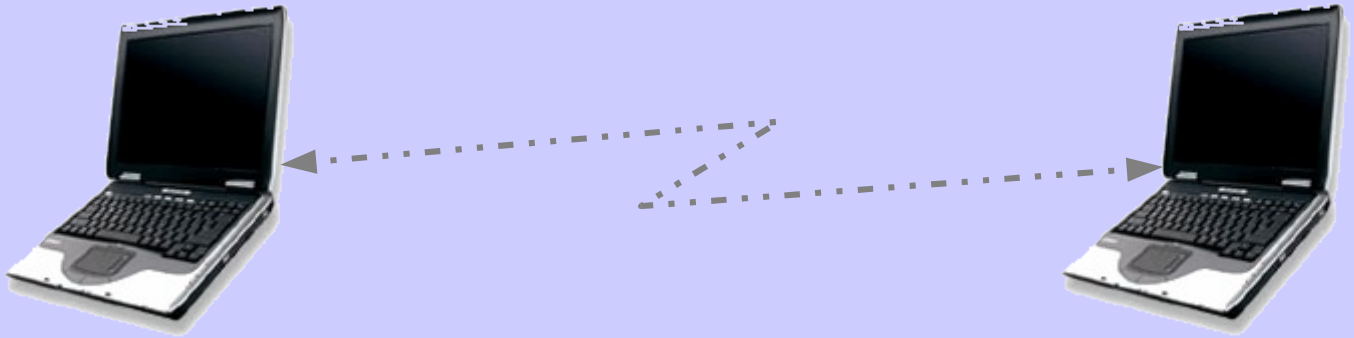
Sécurité des réseaux wi-fi

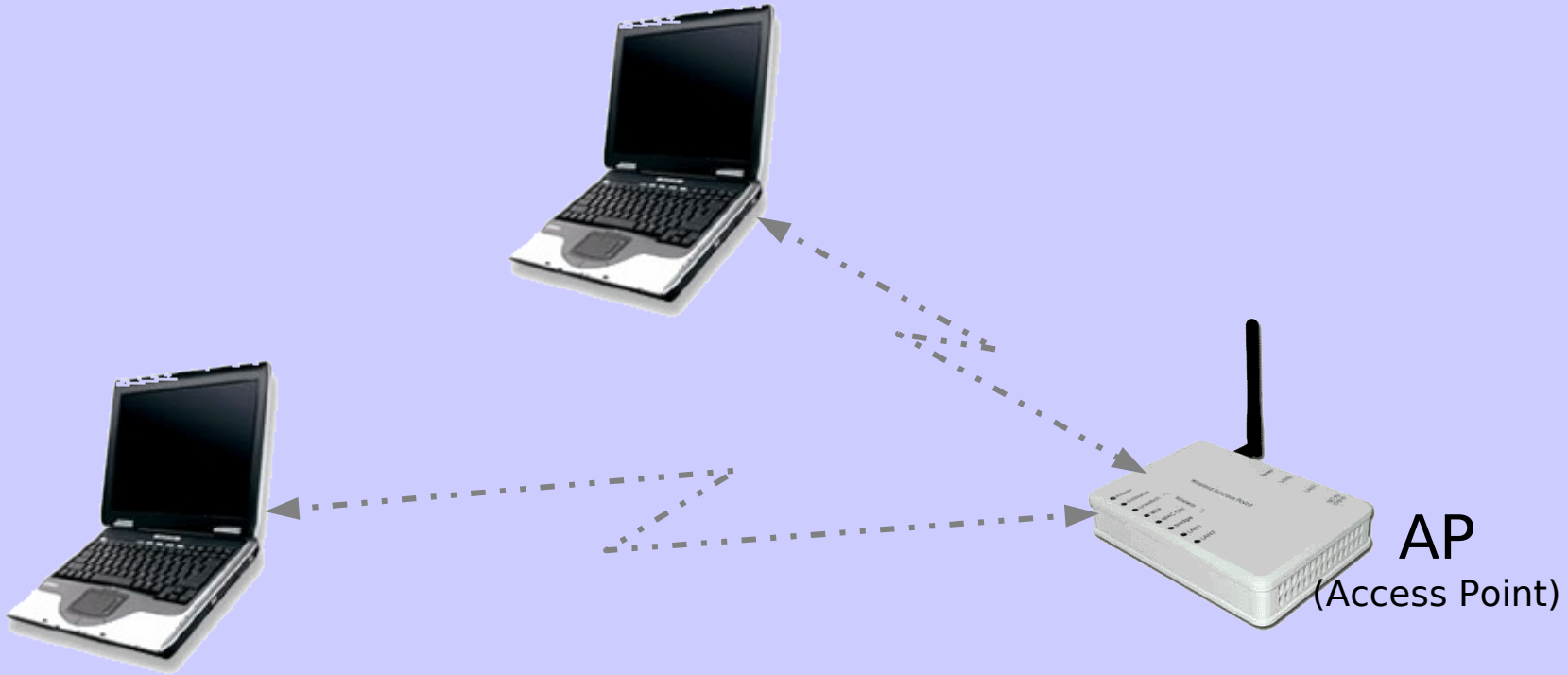
C. Drocourt,
drocourt@iut-amiens.fr

IUT Amiens,
Département Informatique

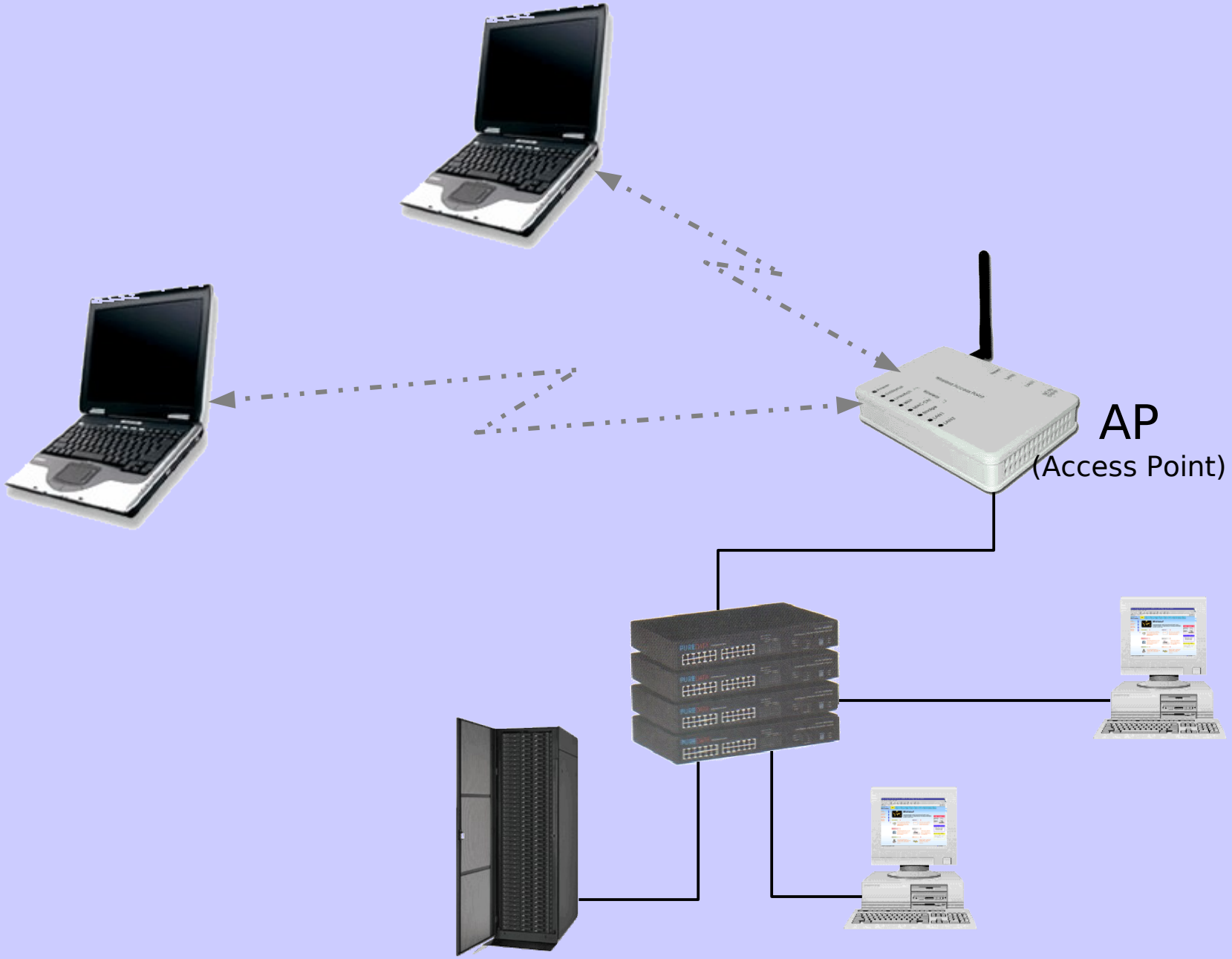
Mode Ad Hoc



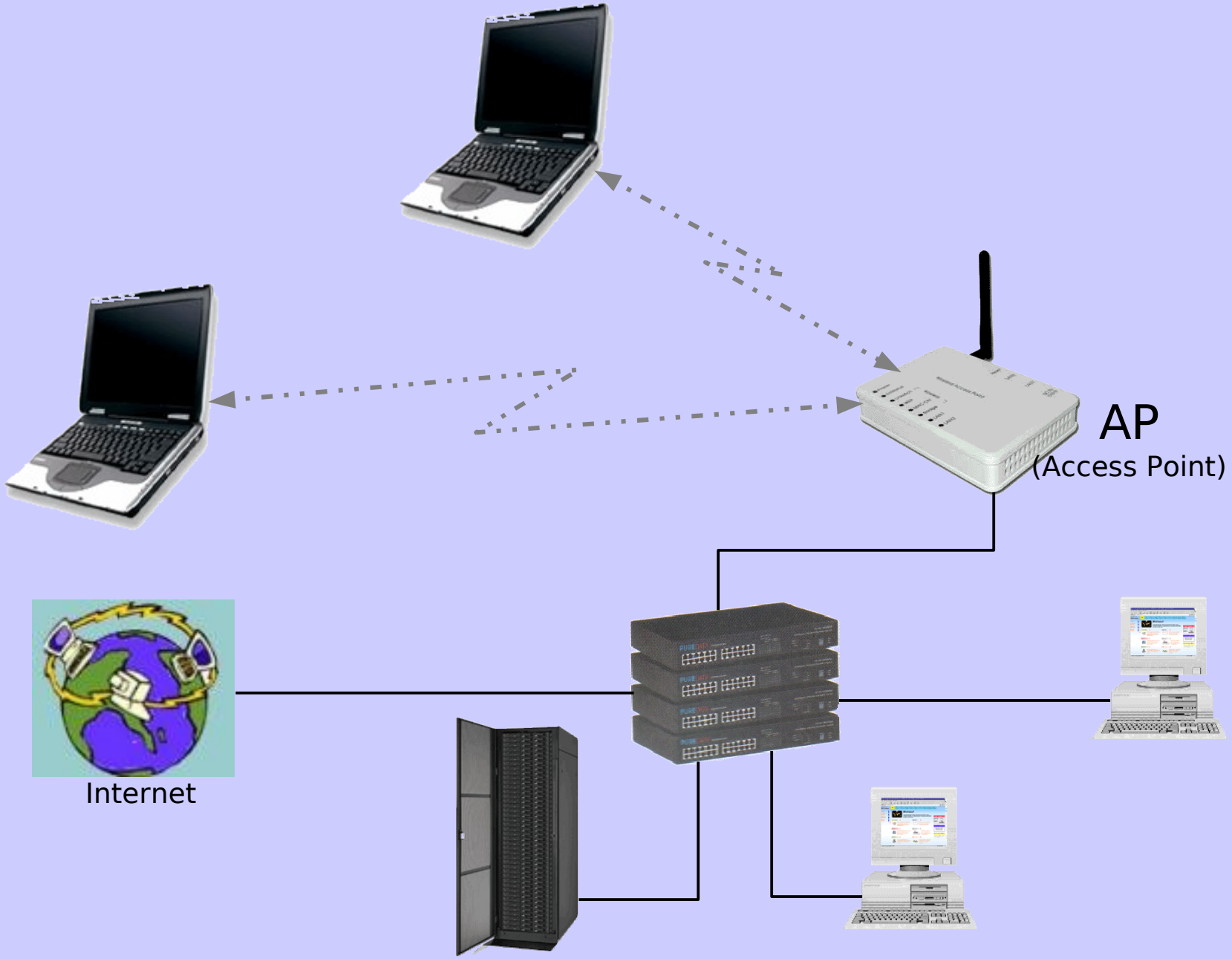
Mode Infrastructure



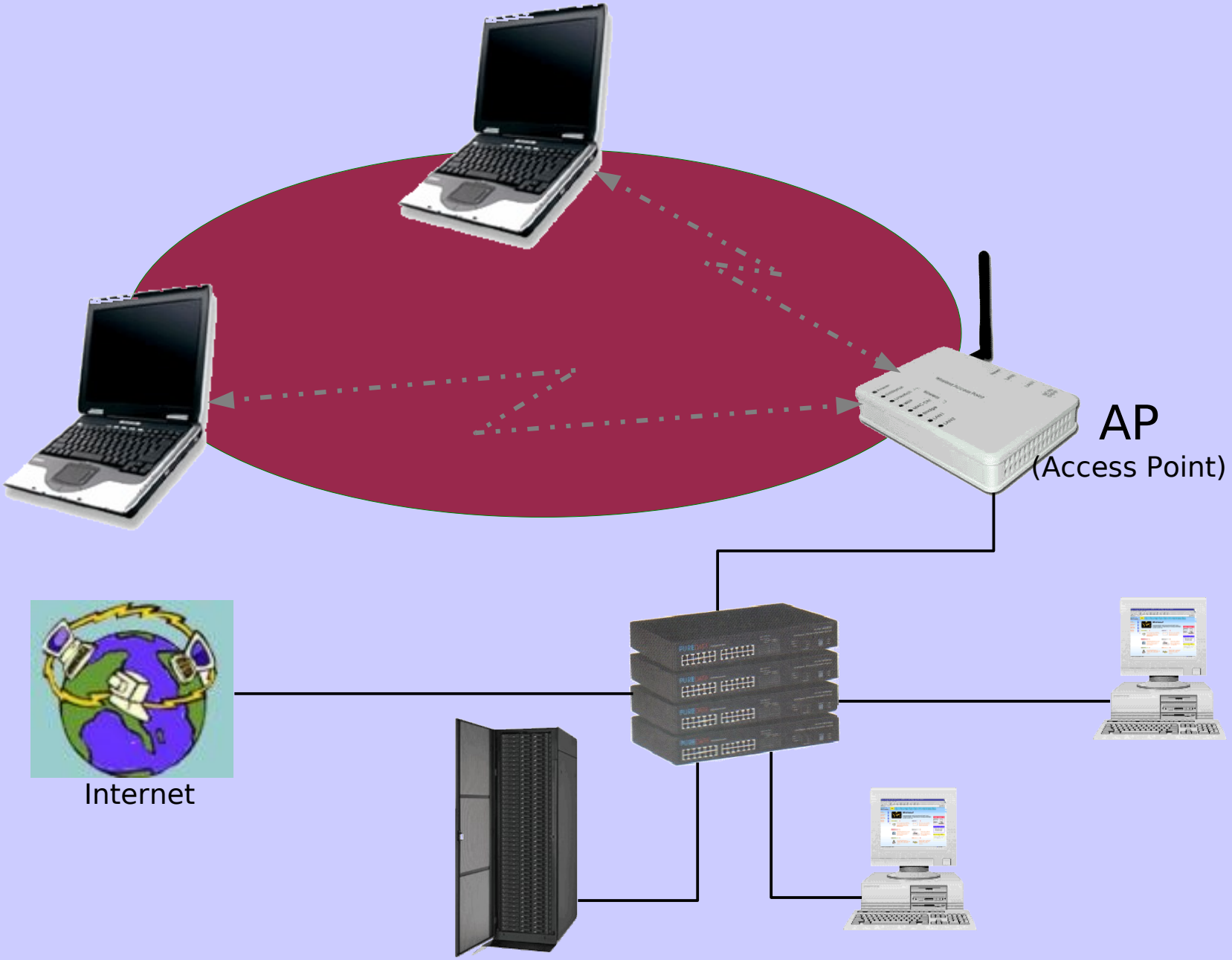
Mode Infrastructure



Mode Infrastructure

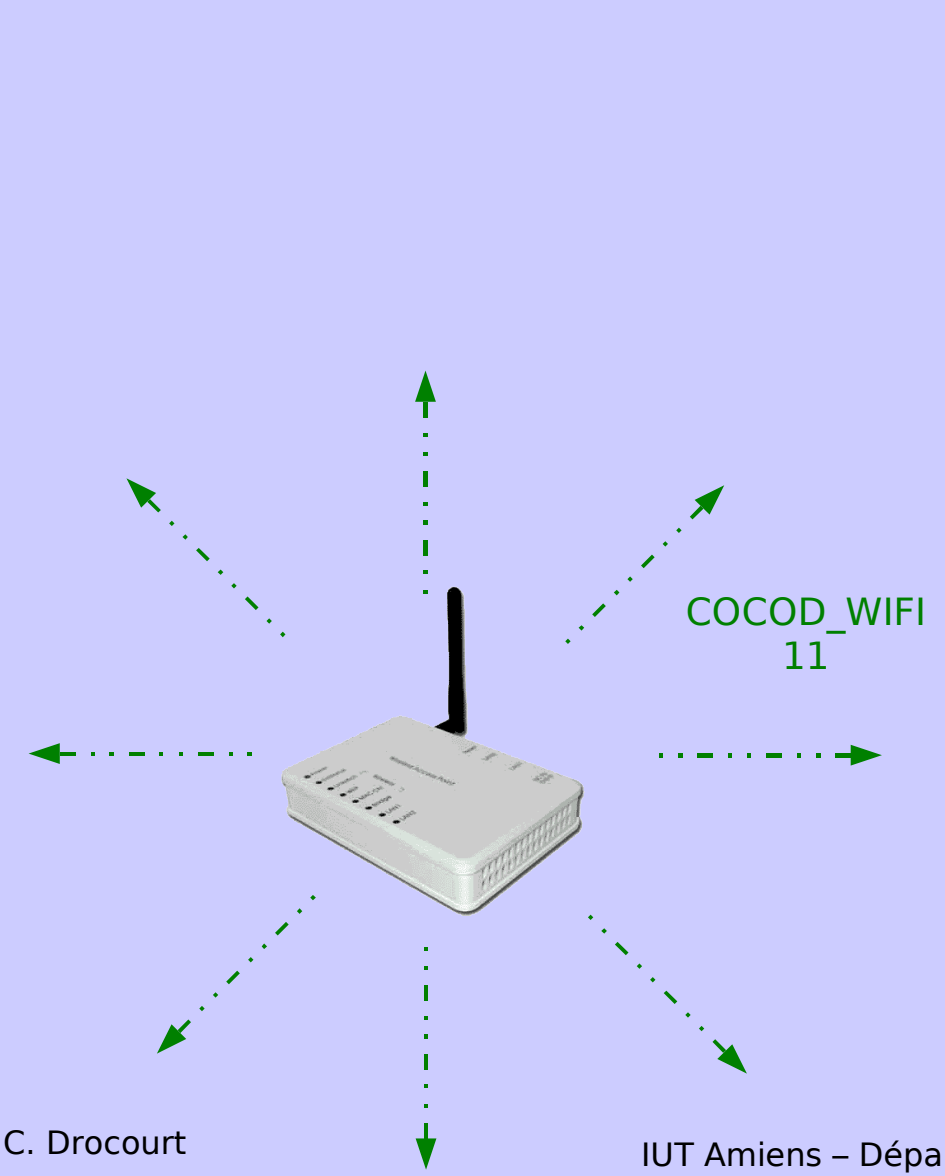


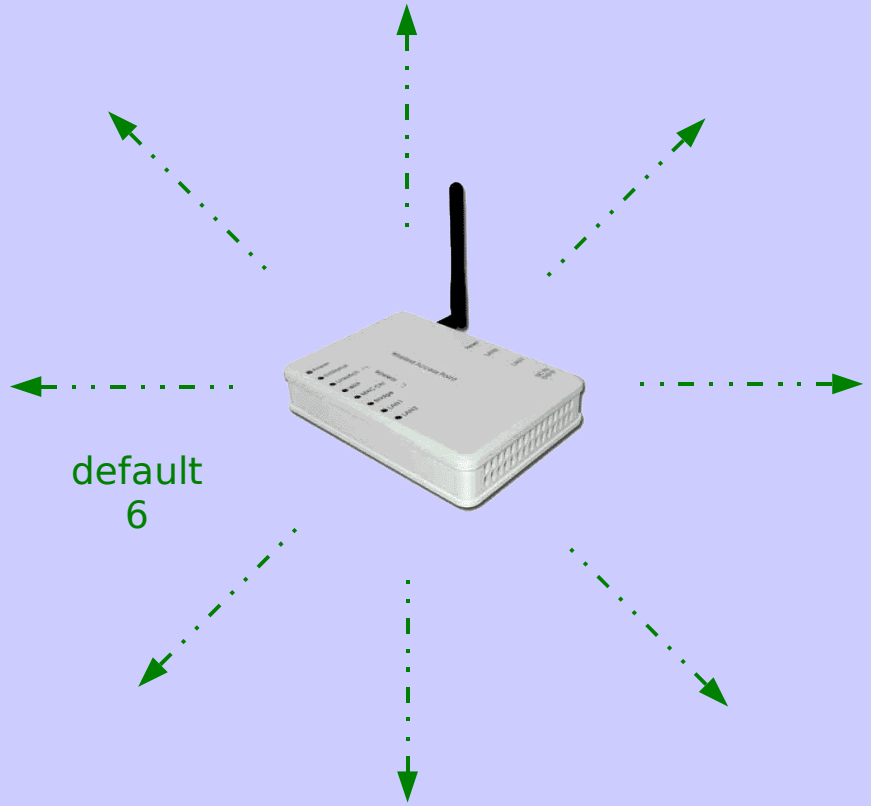
Mode Infrastructure



Sans sécurité

Pour se connecter à un AP, il faut le numéro du canal utilisé, ainsi que son identifiant (SSID) que l'AP diffuse régulièrement (beacon frames).

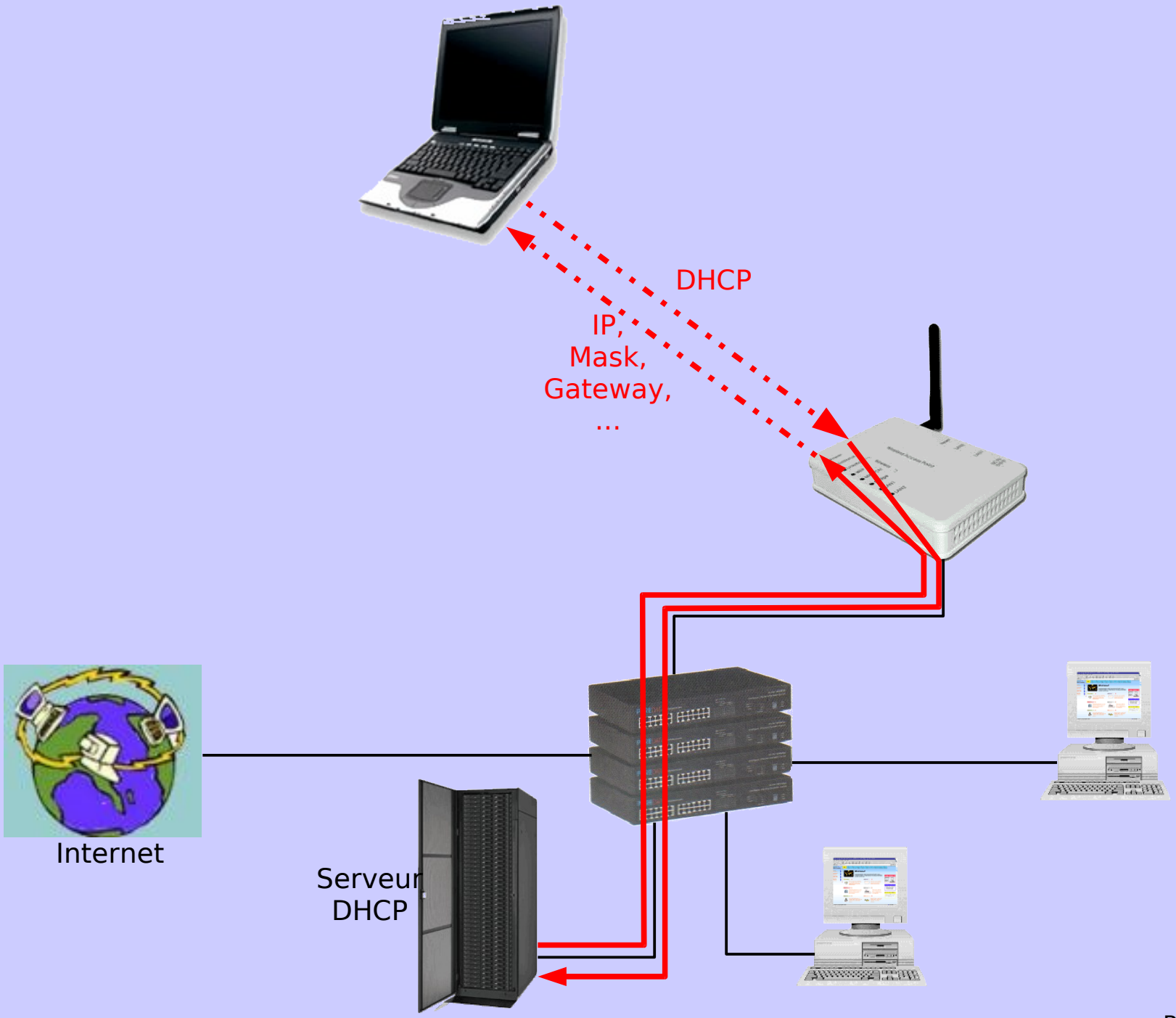




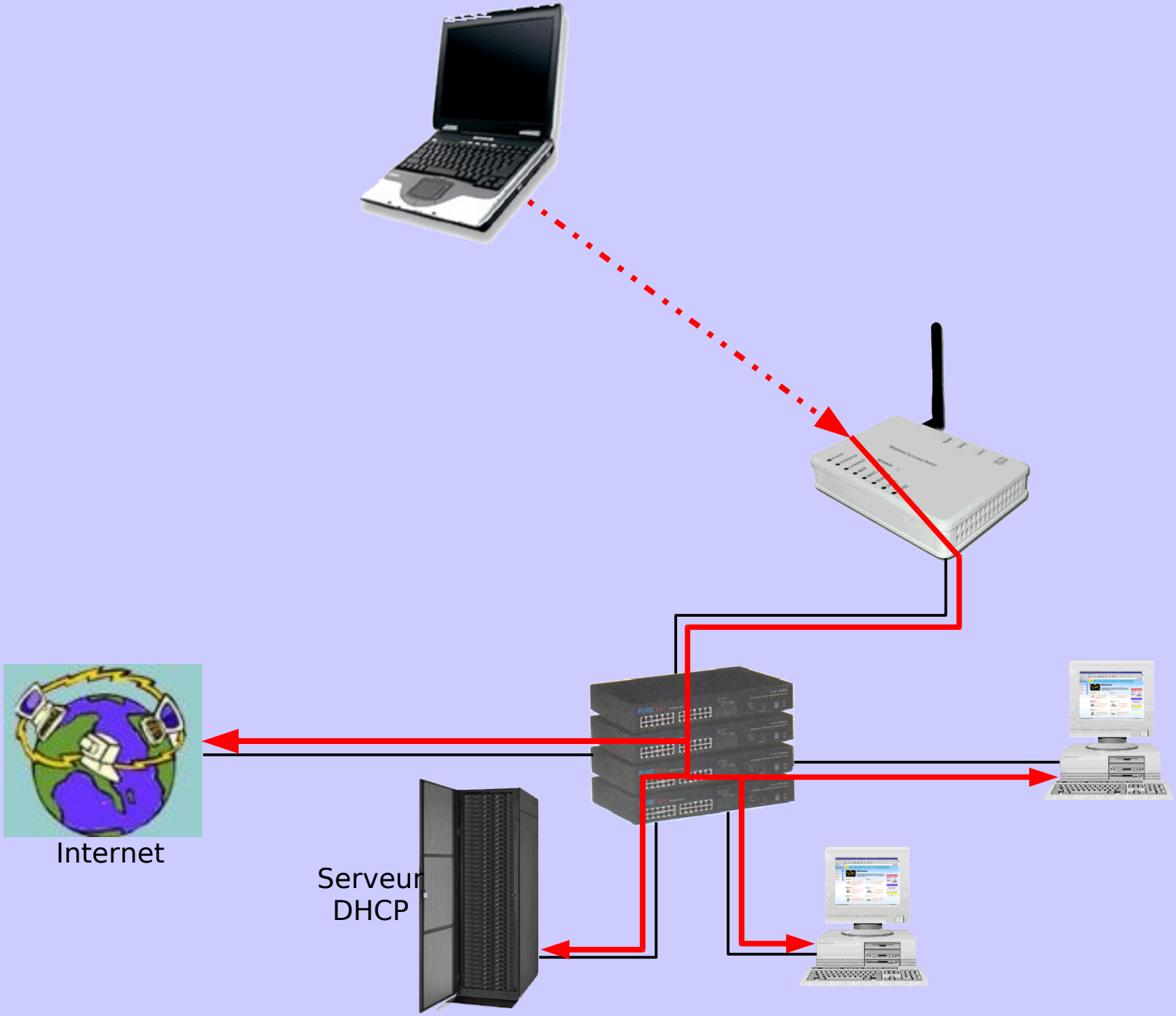
Sans sécurité

```
[root@machine ~]# iwlist eth1 scanning
eth1      Scan completed :
          Cell 01 - Address: 00:40:05:D0:46:00
                    ESSID:"default"
                    Protocol:IEEE 802.11b
                    Mode:Master
                    Channel:6
                    Encryption key:off
                    Bit Rate:22Mb/s
                    Extra: Rates (Mb/s): 1 2 5.5 11 22
                    Signal level=-84 dBm
                    Extra: Last beacon: 113ms ago
          Cell 02 - Address: 00:12:A9:03:00:31
                    ESSID:"COCOD_WIFI"
                    Protocol:IEEE 802.11bg
                    Mode:Master
                    Channel:11
                    Encryption key:on
                    Bit Rate:54Mb/s
                    Extra: Rates (Mb/s): 1 2 5.5 9 11 6 12 18 24 36 48 54
                    Signal level=-82 dBm
                    Extra: Last beacon: 131ms ago
```

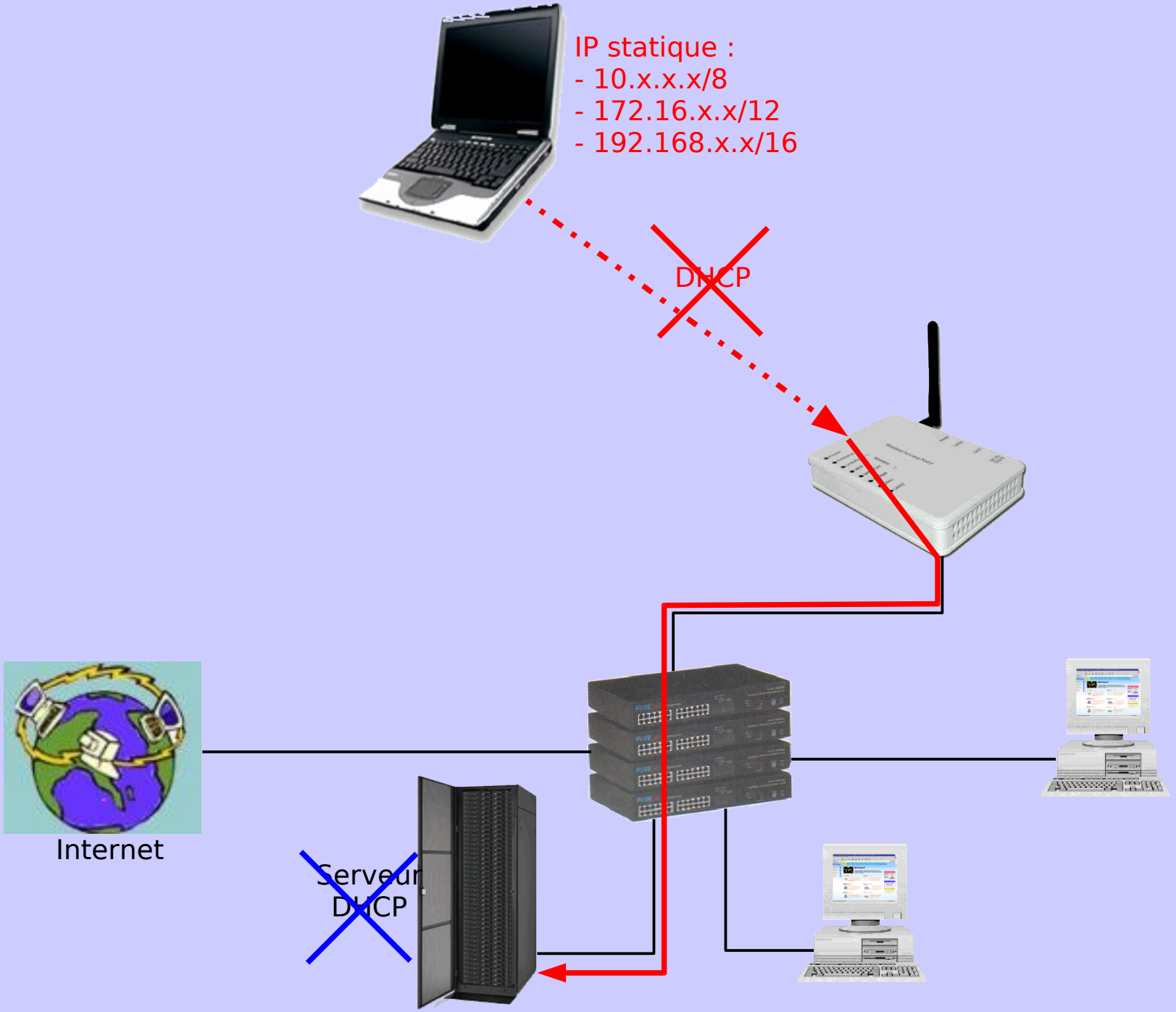
Sans sécurité



Sans sécurité

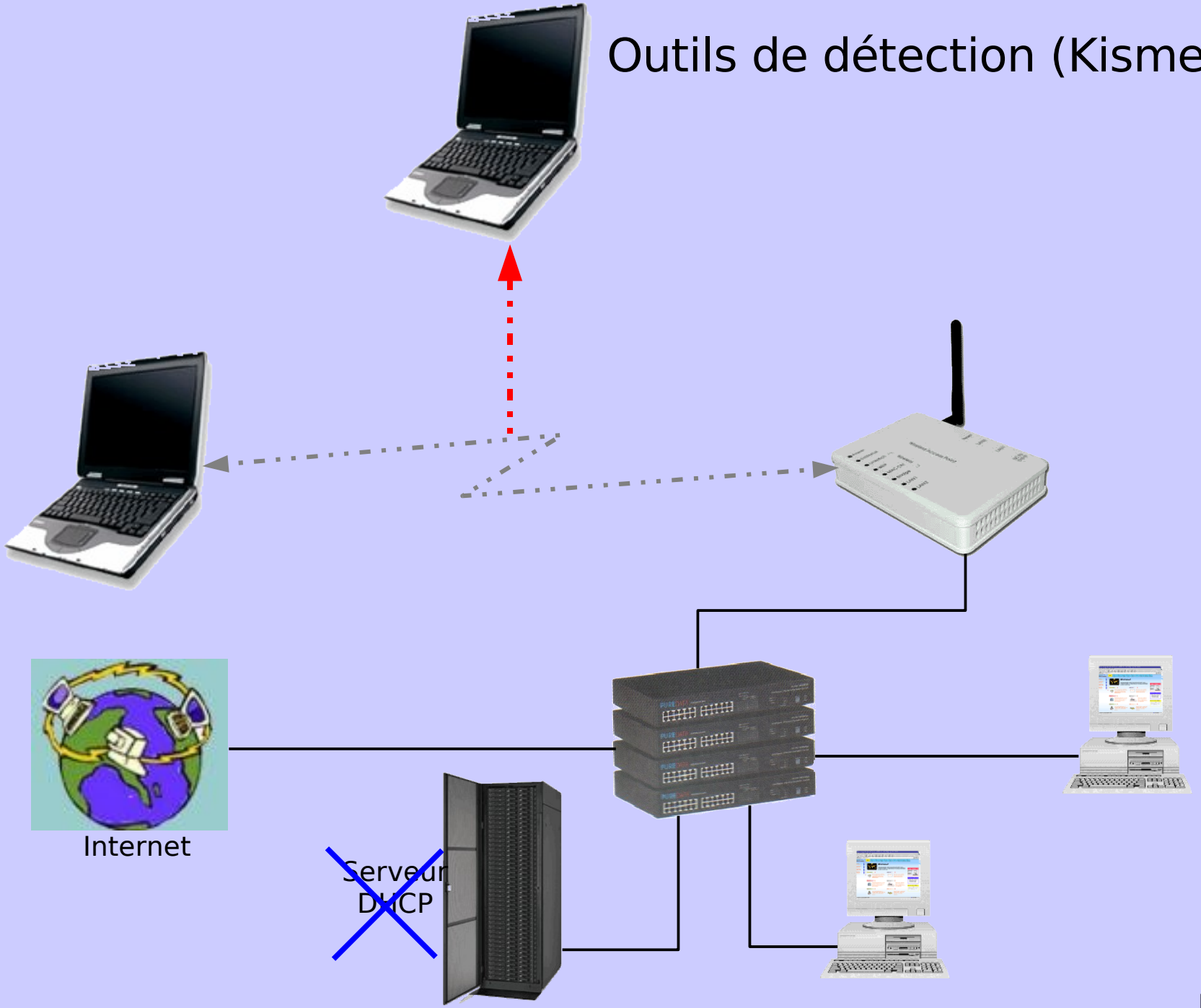


Sécurité 1 : Sans DHCP



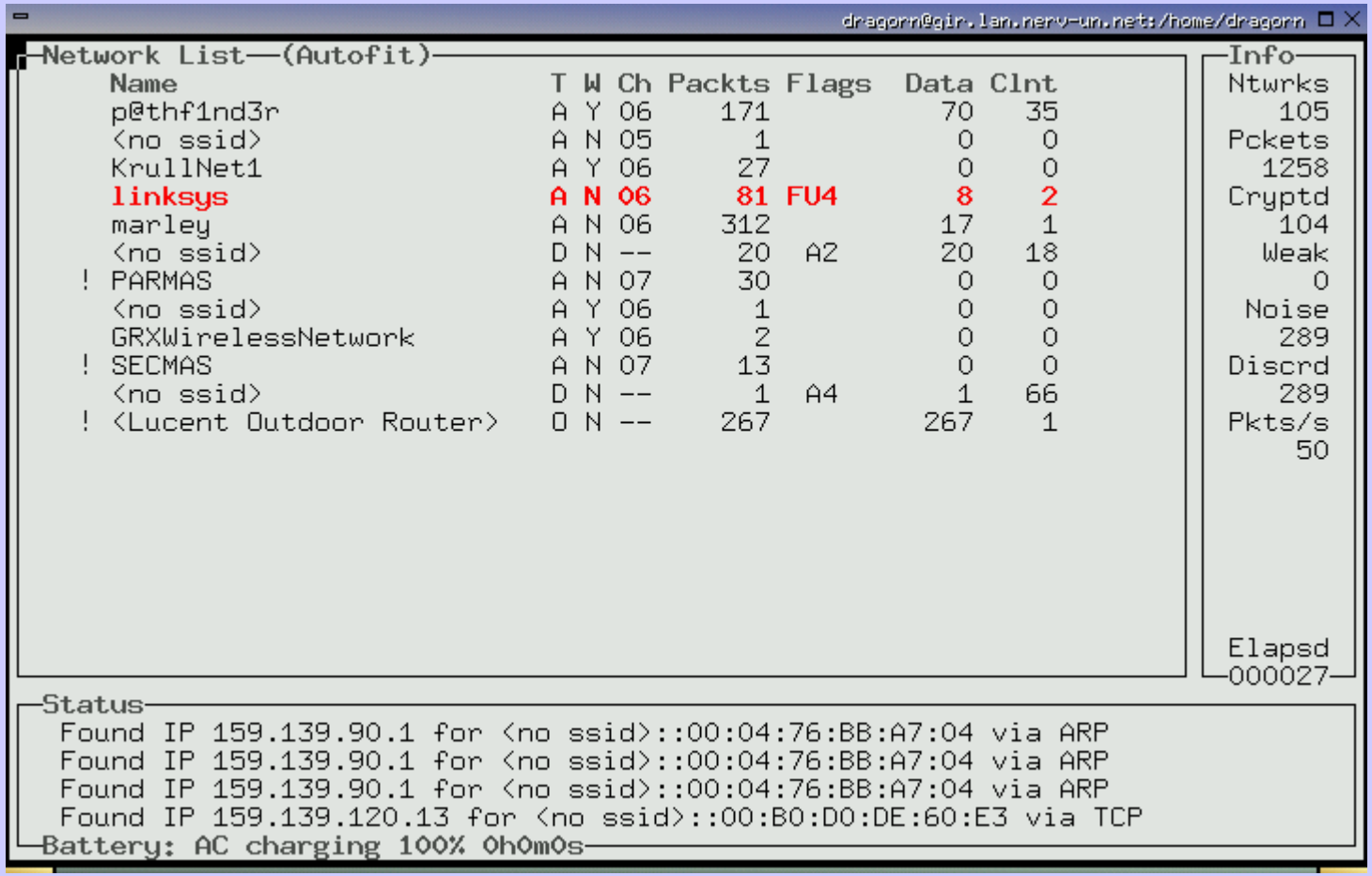
Sécurité 1 : Sans DHCP

Outils de détection (Kismet)



Outils de détection

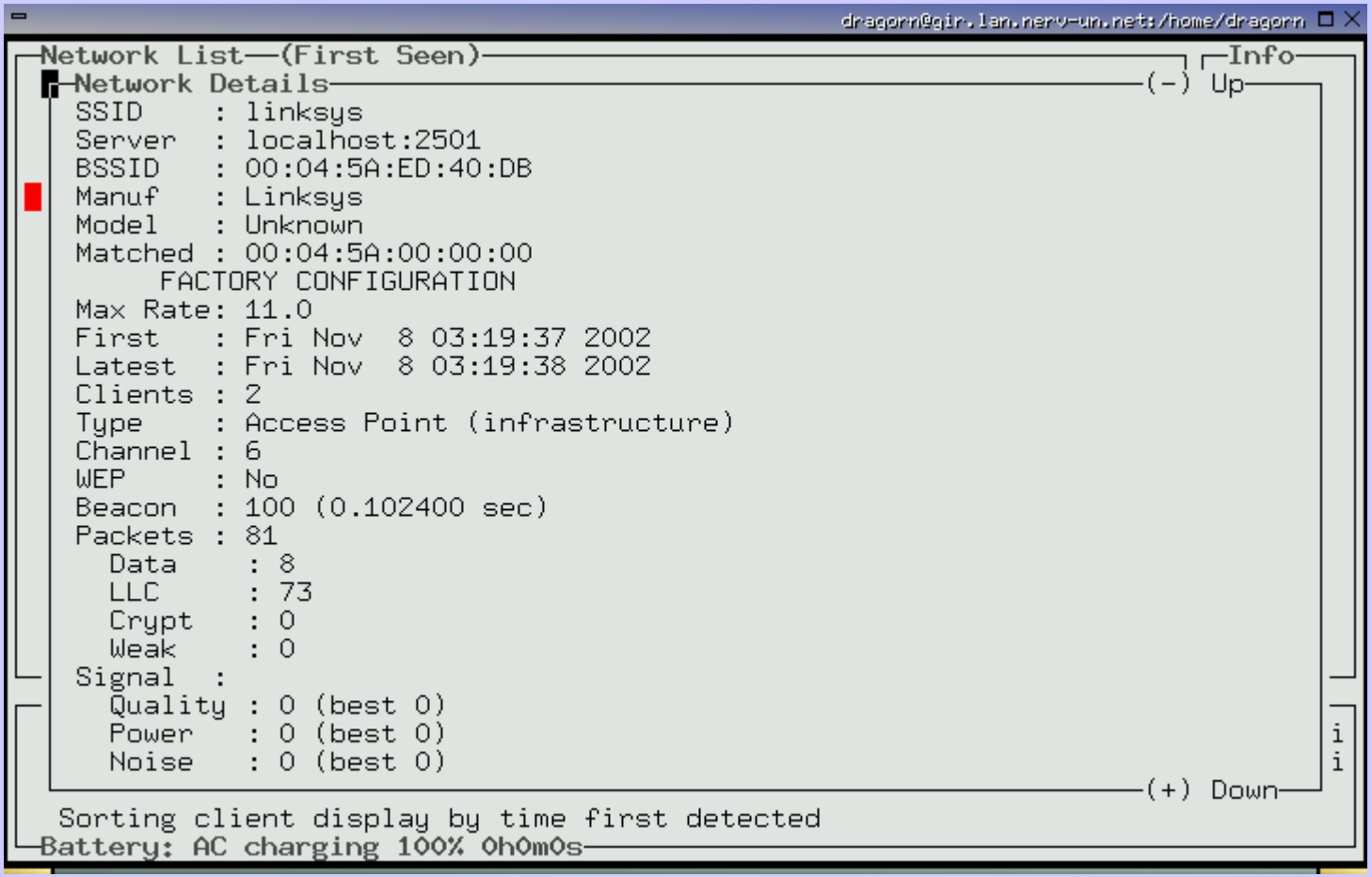
KISMET



http://www.kismetwireless.net/

Outils de détection

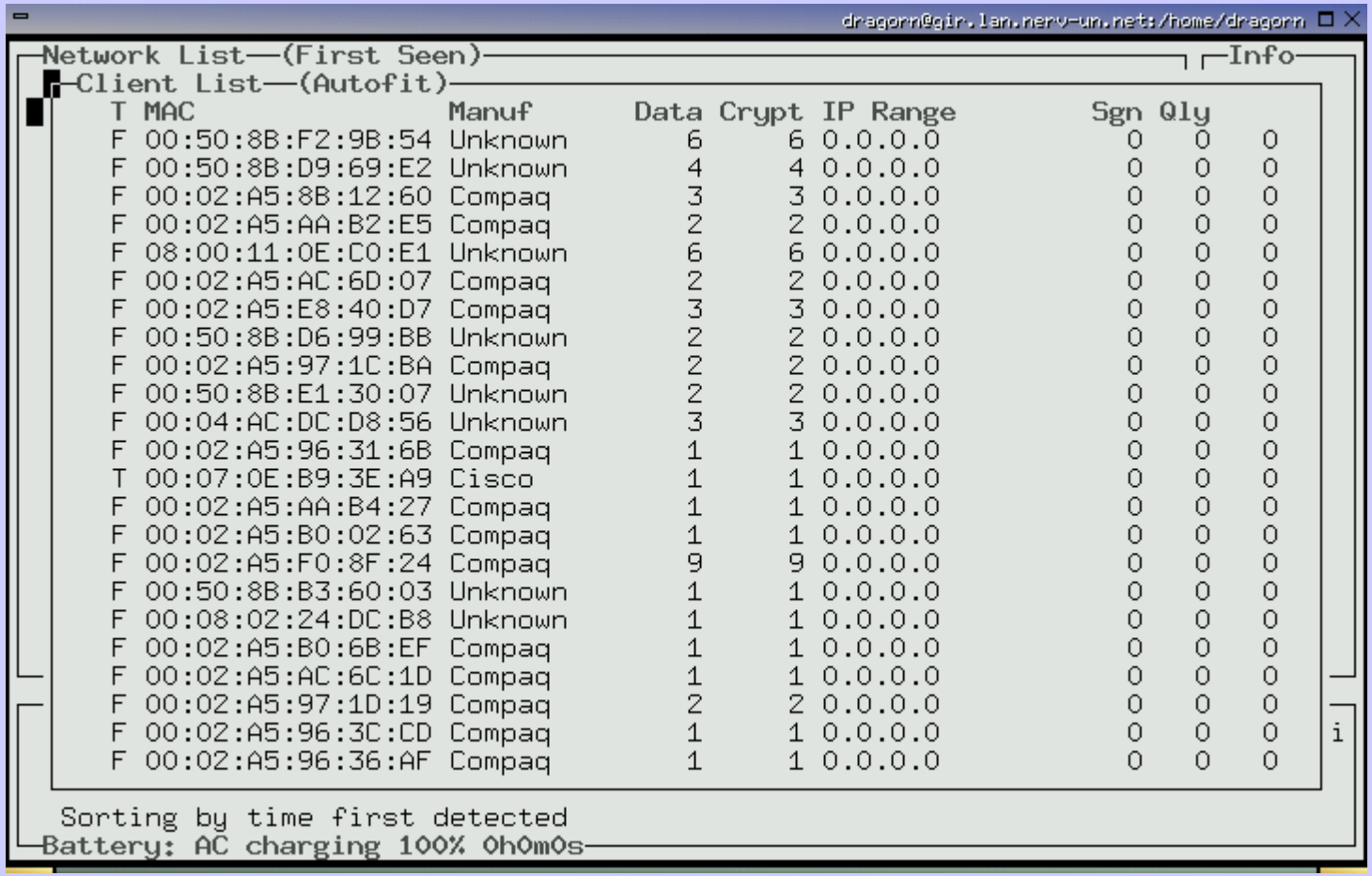
KISMET



http://www.kismetwireless.net/

Outils de détection

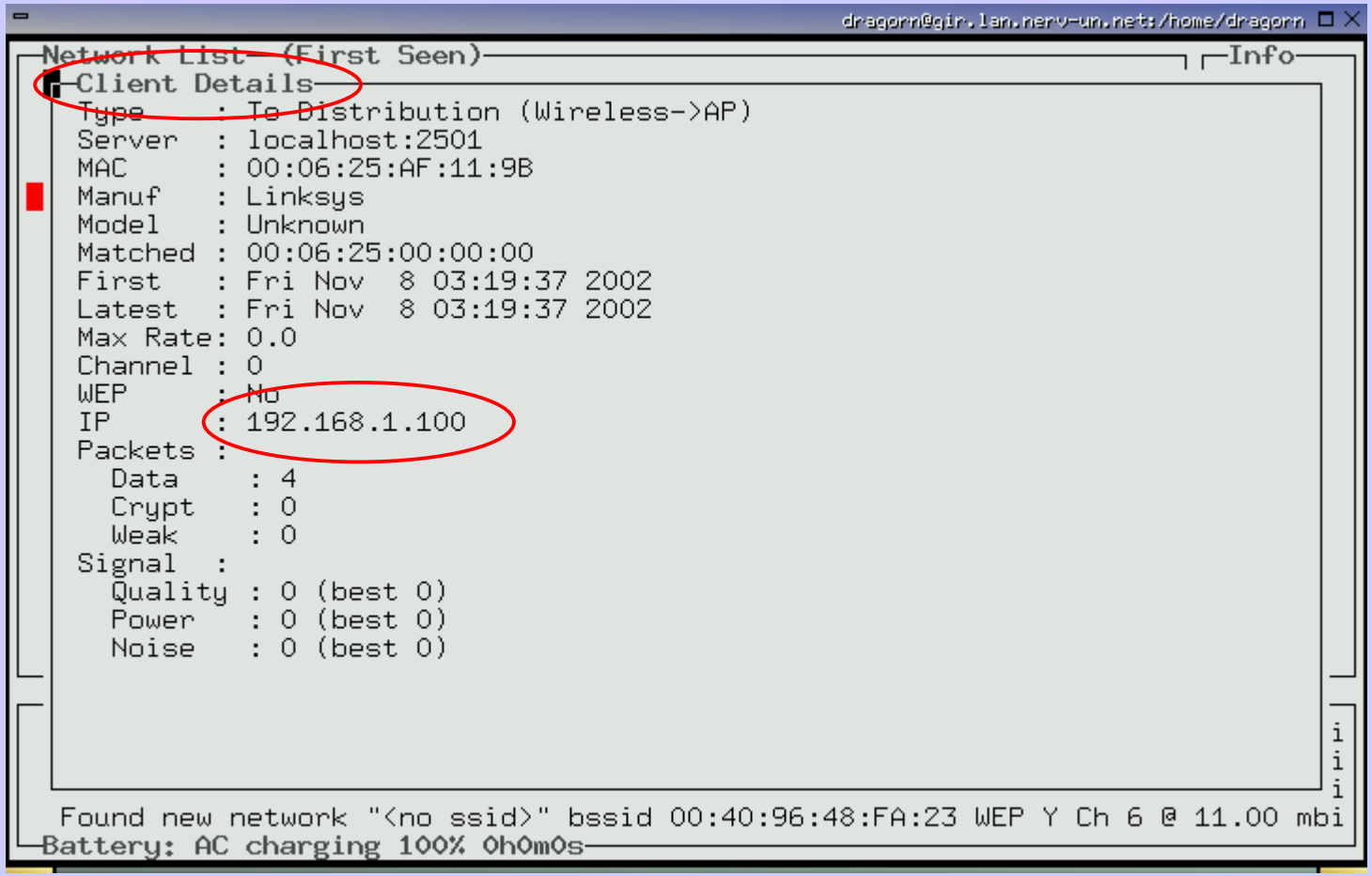
KISMET



http://www.kismetwireless.net/

Outils de détection

KISMET



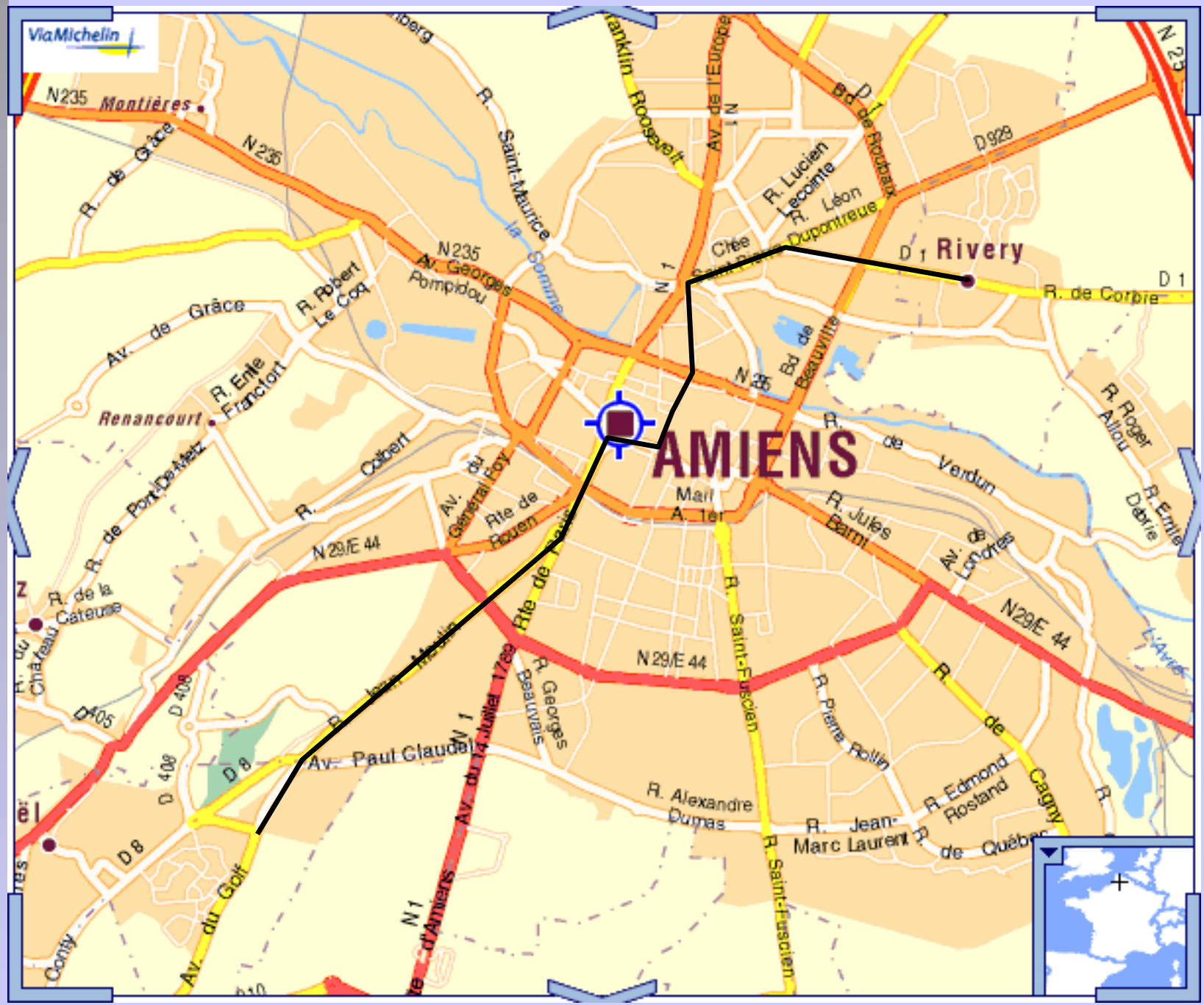
http://www.kismetwireless.net/

Outils de détection

WarDriving...

http://www.worldwidewardrive.org/
http://www.wardriving.com/
http://www.seattlewireless.net/index.cgi/WarDrivingSoftware

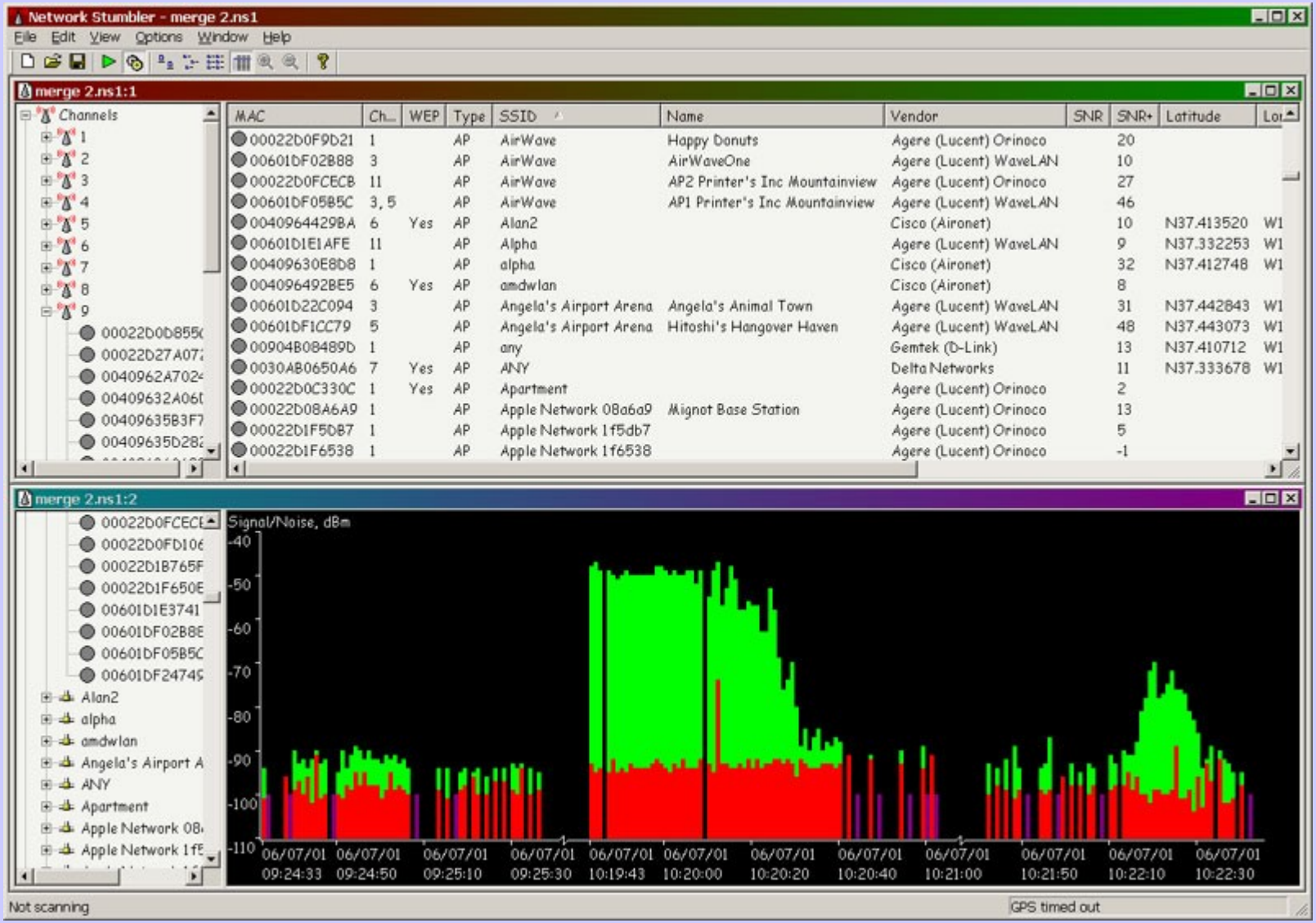
Outils de détection



Distance :
7 km
Bornes :
123
Non cryptés :
31
(25%)

Outils de détection

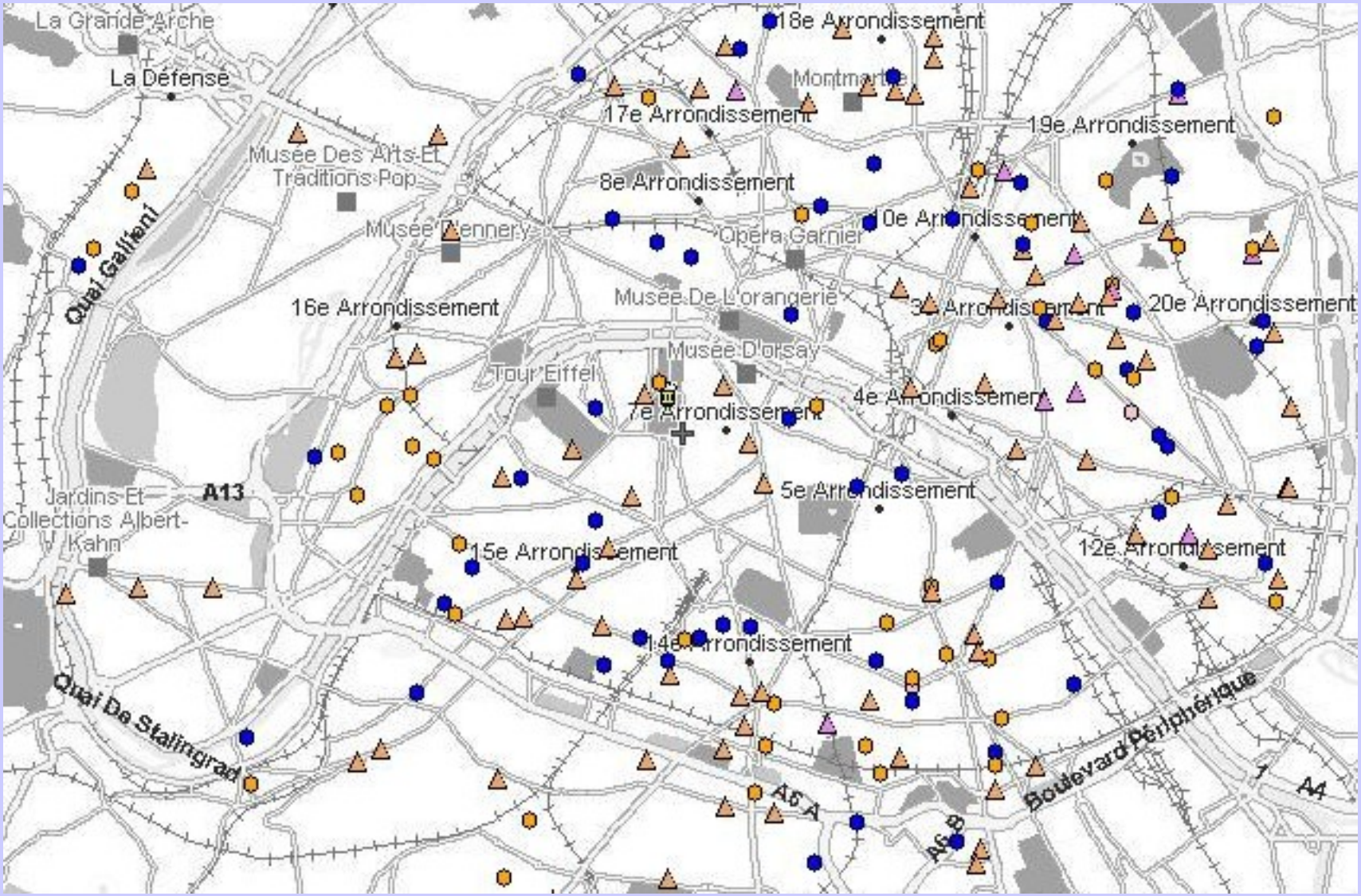
WarDriving...



http://www.netstumbler.com/

Outils de détection

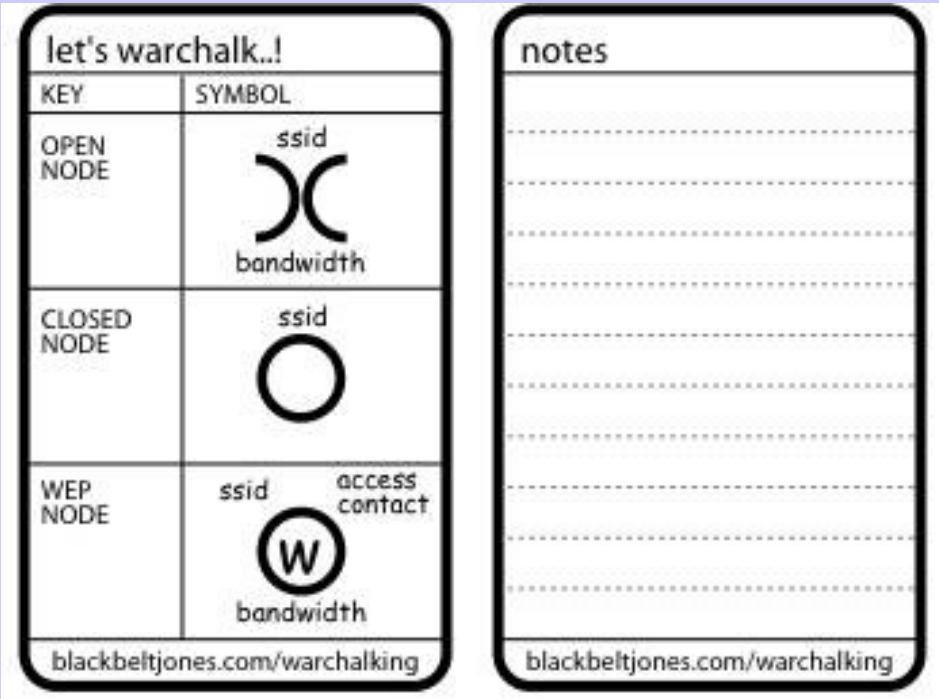
WarDriving...



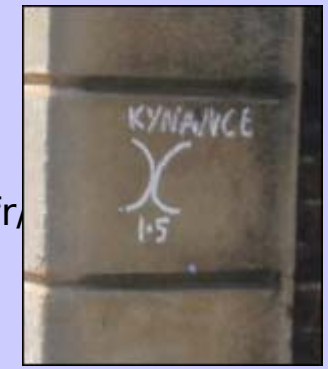
http://www.paris-sansfil.fr/

Outils de détection

WarChalking...(craiefiti)



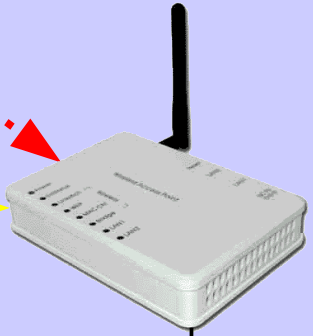
http://craiefiti.free.fr/



Sécurité 2 : Filtrage MAC

Mac :
00:0A:5E:21:B7:53

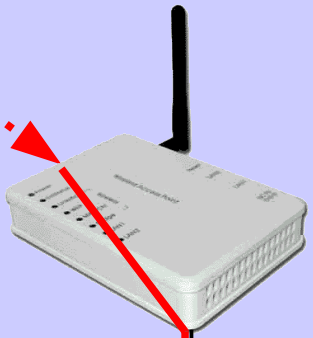
Allow mac :
00:45:8A:53:F4:21
02:A4:21:5B:32:10
...



Internet

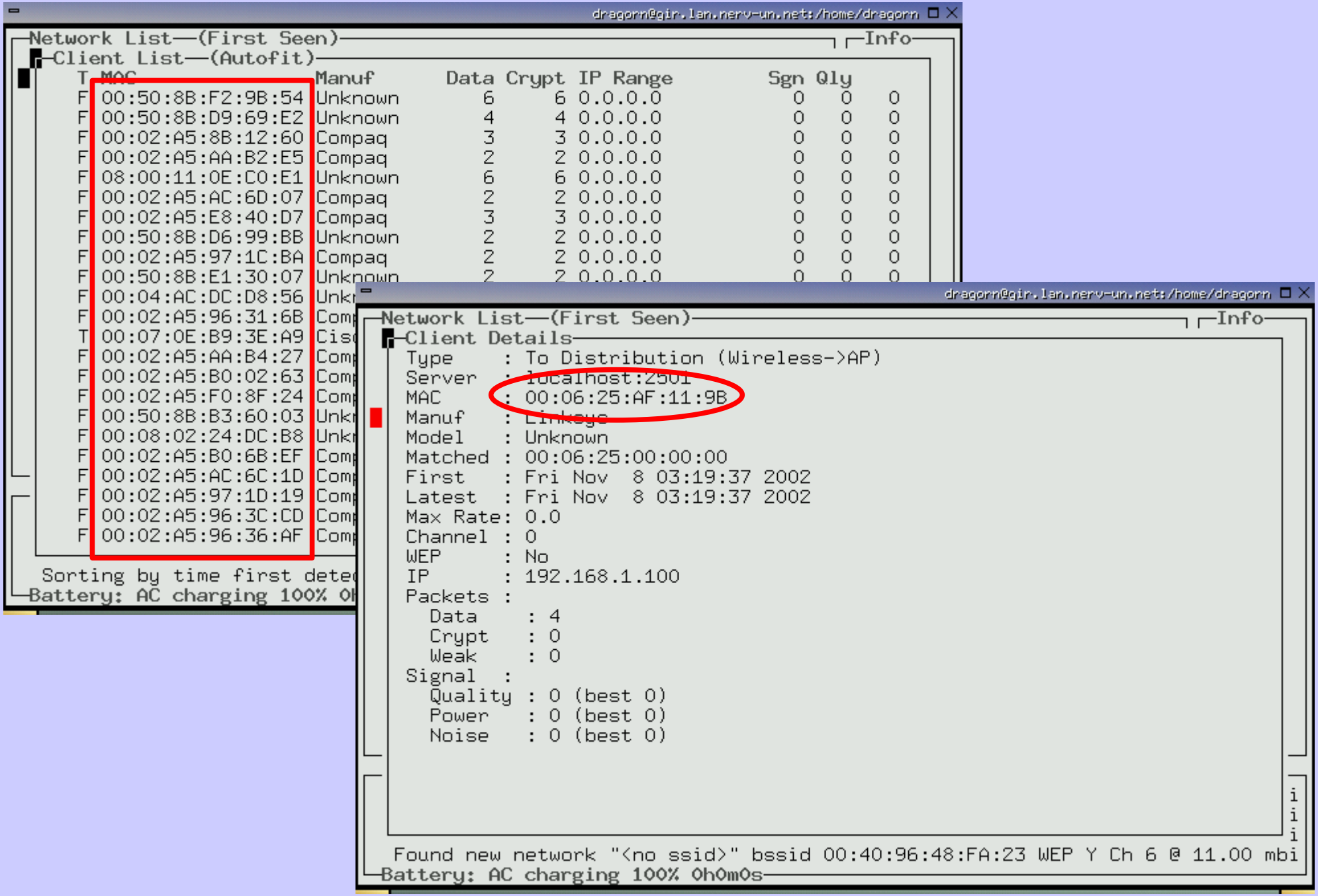
Sécurité 2 : Filtrage MAC

Mac :
00:0A:5E:21:B7:53

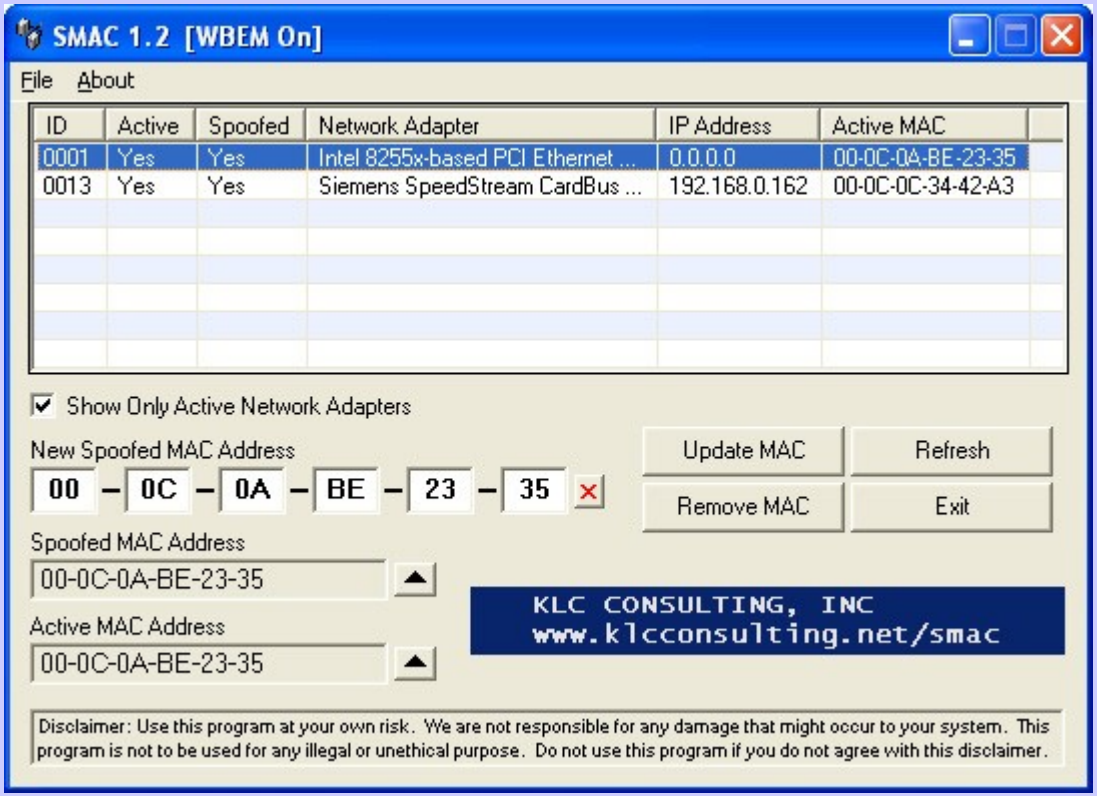


Internet

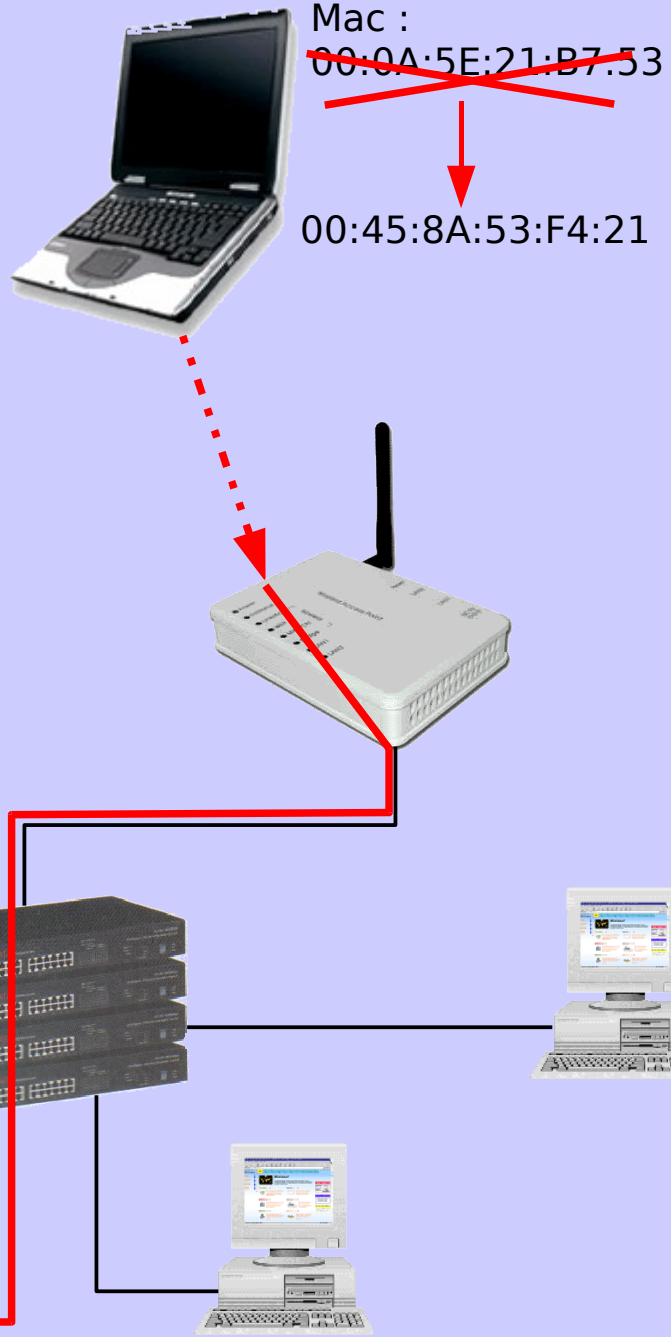
Sécurité 2 : Filtrage MAC



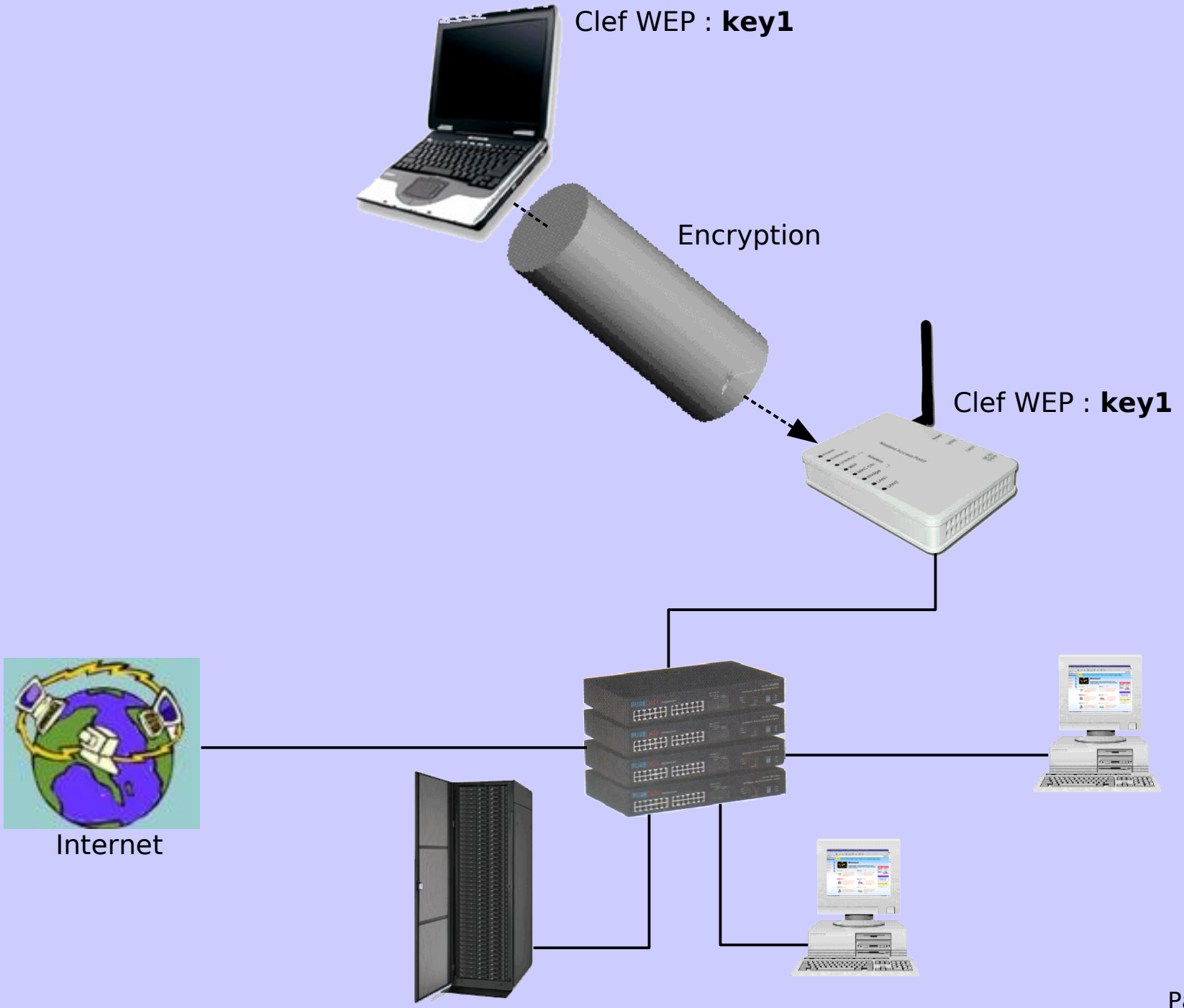
Sécurité 2 : Filtrage MAC



http://www.klcconsulting.net/smac/



Sécurité 3 : WEP



Sécurité 3 : WEP


Clef WEP : **key1**


Clef WEP : **key1**

Problème 1 : Modification de la clef

Clef WEP : **key1**

Clef WEP : **key1**


Internet

Sécurité 3 : WEP

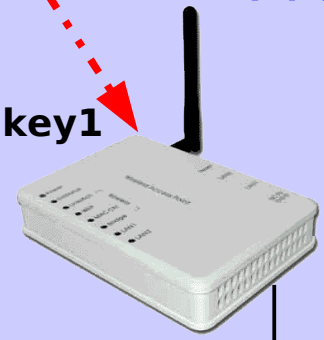
Clef WEP : **key1**

Clef WEP : **key1**

Clef WEP : **key1**

Problème 2 : Confidentialité de la clef

Clef WEP : **key1**



Clef WEP : **key1**

Internet

Sécurité 3 : WEP

Problème 3 : Mécanisme d'encryption

Clef codée sur 64 ou 128 bits dont 24 bits pour le vecteur d'initialisation

- Attaque par « Dictionary cracking »
- Attaque par « Brute force cracking »
- Attaque par « Hacking »

Principe : 24 bits pour le vecteur d'initialisation, le vecteur change à chaque trame donc 2 puissance 24 = 16,8 millions de trames -> Possible en peu de temps suivant le débit.

airsnort : http://airsnort.shmoo.com/
wepcrack : http://wepcrack.sourceforge.net/

Sécurité 4 : 802.1x (2001)

Principe :

- Authentification avec EAP (extensible),

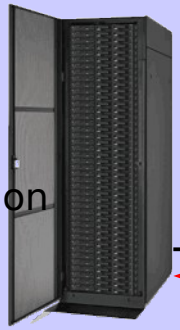
Supplicant

EAP

Authenticator

Seul le trafic entre la station et le serveur est autorisé.

Internet

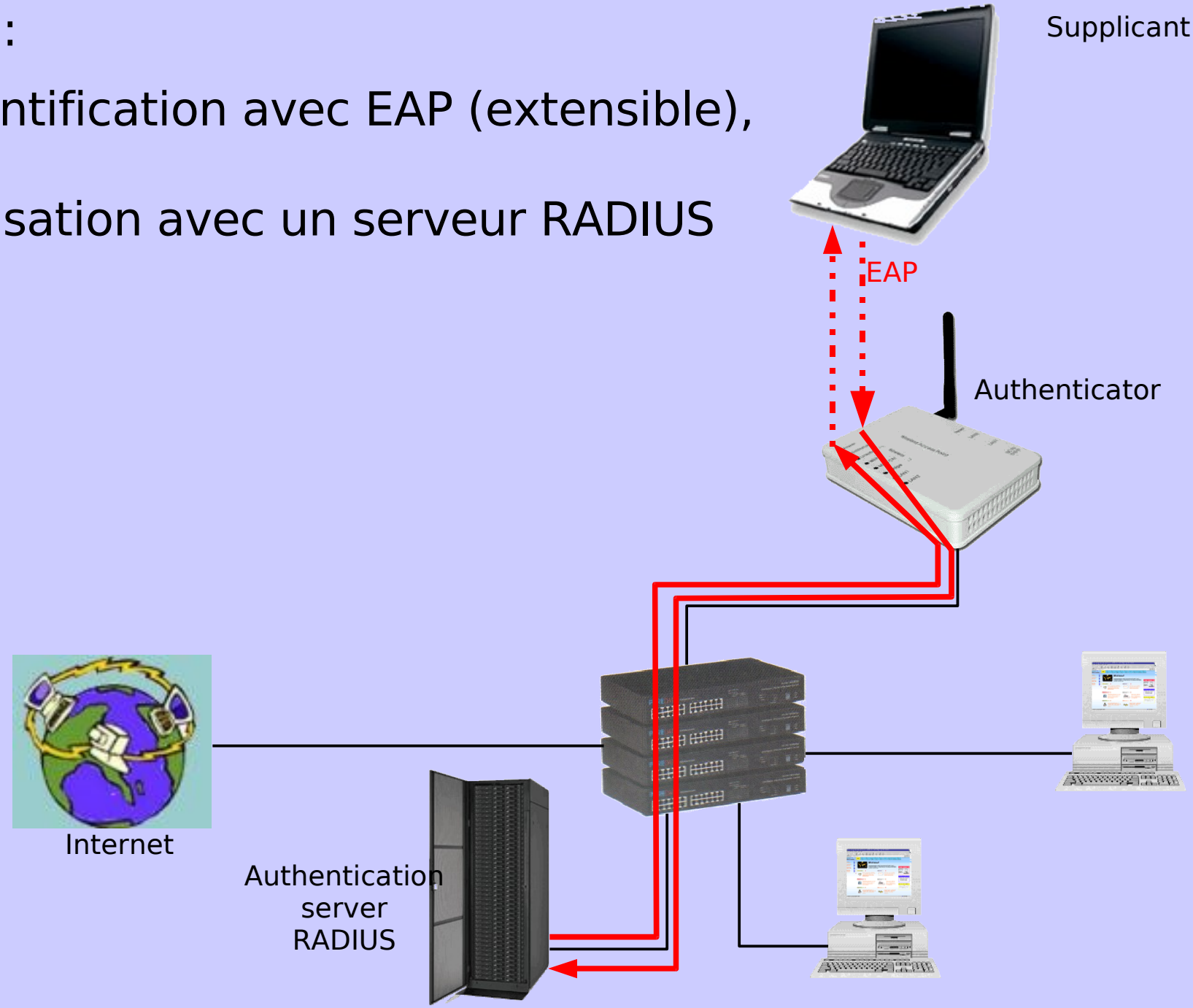


serveur
d'authentification
RADIUS

Sécurité 4 : 802.1x (2001)

Principe :

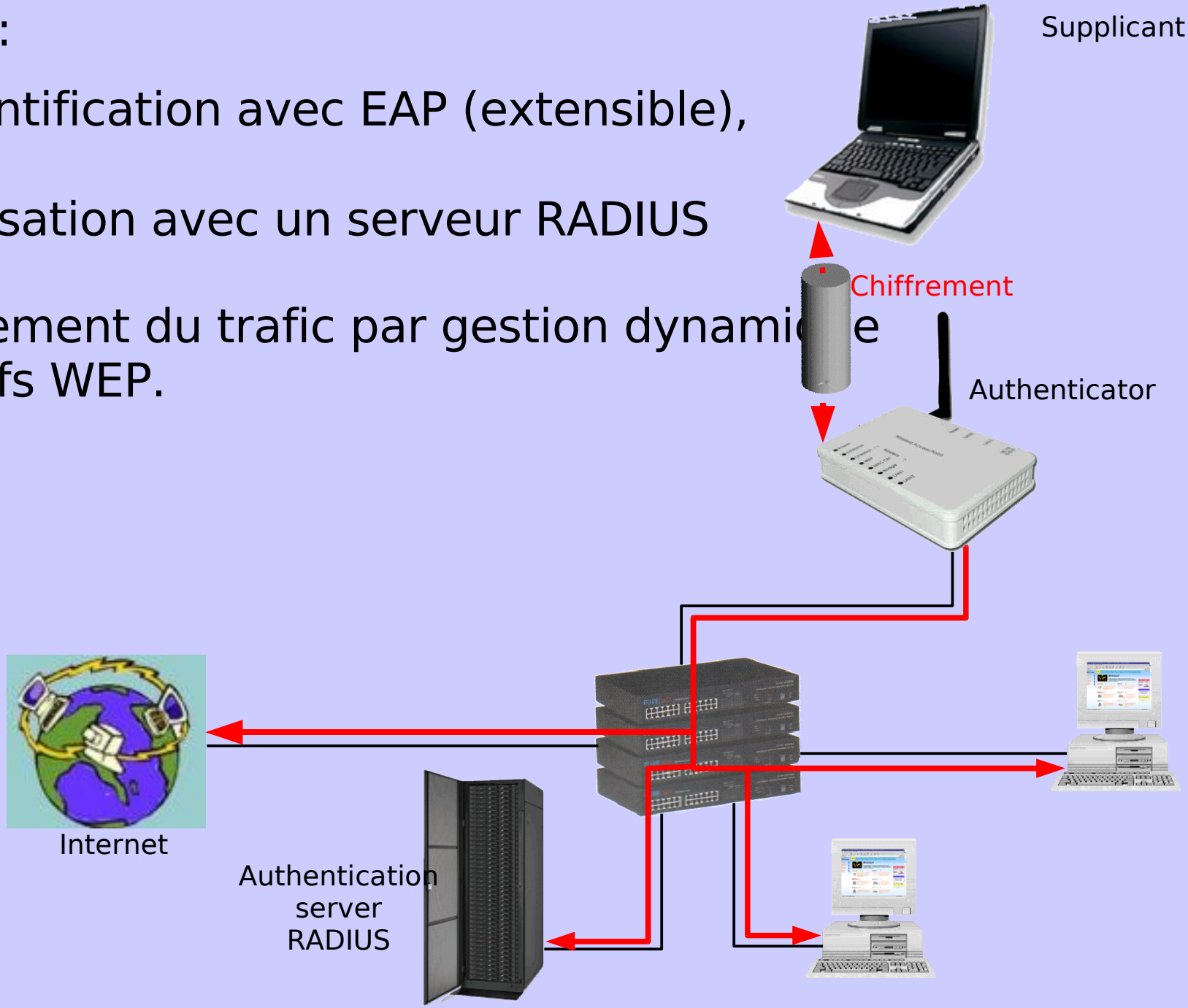
- Authentification avec EAP (extensible),
- Autorisation avec un serveur RADIUS



Sécurité 4 : 802.1x (2001)

Principe :

- Authentification avec EAP (extensible),
- Autorisation avec un serveur RADIUS
- Chiffrement du trafic par gestion dynamique de clefs WEP.



Sécurité 4 : 802.1x (2001)

EAP : Extensible Authentication Protocol

- L'AP ne s'occupe pas des méthodes EAP,
- Le protocole est extensible.

EAP-MD5 est la version la moins sûre d'EAP, car elle gère des noms d'utilisateur et des mots de passe pour l'authentification, elle est vulnérable aux attaques par dictionnaire.
LEAP (Lightweight EAP) est une solution principalement CISCO.

EAP-TLS (Transport Layer Security) est un standard ouvert pris en charge par la quasi-totalité des fournisseurs. Basé sur EAP, il utilise un système de chiffrement avec clés privées et publiques asymétriques par les clients et le serveur RADIUS (PKI – Public Key Infrastructure).

EAP-TTLS (Tunneled TLS) est est solution plus simple à mettre en place que EAP-TLS puisque les clefs sont générés par le serveur et non stocké sur le client.

PEAP (Protected Extensible Authentication Protocol), **EAP-FAST** (Fast Authentication via Secure Tunneling), **EAP-SIM** (Extensible Authentication Protocol - Subscriber Identity Module), ...

Sécurité 5 : WPA (2003)

Le protocole WPA (Wi-Fi Protected Access) se résume par WPA=802.1X+TKIP. L'algorithme TKIP (Temporal Key Integrity Protocol) est le remplacement de l'algorithme de chiffrement WEP :

- il génère régulièrement une nouvelle clé plutôt que d'utiliser une clé fixe pour chiffrer les paquets de données,

- il remplace le CRC par une somme de contrôle cryptographique (MIC : Message Integrity Code).

Avantage : Le protocole peut être utilisé rapidement par mise à jour du firmware des bornes par exemple, puisque l'algorithme général (TKIP) est basé sur RC4 comme pour WEP.

Sécurité 6 : WPA2 (2004)

Pourquoi ?

- TKIP est toujours basé sur l'algorithme RC4, donc souffre toujours d'un problème de sécurité.
- WPA2 est l'adaptation de la norme 802.1i.
- Une faille a déjà été découverte dans WPA, par exemple : *WPA Cracker* par l'équipe de tinypeap. (http://www.tinypeap.com/html/wpa_cracker.html)

Qu'apporte WPA2 ?

- L'encryption des données par l'algorithme AES (Advanced Encryption Standard),

Inconvénient : Impossible de mettre à jour les AP, la puissance demandé par cet algorithme est nettement supérieur à RC4, il faut donc changer les équipements.

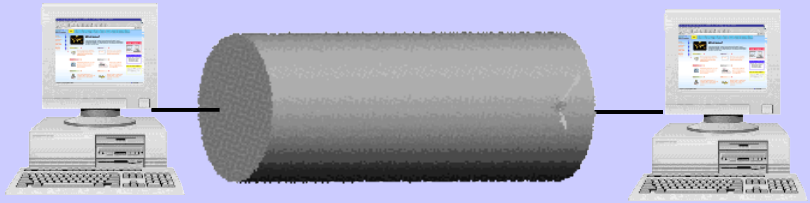
Sécurité 7 : VPN

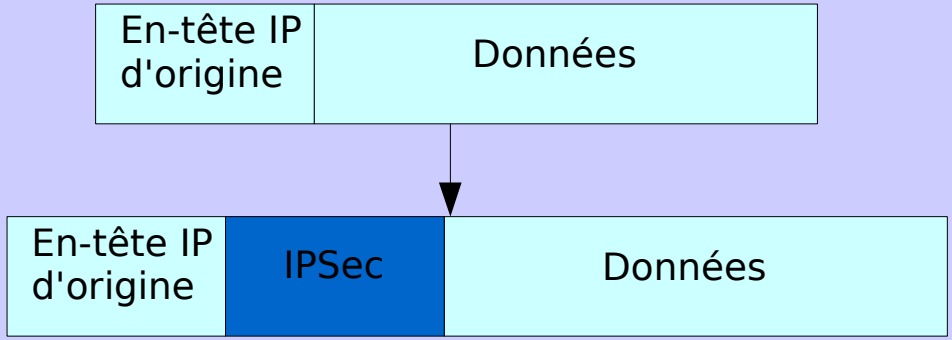
Un VPN (Virtual Private Network) est un moyen permettant de créer une connexion sécurisé sur un réseau quelconque entre deux entités (réseaux, sous réseaux ou utilisateurs individuels). Plusieurs protocoles permettent de le réaliser :
- PPTP de microsoft, niveau 2.
- L2F de CISCO, niveau 2.
- L2TP, niveau 2 et 3.
- IPSEC, niveau 3.

Le plus utilisé étant IPSec.

Sécurité 7 : VPN

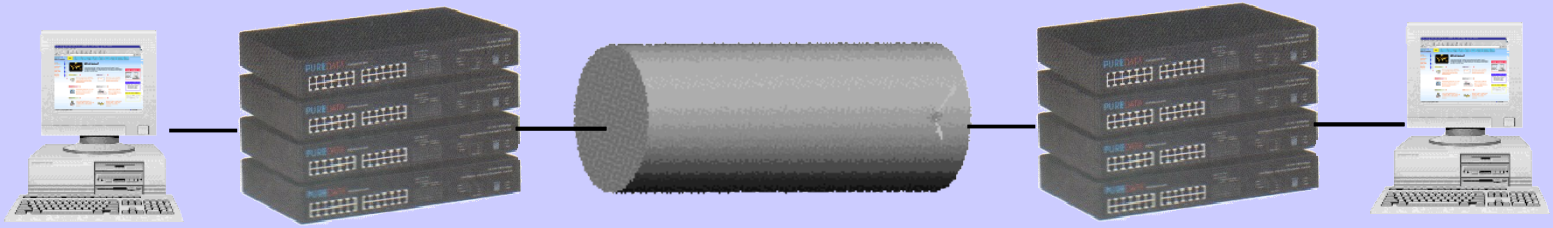
Mode transport : La session est établie entre deux machines, chiffrement de la partie donnée.

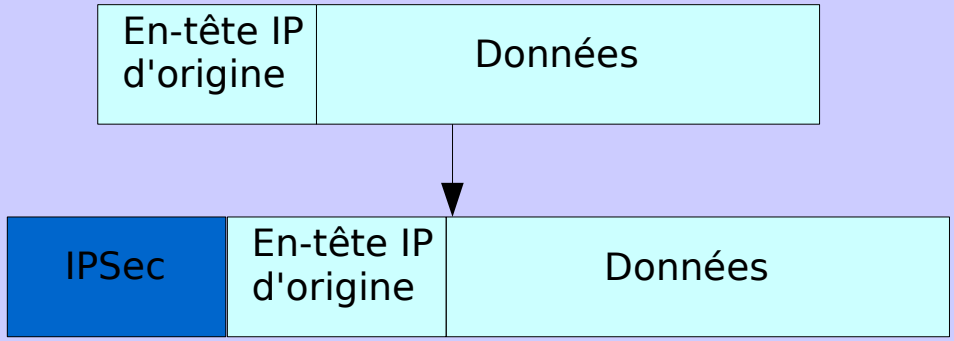




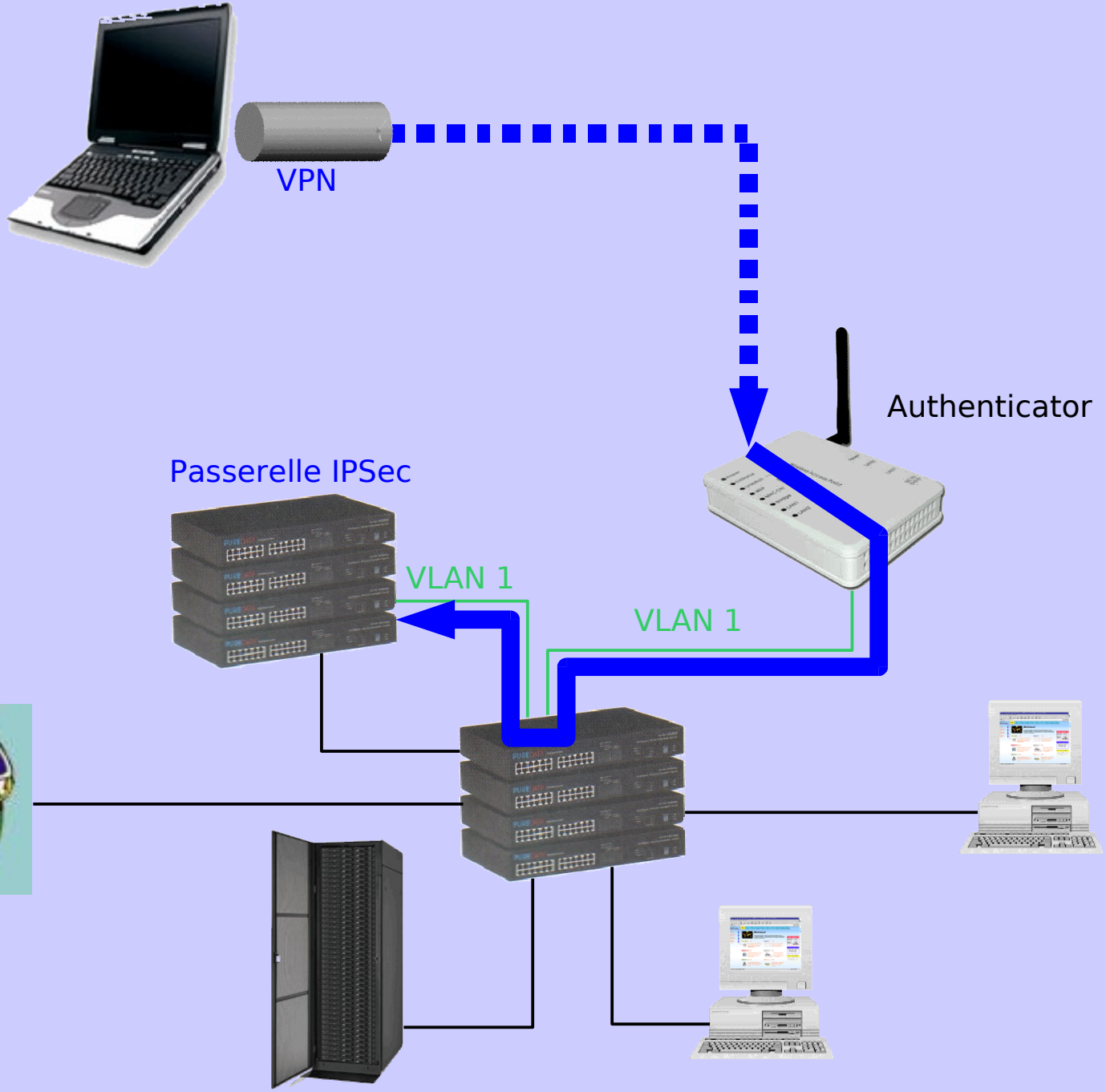
Sécurité 7 : VPN

Mode tunnel : La session est établie entre des ponts ou passerelles.

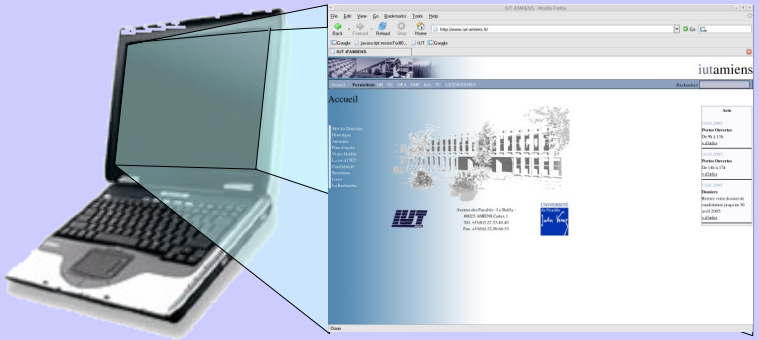




Sécurité 7 : VPN



Sécurité 8 : VPN-SSL



https://www.site.org

Chiffrement ssl

Internet

Bibliographie

http://www.wi-fi.org/
http://www.wireless-fr.org/
http://www.nantes-wireless.org/
http://www.newswireless.net/
http://www.paris-sansfil.fr/
http://airsnort.shmoo.com/
http://wepcrack.sourceforge.net/
http://www.klcconsulting.net/smac/
http://www.kismetwireless.net/
http://www.worldwidewardrive.org/
http://www.wardriving.com/
http://www.seattlewireless.net/index.cgi/WarDrivingSoftware
http://www.netstumbler.com/
http://www.paris-sansfil.fr/