Sécurité des réseaux sans fil

Matthieu Herrb
CNRS-LAAS
matthieu.herrb@laas.fr

Septembre 2003

Plan

- La technologie sans fils
- Faiblesses et Attaques
- Architecture
- Sécurisation des postes clients
- Sécurisation des points d'accès
- Authentification des clients
- Sécurisation des échanges

Introduction au Wifi

Wireless **Fi**delity.

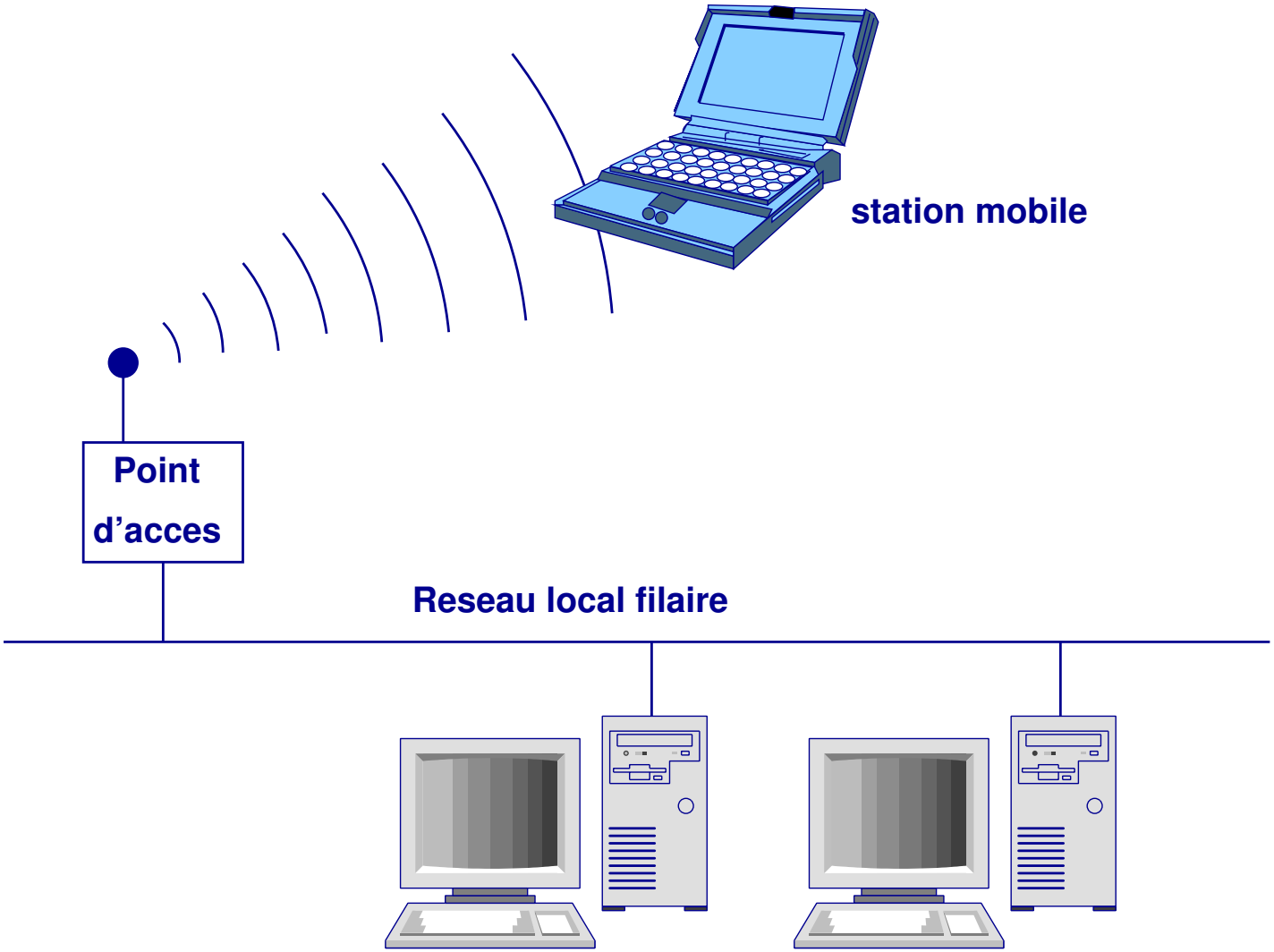
Nouvelles familles de technologies pour la couche physique.

Utilisent les ondes radio pour transporter le signal.

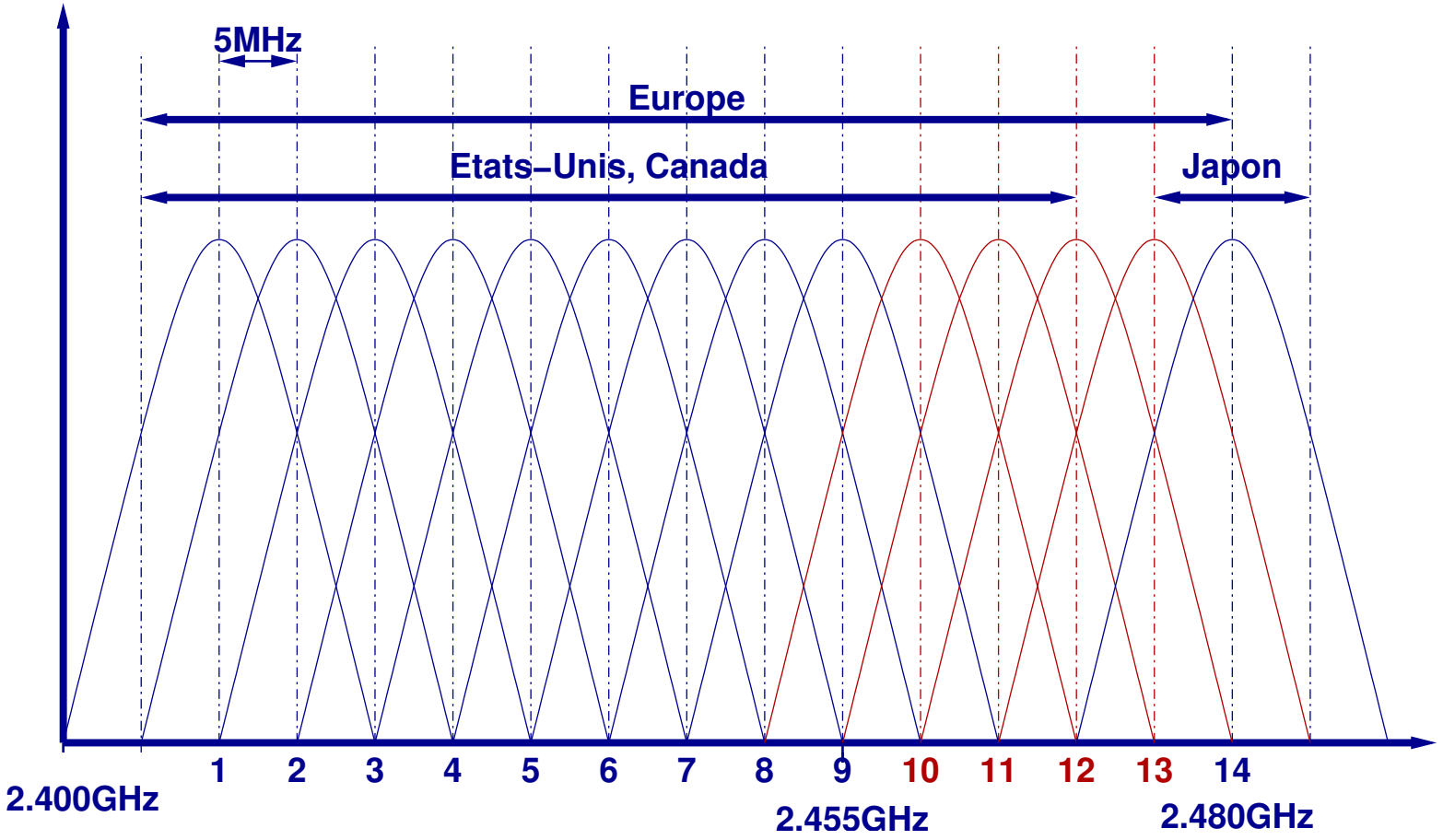
Nom	Débit Max.	Fréq.	Modulation	Remarques
IEEE802.11	2Mb/s	2.4 GHz	FH	
IEEE802.11b	11Mb/s	2.4GHz	DSSS	
IEEE802.11g	54Mb/s	2.4GHz	OFDM	
IEEE802.11a	54Mb/s	5GHz	OFDM	Interdit en Europe
HomeRF	2Mb/s	?	?	Utilise le DECT
HyperLAN	54Mb/s	5GHz	OFDM	Standard Européen
Bluetooth (IEEE802.15)	1Mb/s	2.4GHz	?	Pas IP

Technique d'accès : CSMA/CA (Collision Avoidance)

Principe d'un réseau Wifi



IEEE802.11b : canaux



En France : réglementation mise à jour en juillet 2003 :
http://www.art-telecom.fr/communiques/communiques/2003/index-c220703.htm
http://www.art-telecom.fr/dossiers/rlan/puissances-2-4.htm

IEEE802.11b : BSS

Basic **S**ervice **S**et

Un ensemble de points d'accès et les stations mobiles associées.

SSID : identificateur de réseau - chaîne de caractères.

Pour joindre un réseau Wifi, une station doit connaître le BSSID du réseau.

Facile : il peut être broadcasté périodiquement par les points d'accès.

$\longrightarrow$ il suffit d'écouter pour découvrir les réseaux disponibles.

War Driving : cartographie des réseaux Wifi accessibles. (Avec un portable et un GPS).

http://www.stumbler.net/index.php?cat=5
http://www.dachb0den.com/projects/dstumbler.html

Un point d'accès se comporte comme un **HUB** $\longrightarrow$ écoute du trafic possible.

WEP

Wired **E**quivalent **P**rivacy.

Mécanisme de chiffrement du contenu des paquets Wifi.
Algorithme à clé secrète : RC4 (40 ou 128 bits).

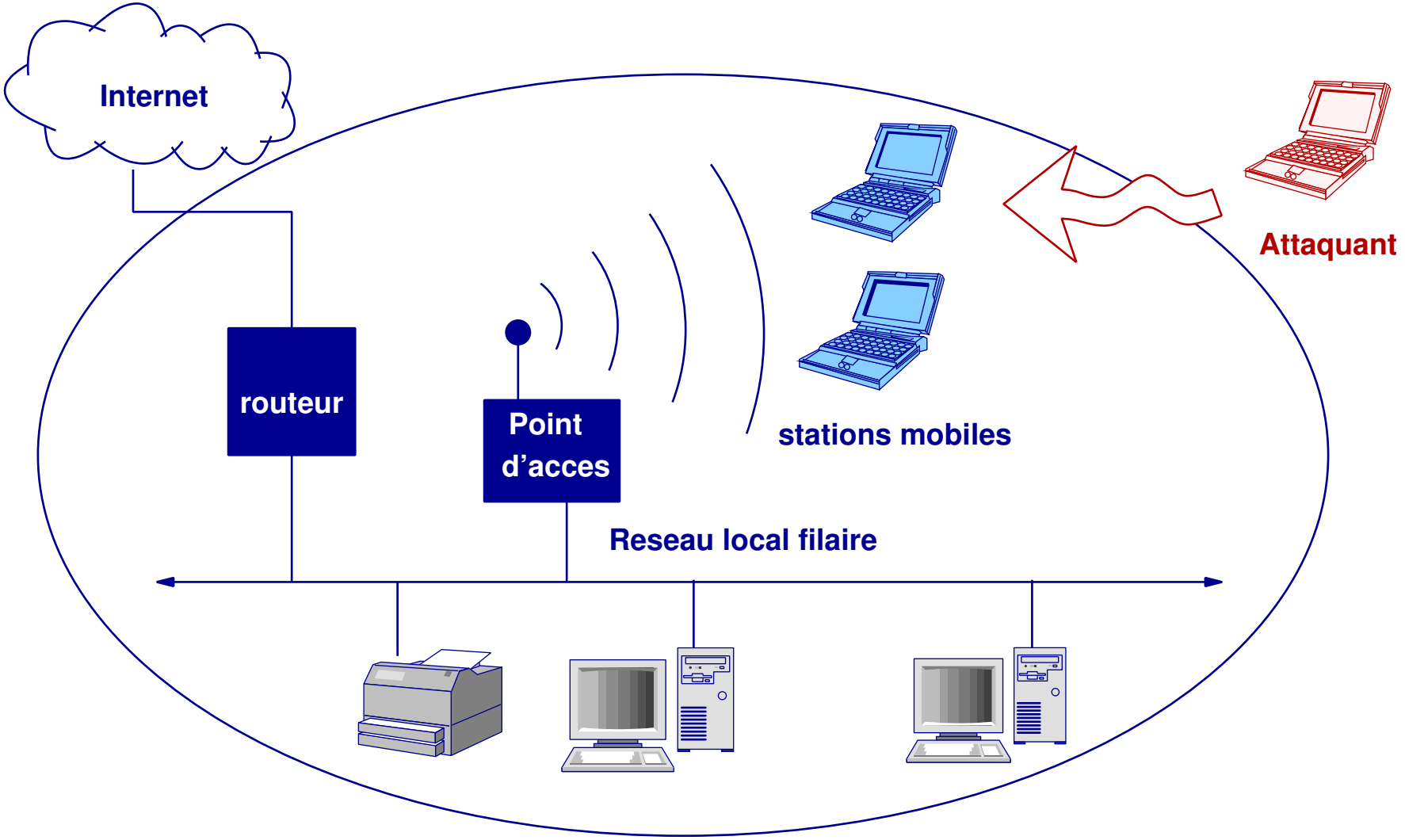
Principe : un mot de passe est positionné sur les points d'accès et les stations mobiles.
Sans le mot de passe, pas de communication.

Problèmes :

- interopérabilité difficile entre implémentations de Web (correspondance mot de passe / clé, longueur des clés).
- gestion des clés : comment diffuser la clé WEP à tous les utilisateurs / visiteurs. Comment la changer périodiquement sur plusieurs points d'accès et plusieurs stations ?
- faiblesses dans l'implémentation : crackage de la clé possible en quelques minutes avec suffisamment de paquets capturés.

http://www.dachb0den.com/projects/bsd-airtools.html

Attaques et risques (1/2)

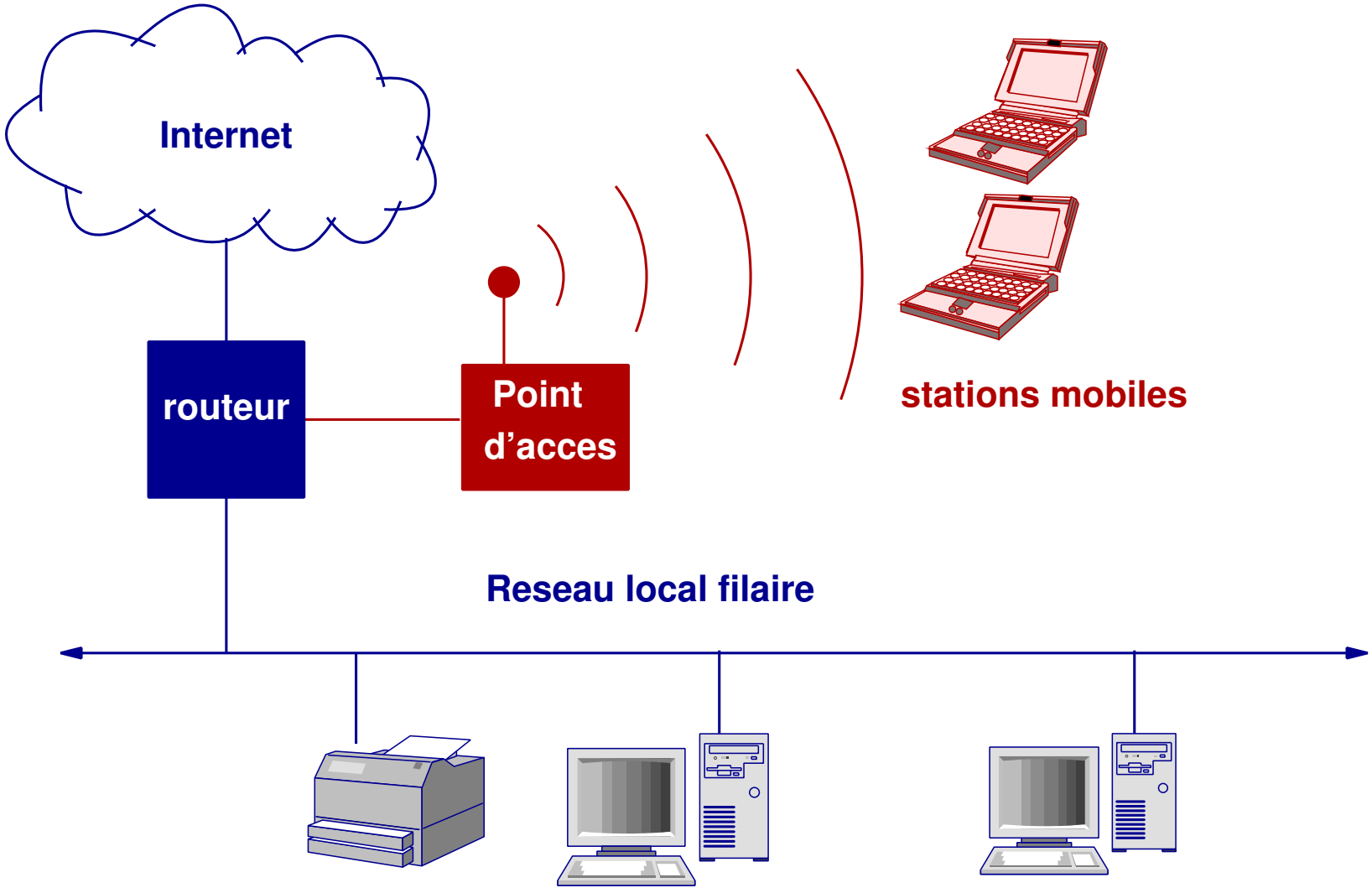


Attaques et risques (2/2)

Point d'accès Wifi : énorme prise RJ 45 de 50m de diamètre.
- déborde du périmètre de sécurité physique
- en libre-service

Attaques :
- **Dénis de service**
  - bande passante partagée et limitée
  - débit utile limité par la station la plus faible
  - point(s) d'accès parasite(s)
- **Interception du trafic**
  média partagé $\longrightarrow$ attaque facile.
  - sniffer passif
  - arp poisoning
- **Utilisation non autorisée**
  - Voir war-driving ci-dessus,...
  - installation de bornes non autorisées : renforcent l'impact des problèmes ci-dessus.

Sécurisation : architecture



Sécurisation des postes sans fil

Buts :

- empêcher les accès non autorisés
- sécuriser les connexions

Moyens :

- outils pour la sécurité locale : mises à jour, anti-virus, configuration rigoureuse, filtre de paquets, etc.
- protocoles de transport sécurisés : SSH, SSL, IPsec

Si le mobile ne change jamais de réseau :

- fixer le SSID (éviter l'utilisation de 'ANY')
- utiliser une entrée statique dans la table ARP pour le routeur

Sécurité des points d'accès

Restreindre l'accès aux interfaces d'administration :
- autoriser l'administration uniquement depuis le réseau filaire
- positionner un mot de passe d'administration
- restreindre les accès SNMP

Activer les logs :
- utiliser la possibilité d'envoyer les logs vers un syslog extérieur
- utiliser les trap SNMP
- surveiller les connexions - repérer les connexions non autorisées

Autres (pas très efficace mais augmente un peu la sécurité malgré tout) :
- activer le WEP
- filtrage par adresse MAC
- supprimer les broadcast SSID

Authentification : portail

Solution la plus simple à mettre en oeuvre

Principe : affecter aux utilisateurs non authentifiés une adresse IP dans un réseau non routable ou une passerelle spécifique.

Après authentification, paramètres normaux.

Exemples d'implémentation :
- NoCatAuth http://nocat.net/
- OpenBSD authpf http://www.openbsd.org/faq/pf/authpf.html

Problèmes :
- ne gère pas le chiffrement
- potentiellement contournable (car basé uniquement sur les adresses IP).

Possibilité de compléter par IPsec entre le routeur et les stations mobiles.

Authentification et chiffrement niveau 2

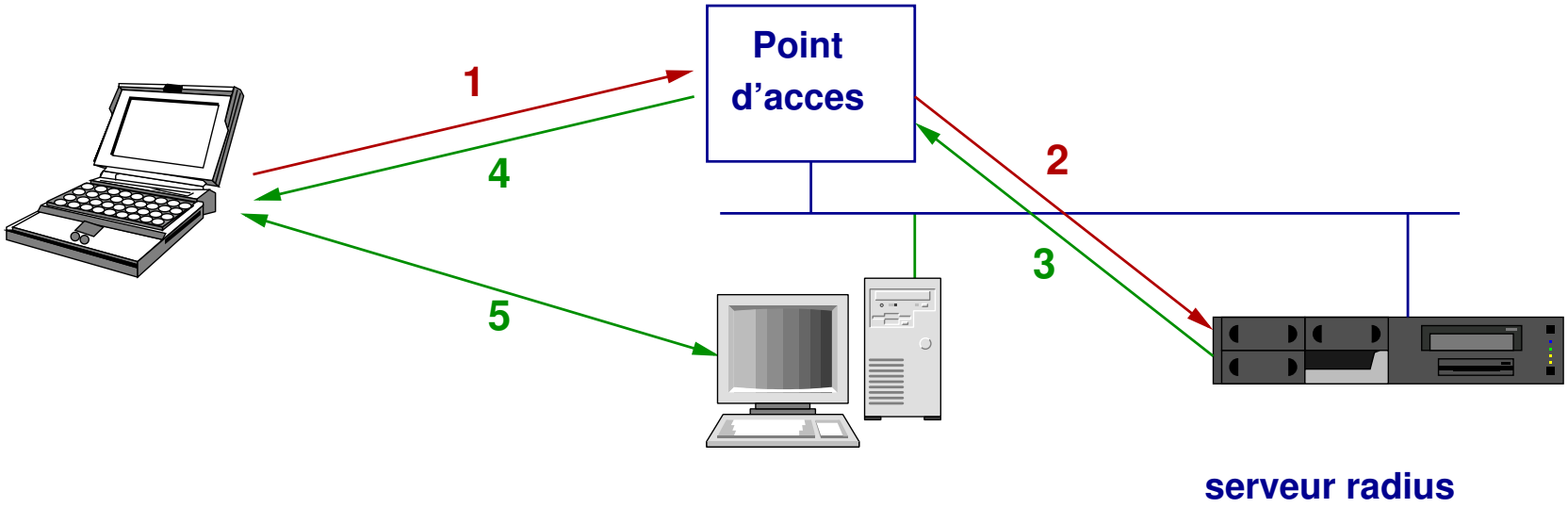
Solution générale aux problèmes de sécurité sur les réseaux publics :
authentification et chiffrement au niveau 2 : IEEE 802.1X & Co.

Domaine qui évolue vite en ce moment (2003) :
- Portail HTTP / SSH
- LEAP (Cisco + Microsoft)
- IEEE 802.1X
- WPA (Wifi Protected Access)
- IEEE 802.11i (intégré dans 802.11g)

Principe :
- Systèmes de niveau 2. Authentification entre le point d'accès et le client.
- basés sur le protocole d'authentification EAP
- utilisent un serveur Radius
- permettent la négociation des clés WEP

Implémentation de IEEE802.1X pour Unix : Open1x
http://open1x.sourceforge.net/

Authentification : LEAP, 802.1X, WPA, 802.11i



1. Le poste non authentifié arrive sur un point d'accès. Présente sa demande d'authentification
2. Le point d'accès vérifie l'authentification vis-à-vis d'un serveur (EAP)
3. Le serveur valide l'authentification.
4. Le point d'accès « ouvre » le réseau au niveau 2.
5. La station mobile peut communiquer à travers le point d'accès.

Conclusion

Les réseaux sans fil sont là pour durer.

Ils sont déjà largement déployés.

La technologie évolue rapidement.

Il faut les prendre en compte pour assurer la sécurité de nos systèmes.

Bibliographie

- 802.11 Security, B.Potter & B. Fleck, O'Reilly, Décembre 2002.
- Sécurité des réseaux sans file 802.11b, Hervé Schauer, mars 2002
  http://www.hsc.fr/ressources/presentations/asprom02/index.html.en
- Sécurité Informatique numéro 40, Juin 2002,
  http://www.cnrs.fr/Infosecu/num40-sansFond.pdf
- Déploiement & sécurité des réseaux sans fil (802.11b), D. Azuelos, Mai 2003
  http://www.urec.cnrs.fr/securite/CNRS/vCARS/DOCUMENTS/Azuelos.pdf
- Recommandation du CERT-A, août 2002
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002.pdf