« Crashcourse: Securing a PLC Networks »

Xavier Carcelle
iAWACS 2010

xavier.carcelle@gmail.com

The today's talk

- “Crashcourse : Securing a PLC networks” : Xavier Carcelle
  - State of the security on the PLC Networks
- Technical presentation of the “PLC security issues” project with the PAIR project of the ESIEA
  - Scenarii of PLC network attacks

Regards and credits

-Great support of the ESIEA Laval and EFiliol for the funding of the hardware

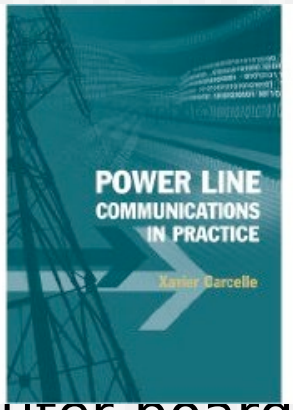
-Support of Spidcom for the MALIKA plateform

-Broadview of the computer security issue from Robert Erra

Outline of the presentation

- Introduction
- PLC Technologies overview
- The electrical cable : a shared medium
- PLC : Security architecture
- Security in HomePlug 1.0./1.1
- Security in HomePlug AV
- Improving the security level of PLC networks
- Conclusion / next steps

Introduction



- Expertise on PLC, wireless

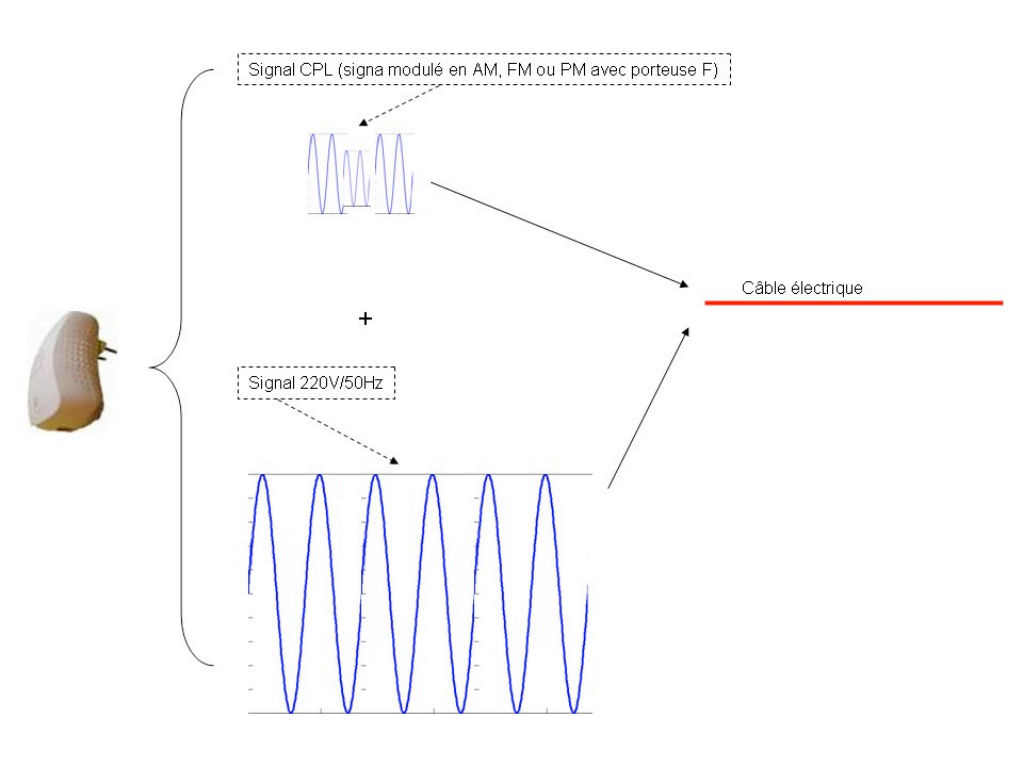
- Co-founder of OpenPattern : FPGA-based IP-router-board
- => FPGA : reprogrammable chip for low level networks applications (SDR, PLC, WiMAX...)
- Co-author of FAIFA (debian experimental package to monitor/configure HPAV PLC chips)
- Currently working on VoIP OpenHardware IPBX

PLC Technologies overview

- Different PLC technologies (depending on bit rate, frequency bands
  - 63-220-400kV / 9Kbits/s / 100kms
  - 110-220V / 200MBits/s /LAN
- Long-time « old » technology/idea (ex : PULSADIS System in EDF 175Hz) now widely used for DSL applications, LANs, remote-metering, IP-backbones
- Re-using proofed MAC/PHY layers technologies heritated from other LAN technologies (coding, modulation, security, medium access…)
- With the coming IEEE 1901 standard, more chipsets/SoC makers to produce PLC chips
- Complementary to Wi-Fi networks : Atheros (45M) just bought Intellon (20M) … common SoC … next BCM, CISCO…

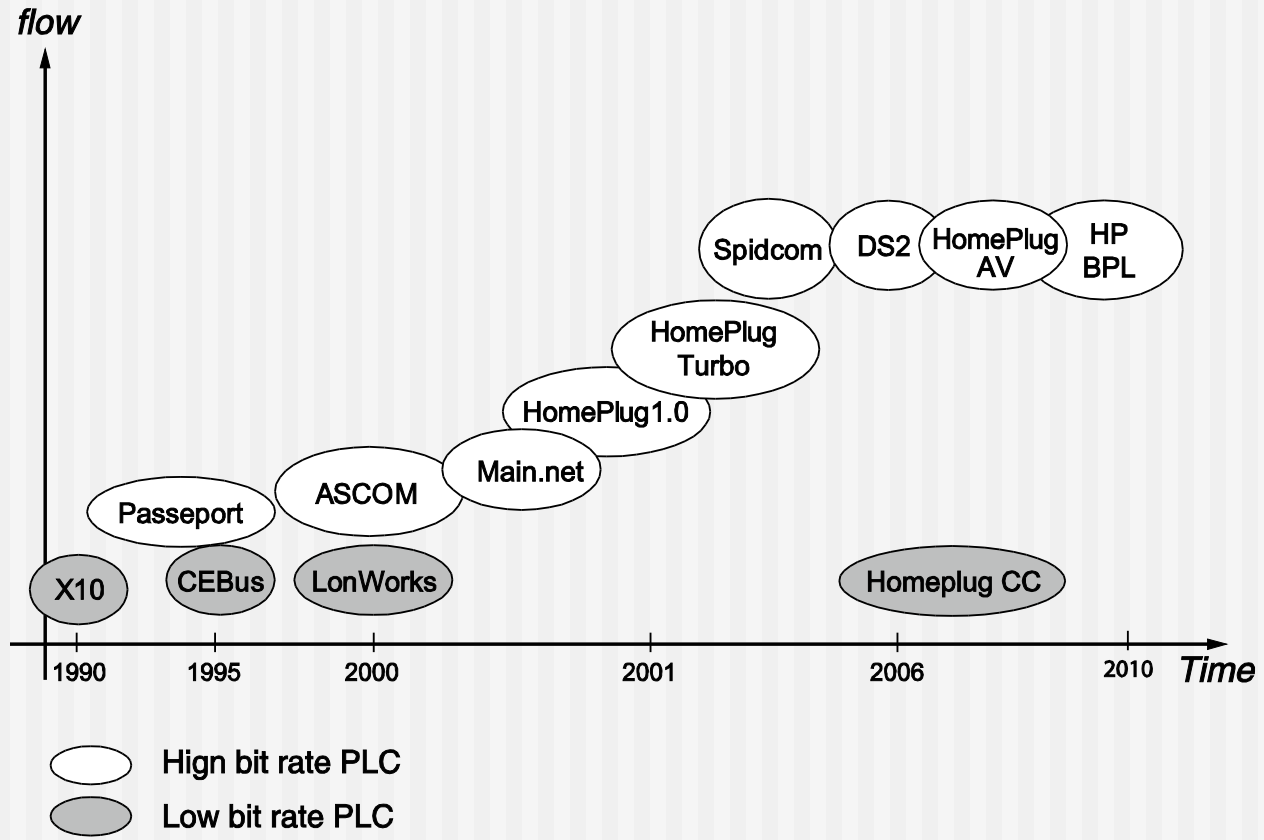
PLC Technologies overview

Principles and « no energized cables » needed

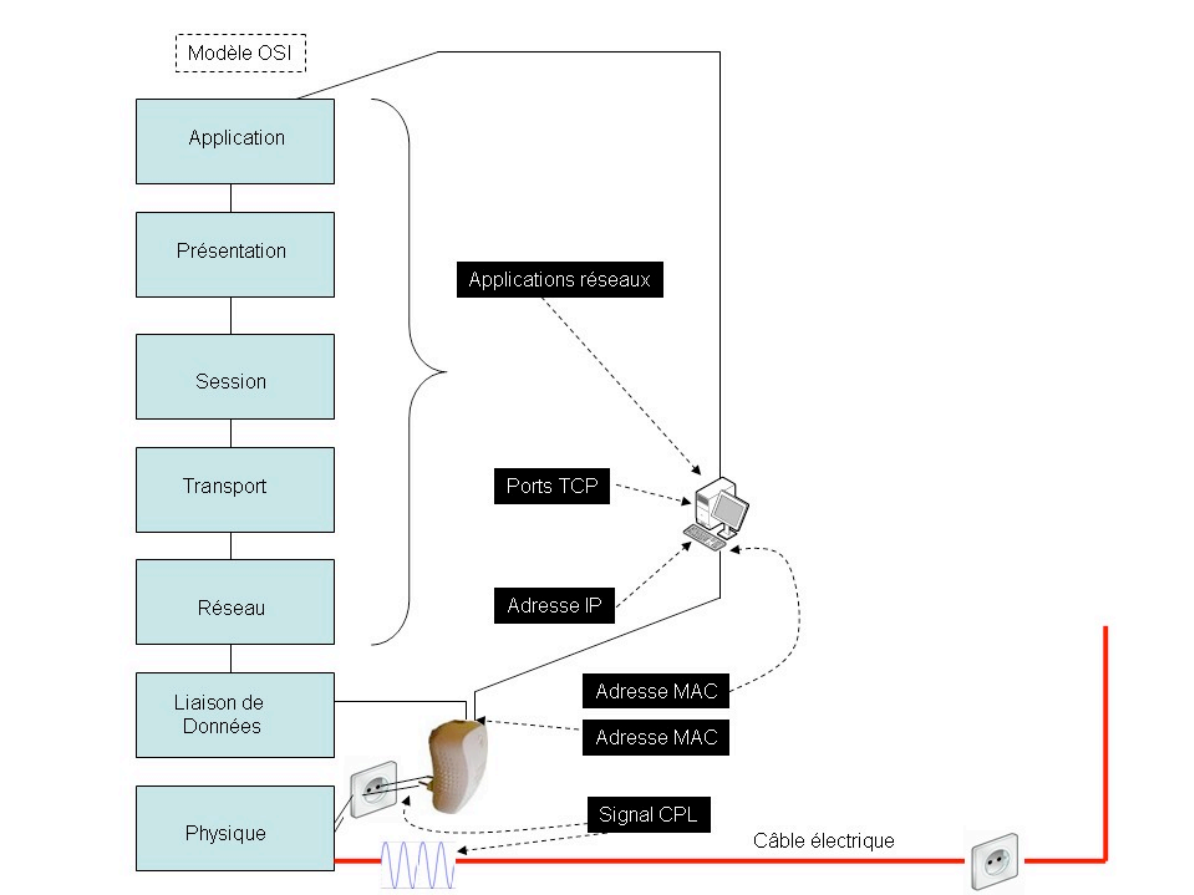


PLC Technologies overview

- From different proprietary technologies to IEEE 1901 standards



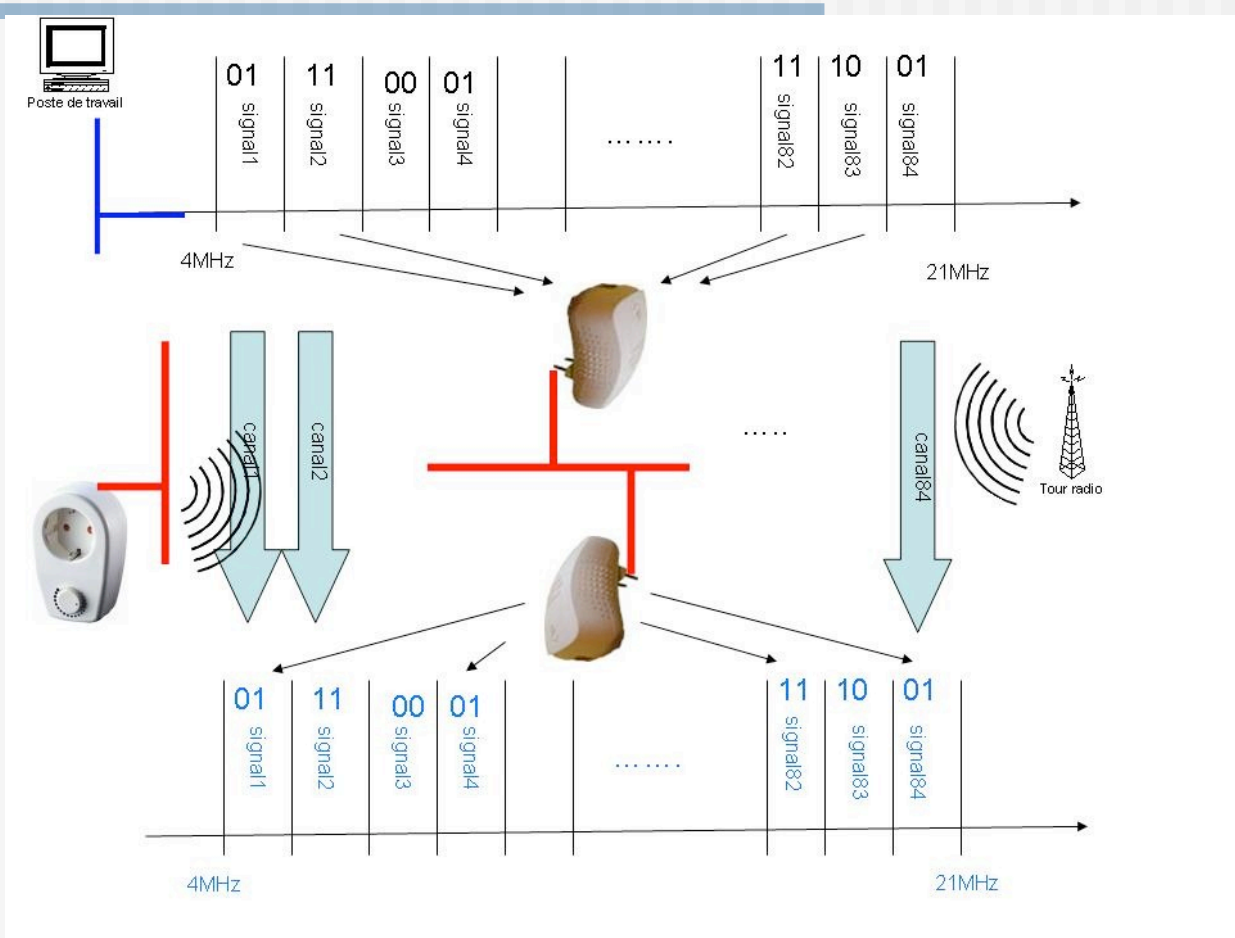
PLC Technologies overview



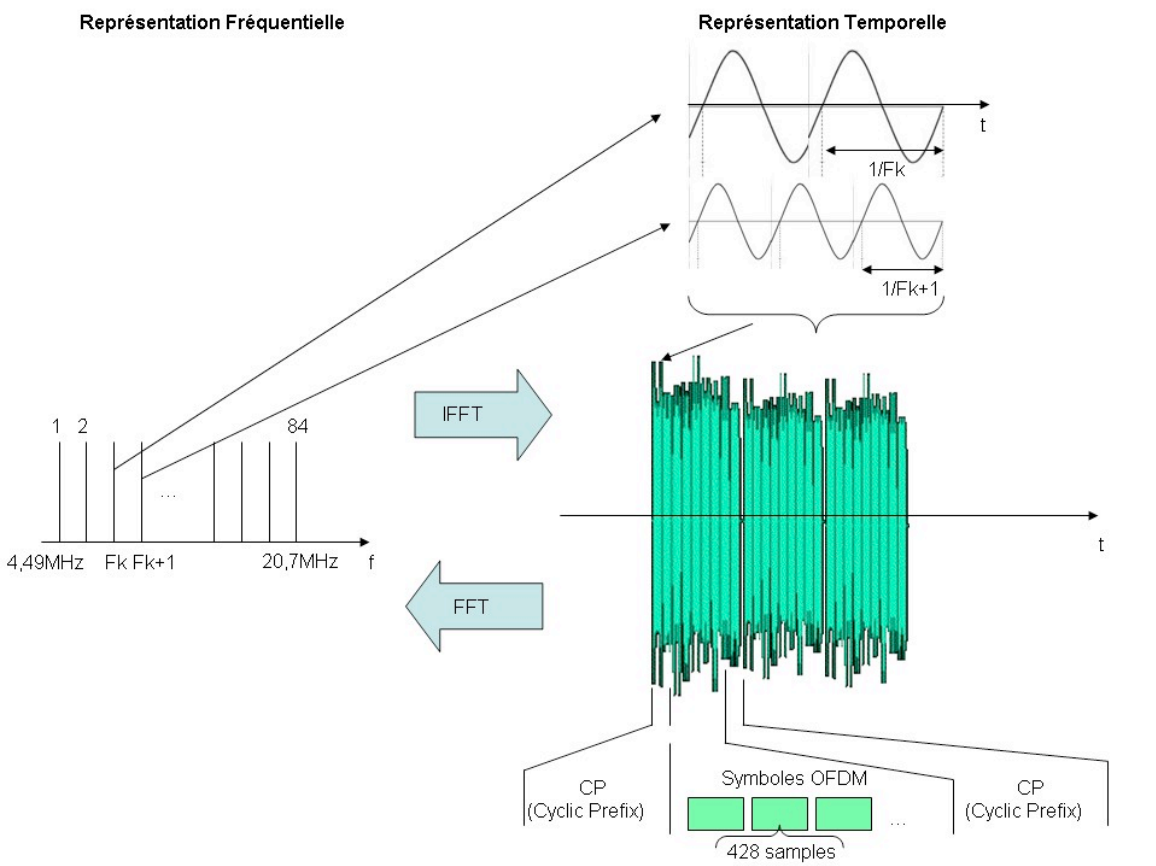
PLC Technologies overview

MAC
CSMA/CA
IEEE 802.3 frames

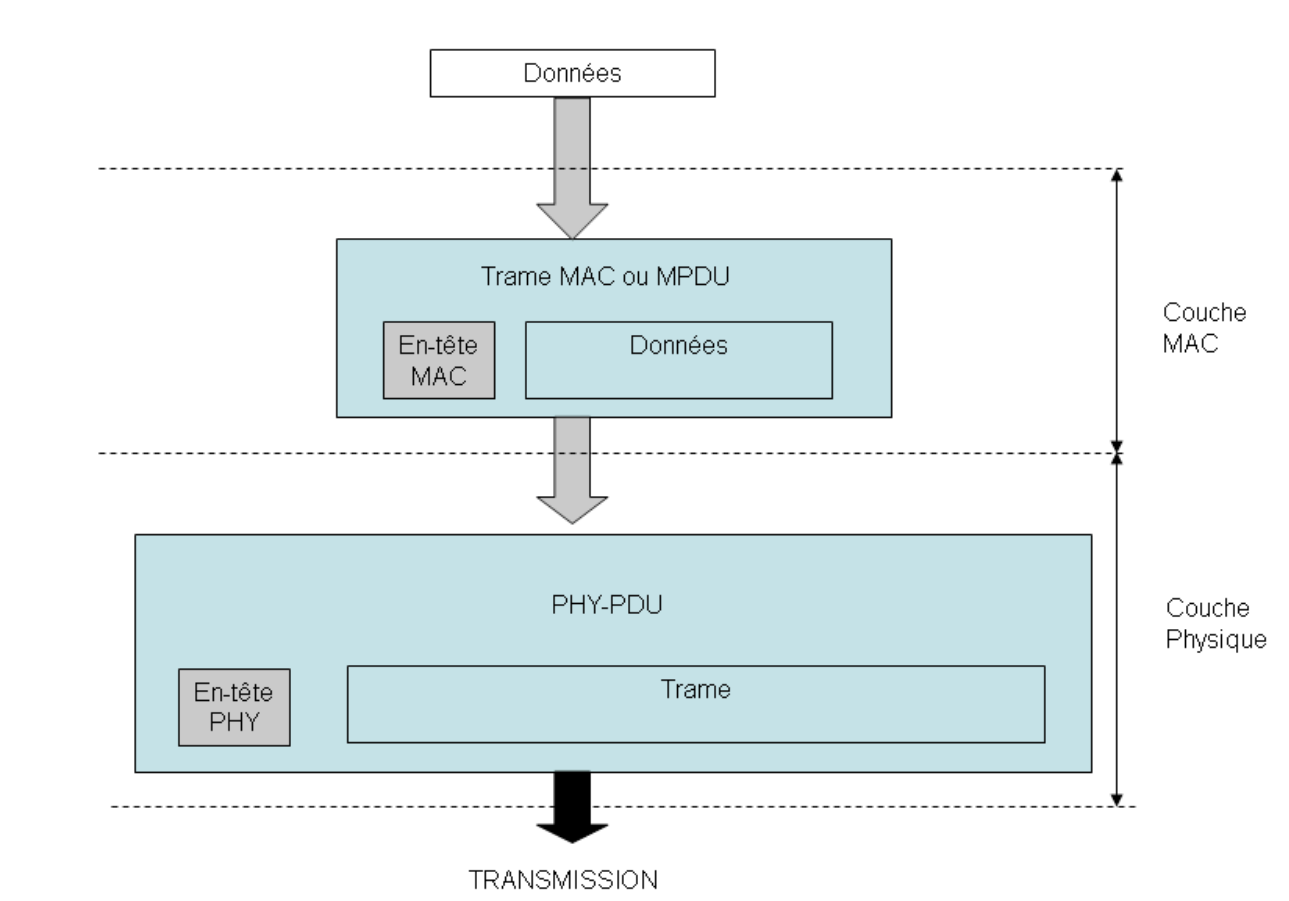
PHY
OFDM sub-bands
Adaptative Coding
(1024-QAM / QPSK)



PLC Technologies overview



PLC Technologies overview



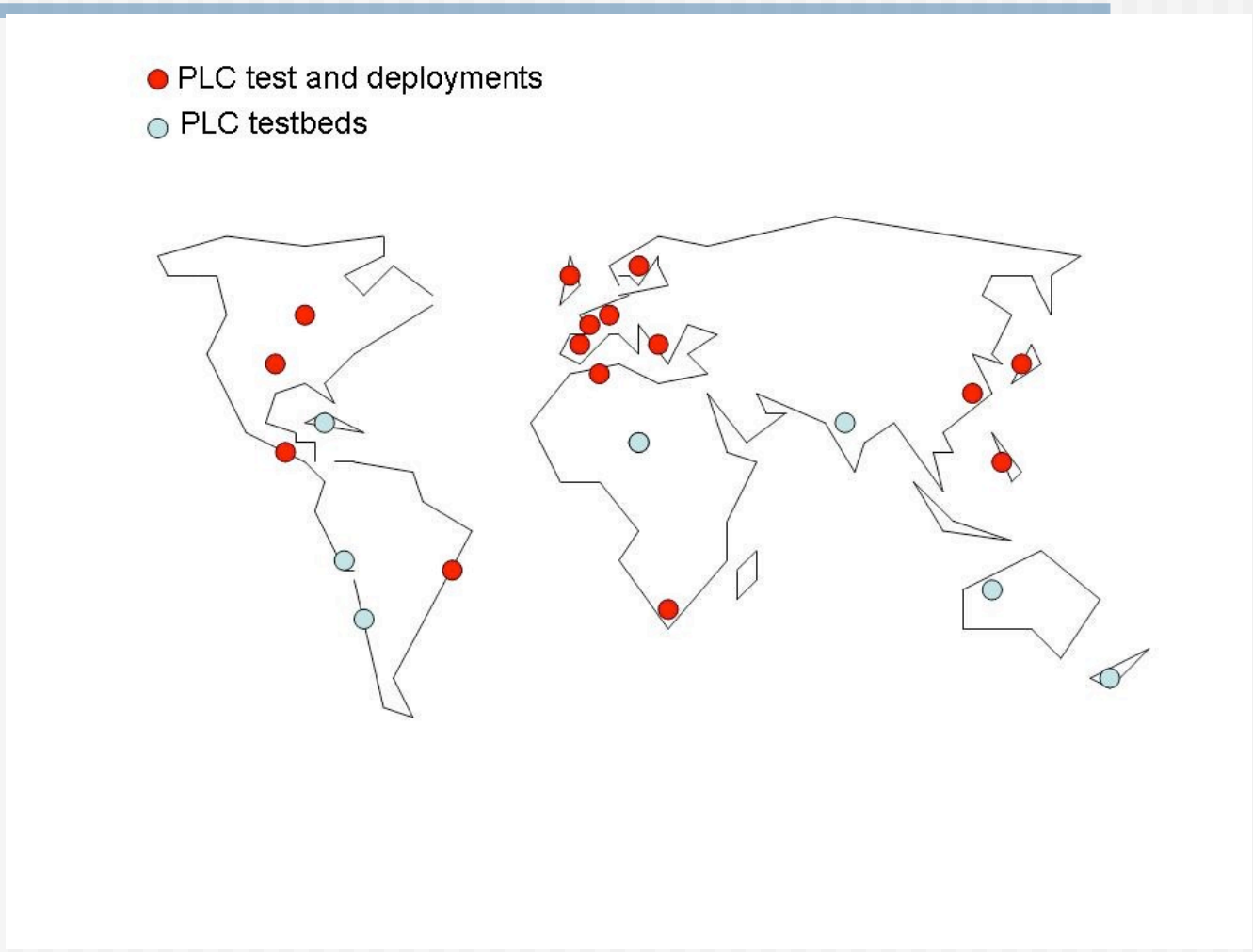
PLC Standards and Techs : Homeplug 1.0, 1.1,AV =>Modulation choices

- PHY =
  - OFDM (84 sub-bands or 917 sub-bands)
  - BQPSK up-to 1024-QAM
  - Turbo-code
  - Wavelets
  - CSMA/CA for HP 1.0, 1.1
  - TDMA with zero-crossing synchronization
  - UDP HD-MPEG optimization for real time streaming

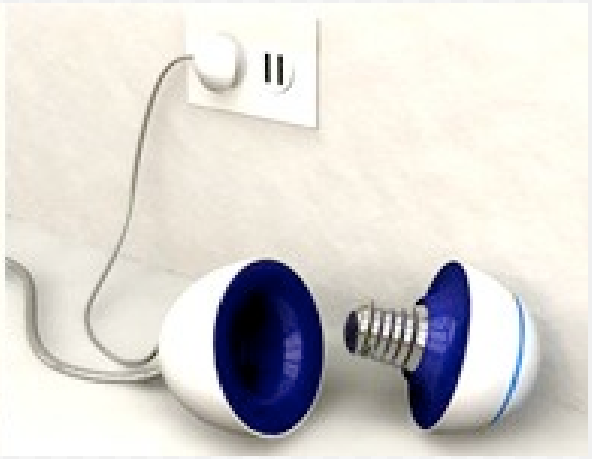
PLC Technologies overview

- Wordwide usage now (US, EU, JP, CN) on different voltage level
- Mass usage of PLC technologies
  - DSL ISP PLC sets of devices (3% of RMA compared to Wi-Fi set for UDP MPEG streams)
    - Freeplugs – more than 2M (HP AV)
    - Liveplugs – 1-3M (HP 1.0 and HP AV)
    - SFR plugs – 1M (HP AV)
      UDP Streams for MPEG IP flows to the TV

PLC World deployments (Nov2008)

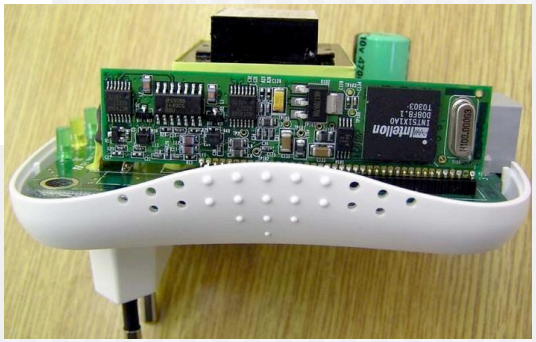


PLC Products ☺



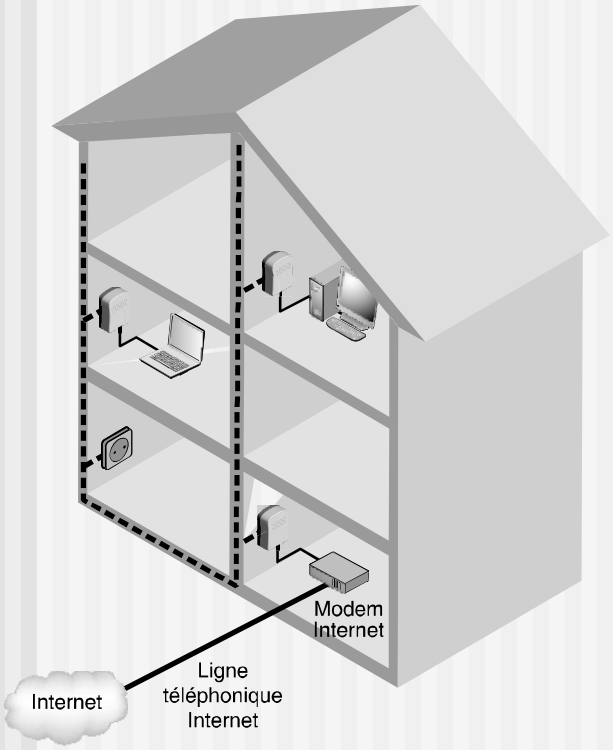
PLC Equipments

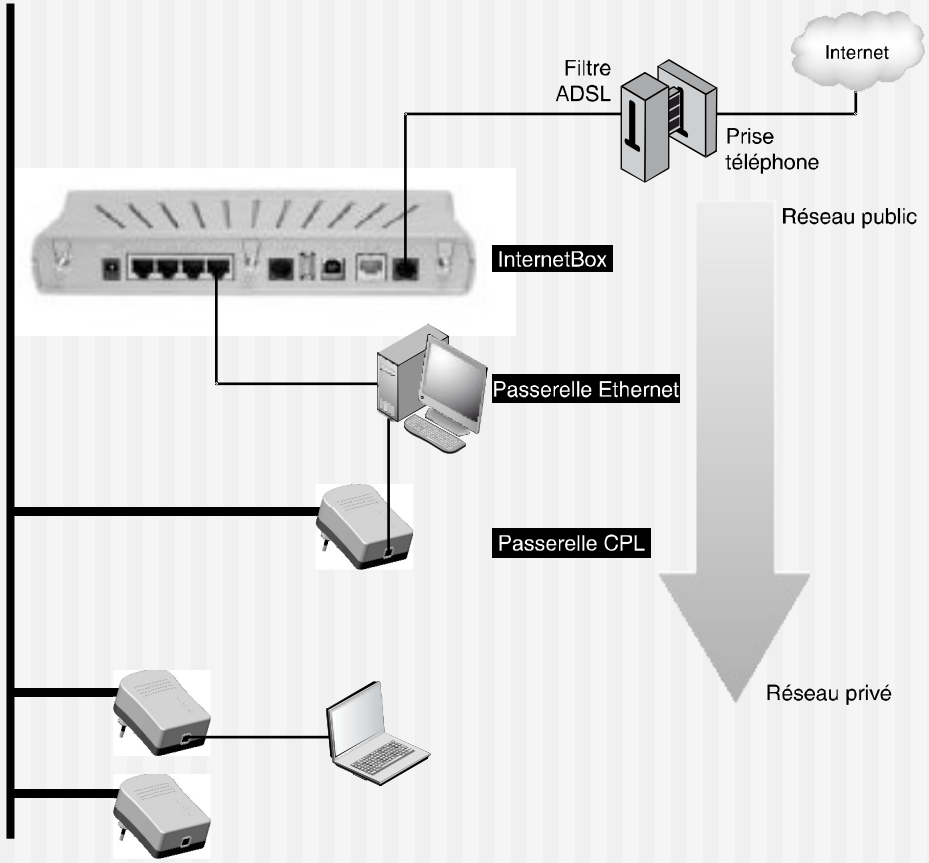
- Ethernet bridges for PLC LAN
- PLC SetTopBoxes (DSL, WLAN, PLC...)
- PLC-MCU Gatewavs
- TV-Slingboxes
- IP-cams
- Y-Power adapter
- PLC ISP devices



PLC Standards and Techs : Homeplug 1.0, 1.1,AV

- Typical apps for ISP





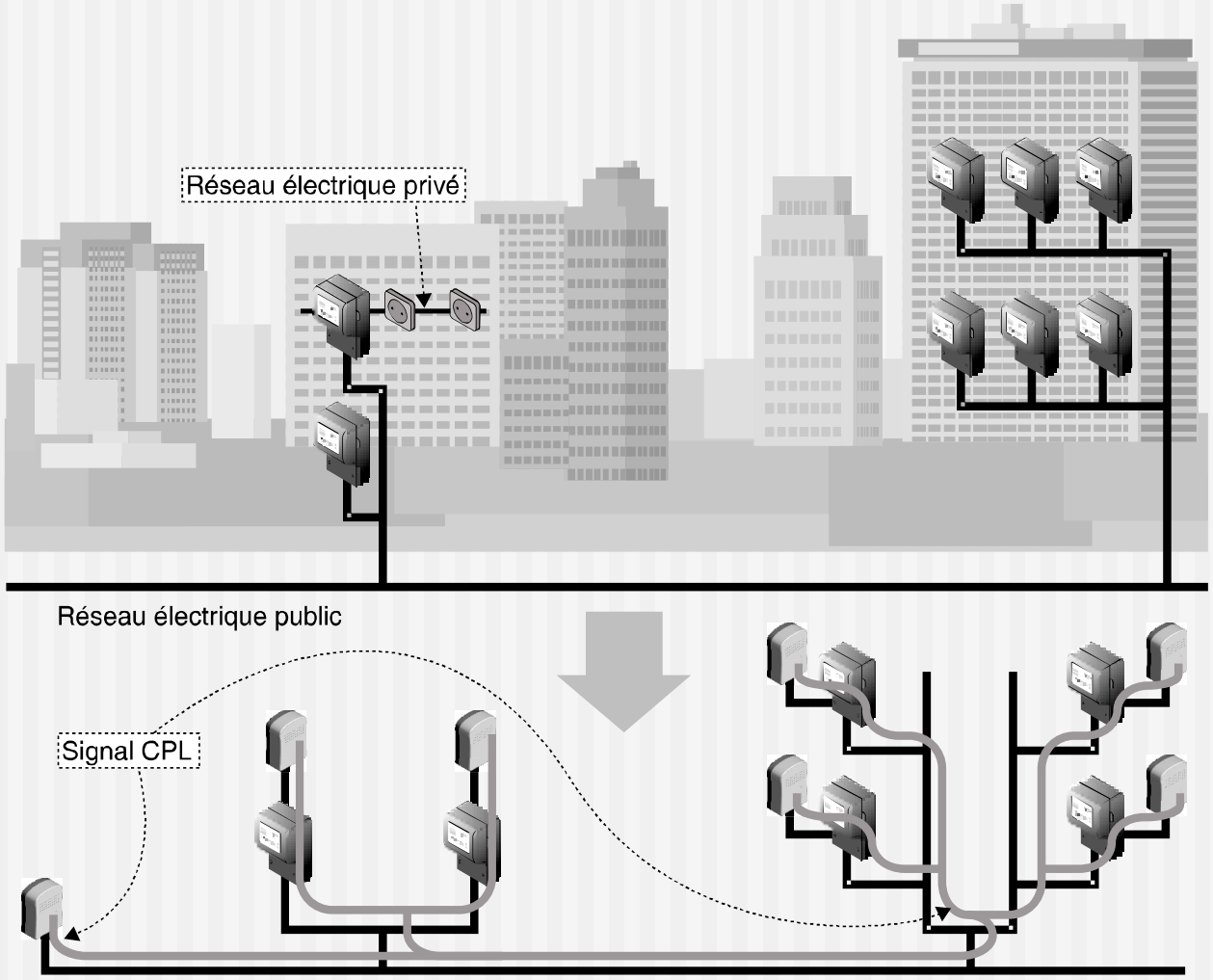
PLC Standards and Techs

- **High-bit-rate techs** (BR > 300KBits/s)
  - HomePlug 1.0 – 14MBits/s
  - HomePlug 1.1 – 85MBits/s
  - UPA (DS2) – 85MBits/s
  - UPA-HD (DS2) – 200MBits/s
  - HomePlug AV – 200MBits/s
  - HD-PLC (CEPCA) – 200MBits/s
  - **IEEE P1901 – MAC Layer** – 200MBits/s

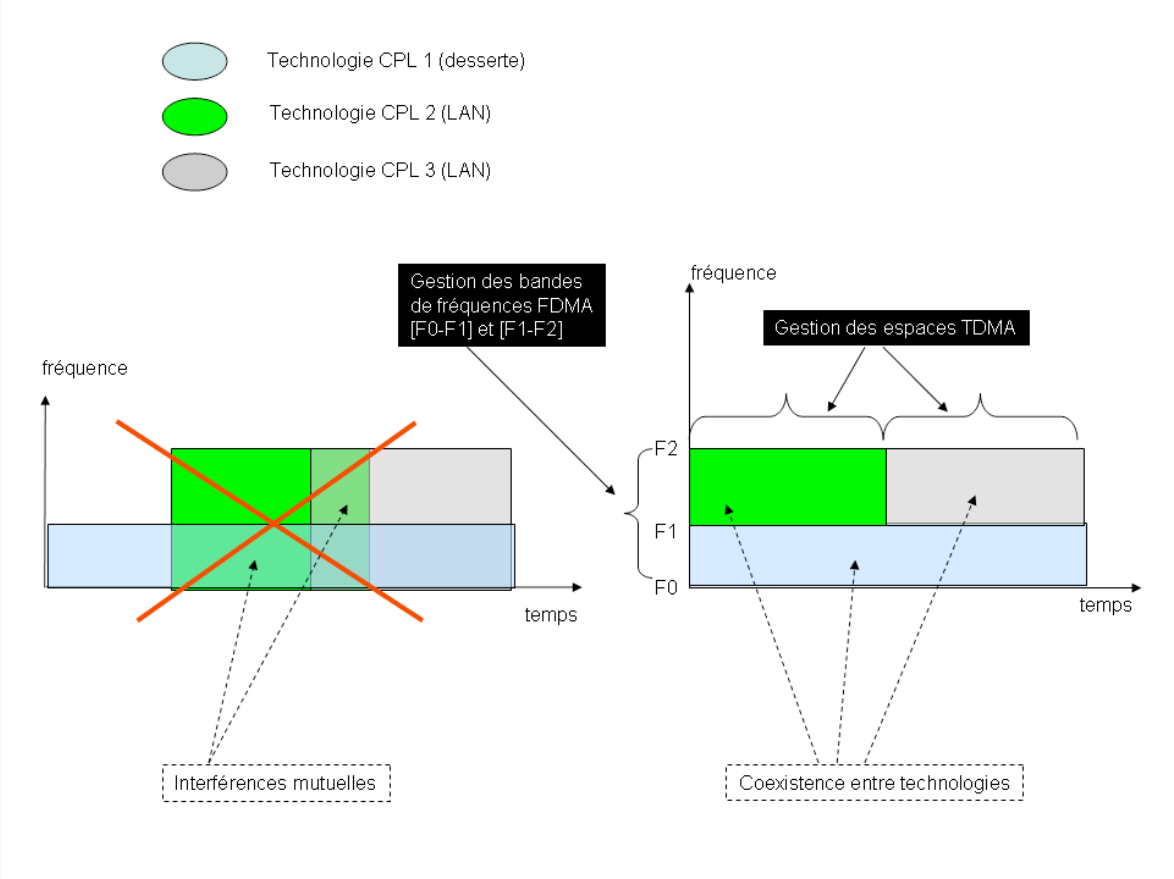
The electrical cable : a shared medium

- In-house electrical cables
- In-building electrical cables (crosstalking between cables, VDSL, ham-radio respect with notching)
- 30-200 households behind the MV/LV transformers
- 3-6dB of mitigation through the electrical nodes (outlet, breakers, meters, plugs)
- The signal does not cross the transformers (i.e. galvanic isolation) but cross 95% of the meters in France !!!!

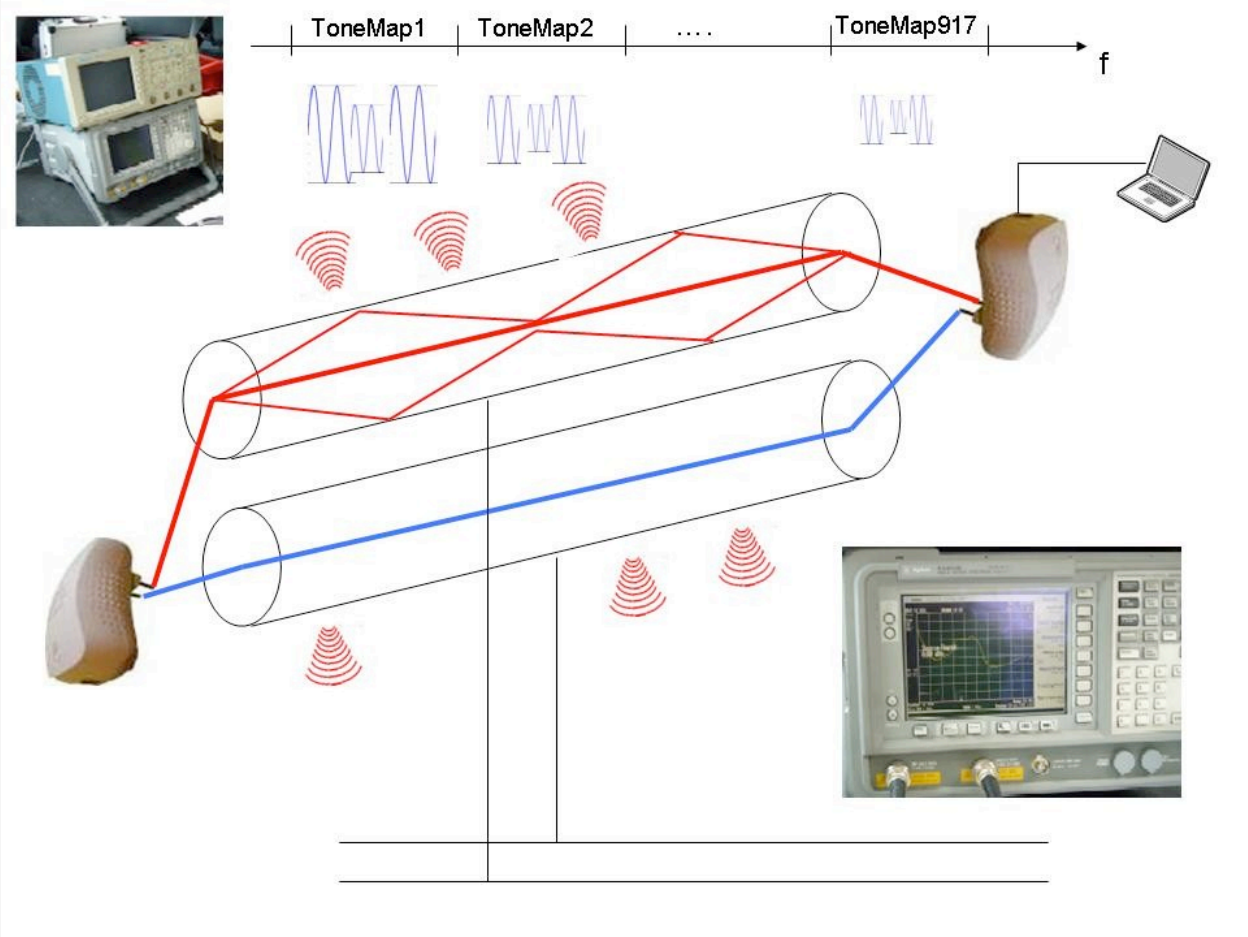
The electrical cable : a shared medium



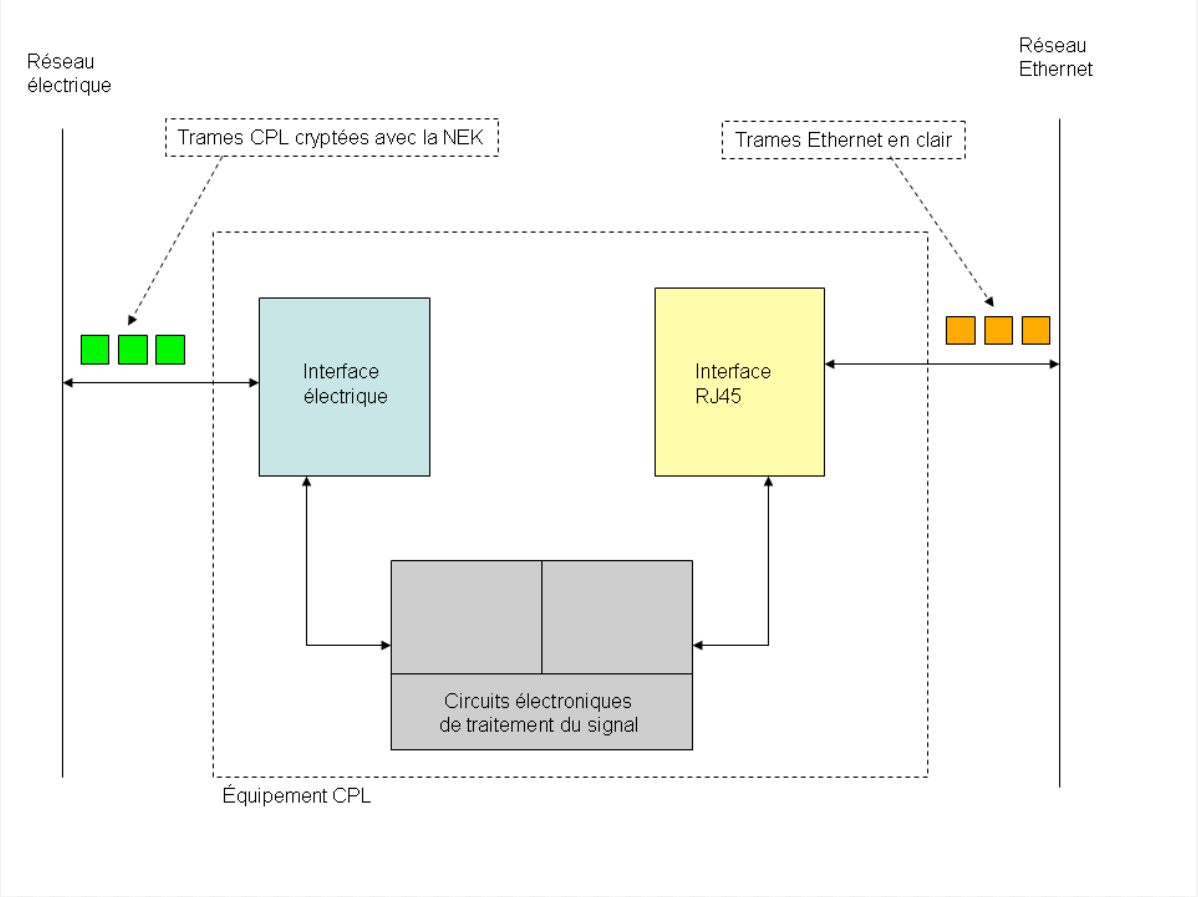
Cohabitation of PLC techs



PLC Security : Access to the PHY layer

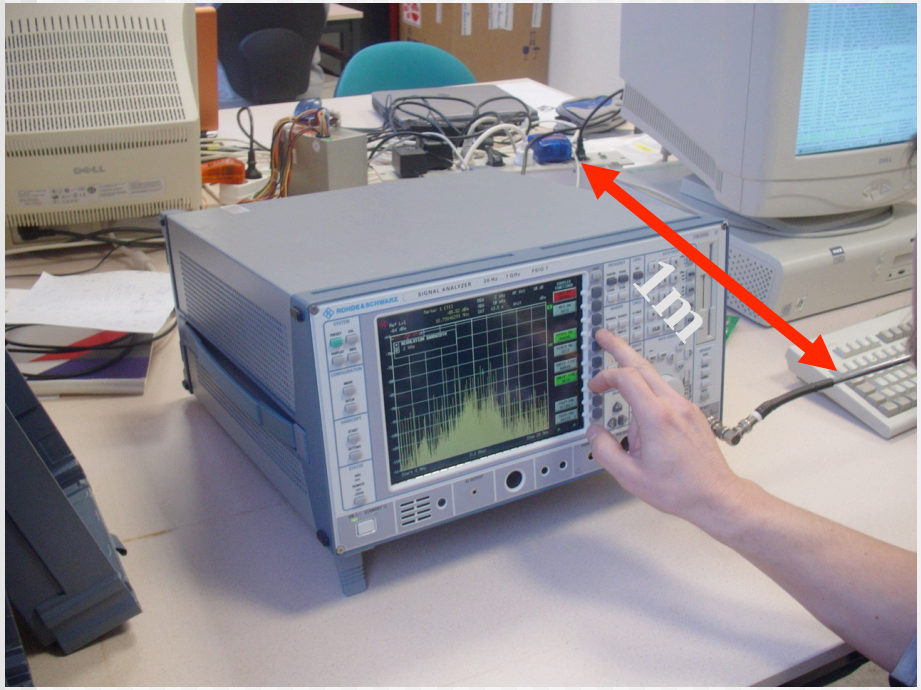


PLC Security : Access to the PHY layer

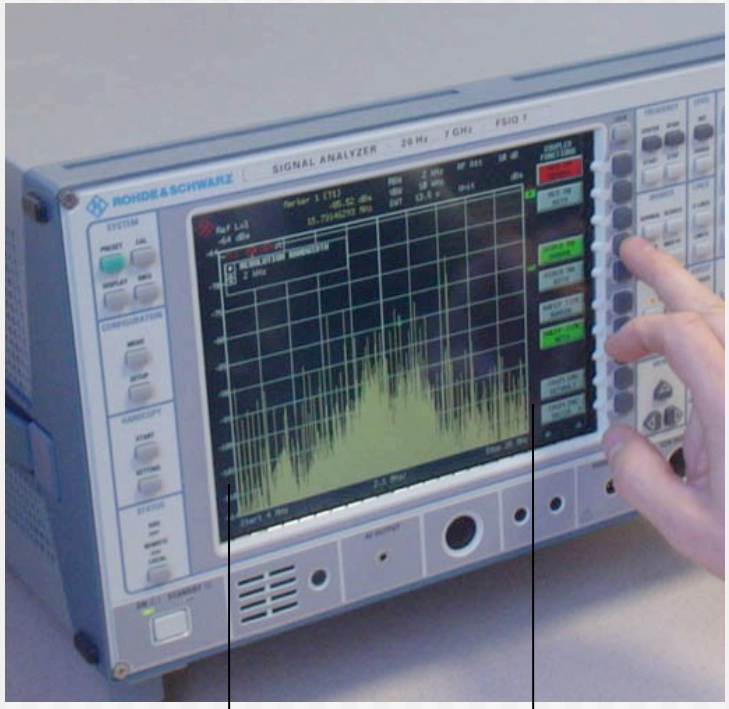


Sniffing the PHY layer

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



60kHz per division
[-110,-95dBm]@1m
Freq_span = 656.25kHz



1-30MHz

OFDM modulation
916 sub-bands

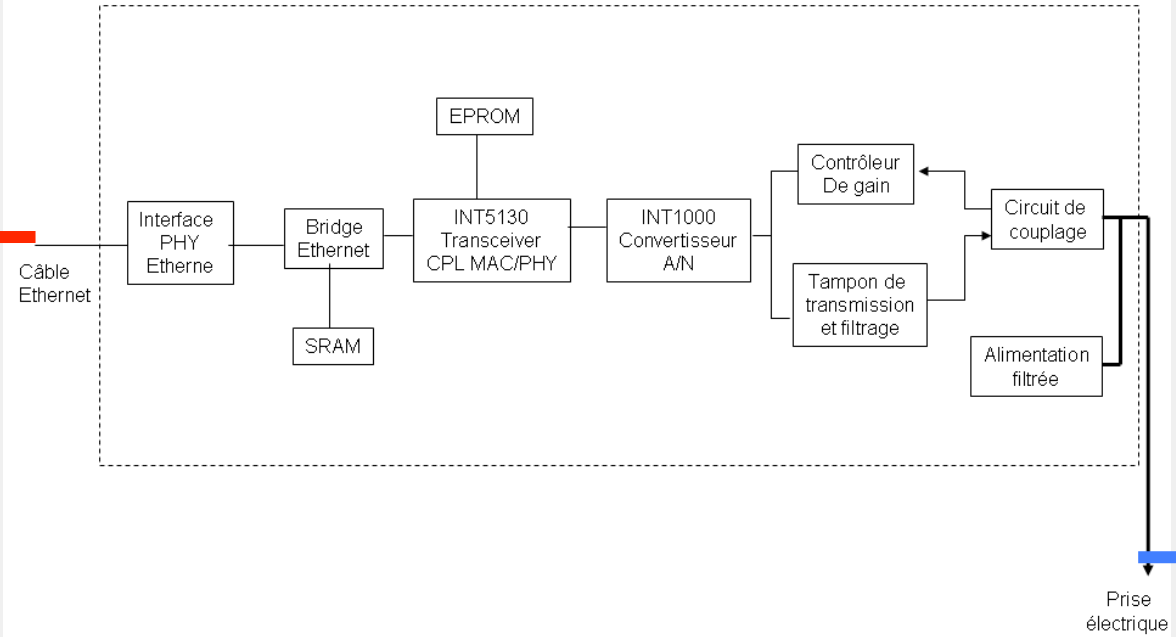
PLC Standards and Techs : Homeplug 1.0, 1.1,AV

- Security
  - HP 1.0 / 1.1 : 56-DES passphrase NEK
    - =>Market default password : **HomePlug**
    - =>Plug-and-play HomeNetworking has a security drawback
  - HP AV : 128-AES shared key + COORD key managment
  - No access to the encrypted keys on the electrical cable
  - Default password for off-the-shelf

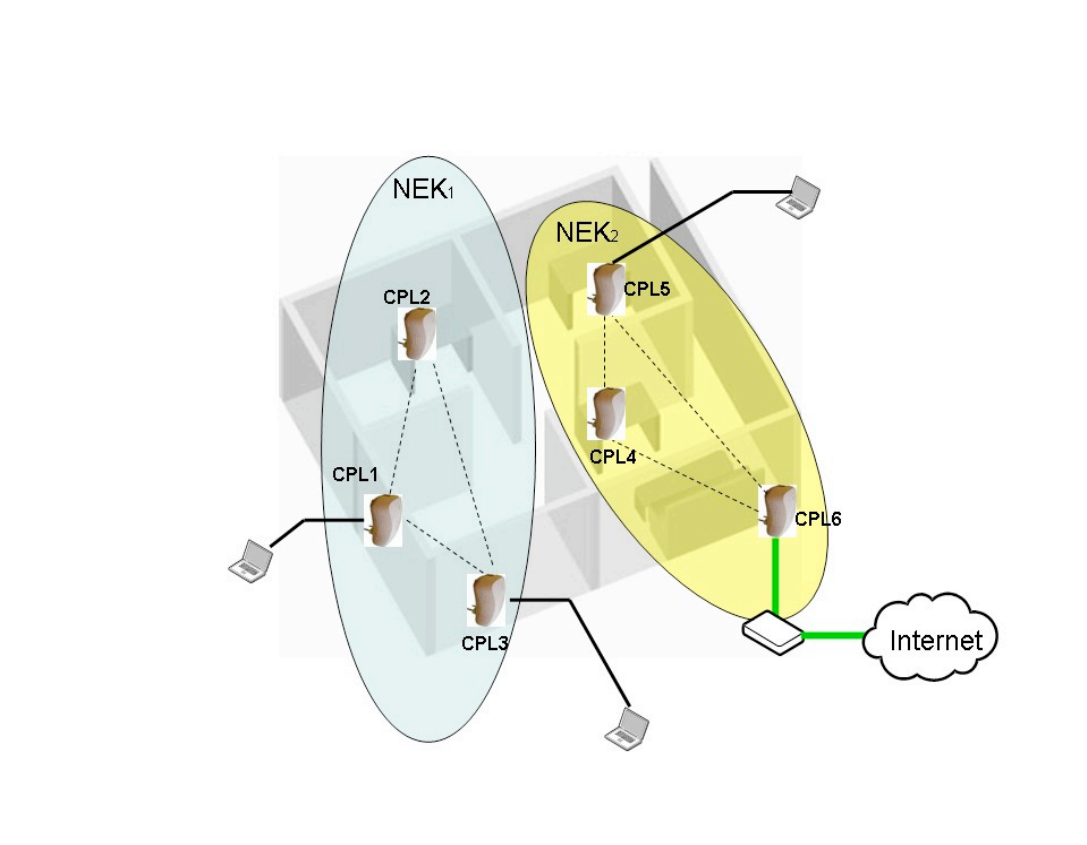
H/W for PLC devices

Ethernet LAN

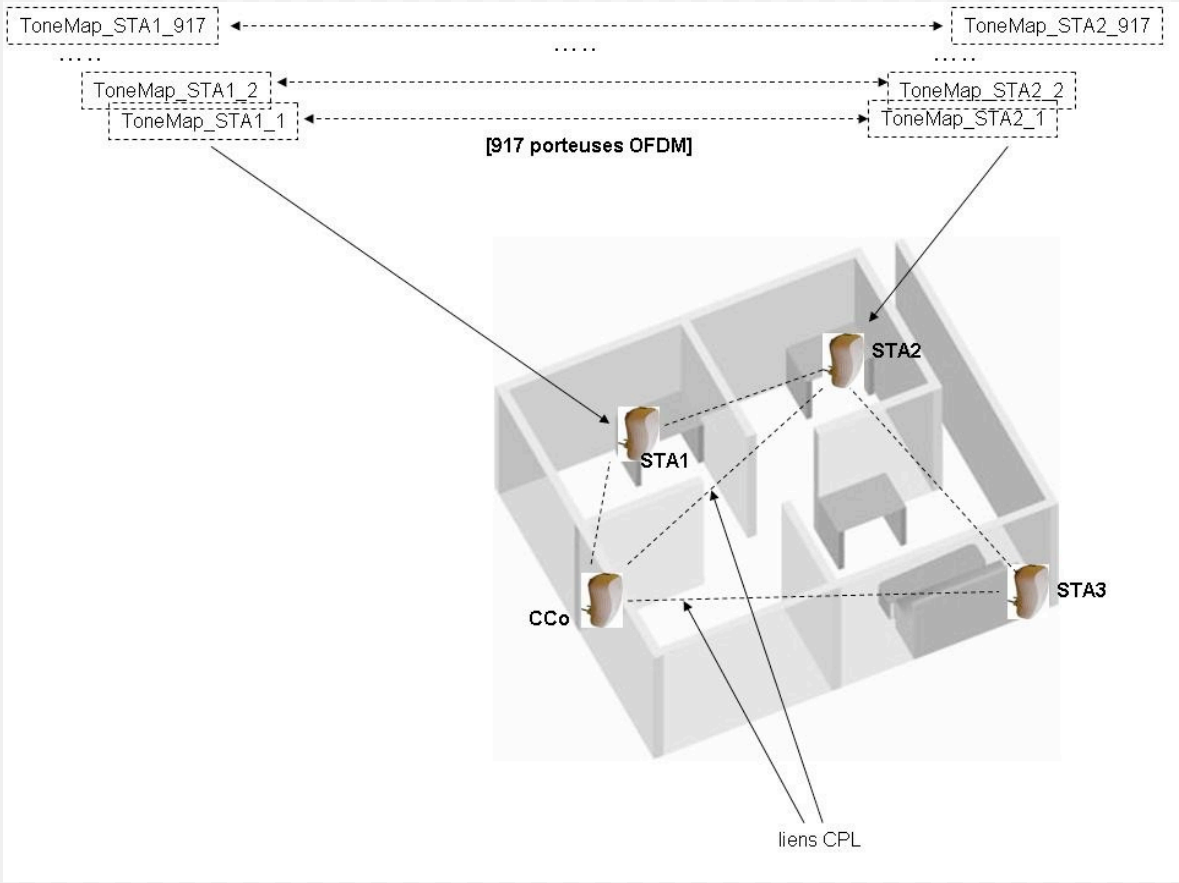
Power LAN



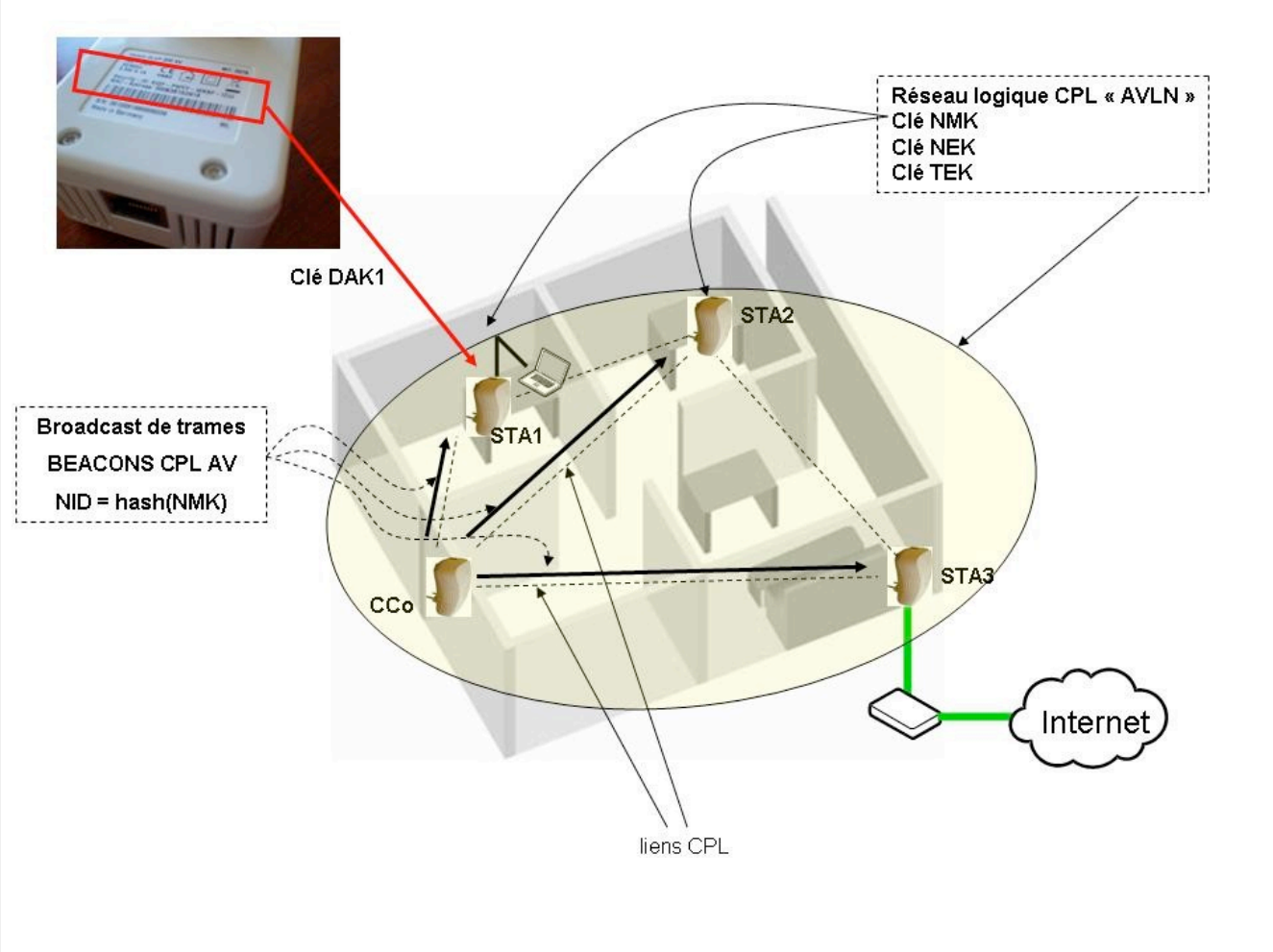
PLC Security : Network Encryption Key



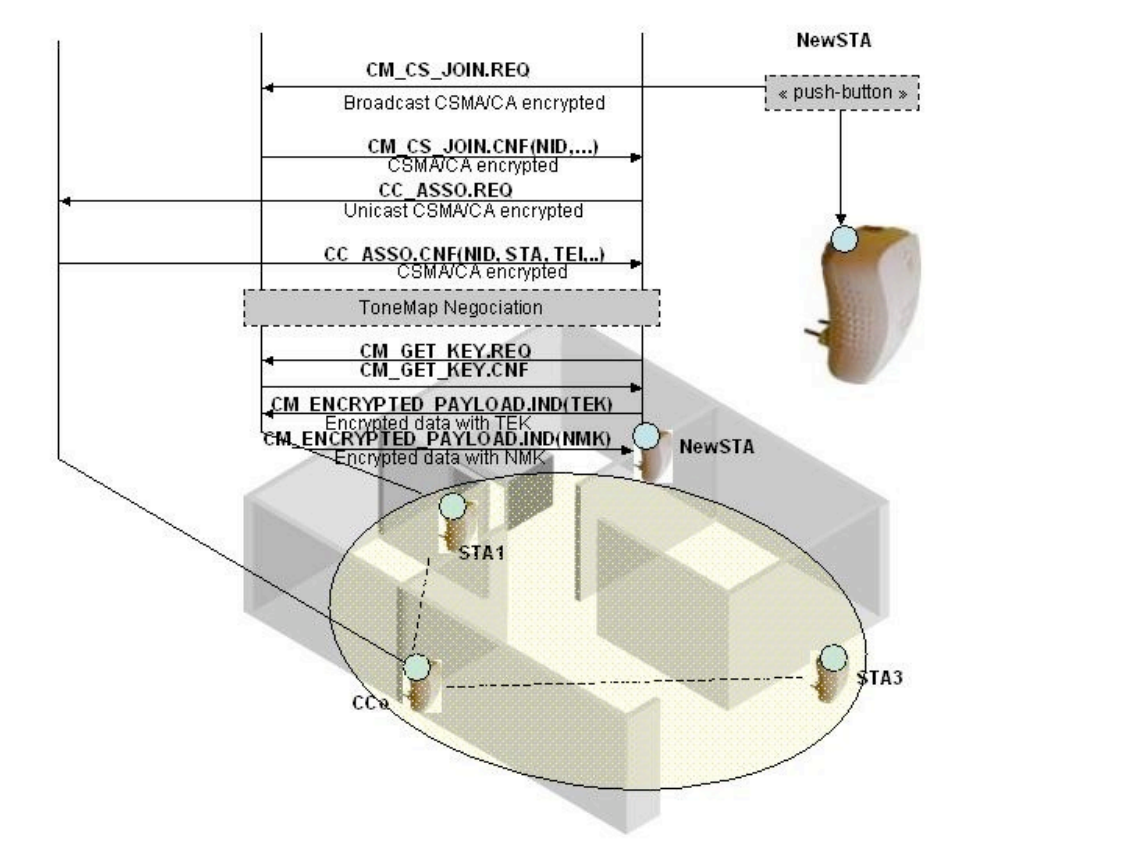
PLC Security architecture



PLC Security architecture



PLC Security : Simple connect mode



Security Issues in PLC

Technology / Standard	Encryption keys	Encryption level	Advantages	Possible exploits
HomePlug 1.0	NEK	DES-56bits	Simplicity	– DES flawless – Only one key per device
HomePlug Turbo	NEK	DES-56	Simplicity	– DES flawless – Only one key per device
HomePlug AV	– NEK – NMK – DAK – TEK	AES-128 bits (rotating keys)	Resistant encryption	Exploit through the « Easy Connect » button
UPA (DS2)	Master-Slave keys handshake	3DES	Central key administration	Interception of the keys during keys handshakes

PLC Security : Possible attacks / exploits

Name of the attack	Short description	Difficulties	Possible improvments
PLC Tempest	Using a complex hardware solutions with [spectrum analyzer + loop antennas + demodulator + CAD]	+++	Possible usage a read-to-use PLC demodulation libraries (OFDM + AM/PM) for PLC standards in the spectrum analyzer (Rhode&Scwartz support)
FPGA PLC device	Implementing an FPGA-bitstream identical to a PLC SoC to be able to dump the PLC frames received on the electrical interface	+++	Thinking the FPGA bitstream with macro-blocks to dump the encrypted frames listened on the medium
HPAV TEK frame sniffing	Using special FAIFA features to switch the HPAV chip into sniff mode	++	Understanding the sniff mode in the HPAV standard
Intellon SoC reverse engineering	Finding the JTAG port on the SoC and use the correct BSDL to access the nucleus firmware	+++	Finding similar nucleus SoC based on the ARM 926-EJS architecture
NEK brute-force	Developing a dictionnary to try words against the passphrase for HPAV devices	++	How many keys to be tested by seconds
HPAV Management spoofing	Comparing the different HomePlug AV chip (Intellon, Giggle, Arkados, Spidcom)	++	Studying the HPAV management frames and reserved bits

PLC Security tools

- Manuel Kasper's *plconfig* (lipcap) for HomePlug 1.0 (**http://neon1.net/)**
- *Wireshark HomePlug 1.0* dissector from Sebastien
- Devolo *dLAN-linux-package-2.0* (libcap 0.8.3)

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

  - **FAIFA scripting**
  - **SCAPY for PLC**
  - **Spidcom MALIKA**

PLC Security : using FAIFA

- OpenSource tool to monitor/configure HP1.0/AV chips (released for 25c3) now packaged for Debian/OpenWRT (DSL boxes BSP for some ISP)
- Tool based on Ethernet frames transmitted to the chips (ETHERTYPE = 0x881e)
- Possibly switching HPAV chips into *sniffing* mode (chip sending up to 100 fps to an arbitrary MAC station)
- Possible remote and flashing on both NVRAM and FW
- SDRAM timing changes resulting in bricks of devices (PLC DoS…)
- Monitoring of the PHY/MAC layer (eq to *wlanconfig wlan0 peers* in 802.11) for OFDM schemas
- Discovering the network topology and per-device statistics collections

Conclusion

- Now widely used technologies and soon IEEE-ed with several vendors implementations (ARM/Linux SoC probably)
- Sniffing the electrical cable is not easy but the electrical cables goes everywhere
- Try default PnP passwords on devices to sniff
- Several exploits/attacks strategies to implement
- Very few exploits released on PLC so far :☺

??? QUESTIONS ???