« Ah, the good old days »

or not …

A review of the work, including a re-examination of the experiments carried out as part of my PhD thesis entitled
« **Sécurité des équipements grand public connectés à Internet** »

- Bachy, Y., Basse, F., Nicomette, V., Alata, E., Kaâniche, M., Courrege, J. C., & Lukjanenko, P. (2015, June). Smart-TV security analysis: practical experiments. In *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (pp. 497-504). IEEE.
- Bachy, Y., Nicomette, V., Alata, E., Kaâniche, M., Courrège, J. C., & Lukjanenko, P. (2015, June). Protocole HbbTV et sécurité: quelques expérimentations. In *Symposium sur la sécurité des technologies de l'information et des communications*.
- Bachy, Y., Nicomette, V., Alata, E., Kaâniche, M., & Courrege, J. C. (2015, September). Security of ISP Access Networks: practical experiments. In *2015 11th European Dependable Computing Conference (EDCC)* (pp. 205-212). IEEE.
- Bachy, Y., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., & Courrège, J. C. (2014, June). Analyse de sécurité des box ADSL. In *Symposium sur la sécurité des technologies de l'information et des communications* (Vol. 2014).
- Bachy, Y., Nicomette, V., Alata, E., Kâaniche, M., & Courrège, J. C. (2014). La sécurité des box ADSL. Analyse de risques et expérimentations. *Revue des Sciences et Technologies de l'Information-Série ISI: Ingénierie des Systèmes d'Information*, *19*(6), pp-63.

The smart home

The abandoned home

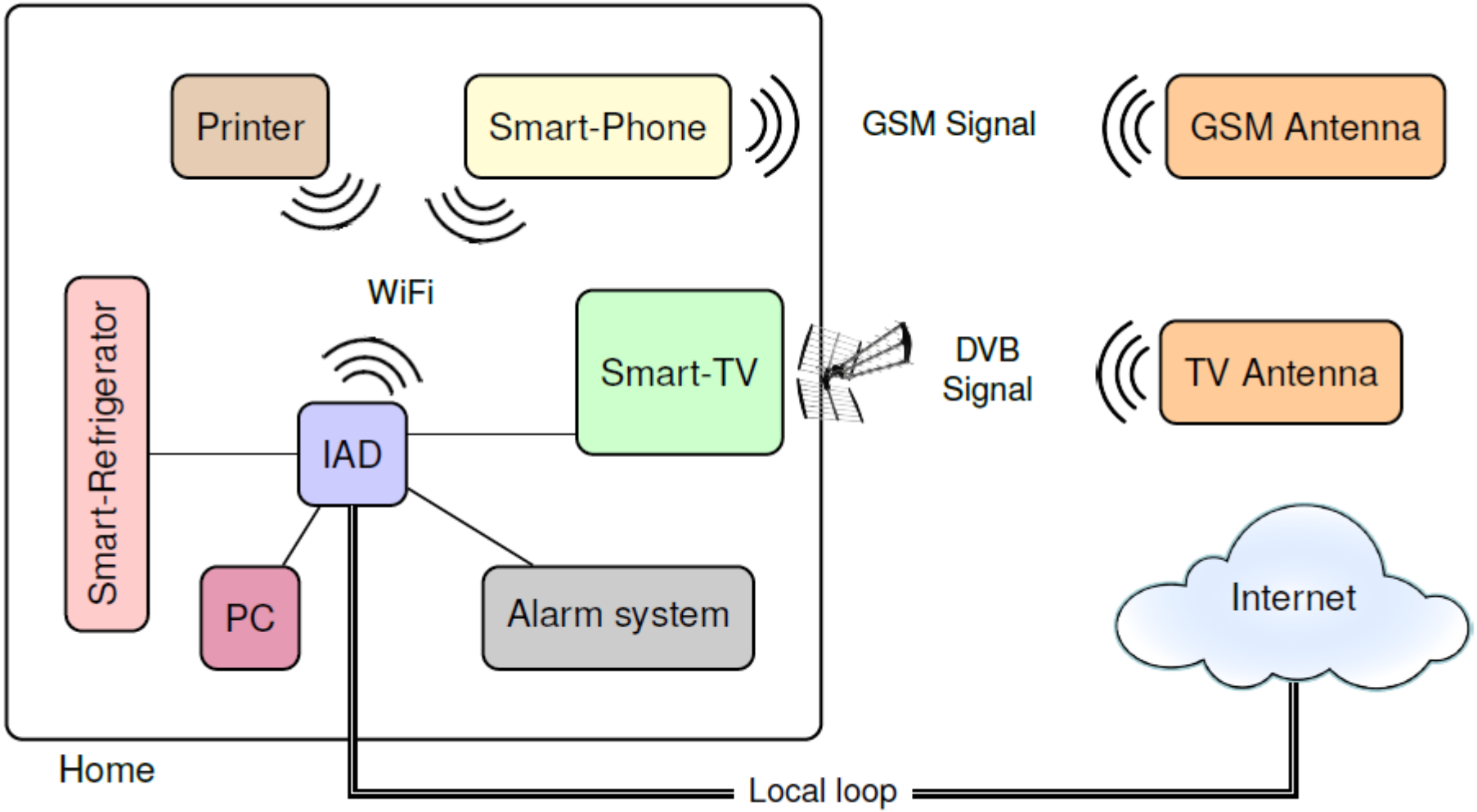
https://www.maison-et-domotique.com/164791-qiara-met-la-cle-sous-la-porte/

https://www.clubic.com/actualite-572658-en-arretant-definitivement-ses-serveurs-wemo-belkin-envoie-des-milliers-d-objets-connectes-a-la-casse.html

https://www.lesnumeriques.com/assistant-domotique/orange-debranchera-les-enceintes-djingo-le-31-mars-et-remboursera-leurs-acquereurs-n159929.html

https://www.igen.fr/domotique/2025/04/nest-fait-du-menage-dans-sa-gamme-et-abandonne-le-marche-europeen-des-thermostats-connectes-149709

Massive interconnections



Massive interconnections

Issues identified ten years ago

- **Architecture of connected devices**
  - Similar to that of a personal computer
  - Generally, more powerful than the device's actual computing requirements

➔ **Devices that can be compromised to execute malicious code**

- **Operating system / firmware**
  - Maintenance often inaccessible to the user
  - Impossibility of verifying the manufacturer's good faith

➔ **Increased risk of vulnerabilities due to delayed or non-existent maintenance**

- **User data**
  - Possibility of storing the user's private information
  - No control over its use

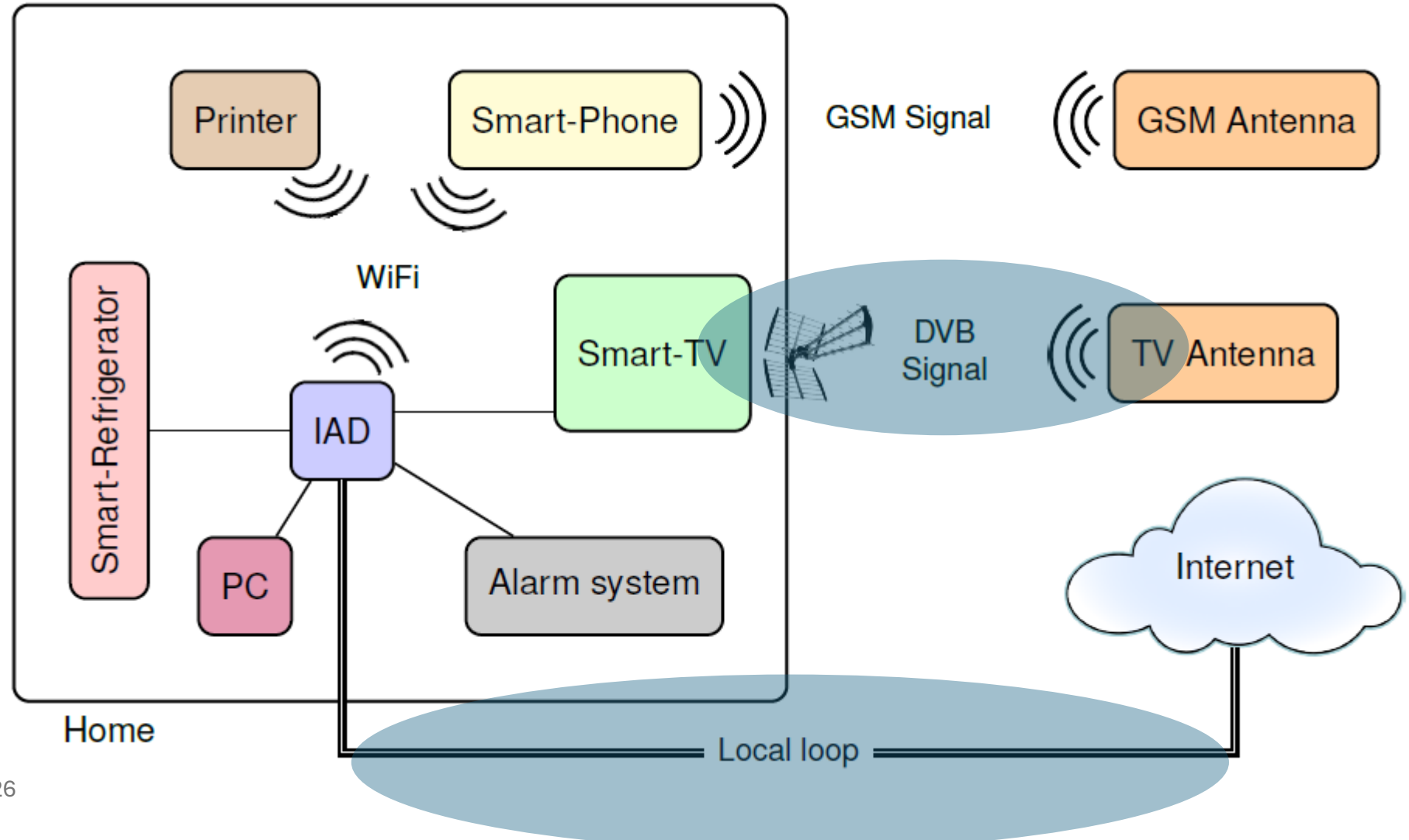
➔ **No guarantee of respect for the user's privacy**

- **Communication interfaces**
  - Connections outside the home
  - The shared local network
  - Some networks are less protected because they have historically not been considered potential targets for attacks

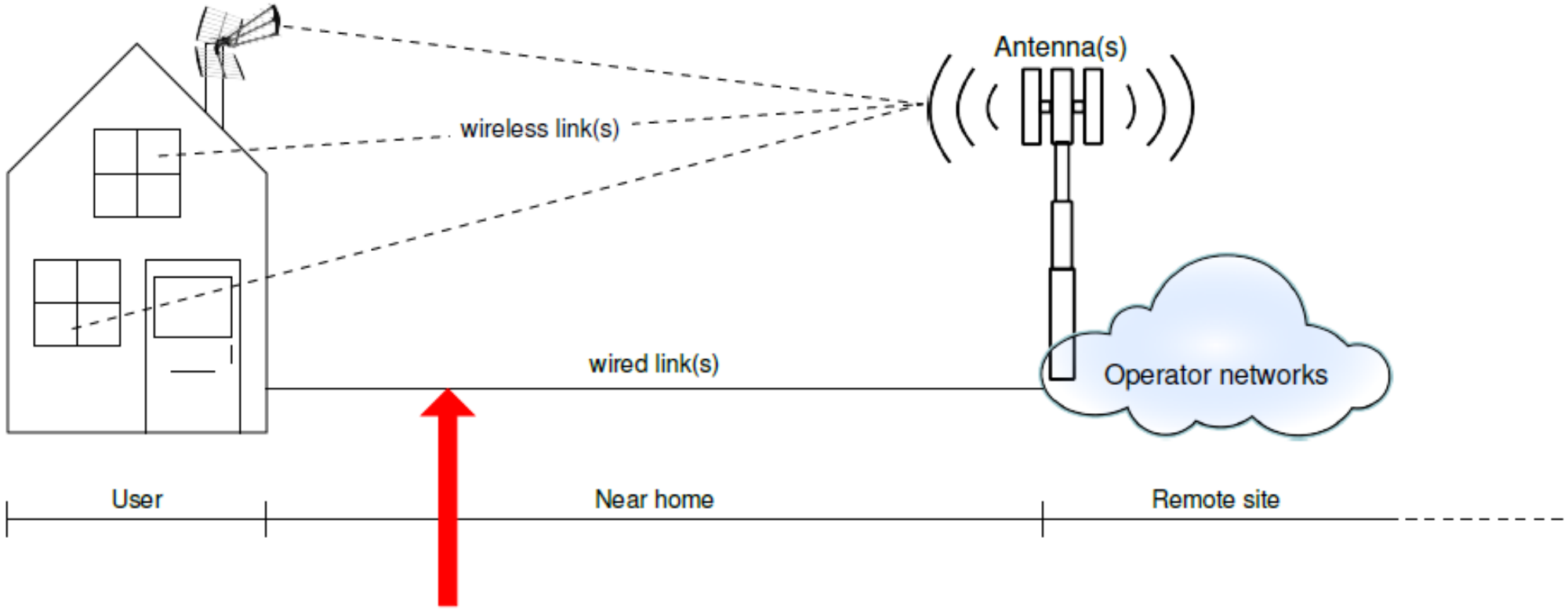
➔ **Increased attack surface due to all these communication interfaces**

➔ **Equipment connected to multiple networks can be used as a relay, once compromised, to attack other devices**

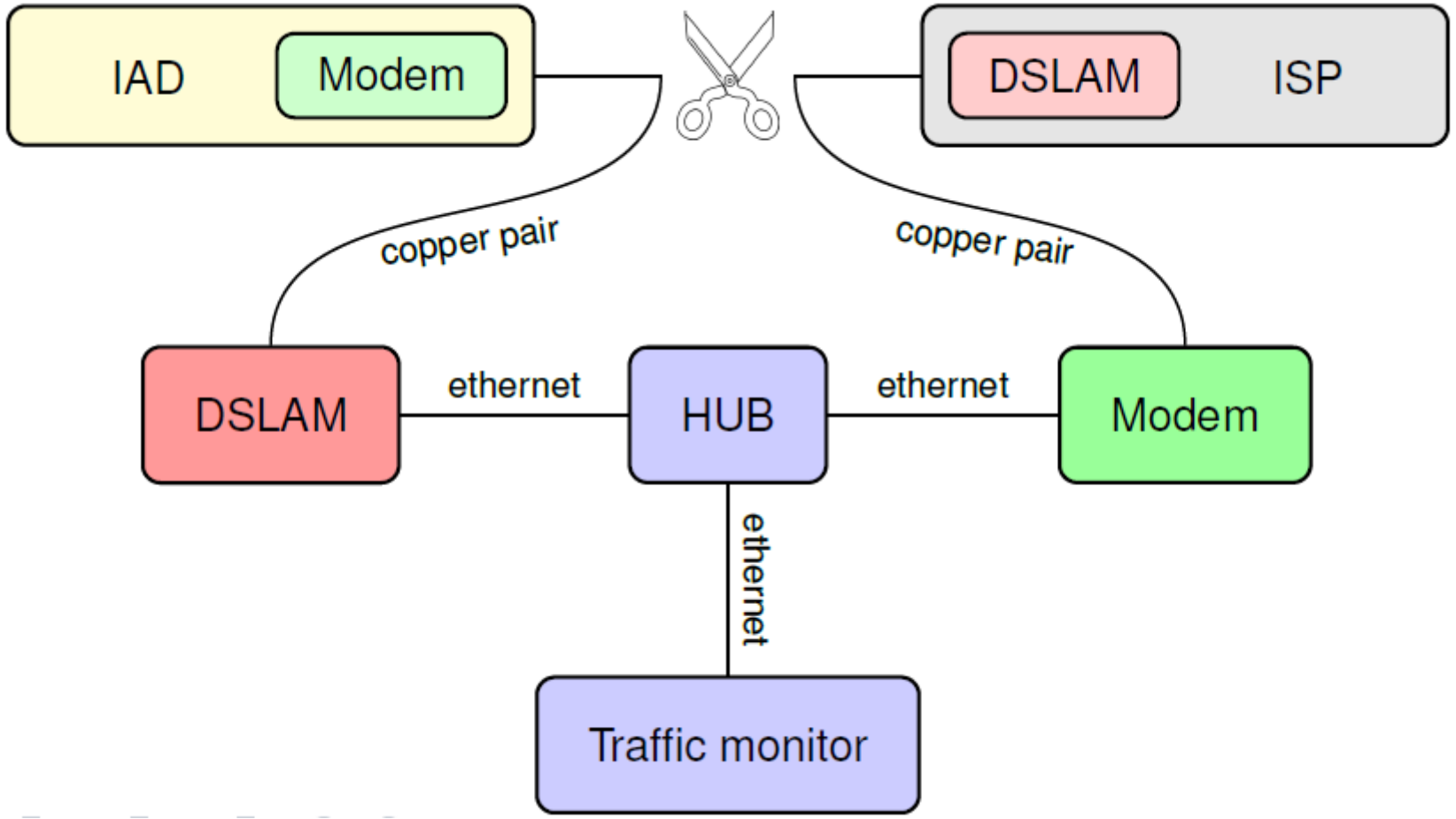
Local loop and DVB-T



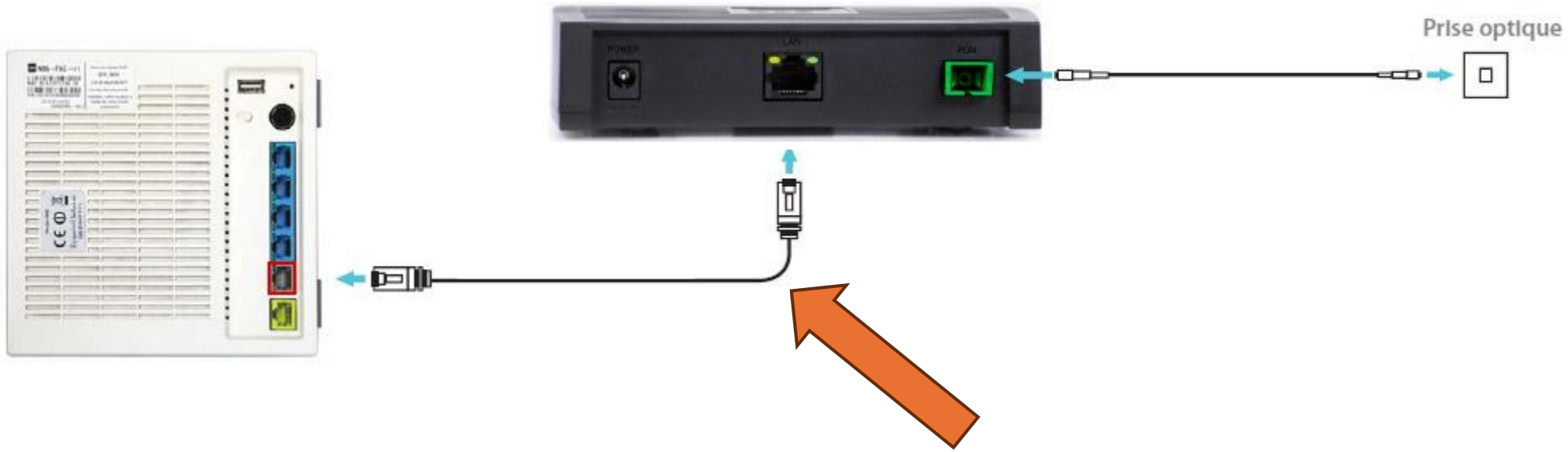
Local loop


Antenna(s)
wireless link(s)
wired link(s)
Operator networks
User
Near home
Remote site

Sniffing the local loop



Sniffing fiber optics



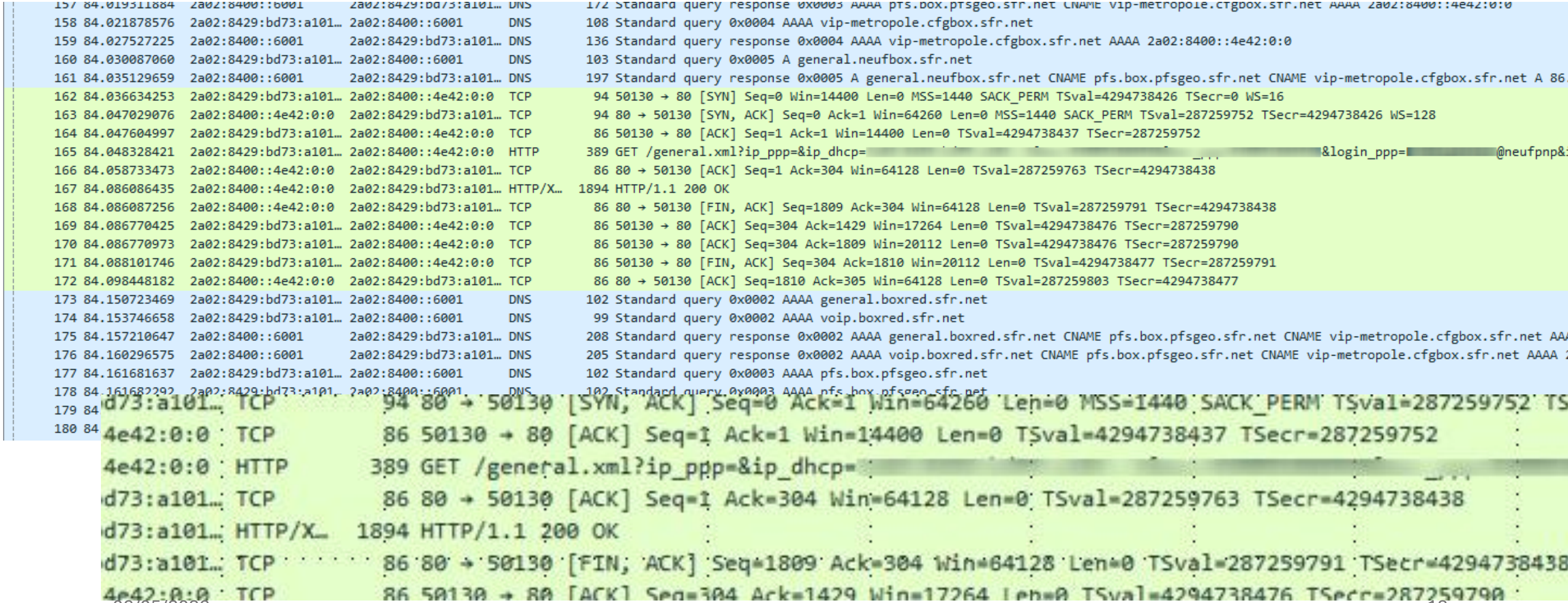
After all, sniffing fiber optics is easy!

Boot-up and update of french internet access devices in 2015

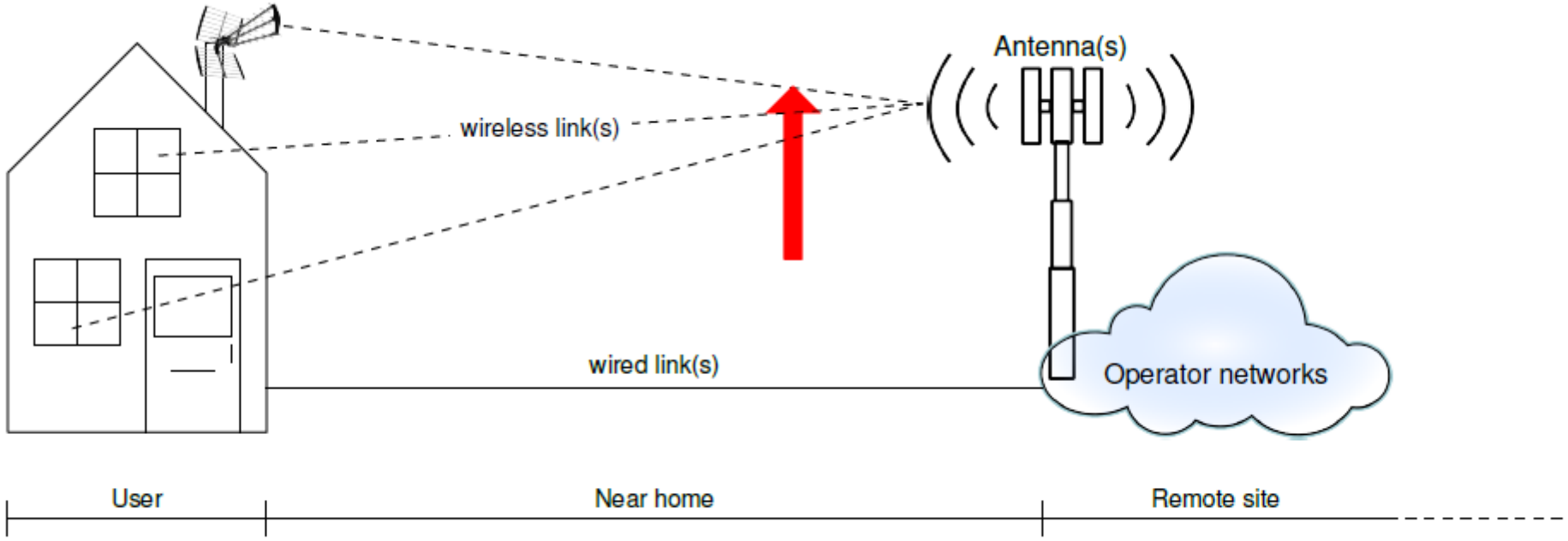
IAD	Protocols used during	
	Boot-up	Update
A	HTTP, FTP, SSL	-
B	HTTP, SSL	SSL
C	SSL	-
D	HTTP	HTTP
E	HTTP	HTTP
F	SSL	-

Box D in 2026 ...

Box D in 2026 ...


157 84.019311884 2a02:8400::6001 2a02:8429:bd73:a101… DNS 172 Standard query response 0x0003 AAAA pfs.box.pfsgeo.sfr.net CNAME vip-metropole.cfgbox.sfr.net AAAA 2a02:8400::4e42:0:0
158 84.021878576 2a02:8429:bd73:a101… 2a02:8400::6001 DNS 108 Standard query 0x0004 AAAA vip-metropole.cfgbox.sfr.net
159 84.027527225 2a02:8400::6001 2a02:8429:bd73:a101… DNS 136 Standard query response 0x0004 AAAA vip-metropole.cfgbox.sfr.net AAAA 2a02:8400::4e42:0:0
160 84.030087060 2a02:8429:bd73:a101… 2a02:8400::6001 DNS 103 Standard query 0x0005 A general.neufbox.sfr.net
161 84.035129659 2a02:8400::6001 2a02:8429:bd73:a101… DNS 197 Standard query response 0x0005 A general.neufbox.sfr.net CNAME pfs.box.pfsgeo.sfr.net CNAME vip-metropole.cfgbox.sfr.net A 86.
162 84.036634253 2a02:8429:bd73:a101… 2a02:8400::4e42:0:0 TCP 94 50130 → 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM TSval=4294738426 TSecr=0 WS=16
163 84.047029076 2a02:8400::4e42:0:0 2a02:8429:bd73:a101… TCP 94 80 → 50130 [SYN, ACK] Seq=0 Ack=1 Win=64260 Len=0 MSS=1440 SACK_PERM TSval=287259752 TSecr=4294738426 WS=128
164 84.047604997 2a02:8429:bd73:a101… 2a02:8400::4e42:0:0 TCP 86 50130 → 80 [ACK] Seq=1 Ack=1 Win=14400 Len=0 TSval=4294738437 TSecr=287259752
165 84.048328421 2a02:8429:bd73:a101… 2a02:8400::4e42:0:0 HTTP 389 GET /general.xml?ip_ppp=&ip_dhcp= &login_ppp= @neufpnp&
166 84.058733473 2a02:8400::4e42:0:0 2a02:8429:bd73:a101… TCP 86 80 → 50130 [ACK] Seq=1 Ack=304 Win=64128 Len=0 TSval=287259763 TSecr=4294738438
167 84.086086435 2a02:8400::4e42:0:0 2a02:8429:bd73:a101… HTTP/X… 1894 HTTP/1.1 200 OK
168 84.086087256 2a02:8400::4e42:0:0 2a02:8429:bd73:a101… TCP 86 80 → 50130 [FIN, ACK] Seq=1809 Ack=304 Win=64128 Len=0 TSval=287259791 TSecr=4294738438
169 84.086770425 2a02:8429:bd73:a101… 2a02:8400::4e42:0:0 TCP 86 50130 → 80 [ACK] Seq=304 Ack=1429 Win=17264 Len=0 TSval=4294738476 TSecr=287259790
170 84.086770973 2a02:8429:bd73:a101… 2a02:8400::4e42:0:0 TCP 86 50130 → 80 [ACK] Seq=304 Ack=1809 Win=20112 Len=0 TSval=4294738476 TSecr=287259790
171 84.088101746 2a02:8429:bd73:a101… 2a02:8400::4e42:0:0 TCP 86 50130 → 80 [FIN, ACK] Seq=304 Ack=1810 Win=20112 Len=0 TSval=4294738477 TSecr=287259791
172 84.098448182 2a02:8400::4e42:0:0 2a02:8429:bd73:a101… TCP 86 80 → 50130 [ACK] Seq=1810 Ack=305 Win=64128 Len=0 TSval=287259803 TSecr=4294738477
173 84.150723469 2a02:8429:bd73:a101… 2a02:8400::6001 DNS 102 Standard query 0x0002 AAAA general.boxred.sfr.net
174 84.153746658 2a02:8429:bd73:a101… 2a02:8400::6001 DNS 99 Standard query 0x0002 AAAA voip.boxred.sfr.net
175 84.157210647 2a02:8400::6001 2a02:8429:bd73:a101… DNS 208 Standard query response 0x0002 AAAA general.boxred.sfr.net CNAME pfs.box.pfsgeo.sfr.net CNAME vip-metropole.cfgbox.sfr.net AA
176 84.160296575 2a02:8400::6001 2a02:8429:bd73:a101… DNS 205 Standard query response 0x0002 AAAA voip.boxred.sfr.net CNAME pfs.box.pfsgeo.sfr.net CNAME vip-metropole.cfgbox.sfr.net AAAA
177 84.161681637 2a02:8429:bd73:a101… 2a02:8400::6001 DNS 102 Standard query 0x0003 AAAA pfs.box.pfsgeo.sfr.net
178 84.161682292 2a02:8429:bd73:a101… 2a02:8400::6001 DNS 102 Standard query 0x0003 AAAA pfs.box.pfsgeo.sfr.net
179 84 d73:a101… TCP 94 80 → 50130 [SYN, ACK] Seq=0 Ack=1 Win=64260 Len=0 MSS=1440 SACK_PERM TSval=287259752 TS
180 84 4e42:0:0 TCP 86 50130 → 80 [ACK] Seq=1 Ack=1 Win=14400 Len=0 TSval=4294738437 TSecr=287259752
4e42:0:0 HTTP 389 GET /general.xml?ip_ppp=&ip_dhcp=
d73:a101… TCP 86 80 → 50130 [ACK] Seq=1 Ack=304 Win=64128 Len=0 TSval=287259763 TSecr=4294738438
d73:a101… HTTP/X… 1894 HTTP/1.1 200 OK
d73:a101… TCP 86 80 → 50130 [FIN, ACK] Seq=1809 Ack=304 Win=64128 Len=0 TSval=287259791 TSecr=4294738438
4e42:0:0 TCP 86 50130 → 80 [ACK] Seq=304 Ack=1429 Win=17264 Len=0 TSval=4294738476 TSecr=287259790

DVB-T

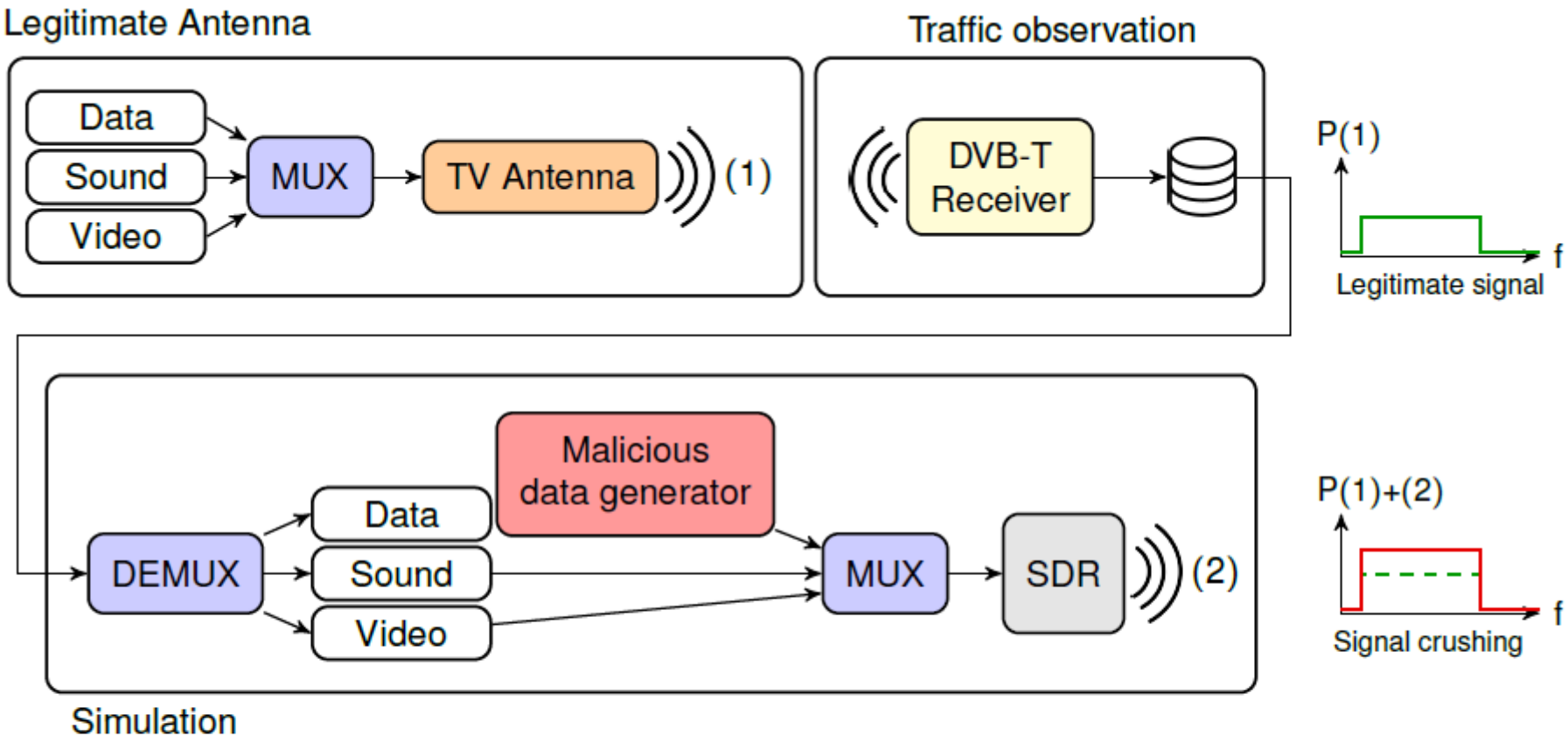

Antenna(s)
wireless link(s)
wired link(s)
Operator networks
User
Near home
Remote site

Broadcasting DVB-T

High frequency modulation
No public-available hardware
Software defined radio (SDR)

Cheap experimental modulator

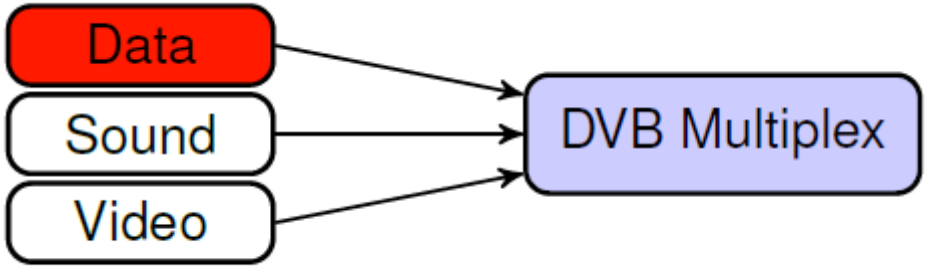
Broadcasting DVB-T



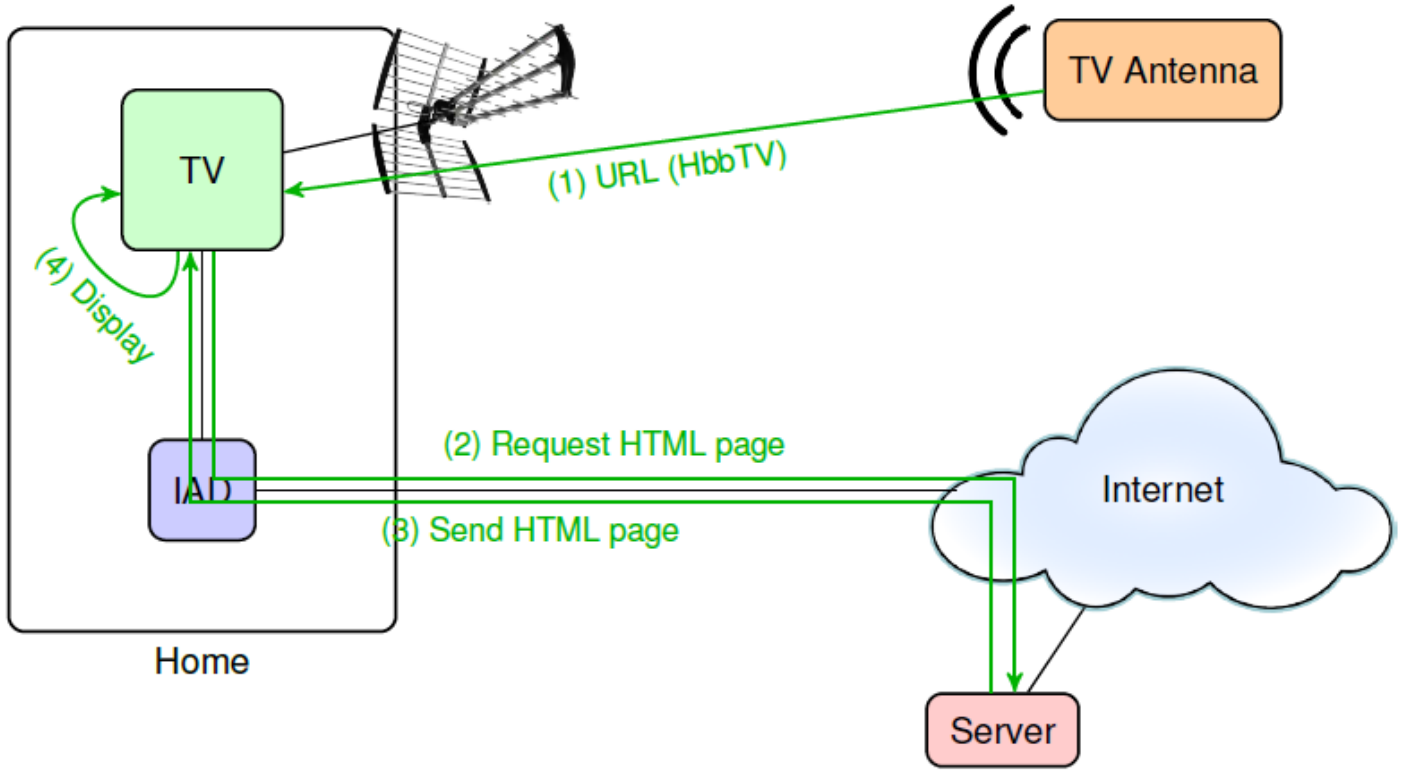
(1) = Legitimate signal

(2) = Malicious signal

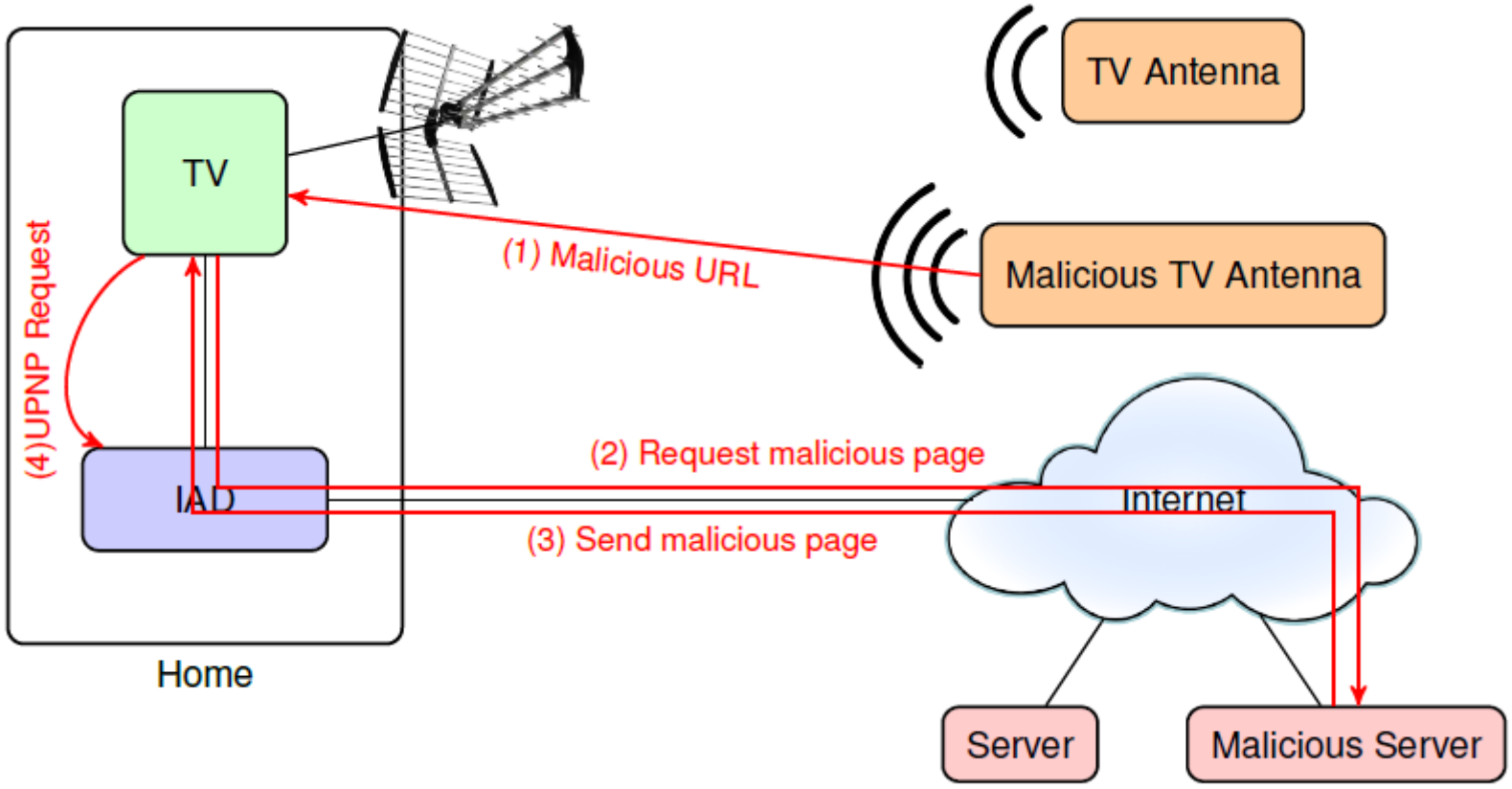
HbbTV



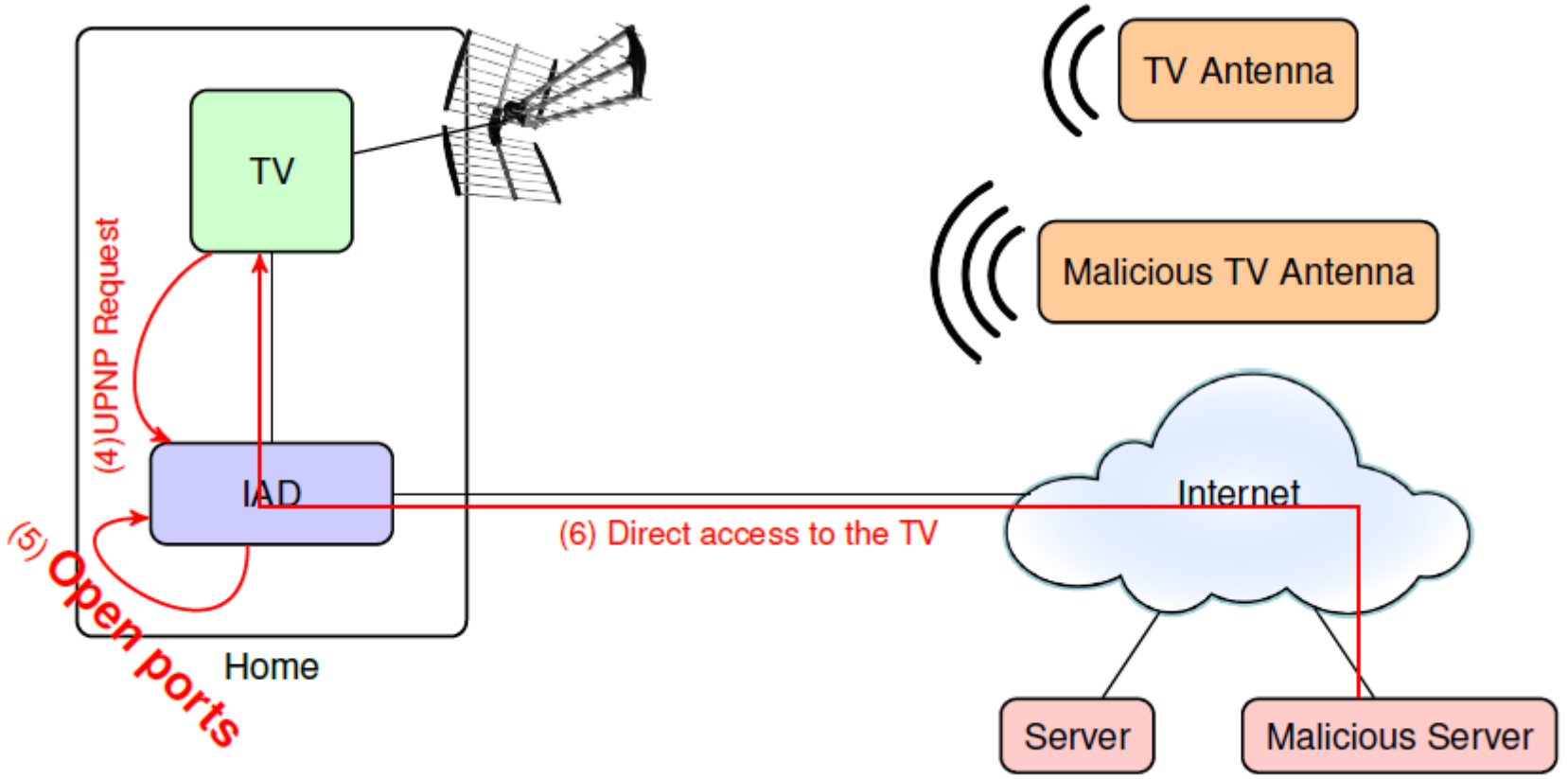
- Information concerning the channel (name, network, etc…)
- URL of interactive content (HbbTV)



Exploiting HbbTV



Exploiting HbbTV

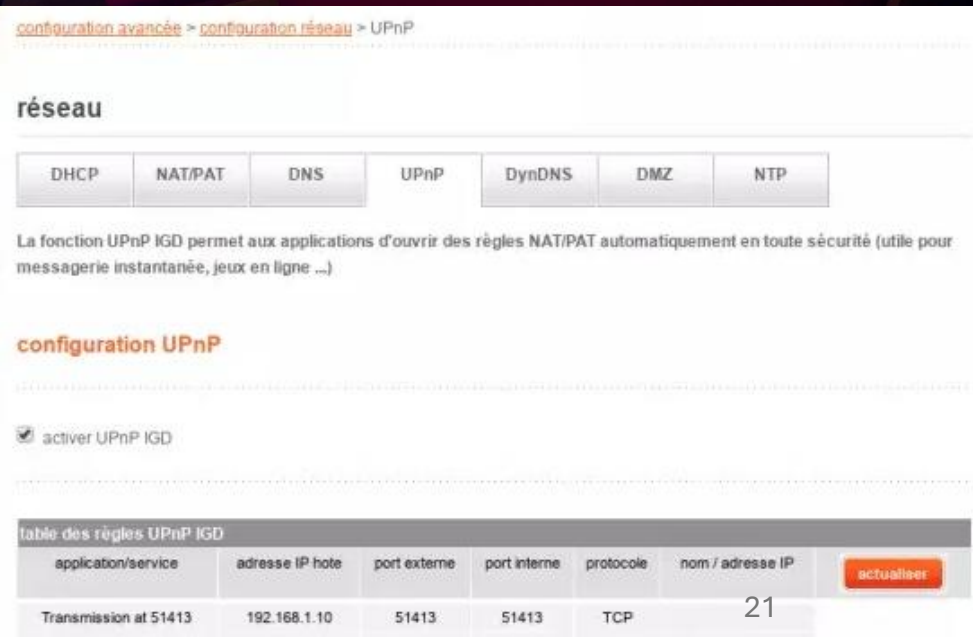


Let’s go!

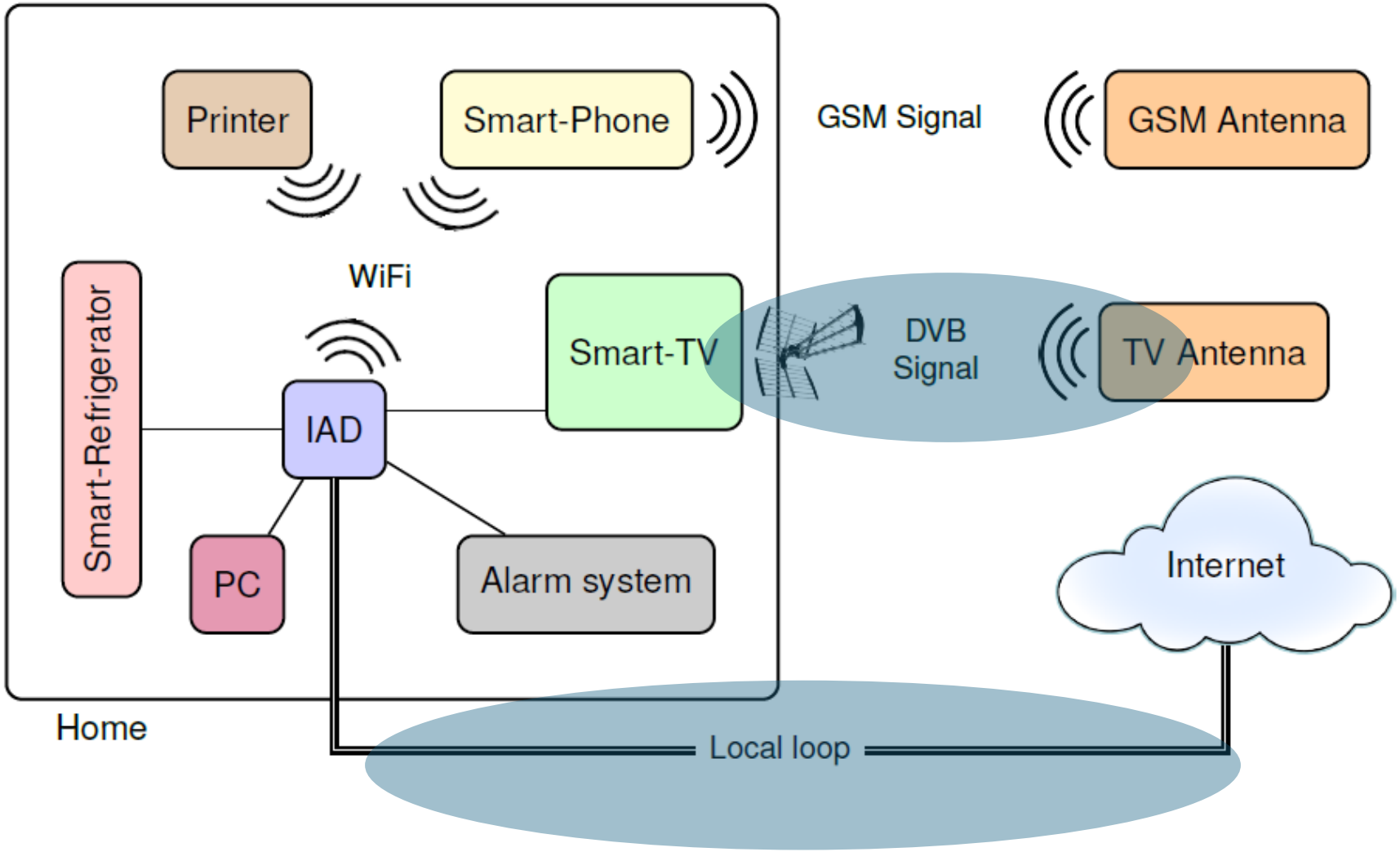
Let’s go!


DIRECT
P+
P-
X
V+
V-
OK
home
blue
back
demo2.MTS


AVALPa
digital engineering


configuration avancée > configuration réseau > UPnP
réseau
DHCP
NAT/PAT
DNS
UPnP
DynDNS
DMZ
NTP
La fonction UPnP IGD permet aux applications d'ouvrir des règles NAT/PAT automatiquement en toute sécurité (utile pour messagerie instantanée, jeux en ligne ...)
configuration UPnP
activer UPnP IGD
table des règles UPnP IGD
application/service
adresse IP hote
port externe
port interne
protocole
nom / adresse IP
actualiser
Transmission at 51413
192.168.1.10
51413
51413
TCP

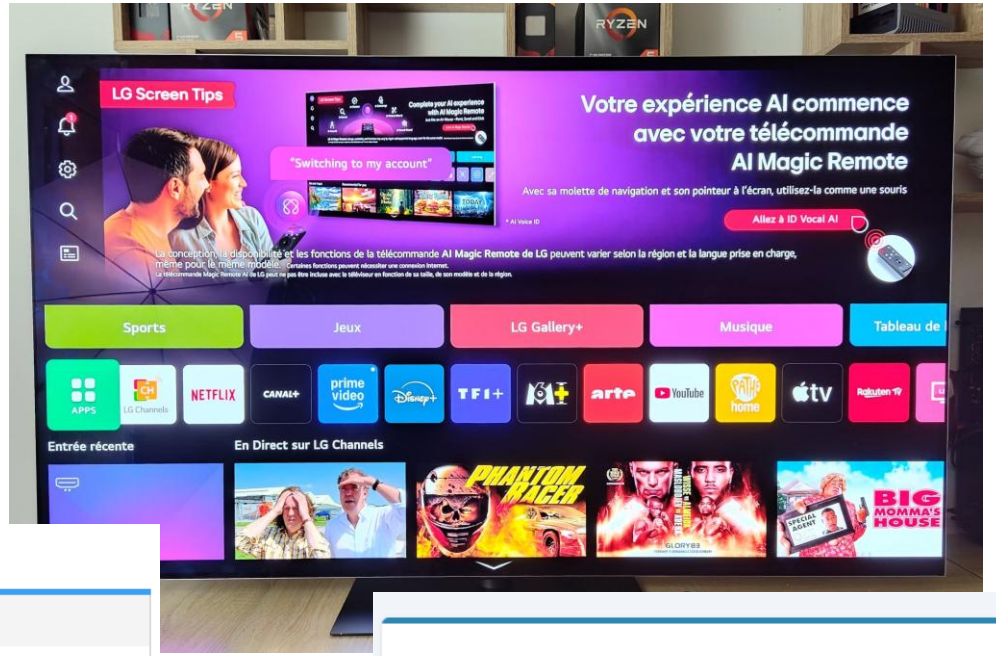
Local loop & DVB - Conclusion



Privacy

Les télés connectées de Samsung, LG et Sony accusées d’espionner les téléspectateurs

https://www.01net.com/actualites/les-teles-connectees-de-samsung-lg-et-sony-accusees-despionner-les-telespectateurs.html



ACTUALITÉ

Mac4Ever / Domotique

Amazon Ring : une nouvelle IA qui décrit ce qui se passe chez vous

DOMOTIQUE

PAR VINCENT LAUTIER - PUBLIÉ LE 26 JUIN 2025 À 11H10

1 COMMENTAIRE

La marque de sonnettes connectées d'Amazon, Ring, lance "Video Descriptions", une nouvelle fonction IA qui vous envoie des alertes textuelles décrivant ce que voient vos caméras. Une nouveauté qui pose qui pose quand même quelques questions sur la vie privée.

https://www.mac4ever.com/domotique/190234-amazon-ring-une-nouvelle-ia-qui-decrit-ce-qui-se-passe-chez-vous

Amazon achète Bee et son bracelet qui vous écoute en permanence

Pierre Dandumont

mercredi 23 juillet 2025 à 19:12 • 53

https://www.igen.fr/domotique/2025/07/amazon-achete-bee-et-son-bracelet-qui-vous-ecoute-en-permanence-151223

Privacy issues were allready there in 2013

Monday, 18 November 2013

LG Smart TVs logging USB filenames and viewing info to LG servers

https://doctorbeet.blogspot.com/2013/11/lg-smart-tvs-logging-usb-filenames-and.html

```
00000330                                                  71 75                 qu
00000340  65 72 79 3d 6d 6f 74 64  65 70 61 73 73 65 25 32  ery=motd epasse%2
00000350  45 74 78 74 3a 2f 4f 62  6c 69 76 69 6f 6e 25 32  Etxt:/Ob livion%2
00000360  45 25 33 32 25 33 30 25  33 31 25 33 33 25 32 45  E%32%30% 31%33%2E
00000370  46 52 45 4e 43 48 25 32  45 42 44 52 69 70 25 32  FRENCH%2 EBDRip%2
00000380  45 78 25 33 32 25 33 36  25 33 34 25 32 44 41 59  Ex%32%36 %34%2DAY
00000390  4d 4f 25 32 45 6d 6b 76  3a 2f 46 52 45 4e 43 48  MO%2Emkv :/FRENCH
000003A0  25 35 46 53 63 52 65 45  6e 45 72 25 32 45 6d 6b  %5FScReE nEr%2Emk
000003B0  76                                               v
```

Extract of a request sent from the television to its manufacturer

Any questions ?