LAAS-CNRS

THALES

Analyse de sécurité des BOX ADSL

Présenté par : **Y. Bachy**

RéSIST

21 Octobre 2014

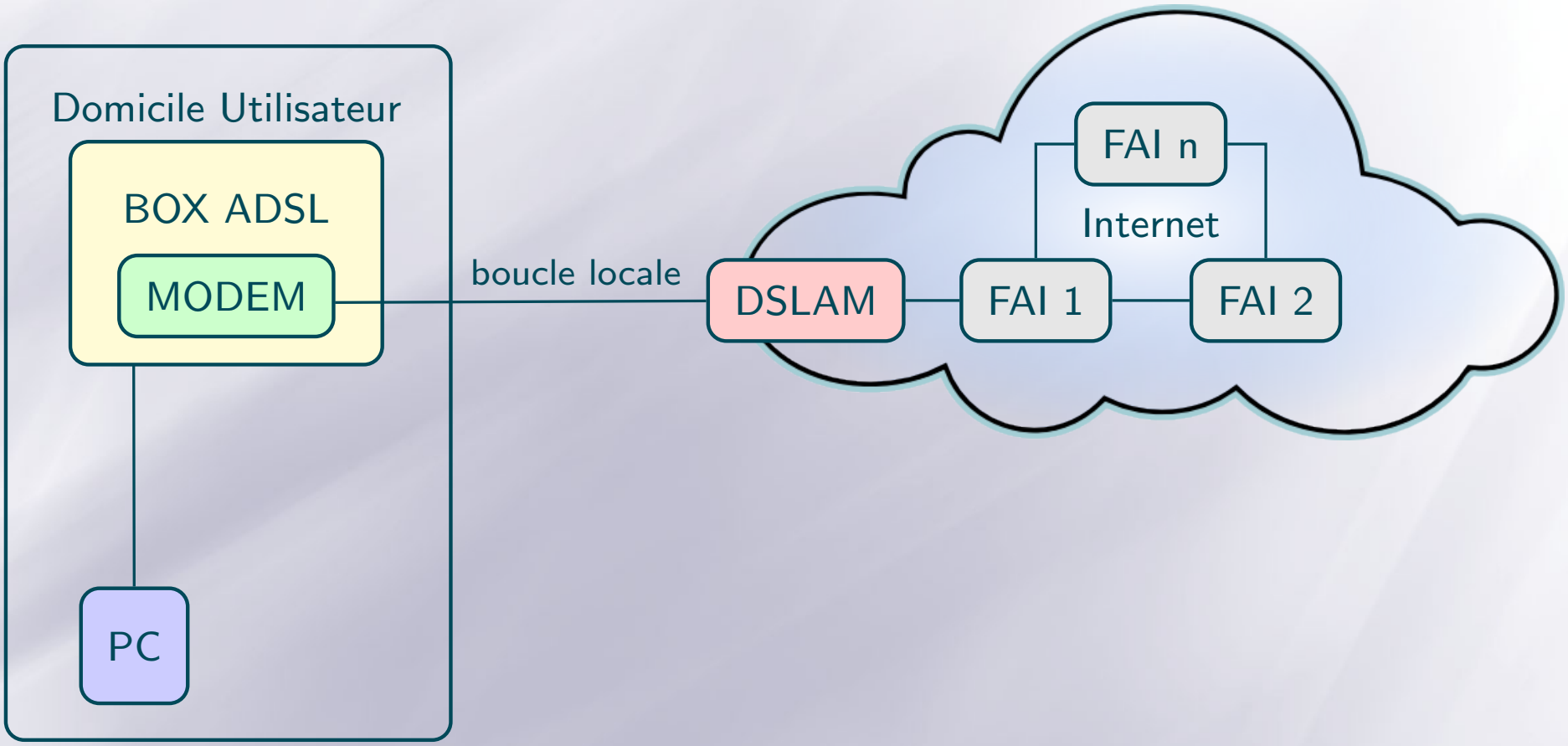
Émergence des équipements grand public connectés

Émergence des équipements grand public connectés

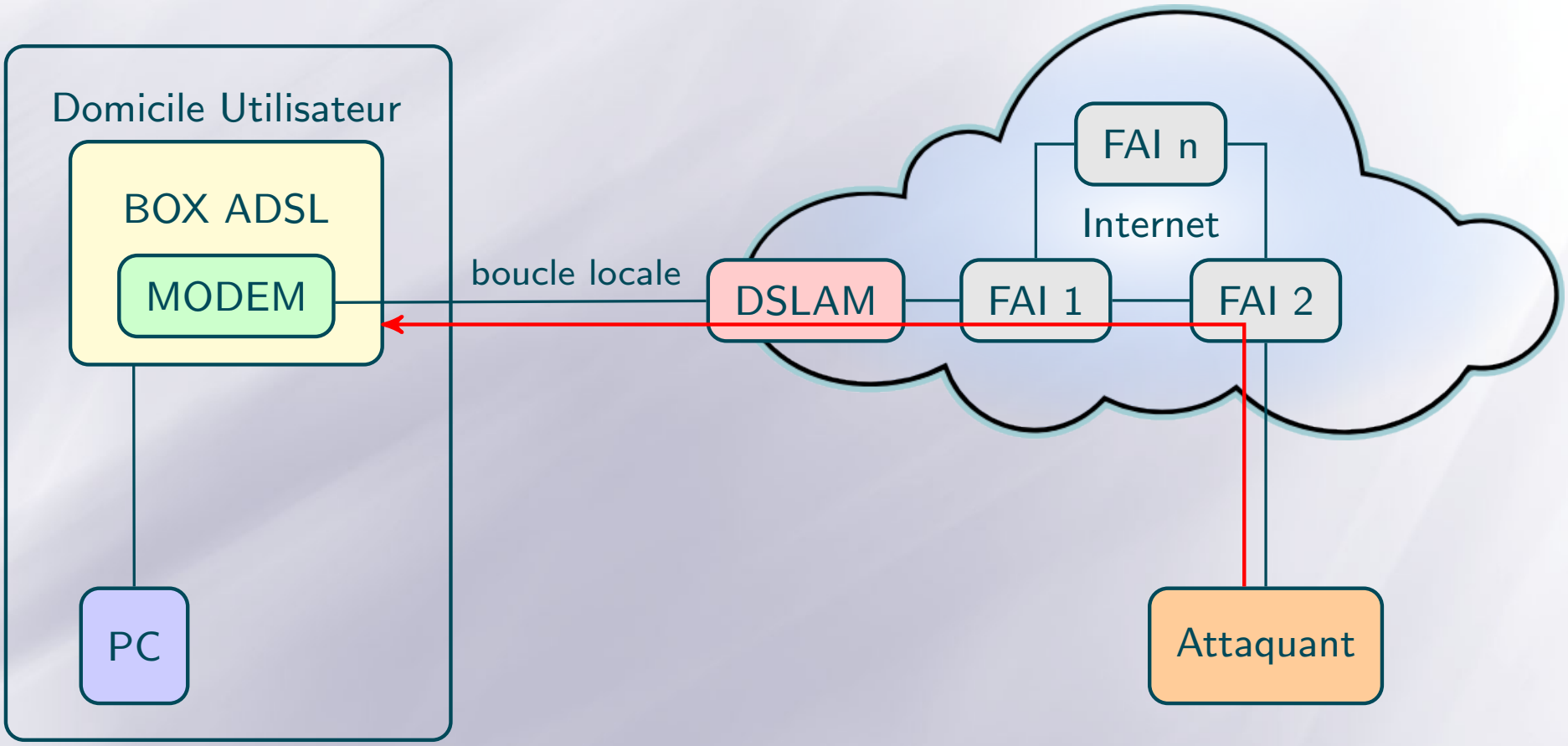
La BOX ADSL

- Introduction à la fin des années 90 d'offres Internet "triple play" proposant trois grands axes de services :
  - Web (NAT, DHCP, ...)
  - Télévision (PVR, Replay, ...)
  - Téléphonie (DECT, répondeur, 3G, ...)
- Développement d'équipements, nommés UAI (*Unité d'Accès Intégré*) ou BOX ADSL, permettant de profiter de ces services.
- De plus en plus de services rendant les box plus riches $\rightarrow$ augmentation de la surface d'attaque

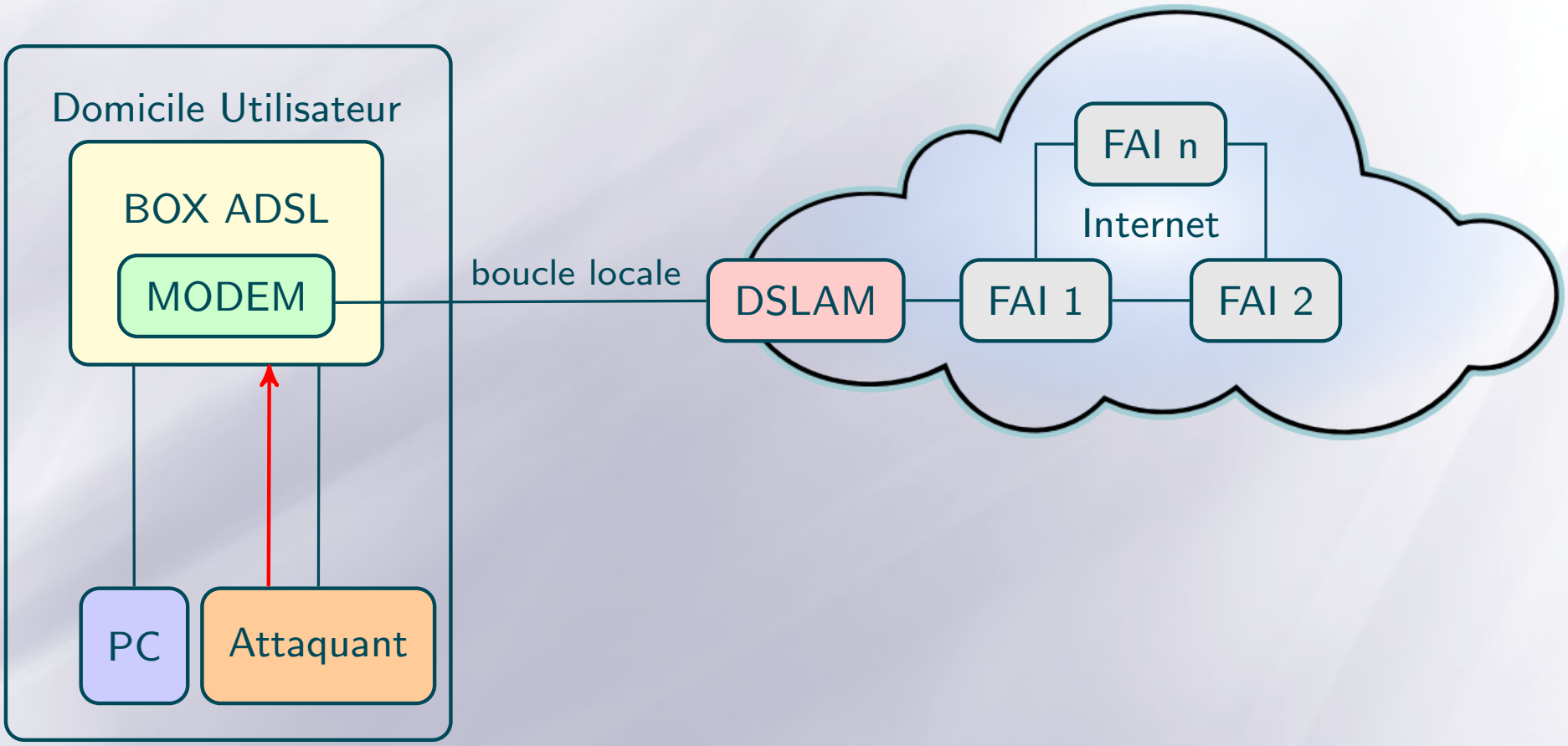
Architecture générale



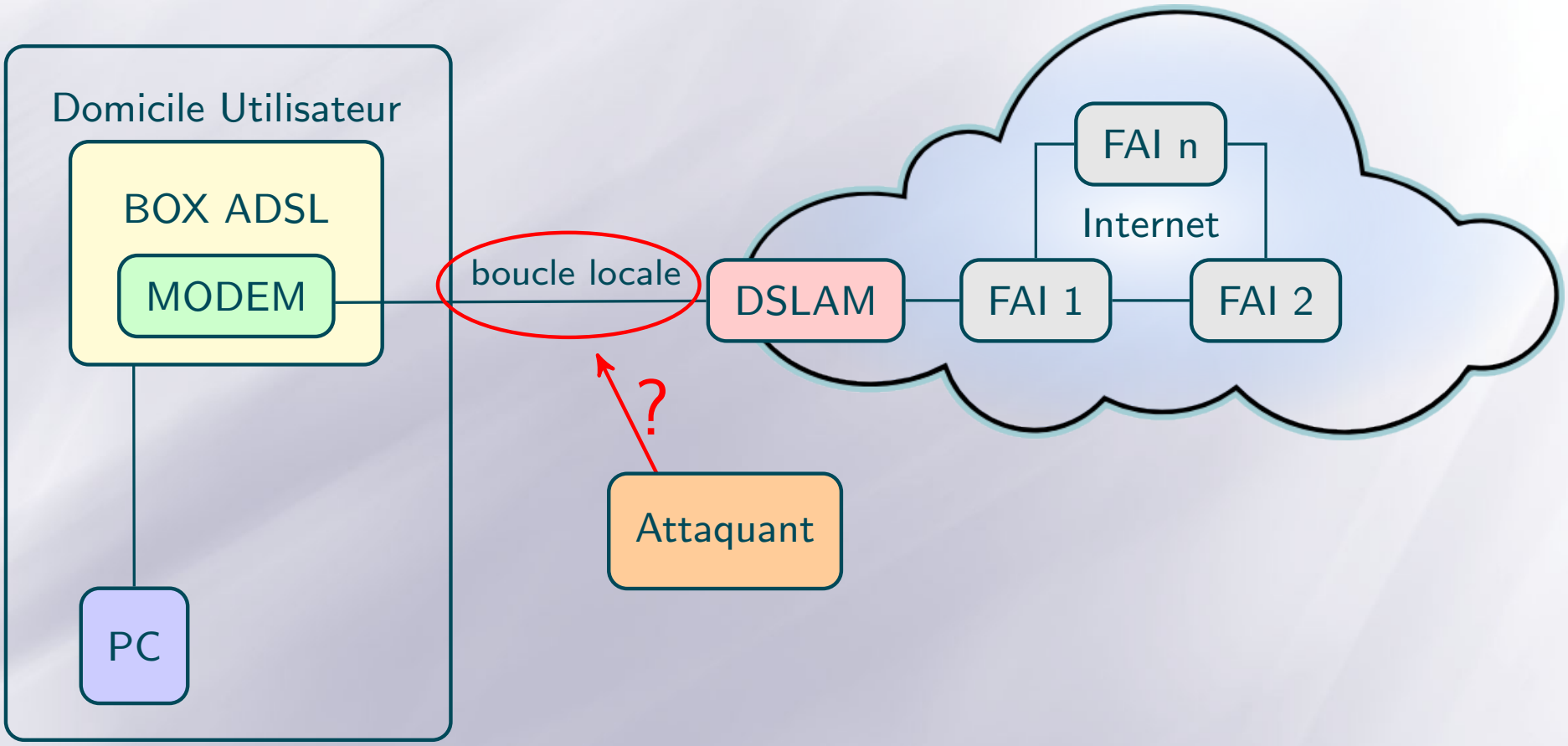
Chemins d'attaque connus (1/2)



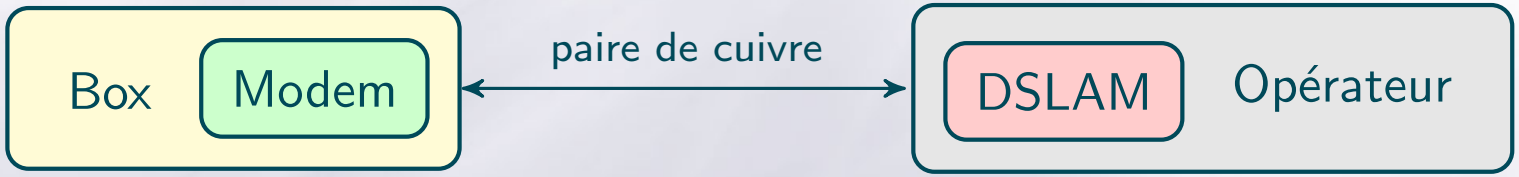
Chemins d'attaque connus (2/2)

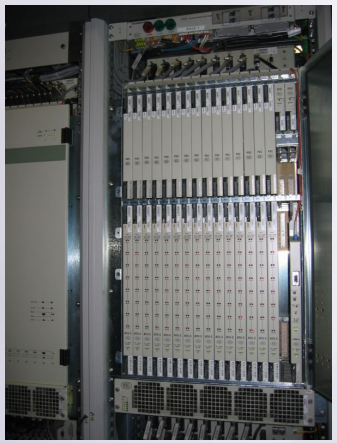


Nouveau chemin d'attaque

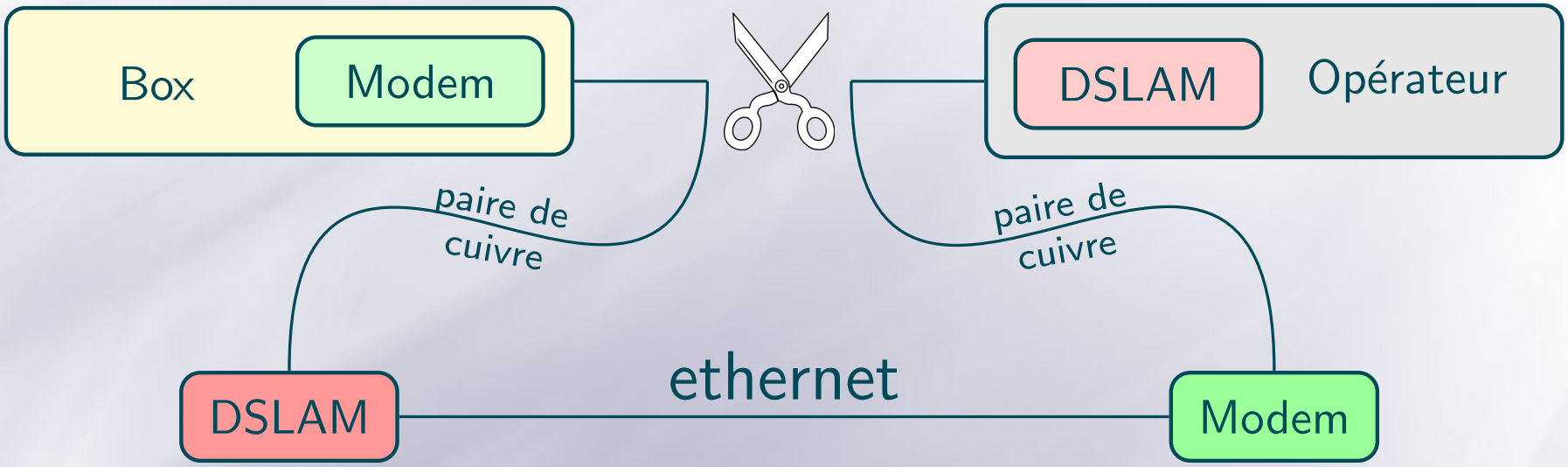


La boucle locale

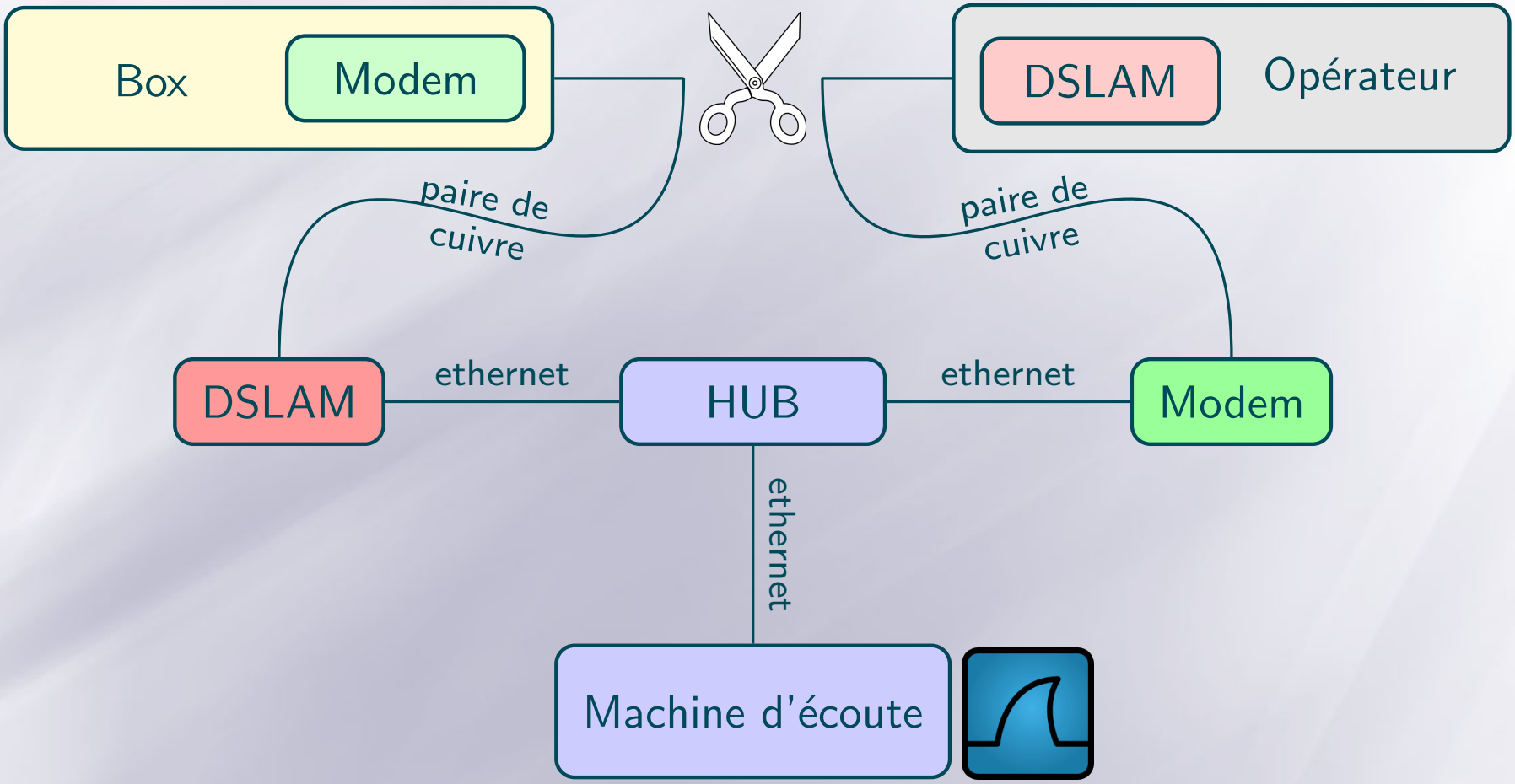




Observation des communications sur la boucle locale (1/2)



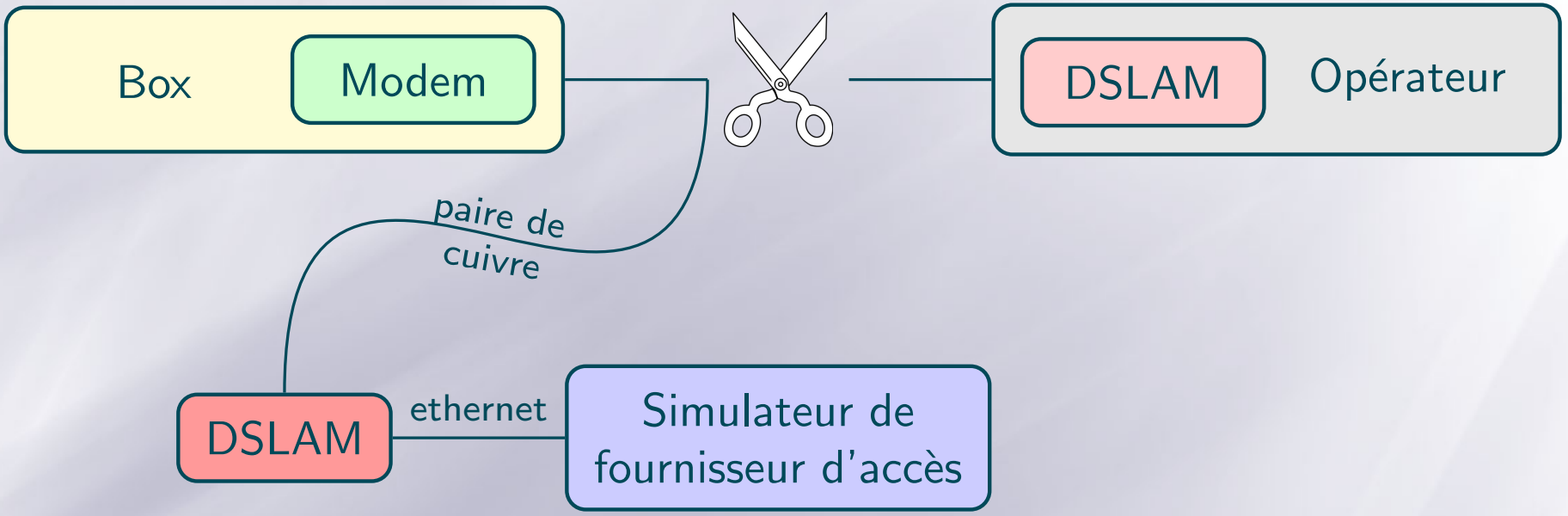
Observation des communications sur la boucle locale (2/2)



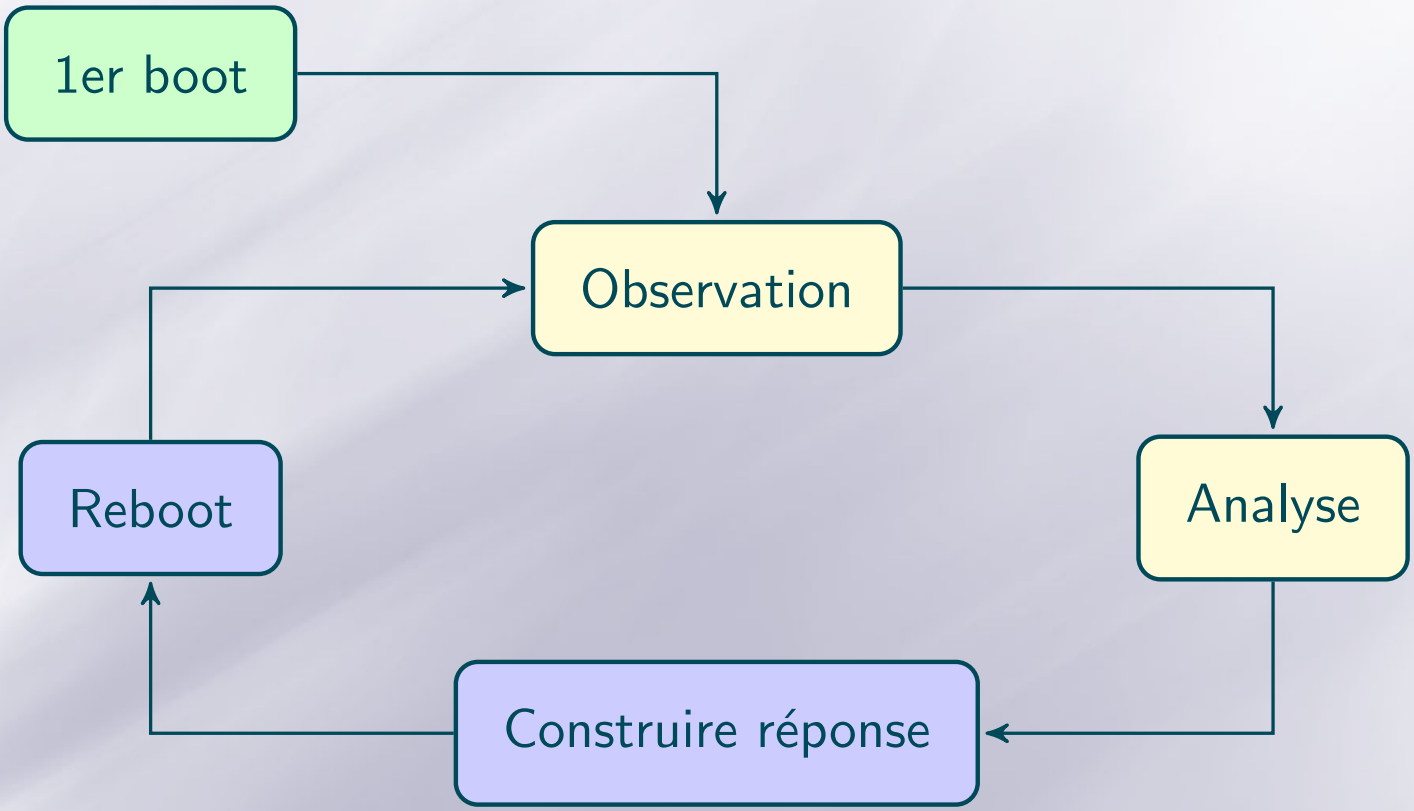
Comparaison de plusieurs BOX ADSL

BOX	ATM	PPP	DHCP	SIP	Configuration	Mise à jour
A	8/35/LLC	chap	no	MD5	HTTP, FTP, SSL	-
B	8/35/LLC	chap	yes	MD5	HTTP, SSL	SSL
C	8/36/VC	no	yes	MD5	SSL	-
D	8/35/LLC	chap	yes	MD5	HTTP	HTTP
E	8/35/LLC	chap	yes	MD5	HTTP	HTTP
F	8/35/LLC	chap	no	MD5	SSL	-

Interruption de la boucle locale



Méthode itérative



Itération 1/4

1er boot

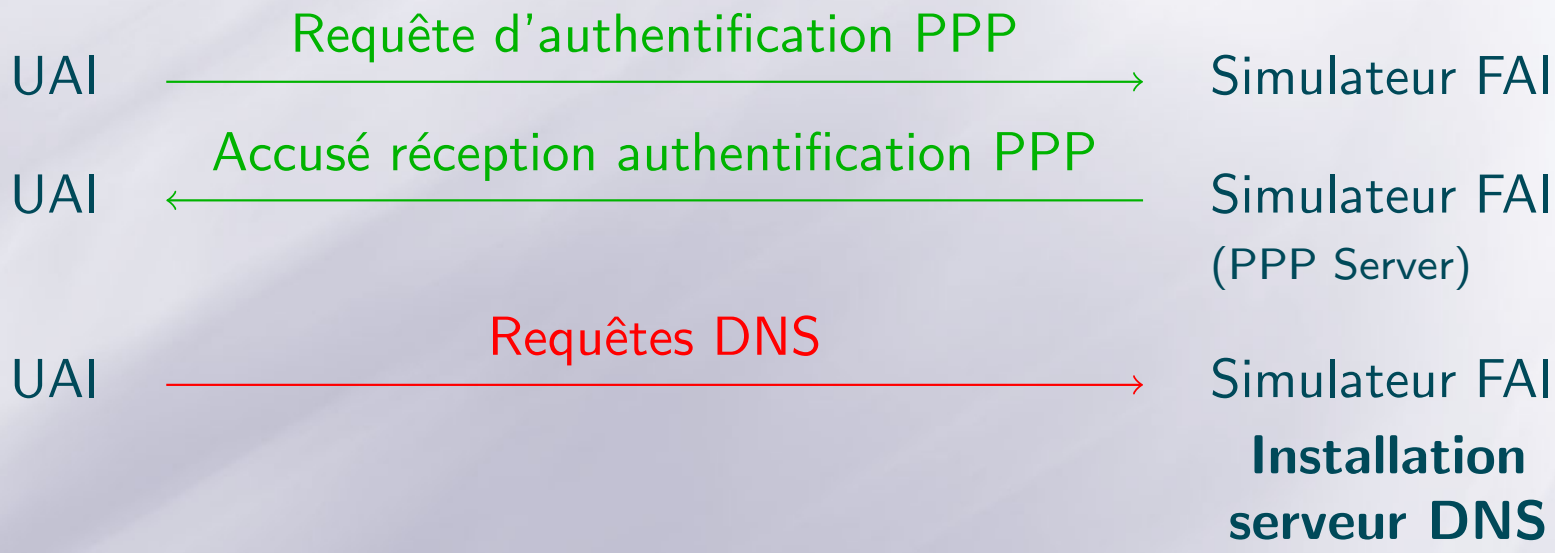
UAI —— Requête d'authentification PPP ——→ Simulateur FAI

Installation serveur PPP

Reboot

Itération 2/4

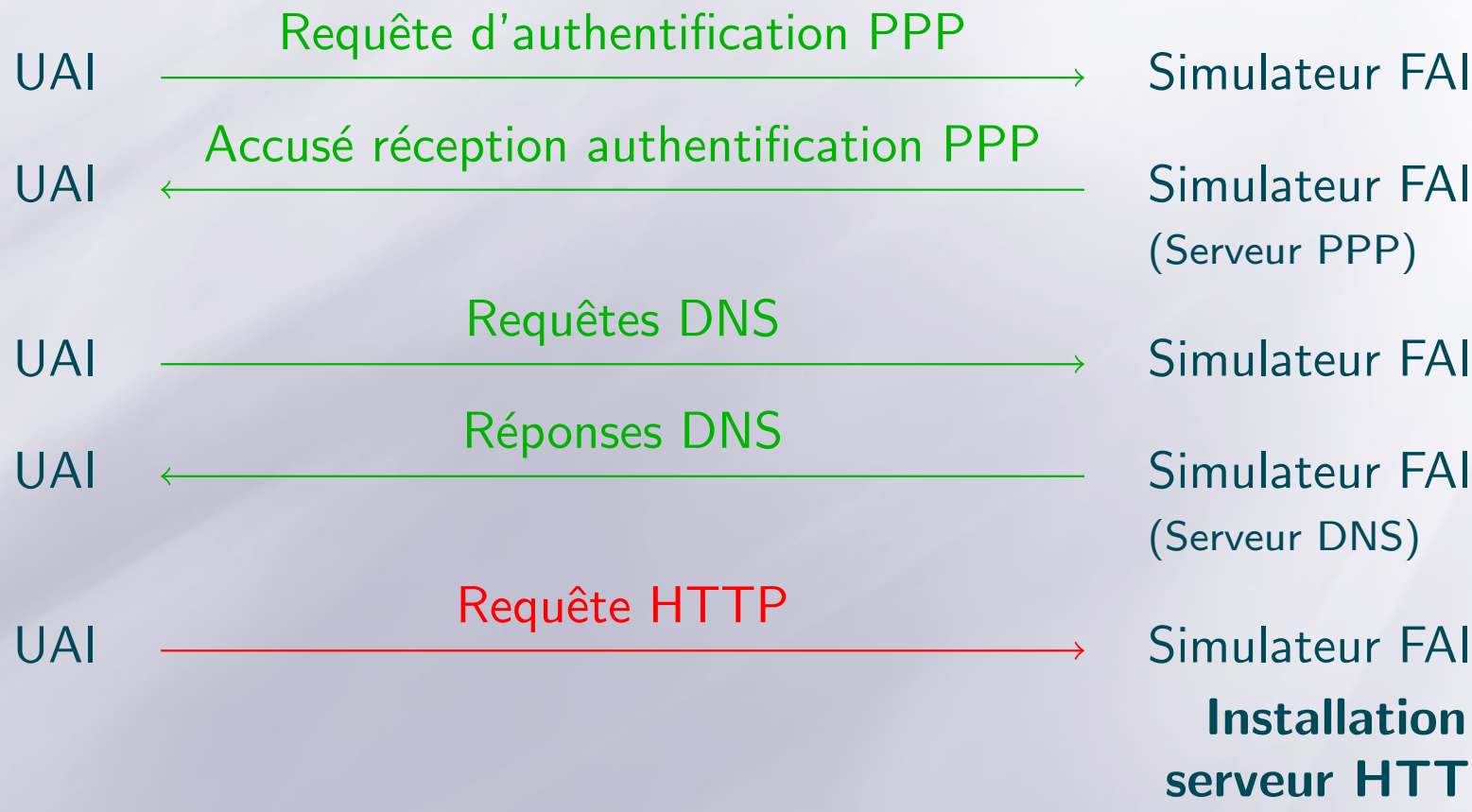
2nd boot



Reboot

Itération 3/4

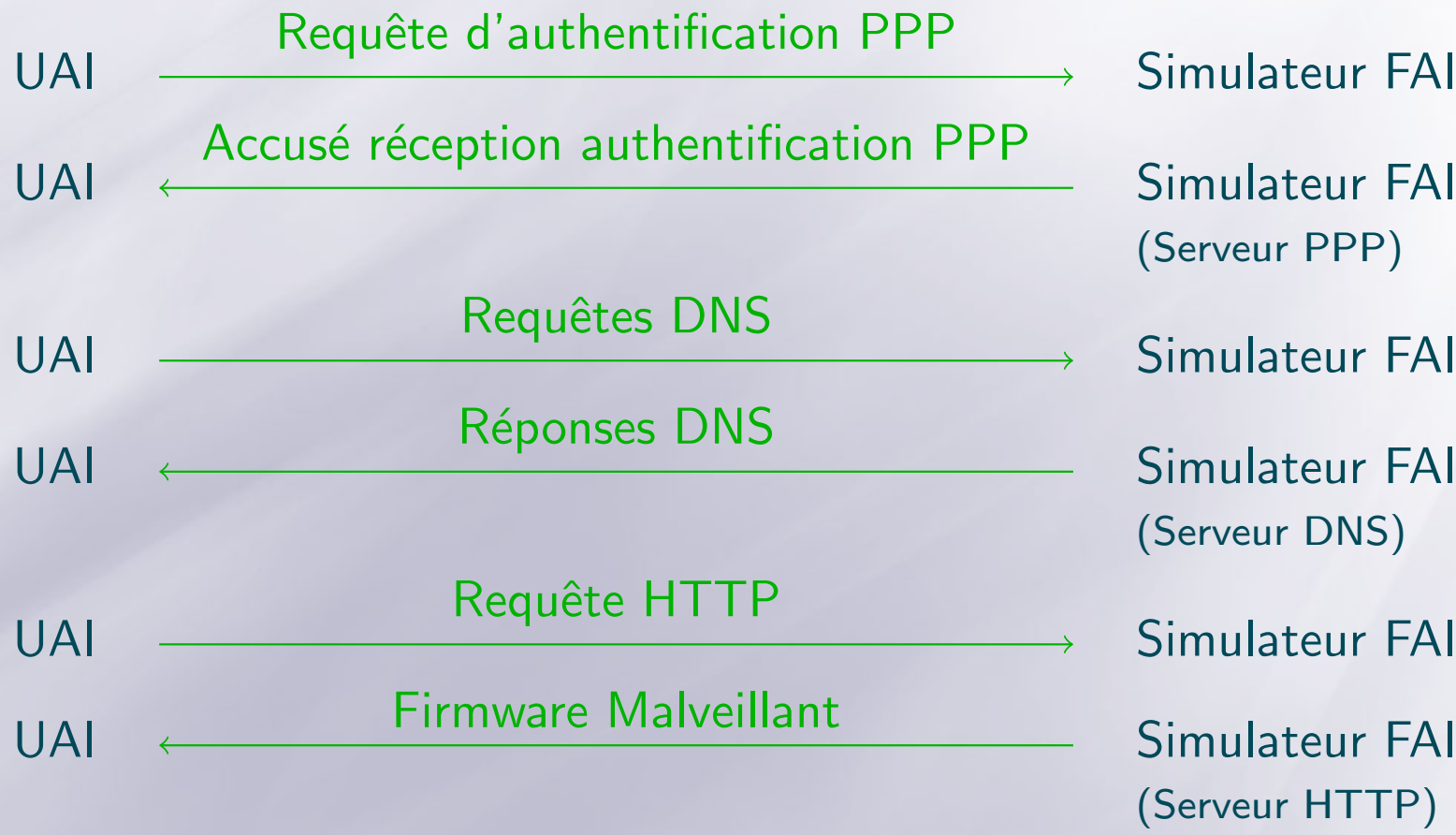
3ème Boot



Reboot

Itération 4/4

4ème Boot



Personnalisation du Firmware

Extraction du firmware

- Pas de signature du firmware
- Pas de chiffrement du firmware
- Compression LZMA

Modifications du firmware

- Désactivation (partielle) du pare-feu
- Ajout d'un compte super-utilisateur
- Désactivation des mises à jour
- Installation de logiciel "soft-phone"

Exploitations réalisées et envisagées

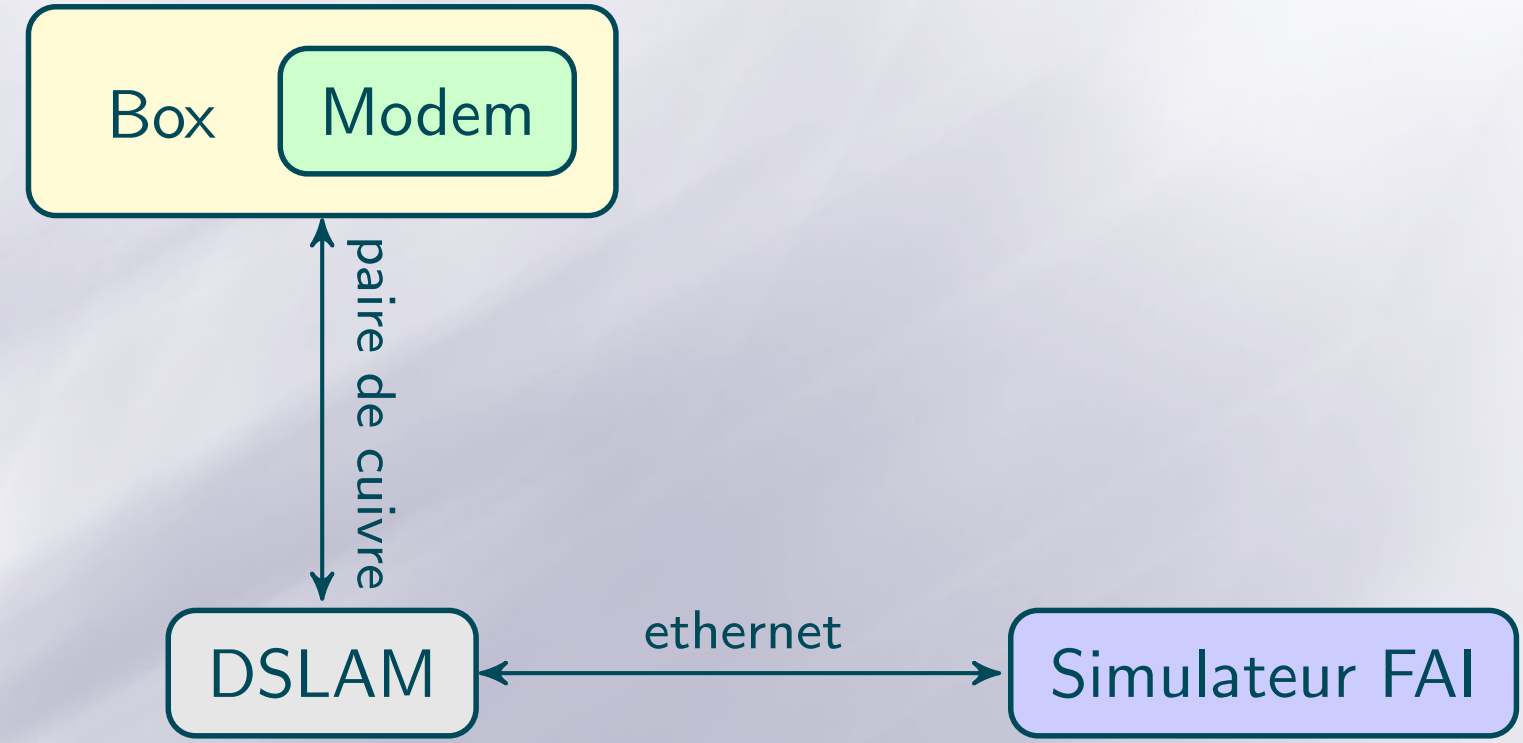
Exploitations réalisées

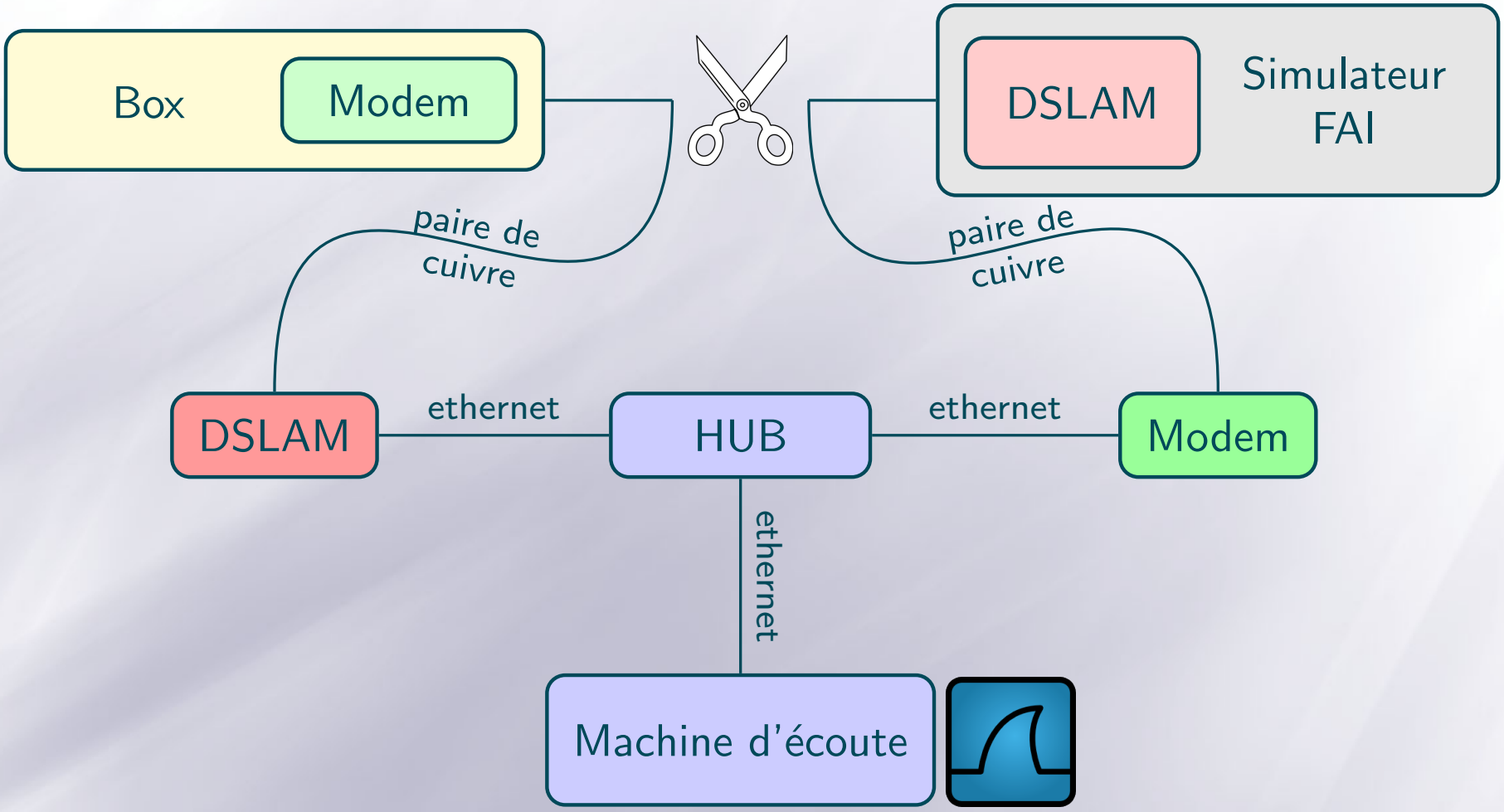
- Utilisation à distance de la box pour émettre des appels "surtaxés"
- Connexion à distance sur la box (via porte dérobée)

Autres exploitations envisagées

- Réalisation d'un botnet
- Attaques DDos
- Proxy
- Analyse du réseau local
- Attaques d'autres équipements connectés sur le réseau local

Simulation FAI




Box
Modem
DSLAM
Simulateur FAI
paire de cuivre
paire de cuivre
DSLAM
ethernet
HUB
ethernet
Modem
ethernet
Machine d'écoute

Contre-mesures

Contre-mesures

- Nécessité de généraliser les méthodes cryptographiques pour les communications sensibles → techniquement simple et peu onéreux
- Nécessité de signer le firmware
- Possibilité d'observer la variation du temps aller retour du signal sur la paire de cuivre

Conclusion

Principale conclusion

- Mise en évidence d'un nouveau chemin d'attaque des BOX ADSL

Contributions

- Une plateforme d'observation des communications ADSL
- Une plateforme de simulation d'un fournisseur d'accès

Perspectives

Perspectives

- Utilisation de cette plateforme afin d'analyser d'autres équipements connectés utilisant le lien internet comme lien privilégié avec leur fournisseur de contenu.
- Application de cette méthode à une autre type de boucle locale, la TNT.


... SINON POUR PROTÉGER VOS DONNÉES SUR INTERNET, JE VOUS CONSEILLE CETTE BOX !
WINGZ