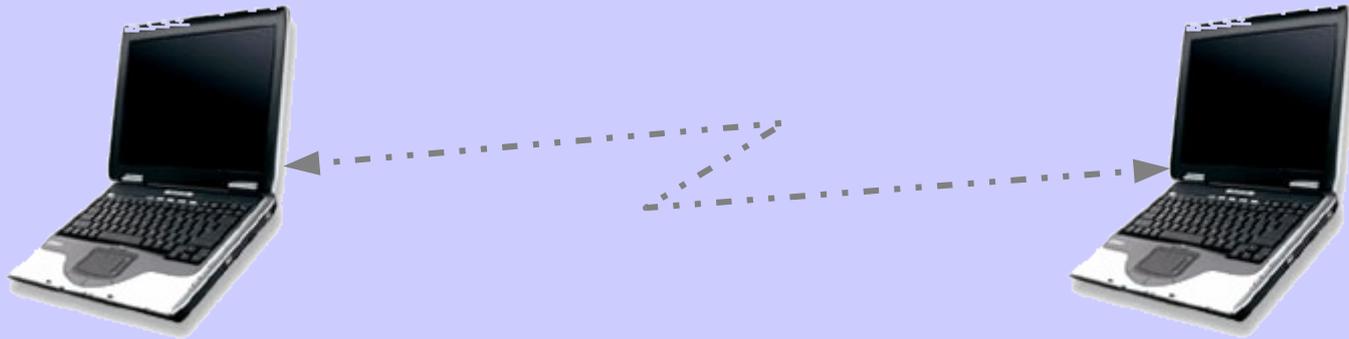


Sécurité des réseaux wi-fi

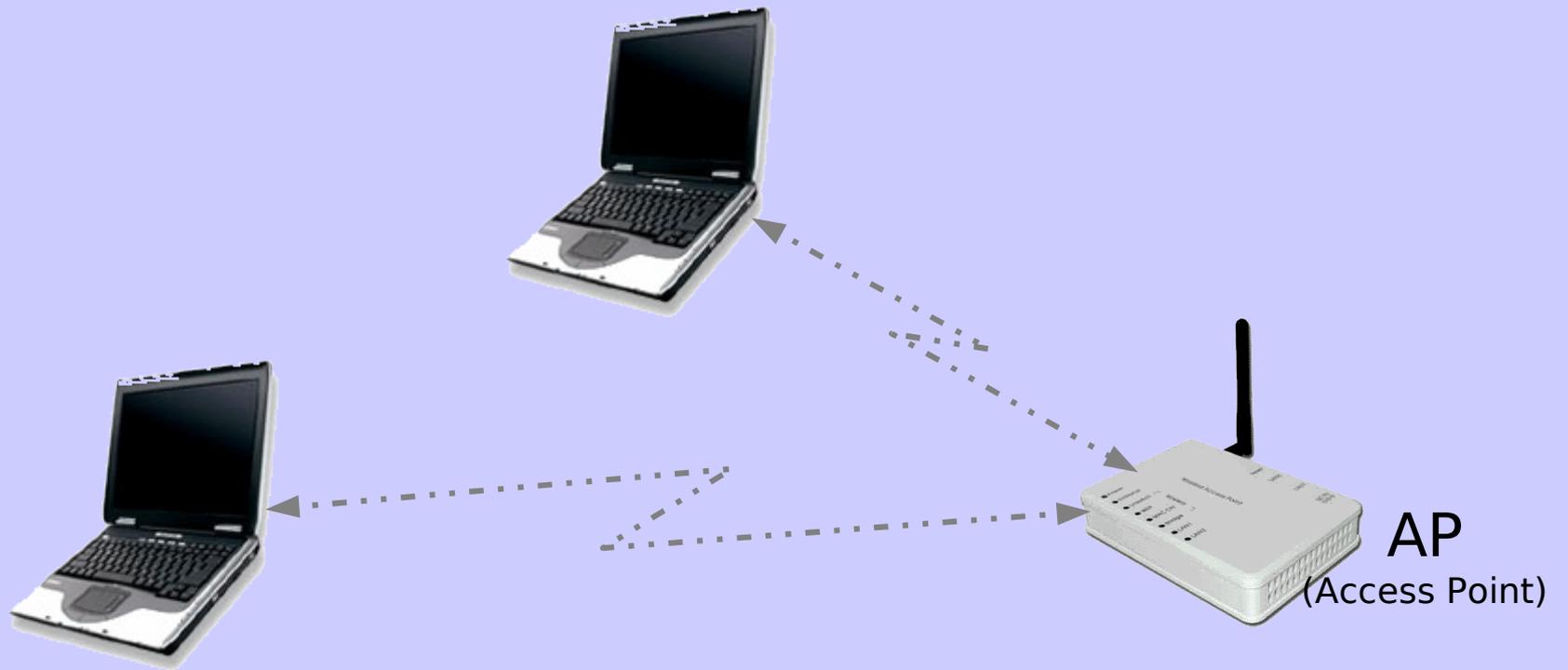
C. Drocourt,
drocourt@iut-amiens.fr

IUT Amiens,
Département Informatique

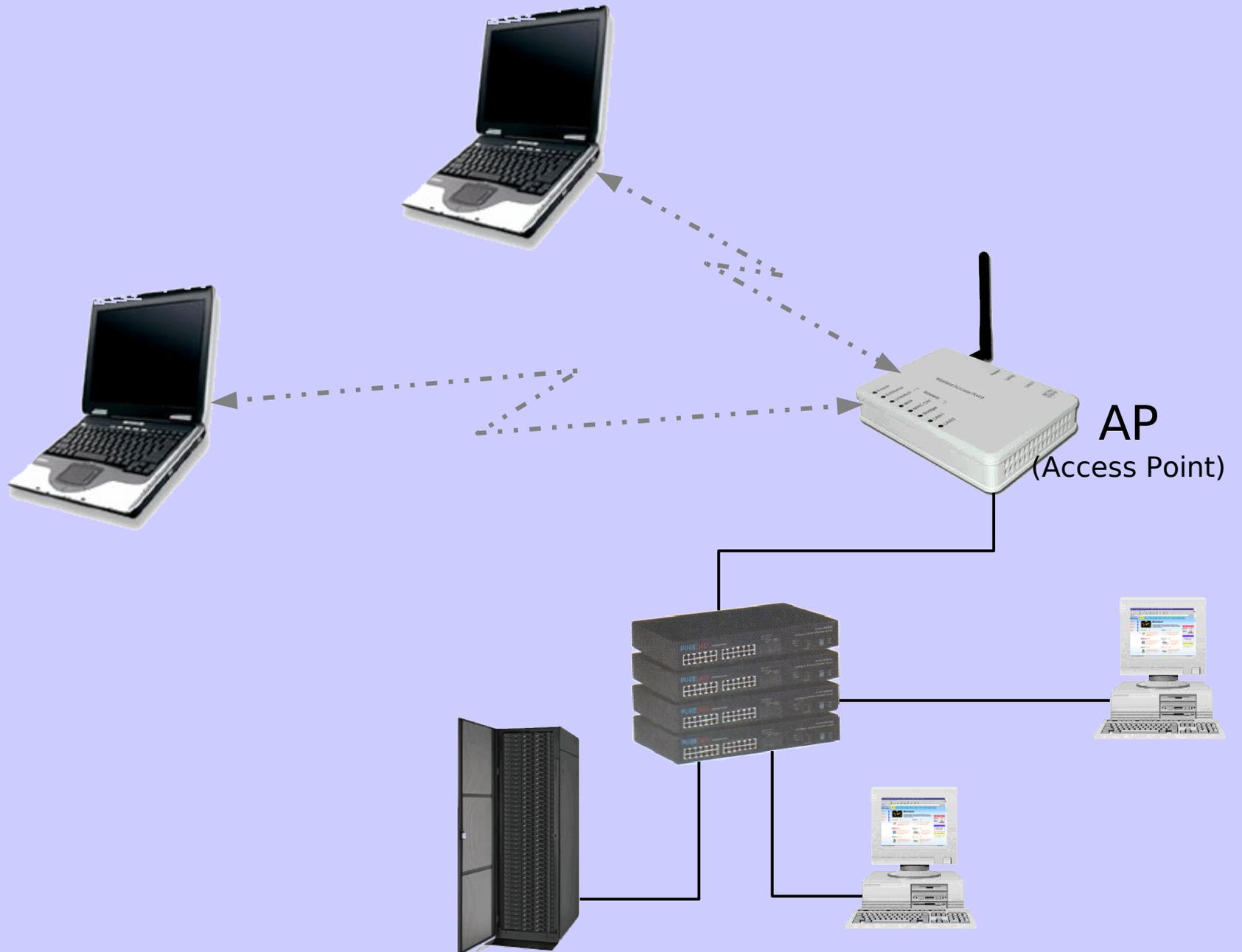
Mode Ad Hoc



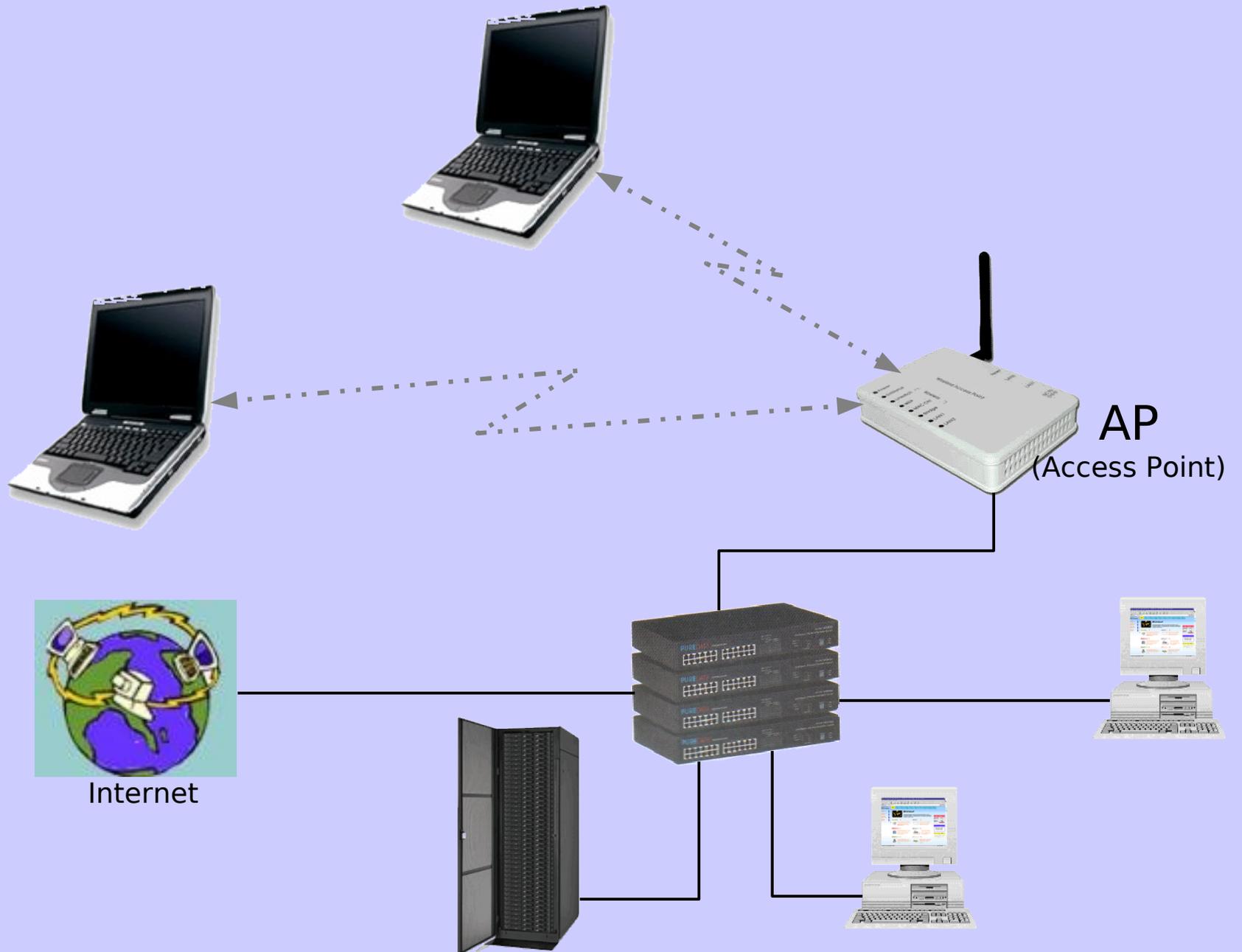
Mode Infrastructure



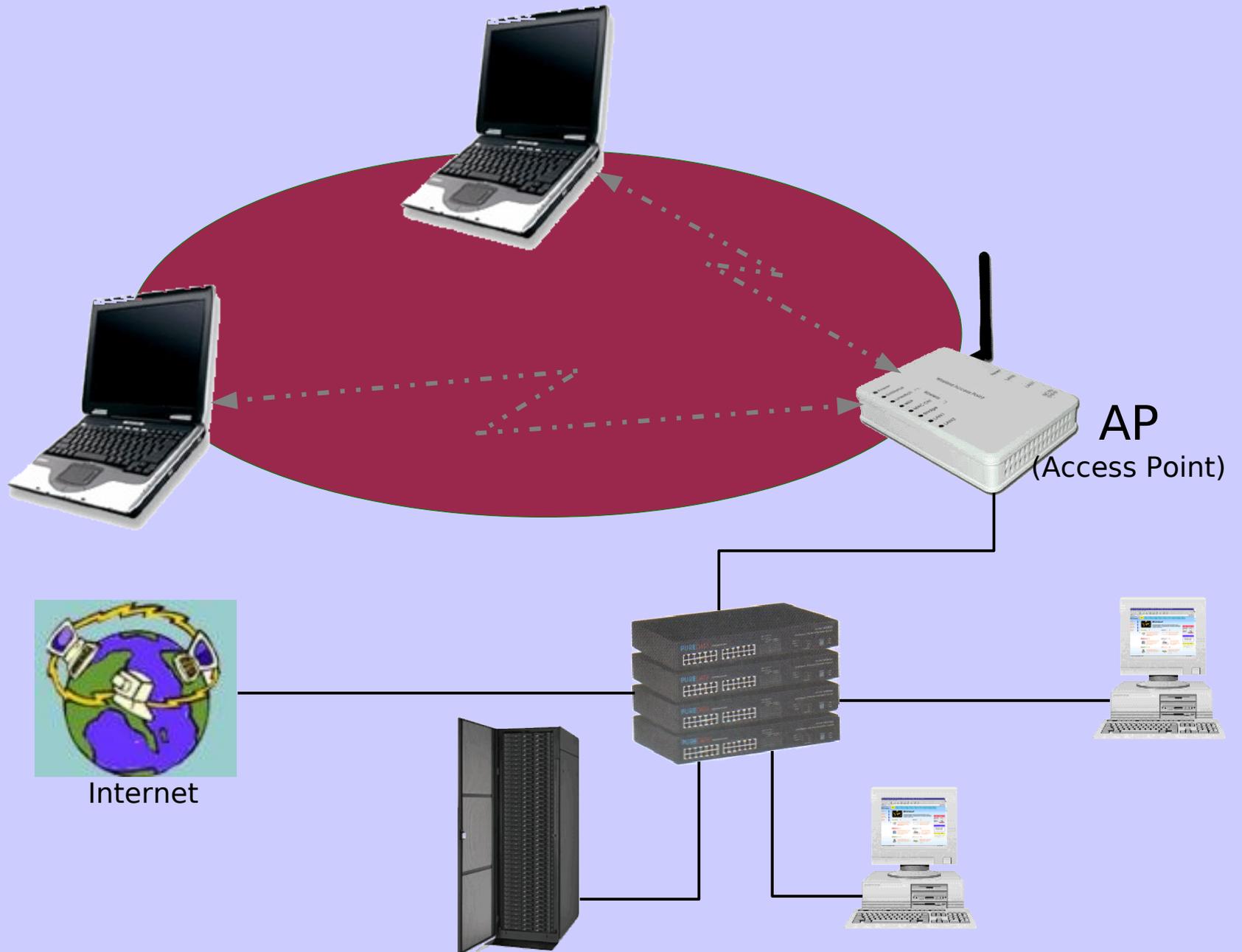
Mode Infrastructure



Mode Infrastructure

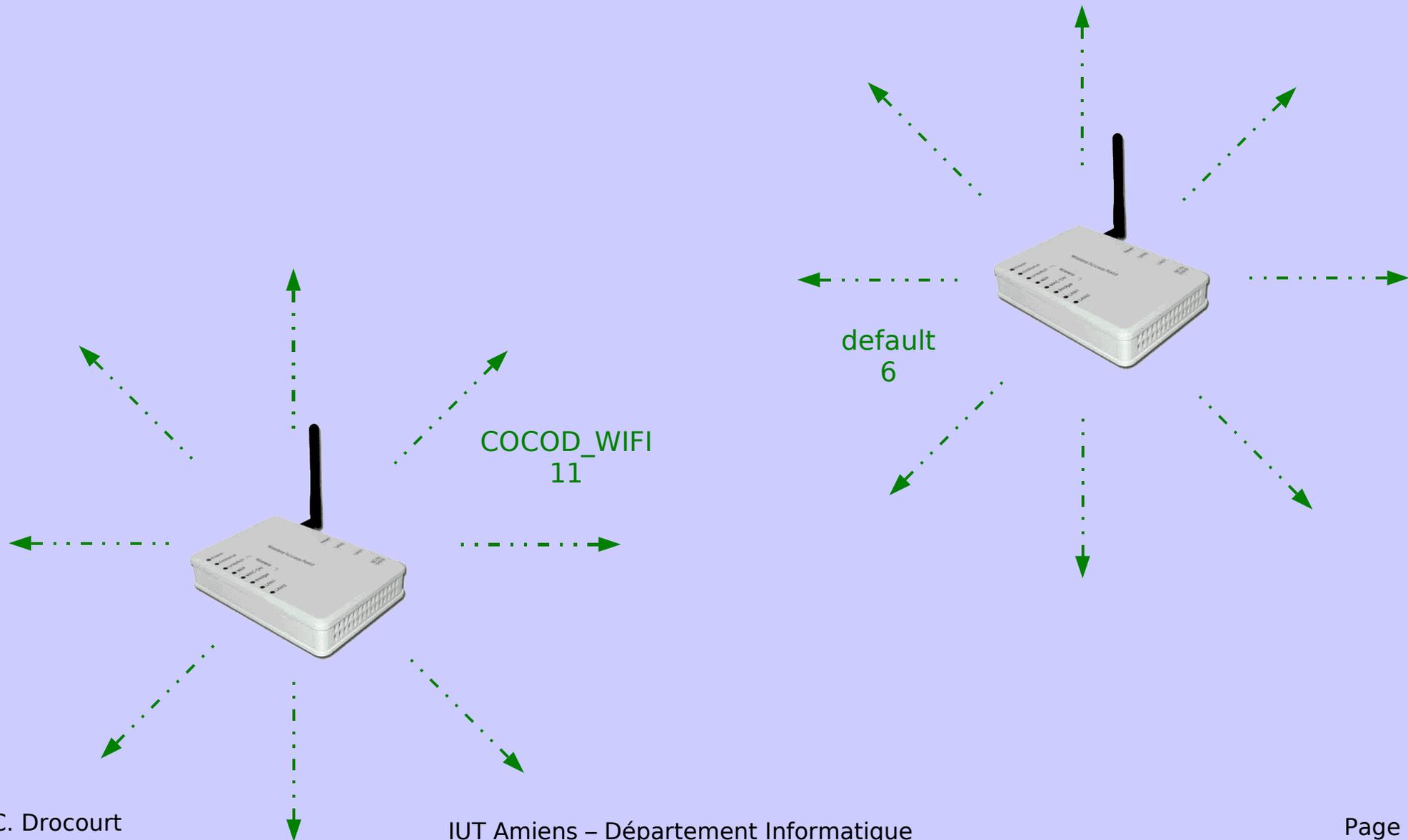


Mode Infrastructure



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).

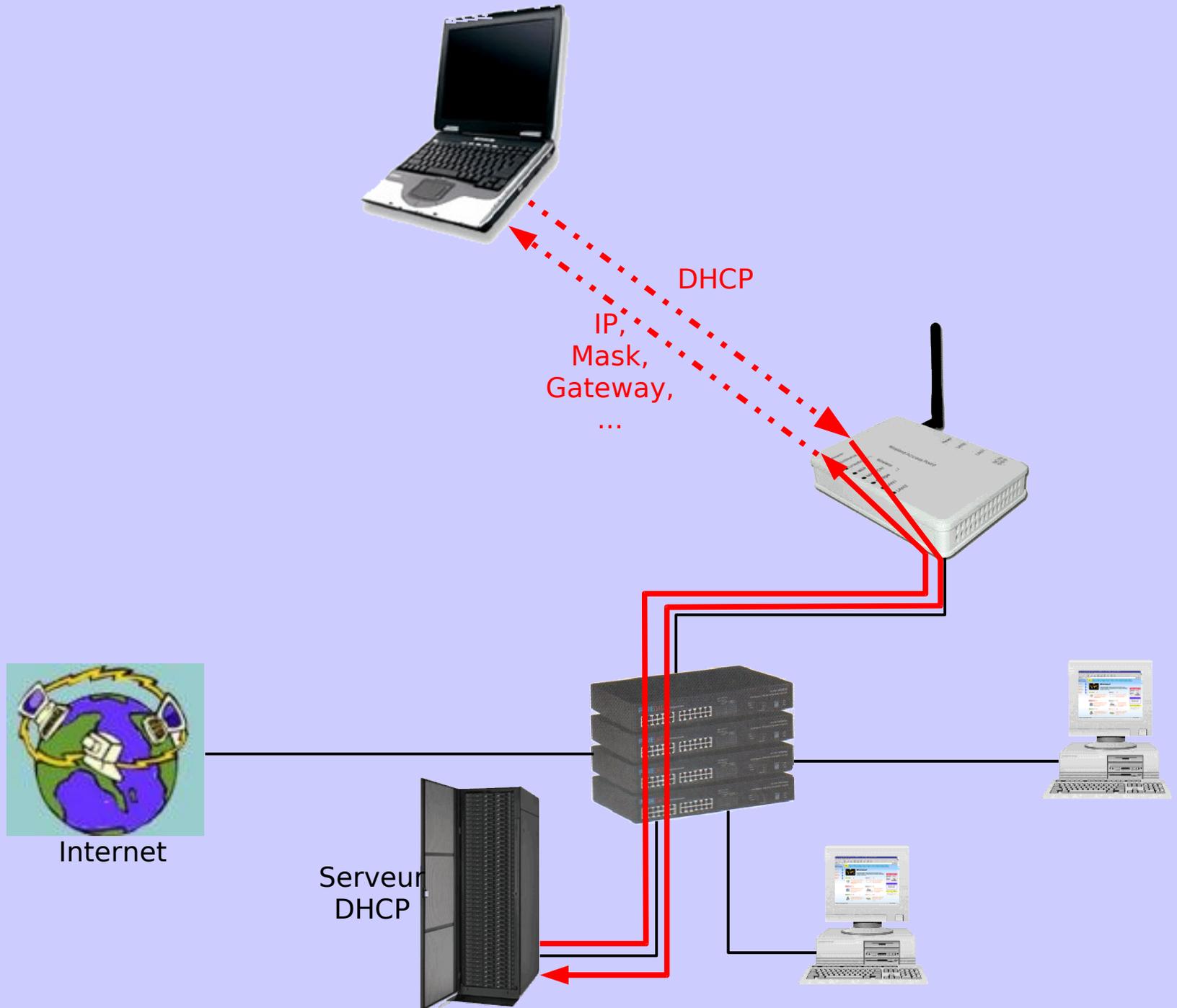


Sans sécurité

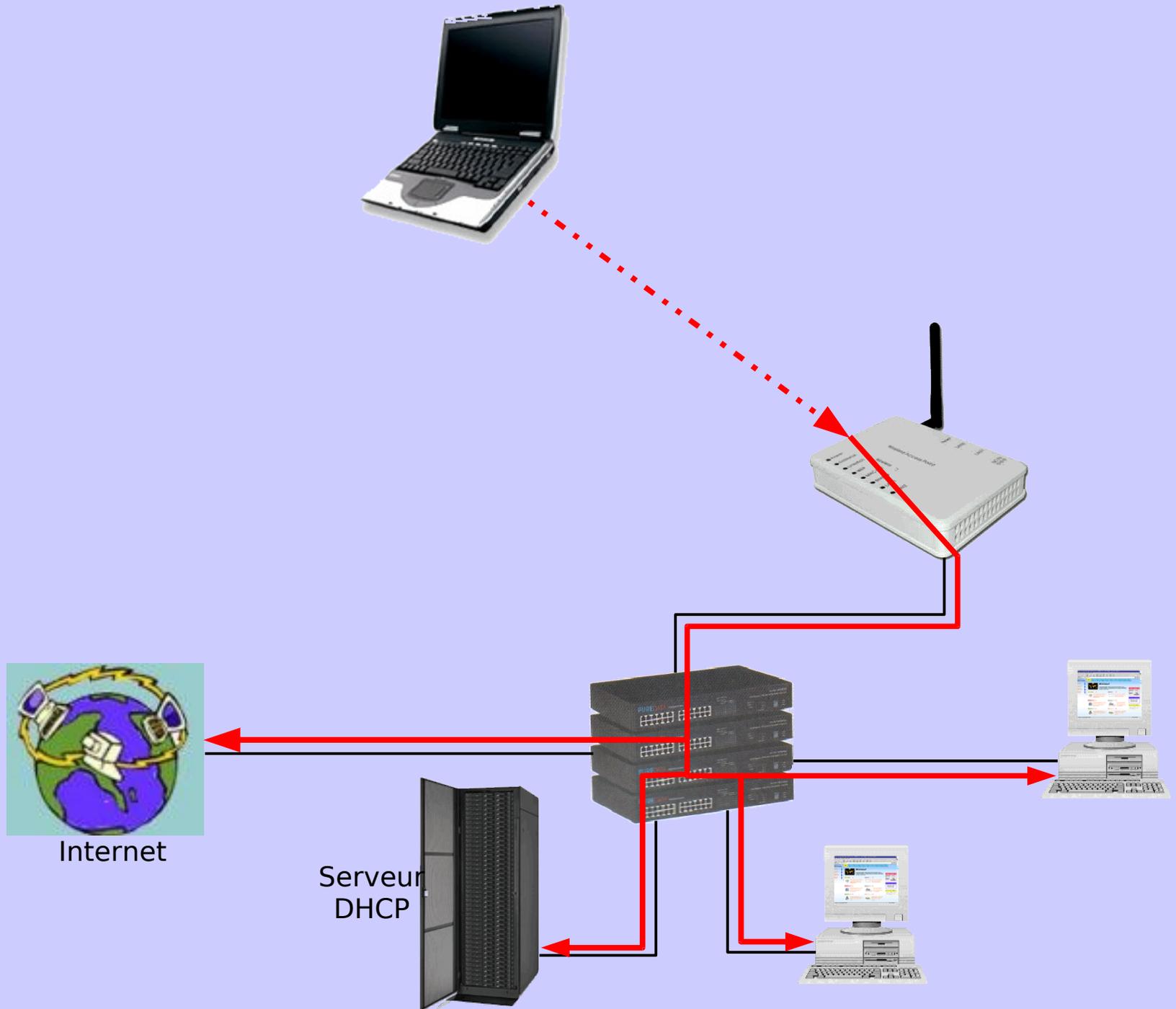


```
[root@machine ~]# iwlist eth1 scanning
eth1      Scan completed :
          Cell 01 - Address: 00:40:05:D0:46:00
                    ESSID:"default"
                    Protocol:IEEE 802.11b
                    Mode:Master
                    Channel:6
                    Encryption key:off
                    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
```

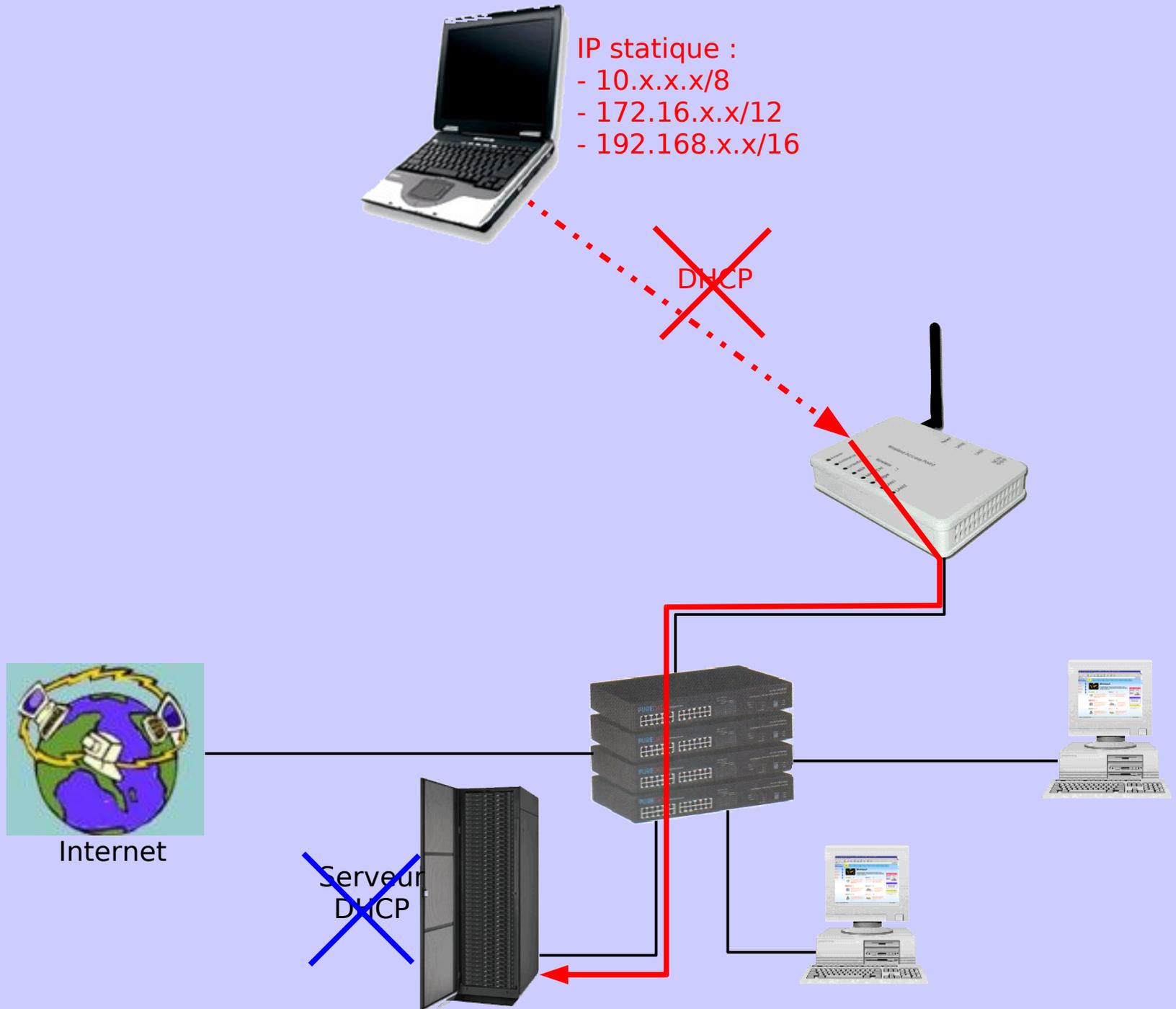
Sans sécurité



Sans sécurité

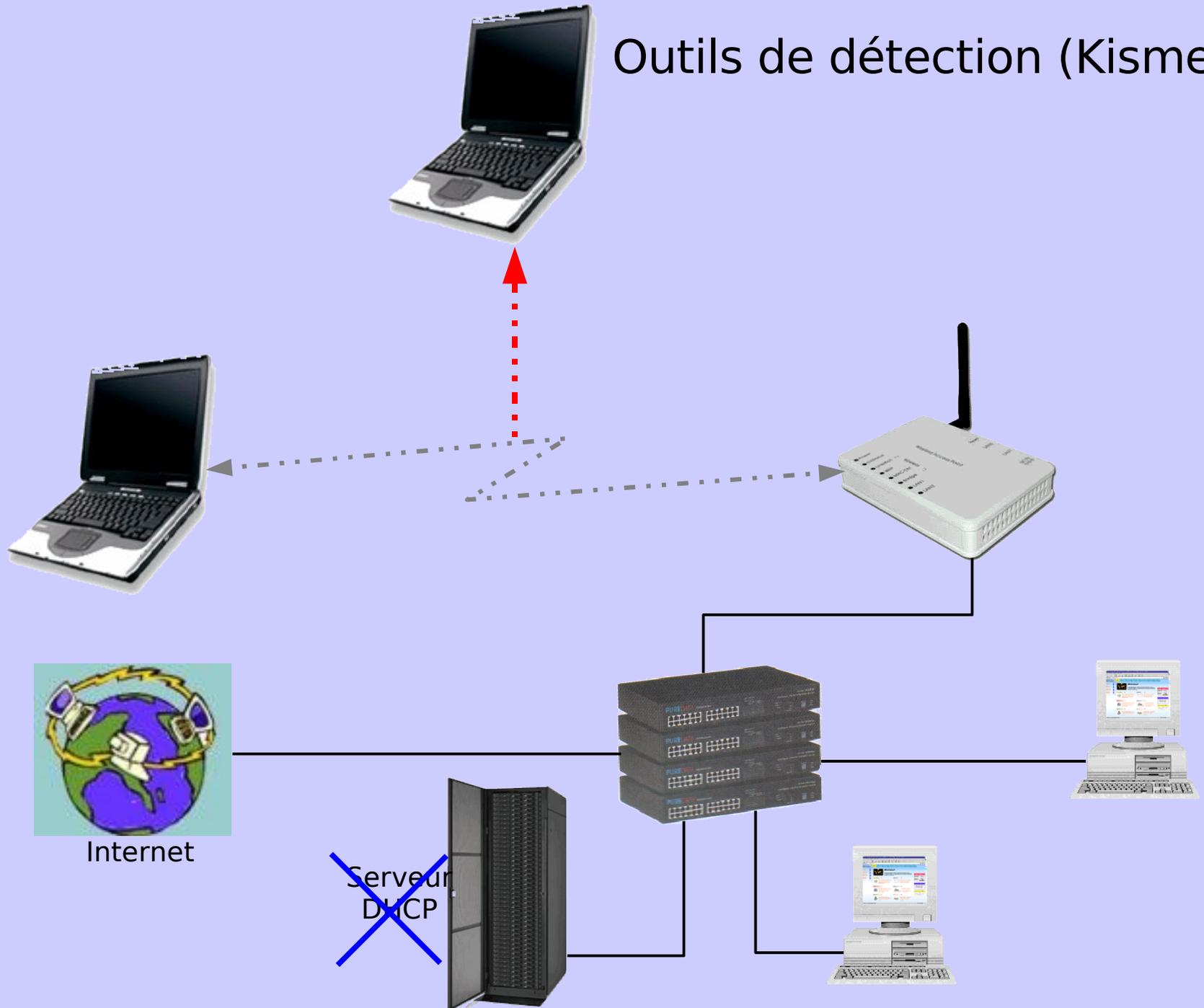


Sécurité 1 : Sans DHCP



Sécurité 1 : Sans DHCP

Outils de détection (Kismet)



Outils de détection

KISMET

```
dragorn@gir.lan.nerv-un.net: /home/dragorn
```

Network List—(Autofit)								Info
Name	T	W	Ch	Pkts	Flags	Data	Clnt	
p@thf1nd3r	A	Y	06	171		70	35	Ntwrks 105
<no ssid>	A	N	05	1		0	0	Pkts 1258
KrullNet1	A	Y	06	27		0	0	Cryptd 104
linksys	A	N	06	81	FU4	8	2	Weak 0
marley	A	N	06	312		17	1	Noise 289
<no ssid>	D	N	--	20	A2	20	18	Discrd 289
! PARMAS	A	N	07	30		0	0	Pkts/s 50
<no ssid>	A	Y	06	1		0	0	
GRXWirelessNetwork	A	Y	06	2		0	0	
! SECMAS	A	N	07	13		0	0	
<no ssid>	D	N	--	1	A4	1	66	
! <Lucent Outdoor Router>	0	N	--	267		267	1	

Elapsd
000027

Status
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP
Found IP 159.139.120.13 for <no ssid>::00:B0:D0:DE:60:E3 via TCP

Battery: AC charging 100% 0h0m0s

<http://www.kismetwireless.net/>

Outils de détection

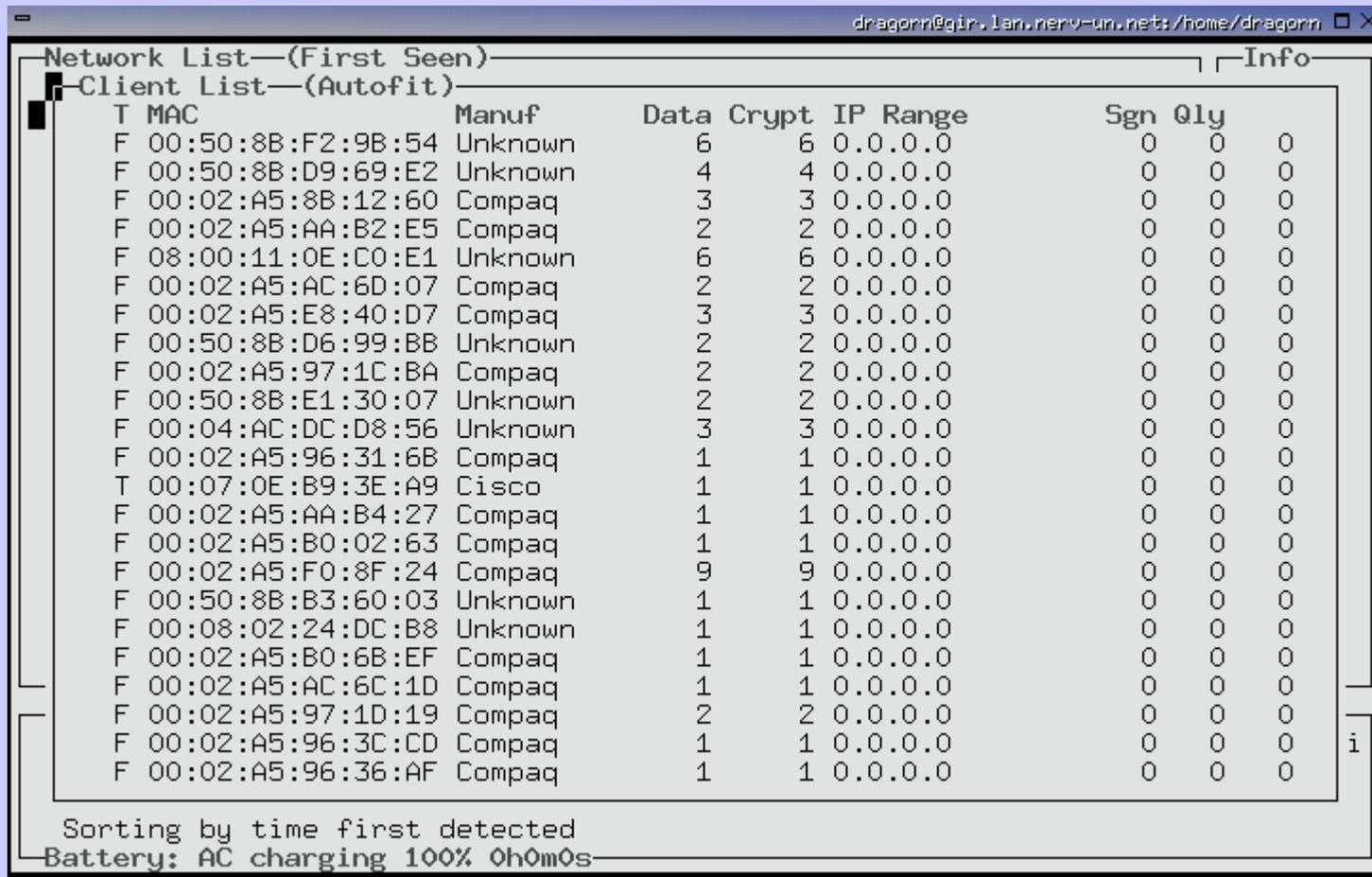
KISMET

```
dragorn@gir.lan.nerv-un.net: /home/dragorn
Network List—(First Seen)—
Network Details
  SSID      : linksys
  Server   : localhost:2501
  BSSID    : 00:04:5A:ED:40:DB
  Manuf    : Linksys
  Model    : Unknown
  Matched  : 00:04:5A:00:00:00
            FACTORY CONFIGURATION
  Max Rate: 11.0
  First    : Fri Nov  8 03:19:37 2002
  Latest   : Fri Nov  8 03:19:38 2002
  Clients  : 2
  Type     : Access Point (infrastructure)
  Channel  : 6
  WEP      : No
  Beacon   : 100 (0.102400 sec)
  Packets  : 81
    Data   : 8
    LLC    : 73
    Crypt  : 0
    Weak   : 0
  Signal   :
    Quality : 0 (best 0)
    Power   : 0 (best 0)
    Noise   : 0 (best 0)
Sorting client display by time first detected
Battery: AC charging 100% 0h0m0s
```

<http://www.kismetwireless.net/>

Outils de détection

KISMET



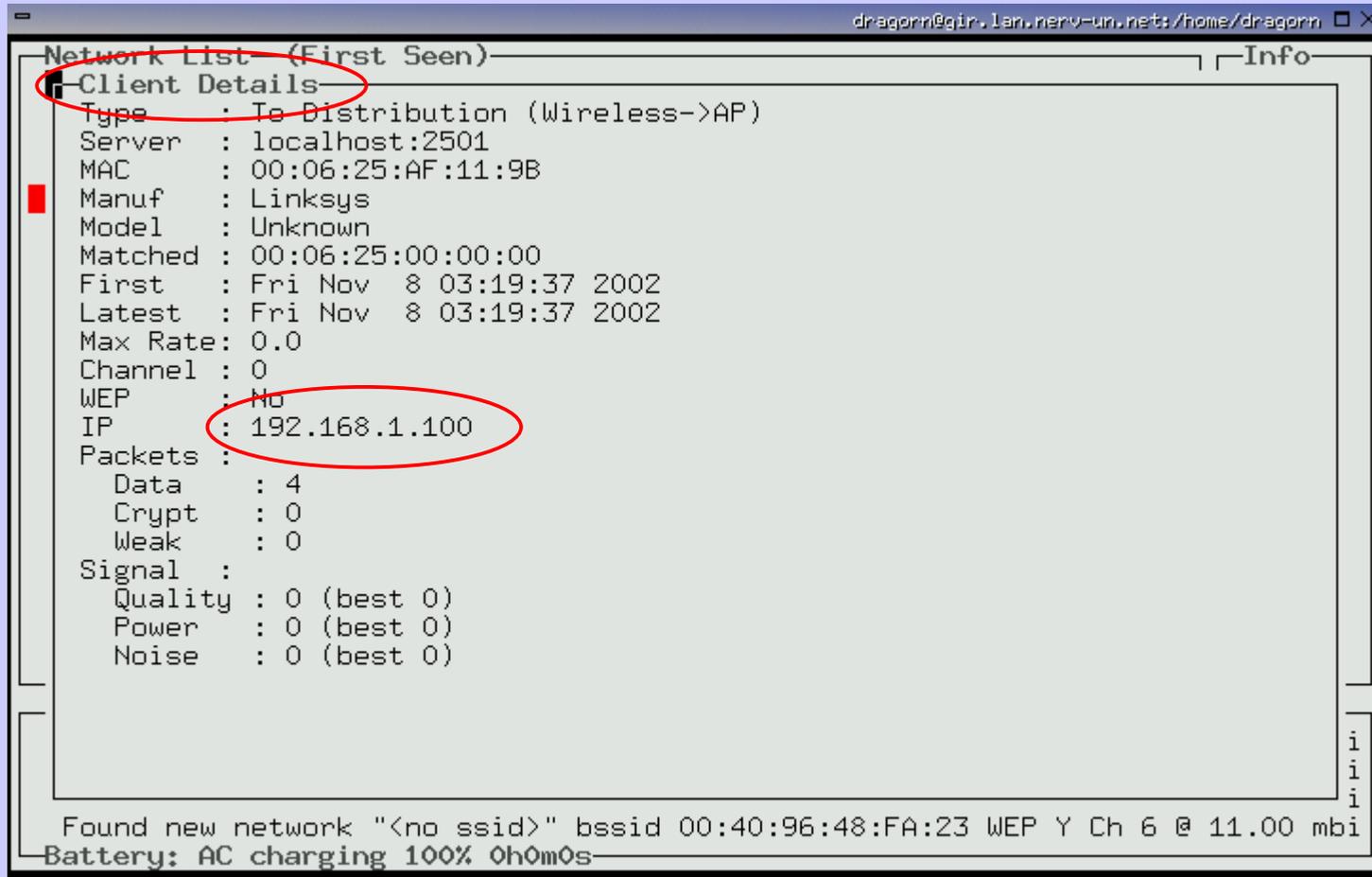
The screenshot shows the Kismet application window with the title bar 'dragorn@gir.lan.nerv-un.net: /home/dragorn'. The main content area is titled 'Client List (Autofit)' and displays a table of detected wireless clients. The table has columns for 'T' (Type), 'MAC', 'Manuf' (Manufacturer), 'Data' (Data rate), 'Crypt' (Encryption), 'IP Range', 'Sgn' (Signal strength), and 'Qly' (Quality). The clients are sorted by time first detected. At the bottom of the window, it shows 'Sorting by time first detected' and 'Battery: AC charging 100% 0h0m0s'.

T	MAC	Manuf	Data	Crypt	IP Range	Sgn	Qly
F	00:50:8B:F2:9B:54	Unknown	6	6	0.0.0.0	0	0
F	00:50:8B:D9:69:E2	Unknown	4	4	0.0.0.0	0	0
F	00:02:A5:8B:12:60	Compaq	3	3	0.0.0.0	0	0
F	00:02:A5:AA:B2:E5	Compaq	2	2	0.0.0.0	0	0
F	08:00:11:0E:C0:E1	Unknown	6	6	0.0.0.0	0	0
F	00:02:A5:AC:6D:07	Compaq	2	2	0.0.0.0	0	0
F	00:02:A5:E8:40:D7	Compaq	3	3	0.0.0.0	0	0
F	00:50:8B:D6:99:BB	Unknown	2	2	0.0.0.0	0	0
F	00:02:A5:97:1C:BA	Compaq	2	2	0.0.0.0	0	0
F	00:50:8B:E1:30:07	Unknown	2	2	0.0.0.0	0	0
F	00:04:AC:DC:D8:56	Unknown	3	3	0.0.0.0	0	0
F	00:02:A5:96:31:6B	Compaq	1	1	0.0.0.0	0	0
T	00:07:0E:B9:3E:A9	Cisco	1	1	0.0.0.0	0	0
F	00:02:A5:AA:B4:27	Compaq	1	1	0.0.0.0	0	0
F	00:02:A5:B0:02:63	Compaq	1	1	0.0.0.0	0	0
F	00:02:A5:F0:8F:24	Compaq	9	9	0.0.0.0	0	0
F	00:50:8B:B3:60:03	Unknown	1	1	0.0.0.0	0	0
F	00:08:02:24:DC:B8	Unknown	1	1	0.0.0.0	0	0
F	00:02:A5:B0:6B:EF	Compaq	1	1	0.0.0.0	0	0
F	00:02:A5:AC:6C:1D	Compaq	1	1	0.0.0.0	0	0
F	00:02:A5:97:1D:19	Compaq	2	2	0.0.0.0	0	0
F	00:02:A5:96:3C:CD	Compaq	1	1	0.0.0.0	0	0
F	00:02:A5:96:36:AF	Compaq	1	1	0.0.0.0	0	0

<http://www.kismetwireless.net/>

Outils de détection

KISMET

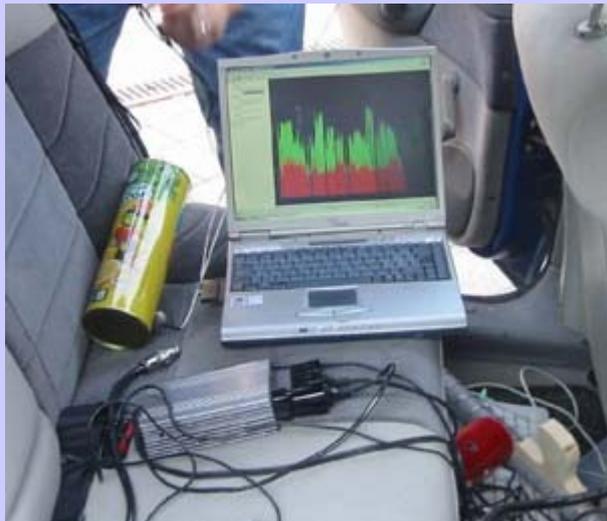


```
dragorn@gir.lan.nerv-un.net: /home/dragorn
Network List (First Seen)
Client Details
Type : To Distribution (Wireless->AP)
Server : localhost:2501
MAC : 00:06:25:AF:11:9B
Manuf : Linksys
Model : Unknown
Matched : 00:06:25:00:00:00
First : Fri Nov 8 03:19:37 2002
Latest : Fri Nov 8 03:19:37 2002
Max Rate: 0.0
Channel : 0
WEP : No
IP : 192.168.1.100
Packets :
  Data : 4
  Crypt : 0
  Weak : 0
Signal :
  Quality : 0 (best 0)
  Power : 0 (best 0)
  Noise : 0 (best 0)
Found new network "<no ssid>" bssid 00:40:96:48:FA:23 WEP Y Ch 6 @ 11.00 mbi
Battery: AC charging 100% 0h0m0s
```

<http://www.kismetwireless.net/>

Outils de détection

WarDriving...

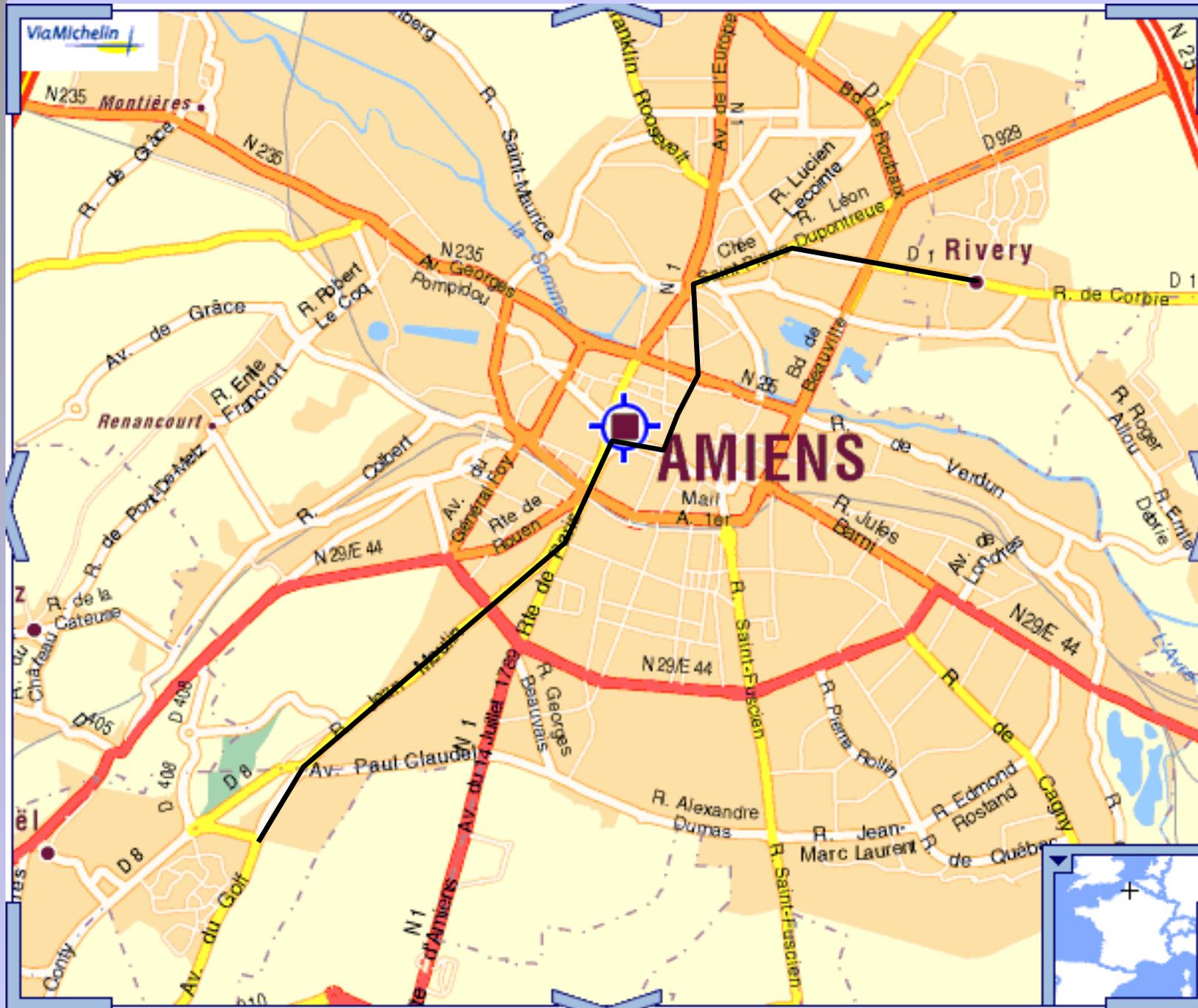


<http://www.worldwidewardrive.org/>

<http://www.wardriving.com/>

<http://www.seattlewireless.net/index.cgi/WarDrivingSoftware>

Outils de détection



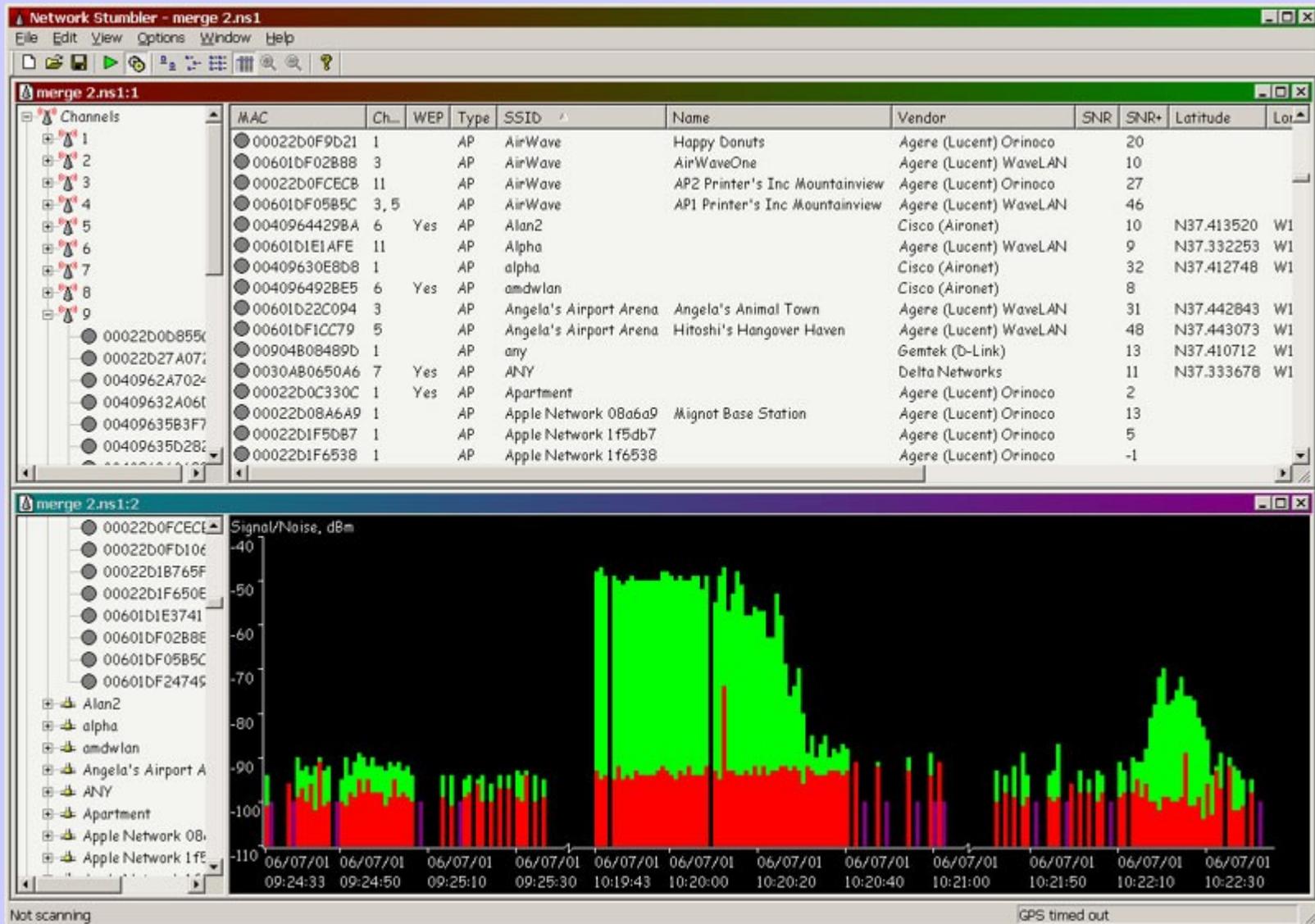
Distance :
7 km

Bornes :
123

Non cryptés :
31
(25%)

Outils de détection

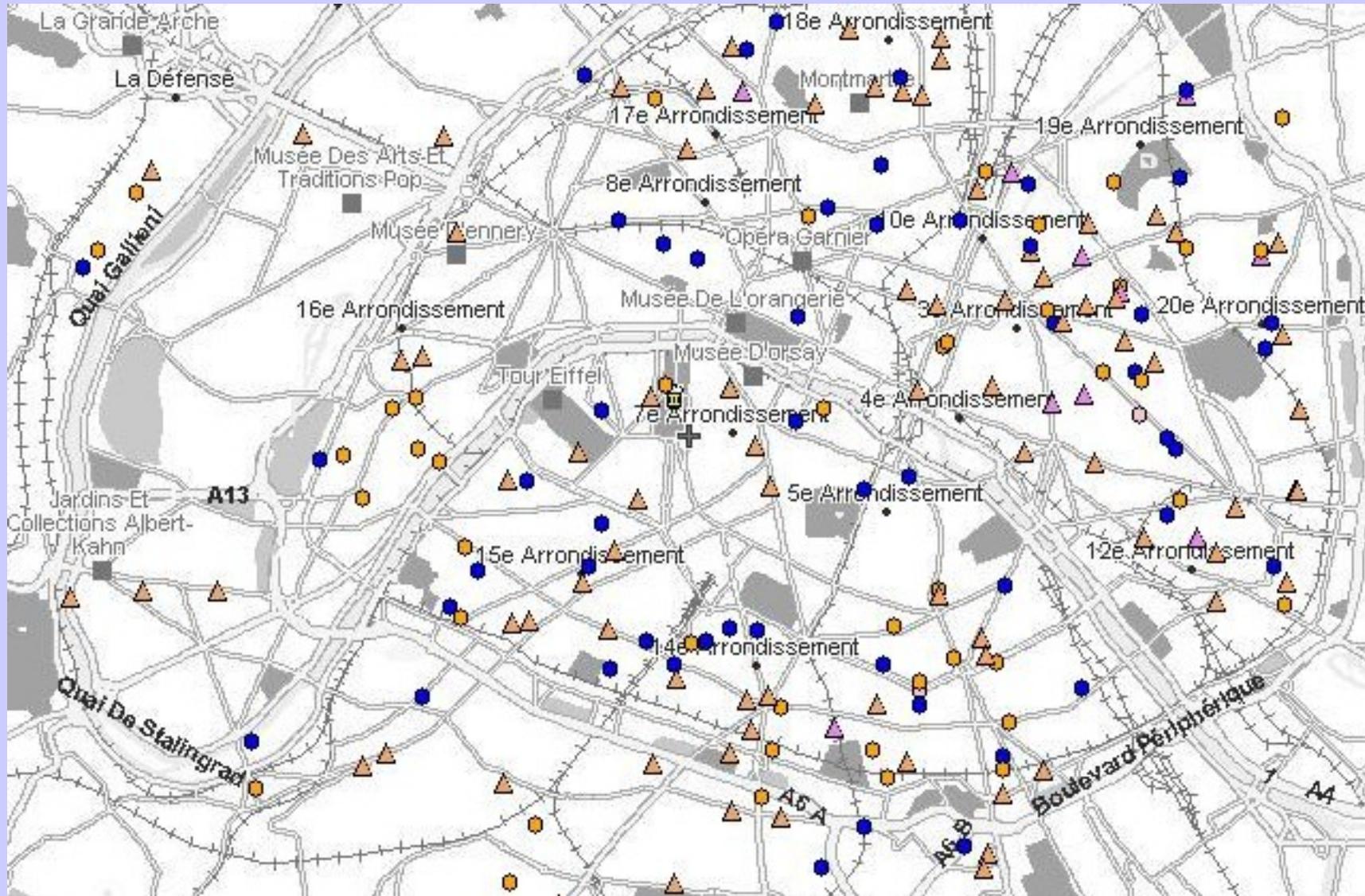
WarDriving...



<http://www.netstumbler.com/>

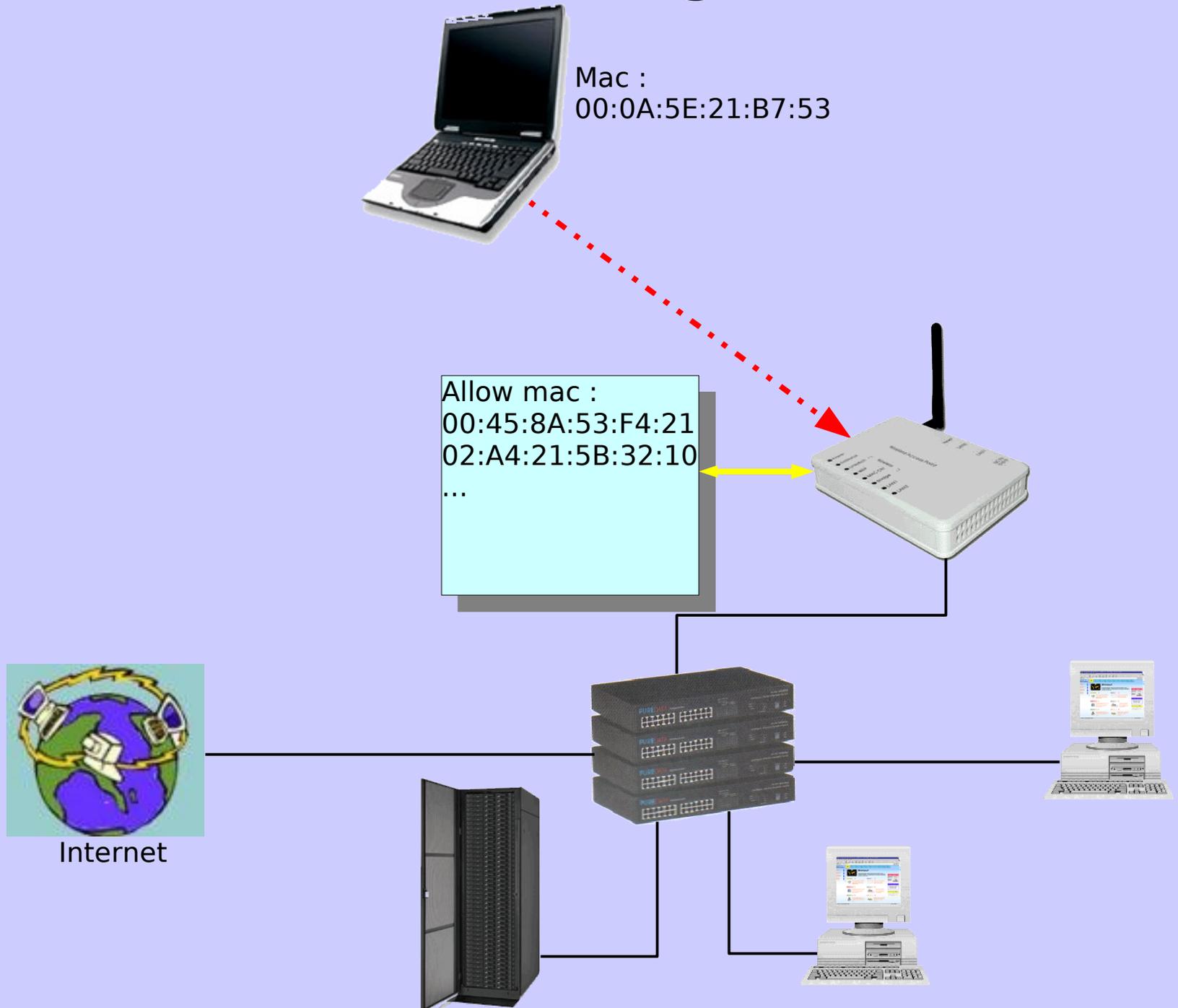
Outils de détection

WarDriving...

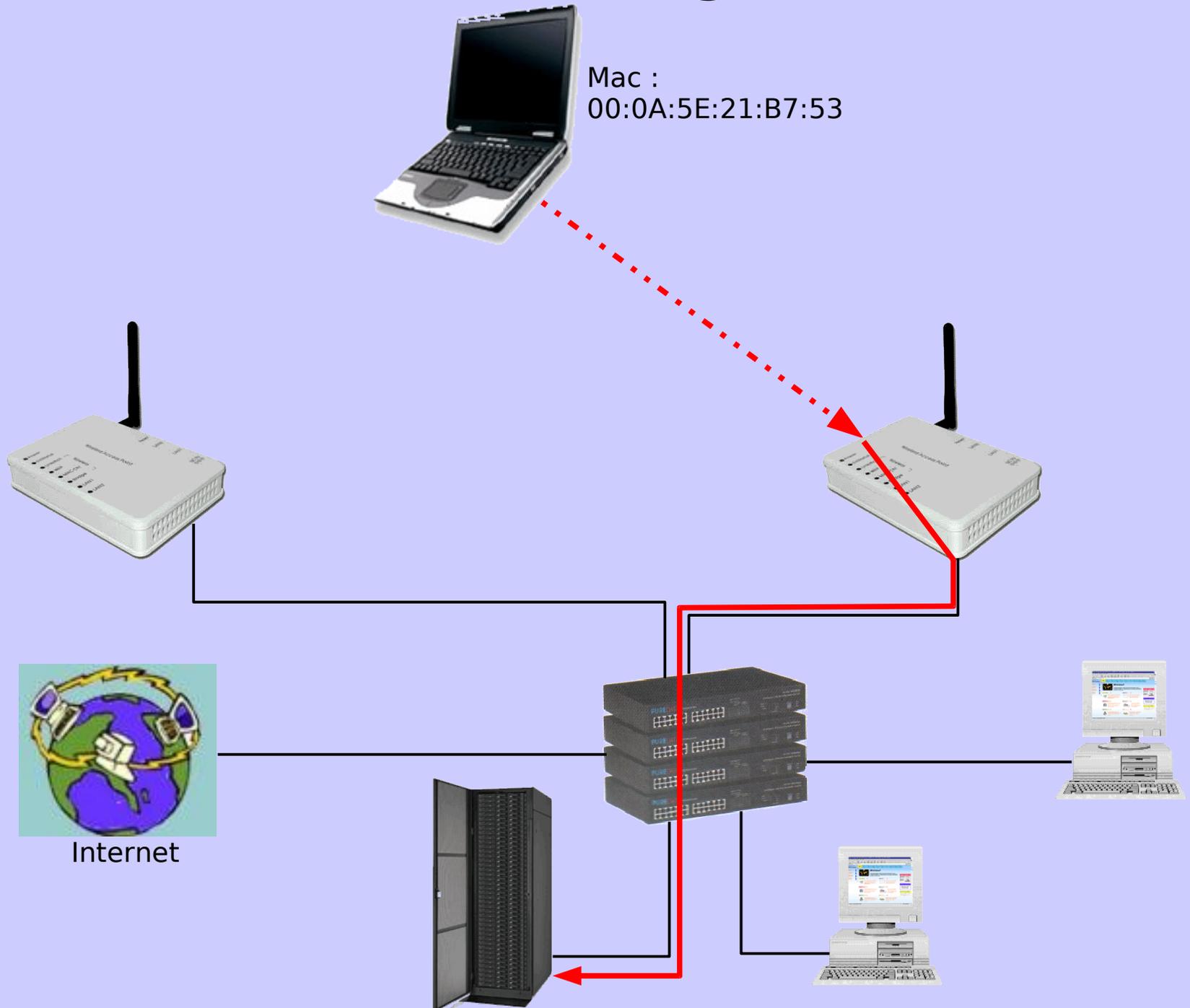


<http://www.paris-sansfil.fr/>

Sécurité 2 : Filtrage MAC



Sécurité 2 : Filtrage MAC



Sécurité 2 : Filtrage MAC

The top screenshot displays a 'Client List' window with the following data:

T	MAC	Manuf	Data	Crypt	IP Range	Sgn	Qly
F	00:50:8B:F2:9B:54	Unknown	6	6	0.0.0.0	0	0
F	00:50:8B:D9:69:E2	Unknown	4	4	0.0.0.0	0	0
F	00:02:A5:8B:12:60	Compaq	3	3	0.0.0.0	0	0
F	00:02:A5:AA:B2:E5	Compaq	2	2	0.0.0.0	0	0
F	08:00:11:0E:C0:E1	Unknown	6	6	0.0.0.0	0	0
F	00:02:A5:AC:6D:07	Compaq	2	2	0.0.0.0	0	0
F	00:02:A5:E8:40:D7	Compaq	3	3	0.0.0.0	0	0
F	00:50:8B:D6:99:BB	Unknown	2	2	0.0.0.0	0	0
F	00:02:A5:97:1C:BA	Compaq	2	2	0.0.0.0	0	0
F	00:50:8B:E1:30:07	Unknown	2	2	0.0.0.0	0	0

The bottom screenshot shows 'Client Details' for the MAC address 00:06:25:AF:11:9B:

- Type : To Distribution (Wireless->AP)
- Server : localhost:2501
- MAC : 00:06:25:AF:11:9B
- Manuf : Linksys
- Model : Unknown
- Matched : 00:06:25:00:00:00
- First : Fri Nov 8 03:19:37 2002
- Latest : Fri Nov 8 03:19:37 2002
- Max Rate : 0.0
- Channel : 0
- WEP : No
- IP : 192.168.1.100
- Packets :
 - Data : 4
 - Crypt : 0
 - Weak : 0
- Signal :
 - Quality : 0 (best 0)
 - Power : 0 (best 0)
 - Noise : 0 (best 0)

Found new network "<no ssid>" bssid 00:40:96:48:FA:23 WEP Y Ch 6 @ 11.00 mbi

Sécurité 2 : Filtrage MAC

SMAC 1.2 [WBEM On]

File About

ID	Active	Spoofed	Network Adapter	IP Address	Active MAC
0001	Yes	Yes	Intel 8255x-based PCI Ethernet ...	0.0.0.0	00-0C-0A-BE-23-35
0013	Yes	Yes	Siemens SpeedStream CardBus ...	192.168.0.162	00-0C-0C-34-42-A3

Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 0C - 0A - BE - 23 - 35

Buttons: Update MAC, Refresh, Remove MAC, Exit

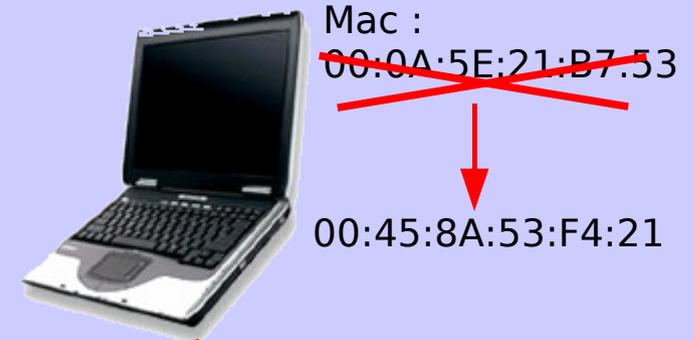
Spoofed MAC Address: 00-0C-0A-BE-23-35

Active MAC Address: 00-0C-0A-BE-23-35

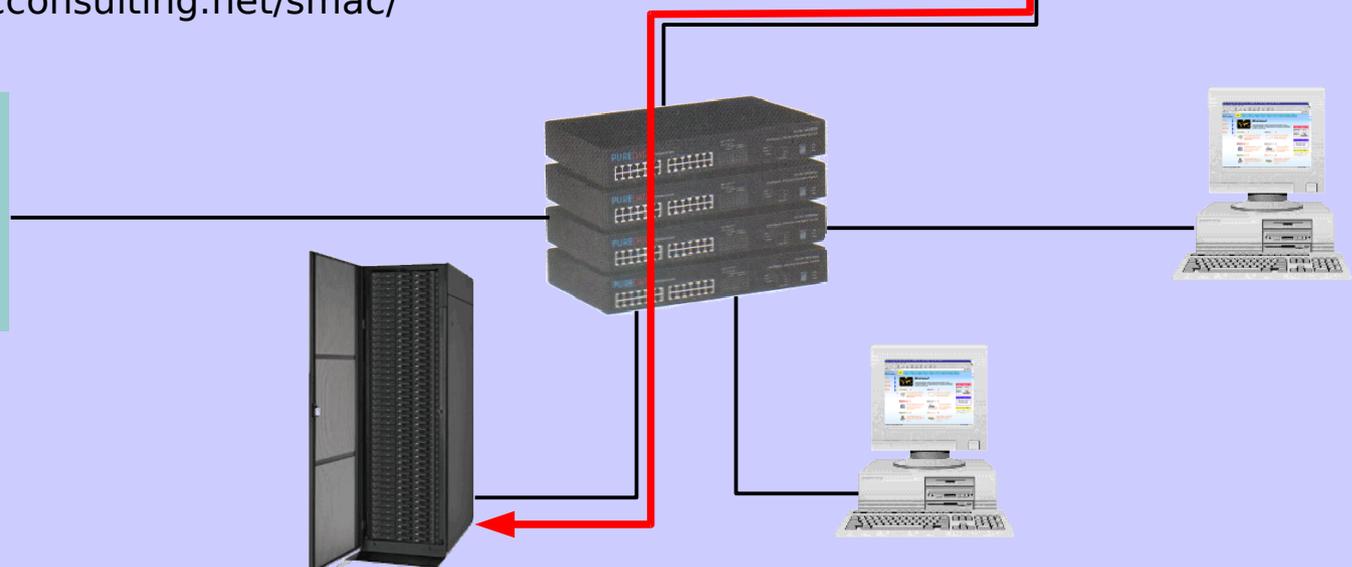
KLC CONSULTING, INC
www.klccconsulting.net/smac

Disclaimer: Use this program at your own risk. We are not responsible for any damage that might occur to your system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with this disclaimer.

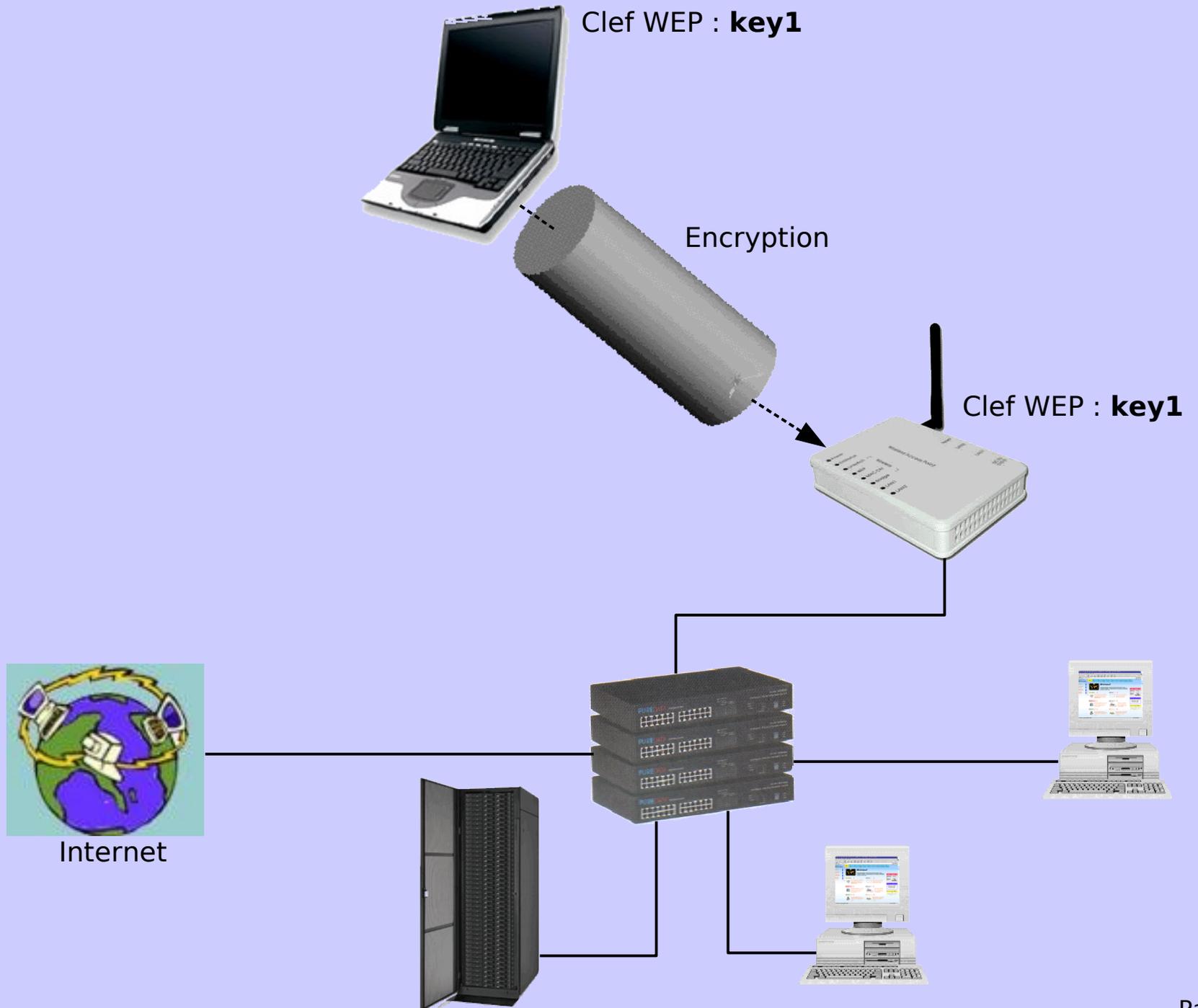
<http://www.klccconsulting.net/smac/>



Internet



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



Problème 2 : Confidentialité de la clef

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 $2^{24} = 16,8$ millions de trames -> Possible en peu de temps suivant le débit.

airsnort : <http://airsnort.shmoo.com/>

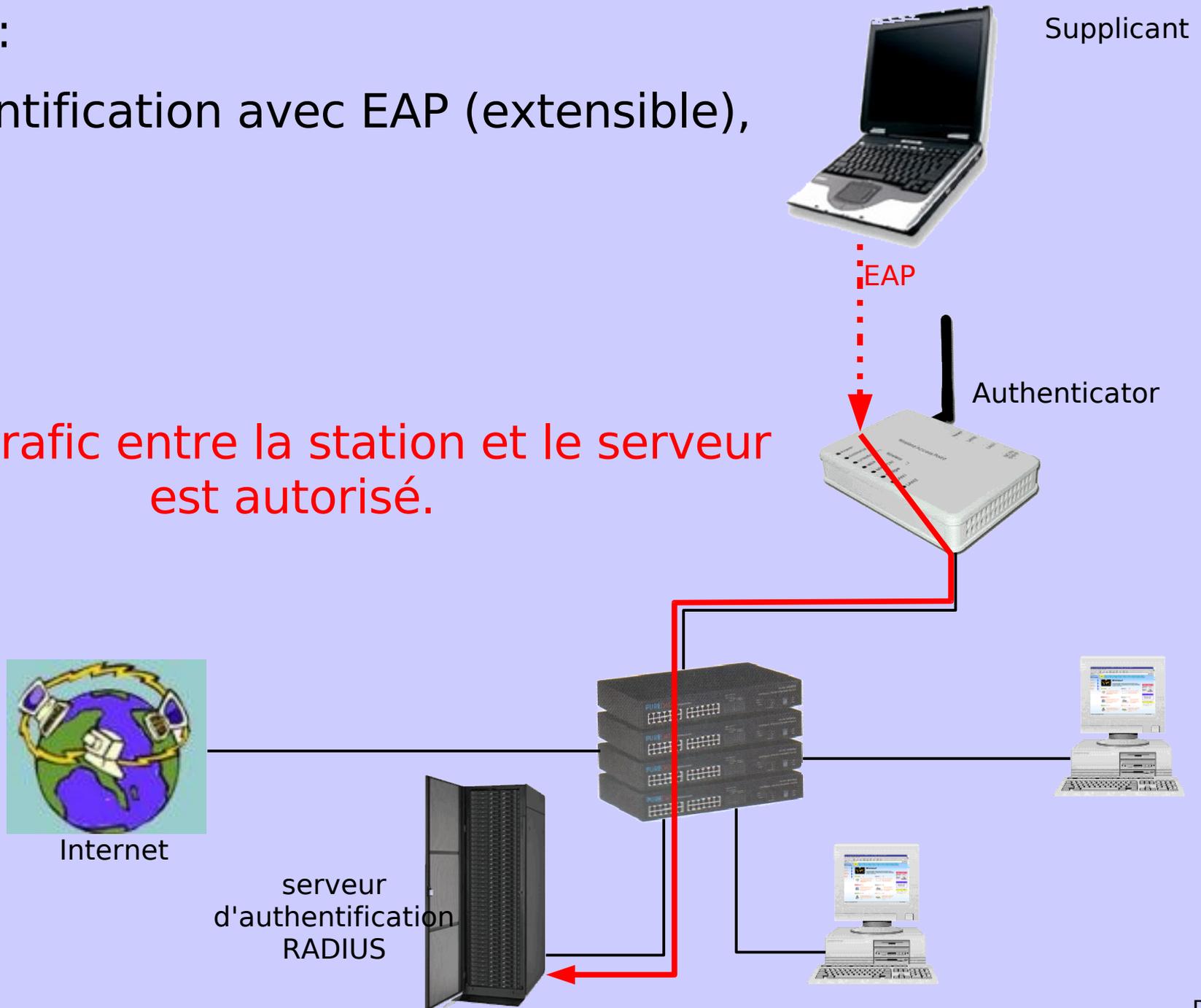
wepcrack : <http://wepcrack.sourceforge.net/>

Sécurité 4 : 802.1x (2001)

Principe :

↳ Authentification avec EAP (extensible),

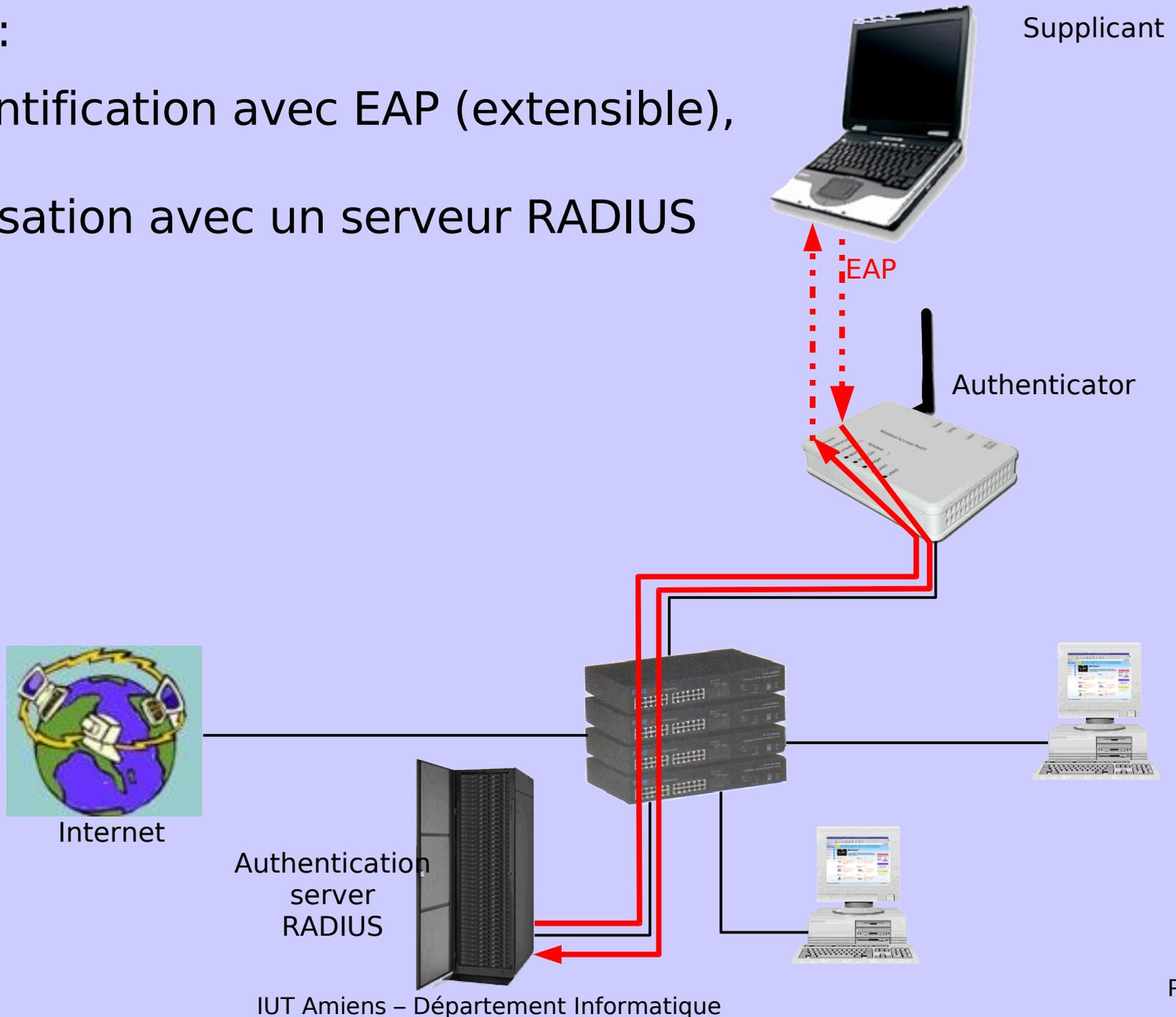
Seul le trafic entre la station et le serveur est autorisé.



Sécurité 4 : 802.1x (2001)

Principe :

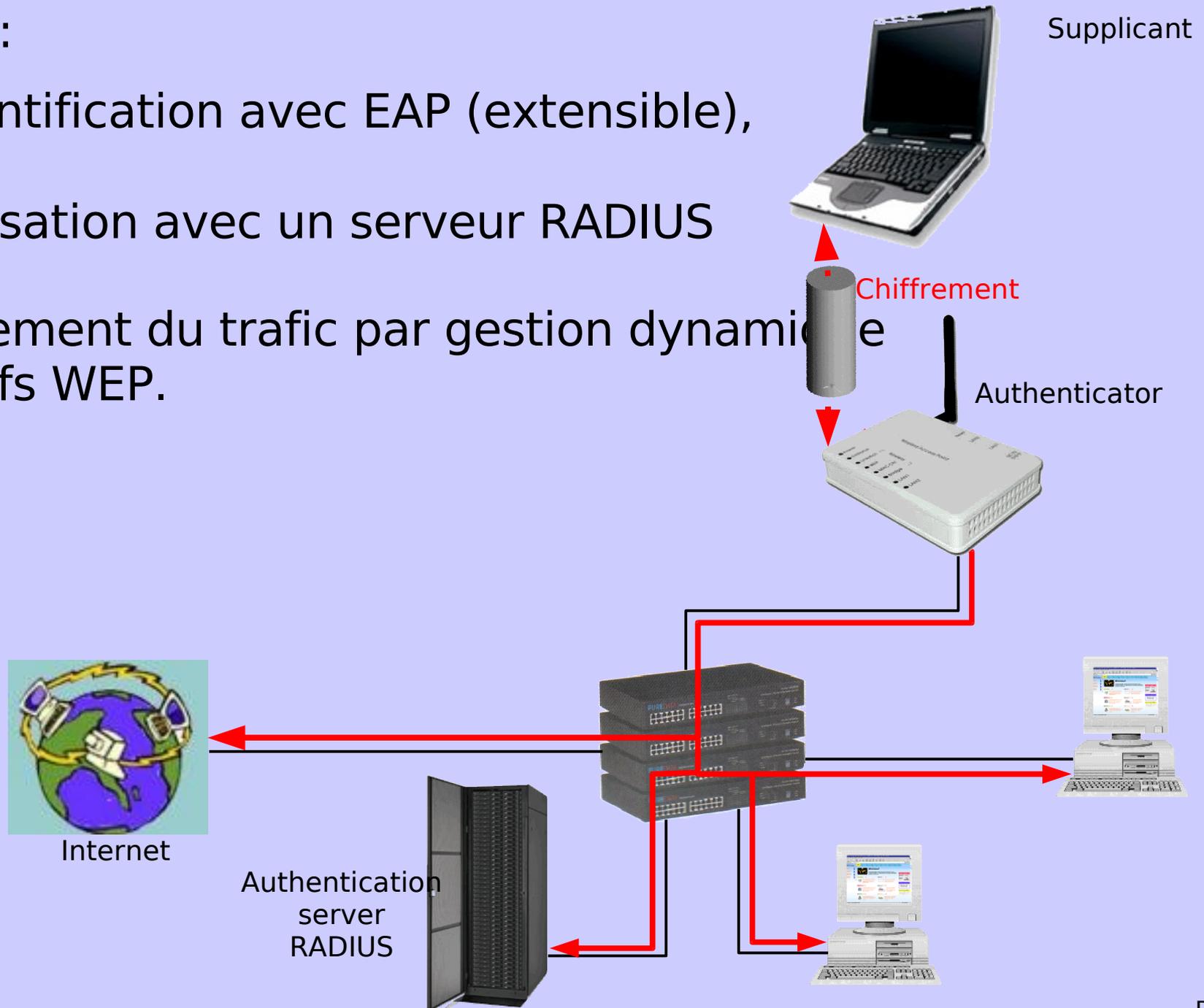
- Authentification avec EAP (extensible),
- Autorisation avec un serveur RADIUS



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 tinfoed.
(http://www.tinfoed.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 demandée par cet algorithme est nettement supérieure à RC4, il faut donc changer les équipements.

Sécurité 7 : VPN

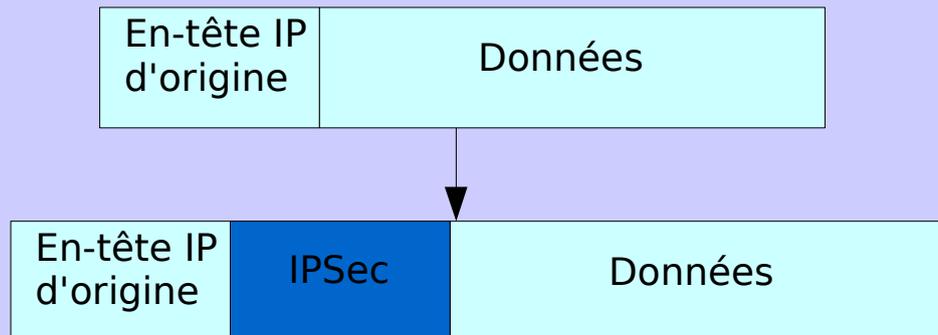
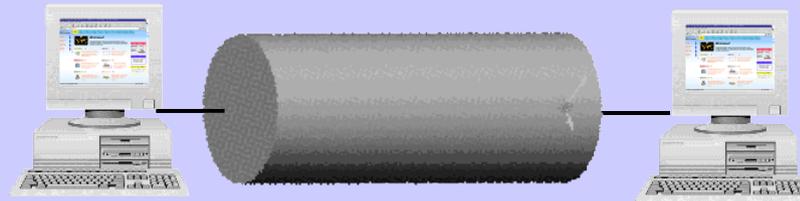
Un VPN (Virtual Private Network) est un moyen permettant de créer une connexion sécurisée sur un réseau quelconque entre deux entités (réseaux, sous réseaux ou utilisateurs individuels). Plusieurs protocoles permettent de le réaliser :

- PPTP de microsoft, niveau 2.
- L2F de CISCO, niveau 2.
- L2TP, niveau 2 et 3.
- IPSEC, niveau 3.

Le plus utilisé étant IPSec.

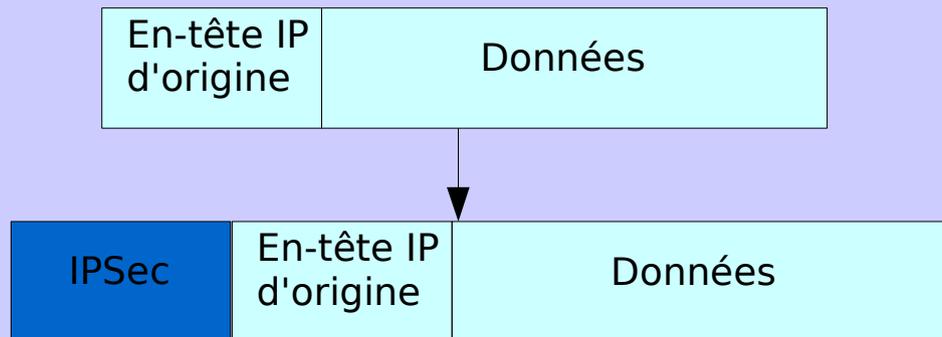
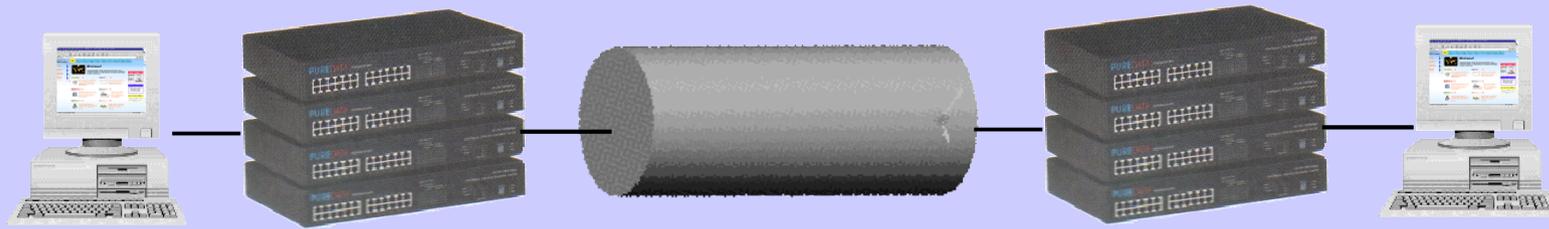
Sécurité 7 : VPN

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

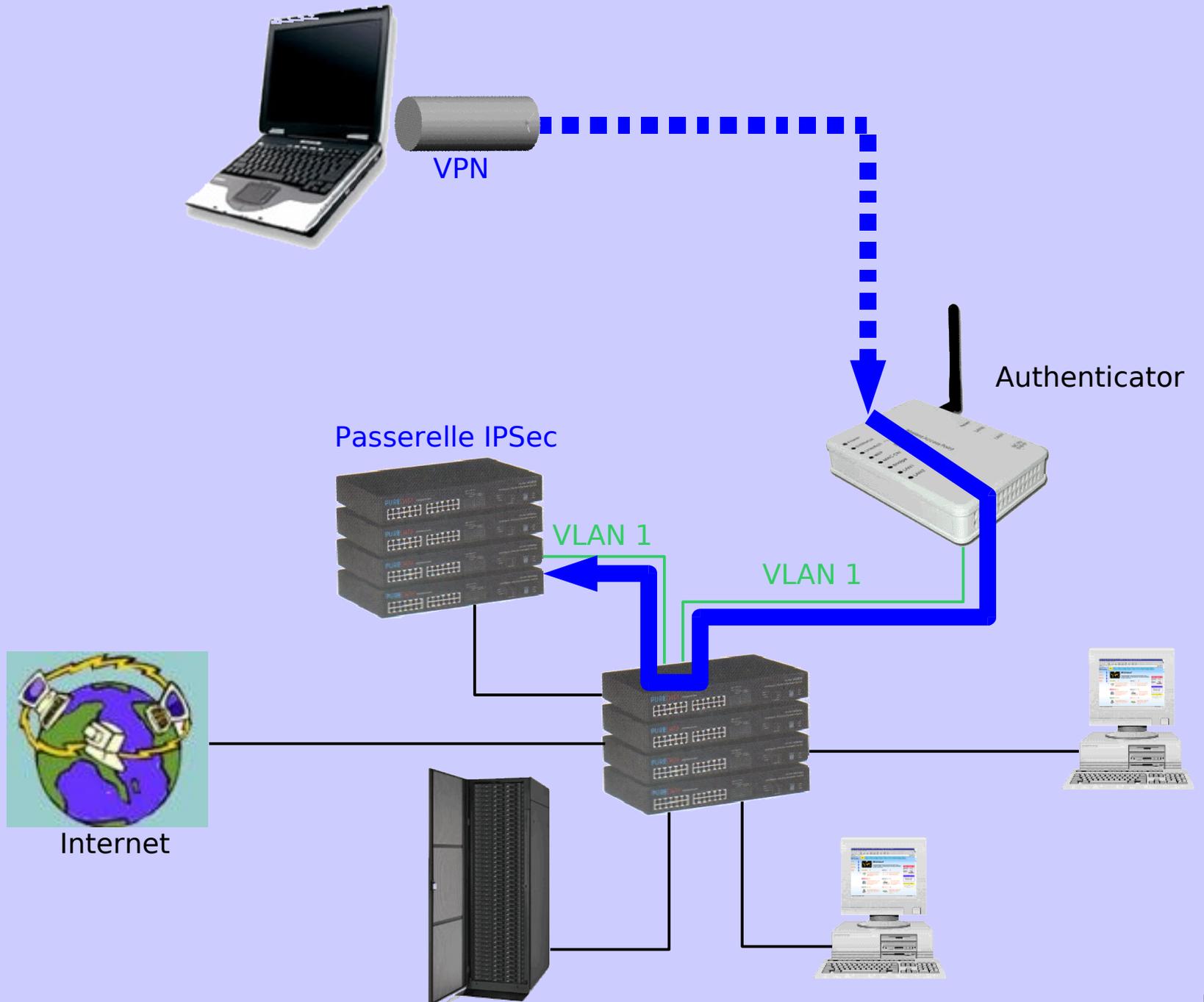


Sécurité 7 : VPN

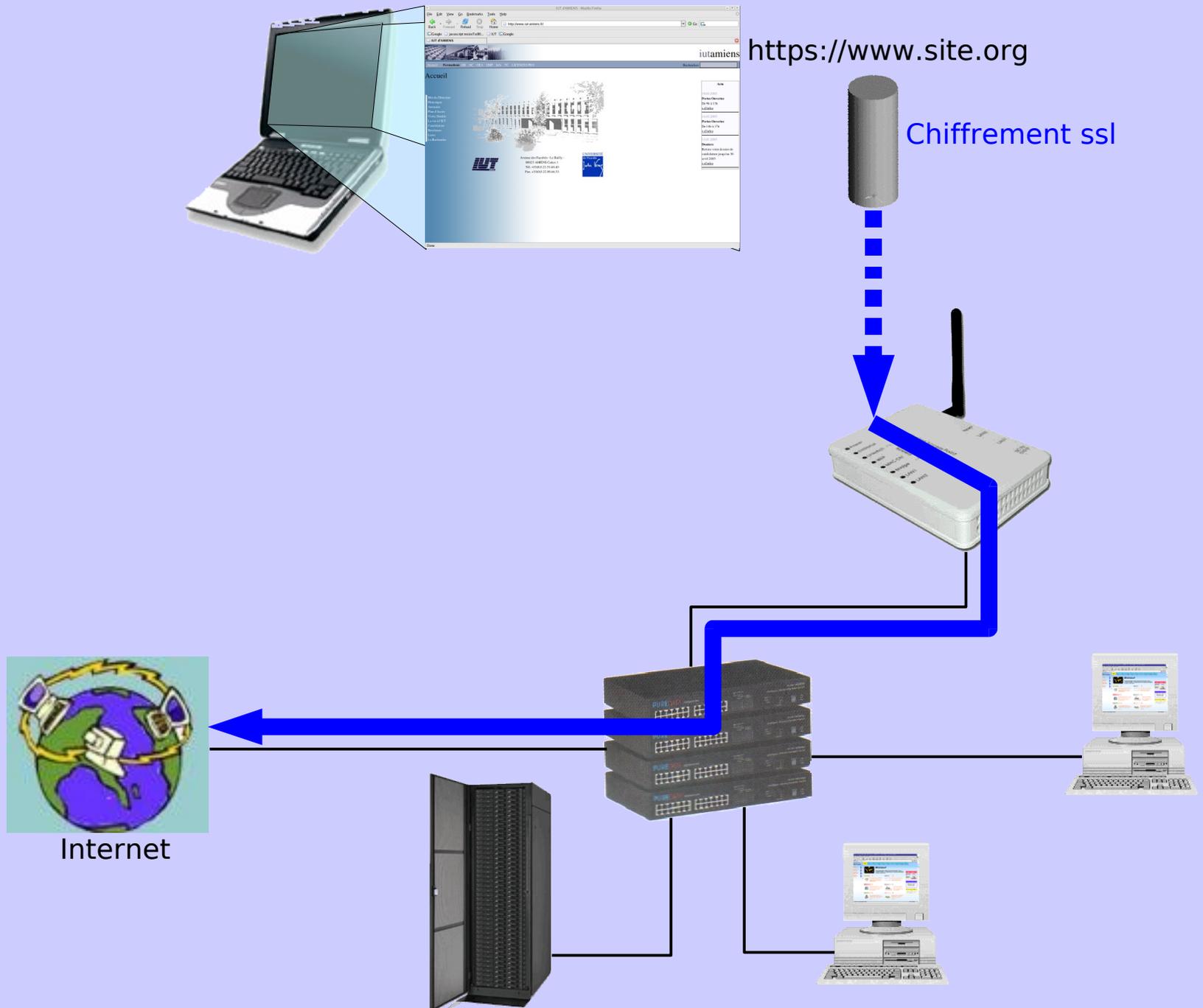
Mode tunnel : La session est établie entre des ponts ou passerelles.



Sécurité 7 : VPN



Sécurité 8 : VPN-SSL



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/>