Guy Pujolle

Cours réseaux et télécoms

Avec exercices corrigés

Avec la contribution de Olivier Salvatori

3e édition

ISBN : 978-2-212-12414-9

EYROLLES

17

Les réseaux sans fil

Les réseaux sans fil définissent une communication par ondes hertziennes dans laquelle le client est quasi immobile dans la cellule où il se trouve. S'il sort de sa cellule, la communication est coupée. Les réseaux de mobiles, au contraire, rendent possibles les changements intercellulaires et la continuité de la communication lorsque le client se déplace fortement. Cette différence tend toutefois à s'atténuer puisque un client dans un réseau de mobiles peut rester immobile, tandis qu'un client dans un réseau sans fil peut désormais se déplacer de cellule en cellule à faible vitesse.

Les catégories de réseaux sans fil

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer facilement de place dans son entreprise. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base. Les communications entre points d'accès s'effectuent de façon hertzienne ou par câble. Ces réseaux atteignent des débits de plusieurs mégabits par seconde, voire de plusieurs dizaines de mégabits par seconde.

IEEE *(Institute of Electrical and Electronics Engineers).*– Organisme américain à l'origine de nombreuses publications et normes concernant notamment les réseaux locaux.

Plusieurs gammes de produits sont actuellement commercialisées, mais la normalisation en cours devrait introduire de nouveaux environnements. Les groupes de travail qui se chargent de cette normalisation sont l'*IEEE* 802.15, pour les petits réseaux personnels d'une dizaine de mètres de portée, l'IEEE 802.11, pour les réseaux LAN *(Local Area Network)*, ainsi que l'IEEE 802.20, nouveau groupe de travail créé en 2003 pour le développement de réseaux un peu plus étendus.

Dans le groupe IEEE 802.15, trois sous-groupes normalisent des gammes de produits en parallèle :

- IEEE 802.15.1, le plus connu, en charge de la norme Bluetooth, aujourd'hui largement commercialisée.
- IEEE 802.15.3, en charge de la norme UWB *(Ultra-Wide Band)*, qui met en œuvre une technologie très spéciale : l'émission à une puissance extrêmement faible, sous le bruit ambiant, mais sur pratiquement l'ensemble du spectre radio (entre 3,1 et 10,6 GHz). Les débits atteints sont de l'ordre du Gbit/s sur une distance de 10 mètres.
- IEEE 802.15.4, en charge de la norme ZigBee, qui a pour objectif de promouvoir une puce offrant un débit relativement faible mais à un coût très bas.

Du côté de la norme IEEE 802.11, dont les produits sont nommés Wi-Fi *(Wireless-Fidelity)*, il existe aujourd'hui trois propositions, dont les débits sont situés entre 11 et 54 Mbit/s. Une quatrième proposition, l'IEEE 802.11n, est en cours de finalisation et les premiers produits sont commercialisés.

La très grande majorité des produits sans fil utilise les fréquences de la bande 2,4-2,483 5 MHz et de la bande 5,15 à 5,3 MHz. Ces deux bandes de fréquences sont libres et peuvent être utilisées par tout le monde, à condition de respecter la réglementation en cours.

Les réseaux IEEE 802.11

La norme IEEE 802.11 a donné lieu à deux générations de réseaux sans fil, les réseaux Wi-Fi qui travaillent à la vitesse de 11 Mbit/s et ceux qui montent à 54 Mbit/s. Les premiers se fondent sur la norme IEEE 802.11b et les seconds sur les normes IEEE 802.11a et IEEE 802.11g. La troisième génération atteindra 320 Mbit/s avec la norme IEEE 802.11n.

Les fréquences du réseau Wi-Fi de base se situent dans la gamme des 2,4 GHz. Dans cette solution de réseau local par voie hertzienne, les communications peuvent se faire soit directement de station à station, mais sans qu'une station puisse relayer automatiquement les paquets vers une autre station terminale, à la différence des *réseaux ad-hoc*, soit en passant par un point d'accès, ou AP *(Access Point)*.

Le point d'accès est partagé par tous les utilisateurs qui se situent dans la même cellule. On a donc un système partagé, dans lequel les utilisateurs entrent en compétition pour accéder au point d'accès. Pour sérialiser les accès, il faut définir une technique d'accès au support physique. Cette dernière est effectuée par le biais d'un protocole de niveau *MAC (Medium Access Control)* comparable à celui d'Ethernet. Ce protocole d'accès est le même pour tous les réseaux Wi-Fi.

De nombreuses options rendent toutefois sa mise en œuvre assez complexe. La différence entre le protocole hertzien et le protocole terrestre *CSMA/CD* d'Ethernet provient de la façon de gérer les collisions potentielles. Dans le second cas, l'émetteur continue à écouter le support physique et détecte si une collision se produit, ce qui est impossible dans une émission hertzienne, un émetteur ne pouvant à la fois émettre et écouter.

Le CSMA/CA *(Carrier Sense Multiple Access/ Collision Avoidance)*

Dans le protocole terrestre CSMA/CD, on détecte les collisions en écoutant la porteuse, mais lorsque deux stations veulent émettre pendant qu'une troisième est en train de transmettre sa trame, cela mène automatiquement à une collision *(voir le cours 14, « Les réseaux Ethernet »)*. Dans le cas hertzien, le protocole d'accès permet d'éviter la collision en obligeant les deux stations à attendre un temps différent avant d'avoir le droit de transmettre. Comme la différence entre les deux temps d'attente est supérieure au temps de propagation sur le support de transmission, la station qui a le temps d'attente le plus long trouve le support physique déjà occupé et évite ainsi la collision, d'où son suffixe CA *(Collision Avoidance)*.

Pour éviter les collisions, chaque station possède un temporisateur avec une valeur spécifique. Lorsqu'une station écoute la porteuse et que le canal est vide, elle transmet.

Suite p. 398

réseau ad-hoc.– Réseau spontané qui n'utilise aucun point d'accès fixe, dans lequel l'infrastructure n'est composée que des stations elles-mêmes, ces dernières jouant à la fois le rôle de terminal et de routeur pour permettre le passage de l'information d'un terminal vers un autre sans que ces terminaux soient reliés directement. La caractéristique essentielle d'un réseau ad-hoc est l'existence de tables de routage dynamiques dans chaque nœud.

MAC *(Medium Access Control)*.– Technique d'accès à un support physique partagé par plusieurs machines terminales, permettant de sérialiser les demandes de transmission pour qu'elles se succèdent sur le support physique sans entrer en collision.

CSMA/CD *(Carrier Sense Multiple Access/ Collision Detection)*.– Technique d'accès employée dans les réseaux Ethernet, dite d'écoute de la porteuse et de détection des collisions, consistant à écouter le canal avant et pendant l'émission. Si le coupleur détecte un signal sur la ligne, il diffère son émission à une date ultérieure ou l'interrompt.

Suite de la page 397

Le risque qu'une collision se produise est extrêmement faible, puisque la probabilité que deux stations démarrent leur émission dans une même microseconde est quasiment nul. En revanche, lorsqu'une transmission a lieu et que deux stations ou plus se mettent à l'écoute et persistent à écouter, la collision devient inévitable. Pour empêcher la collision, il faut que les stations attendent avant de transmettre un temps suffisant pour permettre de séparer leurs instants d'émission respectifs. On ajoute également un petit temporisateur à la fin de la transmission afin d'empêcher les autres stations de transmettre et de permettre au récepteur d'envoyer immédiatement un acquittement.

L'architecture d'un réseau Wi-Fi est cellulaire. Un groupe de terminaux munis d'une carte d'interface réseau 802.11, s'associent pour établir des communications directes et forment un BSS *(Basic Set Service)*.

Comme illustré à la figure 17-1, le standard 802.11 offre deux modes de fonctionnement, le mode infrastructure et le mode *ad hoc*. Le mode infrastructure est défini pour fournir aux différentes stations des services spécifiques sur une zone de couverture déterminée par la taille du réseau. Les réseaux d'infrastructure sont établis en utilisant des points d'accès, ou AP *(Access Point)*, qui jouent le rôle de station de base pour une BSS.

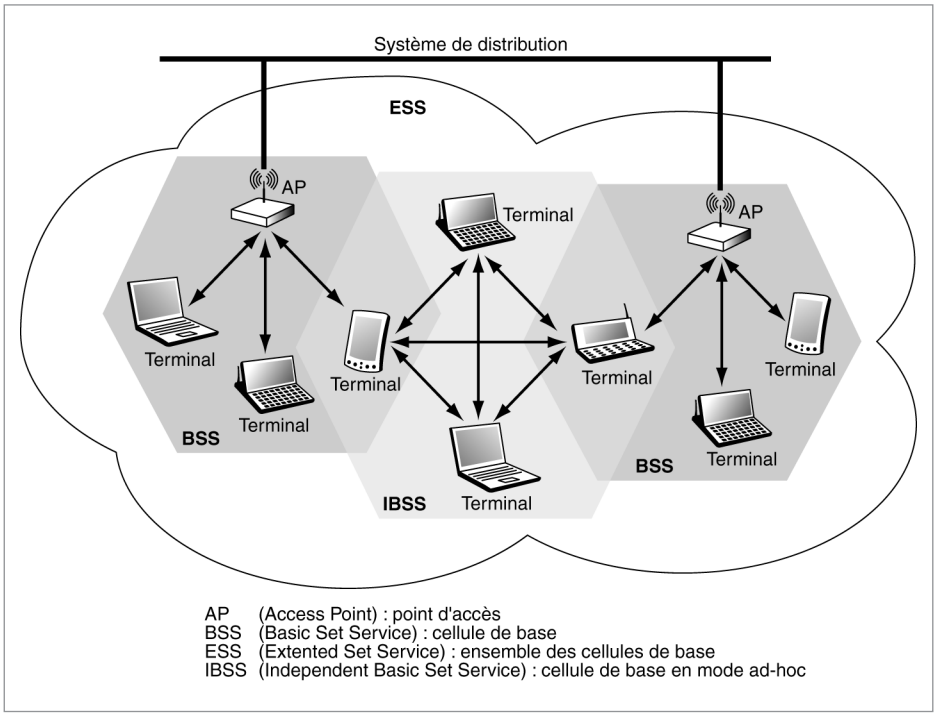

Figure 17-1. *Architecture d'un réseau Wi-Fi.*

Lorsque le réseau est composé de plusieurs BSS, chacun d'eux est relié à un système de distribution, ou DS *(Distribution System)*, par l'intermédiaire de leur point d'accès (AP) respectif. Un système de distribution correspond en règle générale à un réseau Ethernet utilisant du câble métallique. Un groupe de BSS interconnectés par un système de distribution (DS) forment un ESS *(Extented Set Service)*, qui n'est pas très différent d'un sous-système radio de réseau de mobiles.

Le système de distribution (DS) est responsable du transfert des paquets entre les différentes stations de base. Dans les spécifications du standard, le DS est implémenté de manière indépendante de la structure hertzienne et utilise un réseau Ethernet métallique. Il pourrait tout aussi bien utiliser des connexions hertziennes entre les points d'accès.

Sur le système de distribution qui interconnecte les points d'accès auxquels sont connectées les stations mobiles, il est possible de placer une passerelle d'accès vers un réseau fixe, tel qu'Internet. Cette passerelle permet de connecter le réseau 802.11 à un autre réseau. Si ce réseau est de type IEEE 802.*x*, la passerelle incorpore des fonctions similaires à celles d'un pont.

Un réseau en mode *ad hoc* est un groupe de terminaux formant un IBSS *(Independent Basic Set Service)*, dont le rôle consiste à permettre aux stations de communiquer sans l'aide d'une quelconque infrastructure, telle qu'un point d'accès ou une connexion au système de distribution. Chaque station peut établir une communication avec n'importe quelle autre station dans l'IBSS, sans être obligée de passer par un point d'accès. Comme il n'y a pas de point d'accès, les stations n'intègrent qu'un certain nombre de fonctionnalités, telles les trames utilisées pour la synchronisation.

Ce mode de fonctionnement se révèle très utile pour mettre en place facilement un réseau sans fil lorsqu'une infrastructure sans fil ou fixe fait défaut.

Questions-réponses

Question 1.– *Pourquoi peut-il y avoir des collisions sur un réseau sans fil ?*

Réponse.– Dans un réseau sans fil, le point d'accès est partagé entre tous les utilisateurs qui souhaitent y accéder. Si deux utilisateurs accèdent exactement au même instant, les messages entrent en collision. Dans la réalité, cette probabilité est extrêmement faible.

Question 2.– *Le fait d'attendre la valeur d'un temporisateur avant de transmettre ne porte-t-il pas atteinte au débit effectif du système ?*

Réponse.– Effectivement, le fait d'attendre un temporisateur fait diminuer le débit effectif du réseau. Un réseau Wi-Fi a donc un débit plutôt moins bon qu'un Ethernet métallique.

Pour qu'un signal soit reçu correctement, sa portée ne peut dépasser 50 m dans un environnement de bureau, 500 m sans obstacle et plusieurs kilomètres avec une antenne directive. En règle générale, les stations ont une portée maximale d'une vingtaine de mètres en environnement de bureau. Lorsqu'il y a traversée de murs porteurs, cette distance est plus faible.

La couche liaison de données

La couche liaison de données du protocole 802.11 est composée essentiellement de deux sous-couches, LLC *(Logical Link Control)* et MAC. La couche LLC utilise les mêmes propriétés que la couche LLC 802.2. Il est de ce fait possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE. La couche MAC, quant à elle, est spécifique de l'IEEE 802.11.

Le rôle de la couche MAC 802.11 est assez similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente. Cependant, la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version terrestre.

La méthode d'accès utilisée dans Wi-Fi est appelé DCF *(Distributed Coordination Function)*. Elle est assez similaire à celle des réseaux traditionnels supportant le best effort. Le DCF a été conçu pour prendre en charge le transport de données asynchrones, transport dans lequel tous les utilisateurs qui veulent transmettre des données ont une chance égale d'accéder au support.

La sécurité

Dans les réseaux sans fil, le support est partagé. Tout ce qui est transmis et envoyé sur le support peut donc être intercepté. Pour permettre aux réseaux sans fil d'avoir un trafic aussi sécurisé que dans les réseaux fixes, le groupe de travail IEEE 802.11 a mis en place le protocole WEP *(Wired Equivalent Privacy)*, dont les mécanismes s'appuient sur le chiffrage des données et l'authentification des stations. D'après le standard, le protocole WEP est défini de manière optionnelle, et les terminaux ainsi que les points d'accès ne sont pas obligés de l'implémenter.

Pour empêcher l'écoute clandestine sur le support, le standard fournit un algorithme de chiffrement des données. Chaque terminal possède une clé

secrète partagée sur 40 ou 104 bits. Cette clé est concaténée avec un code de 24 bits, l'IV *(Initialization Vector)*, qui est réinitialisé à chaque transmission. La nouvelle clé de 64 ou 128 bits est placée dans un générateur de nombre aléatoire, appelé PRNG (RS4), venant de l'algorithme de chiffrement RSA *(Rivest Shamir Adelman)*. Ce générateur détermine une séquence de clés pseudo-aléatoires, qui permet de chiffrer les données. Une fois chiffrée, la trame peut être envoyée avec son IV. Pour le déchiffrement, l'IV sert à retrouver la séquence de clés qui permet de déchiffrer les données.

Le chiffrement des données ne protège que les données de la trame MAC et non l'en-tête de la trame de la couche physique. Les autres stations ont donc toujours la possibilité d'écouter les trames qui ont été chiffrées.

Associés au WEP, deux systèmes d'authentification peuvent être utilisés :

- Open System Authentication ;
- Shared Key Authentication.

Le premier définit un système d'authentification par défaut. Il n'y a aucune authentification explicite, et un terminal peut s'associer avec n'importe quel point d'accès et écouter toutes les données qui transitent au sein du BSS. Le second fournit un meilleur système d'authentification puisqu'il utilise un mécanisme de clé secrète partagée.

Le mécanisme standard d'authentification de Wi-Fi

Ce mécanisme fonctionne en quatre étapes :

1. Une station voulant s'associer avec un point d'accès lui envoie une trame d'authentification.
2. Lorsque le point d'accès reçoit cette trame, il envoie à la station une trame contenant 128 bits d'un texte aléatoire généré par l'algorithme WEP.
3. Après avoir reçu la trame contenant le texte, la station la copie dans une trame d'authentification et la chiffre avec la clé secrète partagée avant d'envoyer le tout au point d'accès.
4. Le point d'accès déchiffre le texte chiffré à l'aide de la même clé secrète partagée et le compare à celui qui a été envoyé plus tôt. Si le texte est identique, le point d'accès lui confirme son authentification, sinon il envoie une trame d'authentification négative.

La figure 17-2 décrit le processus d'authentification d'une station, reprenant les quatre étapes que nous venons de détailler.

Pour restreindre encore plus la possibilité d'accéder à un point d'accès, ce dernier possède une liste d'adresses MAC, appelée ACL *(Access Control List)*, qui ne permet de fournir l'accès qu'aux stations dont l'adresse MAC est spécifiée dans la liste.

Suite p. 402

Suite de la page 401

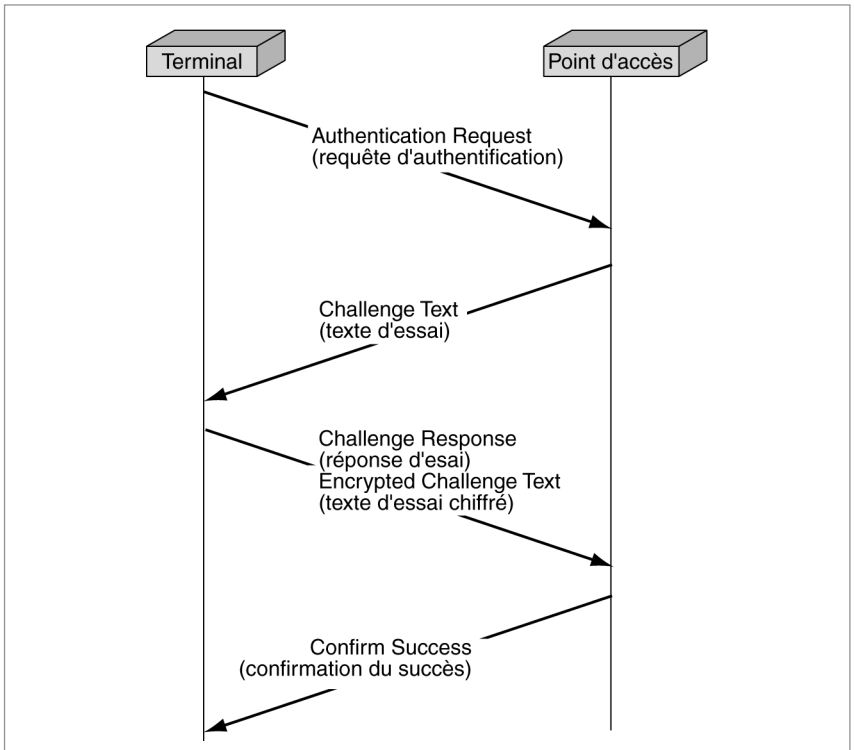

Figure 17-2. *Mécanisme d'authentification d'une station.*

Économie d'énergie

Les réseaux sans fil peuvent posséder des terminaux fixes ou mobiles. Le problème principal des terminaux mobiles concerne leur batterie, qui n'a généralement que peu d'autonomie. Pour augmenter le temps d'activité de ces terminaux mobiles, le standard prévoit un mode d'économie d'énergie.

Il existe deux modes de travail pour le terminal :

- Continuous Aware Mode ;
- Power Save Polling Mode.

Le premier correspond au fonctionnement par défaut : la station est tout le temps allumée et écoute constamment le support. Le second permet une économie d'énergie. Dans ce cas, le point d'accès tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie et stocke les données qui leur sont adressées. Les stations qui sont en veille s'activent à des

périodes de temps régulières pour recevoir une trame particulière, la trame TIM *(Traffic Information Map)*, envoyée par le point d'accès.

Entre les trames TIM, les terminaux retournent en mode veille. Toutes les stations partagent le même intervalle de temps pour recevoir les trames TIM, de sorte à toutes s'activer au même moment pour les recevoir. Les trames TIM font savoir aux terminaux mobiles si elles ont ou non des données stockées dans le point d'accès. Lorsqu'un terminal s'active pour recevoir une trame TIM et s'aperçoit que le point d'accès contient des données qui lui sont destinées, il envoie au point d'accès une requête, appelée *Polling Request Frame*, pour mettre en place le transfert des données. Une fois le transfert terminé, il retourne en mode veille jusqu'à réception de la prochaine trame TIM.

Pour des trafics de type broadcast ou multicast, le point d'accès envoie aux terminaux une trame DTIM *(Delivery Traffic Information Map)*, qui réveille l'ensemble des points concernés.

Questions-réponses

Question 3.– *Un réseau IEEE 802.11 s'appuie sur la technologie Ethernet. Montrer que l'interconnexion des points d'accès n'est généralement pas un problème en utilisant le réseau Ethernet de l'entreprise ?*

Réponse.– Comme IEEE 802.11 est compatible avec Ethernet, il est facile de faire circuler des trames Ethernet sur un réseau Ethernet entre deux point d'accès. C'est d'ailleurs le moyen le plus simple pour installer un réseau Wi-Fi : mettre régulièrement des points d'accès le long du réseau Ethernet de l'entreprise.

Question 4.– *Pourquoi l'attaque par dictionnaire consistant à tester tous les mots du dictionnaire est-elle l'une des plus utilisées ?*

Réponse.– Les utilisateurs choisissant pour la plupart un mot de passe provenant du dictionnaire, il est facile de tester tous les mots du dictionnaire pour trouver le mot de passe.

Question 5.– *Pourquoi les économies d'énergie constituent-elles un point faible des réseaux Wi-Fi ?*

Réponse.– La solution *Power Save Polling Mode* n'est pas obligatoire et n'est généralement pas mise en œuvre par les cartes Wi-Fi. De ce fait, le temps de vie d'une batterie d'un terminal Wi-Fi est assez faible. Le processeur Centrino d'Intel, qui intègre la norme 802.11, constitue une avancée importante dans ce domaine, car sa consommation d'énergie est extrêmement faible et permet aux batteries des PC qui en sont dotés de tenir un temps comparable à celui d'un même PC sans Wi-Fi.

IEEE 802.11b

Le réseau IEEE 802.11b provient de la normalisation effectuée sur la bande des 2,4 GHz. Cette norme a pour origine des études effectuées dans le cadre général du groupe IEEE 802.11.

En ce début des années 2000, la norme IEEE 802.11b s'est imposée comme standard, et plusieurs millions de cartes d'accès réseau Wi-Fi ont été vendues. Wi-Fi a d'abord été déployé dans les campus universitaires, les aéroports, les gares et les grandes administrations publiques et privées, avant de s'imposer dans les réseaux des entreprises pour permettre la connexion des PC portables et des équipements de type PDA.

Wi-Fi travaille avec des stations de base dont la vitesse de transmission est de 11 Mbit/s et la portée de quelques dizaines de mètres. Pour obtenir cette valeur maximale de la porteuse, il faut que le terminal soit assez près de la station de base, à moins d'une vingtaine de mètres. Il faut donc bien calculer, au moment de l'ingénierie du réseau, le positionnement des différents points d'accès. Si la station est trop loin, elle peut certes se connecter mais à une vitesse inférieure.

Aux États-Unis, treize fréquences sont disponibles sur la bande des 83,5 MHz. En Europe, lorsque la bande sera entièrement libérée, quatorze fréquences seront disponibles. Un point d'accès ne peut utiliser que trois fréquences au maximum, car l'émission demande une bande passante qui recouvre quatre fréquences.

Les fréquences peuvent être réutilisées régulièrement. De la sorte, dans une entreprise, le nombre de machines que l'on peut raccorder est très important et permet à chaque station terminale de se raccorder à haut débit à son serveur ou à un client distant.

Questions-réponses

Question 6.– *Montrer qu'avec trois fréquences disponibles, il est possible de faire un plan de fréquences.*

Réponse.– En effet, trois fréquences sont suffisantes pour réaliser un plan de fréquences dans lequel deux antennes qui utilisent la même fréquence n'ont que peu ou pas d'interférences.

Question 7.– *Pourquoi le débit effectif d'un réseau Wi-Fi est-il loin du débit théorique ?*

Réponse.– Tout d'abord, la station s'adapte à son environnement et émet à la vitesse maximale compte tenu des contraintes environnementales. Si la station est trop loin ou travaille avec des interférences, sa vitesse de transmission chute de 11 à 5,5, voire 2 ou même 1 Mbit/s. De plus, les temporisateurs destinés à éviter les collisions font perdre beaucoup de temps. Le débit moyen du point d'accès est alors bien plus faible que le débit théorique.

IEEE 802.11a et g

Les produits Wi-Fi provenant des normes IEEE 802.11a et g utilisent la bande des 5 GHz. Cette norme a pour origine des études effectuées dans le

cadre de la normalisation *HiperLAN* de l'ETSI au niveau européen en ce qui concerne la couche physique. La couche MAC de l'IEEE 802.11b est en revanche conservée.

HiperLAN *(High Performance Radio LAN).–* Normalisation européenne des réseaux locaux sans fil, dont les bandes de fréquences se situent entre 5 150 et 5 300 MHz.

Les produits Wi-Fi provenant de la norme 802.11a ne sont pas compatibles avec ceux de la norme Wi-Fi 802.11b, les fréquences utilisées étant totalement différentes. Les fréquences peuvent toutefois se superposer si l'équipement qui souhaite accéder aux deux réseaux comporte deux cartes d'accès. En revanche, les produits Wi-Fi 802.11g travaillant dans la bande des 2,4 GHz sont compatibles et se dégradent en 802.11b si un point d'accès 802.11b peut être accroché. Il y a donc compatibilité avec la norme 802.11b.

La distance maximale entre la carte d'accès et la station de base peut dépasser les 100 m, mais la chute du débit de la communication est fortement liée à la distance. Pour le débit de 54 Mbit/s, la station mobile contenant la carte d'accès ne peut s'éloigner que de quelques mètres du point d'accès. Au-delà, le débit chute très vite pour être approximativement équivalent à celui qui serait obtenu avec la norme 802.11b à 100 m de distance.

En réalisant de petites cellules, permettant une forte réutilisation des fréquences, et compte tenu du nombre important de fréquences disponibles en parallèle (jusqu'à 8), le réseau 802.11a permet à plusieurs dizaines de clients sur 100 m^2 de se partager plusieurs dizaines de mégabits par seconde. De ce fait, le réseau 802.11a est capable de prendre en charge des flux vidéo de bonne qualité.

La norme IEEE 802.11g a une tout autre ambition, puisqu'elle vise à remplacer la norme IEEE 802.11b sur la fréquence des 2,4 GHz, mais avec un débit supérieur à celui du 802.11b, atteignant théoriquement 54 Mbit/s mais pratiquement nettement moins, plutôt de l'ordre d'une vingtaine de mégabits par seconde.

Questions-réponses

Question 8.– *Montrer que la norme IEEE 802.11a a un potentiel plus important que 802.11b mais qu'elle a du mal à s'imposer.*

Réponse.– La norme IEEE 802.11a a un potentiel plus important que 802.11b parce qu'elle évolue sur une bande passante beaucoup plus large : 200 MHz contre 83 MHz. Dans le partitionnement en fréquence, 802.11a possède 8 bandes passantes contre seulement 3 pour les 2,4 GHz. La norme 802.11a a du mal à s'imposer car son installation est plus complexe et que la norme 802.11g lui fait une concurrence importante du fait de sa compatibilité avec 802.11b.

Qualité de service et sécurité

La qualité de service est toujours un élément essentiel dans un réseau. Les réseaux 802.11 posent de nombreux problèmes pour obtenir de la qualité de service. Tout d'abord, le débit réel du réseau n'est pas stable et peut varier dans le temps. Ensuite, le réseau étant partagé, les ressources sont partagées entre tous les utilisateurs se trouvant dans la même cellule.

En ce qui concerne la première difficulté, les points d'accès Wi-Fi ont la particularité assez astucieuse de s'adapter à la vitesse des terminaux. Lorsqu'une station n'a plus la qualité suffisante pour émettre à 11 Mbit/s, elle dégrade sa vitesse à 5,5 puis 2 puis 1 Mbit/s. Cette dégradation provient soit d'un éloignement, soit d'interférences. Cette solution permet de conserver des cellules assez grandes, puisque le point d'accès s'adapte. L'inconvénient est bien sûr qu'il est impossible de prédire le débit d'un point d'accès. On voit bien que si une station travaille à 1 Mbit/s et une autre à 11 Mbit/s, le débit réel du point d'accès est plus proche de 1 Mbit/s que de 11 Mbit/s. De plus, comme l'accès est partagé, il faut diviser le débit disponible entre les différents utilisateurs.

Le groupe de travail IEEE 802.11 a défini deux normes, 802.11e et 802.11i, dans l'objectif d'améliorer les diverses normes 802.11 en introduisant de la qualité de service et des fonctionnalités de sécurité et d'authentification.

Ces ajouts ont pour fonction de faire transiter des applications possédant des contraintes temporelles, comme la parole téléphonique ou les applications multimédias. Pour cela, il a fallu définir des classes de service et permettre aux terminaux de choisir la bonne priorité en fonction de la nature de l'application transportée.

La gestion des priorités s'effectue au niveau du terminal par l'intermédiaire d'une technique d'accès au support physique modifiée par rapport à celle utilisée dans la norme de base IEEE 802.11. Les stations prioritaires ont des temporisateurs d'émission beaucoup plus courts que ceux des stations non prioritaires, ce qui leur permet de toujours prendre l'avantage lorsque deux stations de niveaux différents essayent d'accéder au support.

Le protocole IEEE 802.11i devrait apporter une sécurité bien meilleure que celle proposée par le WEP. Il devrait être mis en œuvre à partir du début de 2005. Il utilise un algorithme de chiffrement plus performant, avec l'adoption de l'AES *(Advanced Encryption Standard)*. Déjà utilisé par la Défense américaine, ce standard a toutefois le défaut d'être incompatible avec la génération actuelle, de même qu'avec les extensions de sécurité en cours *(voir l'encadré sur la sécurité WPA)*. Le protocole IEEE 802.11i devrait être mis en œuvre avec la génération IEEE 802.11n à un débit de 320 Mbit/s.

La sécurité WPA *(Wi-Fi Protected Access)*

Les mécanismes de sécurité ont fortement progressé depuis le début des années 2000. Le WPA a été introduit en 2003. Il propose deux processus de sécurité : un WEP amélioré, appelé TKIP *(Temporal Key Integrity Protocol)*, et une procédure d'authentification des utilisateurs avec la norme IEEE 802.1x.

TKIP apporte une modification régulière des clés secrètes, de telle sorte que même un attaquant n'a pas le temps d'acquérir un nombre suffisant de trames pour avoir un espoir de casser les clés secrètes. La norme IEEE 802.1x apporte une authentification, qui déborde du strict cadre de l'environnement Wi-Fi. Cette authentification s'effectue comme expliqué au cours 7.

Questions-réponses

Question 9.– *Les terminaux Wi-Fi téléphoniques sont déjà présents en tant que produits sur le marché du Wi-Fi. Montrer que cette solution n'est généralement pas viable.*

Réponse.– Dans les réseaux Wi-Fi actuels, il n'y a pas de qualité de service. Les clients se succèdent dans un ordre relativement aléatoire pour accéder au point d'accès. Si un client connecté est en train d'émettre un gros fichier, ses paquets entrent en compétition avec les paquets de paroles et possèdent la même chance d'accès. Les paquets téléphoniques sont alors fortement retardés, et la probabilité qu'ils arrivent dans les temps au récepteur est faible. Pour que les terminaux Wi-Fi téléphoniques puissent fonctionner d'une façon raisonnable, ils doivent être seuls sur les points d'accès. La norme IEEE 802.11e devrait apporter une solution acceptable à ce problème, en attribuant une priorité forte aux paquets portant de la parole téléphonique.

Question 10.– *Pourquoi le protocole TKIP est-il une solution acceptable pour garantir la confidentialité ? Cette solution vous paraît-elle entraver les performances du réseau Wi-Fi ?*

Réponse.– TKIP permet de changer la clé secrète de chiffrement. Cet algorithme est donc une bonne réponse aux attaques par écoute en ne permettant pas à un attaquant de copier suffisamment de trames pour espérer en découvrir la clé secrète de chiffrement. Si le changement de clé est effectué trop souvent, il est évident que les performances en souffrent, car la distribution de clés est un algorithme complexe et consommateur de temps. Il ne faut donc pas changer la clé trop souvent pour rester dans les performances connues des réseaux IEEE 802.11.

WPAN et IEEE 802.15

Le groupe IEEE 802.15, intitulé WPAN *(Wireless Personal Area Networks)*, a été mis en place en mars 1999 dans le but de réfléchir aux réseaux d'une portée d'une dizaine de mètres, avec pour objectif de réaliser des connexions entre les différents portables d'un même utilisateur ou de plusieurs utilisateurs. Ce réseau peut interconnecter un PC portable (laptop), un téléphone portable, un PDA ou toute autre terminal de ce type. Trois groupes de services ont été définis, A, B et C.

Le groupe A utilise la bande du spectre sans licence d'utilisation (2,4 GHz) en visant un faible coût de mise en place et d'utilisation. La taille de la cellule autour du point d'émission est de l'ordre du mètre. La consommation électrique doit être particulièrement faible pour permettre au terminal de tenir plusieurs mois sans recharge électrique. Le mode de transmission choisi est sans connexion. Le réseau doit pouvoir travailler en parallèle d'un réseau 802.11, c'est-à-dire que sur un même emplacement physique il peut y avoir en même temps un réseau de chaque type, les deux pouvant éventuellement fonctionner de façon dégradée.

Le groupe B affiche des performances en augmentation avec un niveau MAC pouvant atteindre un débit de 100 Kbit/s. Le réseau de base doit pouvoir interconnecter au moins seize machines et proposer un algorithme de QoS, ou qualité de service, pour autoriser le fonctionnement de certaines applications, comme la parole téléphonique, qui demande une qualité de service assez stricte. La portée entre l'émetteur et le récepteur atteint une dizaine de mètres, et le temps maximal pour se raccorder au réseau ne doit pas dépasser la seconde. Enfin, cette catégorie de réseau doit posséder des passerelles avec les autres catégories de réseaux 802.15.

Le groupe C introduit de nouvelles fonctionnalités importantes pour particuliers ou entreprises, comme la sécurité de la communication, la transmission de la vidéo et la possibilité de roaming, ou itinérance, entre réseaux hertziens.

Pour répondre à ces objectifs, des groupements industriels se sont mis en place, comme Bluetooth. Bluetooth regroupe plus de 2 500 sociétés qui ont réalisé une spécification ouverte de connexion sans fil entre équipements personnels. Bluetooth est fondé sur une liaison radio entre deux équipements.

Le groupe de travail IEEE 802.15 s'est scindé en quatre sous-groupes :

- IEEE 802.15.1, pour satisfaire les contraintes des réseaux de catégorie C. Le choix de ce premier groupe s'est tourné vers le réseau Bluetooth, présenté en détail à la section suivante.
- IEEE 802.15.3, pour les contraintes posées par le groupe B, mais qui a finalement débouché sur une proposition très performante avec l'UWB *(Ultra-Wide Band)*, qui sera sur le marché en 2005.
- IEEE 802.15.4, pour les réseaux WPAN de catégorie A, qui a abouti à la proposition ZigBee, d'un réseau à bas débit mais à un coût extrêmement bas.
- IEEE 802.15.2, pour les interférences avec les autres réseaux utilisant la bande des 2,4 GHz.

Bluetooth

Le Bluetooth Special Interest Group, constitué au départ par Ericsson, IBM, Intel, Nokia et Toshiba et rejoint par plus de 2 500 sociétés, définit les spécifications de Bluetooth. Le nom de la norme est celui d'un chef Viking, Harald Bluetooth, qui aurait réussi à unifier les différents royaumes nordiques à la fin du Moyen Âge.

C'est une technologie peu onéreuse, grâce à la forte intégration sur une puce unique de 9 mm sur 9 mm. Les fréquences utilisées sont comprises entre 2 400 et 2 483,5 MHz. On retrouve la même gamme de fréquences dans la plupart des réseaux sans fil utilisés dans un environnement privé, que ce dernier soit personnel ou d'entreprise. Cette bande ne demande pas de licence d'exploitation.

Plusieurs schémas de connexion ont été définis par les normalisateurs. Le premier d'entre eux correspond à un réseau unique, appelé piconet, qui peut prendre en charge jusqu'à huit terminaux, avec un maître et huit esclaves. Le terminal maître gère les communications avec les différents esclaves. La communication entre deux terminaux esclaves transite obligatoirement par le terminal maître. Dans un même piconet, tous les terminaux utilisent la même séquence de saut de fréquence.

Un autre schéma de communication consiste à interconnecter des piconets pour former un scatternet, d'après le mot anglais *scatter*, dispersion. Comme les communications se font toujours sous la forme maître-esclave, le maître d'un piconet peut devenir l'esclave du maître d'un autre piconet. De son côté, un esclave peut être l'esclave de plusieurs maîtres. Un esclave peut se détacher provisoirement d'un maître pour se raccrocher à un autre piconet puis revenir vers le premier maître, une fois sa communication terminée avec le second.

La figure 17-3 illustre des connexions de terminaux Bluetooth dans lesquelles un maître d'un piconet est esclave du maître d'un autre piconet et un esclave est esclave de deux maîtres. Globalement, trois piconets sont interconnectés par un maître pour former un scatternet.

La communication à l'intérieur d'un piconet peut atteindre près de 1 Mbit/s. Comme il peut y avoir jusqu'à huit terminaux, la vitesse effective diminue rapidement en fonction du nombre de terminaux connectés dans une même picocellule. Un maître peut cependant accélérer sa communication en travaillant avec deux esclaves en utilisant des fréquences différentes.

Le temps est découpé en tranches, ou slots, à raison de 1 600 slots par seconde. Un slot fait donc 625 µs de long, comme illustré à la figure 17-4. Un terminal utilise une fréquence sur un slot puis, par un saut de fréquence (Frequency Hop), il change de fréquence sur la tranche de temps suivante, et ainsi de suite.

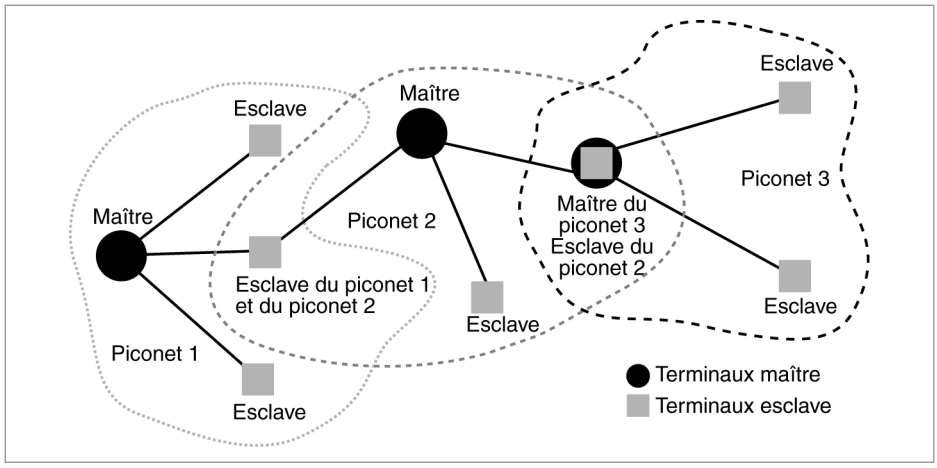

Figure 17-3. *Schéma de connexion de terminaux Bluetooth.*

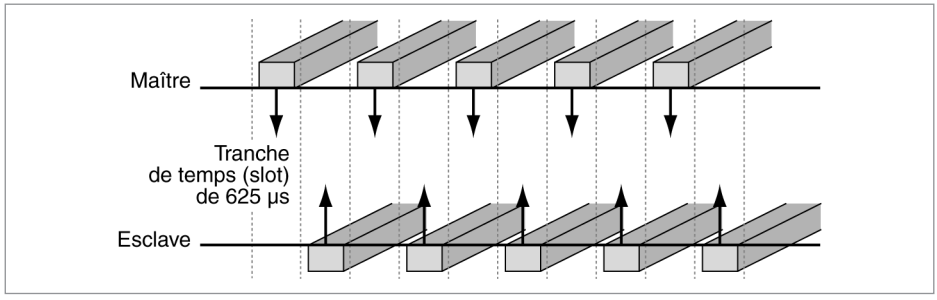

Figure 17-4. *Le découpage en slots.*

Un client Bluetooth utilise de façon cyclique toutes les bandes de fréquences. Les clients d'un même piconet possèdent la même suite de sauts de fréquence, et, lorsqu'un nouveau terminal veut se connecter, il doit commencer par reconnaître l'ensemble des sauts de fréquence pour pouvoir les respecter.

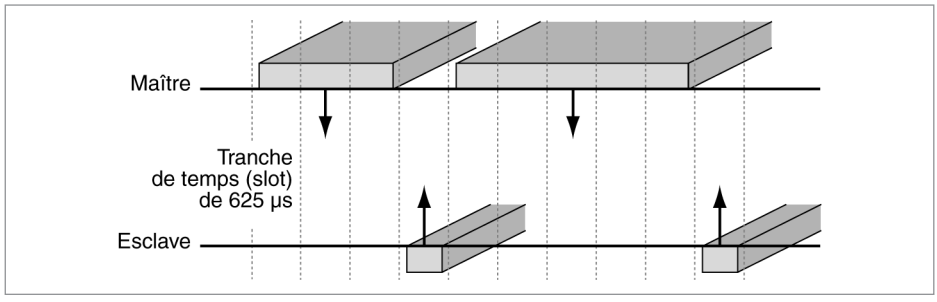

Figure 17-5. *Transmission sur plusieurs slots.*

Une communication s'exerce par paquet. En règle générale, un paquet tient sur un slot, mais il peut s'étendre sur trois ou cinq slots *(voir la figure 17-5)*. Le saut de fréquence a lieu à la fin de la communication d'un paquet.

Questions-réponses

Question 11.– *Pourquoi la portée de Bluetooth n'est-elle que de quelques mètres ?*

Réponse.– La portée n'est que de quelques mètres parce que la puissance d'émission est très faible, beaucoup plus faible que dans Wi-Fi

Question 12.– *La technique d'accès étant de type polling (la station maître interroge à tour de rôle les stations esclaves), montrer qu'une station a un débit minimal garanti.*

Réponse.– Comme le nombre maximal de terminaux esclaves est de sept, le temps nécessaire pour que chaque terminal ait un temps de parole est borné. Un terminal reçoit le droit d'émettre au moins à chaque tour de boucle. Si l'on suppose que toutes les stations sont actives et émettent la trame la plus longue qu'elles peuvent, le temps de réaliser le tour de boucle pour desservir l'ensemble des stations esclaves est le plus long possible et égal à T_{max}. Le débit minimal d'une station est obtenu dans ce cas. Ce débit minimal est garanti puisque la station est certaine de récupérer le droit d'émettre au moins tous les T_{max}.

WiMAX

Les réseaux métropolitains forment une catégorie de réseaux que l'on considère souvent comme la boucle locale radio (BLR). Ils sont aujourd'hui normalisés par la norme IEEE 802.16. Les produits associés sont appelés WiMAX. En réalité, il existe deux technologies WiMAX, l'une fixe et l'autre mobile. La phase 1 de WiMAX offre un débit de l'ordre de 80 Mbit/s et devrait monter à des valeurs de 500 Mbit/s en phase 2. Une phase 3 est déjà dans les cartons pour fournir des débits de l'ordre du Gbit/s.

La norme fixe a pour objectif de proposer des modems *x*DSL utilisant la voie hertzienne que l'on nomme WDSL (*Wireless DSL*). La norme IEEE 802.16 de base correspond aux liaisons radio *x*DSL fixes. La norme IEEE 802.16e apporte des liaisons *x*DSL hertziennes mobiles. Cette norme a été finalisée en 2005, et son déploiement a commencé en 2007. Acceptée comme réseau d'opérateur après validation par l'UIT, elle est totalement différente des solutions Wi-Fi par la possibilité d'obtenir une *qualité de service dure* et une disponibilité bien meilleure.

qualité de service dure.– Qualité de service totalement garantie, et non pas seulement avec une certaine probabilité, répondant à la demande des réseaux d'opérateurs.

Du point de vue des performances, les réseaux WiMAX atteignent un débit total de 80 Mbit/s. Les utilisateurs distribués dans la cellule correspondant à la portée de l'antenne WiMAX sont multiplexés. Le débit devrait être multiplié par un ordre de 10 vers 2010. Pour des portées d'une dizaine de kilomètres,

cette valeur de 80 Mbit/s correspond à des utilisations en zone rurale. Dans les zones urbaines, la puissance doit être réduite afin de ne pas dépasser un ou deux kilomètres de portée.

OFDMA (*Orthogonal Frequency Division Multiple Access*).– Technique d'accès permettant d'allouer une tranche de temps et plusieurs sous-bandes de fréquences simultanément après avoir découpé le spectre alloué.

Le réseau WiMAX mobile est considéré comme le premier réseau de quatrième génération, la 4G, qui succédera à la 3G à partir de 2010. On devrait plutôt parler de pré-4G puisque son débit est relativement faible par rapport aux produits 4G. Ses caractéristiques principales sont l'*OFDMA* et la compatibilité IP.

Les réseaux WiMAX auraient pu connaître un développement plus soutenu, mais les opérateurs ont trop peu investi entre 2005 et 2008. La compétition pour la suprématie 4G sera donc certainement forte, le WiMAX risquant ne pas avoir le temps de s'implanter durablement avant l'arrivée de la nouvelle génération de réseaux de mobiles.

Les classes de WiMAX

WiMAX possède quatre classes de priorités :

UGS (*Unsolicited Grant Service*), la priorité la plus haute, a pour objectif de faire transiter des applications à débit constant en générant des paquets de longueur fixe à des intervalles réguliers. Cette classe reçoit une allocation de tranches à intervalles réguliers de telle sorte que chaque paquet puisse être émis sans attente. Cette classe correspond aux applications de téléphonie classique, qui produisent un débit constant. C'est une classe provenant de l'ATM mais un peu plus sophistiquée : le CBR (*Constant Bit Rate*). Les paramètres de qualité de service sont le *Maximum Sustained Traffic Rate* (trafic moyen en période d'émission), le *Minimum Reserved Traffic Rate* (taux minimal à réserver pour que les paquets puissent passer) et le *Request/Transmission Policy* (indique la politique de retransmission). Dans cette classe, si une tranche de temps est réservée, elle ne peut être préemptée par une autre classe. Il y a donc possibilité de perte de la tranche si le client ne l'utilise pas. Comme nous le verrons avec le WiMAX mobile, une autre classe a été ajoutée pour la téléphonie compressée.

rtPS (*real-time Packet Service*) correspond à la transmission d'applications vidéo. Cette classe prend en charge les applications qui produisent des trames de longueur variable à intervalles réguliers. Les tranches de temps qui ne seraient pas utilisées peuvent être réutilisées. Les paramètres de qualité de service sont *Maximum Sustained Traffic Rate*, *Minimum Reserved Traffic Rate*, *Request/Transmission Policy*, comme dans l'UGS, et *Maximum Latency Traffic Priority* (indique le temps maximal entre deux trames prioritaires).

nrtPS (*non real-time Packet Service*) correspond à des applications élastiques qui acceptent une variabilité du délai et dont les paquets sont de tailles variables, mais qui demandent un débit minimal. Cette classe de trafic est bien adaptée au transfert de fichiers et aux applications sans contraintes temporelles mais qui exigent malgré tout un débit minimal pour être transmis après un temps correspondant à ce débit minimal. Les paramètres définissant la qualité de service sont *Maximum Sustained Traffic Rate*, *Request/Transmission Policy*, *Minimum Reserved Traffic Rate* (trafic minimal souhaité par l'utilisateur) et *Priority Traffic* (trafic des trames indispensables à l'application).

BE (*Best Effort*) ne demande aucune qualité de service particulière et aucun débit minimal. Les paramètres de cette classe de service sont *Maximum Sustained Traffic Rate*, *Traffic Priority* et *Request/Transmission Policy*. Les services associés sont bien entendu ceux qui n'exigent aucune garantie sur le trafic, comme le trafic des applications Web.

Questions-réponses

Question 13.– *La fréquence fixée en France pour les réseaux WiMAX est de 3,5 GHz. Est-ce une bonne fréquence ?*

Réponse.– Non. Cette fréquence est trop élevée et la propagation est fortement perturbée par les obstacles. Si la bande de fréquences été située en dessous de 1 GHz, la portée serait plus importante et la qualité de réception bien meilleure.

Question 14.– *Pourquoi les classes de services ne correspondent pas à celles de DiffServ ?*

Réponse.– Les classes de services de WiMAX correspondent davantage à la technique ATM qu'à l'environnement IP (et donc DiffServ). La raison à cela est que les études préparatoires ont été effectuées dans le monde des télécommunications, qui ont adopté ATM, plus que dans le monde IP soutenant DiffServ.

Question 15.– *Pourquoi la technique WiMAX mobile est-elle interdite en France en 2008 ?*

Réponse.– La technique WiMAX mobile est concurrente de l'UMTS et de ses dérivées de type HSDPA ou HSUPA. Ces dernières ont nécessité l'achat d'une licence 3G très chère par les opérateurs, tandis que les licences WiMAX ont été obtenues à relativement bas prix.

Les réseaux ad-hoc

Les réseaux ad-hoc sont des réseaux spontanés, qui peuvent se mettre en place sans le secours de stations fixes ni de points d'accès et dans lesquels tout est mobile. À peine initialisés, leurs nœuds sont capables, en l'espace de quelques instants, d'échanger de l'information en fonction de leur localisation

L'introduction des réseaux ad-hoc est récente, bien que cette technique soit depuis longtemps testée par les fabricants d'équipements militaires. Du fait de l'absence de structure fixe, le coût de mise en œuvre de ces réseaux est relativement faible, même si le logiciel de contrôle des machines participantes est complexe. Ils ne nécessitent aucune infrastructure, si ce n'est un terminal par utilisateur.

En règle générale, les systèmes de télécommunications demandent beaucoup de temps pour être mis en place. Il n'en va pas de même des réseaux ad-hoc, qui s'appuient sur une infrastructure minimale et ne requièrent pas d'intervention d'administrateur, que ce soit pour leur mise en place ou pour leur gestion. Ils peuvent donc être installés très rapidement, par exemple pour couvrir des événements comme les spectacles sportifs, les conférences ou les festivals.

Un autre type d'application pourrait utiliser ce type de réseau là où les moyens de communication sont inexistants ou détruits, par exemple par une catastrophe naturelle, comme un tremblement de terre.

La particularité d'un réseau ad-hoc provient de la présence dans chaque nœud du réseau d'un logiciel assurant le routage des paquets IP. La solution la plus simple est évidemment d'avoir un routage direct, dans lequel chaque station du réseau peut atteindre directement une autre station sans passer par un nœud intermédiaire. Ce cas ne peut convenir qu'à de petites cellules, d'un diamètre inférieur à 100 m.

Le routage le plus classique des réseaux ad-hoc consiste à faire transiter les paquets par des nœuds intermédiaires dotés de tables de routage. Toute la problématique de tels réseaux est d'optimiser ces tables de routage par des mises à jour plus ou moins régulières. Si les mises à jour sont très régulières, le routage des paquets est rapide, mais au risque de surcharger le réseau. Si les mises à jour ne sont effectuées que lors de l'arrivée de nouveaux flots, cela restreint la charge d'information de supervision circulant dans le réseau mais rend plus délicate la recherche d'une route.

De nombreux écueils peuvent compliquer la constitution de la table de routage. La liaison peut être asymétrique, par exemple, un sens de la communication étant acceptable et l'autre pas. De plus, les signaux peuvent être soumis à des interférences, comme c'est souvent le cas dans les espaces hertziens.

Pour toutes ces raisons, les routes du réseau doivent être sans cesse modifiées, d'où l'éternelle question débattue : faut-il maintenir ou non les tables de routage dans les nœuds mobiles d'un réseau ad-hoc ? En d'autres termes, vaut-il la peine de maintenir à jour des tables de routage qui changent sans arrêt et n'est-il pas plus judicieux de déterminer la table de routage au denier moment ?

Deux grandes familles de protocoles ont été constituées à partir de la normalisation des réseaux ad-hoc, les protocoles réactifs et les protocoles proactifs :

- **Protocoles réactifs.** Ces protocoles travaillent par inondation pour déterminer la meilleure route à suivre lorsqu'un flot de paquets est prêt à être émis. Il n'y a donc pas d'échange de paquets de contrôle, à l'exception des paquets de supervision, qui permettent de déterminer par inondation le chemin pour émettre le flot. Le paquet de supervision qui est diffusé vers tous les nœuds voisins est de nouveau diffusé par ces derniers jusqu'au récepteur. Il est de la sorte possible d'emprunter soit la route déterminée par le premier paquet de supervision arrivé au récepteur, soit d'autres routes en cas de problème sur la route principale.

- **Protocoles proactifs.** Ces protocoles émettent sans arrêt des paquets de supervision afin de maintenir la table de routage en ajoutant de nouvelles lignes et en en supprimant certaines. Les tables de routage sont donc dynamiques et sont modifiées chaque fois qu'une information de supervision influe de façon substantielle sur le comportement du réseau. Une difficulté de cette catégorie de protocoles provient du calcul des tables de routage pour qu'elles soient cohérentes.

Nous décrivons dans les sections qui suivent les deux protocoles issus du groupe de travail MANET *(Mobile Ad Hoc Network)* de l'IETF qui ont été normalisés. Ces protocoles sont représentatifs des deux grandes techniques que nous venons d'introduire.

AODV *(Ad-hoc On Demand Distance Vector)*

AODV est un protocole réactif fondé sur le principe des vecteurs de distance, c'est-à-dire, dans le cas le plus simple, du nombre de sauts entre l'émetteur et le récepteur.

Quand une application a besoin d'envoyer un flot de paquets dans le réseau et qu'une route est disponible dans la table de routage, AODV ne joue aucun rôle. S'il n'y a pas de route disponible, le protocole AODV a pour tâche de trouver la meilleure route.

Cette recherche commence par une inondation de paquets RREQ *(Route REQuest)*. Chaque nœud traversé par un RREQ en garde une trace dans sa mémoire cache et le retransmet. Quand les paquets de recherche de route arrivent à destination ou à un nœud intermédiaire qui connaît lui-même une route valide jusqu'a la destination, un paquet de réponse est généré (RREP) et est envoyé par le chemin inverse, grâce aux informations gardées dans les caches des nœuds traversés par les RREQ.

AODV dispose d'un certain nombre de mécanismes optimisant son fonctionnement. L'inondation se fait, par exemple, au premier essai dans un rayon limité autour de la source. Si aucun chemin n'est trouvé, l'inondation est étendue à une plus grande partie du réseau. En cas de rupture de certains liens, AODV essaie de reconstruire localement les routes rejetées en trouvant des nœuds suppléants. Cette détection de rupture peut d'ailleurs se faire grâce à un mécanisme optionnel de paquets Hello diffusés aux voisins directs.

Si une reconstruction locale n'est pas possible, les nœuds concernés par la rupture des routes utilisant ce lien sont prévenus de sorte qu'ils puissent relancer une nouvelle phase de reconstruction complète.

OLSR *(Optimized Link State Routing)*

OLSR est un protocole proactif à état de lien. Afin de maintenir à jour les tables de routage, chaque nœud implémentant OLSR diffuse régulièrement des informations sur son propre voisinage. Ces informations sont suffisantes pour permettre à chaque nœud de reconstruire une image du réseau et de trouver une route vers n'importe quelle destination.

Contrairement à ce qui se passe dans des protocoles tels qu'OSPF, cette diffusion ne se fait pas par une simple inondation, dans laquelle chaque nœud retransmet simplement chaque nouveau paquet qu'il reçoit. OLSR optimise la diffusion grâce à un système de relais multipoint, appelé MPR *(Multi-Point Relay)*.

Chaque nœud choisit dans ses voisins directs un sous-ensemble minimal de nœuds qui lui permettent d'atteindre tous ses voisins à deux sauts. La diffusion des informations sur les liens utilisées pour le routage se fait ensuite uniquement par les relais multipoint. La couverture totale du réseau est assurée tout en limitant sensiblement le nombre de réémissions. Afin de choisir ses relais multipoint, un nœud a besoin de connaître la topologie complète de son voisinage à deux sauts. Il envoie pour cela périodiquement des paquets Hello contenant la liste des voisins à un saut connus.

L'utilisation des réseaux ad-hoc est intéressante dès que l'on ne peut plus avoir une surface totalement recouverte par les cellules de base. On peut alors étendre l'accès à une cellule du réseau en utilisant des sauts ad-hoc jusqu'à arriver à la cellule. De façon plus précise, le terminal qui ne peut se connecter du fait qu'il se trouve hors de portée d'une cellule Wi-Fi peut se connecter à des stations faisant office de routeurs intermédiaires, autrement dit de nœuds capables de prendre des décisions de routage pour acheminer les paquets vers d'autres nœuds ou des points d'accès

Contrairement à ce qui se passe dans un réseau en mode ad-hoc, la taille du réseau ne dépend pas de la zone de couverture de la station connectée mais du nombre de stations mobiles composant le réseau. La distance entre les stations est limitée par la technique utilisée et l'environnement dans lequel le réseau est installé.

Questions-réponses

Question 16.– *L'option* ad-hoc *des réseaux Wi-Fi correspond-elle vraiment à un réseau ad-hoc ?*

Réponse.– Non. L'option *ad-hoc* des réseaux Wi-Fi ne correspond qu'à une transmission d'un terminal vers un autre, sans possibilité de routage vers un destinataire distant.

Question 17.– *Deux options ont été normalisées pour le routage dans les réseaux ad-hoc. La première solution utilise l'inondation (solution active) et la seconde la mise à jour constante des tables de routage (solution proactive). Dans quel cas, la première solution vous paraît-elle meilleure que la seconde ?*

Réponse.– La solution active cherche à mettre à jour les tables de routage au moment où un terminal souhaite transmettre. La solution proactive essaie de maintenir les tables de routage à jour indépendamment des instants de transmission. La première solution est meilleure lorsque les stations terminales bougent beaucoup et rapidement et que le réseau n'est pas trop important. La solution proactive est meilleure lorsque les terminaux se déplacent peu et que le réseau est important.

Exercices

Les corrigés de ces exercices se trouvent pp. 489-490.

1

Soit un réseau Wi-Fi travaillant à la vitesse de 11 Mbit/s.

a Pourquoi le débit effectif est-il très inférieur à la valeur théorique ?

b Si 11 clients se partagent les ressources d'une cellule, pourquoi chaque utilisateur ne reçoit-il pas plus de 1 Mbit/s en moyenne ?

c Quel peut être le débit théorique maximal dans une cellule ?

d Un client captant les signaux de deux points d'accès doit choisir le point d'accès sur lequel il va se connecter. À votre avis, comment s'effectue ce choix ?

e Si un point d'accès 802.11b se trouve au même endroit qu'un point d'accès 802.11a, quel est l'impact sur le débit ?

f Si deux clients accèdent à un même point d'accès avec des vitesses différentes (par exemple, l'un à 11 Mbit/s et l'autre à 1 Mbit/s), à quelle vitesse le point d'accès doit-il émettre ses trames de supervision ?

g Si deux client se partagent un point d'accès, l'un travaillant à 11 Mbit/s et l'autre à 1 Mbit/s, quel est le débit effectif moyen du point d'accès, en supposant que la partie supervision occupe la moitié du temps de la station d'accès ?

h Quelle solution préconisez-vous pour maintenir un haut débit dans la cellule ?

i Si une carte Wi-Fi pouvait émettre automatiquement à une puissance suffisante pour atteindre le point d'accès, cela allongerait-il le temps de vie des batteries ?

2

Soit un réseau Wi-Fi travaillant à la vitesse de 11 Mbit/s. Les cartes d'accès ainsi que le point d'accès peuvent moduler leur puissance d'émission.

a Si l'on diminue la puissance d'un point d'accès de 100 mW à 10 mW, par exemple, quelles sont les conséquences sur la taille de la cellule ?

b Montrer qu'il faut beaucoup plus de points d'accès pour recouvrir un même territoire.

c Augmente-t-on ainsi la capacité globale du réseau ?

d La mobilité est-elle réduite ?

3

Soit un réseau Bluetooth.

a Pourquoi un réseau Bluetooth peut-il coexister sur la bande des 2,4 GHz avec un réseau Wi-Fi ?

b Montrer que le saut de fréquence est une solution qu'il est plus difficile d'écouter.

c La vitesse du réseau Bluetooth vous paraît-elle suffisante pour transporter de la vidéo ?

4 *On aimerait développer un réseau Wi-Fi de future génération ayant des propriétés meilleures que celles des réseaux Wi-Fi actuels.*

a Montrer qu'un premier inconvénient des réseaux actuels est de ne pas avoir la possibilité de choisir la fréquence entre la bande des 2,4 et des 5 GHz. Qu'en déduisez-vous comme amélioration ?

b Montrer qu'un contrôle de puissance permettrait d'améliorer le débit global d'un réseau Wi-Fi.

c Une bonne partie de la bande passante est perdue par le point d'accès à cause de la supervision et des temporisateurs de démarrage des accès des terminaux vers le point d'accès. Pouvez-vous proposer des améliorations ?

d La détérioration de la capacité d'un point d'accès provient en grande partie de l'éloignement de certains utilisateurs. Pourquoi ? Quel pourrait être le remède ? Indiquer les conséquences du remède proposé.