Avantages et inconvénients du Wi-Fi en milieu professionnel

09/2006 – Bruno Kerouanton – Diffusion libre sous licence Creative Commons

Les technologies de réseaux-locaux sans-fil se démocratisent notamment grâce aux offres Internet grand public. Si ces réseaux offrent des avantages et un confort d'utilisation évidents pour le particulier, il faut en examiner plus précisément les caractéristiques lorsque l'on souhaite s'en servir en entreprise, car un certain nombre d'inconvénients masqués pour le particulier peuvent ressurgir.

Les avantages du Wi-Fi

1. Facilité d'utilisation

L'utilisation de réseaux Wi-Fi procure un confort d'utilisation non négligeable aux utilisateurs tant particuliers que professionnels, ceux-ci n'ayant pas à se « brancher à un mur », et étant par conséquent libres de leurs mouvements et non contraints à se placer près de la prise réseau murale. Ce confort est encore plus fortement perçu par les utilisateurs d'ordinateurs portables, ceux-ci n'ont en effet plus aucun fil à brancher car l'alimentation est fournie par la batterie, ce qui leur procure un confort d'utilisation inégalé.

De plus, pour le personnel extérieur et les nomades, cela permet de se connecter rapidement et sans difficulté au réseau de l'entreprise. Il est même envisageable de mettre en place des réseaux Wi-Fi de plusieurs natures, certains étant raccordés au réseau interne de l'entreprise et à usage exclusif des employés, et d'autres étant semi-publics (forme d'extranet ou de « réseau collaborateurs), voire totalement ouverts à Internet sous la forme de hot-spots.

Au tout début des réseaux 802.11, il y avait un certain nombre de contraintes liés au manque d'interopérabilité entre constructeurs, mais le consortium Wi-Fi a permis de gommer ces différences. Il subsistait néanmoins un certain inconfort lié au fait que les réseaux devaient être configurés manuellement par les utilisateurs, ceux-ci étant dans l'obligation d'assimiler un certain nombre de notions fortement techniques et d'acronymes ésotériques tels que SSID, WEP, ou clefs 128 bits.

Afin de ne pas décourager les utilisateurs, et avec l'arrivée imminente du WPA (voir plus bas) qui introduit à son tour de nouveaux concepts et acronymes indigestes pour le néophyte, certains constructeurs ont commencé à intégrer dans leurs équipements un mécanisme de configuration automatique, qui fonctionne en appuyant sur un seul bouton. Cela représente une avancée considérable, et permet désormais à tout utilisateur sans aucune connaissance en réseaux de bénéficier du Wi-Fi en mode sécurisé WPA.

2. Sécurité

Les réseaux Wi-Fi ont rapidement souffert d'une très mauvaise notoriété à cause de la mauvaise conception des mécanismes de sécurité (WEP) qui pouvaient être contournés sans trop de difficultés, et du fait que par défaut ces mécanismes même insuffisants n'étaient pas activés, laissant le réseau à la merci du tout venant.

Les constructeurs ont réagi en rédigeant la norme 802.11i, qui propose des mécanismes de sécurité plus robustes et basés sur les conclusions tirées de l'échec cuisant du WEP. Malheureusement cette norme impose l'utilisation de l'algorithme de chiffrement AES, ce qui nécessite de changer l'ensemble des équipements Wi-Fi actuels, ceux-ci ne comportant pas le module de chiffrement

adapté.

Afin d'effectuer une transition en douceur vers la norme 802.11i et pour ne pas obliger l'ensemble des utilisateurs à changer leur matériel de suite, la norme WPA a été mise au point et s'est imposée comme standard actuel. Il s'agit en fait d'une version de la norme 802.11i qui a été allégée afin de pouvoir conserver le matériel existant. Ainsi, bien que n'utilisant pas l'algorithme de chiffrement AES, WPA renforce considérablement le niveau de sécurité des liaisons Wi-Fi, et les experts s'accordent à dire que son utilisation permet de s'affranchir en toute confiance des problèmes de sécurité initialement constatés avec le WEP.

L'une des principales évolutions du WPA par rapport au WEP est que la clef de chiffrement permettant de sécuriser le canal radio est recalculée fréquemment, ce qui ne laisse pas le temps à un attaquant de réaliser son attaque. Cet aspect est basé sur le protocole TKIP (Temporal Key Integrity Protocol).

L'autre évolution majeure du WPA permet l'authentification du poste souhaitant se connecter, de manière efficace. Pour cela, il est fait appel à la norme 802.1x, qui définit une méthode d'authentification fonctionnant aussi bien sur les réseaux filaires que radio. Lorsqu'un PC souhaite se raccorder au réseau, le point d'accès ou le commutateur compatible 802.1x lui demande de s'identifier par le biais d'un mot de passe ou mieux encore par le biais d'un certificat X509, selon le mode d'authentification choisi (EAP-TLS, EAP-TTLS, EAP-LEAP, EAP-PEAP etc.). Cette information est envoyée à un serveur Radius, qui effectue la vérification dans sa propre base d'autorisations ou bien via un serveur d'authentification tel qu'Active Directory. Une fois cette étape validée, le point d'accès ou le commutateur autorisent l'accès et attribuent un VLAN à l'ordinateur distant, qui pourra ainsi ensuite obtenir son adresse IP etc.

Il existe des méthodes récentes d'attaque du protocole WPA, mais elles nécessitent des ressources onéreuses (processeurs spécialisés et FPGA)[1], que l'on ne peut pas considérer pour le moment comme étant à la portée du non spécialiste.

3. Autres avantages

La mise en place de réseaux Wi-Fi procure un certain nombre d'avantages annexes. Parmi ceux-ci, le sentiment procuré au personnel et aux visiteurs que l'entreprise est à la pointe de l'innovation, puisqu'elle met en œuvre des nouvelles technologies.

De plus, la démocratisation et la banalisation de cette technologie contribue à une baisse des coûts non négligeable, qui peut constituer un élément décisif lors d'investissements d'autant plus important qu'il est devenu courant d'avoir du Wi-Fi en standard sur les ordinateurs portables voire sur les imprimantes, ce qui réduit donc encore plus le coût perçu.

Les inconvénients du Wi-Fi

Malheureusement, il existe nombre d'inconvénients liés au déploiement d'un réseau Wi-Fi en entreprise. Ces problèmes ne sont que rarement perçus par le particulier, car celui-ci ne se sert généralement que d'un seul point d'accès pour y relier un ou deux ordinateurs au plus. Dès que l'on envisage le déploiement de dizaines voire de centaines de points d'accès, pour un nombre de PC encore plus importants, les caractéristiques ne sont plus tout les mêmes et il faut effectuer une étude

1 Source : http://www.recon.cx/en/s/dhulton.html

sérieuse avant de pouvoir affirmer avec certitude si la rentabilité de l'opération est réelle.

1. Câblage

Si le câblage vers chaque PC n'est désormais plus nécessaire, il faut tout de même acheminer le réseau Ethernet vers l'ensemble des points d'accès, ceux-ci pouvant être nombreux car situés à proximité des postes utilisateurs, de l'ordre de quelques mètres. Au final, et si l'on souhaite obtenir une qualité de réseau correcte il faut prévoir environ un point d'accès pour 5 utilisateurs maximum, soit 20 points d'accès pour 100 personnes.

Il faudra pour chacun de ces points d'accès faire parvenir non seulement le réseau Ethernet, mais également une arrivée 220v afin d'alimenter le point d'accès, ce qui représente un coût de câblage souvent oublié. Une solution existe pour certaines marques de points d'accès, et permet de faire transiter la tension d'alimentation nécessaire au fonctionnement du point d'accès via le câble réseau, évitant ainsi le câblage 220v. Cela nécessite cependant l'acquisition de commutateurs (switches) spéciaux munis de modules d'injection de courant PoE (Power Over Ethernet), au coût souvent élevé.

Dans le cas où l'on souhaite mettre en place plusieurs réseaux distincts pour le personnel interne et externe, ou dans le cadre de plusieurs services ou projets compartimentés, il faudra prévoir l'utilisation de SSID dédiés par réseau. Rares sont les équipements qui sont capables de supporter la gestion simultanée de plusieurs SSID, et on devra par conséquent équiper le bâtiment de plusieurs réseaux Wi-Fi distincts, ce qui augmentera d'autant les coûts de câblage et de gestion.

2. Disponibilité

La résistance aux perturbations électromagnétiques volontaires (brouillage) ou non (moteurs, caténaires, soudures etc.) reste faible malgré l'utilisation de technologies à étalement de spectre. La mise en marche d'un simple four à micro-ondes suffit parfois pour perturber l'ensemble d'un réseau Wi-Fi, provoquant un ralentissement du débit voire la coupure momentanée du réseau. Il faut en tenir compte lors de l'installation des points d'accès.

En pratique, il n'existe aucune garantie de disponibilité ou de qualité d'un réseau sans-fil, qui reste à la merci de perturbations radio. Si l'on souhaite une disponibilité maximale pour les utilisateurs, et leur garantir un accès au réseau, il faut opter pour des liaisons filaires.

3. Bande passante

Par conception, les points d'accès Wi-Fi se comportent en mode « hub » et non en mode « switch ». Cela signifie que le débit total alloué par point d'accès sera en fait réparti entre chaque PC connecté, et sans garantie de bande passante. Par exemple, sur un réseau au débit théorique de 54Mbit/s (802.11g) sur lequel seraient connectés 10 PC, chacun d'entre eux aurait un débit théorique maximal de 5,4Mbit/s.

Comme aucune garantie de la bande passante n'est possible, il est envisageable qu'un PC puisse occuper la quasi-totalité de celle-ci, pénalisant ainsi les autres PC connectés à la même borne qui n'auront qu'un débit minimal. Il est possible de mettre en place sur certains modèles de points d'accès des mécanismes de gestion de la bande passante, mais cela est complexe et doit être mûrement réfléchi.

Sur le plan technique la notion de collision est fréquente, ce qui ralentit considérablement le débit

dès-lors que plusieurs liaisons vers des PC sont en cours. En reprenant l'exemple précédent, les 10 PC n'auront en pratique pas un débit de 5,4Mbit/s, les collisions et les perturbations diverses tendront à ce que le débit soit de l'ordre de 1 ou 2Mbit/s.

Par nature, un réseau radio peut être brouillé ou perturbé de temps à autre. Il faut être conscient que lors du transfert de gros volumes de données (par exemples des fichiers vidéo, etc.), si une perturbation survient et que le protocole de transfert n'est pas en mesure de récupérer cette interruption momentanée, il y a de fortes chances que l'ensemble du transfert échoue, et qu'il faille recommencer. Il existe des protocoles de transfert spécialisés et permettant la réception sans perturbation malgré d'éventuelles erreurs, par exemple dans le domaine de la télévision ou de la voix sur IP, mais ces protocoles ne sont que rarement utilisés pour effectuer des transferts de fichiers plus classiques, et les applications dites « métier » ayant à effectuer de gros transferts de données implémentent encore plus rarement ces mécanismes auto-correcteurs.

4. Lourdeur d'administration

La mise en place d'un réseau Wi-Fi au sein d'une entreprise nécessite une étude préalable au niveau radio, afin de positionner les points d'accès et antennes de manière optimale. Il faut prévoir les éventuelles perturbations radio, l'organisation des canaux radio afin qu'il n'y ait pas de superposition de signaux, et l'optimisation du nombre de points d'accès en fonction du nombre de PC susceptibles de s'y connecter. Cette étude peut être complexe et son coût peut ne pas être négligeable dans le cas d'environnements complexes.

Compte-tenu du nombre de points d'accès que l'on déploiera au final, il sera nécessaire de consacrer des ressources pour leur administration (administrateur réseau), un ou plusieurs serveurs pour le fonctionnement (radius, administration, etc.), et très probablement un logiciel d'administration centralisée afin de ne pas avoir à configurer chaque point d'accès individuellement. Tout cela représente un coût souvent oublié au départ.

Conclusion

Comme on vient de le voir, si le réseau Wi-Fi représente des avantages en confort et en utilisation qui sont considérables, il n'est pas adapté à de lourdes charges, et il faut savoir que les coûts économisés en évitant un câblage Ethernet pour les postes des utilisateurs peuvent être dépassés par d'autres coûts auxquels on n'a pas forcément pensé à l'origine.

En pratique, les réseaux Wi-Fi sont performants en mode client-serveur avec des échanges courts (navigation Internet par exemple), ce qui explique leur succès auprès des particuliers. Il est quasiment certain que lors de l'utilisation d'applications métier « lourdes » (montage vidéo, transferts de gros fichiers, CAO et dessin, etc.) via des réseaux Wi-Fi, cela posera un certain nombre de difficultés.

Les problèmes de sécurité (confidentialité, intégrité) ont été résolus avec succès, ce qui permet un déploiement sans crainte en entreprise par rapport à cet aspect. Cependant l'aspect disponibilité ne pourra en aucun cas être garanti, et pour les applications critiques nécessitant une disponibilité maximale, l'utilisation de réseaux Wi-Fi doit être proscrite.