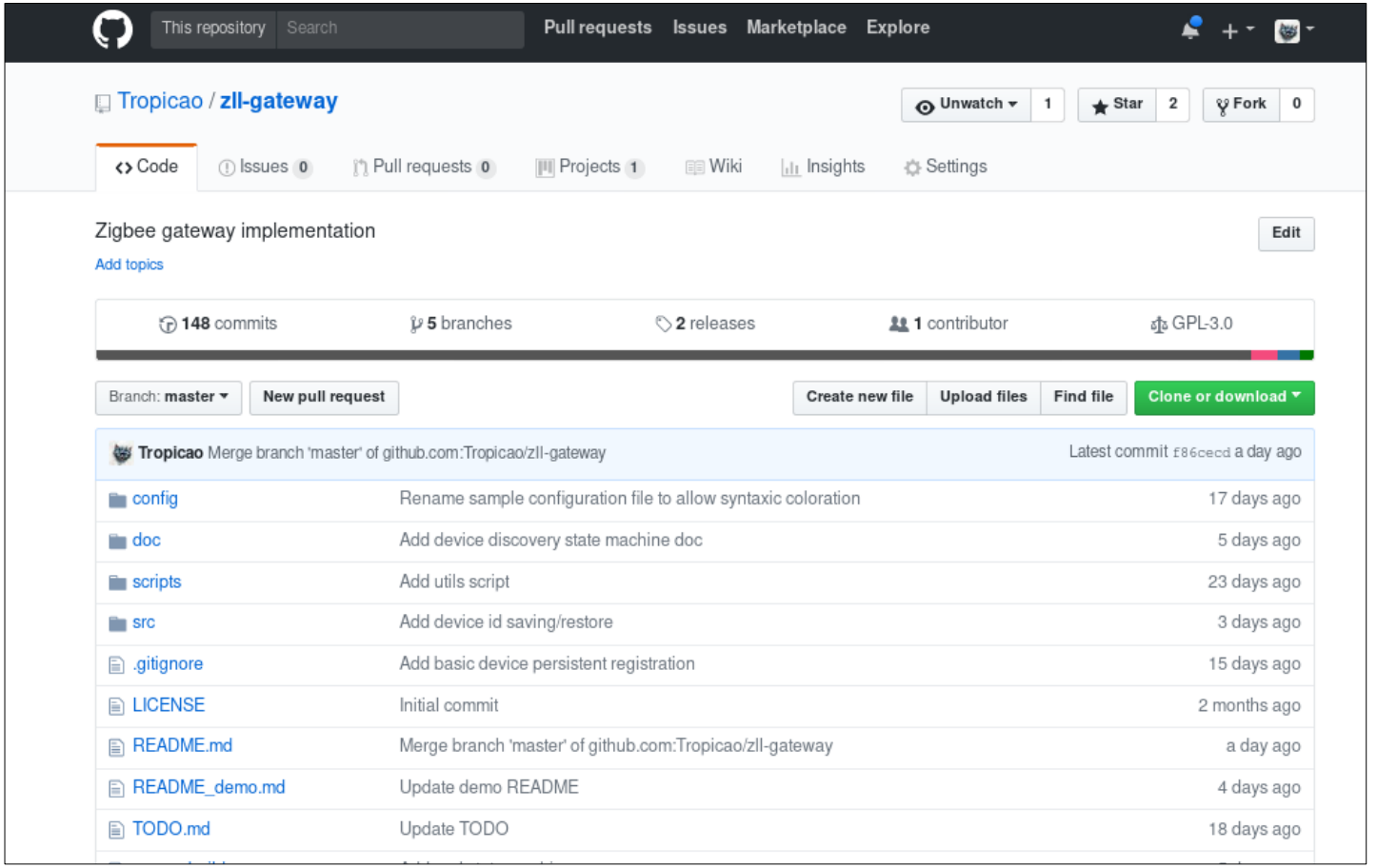
- Hard reset button
- Wait for it to join network
- Changes on temperature : new temperature report
- New cluster : temperature measurement
- New command : report attribute

Xiaomi room sensor

- Zigbee : what is it ?
- Zigbee fundamentals
- Our case : the « bulb issue »
- Implementing our very own gateway : steps and feedback
- Next steps and improvements

Next steps and improvements

Current status



git@github.com:Tropicao/zll-gateway.git

Next steps and improvements

Some major features are still missing...

- Multi-channel management
- Groups management
- ZLL : proper device install (i.e. no « raw » reset for install)
- Generic device management
- Remote devices configuration (e.g. : reporting frequency)

Next steps and improvements

... and a lot of products are to be supported !

osram-lamps.fr
domo-attitude.fr
high5gadgets.ie

alexis.lothore@gmail.com

https://github.com/Tropicao