Réseaux WiFI

Solutions de mise en oeuvre et de sécurité OpenSource/Libre

Présentation

- WIFI
  - Abréviation de Wireless Fidelity
  - Basé sur les standards 802.11 développés par l'IEEE (Institute of Electrical and Electronic Engineers)
  - WIFI est aussi une marque détenue par la Wi-Fi Alliance, organisation à but non lucratif de certification de produits sans fil.
  - Plusieurs modes courants :
    - 802.11b : débit (théorique) max. de 11 Mbps
    - 802.11g : débit (théorique) max. de 54 Mbps
  - Fréquences radio
    - 14 canaux de 2,412 Ghz à 2,484 Ghz.

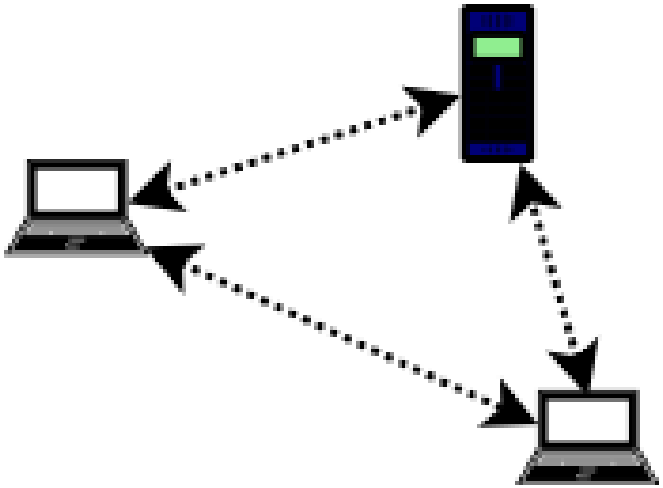
Présentation

- La norme 802.11 définit les deux couches les plus basses du modèle OSI
  - Couche liaison de données
    - Couche MAC
    - Authentification
    - Secret des données par chiffrement
    - Association à un point d'accès et transmission des messages
  - Couche Physique
    - Différents couches en fonction des modes b/g etc.
- Ensuite : TCP/IP.

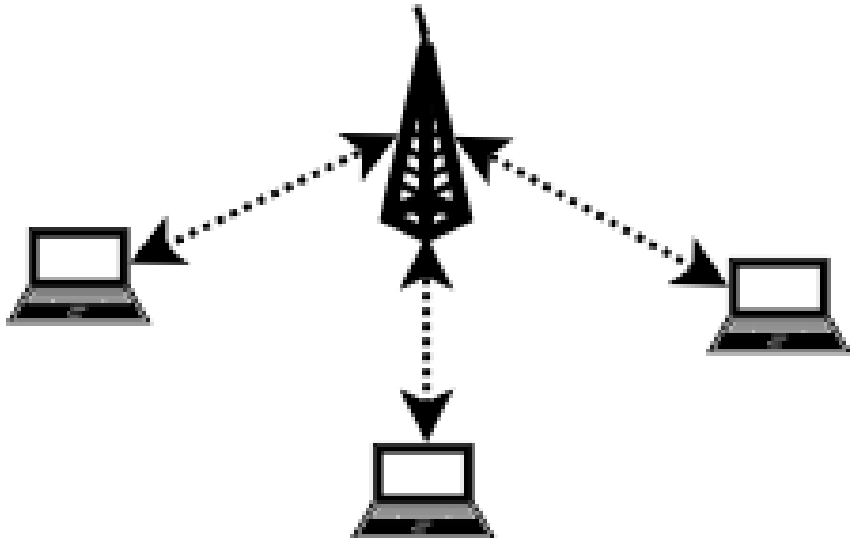
Mise en oeuvre

- Deux modes de communication :
  - Ad Hoc
    - Connexions directes équipement à équipement.
  - AP (Access Point)
    - Clients / AP
      - Connexions à un équipement de type routeur/passerelle.
    - AP / AP
      - Interconnexions de réseaux sans fil.

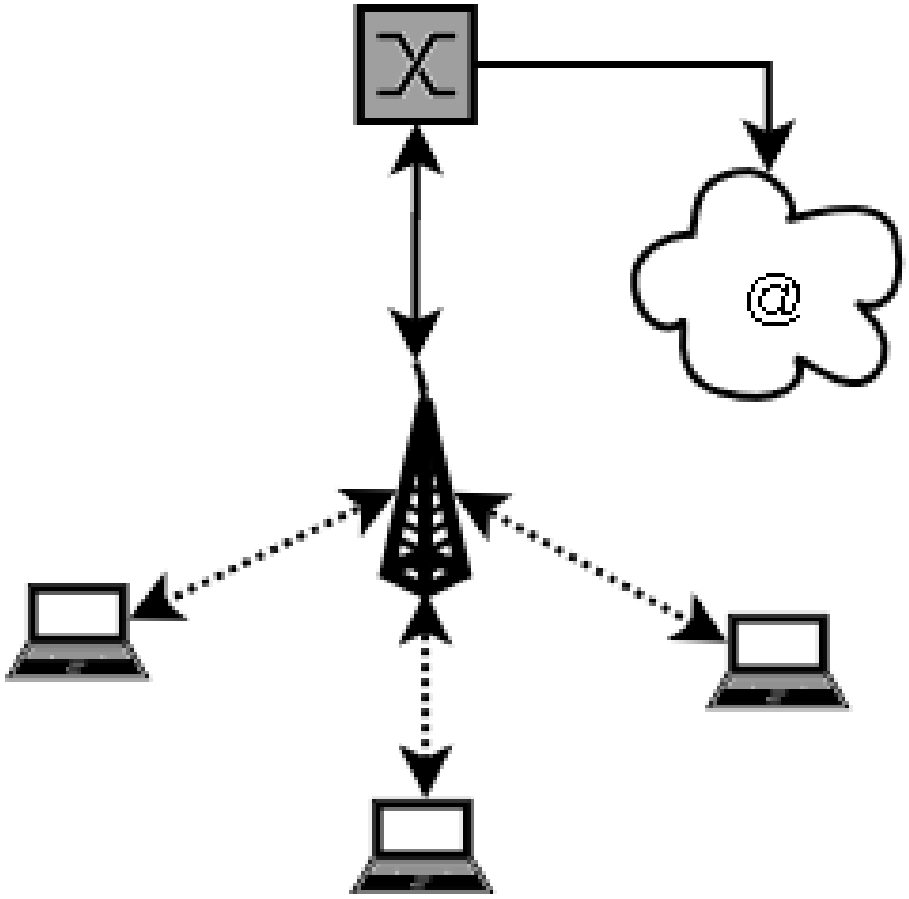
Réseau Ad Hoc



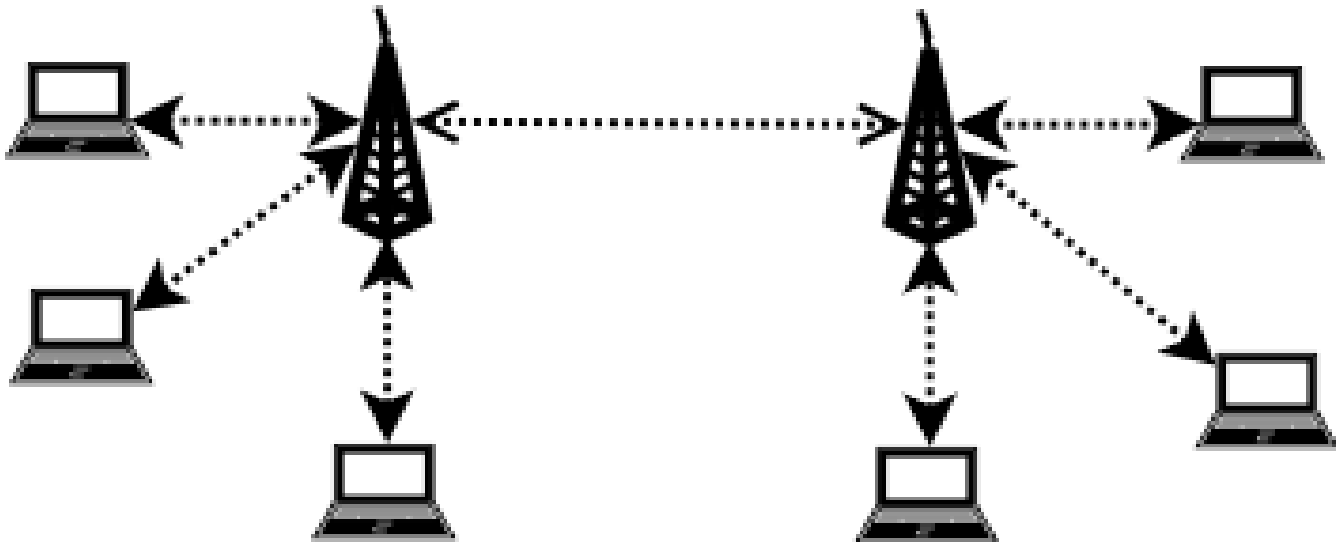
Réseau Clients / AP



Passerelle Wifi



Connexions entre AP



Mise en oeuvre minimale

- Choisir la topologie : Ad Hoc ou AP
- Choisir un canal (une fréquence) et un mode (b, g, b/g)
- Définir un SSID (Service Set Identifier)
- Configurer le réseau TCP/IP
  - Plan d'adressage
  - Routes
  - Serveurs DNS, etc.
- Dans le cas d'un AP
  - Il est possible d'utiliser un serveur DHCP installé sur l'AP pour diffuser les paramètres de connexion cités ci-dessus aux clients.

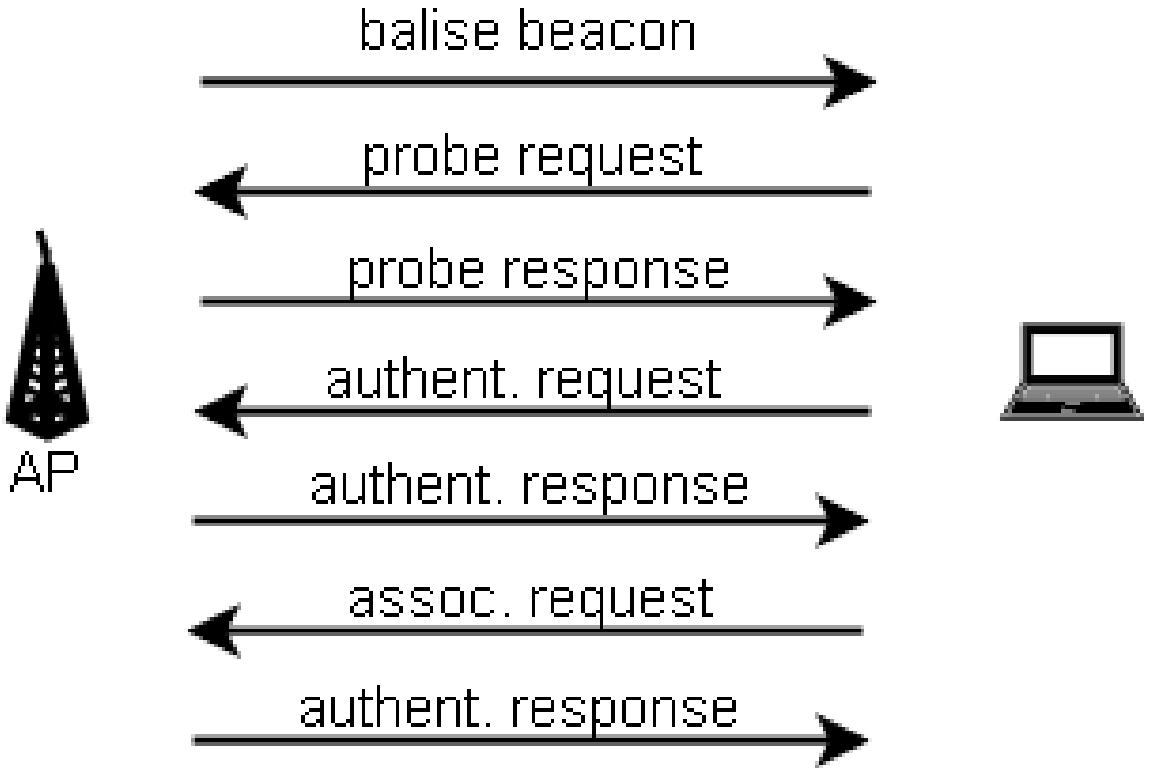
Sécurité

- Par sa nature – sans fil – un réseau Wifi est très vulnérable aux intrusions.
- Toute personne capable de capter le signal d'un appareil ou d'un AP est virtuellement capable :
  - d'écouter le réseau
  - de pénétrer sur le réseau ou sur certains de ces composants
  - de perturber plus ou moins gravement le fonctionnement du réseau
  - de détourner le trafic.

Découverte de réseaux

- Scan
- Activité passive non facilement détectable.
- Consiste à écouter sur chaque canal pendant une courte période.
- Un AP émet toutes les 100 ms une balise.
- Une station qui cherche à joindre un AP émet une trame « probe request ».

Dialogue client - AP



Scan Wifi

- Scan actif
  - Envoi de trames Probe Request et attente/analyse de la réponse.
  - Peut nécessiter d'appeler un SSID
    - Il existe des listes des SSID par défaut pour les principaux matériels.
  - Action détectable... si l'AP dispose de fonctionnalités de journalisation (log).
- Scan passif ou monitoring
  - Ecoute des trames Balise Beacon émises par les AP.
  - Action indétectable si non suivie d'une tentative d'intrusion ou d'association.

Exemples d'outils

- Windows
  - NetStumbler
- Mac OS X
  - KisMac

Absence de sécurité

- Les paramètres par défaut sont dangereux :
  - Par défaut un AP diffuse son SSID.
  - Par défaut un AP n'utilise pas de moyen d'authentification ni de chiffrement
  - Conséquences :
    - N'importe qui peut écouter le réseau et lire le SSID (analyse des trames balise beacon)
    - N'importe qui peut alors s'authentifier et s'associer à un AP.
    - N'importe qui peut écouter et capturer le trafic sur le réseau.
    - N'importe qui peut détourner le trafic vers un AP pirate.
    - Bref : c'est n'importe quoi !

Sécurisation a minima

- Les actions suivantes sont indispensables pour sécuriser un réseau mais nous verrons qu'elles ne sont pas suffisantes !
- Limiter si possible la puissance d'émission de l'AP
- Changer le SSID par défaut sur tous les AP
  - Adopter des SSID non faciles à trouver
- Désactiver la diffusion par l'AP du SSID
  - Chaque client doit connaître le SSID.
- Activer le filtrage sur adresses MAC
  - Pas envisageable si il y a beaucoup de clients et l'AP doit le permettre.
- Activer le chiffrement WEP

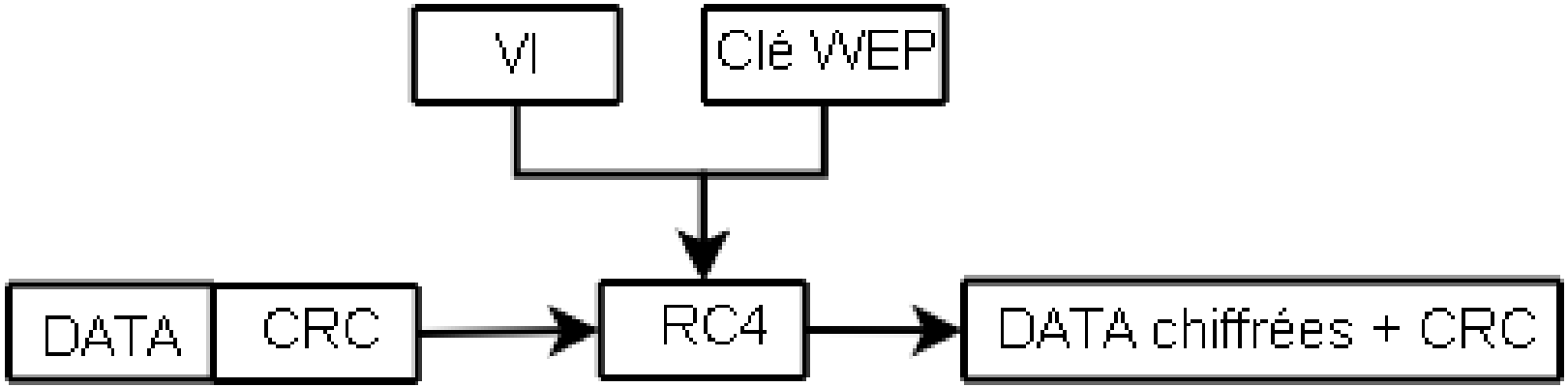
WEP

- Wired Equivalent Privacy
- Comme son nom l'indique, ce protocole devrait fournir au réseau sans fil une sécurité équivalente à celle d'un réseau filaire.
- Interdit l'accès au réseau (AP) aux utilisateurs non authentifiés.
- Chiffre les communications pour interdire l'écoute.
- En tout cas : théoriquement !

WEP

- Apporte au protocole les fonctionnalités de chiffrement et contrôle d'intégrité.
- Chiffrement
  - algorithme RC4 à clef partagée par chaque participant.
- Contrôle d'intégrité
  - Repose sur une somme CRC32.
- Utilise un vecteur d'initialisation (VI) de 24 bits (nombre aléatoire)
- Clef + VI : 64 bits, 128 bits ou plus
  - Longueur réelle de la clef = (Clef + VI) - 24

WEP



Points faibles WEP

- La clé est statique.
- Son changement n'est pas automatique
  - ... et peut être fastidieux si le parc de clients est important.
  - Il est possible cependant de diffuser 4 clefs différentes
- Certains éléments sont diffusés en clair
  - Notamment le vecteur d'initialisation
- WEP « hérite » des vulnérabilités et des faiblesses de l'algorithme RC4.
- CRC32 n'est pas une vraie somme de contrôle cryptographique.
- Mais WEP : c'est encore mieux que rien !

WEP

- WEP peut être une solution satisfaisante pour des cas particuliers, notamment pour les réseaux domestiques.
- Il faut choisir des clefs de longueur supérieure à 128 bits.
- Utiliser pour la clef des chaines de caractères aléatoires.
- WEP tout seul ne suffit pas, il est indispensable de mettre en oeuvre d'autres contre mesures.

Attaque contre WEP

- De plus en plus simples car les outils existent.
  - AirCrack
    - airodump : capture de trafic
    - aireplay : injection de trafic
    - aircrack : cassage de clef
  - Fonctionnement
    - Générer du trafic pour accélérer la capture des VI et le cassage des clefs.

Attaques

- Quels buts ?
  - Utilisation abusive du réseau
  - Ecoute du trafic même chiffré
  - Déni de service
    - Déauthentification des clients légitimes
  - Détournement de trafic
    - Attaque contre l'AP légitime
    - Mise en place d'un AP pirate

Sécurité avancée

- Filtrage sur adresses MAC
- Principe
  - Un équipement dont la MAC est enregistrée sur l'AP peut s'y connecter.
  - Cette protection n'est cependant pas absolue
    - ARP cache poisoning
    - Usurpation d'adresses MAC
  - Il faut quel'AP supporte cette fonctionnalité.

Evolutions du chiffrement

- Objectif : surmonter les faiblesses de WEP
  - Utilisation de clefs temporaires
  - TKIP (Temporal Key Intégrity Protocol) pour renforcer le contrôle d'intégrité
  - Changements plus fréquents des clefs
  - Augmentation de la longueur du VI (48 bits)
  - Utilisation du protocole RADIUS ou du mode PSK (Pre Shared Key)
    - PSK : seule la clef initiale est partagée entre les clients et l'AP
  - EAP : Extensible Authentification Protocol

WPA

- WPA : WiFi Protected Access
- Permet de mettre en oeuvre TKIP et EAP.
- Mais
  - Nécessite de mettre à jour les drivers sur l'AP et les cartes
  - Nécessite RADIUS dans l'absolu
  - Quelques vulnérabilités déjà trouvées.

Sécuriser son réseau

- Pas de recette miracle
- Nécessité de mettre en oeuvre des mesures de sécurité à plusieurs niveaux :
  - Physique
    - Réduction de la puissance d'émission
    - Accès à l'AP depuis le réseau filaire
  - Sur chaque élément
    - Ne pas oublier le mode Ad-Hoc entre clients
  - Logique
    - Filtrage réseau
    - Chiffrement

VPN

- Solution incontournable pour avoir un bon niveau de sécurité.
- Deux technologies :
  - VPN SSL/TLS
    - Avantages
      - Pas de modification de l'OS
    - Inconvénients
      - Déploiement sur chaque machine
  - VPN IPSEC
    - Avantages
      - Plus performants et implémentation dans les OS modernes
    - Inconvénients
      - Déploiement plus lourd

VPN

- Apports du VPN
- Utilisation de la cryptographie pour :
  - authentifier les machines
  - chiffrer les communications
  - contrôler l'intégrité des données échangées
- Possibilité d'authentifier aussi les utilisateurs.

Exemple Libre/OpenSource

- Solution légère
  - AP : Linksys WRT54G
  - Remplacement du firmware d'origine par OpenWRT
  - Utilisation des outils Linux
    - Netfilter/IPtables
    - OpenVPN
- Solution plus complexe
  - Soekris NET4801
  - OpenBSD et les outils standards
    - Pare feu PF
    - hostapd

Références

- OpenWRT : www.openwrt.org
- OpenBSD : www.openbsd.org