Wi-Fi

bases théoriques

et pratiques

Patrick VINCENT
pvincent@erasme.org

PLAN

- Partie 1 - Les réseaux sans Fil
- Partie 2 - La norme Wi-Fi (802.11)
- Partie 3 - Configurer un réseau Wi-Fi : TCP-IP
- Partie 4 - Matériel : Portée, débit et puissance
- Partie 5 - Sécurité
- Partie 6 - Déploiement d'un réseau
- Partie 7 - Élargissement et TPs à la demande

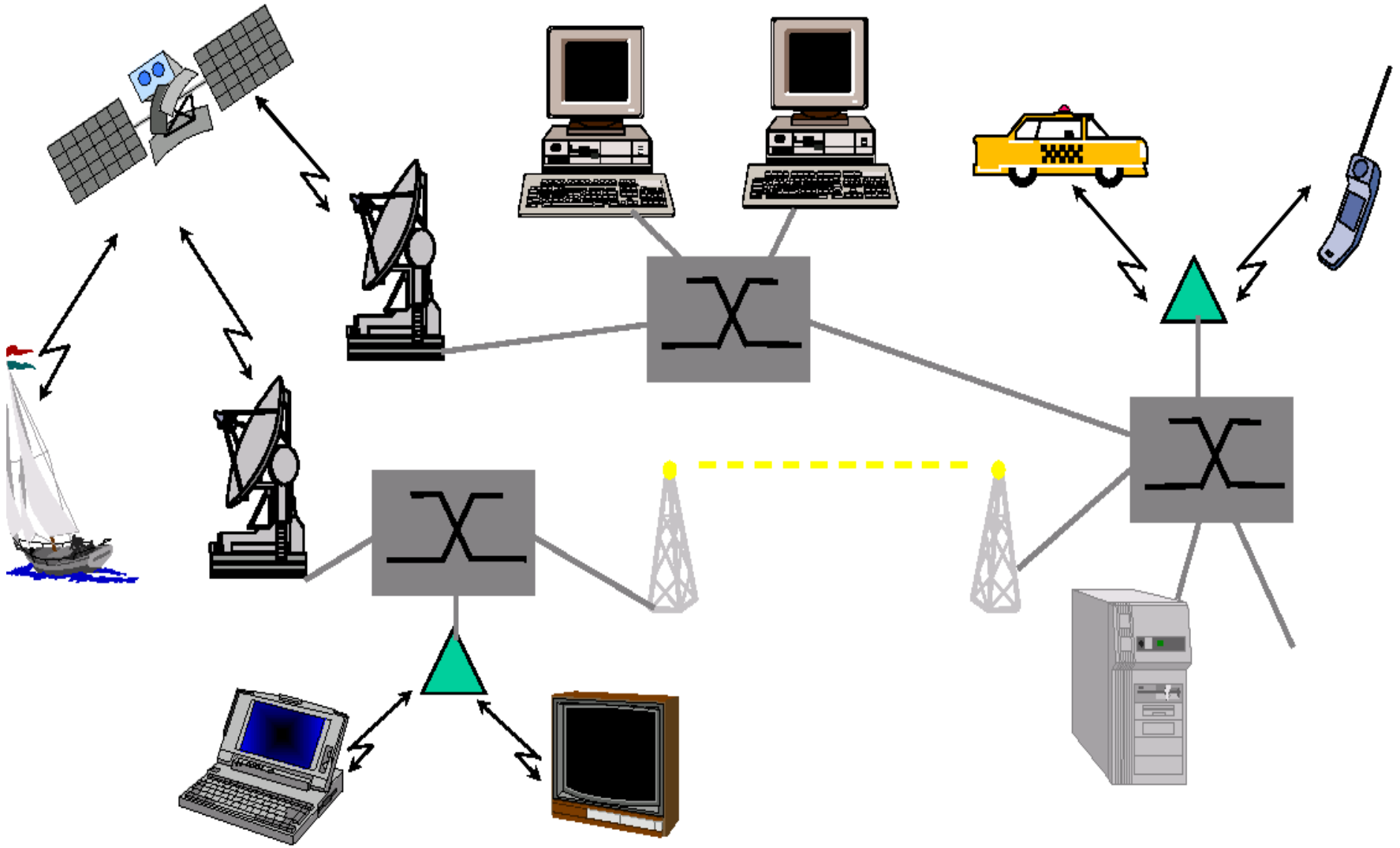
Objectifs

- Maîtriser les aspects théoriques de la norme WiFi et les notions de propagation radio
- Être capable de configurer un réseau sans fil local simple : aspects réseau (IP) et radio (WiFi)
- Être capable d'analyser une problématique de desserte sans fil et de dimensionner une solution
- Maîtriser les aspects liés à la sécurité des configurations

Partie 1

Les réseaux sans fil

Le sans fil omniprésent ?



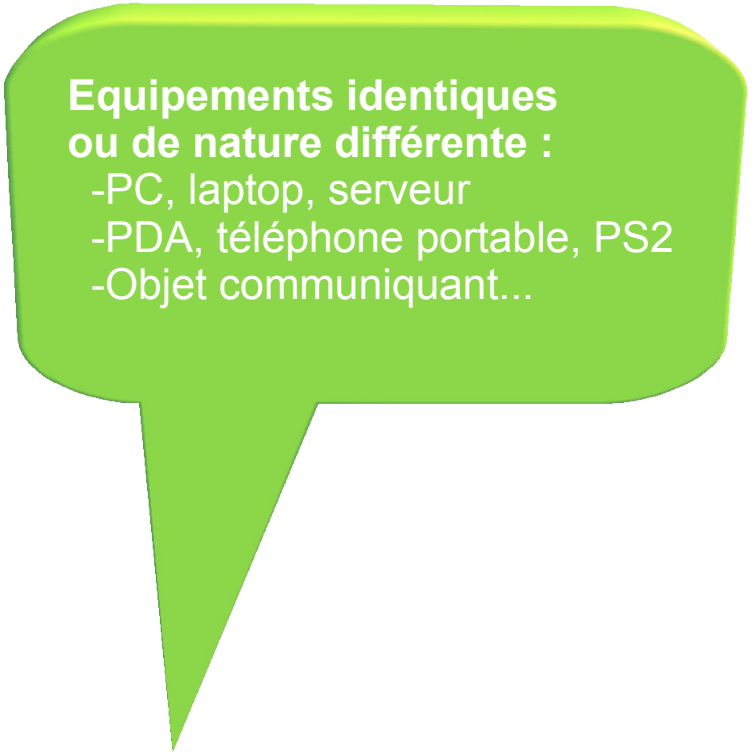
Source : anonyme sur Internet

Définition

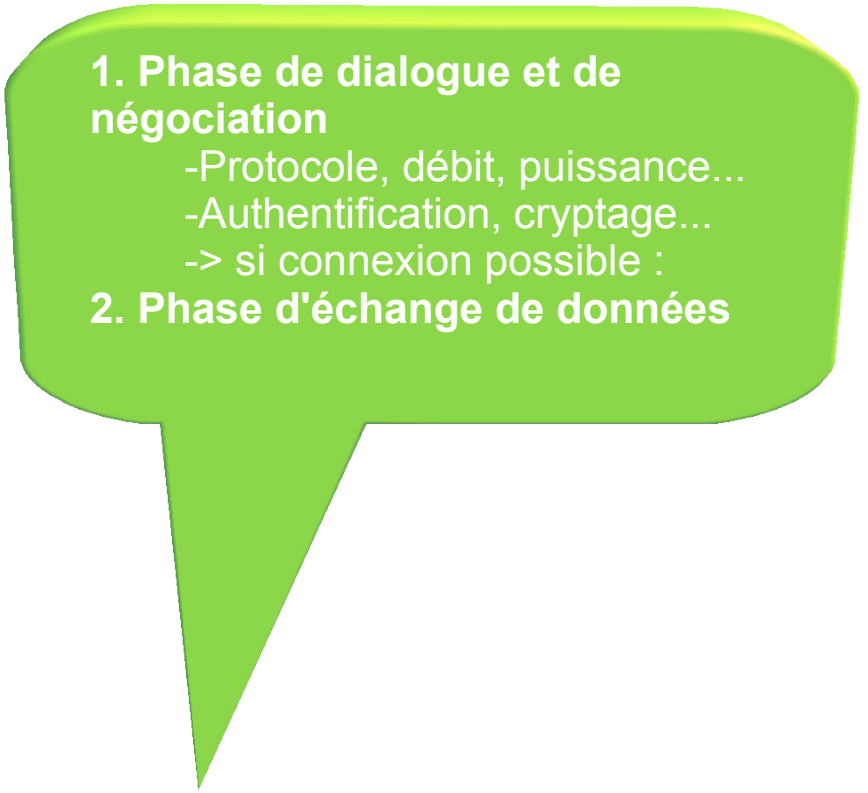
- Des protocoles sans fils connus... et inconnus :
  - IR, Bluetooth, RFID, Zigbee
  - GPS, GPRS, UMTS (3G), Satellite
  - WiFi, Wimax

- Définition d'un réseau sans fil :

« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »

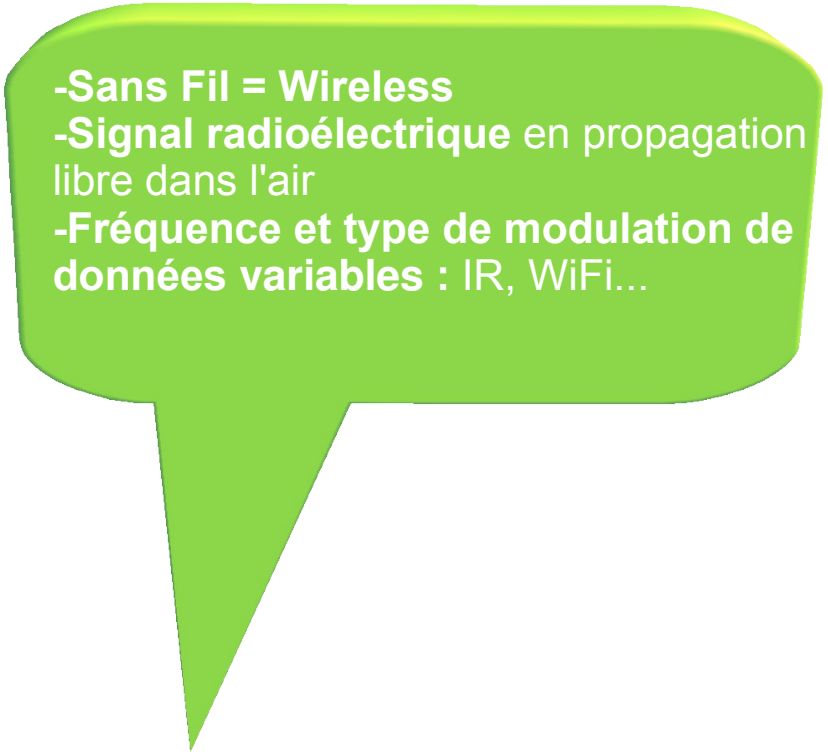


« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »



« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »

« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »



« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement »

Distinction récente pour caractériser une liaison selon :

-la vitesse de déplacement

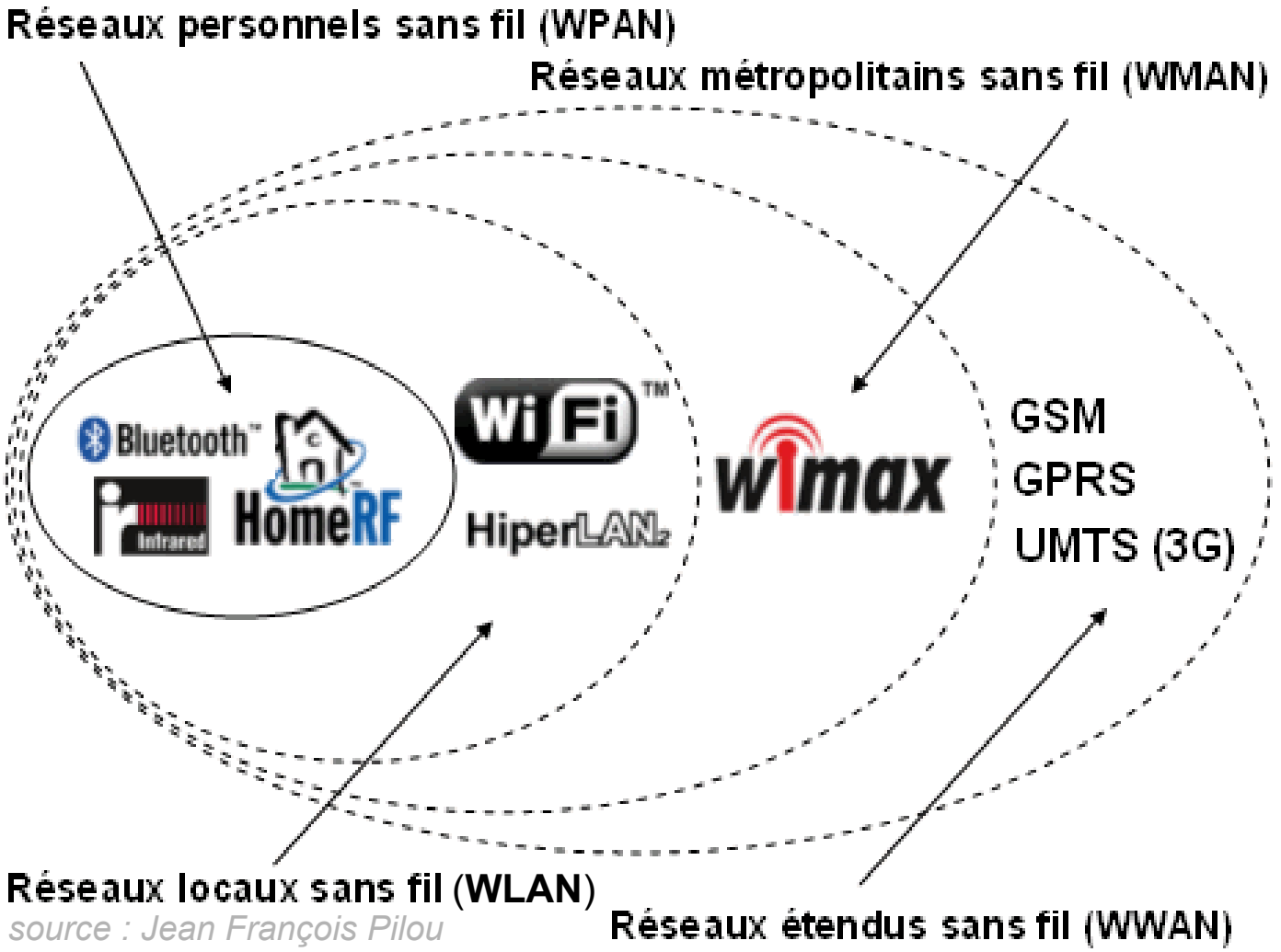
-la zone de couverture

« réseau où au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne, directement ou indirectement... en permettant un déplacement du terminal »

Critères de classification

- Radio : fréquence, modulation et puissance
- Protocole de communication et de sécurité
- Terminaux supportés
- Architecture (topologie) du réseau
- Débit
- Portée
- Coût

Les catégories de réseau sans fil



source : Jean François Pilou

Intérêt du sans fil

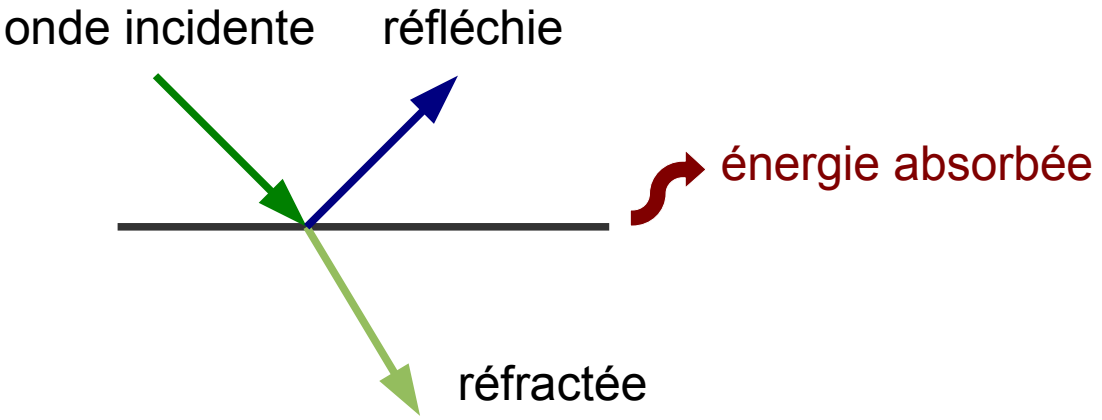
- Facilité de déploiement
- Interopérabilité avec les réseaux filaires
- Débits adaptés à un usage professionnel
- Grande souplesse et faiblement structurant (chantier, exposition, locaux temporaires)
- Non destructif (monuments historiques, sites classés)
- Grande mobilité
- Coût

... et contraintes

- Limites des ondes radio
  - sensibles aux interférences (micro-ondes, autre réseau...)
  - occupation progressive des bandes de fréquence : autorégulation
- Sécurité : données circulant librement
  - nécessite de déployer des solutions de sécurité adaptées
- Réglementation
  - fréquences et puissances d'émission contrôlées par l'Etat
- Débit : mutualisé et variable
  - Partagé entre les utilisateurs et dépendant des conditions d'usage
  - Globalement dix fois inférieur au filaire
- Aspects sanitaires

Notions de propagation radio

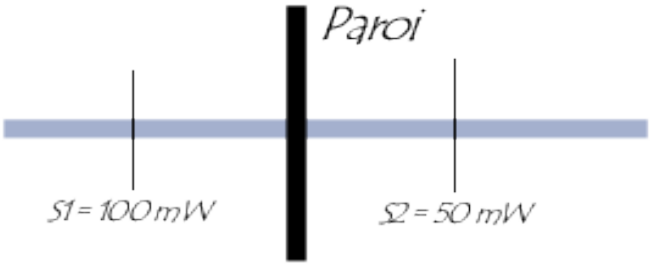
- Les ondes radio se propagent en ligne droite dans plusieurs directions depuis leur source d'émission
- Leur vitesse dans le vide est de 3.10^8 m/s
- Lorsqu'elle rencontre un obstacle, l'onde est divisée et son énergie est répartie :



Gain et atténuation

- Atténuation
  - Lorsqu'elle traverse un obstacle, une partie de l'énergie de l'onde est absorbée
- Amplification
  - Lorsqu'il est capté par une antenne, la puissance du signal de l'onde est amplifié
- L'atténuation (ou le gain) est le rapport entre la puissance du signal avant et après modification

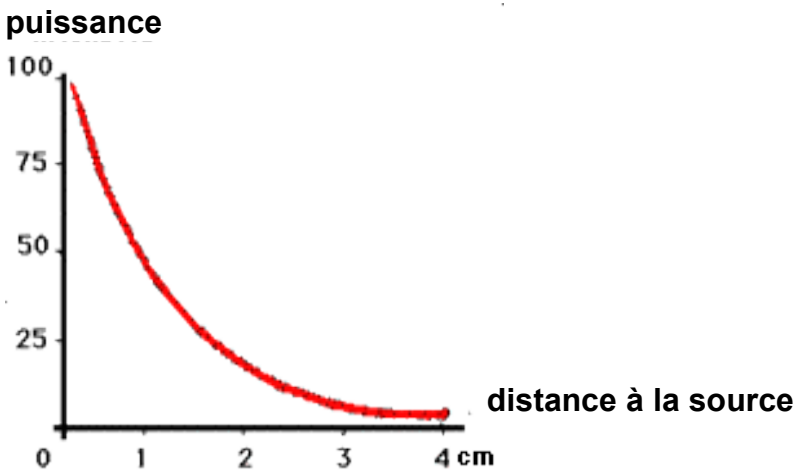
Atténuation (dB) = (10) * log (S2/S1)



$$R\,(dB) = 10 \log \left(\frac{S2}{S1} \right) = -3\,dB$$

Absorption des ondes

- L'énergie d'une onde électromagnétique est progressivement dégradée au cours de sa propagation dans l'air
  - L'onde électromagnétique qui voyage rencontre des électrons qu'elle va exciter. Ceux-ci vont ré émettre à leur tour du rayonnement ce qui perturbera le signal et donc l'atténuera.
- Les signaux se dégradent avec la distance et avec les obstacles, limitant ainsi la portée et le débit de la liaison



Cas perturbants liés au WiFi

- Fréquence
  - La **fréquence** moyenne de la porteuse du WiFi est de **2,437 Ghz**
  - La fréquence de résonance de l'eau est de **2,45 Ghz**
- Longeur d'onde
  - La longueur d'onde du WiFi est de 12,31 cm
  - **Le quart d'onde** (taille des objets absobant l'énergie de cette onde) est de **3,05 cm**
- Les éléments contenant de l'eau et / ou de taille proches de 3 cm absorbent facilement l'énergie du signal du Wi-Fi (feuilles par exemple)

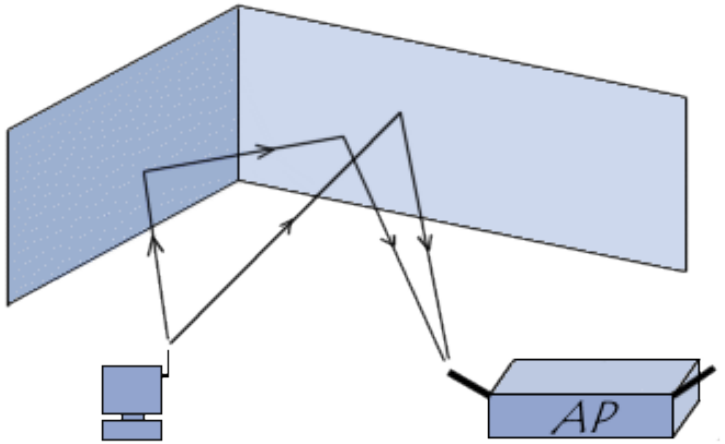
Ondes, fréquences et couverture

- Plus la fréquence est élevée plus le phénomène d'absorption est élevé, donc plus la distance de couverture est faible.
  - C'est pour cela que les communications radio se font sur des fréquences d'une centaine de MHz.
  - Pour le WiFi, par exemple on peut difficilement faire plus de 10km avec du matériel « classique ».

- Plus la fréquence est élevée, plus le débit de de données peut être important mais plus la couverture est faible.
- Puissance élevée : couverture plus grande mais durée

Chemins multiples (multipath)

- Par réflexions successives, une onde peut atteindre une station en empruntant des chemins multiples et générer des interférences
- La présence de deux antennes sur un point d'accès permets de contrôler et de séparer les signaux



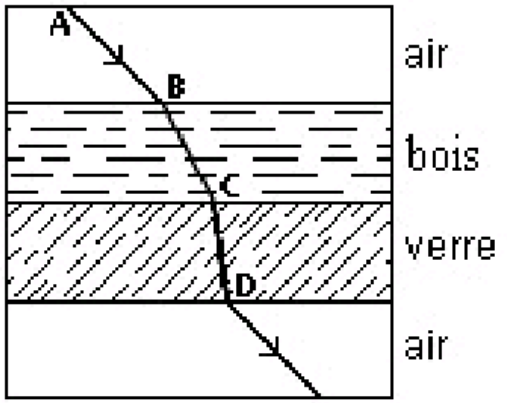
source : Jean François Pilou

En fonction du milieu traversé

Affaiblissement pour le 2.4 GHz

Matériaux	Affaiblissement	Exemples
Air	Négligeable	Champ libre
Bois	Faible	Porte, plancher, cloison
Plastique	Faible	Cloison
Verre	Faible	Vitres non teintées
Verre teinté	Moyen	Vitres teintées
Eau	Moyen	Aquarium, fontaine
Etres vivants	Moyen	Foule, animaux, humains, végétation
Briques	Moyen	Murs
Plâtre	Moyen	Cloisons
Céramique	Elevé	Carrelage
Papier	Elevé	Rouleaux de papier
Béton	Elevé	Murs porteurs, étages, piliers
Verre blindé	Elevé	Vitres pare-balles
Métal	Très élevé	Béton armé, miroirs, armoire métallique, cage d'ascenseur

Réfraction pour le 2.4 GHz



Partie 2

La norme 802.11 (IEEE)

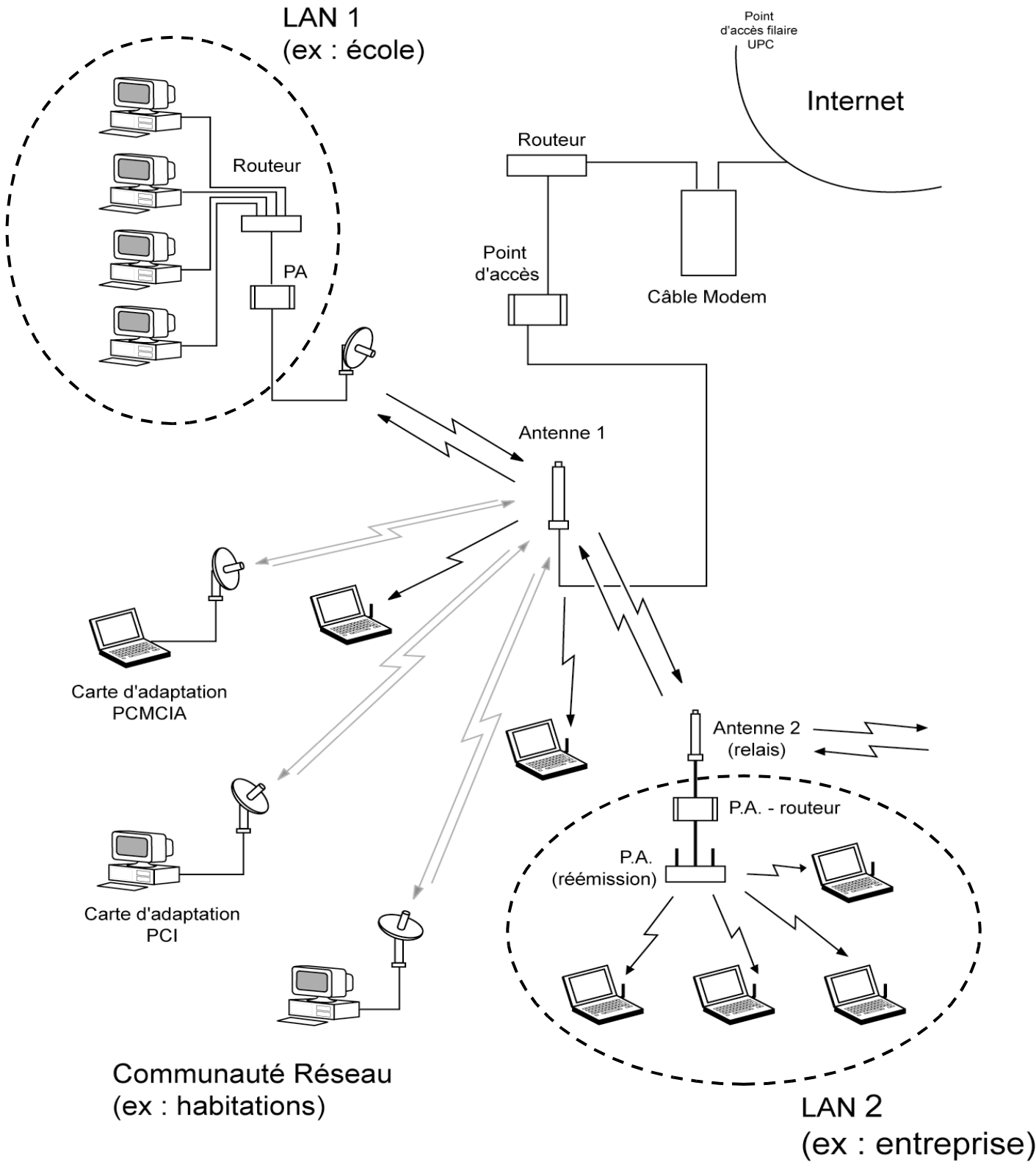
Présentation du Wi-Fi

Définition

- Le Wi-Fi
  - permets à des équipements informatiques de se connecter et d'échanger des données par voie radio
  - s'intègre dans la pile IP (sous-couche)

- Un WLAN
  - est un réseau sans fil local. Il regroupe les équipements associés entre eux utilisant le même nom de réseau
  - fonctionne en architecture cellulaire : chaque **cellule** possède sa zone de couverture et ses caractéristiques d'association

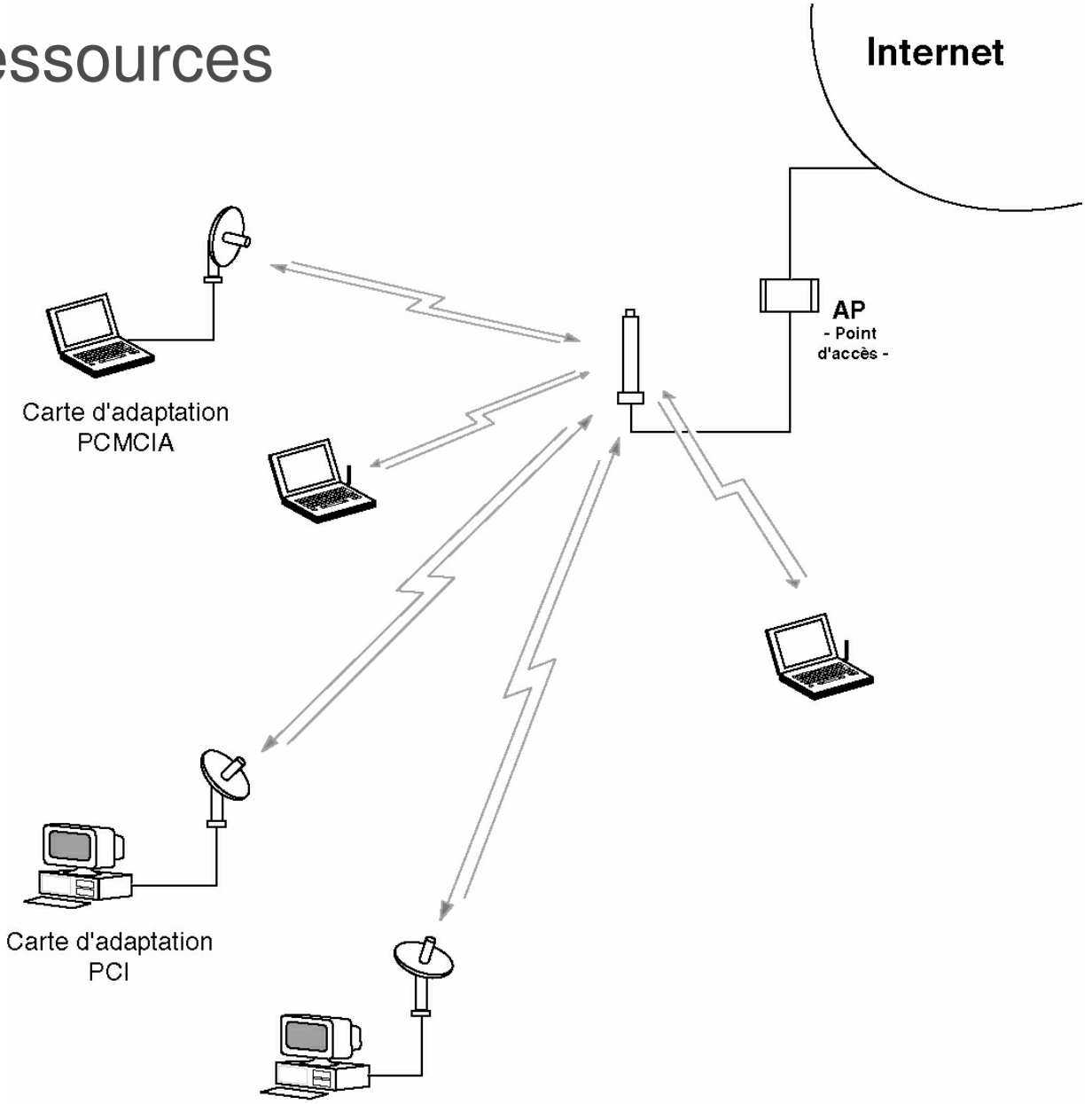
Des possibilités variées



Source : Centre Erasme

Usages

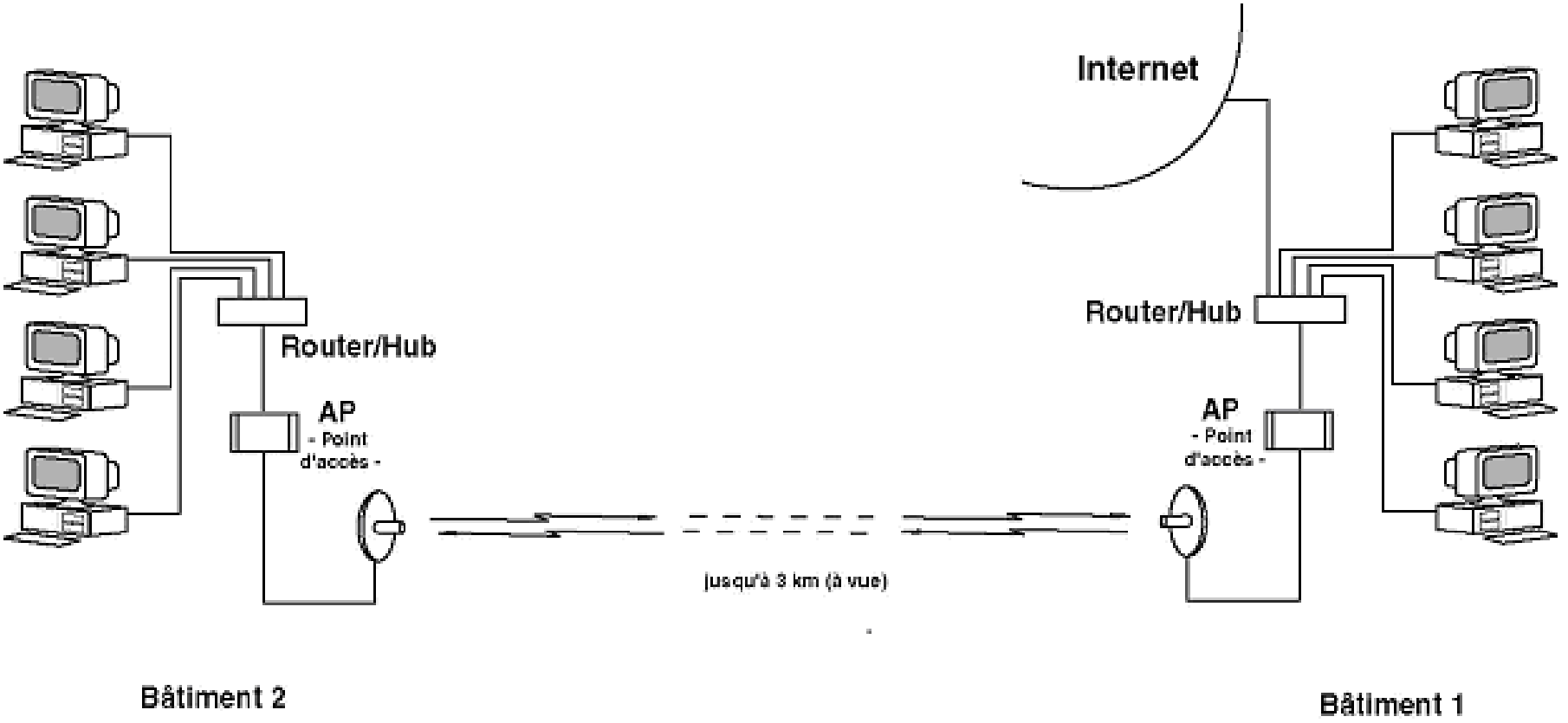
- Partager des ressources



Source : Centre Erasme

Usages

- Étendre un réseau existant



Source : Centre Erasme

Usages du Wi-Fi

- Étendre un réseau existant
  - Pont WiFi
- Partager une ressource
  - Switch / Accès Internet, Imprimante, serveur
- Réaliser un portail d'accès authentifié
  - Hot-Spot
- Utiliser des objets communiquants
  - Lecteur de flux RSS, Nazbatag, localisation
- Accéder à une ressource en mobilité
  - Hopitaux
- Déployer un réseau urbain alternatif aux opérateurs
  - Les villes Internet

Quelques données

- **Débit** : Association de 1 à 54 Mbps. 50 % de débit effectif.
- **Portée** : de quelques centaines de mètres à plusieurs km.

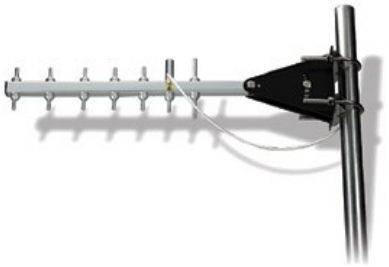
  Ce résultat sera fonction de :
  - la **puissance**$_{em}$: couples AP + antennes choisis
  - la **sensibilité**$_{rec}$: inv proportionnelle au débit choisi
  - **affaiblissement**$_{ligne}$: masques radio et interférences
- **Puissance autorisée par l'ART** : 100 mW en sortie d'antenne pour les réseaux privés et indépendants.
- **Santé** : rayonnement 10 fois inférieur à celui d'un téléphone portable.

Le matériel employé

- **Points d'accès (eq. switch)**

- **Cartes clientes (éq. carte réseau)**

- **Antennes et connectiques**



- **Matériel Ethernet**

Etat des autorisations en France

1- Création ou extension d'**un réseau privé** par technologie WiFi 2.4 Ghz libre dans le Rhône depuis le mois de Janvier 2003.

réseau privé (ou indépendant) = pas de vocation à commercialiser un service de télécommunication ou activité pas assimilée à celle d'un opérateur.

2- Utilisation du WiFi dans le but de **fournir un accès Internet payant à un tiers** : demande de licence expérimentale auprès de l'ART.

Ces deux procédures sont soumises au respect de normes européennes et françaises **d'utilisation des fréquences** et **des puissances** émises (ETSI) :

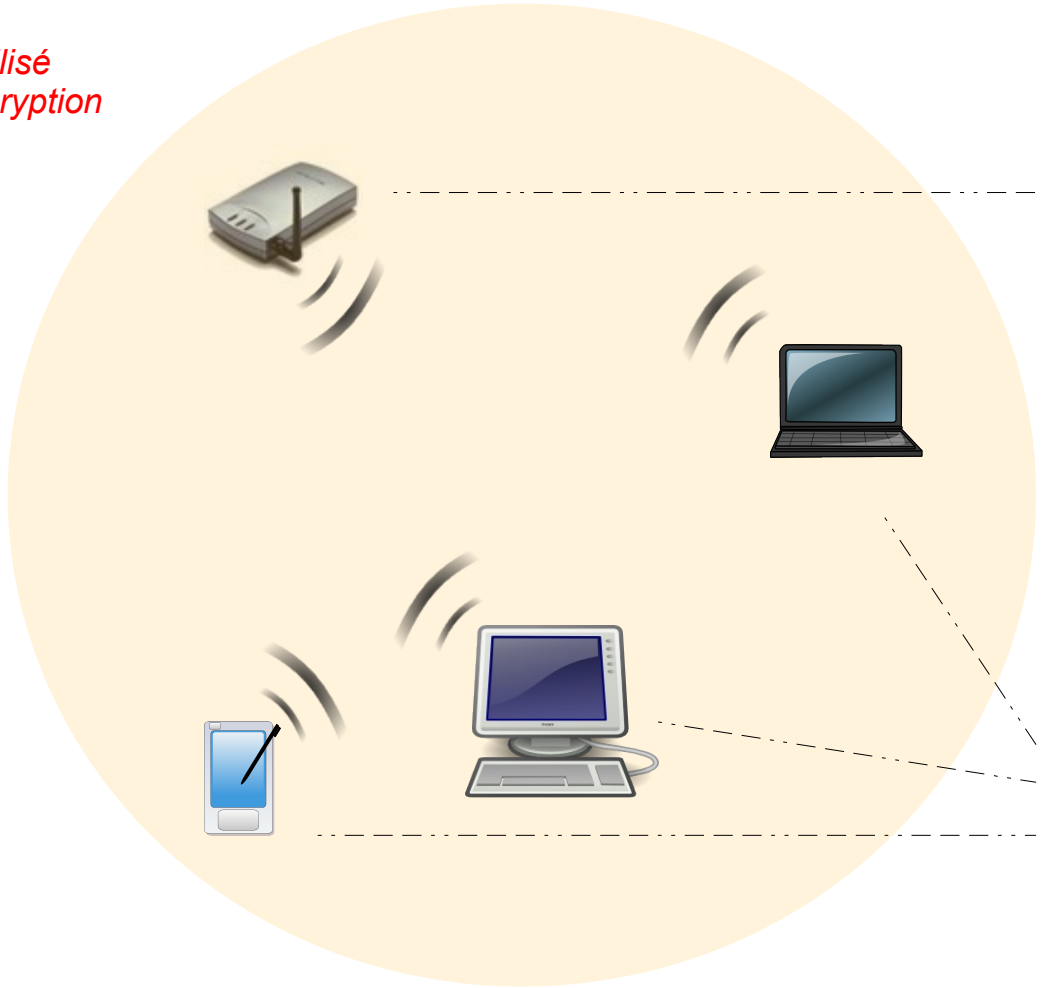
Fréquences en MHz	Intérieur	Extérieur
2400 2454	**100 mW**	**100 mW**
2483,5		**10 mW et 100 mW avec accord Défense sur propriétés privées**

Une architecture cellulaire

Un équipement Wi-Fi
= 2 interfaces

Cellule
(zone de couverture)

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

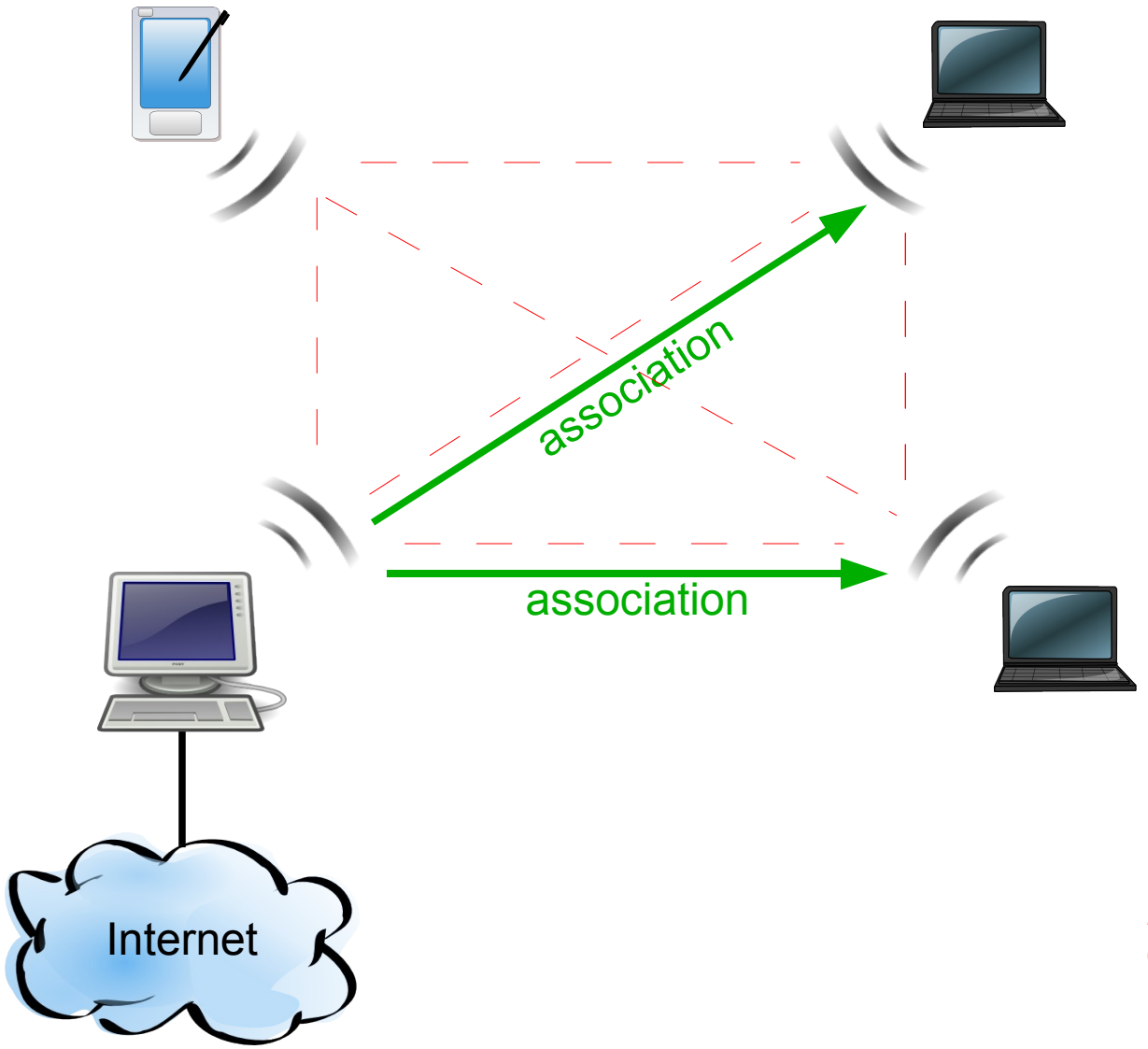


Point d'accès
module WiFi
&
module Ethernet

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

Topologies

Topologie ad-hoc

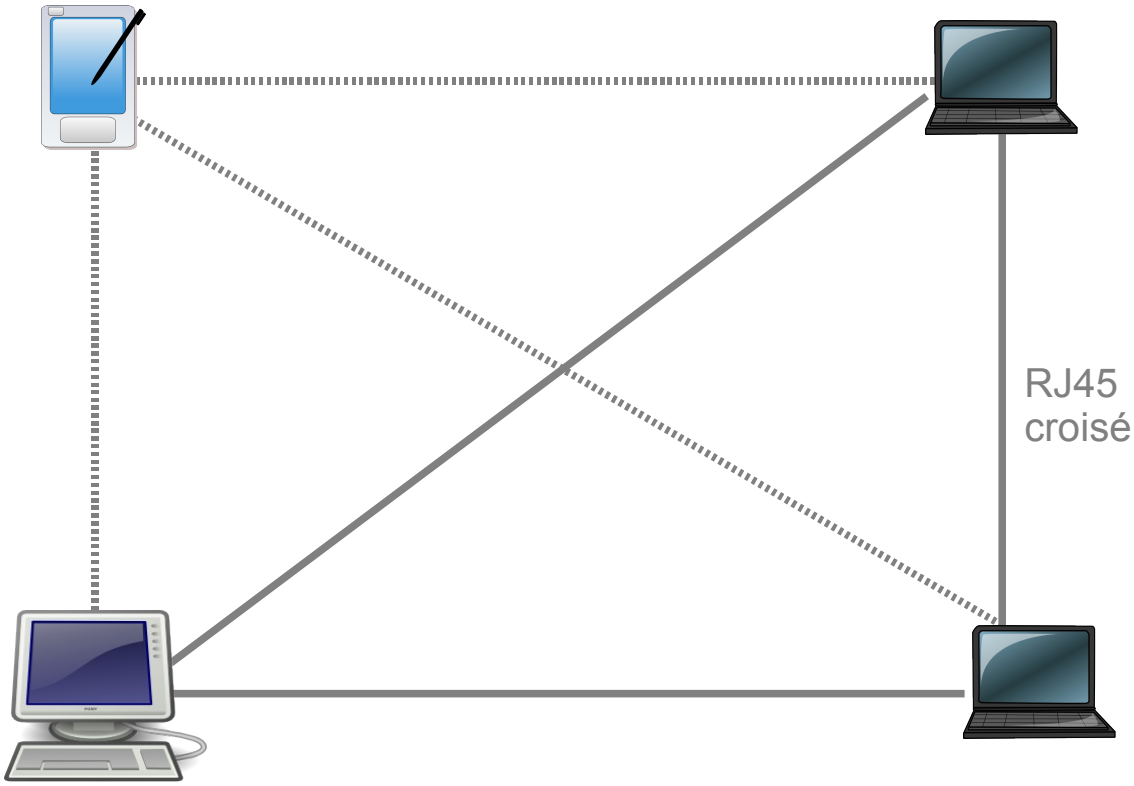


IBSS

Ensemble de services de base indépendant

... équivalent

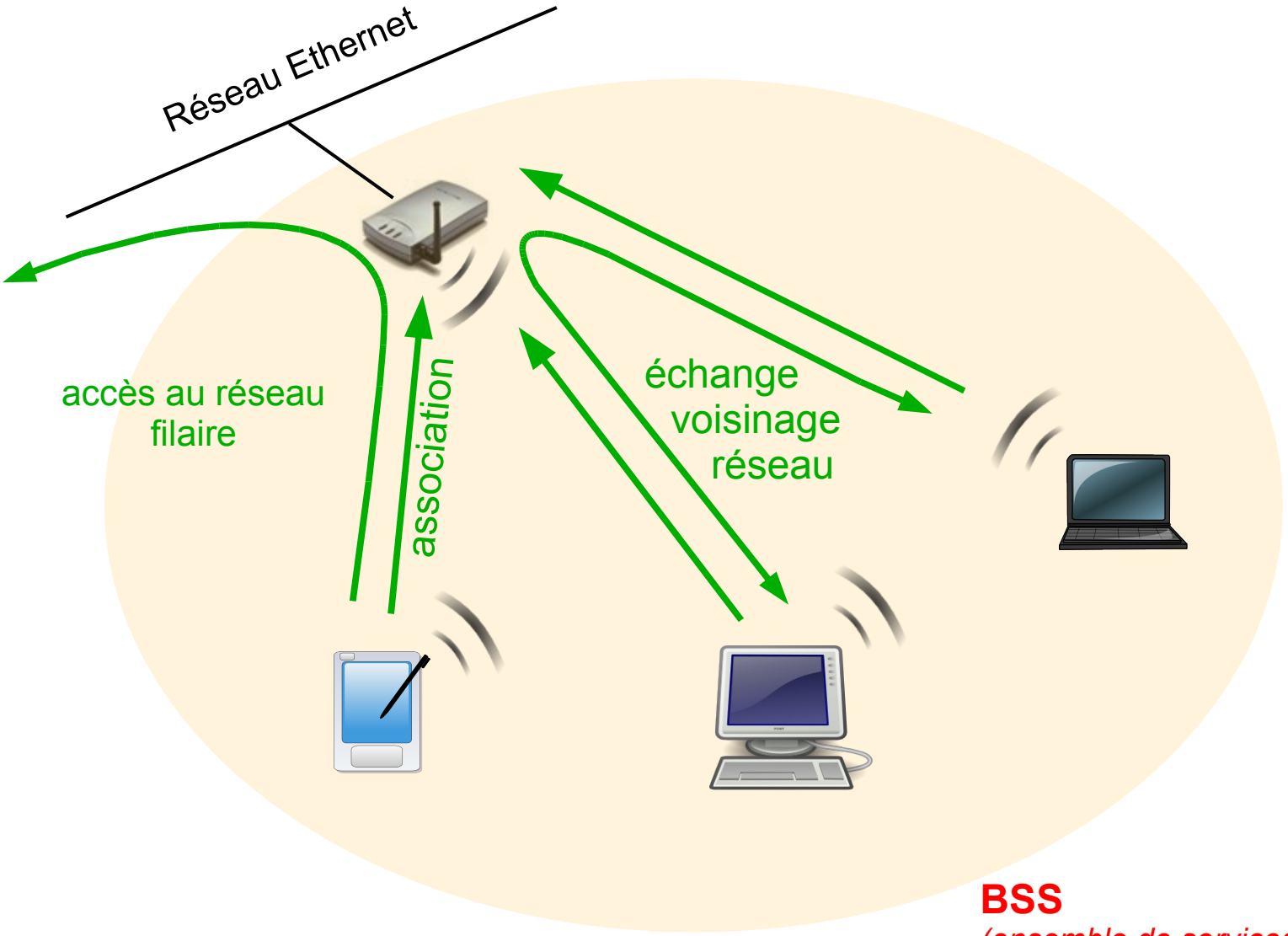
à un câble croisé en Ethernet



Topologie ad-hoc

- Des stations équipées d'adaptateurs WiFi en mode ad-hoc forment un réseau Mesh (ad-hoc)
  - Chaque adaptateur joue successivement le rôle d'AP et de client. Les machines communiquent ensemble en point à point (peer to peer).
  - Ce système n'intègre pas nativement de protocole de routage. Une norme IEEE en étude le prévoit.
  - La portée du réseau est limité aux portées de chaque paire.
- Cet ensemble de services de base indépendants (IBSS) est adapté aux réseaux temporaires lorsqu'aucun AP n'est disponible

Topologie Infrastructure

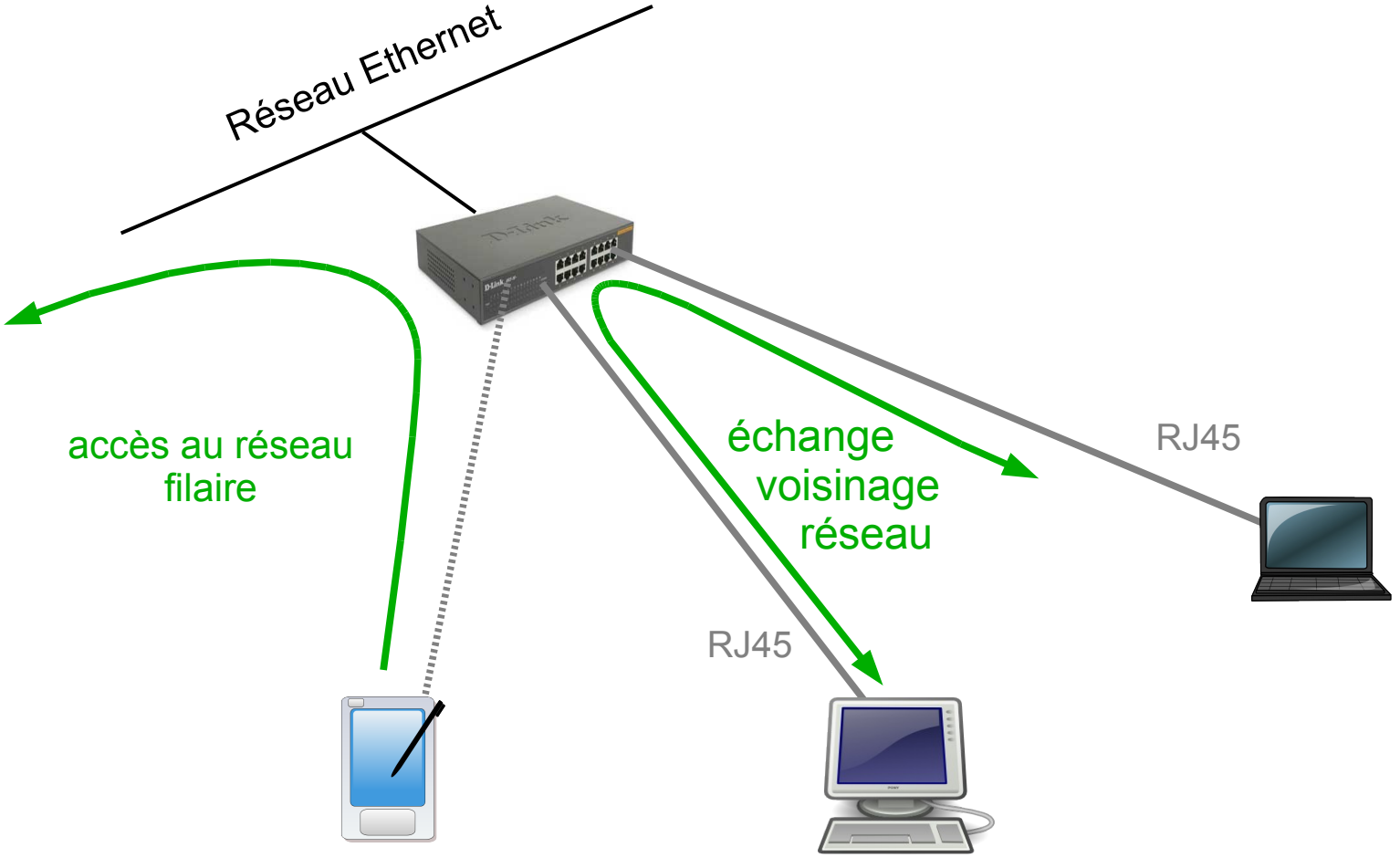


BSS

(ensemble de services de base)

BSSID = @Mac du point d'accès

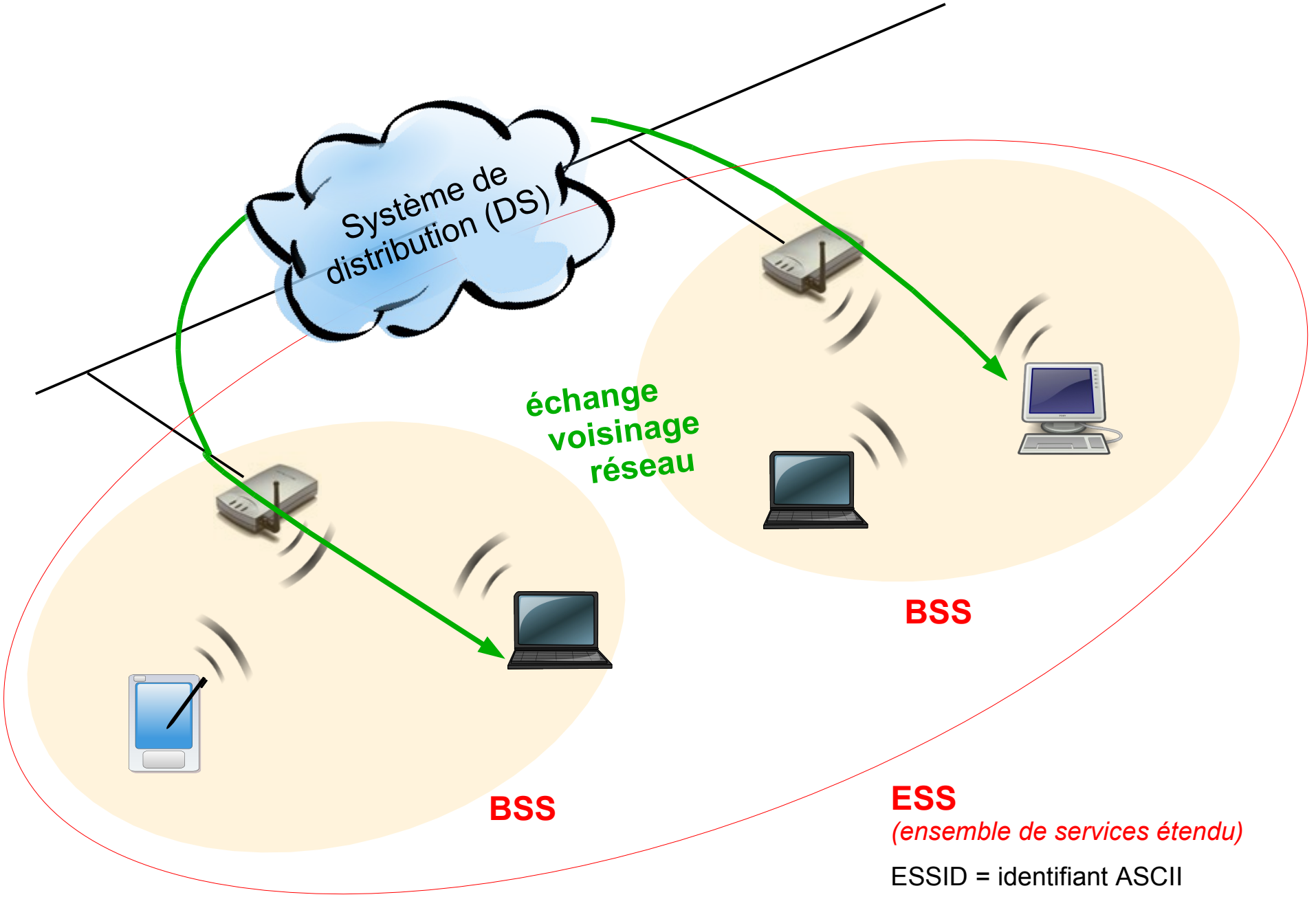
... équivalent à un hub en Ethernet



Topologie infrastructure

- Chaque station se connecte à un point d'accès qui lui offre un ensemble de services de base (BSS)
  - association et ev. authentification
  - connexion à la ressource Ethernet (bridge IP)
  - communication avec les autres stations (IP)
  - BSS caractérisé par son **BSSID** = @Mac du point d'accès
- A un point d'accès peuvent être associées jusqu'à 100 stations
- Le support de transmission est partagé entre les stations, de même que le débit radio
- Le point d'accès est mode **AP** (parent) et les stations en mode **client** (enfant)

Topologie infrastructure étendue

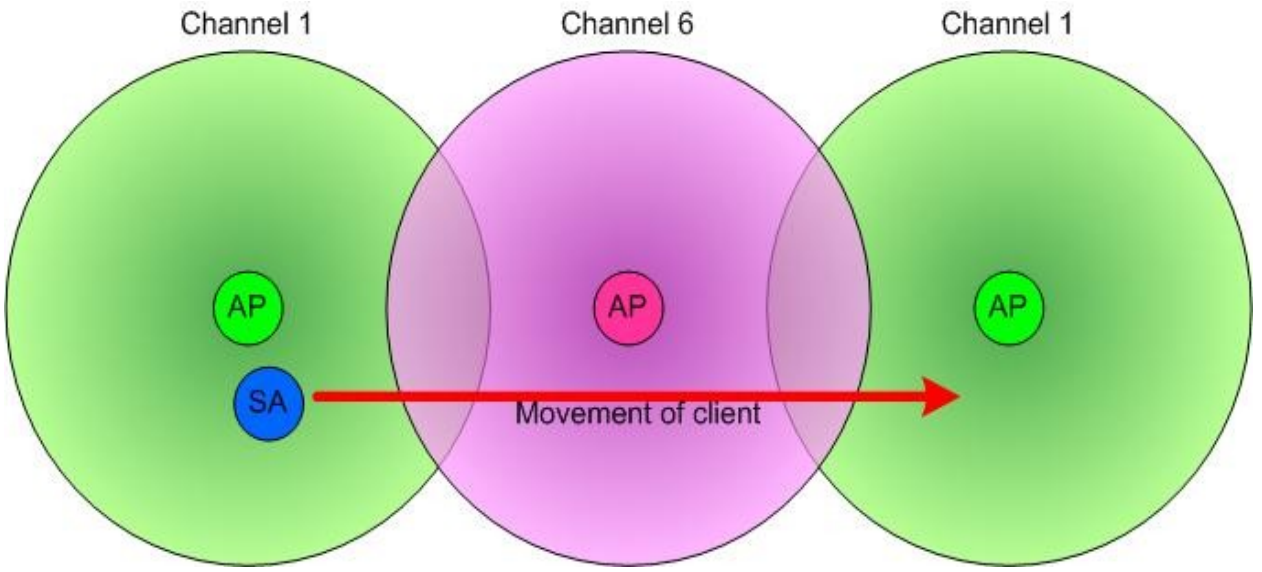


Topologie infrastructure étendue

- En reliant plusieurs points d'accès par un service de distribution (DS) on obtient un ensemble de services étendu (ESS)
  - le ESS est repéré par un (E)**SSID** = identifiant à 32 caractères au format ASCII nécessaire pour s'y associer
  - tous les AP du réseau doivent utiliser le même **SSID**
  - les cellules de l'ESS peuvent être disjointes ou se recouvrir pour offrir un service de mobilité (802.11f)
- Le service de distribution est la dorsale ou le backbone du réseau
  - réseau Ethernet
  - pont WiFi

Mobilité : notion de Roaming

- En fonction de l'organisation spatiale des canaux, on pourra offrir un service continu en mobilité : c'est le roaming (802.11f).
- Ex : flux streamé non coupé en réception
- Lors de la configuration, il faudra être vigilant quant au recouvrement des canaux



Association
et transfert de données

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

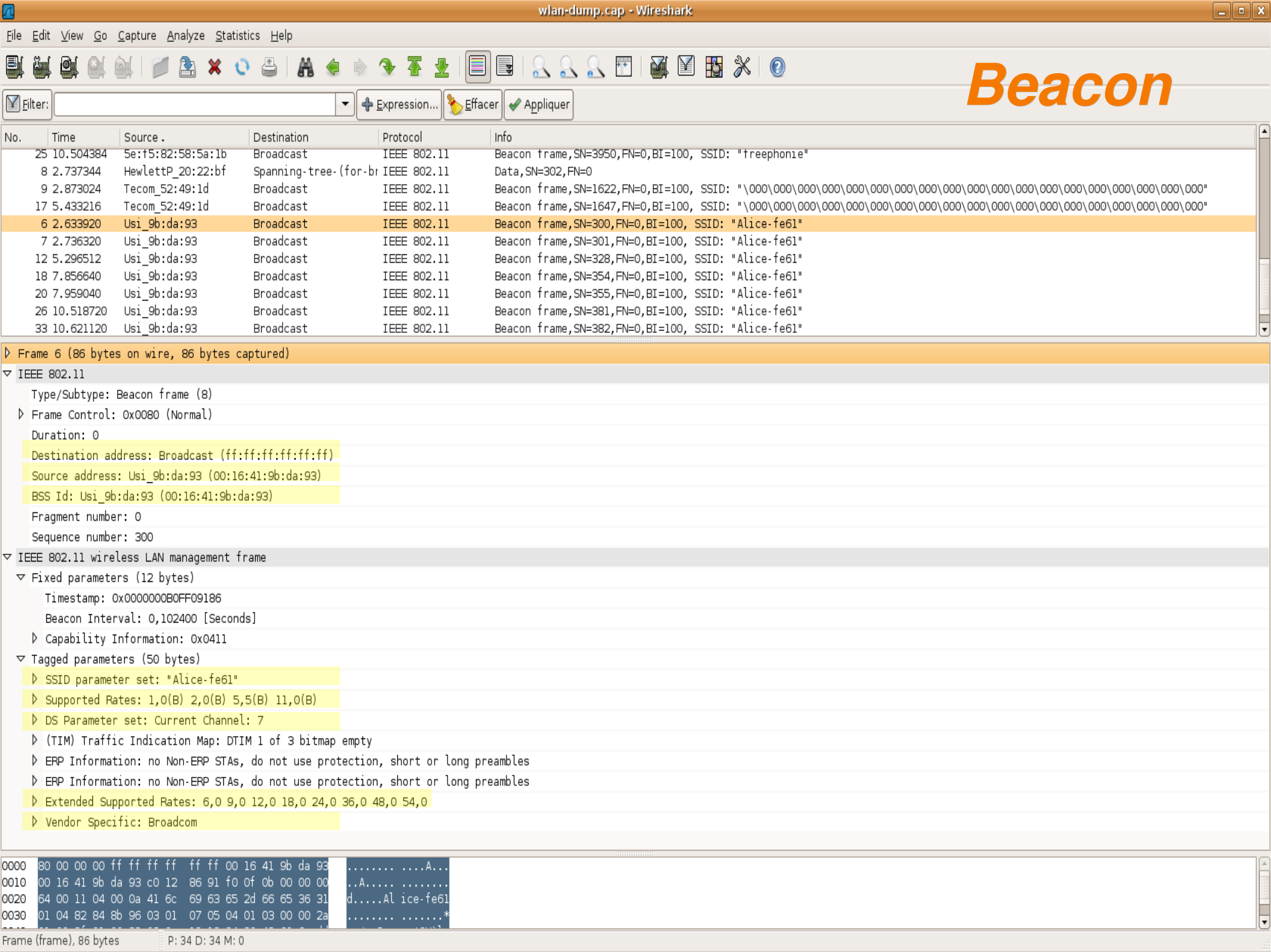
Mode Matériel	AP (parent)	client (enfant)	Ad-Hoc	Bridge	Répéteur	Monitor
Point d'accès	X	X		X	X	(X)
Adaptateur WiFi		X	X			(X)

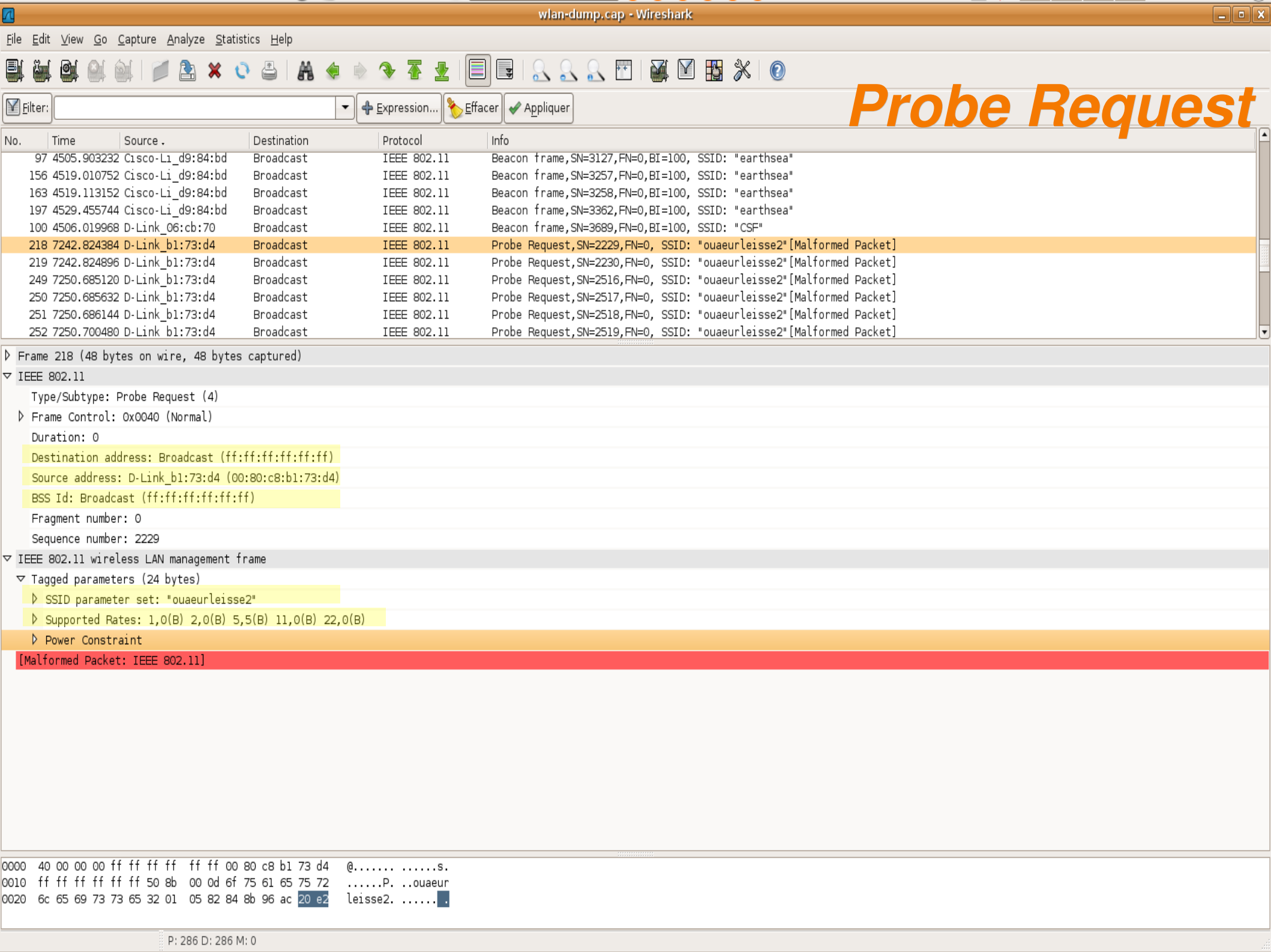
Mécanisme d'association (1)

- Le point d'accès
  - diffuse régulièrement (0,1s) une **trame balise** (*beacon*) avec
    - son **BSSID** (ex : 00:16:41:9B:DA:93)
    - ses **caractéristiques radio** (ex : canal 2 / 54 Mbps / ENC)
    - optionellement son E**SSID** en clair (ex : tsunami)
- L'adaptateur client
  - lorsqu'il détecte son entrée dans une cellule, il diffuse une **requête de sondage** (*probe request*) avec
    - l'E**SSID** sur lequel il est configuré (ex : tsunami)
    - ses **caractéristiques radio** (ex : 11 Mbps)
  - autrement, ou si aucun ESSID n'est configuré
    - il écoute le réseau à la recherche d'un ESSID en clair

Mécanisme d'association (2)

- Le point d'accès
  - lorsqu'il reçoit une **requête de sondage** (probe request) vérifie
    - le E**SSID**
    - les **caractéristiques radio** proposées
  - si les données sont compatibles, il envoie une réponse avec
    - les informations sur sa charge
    - des données de synchronisation (puissance / débit)
- L'adaptateur client
  - évalue la qualité du signal émis et la distance du PA
  - choisit le PA avec le meilleur débit et la plus faible charge en cas de propositions multiples
  - envoie une demande d'association au PA choisi


wlan-dump.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Beacon
Filter: Expression... Effacer Appliquer
No. Time Source Destination Protocol Info
25 10.504384 5e:f5:82:58:5a:1b Broadcast IEEE 802.11 Beacon frame,SN=3950,FN=0,BI=100, SSID: "freephonie"
8 2.737344 HewlettP_20:22:bf Spanning-tree-(for-br IEEE 802.11 Data,SN=302,FN=0
9 2.873024 Tecom_52:49:1d Broadcast IEEE 802.11 Beacon frame,SN=1622,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000"
17 5.433216 Tecom_52:49:1d Broadcast IEEE 802.11 Beacon frame,SN=1647,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000"
6 2.633920 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=300,FN=0,BI=100, SSID: "Alice-fe61"
7 2.736320 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=301,FN=0,BI=100, SSID: "Alice-fe61"
12 5.296512 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=328,FN=0,BI=100, SSID: "Alice-fe61"
18 7.856640 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=354,FN=0,BI=100, SSID: "Alice-fe61"
20 7.959040 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=355,FN=0,BI=100, SSID: "Alice-fe61"
26 10.518720 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=381,FN=0,BI=100, SSID: "Alice-fe61"
33 10.621120 Usi_9b:da:93 Broadcast IEEE 802.11 Beacon frame,SN=382,FN=0,BI=100, SSID: "Alice-fe61"
Frame 6 (86 bytes on wire, 86 bytes captured)
IEEE 802.11
Type/Subtype: Beacon frame (8)
Frame Control: 0x0080 (Normal)
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: Usi_9b:da:93 (00:16:41:9b:da:93)
BSS Id: Usi_9b:da:93 (00:16:41:9b:da:93)
Fragment number: 0
Sequence number: 300
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Timestamp: 0x0000000B0FF09186
Beacon Interval: 0,102400 [Seconds]
Capability Information: 0x0411
Tagged parameters (50 bytes)
SSID parameter set: "Alice-fe61"
Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B)
DS Parameter set: Current Channel: 7
(TIM) Traffic Indication Map: DTIM 1 of 3 bitmap empty
ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
Extended Supported Rates: 6,0 9,0 12,0 18,0 24,0 36,0 48,0 54,0
Vendor Specific: Broadcom
0000 80 00 00 00 ff ff ff ff ff ff 00 16 41 9b da 93 ....A...
0010 00 16 41 9b da 93 c0 12 86 91 f0 0f 0b 00 00 00 ..A..... ....
0020 64 00 11 04 00 0a 41 6c 69 63 65 2d 66 65 36 31 d.....Al ice-fe61
0030 01 04 82 84 8b 96 03 01 07 05 04 01 03 00 00 2a ....*
Frame (frame), 86 bytes
P: 34 D: 34 M: 0


wlan-dump.cap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Effacer Appliquer
Probe Request
No. Time Source Destination Protocol Info
97 4505.903232 Cisco-Li_d9:84:bd Broadcast IEEE 802.11 Beacon frame,SN=3127,FN=0,BI=100, SSID: "earthsea"
156 4519.010752 Cisco-Li_d9:84:bd Broadcast IEEE 802.11 Beacon frame,SN=3257,FN=0,BI=100, SSID: "earthsea"
163 4519.113152 Cisco-Li_d9:84:bd Broadcast IEEE 802.11 Beacon frame,SN=3258,FN=0,BI=100, SSID: "earthsea"
197 4529.455744 Cisco-Li_d9:84:bd Broadcast IEEE 802.11 Beacon frame,SN=3362,FN=0,BI=100, SSID: "earthsea"
100 4506.019968 D-Link_06:cb:70 Broadcast IEEE 802.11 Beacon frame,SN=3689,FN=0,BI=100, SSID: "CSF"
218 7242.824384 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2229,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
219 7242.824896 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2230,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
249 7250.685120 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2516,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
250 7250.685632 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2517,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
251 7250.686144 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2518,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
252 7250.700480 D-Link_b1:73:d4 Broadcast IEEE 802.11 Probe Request,SN=2519,FN=0, SSID: "ouaeurleisse2"[Malformed Packet]
Frame 218 (48 bytes on wire, 48 bytes captured)
IEEE 802.11
Type/Subtype: Probe Request (4)
Frame Control: 0x0040 (Normal)
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: D-Link_b1:73:d4 (00:80:c8:b1:73:d4)
BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
Fragment number: 0
Sequence number: 2229
IEEE 802.11 wireless LAN management frame
Tagged parameters (24 bytes)
SSID parameter set: "ouaeurleisse2"
Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 22,0(B)
Power Constraint
[Malformed Packet: IEEE 802.11]
0000 40 00 00 00 ff ff ff ff ff ff 00 80 c8 b1 73 d4 @..... ......s.
0010 ff ff ff ff ff ff 50 8b 00 0d 6f 75 61 65 75 72 ......P. ..ouaeur
0020 6c 65 69 73 73 65 32 01 05 82 84 8b 96 ac 20 e2 leisse2. ......
P: 286 D: 286 M: 0

Mécanisme d'association

Station

Point d'accès

Broadcast

Beacons

-BSSID
-Radio (canal, débit, puiss)
-(ESSID)

Découverte du réseau

Probe Request

-ESSID
-Débit

Probe Response

-Débit
-Charge

Authentification

Authentification

-Clefs

-Réponse du processus d'authentification

Association

Association Request

Association Response

Mécanisme de roaming

Station

Point d'accès (nouveau)

Point d'accès (ancien)

Re-association Request

Handover

Handover Request

Handover Response

Authentification

Authentification

Association

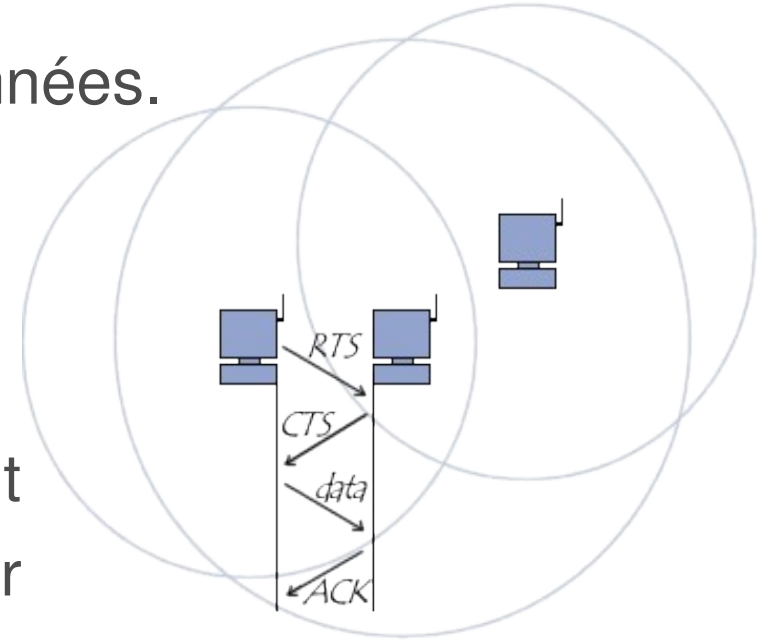
Re-association Response

Mécanisme de transfert de données

- Inspiré du CSMA/CD de l'Ethernet
  - Carrier Sense Multiple Access with Collision Detect
    - Chaque machine est libre de communiquer à n'importe quel moment.
    - Elle vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine.
    - Autrement elles patientent pendant un temps aléatoire avant de recommencer à émettre.
  - Mais en WiFi, deux stations communiquant avec le même récepteur ne s'entendent pas forcément pour savoir si le media est libre (portée).
- CSMA/CA
  - Carrier Sense Multiple Access with Collision Avoidance incluse dans la fonction DCF (Distributed Coordination Function) de la couche MAC du 802.11
  - Utilise un mécanisme d'esquive de collision basé sur l'accusé de réceptions réciproques entre l'émetteur et le récepteur.

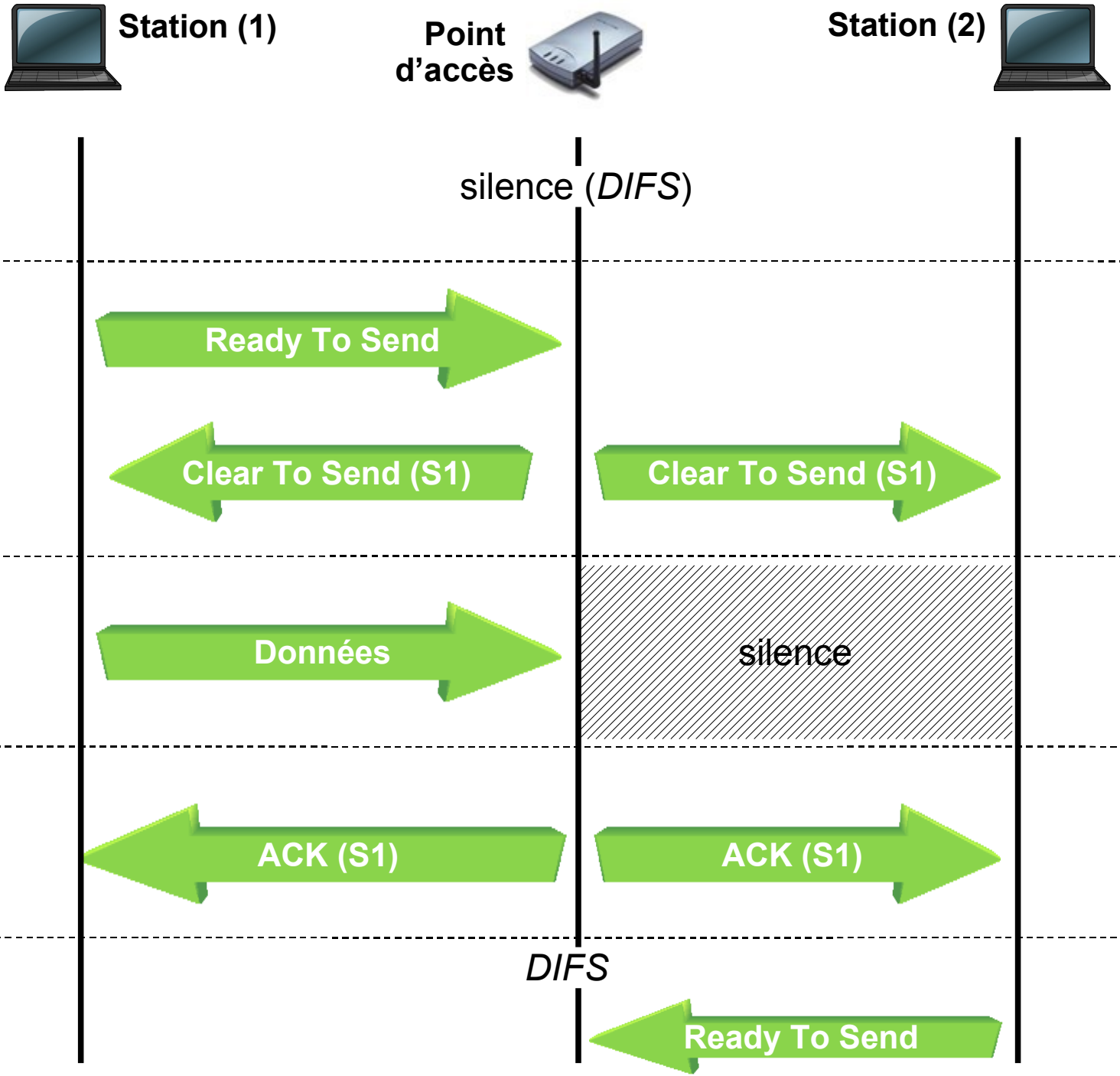
CSMA/CA

- La station voulant émettre écoute le réseau.
- Si le réseau est encombré, la transmission est différée.
- Si le média est libre, la station transmet un message **RTS** (Ready To Send) avec les informations sur le volume de données et sa vitesse de transmission.
- Le récepteur répond par un message **CTS** (Clear To Send) que reçoivent toutes les stations.
- La station effectue l'émission des données.
- A réception de toutes les données, le récepteur envoie un **ACK** (accusé de réception).
- Toutes les stations voisines patientent alors pendant le temps calculé à partir du CTS



Source : Jean François Pilou

Transfert de données



Paramètres radio avancés (BSS)

- **Beacon Interval** : 0 - 3000; default 100 (ms)
  - Intervalle de temps entre deux transmissions d'une trame balise pour les stations cherchant à s'associer (Beacon).
- **DTIM Interval** : 1 – 255; default 100 (ms)
  - Zone de décompte informant les clients WiFi associés en veille (pour l'économie d'énergie) quand se réveiller pour la diffusion suivante des messages Broadcast et Multicast de l'AP (Delivery Traffic Indication Message).
- **Preamble Type** : Long / Short
  - Option longue ou courte du preambule.
  - Choisir court si le réseau est chargé.

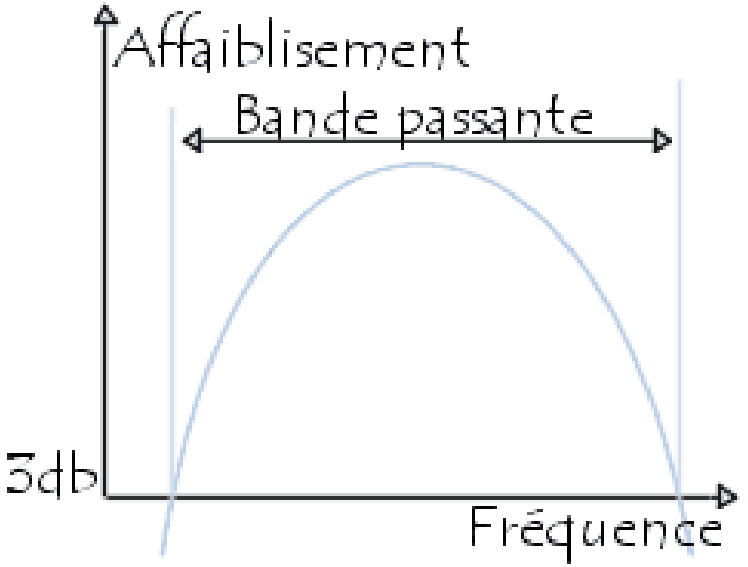
Paramètres radio avancés (BSS)

- **Fragmentation Threshold** : 256 - 2346; default 2346 (octets)
  - Seuil au-dessus duquel les paquets seront fragmentés.
  - Plus le seuil est élevé, plus les conséquences d'une mauvaise réception de ce paquet seront importantes car il faut le retransmettre en entier.
- **RTS Threshold** : 0 - 3000 ; default 2432 (octets)
  - Taille d'un paquet de données à partir de laquelle l'émetteur va faire une demande de droit de parole afin qu'aucun autre émetteur ne fasse d'émission au même moment.
  - Cette valeur est à diminuer dans le cadre d'un réseau avec beaucoup de trafic afin d'éviter les collisions et l'écroulement des débits.

Gamme de fréquence et canaux

Les canaux de transmission

- Un **canal de transmission** est une bande de fréquence étroite utilisable pour une communication
- La largeur du canal (**bande passante**) est en général proportionnelle au débit de la communication
- Des canaux peuvent se recouvrir en partie générant une dégradation de la qualité du signal et du débit



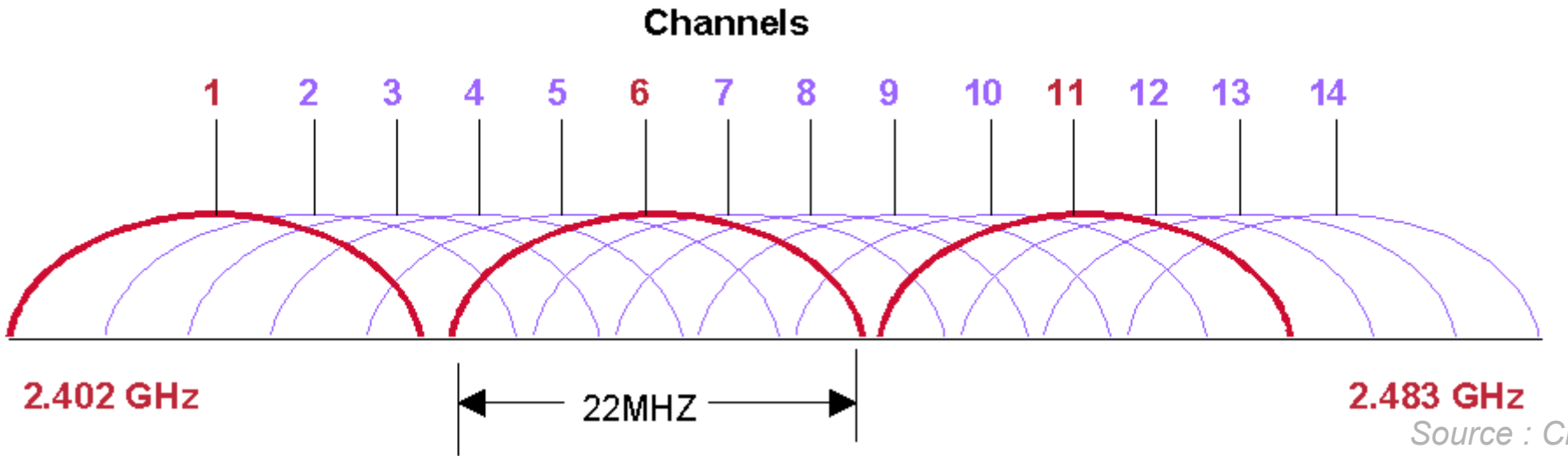
Source : Jean François Pilou

La bande ISM

- Dans chaque pays le gouvernement est le régulateur de l'utilisation des bandes de fréquence
  - ETSI en Europe
  - FCC aux Etats-Unis
- En 1985, les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine (ISM)
  - 902 à 928 Mhz
  - 2.4 à 2.483 Ghz <- **802.11b** et **g**
  - 5.725 à 5.850 Ghz <- **802.11a**
- En Europe, la première bande est utilisée par le GSM, seules les deux autres sont disponibles

Les canaux du 802.11b et g

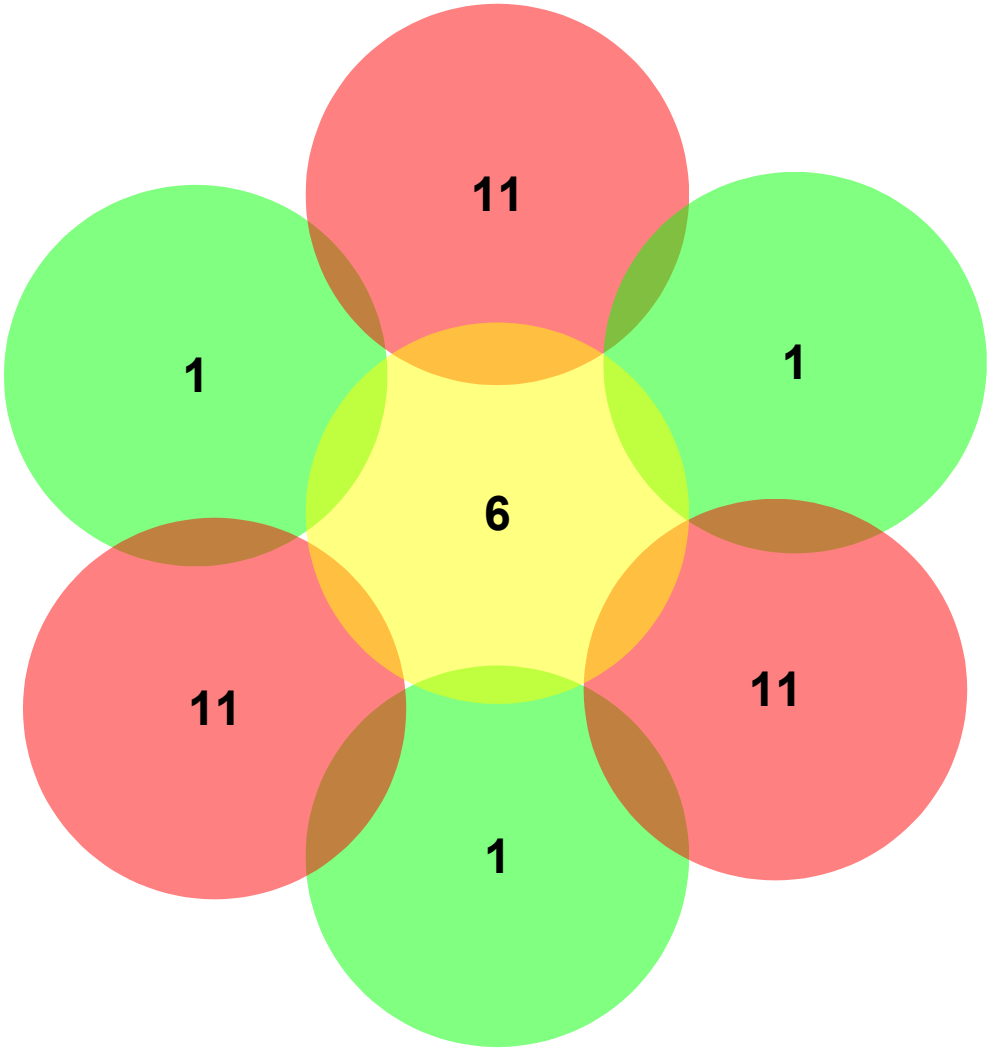
- La bande de fréquence du WiFi (802.11b et g) est divisée en 13 canaux se recouvrant partiellement
- Chaque BSS communique sur **un** canal fixé lors de la configuration de l'AP (Infrastructure) ou de l'adaptateur (ad-hoc)
- Trois canaux seulement sont utilisables simultanément et à proximité : 1, 6 et 11
- Les canaux bas sont réputés plus stables



Source : Cisco

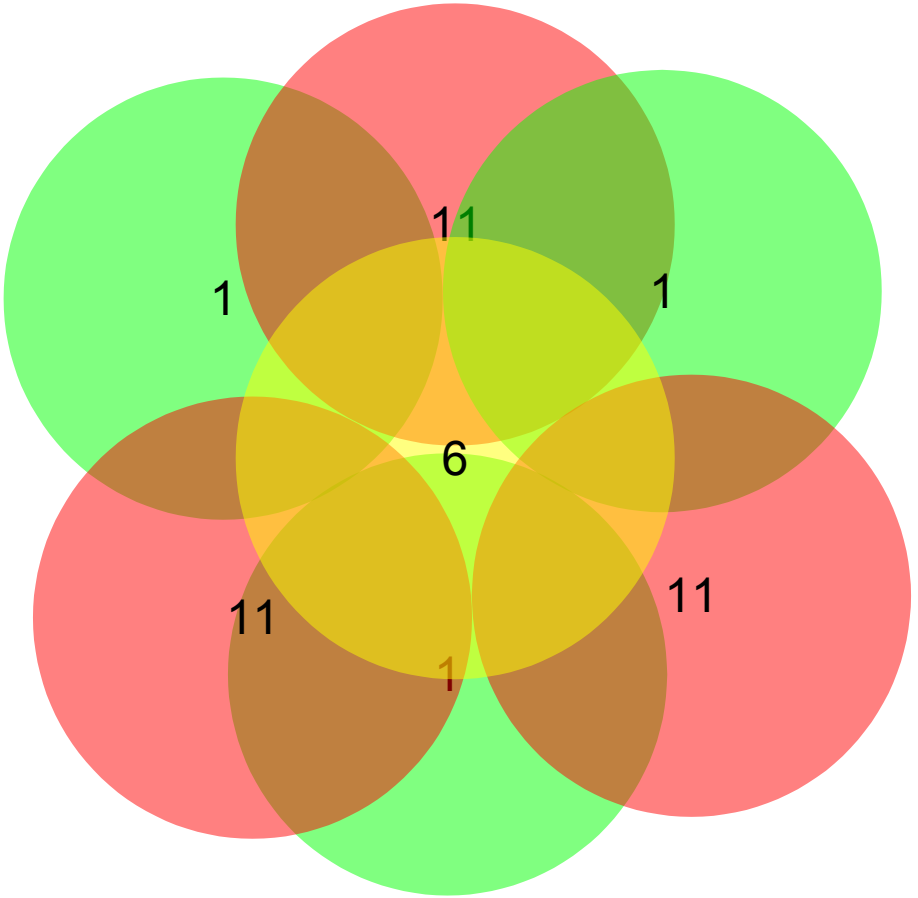
Affectation des canaux

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

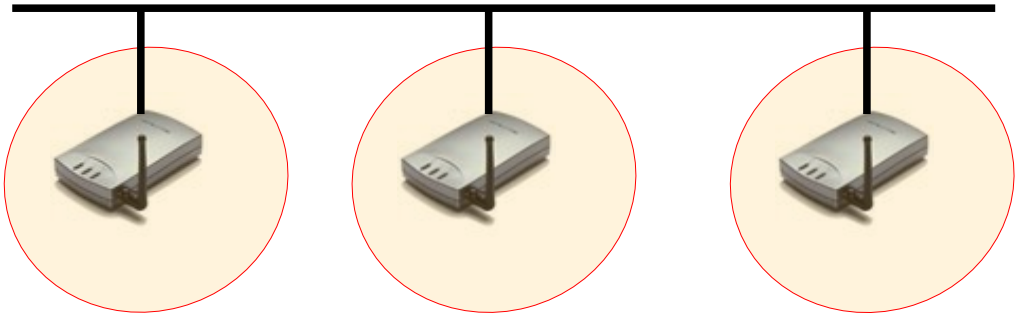


Affectation des canaux

- Affectation de trois canaux qui ne se perturbent pas (cas obligatoire) :

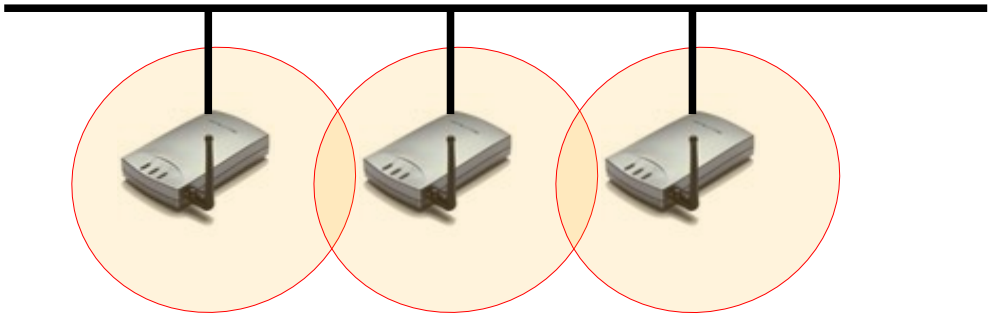


Choix de la topologie



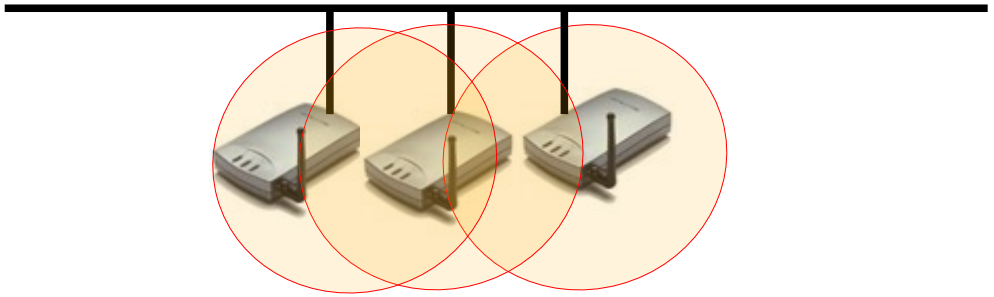
les cellules sont disjointes

- faible nombre de canaux
- pas d'interférence
- pas de mobilité



les cellules sont jointes

- service de mobilité
- exploitation de l'espace
- ev gestion des canaux
- éq réseaux sans fils



les cellules se recouvrent

- densification : nombre important d'utilisateurs
- gestion des canaux
- gestion de l'affectation

Normes et standards

La norme IEEE 802.11

- 802.11
  - Norme technique du IEEE décrivant les caractéristiques d'un réseau local sans Fil (WLAN)
  - Définit le fonctionnement des couches basses d'une liaison WiFi : couche physique et couche liaison de données
- IEEE (Institute of Electrical and Electronics Engineers / www.ieee.org)
  - Organisation professionnelle à but non lucratif regroupant 360 000 membres scientifiques de 175 pays.
  - Organise la publication de normes dans le domaine de l'ingénierie électrique :
    - IEEE 802.3 : Fonctionnement d'Ethernet
    - IEEE 1394 : Fonctionnement du Bus série (FireWire)
    - IEEE 1284 : Port parallèle

Le label Wi-Fi

- Le label Wi-Fi (Wireless-Fidelity)
  - Certification d'un consortium industriel (WiFi Alliance) attestant de la conformité des produits au standard 802.11 et de leur interopérabilité
  - Label industriel et commercial
  - Les produits bénéficiant de la certification peuvent appliquer le logo WiFi (Wireless Fidelity)
- La «Wi-Fi Alliance»
  - Regroupe 260 entreprises : http://www.wifialliance.com/our_members.php
  - Proposent des labels complémentaires marquant les évolutions techniques de sécurité : WEP, WPA2

Le standard 802.11

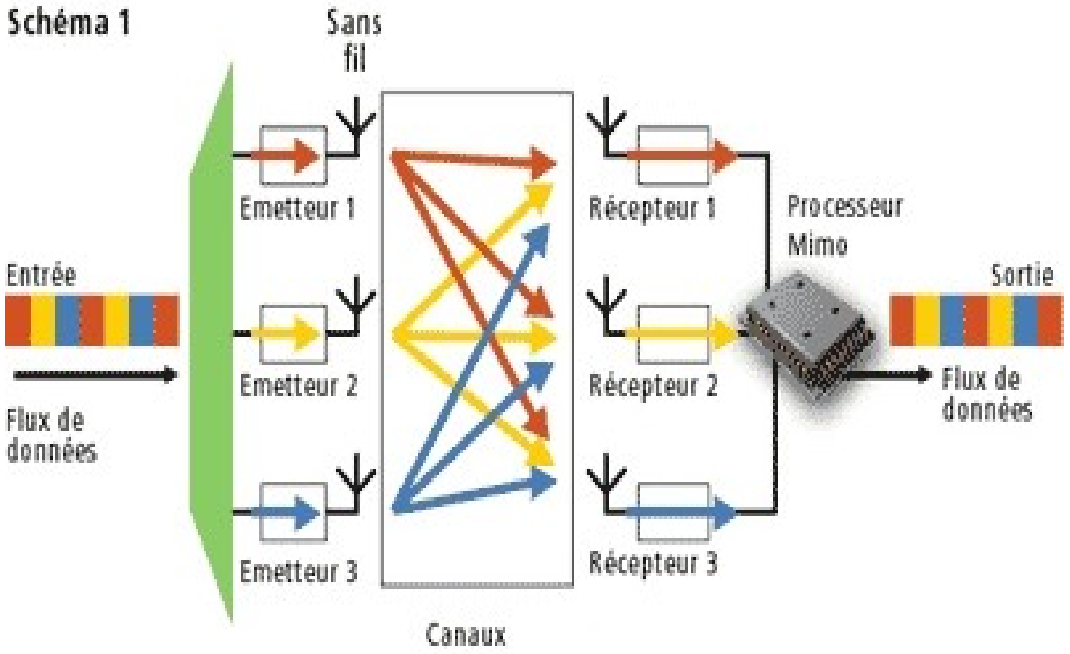
	Débit théorique maximum	Bande de fréquence	Portée maximale	Observations
802.11b	11 Mbps	2,4 GHz	– intérieur : 50 m – extérieur : 200 m (11 Mbps)	– sensible aux interférences (bluetooth, téléphone sans fil, four micro-ondes...) – faible coût (répandue) – non réglementée (1999) – bonne pénétration pour 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

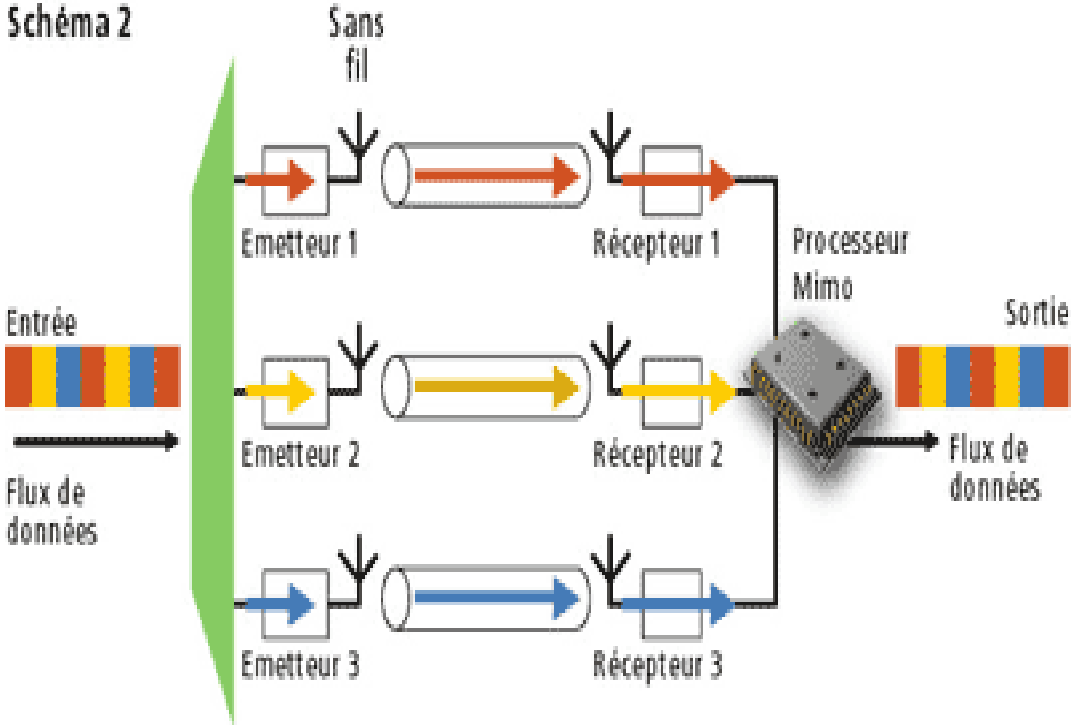
Les différentes normes

- **Origine**
  - **802.11** : 2 Mbits/s (1997)
- **Amendements**
  - **802.11b** : 2,4 Ghz - 11 Mbits/s (bande ISM) - FSSS
  - **802.11a** : 5 Ghz - 54 Mbits/s (bande UN-II) - OFDM
  - **802.11g** : 2,4 Ghz - 54 Mbits/s (bande ISM) - OFDM
  - **802.11e** : Qualité de service
  - **802.11f** : Itinérance (roaming)
  - **802.11h** : Norme européenne pour les fréquences et la gestion d'énergie
  - **802.11i** : Sécurité - chiffrement et authentification AES
- **A venir**
  - **802.11n** : WwiSE ou Super-WiFi - avril 2007 - 540 Mbps - technologie MIMO (multiple-input multiple-output)
  - **802.11s** : Réseau Mesh, en cours d'élaboration. Mobilité sur les réseaux de type adhoc avec routage dynamique OLSR. Débit de 2 Mbps.

MIMO

- Multiple In, Multiple Out = Multiples entrées, Multiples sorties
- La technologie multiplie le nombre de canaux de transmission effectifs (dans un même canal radio)
  - Les émetteurs et les récepteurs utilisent plusieurs antennes (de 2 à 8)
  - On utilise chaque antenne comme un émetteur différent
  - A la réception, un algorithme exploite les interférences liées à la réflexion des ondes pour différencier les différents flux (utilisable en intérieur uniquement)
- Permets d'atteindre
  - des débits de 576 Mbit/s (Fragmentation - Airgo)
  - une portée de 120 mètres (Réplication - Athéros)





Émission

- les signaux sont émis par trois antennes distinctes
- la propagation du signal dans l'air les multiplexe vers chacun des récepteurs

Réception

- l'algorithme de traitement de chaque récepteur isole le signal d'un des émetteurs en utilisant les réflexions
- le protocole dispose donc de trois canaux virtuels
- le débit est multiplié par trois

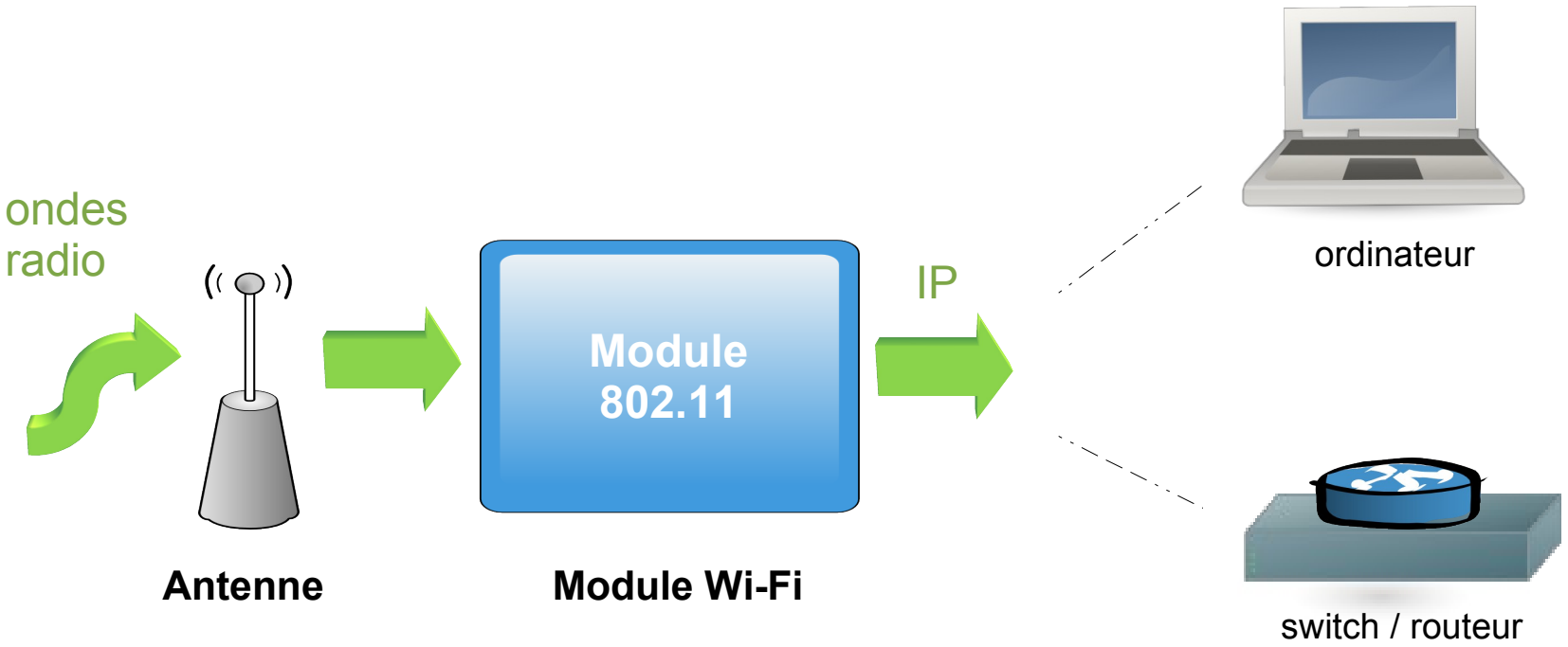
Fonctionnement

Couche 802.11

Fonctionnement

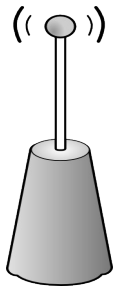
- Tous les équipements WiFi sont équipés d'une antenne et d'un module chargé de la commutation

  ondes radio <-> trames IP

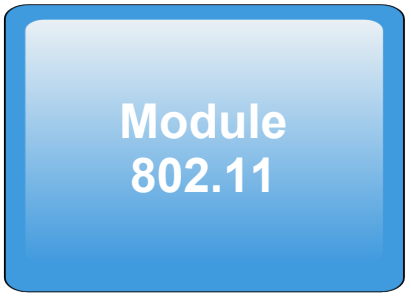


Fonctionnement

ondes radio

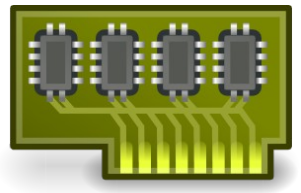


Antenne



Module Wi-Fi

paquet IP



Connexion PCMCIA

port PCMCIA

Fonctionnement

ondes radio

paquet IP

Module 802.11

port PCI

Antenne

Module Wi-Fi

Connexion PCI

Fonctionnement

ondes radio

Antenne

Module 802.11

Module décapsulation Wi-Fi

paquet IP

Module 802.3

Module d'encapsulation Ethernet

trame Ethernet

cablage Ethernet

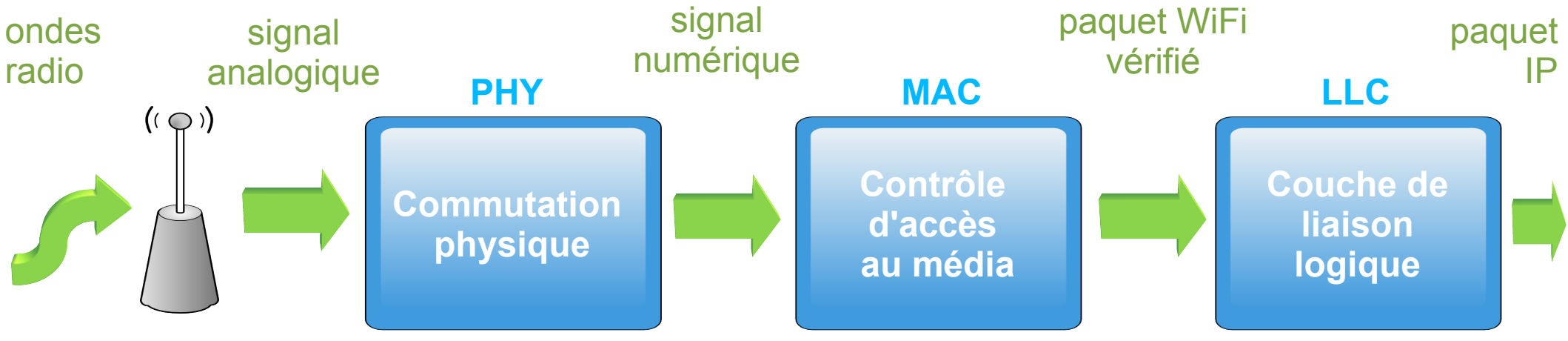
switch / routeur

Le module WiFi

- Modulation

ondes radio <-> trames IP

niveau 1 <-> niveau 3 de la couche OSI



Convertit le signal (gamme de fréquence, puissance et modulation) et **décode l'information**

DSSS / FHSS / ODPM

Gère l'accès au média et s'assure de la transmission des trames

CSMA/CA

- Mode d'association
- Authentification et sécurité
- Fragmentation
- Roaming
- Économie d'énergie

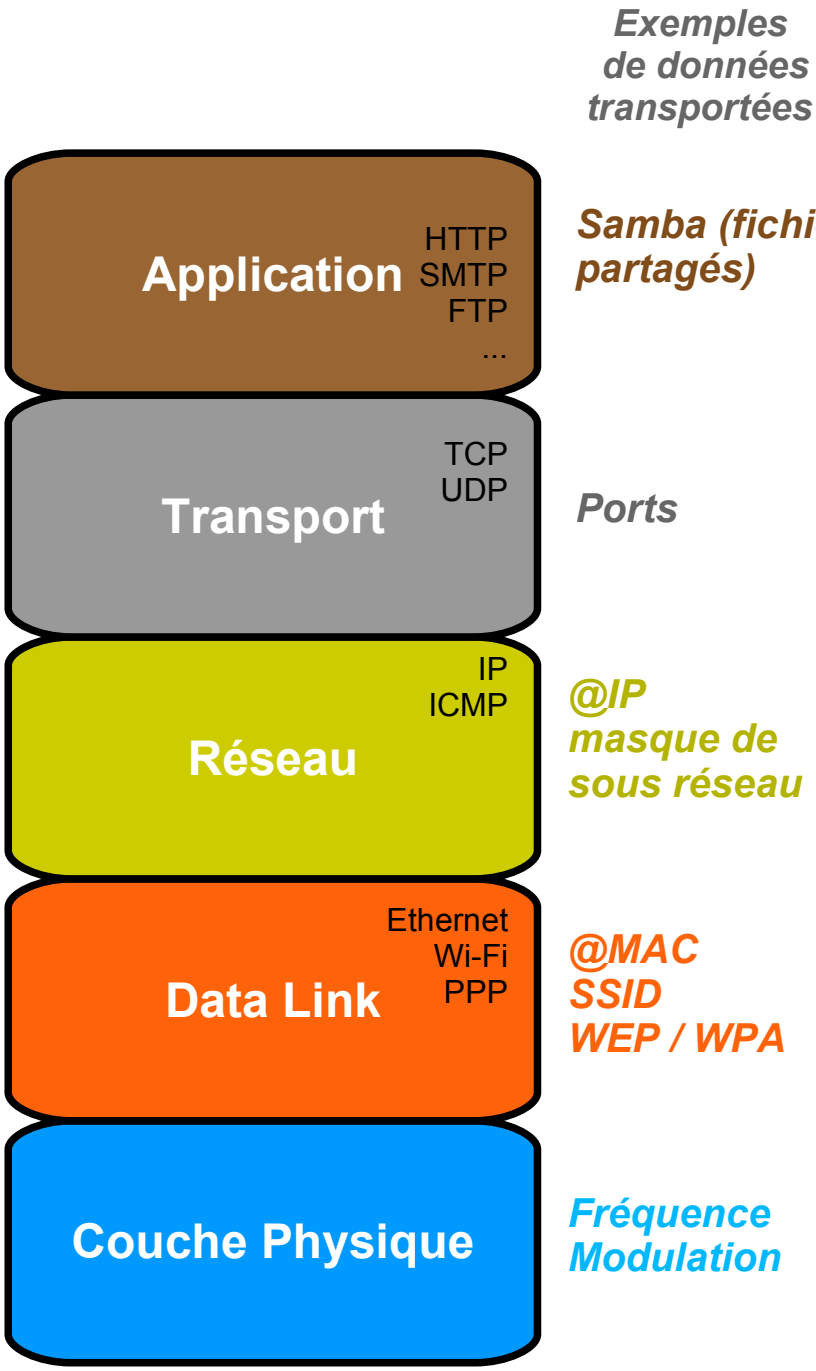
Lien WiFi

Partie 3

Configuration d'un réseau Wi-Fi

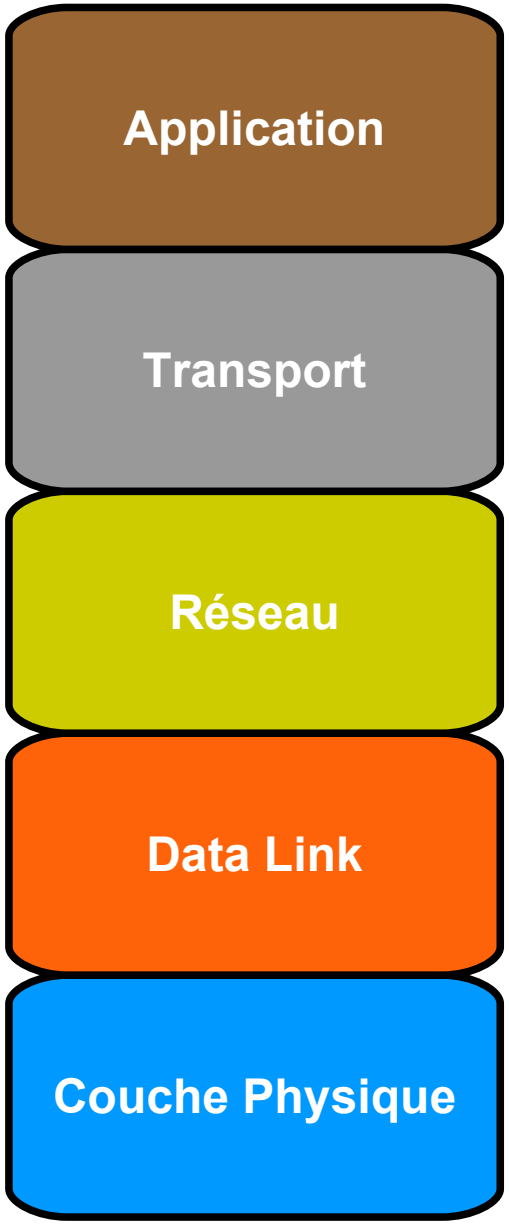
Le modèle OSI

Modèle TCP/IP en couches



- Les réseaux sont généralement organisés en "piles protocolaires"
- chaque couche de la pile offre un niveau d'abstraction supplémentaire à la couche supérieure
- chaque couche offre un service supplémentaire par rapport à la couche inférieure

Les couches 802.11



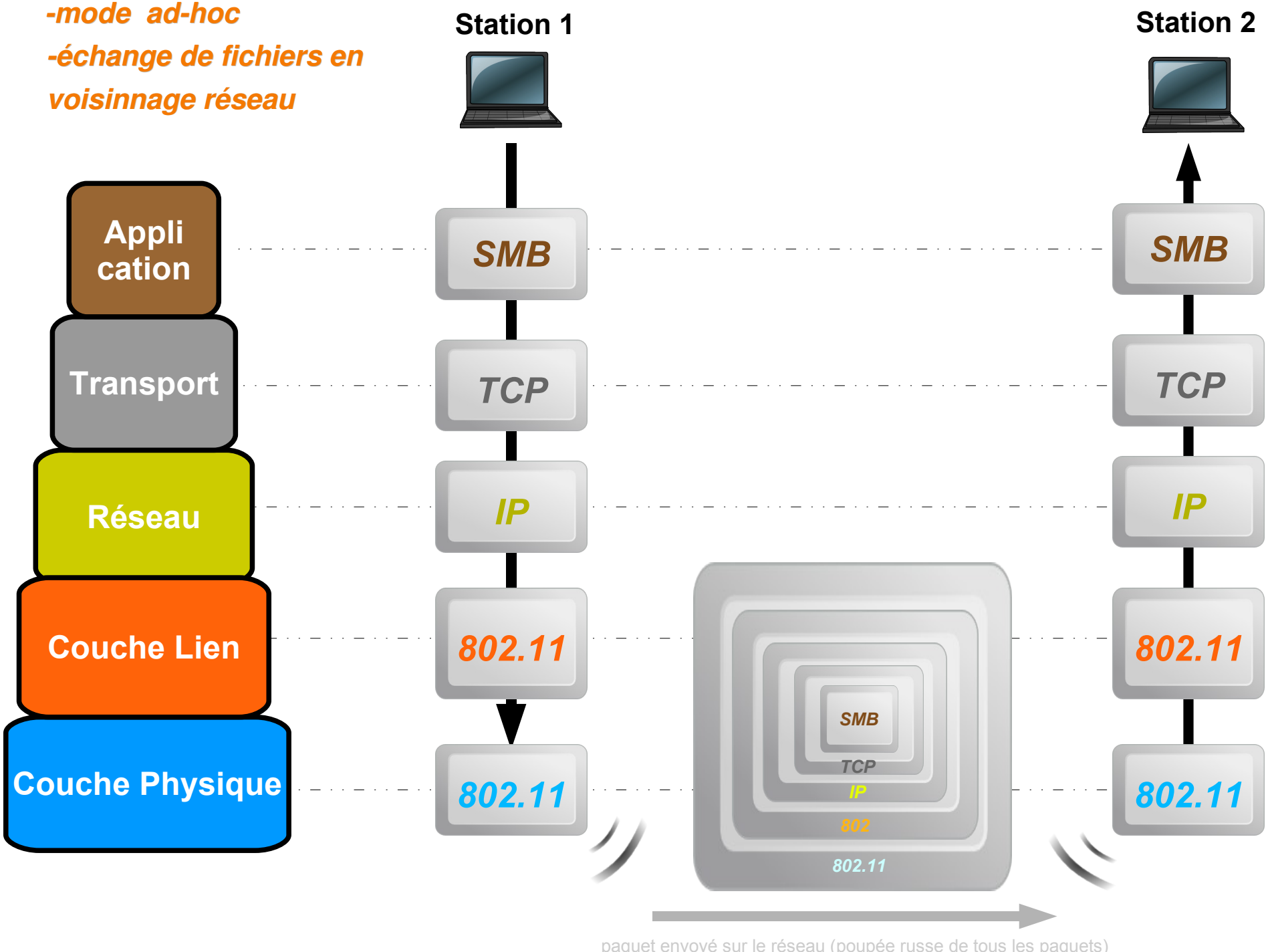
Couches Wi-Fi (802.11 - 802.2)

- **Logical Link Control (LLC)**
  Couche de liaison logique
  lien WiFi
- **Medium Acces Control (MAC)**
  Contrôle d'accès au média
  CSMA/CA (DCF)
- **Couche Physique (PHY)**
  Modulation de données
  IR / DSSS / FHSS / OFDM

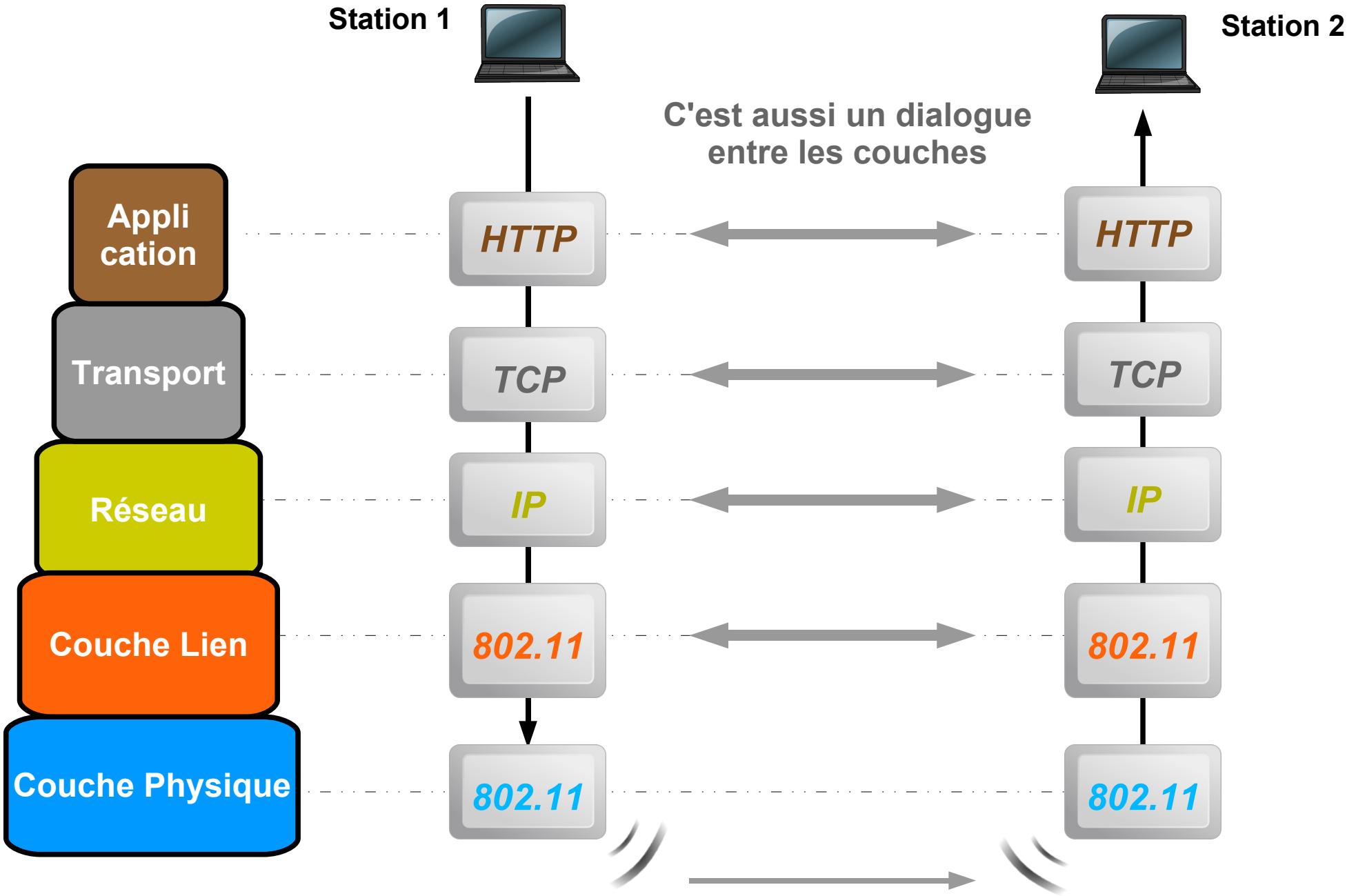
Communication entre deux stations

-mode ad-hoc

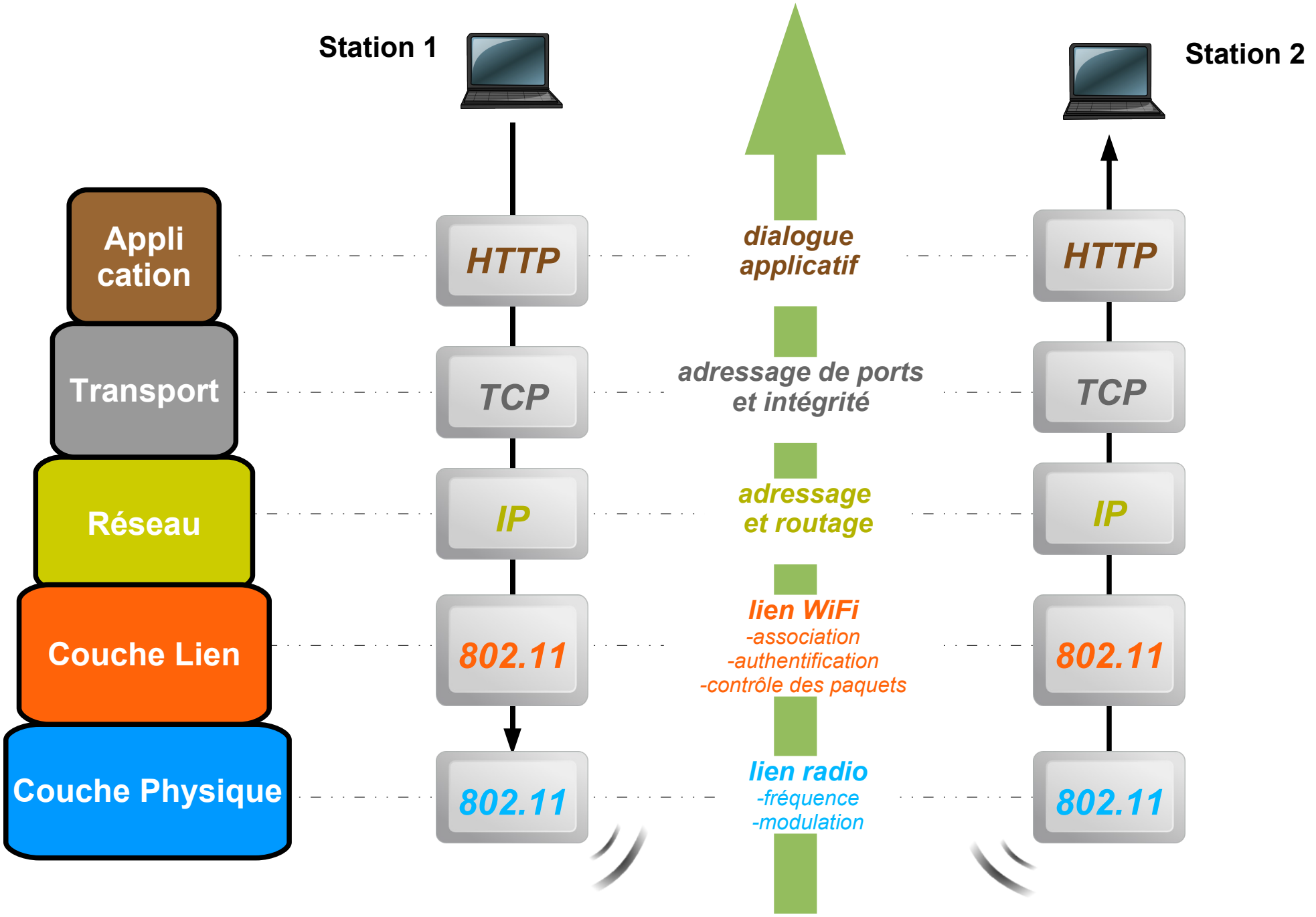
-échange de fichiers en voisinnage réseau



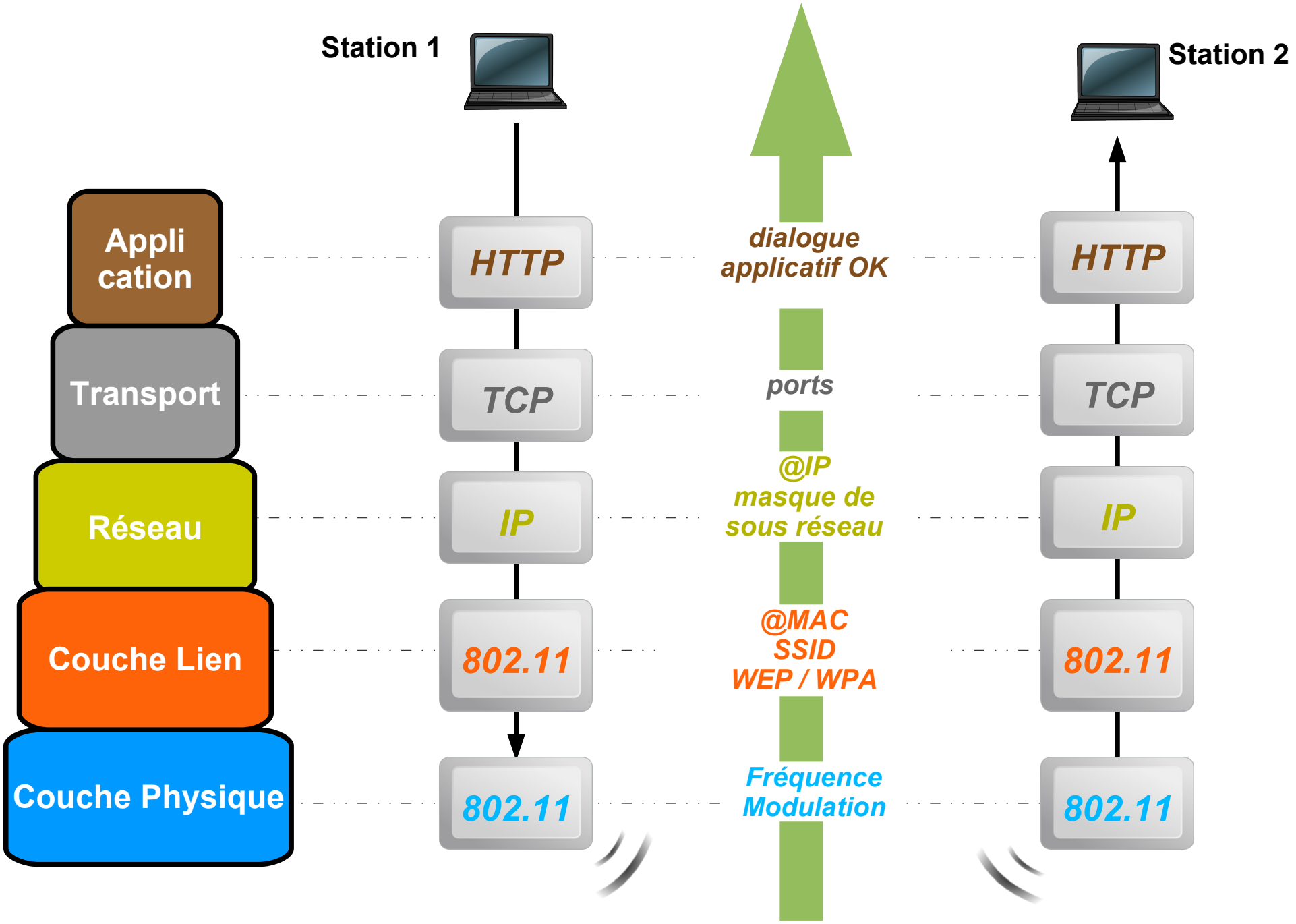
Un dialogue transversal



Des services successifs

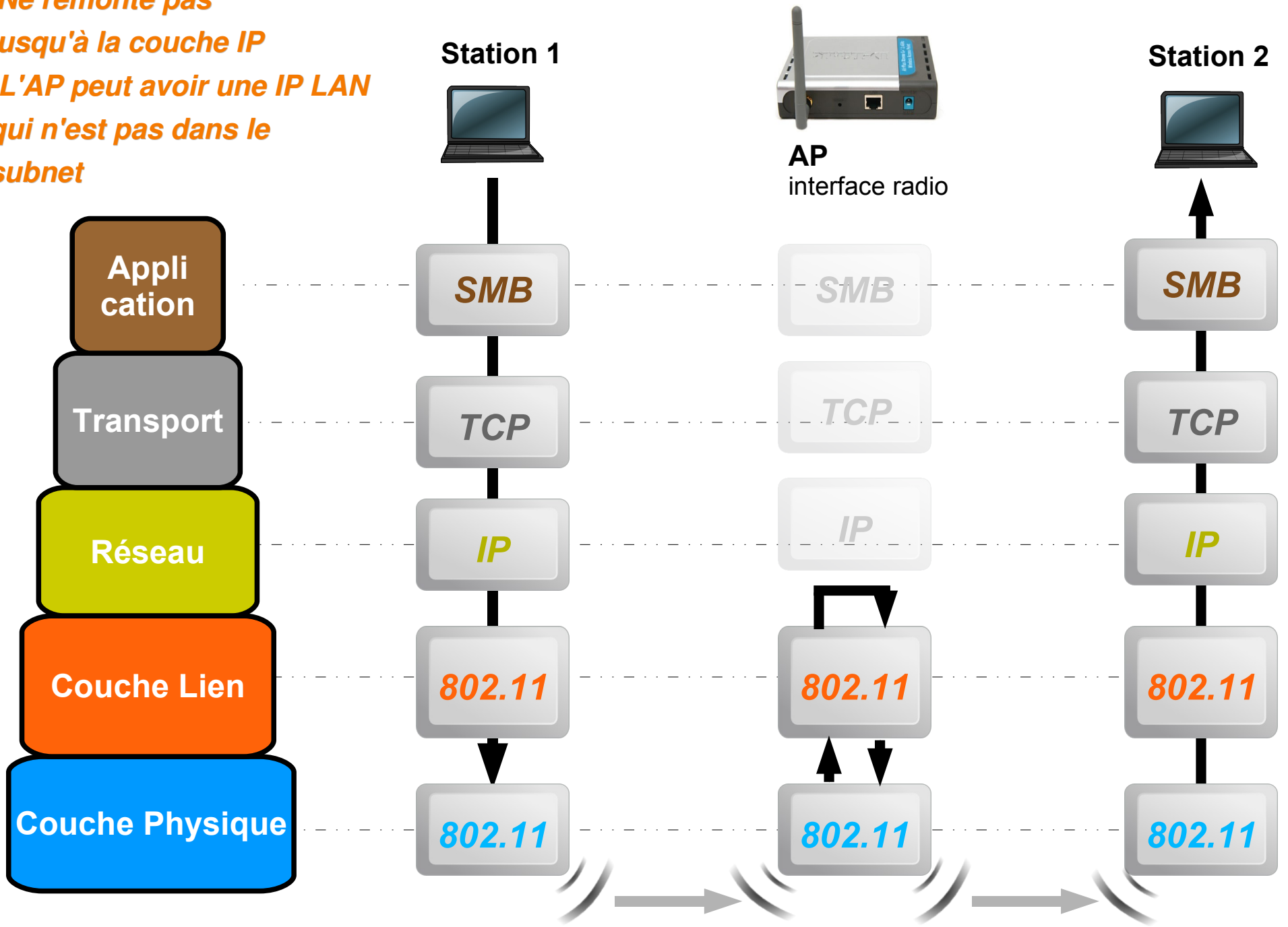


Des filtres successifs



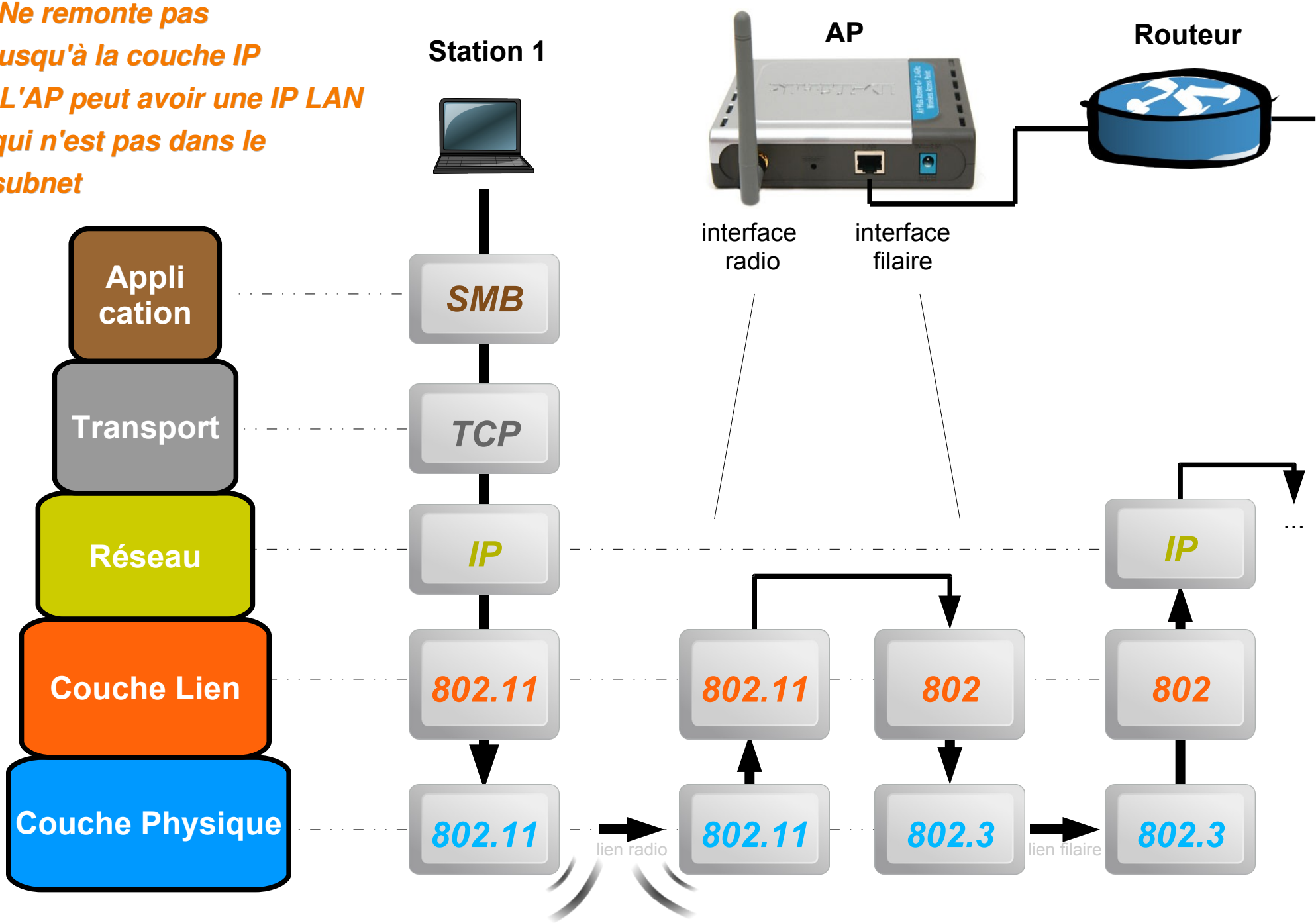
Mode Infrastructure

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

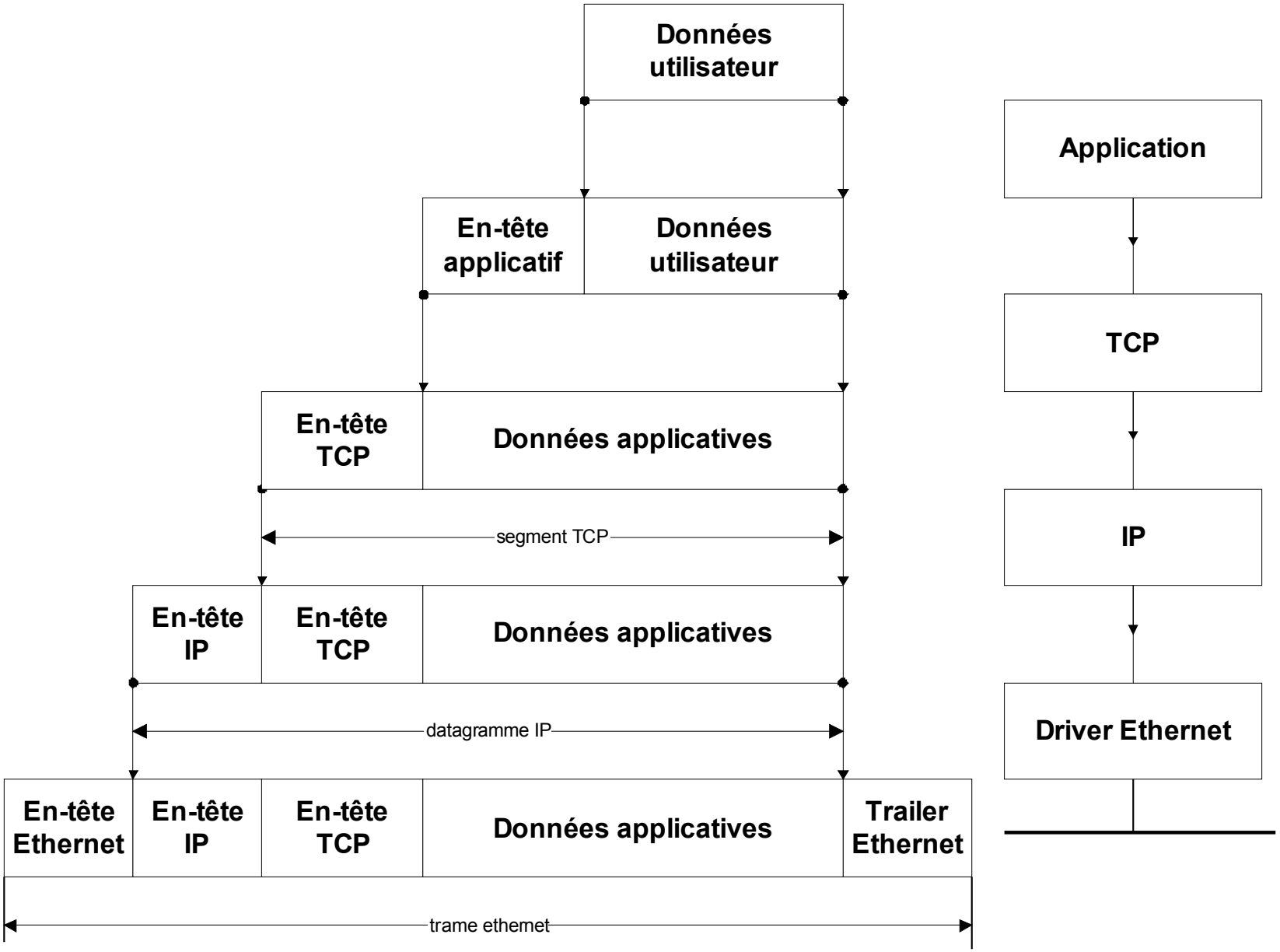


AP = Bridge de niveau 2

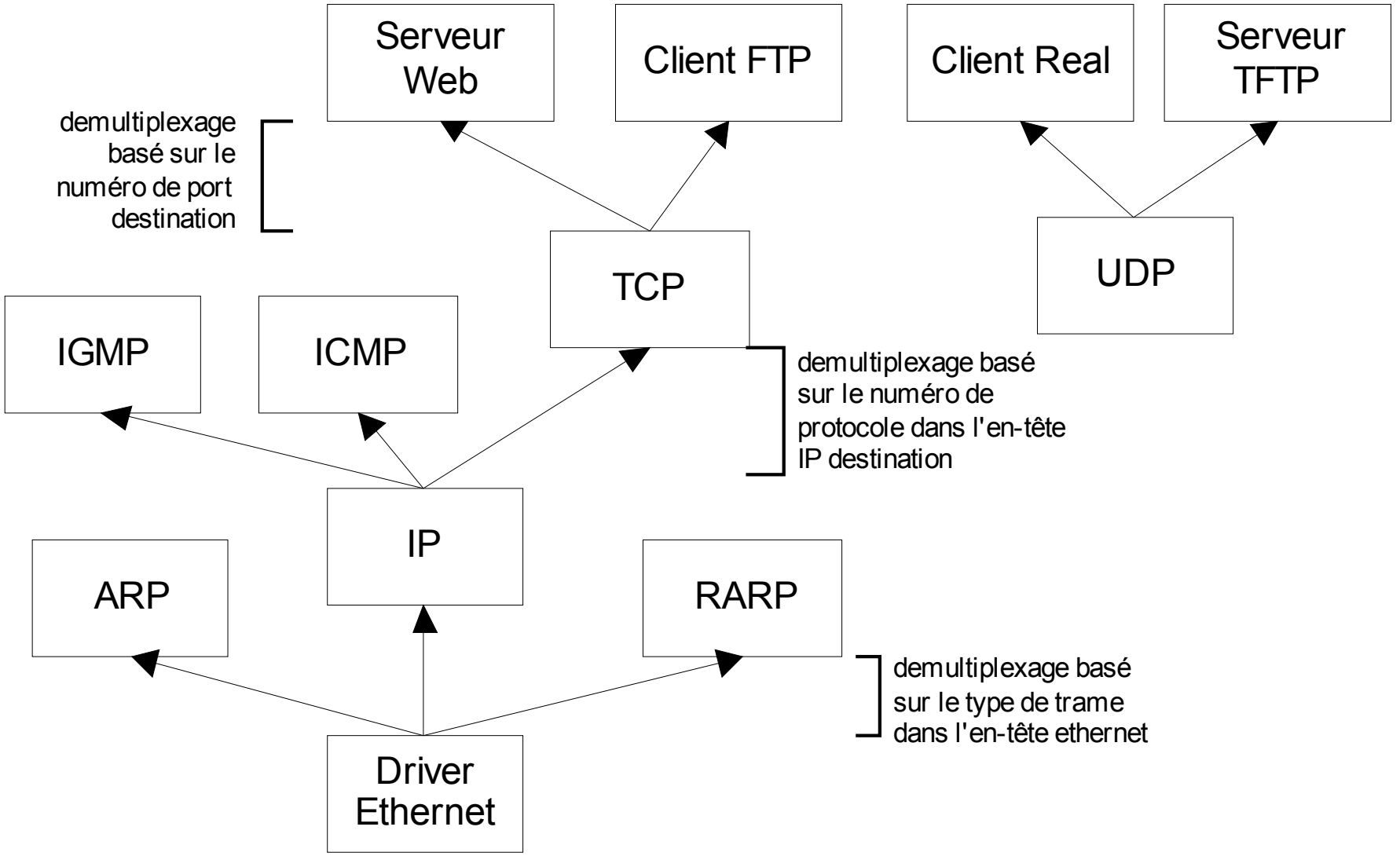
-Ne remonte pas jusqu'à la couche IP
-L'AP peut avoir une IP LAN qui n'est pas dans le subnet



Réseau TCP/IP - Encapsulation



Démultiplexage



Ce qu'il faut retenir

- La couche Wi-Fi (802.11) est indépendante de la couche IP. Elle est préalable à son fonctionnement dans la communication réseau.
- Lors de la configuration du réseau, ces deux aspects sont traités séparément et nécessaires pour la communication entre les équipements :
  - paramètres radio
  - paramètres réseau

Réseau TCP/IP

Les adresses IP

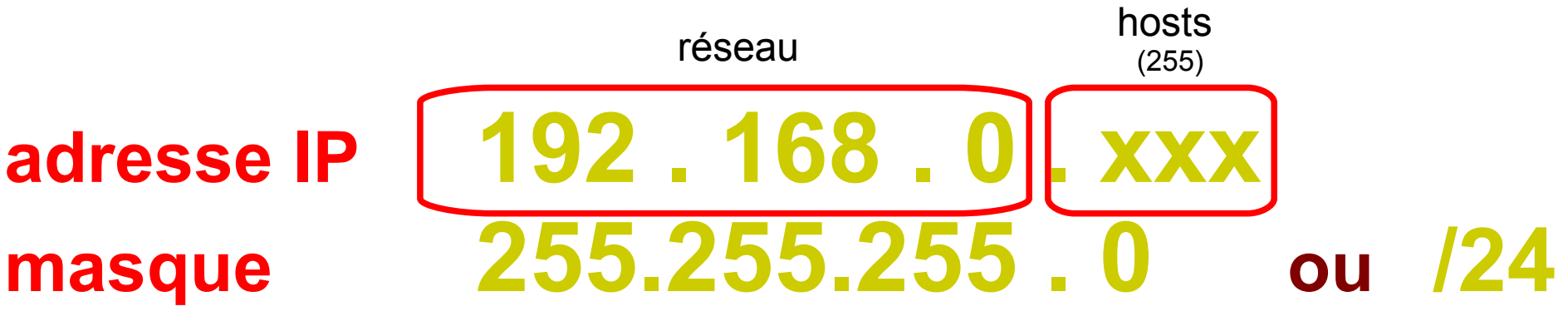
- Dans un réseau, chaque machine est identifiée par une adresse IP, qui doit être unique à l'intérieur du réseau (les réseaux étant délimités par les routeurs).
- Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux.
- Chaque machine ne dispose que d'une adresse par réseau, à l'exception des machines passerelles (routeurs, proxy, gateway) qui possèdent plusieurs interfaces.
- Ces adresses sont composées de 4 nombres entiers (4 octets) entre 0 et 255, notées : xxx.xxx.xxx.xxx
  - De 0.0.0.0 à 255.255.255.255
  - Par exemple : 194.153.205.26

Les adresses IP

- Les 4,3 Milliards d'adresses sont subdivisées en **adresses privées** et en **adresses publiques**.
- Les adresses privées
  - concernent les machines des réseaux locaux (LAN)
  - elles se situent derrière au moins un routeur NAT
  - elles sont d'usage libre / Intranet
  - elles se divisent en trois catégories
    - classe A : **10.0.0.0** à **10.255.255.255** (16387064 @)
    - classe B : **172.16.0.0** à **172.31.255.255** (1032256 @)
    - classe C : **192.168.0.0** à **192.168.255.255** (64516 @)
- Les adresses publiques
  - concernent les machines directement reliées à l'Internet
  - attribuées et contrôlées par l'ICANN

Les masques de sous réseau

- Une adresse IP est constituée de deux parties :
  - A gauche, une partie désigne **le réseau** (netID)
  - A droite, une partie désigne **les ordinateurs** (host-ID)
- Le masque fixe la limite entre ces deux parties.
- Se présente sous la même forme: xxx.xxx.xxx.xxx ou /xx
- Les valeurs non nulles désignent la partie réseau.
  La notation CIDR désigne le nombre de bits du réseau :
  24 -> 3 octets



Les masques de sous-réseau

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

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

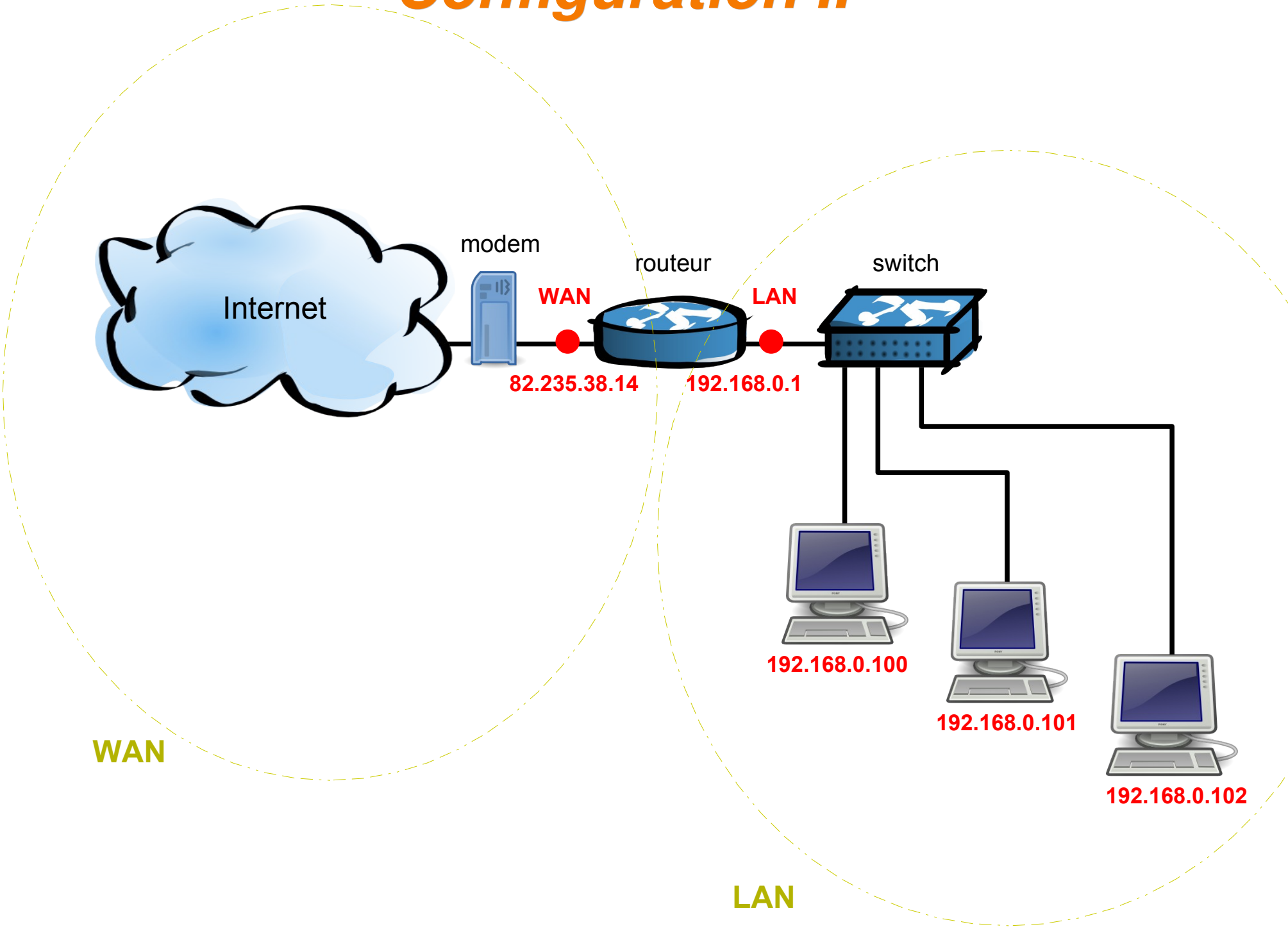
Par défaut, dans un réseau local, on utilisera :

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

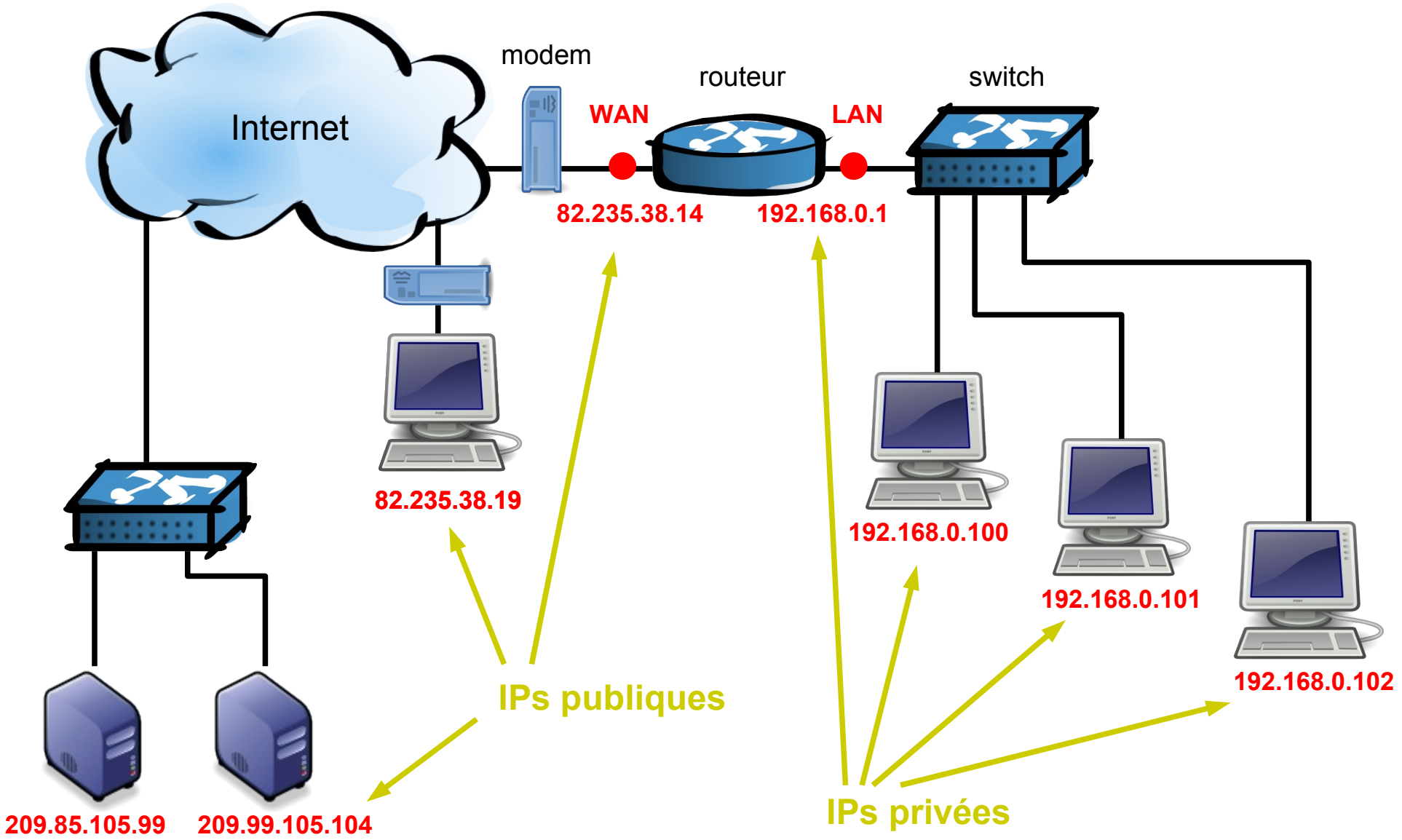
Les masques de sous-réseau

- Nombre de machines = $2^{(32\text{-CIDR})}-2$
- Les deux adresses en moins sont :
  - **l'@ broadcast** : dernière valeur de l'host-ID (ex : 192.168.0.255 / 24)
  - **l'@ réseau** : première valeur de l'host-ID (ex : 192.168.0.0 / 24)
- Des @IP apparemment compatibles peuvent correspondre à des réseaux différents (et donc être non joignables) :
  - **192.168.0.1 / 255.255.255.0** : 254 machines (/24)
  - **192.168.0.2 / 255.255.255.240** : 15 machines (/28)
  - **192.168.0.3 / 255.255.0.0** : 65534 machines (/16)

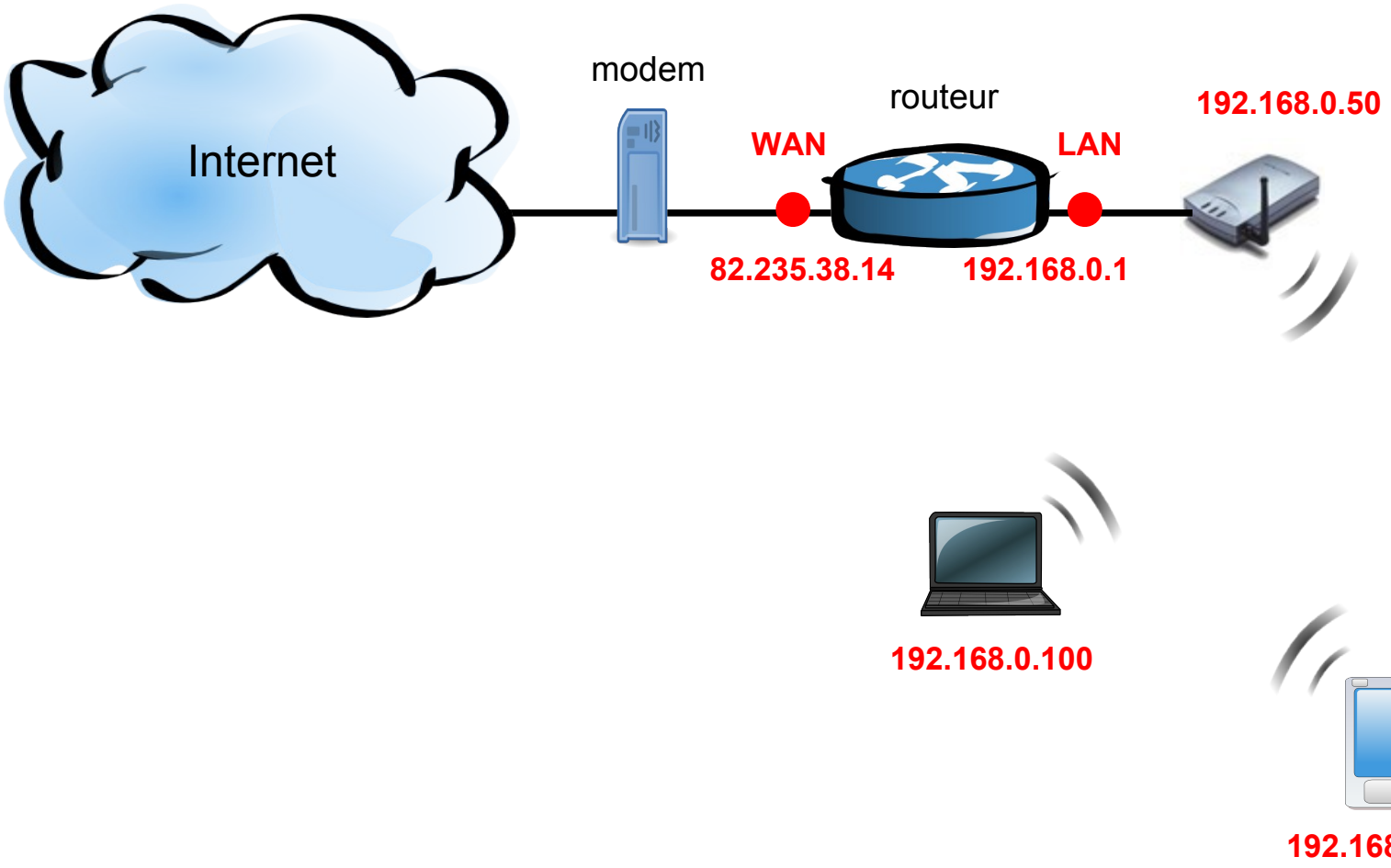
Configuration IP



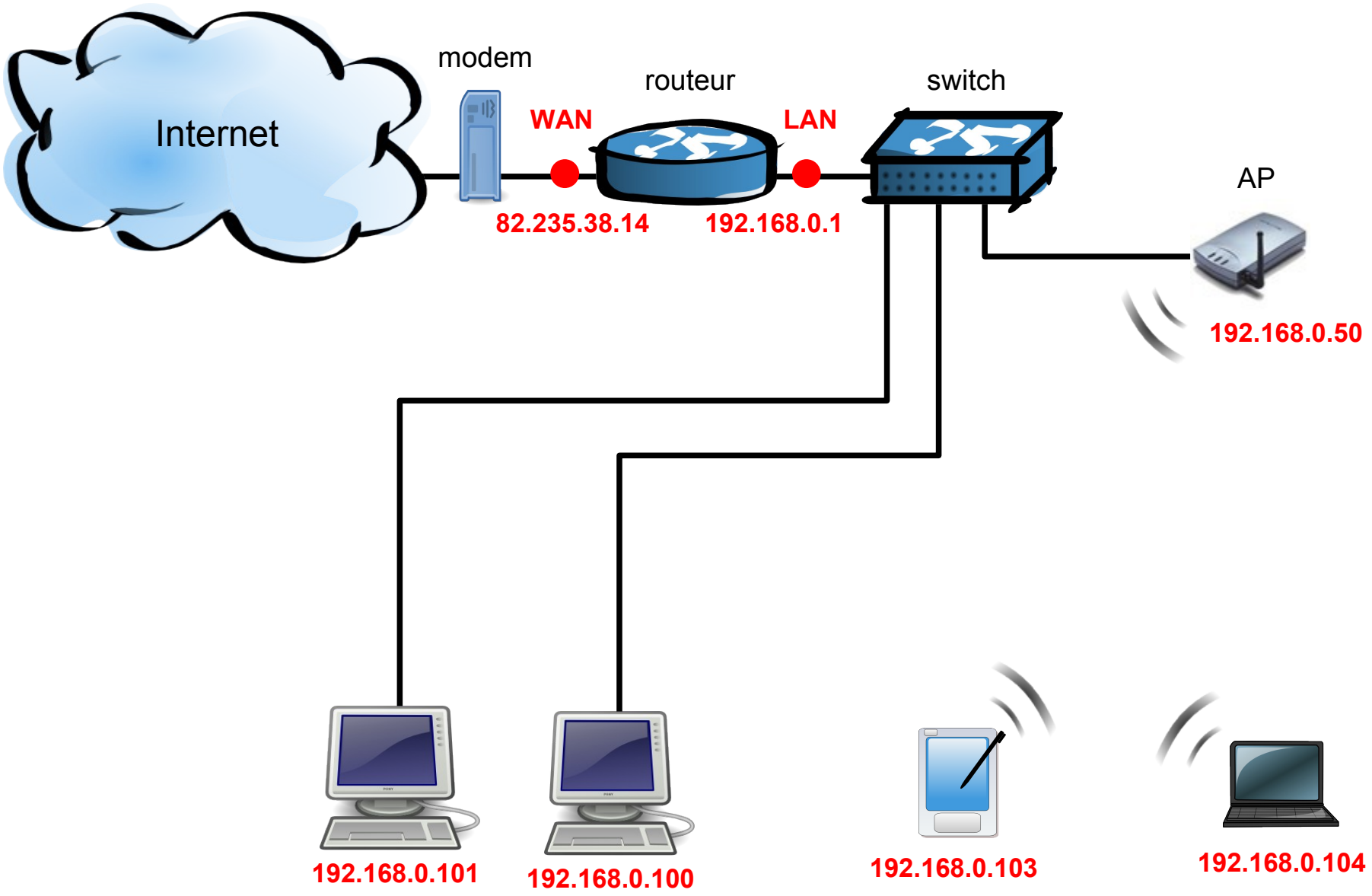
Configuration IP



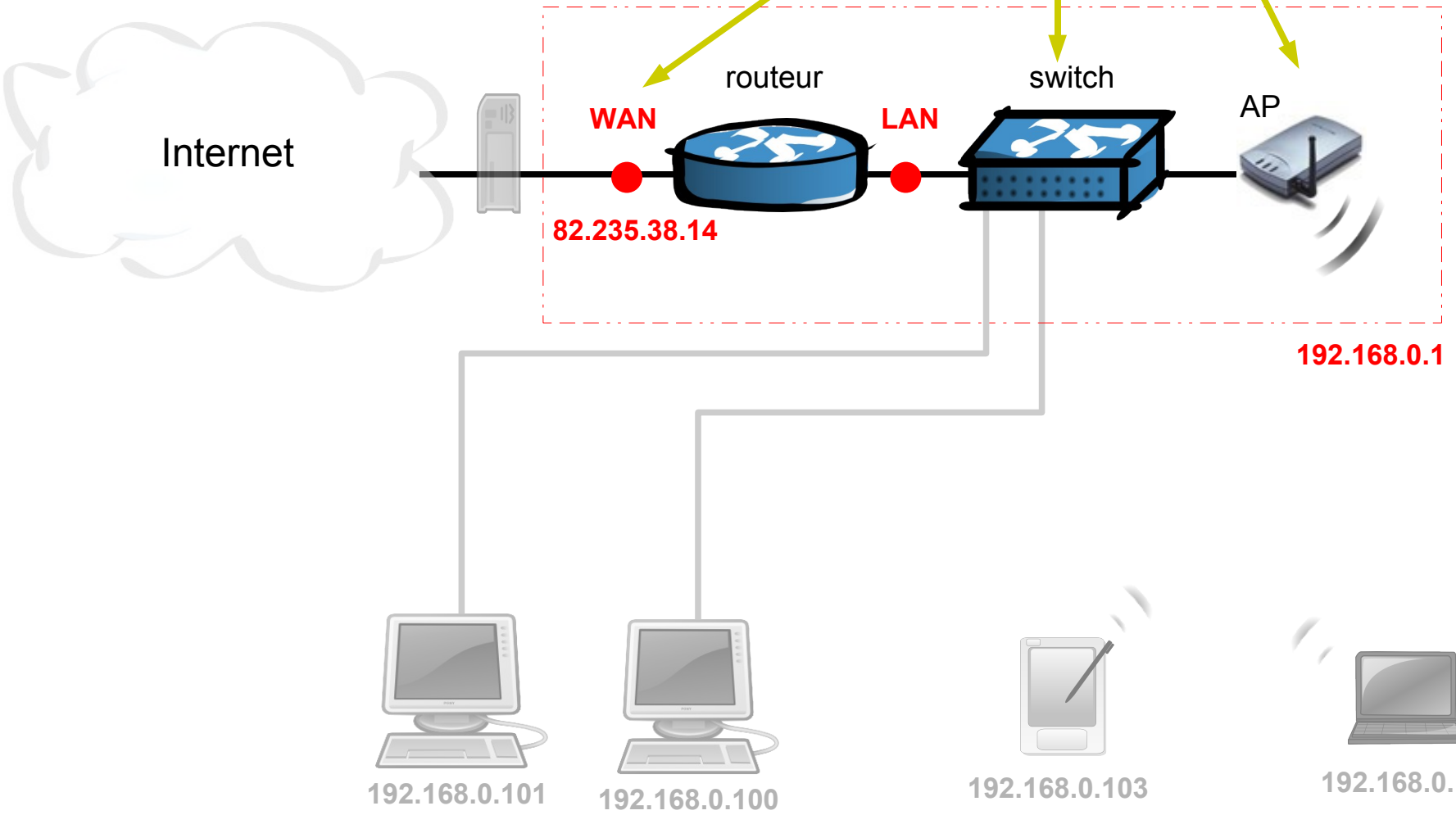
Topologie Infrastructure



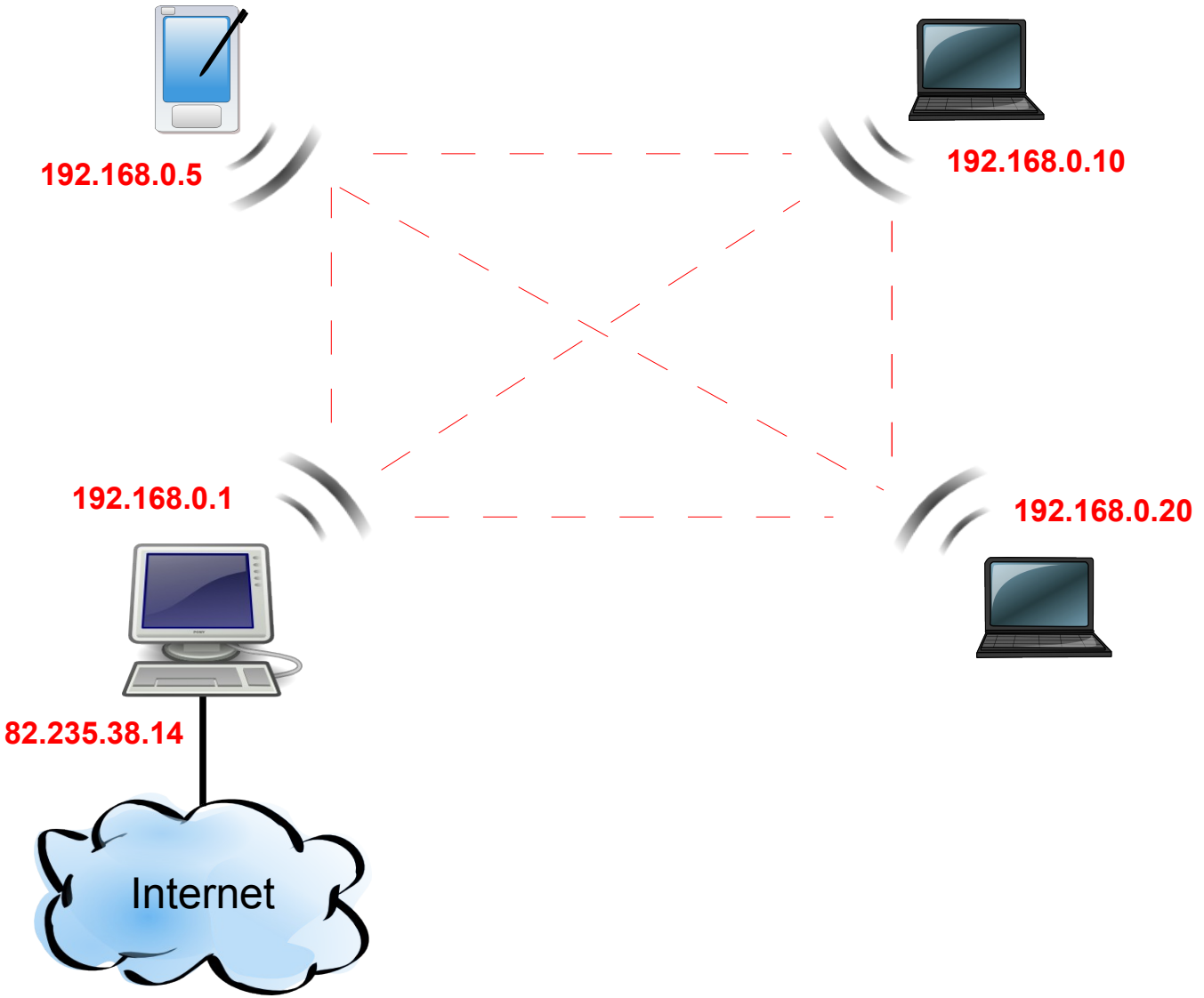
Topologie Infrastructure



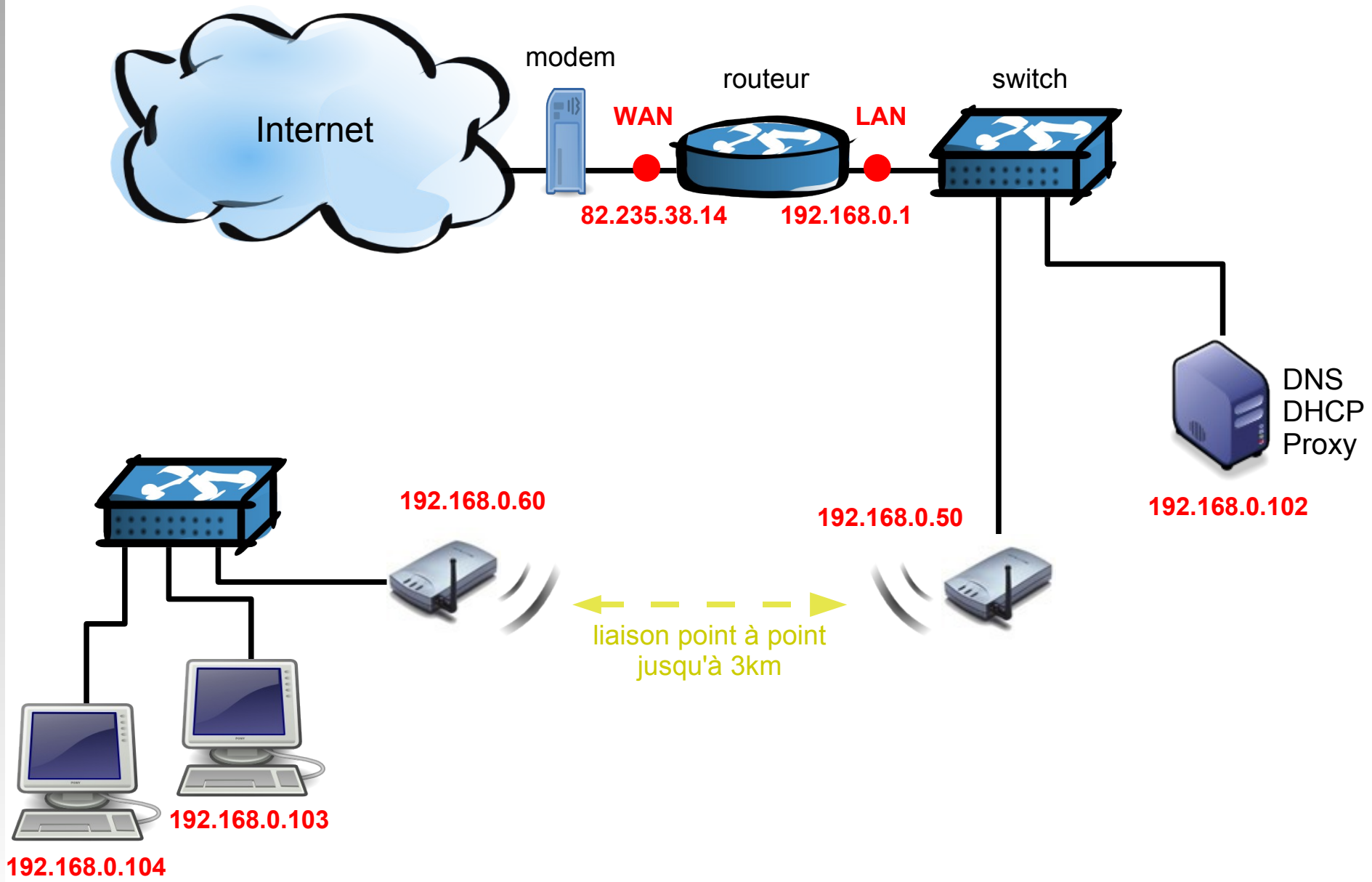
= 3 en 1


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

Topologie ad-hoc



Etendre un réseau existant



Configurations nécessaires

- Pour communiquer dans le cadre du LAN (*) les machines ont besoin de :
  - **une adresse IP** + **un masque de sous-réseau**

- Pour sortir sur Internet une machine a besoin de :
  - **une adresse IP** + **un masque de sous-réseau**
  - **une passerelle** (Gateway)
  - **un serveur de résolution de nom** (DNS)

* : échange de fichiers (SMB), ping (ICMP), FTP, Pages Web (HTTP)...

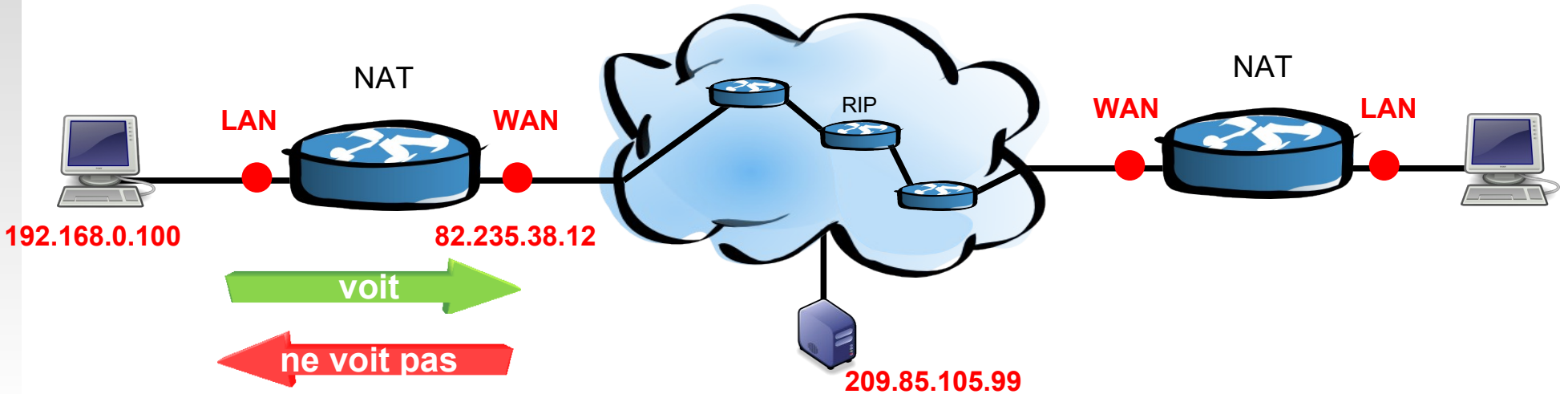
Serveur DHCP

- Distribue dynamiquement aux machines en effectuant la requête
  - une adresse IP + plage de sous réseau
  - la passerelle de sortie
  - une adresse de DNS

    -> configure automatiquement **la couche IP** du réseau
- Cette configuration dynamique est particulièrement adaptée aux réseaux de type Infrastructure.
- La plupart des AP - routeurs intègrent cette option.
- Faiblesse sécurité : paramètres IP connus.

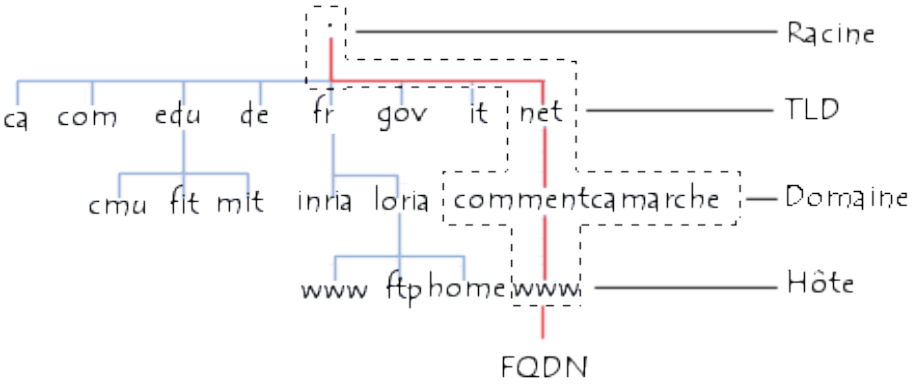
Les routeurs

- Possèdent deux interfaces. Ils transmettent leurs paquets IP d'une interface à l'autre.
- Routage NAT
  - Permets une translation d'adresse :
    une @IP publique <-> n * @IP privées
  - Le réseau public (WAN) est visible depuis le réseau privé (LAN) mais pas l'inverse.



Le serveur DNS

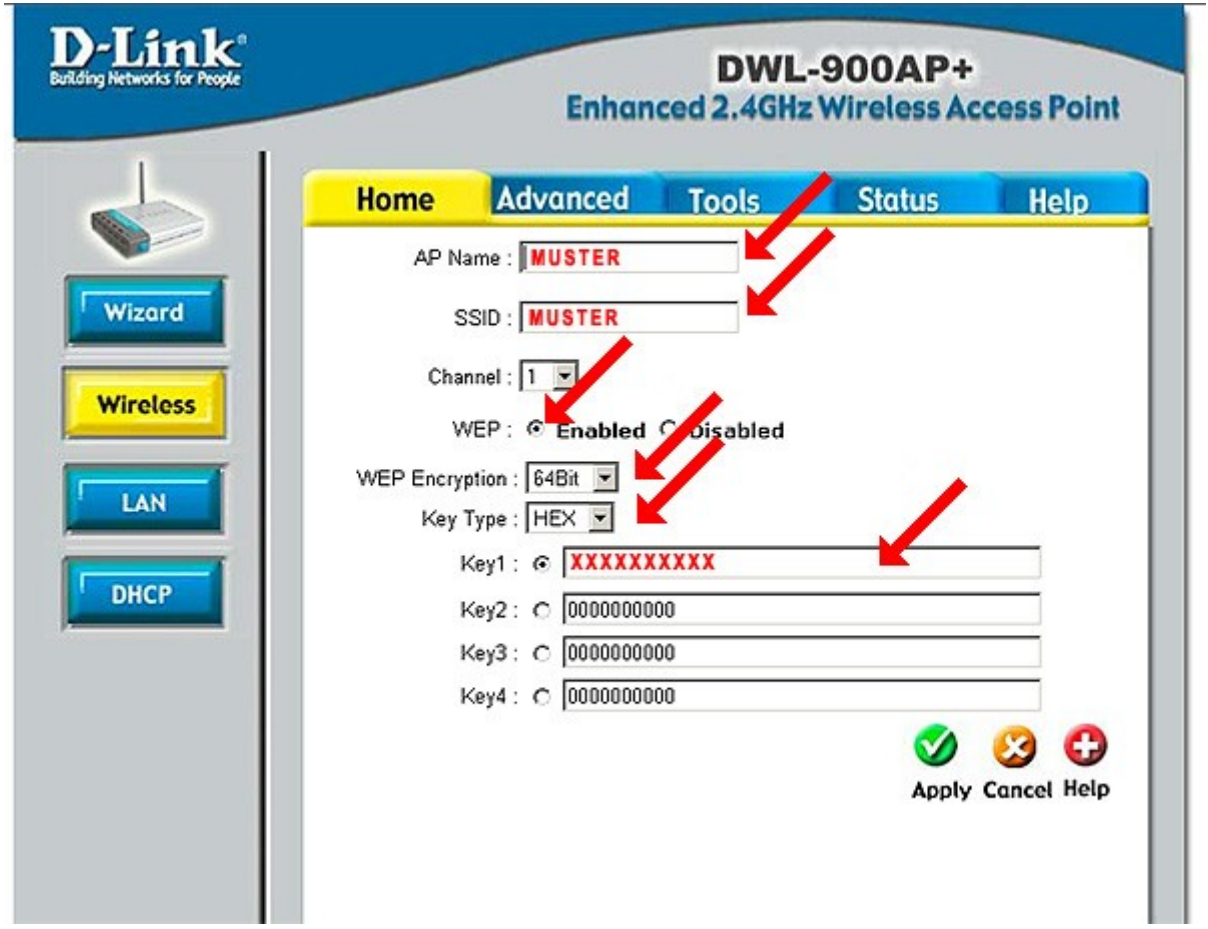
- Un DNS (Domain Name System) effectue la corrélation entre **une @IP** et **un nom de domaine** associé
  - ex : 209.85.135.99 <-> google.fr
- Le serveur qui effectue la résolution de nom est en général hébergé au niveau du FAI et son adresse est récupérée dynamiquement en même temps que l'IP publique (routeur, PC).



Configuration du réseau Wi-Fi

Réglages Radio de l'AP

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

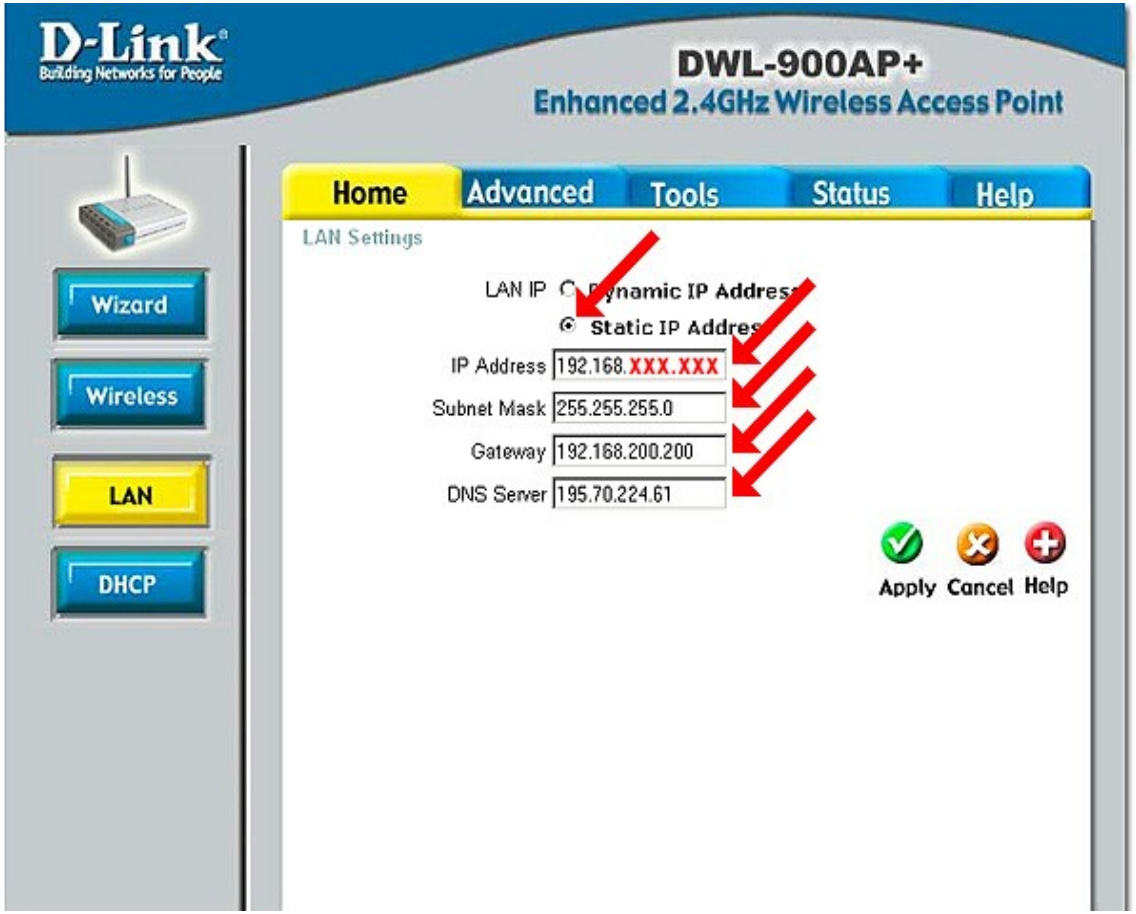


- Configuration Radio avancée
  - Puissance d'émission
  - Chiffrement et authentification : WEP / WPA
  - Filtrage des adresses MAC
  - Radio : Débits, DTIM, Fragmentation, Beacon...

Réglages TCP/IP de l'AP

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

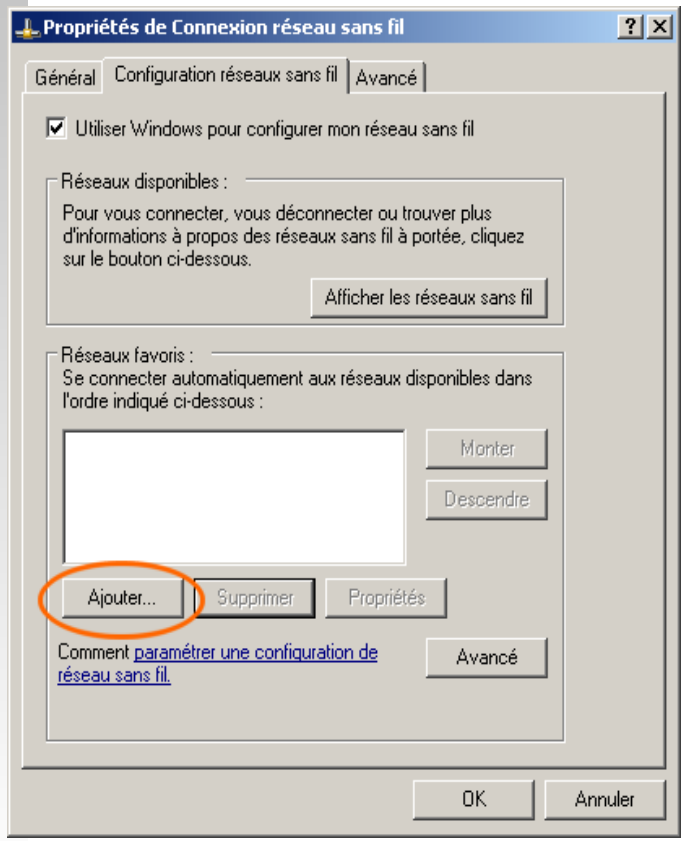
  ou
  - attribution en DHCP
- @IP LAN
  (interface Radio et Switch)
  - Activation DHCP - Plage

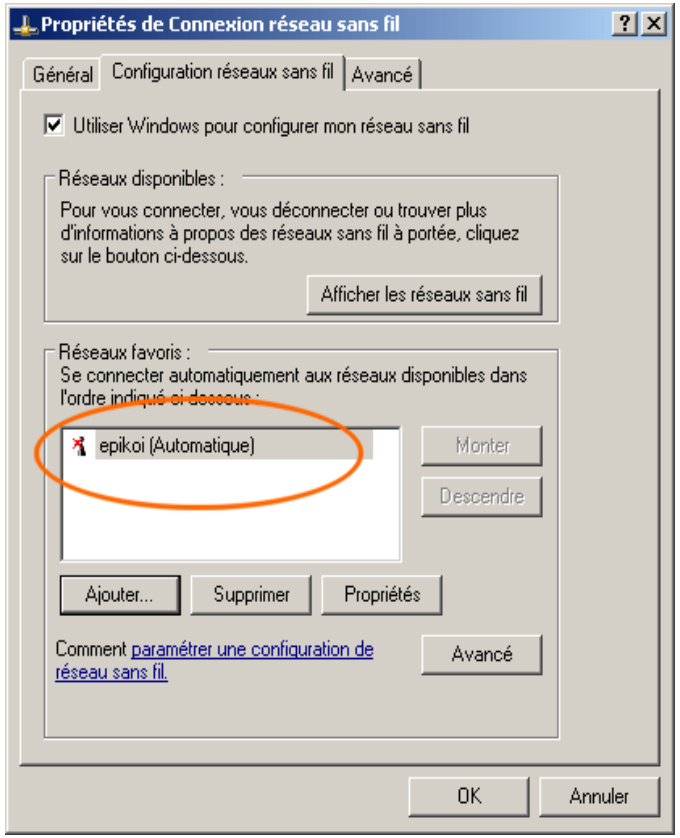


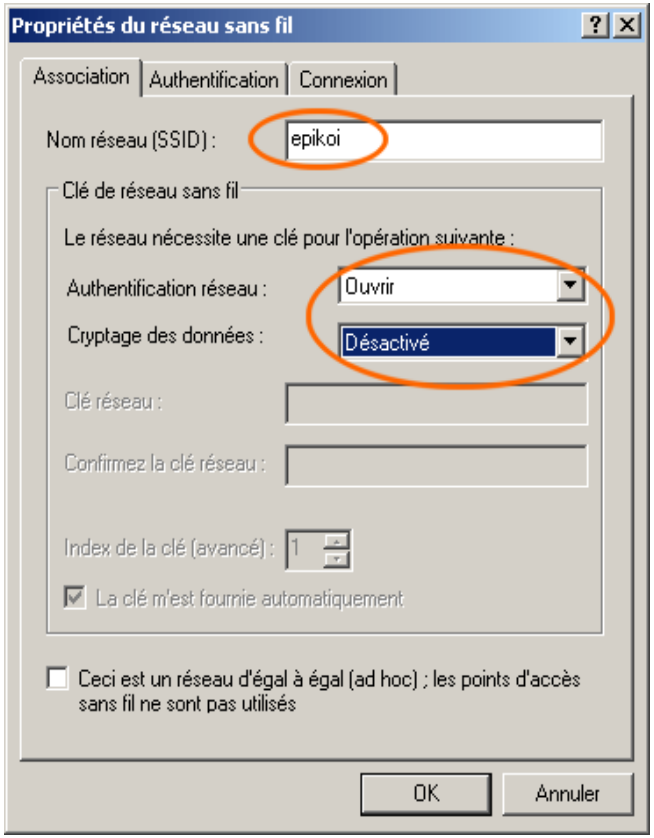
Réglages radio de l'adaptateur Wi-Fi

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

CRYPTAGE ► AUTHENTIFICATION ▼	Pas de Cryptage	WEP	TKIP	TKIP
Ouverte	X	(X)		
Partagée	(X)	X		
WPA-PSK			X	
WPA-EAP (802.1x)				X





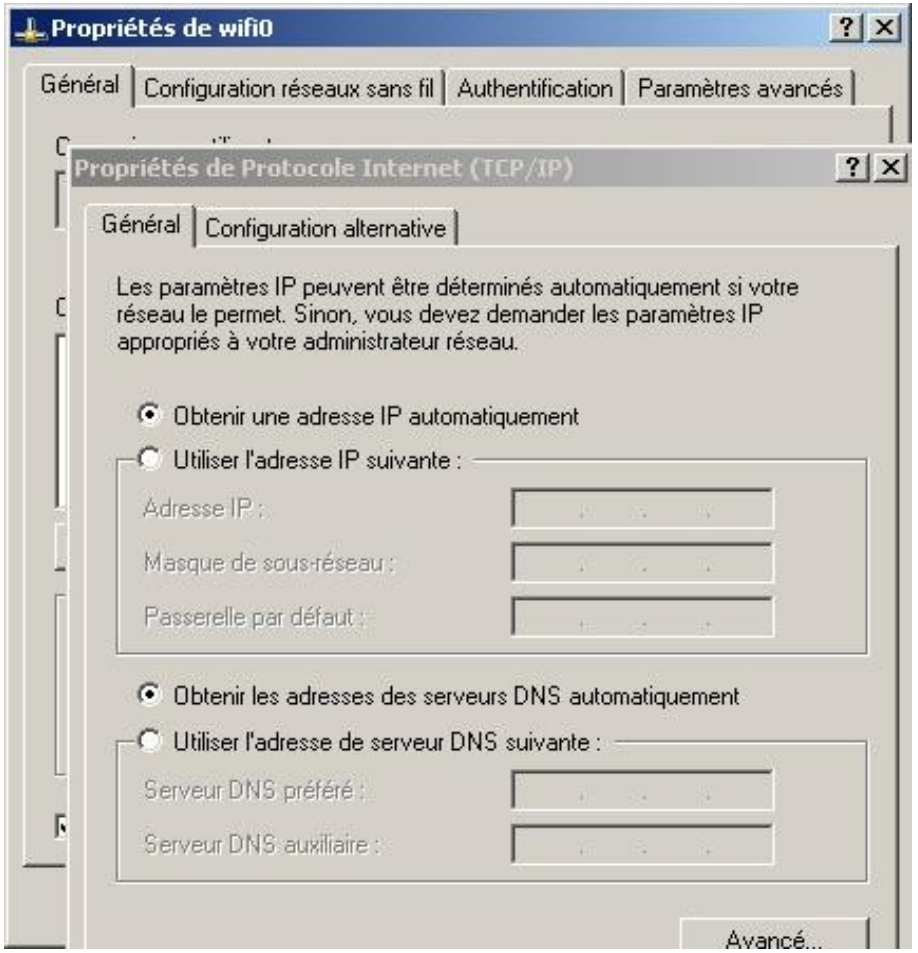


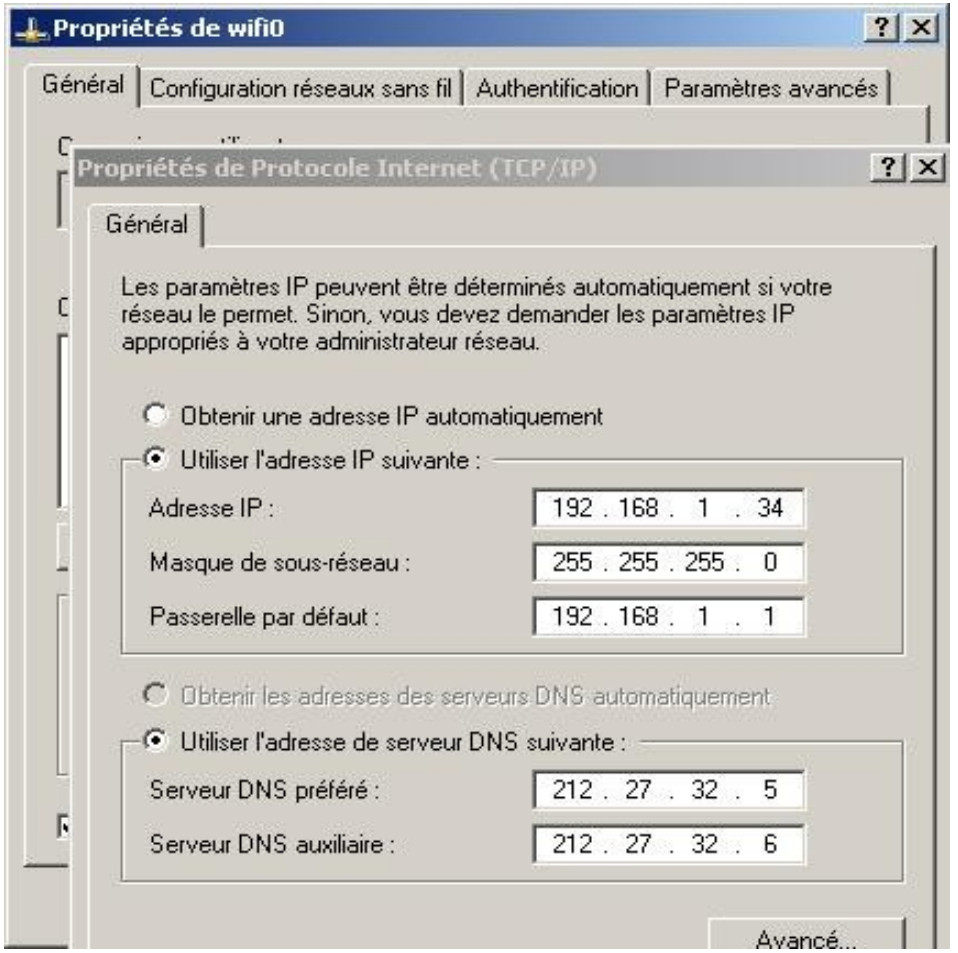
Réglages TCP/IP de l'adaptateur Wi-Fi

- DHCP

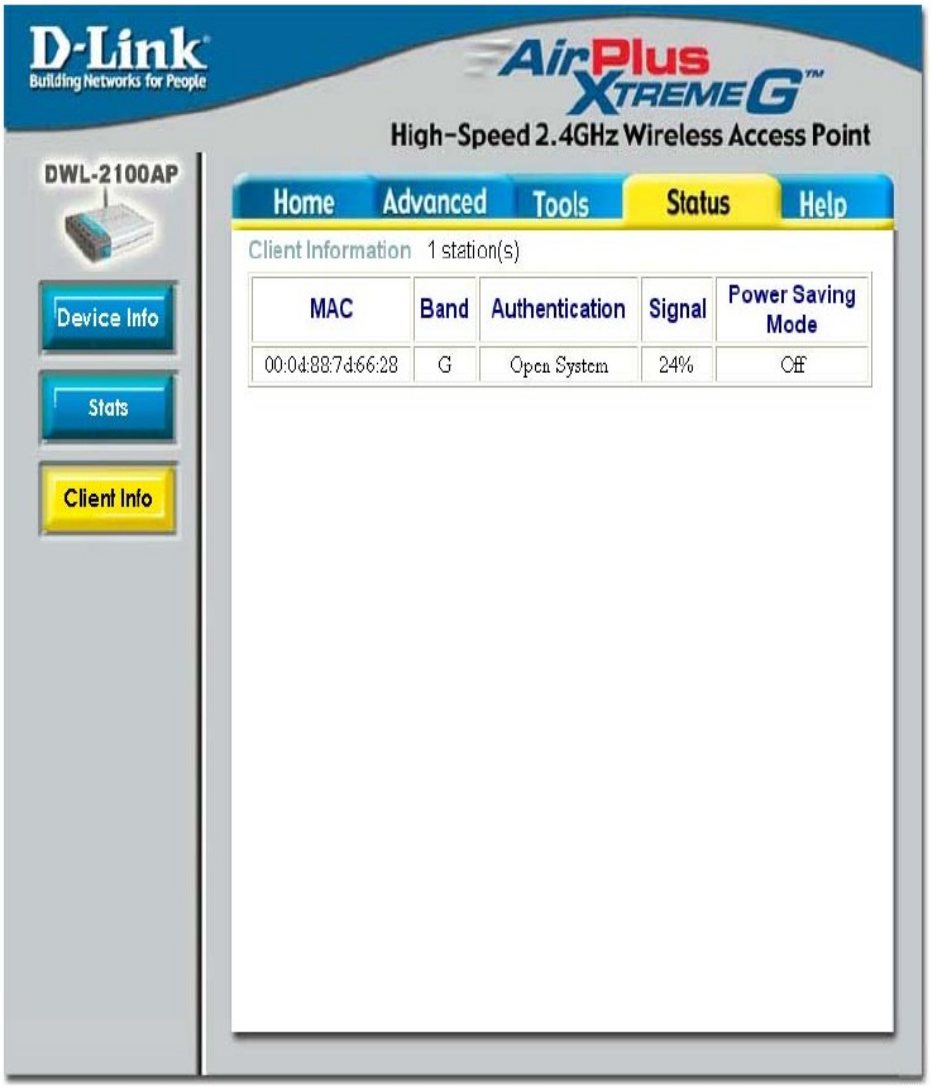
OU

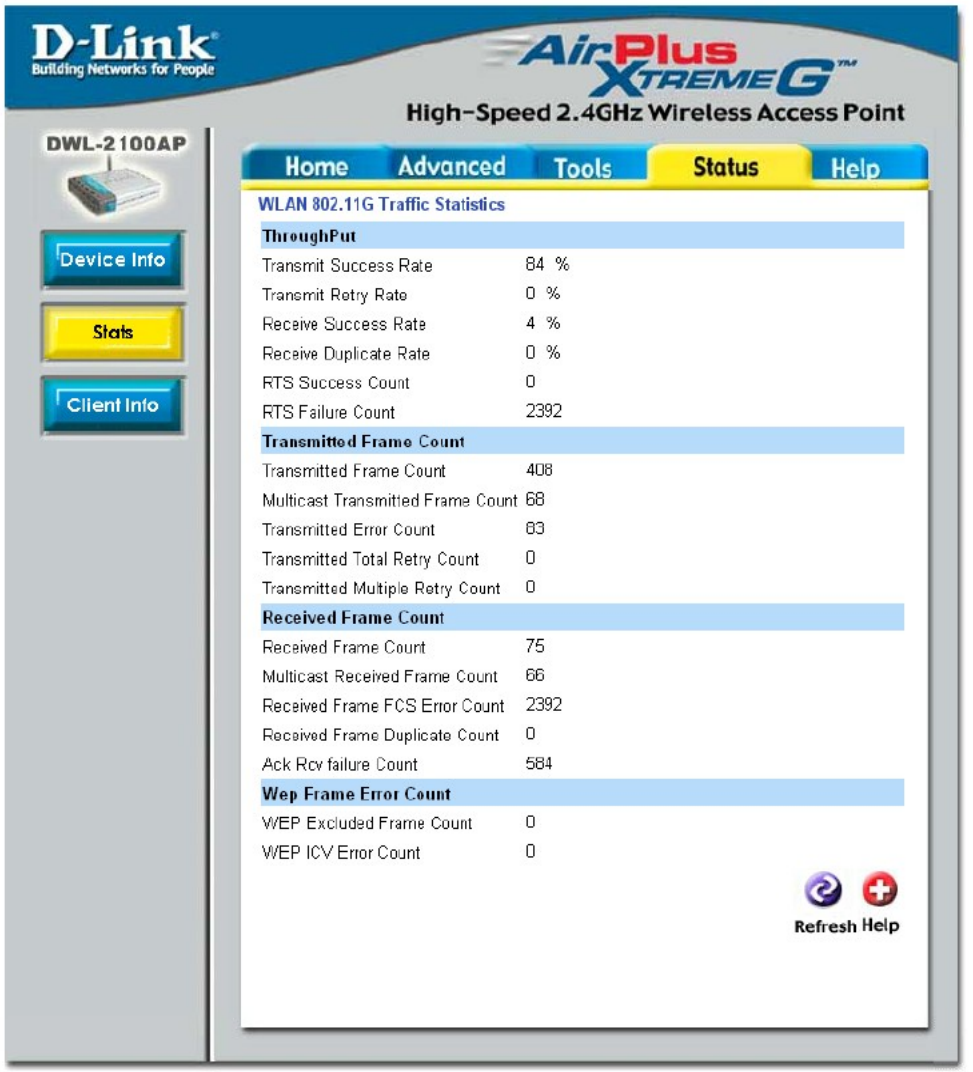
- Valeurs fixes
  - @IP / masque
  - Passerelle
  - DNS



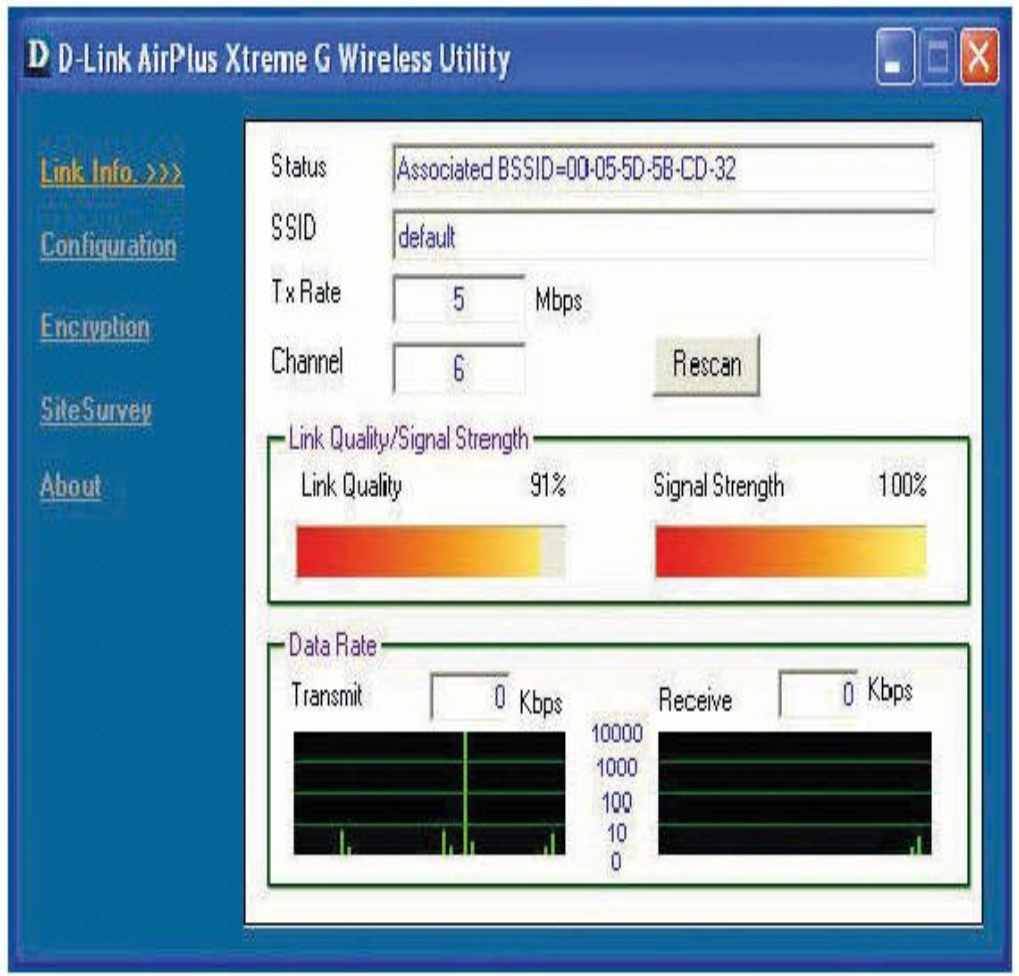


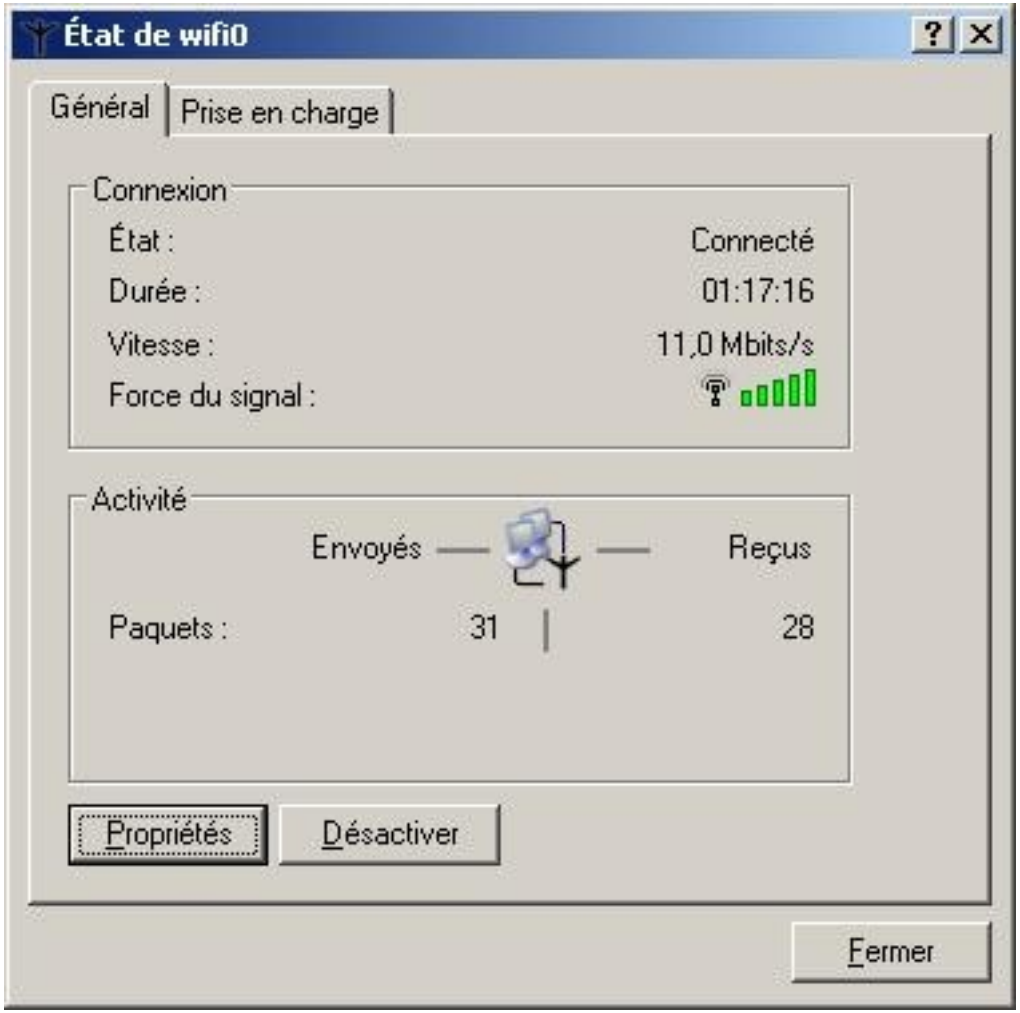
Diagnostics d'association (AP)





Diagnostics en mobilité (client)

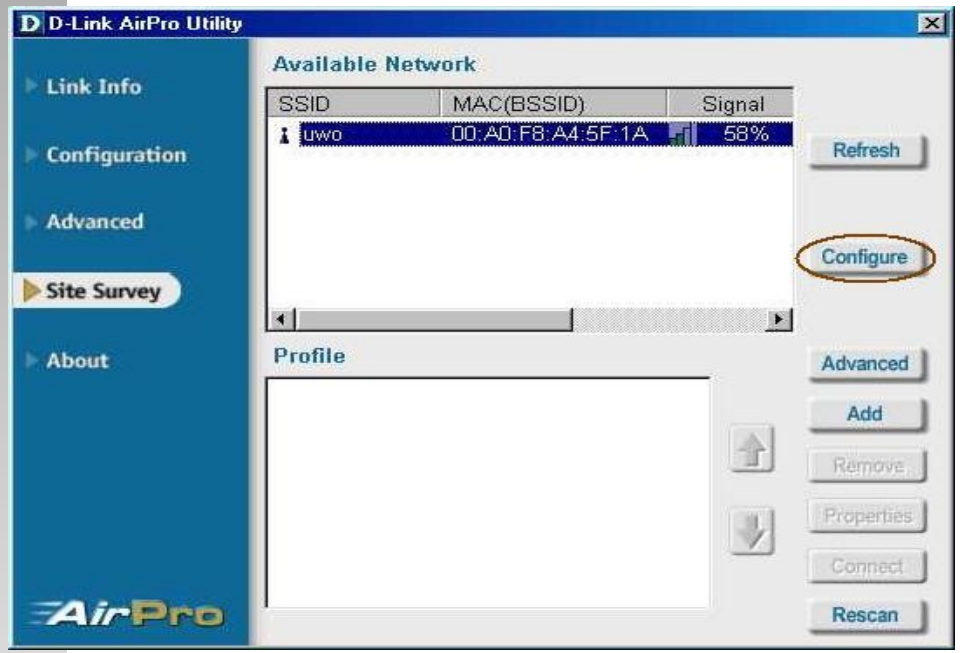


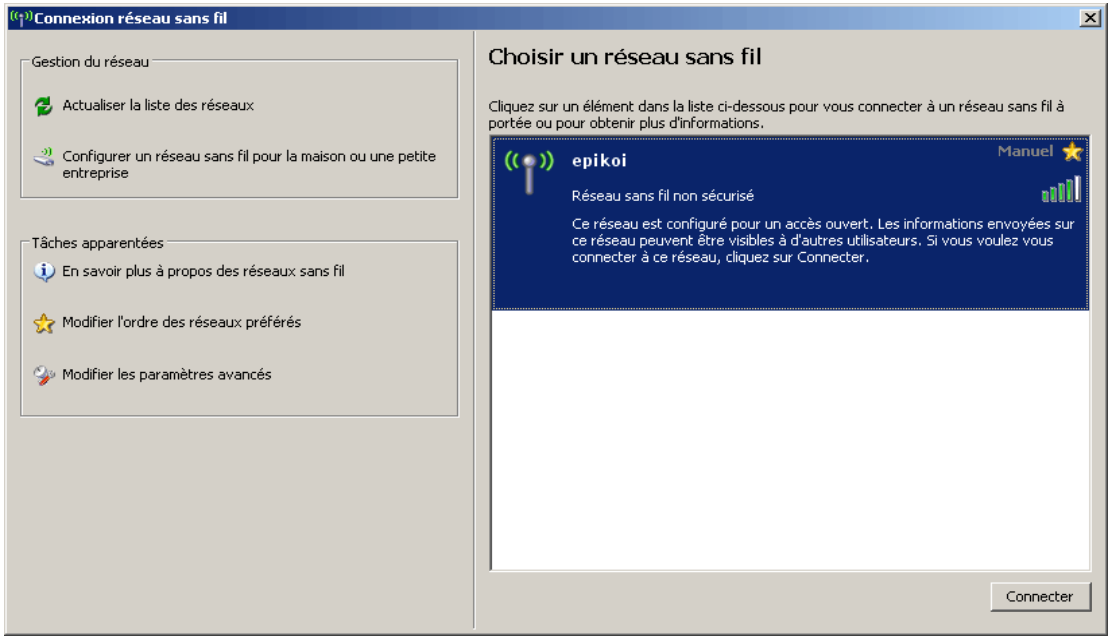


Outil Fabricant (Dlink)
-Puissance du signal
-Qualité du signal

Outil générique (Windows)
-Puissance du signal

Détection des réseaux (client)

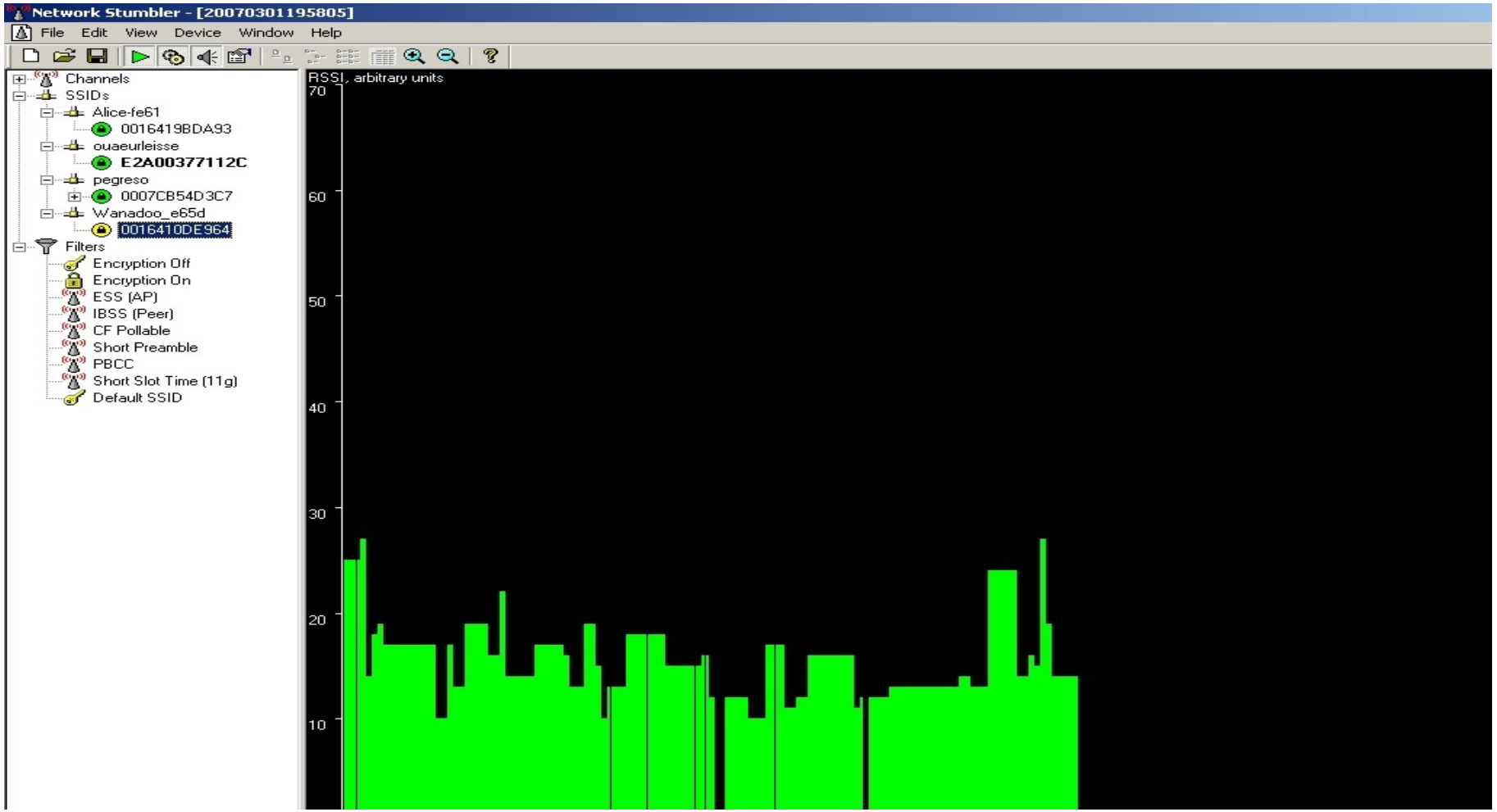




Outil Fabricant (Dlink)
-SSID
-BSSID
-Puissance du Signal

Outil générique (Windows)
-SSID
-Puissance du signal

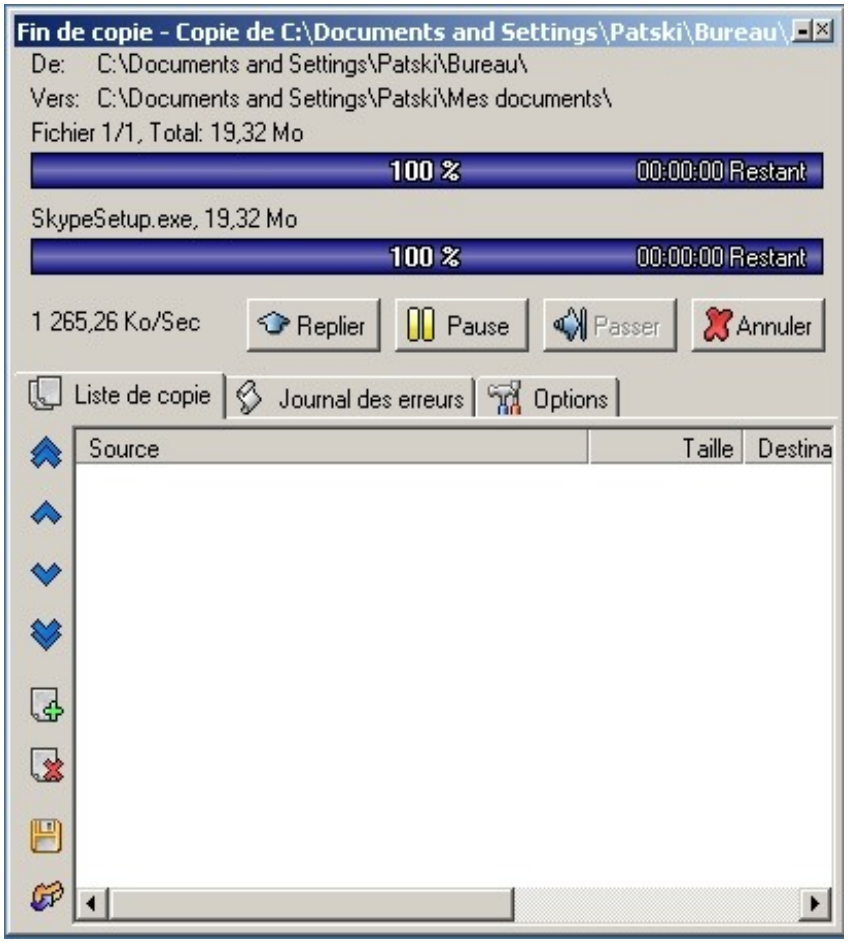
Outils génériques (client)



NetStumbler
-SSID
-BSSID
-Puissance du Signal

-type d'encryption
-rapport S/B

Mesure de débit



SuperCopier
(Windows)

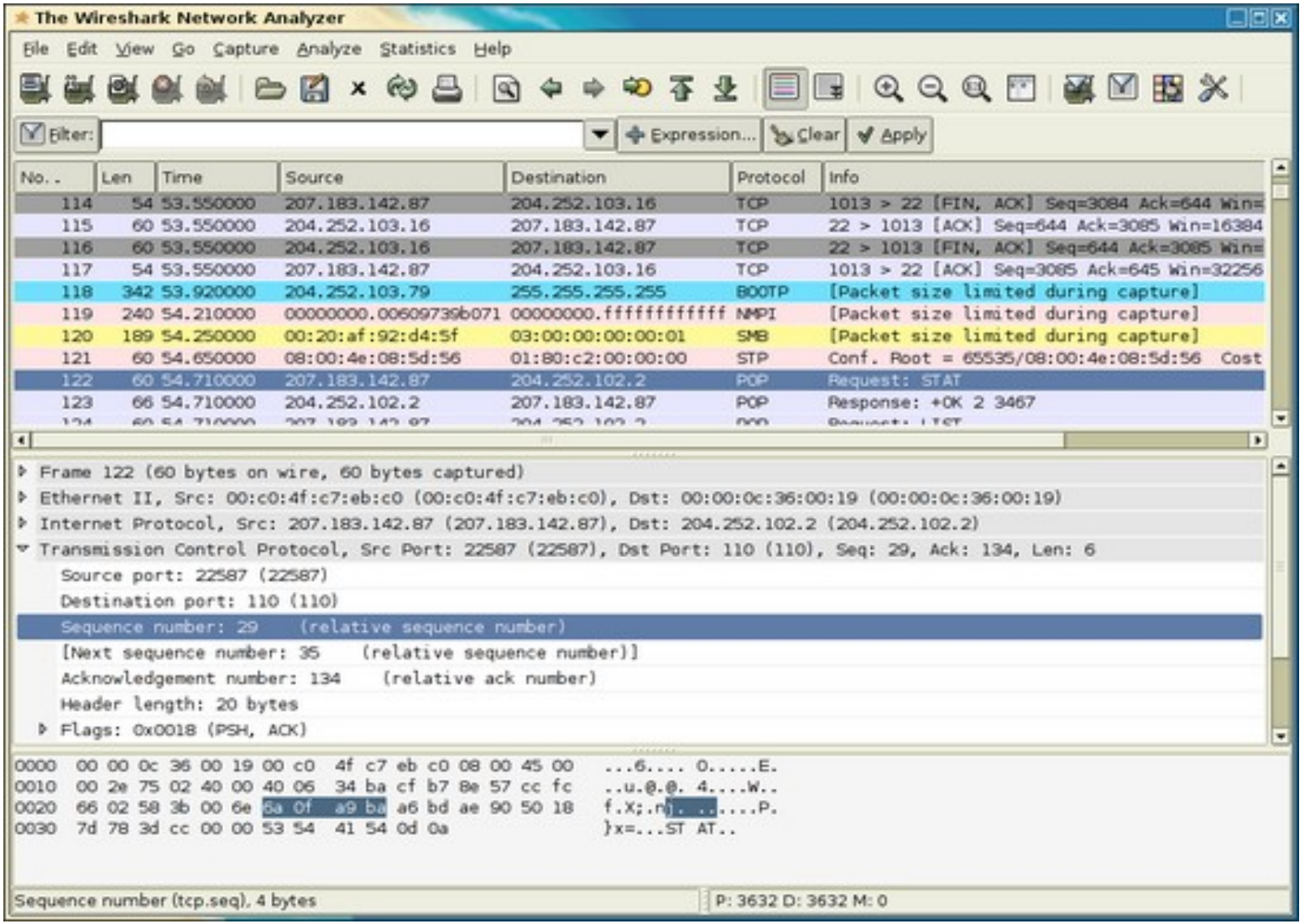
```
C:\>iperf -c 195.128.64.194 -p 4665 -t 60
------------------------------------------------------------
Client connecting to 195.128.64.194, TCP port 4665
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[1916] local 172.27.7.106 port 4632 connected 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)

Partie 4

Matériel

-

Liens entre portée, débit et puissance

Chipsets et Fabricants

- Quelques fabricants de Chipsets recouvrent la quasi totalité des cartes
  - Prism (Interstil) : Dlink, Linksys, Netgear
  - Texas Instrument : Dlink, US-Robotics
  - Hermes : Onorico, Buffalo
  - Atheros et Broadcom: dernirères versions 54Mbps
- Certains Chipsets ne sont pas utilisables en écoute
- Le label Wi-Fi garantit l'interropérabilité du matériel et des normes vues jusque-là.
  - En cas de mélange des normes, le débit maximal sera le plus faible à savoir celui de la norme 802.11b
  - Quelques normes propriétaires rares (Dlink : 802.11+ ; Cisco : TKIP...)

Points d'accès

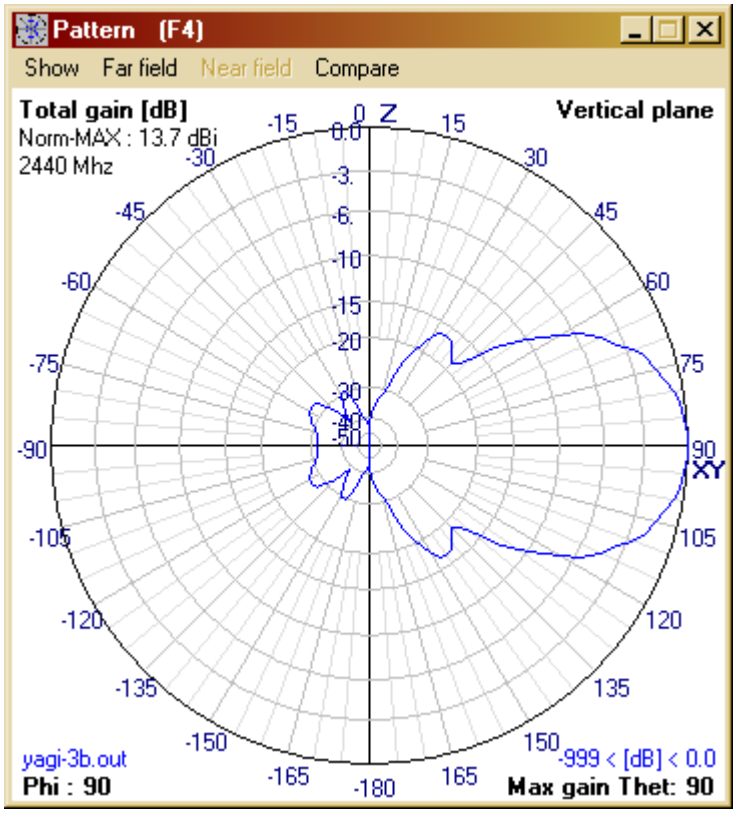
- **Points d’accès (eq. switch)**
  - Sensibilité en réception et puissance de sortie.
  - Topologies supportées (AP, Bridge, AP Client, repéteur…)
  - Services supplémentaires (DHCP, routage, filtrage des clients, 802.1x, 802.1q)
  - Exemple du Cisco et du Dlink

Adaptateurs WiFi

- **Cartes clientes (éq. carte réseau)**
  - Tous types d'adaptation : PCMCIA, PCI, USB, CF
  - Trois types de réception : directe, patch ou avec antenne extérieure
  - Bonne interopérabilité

Antennes

- Le **gain** d'une antenne est exprimé en **dBi**
  - 3 dB <-> multiplication par 2 ; 6 par 4 ; 9 par 8
- On note la répartition spatiale de ce gain sur un diagramme
- Le choix d'une antenne doit se faire sur le compromis : **ouverture angulaire/portée** (et prix)



Antennes

	Gain	Ouverture	Coût	Nom
Directionelle	12 à 19 dBi	45 à 60 °	30 à 60 euros	Yagi – Grids
Sectorielle	9 à 12 dBi	120 °	60 à 100 euros	Patch
Omni-directionelle	7 à 9 dBi	360 °	100 à 150 euros	
Ricorée	8 dBi	50 °	10 euros	Pringles
Mini-omni	2 dBi	360 °		

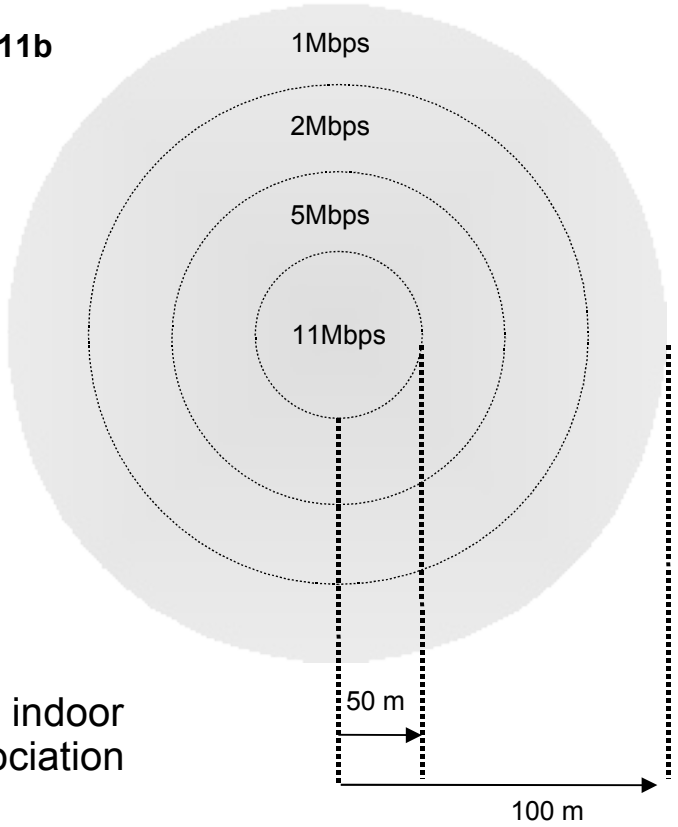
Les connectiques

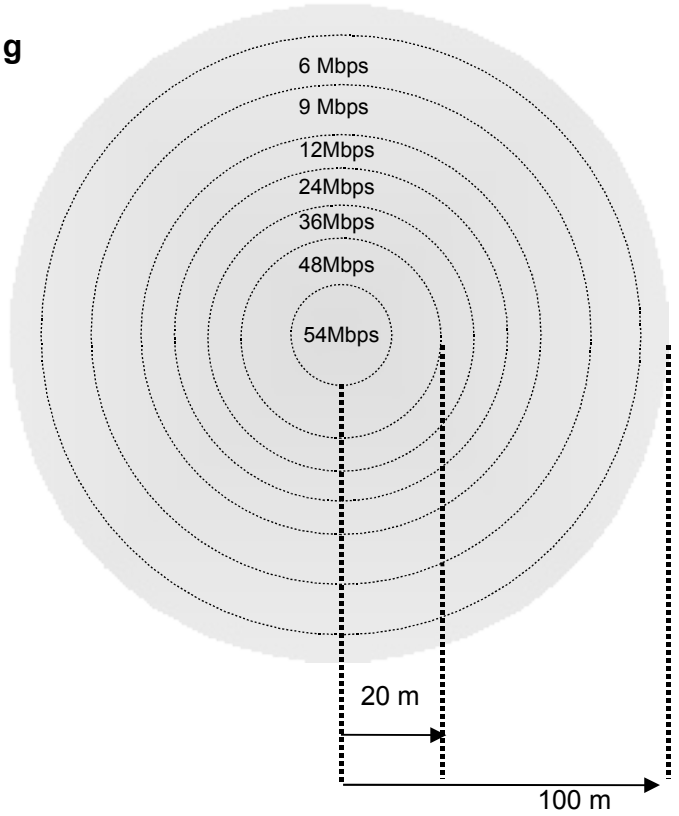
- Type N
  - La connectique d'antenne standard
- Type TNC-RP
  - Utilisée par les constructeurs Cisco et Linksys
- Type SMA
  - Répandue sur les cartes PCI et le matériel Dlink
- Type MMCX
  - Dédiées aux sorties mini-PCMCIA

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)

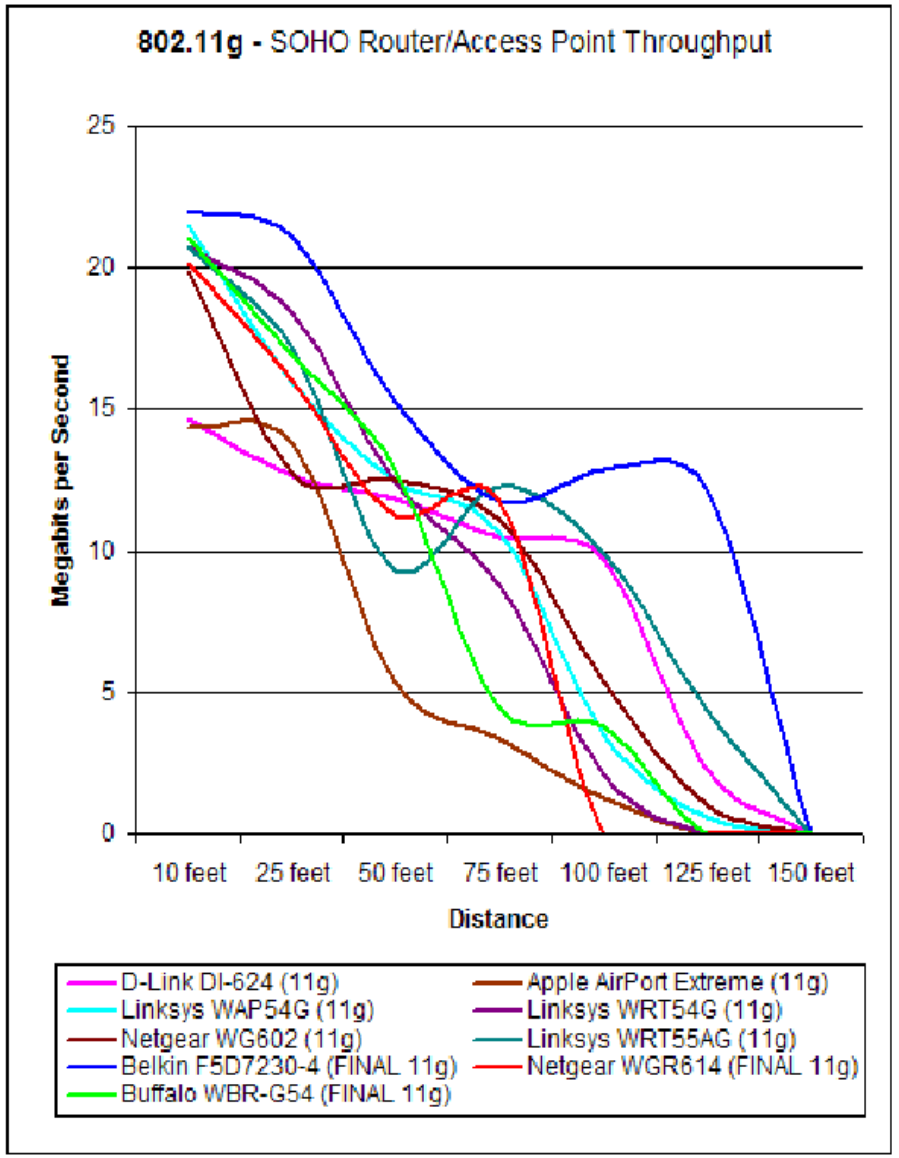
débits indoor d'association

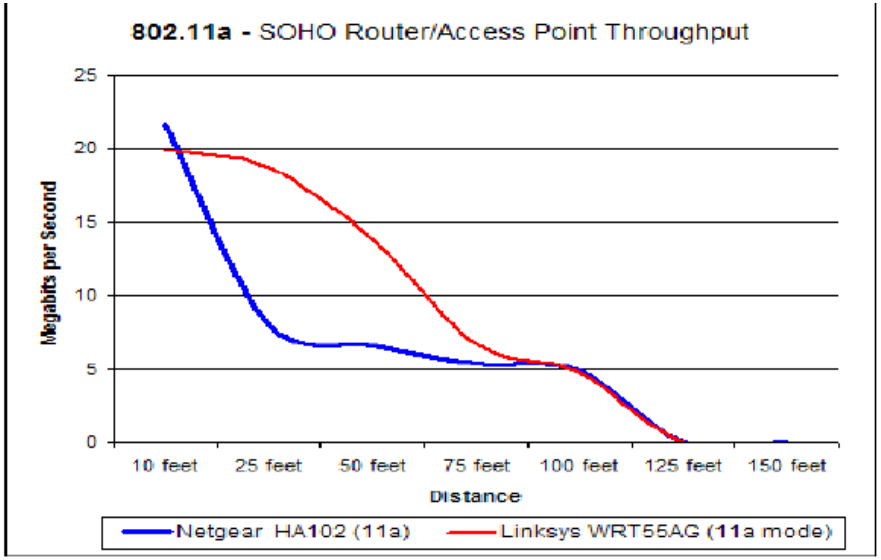


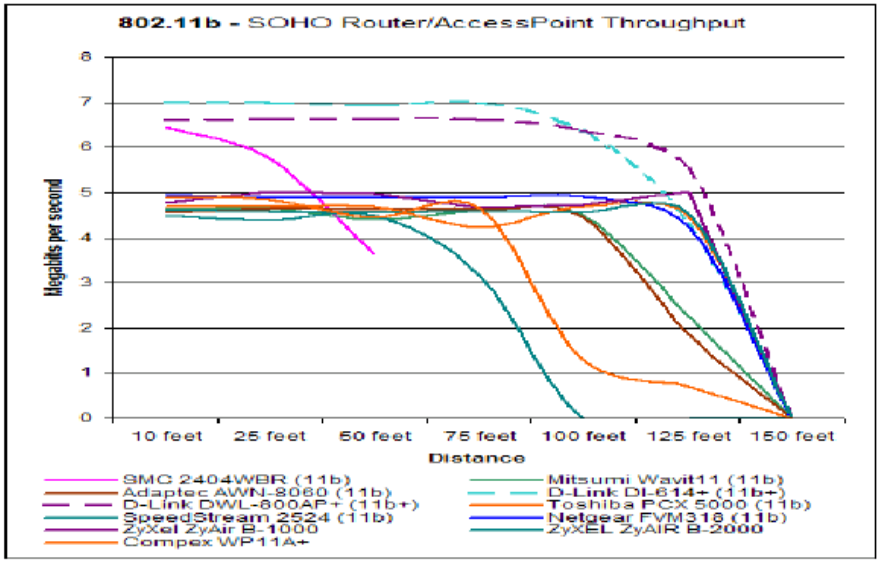


Débits effectifs

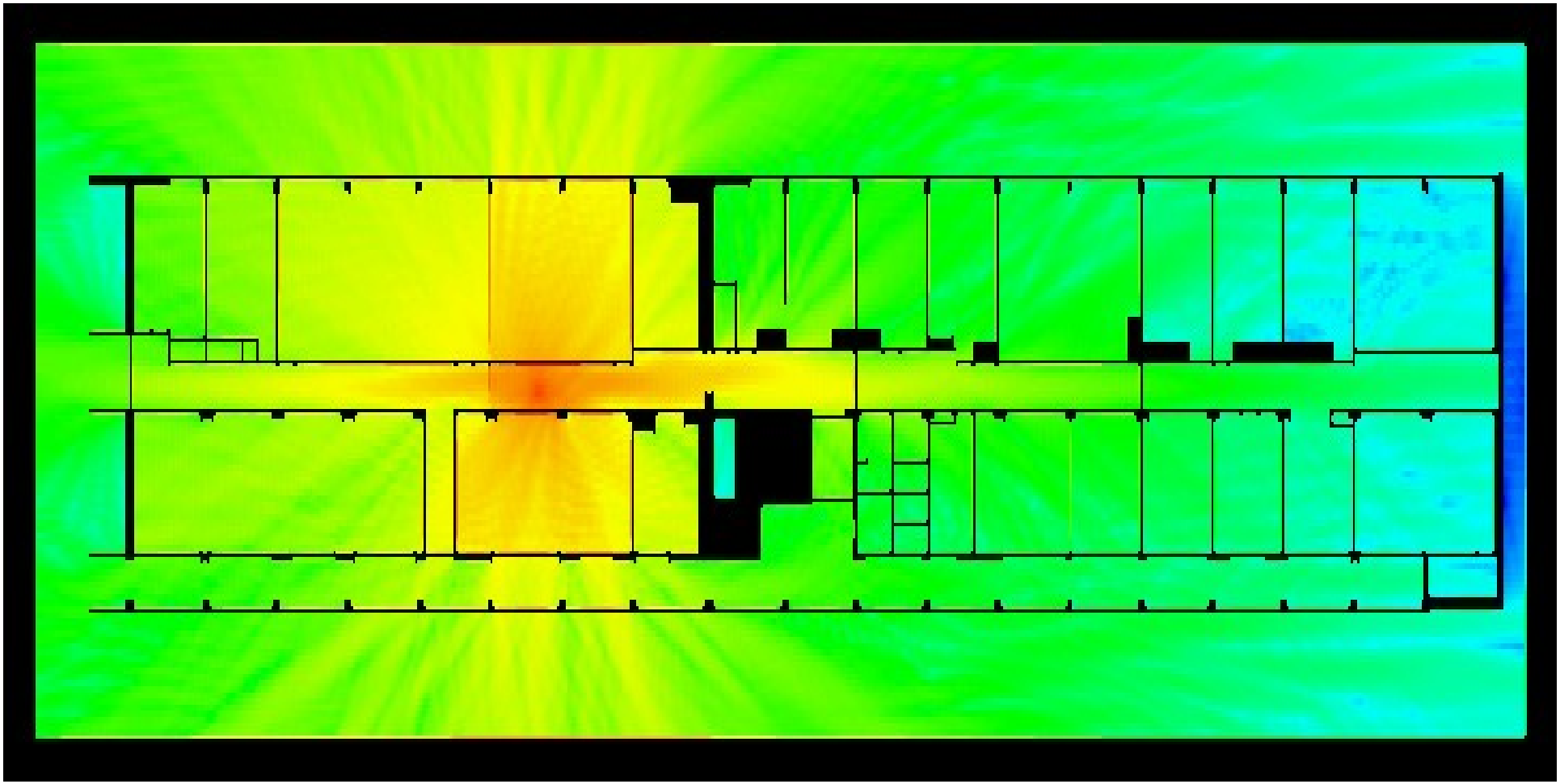
- Débit en ftp binaire ≈ 50 % du débit annoncé.







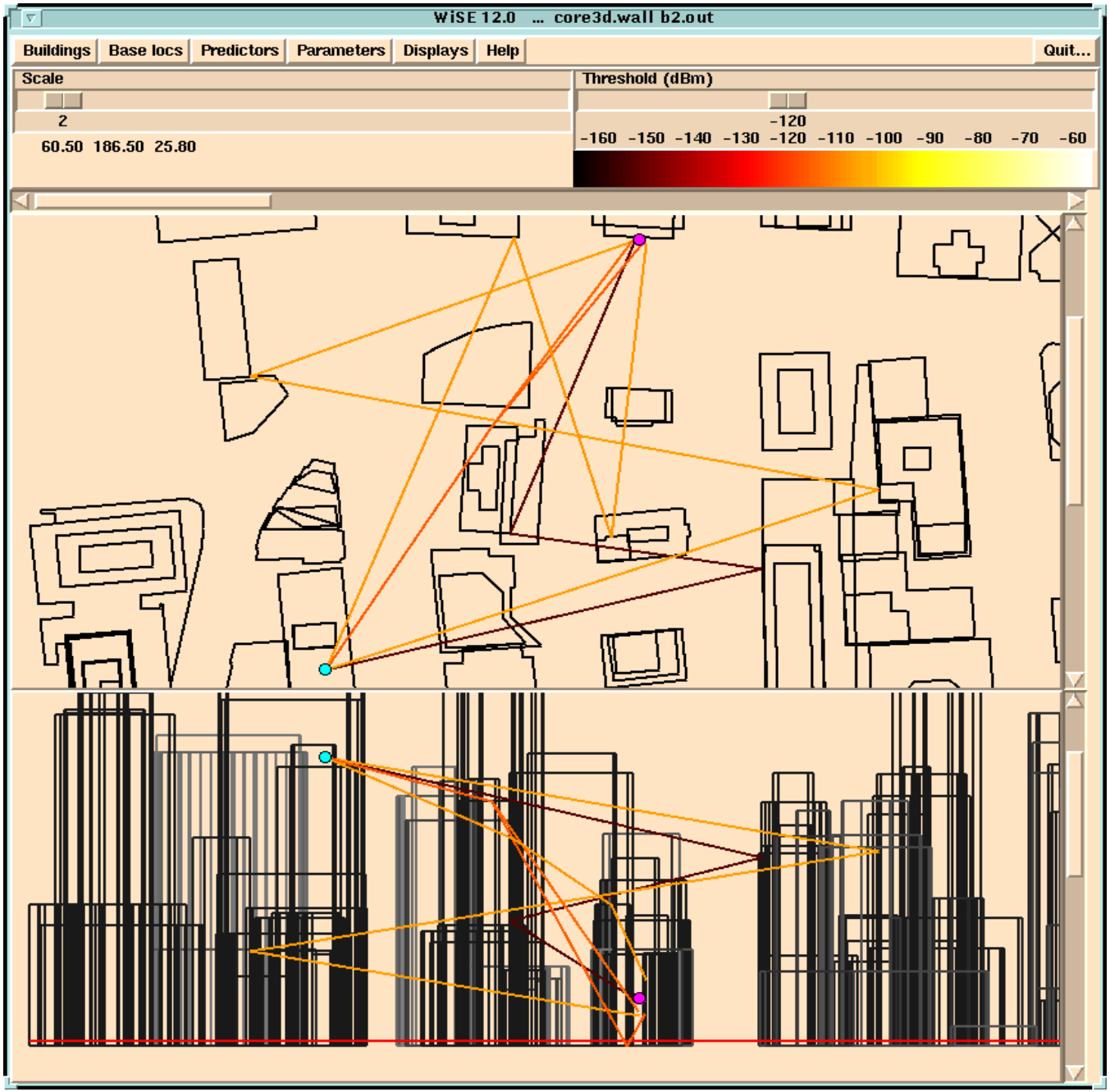
Propagation des ondes en indoor



- réflexions multiples
- diffractions multiples
- géométrie 3D
- influence de la polarisation

Références : John C. Stein

Propagation des ondes en milieu urbain



Références : John C. Stein

Calcul de la PIRE

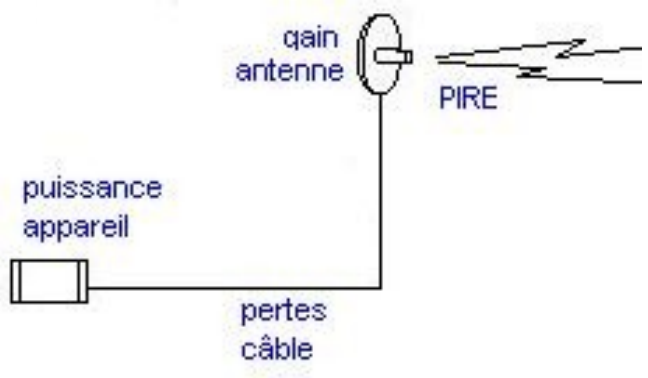
- La PIRE est la puissance effective rayonnée en sortie d'antenne
- Elle est limitée à 100 mW à l'extérieur (et à l'intérieur) en France.
- 100 mW = 20 dBm
- Compter 1 dB par mètre en moyenne pour les pertes

PIRE (dBm) =

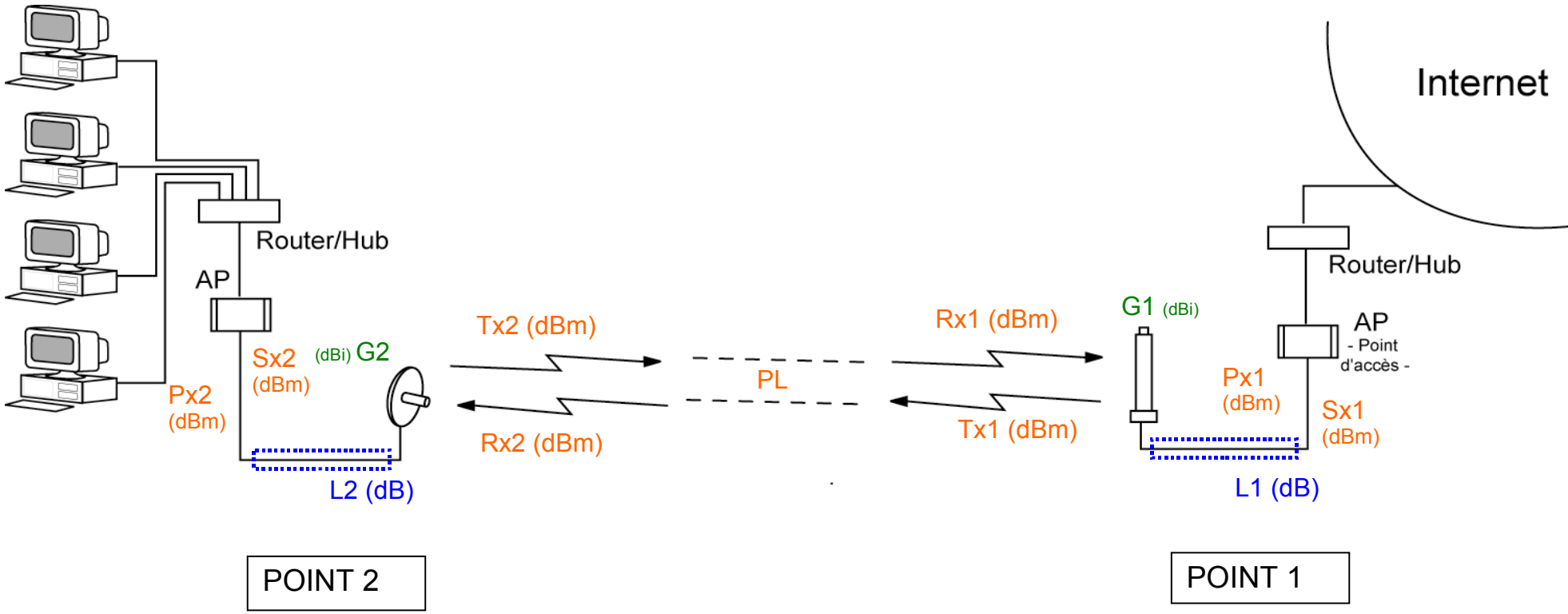
puissance en sortie AP (dBm)

– pertes câbles (dB)

+ gain d'antenne (dBi)



Théorie de portée radio



- Le champ doit être exempt de masque (bâtiment, arbres...) et doit respecter la zone de Fresnel.
- Les résultats sont très dépendants des sensibilité de réception des appareils.
- Avec 10 mW en sortie d'AP, 3m de câble et 2 Yagis à 14 dBi on peut obtenir sur un lien de 2 à 3 km.

Calcul de portée d'un lien

- Outils de calcul
  - http://reseau.erasme.org/article.php3?id_article=10
  - http://www.swisswireless.org/wlan_calc_fr.html
  - http://www.temcom.com/pages/dBCalc_fr.html

- **A retenir** : le meilleur résultat de portée est obtenu avec l'utilisation de matériel aux caractéristiques symétriques de part et d'autre
  - AP (sensibilité de réception et puissance émission)
  - Antennes (Gain)
  - Connectiques et câbles (Pertes en ligne)

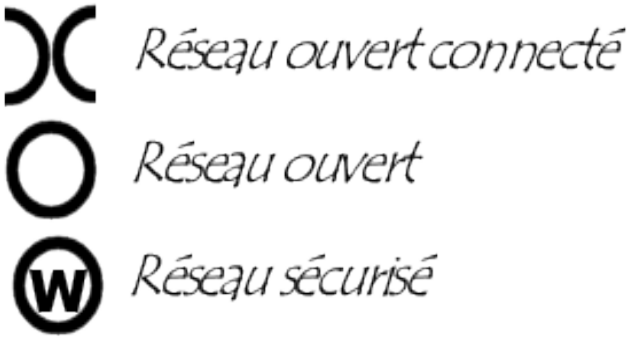
Partie 5

Sécurité

Les risques

Un manque de sécurité intrinsèque

- Propagation des ondes vaste et peu maîtrisée
  - Réseau sans fil équivalent à des câbles RJ45 qui pendent aux fenêtres ;)
- Problèmes d'usage
  - AP souvent vendus et installés sans sécurité par défault
  - AP temporaires laissés en marche à l'insu des resp. IF
- Le War-Driving
  - Un repérage des réseaux urbains accessibles :



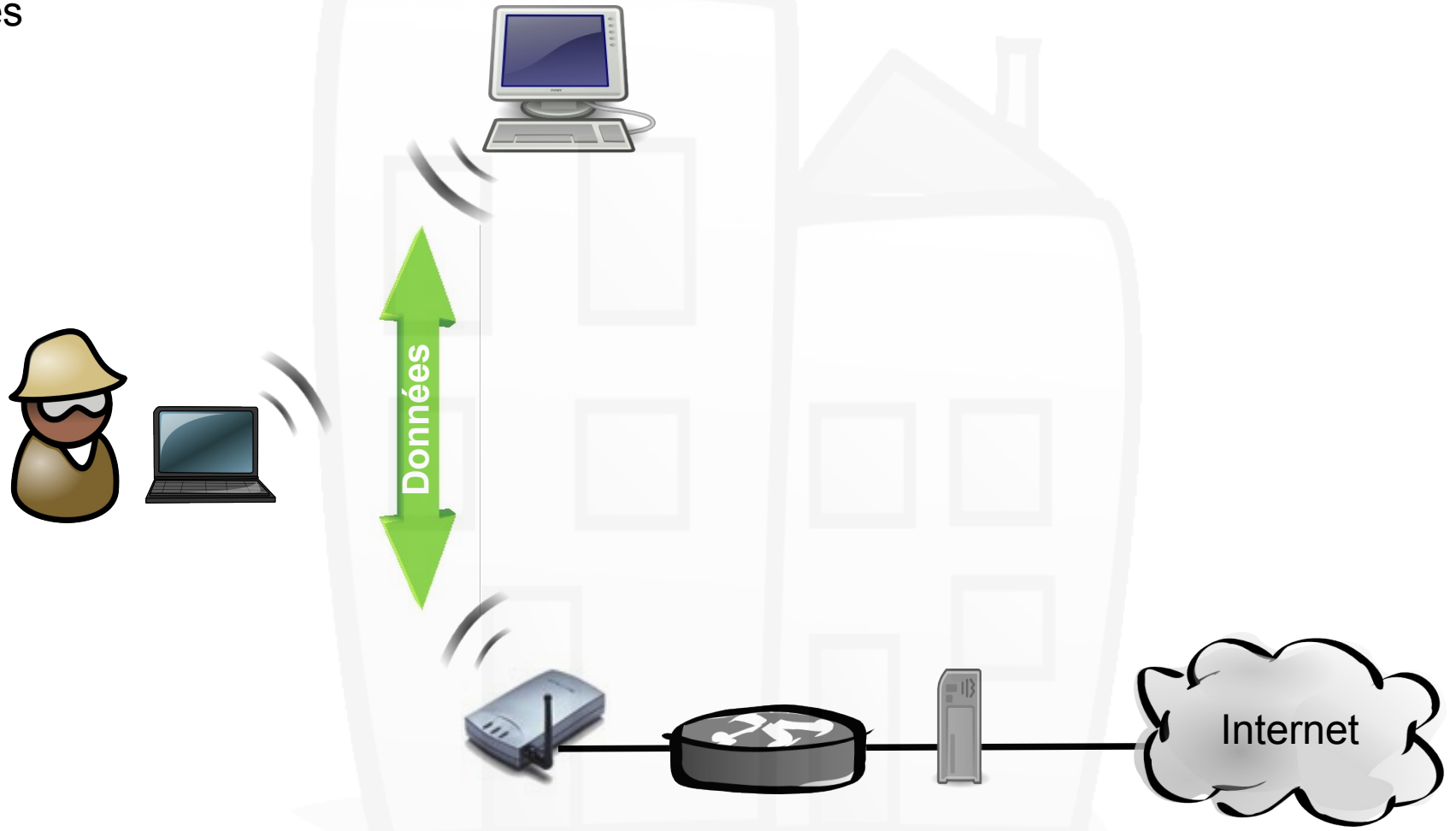
  - Voir : http://www.nantes-wireless.org/pages/wiki/index.php?pagename=WarDriving

Attaques possibles

- L'écoute des données
- L'intrusion et le détournement de connexion
- L'occupation de la Bande Passante
- Le brouillage des transmissions
- Le dénis de service

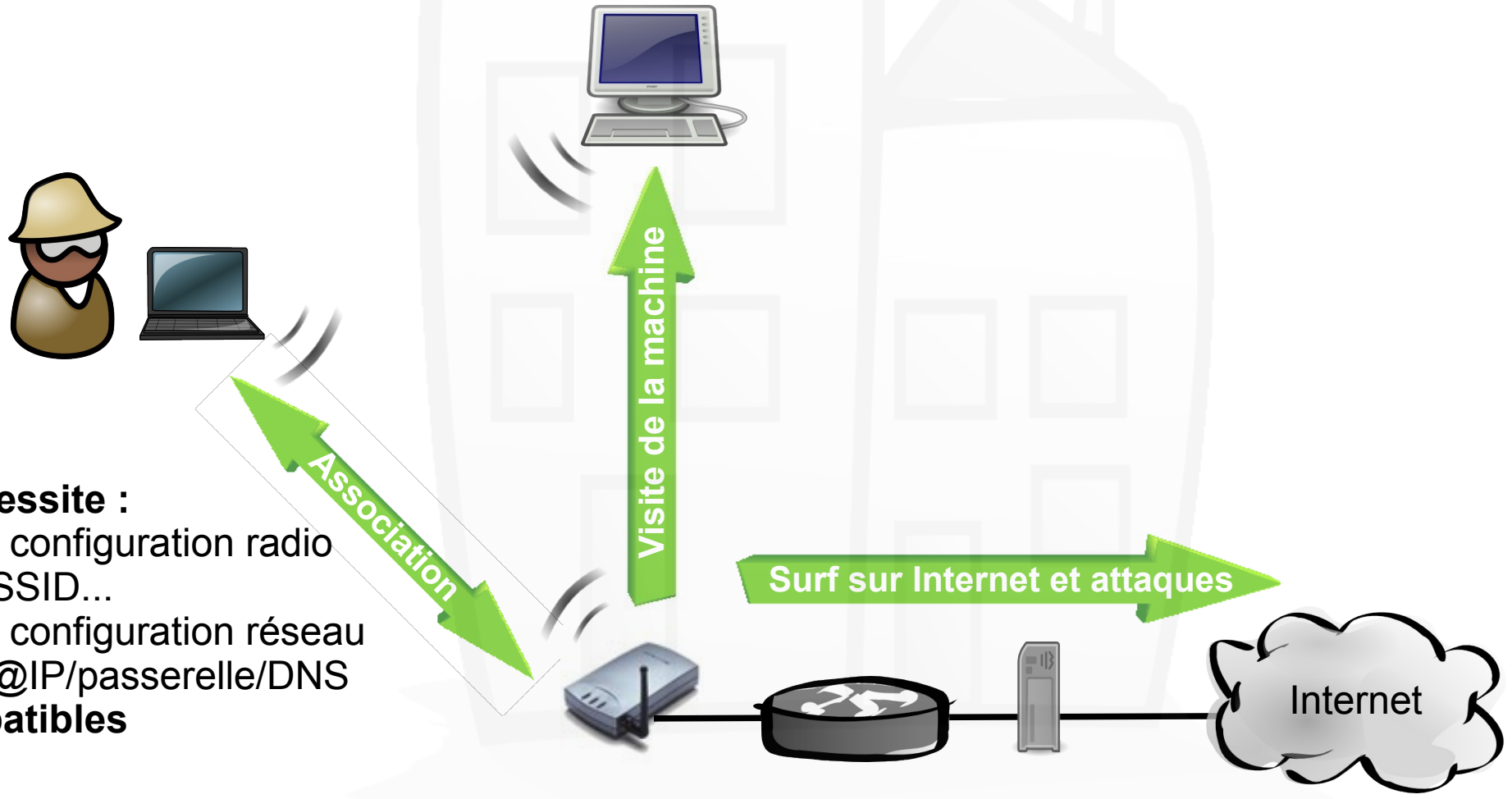
L'écoute des données

• **Solution efficace :**
le chiffrement
(ou cryptage)
des données



L'intrusion et le détournement de connexion

- **Solution efficace :**
  -restreindre l'accès radio
  -restreindre l'accès réseau
  -authentifier la personne



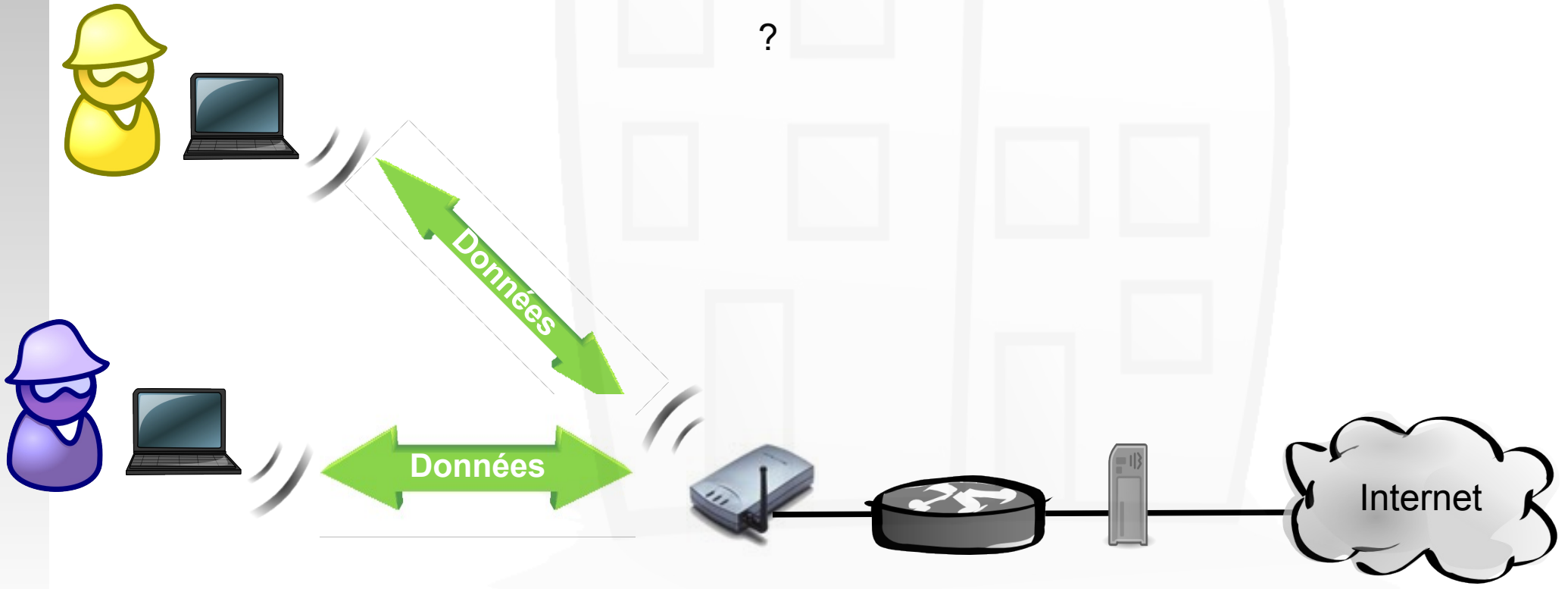
- **Nécessite :**
  -une configuration radio
    -SSID...
  -une configuration réseau
    -@IP/passerelle/DNS

compatibles

L'occupation de la bande passante

• Echange de fichiers lourds bloquant la bande passante de l'utilisateur principal. (importante de l'upload)

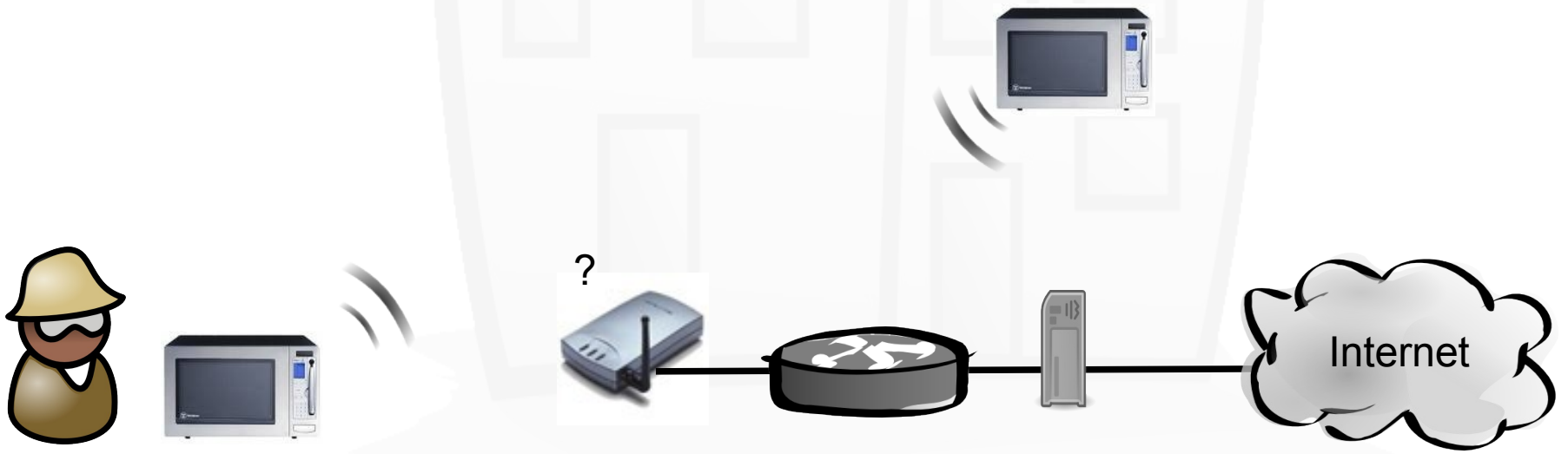
• **Prérequis et solutions :** identiques.



Le brouillage de transmission

- **Provenance :**
téléphones DETC,
fours à micro-ondes

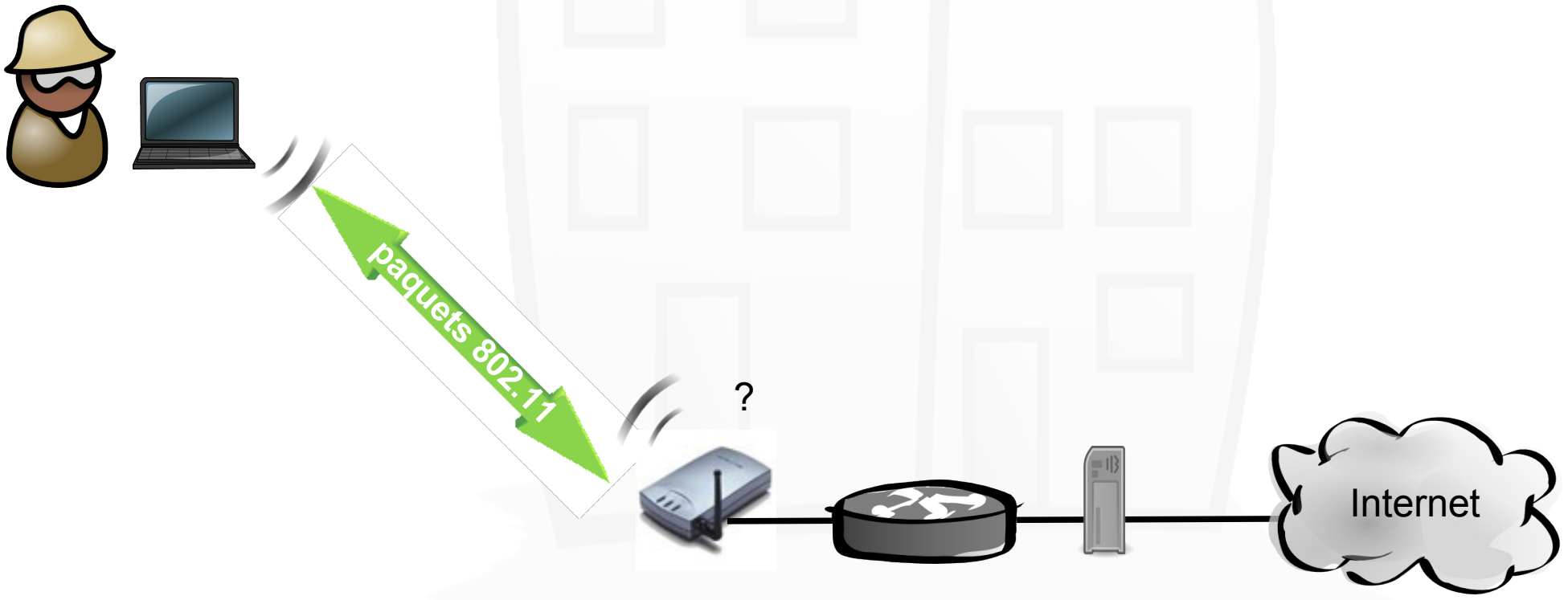
- **Solution efficace :**
couper la source
ou s'éloigner



Le dénis de service

• Utilise la connaissance du protocole CSMA/CA pour occuper le PA ou lui envoyer des paquets chiffrés pour la mettre HS

• **Solution efficace :**
-WPA

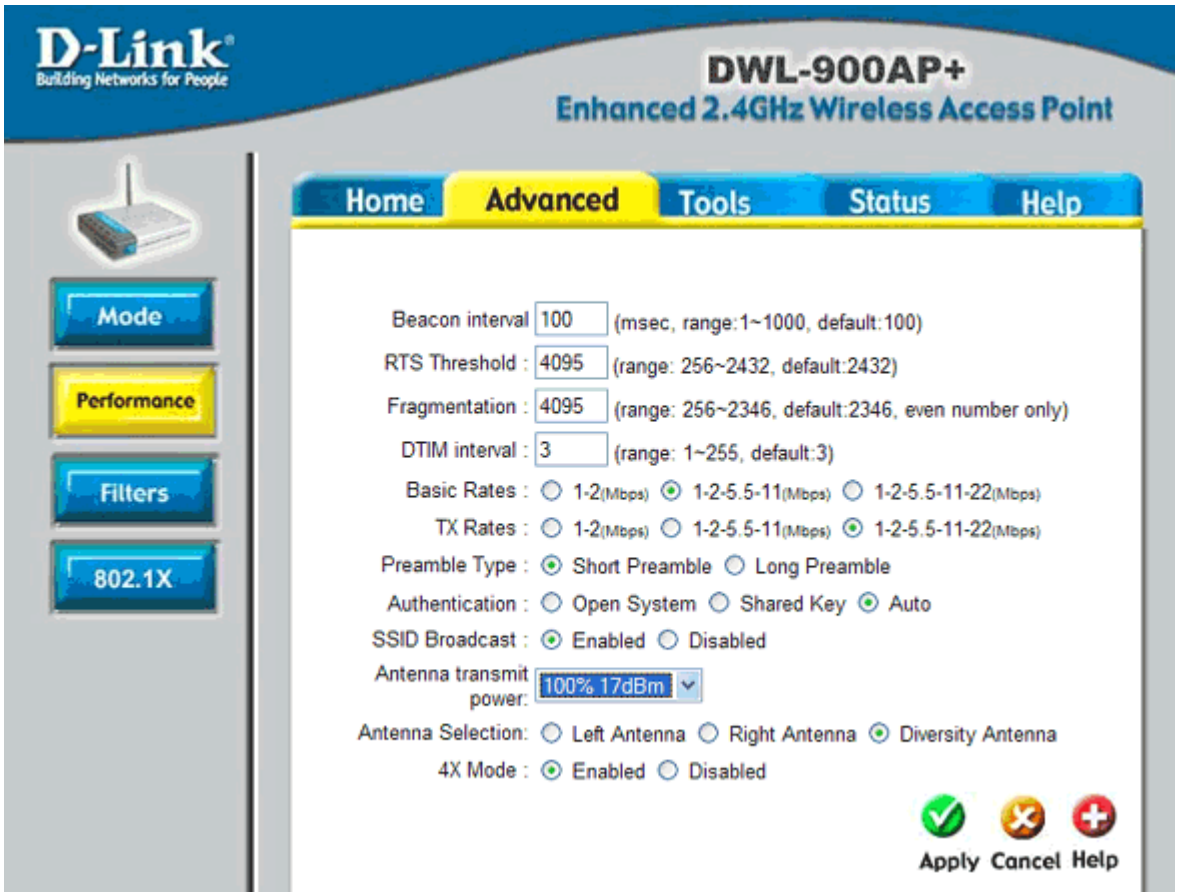


Les solutions

Une configuration radio adaptée

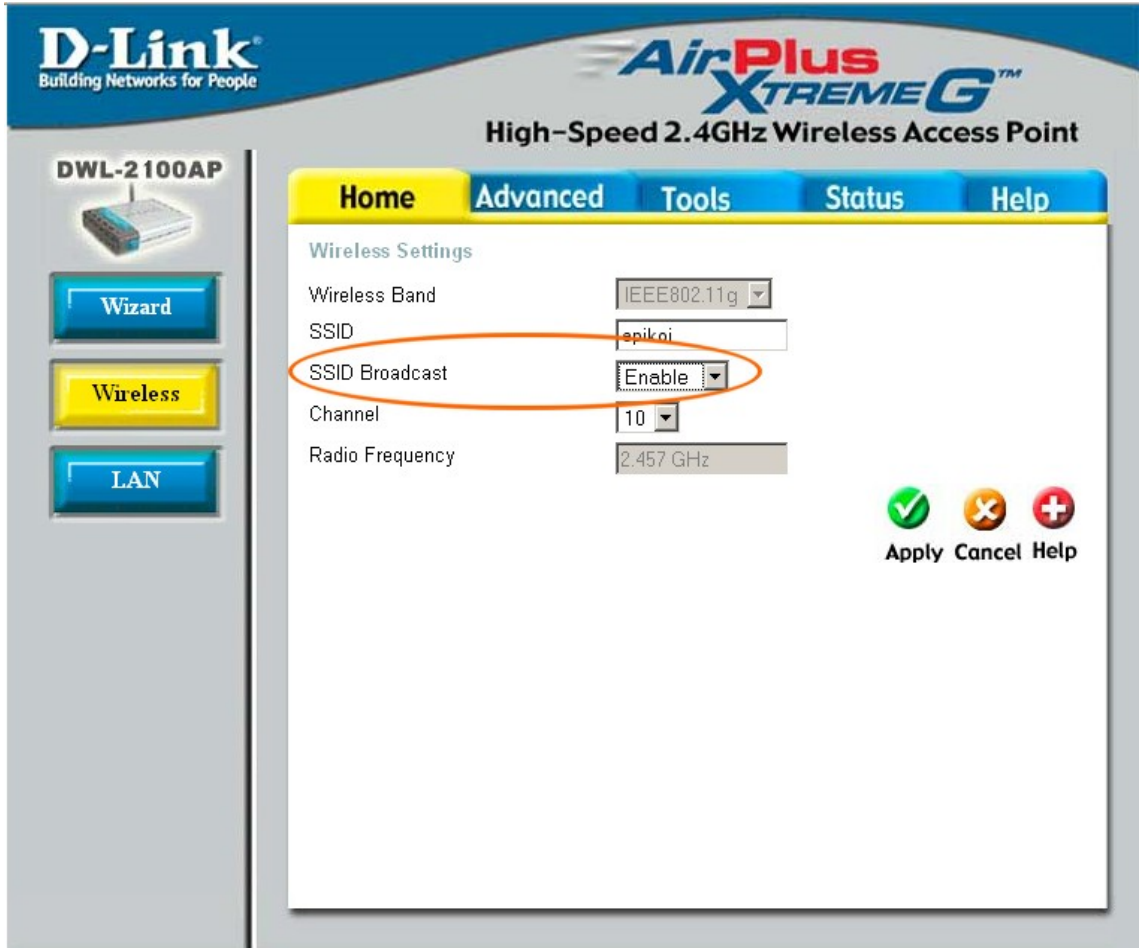
En fonction de la zone effective à couvrir :

- **Positionner les points d'accès** de manière optimale
- **Diminuer la puissance d'émission** du PA
- Faire des **tests** en situation



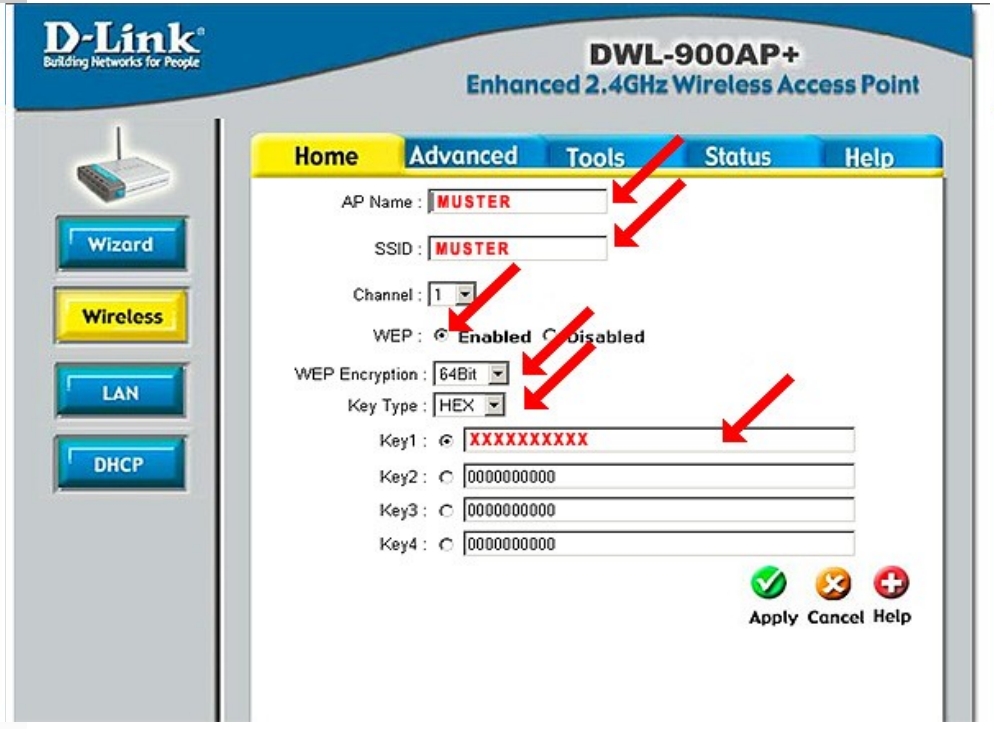
Ne pas Broadcaster le SSID

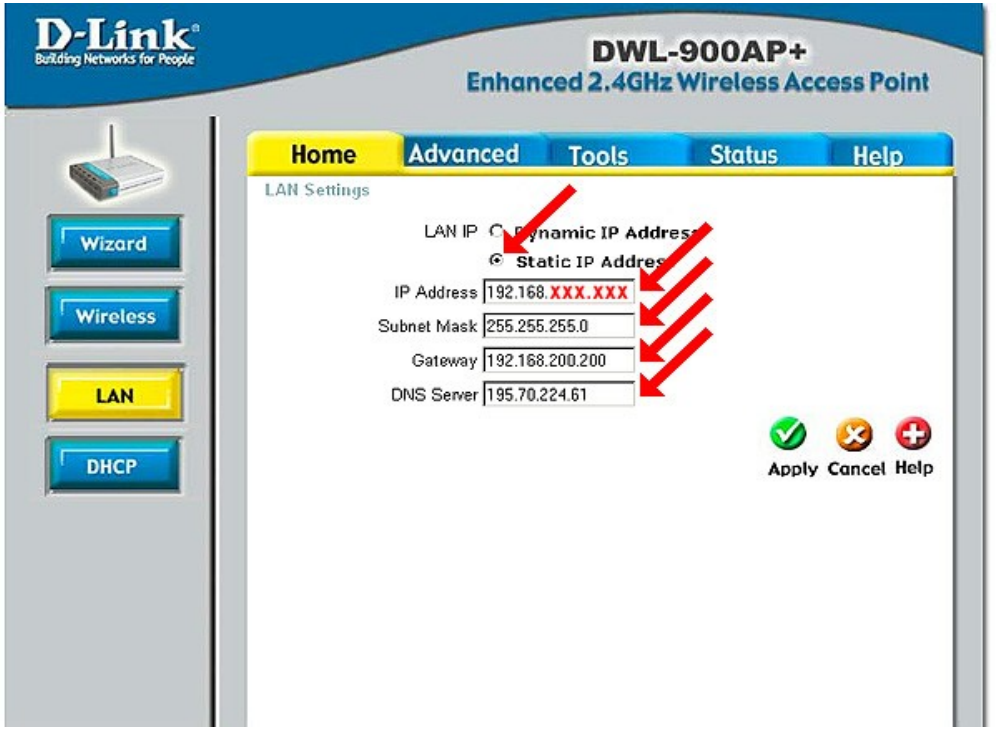
- Le SSID ne sera pas visible par défaut par les nouveaux utilisateurs.
- Les personnes utilisant des outils d'écoute pourront le détecter.
- Si le réseau n'a pas vocation à accueillir de nouveaux utilisateurs régulièrement, à mettre en place.



Modifier les valeurs par défault

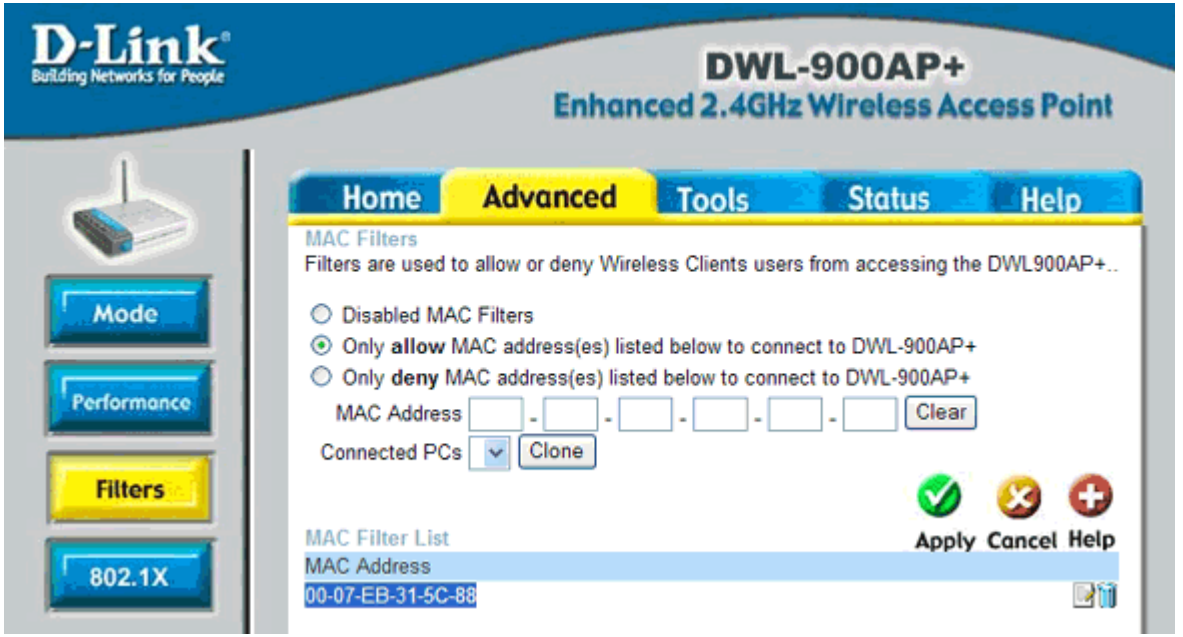
- Modifier le mot de passe d'administration
- Changer le SSID et le nom de l'AP par défault
  - donne des indications sur le modèle
- Changer l'adressage IP par défault





Filtrer les @MAC

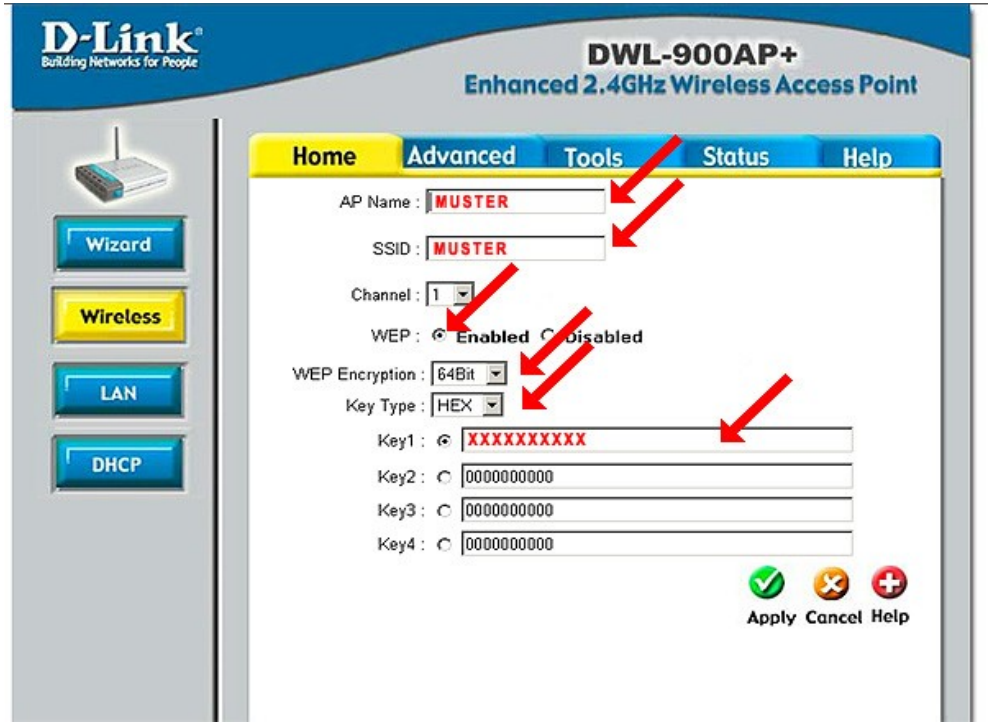
- Possibilité de lister les @Mac des stations autorisées ou interdites
- @MAC = identifiant unique de chaque interface réseau 802 (WiFi, Ethernet) : 01:23:F5:67:29:A1
  - attribuée par le fabriquant et l'IEEE (plaque d'immatriculation)
  - mais peut être falsifiée



Chiffrer les données : WEP

- WEP = Wired Equivalent Privacy
- Protocole de chiffrement utilisant une clef secrète statique de 64 ou 128 bits

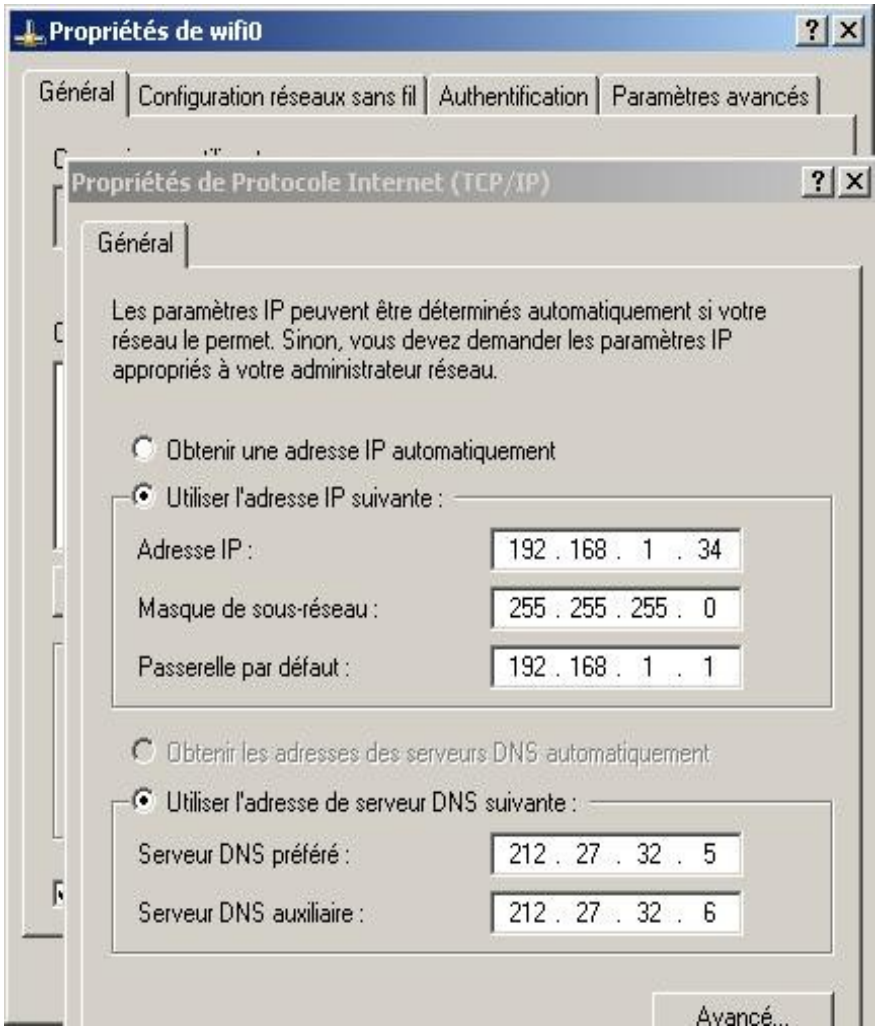
- Fiabilité
  - Une clef de 128 bits couvre 3/4 des risques pour un particulier
  - Une attaque de force brute permets de casser une clef de 64 bits
  - Une capture d'un million de paquets permets de casser une clef de 64 ou 128 bits (faille algorithmique)
- Nécessite d'être configurée sur l'AP et toutes les stations



Désactiver le serveur DHCP

- Une configuration réseau n'étant pas attribuée automatiquement rend la prospective plus dissuasive
- Néanmoins le gain de sécurité est faible et fait perdre la souplesse d'administration du DHCP

-> solution réservée aux besoins spécifiques

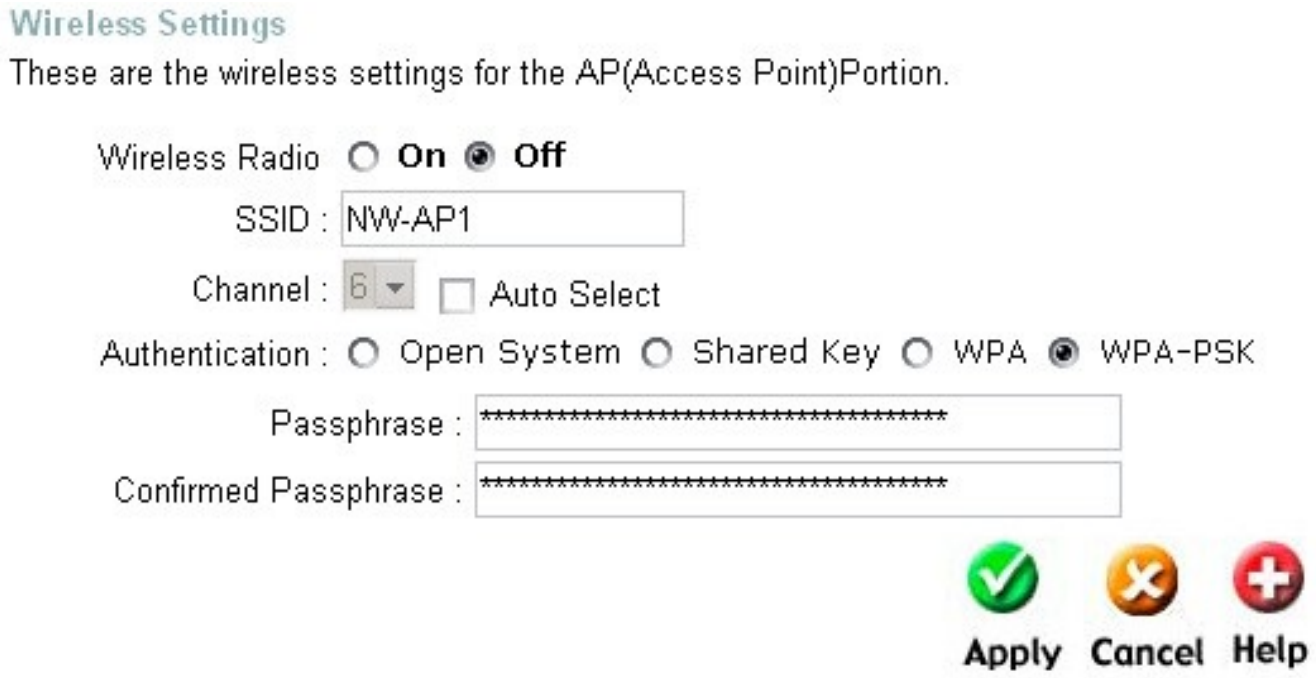


WPA : authentification + chiffrement

- Wi-Fi Protected Access (WPA et WPA2)
  - comble les lacunes du WEP
  - récent donc pas implémenté sur tous les matériels (voir maj firmware)
  - respecte la norme 802.11i (2004)
- Chiffrement : TKIP
  - Temporal Key Integrity Protocol
  - Vecteurs d'initialisation tournants et vérification d'intégrité
- Authentification
  - personnel : WPA - PSK
  - entreprise : 802.1/x - EAP avec serveur Radius

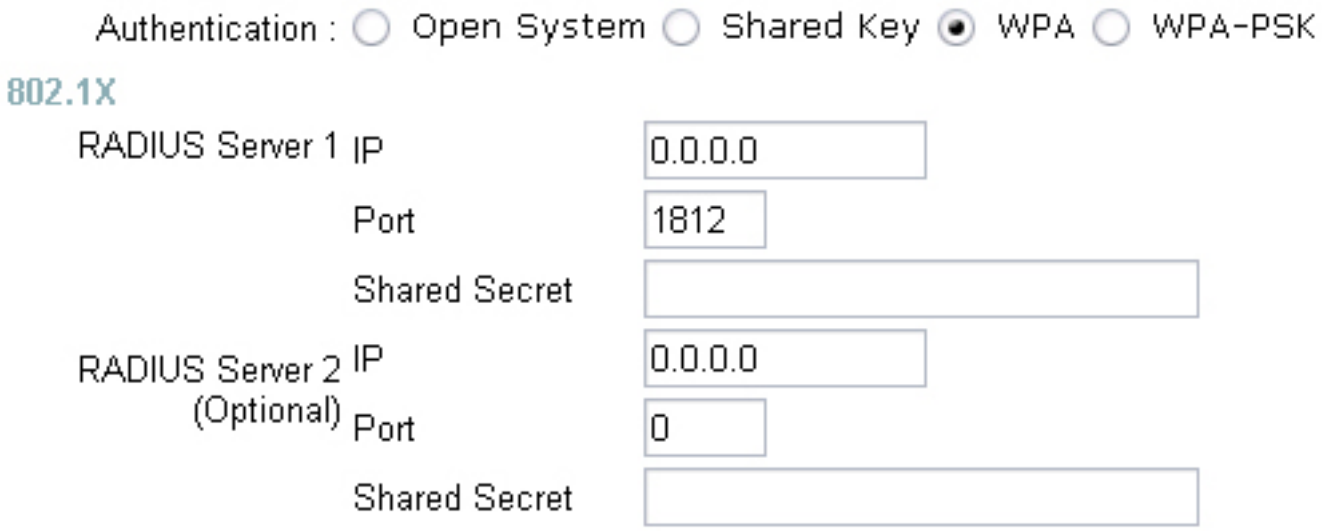
WPA – PSK (personnel)

- Nécessite une Pass-Phrase devant être saisie sur l'AP et le client
- Cette clef sert à la fois à l'authentification (Pre-Shared-Key) et au chiffrement (TKIP)



WPA – EAP / 802.1x (entreprise)

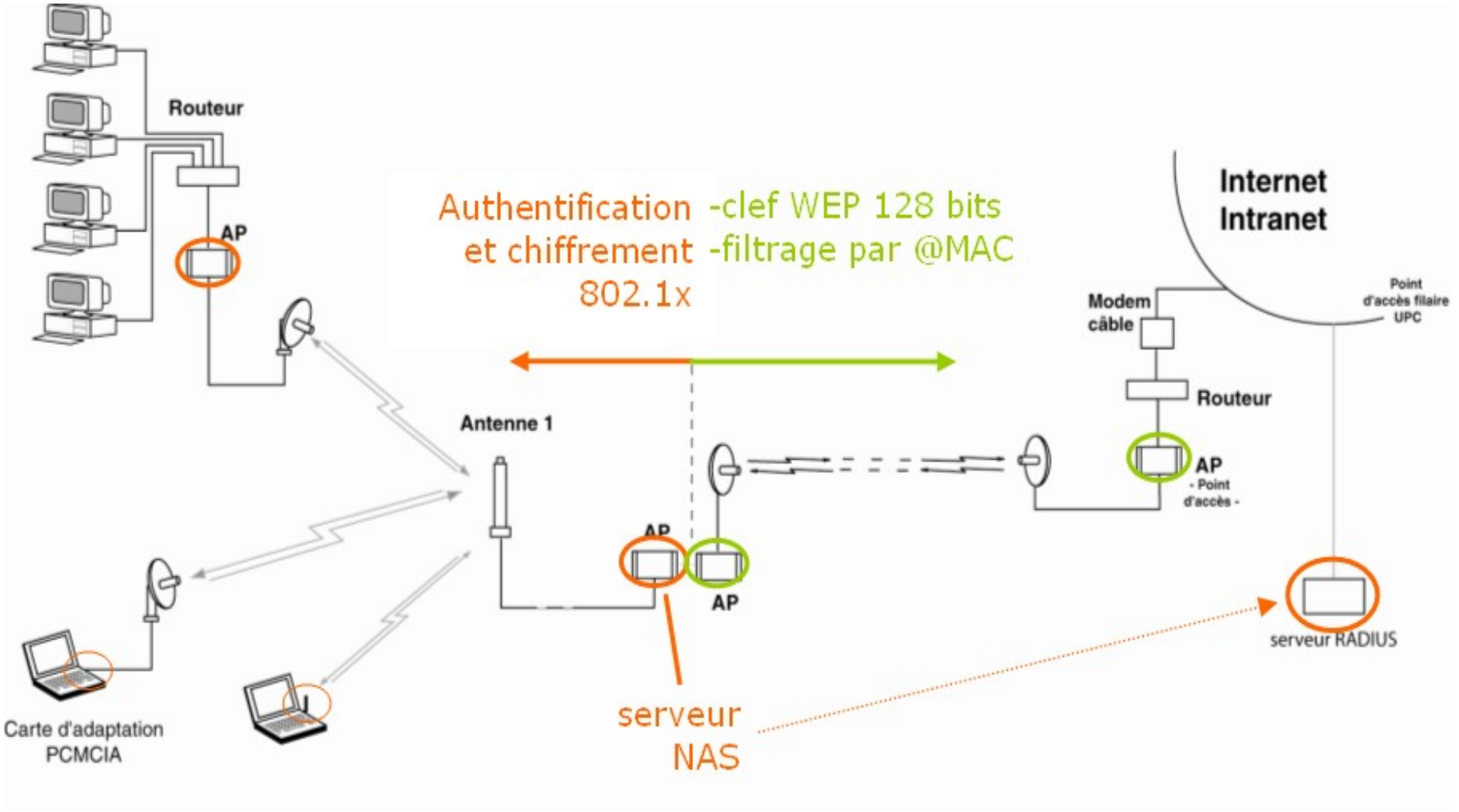
- Utilise un serveur Radius centralisé pour gérer l'authentification : robuste mais compliqué
- Cette clef sert à la fois à l'authentification (Pre-Shared-Key) et au chiffrement (TKIP)



WPA (suite et fin)

- Faiblesses
  - L'utilisation de Pass-Phrase trop courtes voire trop communes pouvant être brute-forcées.
  - La possibilité de générer des trames "DISASSOCIATE" et cela relancera ainsi le procéssus d'identification du WPA.
- Pour en savoir plus
  - http://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access
  - http://reseau.erasme.org/rubrique.php3?id_rubrique=15
  - http://www.freeradius.org/

Une exemple de sécurisation complet



Synthèse

Résumé des solutions

		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

Partie 6

Déployer
un réseau sans fil

Méthodologie

- Théorie
- Evaluation des besoins
- Etude de site
- Dimensionnement
- Sécurité
- Documentation
- Fonctionnement, optimisation et maintenance

Analyse des besoins

- Quel est le nombre des utilisateurs et leur perspective d'évolution ?
- Quelle est la densité des utilisateurs et leur espacement ?
- Le profil des utilisateurs (accès restreint ou public)?

- Nature et importance des données qui transiteront ?
- Quelles sont les applications utilisées actuellement, ou plus tard (dans 2 ans)?
- Quels sont les types de trafic (sporadique ou continu) et les volumes de trafic effectifs ?
- Quels sont le besoin de débit minimum des utilisateurs en accès sans fil ?

- Types des stations qui seront connectées, leurs compatibilité ?
- Quel est la topologie et le plan d'adressage du réseau filaire amont ?
- Existe t il des services réseau : DHCP, DNS, Proxy ?
- Des restrictions ? Des filtrages ?

Etude de site

- Objectif
  - Déterminer avec précision des emplacements des APs
  - Paramétrer la radio des APs et (puissance de transmission, couverture, canaux, type d'antennes)
- Procédure
  - Rassembler les plans des locaux. Y-indiquer l'emplacement des prises LAN, secteur, coupe-feu, etc.)
  - Localiser les éventuelles sources d'interférences et évaluer leur importance (cages d'ascenseur, éléments en mouvement, rayonements...)
  - Faire des tests avec un AP et un portable pour évaluer la puissance et la qualité du signal
  - Fixer l'orientation des antennes et la puissance des APs
  - Envisager des installations électriques autonomes

Dimensionnement

- Evaluer la capacité des Aps

	Exemple de type d'application	Nombre utilisateurs
802.11b	– Consultation messagerie – Navigation Internet	50
	– Téléchargement de fichier peu volumineux	25
	– Téléchargement de fichier volumineux – VoIP, vidéoconférence…	10
802.11a **802.11g**	– Téléchargement de fichier volumineux – VoIP, visé	50

- Effectuer le plan d'adressage réseau du site

Stratégie de sécurité

- Dimensionner des solutions de sécurité adaptées
  - Wi-Fi
    - Réglage de la puissance
    - Ne pas broadcaster le SSID
    - Limitation des @Mac
    - WPA à défaut Clef WEP
  - IP
    - @IP fixes
    - Tunnel VPN
  - En informer les utilisateurs
- Faire des audits sécurité régulièrement
  - notamment : log des utilisateurs et des @Mac au niveau AP(-> à rediriger éventuellement dans un fichier de log)
  - ping de toutes les adresses IP du Subnet (attribuées ou statiques)
  - évolution des débits

Documentation

- Documenter l'historique de l'installation
  - Guide d'implémentation et de mise en marche du réseau
  - Historique des interventions
- Produire un plan WiFi
  - APs et identification
  - Zone de couverture, canal, antennes, débits
  - Réglage de sécurité
- Produire un plan du réseau
  - Schéma IP des connexions et des équipements
  - Plan d'adressage
  - Distribution des adresses : DHCP, DNS, Proxy, ect
  - Anticiper le manque d'adresses

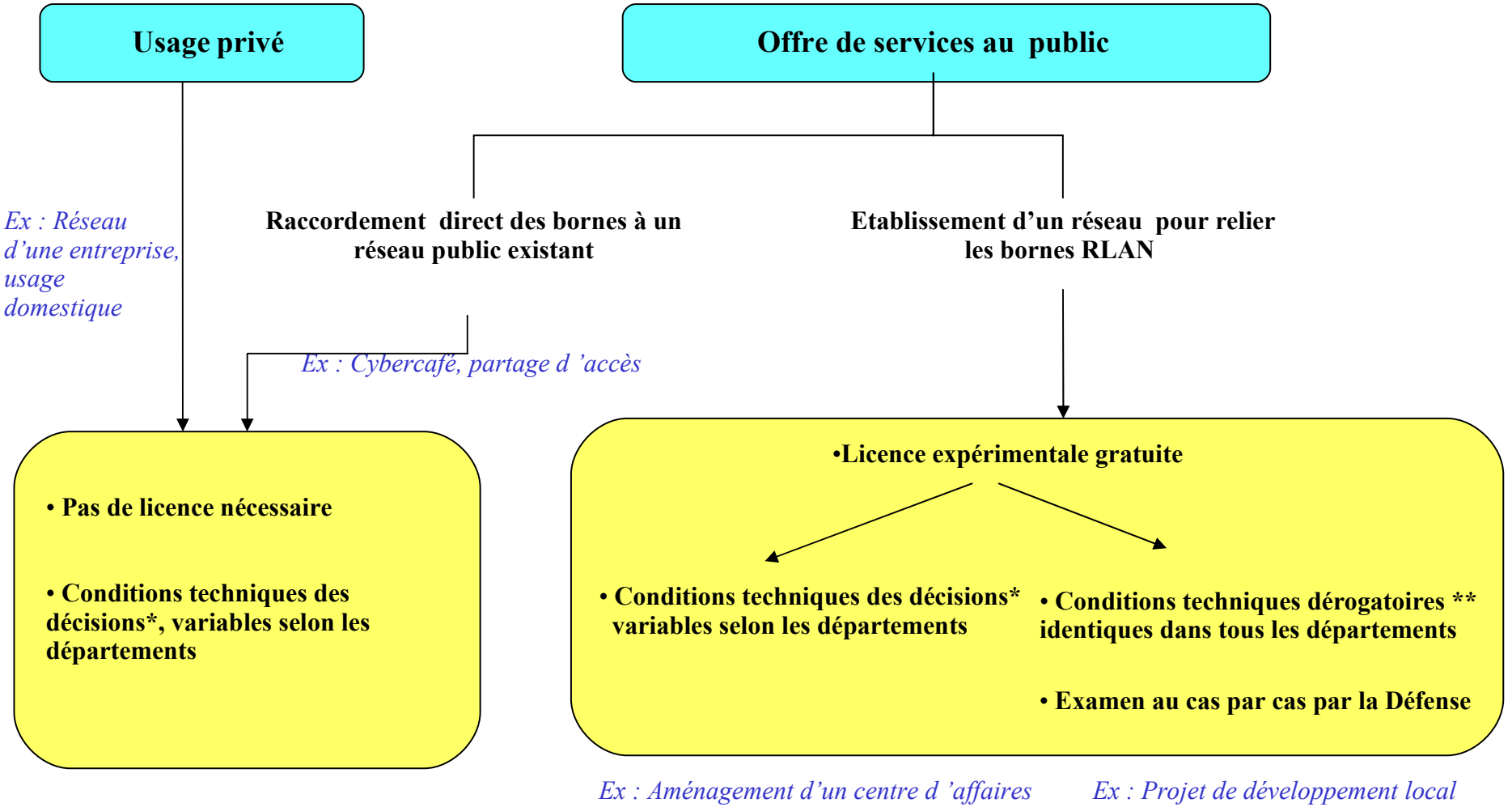
Partie 7

Compléments

Aspects juridiques

Aspects juridiques (radio)

Le cadre réglementaire pour les RLAN en 2,4 GHz



** détaillées dans le communiqué de presse du 7 novembre 2002*
*** puissance rayonnée (PIRE) de 100 mW en extérieur et en intérieur*

Source : http://www.art-telecom.fr - 19/11/2002

Aspects juridiques (contenu)

- La loi contre le terrorisme (LCT) du 29 octobre 2005 impose à tous ceux qui proposent un accès à Internet au public (particuliers, cybercafés ou des fournisseurs d'accès à Internet) de conserver les données de connexion pendant 3 ans et à les communiquer si nécessaire aux services de police.
- En pratique, le log des adresses MAC connectées suffit.
- Certains points d'accès embarquent des solutions d'enregistrement des logs.
- En cas d'utilisation de votre réseau à votre insu vous êtes responsable de ce qui est fait depuis votre connexion

Aspects sanitaires

Des éléments concrets

- Les normes européennes d'utilisation des ondes WiFi spécifient une puissance rayonnée < 100 mW.
- Le WiFi rayonne moins que la plupart des équipements quotidiens
    - Téléphone GSM : < 2W ;
    - Téléphone DTEC : < 500 mW ;
    - Antennes GSM : 20 à 50 W ;
    - four à micro-ondes : 1 kW ;
    - émetteur de la tour Eiffel : 6 MW
- La puissance d'un champ électro-magnétique décroît avec le carré de la distance.
- Un élément radio WiFi à 1 mètre revient à poser un téléphone portable en marche à 3 mètres.

... mais des questions subsistent

- L’utilisation de radio-fréquences suscite des interrogations.
- Les nombreuses études en cours, surtout au sujet de l’utilisation des téléphones mobiles, sont globalement rassurantes.
- Néanmoins l'accumulation des ondes et l'inconnu des effets à long terme incitent au principe de précaution.
- Depuis 2002, presque tous les constructeurs se sont ralliés à des utilisations de l'ordre de 30 mW en sortie d'antenne WiFi.
- Voir : http://reseau.erasme.org/article.php3?id_article=29

TPs à la demande

Liste des TPs

- Configurer un client en mode infrastructure
- Dimensionner un WLAN : mesure de débit / qualité / portée / QOS
- Configurer un point d'accès : configuration WiFi basique
- Configurer un point d'accès : routage / DHCP / DNS
- Configurer un point d'accès : sécurité
- Configurer un réseau ad-Hoc
- Configurer un pont WiFi : antennes / tests / qualité
- Ecouter un réseau sans fil / craquer une clef WEP
- Manipuler des objets communicants : Nabaztag

Remerciements

Sources et références

- Merci aux auteurs de ces contributions :
  - http://fr.wikipedia.org/wiki/Wi-Fi
  - http://www.canardwifi.com/
  - http://reseau.erasme.org/rubrique.php3?id_rubrique=38
  - http://www.commentcamarche.net/wifi/ (Jean François Pilou)
  - http://www.swisswireless.org/wlan_calc_fr.html
  - http://www.topachat.com/comprendre/wifi.php
  - http://www.ebg.net/evenements/pdf/EBG_LBwifi.pdf
  - http://www.journaldunet.com/wifi/localisation/36661/rhone.shtml
- Un remerciement particulier à Michel Blanc pour son excellent cours sur Linux
  - http://reseau.erasme.org/article.php3?id_article=1160

Crédits

- 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 !