Sécurité des réseaux domestiques Optimaux les grands remèdes ?

N. Prigent — THOMSON / Supélec
C. Bidan — Supélec
O. Heen — THOMSON
A. Durand — THOMSON

Supélec

TECHNICOLOR. grass valley RCA THOMSON

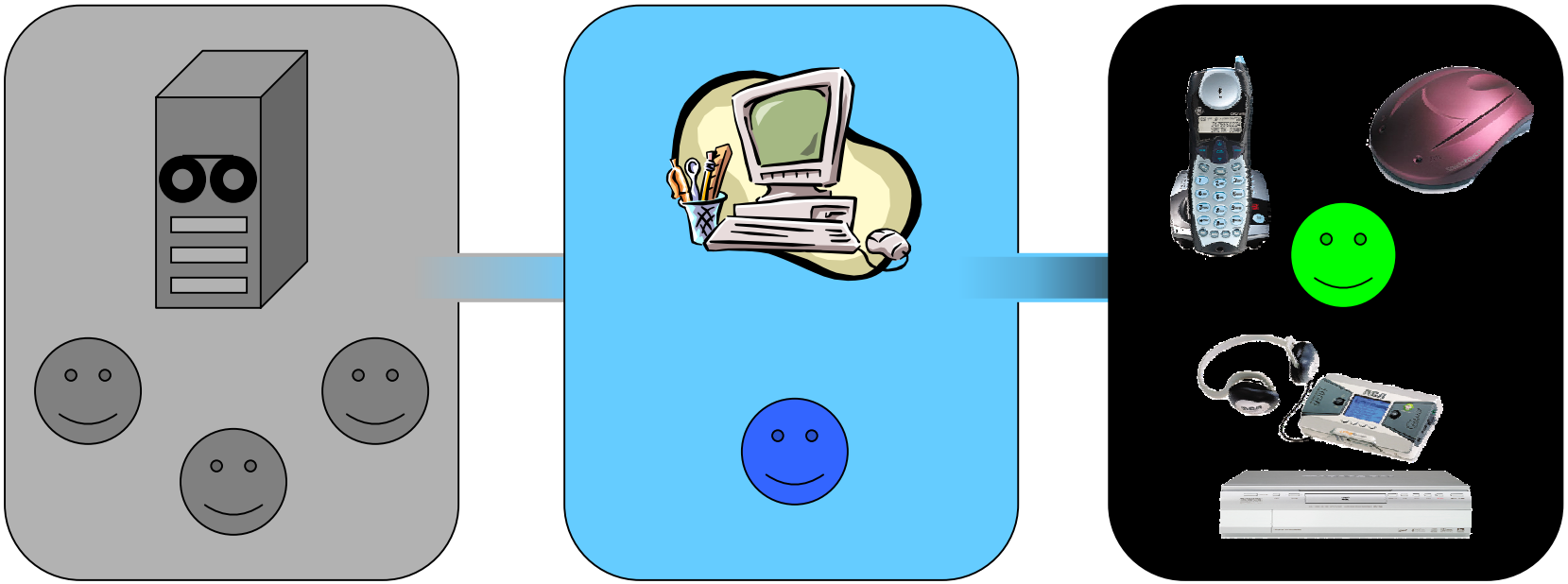
- Les réseaux domestiques
- Les menaces
- Le problème de la frontière
- Vers des réseaux domestiques sécurisés

TECHNICOLOR grass valley RCA THOMSON

- Les réseaux domestiques
- Les menaces
- Le problème de la frontière
- Vers des réseaux domestiques sécurisés

TECHNICOLOR grass valley RCA THOMSON

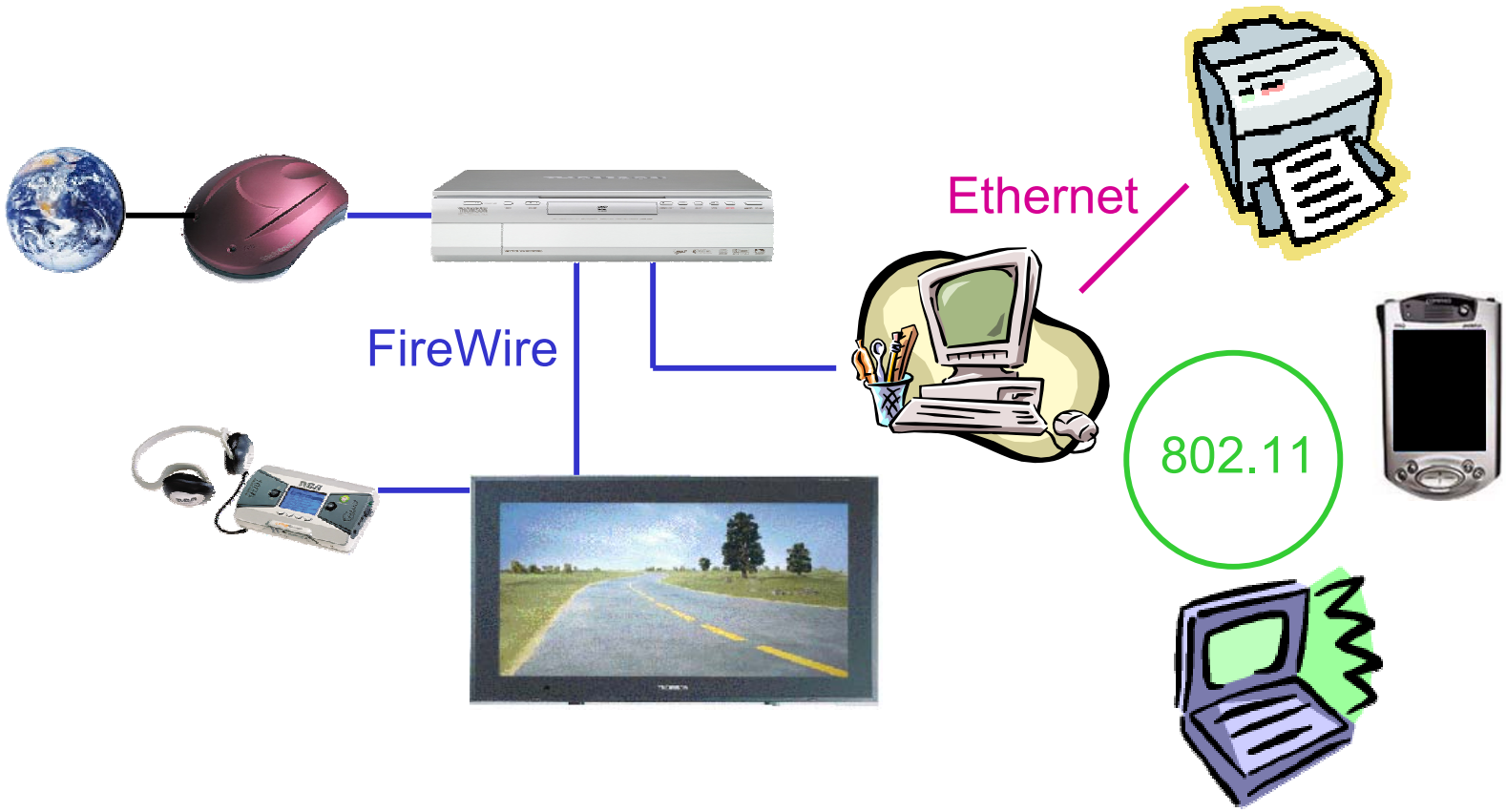
Ubiquitous Computing



Les réseaux domestiques

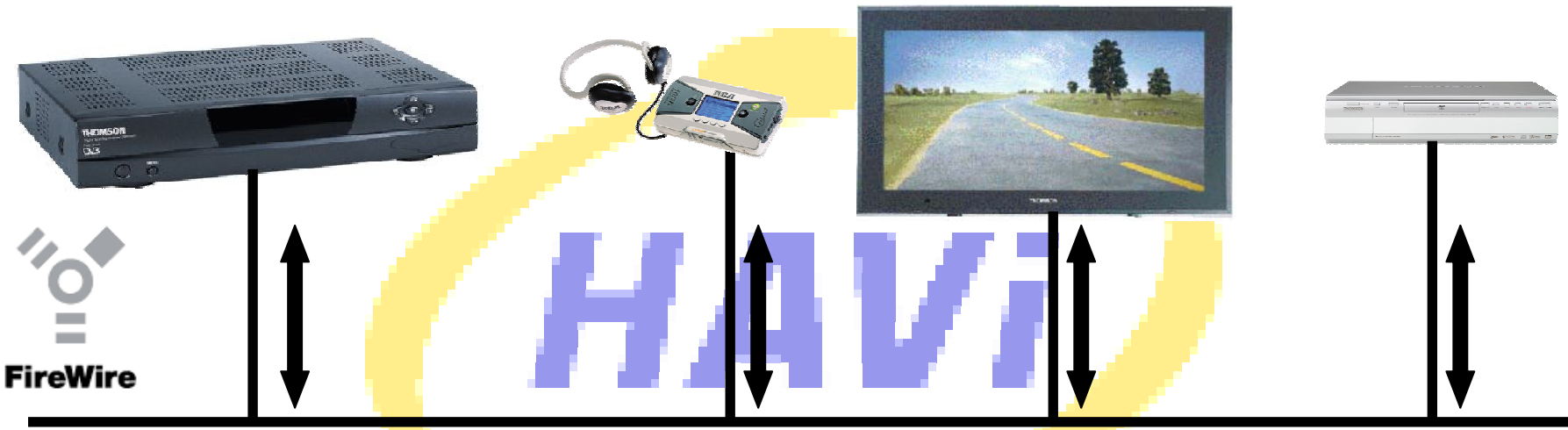
- *Ubiquitous Computing* appliquée au domicile
- Automatisation des configurations
- Usage transparent des technologies

Les réseaux domestiques



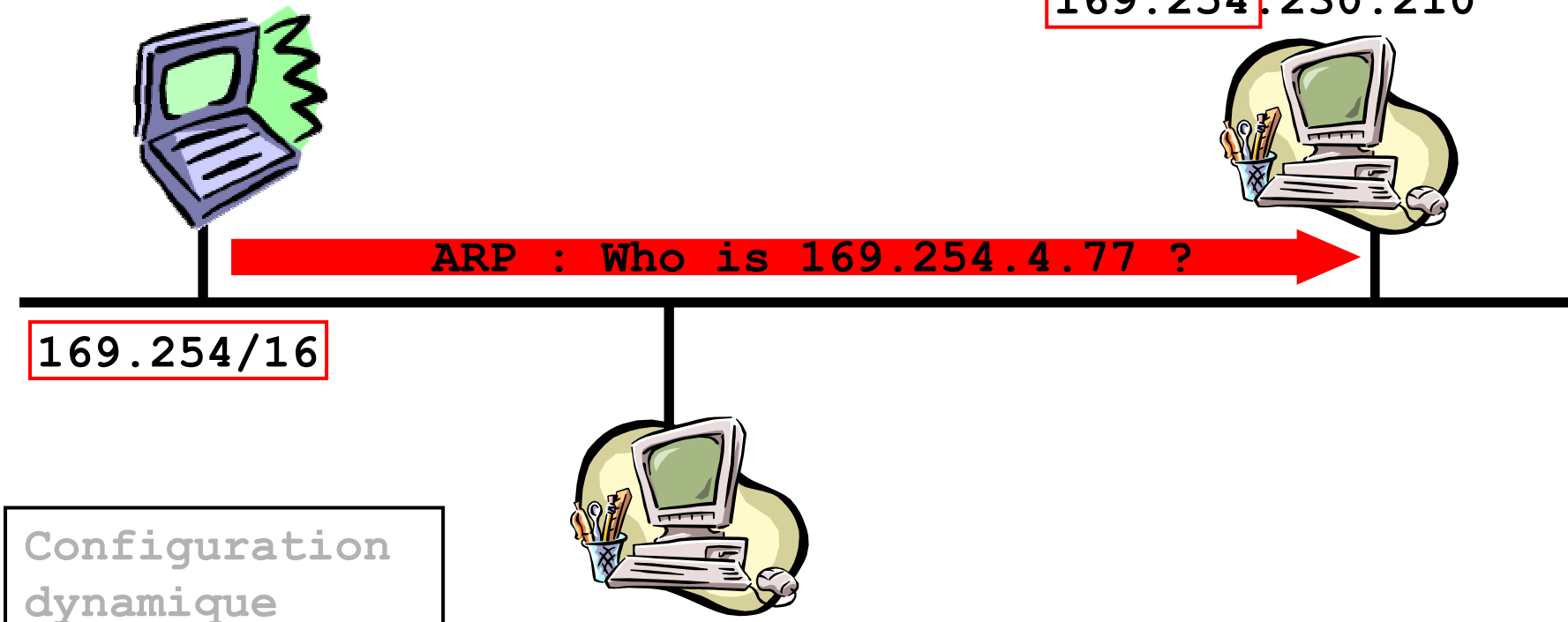
HAVi : configuration réseau

HAVi : déclaration des services



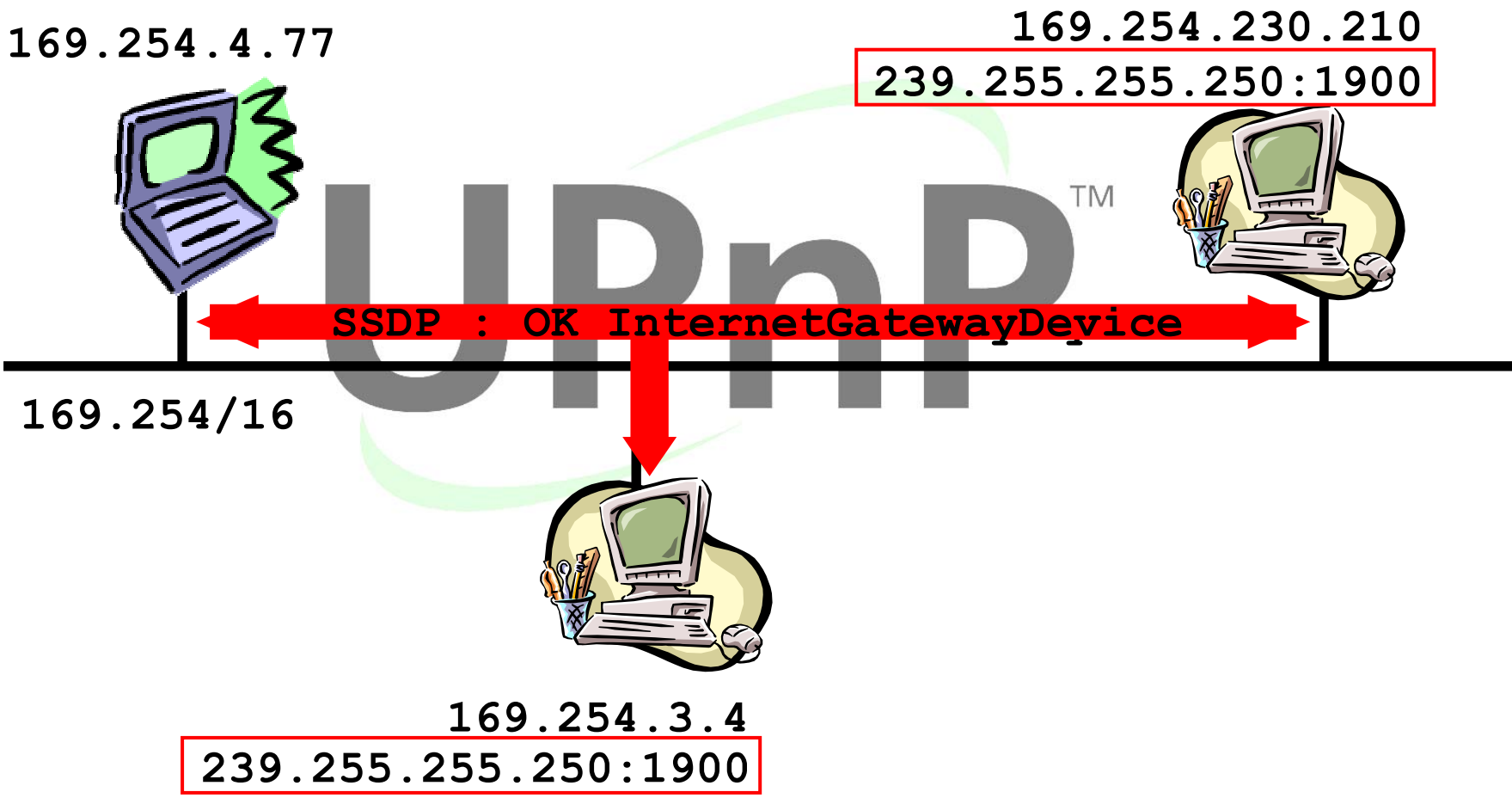
HAVi : accès aux services

UPnP Acquisition d'une adresse IP



Configuration dynamique d'adresse IPv4 locale au lien

Recherche des services



Hétérogénéité

- Puissances de calcul hétérogènes
- Capacités de stockage hétérogènes
- Canaux de communications hétérogènes

Dynamicité

- Évolution non-rationnelle du réseau
- Interconnexion erratique des dispositifs
- Évolution parallèle des sous-réseaux

Inexpérience des utilisateurs

- Pas d'administrateur local
- Utilisateurs non-formés
- Utilisateurs passifs

- Les réseaux domestiques
- Les menaces
- Le problème de la frontière
- Vers des réseaux domestiques sécurisés

TECHNICOLOR grass valley RCA THOMSON

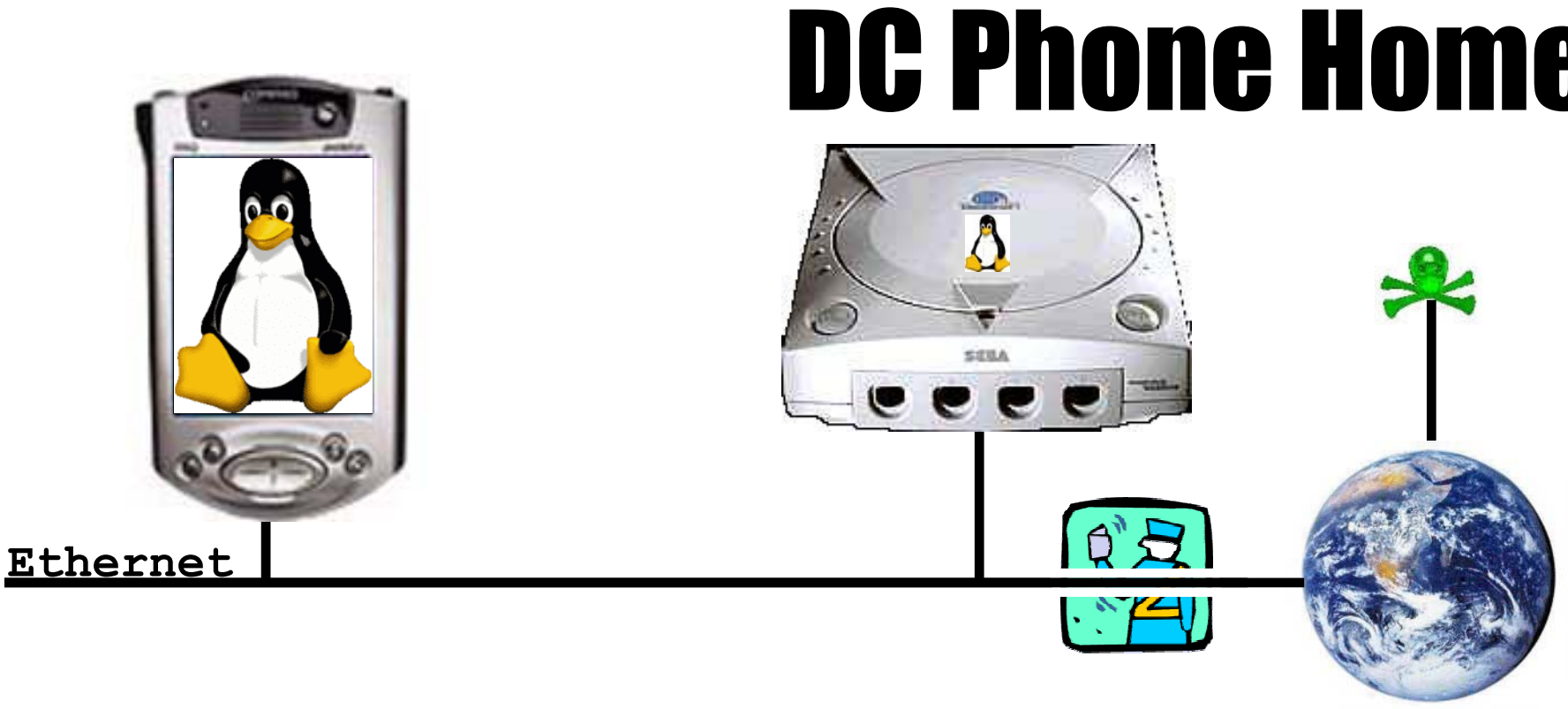
Mobiles d'attaques

- Jeu, vandalisme
- Atteinte à la vie privée
- Vol de ressources
- Rebond, utilisation pour un *DDoS*

Opportunités d'attaques (1/2)
Attaques traditionnelles

KISMET

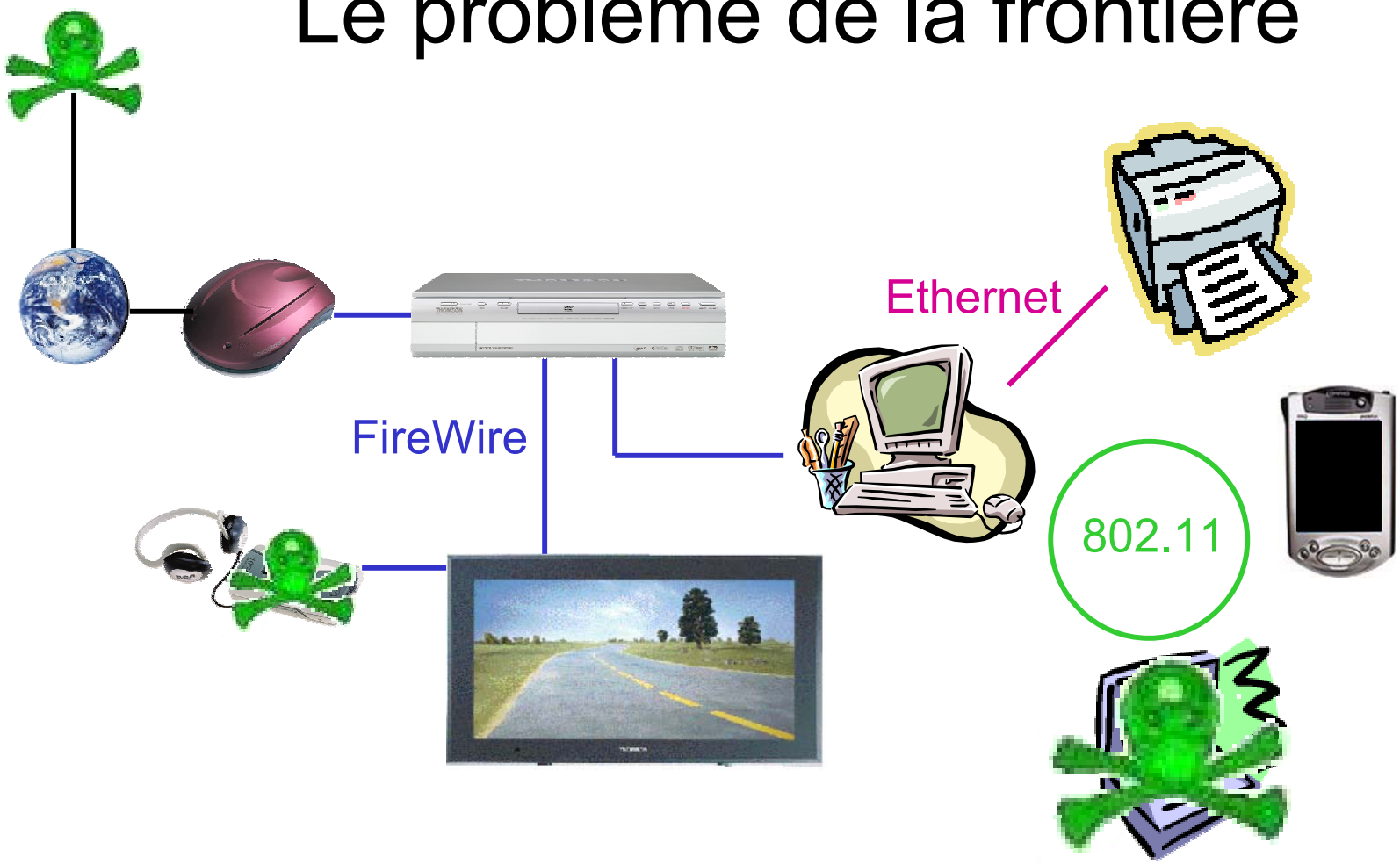
Opportunités d'attaques (2/2)
Nouvelles attaques



- Les réseaux domestiques
- Les menaces
- Le problème de la frontière
- Vers des réseaux domestiques sécurisés

TECHNICOLOR grass valley RCA THOMSON

Le problème de la frontière



Frontière

- Démarcation entre les dispositifs d'un réseau domestique donné et les autres

Services de Sécurité

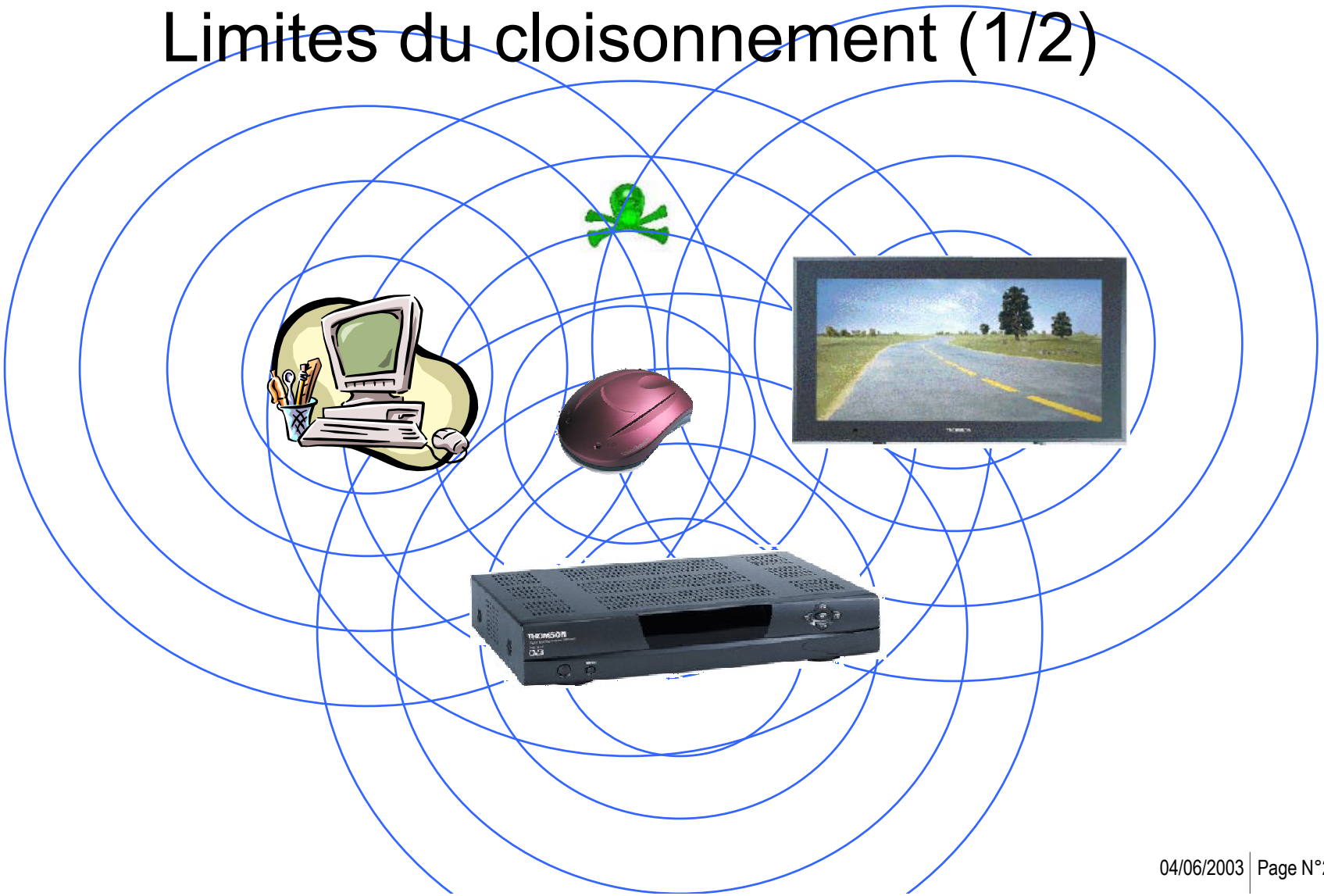
- Authentification des dispositifs
- Confidentialité des communications
- Authenticité des communications

Propriétés De La Frontière

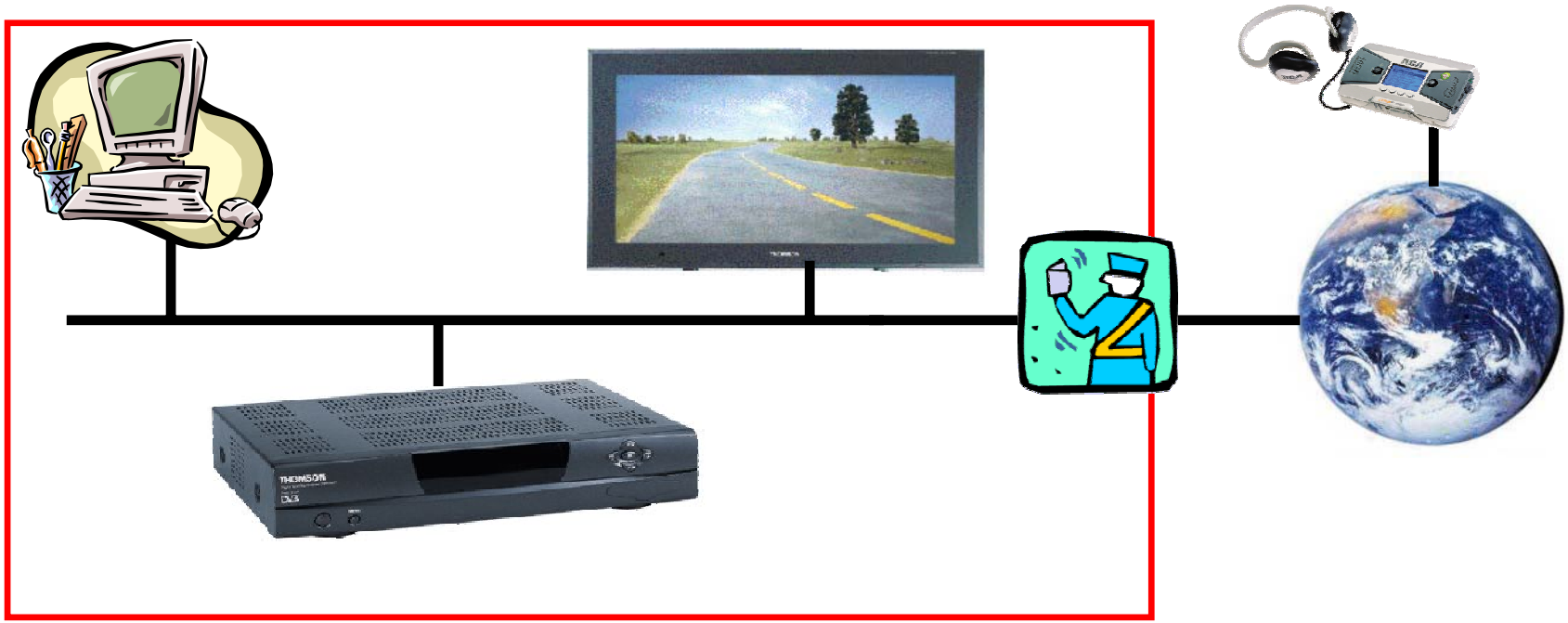
- Non-ambiguë
- Évolutive
- Robuste au fractionnement

Cloisonnement

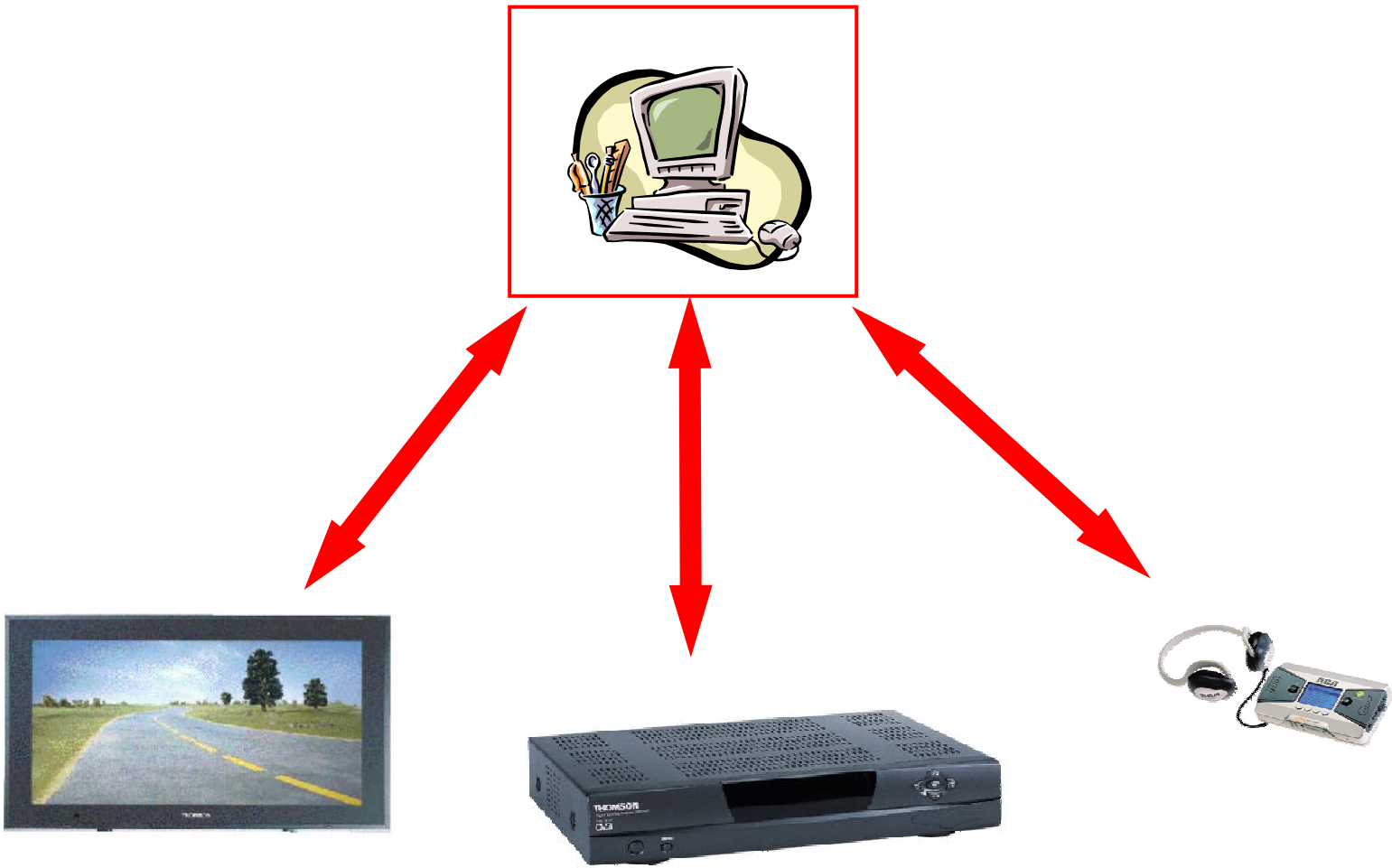
Limites du cloisonnement (1/2)



Limites du cloisonnement (2/2)

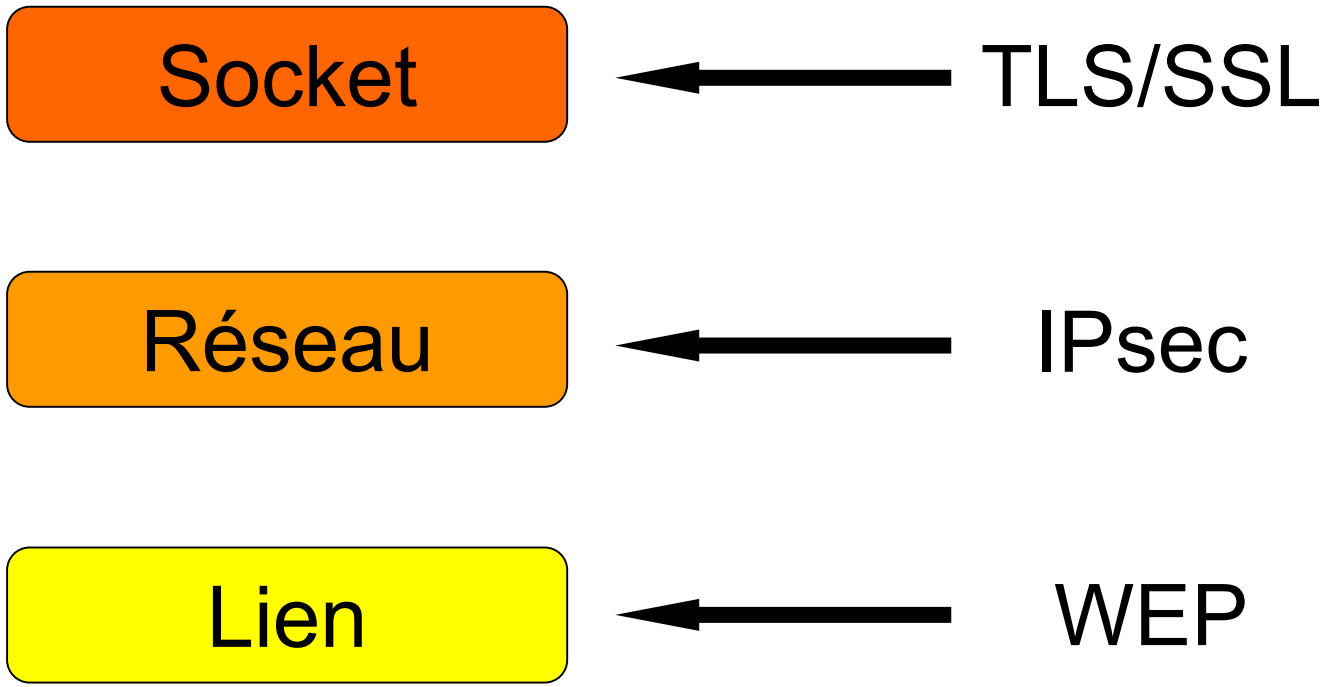


Solutions centralisées



Limites des solutions centralisées

Réseaux Privés Virtuels



Limites des Réseaux Privés Virtuels

- Mise en œuvre relativement complexe
- Mesures rarement activées
- Sécurité très dépendante de l'utilisateur

- Les réseaux domestiques
- Les menaces
- Le problème de la frontière
- Vers des réseaux domestiques sécurisés

TECHNICOLOR grass valley RCA THOMSON

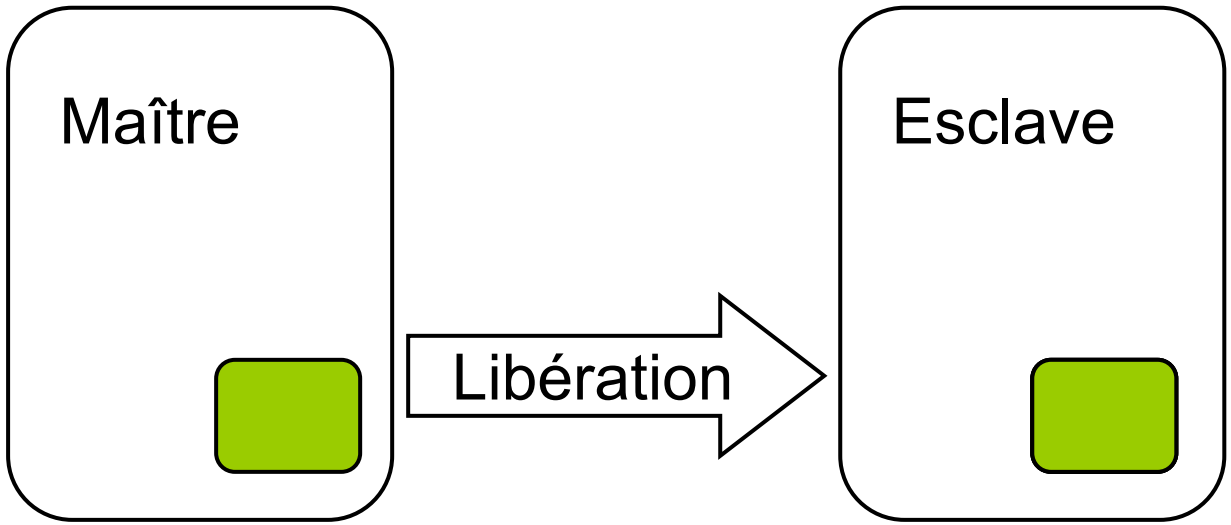
Réseaux domestiques sécurisés

- Sécurité activée par défaut
- Sécurité auto-configurée au maximum
- Utilisateur restreint à la tâche d'autorité

Bluetooth : gestionnaire de sécurité

- Contrôle d'accès au dispositif
- Chiffrement des communications
- Mémorisation des opérations réalisées

Le *Resurrecting Duckling*



Extensions du *Resurrecting Duckling*

- Passage de politiques lors du marquage
- Diminution des exigences sur le canal
- Sécurisation des réseaux spontanés

Conclusion

- Réseaux domestiques vulnérables
- Nécessité de démarcation simple de la frontière
- Solutions traditionnelles non-adaptées
- Nouvelles propositions à améliorer

Références

- [WeCT] Mark Weiser, *The Computer For The 21st Century*
- [DHDC] Chris Davis, Aaron Higbee, *DC Phone Home*
- [SARD] Frank Stajano, Ross Anderson, *The Resurrecting Duckling, Security Issues for Ad-Hoc Wireless Networks*
- [StWN] Frank Stajano, *The Resurrecting Duckling – What Next*
- [BaTS] D. Balfanz, D. K. Smetters, P. Stewart, H. Chi Wong, *Talking to Strangers: Authentication in Ad Hoc Wireless Networks*
- [FeSN] Laura Marie Feeney, Bengt Ahlgren, Assar Westerlund, *Spontaneous Networking: An Application-oriented Approach to Ad Hoc Networking*