Comprendre le Wi-Fi

Patrick VINCENT
pvincent@erasme.org

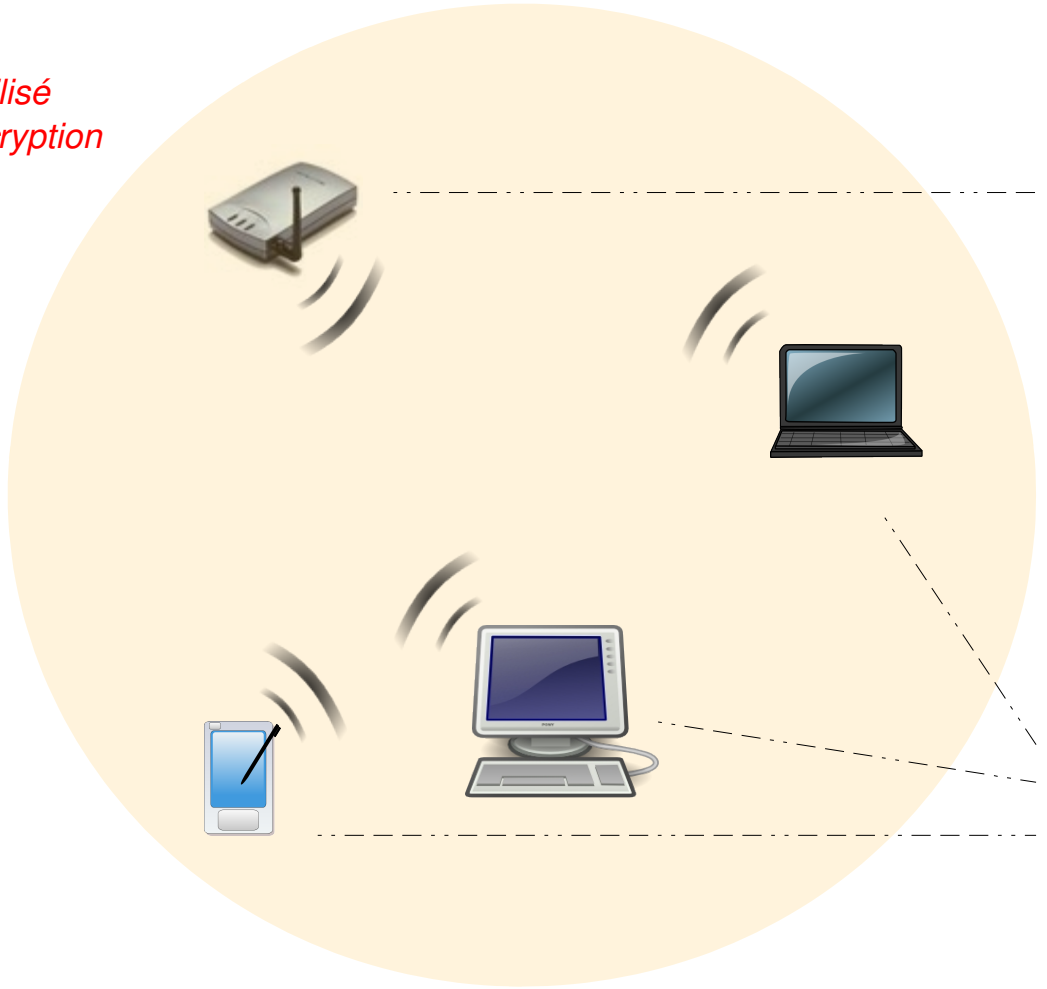
Le standard 802.11

	Débit théorique maximum	Bande de fréquence	Portée maximale	Observations
802.11b	11 Mbps	2,4 GHz	– intérieur : 50 m – extérieur : 200 m (11 Mbps)	– sensible aux interférences (bluetooth, téléphone sans fil, four micro-ondes...) – faible coût (répandue) – non réglementée (1999) – bonne pénétration pour la majorité des matériaux
802.11a	54 Mbps	5 GHz	– intérieur : 20 m	– réglementée – fréquences radio élevées (couverture plus faible tributaire des obstacles) – plus chère – pas d'interférence avec les appareils électroniques
802.11g	54 Mbps	2,4 GHz	– intérieur : 20 m – extérieur : 50 m (54 Mbps)	- compatible avec 802.11b - s'imposera devant le 802.11b

Une architecture cellulaire

Cellule
(zone de couverture)

-ID
- Débit
- Canal utilisé
- Mode d'encryption



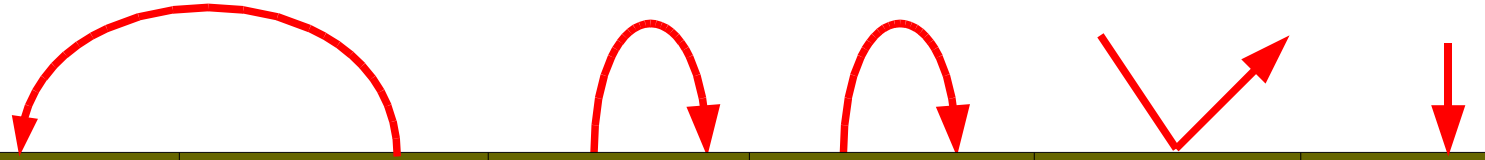
Point d'accès
module WiFi
&
module Ethernet

Un équipement
Wi-Fi
= 2 interfaces

Adaptateur WiFi
module WiFi
&
module PCI, PCMCIA,
CompactFlash ou USB

Les modes d'association

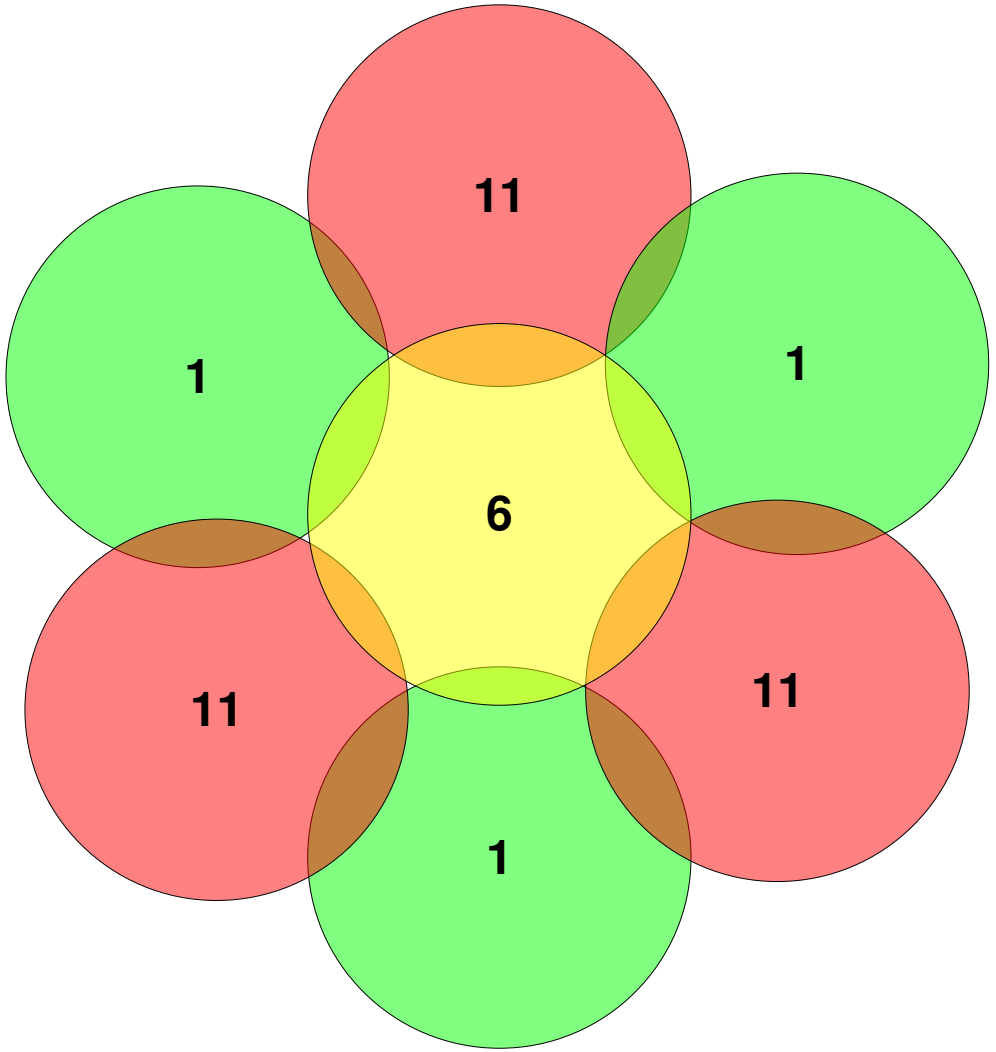
- Le mode d'association configuré sur un module WiFi détermine ses possibilités de connexion avec les autres :
  - **mode *AP*** (access point) : fonction d'association parent (diffuse un SSID, fonction switch et répartition de charge, gère la sécurité)
  - **mode *client* ou *managed*** : fonction d'association enfant
  - **mode *ad-hoc*** et **mode *bridge*** : pont réseau
  - **mode *repeater*** : réémission des trames
  - **mode *monitor*** : écoute et enregistrement des trames



Mode Matériel	AP (parent)	client (enfant)	Ad-Hoc	Bridge	Répéteur	Monitor
Point d'accès	X	X		X	X	(X)
Adaptateur WiFi		X	X			(X)

Affectation des canaux

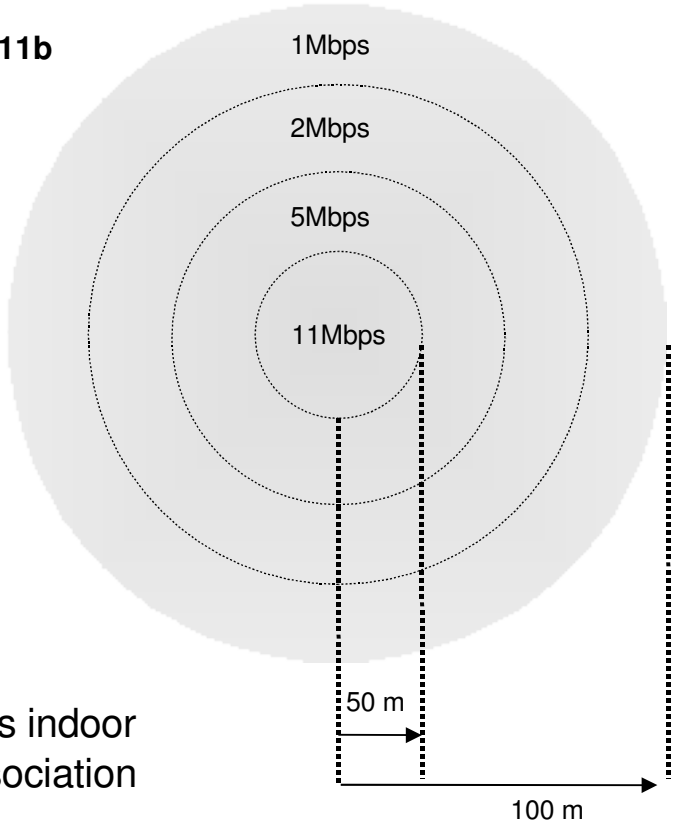
- Affectation de trois canaux qui ne se perturbent pas (cas limite - interférences et réflexions) :

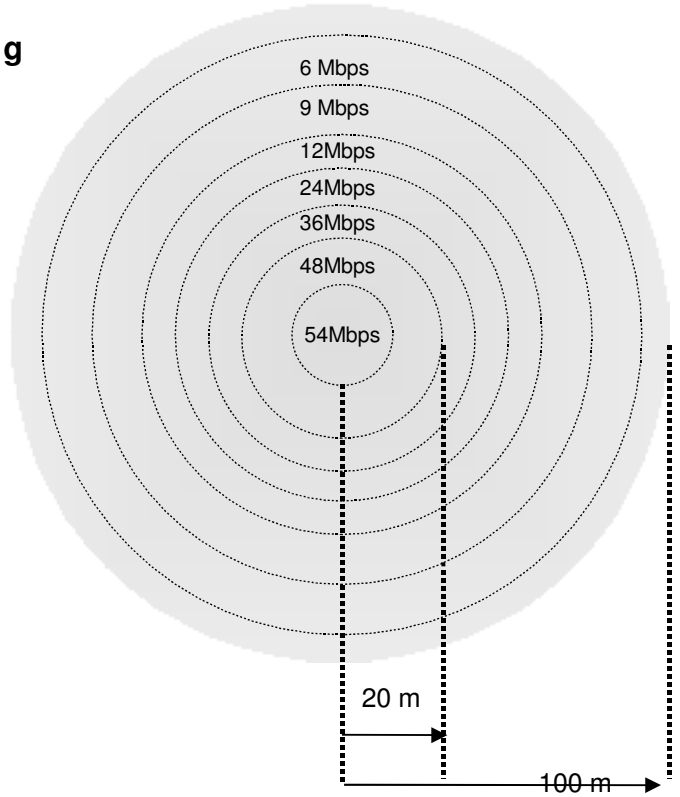


Débit d'association

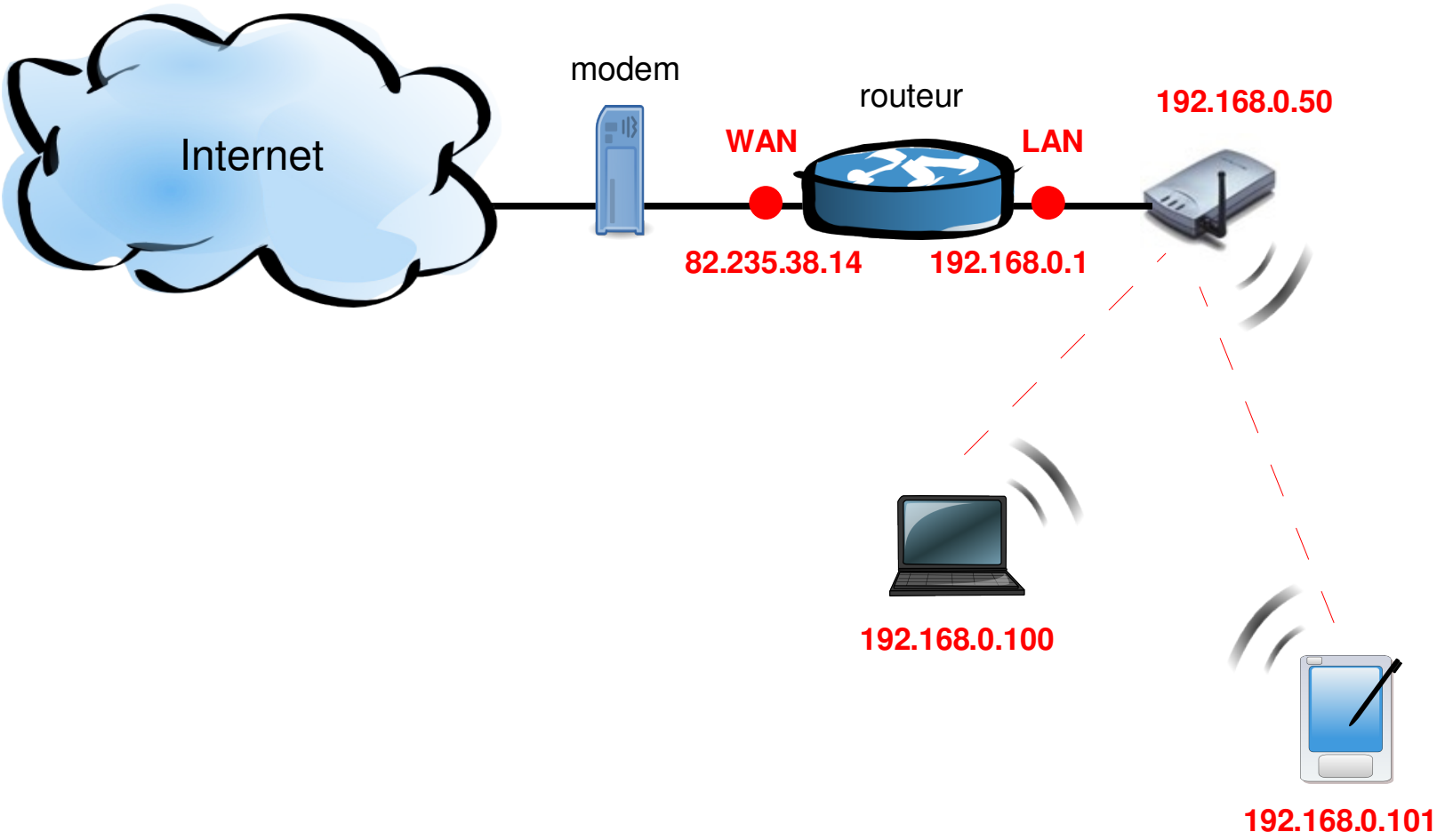
- Variable : 54 - 48 - 36 - 24 - 12 - 11 - 5,5 - 2 - 1 Mbit/s
- Adapté automatiquement en fonction
  - de la puissance reçue par l'appareil (distance)
  - du rapport Signal/Bruit (qualité du signal)

débits indoor d'association

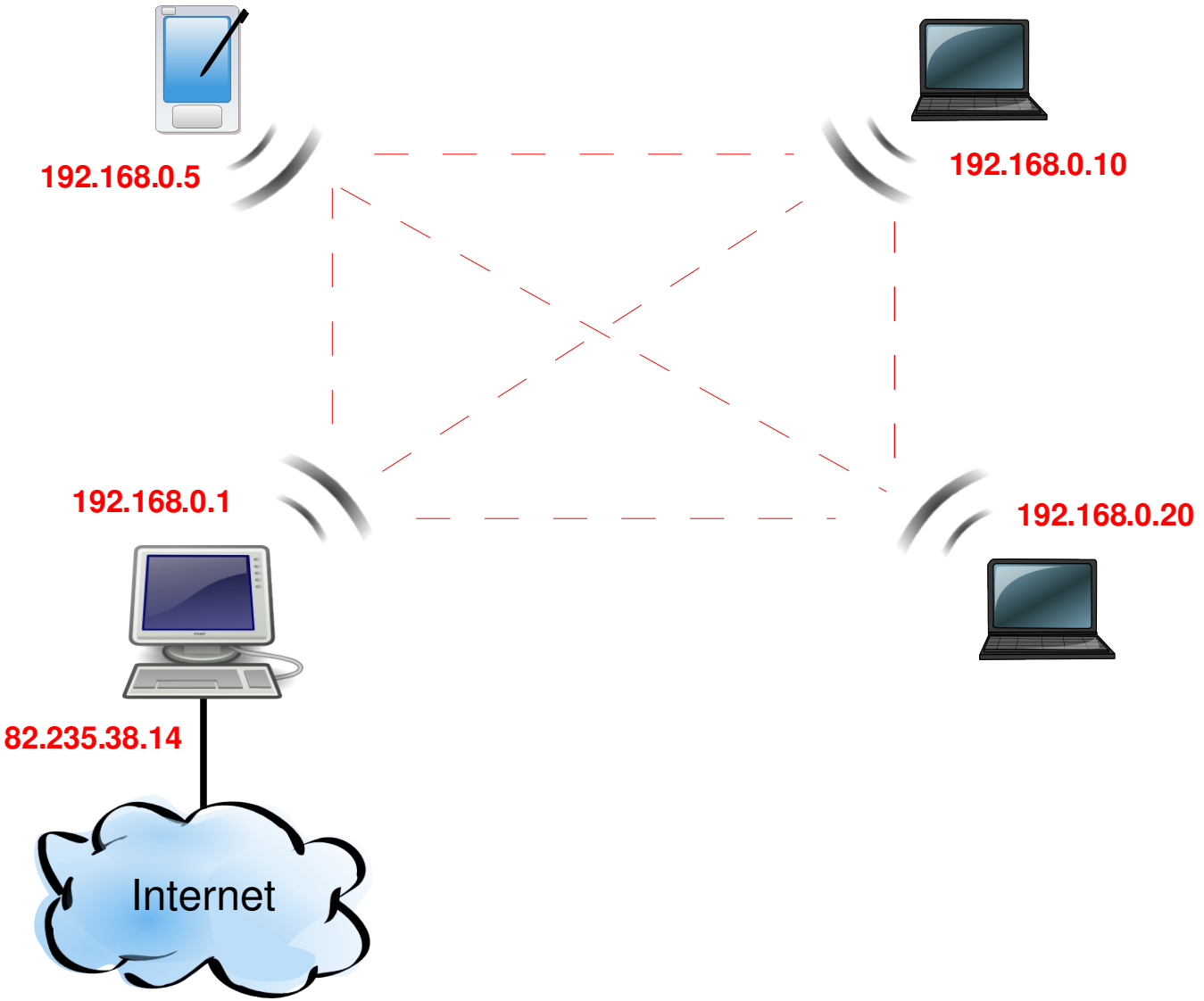




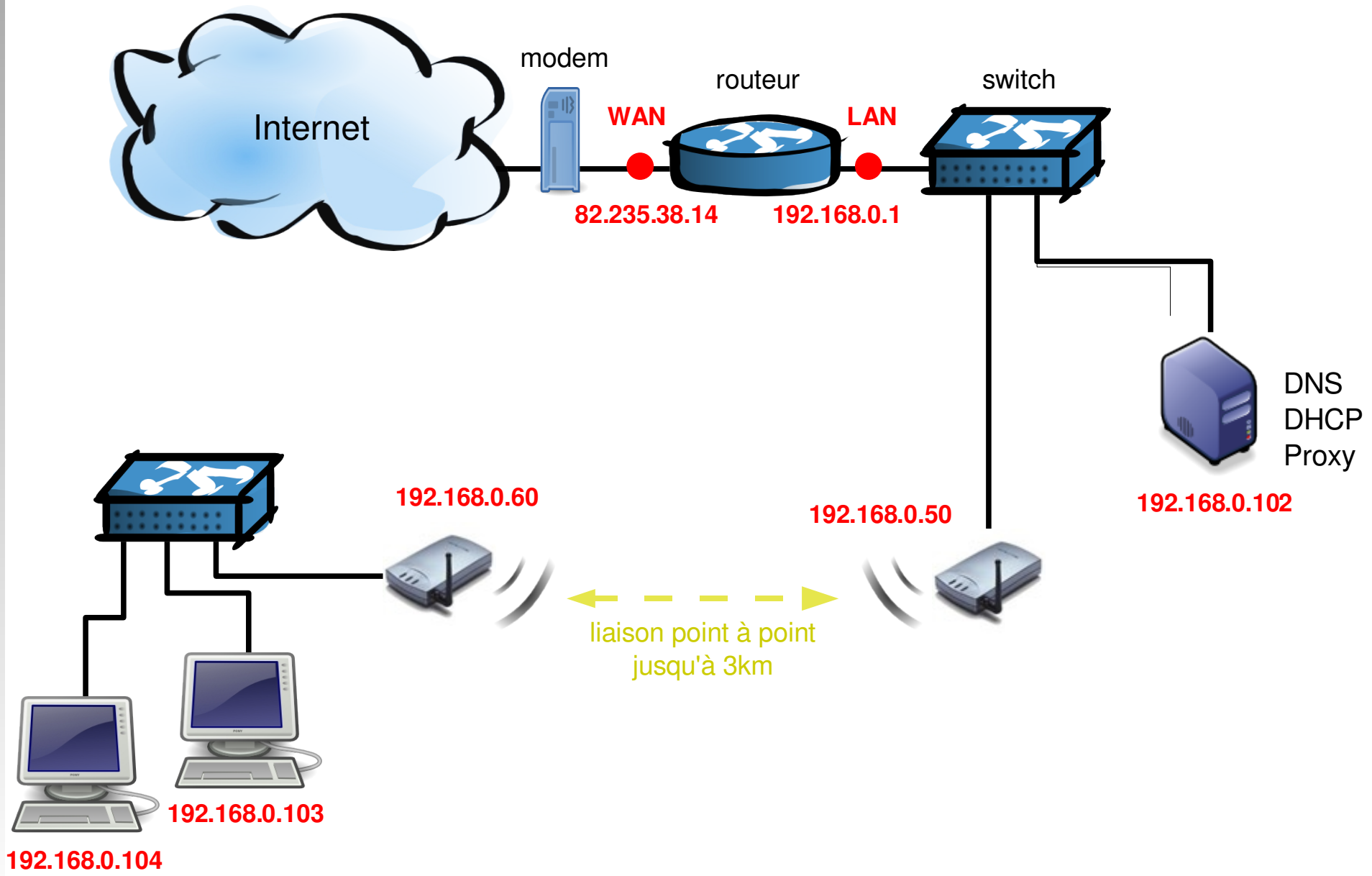
Topologie Infrastructure



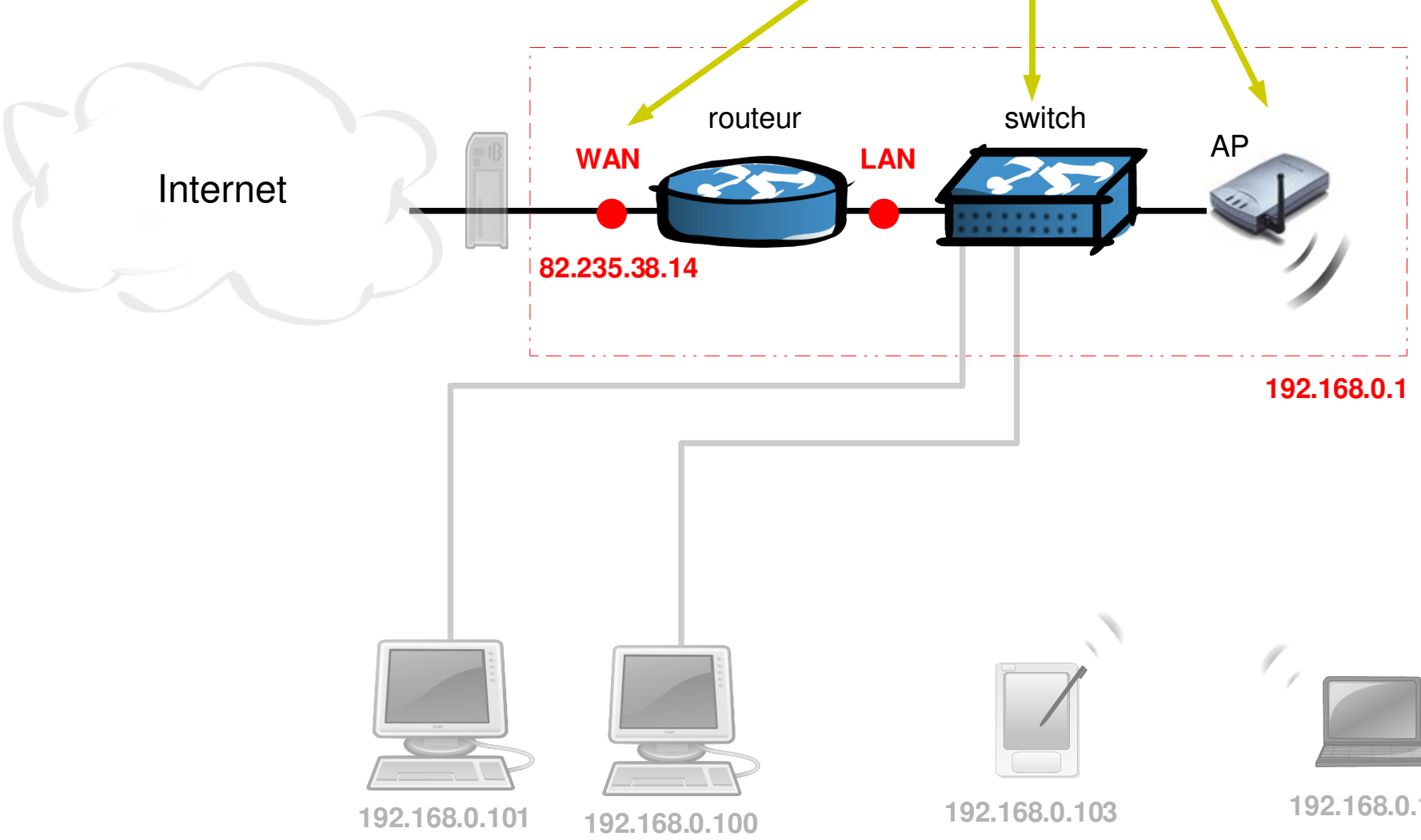
Topologie ad-hoc



Topologie Bridge



= 3 en 1

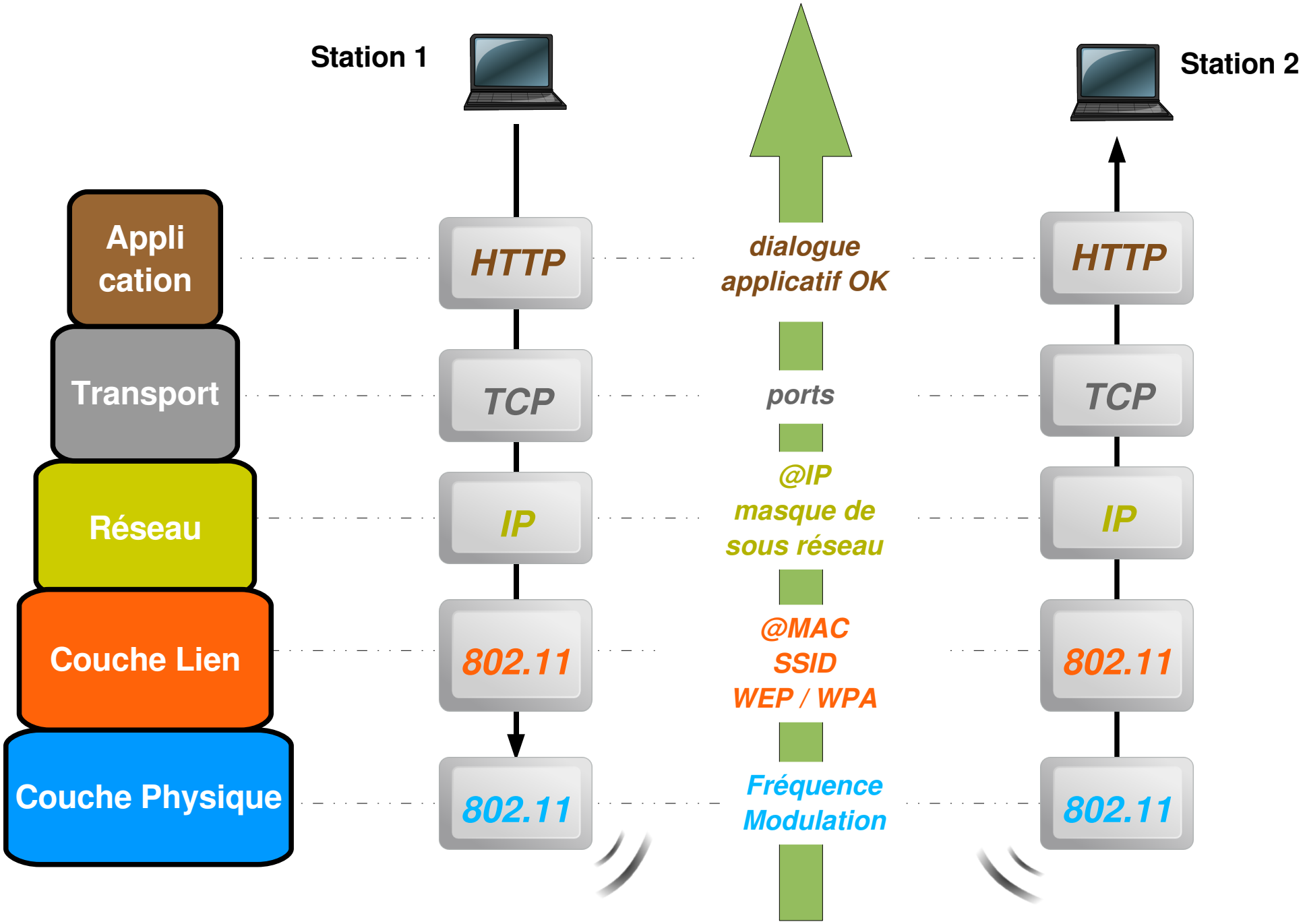

Internet
WAN
routeur
LAN
switch
AP
82.235.38.14
192.168.0.1
192.168.0.101
192.168.0.100
192.168.0.103
192.168.0.104

Résumé des solutions de sécurité

		Interception de données	Intrusion	Occupation de BP	Brouillage des transmissions	Dénis de service
Wi-FI	**Réglage de la puissance**	+	+	+	-	+
	Ne pas broadcaster le SSID	-	+	+	-	+
	Limitation des @Mac	-	+	+	-	+
	Clef WEP	++	+	+	-	+
	WPA	+++	++	+	-	+
IP	**@IP fixes**	-	+	+	-	-
	Tunnel VPN	+++	+	-	-	-

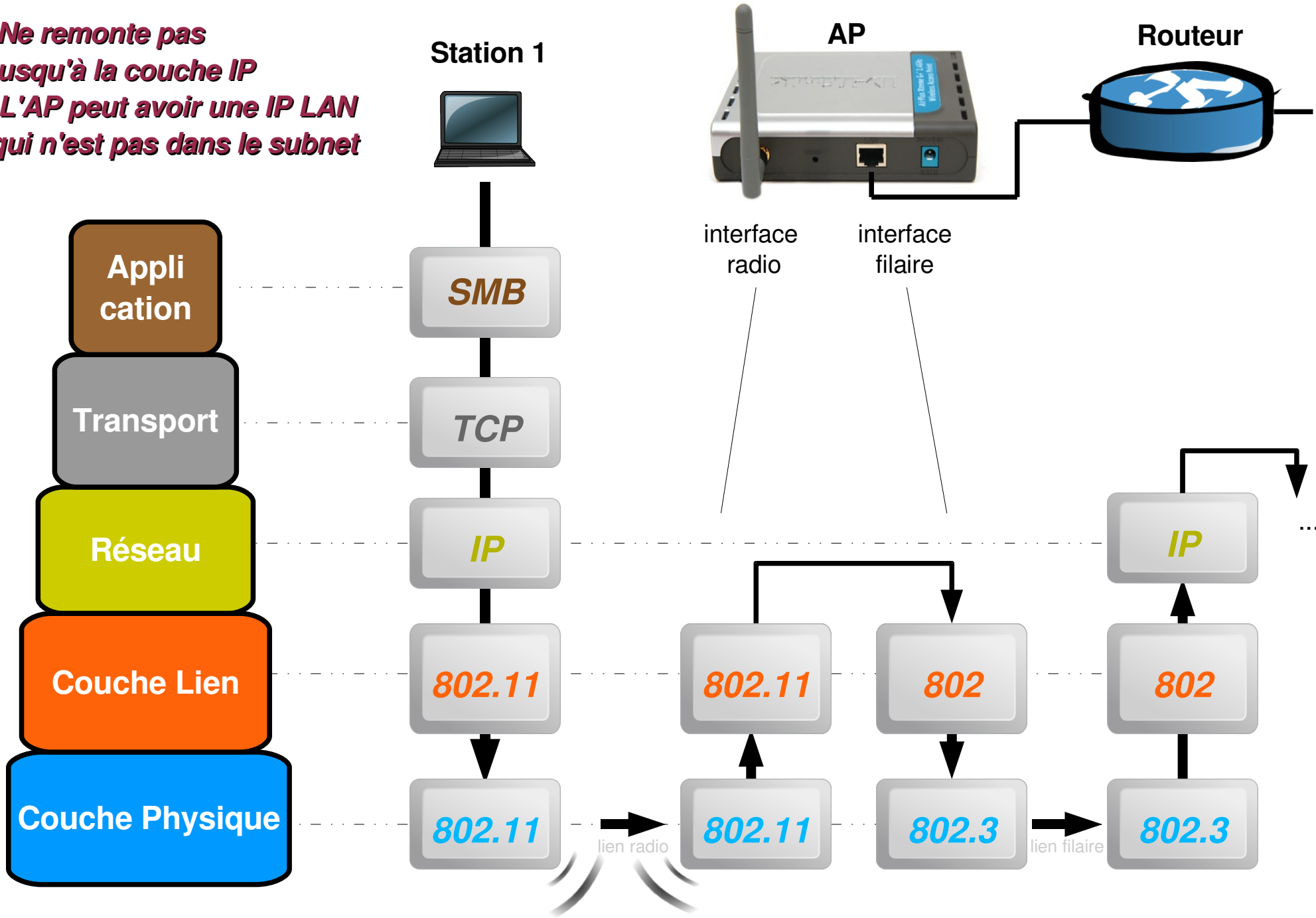
- : ne fonctionne pas
+ : fonctionne mais peu fiable
++ : recommandé
+++ : meilleure solution

Les couches du modèle OSI



AP = bridge de niveau 2

-Ne remonte pas jusqu'à la couche IP
-L'AP peut avoir une IP LAN qui n'est pas dans le subnet



Configuration du réseau Wi-Fi

Patrick VINCENT
pvincent@erasme.org

@ IP / masques de sous-réseau

- Les équipements qui veulent communiquer entre eux, doivent utiliser la **même adresse réseau** (masque) et une **adresse d'ordinateur** (host) **différente :**

Adresse IP de l'ordinateur 1	Adresse IP de l'ordinateur 2	Masque de sous réseau
192.168.0.1	192.168.0.2	255.255.255.0
192.168.10.1	192.168.0.3	255.255.0.0
192.56.78.98	81.63.75.17	0.0.0.0

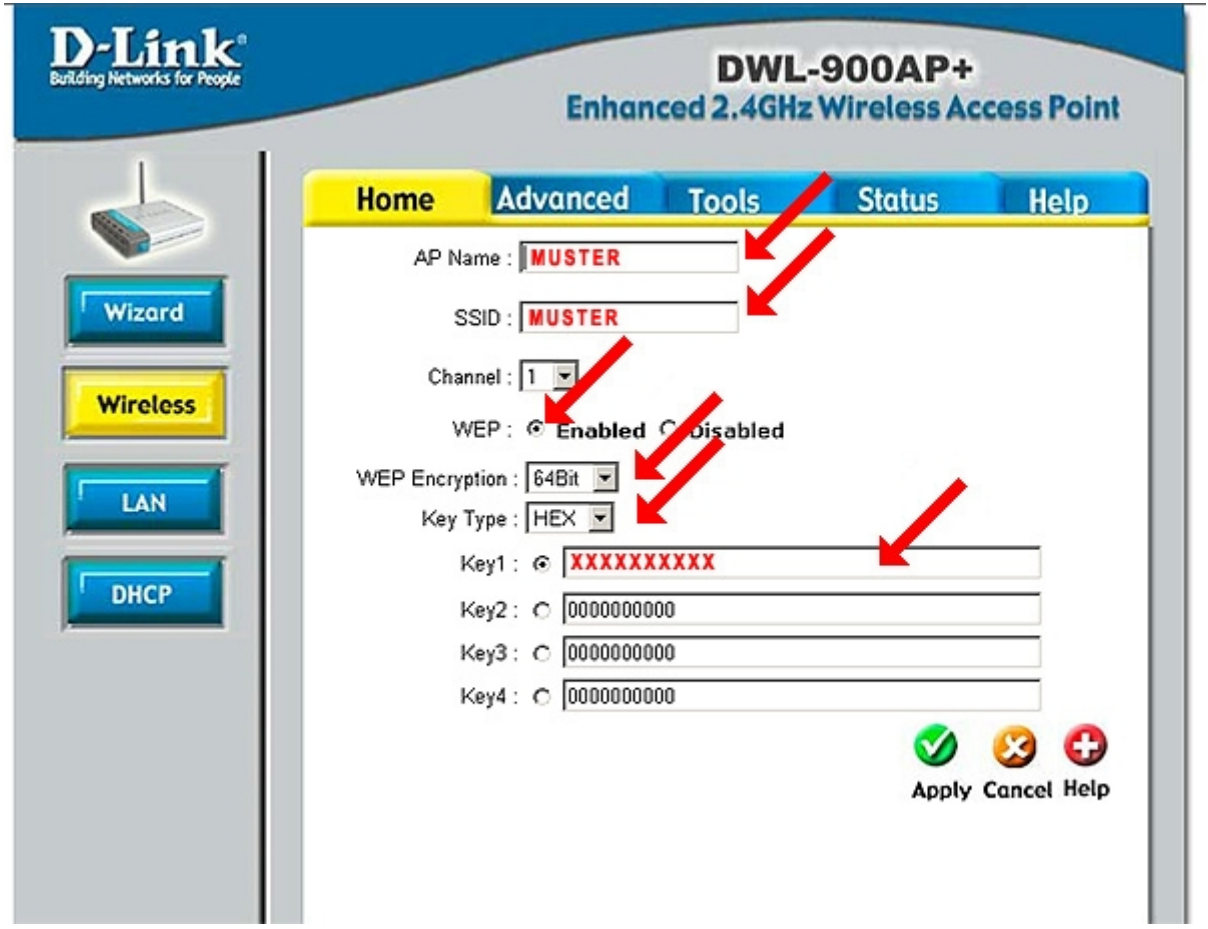
Masque de sous réseau	Notation CIDR	Nombre de machines
255.255.255.252	/30	2
255.255.255.248	/29	6
255.255.255.240	/28	14
255.255.255.224	/27	30
255.255.255.192	/26	62
255.255.255.128	/25	126
255.255.255.0	/24	254
255.255.254.0	/23	510
255.255.252.0	/22	1022
255.255.248.0	/21	2046
255.255.240.0	/20	4094
255.255.224.0	/19	8190
255.255.192.0	/18	16382
255.255.128.0	/17	32766
255.255.0.0	/16	65534
255.254.0.0	/15	131070
255.252.0.0	/14	262142
255.248.0.0	/13	524286
255.240.0.0	/12	1048574
255.224.0.0	/11	2097150
255.192.0.0	/10	4194302

Par défaut, dans un réseau local, on utilisera :

192.168.0.xxx / 255.255.255.0 : 254 machines (/24)

Réglages Radio de l'AP

- Configuration Radio
  - Nom
  - (E)SSID
  - Canal d'émission
  - SSID Broadcast
  - Topologie : AP, Client, Bridge, Repeater...



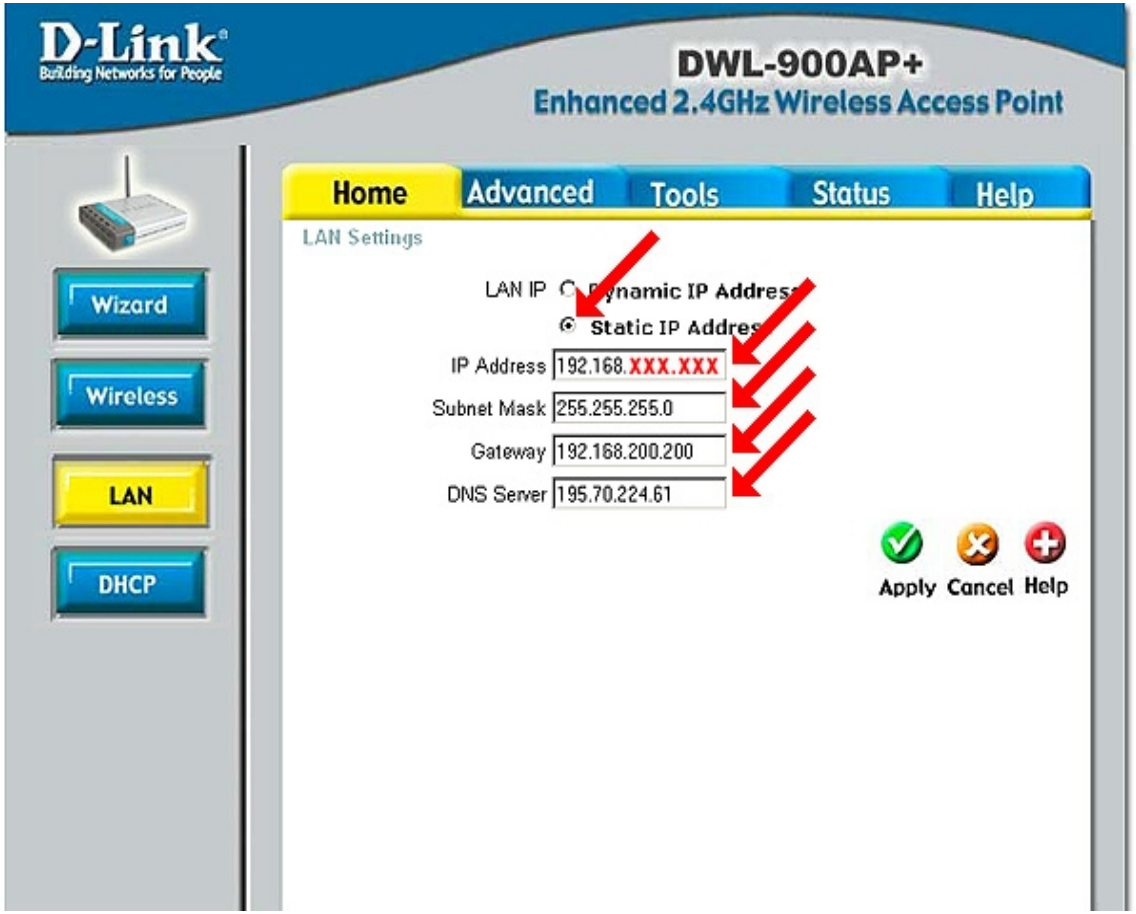
- Configuration Radio avancée
  - Puissance d'émission
  - Chiffrement et authentification : WEP / WPA
  - Filtrage des adresses MAC
  - Radio : Débits, DTIM, Fragmentation, Beacon...

Réglages TCP/IP de l'AP

- @IP WAN (interface Ethernet)
  - @IP / Masque
  - Passerelle
  - DNS

  ou

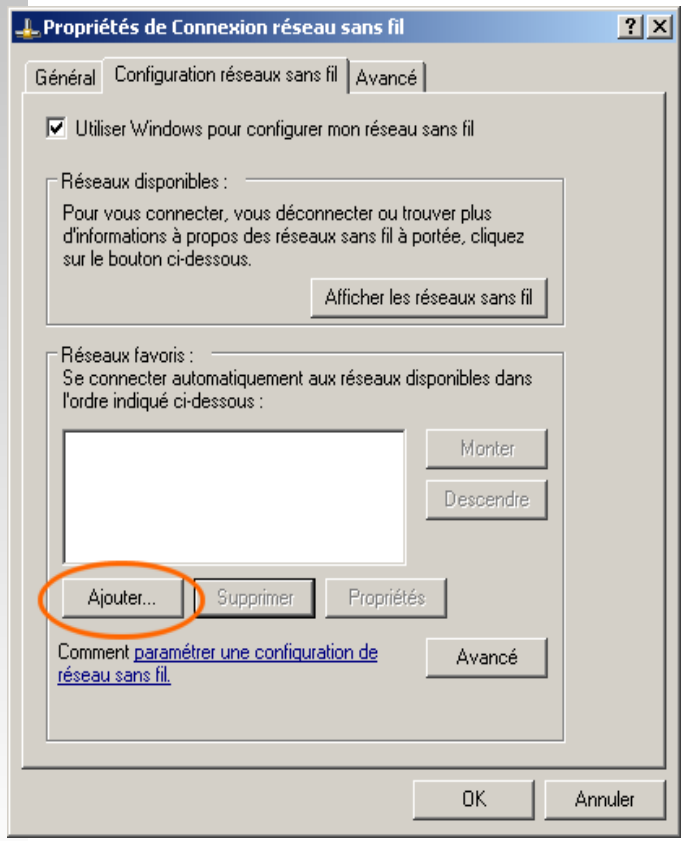
  - attribution en DHCP
- @IP LAN (interface Radio et Switch)
  - Activation DHCP - Plage

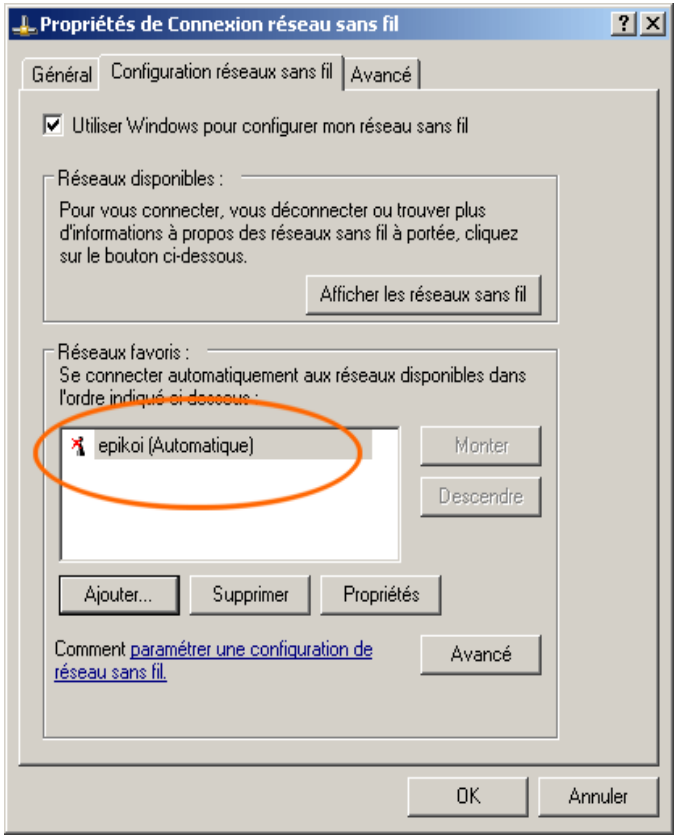


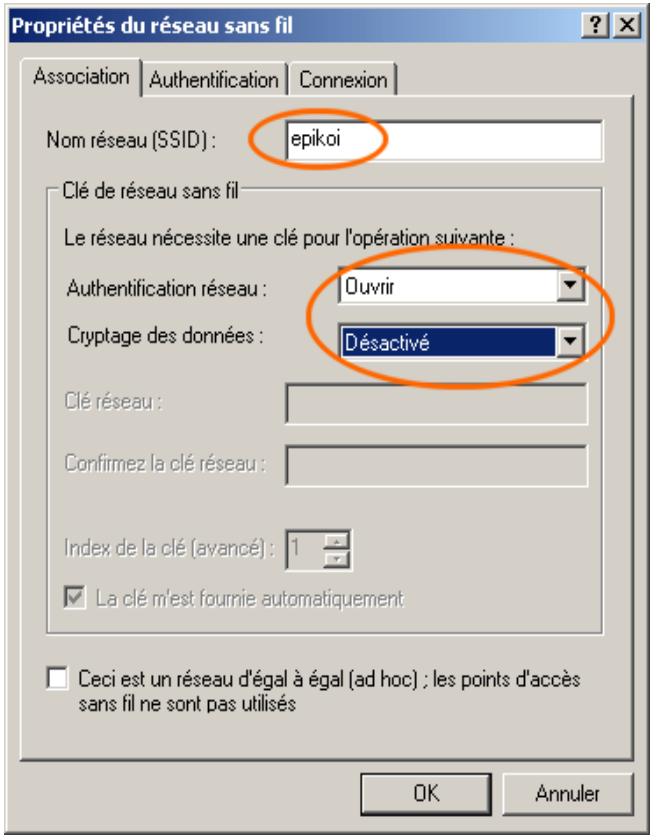
Réglages radio de l'adaptateur Wi-Fi

- Configuration Radio
  - (E)SSID
  - Topologie : Infrastructure ou ad-hoc
  - Cryptage et authentification :

CRYPTAGE → / AUTHENTIFICATION ↓	Pas de Cryptage	WEP	TKIP	TKIP
Ouverte	X			
Partagée		X		
WPA-PSK			X	
WPA-EAP (802.1x)				X





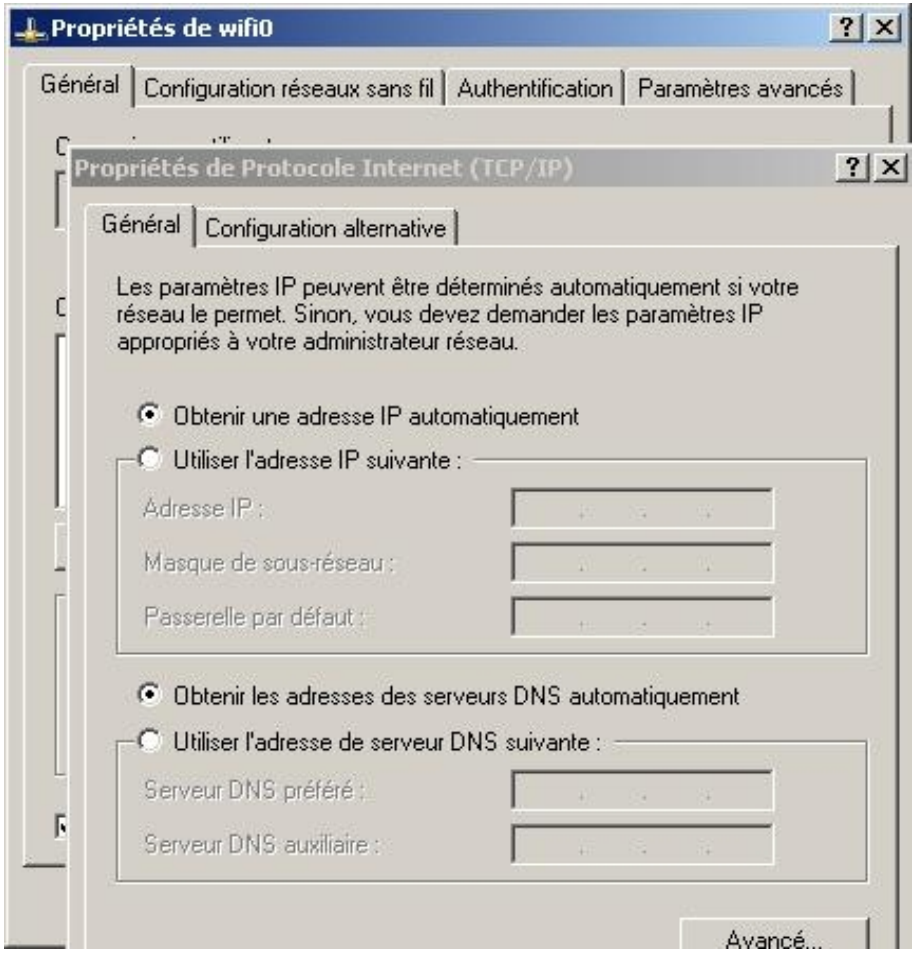


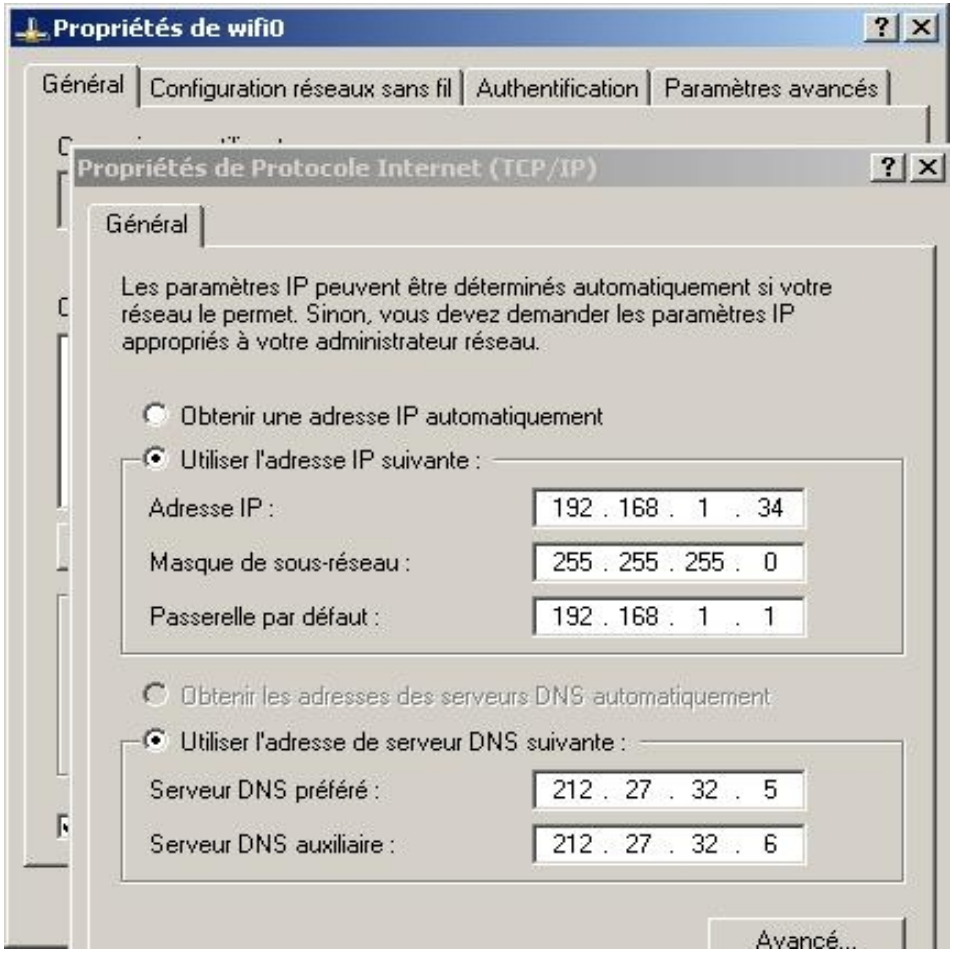
Réglages TCP/IP de l'adaptateur Wi-Fi

- DHCP

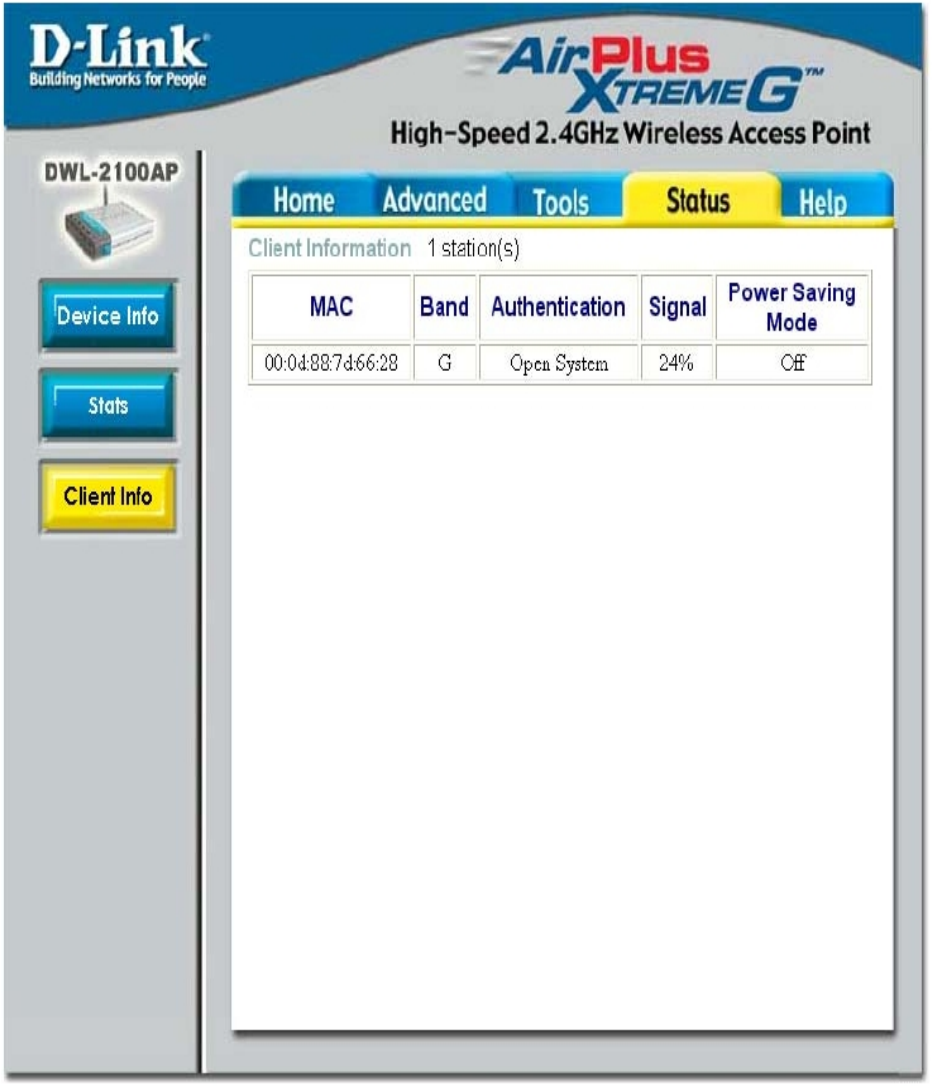
OU

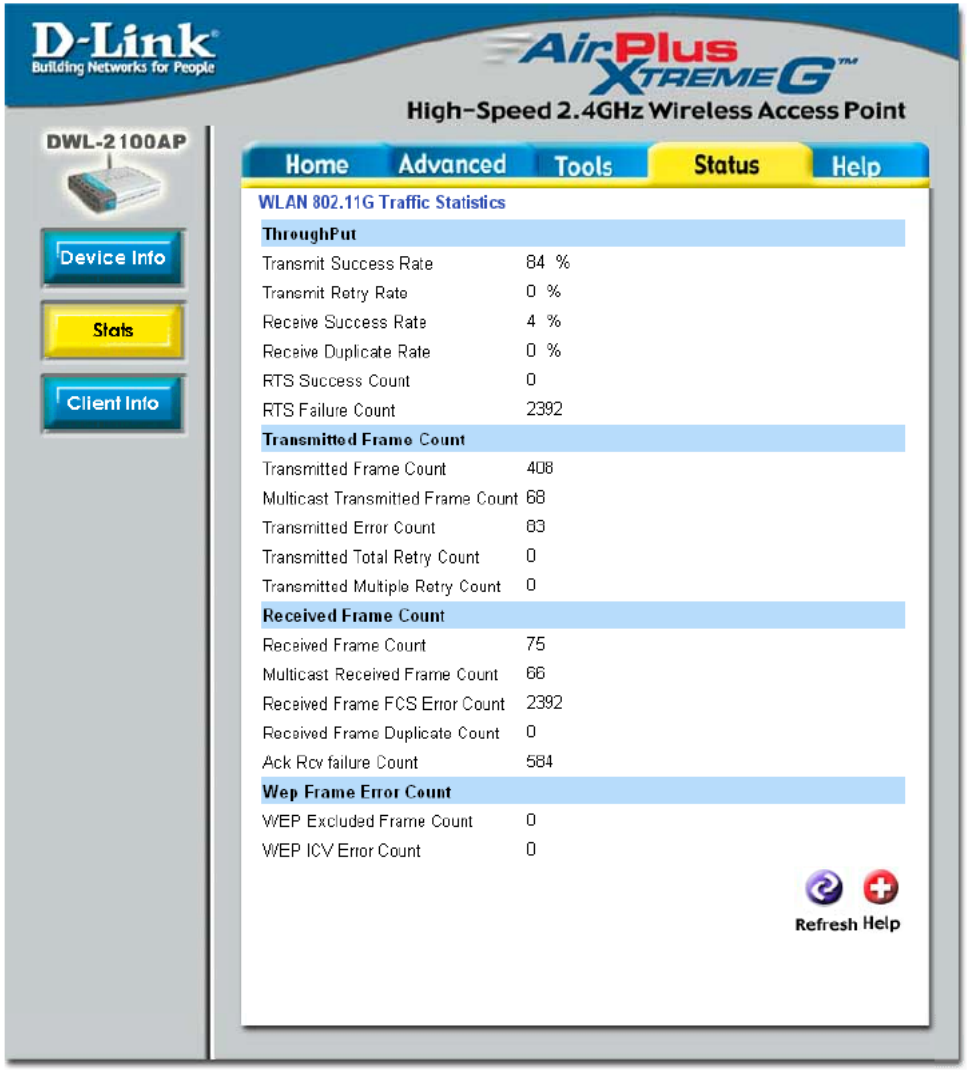
- Valeurs fixes
  - @IP / masque
  - Passerelle
  - DNS



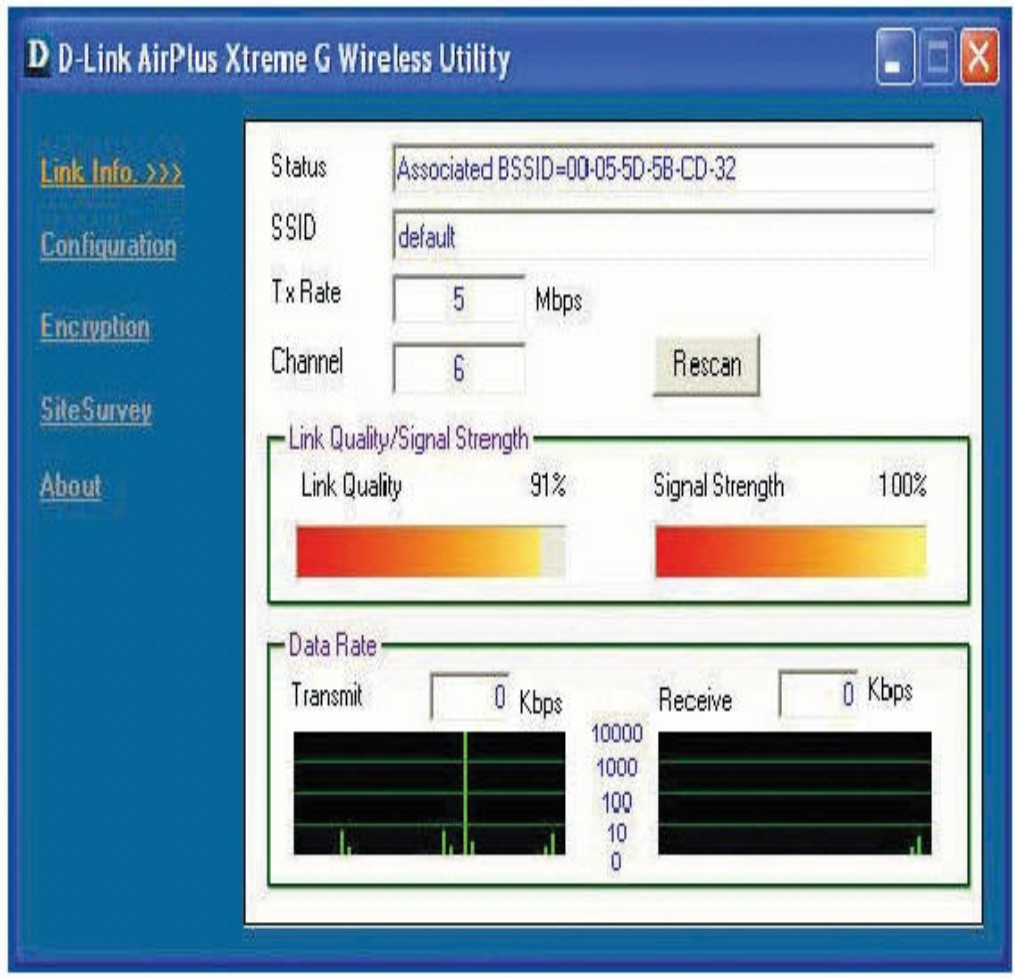


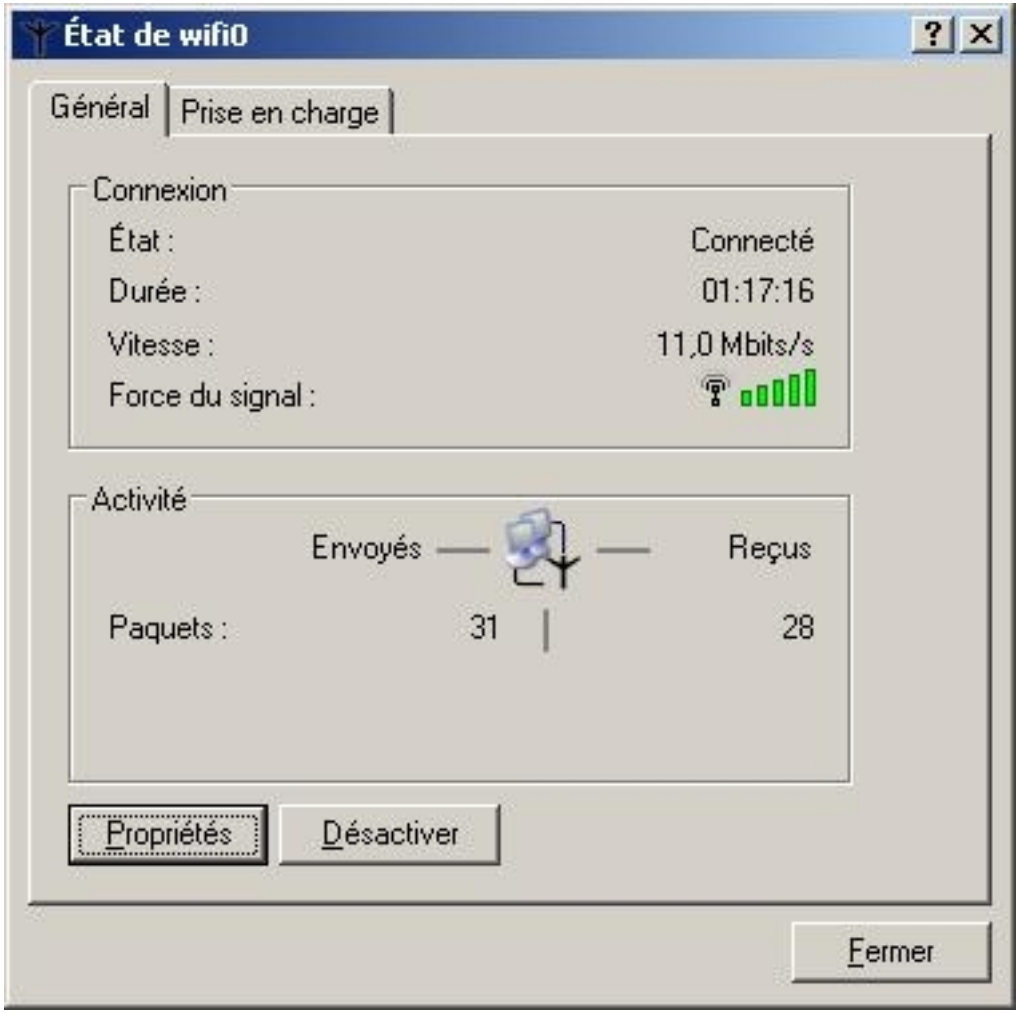
Diagnostics d'association (AP)





Diagnostics en mobilité (client)

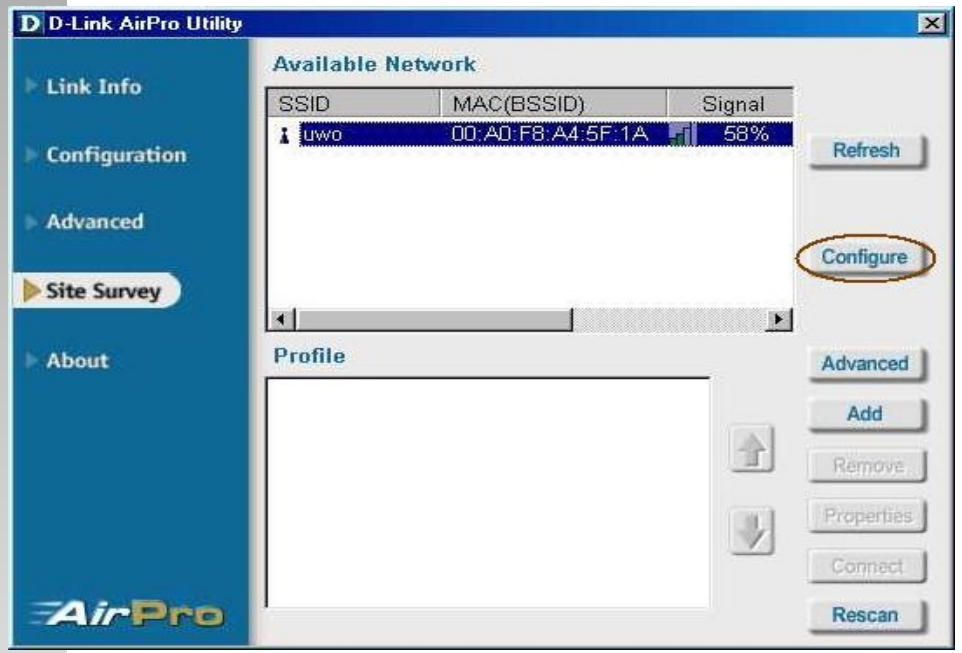


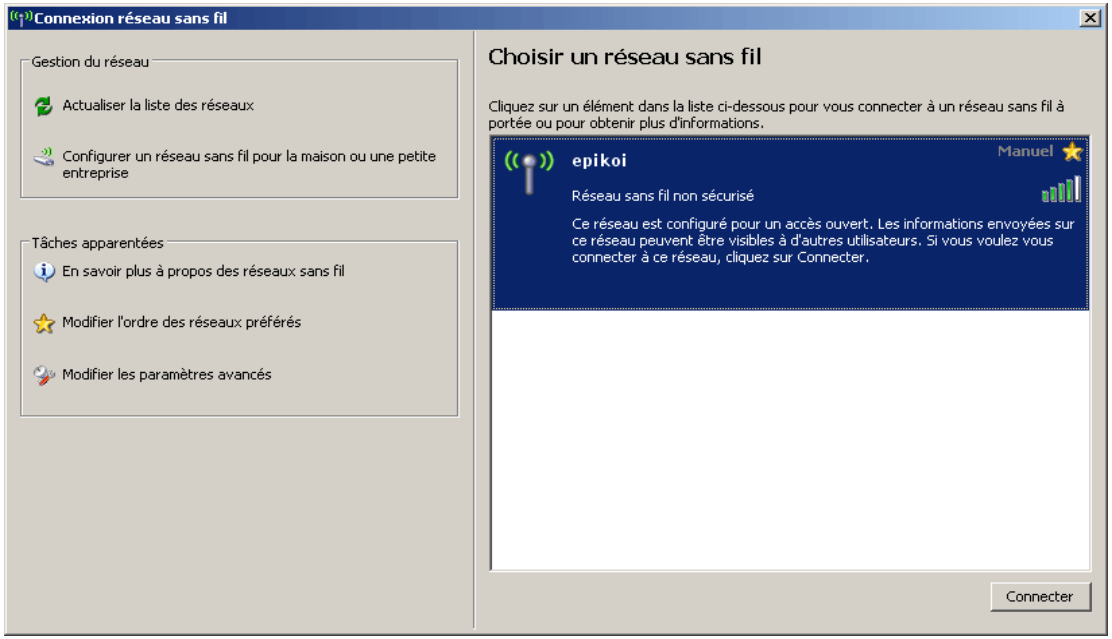


Outil Fabricant (Dlink)
-Puissance du signal
-Qualité du signal

Outil générique (Windows)
-Puissance du signal

Détection des réseaux (client)

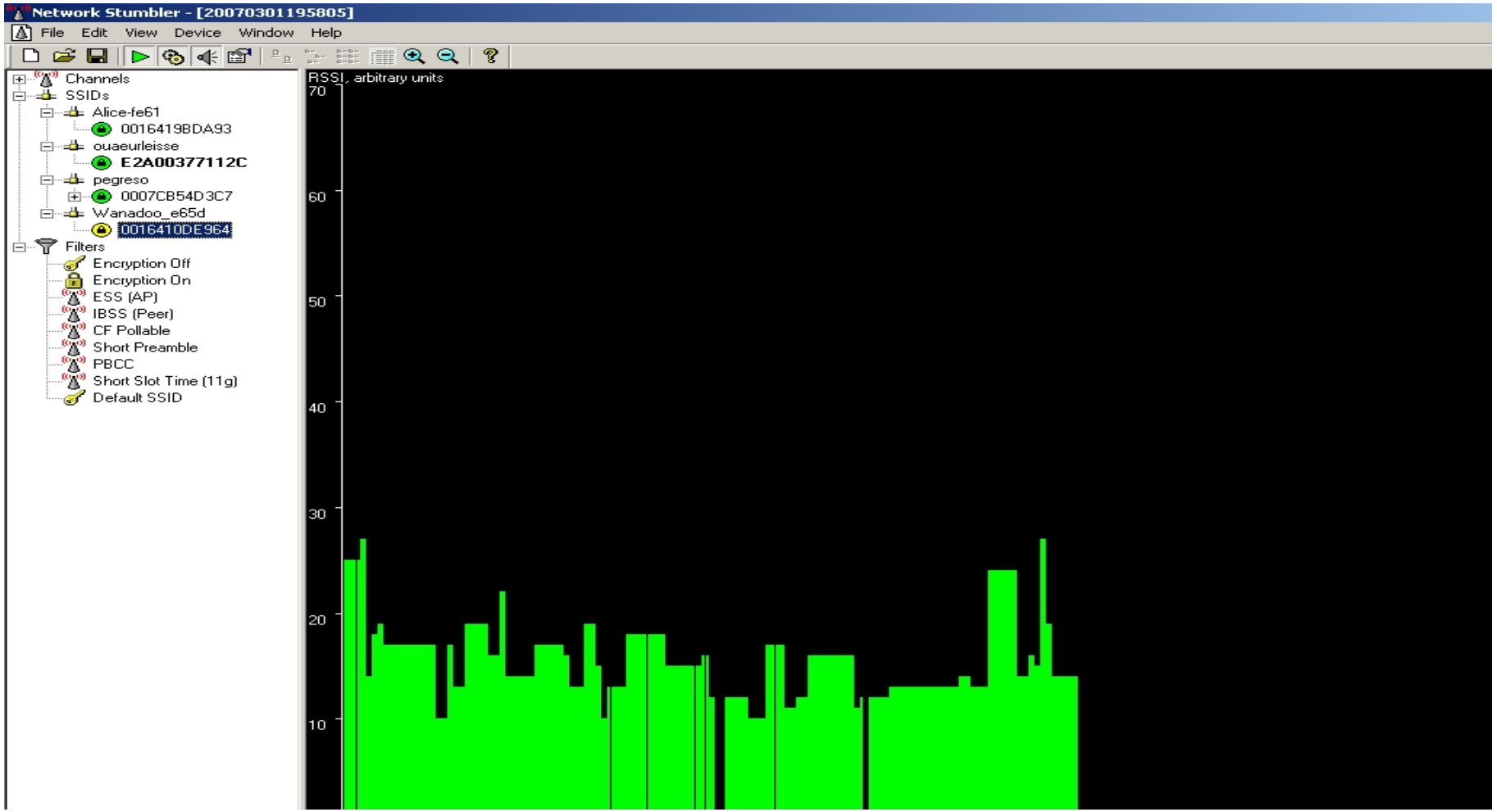




Outil Fabricant (Dlink)
-SSID
-BSSID
-Puissance du Signal

Outil générique (Windows)
-SSID
-Puissance du signal

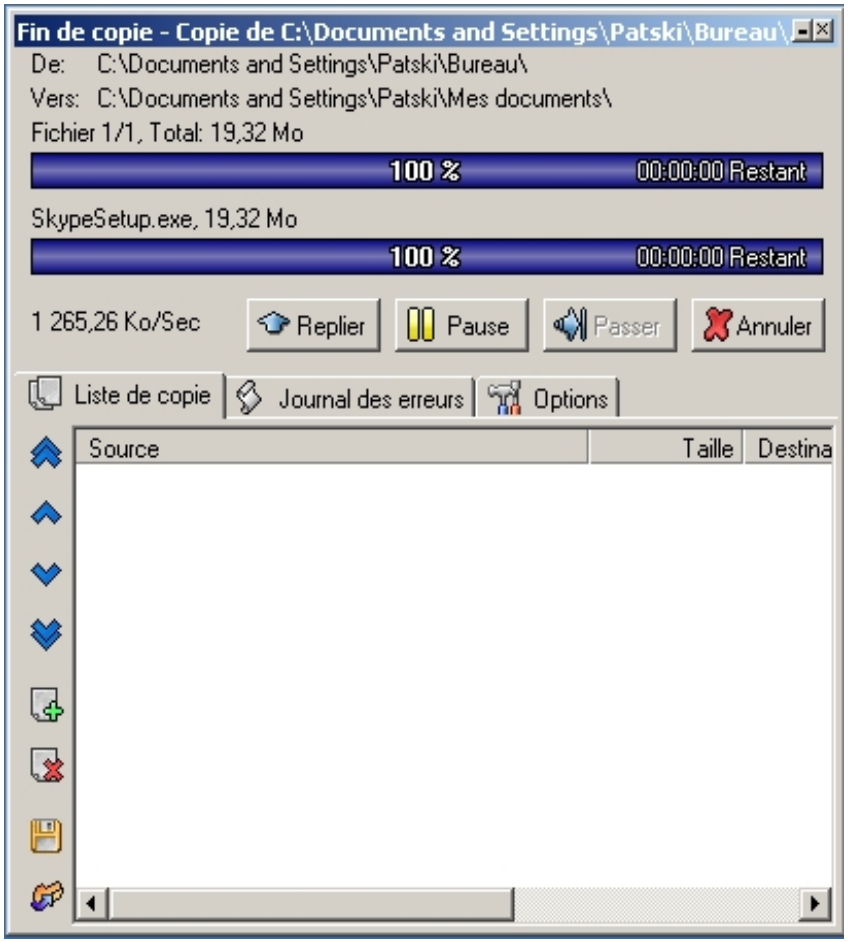
Outils génériques (client)



NetStumbler

-SSID
-BSSID
-Puissance du Signal
-type d'encryption
-rapport S/B

Mesure de débit



SuperCopier
(Windows)

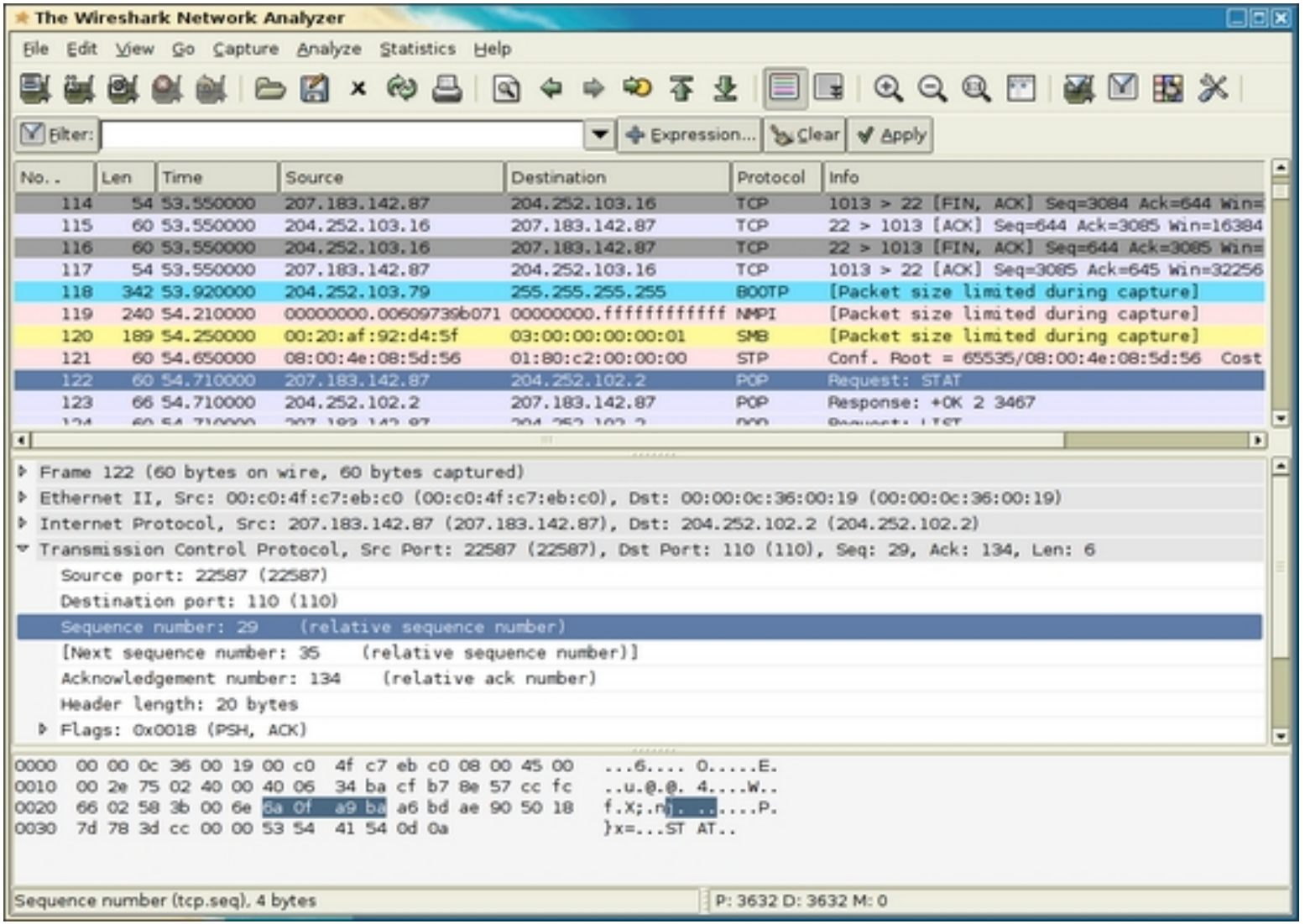
```
C:\>iperf -c 195.128.64.194 -p 4665 -t 60
------------------------------------------------------------
Client connecting to 195.128.64.194, TCP port 4665
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[1916] local 172.27.7.106 port 4632 connected with 195.128.64.194 port 4665
[ ID] Interval       Transfer     Bandwidth
[1916]  0.0-64.3 sec   160 KBytes  20.4 Kbits/sec

C:\>iperf -c 195.128.64.194 -p 4665 -t 180
------------------------------------------------------------
Client connecting to 195.128.64.194, TCP port 4665
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[1916] local 172.27.7.106 port 4633 connected with 195.128.64.194 port 4665
[ ID] Interval       Transfer     Bandwidth
[1916]  0.0-187.1 sec   528 KBytes  23.1 Kbits/sec

C:\>iperf -c 195.128.64.194 -p 4665 -t 60
------------------------------------------------------------
Client connecting to 195.128.64.194, TCP port 4665
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[1916] local 172.27.7.106 port 4667 connected with 195.128.64.194 port 4665
[ ID] Interval       Transfer     Bandwidth
[1916]  0.0-65.1 sec   136 KBytes  17.1 Kbits/sec
```

Iperf
(Windows) en ligne de commande

Ecoute et enregistrement de trafic



WireShark + WinPcap (Windows)

Pour le WiFi ajouter Airpcap

Airpcap permet l'émulation du mode monitor sur l'interface radio des adaptateurs USB (Windows)

Crédits

- **Merci aux auteurs de ces contributions :**
  - http://stielec.ac-aix-marseille.fr/cours/caleca/wifi/
  - http://www.ebg.net/evenements/pdf/EBG_LBwifi.pdf
  - http://reseau.erasme.org/article.php3?id_article=1160
- **Contenu**
  - non garanti exempt d'erreurs ;)
  - sous licence Creative Commons
    - Paternité
    - Pas d'Utilisation Commerciale
    - Partage des Conditions Initiales à l'Identique
    - http://creativecommons.org/licenses/by-nc-sa/2.0/fr/
- **Pour toute question ou contact :** pvincent@erasme.org
- **Merci !**