# Introduction à la sécurité du WiFi

Guillaume Duc
<guillaume.duc@guiduc.org>

Association Brest Wireless

20/05/2006

# Informations

- Copyright © 2006 Guillaume Duc
- Présentation placée sous licence Creative Commons Paternité 2.0 France dont les détails sont disponibles à l'adresse `http://creativecommons.org/licenses/by/2.0/fr/`
- Transparents disponibles à l'adresse `http://www.guiduc.org/cours/misc/wifi/intro-securite.pdf`
- Petit rappel : Il est interdit de pirater un réseau WiFi dont on n'est pas le propriétaire. Les outils de piratage cités dans ce document ne doivent être utilisés qu'avec l'accord explicite du propriétaire du réseau visé

# Plan



# Plan



# Qu'est-ce que la sécurité ?

- Plusieurs aspects à prendre en compte :
  - Confidentialité
  - Intégrité
  - Authentification
  - Disponibilité
  - Traçabilité...

# Confidentialité

- Empêcher une personne non autorisée d'écouter une communication
- Problème du WiFi : Ondes radio qui peuvent être captées par n'importe qui à distance
- Solution : Chiffrement (WEP, WPA)

# Intégrité

- Empêcher une personne non autorisée de modifier le contenu d'une communication
- Problème du WiFi : Ondes radio qui peuvent être facilement perturbées à distance
- Solution : Contrôle d'intégrité (CRC pour le WiFi normal et pour le WEP, Michael ou AES CCMP pour WPA/WPA2)

# Authentification

- S'assurer le l'identité des entités qui communiquent
- Problème du WiFi : Tout le monde peut émettre (y compris à distance), d'où la nécessité de vérifier l'identité des stations
- Solutions :
  - WEP : Partage d'un secret commun (la clé)
  - WPA : Partage d'un secret commun (PSK) ou authentification via norme 802.1x

# Disponibilité

- S'assurer que la communication est possible dès que l'on en a besoin
- Problème du WiFi : Ondes radios qui peuvent être facilement brouillées
- Solution : aucune. . .

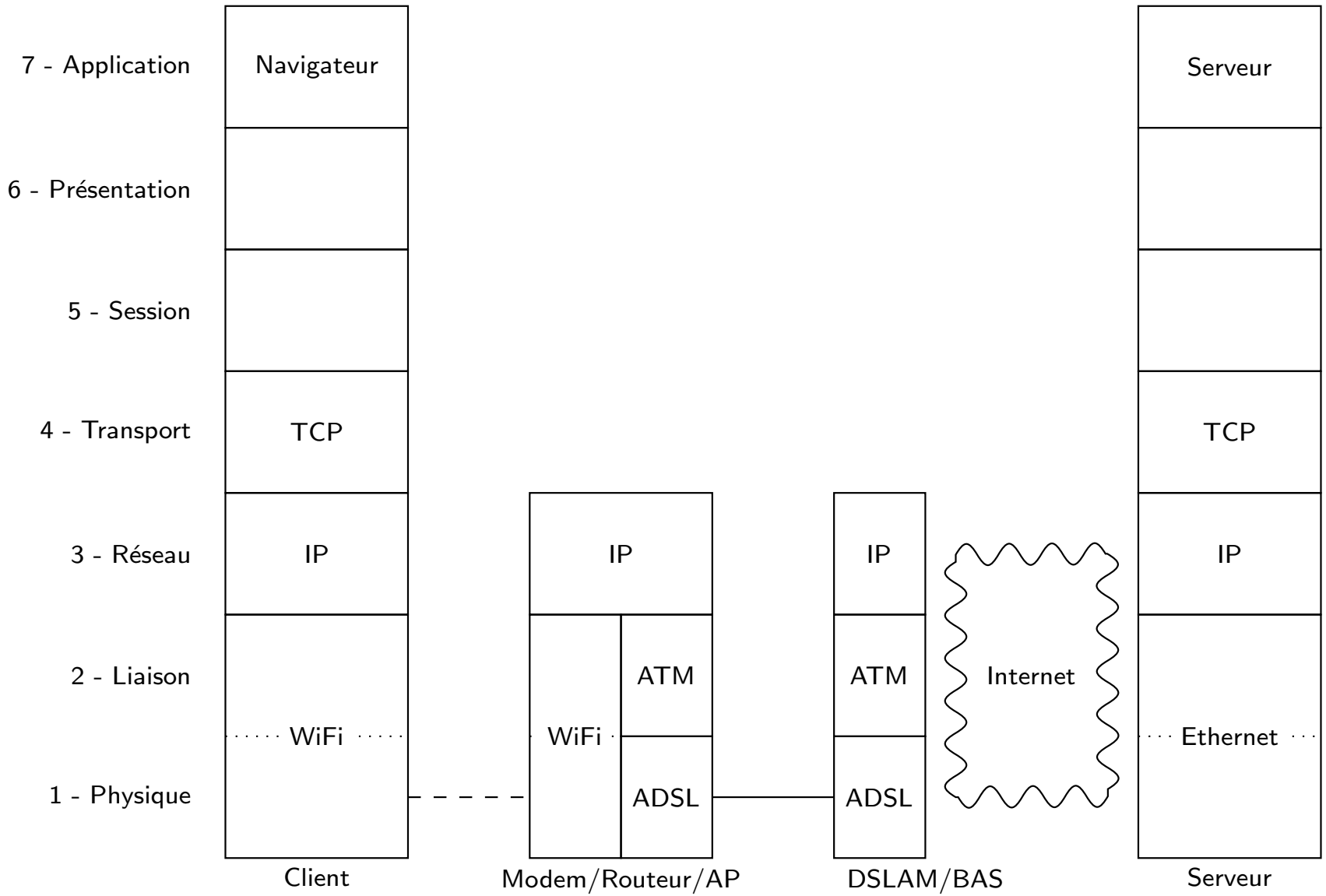
# Traçabilité (Audit)

- Pouvoir, *a posteriori*, savoir tout ce qui s'est passé sur un réseau
- Pas liée directement au WiFi mais obligation légale de conserver un certain nombre d'informations liées aux connections Internet
- Difficile dans le cas où l'authentification n'est pas assurée ou si les ressources sont insuffisantes...

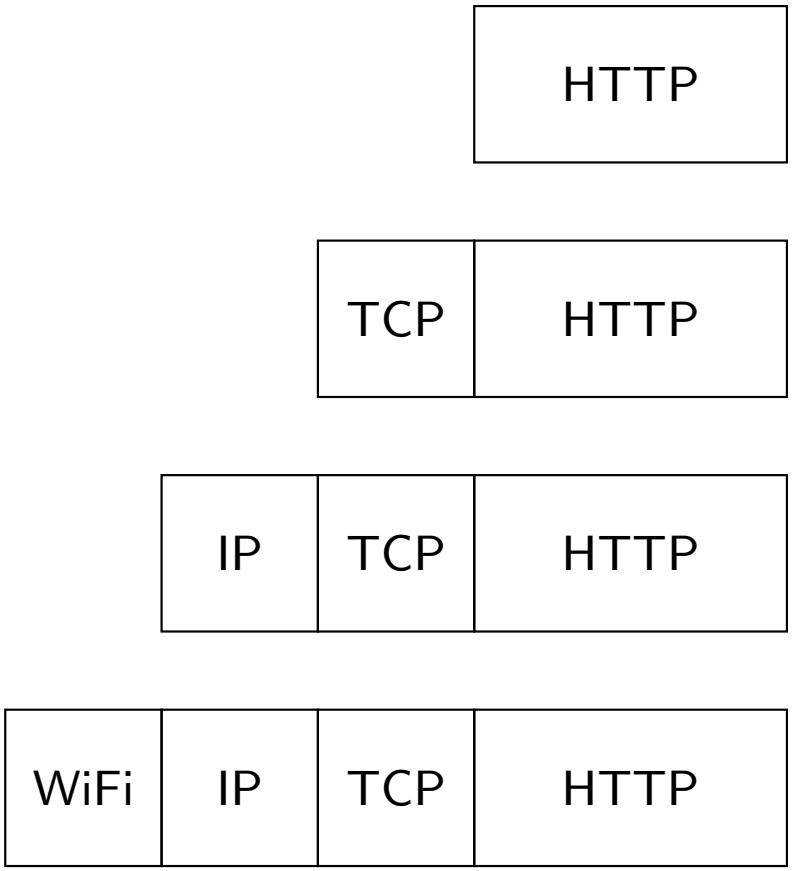
# Plan



# Quelques rappels de réseau



# Encapsulation



# Sécurité à quel niveau ?

- Niveaux 1-2 : WEP, WPA, IEEE 802.1x $\rightsquigarrow$ Sécurité uniquement au niveau de la liaison WiFi
- Niveau 3 : IPsec, VPN
- Niveaux 6-7 : SSL (HTTPS, SMTPS, *etc.*), SSH, *etc.* $\rightsquigarrow$ Sécurité de bout en bout
- Par la suite, nous nous concentrerons principalement sur la sécurité au niveau du WiFi (niveaux 1 et 2)

# Wired Equivalent Privacy (WEP)

- *Wired Equivalent Privacy* = Confidentialité équivalente au filaire
- Mécanisme intégré à la norme WiFi IEEE 802.11 (ratifiée en septembre 1999) afin de garantir un niveau de confidentialité équivalent à celui obtenue dans le cas d'un réseau filaire

# Plan



# Confidentialité 1/2

- Le WEP utilise l'algorithme de chiffrement de flux RC4
- Principe :
  - RC4 génère, à partir d'une clé de taille fixe, un flux de bits pseudo-aléatoires
  - Les données à chiffrer sont combinées (via un simple ou-exclusif) avec ce flux
  - À la réception, il suffit de combiner les données chiffrées avec le flux pseudo-aléatoire pour obtenir les données en clair
- Algorithme relativement sûr (il est l'un des algorithme standard utilisé par le protocole SSL) si bien utilisé

# Confidentialité 2/2

- Les clés de chiffrement utilisés sont composées de deux parties :
  - une partie fixe réellement secrète
  - un vecteur d'initialisation (IV), modifié à chaque paquet et transmis en clair
- Exemple :
  - WEP 64 bits : Clé fixe de 40 bits, IV de 24 bits
  - WEP 128 bits : Clé fixe de 104 bits, IV de 24 bits
  - WEP 256 bits : Clé fixe de 232 bits, IV de 24 bits

# Intégrité

- CRC (*Cyclic Redundancy Check*) calculé sur les données et ajouté avant chiffrement à la fin du paquet

# Authentification

- Deux modes d'authentification :
  - Ouvert (*open*) : Si le point d'accès arrive à déchiffrer les données, c'est que l'expéditeur connaît la clé
  - Restreint (*restricted*) : Le point d'accès envoie un challenge au client, qui le chiffre avec la clé et le renvoie. Si le point d'accès arrive à déchiffrer le challenge, c'est bon
  - $\rightsquigarrow$ Il n'y a pas d'authentification à proprement parlé

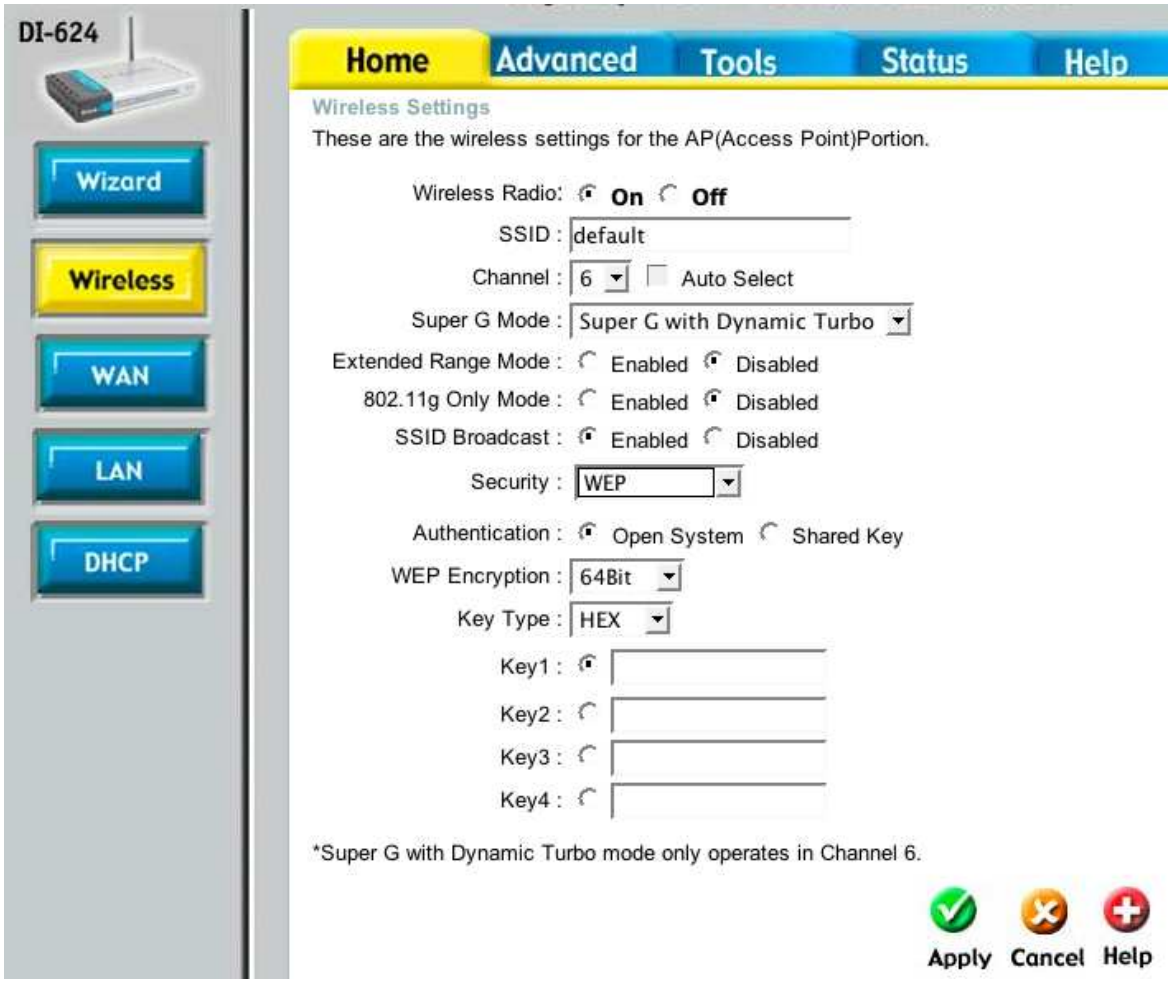
# Plan



# Saisie de la clé

- Il faut tout d'abord générer une clé puis la rentrer dans ses équipements WiFi
- Cette saisie peut se faire sous deux formes :
  - Sous forme hexadécimale (0-9 a-f) : 10 chiffres pour une clé de 40 bits, 26 pour une clé de 104 bits et 58 pour une clé de 232 bits
  - Sous forme d'un mot de passe qui est ensuite transformé en clé

# Exemple : DLink 624



# Exemple : Linksys WAP54G

# Exemple : Linksys WAP54G

# Plan



# Intégrité

- Le chiffrement RC4 et le CRC sont des opérations linéaires
- Il est donc très facile de modifier un paquet, sans connaître la clé, sans se faire détecter
- Cette faille est utilisée pour faciliter l'injection de trafic, qui permet d'accélérer les attaques suivantes

# Intégrité

- WEP est un protocole sans état
- Il est donc possible de rejouer un paquet sans être détecté, ce qui peut poser quelques problèmes

# Authentification

- La clé de chiffrement doit être connue par toutes les stations du réseau
- Or le partage de secret est toujours très compliqué (fuites possibles, problème lors de la sortie du groupe, *etc.*)
- De plus, on ne peut pas distinguer deux personnes qui connaissent la clé

# Confidentialité

- Mauvaise utilisation de l'algorithme RC4
- Deux paquets ne doivent jamais être chiffrés en utilisant la même clé
- Or il n'y a que l'IV qui change entre deux paquets. Cet IV fait 24 bits et donc en moyenne, tous les $2^{12} = 4096$ paquets, on obtient une collision, c'est-à-dire deux paquets qui sont chiffrés avec la même clé
- Lors d'une collision, on obtient des informations sur les données en clair. Si on arrive à obtenir les données en clair entièrement, on peut déchiffrer n'importe quel paquet chiffré avec le même IV
- D'autres attaques existent mais leur fonctionnement dépasse le cadre de cette introduction

# Outils

- AirSnort : l'un des premiers programmes qui implémente l'attaque Fluhrer-Mantin-Shamir (nécessite la capture de 5 à 10 millions de paquets)
- Aircrack : outil récent permettant de casser des clés beaucoup plus rapidement (au minimum 200.000 à 500.000 paquets)
- WepLab et WepAttack : permettent d'attaquer le mot de passe servant à générer la clé à l'aide d'un dictionnaire
- Wifitap : outil permettant de d'injecter du trafic rendant une attaque contre une clé WEP beaucoup plus rapide
- Auditor Security Collection : Live-CD contenant différents outils pour attaquer un réseau (le sien, pas celui de son voisin...)

# WiFi Protected Access

- WPA a été conçu par l'alliance WiFi afin de combler les failles du WEP en attendant la sortie de la norme IEEE 802.11i
- Les premiers équipements certifiés WPA sont apparus en avril 2003 et le WPA est devenu obligatoire en novembre 2003
- La norme 802.11i a été ratifiée en juin 2004 et la deuxième version du WPA (WPA 2) l'implémente.

# Plan



# Intégrité / WPA

- Utilisation de l'algorithme *Michael* (*Message Integrity Code*) qui est beaucoup plus sûr qu'un simple CRC
- Intégration d'un compteur permettant d'empêcher les attaques par rejeu

# Intégrité / WPA2

- Utilisation de l'algorithme de chiffrement AES en mode CCMP (Counter mode / CBC-MAC Protocol) permettant d'assurer l'intégrité en même temps que le chiffrement

# Authentification / WPA & WPA 2

- Deux modes d'authentification :
  - Clé pré-partagée (WPA Personnel), similaire au WEP
  - Authentification via un serveur suivant la norme 802.1x (WPA Entreprise), permettant une authentification forte via plusieurs mécanismes (nom d'utilisateur et mot de passe, carte SIM, *etc.*)

# Confidentialité / WPA

- Afin d'assurer la compatibilité avec le matériel existant, WPA utilise l'algorithme de chiffrement RC4 (comme le WEP)
- Cependant, le vecteur d'initialisation utilisé est beaucoup plus long (48 bits), et la partie fixe de la clé est renouvelée régulièrement à partir d'une clé principale grâce à l'algorithme TKIP (*Temporal Key Integrity Protocol*)
- Ainsi un attaquant n'a pas assez de temps pour capturer un nombre suffisant de paquet avant que la clé ne change

# Confidentialité / WPA2

- Utilisation de l'algorithme de chiffrement par bloc AES en mode CCMP (algorithme très robuste)
- Cet algorithme est également utilisé dans WPA1 mais sans garantie d'interopérabilité...

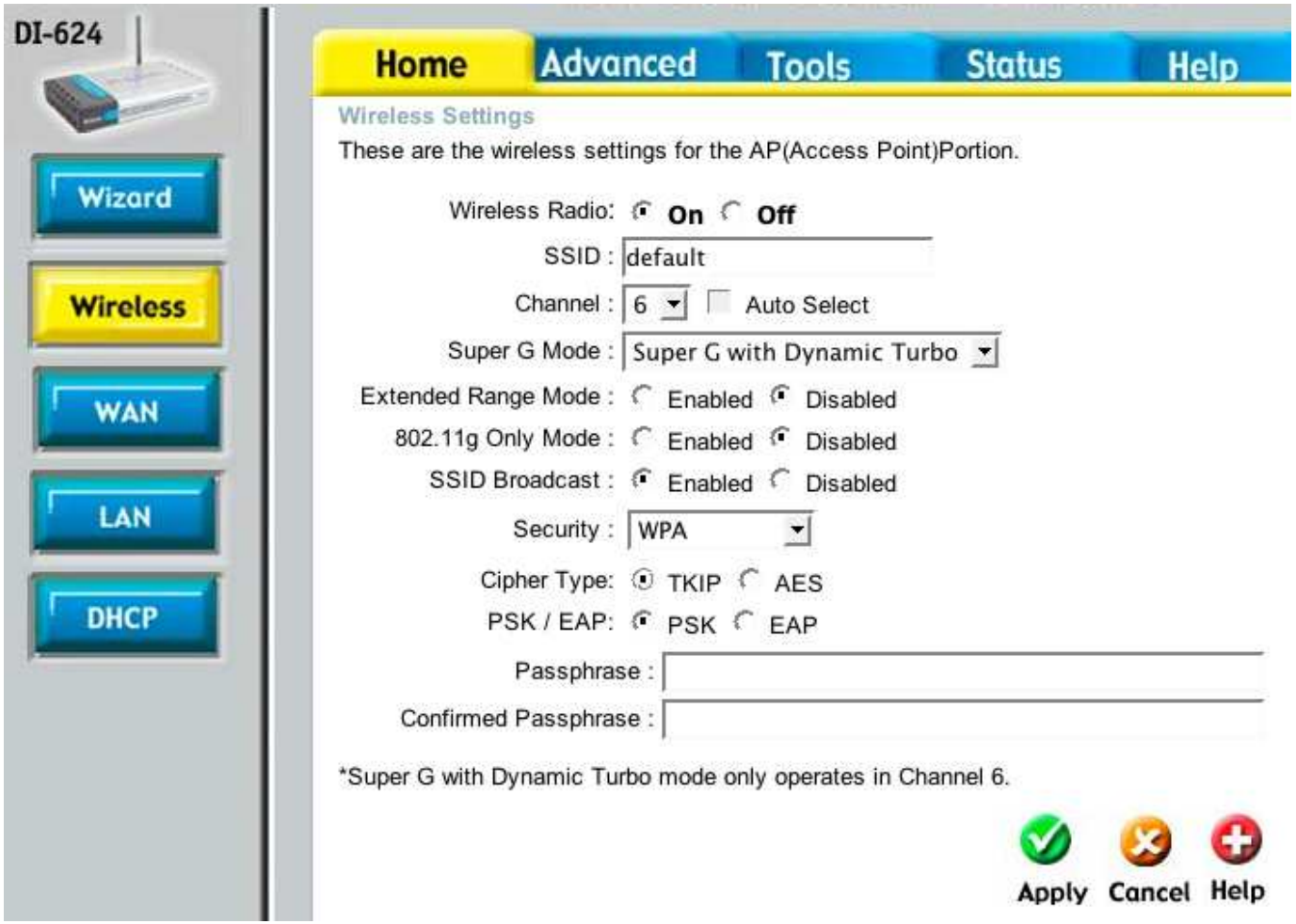
# Plan



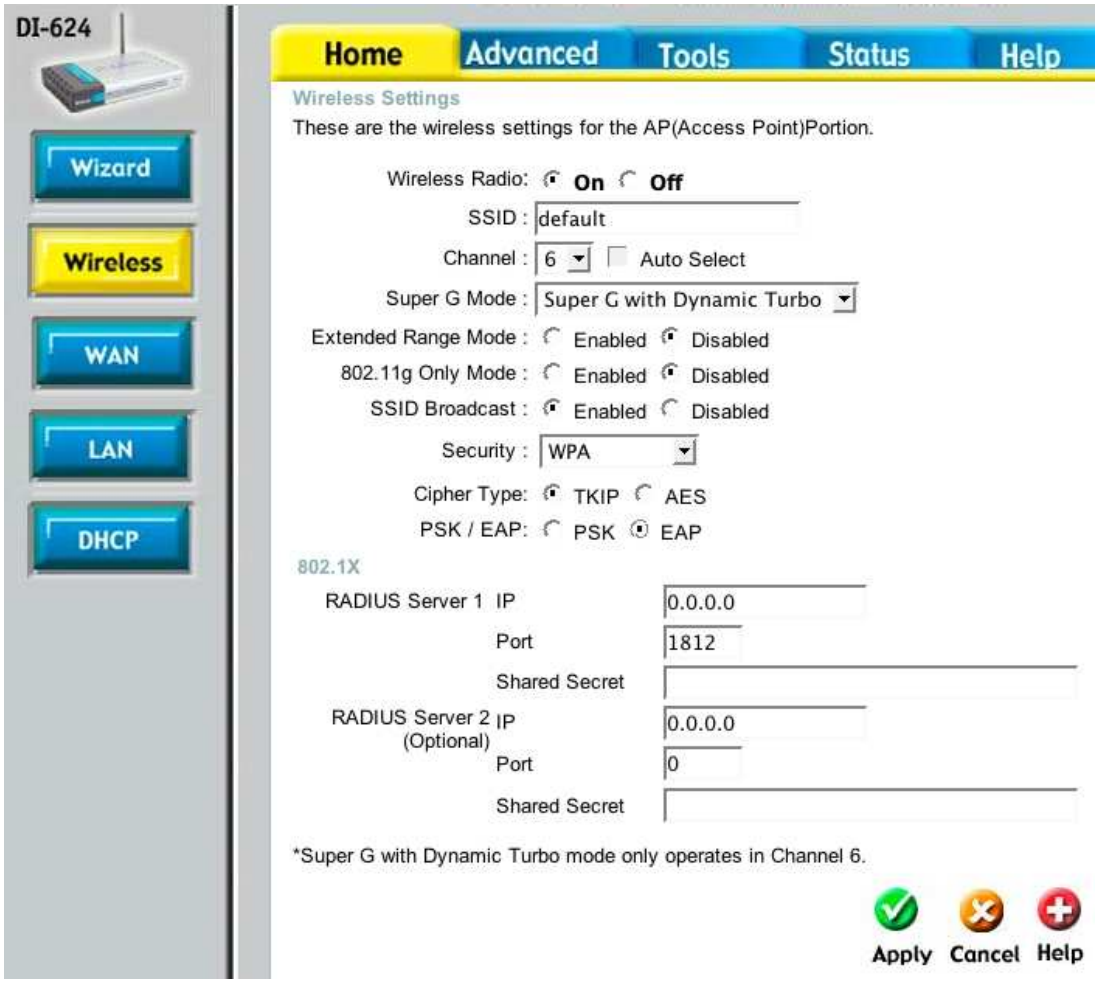
# Clé pré-partagée

- Saisie par mot de passe (8 à 63 caractères ASCII) ou directement (64 chiffres hexadécimaux)

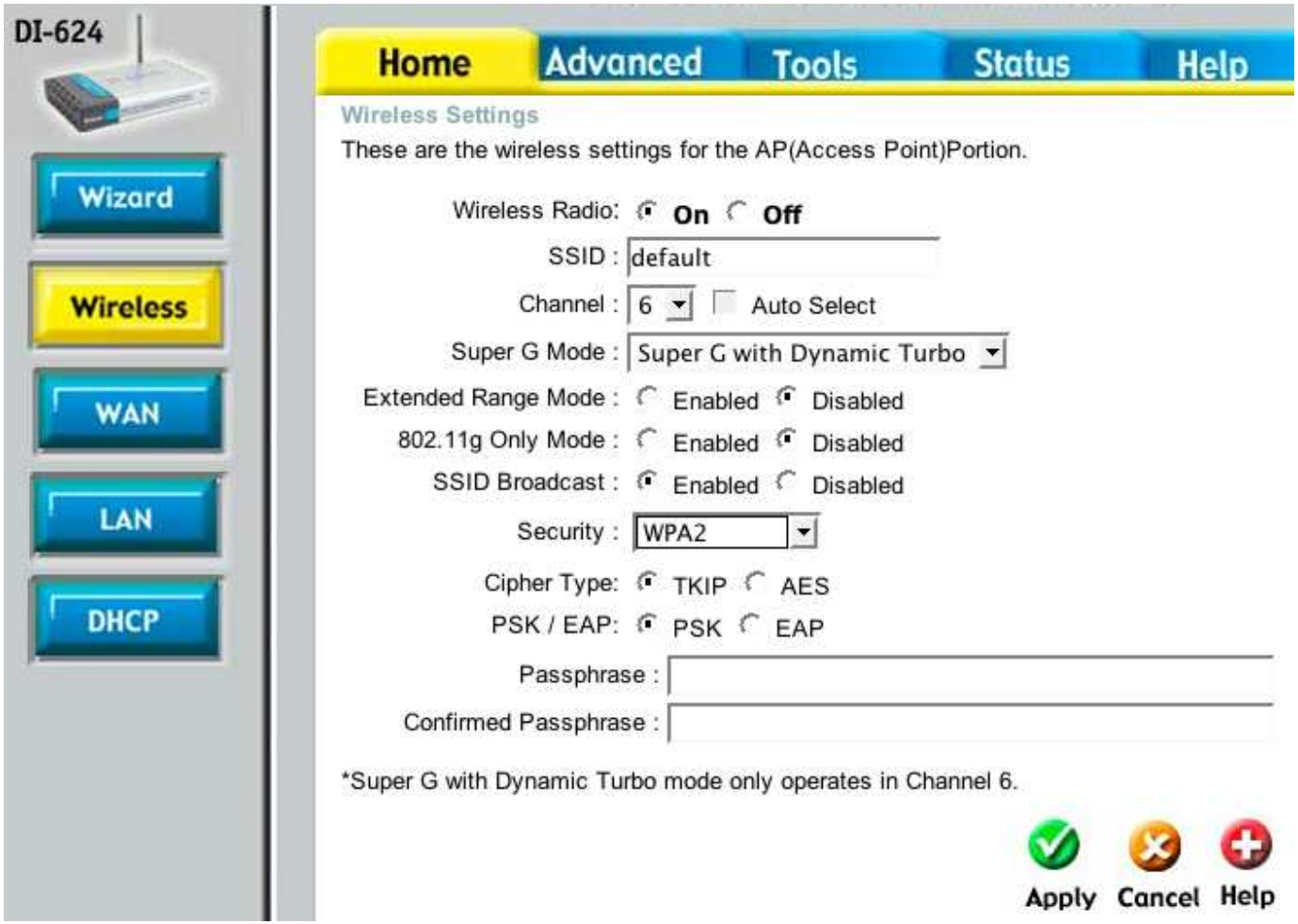
# Exemple : DLink 624



# Exemple : DLink 624

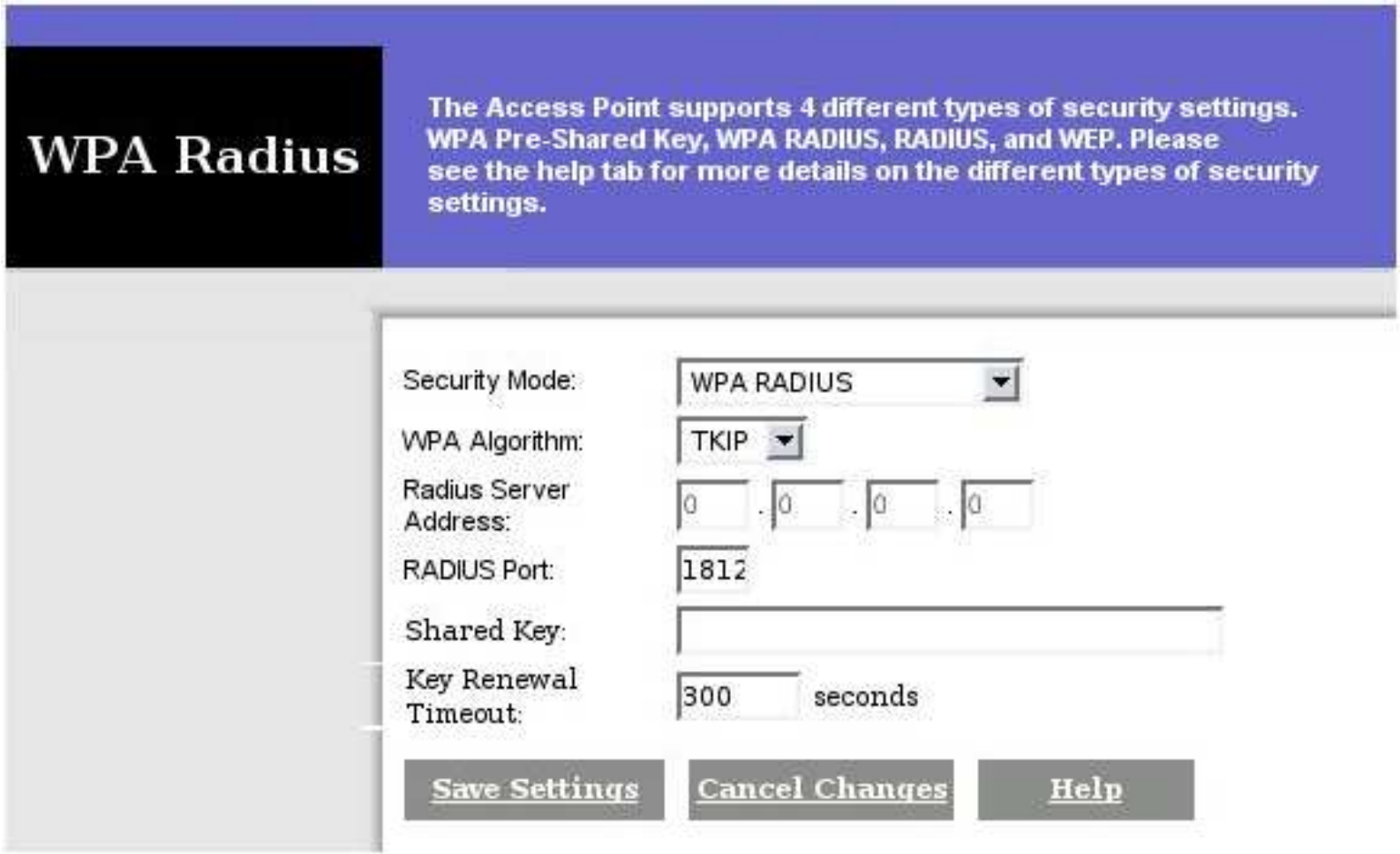


# Exemple : DLink 624



# Exemple : Linksys WAP54G

# Exemple : Linksys WAP54G



# Plan



# SecureEasySetup

- Développé par HP, Broadcom et Cisco (Lynksys)
- Permet de sécuriser très simplement son réseau avec du WPA
- Pour l'utilisateur :
  - Pression d'un bouton sur l'AP
  - Pression d'un bouton dans le logiciel sur le client
  - Et voilà...
- Par derrière, échange de la clé entre l'AP et le client de façon sécurisée (Diffie-Hellman)
- Problème : d'autres clients peuvent récupérer la clé durant les deux minutes suivant la pression du bouton...
- Mais c'est mieux que rien (au moins la sécurité est très simple à mettre en place)

# Plan



# Clé pré-partagée

- Si la clé pré-partagée est saisie via un mot de passe, une attaque par dictionnaire est possible si le mot de passe n'est pas assez fort et long (exemple sa date de naissance ou le prénom de sa petite amie)
- Solution : saisir la clé en mode hexadécimal de façon totalement aléatoire

# WPA / WPA2

- Sinon, WPA et WPA2 sont très robustes (pas d'attaques pratiques connues)

# Plan



# Filtrage par adresse MAC (*Medium Access Control*)

- Chaque carte WiFi (comme chaque carte Ethernet) dispose d'une adresse *à priori* unique sur 6 octets (48 bits), c'est son adresse MAC
- Cette adresse est souvent notée sous la forme : `XX:XX:XX:XX:XX:XX` où `X` est un chiffre hexadécimal
- Les points d'accès WiFi permettent souvent de définir une liste d'adresse MAC autorisées à se connecter ou au contraire interdites
- Cependant, il est assez simple de changer l'adresse MAC de sa carte et donc de contourner cette protection

# Plan



# Portail captif 1/2

- Permet d'authentifier les utilisateurs se connectant à un réseau WiFi
- Scénario :
  - L'utilisateur se connecte au réseau
  - Le point d'accès redirige toutes ses requêtes web vers un serveur d'authentification
  - Après avoir entré un nom d'utilisateur et un mot de passe valides, le point d'accès autorise alors le client (identifié par son adresse MAC ou son IP) à accéder à Internet

# Portail captif 2/2

- Exemples : WiFiDog, Chillispot, Talweg, NoCatSplash, *etc.*
- Sécurité :
  - Authentification : sûre si la communication entre le client et le serveur d'authentification est protégée par SSL (HTTPS)
  - Possibilité d'usurpation d'un client déjà connecté en usurpant son adresse MAC et/ou son adresse IP
  - N'assure pas, *à priori*, la confidentialité des échanges après l'authentification donc utiliser SSL ou VPN...
  - N'assure pas, *à priori*, la fonction d'audit : on peut savoir à un instant donné qui était connecté mais pas qui a fait quoi (difficile...)

# Plan



# IPsec / VPN

- Un VPN (*Virtual Private Network*) est un réseau privé virtuel qui relie de façon sécurisée un ensemble d'ordinateurs au dessus d'un réseau non sécurisé
- Utilisé par exemple pour connecter de façon sécurisée des postes nomades à un réseau d'entreprise
- Utilisation (la plupart du temps) de protocoles cryptographiques forts (IPsec, encapsulation dans du SSL, *etc.*)
- Exemples : IPsec manuel (un peu difficile à mettre en place), OpenVPN, Tinc, *etc.*
- Nécessite quelques connaissances en réseau et en administration système pour être mis en place

# Plan



# SSL

- SSL permet de garantir une sécurité de bout en bout de la connexion, quelque soit la sécurité (ou l'insécurité) des couches basses
- Exemples :
  - HTTPS, SMTPS, POPS, IMAPS (couche SSL/TLS)
  - SSH
- Très bonne sécurité (confidentialité, authentification et intégrité) dès lors que l'on ne néglige pas l'étape de vérification du certificat électronique...

# Conclusions

- Le WEP est mort
- Bonne sécurité chez soi :
  - WPA/WPA2 avec une clé partagée choisie aléatoirement
  - Filtrage par MAC pour retarder (un peu) l'attaque
- Sur un point d'accès public (hotspot) :
  - Utilisez des VPN ou les protocoles sécurisés (HTTPS, SMTPS, POPS...)