UNITE D'ENSEIGNEMENT (UE)

RESEAUX SANS FIL & IOT

RESEAU WIFI : Bases théoriques et pratiques

Volume horaire = 15 heures

Présenté par Dr Zamblé

PLAN DU COURS

- Chapitre 1 : Les réseaux sans Fil
- Chapitre 2 : La norme WiFi (802.11)
- Chapitre 3 : Configurer un réseau WiFi : TCPIP
- Chapitre 4 : Matériel - Portée, débit et puissance
- Chapitre 5 : Sécurité
- Chapitre 6 : Déploiement d'un réseau
- Chapitre 7 : Travaux pratiques

OBJECTIFS DU COURS

🎯 Objectifs du cours :

À la fin de ce cours, l'étudiant (e) doit être capable de :

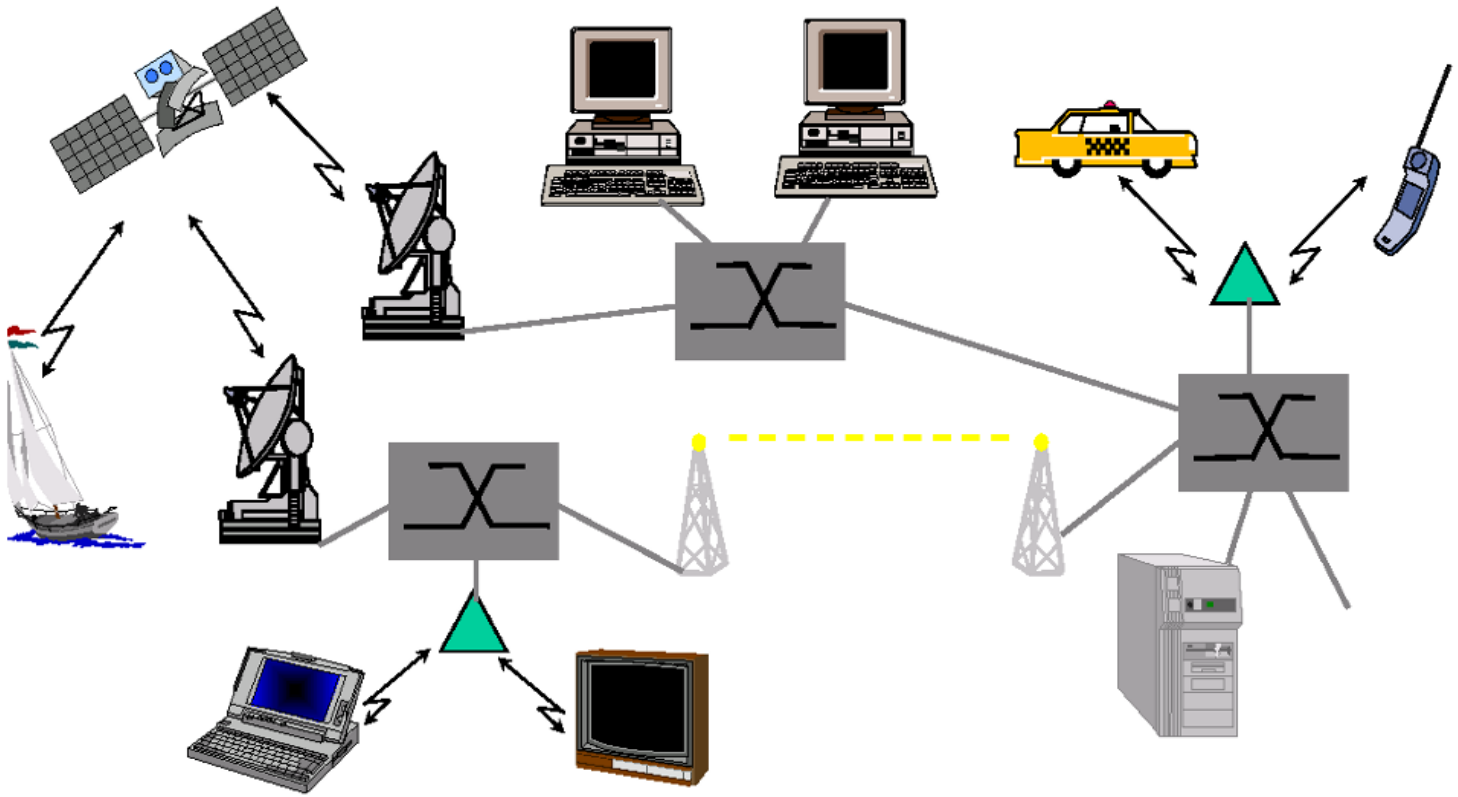
1. Maîtriser les aspects théoriques de la norme WiFi et les notions de propagation radio,
2. Être capable de configurer un réseau sans fil local simple : aspects réseau (IP) et radio (WiFi),
3. Être capable d'analyser une problématique de desserte sans fil et de dimensionner une solution,
4. Maîtriser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

PLAN DU COURS

Chapitre 1 : Les réseaux sans Fil

Définition

- Le sans fil omniprésent ?



Définitions :

- 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 .

Equipements identiques ou de nature différente :
-PC, laptop, serveur
-PDA, téléphone portable, PS2
-Objet communiquant...

Chapitre 1 : Les réseaux sans Fil

Définition

1. Phase de dialogue et de négociation
-Protocole, débit, puissance...
-Authentification, cryptage...
-> si connexion possible :
2. Phase d'échange de données

-Sans Fil = Wireless
-Signal radioélectrique en propagation libre dans l'air
-Fréquence et type de modulation de données variables : IR, WiFi...

-Connexion directe : IR, Bluetooth ...
ou
-Utilisation d'une borne de connexion intermédiaire : GSM, WiFi ...

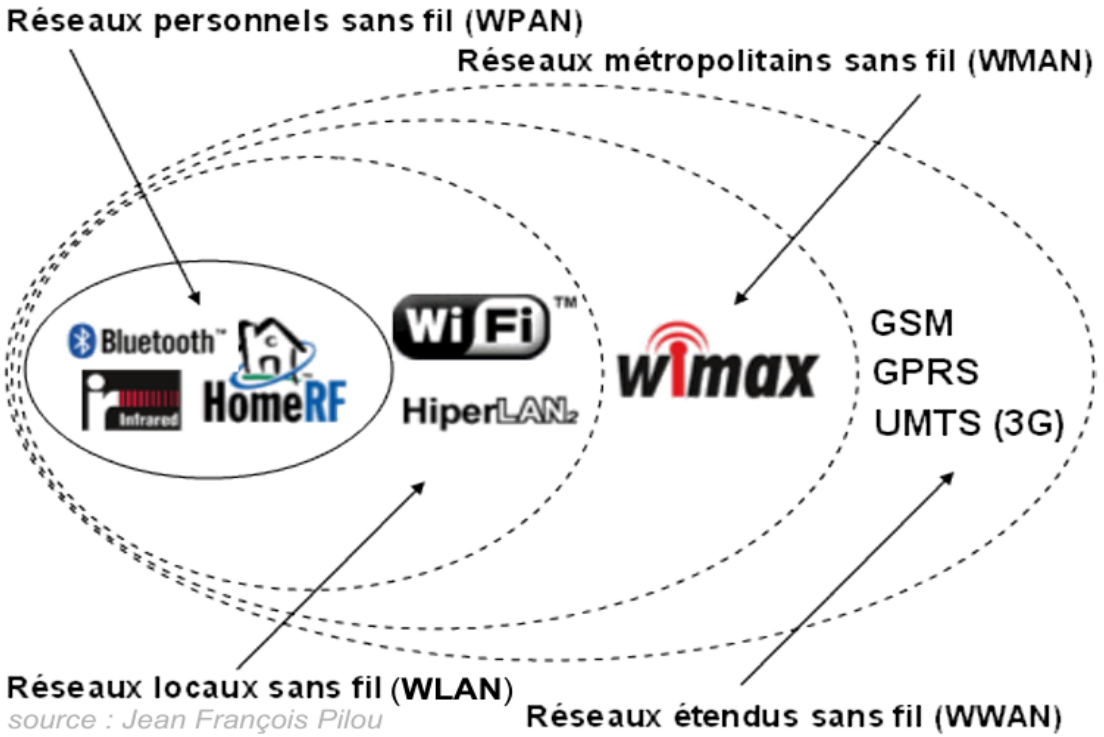
Distinction récente pour caractériser une liaison selon :
-la vitesse de déplacement
-la zone de couverture

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

Chapitre 1 : Les réseaux sans Fil

Critères de classification

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



source : Jean François Pilou

Chapitre 1 : Les réseaux sans Fil

Intérêt du sans fil et contraintes

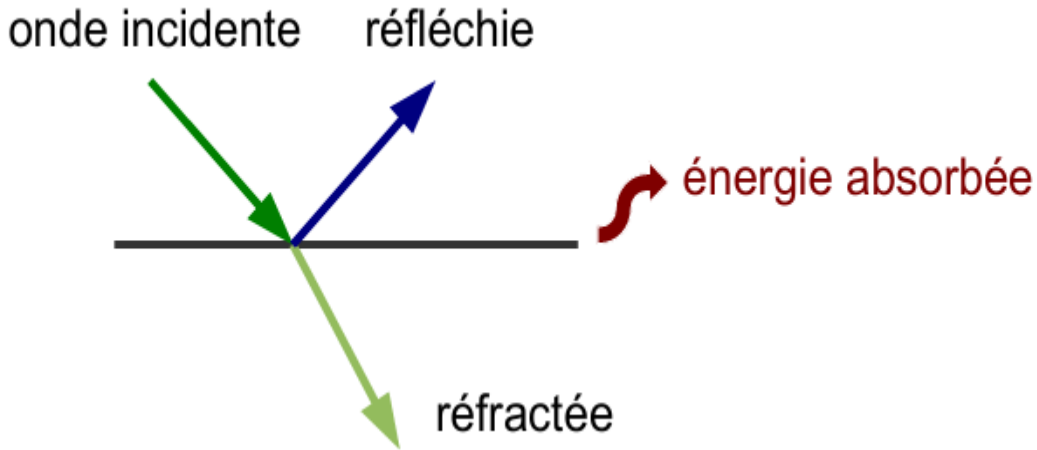
- Facilité de déploiement
- Interopérabilité avec les réseaux filaires
- Débits adaptés à un usage professionnel
- Grande souplesse et faiblement structurant (chantier, exposition, locaux temporaires)
- Non destructif (monuments historiques, sites classés)
- Grande mobilité
- Coût

Contraintes :

- Limites des ondes radio :
  - sensibles aux interférences (microondes, 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

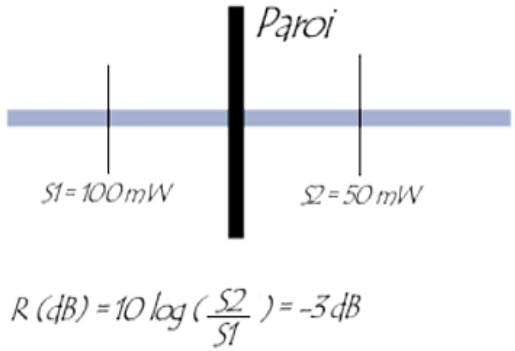
- Les ondes radio se propagent en ligne droite dans plusieurs directions depuis leur source d'émission
- Leur vitesse dans le vide est de 3.108 m/s
- Lorsqu'elle rencontre un obstacle, l'onde est divisée et son énergie est répartie :



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 amplifiée.
- L'atténuation (ou le gain) : L'atténuation (ou le gain) est le rapport entre la puissance du signal avant et après modification.

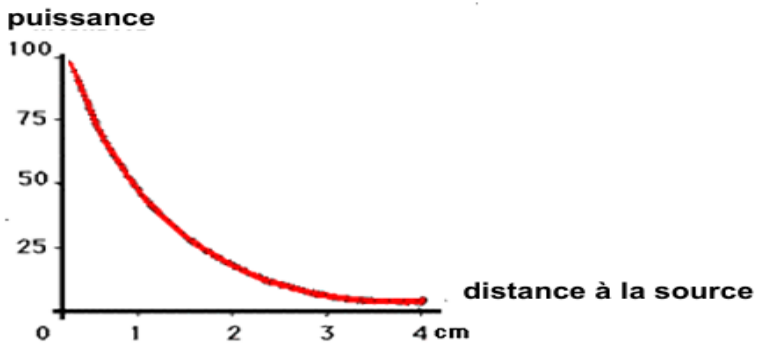
Atténuation (dB) = (10) * log (S2/S1)



Notions de propagation radio

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 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 absorbant 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 WiFi (feuilles par exemple).

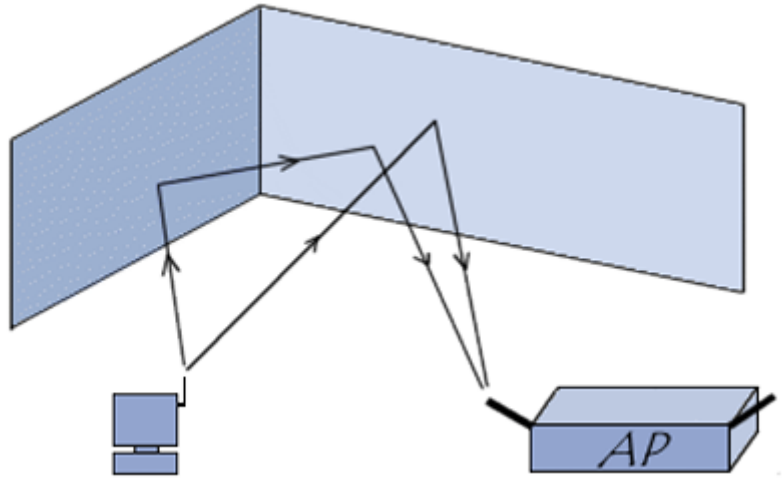
Notions de propagation radio

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 données peut être important mais plus la couverture est faible.
- Puissance élevée : couverture plus grande mais durée de vie des batteries plus faibles.

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 permet de contrôler et de séparer les signaux.



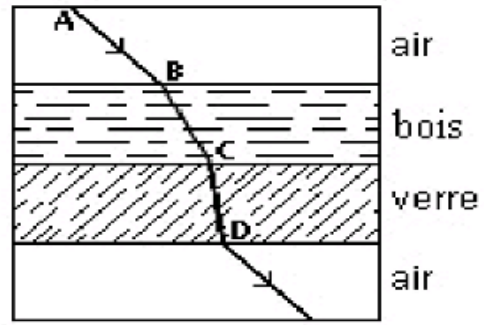
Notions de propagation radio

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



Fin du chapitre 1

PLAN DU COURS

Chapitre 2 : La norme WiFi (802.11)

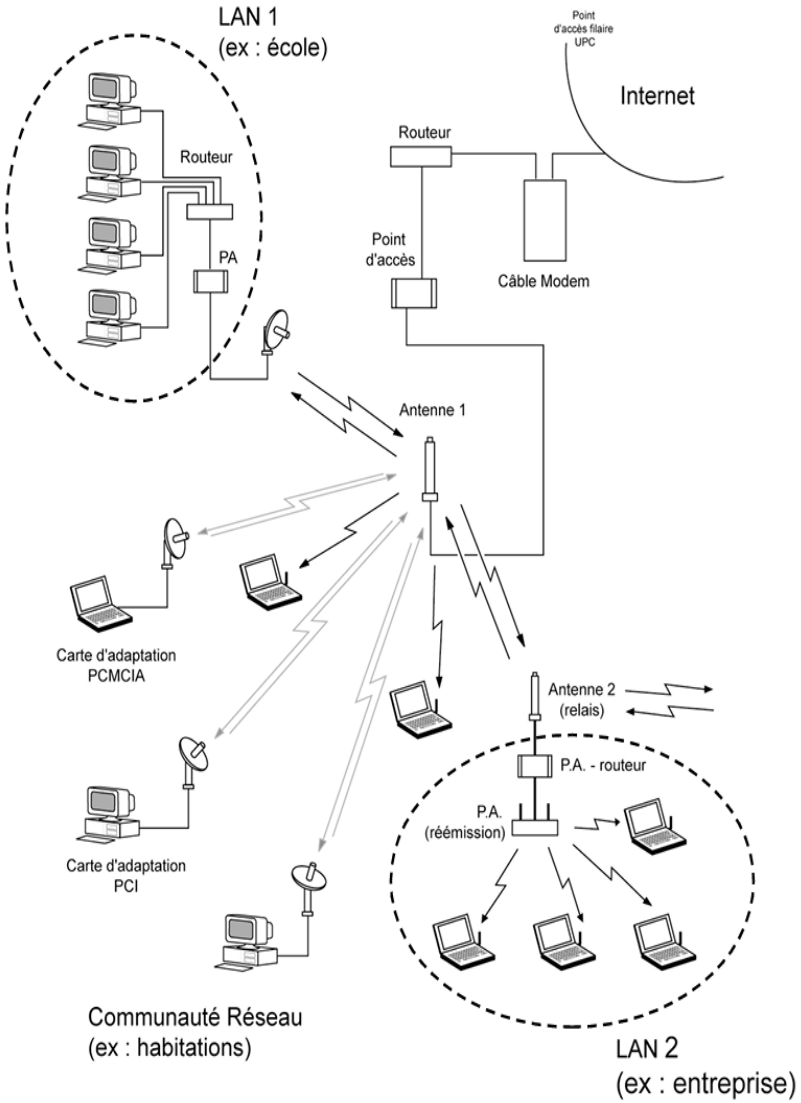
Présentation du WiFi

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

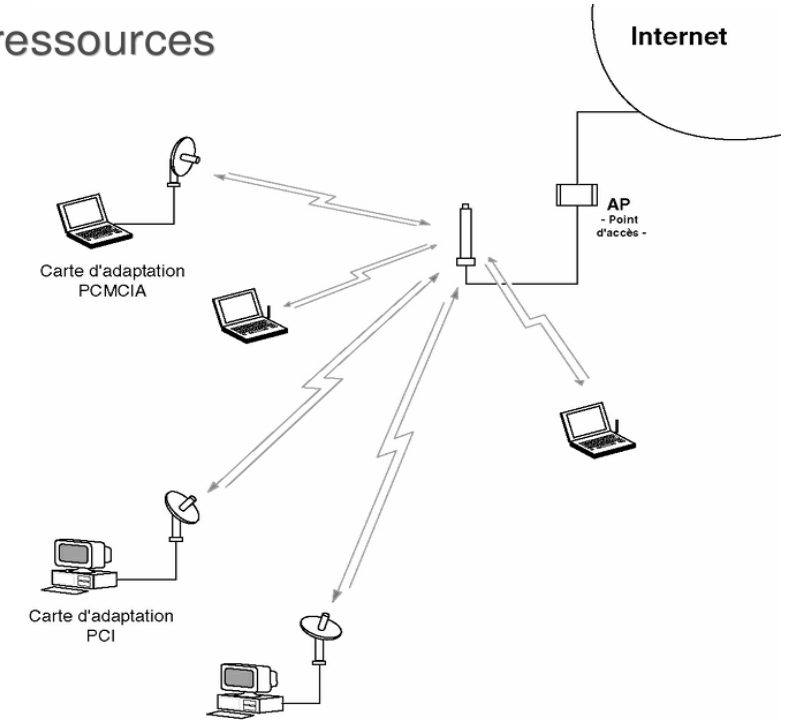


Chapitre 2 : La norme WiFi (802.11)

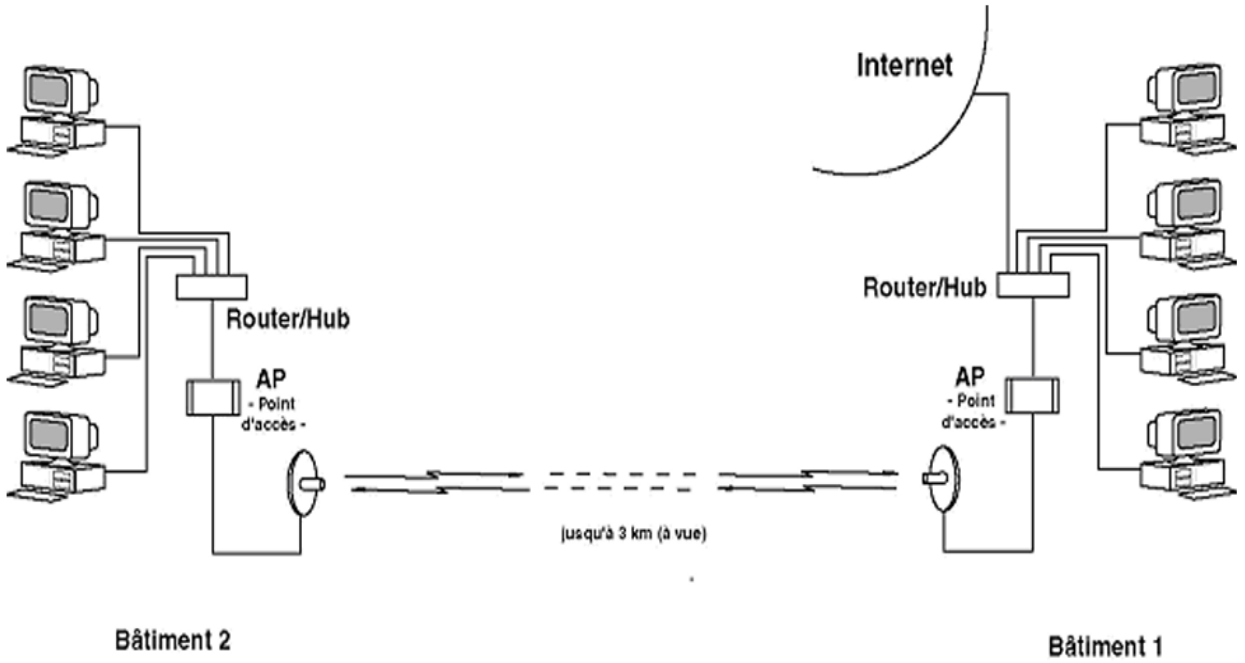
Présentation du WiFi

Usages

- Partager des ressources



- Étendre un réseau existant



Chapitre 2 : La norme WiFi (802.11)

Présentation du WiFi

Usages du Wi-Fi

- Étendre un réseau existant
  - Pont WiFi
- Partager une ressource
  - Switch / Accès Internet, Imprimante, serveur
- Réaliser un portail d@ccès 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.

Chapitre 2 : La norme WiFi (802.11)

Présentation du WiFi

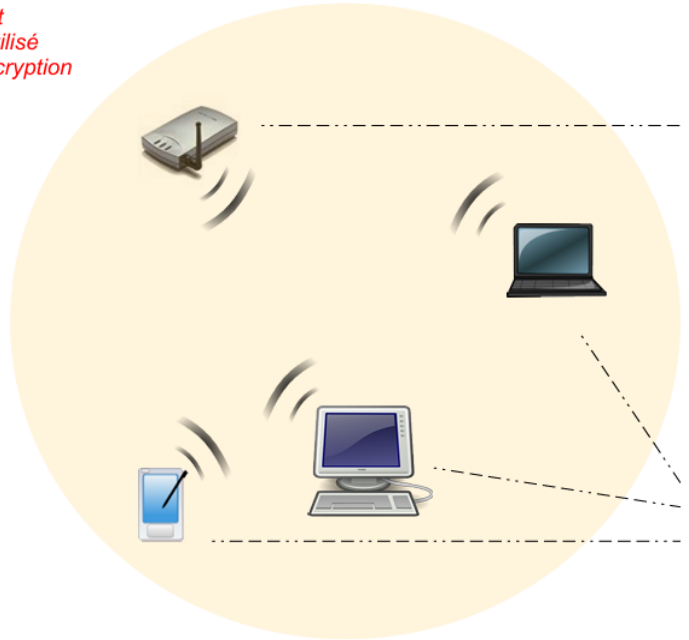
Le matériel employé

- Points d'accès (eq. switch)
- Cartes clientes (éq. carte réseau)
- Antennes et connectiques
- Matériel Ethernet

Une architecture cellulaire

Un équipement Wi-Fi
= 2 interfaces

Cellule
(zone de couverture)
-ID
- Débit
- Canal utilisé
- Mode d'encryption



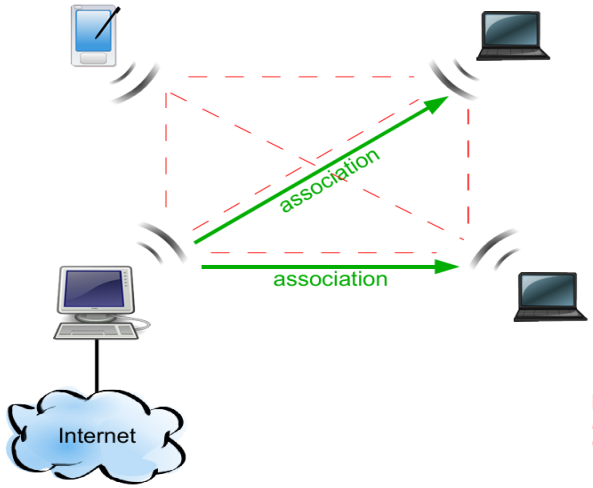
Point d'accès
module WiFi
&
module Ethernet

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

Chapitre 2 : La norme WiFi (802.11)

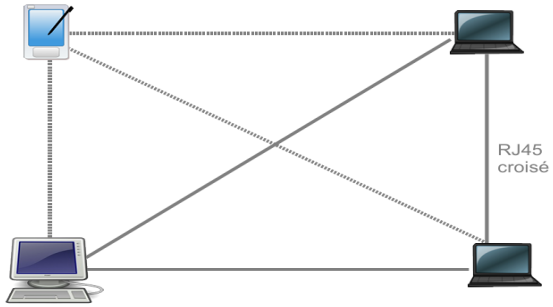
Topologies

Topologie ad-hoc



IBSS
Ensemble de services de base indépendant

... équivalent à un câble croisé en Ethernet

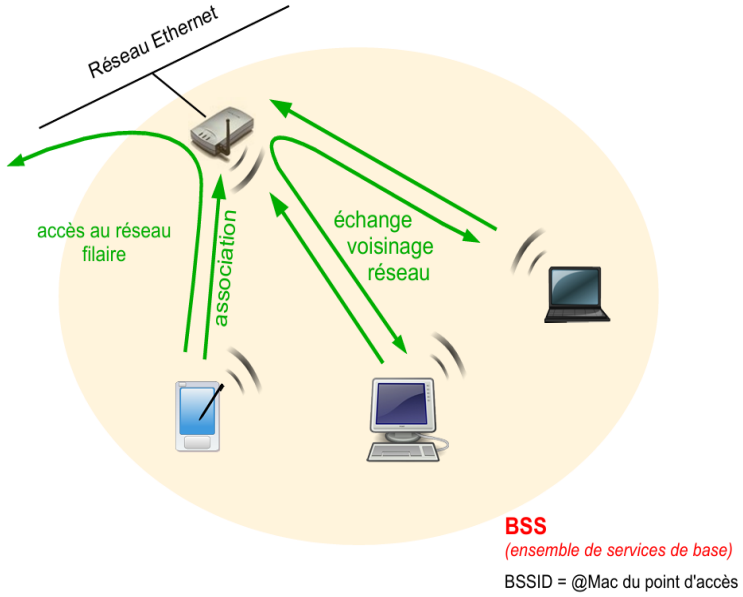


- Des stations équipées d@adaptateurs WiFi en mode ad-hoc forment un réseau Mesh (ad-hoc)
  - Chaque adaptateur joue successivement le rôle d@AP et de client. Les machines communiquent ensemble en point à point (peer to peer).
  - Ce système n@ntègre pas nativement de protocole de routage. Une norme 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@ucun AP n@st disponible

Chapitre 2 : La norme WiFi (802.11)

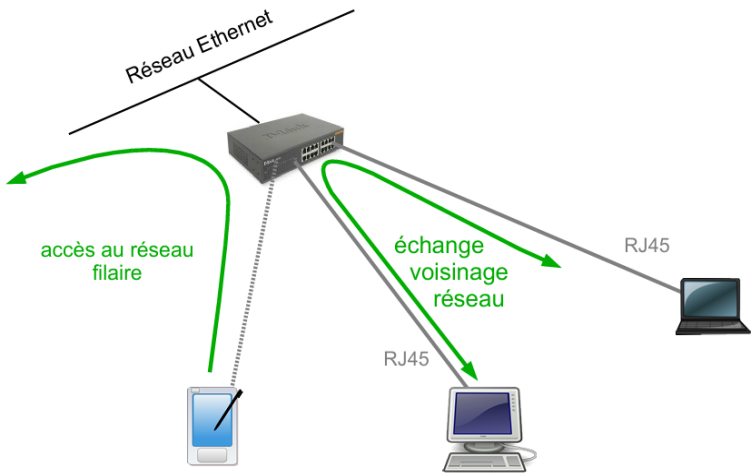
Topologies

Topologie Infrastructure



BSS
(ensemble de services de base)
BSSID = @Mac du point d'accès

... équivalent à un hub en Ethernet

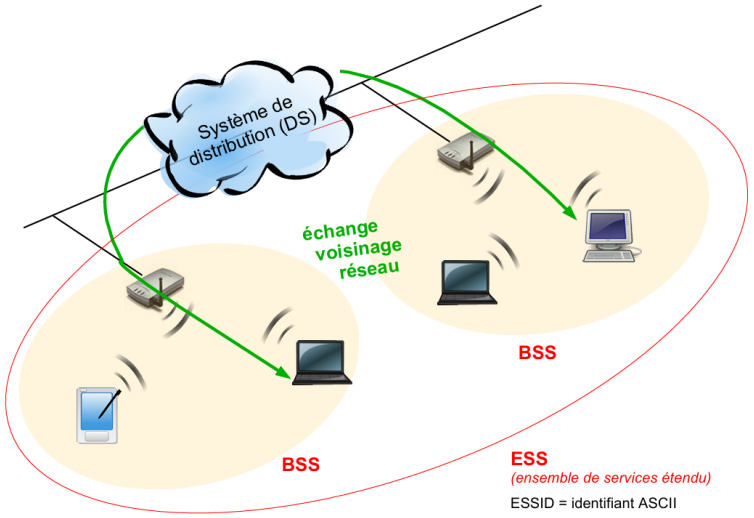


- Chaque station se connecte à un point d@accès qui lui offre un ensemble de services de base (BSS)
  - association et ev. authentification
  - connexion à la ressource Ethernet (bridge IP)
  - communication avec les autres stations (IP)
  - BSS caractérisé par son **BSSID** = @Mac du point d@accès
- A un point d@accès peuvent être associées jusqu@ 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)

Chapitre 2 : La norme WiFi (802.11)

Topologies

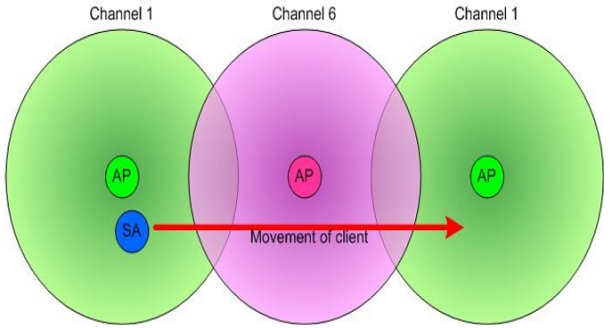
Topologie infrastructure étendue



- 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



Chapitre 2 : La norme WiFi (802.11)

Association et transfert de données

1. Mode Infrastructure

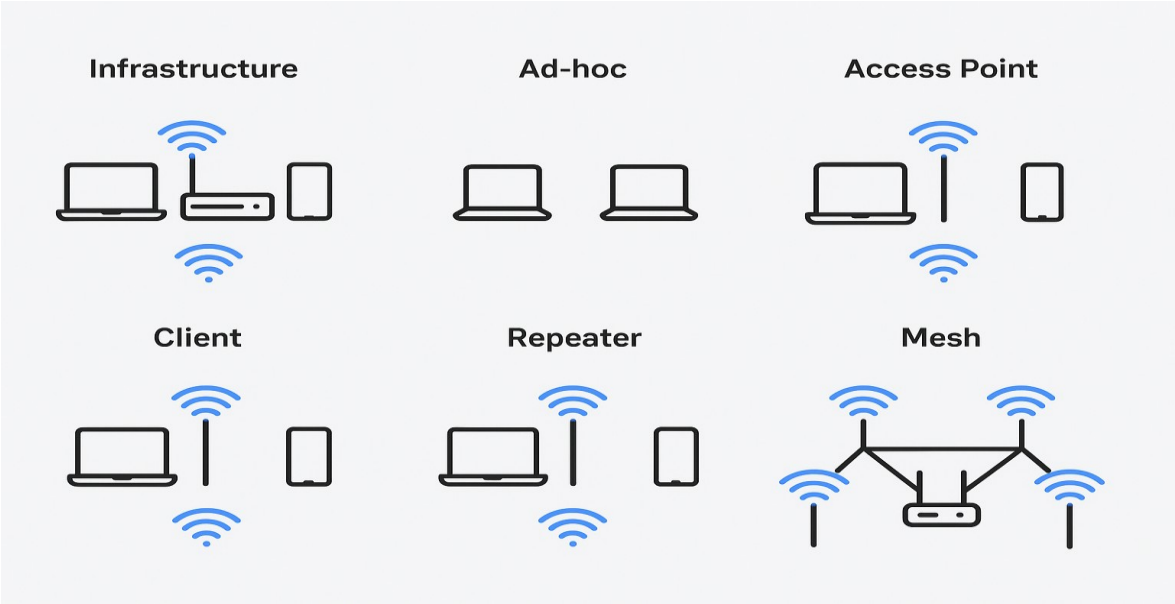
- Description : Le périphérique Wi-Fi (station) s'associe à un point d'accès (AP) central qui gère les communications.
- Rôle :
  - L'AP sert de relais entre les périphériques et le réseau filaire.
  - Le trafic passe toujours par le point d'accès.
- Exemple : connexion d'un PC portable à une box Internet.
- Avantages : gestion centralisée, meilleure sécurité, roaming possible entre plusieurs AP.

2. Mode Ad-hoc (peer-to-peer)

- Description : Les périphériques Wi-Fi communiquent directement entre eux sans passer par un point d'accès.
- Rôle :
  - Création rapide d'un petit réseau temporaire.
  - Idéal pour le partage de fichiers ou de jeux en réseau local sans infrastructure.
- Exemple : deux ordinateurs connectés directement pour transférer des fichiers.
- Limite : portée et sécurité plus réduites, pas d'accès direct à Internet (sauf si un périphérique partage sa connexion).

3. Mode Point d'accès (AP)

- Description : Le module Wi-Fi fonctionne lui-même comme un point d'accès.
- Rôle :
  - Il diffuse un SSID et accepte des associations de stations.
  - Fournit la connexion vers un réseau filaire ou l'Internet.
- Exemple : smartphone en mode "partage de connexion Wi-Fi" (tethering).



Chapitre 2 : La norme WiFi (802.11)

Association et transfert de données

4. Mode Client (Station mode / STA)

- Description : Le module se comporte comme un client Wi-Fi et se connecte à un point d'accès existant.
- Rôle : Permet à un appareil qui n'a pas de carte réseau filaire (ex. imprimante) d'accéder au réseau via Wi-Fi.

5. Mode Repeater / WDS (Wireless Distribution System)

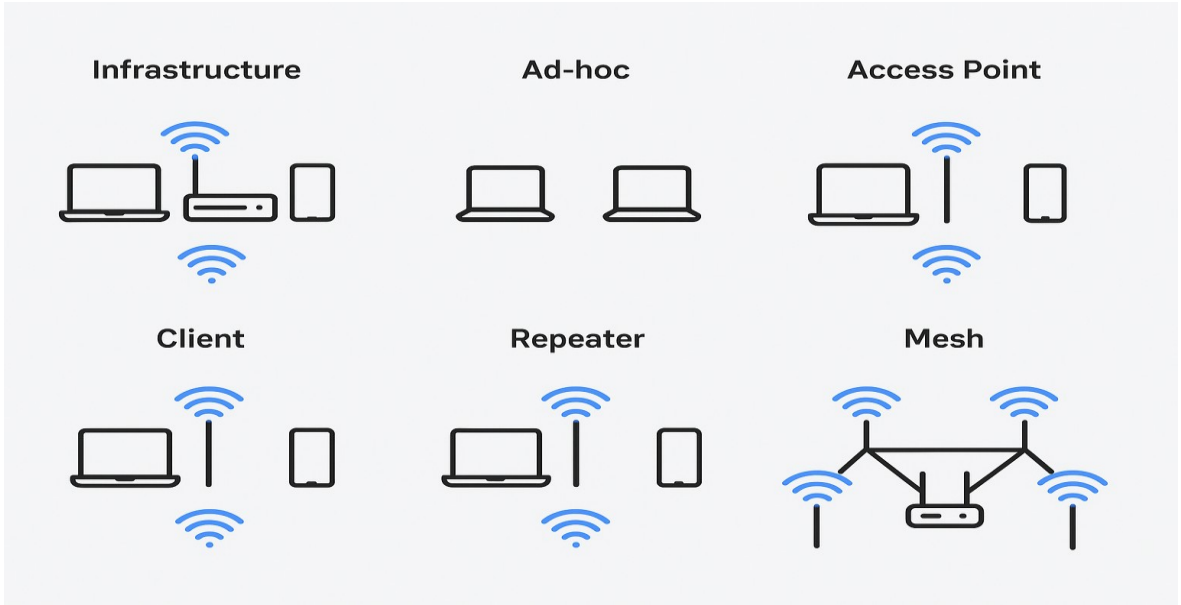
- Description : Le module Wi-Fi reçoit un signal d'un point d'accès et le retransmet pour étendre la portée.
- Rôle : Sert de relais pour améliorer la couverture sans fil.

6. Mode Mesh

- Description : Les modules Wi-Fi créent un réseau maillé où chaque nœud peut transmettre les données d'un autre.
- Avantage : couverture étendue et redondance de chemin en cas de panne d'un nœud.

📌 **En résumé :**

- Infrastructure = client ↔ point d'accès ↔ réseau.
- Ad-hoc = client ↔ client.
- AP = le module devient un point d'accès.
- Client = le module rejoint un point d'accès.
- Repeater/WDS = relais Wi-Fi.
- Mesh = réseau maillé intelligent.



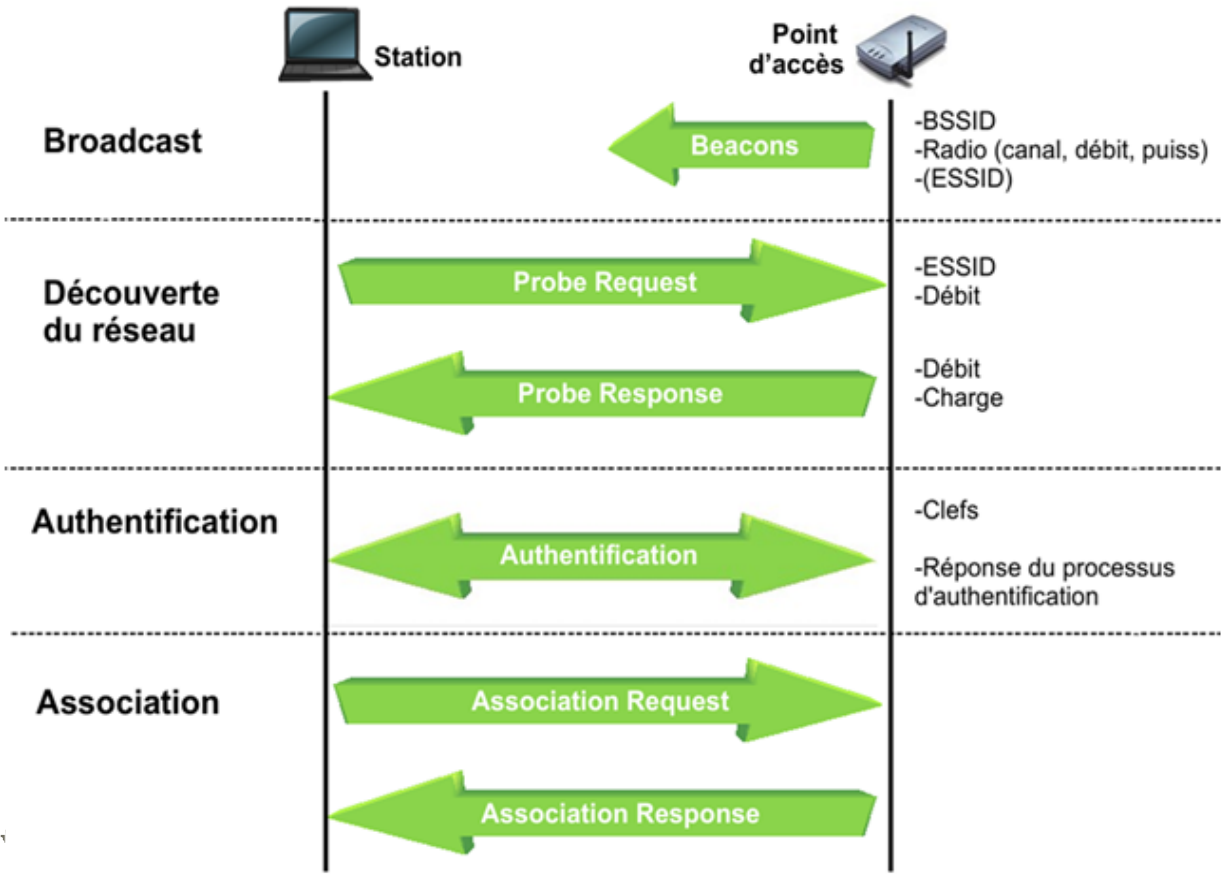
Association et transfert de données

Mécanisme d'association

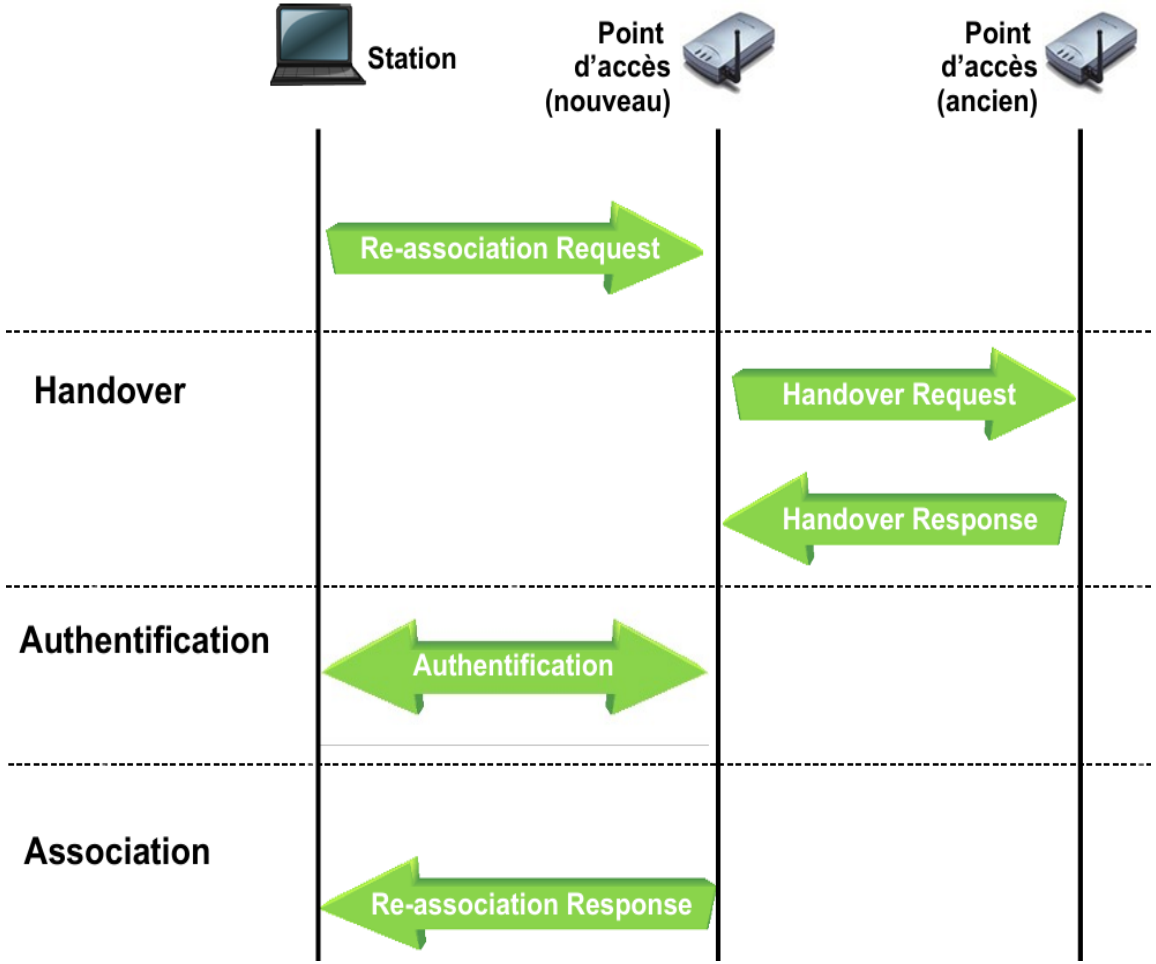
- Le point d'accès
  - diffuse régulièrement (0,1s) une **trame balise** (*beacon*) avec
    - son **BSSID** (ex : 00:16:41:9B:DA:93)
    - ses **caractéristiques radio** (ex : canal 2 / 54 Mbps / ENC)
    - optionellement son **ESSID** en clair (ex : tsunami)
- L'adaptateur client
  - lorsqu'il détecte son entrée dans une cellule, il diffuse une **requête de sondage** (*probe request*) avec
    - l'**ESSID** 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
- Le point d'accès
  - lorsqu'il reçoit une **requête de sondage** (probe request) vérifie
    - le **ESSID**
    - 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

Association et transfert de données

Mécanisme d'association



Mécanisme de roaming



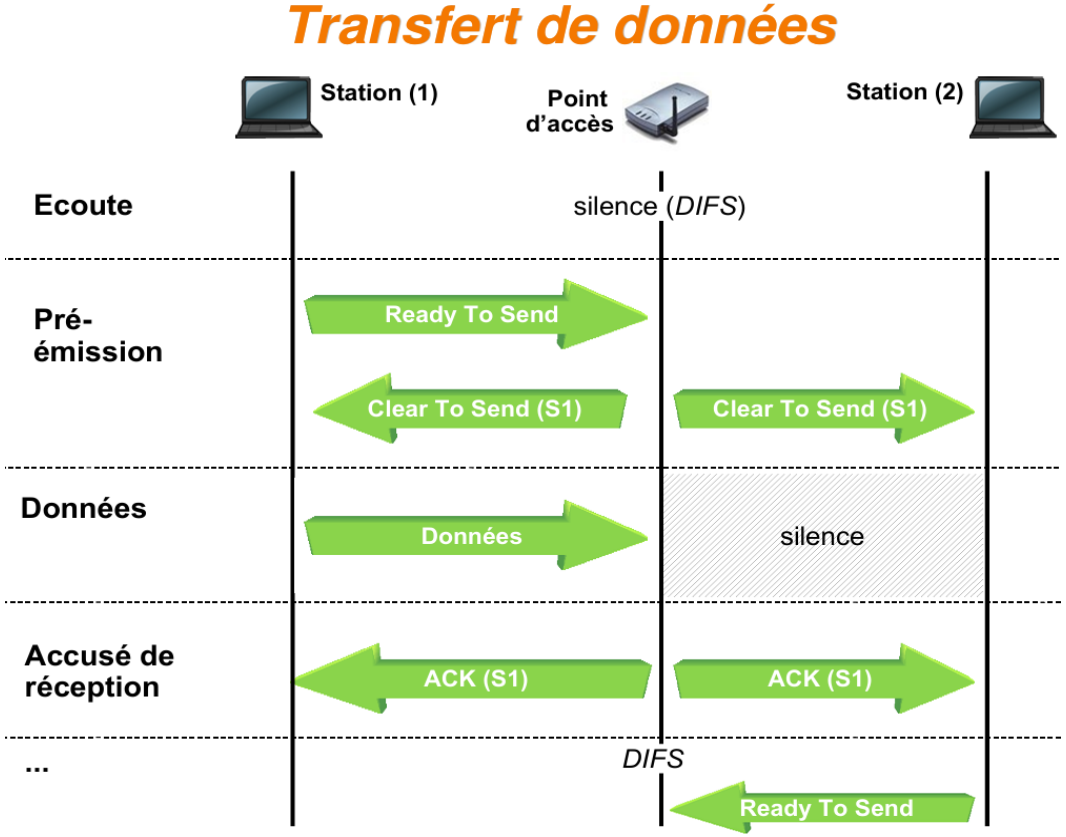
Chapitre 2 : La norme WiFi (802.11)

Association et transfert de données

Etapes principales du transfert de données

1. **Association préalable :**
   - La station s'associe au point d'accès (processus d'authentification + association).
   - Une fois associée, elle peut envoyer/recevoir des trames de données.
2. **Accès au médium (CSMA/CA) :** Wi-Fi utilise le protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) :
   - La station écoute le canal radio.
   - Si le médium est libre, elle transmet.
   - Si occupé, elle attend un délai aléatoire (backoff).
3. **Transmission des trames :**
   - Les données sont découpées en trames MAC (encapsulation des paquets IP/TCP/UDP).
   - Chaque trame contient un en-tête, le contenu (payload) et un contrôle d'erreur (CRC).
4. **Accusés de réception (ACK) :**
   - Après réception correcte d'une trame, le destinataire envoie un ACK.
   - Si l'ACK n'est pas reçu, la trame est retransmise.
5. **Mécanismes de fiabilité et QoS :** Fragmentation, réassemblage, priorisation du trafic (VoIP, vidéo, données).

👉 **En résumé :** Le transfert des données en Wi-Fi fonctionne par écoute du canal (CSMA/CA), envoi de trames, accusés de réception, et réémission si nécessaire pour garantir l'intégrité.



Association et transfert de données

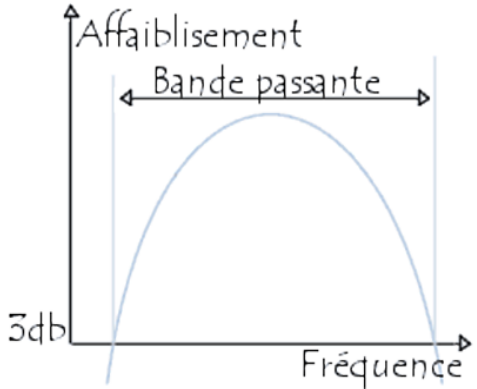
Paramètres radio avancées (BSS – Basic Service Set).

Paramètre	Description	Impact sur les performances	Impact sur la sécurité
Beacon Interval : 0 – 3000, Default 100 (ms)	Temps entre deux annonces de l'AP (ms).	Intervalle ↓ = meilleure réactivité mais plus de trafic de gestion.	Intervalle élevé peut rendre le réseau moins détectable.
DTIM Interval : 1± 255, Default 100 (ms)	Fréquence des notifications aux clients en veille.	Valeur faible = réactivité ↑ mais batterie ↓.	Aucun impact direct.
Preamble Type : Long / Short	Définit la longueur de la séquence de synchronisation placée au début des	**Long Preamble** : augmente la compatibilité avec anciens équipements (802.11b) mais réduit légèrement le débit. - **Short Preamble** : réduit l'overhead, améliore le débit, mais nécessite que tous les clients le supportent.	Aucun impact direct sur la sécurité. Cependant, en environnement mixte, utiliser un type incompatible peut provoquer des désynchronisations → perte de stabilité et donc risque indirect de déni de service.
Fragmentation Threshold : 256 - 2346, Default 2346 (octets)	Taille max avant fragmentation.	Utile en environnement bruité, mais augmente overhead.	Aucun impact direct, mais fragmentation excessive peut ralentir un attaquant par injection.
RTS/CTS Threshold : 0 - 3000, Default 2432 (octets)	Utilisation du protocole anti-collisions.	Améliore la stabilité dans les réseaux encombrés.	Aucun impact direct, mais évite certaines attaques par déni de service liées aux collisions.

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



La bande ISM

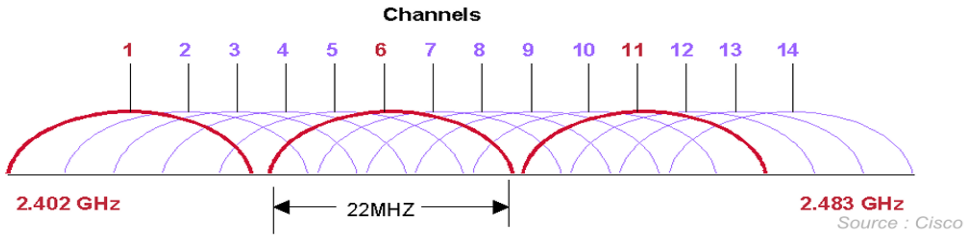
- Dans chaque pays le gouvernement est le régulateur de l'utilisation des bandes de fréquence
  - ETSI en Europe
  - FCC aux Etats-Unis
- En 1985, les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine (ISM)
  - 902 à 928 Mhz
  - 2.4 à 2.483 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

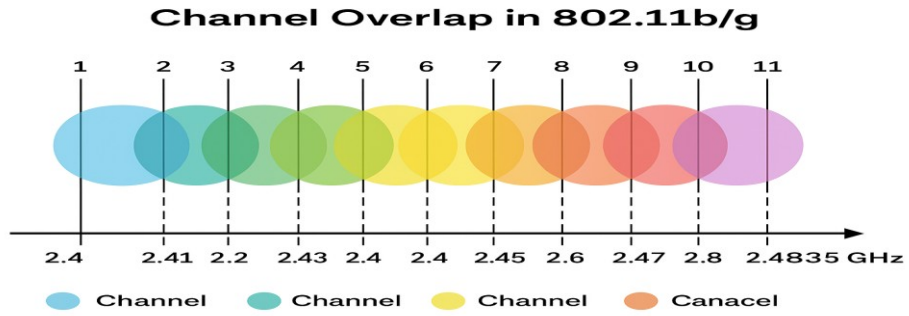
Chapitre 2 : La norme WiFi (802.11)

Gamme de fréquence et canaux

Les canaux du 802.11b et g

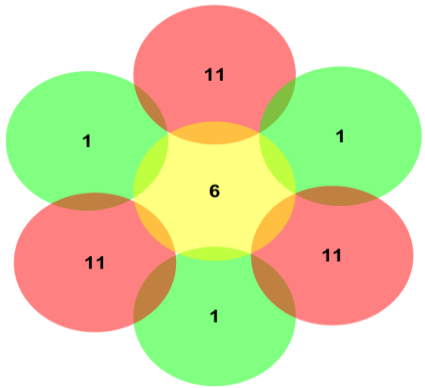
- La bande de fréquence du WiFi (802.11b et g) est divisée en 13 canaux se recouvrant partiellement
- Chaque BSS communique sur **un** canal fixé lors de la configuration de l'AP (Infrastructure) ou de l'adaptateur (ad-hoc)
- Trois canaux seulement sont utilisables simultanément et à proximité : 1, 6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



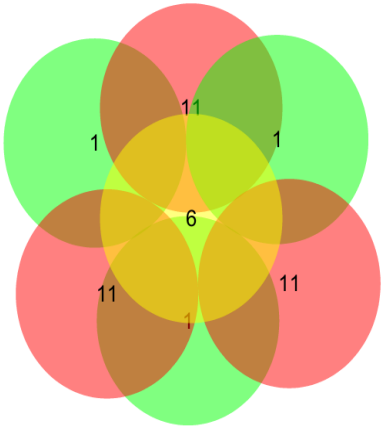


Affectation des canaux

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

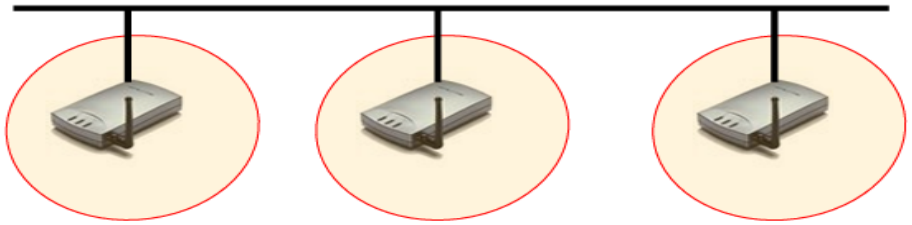


- Affectation de trois canaux qui ne se perturbent pas (cas obligatoire) :



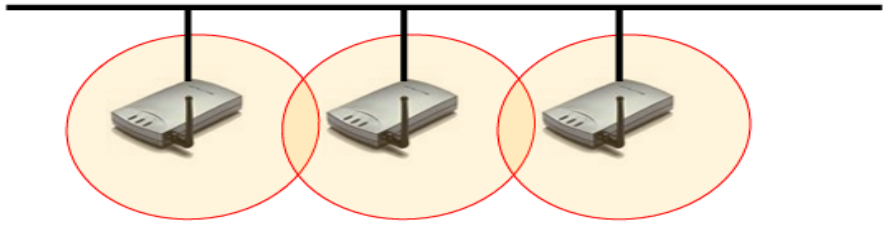
Gamme de fréquence et canaux

Choix de la topologie



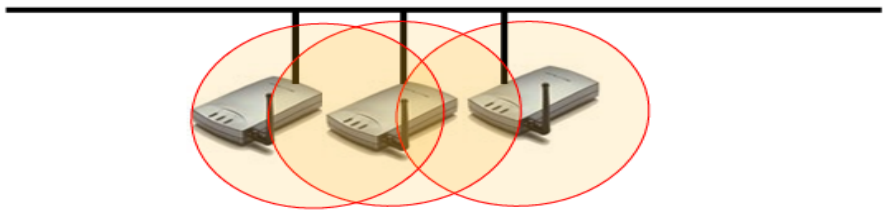
les cellules sont disjointes

- 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

Chapitre 2 : La norme WiFi (802.11)

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

Chapitre 2 : La norme WiFi (802.11)

Normes et standards

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

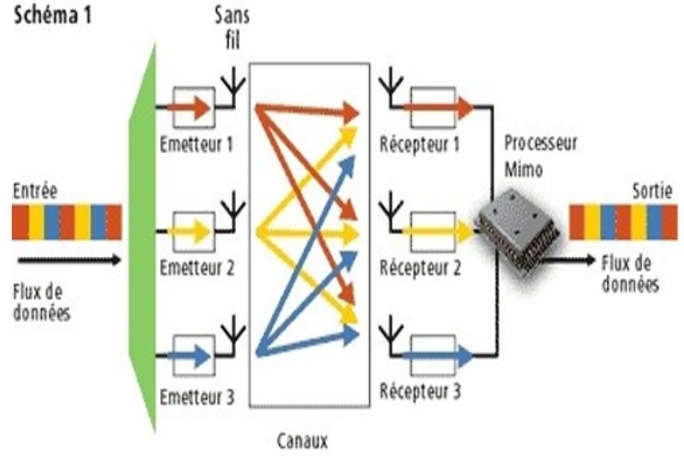
- **Origine**
  - **802.11** : 2 Mbits/s (1997)
- **Amendements**
  - **802.11b** : 2,4 Ghz - 11 Mbits/s (bande ISM) - FSSS
  - **802.11a** : 5 Ghz - 54 Mbits/s (bande UN-II) - OFDM
  - **802.11g** : 2,4 Ghz - 54 Mbits/s (bande ISM) - OFDM
  - **802.11e** : Qualité de service
  - **802.11f** : Itinérance (roaming)
  - **802.11h** : Norme européenne pour les fréquences et la gestion d'énergie
  - **802.11i** : Sécurité - chiffrement et authentification AES
  - **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.

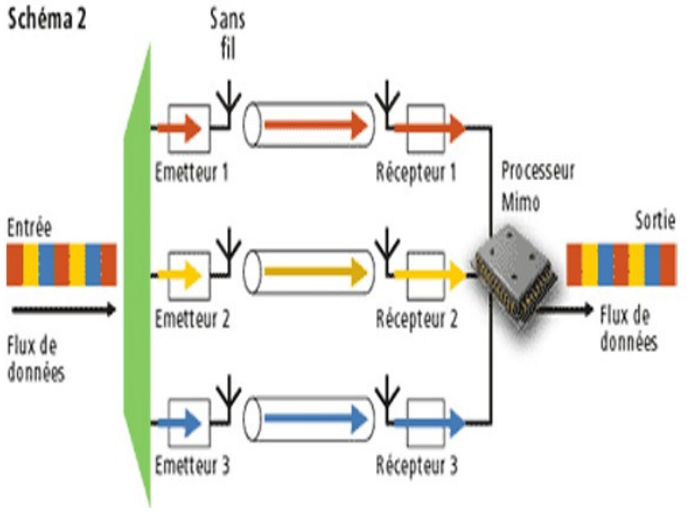
Chapitre 2 : La norme WiFi (802.11)

Normes et standards

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

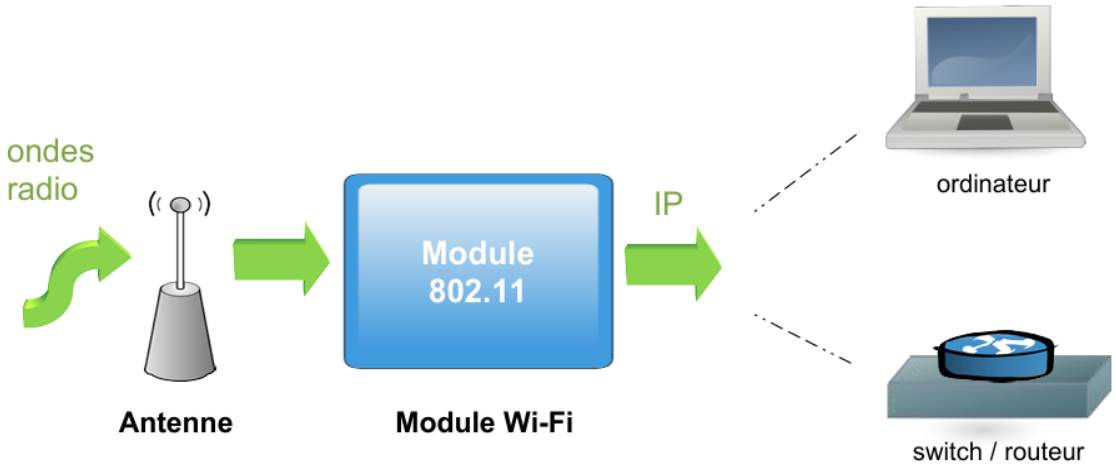
- l'algorithme de traitement de chaque récepteur isole le signal d'un des émetteurs en utilisant les réflexions
- le protocole dispose donc de trois canaux virtuels
- le débit est multiplié par trois

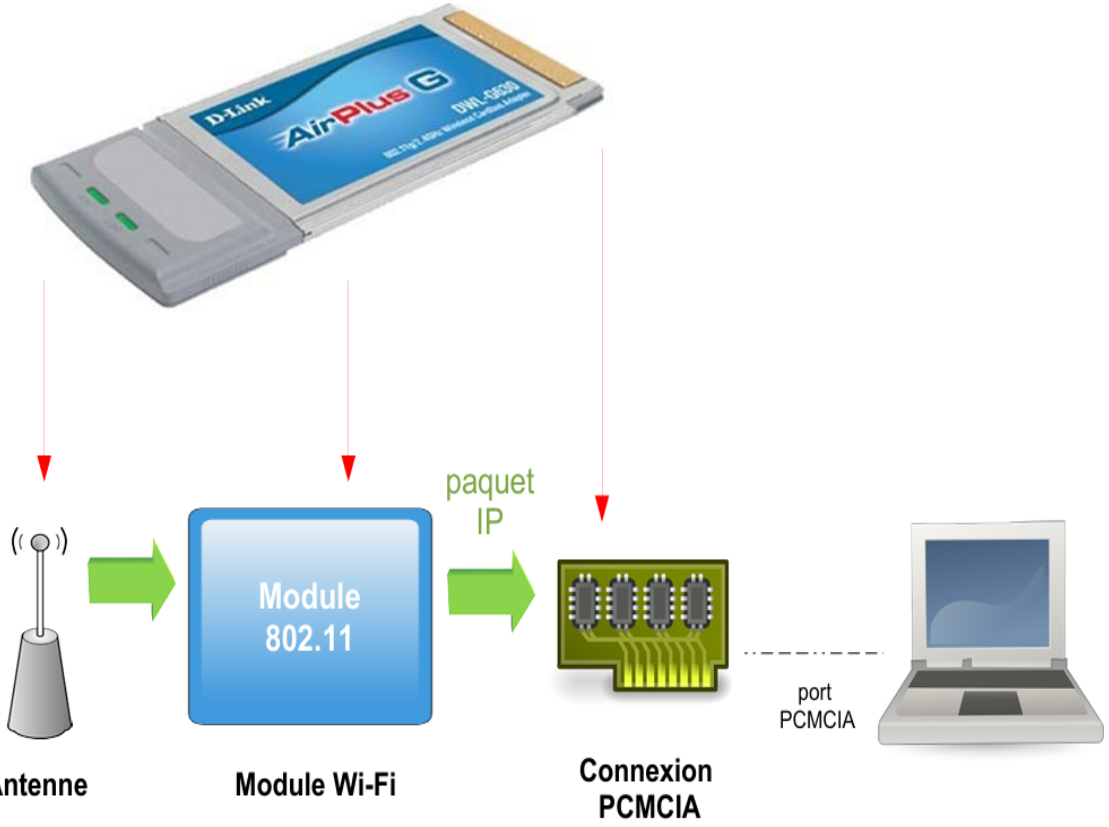
Fonctionnement - Couche 802.11

Fonctionnement

- Tous les équipements WiFi sont équipés d@ne antenne et d@n module chargé de la commutation

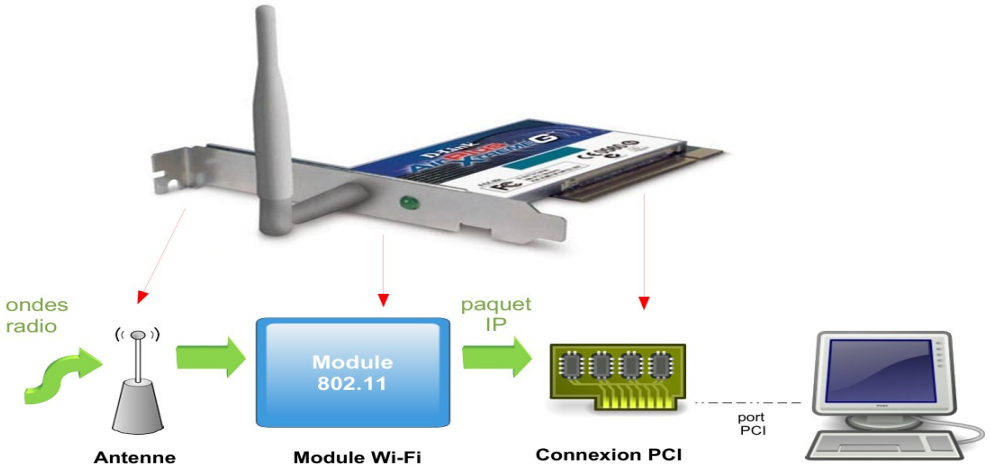
  ondes radio <-> trames IP

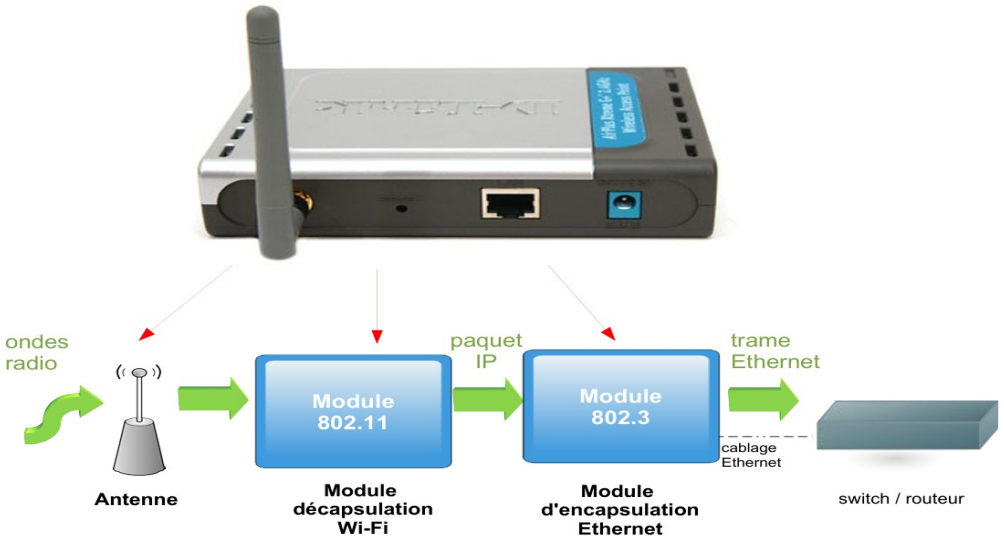




Chapitre 2 : La norme WiFi (802.11)

Fonctionnement - Couche 802.11



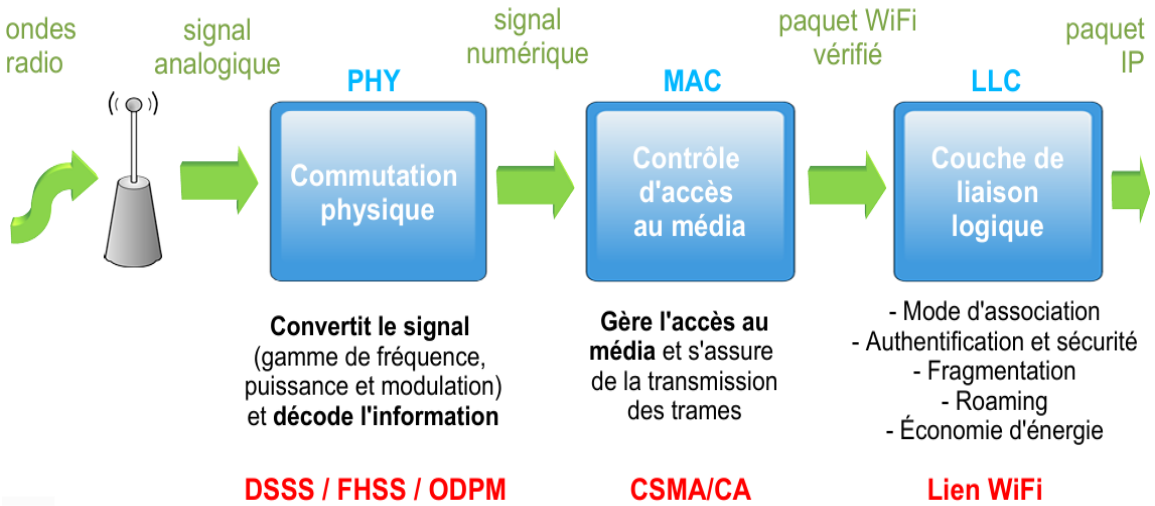


Le module WiFi

- Modulation

ondes radio <-> trames IP

niveau 1 <-> niveau 3 de la couche OSI



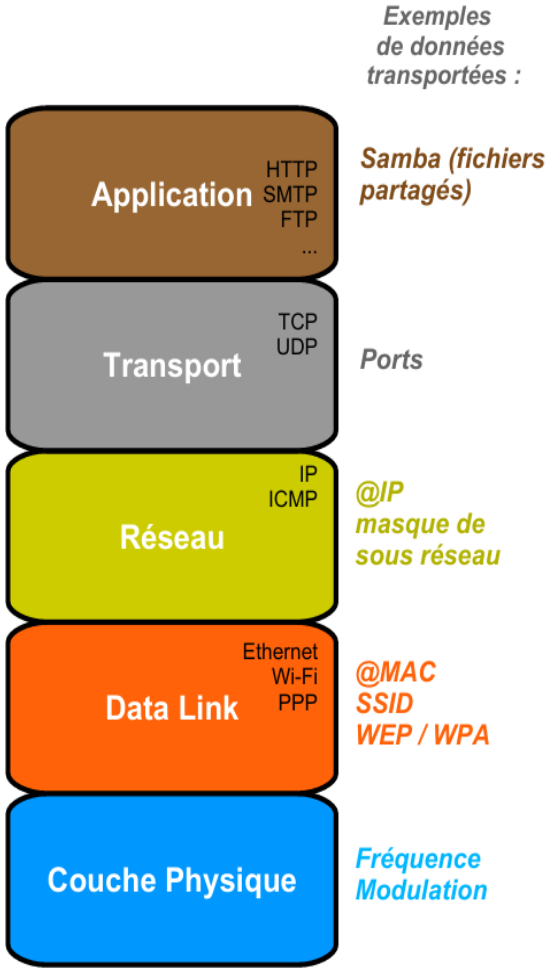
Fin du chapitre 2

PLAN DU COURS

Chapitre 3 : Configurer un réseau WiFi – TCP/IP

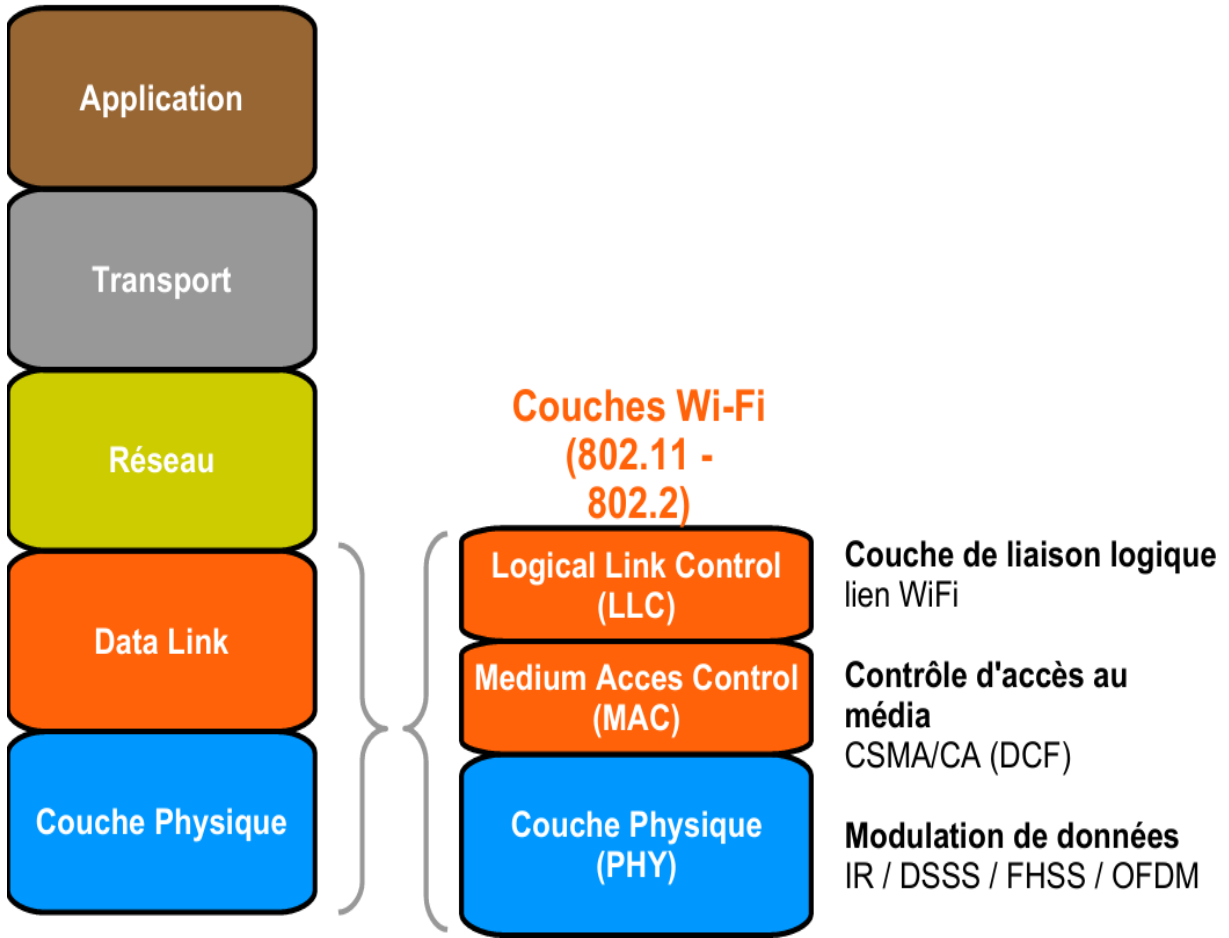
Le modèle OSI

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

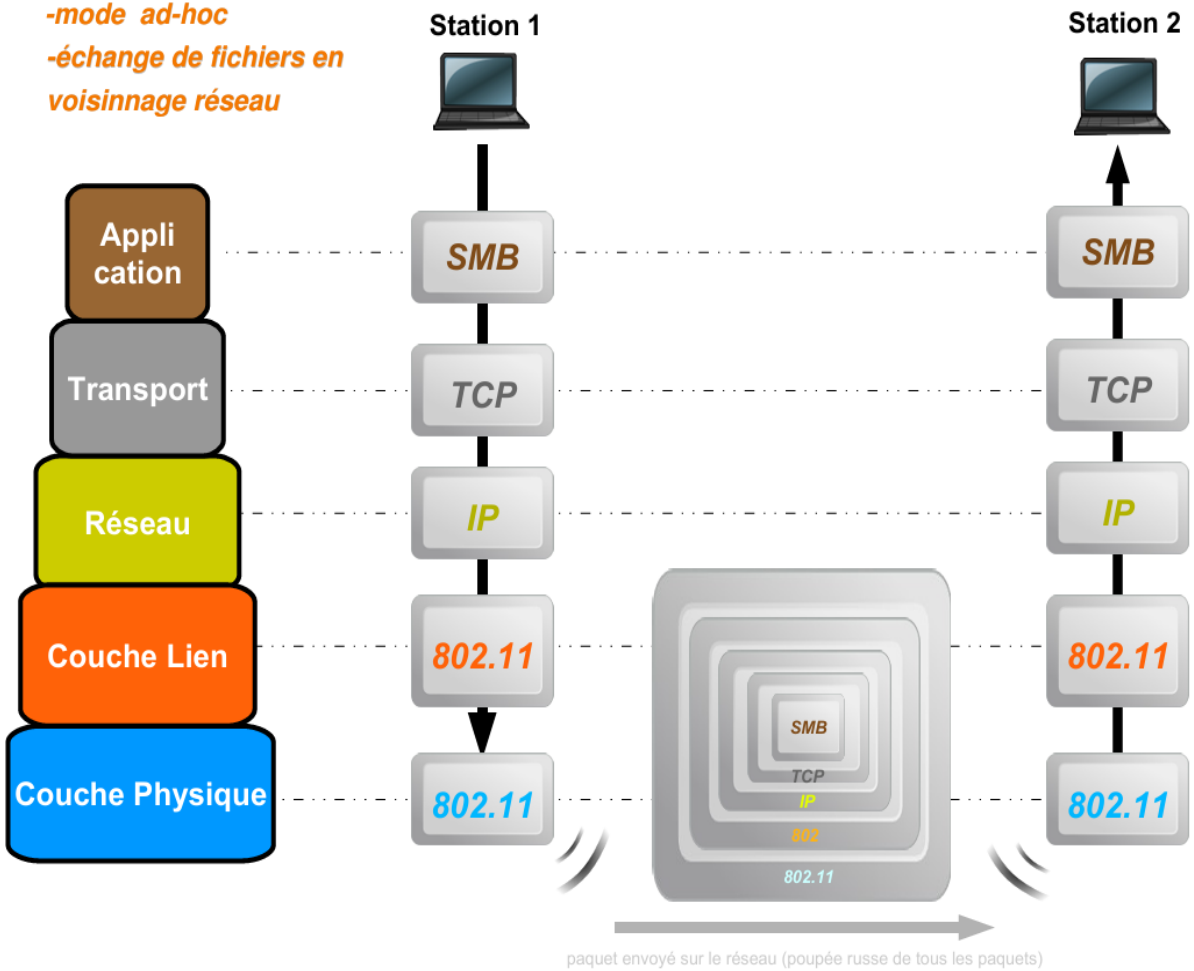
Les couches 802.11



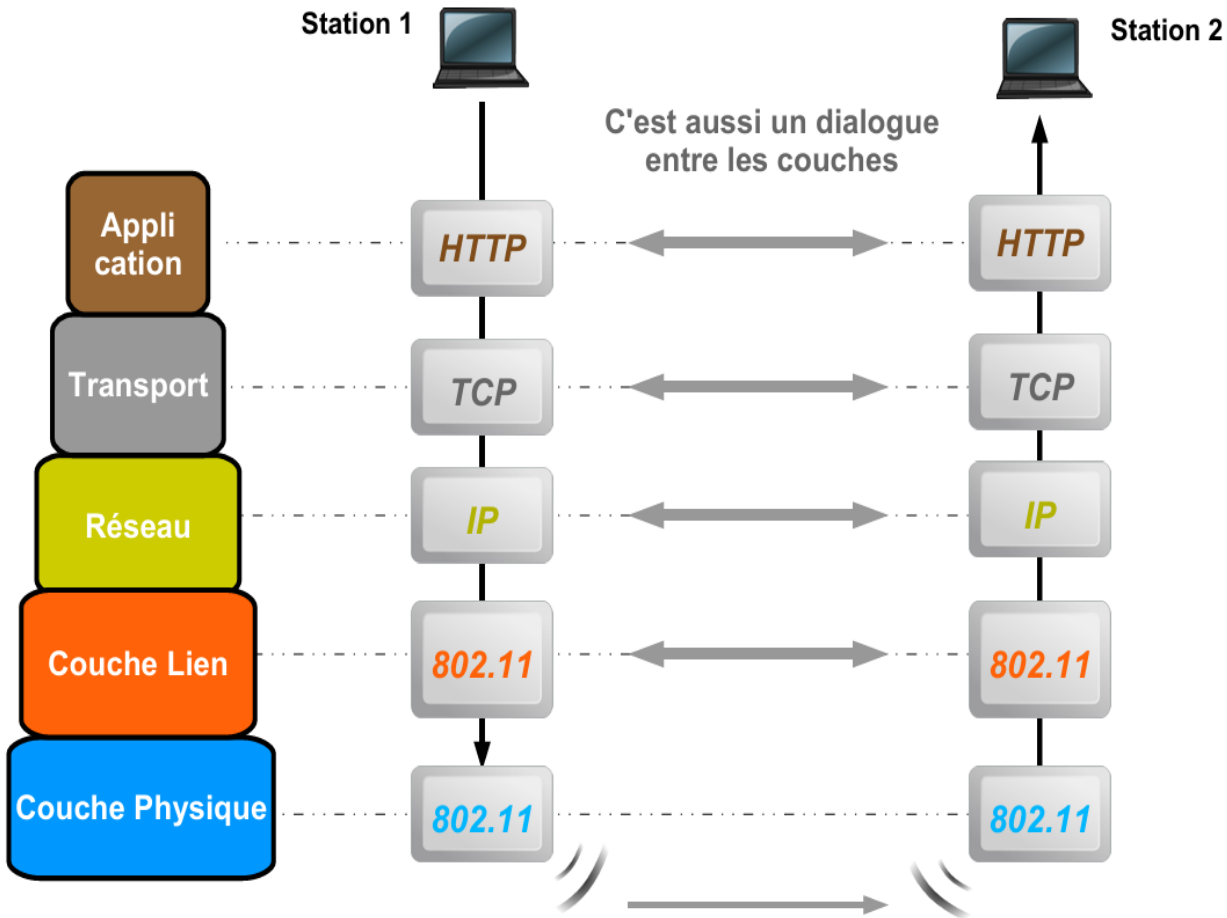
Le modèle OSI

Communication entre deux stations

-mode ad-hoc
-échange de fichiers en voisinnage réseau



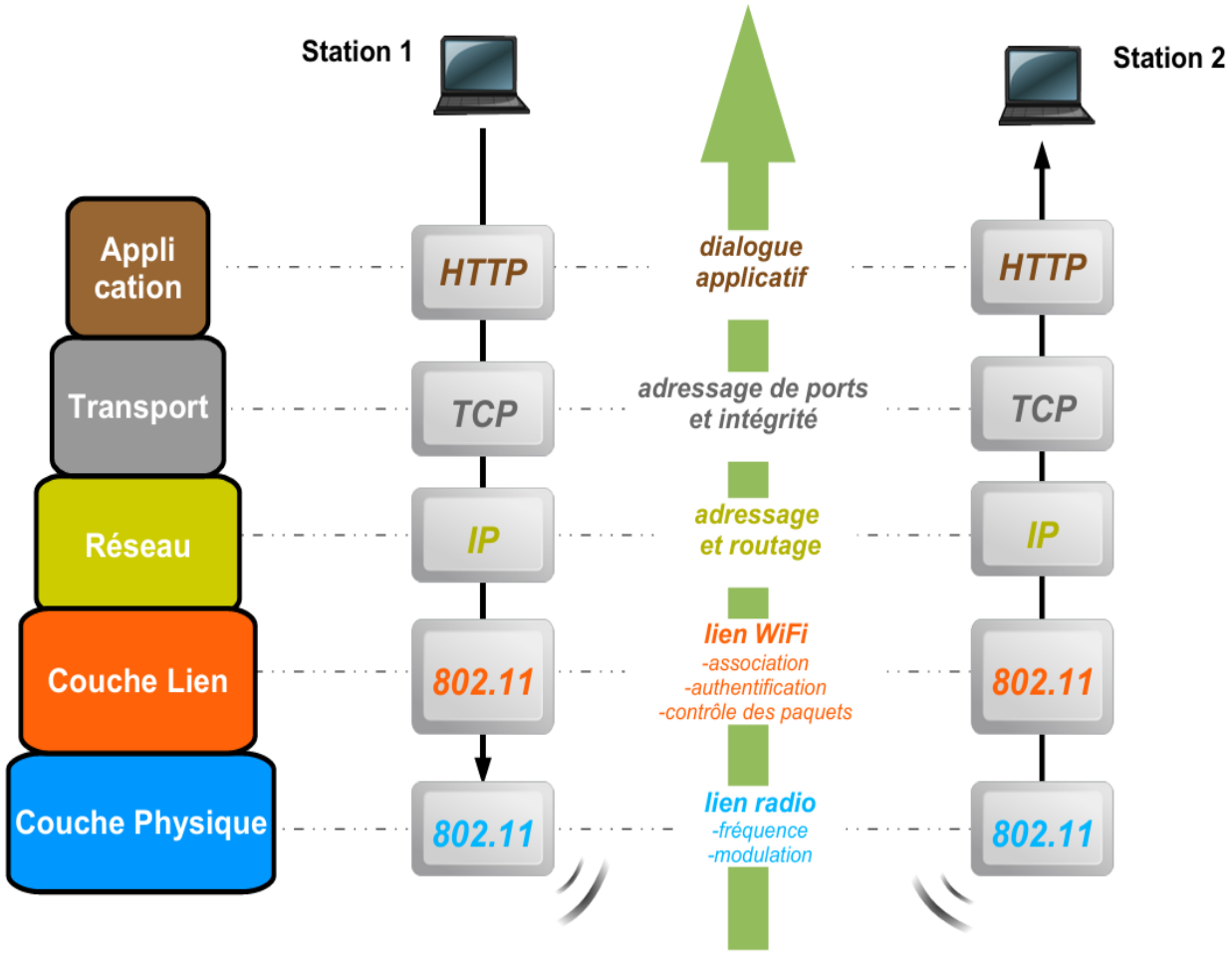
Un dialogue transversal



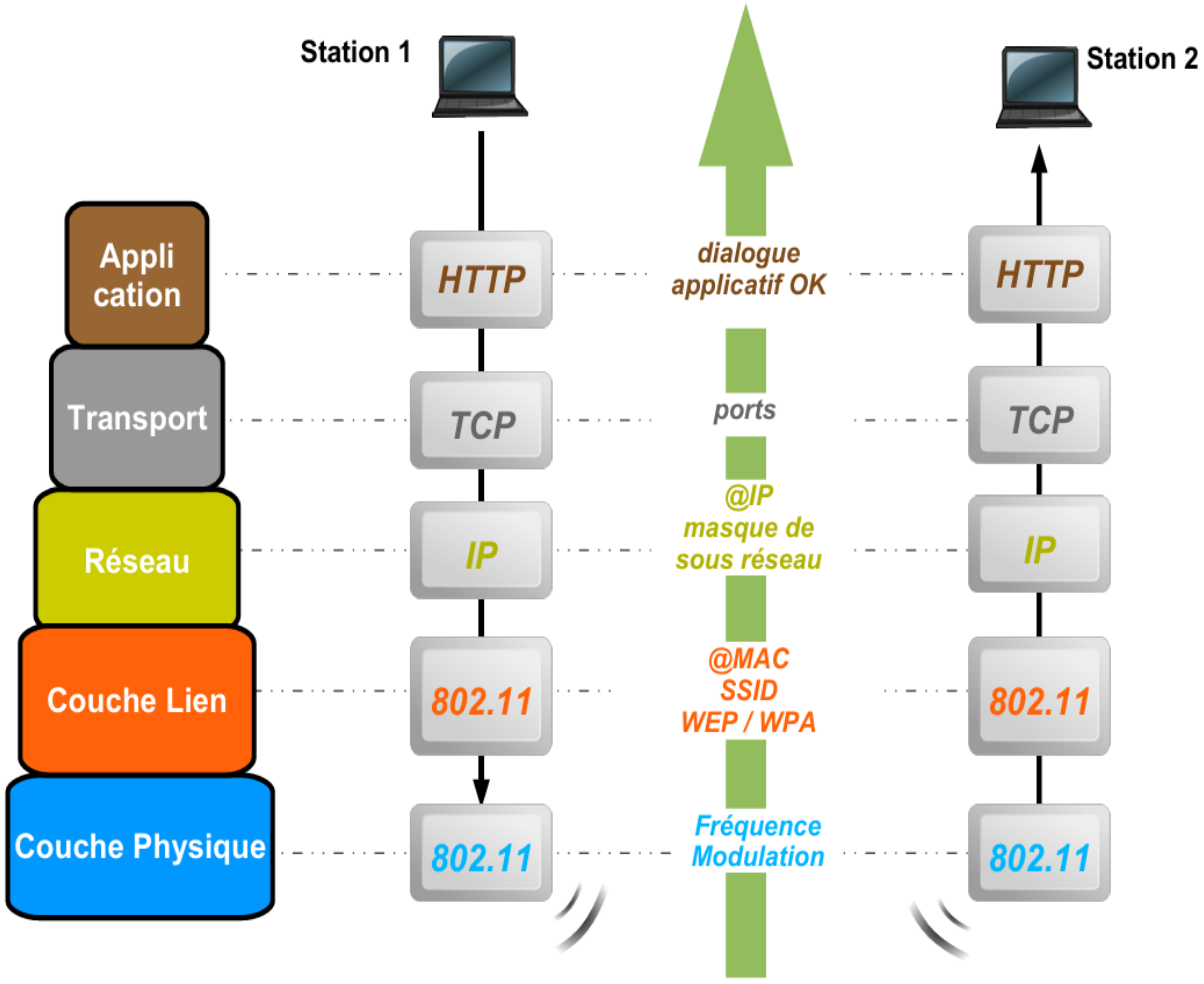
Chapitre 3 : Configurer un réseau WiFi – TCP/IP

Le modèle OSI

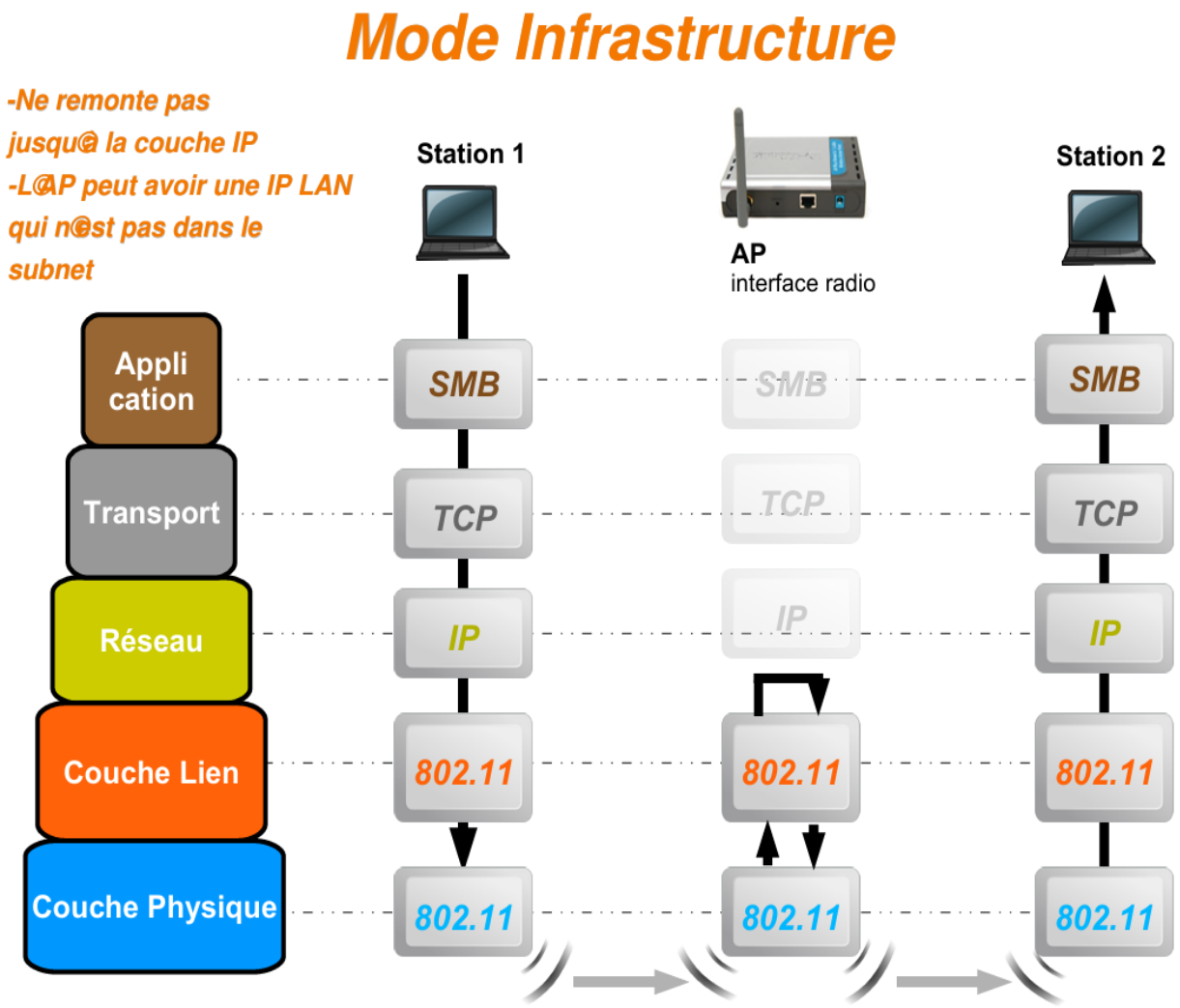
Des services successifs

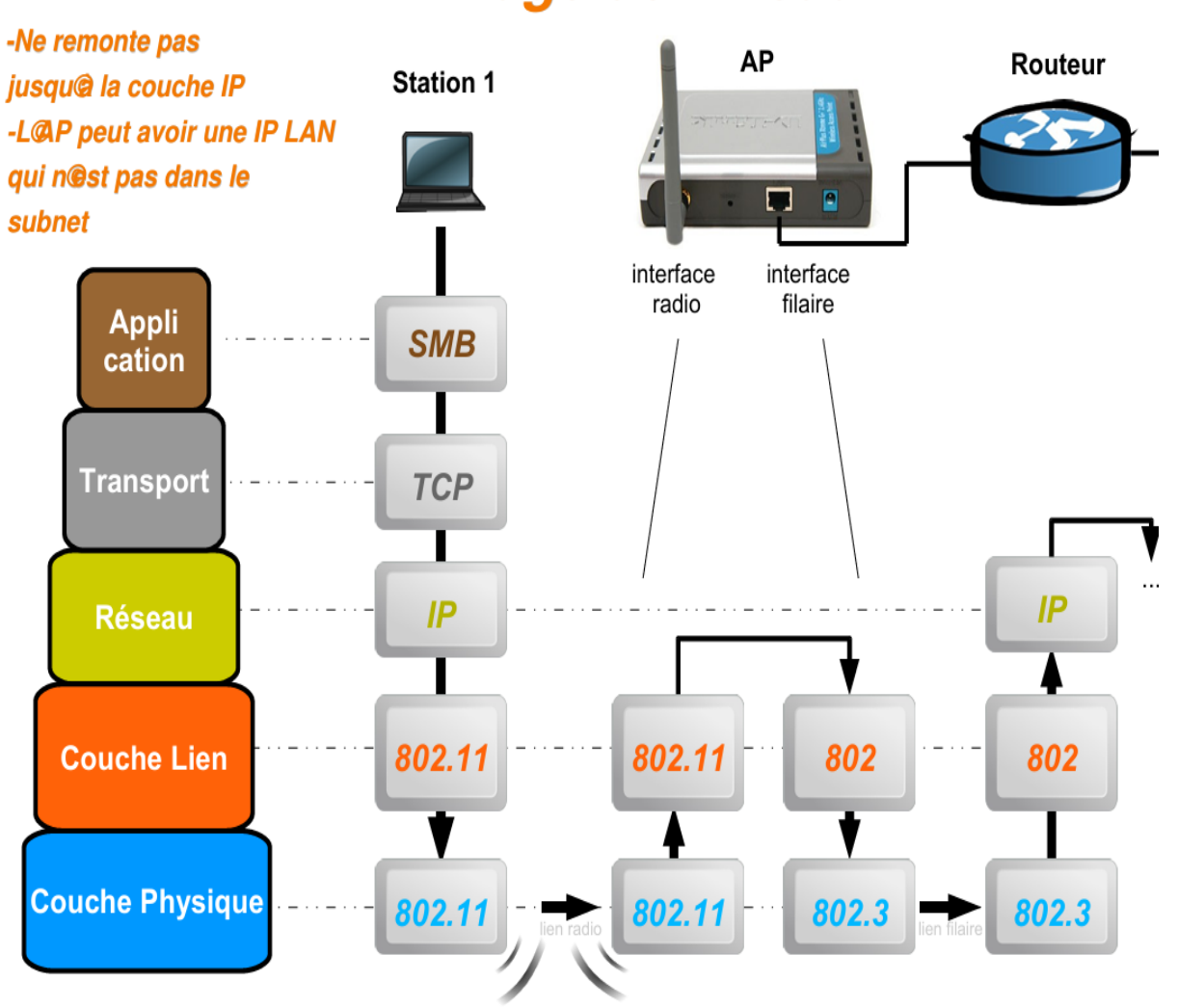


Des filtres successifs



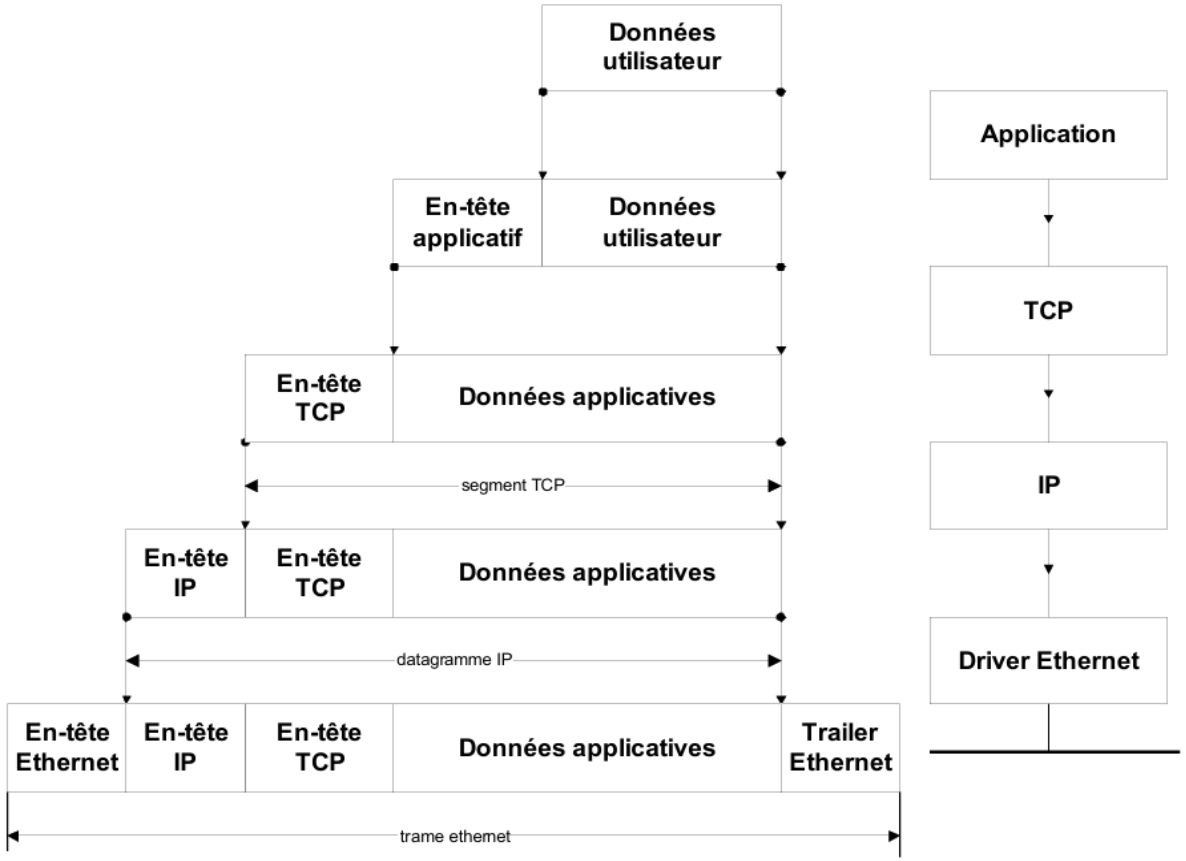
Le modèle OSI



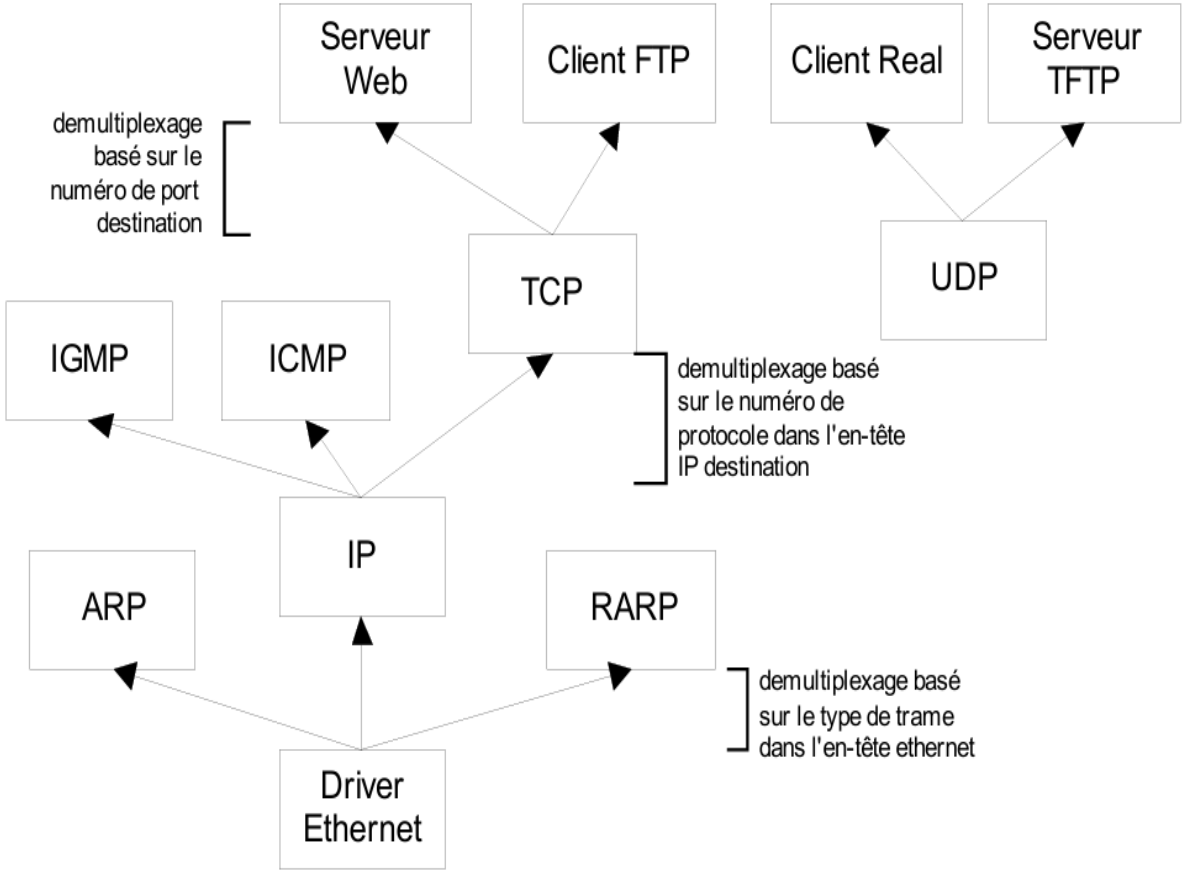


Le modèle OSI

Réseau TCP/IP - Encapsulation



Démultiplexage



Le modèle OSI

Ce qu@l 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 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

Réseau TCP/IP

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

	réseau	hosts (255)	
adresse IP	192 . 168 . 0	. xxx	
masque	255.255.255 . 0		ou /24

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

Par défaut, dans un réseau local, on utilisera :

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

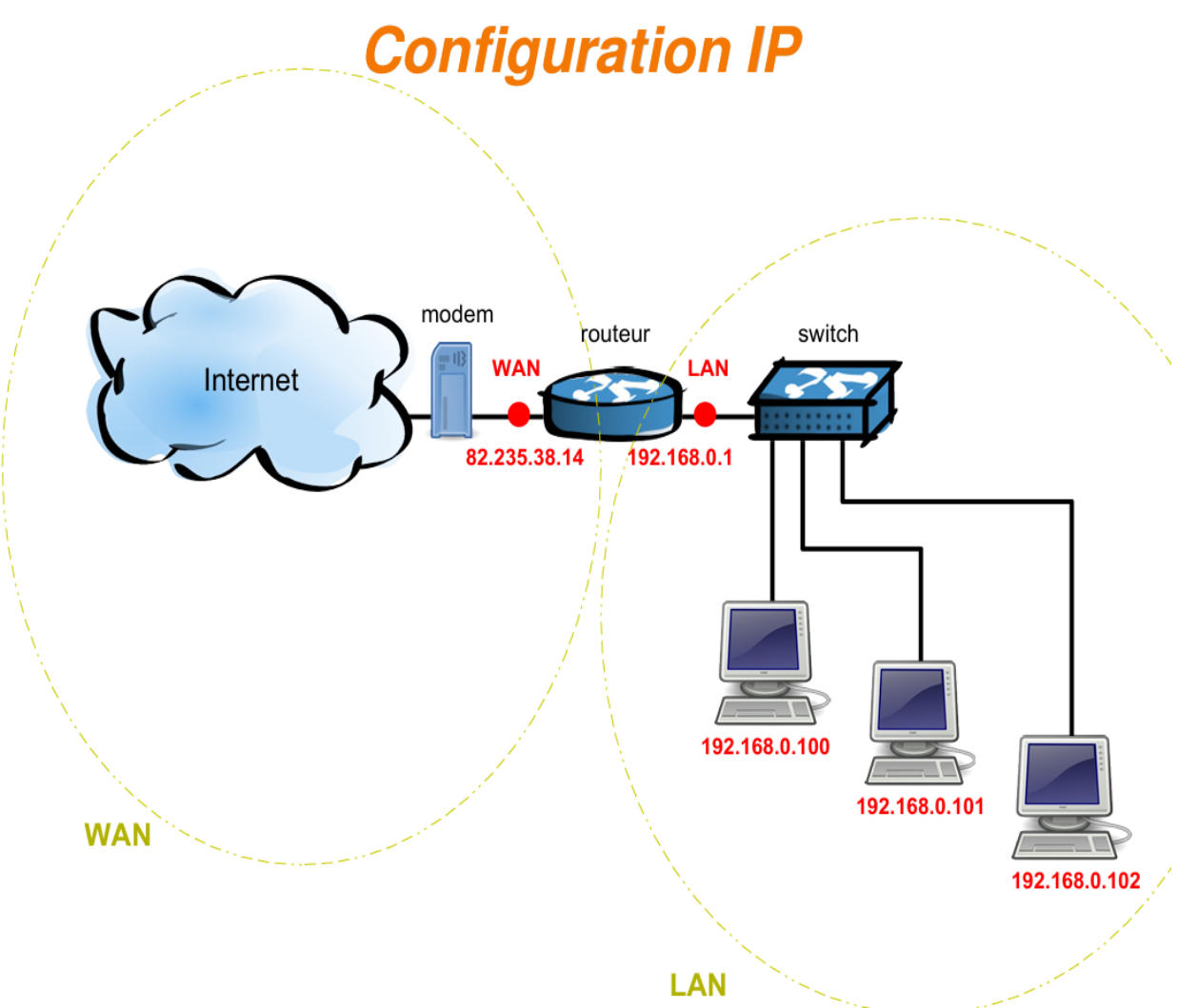
Masque de sous réseau	Notation CIDR	Nombre de machines
255.255.255.252	/30	2
255.255.255.248	/29	6
255.255.255.240	/28	14
255.255.255.224	/27	30
255.255.255.192	/26	62
255.255.255.128	/25	126
255.255.255.0	/24	254
255.255.254.0	/23	510
255.255.252.0	/22	1022
255.255.248.0	/21	2046
255.255.240.0	/20	4094
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

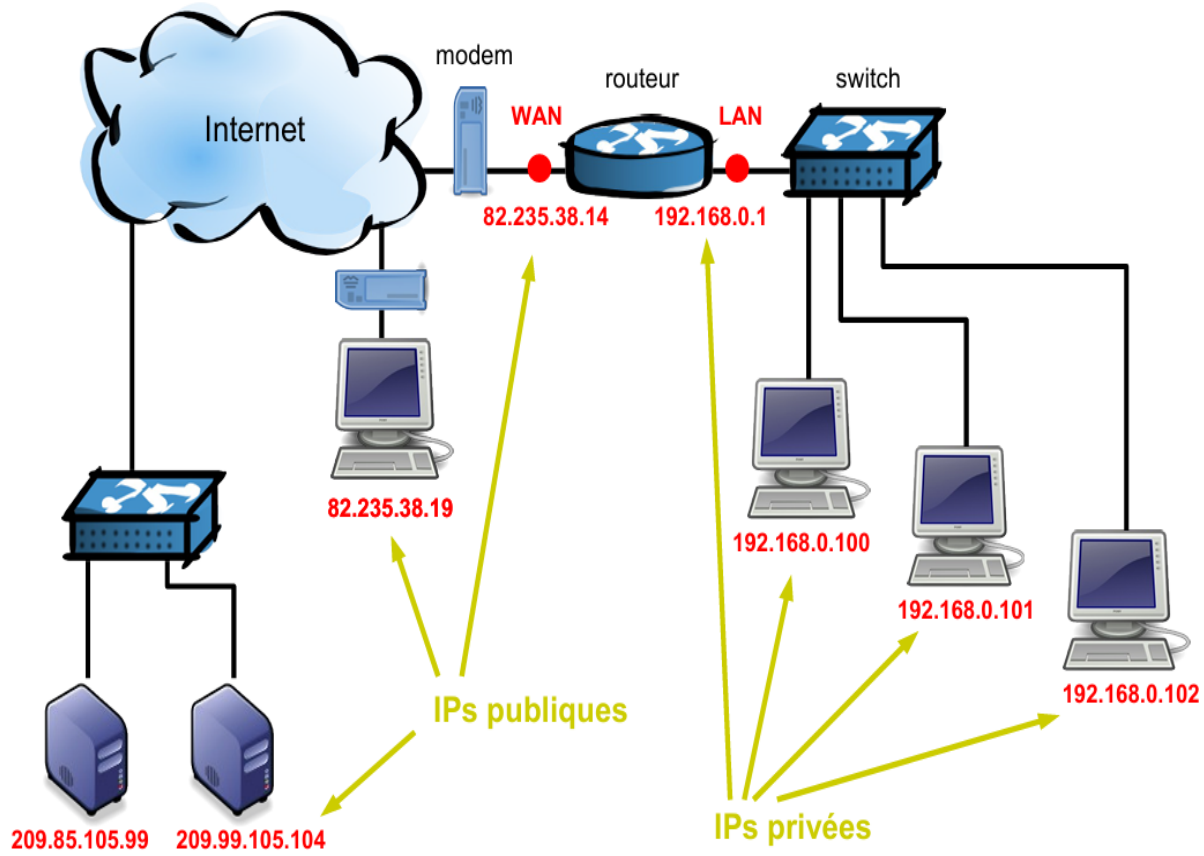
Réseau TCP/IP

- 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)

Chapitre 3 : Configurer un réseau WiFi – TCP/IP

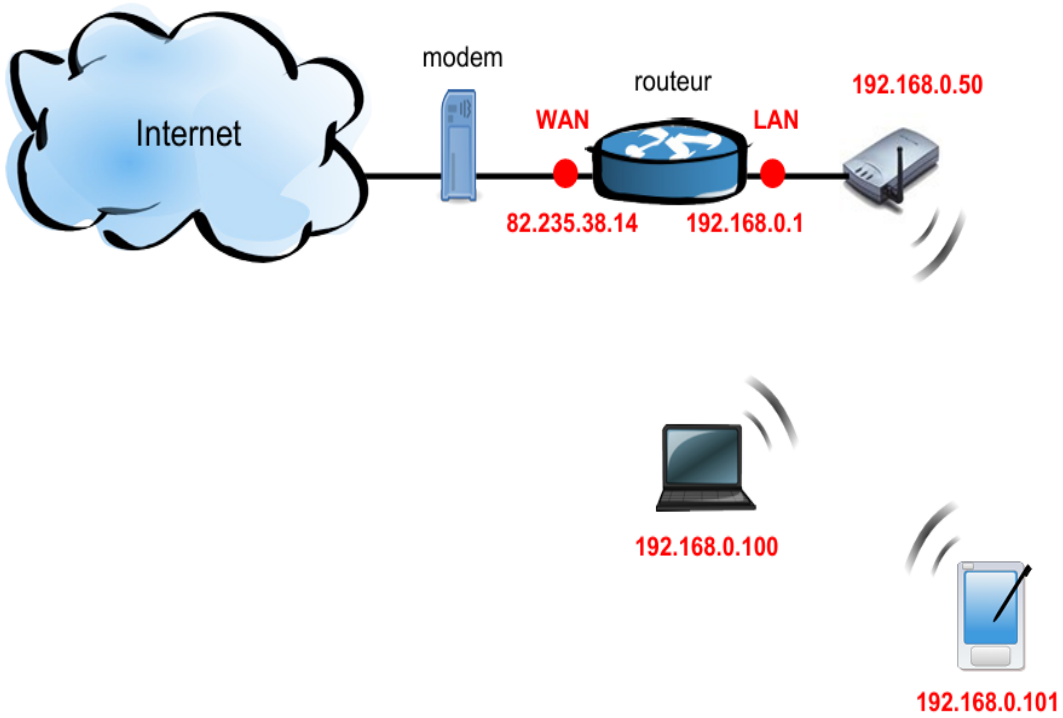
Réseau TCP/IP

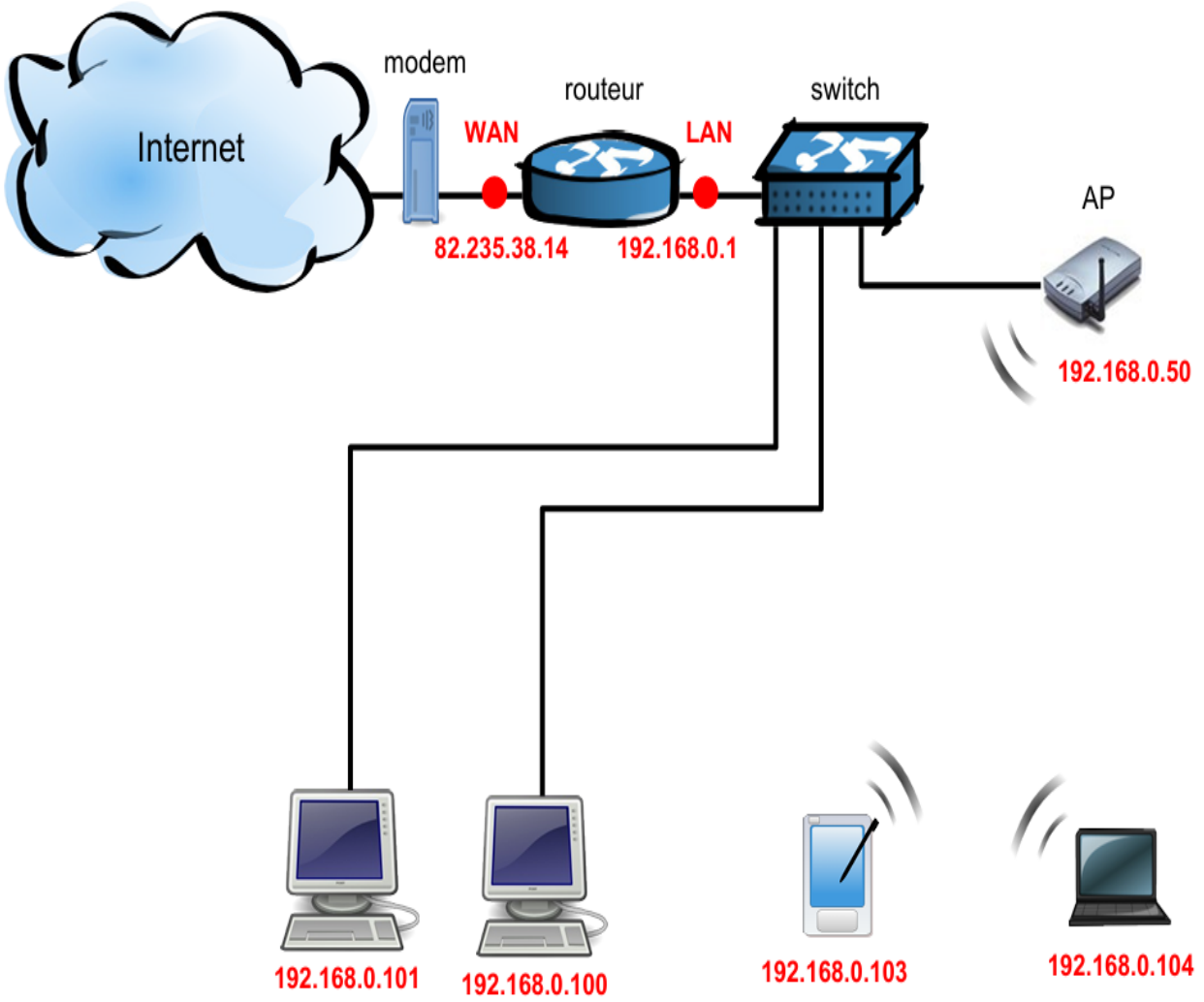




Réseau TCP/IP

Topologie Infrastructure



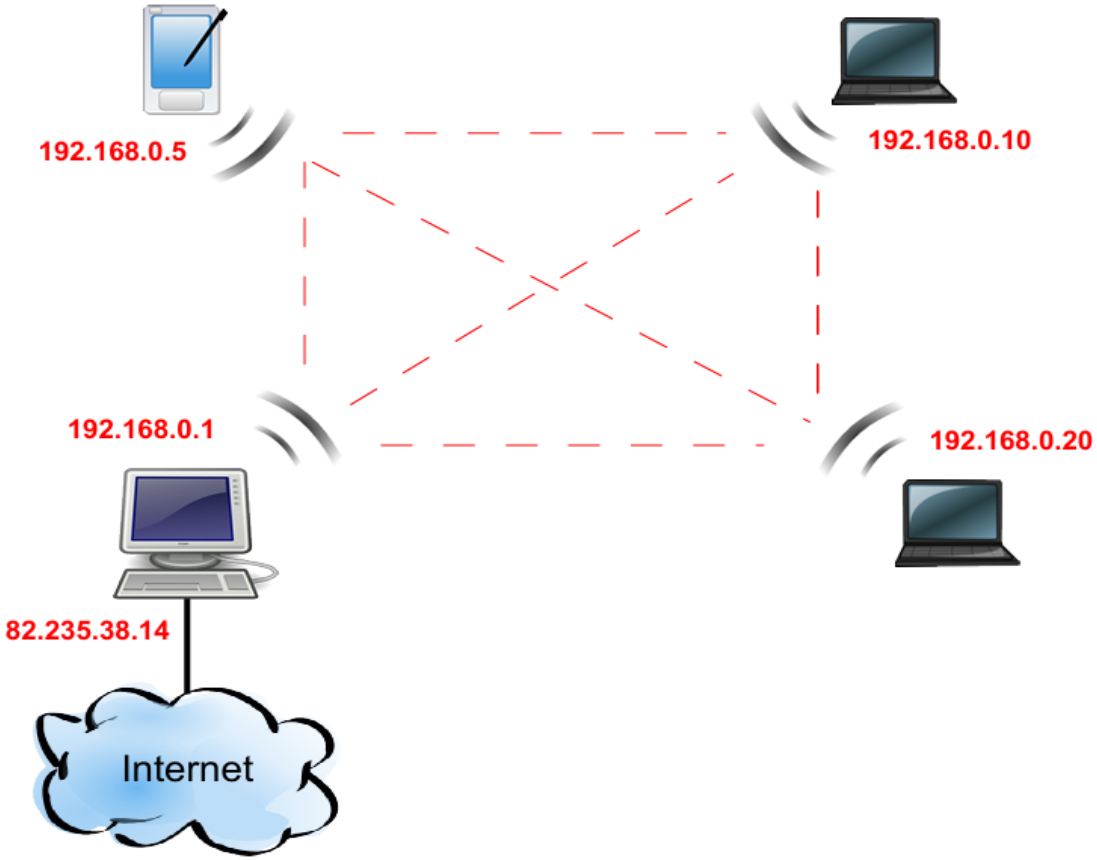


Chapitre 3 : Configurer un réseau WiFi – TCP/IP

Réseau TCP/IP

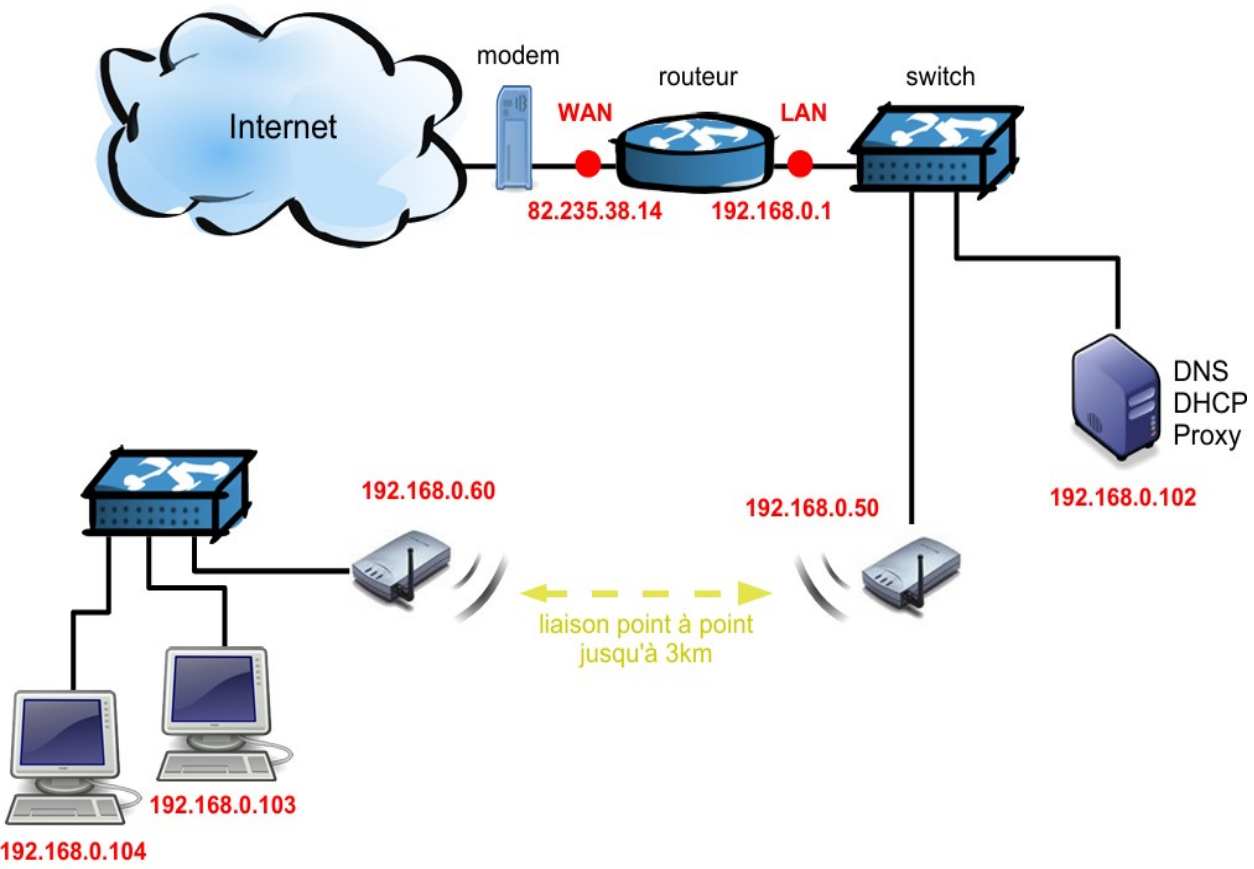
= 3 en 1

Topologie ad-hoc



Réseau TCP/IP

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)...

Réseau TCP/IP

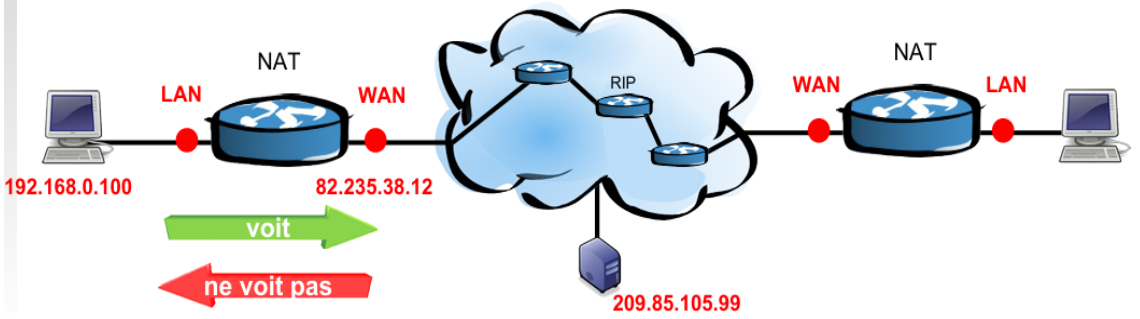
Serveur DHCP

- 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

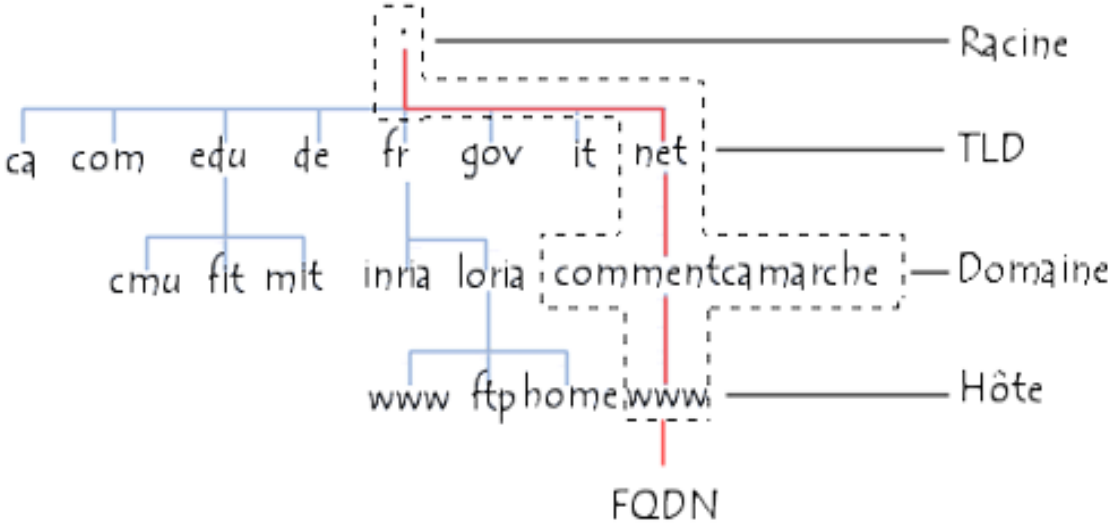
- Possèdent deux interfaces. Ils transmettent leurs paquets IP d'une interface à l'autre.
- Routage NAT
  - Permets une translation d'adresse :
    une @IP publique <-> n * @IP privées
  - Le réseau public (WAN) est visible depuis le réseau privé (LAN) mais pas l'inverse.



Réseau TCP/IP

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).

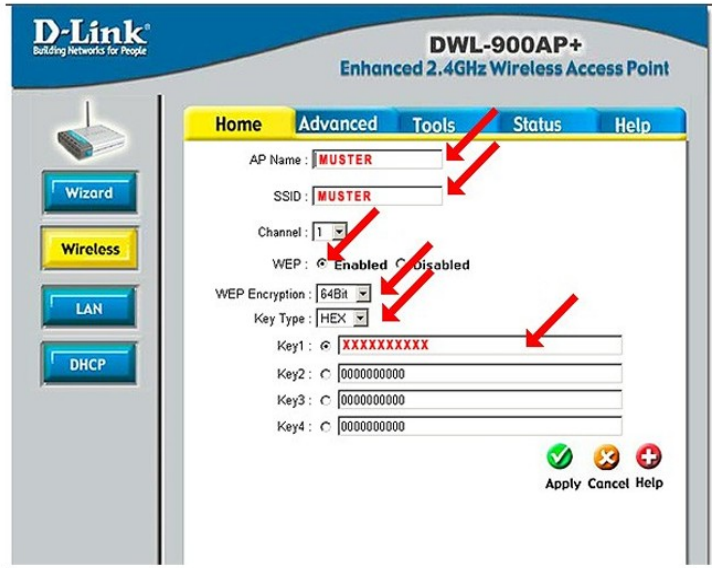


Chapitre 3 : Configurer un réseau WiFi – TCP/IP

Configuration du réseau WiFi

Réglages Radio de l@AP

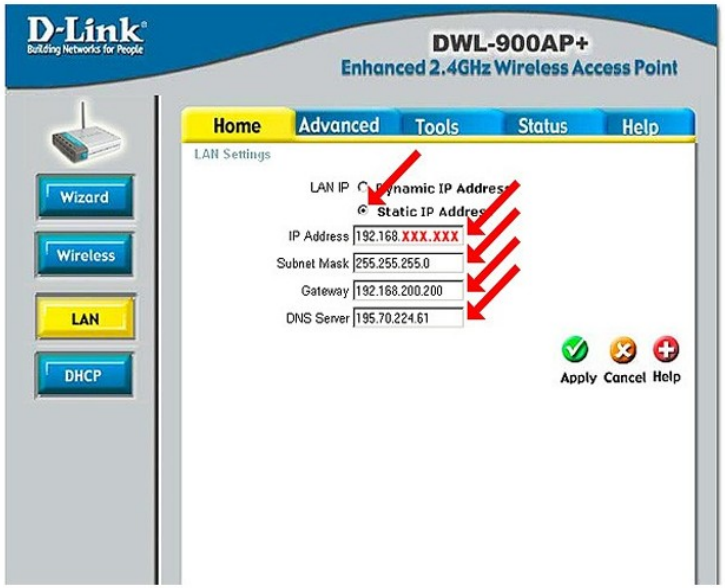
- Configuration Radio
  - Nom
  - (E)SSID
  - Canal d©mission
  - SSID Broadcast
  - Topologie : AP, Client, Bridge, Repeater...
- Configuration Radio avancée
  - Puissance d©mission
  - Chiffrement et authentification : WEP / WPA
  - Filtrage des adresses MAC
  - Radio : Débits, DTIM, Fragmentation, 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



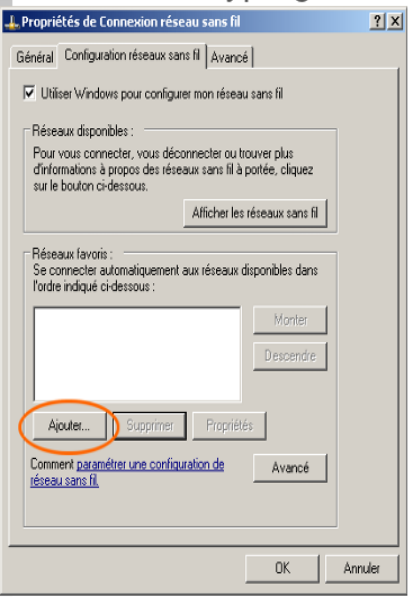
Chapitre 3 : Configurer un réseau WiFi – TCP/IP

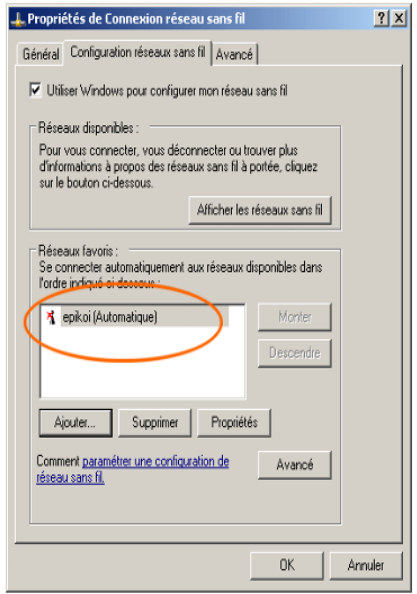
Configuration du réseau WiFi

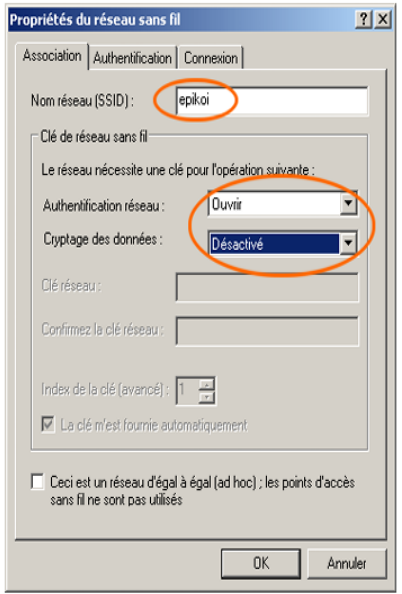
Réglages radio de l@daptateur Wi-Fi

- 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





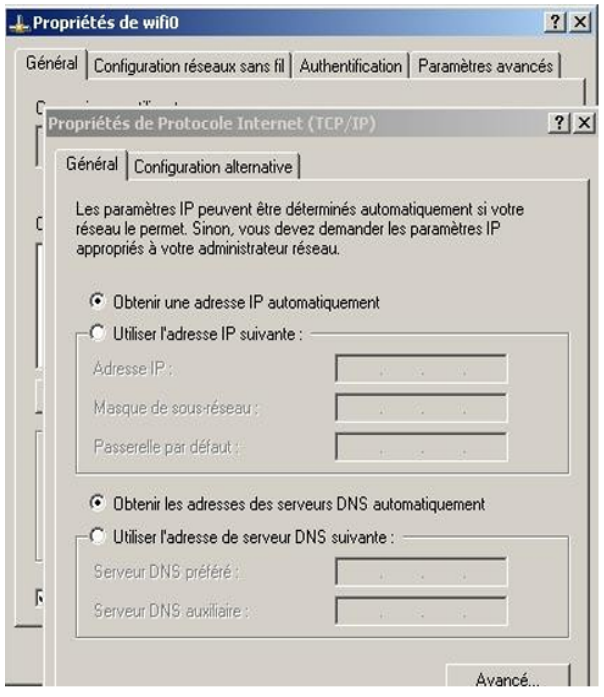


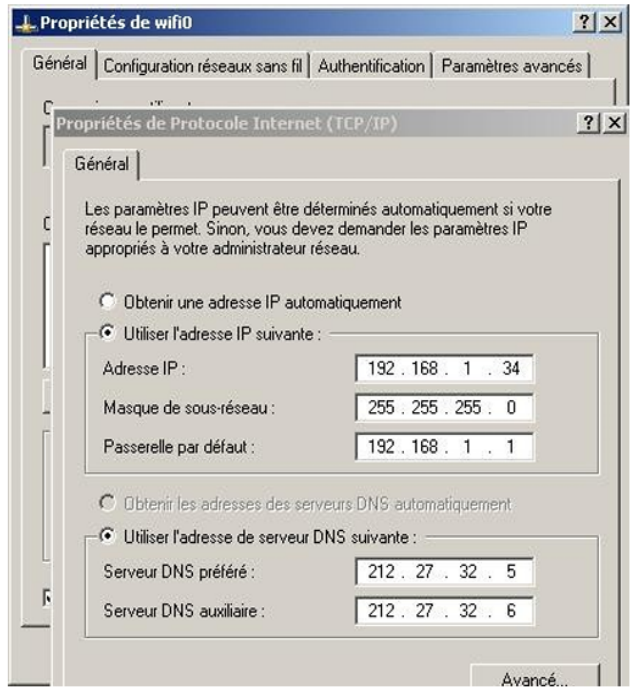
Réglages TCP/IP de l@daptateur Wi-Fi

- DHCP

OU

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

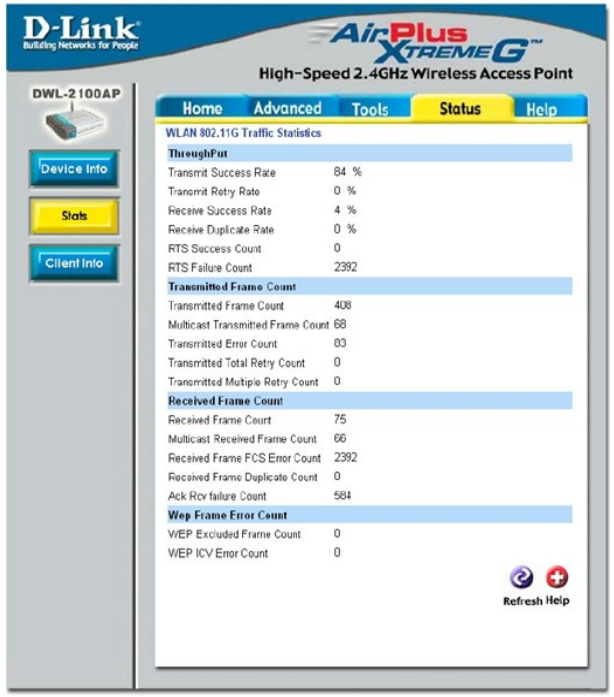




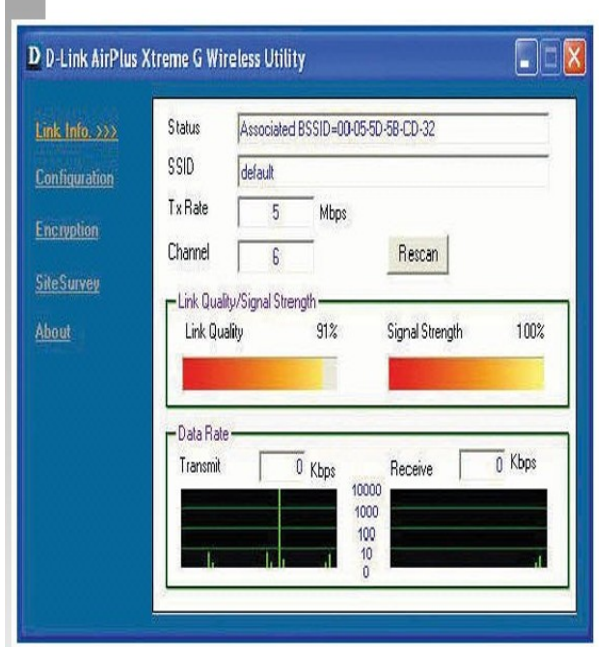
Chapitre 3 : Configurer un réseau WiFi – TCP/IP

Configuration du réseau WiFi

Diagnostics d@ssociation (AP)



Diagnostics en mobilité (client)



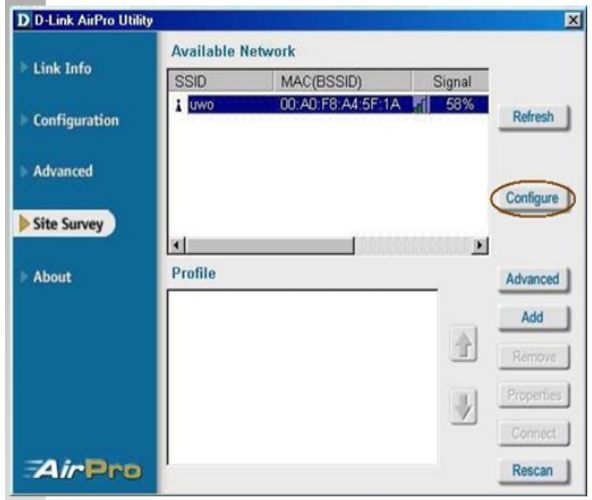
Outil Fabricant (Dlink)
-Puissance du signal
-Qualité du signal

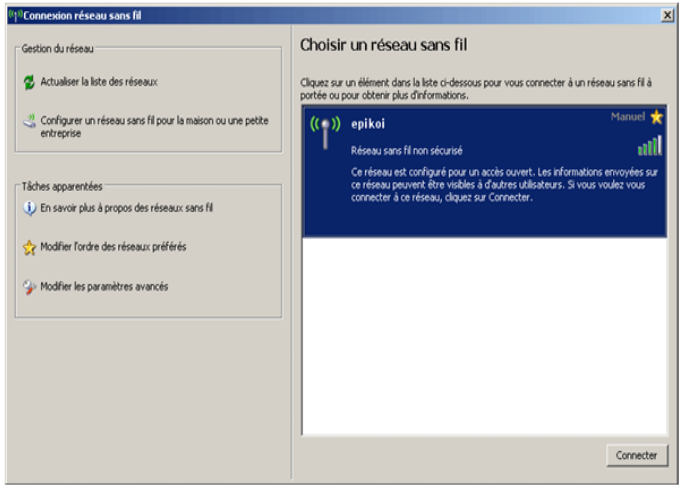
Outil générique (Windows)
-Puissance du signal

Chapitre 3 : Configurer un réseau WiFi – TCP/IP

Configuration du réseau WiFi

Détection des réseaux (client)

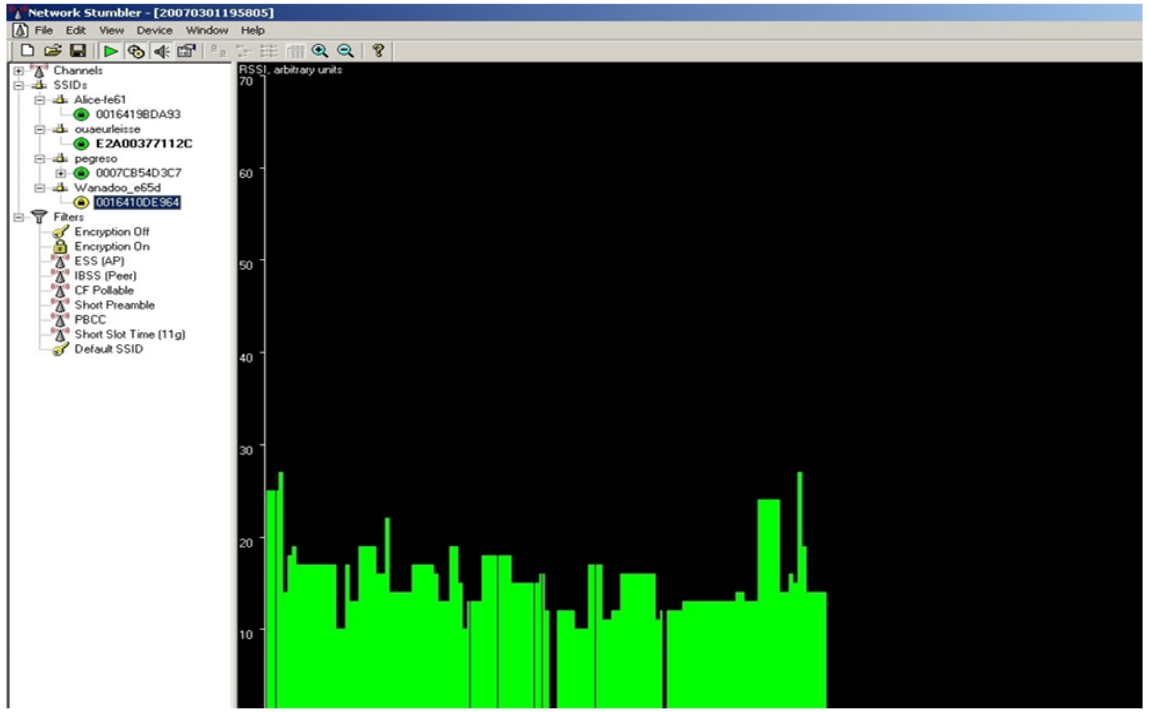




Outil Fabricant (Dlink)
-SSID
-BSSID
-Puissance du Signal

Outil générique (Windows)
-SSID
-Puissance du signal

Outils génériques (client)

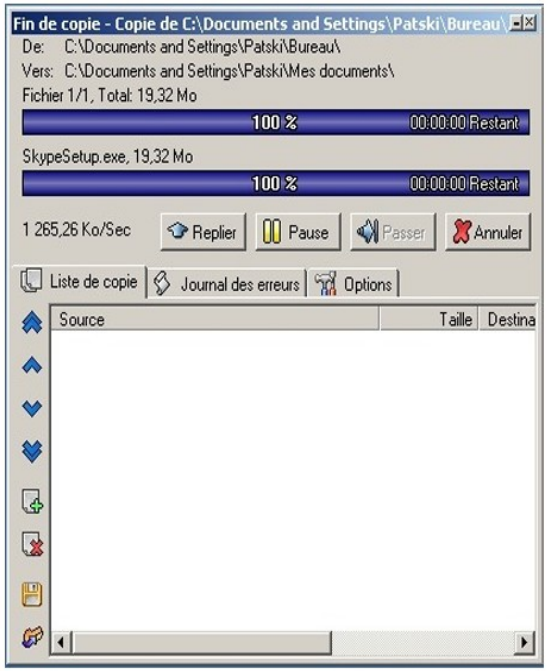


NetStumbler
-SSID
-BSSID
-Puissance du Signal
-type d'encryption
-rapport S/B

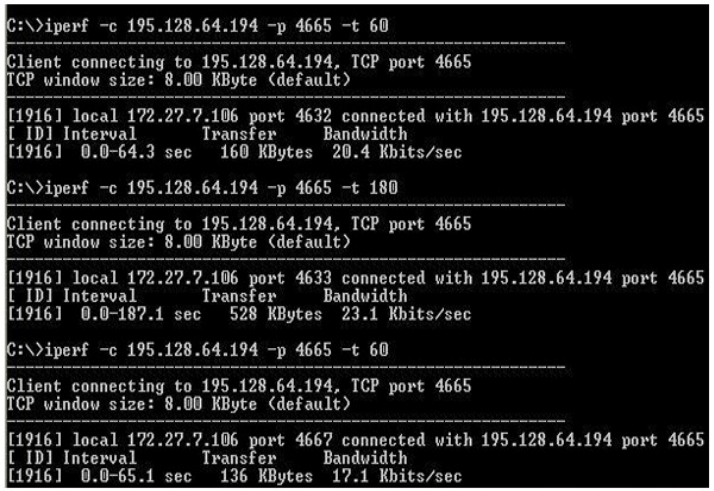
Chapitre 3 : Configurer un réseau WiFi – TCP/IP

Configuration du réseau WiFi

Mesure de débit

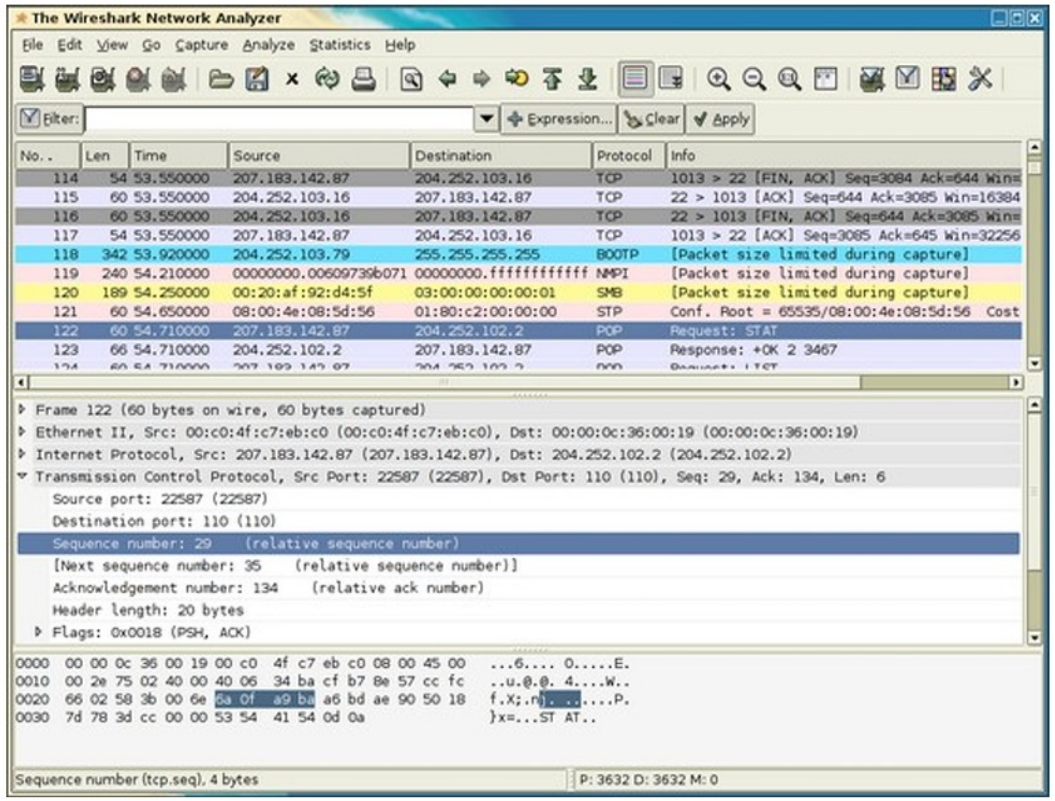


SuperCopier
(Windows)



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)

Fin du chapitre 3

PLAN DU COURS

Chapitre 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, USRobotics
  - Hermes : Onorico, Buffalo
  - Atheros et Broadcom: dernirères versions 54Mbps
- Certains Chipsets ne sont pas utilisables en écoute
- Le label WiFi garantit l'interopérabilité 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 (eq. switch) :

- Sensibilité en réception et puissance de sortie.
- Topologies supportées (AP, Bridge, AP Client, répéteur…)
- Services supplémentaires (DHCP, routage, filtrage des clients, 802.1x, 802.1q)
- Exemple du Cisco et du Dlink.

Chapitre 4 : Matériel – Liens entre portée, débit et puissance

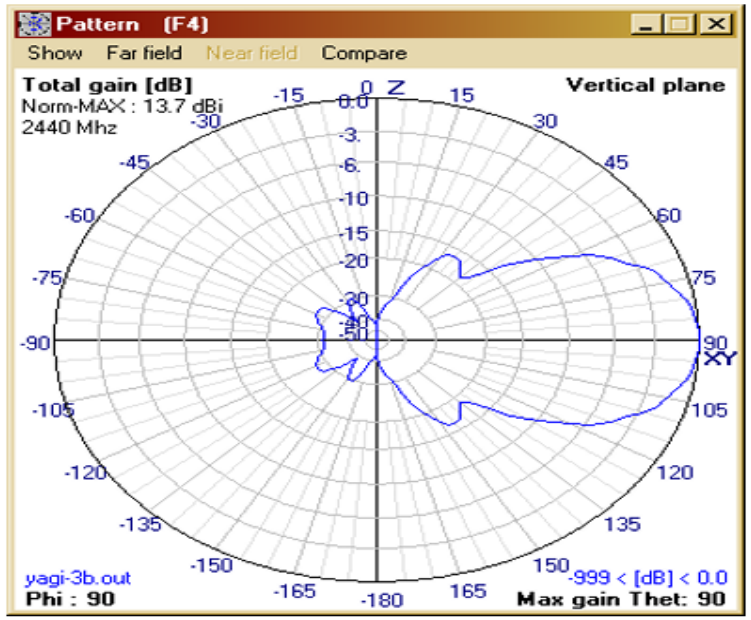
Adaptateurs WiFi et antennes

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).

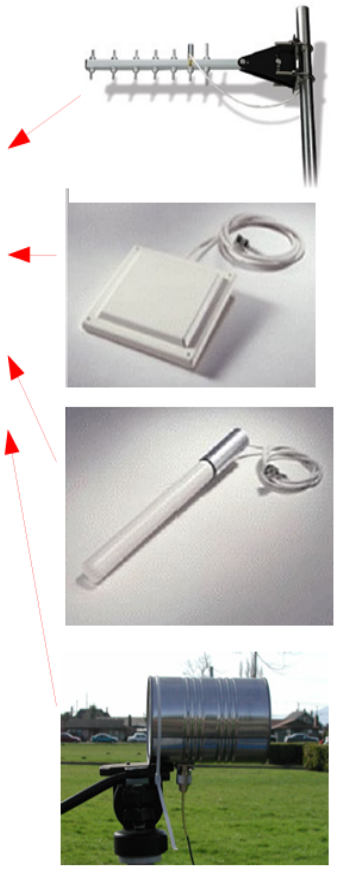


Chapitre 4 : Matériel – Liens entre portée, débit et puissance

Adaptateurs WiFi et antennes

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 :

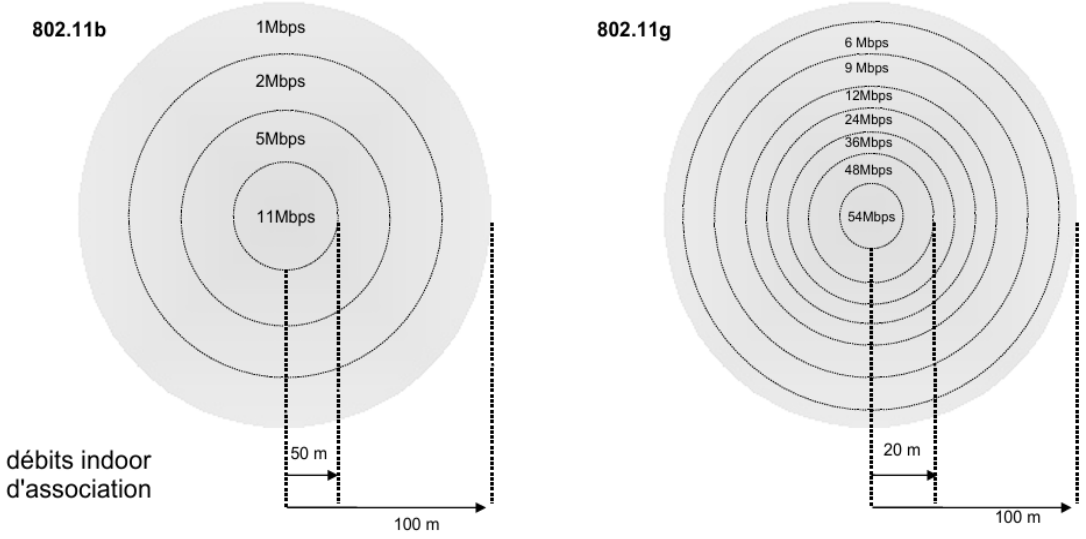
- Type N
  - La connectique d'antenne standard
- Type TNC-RP
  - Utilisée par les constructeurs Cisco et Linksys
- Type SMA
  - Répandue sur les cartes PCI et le matériel Dlink
- Type MMCX
  - Dédiées aux sorties mini-PCMCIA

Chapitre 4 : Matériel – Liens entre portée, débit et puissance

Débits et propagation d'ondes WiFi

Débit d'association :

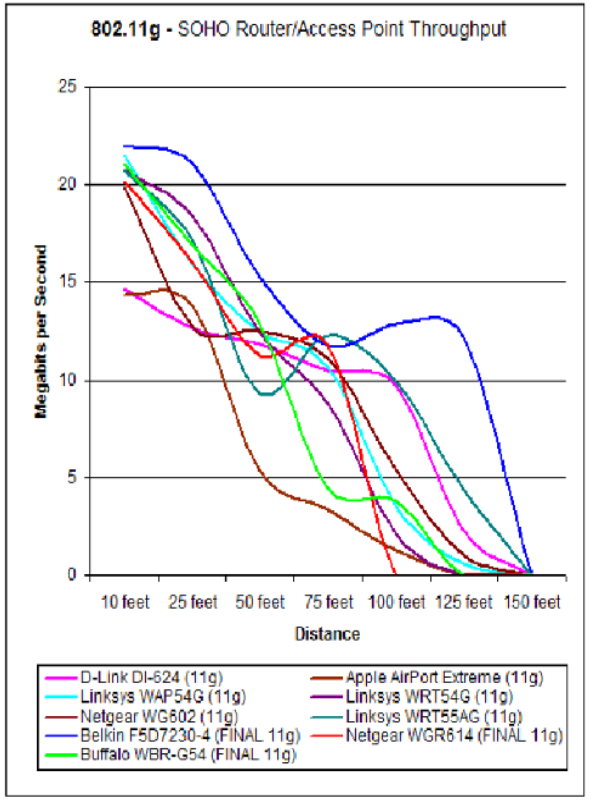
- Variable : 54 - 48 - 36 - 24 - 12 - 11 - 5,5 - 2 - 1 Mbit/s
- Adapté automatiquement en fonction
  - de la puissance reçue par l'appareil (distance)
  - du rapport Signal/Bruit (qualité du signal)

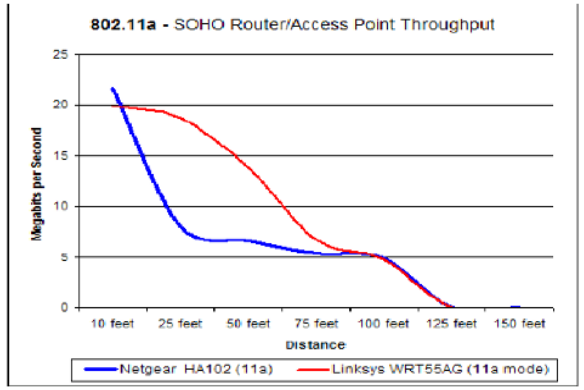


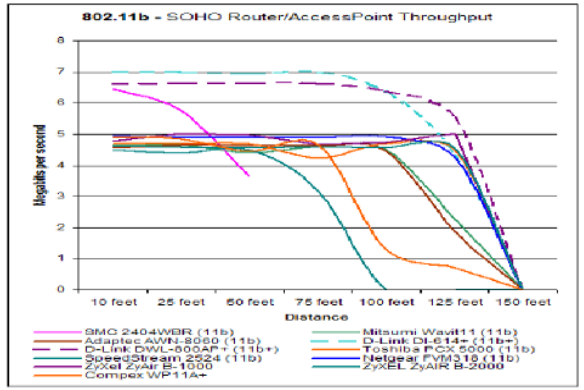
débits indoor d'association

Débits effectifs :

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



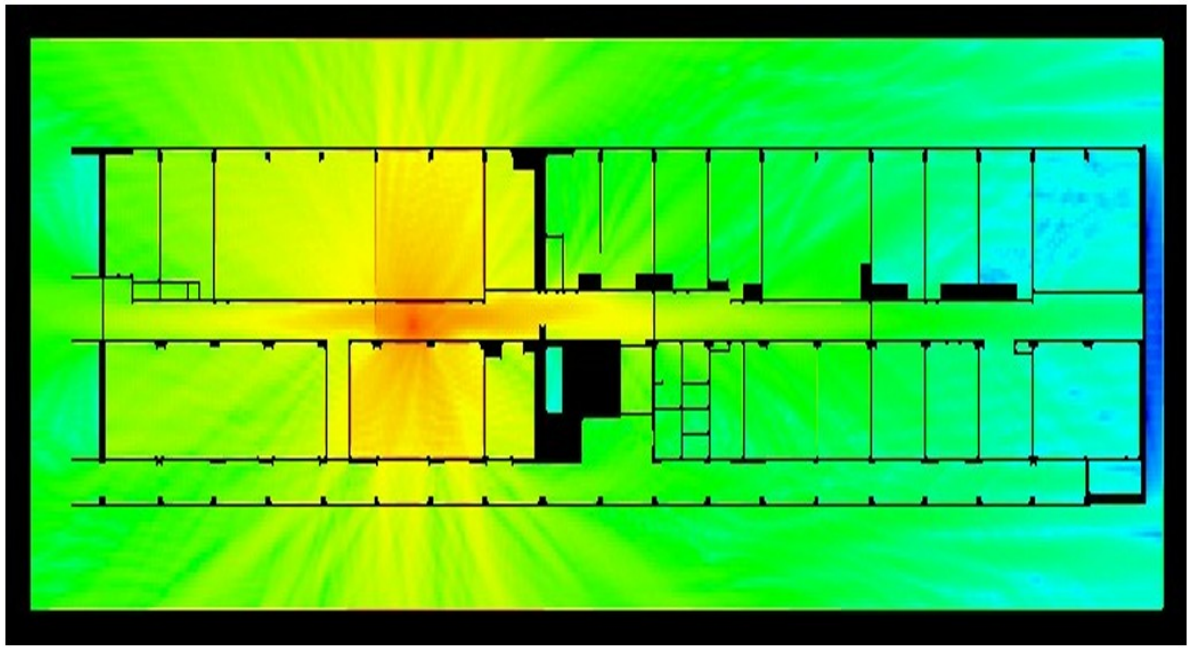




Chapitre 4 : Matériel – Liens entre portée, débit et puissance

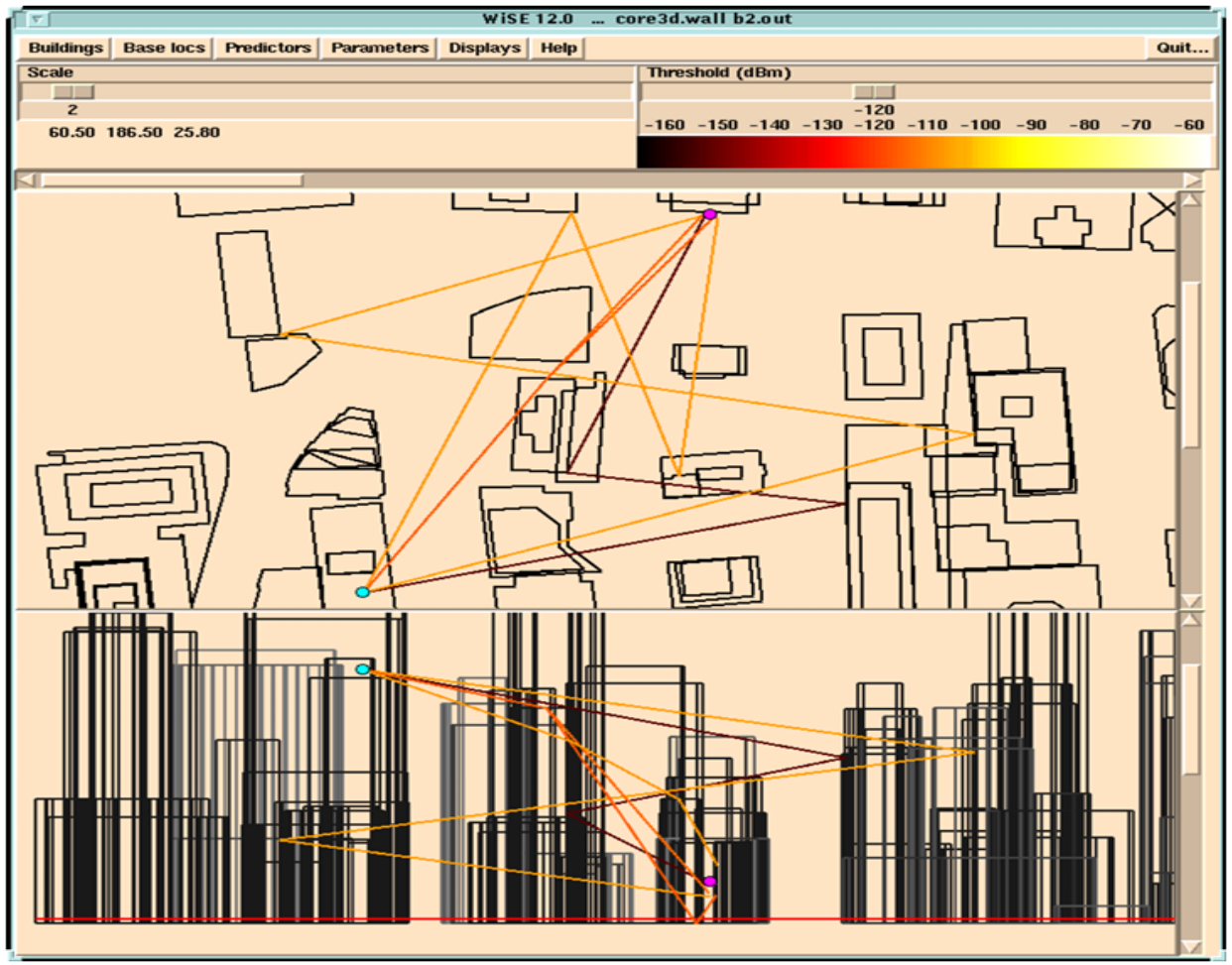
Débits et propagation d'ondes WiFi

Propagation des ondes en indoor :



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

Propagation des ondes en milieu urbain :



Chapitre 4 : Matériel – Liens entre portée, débit et puissance

Débits et propagation d'ondes WiFi

Calcul de la PIRE :

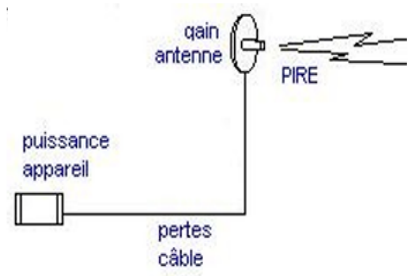
- La PIRE est la puissance effective rayonnée en sortie d'antenne.
- Elle est limitée à 100 mW à l'extérieur (et à l'intérieur) en France : 100 mW = 20 dBm
- Compter 1 dB par mètre en moyenne pour les pertes.

PIRE (dBm) =

puissance en sortie AP (dBm)

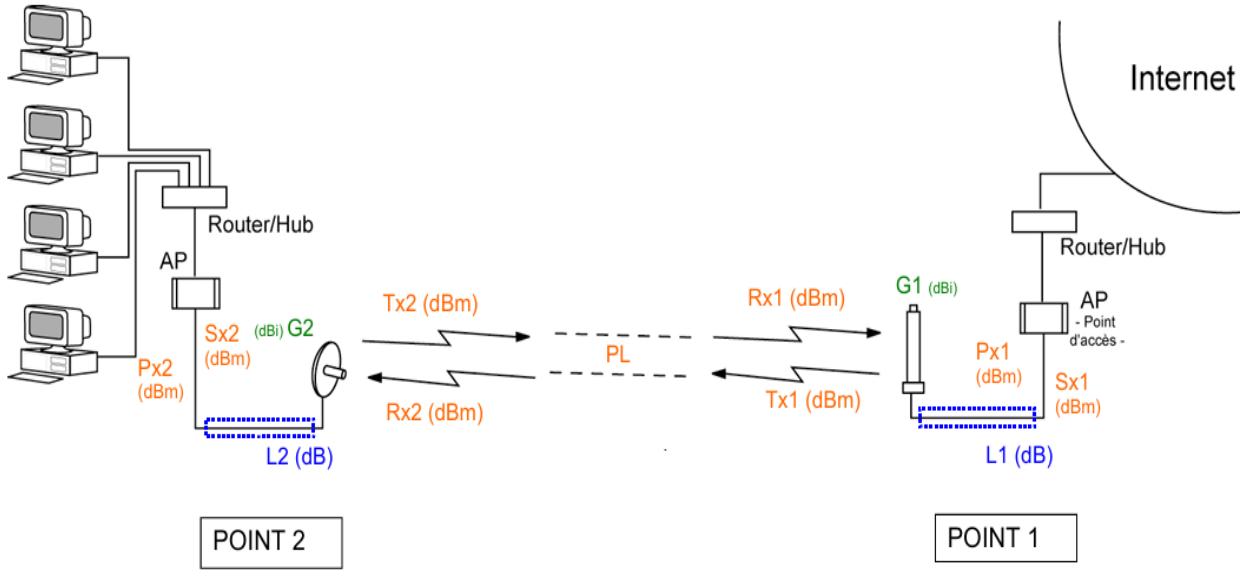
± pertes câbles (dB)

+ 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 sensibilités 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.



Débits et propagation d'ondes WiFi

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).

Fin du chapitre 4

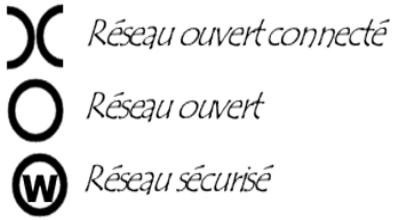
PLAN DU COURS

Chapitre 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 défaut
  - AP temporaires laissés en marche à l@nsu des resp. IF
- Le War-Driving
  - Un repérage des réseaux urbains accessibles :



Attaques possibles :

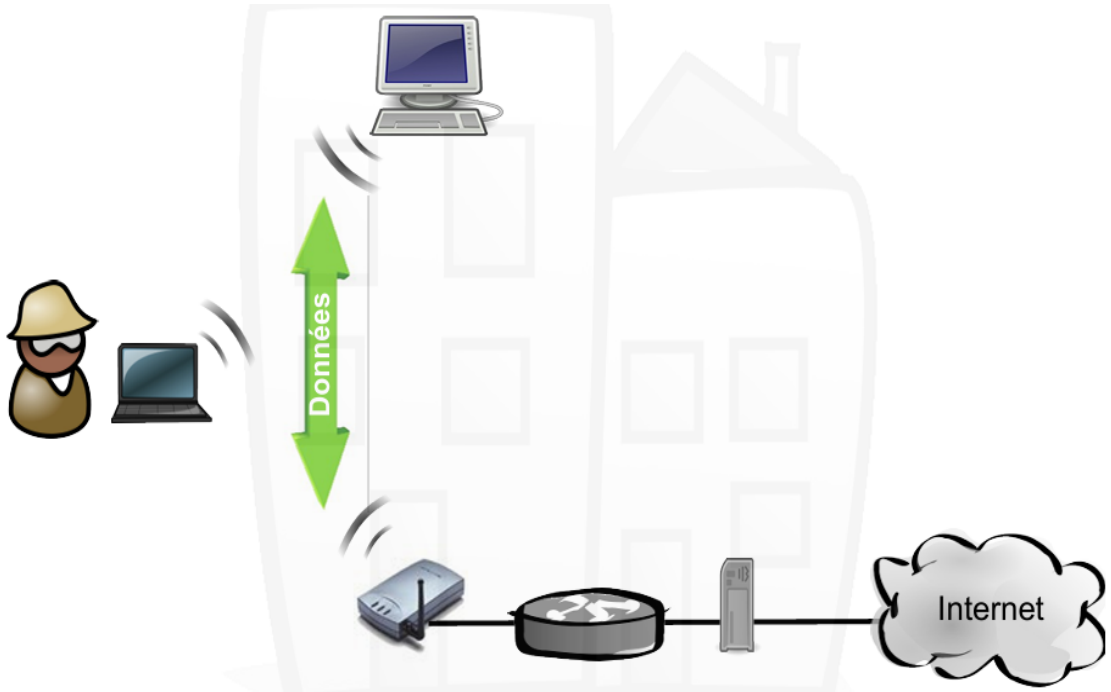
- L'écoute des données
- L'écoute des données
- L'intrusion et le détournement de connexion
- L'intrusion et le détournement de connexion
- L'occupation de la Bande Passante
- Le brouillage des transmissions
- Le déni de service.

Voir : http://www.nanteswireless.org/pages/wiki/index.php?pagename=WarDriving

Les risques

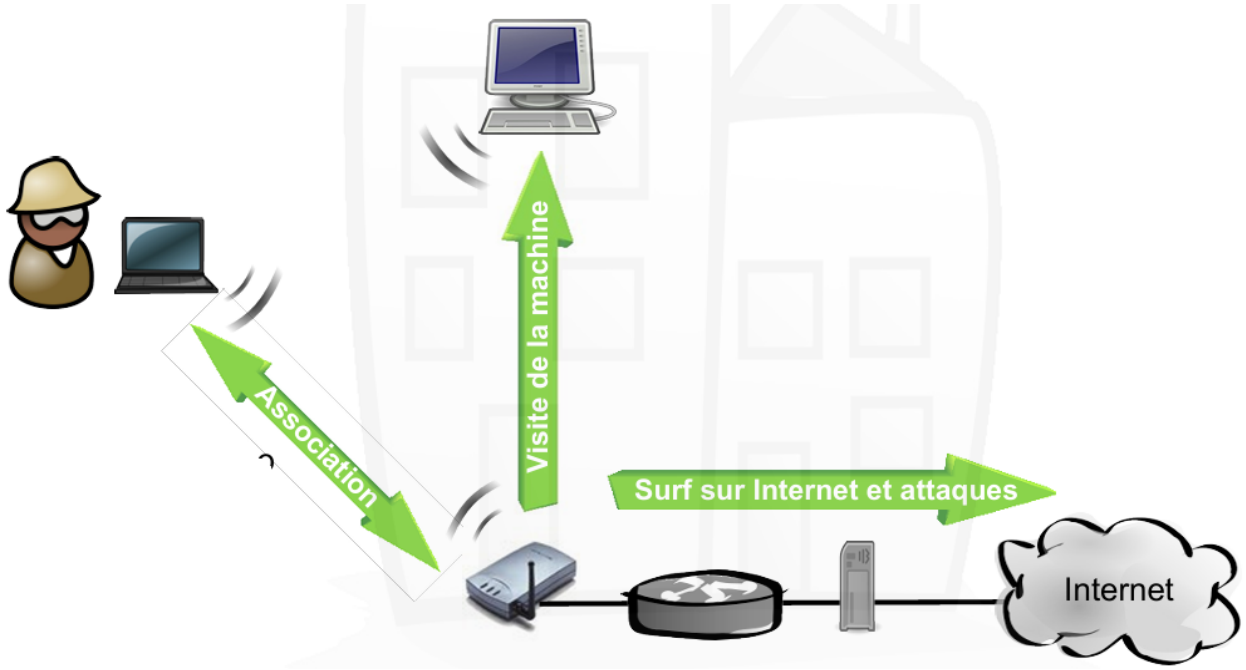
L'écoute des données :

- Solution efficace : le chiffrement (ou cryptage) des données.



L'intrusion et le détournement de connexion :

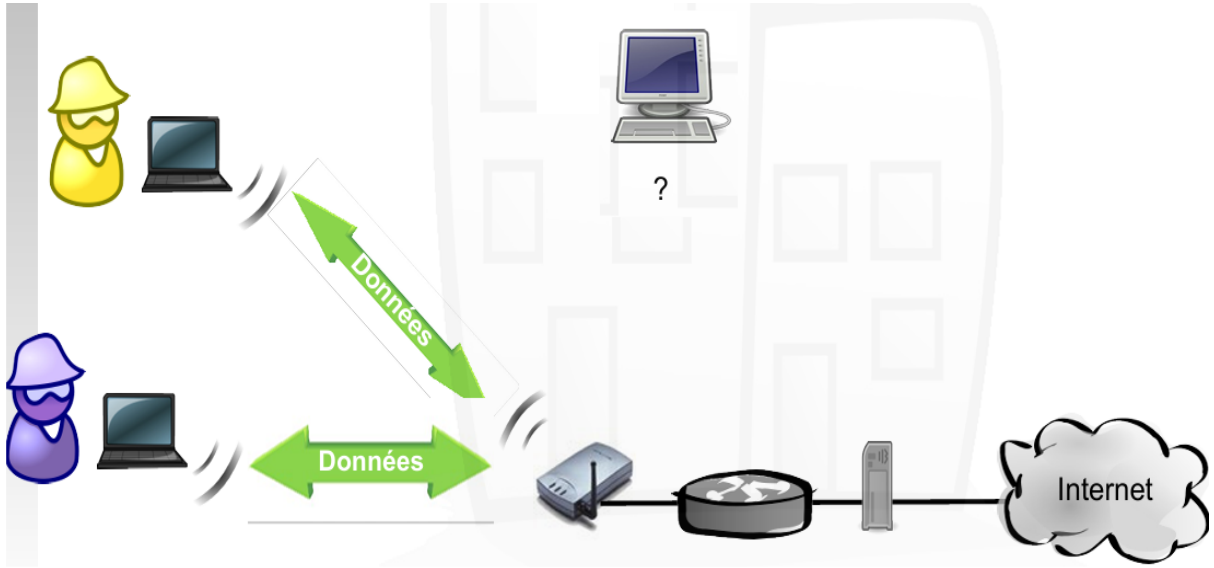
- Solution efficace : restreindre l'accès radio; restreindre l'accès réseau; authentifier la personne.
- Nécessite : une configuration radio-SSID; une configuration réseau-@IP/passerelle/DNS compatibles.



Les risques

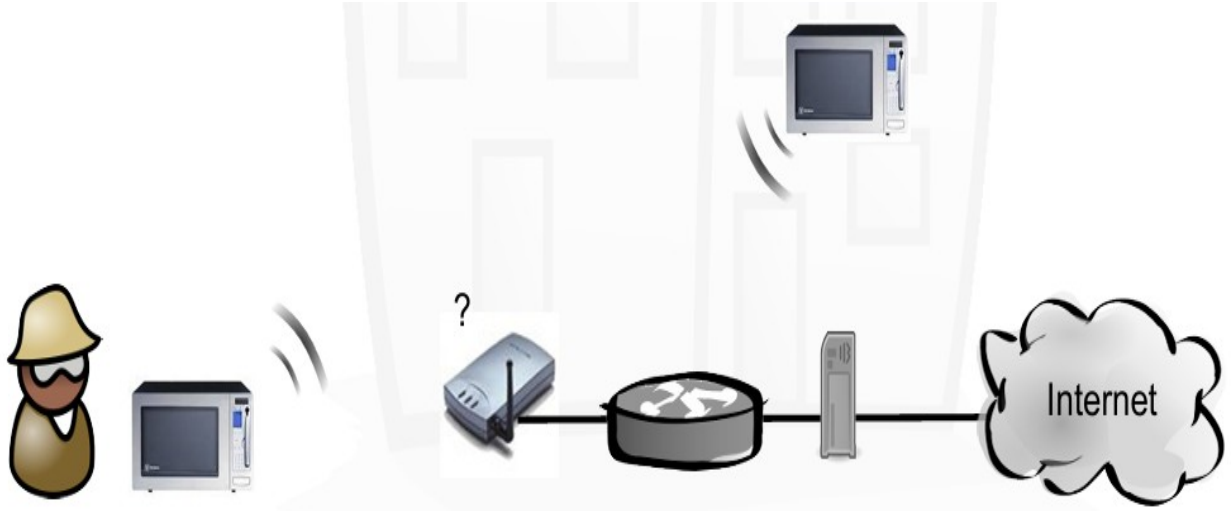
L'occupation de la bande passante :

- Echange de fichiers lourds bloquant la bande passante de l'utilisateur principal (importante de l'upload)
- Prérequis et solutions : identiques.



Le brouillage de transmission :

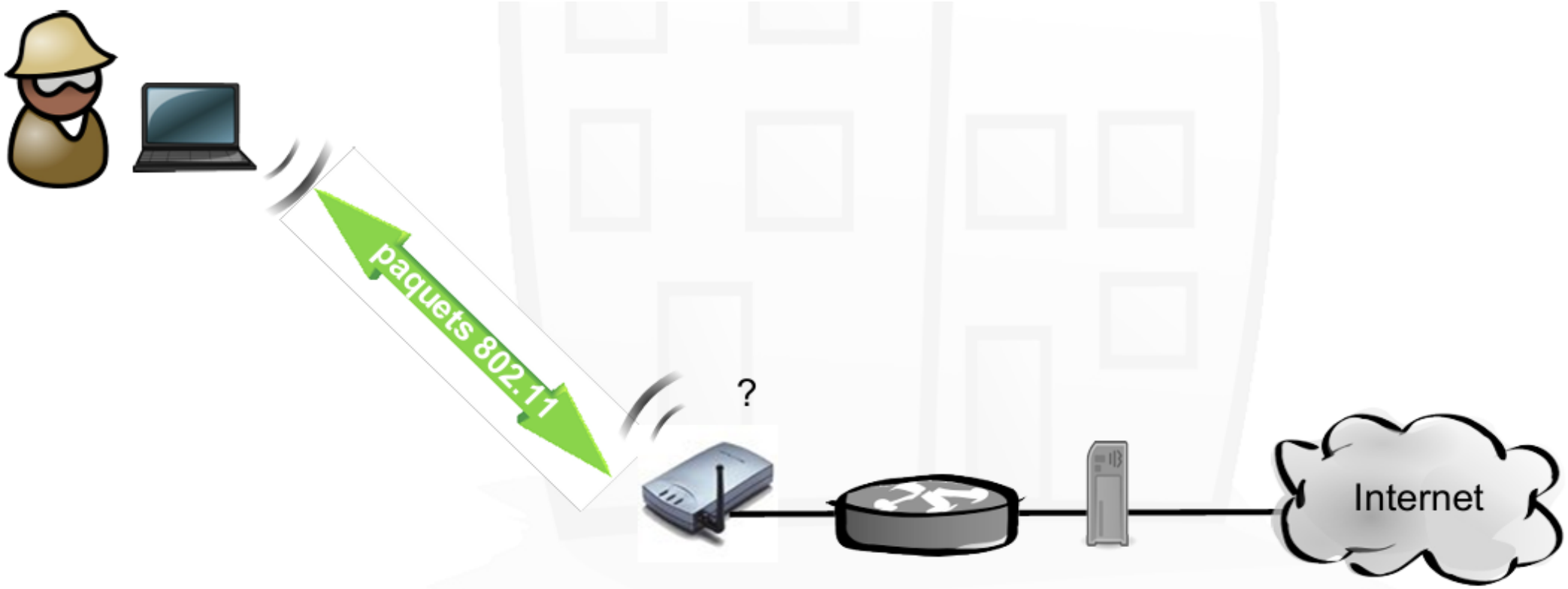
- Provenance : téléphones DETC, fours à micro-ondes
- Solution efficace : couper la source ou s'éloigner



Les risques

Le déni 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.



Chapitre 5 : Sécurité

Les solutions

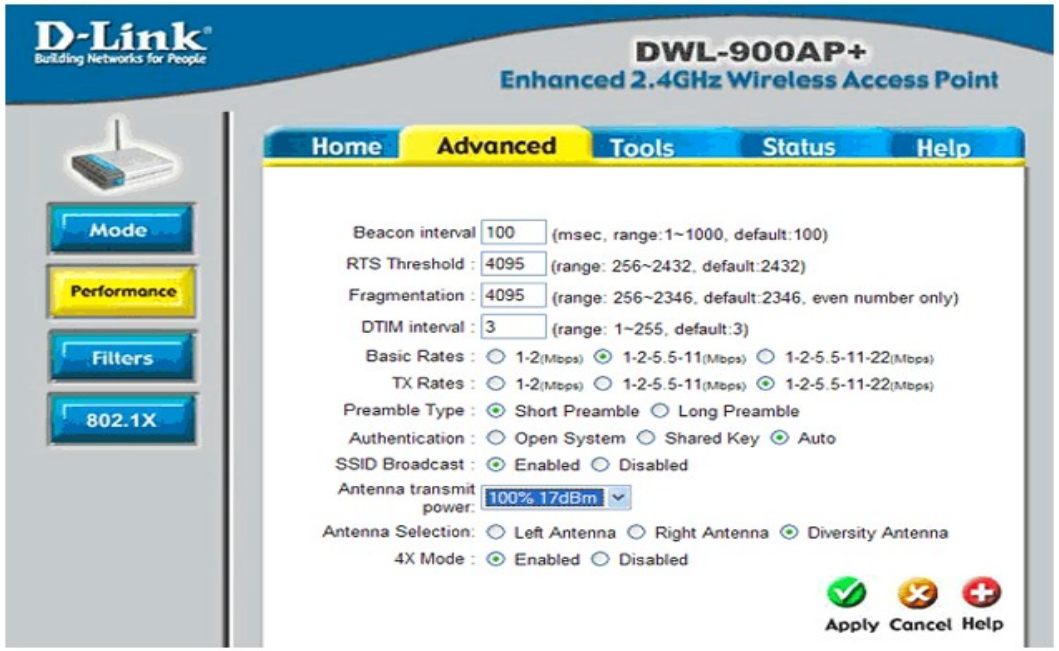
Une configuration radio adaptée :

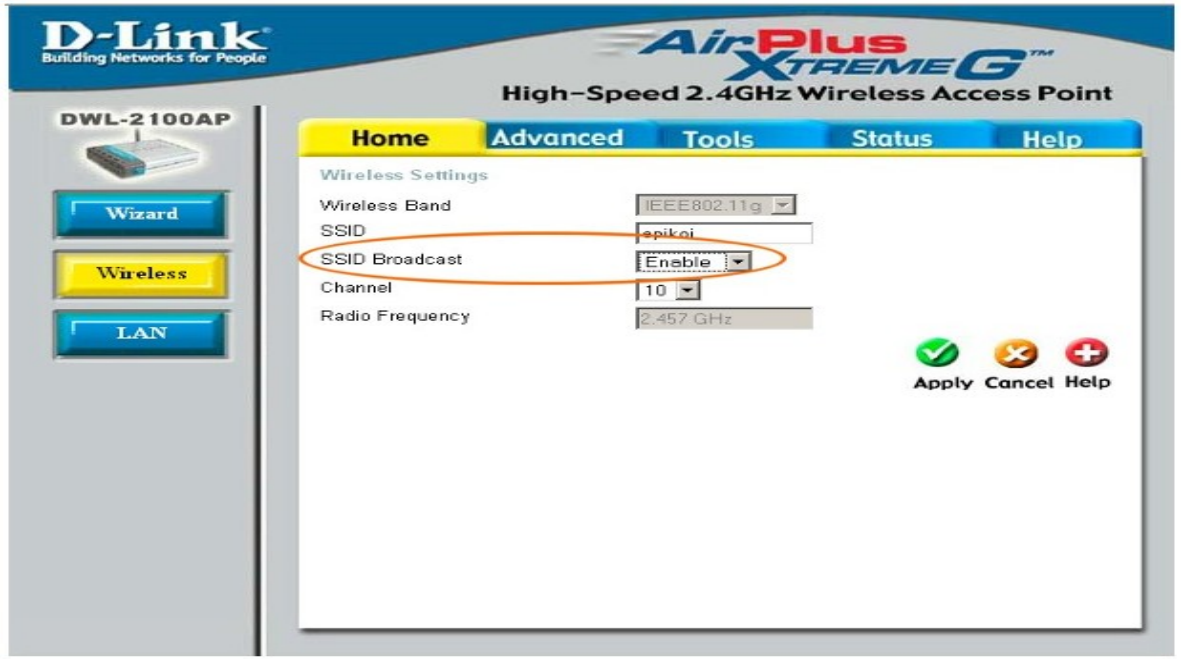
En fonction de la zone effective à couvrir :

- Positionner les points d'accès de manière optimale 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.



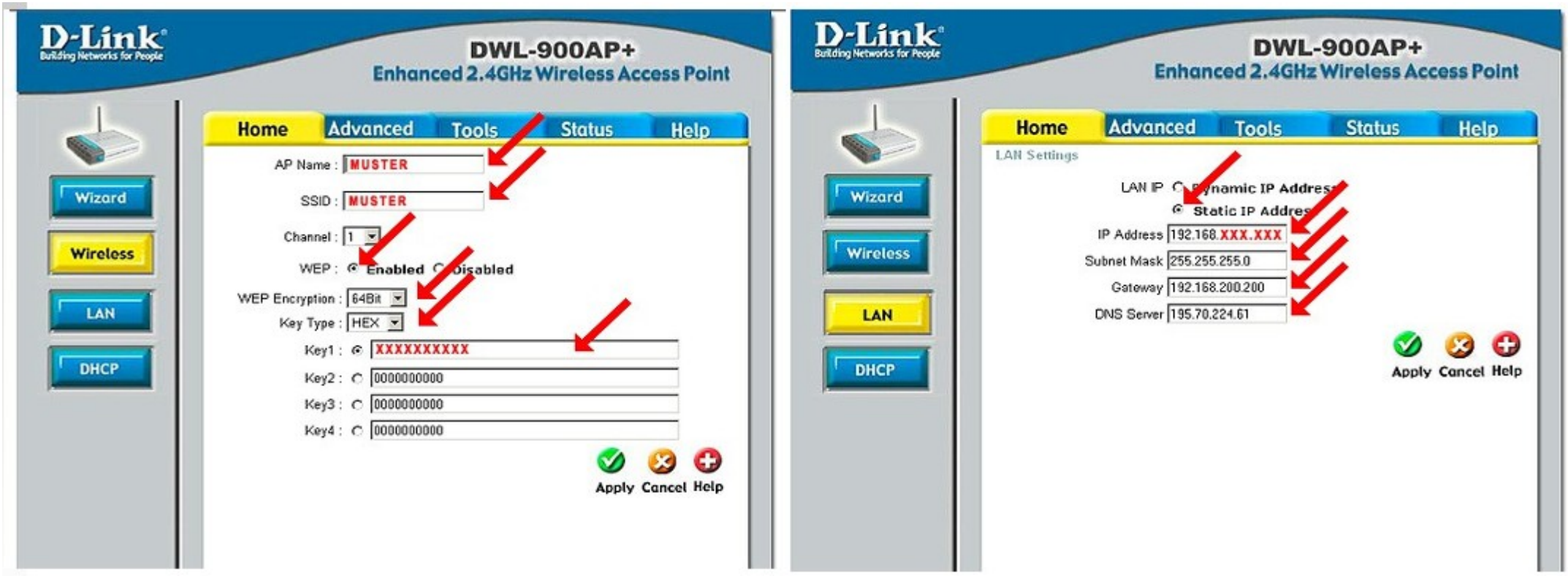


Chapitre 5 : Sécurité

Les solutions

Modifier les valeurs par défaut :

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

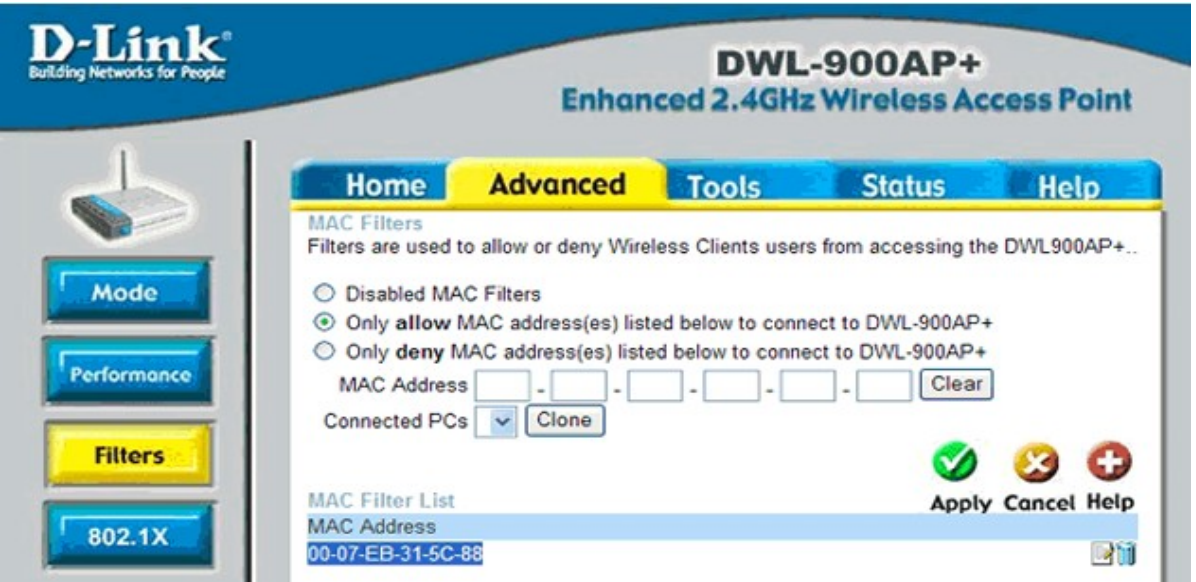


Chapitre 5 : Sécurité

Les solutions

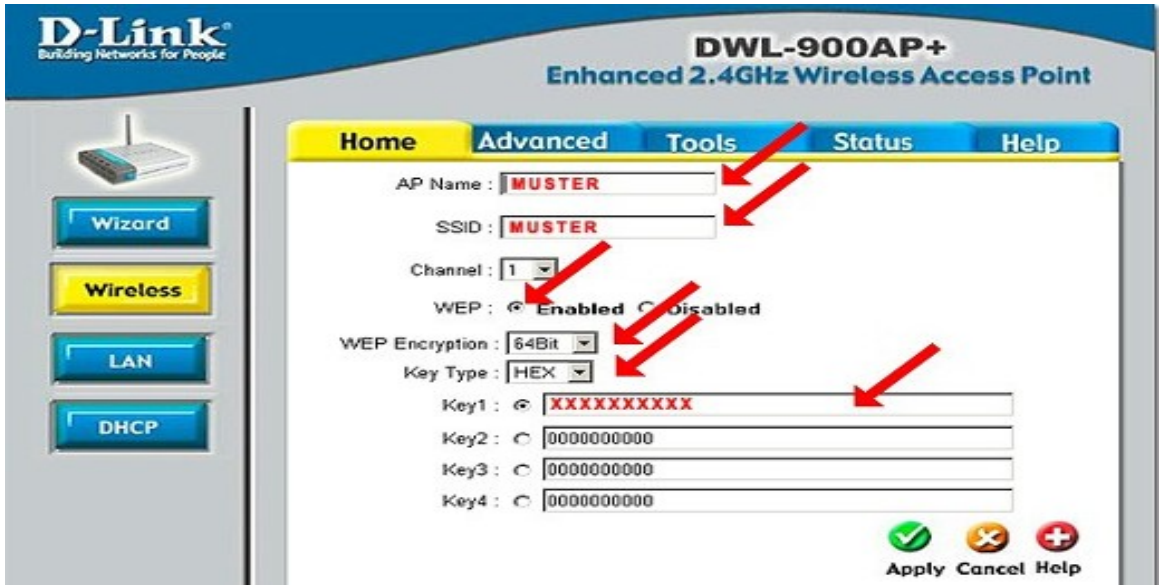
Filtrer les @MAC :

- 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 permet de casser une clef de 64 bits
  - Une capture d'un million de paquets permet de casser une clef de 64 ou 128 bits (faille algorithmique)
  - Nécessite d'être configurée sur l'AP et toutes les stations.

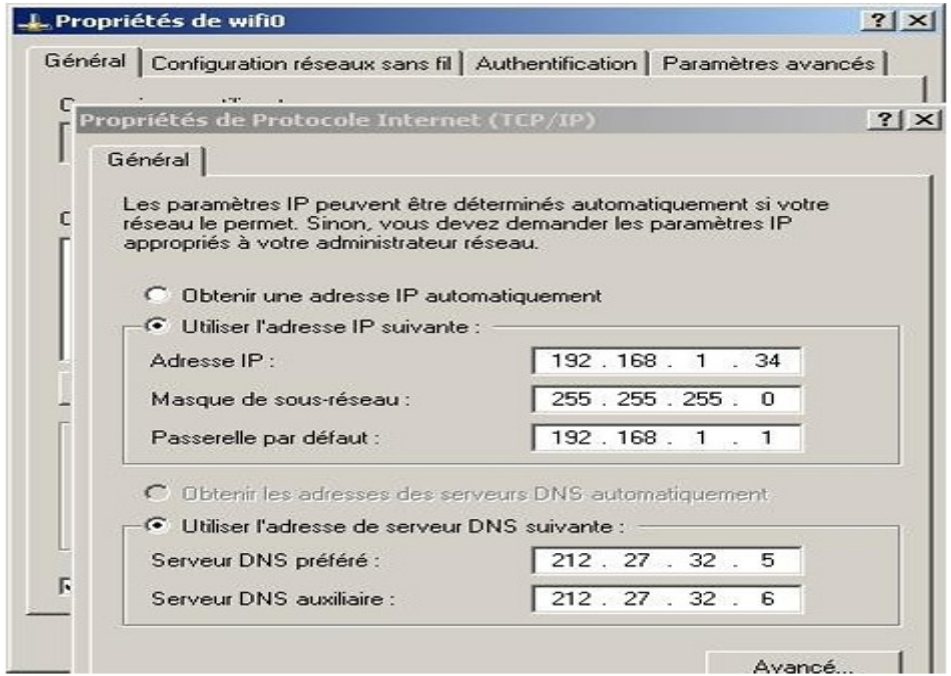


Chapitre 5 : Sécurité

Les solutions

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 :

- WiFi Protected Access (WPA et WPA2)
  - comble les lacunes du WEP
  - 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.

Chapitre 5 : Sécurité

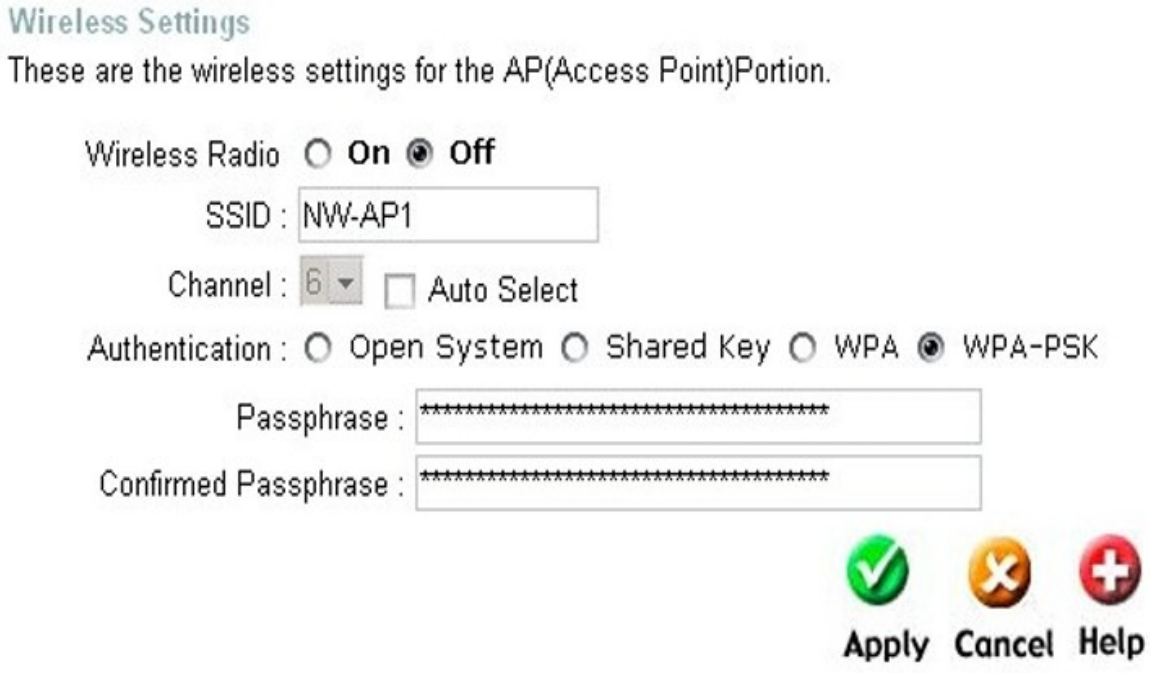
Les solutions

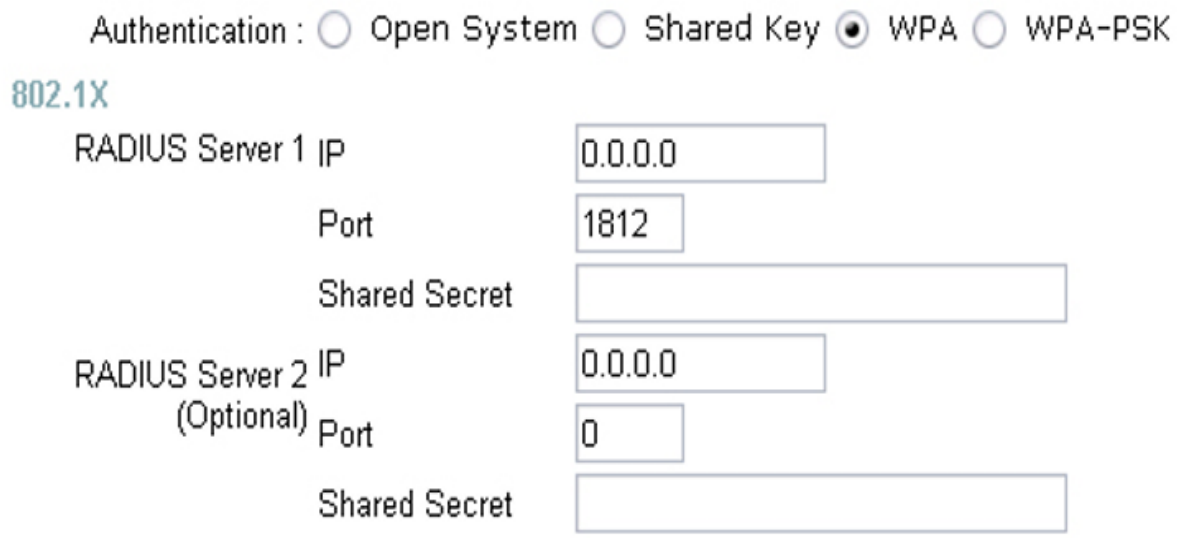
WPA – PSK (personnel) :

- 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).





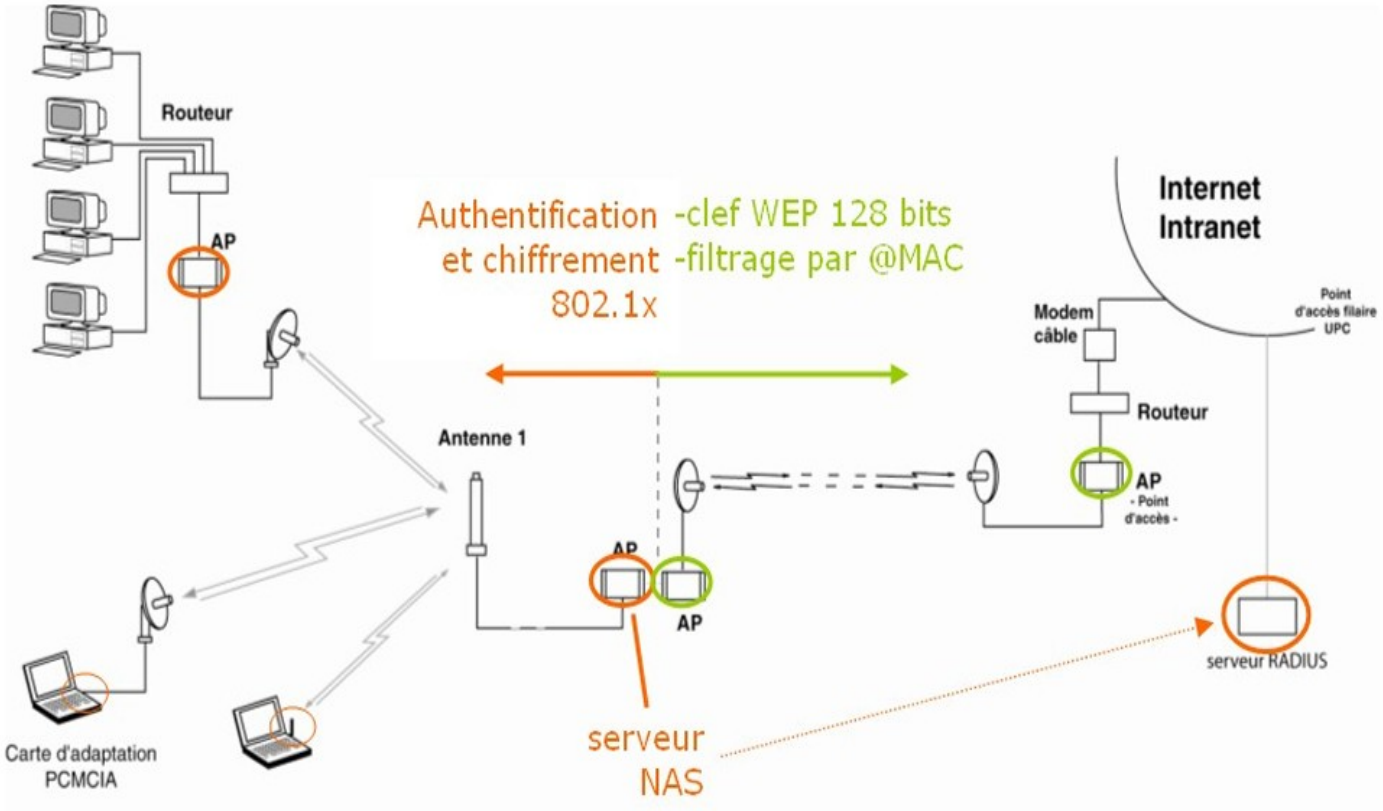
Chapitre 5 : Sécurité

Les solutions

WPA :

- 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 processus d'identification du WPA.
- Pour en savoir plus
  - http://fr.wikipedia.org/wiki/WiFi_Protected_Access
  - http://reseau.erasme.org/rubrique.php3?id_rubrique=15
  - http://www.freeradius.org/

Un exemple de sécurisation complet :



Les solutions

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

Fin du chapitre 5

PLAN DU COURS

Chapitre 6 : Déploiement d'un réseau sans fil

Méthodologie et analyse des besoins

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, leur 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 et dimensionnement

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, rayonnements ...)
  - 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
  - WiFi
    - 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

Chapitre 6 : Déploiement d'un réseau sans fil

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.

Aspects juridiques

Le cadre réglementaire pour les RLAN en 2,4 GHz

Usage privé

Ex : Réseau d'une entreprise, usage domestique

- **Pas de licence nécessaire**
- **Conditions techniques des décisions*, variables selon les départements**

Offre de services au public

Raccordement direct des bornes à un réseau public existant

Ex : Cybercafé, partage d 'accès

Etablissement d'un réseau pour relier les bornes RLAN

- **Licence expérimentale gratuite**
  - **Conditions techniques des décisions* variables selon les départements**
  - **Conditions techniques dérogatoires ** identiques dans tous les départements**
  - **Examen au cas par cas par la Défense**

Ex : Aménagement d'un centre d 'affaires

Ex : Projet de développement local

* Détaillées dans le communiqué de presse du 7 novembre 2002

** Puissance rayonnée (PIRE) de 100 mW en extérieur et en intérieur

Chapitre 6 : Déploiement d'un réseau sans fil

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 microondes : 1 kW ;
  - émetteur de la tour Eiffel : 6 MW
- La puissance d'un champ électromagnétique 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 radiofréquences 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

Fin du chapitre 6

PLAN DU COURS

Aspects sanitaires

Voici comment obtenir Cisco Packet Tracer et l'installer sur votre ordinateur :

Etape 1 : Créer un compte sur Cisco Networking Academy (NetAcad)

1. Rendez-vous sur : https://www.netacad.com/
2. Cliquez sur "S'inscrire" ou "Sign up".
3. Créez un compte gratuit (vous pouvez choisir "Self-paced courses").
4. Inscrivez-vous à un cours gratuit qui donne accès à Packet Tracer (ex. "Introduction to Packet Tracer").

Etape 2 : Télécharger Packet Tracer

1. Une fois connecté sur NetAcad :
   - Allez dans votre tableau de bord.
   - Accédez au cours "Introduction to Packet Tracer".

Etape 2 : Télécharger Packet Tracer (suite et fin)

2. Dans le premier module, vous verrez le lien de téléchargement : Choisissez la version correspondant à votre système d'exploitation (Windows, macOS, Linux).

Etape 3 : Installer Packet Tracer

1. Téléchargez le fichier d'installation.
2. Lancez l'installateur et suivez les instructions.
3. Une fois installé, connectez-vous avec votre compte NetAcad lors du premier lancement.

Remarque importante :

- Packet Tracer est gratuit pour les apprenants via NetAcad.
- Actuellement, la version la plus récente est la 8.x.

Chapitre 7 : Travaux pratiques

En cours de construction

Fin du chapitre 7