



Pôle de Compétences TIC Grand Est

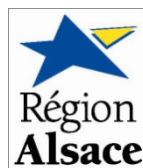


SUD ALSACE  
MULHOUSE

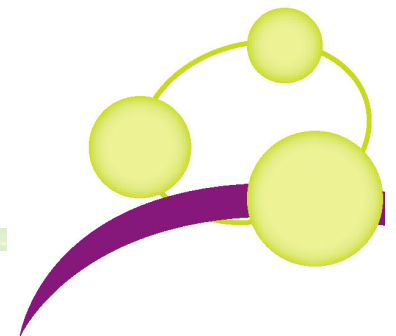
## ThemaTIC sécurité informatique

# La face cachée du WIFI

Jeudi 24 septembre 2009



- **17h00 : Accueil des participants**
- **17h15 : Intervention**
  - **5 histoires vraies**, des situations où le WIFI perturbe le bon fonctionnement d'une société
  - **10 bonnes questions à se poser** quand on choisit d'implanter du WIFI
- **18h30 : Questions / réponses**



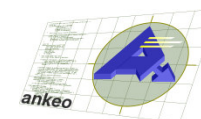
➤ **Daniel Jordan, Newnet Technology**

- Conseils stratégiques et accompagnement pour l'évolution des infrastructures réseaux



➤ **Jean Marc Boursot, Ankeo**

- Audit, conseil et ingénierie en sécurité informatique et réseau



➤ **Jerome Castellano, Seiso**

- Conseil en système et sécurité informatique



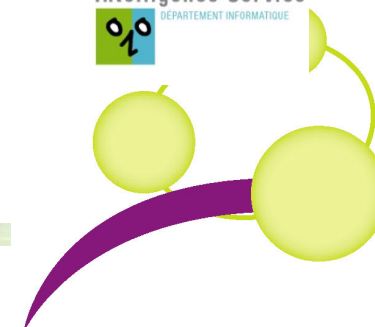
➤ **Arnaud Feist, Spie communications**

- Intégrateur de solutions réseaux et télécoms



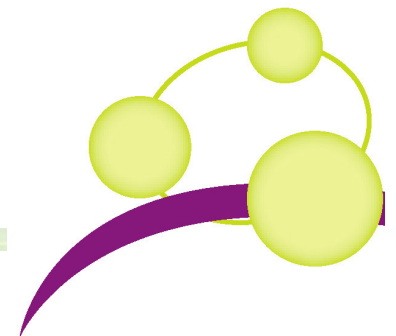
➤ **Frédéric Perrenot, Intelligence Service 001**

- Informaticien référent pour TPE et indépendants



### ➤ Situation du client :

- Client porté sur les nouvelles technologies
- Pré-étude sur les besoins en téléphonie et la couverture WiFi (80% téléphones IP WiFi)
- Besoins de raccorder un nouveau site distant avec 2 PC et 1 téléphone IP WiFi)
- Bâtiments techniques au voisinage à couvrir
- Utilisation du WiFi également pour économiser des travaux de câblage (!!!)
- Devis global 50KEUR dont 5KEUR de pré-étude



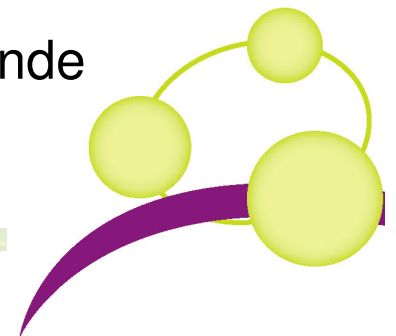
## ➤ Différences entre prévision et réalisation :

### Prévision

- Nombre de bornes WiFi au siège 10
- Nouveaux bâtiments distants 1 téléphone WiFi (1 borne WiFi)
- 2 PC en WiFi pour économie de câblage
- Budget 50KEUR

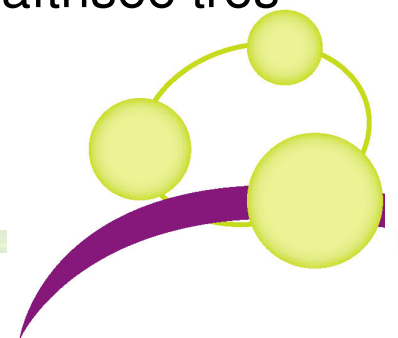
### Réalisation

- Économie de 3 bornes pour 2.5%
- plusieurs PC en WiFi et 4 téléphone WiFi
- Stoppé en nombre par nous car augmentation constante
- Réel dépassement >30%
- Nouvelles applications et changement d'habitudes de travail augmentant massivement la bande passante



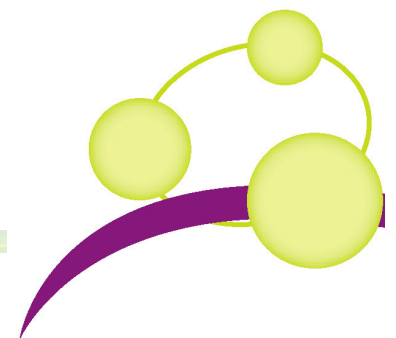
## ➤ Conséquences :

- Pré-étude partiellement obsolète
- Coupure de communication entre l'annexe et le bâtiment principal (roaming inopérant)
- Sous couverture dans certains endroit (salle de réunion, angles du bâtiment, etc)
- Problèmes de qualité en WiFi dans le bâtiment distant et au siège dues à la surpopulation des équipements PC WiFi Data non prévus
- Surcoûts de >30% dues aux problèmes de couvertures provoqué par l'économie des bornes et aux changements des besoins au cour du projet
- Insatisfaction des utilisateurs grandissante et non maîtrisée très difficile à regagner



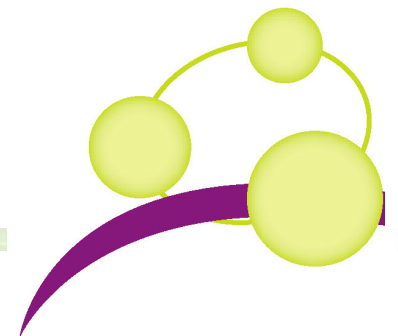
## ➤ Conclusion :

- Tout changement dans les habitudes de travail et l'usage du réseau peut influencer sur le réseau WiFi
- Tout changement d'utilisation du bâtiment influe sur le WiFi
- Le WiFi est un surcoût et non une économie (en WiFi pas de projet au rabais)



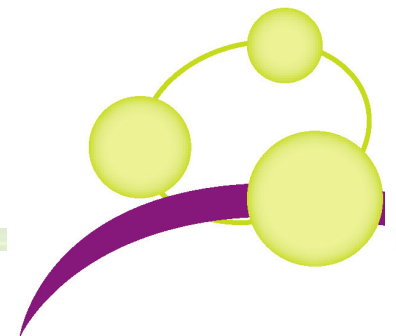
### ➤ Situation :

- Soit une institution
  - elle est située en centre ville
  - elle possède un réseau de 20 postes environ
  - elle accueille des enfants
  - son accès à Internet se fait via des équipements grand public
  - elle utilise le wifi
  - elle a un prestataire informatique pour gérer son réseau et ses équipements
- Soit Monsieur X
  - il habite dans la même zone
  - il accède à internet par wifi



### ➤ Les erreurs :

- Monsieur X peut se connecter sur le réseau wifi de l'institution (pas de mot de passe ni de protection d'aucune sorte) et a accès à Internet par ce biais
- Connecté, il verra le serveur, les postes et les équipements réseau
- Il peut accéder à l'ensemble des équipements en raison de mots de passe par défaut



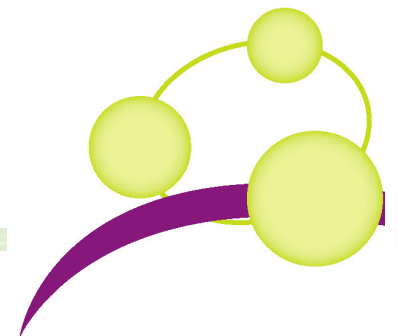
### ➤ Les risques et solutions :

#### ■ Risques

- Utilisation de l'accès de l'entreprise pour faire des échanges de fichiers à caractère pédophile (par goût ou pour nuire) ou illégaux
- Saturation de l'accès avec l'utilisation externe
- Prise de contrôle du réseau et utilisation des machines pour lancer des attaques
- Vol d'informations sur le réseau
- Falsification ou destruction d'informations

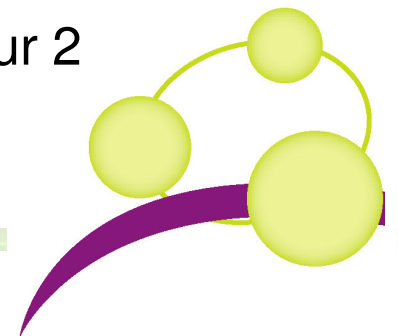
#### ■ Solutions

- Chiffrement du wifi (ou mieux)
- Politique de mots de passe
- Sécurité du réseau interne



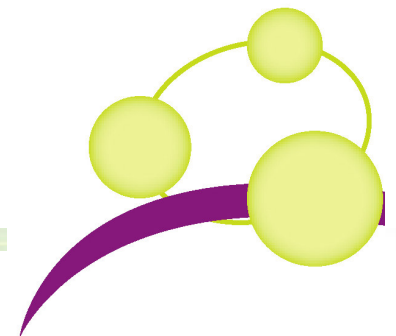
### ➤ Situation:

- Soit une entreprise
  - elle possède un réseau de plusieurs dizaines de postes
  - elle prend la sécurité du système d'information au sérieux via son équipe informatique et des sociétés spécialisées
  - son accès à Internet se fait via des équipements assez restrictifs
  - elle utilise le wifi mais de manière sécurisée
  - elle a une forte croissance
- Soit Monsieur X
  - il travaille pour cette société
  - il est avec 3 collègues dans un bureau prévu pour 2 personnes



### ➤ Erreurs, risques et solutions :

- Erreur :
  - Monsieur X peut installer ses propres équipements wifi (ou réseau en général)
- Risque :
  - Intrusion sur le système d'information de l'entreprise par un accès wifi non protégé
- Solutions :
  - Contrôler les bornes « sauvages »
  - Prévoir une authentification



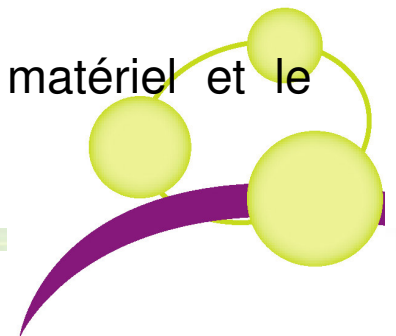
## Histoire vraie n°4 : le cas du garage automobile

### ➤ Situation:

- Un petit garage automobile au centre d'un village. Le local est entouré par des maisons individuelles.
- Monsieur Martin, un voisin utilise le WiFi, chez lui, pour se connecter à sa Box et surfer sur Internet.

### La configuration du garage

- Une station de travail pour la gestion quotidienne du garage et un ordinateur portable utilisé pour la recherche des pannes sur les véhicules de la marque.
- Un Modem ADSL/Routeur, une borne sans fil, pour la connexion à Internet et l'interconnexion des équipements informatiques.
- L'ordinateur portable est connecté au réseau en WiFi.
- Un prestataire informatique a installé et configuré le matériel et le réseau.



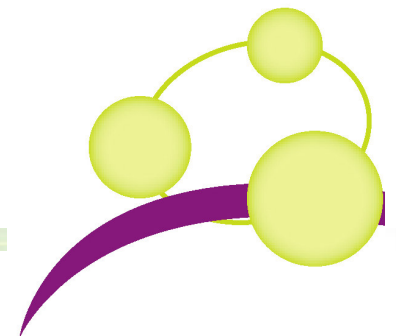
### ➤ Situation suite:

#### Pourquoi le choix d'un réseau sans-fil ?

- Afin de faciliter le déplacement de l'ordinateur dans le garage entre les différents véhicules en réparation et de faciliter l'utilisation de ce dernier à l'intérieur de l'habitacle.

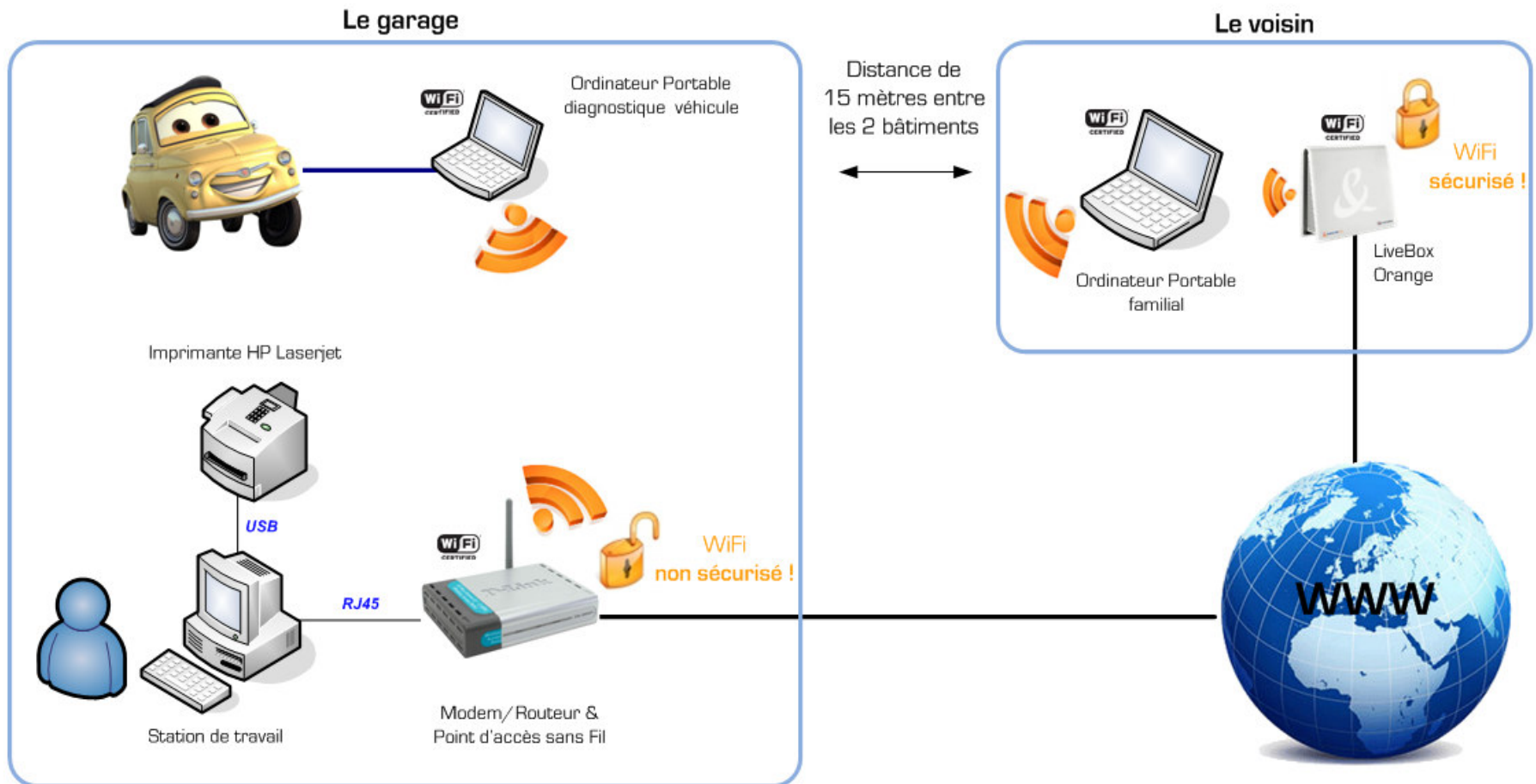
#### Configuration du WiFi.

- Le prestataire informatique du garage n'a activé aucune protection sur le réseau sans fil.
- **Absence totale de sécurité** : Réseau WiFi ouvert, accessible et visible par tous !...



# Histoire vraie n°4 : le cas du garage automobile

## ➤ Situation en image:

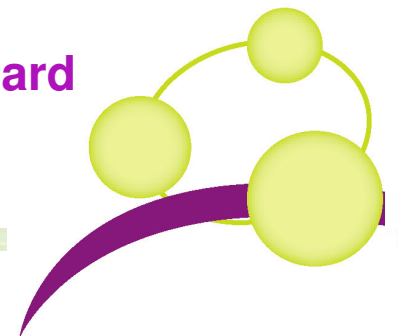


## Histoire vraie n°4 : le cas du garage automobile

### ➤ Les risques et conséquences:

- Un accès libre au réseau de l'entreprise, aux dossiers partagés, à Internet, à la configuration du Modem/Routeur et à la messagerie du garage
- Monsieur Martin a utilisé à plusieurs reprises la connexion Internet du garage pour surfer sur Internet...
- Il a signalé ce problème au garagiste. La bonne foi de ce dernier a permis d'éviter le pire :
  - Usurpation d'identité, dégradation et vol des données de l'entreprise,
  - Téléchargements illégaux (musiques, films,...),
  - Navigation sur des sites Interdits (pédophiles,...),

**Dans ce cas, La responsabilité du chef d'entreprise à l'égard du traitement des données informatiques est engagée**  
(Code Pénal – Article 34 de la loi du 6 janvier 1978)



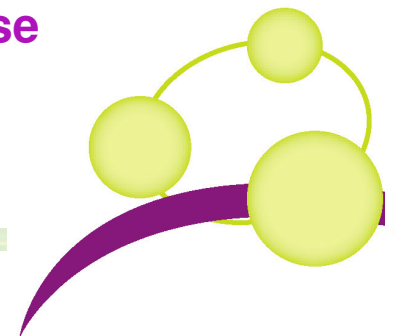
## Histoire vraie n°4 : le cas du garage automobile

### ➤ **Les solutions:** sécuriser le réseau

- en paramétrant les différentes options de sécurité proposées par le constructeur de la borne sans fil.
- **Changer le nom du réseau WiFi (SSID)** par défaut et ne pas le diffuser,
- Mettre en place une **clé de sécurité (WEP, WPA)** basée sur une paraphrase avec caractères spéciaux ( @ ! % \$ ),
- Activer le **filtrage des adresses MAC**, empêchant des ordinateurs non identifiés de se connecter au réseau WiFi de l'entreprise.
- Pour plus de sécurité, **remplacer systématiquement les mots de passe par défaut** des différents équipements et accès par des mots de passe personnels et confidentiels

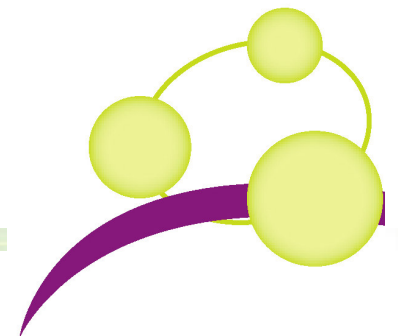
**En activant les différentes sécurités, le chef de l'entreprise se dégage de toutes responsabilités en cas de vol et de détérioration des données informatiques.**

*(Code Pénal – Article 34 de la loi du 6 janvier 1978)*



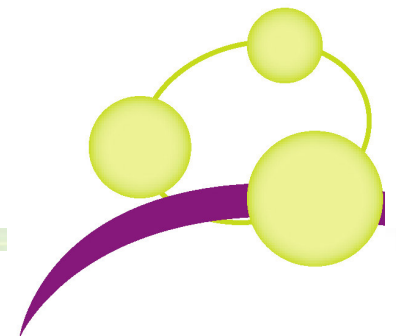
### ➤ Situation

- Le client: un hôtel 3 étoiles, 86 chambres
- Cadre: Strasbourg, vieux bâtiments, murs épais
- Besoins du clients: fournir un accès internet gratuit à ses clients



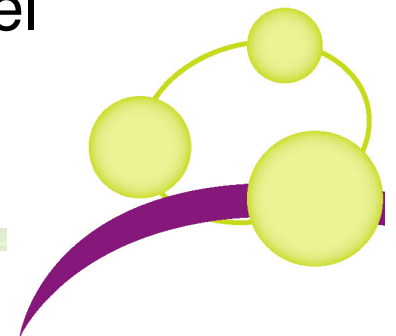
### ➤ Mise à disposition de l'accès internet

- Considéré comme un fournisseur d'accès à internet
  - responsabilité
- Loi:
  - LCEN, 21 juin 2004
  - Loi sur la lutte contre le terrorisme de janvier 2006
  - Hadopi, à venir
- Quelques recommandations:
  - Pouvoir identifier tous les accès à internet
  - Contrôler les accès internet
- Risques:
  - Amendes, jusqu'à 75 000 €
  - Emprisonnement, jusqu'à 3 ans



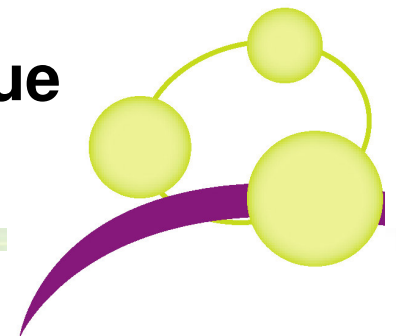
### ➤ Déploiement du WIFI

- Le client a déjà déployé du Wifi dans d'autres de ces hôtels
  - Solution = Wifi
- Problématique du Wifi: fonctionnement dans les bandes de fréquences 2.4 GHz et 5GHz:
  - Couverture jusqu'à 100m en champ libre
  - Sensibilité aux obstacles
  - Nécessité de câblage
- WiFi pas adapté à l'environnement de l'hôtel



### ➤ Solutions

- Mise en place de boîtier gérant l'ensemble des réglementations:
  - Identification des accès
  - Génération de code d'accès
  - Filtrage des accès
- Accès à l'internet
  - Utilisation du câblage téléphonique (DSLAM)
  - Permet de faire passer de l'ethernet sur du câblage téléphonique
  - Débit jusqu'à 20Mbit/s, distance 300 m
- **Conclusion: le WiFi c'est pas automatique**



# 10 bonnes questions à poser quand on choisit d'implanter du WIFI

Le jeu de questions/réponses qui suit est destiné aux personnes non qualifiées voulant mettre en oeuvre une solution réseau de type Wi-Fi dans leur environnement professionnel.

Ne posez aucune question !

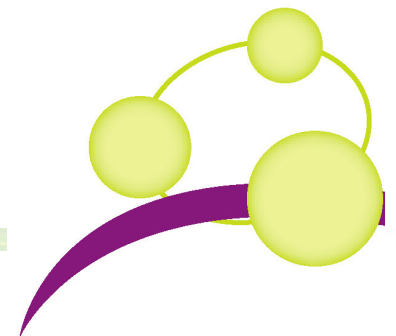
Votre prestataire fera preuve de compétence en traitant toutes les questions qui vont suivre de lui-même. Assurez-vous simplement que tous les sujets ont été abordés et faites-lui confiance pour ce qui est des choix techniques.

### Question n° 1 : Le Wi-Fi s'impose-t-il ?

Gardez à l'esprit que la solution filaire sera toujours de loin la meilleure. Viennent en second choix, le sans fil ou plus récemment, le courant porteur.

Ne demandez pas un réseau sans fil sinon nous vous le vendrons ! Énumérez soigneusement vos besoins et laissez votre prestataire confirmer votre intuition.

En clair, le sans fil doit se justifier car il implique un certain nombre de contraintes. Rassurez-vous cependant car ces dernières ne sont pas insurmontables et ne doivent en aucun cas vous décourager.

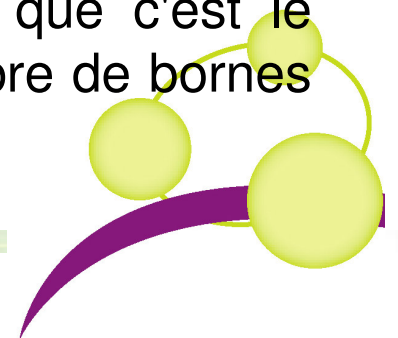


# Question n° 2 : Combien d'utilisateurs avez-vous ?

Il s'agit d'une question piège car il faut en réalité compter tous les matériels susceptibles d'utiliser votre futur réseau sans fil.

Les ordinateurs bien sûr, fixes ou portables, les imprimantes réseau qui sont de plus en plus pré-équipées d'une interface Wi-Fi, sans oublier les assistants électroniques (PDA) ou autres téléphones (smartphone ou combiné VoIP), etc.

Si vous avez l'intention de mettre un service d'accès internet sans fil à disposition de votre clientèle (hotspots), n'oubliez pas que c'est le nombre d'utilisateurs simultanés qui déterminera le nombre de bornes nécessaires..

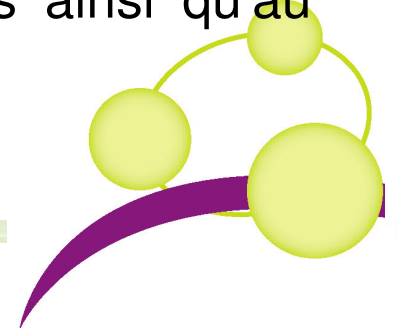


### Question n° 3 : Quels seront les usages ?

Déterminez l'ensemble des services qui seront supportés par votre réseau sans fil.

Il est évident que se contenter de naviguer sur internet et consulter sa messagerie n'est pas comparable à l'utilisation quotidienne d'un serveur de fichiers ou d'un PGI (Progiciel de Gestion Intégré) d'entreprise par un groupe de travail très actif.

Au même titre que le nombre d'utilisateurs, le nombre de services sera déterminant quant à la quantité de bornes nécessaires ainsi qu'au choix de la technologie (performances).



### Question n° 4 : Faut-il investir dans une étude du site ?

Un plan détaillé décrivant les positions retenues pour les bornes même simplifié, est obligatoire. Vous aurez une idée bien plus concrète des éventuels obstacles que votre réseau sans fil devra contourner.

Un autre avantage est de pouvoir éviter ou au pire limiter les interférences entre les bornes elles-mêmes.

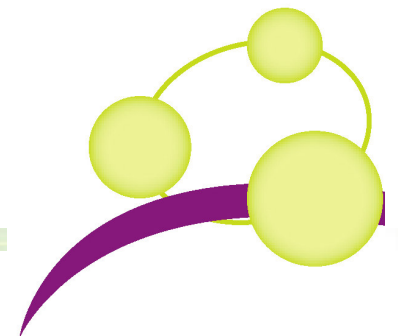
Quelque soit la qualité du schéma, il ne vous évitera pas des mesures sur le site car les matériaux dans les murs influencent fortement le passage du signal Wi-Fi. Sans oublier les bornes de vos voisins qui perturberont votre installation.

# Question n° 5 : Les téléphones Wi-Fi (VoIP) fonctionneront-ils ?

Pas forcément !

La problématique vient des personnes mobiles car lorsque votre téléphone se détachera d'une borne trop lointaine pour se connecter à une autre plus proche, vous pouvez perdre la communication (idem pour les PDA ou ordinateurs portables).

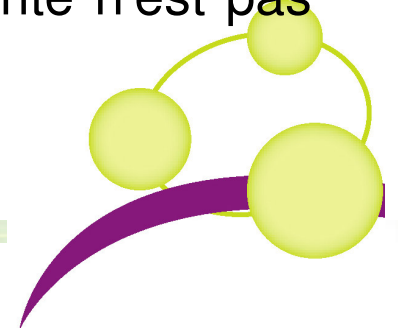
C'est pour cette raison que vous devez indiquer ce besoin tout de suite à votre prestataire s'il oublie de vous le demander. Les solutions techniques existent mais ont une influence sur le coût.



# Question n° 6 : Le réseau sans fil est-il facilement piraté ?

Sujet au combien délicat car même si la technologie s'est grandement améliorée dans ce domaine, l'incompétence du prestataire peut rapidement mettre votre réseau à disposition de quelques opportunistes.

Ici, impossible d'échapper au jargon technique et aux notions pointues. Si votre prestataire a fait un sans faute jusqu'ici en posant toutes les bonnes questions, faites-lui simplement confiance pour cette partie sans pour autant omettre de lui rappeler que vous souhaitez que la sécurité soit au coeur de la solution retenue. La sécurité n'est pas une option !

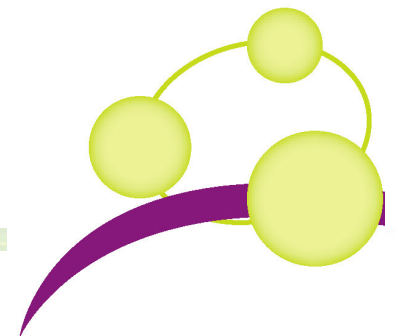


### Question n° 7 : Les bornes peuvent-elle servir de hotspot ?

La mise à disposition d'un accès internet sans fil gratuit est devenue très courante aujourd'hui (restaurants, cafés, campings, hôtels, etc).

Pas question d'ouvrir votre réseau au public !

Si vous souhaitez mettre ce type de service en place, il faudra déployer des réseaux parallèles. La solution matérielle étant bien sûr la plus sécurisée mais sachez qu'il existe des moyens de faire passer plusieurs réseaux étanches l'un à l'autre sans pour autant doubler le matériel.



### Question n° 8 : Quelles sont mes responsabilités ?

La tendance législative actuelle est d'imposer la traçabilité des échanges sur internet. Même si nous en sommes pas encore là dans tous les domaines, quelques briques sont déjà bien en place.

Les bornes Wi-Fi publiques doivent être associées à une machine capable de mémoriser les échanges faits sur le réseau internet durant l'année écoulée. Cela a un coût et implique des contraintes de sauvegardes supplémentaires.

Mais le Wi-Fi n'est plus le seul visé ! Nos fournisseurs d'accès internet seront peut-être un jour obligés de dénoncer leurs clients et n'oubliez pas que vous êtes en partie responsable de ce que fait votre réseau...

### Question n° 9 : Faut-il impérativement rester standard ?

Le prestataire avisé vous conseillera toujours de privilégier les standards afin de garantir un minimum le caractère évolutif de votre réseau sans fil.

Cependant cela ne signifie pas forcément que les performances doivent être obtenues au détriment de la compatibilité. Il existe un grand nombre de bornes diverses pour des applications variées. Elles peuvent être associées à des antennes avec des caractéristiques spécifiques (directionnelles, amplificatrices, etc).

Pratiquement tous les constructeurs proposent des versions « turbo » des standards mais spécifiques à la marque et impliquant d'acheter tout le matériel chez eux.

### Question n° 10 : Les normes sont-elles respectées ?

Le fait qu'un produit soit en vente ne signifie pas que vous pourrez l'utiliser en toute circonstance.

La puissance émettrice de vos bornes ainsi que de tout produit sans fil, est réglementée. Vous devrez faire la différence entre intérieur et extérieur. Méfiez-vous des antennes optionnelles qui risquent de vous mettre en faute.

Les réglementations en matière de protection contre les incendies imposent une norme si vos bornes doivent être placées dans les faux plafonds. Des bornes adaptées existent, ne vous en privez pas..

# Questions / Réponses

**N'hésitez pas à poser toutes vos questions à nos  
différents intervenants ...**

