ไฟฟ้า

FAIFA

A first OpenSource PLC tool

Xavier Carcelle - xavier.carcelle#openpattern.org
Florian Fainelli – florian.fainelli#openpattern.org
Nicolas Thill – nico#openwrt.org

FAIFA in Lao Langage

- ໄຟຟ້າ = FAIFA
- ໄຟ : Fire
- ຟ້າ : Light
- FAIFA = Faï + Fa
- Laos = country between Thailand and Vietnam with large electrical ressources but very low income per person

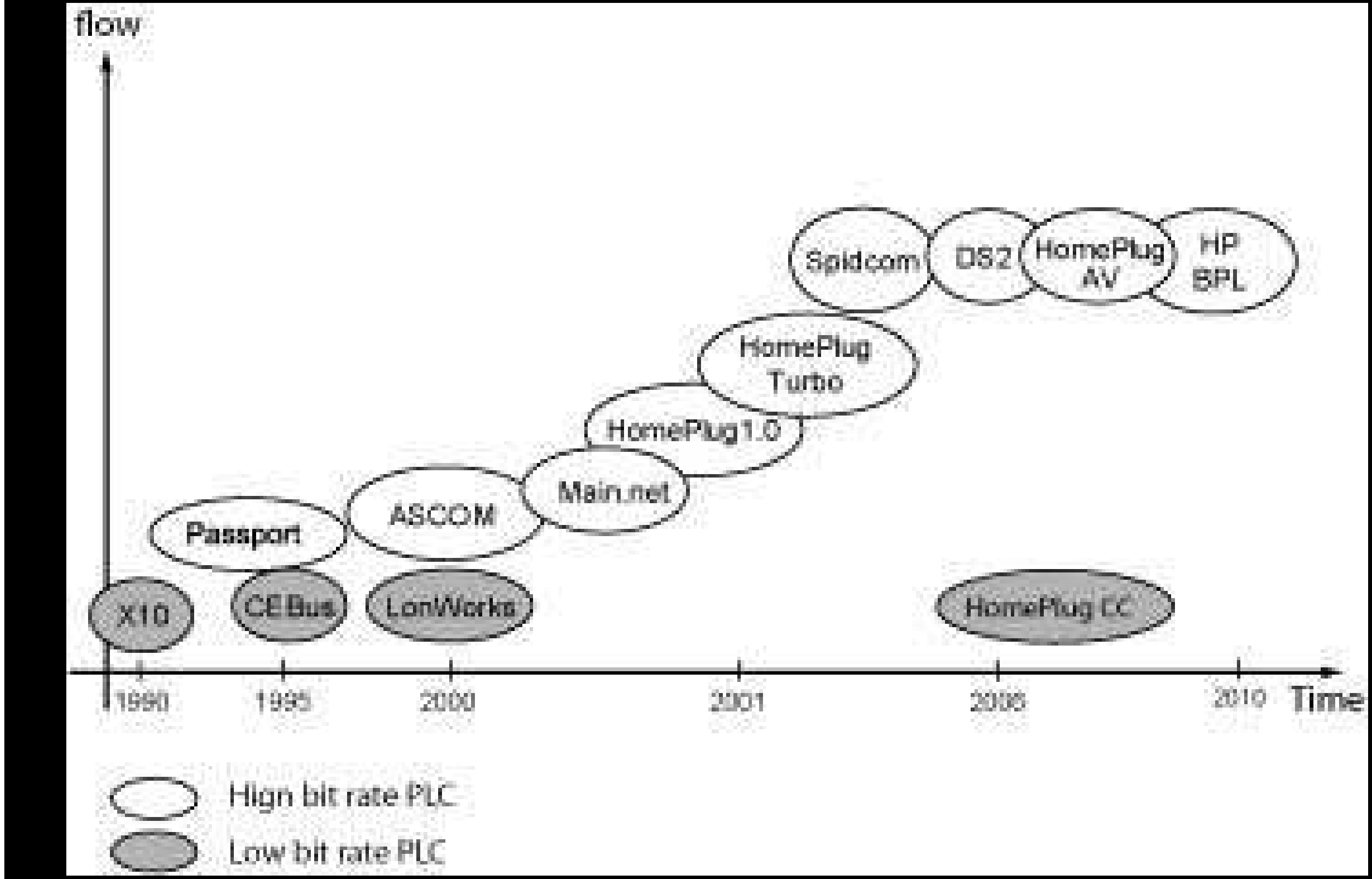
0x00 - Outline

- ***0x01 - PowerLineCommunications 101 class***
  - *Technology introduction*
  - *PHY/MAC layers in PLC*
  - *Security issues in PLC*
- ***0x02 - Targeting HomePlug AV***
  - *H/W implementations*
  - *On-board designs*
  - *Potential exploits*
- ***0x03 - Explaining the FAIFA tool***
  - *Existing open tool for PLC*
  - *Features / Tool design*
  - *Demo*
  - *Coming next*

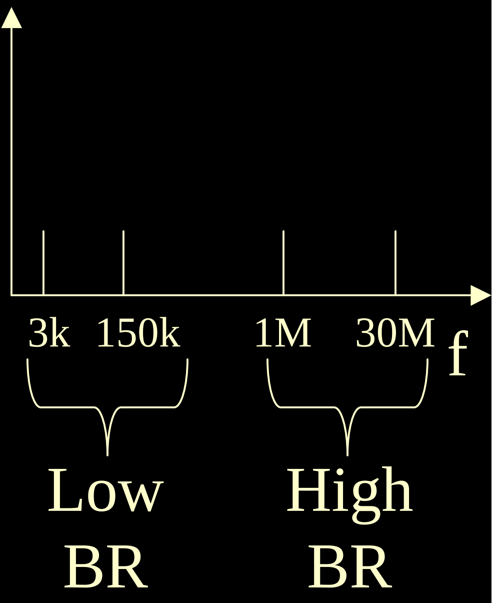
0x01 - PLC 101 crashclass

- *PowerLineCommunications = usage of electrical cables for LAN (public or private electrical networks)*
- *Equivalent of an ETHERNET hub at layer1 and 2*

0x01 - PLC 101 History



Upcoming IEEE 1901 based on HomePlug AV

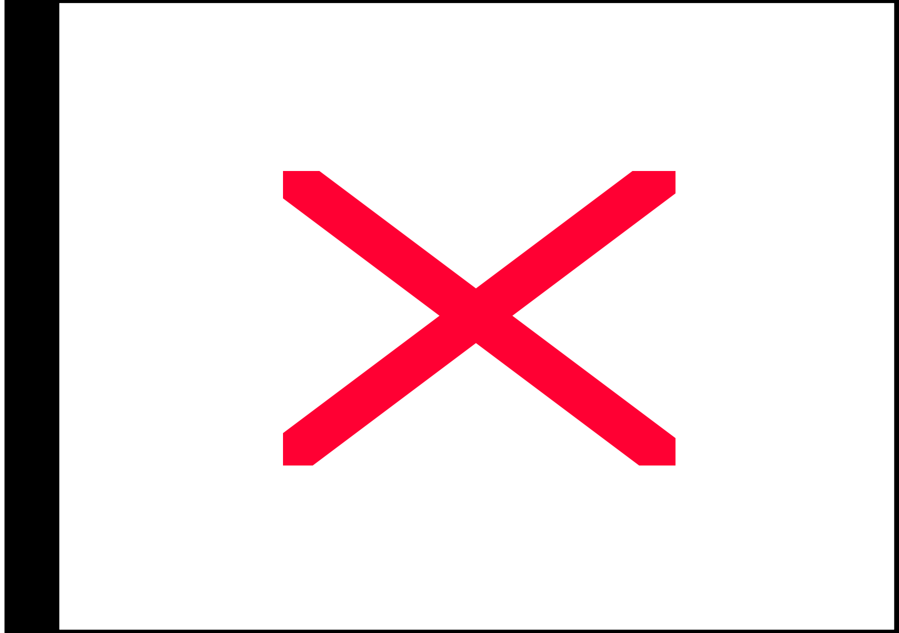

3k 150k 1M 30M f

Low BR

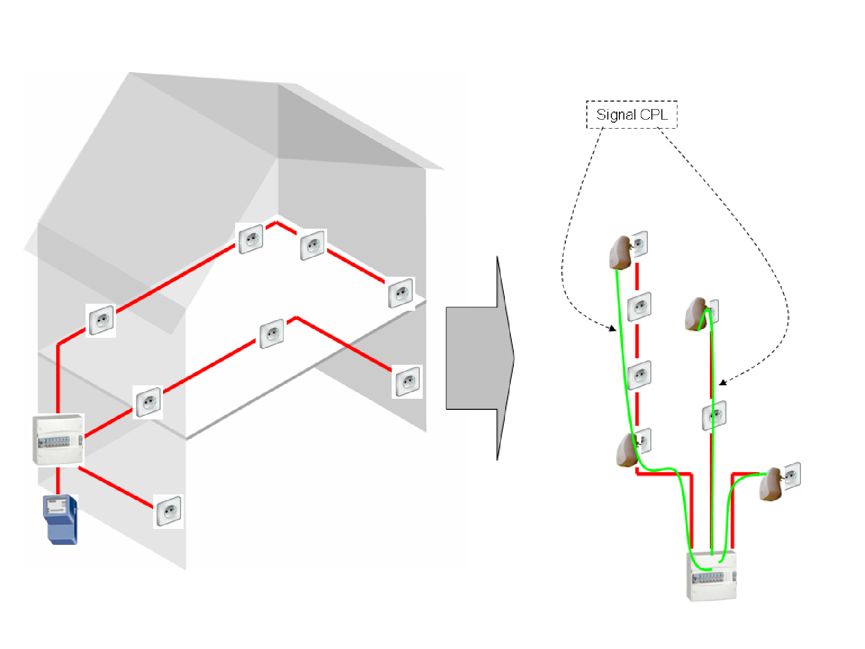
High BR

0x01 - PLC 101 crashclass

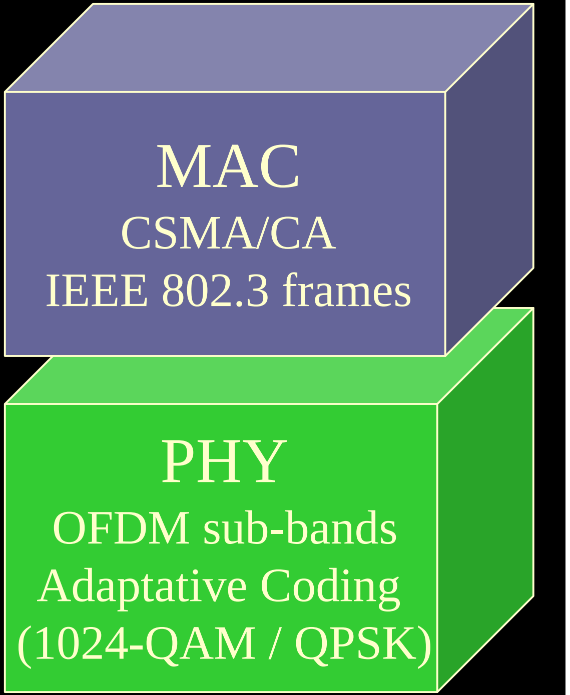
Outdoor



Indoor

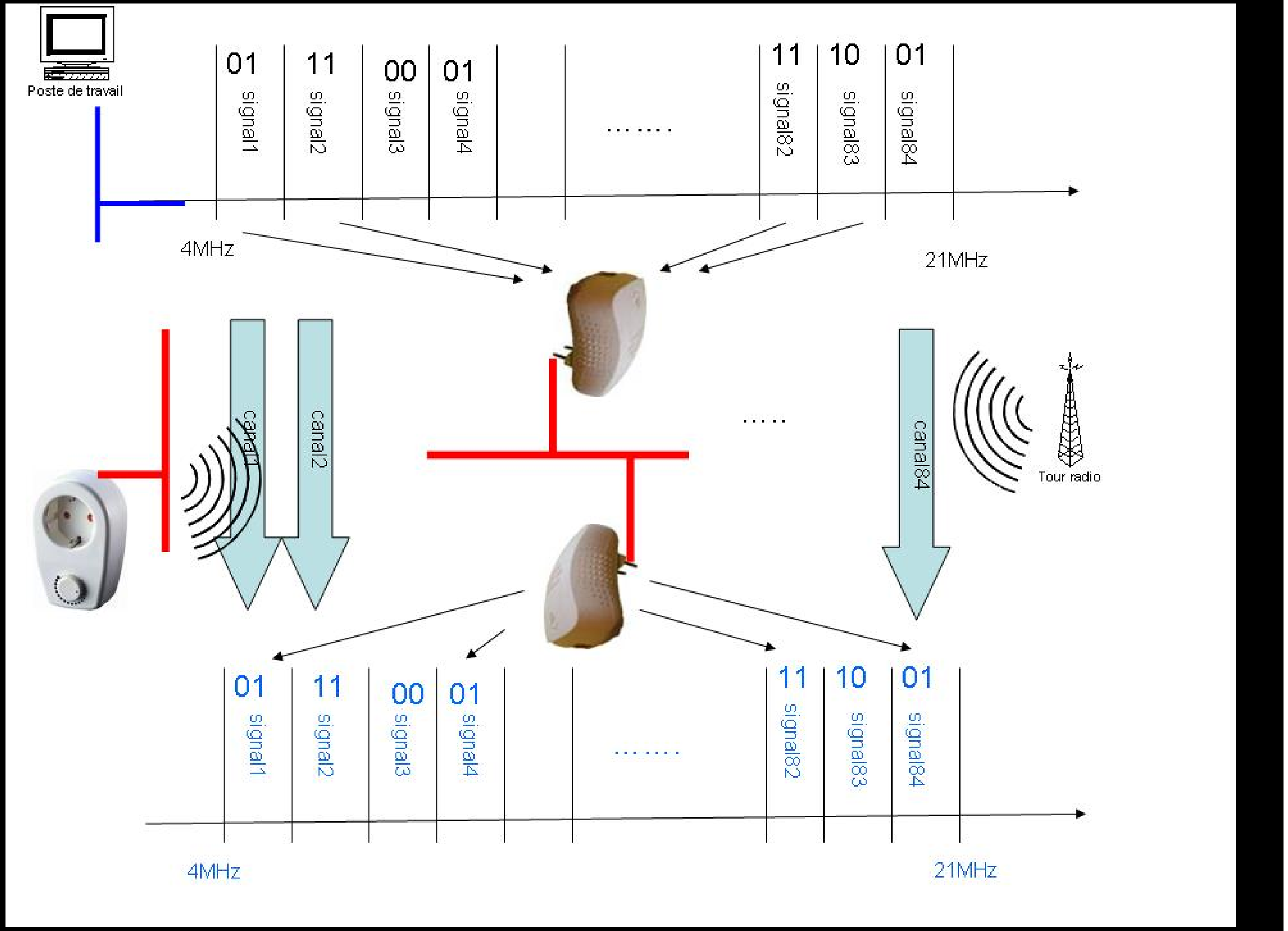


PHY/MAC layers in PLC (high BR)



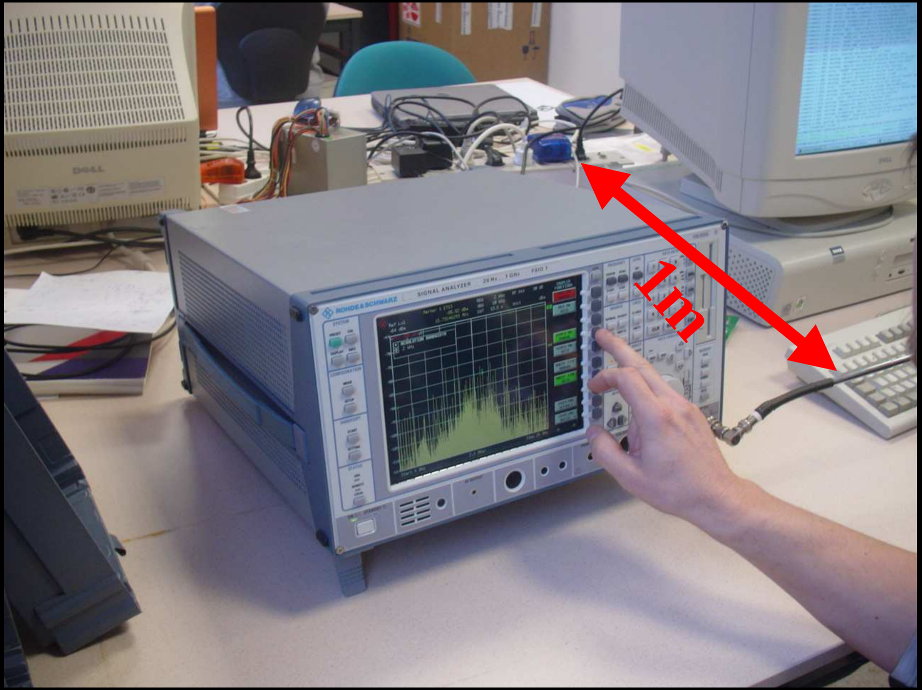
MAC
CSMA/CA
IEEE 802.3 frames

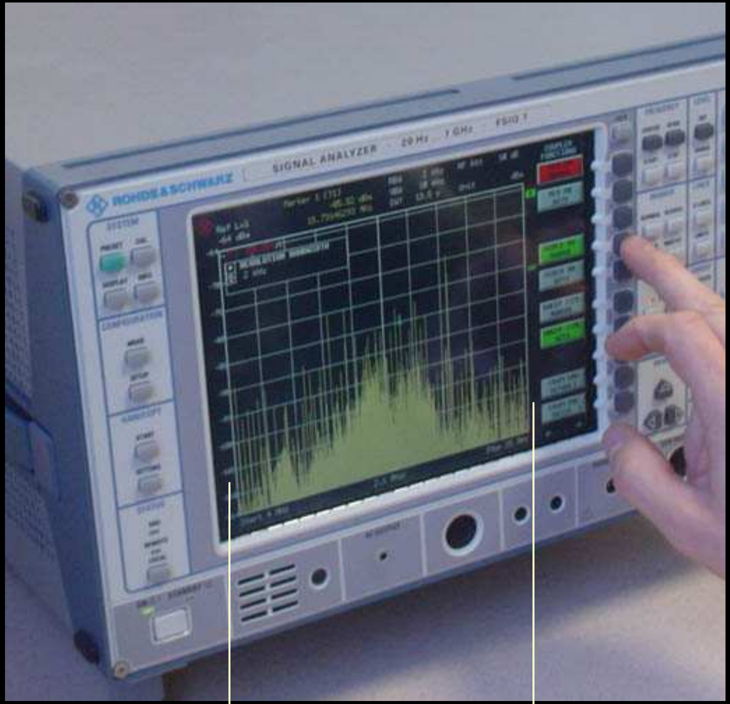
PHY
OFDM sub-bands
Adaptative Coding
(1024-QAM / QPSK)



Sniffing PLC communications

Rohde & Schwarz Signal Analyzer FS10 - 20Hz – 7GHz





60kHz per division

[-110,-95dBm]@1m

Freq_span = 656.25kHz

1-30MHz

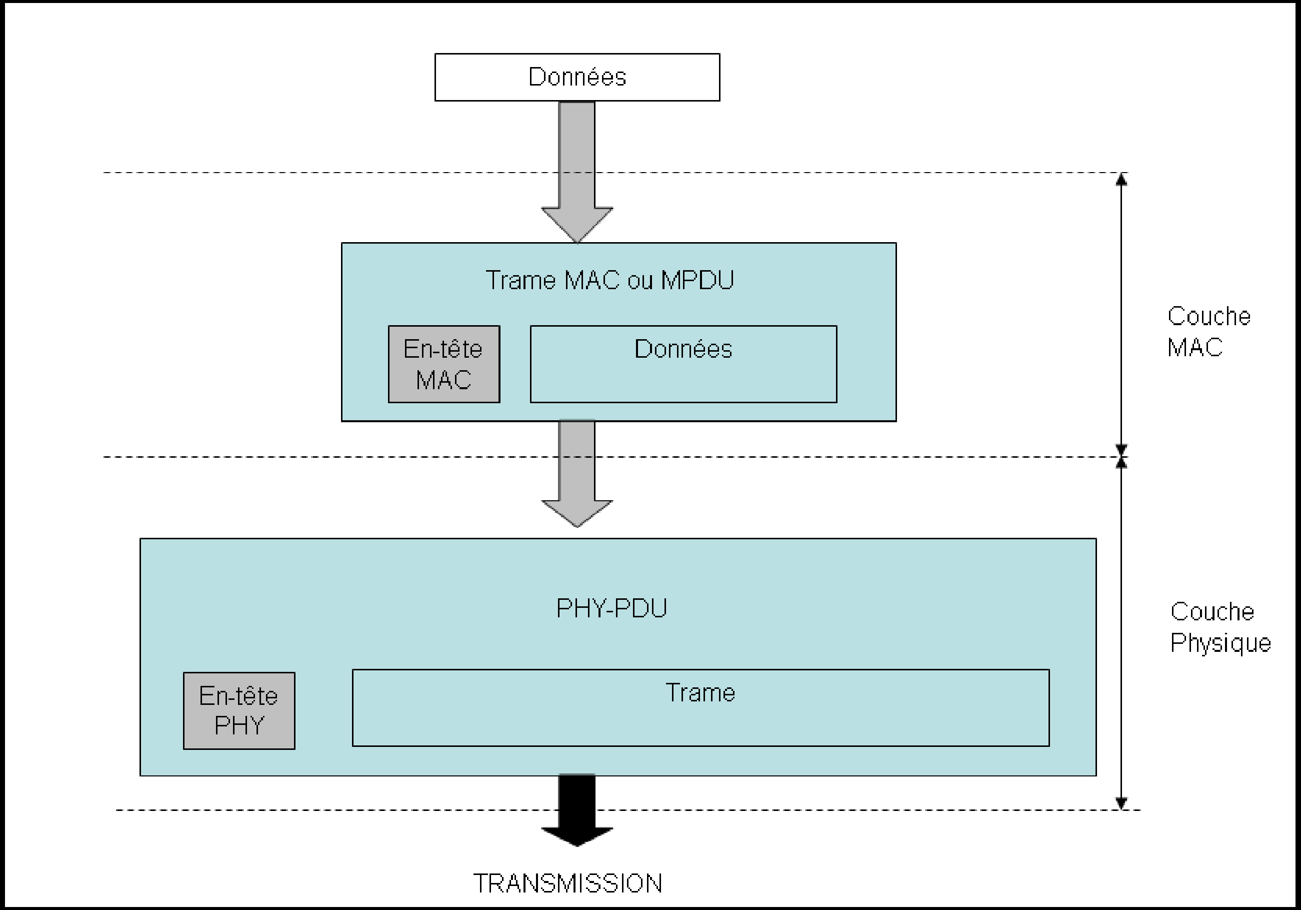
OFDM modulation

916 sub-bands

PLC Equipments

- Ethernet bridges for PLC LAN
- PLC SetTopBoxes (DSL, WLAN, PLC…)
- PLC-MCU Gateways
- TV-Slingboxes
- IP-cams
- Y-Power adapters
- PLC ISP devices

PHY/MAC layers in PLC



Security issues in PLC

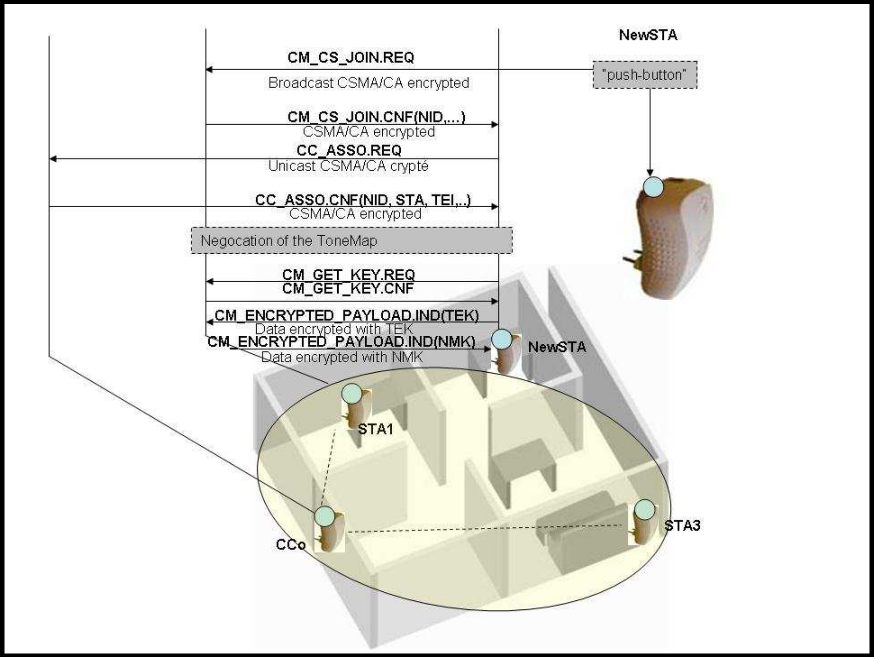
- Difficult access to the Medium
- Complete Hardware sniffing solution difficult to implement (Logic Analyzer + adaptive CAN + Demodulator + DataDumping + Decryption)
- Adaptative modulations between nodes based on the channel quality change ev. 5s

Security Issues in PLC

- HomePlug 1.0 : Security at Layer2 by NEK (56-DES encryption)
- HomePlug AV : Security at Layer2 by NEK (AES-128 encryption) and COO / STA Architecture
- Encryption frames do not appear on the RJ45 interface if NEK wrong
- INT5500, INT6000 chip embedd the NEK functionnality allowing separation between electrical interface and RJ45 interface

Security Issues in PLC

- HomePlug AV holds a « easy-connect » mode with a TEK (Temporary Encryption Key)

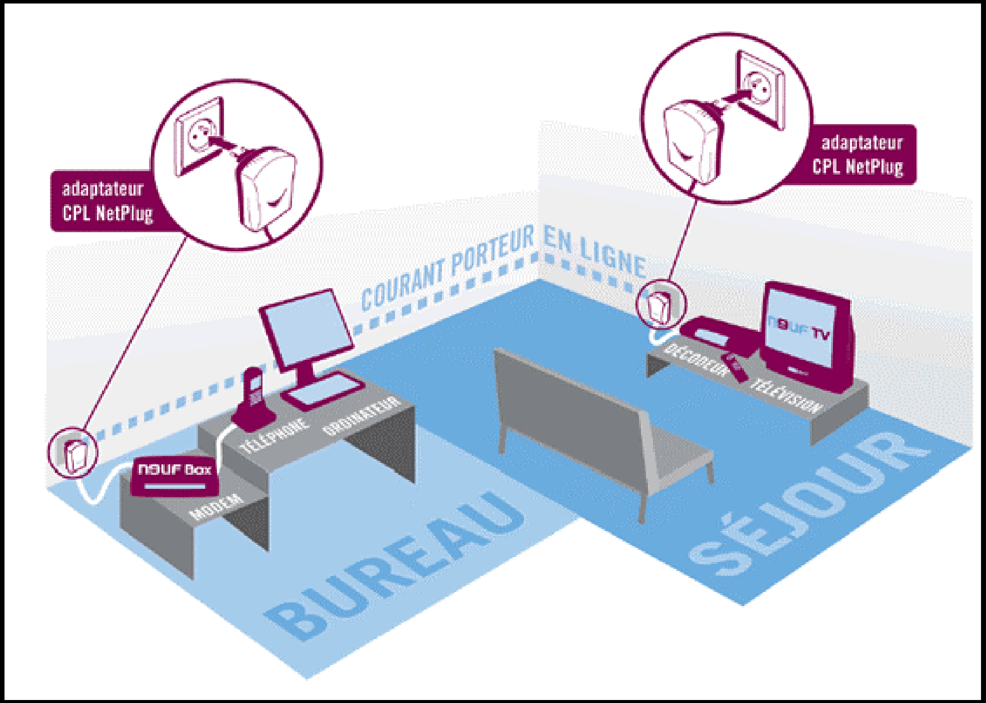


0x02 – Focus on HomePlug AV

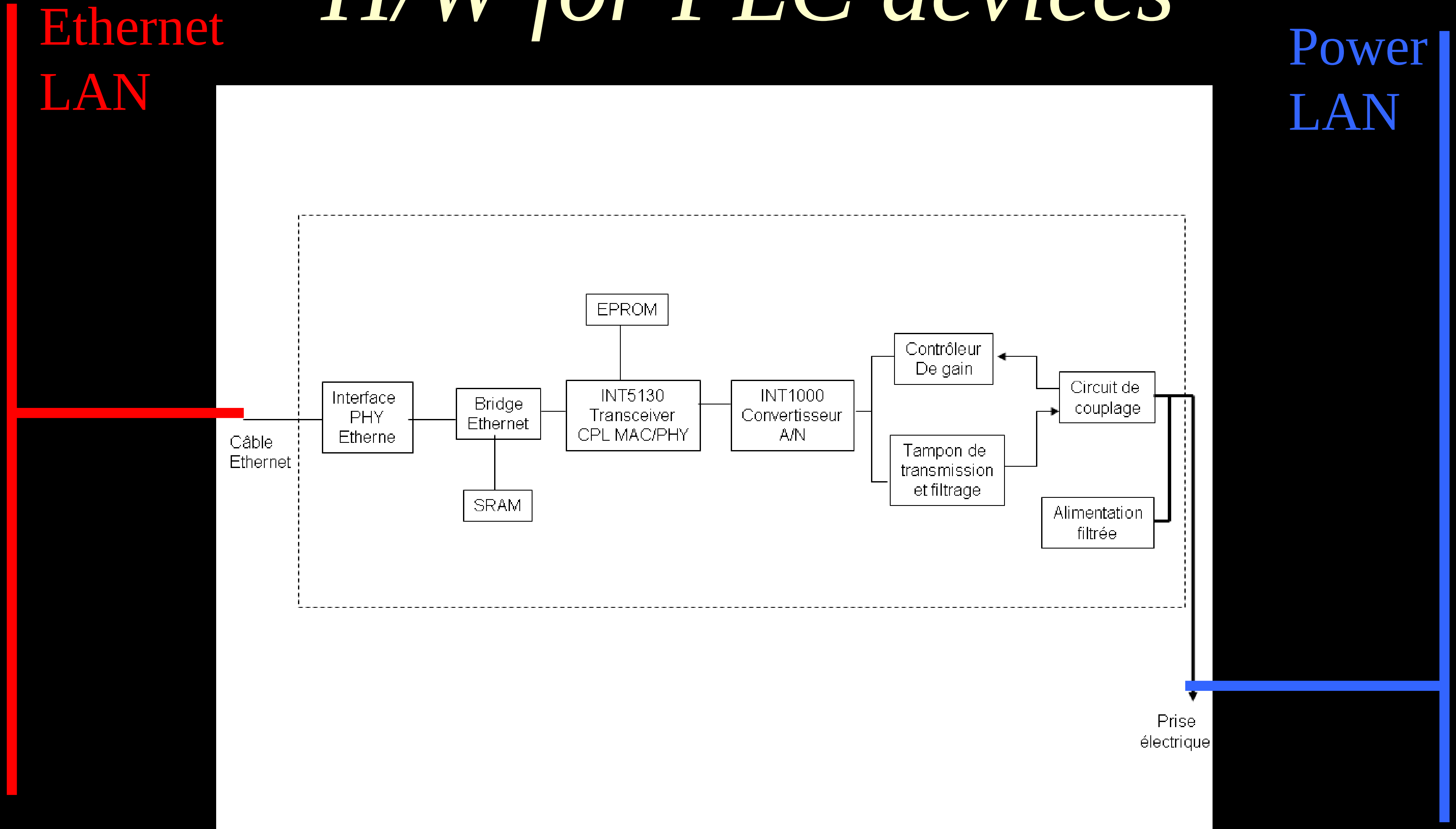
- HomePlug AV allows 200Mbits/s at the PHY Layer
- ETHERTYPE = 0x88e1
- 256 devices on a logical PLC networks
- COO / STA architecture
- FAIFA allows real-time monitoring of the PHY layer coding / modulation scheme
- CSMA / CA and TDMA (50/60Hz carrier-based) modes

ISP Applications

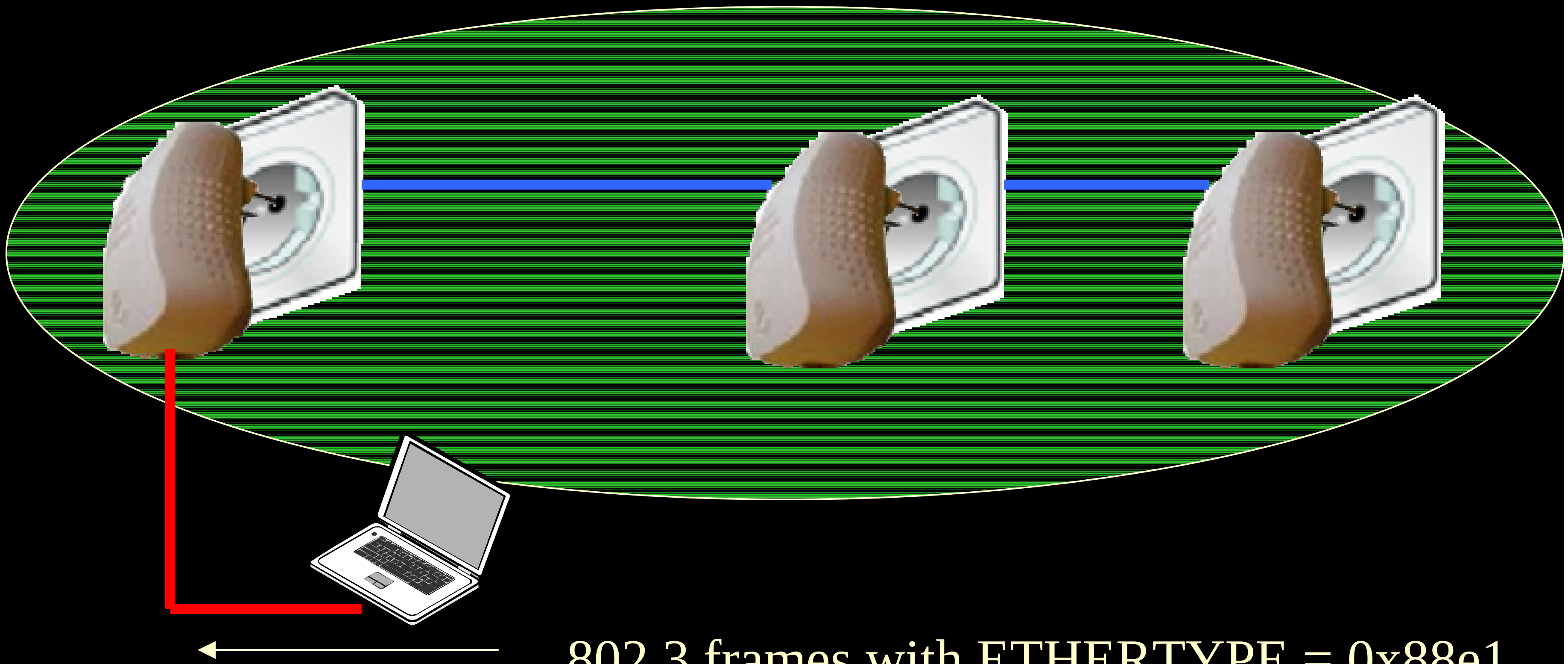
- 2-3 devices typical applications with one device connected to the DSL-box, one to the video decoder



H/W for PLC devices



HomePlug AV devices configuration

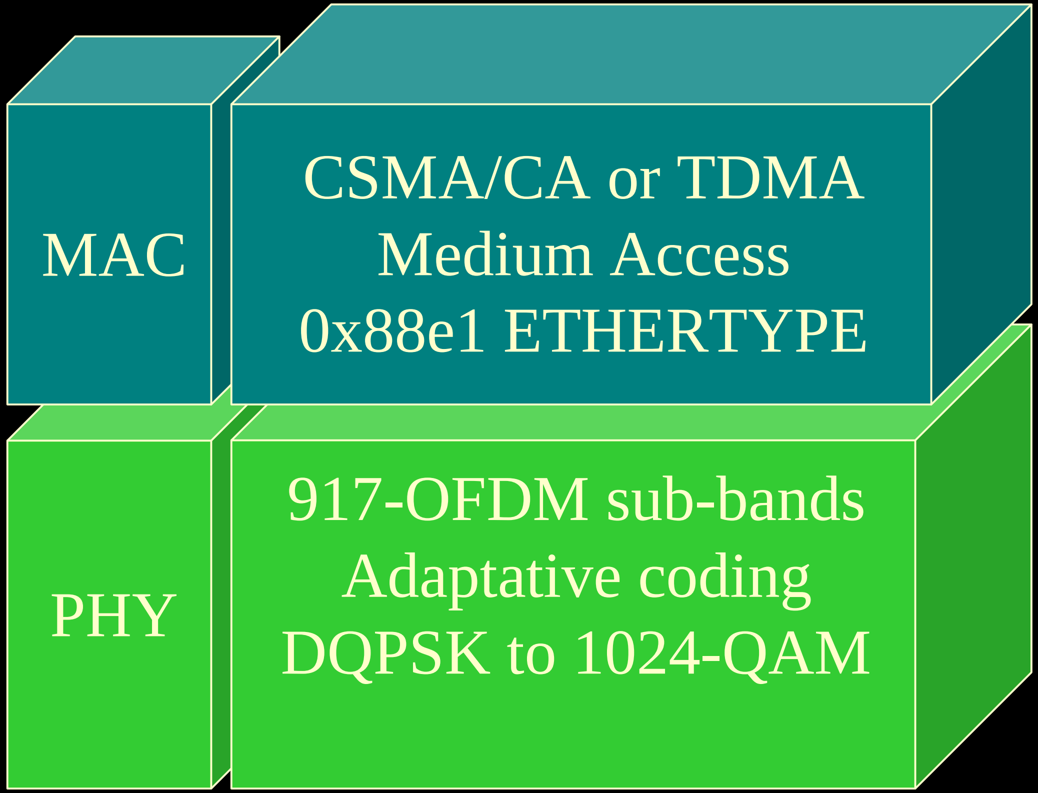


802.3 frames with ETHERTYPE = 0x88e1

0x03 – The FAIFA Tool

- Trac for development repository available at https://dev.open-plc.org/
- Different behaviour with the different INT6000 firmwares (INT6000-MAC-1.4, 3.0, 3.1)

HomePlug AV 101



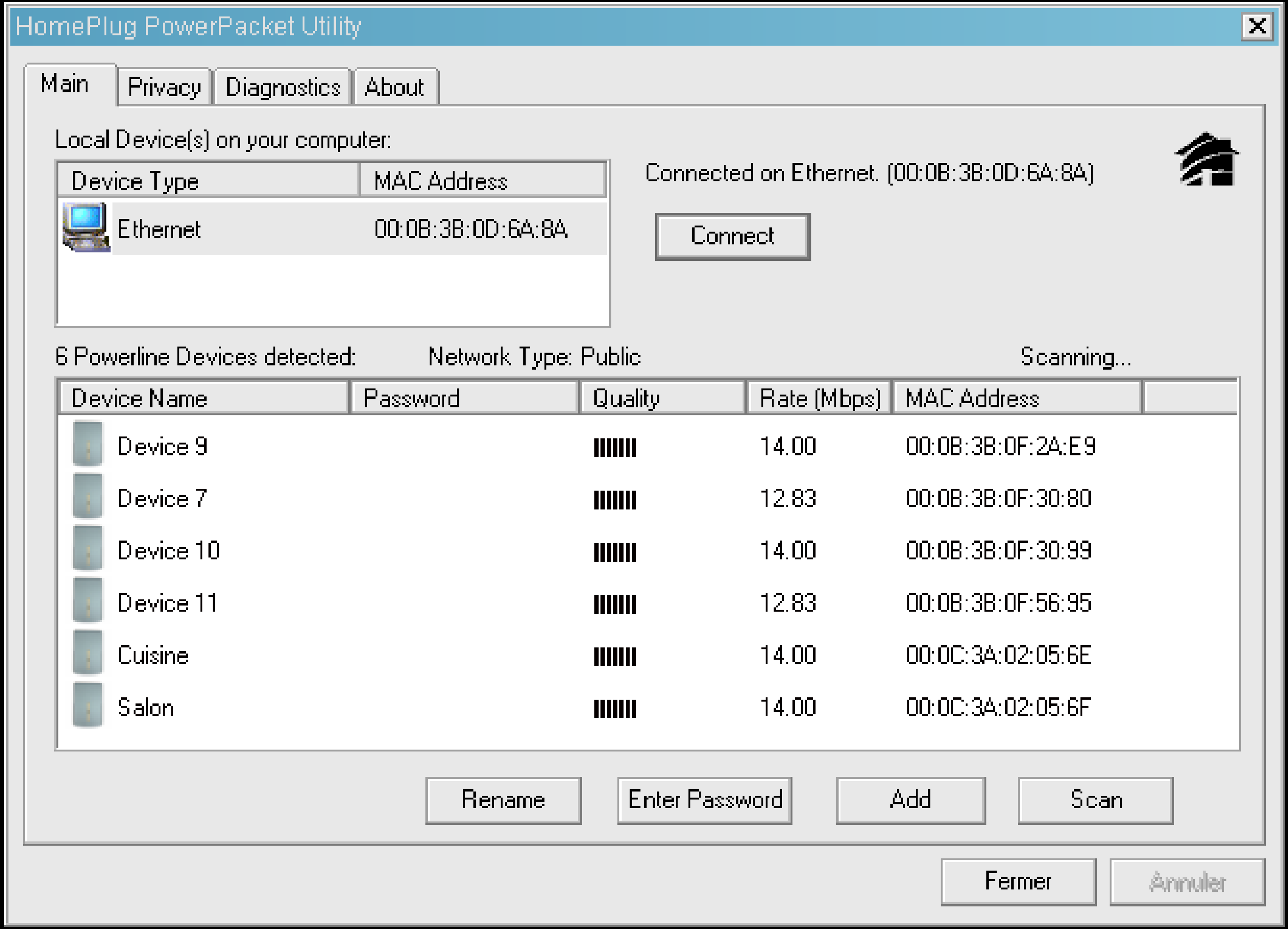
MAC

CSMA/CA or TDMA
Medium Access
0x88e1 ETHERTYPE

PHY

917-OFDM sub-bands
Adaptative coding
DQPSK to 1024-QAM

Existing tools for HomePlug AV configuration



Local Device(s) on your computer:

Device Type	MAC Address
Ethernet	00:0B:3B:0D:6A:8A

Connected on Ethernet. (00:0B:3B:0D:6A:8A)

6 Powerline Devices detected: Network Type: Public Scanning...

Device Name	Password	Quality	Rate (Mbps)	MAC Address
Device 9		IIIIIII	14.00	00:0B:3B:0F:2A:E9
Device 7		IIIIIII	12.83	00:0B:3B:0F:30:80
Device 10		IIIIIII	14.00	00:0B:3B:0F:30:99
Device 11		IIIIIII	12.83	00:0B:3B:0F:56:95
Cuisine		IIIIIII	14.00	00:0C:3A:02:05:6E
Salon		IIIIIII	14.00	00:0C:3A:02:05:6F

Existing Open tools for HomePlug

- Manuel Kasper’s *plconfig* (raw sockets) for HomePlug 1.0 (**http://neon1.net/)**
- *Wireshark HomePlug 1.0* dissector
- Devolo *dLAN-linux-package-2.0* (libpcap 0.8.3)

=>**Needs for a fully integrated package-based PLC OpenSource tool**

FAIFA’s features and design

- To be embedded Linux tool with .deb, .rpm versions
- Scriptable for tcpdump, wireshark and others …
- Configuration of a PLC networks with the different NEK (Network Encrytion Keys) – The « WPA key » of the PLC
- Complete monitoring of the MAC / PHY layers for advanced users
- Access to the NVRAM / SDRAM of the PLC chip
- Sniffer mode

FAIFA in action

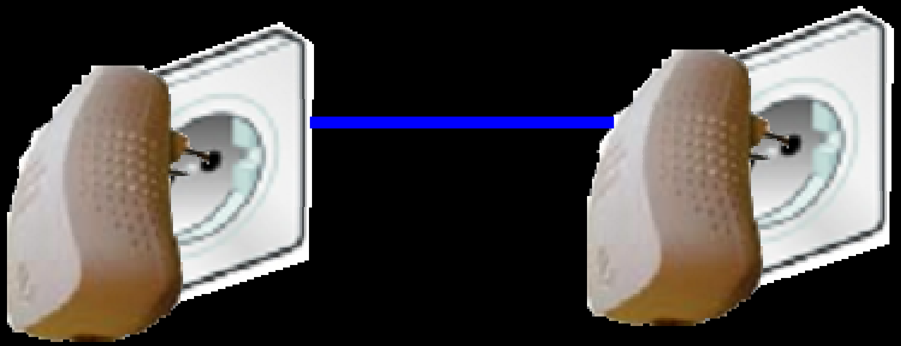
- Downloadable from http://open-plc.org/
- #./faifa –i eth0 –m
  - type   description
  - ------ -----------
  - 0xA000 Get Device/SW Version Request
  - 0xA030 Get Link Statistics Request
  - 0xA038 Network Info Request (Vendor-Specific)
  - 0xA050 Set Encryption Key Request
  - 0xA054 Get Manufacturing String Request

FAIFA in action

- Play with the different MMTYPE in the 802.3 frames with ETHERTYPE = 0x88e1
- Examples :
  - 0xA000 : Get device / SW Version
  - 0xA030 : Get link statistics
  - 0xA070 : Tone Maps
  - 0xA034 : Sniffer Mode

Demo with PLC devices

- Device detection (MMTYPE = 0xA000)
- Topology detection (MMTYPE = 0xA038)
- Link Statistics (MMTYPE = 0xA070)
- Sniffer Mode (MMTYPE = 0x?)



FAIFA Contributions

- Looking for testers (latest releases on different HomePlug AV devices)
- Looking for developers : packaging, optimization, GUI implementations, wireshark dissector
- Prototyping a PLC stack on a FPGA with a HomePlug based PHY-chip

FAIFA Questions

- Contact : dev@open-plc.org
- Website : http://open-plc.org
- ?? Questions ??