***Réseaux Radio Wifi***

**Définitions/Normes**

Le réseau radio wifi est un réseau à couverture limité à une zone géographique de faible taille => réseau local radio. Ce réseau fournit une bande passante partagée.

**Bande passante**

C’est la plage de fréquence à l’intérieur de laquelle la fonction est utilisable. Ex : l’oreille est un filtre qui agit sur la plage de fréquence 20Hz-20Khz.

Le filtre de l’oreille est accordé à cette plage de fréquence, il coupe toutes les autres fréquences.

**Canal de transmission**

Un canal de transmission Wifi est une bande de fréquence à l’intérieur de laquelle la puissance du signal est comprise en Pmin et Pnominal. Dans l’exemple ci-dessus l’oreille fonctionne sur le canal audible 20hz-20Khz

**Réseau radio à accès multiple**

Le réseau WIFI fournit un ensemble de canaux qui offrent chacun une bande passante partageable. Ce réseau comprend 2 fréquences de fonctionnement possibles

* Bande ISM => 2.4Ghz
* Bande passante11mb/s,54mb/s,100mb/s
* Bande VNI => 5Ghz
* Bande passante jusqu’a 300Mb/s

**Normalisation (WECA-IEEE-ETSI)**

3 types de technologie WIFI (la norme wifi est gérée par l’IEEE sous le N°802.11)

* 802.11b => Bande 2.4Ghz, débit 11mb/s

Portée 200m en outdoor

50m en indoor

* 802.11g => Bande 2.4Ghz ,54Mb/s

Portée 100m à 500m

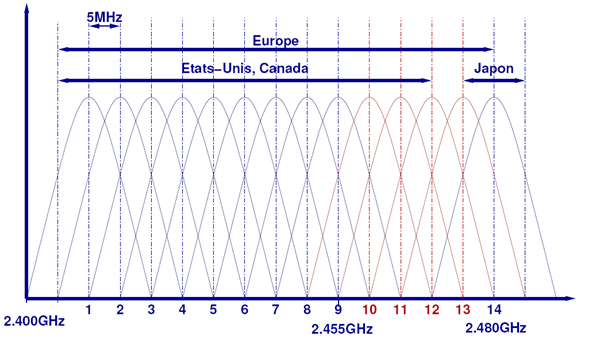
* 802.11nn=>Bande 2.4Ghz, 100 à 300Mb/s

Portée jusqu’à 100m

**Infrastructure**

* Modes d’utilisation => 1 point d’accès amène les utilisateurs Wifi
* Mode bridge => permet de relier 2 LAN, ou 2 bâtiments
* Mode Ad hoc =>connecter des postes WIFI entre eux.

**Structure du signal radio**



Le signal radio Wifi est composé de 13 bandes de fréquences (canaux radio). Une 14 ème fréquence est réservée pour les opérations internes aux opérateurs.

Chaque canal émet avec une fréquence centrale espacée de 5Mhz du canal voisin.

**Mobilité dans le réseau :**

Pour assurer la mobilité des postes couvert par plusieurs points d’accès, il faut que les fréquences utilisées par ces points d’accès puissent se recouvrir (mobilité sans rupture du trafic => handover)

**Gestion du réseau**

Un réseau wifi peut être composé de plusieurs points d’accès, chacun d’eux contrôlent une zone de couverture.

Chaque point d’accès assure la gestion des machines présentes dans sa zone. Les machines sont, soit présentes dans la zone de couverture ou bien en cours d’identification (association avec le point d’accès). Les machines doivent transmettre selon une procédure dictée par le PA. Le PA envoie régulièrement une trame de balise pour indiquer aux machines les paramètres Wifi utilisées :

* Le canal
* La puissance
* L’identifiant de réseau BSSID (basic set service ID)
* Le taux de la charge de la zone
* Le délai d’entrée dans le réseau
* L’identifiant de canal permet à un nouveau poste en cours d’association de se caler sur la fréquence. - L’identifiant BSSID donne le nom du réseau.
* Le taux de charge permet à un nouvel entrant de choisir son réseau.
* Le réseau Wifi identifie chacun des PA avec un N° propre (BSSID)
* Un BSSID est identifié par un nom visible pour la machine et une adresse MAC non visible.

Un groupe de PA peut être administré dans un réseau global dont le nom sera l’identifiant comme tous les PA (ESSID => Extended Service Set ID)

**Processus d’association**

Ce processus permet d’intégrer un poste nomade dans le réseau en évitant les conflits d’accès. Un premier processus consiste à régler les collisions possibles. Ce processus appelé CSMA/CA est identique au processus CSMA/CD utilisé sur la filaire.

* Processus de sondage (PROBE) => Ce processus permet de choisir le meilleur PA lors du déplacement.
* Processus d’authentification => négociation entre le PA et le poste pour l’entrée dans le réseau. Ce processus permet de vérifier les droits du poste (clé de chiffrage)
* Processus d’association => allocation des paramètres physiques d’accès au réseau

**Sécurité**

Le réseau Wifi est un réseau ouvert qui nécessite donc des précautions de sécurité sur les accès par les postes nomades.

L’accès au réseau Wifi peut se faire suivant 3 niveaux de sécurité.

* Pas de sécurité => sans sécurisation
* Niveau faible => clé WEP
* Niveau fort => WPA 2
* Niveau très fort => Authentification + acceptation + autorisation => ce processus utilise les services d’un serveur d’authentification (RADIUS) => ce niveau est aussi appelé WPA2 Entreprise.

Le processus de cryptage des données en Wifi utilise un algorithme à clés symétriques. Dans ce cas les clés sont identiques sur le PA et les postes et ne sont connus que de ces 2 équipements. Ce mode et simple à mettre en œuvre mais nécessite un cryptage très robuste. Ce mode est utilisé entre le PA et le poste, le PA décide alors :

* Accepter directement l’entrée du poste da ns le réseau => Authentification locale .
* Laisser l’authentification à un serveur d’authentification. Authentification Radius

**Stratégies de sécurité**

Pour renforcer la sécurisation du réseau, l’admin doit appliquer plusieurs opérations :

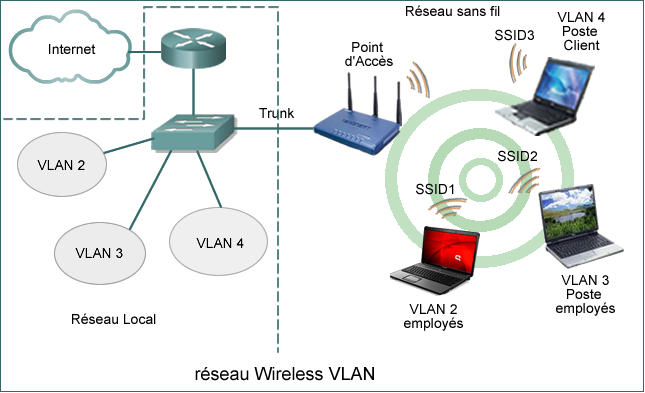
* Cacher le SSID
* Définir les @mac qui seront autorisées dans le réseau.
* Placer les PA et régler leur puissance de sorte qu’il ne génère pas ou peu de signal à l’exterieur de l’entreprise.
* Crypter les données (faible ou fort)
* Réduire la durée de vie des clés.

Nota : L’algorithme de cryptage Wpa 2 est l’algorithme AES qui remplace l’algorithme TKIP.

**Les WLAN (wireless LAN)**

Cette Architecture permet d’integrer les postes nomades WIFI dans une structure de sous reseau VLAN/WIFI.

La réseau WLAN utilise un fonctionnement qui met en œuvre des réseaux multiple (multiSSID) dans un réseau Wifi. La norme Wifi autorise jusqu’à 16 SSID simultanés sur un PA.



Le schéma ci dessus, le point d’accès assure la gestion des 2sous réseaux radio (invité/employé) et leur liaison avec les 2 sous réseaux vlan.

Nous utiliserons dans ce schéma un commutateur de niveau 3 c’est-à-dire sachant traiter les couches 2 et 3 du modèle OSI.