# Réseaux sans fil dans les pays en développement

Un guide pratique pour la planification et la construction d'infrastructures de télécommunication à bas prix

# Réseaux sans fil dans les pays en développement

Pour plus d'informations sur ce projet, visitez notre site: *http://wndw.net/*

Première édition, Janvier 2006
Édition en français, Novembre 2006

ISBN10: 0-9778093-2-3
ISBN13: 978-0-9778093-2-5

# Table des matières

# Matériel réseau



# Sécurité



# Construire un noeud extérieur



# Dépannage



# Études de Cas

# Avant-propos

Ce livre fait partie d'une collection de matériel en rapport avec le réseautage sans fil dans les pays en développement. Tous les documents de la collection ne sont pas disponibles au moment de cette première parution, mais la collection complète comportera:

- Des livres imprimés ;
- Une version PDF Sans-GDN (DRM-Free) du livre ;
- Une liste de discussion archivée sur les concepts et techniques décrits dans ce livre ;
- Des études de cas additionnelles, du matériel et de l'information pour des cours de formation.

Pour avoir accès à tout ce matériel et plus, visitez notre site Web à *http://wndw.net/*



Consultez le site Web (*http://wndw.net/*) pour plus de détails concernant la commande d'une copie imprimée. Le document PDF sera mis à jour périodiquement et la commande à partir du service d'impression à la demande s'assurera que vous recevrez toujours la dernière version.

Le site Web inclura des études de cas additionnelles, l'équipement disponible actuellement et plus de références provenant de sites Web externes. Volontaires et idées sont les bienvenus. Veuillez s'il-vous-plaît joindre notre liste de discussion et nous envoyer vos idées.

Le matériel de formation a été écrit pour des cours offerts par l'Association pour le Progrès des Communications et l'*Abdus Salam International Center for Theoretical Physics*. Veuilliez-vous référer *http://www.apc.org/wireless/* et *http://wireless.ictp.trieste.it/* pour plus de détails sur ces cours et leurs matériels didactiques. L'information additionnelle a été offerte par l'*International Network for the Availability of Scientific Publications*, *http://www.inasp.info/*. Quelques-uns de ces matériels ont été directement incorporés à ce livre.

# Crédits

Ce livre a été initié comme un projet BookSprint durant la session 2005 de la conférence WSFII à Londres, Angleterre (*http://www.wsfii.org/*). Une équipe initiale de sept personnes en a établi les premières grandes lignes au cours de l'événement, a présenté les résultats à la conférence et a écrit le livre en quelques mois. Rob Flickenger a fait figure d'auteur et d'éditeur principal.

Au cours du projet, le groupe initial et central a activement sollicité des contributions et la rétroaction de la communauté de réseaux sans fil.

## Groupe central

- **Corinna "Elektra" Aichele**. Les intérêts principaux d'Elektra incluent les systèmes d'énergie autonomes et la communication sans fil (antennes, connexions sans fil sur une longue distance, réseautage maillé). Elle a réalisée une petite distribution de Linux Slackware relié à un réseautage maillé sans fil. Cette information est évidemment redondante si nous lisons le livre... *http://www.scii.nl/~elektra*
- **Rob Flickenger** a été l'auteur, l'éditeur et l'illustrateur principal de ce livre. Rob est écrivain professionnel depuis 2002. Il a écrit et édité plusieurs livres, incluant *Building Wireless Community Networks* ainsi que *Wireless Hacks*, publiés par O'Reilly Media. Il a été le co-fondateur de Metrix Communication LLC (*http://metrix.net/*), une compagnie de matériel sans fil dédiée aux logiciels open source et open standards (logiciels libres) et au réseautage sans fil ubiquitaire. Avant de devenir un membre actif de *SeattleWireless* (*http://seattlewireless.net/*), il a été le père fondateur du projet *NoCat* (*http://nocat.net/*).

  Le but de Rob est la réalisation de la *Largeur de bande infinie, partout et gratuite* (*Infinite Bandwidth Everywhere for Free*).
- **Carlo Fonda** est membre de l'Unité de Radio Communications à l' *Abdus Salam International Center for Theoretical Physics* à Trieste, Italie.
- **Jim Forster** a dédié sa carrière au développement de logiciels. Il a surtout travaillé sur les systèmes d'explotation et sur la réseautique au sein de compagnies dans le domaine. Il détient de l'expérience au sein de plusieurs nouvelles compagnies de Silicon Valley. Certaines ayant connu

un échec, et une ayant particulièrement réussi, à savoir *Cisco Systems*. Après y avoir consacré plusieurs années de travail en développement de produits, ses plus récentes activités incluent le travail sur des projets et des politiques pour améliorer l'accès à Internet dans les pays en développement. Il peut être contacté à *jrforster@mac.com*.

- **Ian Howard.** Après avoir volé à travers le monde durant sept ans comme parachutiste de l'armée canadienne, Ian Howard a décidé d'échanger son fusil contre un ordinateur.

  Après avoir terminé un baccalauréat en sciences environnementales à l'Université de Waterloo, il a écrit dans une proposition: « la technologie sans fil a la possibilité de réduire la brèche digitale. Les nations pauvres, qui ne possèdent pas comme nous l'infrastructure pour l'inter-connectivité, auront à présent l'opportunité de créer une infrastructure sans fil ». Comme récompense, *Geekcorps* l'envoya au Mali comme responsable de programme où il a travaillé à la tête d'une équipe oeuvrant á l'équipement de stations de radio avec des connexions sans fil et où il conçu des systèmes de partage de données.

  Il est actuellement un consultant pour plusieurs programmes *Geekcorps*.

- **Tomas Krag** consacre ses jours à travailler avec *wire.less.dk*, une compagnie enregistrée sans but lucratif qu'il a fondé, avec son ami et collègue Sebastian Büttrich, au début de 2002 et qui est installée à Copenhague. *wire.less.dk* se spécialise dans les solutions de réseautage sans fil communautaire et se concentre particulièrement sur les réseaux sans fil à bas prix pour les pays en développement.

  Tomas est aussi associé à la *Tactical Technology Collective http://www.tacticaltech.org/*, une organisation sans but lucratif située à Amsterdam qui se dédie à « renforcer les mouvements technologiques sociaux et les réseaux dans les pays en développement et en transition, ainsi qu'à promouvoir l'usage efficace, conscient et créatif des nouvelles technologies de la part de la société civile ». Actuellement, la plus grande partie de son énergie se concentre sur le projet *Wireless Roadshow* (*http://www.thewirelessroadshow.org/*), une initiative qui appuie les partenaires de la société civile dans les pays en développement dans la planification, la construction et la viabilité des solutions de connectivité basées sur l'utilisation de spectres à exemption de licences, de technologie et de connaissances libres.

- **Marco Zennaro**, aussi connu sous le nom de Marcus Gennaroz, est un ingénieur en électronique travaillant à l'ICTP à Trieste, Italie. Depuis son adolescence, il fait usage des BBS (ou babillards électroniques) et est un radioamateur. Il est donc heureux d'avoir été en mesure de fusionner les deux champs en travaillant dans le domaine du réseautique sans fil. Il apporte toujours son Apple Newton.

En plus du groupe principal, plusieurs ont contribué par leurs écrits, rétroactions, corrections et d'autres qualités qui font de ce projet ce qu'il est présentement.

## Contributors

- **Sebastian Büttrich** (*http://wire.less.dk/*) est un généraliste en technologie avec une formation en programmation scientifique et physique. Originaire de Berlin, Allemagne, il a travaillé pour *IconMedialab* à Copenhague de 1997 à 2002. Il détient un Doctorat en physique quantique de l'Université Technique de Berlin. Sa formation en physique englobe des domaines tels que les dispositifs RF et la spectroscopie micro-ondes, les systèmes photovoltaïques et les mathématiques avancées.

  Il est également un musicien professionnel.

- **Kyle Johnston,** *http://www.schoolnet.na/*

- **Adam Messer**. Avec une formation initiale d'entomologiste, Adam Messer s'est métamorphosé en professionnel des télécommunications après qu'une conversation fortuite en 1995 l'ait mené à créer l'un des premiers Fournisseur d'Accès à Internet (FAI) de l'Afrique. Devenant un des pionniers dans le domaine des services de données sans fil en Tanzanie, Messer a travaillé durant 11 ans en Afrique de l'Est et du Sud dans le domaine de la transmission de la voix et des données tant pour des nouvelles entreprises que pour des compagnies multinationales de cellulaires. Il réside présentement à Amman, Jordanie.

- **Ermanno Pietrosemoli** s'est consacré au cours des vingt dernières années à planifier et construire des réseaux d'ordinateurs. Comme président de l'École Latino-américaine de Réseaux, *Escuela Latinoamericana de Redes "EsLaRed"*, *www.eslared.org.ve*, il a enseigné dans le domaine des données de communication sans fil dans plusieurs pays tout en conservant sa base à Mérida, Venezuela.

- **Dana Spiegel** est un consultant indépendant en logiciels et fondateur de *sociableDESIGN* (*www.sociableDESIGN.com*), une firme de consultants qui se spécialise en logiciels sociaux et les technologies sans fil. Il est également Directeur Exécutif et membre du Conseil d'Administration de *NYCwireless* (*www.nycwireless.net*), une organisation sans but lucratif situé à New York City qui préconise et permet la croissance des réseaux sans fils libres et publics. Il écrit aussi le blog *Wireless Community* (*www.wirelesscommunity.info*).

## Appuis

- **Lisa Chan** (*http://www.cowinanorange.com/*)**:** l'éditrice principale.
- **Richard Lotz** (*http://greenbits.net/~rlotz/*) a réalisé une révision technique et a fournit différentes suggestions. Il travaille sur des projets *SeattleWireless* et préfère laisser son noeud (et sa maison) déconnectés.
- **Casey Halverson** (*http://seattlewireless.net/~casey/*) a réalisé une révision technique et a fournit différentes suggestions.
- **Catherine Sharp** (*http://odessablue.com/*) a offert son appui pour l'édition.
- **Matt Westervelt** (*http://seattlewireless.net/~mattw/*) a réalisé une révision technique et a offert son appui pour l'édition. Matt est le fondateur de *SeattleWireless* (*http://seattlewireless.net/*) et un « évangéliste » de la cause de FreeNetworks partout à travers le monde. Il a abandonné le monde corporatif pour donner naissance à Metrix Communication LLC (*http://metrix.net/*), une compagnie créée pour approvisionner *FreeNetworkers* en produits de réseautage sans fil basés sur des standards de haute qualité. Étant enfant, il a beaucoup écouté La rue Sésame et a la ferme conviction (peut-être erronée) que la coopération peut résoudre plusieurs des problèmes du monde.

## Remerciements spéciaux

Le groupe central voudrait remercier les organisateurs de la conférence WSFII pour avoir facilité l'espace, le support et également fourni la largeur de bande qui ont servi comme incubateur de ce projet. Nous voudrions tout particulièrement remercier les réseauteurs communautaires partout dans le monde, qui dédient autant de temps et d'énergie afin d'atteindre la promesse de l'Internet global. Sans vous, les réseaux communautaires ne pourraient exister.

L'équipe Booksprint veut remercier les importantes contributions de collègues et amis partout autour du globe ayant rendu possible la traduction dans diverses langues du livre « Réseaux sans fil dans les pays en développement ».

La traduction française a été réalisée par Alexandra Dans, et révisée par Ian Howard, Nadia Haouel, Marouen Mraihi, Stéphane Nicolas, Frédéric Renet, François Proulx, Victor Tonon et Antoine Guillemot. Toutes leurs contributions ont été éditées par Jean-Philippe Dionne, notre rédacteur en chef, responsable de garantir que les concepts techniques ont été préservés et exprimés correctement. La coordination de cet effort collectif a été développée à travers l'initiative WiLAC, *http://www.wilac.net*

# 1
# Par où commencer?

Ce livre a été écrit par une équipe composée d'individus dont les compétences ont permis de contribuer à l'expansion sans borne d'Internet, repoussant ainsi ses limites plus loin que jamais. La grande popularité des réseaux sans fil provoque une baisse continuelle des coûts des équipements, alors que leur capacité ne cesse d'augmenter. En appliquant cette technologie dans les régions ayant un important besoin d'infrastructures de communication, un plus grand nombre de personnes pourront être connectées en moins de temps et à faible coût.

Nous espérons non seulement vous convaincre que ceci est possible, mais aussi vous montrer comment nous avons construit de tels réseaux. Nous présenterons l'information et les outils dont vous aurez besoin pour démarrer un projet de réseau dans votre communauté locale.

L'infrastructure sans fil peut être bâtie à de très bas coûts en comparaison aux alternatives câblées traditionnelles. Mais on ne construit pas des réseaux sans fil uniquement pour économiser. En fournissant plus facilement et à moindre coût l'accès à Internet à votre communauté locale, celle-ci profitera directement de ce qu'Internet a à offrir. Le temps et l'effort ménagés pour donner accès au réseau global d'information se traduisent en source de richesse à l'échelle locale car plus de travail peut être accompli en moins de temps et avec moins d'efforts.

De plus, le réseau accroît sa valeur si plus de personnes y sont connectées. Les communautés connectées à Internet haute vitesse ont une voix dans le marché global, où les transactions se succèdent à la vitesse de la lumière autour du monde. Les gens sont en train de réaliser partout dans le monde que l'accès à Internet leur donne une voix pour discuter de leurs problèmes, de politique et tout ce qui est important dans leurs vies, d'une façon que ni le téléphone ni la télévision ne peuvent concurrencer. Ce qui jusqu'à tout ré-

cemment encore apparaissait comme de la science fiction est maintenant en train de devenir une réalité, et cette réalité se construit sur des réseaux sans fil.

Mais même sans accès à Internet, les réseaux de communauté sans fil ont une valeur énorme. Ils permettent aux personnes de collaborer dans des projets, peu importe la distance qui les sépare. Les communications vocales, le courriel et autres données peuvent s'échanger à des coûts très bas. En faisant participer les personnes des communautés locales dans la construction du réseau, la connaissance et la confiance sont répandues dans toute la communauté, et les gens commencent à comprendre l'importance de jouer un rôle dans leur infrastructure de communications. En effet, ils se rendent compte que les réseaux de communication sont construits pour permettre aux personnes de se connecter les unes aux autres.

Dans ce livre, nous nous concentrerons sur les technologies de réseaux de données sans fil de la famille 802.11. Même si un réseau de la sorte peut transporter des données, de la voix et des vidéos (tout comme le trafic traditionnel Web et Internet), les réseaux décrits dans ce livre sont des réseaux de données. En particulier, nous n'aborderons pas les GSM, CDMA ou autres technologies de voix sans fil puisque le coût de déploiement de ces technologies est bien au-dessus des possibilités de la plupart des projets communautaires.

## But de ce livre

Le but global de ce livre est de vous aider à construire dans votre communauté locale une technologie de communication accessible en faisant le meilleur usage possible des ressources disponibles. En utilisant un équipement peu onéreux, vous pouvez construire des réseaux de données de haute vitesse capables de connecter des zones éloignées entre-elles, fournir un réseau à large bande passante dans des zones sans services téléphoniques et finalement connecter vos voisins et vous-même à l'Internet global. En utilisant des ressources locales pour les matériaux et en fabriquant vous-même certaines parties, vous pouvez construire des liens de réseau fiables avec un budget très restreint. Et en travaillant avec votre communauté locale, vous pouvez construire une infrastructure de télécommunication dont tous ceux qui y participent peuvent profiter.

Ce livre n'est pas un guide pour configurer une carte radio dans votre portable ou pour choisir des matériels pour les consommateurs typiques afin d'équiper votre réseau à la maison. L'emphase est mise sur la construction d'infrastructures destinées à être employées comme une épine dorsale pour de grands réseaux sans fil. Avec ce but en tête, l'information est présentée à partir de plusieurs points de vue, incluant les facteurs techniques, sociaux et

financiers. L'importante collection d'études de cas présente les expériences de plusieurs groupes dans la construction de ces réseaux, les ressources qui y ont été investies et les résultats de ces essais.

Depuis les toutes premières expériences à la fin du dernier siècle, la communication sans fil est devenue un champ en rapide évolution dans le domaine des technologies de la communication. Même si nous offrons des exemples spécifiques portant sur la construction de dispositifs de transfert de données à haute vitesse, les techniques décrites dans ce livre ne visent pas à remplacer l'infrastructure câblée existante (comme les systèmes téléphoniques et les épines dorsales de fibre optique). Ces techniques visent plutôt à élargir les systèmes existants en fournissant une connectivité à des zones où des installations de fibre ou de tout autre câble physique, seraient impraticables.

Nous souhaitons que ce livre vous soit d'utilité dans la résolution de vos propres enjeux communicationnels.

# Adapter votre réseau actuel à la technologie sans fil

Si vous êtes un administrateur de réseau, vous vous demandez peut-être comment la technologie sans fil peut s'adapter à votre infrastructure de réseau actuelle. La technologie sans fil peut être utilisée de plusieurs façons: comme une simple extension (comme un câble Ethernet de plusieurs kilomètres) à un point de distribution (comme un grand commutateur externe). Voici seulement quelques exemples décrivant comment votre réseau peut bénéficier de la technologie sans fil.

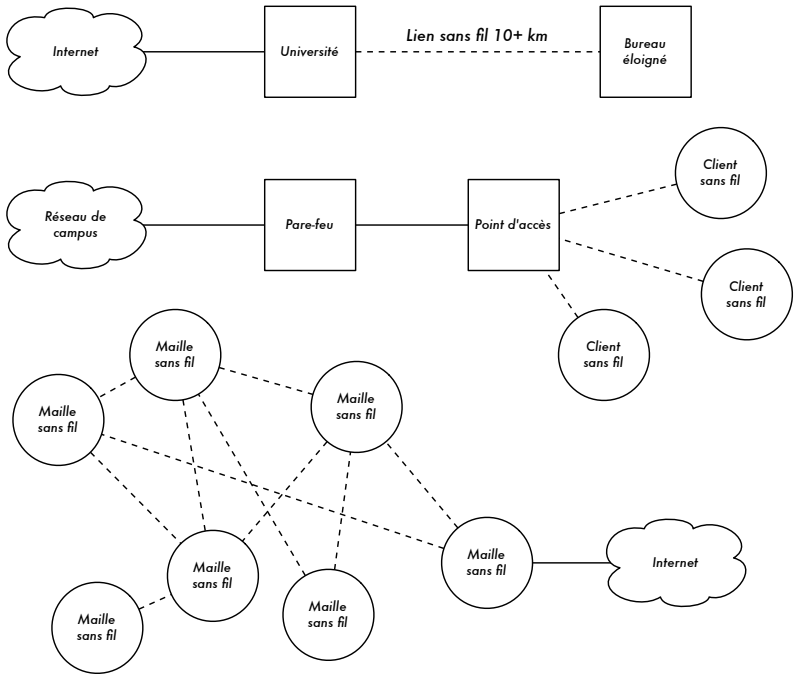


*Figure 1.1: Quelques exemples de réseaux sans fil.*

# Protocoles de réseaux sans fil

La technologie de base utilisée pour construire des réseaux sans fil peu coûteux est la famille des protocoles 802.11, aussi connue sous le nom de *WiFi* (*Wireless Fidelity*). La famille 802.11 de protocoles radio (802.11a, 802.11b, et 802.11g) a connue une incroyable popularité aux États-Unis et en Europe. En mettant en œuvre une série de protocoles communs, des manufacturiers du monde entier ont construit un équipement hautement interopérable. Cette décision s'est avérée être un avantage significatif tant pour l'industrie que pour le consommateur. Ceux-ci sont maintenant en mesure d'acheter des équipements peu coûteux en grande quantité. Si ceux-ci avaient choisi de mettre en place leurs propres protocoles propriétaires, il serait peu probable que la gestion de réseau sans fil soit aussi peu coûteuse et omniprésente qu'elle l'est aujourd'hui.

Même si de nouveaux protocoles tel que le 802.16 (aussi connu sous le nom de *WiMax*) promettent de résoudre certains problèmes actuellement observés avec les 802.11, ils ont encore un long chemin à parcourir avant d'égaler le prix et la popularité de l'équipement 802.11. Comme l'équipement qui maintient la technologie *WiMax* vient tout juste de devenir disponible au moment où nous rédigeons ce livre, nous nous concentrerons principalement sur la famille 802.11.

Il y a plusieurs protocoles dans la famille 802.11, et tous ne sont pas directement reliés au protocole de radio. Les trois standards sans fil actuellement mis en place dans la plupart des dispositifs disponibles sont:

- **802.11b.** Ratifié par l'*IEEE* le 16 septembre 1999, le 802.11b est probablement le plus populaire des protocoles de réseaux sans fil utilisés aujourd'hui. Des millions de dispositifs l'utilisant ont été vendus depuis 1999. Il utilise une modulation de fréquence nommée ***Direct Sequence Spread Spectrum*** (***DSSS***) dans une portion de la bande *ISM* de 2400 GHz à 2484 GHz. Cette modulation a un taux de transmission maximum de 11 Mbps, avec une vitesse réelle de données utilisables allant jusqu'à 5 Mbps.
- **802.11g.** Comme il n'a été finalisé qu'en juin 2003, le protocole 802.11g est arrivé relativement tard sur le marché sans fil. Malgré ses débuts tardifs, le 802.11g est maintenant un standard *de facto* dans les réseaux sans fil. Il est utilisé de manière standard dans pratiquement tous les ordinateurs portables et la plupart des dispositifs *handheld*. Le protocole 802.11g utilise la même plage *ISM* que le 802.11b mais avec un schéma de modulation nommé ***Orthogonal Frequency Division Multiplexing*** (***OFDM***). Il a un taux de transmission de données maximum de 54 Mbps (avec un rendement réel jusqu'à 25 Mbps), et peut maintenir une compatibilité avec le très populaire 802.11b en diminuant son taux de transmission à 11 Mbps.
- **802.11a.** Également ratifié par l'*IEEE* le 16 septembre 1999, le protocole 802.11a utilise l'*OFDM*. Il a un taux de transmission maximum de 54 Mbps, avec un rendement réel jusqu'à 27 Mbps. Le protocole 802.11a opère sur la bande *ISM* entre 5725 GHz et 5825 GHz, et dans une portion de la bande *UNII* entre 515 GHz et 535 GHz. Ceci le rend incompatible avec les protocoles 802.11b et 802.11g, et sa haute fréquence implique une portée plus basse comparée au 802.11b/g à la même puissance. Bien que cette partie du spectre soit relativement inutilisée comparée à la plage des 2,4GHz du 802.11b/g, son usage est malheureusement légal uniquement dans quelques parties du globe. Vérifiez avec les autorités locales avant d'utiliser un équipement 802.11a, particulièrement dans des applications extérieures. L'équipement 802.11a est encore assez peu coûteux, mais n'est pas encore aussi populaire que le 802.11b/g.

En plus des standards ci haut mentionnés, il y a des fabricants qui offrent des extensions qui permettent des vitesses de jusqu'à 108 Mbps, un meilleur chiffrage et une portée plus importante. Malheureusement, ces extensions ne fonctionnent pas entre les équipements de manufacturiers différents et les acheter implique de vous lier à un vendeur spécifique. De nouveaux équipements et standards (comme le 802.11n, le 802.16, *MIMO* et *WiMAX*) promettent une augmentation significative en vitesse et en fiabilité, mais cet équipement commence tout juste à se vendre au moment où nous rédigeons

ces lignes et la disponibilité et l'interopérabilité entre les vendeurs demeurent peu claires.

Étant donné la disponibilité de l'équipement, la meilleure portée et la nature libre des licences de la bande ISM 2,4GHz, ce livre se concentrera sur la construction de réseaux utilisant les protocoles 802.11b et 802.11g.

# Questions et réponses

Si vous êtes nouveau dans le monde des réseaux sans fil, vous avez sûrement un certain nombre de questions sur ce que la technologie peut faire et ses coûts. Voici quelques-unes des questions les plus fréquemment posées, avec leur réponse respective et des suggestions de lecture dans les pages mentionnées à leur droite.

## Énergie

- Comment puis-je fournir de l'énergie à ma radio si l'électricité n'est pas disponible? **Page 202.**
- Dois-je installer un câble électrique jusqu'en haut de la tour? **Page 189.**
- Comment puis-je utiliser des panneaux solaires pour fournir l'énergie à mon nœud de réseau sans fil tout en le conservant en ligne durant la nuit? **Page 202.**
- Pour combien de temps mon point d'accès peut fonctionner à l'aide d'une batterie? **Page 204.**

## Gestion

- Comment puis-je surveiller et gérer des points d'accès à distance à partir de mon bureau? **Page 180.**
- Que dois-je faire si le réseau fait défaillance? **Page 181, 217.**
- Quels sont les problèmes les plus fréquents que l'on doit affronter avec les réseaux sans fil et comment puis-je les résoudre? **Page 219.**

## Distance

- Quelle est la portée de mon point d'accès? **Page 58.**
- Existe-t-il une formule qui me permette de la portée d'un point d'accès donné? **Page 59.**

- Comment puis-je savoir si un emplacement éloigné peut se connecter à Internet à l'aide d'un lien sans fil? **Page 66.**
- Le manufacturier dit que mon point d'accès à une portée de 300 m. Est-ce vrai? **Page 58.**
- Comment puis-je fournir une connectivité sans fil à plusieurs clients éloignés et dispersés partout dans la ville? **Page 34.**
- Est-ce vrai que je peux arriver à avoir une distance beaucoup plus importante en utilisant une boîte de conserve ou un papier d'aluminium comme antenne? **Page 112.**
- Puis-je utiliser la technologie sans fil pour me connecter à un site éloigné et partager une connexion centrale unique à Internet? **Page 33.**
- Mes liens sans-fil semblent trop longs. Puis-je placer un répéteur au milieu pour les améliorer? **Page 70.**
- Sinon, dois-je utiliser un amplificateur? **Page 68, 110.**

## Installation

- Comment puis-je installer mon AP pour usage interne sur le toit de ma demeure près de l'antenne? **Page 188.**
- Est-ce réellement utile d'ajouter un parafoudre ou une prise de terre au mât de mon antenne, où puis-je me débrouiller sans cela? **Page 143, 199.**
- Puis-je construire un mât d'antenne tout seul? Quelle hauteur puis-je atteindre? **Page 191.**
- Pourquoi mon antenne fonctionne beaucoup mieux si je la place dans une autre direction? **Page 103.**
- Quel canal dois-je utiliser? **Page 17.**
- Les ondes de radio traversent-elles les édifices et les arbres? Qu'arrive t-il avec les personnes? **Page 19.**
- Les ondes de radio pourront-elles traverser une colline qui se trouve dans son chemin? **Page 25.**
- Comment puis-je construire un réseau maillé? **Page 45.**
- Quel type d'antenne est le mieux adapté pour mon réseau? **Page 104.**
- Puis-je construire un point d'accès en utilisant un vieil ordinateur? **Page 145.**
- Comment puis-je installer Linux sur mon AP? Pourquoi devrais-je le faire? **Page 155.**

## Coûts

- Comment puis-je savoir si un lien sans fil est possible avec un petit montant d'argent? **Page 136.**
- Quel est le meilleur AP pour le plus faible coût? **Page 134.**
- Comment puis-je attirer des clients et les facturer pour l'utilisation de mon réseau sans fil? **Page 167, 180.**

## Partenaires et Clients

- Si je suis un fournisseur de connexions, dois-je toujours avoir recours à un service ISP? Pourquoi? **Page 32.**
- Avec combien de clients puis-je couvrir mes coûts? **Page 251.**
- Mon réseau sans fil peut supporter combien de clients? **Page 55.**
- Comment faire pour que mon réseau sans fil soit plus rapide? **Page 72.**
- Ma connexion Internet est-elle aussi rapide qu'elle pourrait l'être? **Page 83.**

## Sécurité

- Comment puis-je protéger mon réseau sans fil des accès non autorisés? **Page 164.**
- Est-ce vrai qu'un réseau sans fil est toujours peu sécuritaire et ouvert aux attaques de pirates informatiques? **Page 161.**
- Comment puis-je voir ce qui se déroule sur mon réseau? **Page 170.**

## Information et licence

- Quels autres livres puis-je lire pour améliorer mes connaissances en réseaux sans fil? **Page 267.**
- Où puis-je trouver plus d'informations en ligne? **Page 262.**
- Étant enseignant, puis-je utiliser des parties de ce livre au sein de mes cours? Puis-je imprimer et vendre des copies de ce livre? **Oui. Voir la section « Avant-propos » pour plus de détails.**

# 2
# Une introduction à la physique des ondes radio

Les communications sans fil font usage d'ondes électromagnétiques pour envoyer des signaux sur de longues distances. Du point de vue de l'usager, les connexions sans fil ne sont pas particulièrement différentes de celles d'autres connexions de réseau: votre navigateur Internet, courriel et autres applications fonctionnent toutes de la même façon. Mais les ondes radio ont certaines propriétés inattendues comparées au câble Ethernet. Par exemple, il est très facile de voir le chemin pris par le câble Ethernet: localisez la prise sortant de votre ordinateur, suivez le câble jusqu'à l'autre extrémité, et vous l'aurez trouvé! Vous pouvez aussi être certain que de faire fonctionner plusieurs câbles Ethernet à côté les uns des autres ne causera pas de problèmes, puisque les câbles conservent efficacement leurs signaux au sein du fil lui-même.

Mais comment pouvez-vous savoir où vont les ondes émanant de votre carte sans fil? Que se produit-il quand ces ondes rebondissent sur des objets dans la salle ou sur d'autres bâtiments s'il s'agit d'un lien extérieur? Comment plusieurs cartes sans fil peuvent-elles être employées dans le même secteur sans interférer les unes avec les autres?

Afin de construire des liens sans fil stable et à haute vitesse, il est important de comprendre comment les ondes radio se comportent dans le monde réel.

## *Qu'est qu'une onde?*

Nous connaissons tous des vibrations ou des oscillations prenant diverses formes: un pendule, un arbre balançant dans le vent, la corde d'une guitare sont tous des exemples d'oscillations.

Ce qu'ils ont en commun est que quelque chose, un certain milieu ou un objet, se balance d'une façon périodique, avec un certain nombre de cycles par unité de temps. Ce genre d'onde est parfois appelé une onde ***mécanique***, puisqu'elle est définie par le mouvement d'un objet ou de son milieu de propagation.

Quand de telles oscillations voyagent (c'est-à-dire, quand l'oscillation ne reste pas attachée à un endroit) nous parlons alors d'ondes se *propageant dans l'espace*. Par exemple, un chanteur crée des oscillations périodiques dans ses cordes vocales. Ces oscillations compriment et décompriment périodiquement l'air, et ce changement périodique de pression atmosphérique abandonne alors les lèvres du chanteur pour entreprendre un voyage, à la vitesse du son. Une pierre plongeant dans un lac cause une perturbation, qui voyage alors à travers le lac comme une ***onde***.

Une onde a une certaine ***vitesse***, ***fréquence*** et ***longueur***. Celles-ci sont unies par une simple relation:

```
Vitesse = Fréquence * Longueur d'onde
```

La longueur d'onde (parfois nommé ***lambda***, **λ**) est la distance séparant deux crêtes successives d'une onde périodique. La fréquence est le nombre d'ondes entières qui passent par un point fixe en une seconde. La vitesse est mesurée en mètres/secondes, la fréquence est mesurée en cycles par seconde (ou Hertz, abrégé ***Hz***), et la longueur d'onde est mesurée en mètres.

Par exemple, si une onde voyage sur l'eau à un mètre par seconde, et oscille cinq fois par seconde, alors chaque onde aura une longueur de vingt centimètres:

```
1 mètre/seconde = 5 cycles/seconde * λ
0 = 1/5 mètres
0 = 0,2 mètres = 20 cm
```

Les ondes ont également une caractéristique nommée ***amplitude***. Celle-ci est la distance entre le centre d'une onde et l'extrémité d'une de ses crêtes, pouvant être illustrée comme étant la « hauteur » d'une vague d'eau. La relation entre fréquence, longueur d'onde et amplitude est illustrée par la Figure 2.1.

Il est facile d'apercevoir des ondes sur l'eau. Laissez simplement tomber une pierre dans un lac et vous pouvez voir les vagues pendant qu'elles se déplacent sur l'eau avec le temps. Dans le cas des ondes électromagnétiques, ce qui pourrait être plus difficile à comprendre est: « qu'est ce qui est en train d'osciller? ».

Afin de comprendre ceci, nous devons en premier lieu comprendre les forces électromagnétiques.

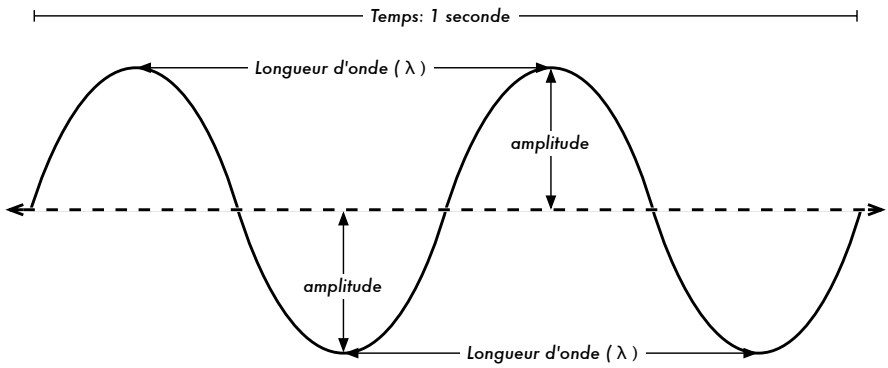


*Figure 2.1: Longueur d'onde, amplitude, et fréquence. Pour cette onde, la fréquence est de 2 cycles par seconde, ou 2 Hz.*

## Forces électromagnétiques

Les forces électromagnétiques sont les forces entre les charges électriques et les courants. Nous y sommes déjà habitués par exemple lorsque notre main touche une poignée de porte après avoir marché sur un tapis synthétique, ou lorsque nous frôlons une barrière électrique. Un exemple plus fort des forces électromagnétiques est la foudre que nous voyons pendant les orages. La ***force électrique*** est la force entre les charges électriques. La ***force magnétique*** est la force entre les courants électriques.

Les électrons sont des particules qui portent une charge électrique négative. Il existe aussi d'autres particules, mais les électrons sont responsables de l'essentiel de ce que nous devons connaître sur la façon dont les ondes radio se comportent.

Regardons ce qui se produit sur un morceau de fil de fer droit dans lequel nous enfonçons les électrons d'un côté puis de l'autre, périodiquement. À un instant donné, le dessus du fil est chargé négativement - tous les électrons y sont recueillis. Ceci crée un champ électrique du positif au négatif le long du fil. À l'instant suivant, les électrons ont tous été conduits à l'autre extrémité, et le champ électrique va dans l'autre sens. Lorsque ceci se produit à plusieurs reprises, les vecteurs de champ électrique (flèches du positif au négatif) abandonnent le fil de fer, pour ainsi dire, et sont irradiés en-dehors, dans l'espace autour du fil.

Ce que nous venons de décrire est connu sous le nom de dipôle (en raison des deux pôles, le plus et le moins), ou plus communément ***antenne dipôle***.

C'est la forme la plus simple d'antenne omnidirectionnelle. Le mouvement du champ électrique est généralement nommé ***onde électromagnétique***.

Revenons à la relation:

```
Vitesse = Fréquence * Longueur d'onde
```

Dans le cas d'ondes électromagnétiques, la vitesse est la vitesse de la lumière, notée **c**.

$$c = 300\ 000\ km/s = 300\ 000\ 000\ m/s = 3*10^8\ m/s$$
$$c = f * \lambda$$

Les ondes électromagnétiques sont différentes des ondes mécaniques en ce qu'elles ne requièrent aucun medium pour se propager. Les ondes électromagnétiques peuvent même se propager à travers le vide de l'espace.

## Puissances de dix

En physique et en mathématiques, il est souvent question de puissances de dix pour exprimer les nombres. Nous utiliserons également ces termes, par exemple dans le gigahertz (GHz), les centimètres (cm), les microsecondes ($\mu$s), et ainsi de suite. Voici un petit rappel sur les puissances de dix:

| Puissances de dix | | | |
|---|---|---|---|
| Nano- | $10^{-9}$ | 1/1000000000 | n |
| Micro- | $10^{-6}$ | 1/1000000 | $\mu$ |
| Milli- | $10^{-3}$ | 1/1000 | m |
| Centi- | $10^{-2}$ | 1/100 | c |
| Kilo- | $10^{3}$ | 1 000 | k |
| Mega- | $10^{6}$ | 1 000 000 | M |
| Giga- | $10^{9}$ | 1 000 000 000 | G |

En connaissant la vitesse de la lumière, nous pouvons calculer la longueur d'onde pour une fréquence donnée. Prenons par exemple la fréquence du protocole de réseautage sans fil 802.11b, qui est:

```
f = 2,4 GHz
  = 2 400 000 000 cycles / seconde

Longueur d'onde lambda (λ) = c / f
                           = 3*10^8 / 2,4*10^9
                           = 1,25*10^-1 m
                           = 12,5 cm
```

La fréquence et la longueur d'onde déterminent globalement le comportement d'une onde électromagnétique: des antennes que nous construisons aux objets qui se trouvent dans le chemin des réseaux que nous voulons installer. Elles auront un impact sur les différents standards que nous pouvons choisir. Il est donc très utile de comprendre les idées de base concernant la fréquence et la longueur d'onde pour entreprendre le travail dans le domaine du sans fil.

# *Polarisation*

Une autre caractéristique importante des ondes électromagnétiques est la ***polarisation***. La polarisation décrit la direction du vecteur de champ électrique.

Si vous imaginez une antenne dipôle alignée verticalement (le morceau droit du fil), les électrons se déplacent seulement vers le haut et vers le bas, mais non vers les côtés (parce qu'il n'y a aucun espace pour se déplacer) et les champs électriques pointent donc uniquement vers le haut ou vers le bas, verticalement. Le champ abandonnant le fil et voyageant comme une onde a une polarisation strictement linéaire (et dans ce cas-ci, verticale). Si nous mettions l'antenne à plat sur le sol (de façon horizontale), nous trouverions une polarisation linéaire horizontale.

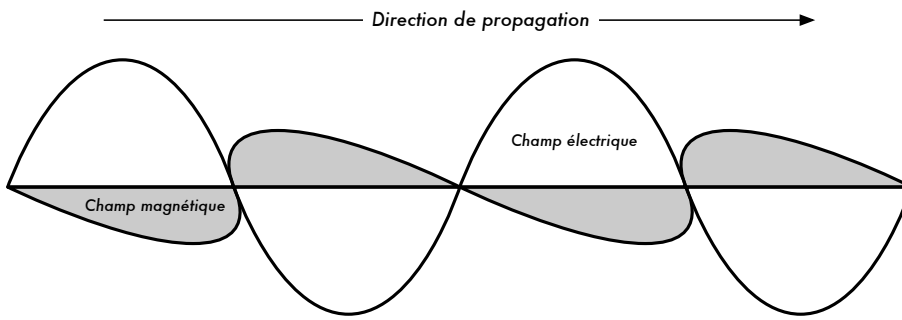


*Figure 2.2: Les deux composantes complémentaires d'une onde électromagnétique: son champ électrique son champ magnétique. La polarisation décrit l'orientation du champ électrique.*

La polarisation linéaire n'est qu'un cas particulier, et n'est jamais aussi parfaite: en général, il y aura toujours certaines composantes du champ pointant aussi vers d'autres directions. Le cas le plus typique est la polarisation elliptique, avec les extrêmes des polarisations linéaires (seulement une direction) et circulaires (les deux directions à force égale).

Comme nous pouvons l'imaginer, la polarisation devient importante au moment d'aligner les antennes. Si vous ignorez tout de la polarisation, vous courrez le risque d'obtenir un très faible signal même avec la plus puissante des antennes. On dit alors que cette polarisation est en déséquilibre (*mismatch polarization* en anglais).

# Le spectre électromagnétique

Les ondes électromagnétiques utilisent un large éventail de fréquences (et, en conséquence, de longueurs d'ondes). Nous nommons cette gamme de fréquences et de longueurs d'ondes, le ***spectre électromagnétique***. La partie du spectre la plus connue par les humains est probablement la lumière, la partie visible du spectre électromagnétique. La lumière se trouve approximativement entre les fréquences de $7,5*10^{14}$ hertz et $3,8*10^{14}$ hertz, correspondant aux longueurs d'ondes comprises entre 400 nm (violet/bleu) à 800 nm (rouge).

Nous sommes également régulièrement exposés à d'autres régions du spectre électromagnétique, y compris le ***CA*** (courant alternatif) ou réseau électrique à 50/60 hertz, rayons X, rayonnement Roentgen, ultraviolet (du côté des fréquences plus élevées de la lumière visible), infrarouge (du côté des plus basses fréquences de la lumière visible) et plusieurs autres. La ***radio*** est le terme utilisé pour la partie du spectre électromagnétique dans lequel des ondes peuvent être produites en appliquant le courant alternatif à une antenne soit une plage allant de 3 hertz à 300 gigahertz, mais dans un sens plus étroit du terme, la limite supérieure de fréquence serait 1 gigahertz.

Lorsque nous parlons de radio, la plupart des gens pensent à la radio FM, qui utilise une fréquence d'autour de 100 MHz. Entre la radio et l'infrarouge, nous trouvons une région de micro-ondes – avec des fréquences d'environ 1 GHz à 300 GHz, et des longueurs d'ondes de 30 cm à 1 mm.

L'usage le plus populaire des micro-ondes est indubitablement le four à micro-ondes, qui de fait fonctionne exactement dans la même plage d'ondes que les standards sans fil dont il est question dans cet ouvrage. Ces plages se retrouvent au sein des bandes ouvertes pour usage général sans licence. Cette région est nommée ***bande ISM***, pour Industriel, Scientifique et Médical. La plupart des autres parties du spectre électromagnétique sont fortement contrôlées par les législations et licences, ces dernières constituant un

important facteur économique. Ceci est particulièrement vrai pour les parties du spectre qui sont utilisées dans les émissions de télévision et de radio, ainsi que pour les communications vocales et le transport des données. Dans la plupart des pays, les bandes ISM ont été réservées pour un usage sans licence.

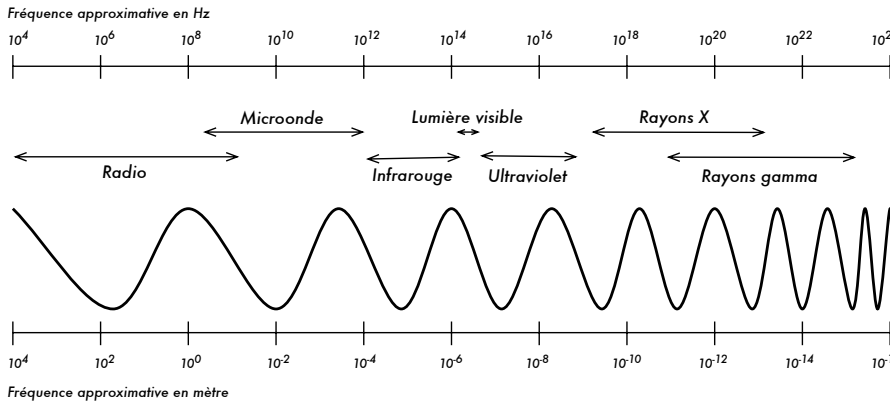


*Figure 2.3: Le spectre électromagnétique.*

Les fréquences les plus intéressantes pour nous sont les 2400-2484 GHz, utilisées par les standards de radio 802.11b et 802.11g (ce qui correspond à des longueurs d'ondes d'environ 12,5 cm). D'autres équipements habituellement disponibles utilisent le standard 802.11a, qui fonctionne à 5150-5850 GHz (avec des longueurs d'ondes d'environ 5 à 6 cm).

# *Largeur de bande*

Un terme que vous retrouverez souvent en physique de radio est la ***largeur de bande*** aussi appelée de manière impropre mais fort commune la ***bande passante***. La largeur de bande est simplement une mesure de gamme de fréquences. Si une gamme de fréquences de 2,40 GHz à 2,48 GHz est utilisée par un dispositif quelconque, la largeur de bande sera alors 0,08 GHz (ou plus communément 80MHz).

Il est donc facile de comprendre que la largeur de bande est intimement en rapport avec la quantité de données que vous pouvez y transmettre –plus il y a d'espace de fréquence, plus de données vous pourrez y inclure à un certain moment. Le terme largeur de bande ou bande passante est souvent utilisé pour faire référence à quelque chose que nous devrions nommer taux de transmission de données, par exemple lorsque nous disons « ma connexion Internet a une bande passante de 1 Mbps », nous voulons dire « je peux transmettre des données à 1 mégabit par seconde ».

# Fréquences et canaux

Regardons de plus près comment la bande 2,4GHz est utilisée au sein du standard 802.11b. Le spectre est divisé en parties égales distribuées sur la largeur de bande appelées des canaux. Notez que les canaux ont une largeur de 22 MHz mais sont séparées seulement de 5 MHz. Ceci signifie que les canaux adjacents se superposent et peuvent interférer les uns avec les autres. Ceci est illustré par la figure 2,4.

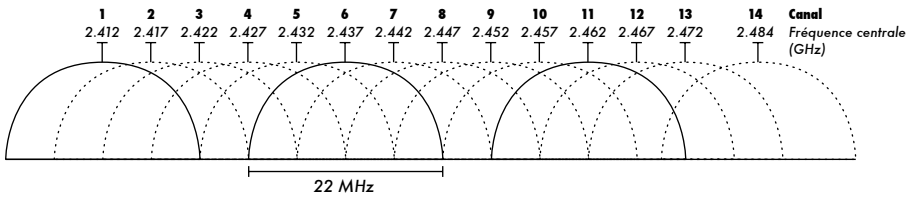


*Figure 2.4: Canaux et centre de fréquences pour le standard 802.11b. Notez que les chaînes 1,6 et 11 ne se superposent pas.*

Pour une liste complète des canaux et de leur centre de fréquences pour le standard 802.11b/g et 802.11a, voir l'Appendice A.

# Comportement des ondes radio

Il y a quelques règles simples qui peuvent être très utiles pour concevoir un réseau sans fil:

- Plus la longueur d'onde est grande, plus loin celle-ci ira.
- Plus la longueur d'onde est grande, mieux celle-ci voyagera à travers et autour des choses.
- À plus courte longueur d'onde, plus de données pourront être transportées.

Même si ces règles semblent très simples, il est plus facile de les comprendre grâce à des exemples.

## Les ondes plus longues voyagent plus loin

À niveaux égaux de puissances, les ondes avec une plus grande longueur d'onde tendent à voyager plus loin que les ondes avec des longueurs d'onde plus courtes. Cet effet est souvent observé dans la radio FM lorsque nous comparons la gamme d'un émetteur FM à 88MHz à la gamme à 108MHz. À la même puissance, les émetteurs avec une fréquence plus basse (donc une longueur d'onde plus élevée) tendent à atteindre des distances beaucoup plus grandes que les émetteurs à fréquence plus élevée.

## Les ondes plus longues contournent les obstacles

Une vague sur l'eau qui a une longueur de 5 mètres ne sera pas arrêtée par un morceau de 5 millimètres de bois sortant en dehors de l'eau. À l'inverse, si le morceau de bois avait une longueur de 50 mètres (par exemple un bateau), celui-ci s'interposerait dans le chemin de la vague. La distance qu'une onde peut parcourir dépend du rapport entre la longueur de l'onde et la taille des obstacles qui se trouvent dans son chemin de propagation.

Il est plus difficile de visualiser des ondes se déplaçant à travers des objets solides, mais tel est le cas des ondes électromagnétiques. De plus les grandes longueurs d'ondes (et donc à plus basse fréquence) tendent à mieux pénétrer les objets que les plus courtes longueurs d'onde (et donc à fréquence plus élevée). Par exemple, la radio FM (88-108MHz) peut voyager à travers des bâtiments et d'autres obstacles facilement, alors que des ondes plus courtes (tels les téléphones GSM fonctionnant à 900MHz ou à 1800MHz) ont plus de difficultés pour faire de même. Cet effet est partiellement dû à la différence dans les niveaux de puissance utilisés par la radio FM et les téléphones GSM, mais également à la longueur d'onde plus courte des signaux GSM.

## Les ondes plus courtes peuvent transporter plus de données

Plus rapide est l'oscillation ou cycle d'une onde, plus d'information celle-ci pourra transporter- chaque oscillation ou cycle peut être par exemple utilisé pour transporter un bit digital, un « 0 » ou un « 1 », un « oui » ou un « non ».

Il y a un autre principe qui peut être appliqué à tous les types d'ondes et qui peut s'avérer extrêmement utile à l'heure de comprendre la propagation des ondes radio. Le principe est connu sous le nom de ***Principe de Huygens***, en hommage à Christiaan Huygens (1629-1695), un mathématicien, physicien et astronome hollandais.

Imaginez que vous preniez un petit bâton et le plongiez verticalement dans la surface d'un lac immobile, faisant que l'eau se balance et danse. Les vagues abandonneront le centre du bâton - l'endroit où vous l'avez plongé- en faisant des cercles. Maintenant, partout où les particules de l'eau se balancent et dansent, elles feront faire la même chose aux particules voisines: à partir de chaque point de perturbation, une nouvelle vague circulaire prendra naissance. Ceci explique de façon très simple le Principe de Huygens. Dans les mots de wikipedia.org:

> *« Le principe du Huygens est une méthode d'analyse appliquée aux problèmes de la propagation d'onde dans la limite lointaine de ce champ. Il*

*reconnaît que chaque point d'une onde avançant de manière frontale est en fait le centre d'une nouvelle perturbation et la source d'une nouvelle série d'ondes ; et que, prise dans son ensemble, l'onde qui avance peut être considérée comme la somme de toutes les ondes secondaires qui surgissent des points dont le milieu a déjà été traversé. Cette vision de la propagation d'onde aide à mieux comprendre une variété de phénomènes d'ondes, tels que la diffraction. »*

Ce principe est vrai tant pour les ondes radio que pour les vagues sur l'eau, pour le son comme pour la lumière –même si pour la lumière, la longueur d'onde est bien trop courte pour que ses effets puissent directement être appréciés par l'œil humain.

Ce principe nous aidera à comprendre la diffraction et les zones Fresnel, le besoin d'établir des lignes de vue ainsi que le fait que parfois nous puissions tourner les coins de rues, sans avoir besoin de ligne de vue.

Observons maintenant ce qui arrive aux ondes électromagnétiques tandis qu'elles voyagent.

## Absorption

Lorsque les ondes électromagnétiques passent à travers un matériel quelconque, elles en sortent généralement affaiblies ou amorties. La puissance qu'elles vont perdre va dépendre de leur fréquence et naturellement du matériel. Une fenêtre de verre clair est évidemment transparente pour la lumière, alors que le verre utilisé dans les lunettes de soleil élimine une partie de l'intensité de la lumière ainsi que la radiation ultraviolette.

Souvent, un coefficient d'absorption est employé pour décrire l'impact d'un matériel sur la radiation. Pour les micro-ondes, les deux matériaux absorbants principaux sont:

- Le **Métal**. Les électrons peuvent bouger librement dans les métaux, et peuvent aisément balancer et absorber ainsi l'énergie d'une onde qui passe.
- L'**eau**. Les micro-ondes font que les molécules d'eau se bousculent, capturant de ce fait une partie de l'énergie de l'onde[1].

---

**1.** Un mythe généralement répandu est que l'eau "résonne" à 2,4GHz, ce qui explique pourquoi cette fréquence est employée dans les fours à micro-ondes. En fait, l'eau ne semble pas avoir une fréquence de résonance particulière. L'eau tourne et bouscule autour d'une source radio proche, et se réchauffe lorsqu'elle se trouve en présence d'ondes radio de puissance élevée à n'importe quelle fréquence. 2,4GHz est une fréquence ISM sans licence, ce qui en fait un bon choix politique pour une utilisation dans les fours à micro-ondes.

Pour les fins pratiques du réseautage sans fil, nous pouvons considérer le métal et l'eau comme des matériaux absorbants parfaits: nous ne pourrons pas passer à travers eux (bien que des couches minces d'eau permettent le passage d'une certaine puissance). Ces matériaux sont à la micro-onde ce qu'est un mur de brique à la lumière. Si nous parlons d'eau, nous devons nous rappeler qu'elle se présente sous différentes formes: la pluie, le brouillard et la brume, des nuages bas et ainsi de suite. L'eau sous toutes ses formes se présentera dans le chemin des liens de radio. Elles ont une forte influence, et dans plusieurs circonstances, elles peuvent faire en sorte qu'un changement climatique rompe un lien radio.

Il y a d'autres matériaux qui ont un effet plus complexe sur l'absorption radio.

Pour les **arbres** et le **bois**, la quantité d'absorption dépend de la quantité d'eau qu'ils contiennent. Un morceau de bois mort et sec est plus ou moins transparent pour les ondes radio, un morceau de bois frais et humide absorbera, au contraire, beaucoup l'onde.

**Les plastiques** et matériaux similaires n'absorbent généralement pas beaucoup d'énergie de radio, mais ceci varie dépendamment de la fréquence et du type de matériel. Avant de construire une composante avec du plastique (par exemple une protection climatique pour un dispositif de radio et ses antennes), il est toujours mieux de mesurer et vérifier que le matériel en question n'absorbe pas l'énergie de radio autour de 2,4GHz. Une façon simple de mesurer l'absorption du plastique à 2,4GHz est de mettre un échantillon dans le four à micro-ondes pour quelques minutes. Si le plastique se réchauffe, c'est qu'il absorbe alors l'énergie de radio et ne devrait donc pas être utilisé.

Pour terminer, parlons de nous-mêmes: les humains. Nous (ainsi que les autres animaux) sommes surtout constitués d'eau. En ce qui a trait au réseautage radio, nous pouvons être décrits comme des grands sacs d'eau, avec une absorption également forte. Orienter un point d'accès dans un bureau de manière telle que son signal doit passer à travers plusieurs personnes, est une erreur importante lors de la conception des réseaux dans les bureaux. Ceci est également vrai pour les hotspots, les installations dans les cafés et les bibliothèques et autres installations extérieures.

## Réflexion

Tout comme la lumière visible, les ondes radio sont réfléchies lorsqu'elles entrent en contact avec des matériaux qui sont appropriés pour cela: pour les ondes radio, les sources principales de réflexion sont le métal et les superficies d'eau. Les règles pour la réflexion sont assez simples: l'angle sur lequel une onde frappe une surface est le même angle sur lequel elle sera déviée. Notez qu'aux yeux d'une onde radio, une grille dense de métal agit

de la même façon qu'une surface solide, tant et aussi longtemps que la distance entre les barreaux est petite en comparaison à la longueur d'onde. À 2,4GHz, une grille de métal avec une maille d'un centimètre agira de la même façon qu'une plaque de métal.

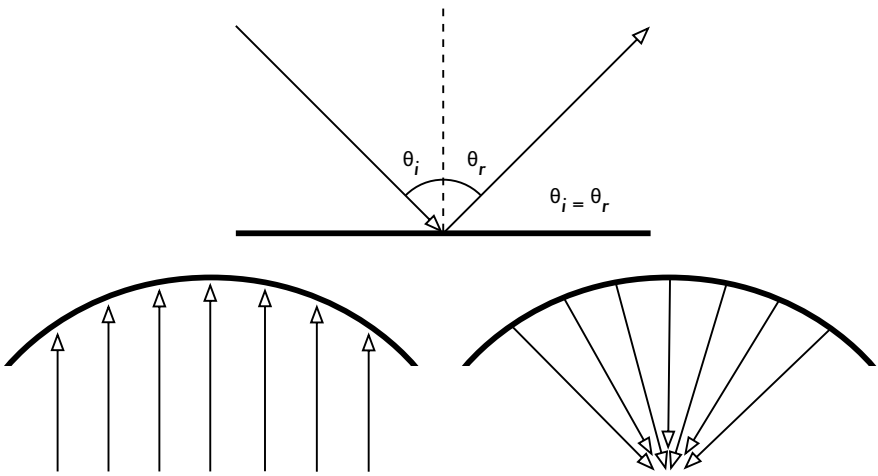


*Figure 2.5: Réflexion d'ondes radio. L'angle d'incidence est toujours égal à l'angle de réflexion. Une antenne parabolique utilise cet effet afin de conduire dans une même direction les ondes radio éparpillées sur sa surface.*

Bien que les règles de la réflexion soient tout à fait simples, les choses peuvent devenir très compliquées lorsque vous imaginez l'intérieur d'un bureau avec beaucoup de petits objets en métal de formes variées et compliquées. Il en va de même pour des situations urbaines: regardez autour de vous dans votre ville et essayez de repérer tous les objets en métal. Ceci explique pourquoi les ***effets par trajets multiples*** (c.-à-d. des signaux atteignant leur cible le long de différents chemins, et donc à des temps différents) jouent un rôle si important dans le domaine du réseautage sans fil. La surface de l'eau, avec des vagues et une ondulation changeant tout le temps, la rend un objet de réflexion très compliqué et donc très difficile à prévoir et à calculer avec précision.

Nous devrions également ajouter que la polarisation a un impact: en général, des ondes avec des polarisations différentes seront réfléchies différemment.

Nous employons la réflexion à notre avantage dans la construction d'une antenne: par exemple nous installons des antennes paraboliques énormes derrière notre émetteur de radio pour rassembler les signaux de radio et concentrer notre signal dans un point ou une direction particulière.

## Diffraction

La diffraction est le repli  apparent des vagues en frappant un objet. C'est l'effet des « ondes tournant les coins ».

Imaginez une vague sur l'eau voyageant dans un front d'onde droit, exactement comme une vague qui se forme sur une plage océanique. Maintenant nous plaçons une barrière solide, disons une barrière solide en bois, de manière à la bloquer. Nous avons coupé une ouverture étroite dans le mur, telle une petite porte. À partir de cette ouverture, une vague circulaire naîtra, et elle atteindra naturellement des points qui ne sont pas alignés en ligne droite avec cette ouverture mais se dispersera sur chacun de ses côtés. Si vous regardez ce front de vagues – qui pourrait aussi bien être une onde électromagnétique – comme étant un faisceau de lumière (une ligne droite), il peut sembler difficile d'expliquer comment il peut atteindre des points qui devraient être cachés par une barrière. Si nous le modélisons un front d'ondes, le phénomène prend tout son sens.

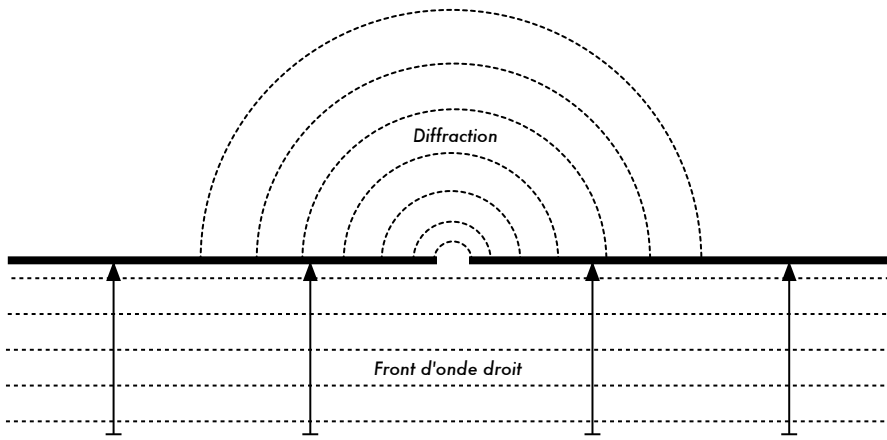


*Figure 2.6: Diffraction à travers une ouverture étroite.*

Le principe de Huygens fournit un modèle pour comprendre ce comportement. Imaginez qu'à n'importe quel moment, chaque point sur un front d'ondes peut être considéré le point de départ pour une "ondelette" sphérique. Cette idée a été travaillée plus tard par Fresnel, et même si elle décrit adéquatement le phénomène, celui-ci est toujours matière à discussion. Mais pour les fins de ce livre, le modèle de Huygens décrit assez bien le phénomène en question.

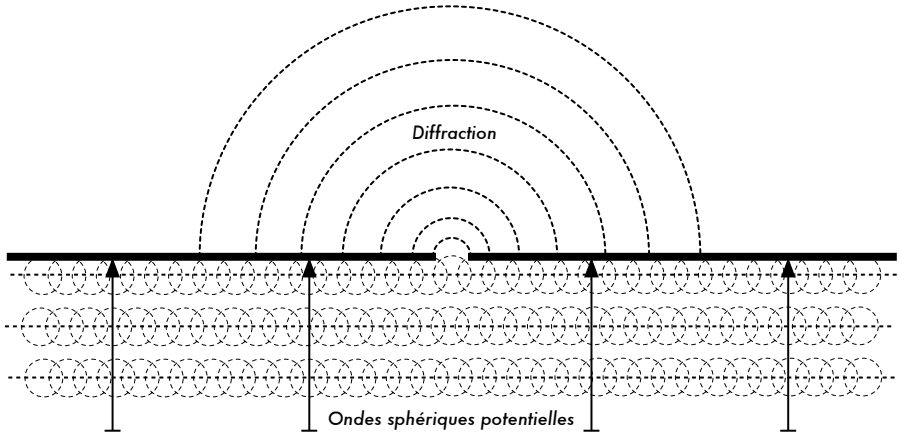


*Figure 2.7: Le principe Huygens.*

Par l'effet de la diffraction, les ondes vont se replier autour des coins ou par une ouverture dans une barrière. Les longueurs d'onde de la lumière visible sont trop petites pour que les humains puissent observer leurs effets directement. Les micro-ondes, avec une longueur d'onde de plusieurs centimètres, montreront les effets de la diffraction lorsque les ondes frappent des murs, des sommets de montagne, et d'autres obstacles. Une obstruction semble faire changer la direction de l'onde en la faisant « tourner » les coins.

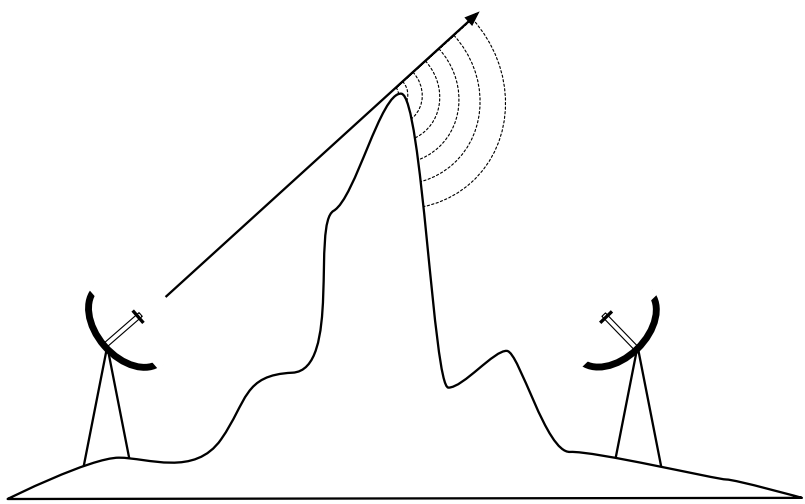

*Figure 2.8: Diffraction sur le sommet d'une montagne.*

Notez qu'avec la diffraction il y a perte de puissance: l'énergie de l'onde diffractée est significativement plus faible que celle du front d'ondes qui l'a causé. Mais dans quelques applications très spécifiques, vous pouvez tirer profit de l'effet de la diffraction pour éviter des obstacles.

## Interférence

En travaillant avec des ondes, un plus un n'est pas nécessairement égal à deux. Le résultat peut tout aussi bien être zéro.

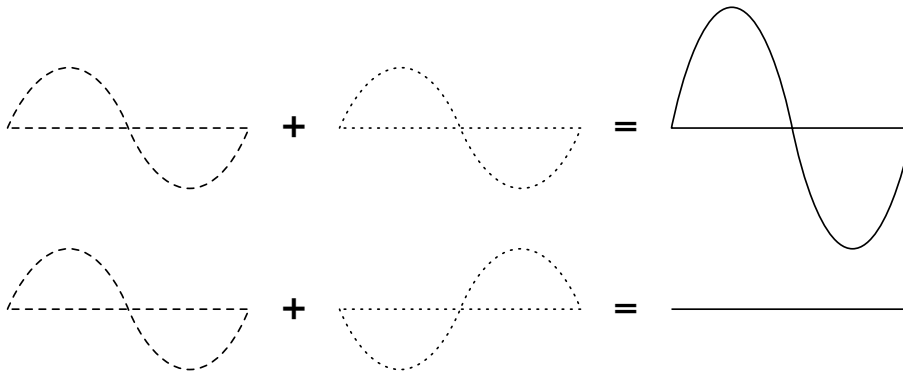

*Figure 2.9: Interférence constructive et destructive.*

Ceci est plus facile à comprendre lorsque vous dessinez deux ondes sinusoïdales et ajoutez les amplitudes. Lorsqu'une pointe coïncide avec une autre pointe, vous obtenez les résultats maximum (1 + 1 = 2). Ceci s'appelle ***l'interférence constructive***. Lorsqu'une pointe coïncide avec une vallée, vous obtenez une annihilation complète ((1 + (-)1 = 0),appelée une ***interférence destructive***.

Vous pouvez essayer ceci avec des vagues sur l'eau et deux petits bâtons pour créer des vagues circulaires - vous verrez que là où deux vagues se croisent, il y aura des secteurs avec des pointes plus élevées et d'autres qui demeurent presque plats et calmes.

Afin que toutes les séries d'ondes s'ajoutent ou s'annulent parfaitement les unes aux autres, elles doivent exactement avoir la même longueur d'onde et leurs phases doivent être en relation, ceci implique une relation entre les positions des crêtes d'es ondes.

Dans le domaine de la technologie sans fil, le mot interférence est typiquement employé dans un sens plus large, pour la perturbation par d'autres sources de radio fréquence, par exemple des canaux adjacents. Ainsi, lorsque les réseauteurs sans fil parlent d'interférence, ils parlent généralement de toutes sortes de perturbations par d'autres réseaux, et d'autres sources de micro-ondes. L'interférence est l'une des sources principales de difficulté dans la construction de liens sans fil, particulièrement dans les environnements urbains ou les espaces fermés (telle qu'une salle de conférence) où plusieurs réseaux peuvent se faire concurrence dans un même spectre.

Toutes les fois que des ondes d'amplitudes égales et de phases opposées se croisent, l'onde est annihilée et aucun signal ne peut être reçu. Plus couramment, les ondes se combineront pour donne une onde complètement déformée qui ne pourra pas être employée efficacement pour la communication. Les techniques de modulation et l'utilisation de canaux multiples aident à résoudre les problèmes d'interférence, mais ne l'éliminent pas complètement.

# Ligne de vue

Le terme ***ligne de vue*** (dont l'abréviation est ***LOS*** en anglais pour ***Line Of Sight***), est assez facile à comprendre lorsque nous parlons de lumière visible: si nous pouvons apercevoir un point B à partir du point A où nous sommes situés, nous avons une ligne de vue. Vous n'avez qu'à dessiner une ligne du point A au point B et, si rien ne croise le chemin, vous avez une ligne de vue.

Les choses deviennent un peu plus compliquées lorsque nous traitons de micro-ondes. Rappelez-vous que la plupart des caractéristiques de propagation des ondes électromagnétiques vont s'accroître dépendamment de leur longueur d'onde. Ceci est également le cas pour l'élargissement des ondes lorsqu'elles voyagent. La lumière a une longueur d'onde d'environ 0,5 micromètre, les micro-ondes utilisées en réseaux sans fil ont une longueur d'onde de quelques centimètres. En conséquence, leurs faisceaux sont beaucoup plus larges - ils ont, pour ainsi dire, besoin de plus d'espace pour voyager.

Notez que les faisceaux lumineux s'élargissent de la même façon, et si vous les laissez voyager assez longtemps, vous pouvez voir les résultats malgré leur courte longueur d'onde. Lorsque nous pointons un laser bien focalisé à la lune, son faisceau s'élargira à plus de 100 mètres de rayon avant qu'il n'atteigne la surface. Par une nuit claire, vous pouvez voir cet effet par vous-même en utilisant un pointeur laser peu coûteux et des jumelles. Plutôt que de pointer la lune, pointez une montagne éloignée ou une structure inoccupée (telle qu'une tour d'eau). Le rayon de votre faisceau augmentera à mesure que la distance augmente.

La ligne de vue dont nous avons besoin afin d'avoir une connexion sans fil optimale entre deux points A à B doit donc être plus large qu'une simple ligne entre ces points- sa forme ressemble plus à celle d'un cigare, d'une saucisse ou plus mathématiquement d'une ellipse. Sa largeur peut être décrite par le concept des zones de Fresnel.

## Comprendre les zones de Fresnel

La théorie exacte des zones de Fresnel est assez compliquée. Cependant, il est tout à fait facile de comprendre le concept: grâce au principe de Huygens, nous savons qu'à chaque point d'un front d'ondes une onde circulaire prend naissance. Nous savons que les faisceaux de micro-ondes s'élargissent. Nous savons que les ondes d'une fréquence peuvent interférer les unes sur les autres. La théorie des zones de Fresnel examine simplement une ligne de A à B, et puis l'espace autour de cette ligne qui contribue à ce qui arrive au point B. Quelques ondes voyagent directement de A à B, alors que d'autres voyagent sur des chemins en dehors de cet axe. En conséquence, leur chemin est plus long, introduisant un déphasage entre le faisceau direct et indirect. Toutes les fois que le déphasage est d'une longueur d'onde complète, vous obtenez l'interférence constructive: les signaux s'ajoutent de façon optimale. En adoptant cette approche et en calculant bien, vous trouvez des zones circulaires autour de la ligne droite de A à B qui contribuent à ce que le signal arrive au point B, d'autres au contraire vont diminuer le signal reçu en B.

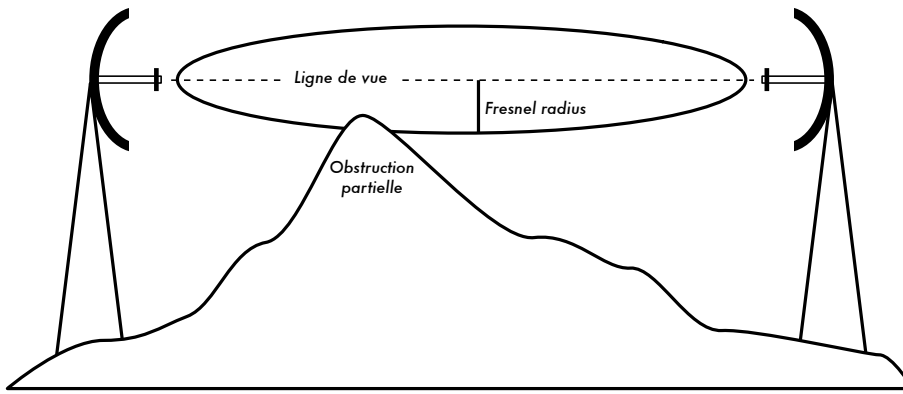


*Figure 2.10: La zone Fresnel est partiellement bloquée sur ce lien, même si la ligne de vue apparaît clairement.*

Notez qu'il y a beaucoup de zones Fresnel possibles, mais nous sommes principalement concernés par la zone 1. Si ce secteur est bloqué par un obstacle, par exemple un arbre ou un bâtiment, le signal arrivant à l'extrémité B serait diminué. En établissant des liens sans fil, nous devons donc être sûrs que ces zones soient exemptes d'obstacles. Naturellement rien n'est jamais parfait, ce qui, dans le domaine du réseautage sans fil, nous amène à vérifier que le secteur contenant environ 60 pour cent de la première zone de Fresnel devrait être maintenu libre d'obstacles.

Voici la formule pour calculer la première zone Fresnel:

```
r = 17,31 * √(N(d1*d2)/(f*d))
```

...où r est rayon de la zone en mètres, **N** est la zone à calculer, **d1** et **d2** sont les distances de l'obstacle par rapport aux extrémités lien en mètres, **d** est la distance totale du lien en mètres, et **f** est la fréquence en MHz. Notez que ceci vous donne le rayon de la zone en son centre. Dans le cas où vous installez vos antennes en hauteur, pour calculer la hauteur nécessaire par rapport le sol, vous devrez vous assurez que le sol ne rencontre pas la zone de Fresnel entre vos deux points.

Par exemple, calculons la taille de la première zone Fresnel au milieu d'un lien de 2km, transmettant à 2,437 GHz (802.11b chaîne 6):

```
r = 17,31 √(1 * (1000 * 1000) / (2437 * 2000))
r = 17,31 √(1000000 / 4874000)
r = 7,84 mètres
```

Supposons que nos deux tours en A et B ont une hauteur de dix mètres, la première zone de Fresnel passerait juste à 2.16 mètres au-dessus du niveau du sol au milieu du lien. Mais de quelle hauteur devrait être une structure à ce point pour libérer 60% de la première zone?

```
r = 17,31 √(0,6 *(1000 * 1000) / (2437 * 2000))
r = 17,31 √(600000 / 4874000)
r = 6,07 mètres
```

En soustrayant 10 m au résultat, nous pouvons voir qu'une structure d'une hauteur de 5,30 mètres au centre du lien bloquerait jusqu'à 60% de la première zone de Fresnel. Pour améliorer la situation, nous devrions placer nos antennes plus haut, ou changer la direction du lien pour éviter l'obstacle.

# Énergie

N'importe quelle onde électromagnétique transporte de l'énergie ou de la puissance: nous pouvons le sentir lorsque nous profitons (ou souffrons) de la chaleur du soleil. La puissance P est d'une importance cruciale pour le fonctionnement des liens sans fil: vous aurez besoin d'un minimum de puissance afin que le récepteur puisse donner un sens au signal reçu.

Dans le troisième chapitre, nous reviendrons sur les détails de la puissance de transmission, des pertes, des gains et de la sensibilité de la radio. Ici nous discutons brièvement de comment la puissance P est définie et mesurée.

Le champ électrique est mesuré en V/m (différence potentielle par mètre), la puissance contenue en son sein est proportionnelle au carré du champ électrique.

$$P \sim E^2$$

De façon pratique, nous mesurons la puissance au moyen d'une certaine forme de récepteur, par exemple une antenne et un voltmètre, wattmètre, oscilloscope, ou même une carte radio et un ordinateur portatif. Observer la puissance d'un signal revient à observer le carré du signal exprimé en Volts.

## Calculer avec des dBs

De loin, la technique la plus importante pour calculer la puissance est d'utiliser les ***décibels*** (***dB***). Il n'y a pas de nouvelle physique cachée dans ceci – ce n'est qu'une méthode pratique pour simplifier les calculs.

Le décibel est une unité sans dimensions[2], c.-à-d., qu'il définit un rapport entre deux mesures de puissance. Il est défini par:

```
dB = 10 * Log (P1 / P0)
```

Où **P1** et **P0** peuvent être n'importe qu'elle valeur que vous voulez comparer. Généralement, dans notre cas, elles représenteront une certaine quantité de puissance.

Pourquoi les décibels sont-ils si maniables? Beaucoup de phénomènes de la nature se comportent d'une manière que nous appelons exponentielle. Par exemple, l'oreille humaine peut percevoir un bruit deux fois plus fort qu'un autre si celui-ci a un signal physique dix fois plus fort.

Un autre exemple, tout à fait pertinent à notre champ d'intérêt, est l'absorption. Supposez qu'un mur se trouve dans le chemin de notre lien sans fil, et que chaque mètre de mur enlève la moitié du signal disponible. Le résultat serait:

```
0 mètres    =     1 (signal complet)
1 mètre     =     1/2
2 mètres    =     1/4
3 mètres    =     1/8
4 mètres    =     1/16
n mètres    =     1/2^n  = 2^-n
```

---

**2.** Un autre exemple d'unité sans dimension est le pourcentage (%) qui peut également être utilisé avec toutes sortes de quantités ou chiffres. Tandis que des mesures comme les pieds ou les grammes sont fixes, les unités sans dimensions représentent une relation.

Ceci est un comportement exponentiel.

Mais une fois que nous avons employée l'astuce d'appliquer le logarithme (log), les choses deviennent beaucoup plus faciles: au lieu de prendre une valeur à la nième puissance, nous multiplions simplement par n. Au lieu de multiplier des valeurs, nous les additionnerons.

Voici quelques valeurs couramment utilisées qu'il est important de mémoriser:

```
 +3 dB = double puissance
 -3 dB = moitié de puissance
 10 dB = ordre de magnitude (dix fois la puissance)
-10 dB = un dixième de puissance
```

En plus des mesures sans dimensions comme les dBs, il y a un certain nombre de définitions relatives à une certaine base de valeur P0. Les plus pertinentes pour nous sont les suivantes:

```
dBm   relatif à  P0 = 1 mW
dBi   relatif à une antenne isotrope idéale
```

Une ***antenne isotrope*** est une antenne hypothétique qui distribue également la puissance dans toutes les directions. L'antenne qui y ressemble le plus est l'antenne dipôle, bien qu'il faille souligner qu'une antenne isotrope parfaite ne peut être construite en réalité. Le modèle isotrope est cependant utile pour décrire le gain relatif de puissance d'une antenne existant dans le vrai monde.

Une autre convention commune (mais moins pratique) pour exprimer la puissance est le ***milliwatts***. Voici les niveaux de puissance équivalents exprimés en milliwatts et dBm:

```
  1 mW      = 0 dBm
  2 mW      = 3 dBm
100 mW      = 20 dBm
  1 W       = 30 dBm
```

# Physique dans le monde réel

Ne vous inquiétez pas si les concepts de ce chapitre représentent un véritable défi. Comprendre comment les ondes radio se propagent et interagissent avec environnement est un champ d'étude complexe en soi. La plupart des personnes trouvent difficile de comprendre un phénomène qu'elles ne peuvent pas observer avec leurs propres yeux. À présent, vous devriez comprendre que les ondes radio ne voyagent pas selon un chemin droit et

prévisible. Pour construire des réseaux de transmission fiables, vous devrez pouvoir calculer combien vous avez besoin de puissance pour parcourir une distance donnée, et prévoir comment les ondes voyageront le long du trajet.

Il y a beaucoup plus à apprendre sur la physique de radio, malheureusement nous n'avons pas assez d'espace pour ce faire au sein de cet ouvrage. Pour plus d'informations sur ce champ en évolution, consultez les ressources énumérées dans l'Annexe A. Maintenant que vous avez une bonne idée de la façon dont les ondes radio interagissent  dans le monde réel, vous êtes prêts à les utiliser pour communiquer.

# 3
# Conception d'un réseau

Avant d'acheter l'équipement ou de choisir une plateforme matérielle, vous devriez avoir une idée claire de la nature de votre problème de communication. Vous lisez sans doute ce livre parce que vous devez interconnecter des réseaux informatiques afin de partager des ressources puis d'accéder à Internet. La conception du réseau que vous choisissez de mettre en oeuvre devrait convenir au problème de communication que vous essayez de résoudre. S'agit-il de connecter un site distant à une connexion Internet au centre de votre campus? Est-il probable que la taille de votre réseau augmente afin d'inclure plusieurs sites distants? La plupart des composantes de votre réseau seront-elles installées à des endroits fixes ou votre réseau croîtra-t-il jusqu'à inclure des centaines d'ordinateurs portatifs mobiles et d'autres appareils?

Pour résoudre un problème complexe, il est souvent utile de faire un schéma de vos ressources et problèmes. Dans ce chapitre, nous nous concentrerons sur différentes façons d'établir des réseaux sans fil pour résoudre les problèmes de communication, ainsi que sur les schémas de la structure essentielle du réseau. Nous aborderons ensuite les concepts de réseautique qui définissent le TCP/IP, le langage principal de communication réseau actuellement parlé sur Internet. Finalement, nous présenterons plusieurs méthodes simples pour obtenir une circulation efficace de l'information à travers votre réseau et le reste du monde.

## *Conception du réseau physique*

Il peut sembler bizarre de parler de réseau « physique » en construisant des réseaux sans fil. Après tout, où se trouve la partie physique du réseau? Dans les réseaux sans fil, le support physique que nous employons pour la communication est évidemment l'énergie électromagnétique. Toutefois, dans le contexte de ce chapitre, le réseau physique se rapporte simplement à la dis-

position des objets dans l'espace.. Comment allez-vous organiser votre équipement afin de pouvoir joindre vos clients sans fil? Qu'ils soient tous concentrés dans un édifice à bureau ou dispersés sur plusieurs kilomètres, les réseaux sans fil sont déployés selon les trois configurations logiques suivantes:

- Liaisons point à point
- Liaisons point à multipoints
- Liaisons multipoints à multipoints

La disposition physique du réseau que vous choisissez dépendra de la nature du problème que vous essayez de résoudre. Même si votre réseau peut intégrer ces trois configurations à la fois, chaque liaison individuelle devra se configurer en l'une des topologies mentionnées ci-haut. La mise en œuvre de chacune de ces topologies s'explique mieux par un exemple.

## Point à point

Les liaisons ***Point à point*** fournissent généralement une connexion Internet là où un tel accès n'est pas disponible autrement. Un des côtés de la liaison point à point a une connexion directe à Internet, alors que l'autre côté emploie le lien pour y accéder. Par exemple, une université peut avoir une connexion *Frame Relay* ou VSAT au centre du campus, mais pourra partager une telle connexion avec un bâtiment important en dehors du campus. Si le bâtiment principal offre une vue sans obstacle sur le site distant, une connexion point à point peut être employée pour les relier. Ceci peut étendre ou même remplacer des liens dial-up existants. Avec les antennes appropriées et une bonne ligne de vue, il est possible d'installer des liaisons point à point fiables de plus de trente kilomètres.

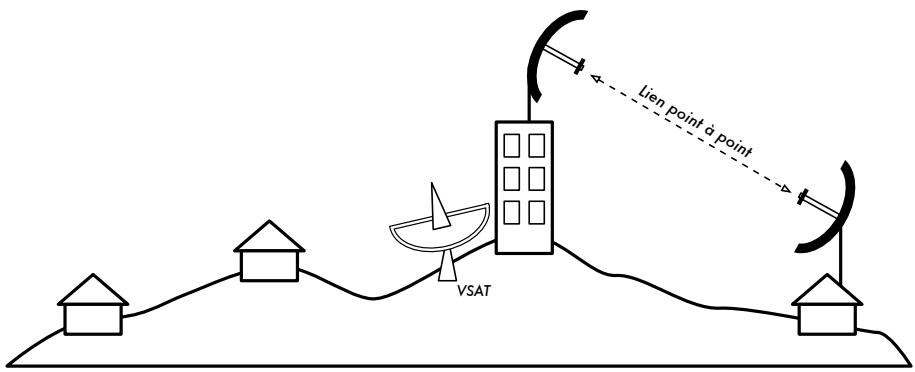


*Figure 3.1: Une liaison point à point permet à un site distant de partager une connexion centrale à Internet.*

Évidemment, une fois que la connexion point à point a été réalisée, il est possible d'en ajouter d'autres afin d'étendre davantage le réseau. Dans notre exemple, si le bâtiment éloignéest au sommet d'une grande colline, il peut être possible de voir d'autres endroits importants qui ne peuvent pas être vus directement à partir du campus central. En installant une autre liaison point à point sur le site distant, un autre noeud peut s'unir au réseau et se servir de la connexion Internet centrale.

Évidemment, une fois que la connexion point à point a été réalisée, il est possible d'en ajouter d'autres afin d'étendre davantage le réseau. Dans notre exemple, si le bâtiment éloignéest au sommet d'une grande colline, il peut être possible de voir d'autres endroits importants qui ne peuvent pas être vus directement à partir du campus central. En installant une autre liaison point à point sur le site distant, un autre noeud peut s'unir au réseau et se servir de la connexion Internet centrale.

## Point à multipoint

Un autre type de réseau assez populaire est le ***point à multipoint***. Dans toute situation ou plusieurs nœuds sont connectés à un point d'accès principal, on parle de réseau point à multipoint. L'exemple typique d'une application point à multipoint est l'utilisation d'un point d'accès sans fil qui fournit une connexion à plusieurs ordinateurs portatifs. Les ordinateurs portatifs ne communiquent pas les uns avec les autres directement, mais doivent être dans le champ du point d'accès afin d'accéder au réseau.

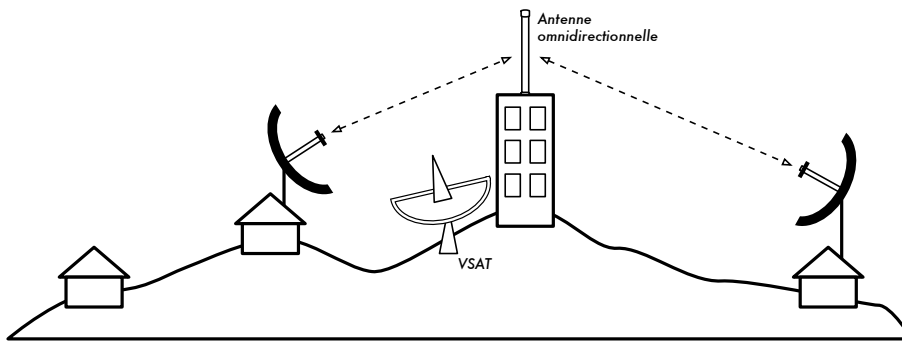


*Figure 3.2: Le VSAT central est maintenant partagé par plusieurs sites distants grâce à une antenne omnidirectionnelle. Les trois sites peuvent aussi communiquer directement à des vitesses beaucoup plus rapides que le VSAT.*

Le réseautage point à multipoint peut également s'appliquer à notre exemple précédent de l'université. Supposez que le bâtiment distant sur la colline est relié au campus central par une liaison point à multipoint. Plutôt que d'installer plusieurs liaisons point à points pour distribuer la connexion Internet, une seule antenne qui soit visible de plusieurs bâtiments distants pourrait

être employée. C'est un exemple classique d'une connexion ***point*** (site distant sur la colline) ***à multipoint*** (plusieurs bâtiments plus bas, dans la vallée).

Notez qu'il y a un certain nombre de questions relatives à la performance quant à l'usage des réseaux point à multipoint sur de très grandes distances, elle seront abordées plus tard dans ce chapitre. De tels liens sont possibles et utiles dans plusieurs circonstances, mais ne commettez pas l'erreur classique d'installer une antenne radio de grande puissance au milieu de la ville et compter pouvoir servir des milliers de clients, comme vous pourriez le faire avec une station de radio FM. Comme nous le verrons, les réseaux informatiques se comportent très différemment des stations d'émission radiophoniques.

## Multipoint à multipoint

Le troisième type de conception de réseau est le ***multipoint à multipoint***, qui est aussi connu sous le nom de réseau ***ad hoc*** ou ***maillé*** (*mesh* en anglais). Dans un réseau multipoint à multipoint, il n'y a aucune autorité centrale. Chaque noeud sur le réseau porte le trafic de tout autre selon le besoin, et tous les noeuds communiquent les uns avec les autres directement.

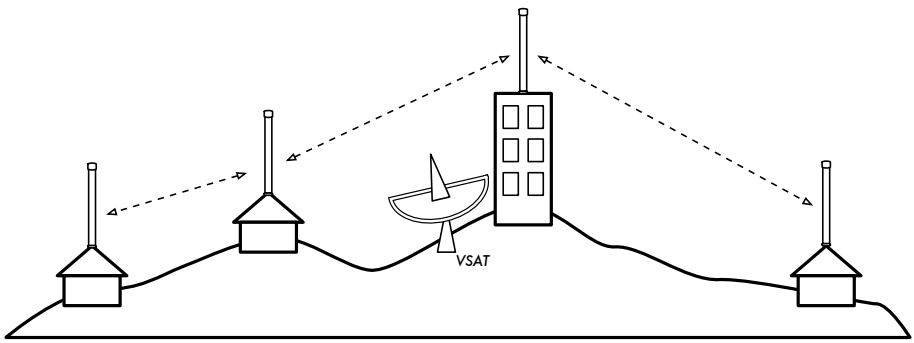


*Figure 3.3: Un réseau multipoint à multipoint maillé. Chaque point peut accéder à un autre à de très grandes vitesses ou utiliser la connexion centrale VSAT pour avoir accès à Internet.*

L'avantage de ce type de conception réseau est que même si aucun des noeuds n'est dans le rayon d'un point d'accès central, ils peuvent toujours communiquer entre eux. Les bonnes installations de réseau maillé s'auto maintiennent, étant donné qu'elles détectent automatiquement les problèmes de routage et les corrigent convenablement. Prolonger un réseau maillé est aussi simple que d'ajouter plus de noeuds. Si un des noeuds dans le « nuage » s'avère justement être une passerelle Internet, alors cette connexion peut être partagée entre tous les clients.

Deux grands inconvénients à cette topologie sont la complexité accrue et une performance moindre . La sécurité dans un tel réseau pose également problème, vu que chaque participant porte potentiellement le trafic de tous les autres. Le dépannage des réseaux Multipoint à multipoint tend à être compliqué en raison du grand nombre de variables qui changent lorsque les nœuds se déplacent. Les mailles multipoint à multipoint n'ont généralement pas la même capacité que les réseaux point à point ou point à multipoint en raison de la surcharge additionnelle à administrer le routage du réseau et l'usage plus intensif du spectre de radio.

Néanmoins, les réseaux maillés sont utiles dans plusieurs circonstances. À la fin de ce chapitre nous verrons un exemple de la façon d'établir un réseau multipoint à multipoint maillé en utilisant un protocole de routage appelé OLSR.

## Utiliser la technologie appropriée

Toutes ces topologies de réseau peuvent se complémenter dans un grand réseau et peuvent évidemment se servir des techniques traditionnelles de câblage de réseau lorsque c'est possible. Par exemple, le fait d'employer un lien sans fil de longue distance pour offrir l'accès à Internet à un emplacement éloigné puis d'y configurer un point d'accès pour offrir un accès local, est une pratique courante. Un des clients à ce point d'accès peut également agir en tant que noeud maillé, permettant au réseau de s'étendre organiquement entre les utilisateurs d'ordinateurs portables qui partageront la liaison originale point à point d'accès à Internet.

À présent que nous avons une idée claire de la façon dont les réseaux sans fil sont habituellement organisés, nous pouvons aborder comment la communication est possible sur de tels réseaux.

# *Le réseau logique*

La communication est seulement possible lorsque les participants parlent un même langage. Or une fois que la communication devient plus complexe qu'une simple radiodiffusion, le ***protocole*** devient aussi important que le langage. Toutes les personnes dans une salle peuvent parler anglais, mais sans un ensemble de règles qui établissent qui a le droit d'utiliser le microphone, un individu ne pourra pas communiquer ses idées à toute l'assistance. Imaginez maintenant une salle aussi grande que le globe, remplie de tous les ordinateurs qui existent. Sans un ensemble commun de protocoles de transmission pour réguler quand et comment chaque ordinateur peut parler, l'Internet serait un désordre chaotique où chaque machine essayerait de parler en même temps.

***TCP/IP*** fait référence à une suite de protocoles qui rendent possible la conversation sur le réseau Internet. Comprendre le TCP/IP vous permet de mettre en oeuvre des réseaux de pratiquement n'importe quelle taille et finalement faire partie intégrante du réseau Internet.

## Le modèle TCP/IP

Les réseaux informatiques sont souvent décrits comme étant construits sur beaucoup de couches. Chaque couche dépend de l'opération de toutes les couches subjacentes avant que la communication puisse avoir lieu, mais ne doit échanger les données qu'avec la couche au-dessus ou en-dessous d'elle. Le modèle de réseaux TCP/IP[1] comprend cinq couches, comme le démontre le diagramme suivant:

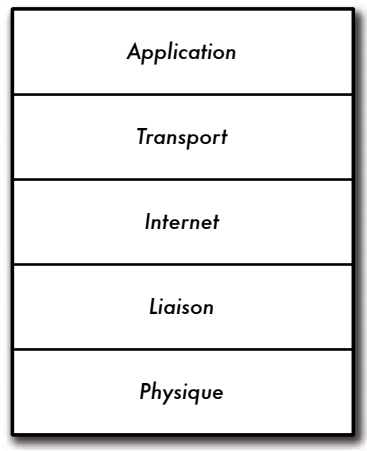


*Figure 3.4: Le modèle de réseautage TCP/IP.*

Dans la section précédente sur les topologies réseau, on a décrit la couche un: ***la couche physique***. C'est le milieu physique où les communications ont lieu. Ce peut être un câble de cuivre CAT5, un câble de fibre optique, des ondes radio, ou n'importe quel autre medium.

La couche suivante se nomme ***couche liaison de données*** (*data link* en anglais). À chaque fois que deux noeuds ou plus partagent le même medium physique (par exemple, plusieurs ordinateurs branchés à un hub, ou une salle remplie d'ordinateurs portatifs utilisant le même canal de radio) ils emploient la couche liaison de données pour déterminer à qui est le tour de transmettre sur le medium. Les exemples courants de protocoles de liaison de données sont Ethernet, Token Ring, ATM et les protocoles de gestion de

**1.** Le modèle TCP/IP n'est pas un Standard international et sa définition peut varier. Ici nous l'incluons comme modèle pragmatique utilisé pour comprendre et résoudre des problèmes dans les réseaux Internet.

réseau sans fil (802.11a/b/g). La communication sur cette couche est nommée ***liaison locale*** puisque tous les noeuds connectés à cette couche peuvent communiquer avec les uns avec les autres directement. Sur des réseaux de type Ethernet, chaque nœuds a sa propre ***adresse MAC*** qui est un numéro unique de 48 bits assigné à chaque appareil du réseau lors de sa fabrication.

Juste au-dessus de la couche liaison de données se trouve la ***couche Internet***. Pour TCP/IP, ceci est le Protocole Internet (***IP***). Au niveau de la couche Internet, les paquets peuvent quitter le réseau de liaison locale et être retransmis sur d'autres réseaux. Les routeurs effectuent cette fonction sur un réseau en ayant au moins deux interfaces de réseau, une sur chacun des réseaux à être interconnectés. Les noeuds sont accessibles sur Internet par leur adresse IP uniqueglobale.

Une fois que le routage Internet est établi, une méthode est nécessaire pour accéder à un service particulier à une adresse IP donnée. Cette fonction est assurée par la couche suivante, la ***couche transport***.TCP et UDP sont des exemples communs de protocoles de la couche transport. Quelques protocoles de la couche transport (telle que le TCP) s'assurent que toutes les données arrivent à destination et soient rassemblées et livrées à la prochaine couche dans l'ordre approprié.

Finalement, au sommet, nous retrouvons la ***couche application***. C'est la couche à laquelle la plupart des usagers de réseau sont exposés et c'est le niveau où la communication humaine se produit. HTTP, FTP et SMTP sont tous des protocoles de couche application. Les personnes se retrouvent audessus de toutes les couches et ont besoin de peu ou d'aucune connaissance des couches sous-jacentes pour utiliser efficacement le réseau.

On peut voir le modèle TCP/IP comme une personne qui livre une lettre à un édifice à bureaux au centre ville. Il devra d'abord interagir avec la rue (la couche physique), faire attention au trafic sur cette rue (la couche liaison de données), tourner à l'endroit approprié pour se connecter à d'autres rues et arriver à l'adresse correcte (la couche Internet), se rendre à l'étage et au numéro de salle appropriée (la couche transport), et finalement trouver le destinataire ou un réceptionniste qui pourra lui remettre la lettre (la couche application). En Anglais, on peut facilement se rappeler des cinq couches en employant la phrase mnémonique « ***P****lease* ***D****on't* ***L****ook* ***I****n* ***T****he* ***A****ttic* » pour la suite de couches **P**hysique, **D**onnées (**L**iaison), **I**nternet, **T**ransport et **A**pplication.

# 802.11 Réseaux sans fil

Avant que des paquets puissent être expédiés et routés sur Internet, les couches un (physique) et deux (liaison de données) doivent être connectées. Sans connectivité locale, les noeuds réseau ne peuvent pas parler entre eux ni transmettre des paquets.

Pour fournir la connectivité physique, les réseaux sans fil doivent fonctionner dans la même partie du spectre de radio. Comme nous l'avons vu au sein du chapitre deux, ceci signifie que les radios 802.11a parleront aux radios 802.11a à environ 5GHz, et les radios 802.11b/g parleront à d'autres radios 802.11b/g à environ 2,4GHz. Mais un dispositif 802.11a ne peut pas interagir avec un dispositif 802.11b/g car ils utilisent des parties complètement différentes du spectre électromagnétique.

Plus spécifiquement, les cartes sans fil doivent s'accorder sur un canal commun. Si une carte radio 802.11b est placée sur le canal 2 tandis qu'une autre est placée sur le canal 11, alors les radios ne peuvent pas communiquer entre elles.

Lorsque deux cartes sans fil sont configurées pour employer le même protocole sur le même canal radio, alors elles peuvent négocier la connectivité de la couche liaison de données. Chaque dispositif 802.11a/b/g peut fonctionner dans un des quatre modes possibles suivants:

1. Le ***mode maître*** (aussi nommé ***AP*** ou ***mode infrastructure***) est employé pour créer un service qui ressemble à un point d'accès traditionnel. La carte sans fil crée un réseau avec un canal et un nom spécifique (appelé le ***SSID***) pour offrir ses services. Sur ce mode, les cartes sans fil contrôlent toutes les communications liées au réseau (authentification des clients sans fil, contrôle d'accès au canal, répétition de paquets, etc...) Les cartes sans fil en mode maître peuvent seulement communiquer avec les cartes qui sont associées à lui en mode administré.
2. Le ***mode administré*** (*managed mode* en anglais) est également parfois désigné sous le nom de mode ***client***. Les cartes sans fil en mode administré joindront un réseau créé par un maître et changeront automatiquement leur canal pour que celui-ci corresponde à celui du maître. Ensuite, elles présentent leurs identifications au maître. Si celles-ci sont acceptées, elles sont alors ***associées*** au maître. Les cartes en mode administré ne communiquent pas entre-elles directement et communiqueront uniquement avec un maître associé.
3. Le ***mode ad hoc*** crée un réseau multipoint à multipoint où il n'y a aucun noeud maître ou AP. En mode ad hoc, chaque carte sans fil communique directement avec ses voisins. Les noeuds doivent être à la portée des

autres pour communiquer, et doivent convenir d'un nom de réseau et un canal.

4. Le ***mode moniteur*** est employé par certains outils (tels que Kismet, chapitre six) pour écouter passivement tout le trafic radio sur un canal donné. Lorsqu'elles se trouvent en mode moniteur, les cartes sans fil ne transmettent aucune donnée. Ceci est utile pour analyser des problèmes sur un lien sans fil ou observer l'utilisation de spectre dans le secteur local. Le mode moniteur n'est pas utilisé pour des communications normales.

Lorsque nous réalisons une liaison point à point ou point à multipoint, une radio fonctionnera typiquement en mode maître, alors que l'autre (ou les autres) fonctionnera en mode réseau. Dans un réseau maillé multipoint à multipoint, toutes les radios fonctionnent en mode ad hoc de sorte qu'elles puissent communiquer les unes avec les autres directement.

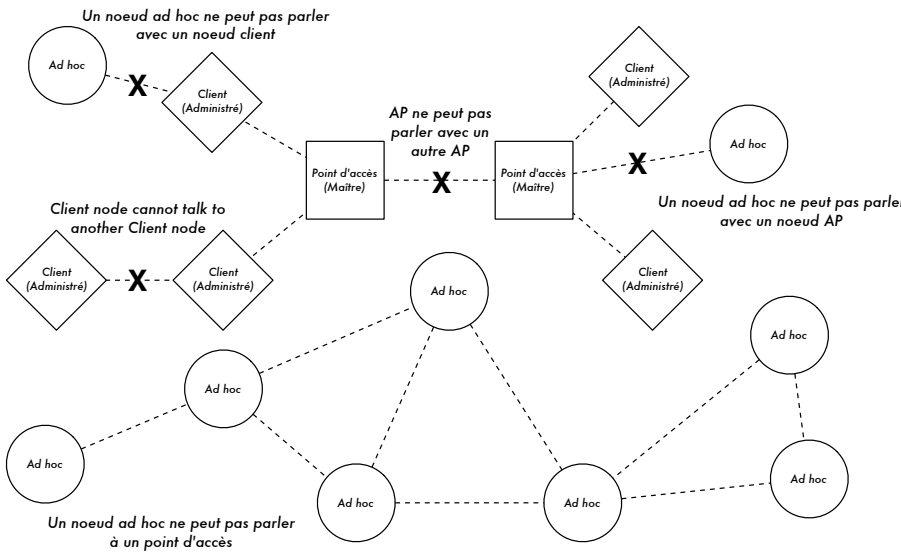


*Figure 3.5: AP, Clients et nœuds Ad Hoc.*

Il est important d'avoir à l'esprit ces modes lors de la conception d'un réseau. Rappelez-vous que les clients en mode administré ne peuvent pas communiquer entre eux directement, ainsi il est probable que vous vouliez installer un répéteur en mode maître ou ad hoc. Comme nous le verrons plus tard dans ce chapitre, le mode ad hoc est plus flexible mais a un certain nombre de problèmes de performance par rapport aux modes maître et administré.

Maintenant que vos cartes sans fil fournissent une connectivité physique et de liaison de données, elles sont prêtes à commencer à passer des paquets sur la couche 3: la couche Internet.

# Réseautage Internet

Les adresses IP, l'adressage de réseau, le routage et la transmission (« *fowarding* » en anglais) sont des concepts importants et très liés en réseautique Internet. Une ***adresse IP*** est un identifiant d'un noeud réseau tel qu'un PC, un serveur, un routeur, ou un pont. ***L'adressage réseau*** est le système utilisé pour attribuer ces identifiants dans des groupes convenables. Le ***routage*** permet de retracer ces groupes au sein du réseau. Les résultats du processus de routage sont maintenus dans une liste appelée ***table de routage***. La ***transmission*** consiste à utiliser la table de routage afin d'envoyer un paquet de données soit à la destination finale ou nœud suivant, plus proche de la destination.

## Adresses IP

Dans un réseau IP3, l'adresse est un numérotation de 32 bits, normalement écrit en quatre chiffres de 8 bits exprimés en forme décimale, séparée par des points. Des exemples d'adresses IP sont 10.0.17.1, 192.168.1.1, ou 172.16.5.23.

## Adressage réseau

Les réseaux interconnectés doivent suivre un plan d'adressage IP. Au niveau de l'Internet global, il y a des comités de personnes qui assignent des adresses IP selon une méthode cohérente et logique pour s'assurer que les adresses ne se dupliquent pas dans le réseau, et que des raccourcis puissent être utilisés pour référer aux groupes d'adresses. Ces groupes d'adresses s'appellent sous-réseaux ou ***subnet*** en plus court. Les plus grands subnets peuvent être subdivisés en plus petits subnets. Parfois un groupe d'adresses liées se nomme ***espace d'adressage***.

Sur Internet, aucune personne ou organisation ne possède vraiment ces groupes d'adresses parce que les adresses ont un sens uniquement si le reste de la communauté d'Internet est d'accord sur leur usage. C'est en faisant des accords que les adresses sont assignées aux organismes selon leur besoin et leur taille. Une organisation à qui on a assigné une série d'adresses peut alors assigner une portion de ces adresses à une autre organisation comme partie d'un contrat de service. Les adresses qui ont été assignés de cette manière, en commençant par les comités reconnus internationalement, puis distribuées hiérarchiquement par des comités nationaux ou régionaux , se dénomment ***adresses IP globalement routées***.

Parfois il n'est pas simple ou possible pour un individu ou une organisation d'obtenir plus d'une adresse IP globalement routée. Dans ce cas, il est possible d'utiliser une technique connue sous le nom de ***Traduction d'adresse***

***réseau*** (ou *Network Address Translation*, ***NAT*** en anglais). Un appareil NAT est un routeur avec deux ports réseau. Le port extérieur utilise une adresse IP globalement routée, alors que le port intérieur utilise une adresse IP d'une classe spéciale connue sous le nom d'adresses privées[2]. Le routeur NAT permet qu'une seule adresse globale puisse être partagée avec tous les usagers internes, lesquels utilisent des adresses privées. Il convertit les paquets d'une forme d'adressage à une autre tandis que les paquets passent par lui. De sorte que les usagers ont l'impression d'être directement connectés à Internet et n'ont besoin d'aucun logiciel ou pilote spécial pour partager une seule adresse IP globalement routée.

## Routage

L'Internet change et se développe constamment. De nouveaux réseaux sont continuellement ajoutés et des liens entre les réseaux sont s'ajoutés, enlevés, rompu et se rétabli à nouveau. C'est le travail du ***routage*** de déterminer le meilleur chemin pour arriver à destination et de créer une table de routage présentant le meilleur chemin pour toutes les différentes destinations.

Le ***routage statique*** est le terme utilisé quand la table de routage est créée par configuration manuelle. Ceci est parfois opportun pour de petits réseaux mais peut facilement devenir très difficile et enclin aux erreurs pour de plus grands réseaux. Pire encore, si le meilleur chemin à un réseau devient inutilisable en raison d'un problème à l'équipement ou pour d'autres raisons, le routage statique ne se servira pas du deuxième meilleur chemin.

Le ***routage dynamique*** est une méthode dans laquelle les éléments réseau, en particulier les routeurs, échangent de l'information sur leur état et l'état de leurs voisins dans le réseau, et emploient ensuite cette information pour sélectionner automatiquement le meilleur chemin et pour créer la table de routage. Si quelque chose change, comme un routeur qui ne fonctionne plus ou un nouveau routeur qui serait mis en service, alors les protocoles dynamiques de routage fonts des ajustements à la table routage. Le système d'échange de paquets et de prise de décision est connu comme protocole ***de routage***. Il y a beaucoup de protocoles de routage qui sont aujourd'hui employés au niveau d'Internet, entre autres l'OSPF, le BGP, le RIP et l'EIGRP.

Les réseaux sans fil sont comme les réseaux câblés du fait qu'ils ont besoin de protocoles dynamiques de routage, mais ont également assez de différences pour requérir de protocoles de routage orientés à leurs besoins spécifiques. En particulier, les connexions de réseau câblé fonctionnent généralement bien ou ne fonctionnent pas du tout (par exemple, un câble Ethernet est branché, ou il ne l'est pas). Les choses ne sont pas aussi claires

---

**2.** Le terme adresses privées est définit à RFC 1918, http://www.ietf.org/rfc/rfc1918

en travaillant avec des réseaux sans fil. La communication sans fil peut être affectée par des objets entrant dans le chemin du signal, ou par des signaux faisant interférence. En conséquence, les liens peuvent bien fonctionner ou fonctionner pauvrement, ou encore varier entre les deux extrêmes. Puisque les protocoles de réseau existants ne tiennent pas compte de la qualité d'un lien en prenant des décisions concernant le routage, les comités IEEE 802.11 et l'IETF travaillent à normaliser des protocoles pour les réseaux sans fil. Actuellement, il est difficile de savoir quand est-ce qu'une norme unique prenant en considération les liens de qualité variable émergera.

Entre-temps, il y a plusieurs tentatives de programmation ad hoc qui essayent de résoudre le problème. En voici quelques exemples: ***Hazy Sighted Link State*** (***HSLS***), ***Ad-hoc On-demand Distance Vector*** (***AODV***) et ***Optimized Link State Routing*** (***OLSR***). Un autre exemple est SrcRR, une combinaison de DSR et ETX mis en œuvre par le projet Roofnet du M.I.T. Plus loin dans ce chapitre nous verrons un exemple de comment mettre en marche un réseau utilisant OLSR pour prendre des décisions de routage.

## «Forwarding»

Le « ***Fowarding*** » est beaucoup plus simple que l'adressage et le routage. Chaque fois qu'un routeur reçoit un paquet de données, il consulte sa table de routage interne. En commençant par le bit le plus significatif, la table de routage recherche l'entrée qui ait le plus grand nombre de bits correspondant à l'adresse de destination. Ceci s'appelle le ***préfixe*** d'adresse. Si une entrée avec un préfixe correspondant est trouvée dans la table de routage, alors le champ ***nombre de sauts*** (***Hop count*** en anglais) ou ***temps de vie*** (***Time-To-Live*** en anglais, ***TTL***) est décrémenté. Si le résultat est zéro, alors le paquet est abandonné et une notification d'erreur est retournée à l'expéditeur. Autrement, le paquet est envoyé au noeud ou à l'interface indiquée dans la table de routage. Par exemple, si la table de routage contient ces entrées:

```
Destination     Passerelle      Masque          Drapeaux  Métrique  Interface

10.15.6.0       0.0.0.0         255.255.255.0   U     0         eth1
10.15.6.108     10.15.6.7       255.255.255.255 UG    1         eth1
216.231.38.0    0.0.0.0         255.255.255.0   U     0         eth0
0.0.0.0         216.231.38.1    0.0.0.0         UG    0         eth0
```

... et qu'un paquet arrive avec l'adresse de destination 10.15.6.23, alors le routeur l'enverrait sur l'interface eth1. Si le paquet a une destination 10.15.6.108, alors il serait expédié à la passerelle 10.15.6.7 (puisqu'elle est plus spécifique et correspond a plus de bits d'ordre élevé que la route au réseau 10.15.6.0).

Une destination 0.0.0.0 est une convention spéciale désignée sous le nom de ***passerelle par défaut***. Si aucun autre préfixe ne correspond à l'adresse de destination, alors le paquet est envoyé à la passerelle par défaut. Par exemple, si l'adresse de destination était 72.1.140.203, alors le routeur expédierait le paquet à 216.231.38.1 (qui l'enverraient vraisemblablement plus près de la destination finale et ainsi de suite).

Si un paquet arrive et aucune entrée n'est trouvée (c.-à-d., il n'y a aucune passerelle par défaut définie et aucun préfixe ne correspond à une route connue), alors on abandonne le paquet et une notification d'erreur est retournée à l'expéditeur.

Le champ TTL est employé pour détecter des boucles de routage. Sans lui, un paquet pourrait sans cesse être envoyé dans les deux sens entre deux routeurs qui s'identifient mutuellement comme le prochain meilleur relais. Ce genre de boucles cause une grande quantité de trafic inutile sur un réseau et peut donc menacer sa stabilité. L'utilisation du champ TTL ne règle pas le problème des boucles de routage, mais peut aider à empêcher qu'elles détruisent un réseau à cause d'une simple mauvaise configuration.

## Tout rassembler

Une fois que tous les noeuds réseau ont une adresse IP, ils peuvent envoyer des paquets de données aux adresses IP de n'importe quel autre noeud. Par l'utilisation du routage et du fowarding, ces paquets peuvent accéder à des noeuds sur des réseaux qui ne sont pas physiquement connectés au noeud d'origine. Ce processus décrit bien ce qui déroule sur Internet, tel qu'illustré par la Figure 3.6.

Dans cet exemple, vous pouvez voir le chemin que les paquets prennent pendant qu'Alice cause avec Bob en utilisant un service de messages instantanés. Chaque ligne pointillée représente un câble Ethernet, un lien sans fil, ou n'importe quel autre genre de réseau physique. Le symbole du nuage est généralement employé pour remplacer « Internet » et représente tout autres réseaux IP intervenants. Aussi longtemps que les routeurs expédient le trafic IP vers la destination finale, ni Alice ni Bob n'ont besoin de savoir comment ces réseaux fonctionnent. Sans les protocoles Internet et la coopération de tous sur le réseau, ce genre de communication serait impossible.

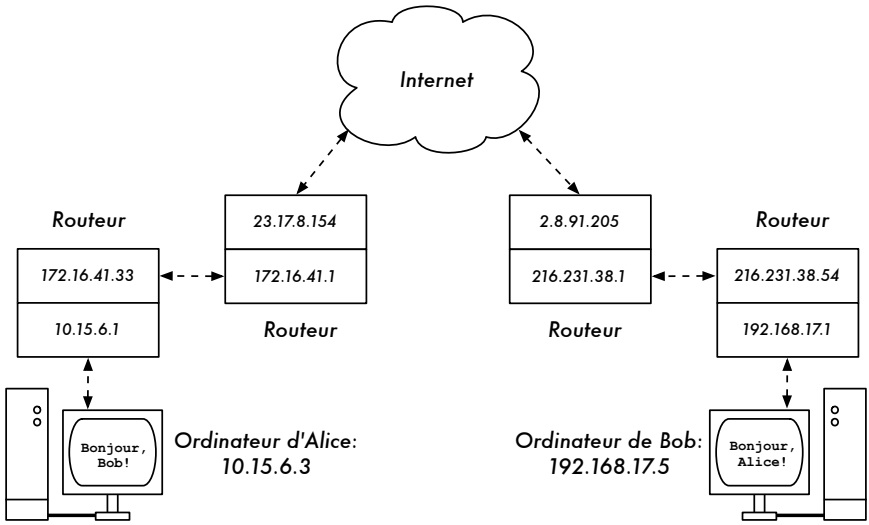


*Figure 3.6: Réseautage Internet. Chaque segment de réseau a un routeur avec deux adresses IP, réalisant un «lien local» à deux réseaux différents. Les paquets sont expédiés entre les routeurs jusqu'à ce qu'ils atteignent leur destination finale.*

Maintenant que nous avons vu comment les paquets circulent sur des réseaux IP, observons un genre très spécialisé de réseau IP: un OLSR maillé.

# Réseautage maillé avec OLSR

La plupart des réseaux WiFi fonctionnent en mode infrastructure - ils se composent d'un point d'accès quelque part (avec une radio fonctionnant en mode maître), relié à une ligne DSL ou à tout autre réseau câblé à grande échelle. Dans un tel ***hotspot***, le point d'accès agit habituellement en tant que station principale qui distribue l'accès Internet à ses clients, qui opèrent en mode administré. Cette topologie est semblable à celle d'un service de téléphone mobile (GSM). Les téléphones mobiles se connectent à une station de base - sans la présence d'une station de base les téléphones mobiles ne peuvent pas communiquer entre eux. Si, pour plaisanter, vous faites un appel à un ami qui s'assoit de l'autre côté de la table, votre téléphone envoie des données à la station base de votre fournisseur qui peut se trouver à plusieurs kilomètres de distance. Puis, la station de base envoie ces données de nouveau au téléphone de votre ami.

Les cartes WiFi en mode administré ne peuvent pas communiquer directement, non plus. Les clients - par exemple, deux ordinateurs portatifs sur la même table - doivent utiliser le point d'accès comme relais. N'importe quel trafic entre des clients connectés à un point d'accès doit être envoyé deux fois. Si les clients A et C communiquent, le client A envoie des données au point d'accès B, puis le point d'accès retransmet les données au client C.

Une seule transmission peut avoir une vitesse de 600 kByte/sec (à peu près la vitesse maximum que vous pourriez atteindre avec 802.11b). Dans notre exemple, comme les données doivent être répétées par le point d'accès avant qu'elles n'atteignent leur cible, la vitesse efficace entre les deux clients sera de seulement 300 kByte/sec.

En mode ad hoc il n'y a aucun rapport hiérarchique de maître-client. Les noeuds peuvent communiquer directement aussi longtemps qu'ils sont dans la portée de leurs interfaces sans fil. Ainsi, dans notre exemple les deux ordinateurs pourraient atteindre la vitesse maximum en fonctionnant en mode ad hoc, dans des circonstances idéales.

L'inconvénient au mode ad hoc est que les clients ne répètent pas le trafic destiné à d'autres clients. Dans l'exemple de point d'accès, si deux clients A et C ne peuvent pas directement « se voir » avec leurs interfaces sans fil, ils peuvent tout de même communiquer aussi longtemps que l'AP est à portée des deux clients.

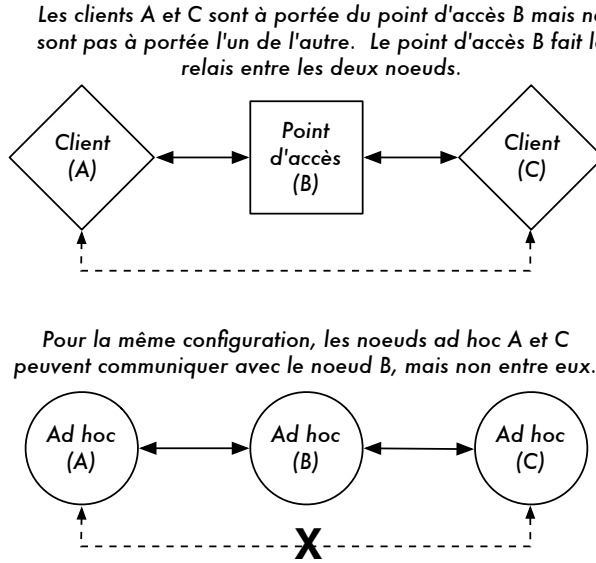


*Figure 3.7: Le point d'accès B va transmettre le trafic entre les clients A et C. En mode Ad hoc, le nœud B ne transmettra pas le trafic entre A et C par défaut.*

Les noeuds ad hoc ne répètent pas de données par défaut, mais ils peuvent efficacement le faire si le **routage** est appliqué. Les réseaux maillés sont basés sur la stratégie que chaque noeud agit en tant que relais pour prolonger la couverture du réseau sans fil. Plus il y aura de noeuds, meilleure sera la couverture radio et la portée du nuage maillé.

Sur ce point, nous devons mentionner un compromis crucial. Si le dispositif emploie seulement une interface radio, la largeur de bande disponible est sensiblement réduite chaque fois que le trafic est répété par des noeuds intermédiaires sur le chemin de A à B. En outre, il y aura interférence dans la transmission due aux noeuds partageant le même canal. Ainsi, les réseaux maillés ad hoc bon marché peuvent fournir une bonne couverture radio jusqu'aux zones les plus éloignées d'un réseau sans fil communautaire mais au prix de la vitesse; particulièrement si la densité des noeuds et la puissance de transmission sont élevées.

Si un réseau ad hoc se compose seulement de quelques noeuds qui sont en service à toute heure, s'il n'est pas mobile et a toujours des liens radio stables(ainsi qu'une longue liste de bien d'autres conditions) il est possible d'écrire à la main une table de routage individuelle pour tous les nœuds.

Malheureusement, ces conditions sont rarement réunies dans la vraie vie. Les noeuds peuvent cesser de fonctionner, les dispositifs WiFi se désorienter et l'interférence peut rendre les liens radio inutilisables à tout moment. Et personne ne veut mettre à jour plusieurs tables de routage à la main si un noeud est ajouté au réseau. En employant des protocoles de routage qui maintiennent automatiquement différentes tables de routage dans tous les noeuds impliqués, nous pouvons éviter ces problèmes. Les protocoles de routage les plus courants dans le monde câblé (tel que l'OSPF) ne fonctionnent pas bien dans un tel environnement parce qu'ils ne sont pas conçus pour traiter des liens perdus ou des topologies qui changent rapidement.

## Routage maillé avec olsrd

« *Optimized Link State Routing Daemon* », *olsrd*, de *olsr.org* est une application de routage destinée aux réseaux sans fil. Nous nous concentrerons sur ce logiciel de routage pour plusieurs raisons. C'est un projet de code source libre qui fonctionne avec Mac OS X, Windows 98, 2000, XP, Linux, FreeBSD, OpenBSD et NetBSD. Olsrd est disponible pour les points d'accès qui utilisent Linux comme Linksys WRT54G, Asus Wl500g, Access Cube ou des Pocket PCs utilisant Familiar Linux et est inclus dans les kits Metrix utilisant Metrix Pebble. Olsrd , peut gérer des interfaces multiples et est extensible avec différents plug-ins. Il supporte IPv6 et il est activement développé et utilisé par des réseaux communautaires partout dans le monde.

Il existe plusieurs implantations pour olsr, lequel a commencé comme une ebauche de l'IETF écrit à l'INRIA en France. L'application d'olsr.org a pris naissance au sein de la thèse de maîtrise d'Andreas Toennesen à l'université d'UniK. Le daemon de routage a été modifié sur la base de l'expérience pratique des réseaux communautaires libres. Olsrd diffère maintenant de manière significative de l'ébauche originale parce qu'il inclut un mécanisme appelé *Link Quality Extension* (prolongation de la qualité du lien) qui mesure

la perte de paquet entre les noeuds et calcule des itinéraires selon cette information. Cette prolongation brise la compatibilité avec les démons de routage qui respectent l'ébauche de l'INRIA. L'olsrd fourni par olsr.org peut être configuré pour se comporter selon La l'ébauche de l'IETF qui n'a pas cette caractéristique. Cependant il n'y a aucune raison de désactiver le *Link Quality Extension* à moins que la conformité avec d'autres implantations soit exigée.

## Théorie

Lorsque l'olsrd fonctionne pendant un certain temps, un noeud connaît l'existence de chaque autre noeud dans le nuage maillé et sait quels noeuds peuvent être employés pour router le trafic vers eux. Chaque noeud maintient une table de routage couvrant le nuage maillé en entier. Cette approche de routage maillé s'appelle ***routage proactif***. En revanche, les algorithmes de ***routage réactif*** vont procéder au routage uniquement lorsqu'il est nécessaire d'envoyer des données à un noeud spécifique.

Il y a des avantages et des désavantages au routage proactif, et il y a beaucoup d'autres solutions sur la façon de faire un routage maillé dont il est intéressant de mentionner. Le principal avantage du routage proactif est que nous savons qui est en dedans et en dehors du réseau et il n'est pas nécessaire d'attendre jusqu'à ce qu'un itinéraire soit trouvé. Entre les désavantages nous retrouvons le trafic de protocole élevé et une charge de CPU plus importante. À Berlin, la communauté Freifunk opère un nuage maillé où olsrd doit contrôler plus de 100 interfaces. La charge moyenne de CPU provoquée par l'olsrd sur un Linksys WRT54G fonctionnant à 200 mégahertz est d'environ 30% dans le maillage de Berlin. Il y a clairement une limite à l'utilisation du protocole proactif: elle dépend du nombre d'interfaces impliquées et combien de fois les tables de routage sont mises à jour. Le maintien des routes dans un nuage maillé avec des noeuds statiques implique moins d'efforts qu'un maillage avec des noeuds qui sont constamment en mouvement, puisque la table de routage doit être mise à jour moins souvent.

## Mécanisme

Un noeud utilisant olsrd envoie constamment des messages de « *Hello* » à un intervalle donné afin que les voisins puissent détecter sa présence. Chaque noeud calcule statistiquement combien de « *Hello* » ont été perdus ou reçus de chaque voisin ; obtenant de ce fait des informations sur la topologie et la qualité des liens des noeuds dans le voisinage. L'information topologique obtenue est diffusée en tant que messages de contrôle de topologie (*TC messages*) et expédiée par les voisins que l'olsrd a choisi comme relais 'multipoint'.

Le concept des relais multipoint est une nouvelle solution au routage proactif qui vient de l'ébauche du standard OLSR. Si chaque nœud retransmet l'information topologique qu'il a reçue, une surcharge inutile pourrait se produire. De telles transmissions sont redondantes si un noeud a beaucoup de voisins. Ainsi, un noeud d'olsrd décide quels voisins sont des relais multipoints favorables qui devraient expédier ses messages de contrôle de topologie. Notez que les relais multipoints sont seulement choisis uniquement aux fins de retransmettre des messages TC. La charge utile (payload) est routée en utilisant tous les noeuds disponibles.

OLSR, spécifie deux autres types de message qui informent si un noeud offre une passerelle à d'autres réseaux (messages HNA) ou a des interfaces multiples (messages MID). Il n'y a pas grand chose à dire au sujet de ces messages à part le fait qu'ils existent. Les messages HNA rendent l'olsrd très pratique pour se connecter à Internet avec un appareil mobile. Quand un noeud se à l'intérieur du maillage, il détectera des passerelles dans d'autres réseaux et choisira toujours celle vers laquelle il a le meilleur itinéraire. Cependant, l'olsrd n'est pas infaillible. Si un noeud annonce qu'il est une passerelle Internet, même s'il ne l'est pas parce qu'il ne l'a jamais été ou parce qu'il n'est pas en ligne à ce moment là, les autres noeuds feront néanmoins confiance à cette information. Cette pseudo passerelle est un trou noir. Pour surmonter ce problème, une application de passerelle dynamique plug-in a été développée. Le plug-in va automatiquement détecter si la passerelle est vraiment connectée et si le lien est toujours actif. Si ce n'est pas le cas, l'olsrd cesse d'envoyer de faux messages HNA. Il est fortement recommandé de compiler et d'utiliser ce plugin au lieu de dépendre des messages HNA statiques.

## Pratique

Olsrd accomplit le routage IP dans l'espace-usager; l'installation est donc assez facile. Les paquets d'installation sont disponibles pour OpenWRT, AccessCube, Mac OS X, Debian GNU/Linux et Windows. OLSR est une partie standard de Metrix Pebble. Si vous devez faire une compilation de la source, veuillez lire la documentation qui est fournie avec le paquet. Si tout est configuré correctement tout ce que vous devez faire est de démarrer le programme olsr.

Tout d'abord, il faut s'assurer que chaque noeud a une adresse IP unique statiquement assignée pour chaque interface utilisée dans le maillage. Il n'est pas recommandé (ni faisable) d'utiliser le DHCP dans un réseau maillé IP. Une requête DHCP ne sera pas répondue par un serveur DHCP si le noeud qui la demande a besoin d'un lien multi-bond pour se connecter à lui et déployer un relais dhcp dans tout un maillage est quasiement impraticable. Ce problème pourrait être résolu en utilisant IPv6, puisqu'il y a beaucoup d'espace disponible pour générer une adresse IP unique à partir de l'adresse

MAC de chaque carte impliquée (comme suggéré par K. Weniger et M. Zitterbart (2002) dans « *IPv6 Stateless Address Autoconfiguration in large mobile ad hoc networks* »).

Une page-wiki où chaque personne intéressée peut choisir une adresse IPv4 individuelle pour chaque interface exécutant olsr daemon, pourrait convenir. Cependant, il n'y a pas de manière facile d'automatiser le processus si IPv4 est employé.

Par convention, l'adresse de diffusion générale (broadcast en anglais) devrait être 255.255.255.255 sur les interfaces maillées. Il n'y a aucune raison d'entrer l'adresse de diffusion explicitement puisque olsrd peut être configuré pour remplacer toute adresse de diffusion par sa valeur par défaut. Nous n'avons qu'à nous assurer que les configurations sont partout identiques. Olsrd peut faire ceci par lui-même. Lorsqu'un fichier de configuration olsrd par défaut est établi, cette caractéristique devrait être activée afin d'éviter des confusions du genre: « pourquoi les autres noeuds ne peuvent pas voir ma machine?!? »

Configurez maintenant l'interface sans fil. Voici un exemple de commande sur la façon de configurer une carte WiFi avec le nom wlan0 en utilisant Linux:

```
iwconfig wlan0 essid olsr.org mode ad-hoc channel 10 rts 250 frag 256
```

Vérifiez que la partie sans fil de la carte WiFi a été configurée de façon à ce qu'elle ait une connexion ad hoc à d'autres noeuds à portée directe (saut unique). Assurez-vous que l'interface joint le même canal sans fil, emploie le même nom sans fil ESSID (*Extented Service Set Identifier*) et à la même Cell-ID que toutes les autres cartes WiFi qui constituent le maillage. Plusieurs cartes WiFi ou leurs pilotes respectifs n'agissent pas conformément à la norme 802.11 pour les réseaux ad hoc et ne peuvent donc pas se connecter à une cellule. De même, elles ne peuvent pas se connecter à d'autres appareils sur la même table, même si elles sont configurées avec le même canal et le même nom de réseau sans fil. Aussi, elles peuvent confondre d'autres cartes qui se comportent selon la norme en créant leur propre Cell-ID sur le même canal avec le même nom de réseau sans fil. Les cartes WiFi faites par Intel qui sont fournies avec Centrino Notebooks sont réputées pour avoir ce comportement.

Vous pouvez vérifier ceci avec la commande **`iwconfig`** en utilisant GNU-Linux. Voici les résultats sur mon ordinateur:

```
wlan0   IEEE 802.11b  ESSID:"olsr.org"
        Mode:Ad-Hoc  Frequency:2.457 GHz  Cell: 02:00:81:1E:48:10
        Bit Rate:2 Mb/s   Sensitivity=1/3
        Retry min limit:8   RTS thr=250 B   Fragment thr=256 B
        Encryption key:off
        Power Management:off
        Link Quality=1/70  Signal level=-92 dBm  Noise level=-100 dBm
        Rx invalid nwid:0  Rx invalid crypt:28  Rx invalid frag:0
        Tx excessive retries:98024 Invalid misc:117503 Missed beacon:0
```

Il est important de configurer la valeur- seuil RTS – « *Request To Send* » pour un réseau maillé, afin de limiter l'effet de collisions entre les transmissions des noeuds du même canal. RTS/CTS s'assure que le canal est libre avant chaque transmission de paquet. Ceci implique une surcharge, mais augmente la performance lorsqu'il existe des noeuds cachés, lesquels sont inhérents aux réseaux maillés! Ce paramètre établit la taille du plus petit paquet (en octets) pour lesquels le noeud envoie RTS. La valeur seuil du RTS doit être plus petite que la taille du paquet IP ainsi que la valeur du seuil de fragmentation (*fragmentation threshold* en anglais), autrement il serait désactivé. Dans notre exemple, cette valeur est de 256 bytes. Le TCP est très sensible aux collisions, il est donc important d'activer le RTS.

La fragmentation permet de diviser un paquet IP dans un éclat de plus petits fragments transmis. Bien que ceci ajoute de la surcharge, dans un environnement bruyant ceci réduit la pénalité due aux erreurs et permet aux paquets de traverser des rafales d'interférence. Les réseaux de maille sont très bruyants parce que les noeuds utilisent le même canal et donc les transmissions sont susceptibles de se faire mutuellement interférence. Ce paramètre établit la taille maximum avant qu'un paquet de données soit divisé et envoyé dans une rafale - une valeur égale à la taille maximum du paquet IP neutralise le mécanisme, le seuil de fragmentation doit donc être plus petit que la taille du paquet IP. Le réglage du seuil de fragmentation est recommandé.

Une fois qu'une adresse IP et un *masque de réseau* est assigné et l'interface sans fil fonctionne, le fichier de configuration d'olsrd doit être changé pour que celui-ci trouve et utilise les interfaces sur lesquelles il est censé travailler.

Pour Mac OS-X et Windows il y a des interfaces graphiques intéressants disponibles pour la configuration et la surveillance du démon. Malheureusement, ceci pousse certains usagers qui ne possèdent pas les connaissances de base à faire des choses stupides; comme de permettre les trous noirs. Sur BSD et Linux le fichier de configuration **`/etc/olsrd.conf`** doit être édité avec un éditeur de texte.

## Une configuration olsrd simple

Nous n'allons pas fournir ici un fichier complet de configuration. Voici quelques arrangements essentiels qui devraient être vérifiés.

```
UseHysteresis           no
TcRedundancy            2
MprCoverage             3
LinkQualityLevel        2
LinkQualityWinSize      20

LoadPlugin "olsrd_dyn_gw.so.0.3"
{
       PlParam     "Interval"   "60"
       PlParam     "Ping"       "151.1.1.1"
       PlParam     "Ping"       "194.25.2.129"
}

Interface "ath0" "wlan0" {
       Ip4Broadcast 255.255.255.255
}
```

Il y a beaucoup plus d'options disponibles dans **`olsrd.conf`**, mais ces options de base devraient être suffisantes pour commencer. Après avoir fait ces étapes, olsrd peut être démarré à l'aide d'une commande simple dans un terminal:

```
olsrd -d 2
```

Je recommande de l'exécuter avec l'option de débogage -d 2 sur votre poste de travail, spécialement lorsque c'est pour la première fois. Vous pouvez voir ce qu'olsrd fait et surveiller le fonctionnement des liens à vos voisins. Sur les systèmes embarqués, le niveau de debogage devrait être 0 (éteint), parce que le débogage crée beaucoup de charge sur l'unité centrale de traitement.

Le résultat devrait ressembler à ceci:

```
--- 19:27:45.51 ------------------------------------------- DIJKSTRA

192.168.120.1:1.00 (one-hop)
192.168.120.3:1.00 (one-hop)

--- 19:27:45.51 ------------------------------------------------ LINKS

IP address       hyst   LQ     lost   total  NLQ    ETX
192.168.120.1    0.000  1.000  0      20     1.000  1.00
192.168.120.3    0.000  1.000  0      20     1.000  1.00

--- 19:27:45.51 ---------------------------------------- NEIGHBORS

IP address       LQ     NLQ    SYM   MPR   MPRS  will
192.168.120.1    1.000  1.000  YES   NO    YES   3
192.168.120.3    1.000  1.000  YES   NO    YES   6
```

```
--- 19:27:45.51 ------------------------------------------ TOPOLOGY

Source IP addr   Dest IP addr     LQ     ILQ    ETX
192.168.120.1    192.168.120.17   1.000  1.000  1.00
192.168.120.3    192.168.120.17   1.000  1.000  1.00
```

## Utiliser OLSR sur Ethernet et sur des interfaces multiples

Il n'est pas nécessaire d'avoir une interface sans fil pour tester ou utiliser olsrd; bien que ce soit pour cela que olsrd a été conçu. Il peut aussi bien être employé sur n'importe quel interface réseau (NIC). Les interfaces WiFi ne doivent pas toujours fonctionner en mode ad hoc pour former une maille lorsque les noeuds du maillage ont plus d'une interface. C'est peut-être une bonne option de faire fonctionner des liens dédiés en mode infrastructure. Beaucoup de cartes et pilotes WiFi ont des problèmes en mode ad hoc, mais le mode infrastructure fonctionne très bien; parce que tout le monde s'attend au moins à ce que cette caractéristique fonctionne. Le mode ad hoc n'a pas eu beaucoup d'usagers jusqu'ici, en conséquence son application a été faite sans grand soin par plusieurs fabricants. À présent, avec la montée en popularité des réseaux maillé, cette situation s'améliore.

Plusieurs personnes emploient olsrd sur des interfaces câblés et sans fil car elles ne pensent pas à l'architecture de réseau. Elles connectent simplement des antennes à leurs cartes de WiFi, relient des câbles à leurs cartes Ethernet, exécutent olsrd sur tous les ordinateurs et toutes les interfaces et démarrent. Ceci est un abus d'un protocole qui a été conçu pour faire des réseaux sans fil sur des liens présentant des pertes; mais pourquoi pas?

Ils s'attendent à ce qu'olsrd soit un super protocole. Il n'est évidemment pas nécessaire d'envoyer des messages «hello» sur une interface câblée toutes les deux secondes; mais cela fonctionne. Ceci ne devrait pas être pris comme une recommandation; pourtant, il est simplement étonnant de voir ce que certaines personnes font avec un tel protocole. En fait, l'idée d'avoir un protocole qui fait tout pour les novices qui veulent avoir un LAN routé de petite à moyenne dimension est très attrayante.

## Plug-in

Un certain nombre de *plug-in* sont disponibles pour olsrd. Visitez le site web *olsr.org* pour une liste complète. Voici une marche à suivre pour la visualisation de la topologie réseau **`olsrd_dot_draw`**.

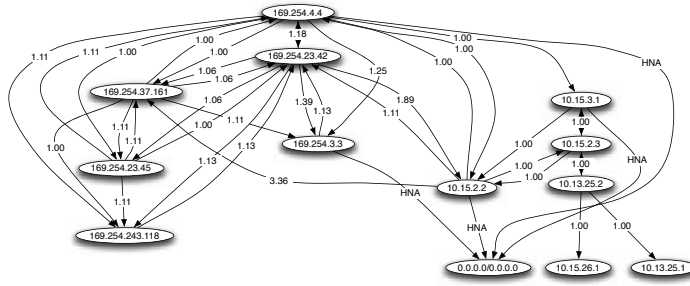


*Figure 3.8: Une topologie réseau OLSR automatiquement générée.*

Il est souvent une bonne chose pour la compréhension d'un réseau maillé d'avoir la capacité de montrer la topologie du réseau graphiquement. Olsrd_dot_draw produit la topologie dans un fichier au format dot sur le port TCP 2004. Les outils de graphviz peuvent alors être utilisés pour tracer les graphiques.

## Installer le plugin dot_draw

Compilez les plugins d'olsr séparément et installez-les. Pour charger les plugins ajoutez les lignes suivantes à **`/etc/olsrd.conf`**

```
LoadPlugin     "olsrd_dot_draw.so.0.3"
{
       PlParam "accept" "192.168.0.5"
       PlParam "port" "2004"
}
```

Le paramètre «*accept*» indique quel hôte est accepté pour visualiser l'Information Topologique (un seul actuellement) et c'est l'hôte local par défaut. Le paramètre «port» indique le port TCP.

Ensuite, redémarrez olsr et vérifiez si vous recevez un résultat sur le port TCP 2004

```
telnet localhost 2004
```

Après un moment un texte devrait apparaître.

Maintenant vous pouvez sauvegarder les descriptions graphiques résultantes et exécuter les outils **`dot`** ou **`neato`** du paquet de graphviz pour obtenir des images.

Bruno Randolf a écrit un petit programme Perl qui obtient sans interruption l'Information Topologique d'olsrd et la montre à l'aide de graphviz et des outils d'ImageMagick.

En premier lieu, installer les paquets suivants sur votre poste de travail:

- graphviz, *http://www.graphviz.org/*
- ImageMagick, *http://www.imagemagick.org/*

Téléchargez le programme à:
*http://meshcube.org/nylon/utils/olsr-topology-view.pl*

À présent vous pouvez démarrer le programme avec **`./olsr-topology-view.pl`** et visualiser la topologie mise à jour presque en temps réel.

## Dépannage

Aussi longtemps que les cartes WiFi peuvent se «voir» mutuellement avec leurs radios, les *pings* fonctionneront, même si olsrd ne fonctionne pas. Ceci fonctionne parce que les masques réseau sont suffisamment grand pour faire de chaque noeud un lien local. ADe cette façon, les problèmes de routage sont évités au premier saut. Ceci devrait être vérifié en premier si les choses ne semblent pas fonctionner comme prévu. La plupart des maux de tête que les gens ont avec le WiFi en mode ad hoc sont provoqués par le fait que ce mode a été implanté sans soin dans les pilotes et les cartes. S'il n'est pas possible de faire un *ping* aux noeuds directement lorsqu'ils sont à portée, ceci peut être un problème de carte ou de pilote ou encore une mauvaise configuration de réseau.

Si chaque machine peut faire *ping* à une autre, mais l'olsrd ne trouve pas les routes, alors les adresses IP, le masque de réseau et l'adresse de diffusion devraient être vérifiés.

Etes-vous derrière un Firewall? Assurez-vous qu'il ne bloque pas le port UDP 698.

Amusez-vous bien!

# *Évaluation de la capacité*

Les liens sans fil peuvent fournir aux usagers une ***capacité de traitement*** sensiblement plus grande que les connexions d'Internet traditionnelles, tels que VSAT, dialup, ou DSL. La capacité de traitement est également désignée sous le nom de ***capacité du canal***, ou simplement de ***largeur de bande*** (bien que ce terme ne garde aucune relation avec la largeur de bande radio). Il est important de comprendre que la vitesse mentionnée d'un dispositif sans fil (la ***vitesse de transfert de données*** ou « ***data rate*** » en anglais) se rap-

porte au taux auquel les radios peuvent échanger des symboles et non au rendement que l'usager va observer. Comme nous l'avons mentionné précédemment, un lien 802.11g peut employer 54Mbps de radio, mais le rendement réel sera de 22Mbps. Le reste est le taux (*overhead*) que les radios 802.11g ont besoin afin de coordonner leurs signaux.

La capacité de traitement est une mesure de bits par temps. 22Mbps signifie qu'en une seconde donnée, jusqu'à 22 mégabits peuvent être envoyés d'une extrémité du lien à l'autre. Si les usagers essayent d'envoyer plus de 22 mégabits à travers le lien, cela prendra plus qu'une seconde. Comme les données ne peuvent pas être envoyées immédiatement, elles sont placées dans une ***queue*** puis transmises aussi rapidement que possible. Cette queue augmente le temps nécessaire pour que les bits qui y ont été placé le plus récemment puissent traverser le lien. Le temps pris pour que les données traversent un lien s'appelle ***latence*** et une latence élevée est généralement désignée sous le nom de ***décalage*** (*lag* en anglais). Votre lien enverra par la suite tout le trafic placé dans la queue, mais vos usagers se plaindront probablement à mesure que le décalage augmente.

De quelle capacité de traitement vos usagers ont réellement besoin? Ceci va dépendre de combien d'usagers vous avez et comment ceux-ci utilisent le lien sans fil. Différentes applications d'Internet requièrent de différentes capacités de traitement.

| Application | Largeur de bande / Usager | Notes |
|---|---|---|
| Messagerie de texte / IM | < 1 Kbps | Comme le trafic est peu fréquent et asynchrone, IM tolérera un latence élevée. |
| Courriel | 1 à 100 Kbps | Comme avec IM, le courriel est asynchrone et intermittent, il tolérera la latence. Les grandes pièces jointes, virus et spam augmenteront de manière significative à l'utilisation de la largeur de bande. Notez que les services de courriel (tels que Yahoo ou Hotmail) devraient être considérés comme de la navigation Web et non comme du courriel. |

| Application | Largeur de bande / Usager | Notes |
|---|---|---|
| Navigation Web | 50 - 100+ Kbps | Les navigateurs Web utilisent le réseau seulement lorsque des données sont demandées. Comme la communication est asynchrone, une quantité considérable de délai peut être tolérée. Plus les navigateurs Web requièrent des données (grandes images, longs téléchargements, etc...), plus l'utilisation de la largeur de bande augmente. |
| *Streaming audio* | 96 - 160 Kbps | Chaque usager d'un service *streaming audio* utilisera une quantité constante d'une largeur de bande relativement importante aussi longtemps qu'il est en marche. Ce service peut tolérer de la latence passagère en utilisant une mémoire tampon côté client. Mais des périodes prolongées de délai causeront des «sauts» audio ou des échecs de session. |
| Voix sur IP (VoIP) | 24 - 100+ Kbps | Comme avec le streaming audio, VoIP nécessite une quantité constante de largeur de bande pour chaque usager pour la durée de l'appel. Mais avec VoIP, la largeur de bande employée est approximativement égale dans les deux directions. La latence sur une connexion de VoIP est immédiate et gênante pour les usagers. Un délai supérieur à quelques millisecondes est inacceptable pour VoIP. |
| *Streaming video* | 64 - 200+ Kbps | Comme avec le *streaming audio*, une faible quantité de latence intermittente peut être compensée en utilisant une importante mémoire tampon côté client. Le *Streaming video* demande une capacité de traitement élevée et une faible latence pour fonctionner correctement. |

| Application | Largeur de bande / Usager | Notes |
|---|---|---|
| Applications d'échange de fichiers Poste-à-poste (*Peer-to-Peer* ou *P2P* en anglais): BitTorrent, KaZaA, Gnutella, eDonkey, etc. | 0 - infinis Mbps | Même si les applications pair à pair vont tolérer n'importe quelle quantité de latence, ils tendent à épuiser toute la largeur de bande disponible en transmettant des données à autant de clients que possible et aussi rapidement que possible. L'utilisation de ces applications posera des problèmes de latence et de rendement pour tous les autres usagers du réseau à moins que vous mettiez en œuvre une mise en forme du trafic (*bandwith shaping*). |

Pour estimer la capacité de traitement nécessaire que vous aurez besoin pour votre réseau, multipliez le nombre prévu d'usagers par le type d'application qu'ils utiliseront le plus probablement. Par exemple, 50 usagers qui font principalement de la navigation Web consommeront probablement 2,5 à 5Mbps ou plus de largeur de bande aux heures maximales et toléreront de la latence. D'autre part, 50 usagers simultanés de VoIP auraient besoin de 5Mbps ou de plus de largeur de bande **dans les deux directions** avec aucune latence en absolu. Comme l'équipement sans fil 802.11g est » (c'est-à-dire, il transmet ou reçoit, mais ne fait jamais les deux en même temps), vous devriez doubler en conséquence la capacité de traitement exigée, pour un total de **10Mbps**. Vos liens sans fil doivent fournir cette capacité chaque seconde, sans quoi les conversations auront un délai.

Vos usagers n'utiliseront probablement pas la connexion précisément au même moment, il est courant de ***surévaluer*** la capacité de traitement disponible par un certain facteur (c'est-à-dire, permettre plus d'usagers que ce que la largeur de bande disponible maximum peut supporter). Un dépassement par un facteur de 2 à 5 est tout à fait courant. Très probablement, vous procéderez à une surévaluation lorsque vous établirez votre infrastructure de réseau. En surveillant soigneusement la capacité de traitement dans tout votre réseau, vous pourrez planifier le moment où il sera nécessaire d'améliorer diverses parties du réseau et combien de ressources additionnelles seront nécessaires.

Attendez vous à ce que peu importe la capacité de traitement que vous fournirez, vos usagers trouveront très probablement des applications qui l'utiliseront au complet. Comme nous le verrons à la fin de ce chapitre, il existe des techniques de répartition de bande passante pouvant aider à atténuer certains problèmes de latence. En utilisant une mise en forme de largeur de bande (*bandwith shaping* en anglais), une cache web et d'autres techniques,

vous pourrez réduire la latence et augmenter la capacité de traitement globale du réseau de manière significative.

Pour avoir une expérience de ce que représente un décalage dans une connexion, l'ICTP a construit un simulateur de largeur de bande. Il téléchargera simultanément une page Web à toute vitesse et à une autre à un taux réduit que vous choisirez. Cette démonstration vous offre une compréhension immédiate de la façon dont une faible bande passante et une latence élevée réduisent l'utilité d'Internet en tant qu'outil de communications. Ce simulateur est disponible à *http://wireless.ictp.trieste.it/simulator/*.

# Planification des liens

Un système de communication de base se compose de deux radios, chacune avec son antenne associée, les deux séparées par la trajectoire à couvrir. Afin d'avoir une communication entre les deux, les radios exigent une puissance minimum de signal provenant de l'antenne. Le processus pour déterminer si un lien est viable se nomme calcul du ***potentiel de puissance***. Le fait que les signaux puissent passer entre les radios dépend de la qualité de l'équipement employé et de l'***affaiblissement du signal dû à la distance que l'on appelle***: ***perte de trajet*** (*path loss* en anglais) dû à la distance.

## Calculer le potentiel de puissance

La puissance disponible dans un système 802.11 peut être caractérisée par les facteurs suivants:

- **Puissance de transmission**. Elle est exprimée en milliwatts ou en dBm. La puissance de transmission s'étend de 30mW à 200mW ou davantage. La puissance TX dépend souvent du taux de transmission. La puissance TX d'un dispositif donné devrait être indiquée dans la documentation fournie par le fabricant, mais peut parfois être difficile à trouver. Les bases de données en ligne telles que celle fournie par SeattleWireless (*http://www.seattlewireless.net/HardwareComparison*) peuvent aider.
- **Gain d'Antenne**. Les antennes sont des dispositifs passifs qui créent un effet d'amplification en vertu de leur forme physique. Les antennes ont les mêmes caractéristiques en réception et en transmission. Ainsi une antenne de 12 dBi est simplement une antenne de 12 dBi, sans spécifier si elle est en mode transmission ou réception. Les antennes paraboliques ont un gain de 19-24 dBm, les antennes omnidirectionnelles, dBi 5-12 et les antennes sectorielles ont un gain approximatif de 12-15 dBi.
- **Niveau minimum de signal reçu**, ou simplement la sensibilité du récepteur. Le RSL minimum est toujours exprimé en dBm négatif (- dBm) et est la plus faible puissance de signal que la radio peut distinguer. Le RSL

minimum dépend du taux de transmission et en règle générale, le taux le plus bas (1 Mbps) a la plus grande sensibilité. Le minimum sera habituellement dans la gamme de -75 à -95 dBm. Comme la puissance TX, les caractéristiques de RSL devraient être fournies par le fabricant de l'équipement.

- **Pertes dans les câbles**. Une partie de l'énergie du signal est perdue dans les câbles, les connecteurs et d'autres dispositifs, allant des radios aux antennes. La perte dépend du type de câble utilisé et de sa longueur. La perte de signal pour les câbles coaxiaux courts comprenant des connecteurs est assez faible, dans la gamme de 2 ou 3 dB. Il est préférable d'avoir des câbles aussi courts que possible.

En calculant la perte de trajet, plusieurs effets doivent être considérés. On doit tenir compte de la ***perte en espace libre***, ***de*** l'***atténuation et la diffusion***. La puissance du signal est diminuée par la propagation géométrique des ondes, généralement connue sous le nom de perte en espace libre. En ignorant tout le reste, plus les deux radios sont éloignées, plus petit est le signal reçu, dû à la perte en espace libre. Ceci est indépendant de l'environnement et dépend uniquement de la distance. Cette perte se produit parce que l'énergie rayonnée du signal en fonction de la distance de l'émetteur.

En utilisant des décibels pour exprimer la perte et 2,45 GHz comme fréquence du signal, l'équation pour la perte en espace libre est:

```
Lfsl = 40 + 20*log(r)
```

Où Lfsl ,la perte de signal, est exprimée en dB et r est la distance entre l'émetteur et le récepteur en mètres.

La deuxième cause de perte lors du parcours est l'atténuation. Ceci a lieu lorsqu'une partie de la puissance du signal est absorbée quand l'onde traverse des objets solides tels que des arbres, des murs, des fenêtres et des planchers de bâtiments. L'atténuation peut varier considérablement dépendamment de la structure de l'objet que le signal traverse et elle est très difficile à mesurer. La manière la plus commode d'exprimer sa contribution à la perte totale est en ajoutant une perte supplémentaire à l'espace libre. Par exemple, l'expérience prouve que les arbres ajoutent une perte de 10 à 20 dB par arbre dans le chemin direct, alors que les murs contribuent à une perte de 10 à 15 dB dépendant de la construction.

Le long du trajet du lien, l'énergie RF quitte l'antenne de transmission et se disperse. Une partie de l'énergie RF atteint l'antenne de réception directement, alors qu'une partie rebondit sur le sol. Une partie de l'énergie RF qui rebondit atteint l'antenne de réception. Puisque le signal reflété a un plus long trajet à franchir, il arrive plus tard à l'antenne de réception que le signal direct. Cet effet s'appelle ***trajets multiples*** (***multipath***), effacement ou dis-

persion du signal. Dans certains cas les signaux reflétés s'ajoutent et ne posent aucun problème. Quand ils sont en relation de phase, le signal reçu est presque nul. Cependant, dans certains cas le signal à l'antenne de réception peut être annulé par les signaux reflétés. Ceci est connu sous le nom d'***annulation*** («***nulling***» en anglais). Il existe une technique simple qui employée pour traiter les trajets multiples appelée ***diversification d'antenne***. Elle consiste à ajouter une deuxième antenne à la radio. Le phénomène des trajets multiples est en fait très localisé. Si deux signaux s'annulent à une position, ils n'en feront pas autant à la deuxième. S'il y a deux antennes, au moins l'une d'entre elles devrait pouvoir recevoir un signal utilisable, même si l'autre reçoit un signal « déformé ». Dans les périphériques commerciaux, on emploie la diversité de commutation d'antenne: il y a de multiples antennes sur des entrées multiples avec un récepteur simple. Le signal est ainsi reçu uniquement par une antenne à la fois. En transmettant, la radio utilise l'antenne qui a été utilisée la dernière fois pour la réception. La distorsion donnée par les trajets multiples dégrade la capacité du récepteur de récupérer le signal de façon similaire à la perte de signal. Une manière simple d'appliquer les effets de la diffraction dans le calcul de la perte de trajet est de changer l'exposant du facteur de distance dans la formule de perte en espace libre. L'exposant a tendance à augmenter avec la portée dans un environnement avec beaucoup de diffusion. Un exposant de 3 peut être employé dans un environnement extérieur avec des arbres, alors qu'un exposant de 4 peut être employé dans un environnement intérieur.

Lorsque nous combinons perte en espace libre, l'atténuation et la diffusion, la perte de trajet est:

```
L(dB) = 40 + 10*n*log(r) + L(permise)
```

Où n est l'exposant mentionné.

Pour une évaluation approximative de la viabilité du lien, on peut évaluer uniquement la perte liée à l'espace libre. Cependant, l'environnement peut causer davantage de perte de signal et devrait être considéré pour une évaluation exacte du lien. L'environnement est en fait un facteur très important et ne devrait jamais être négligé.

Pour évaluer si un lien est viable, on doit connaître les caractéristiques de l'équipement employé et évaluer la perte de trajet. Notez qu'en effectuant ce calcul, vous devriez ajouter la puissance TX uniquement d'un côté du lien. Si vous employez différentes radios de chaque côté du lien, vous devriez calculer la perte de trajet deux fois, une fois pour chaque direction (en employant la puissance TX appropriée pour chaque calcul). Additionner tous les gains et soustraire toutes les pertes donne:

```
  TX puissance de Radio 1
+ Gain de l'antenne de Radio 1
- Perte dans les câbles de Radio 1
+ Gain de l'antenne de Radio 2
- Perte dans les câbles de Radio 2
  ————————————————————————————————
           = Gain total
```

Soustraire la perte de trajet du Gain Total:

```
              Gain   total
            - Perte de trajet
              ———————————————
= Niveau du signal à un des côtés du lien
```

Si le résultat du niveau du signal est plus grand que le niveau minimum de signal reçu, alors le lien est viable! Le signal reçu est assez puissant pour que les radios puissent l'employer. Rappelez-vous que le RSL minimum est toujours exprimé en dBm négatif, ainsi -56dBm est plus grand que 70dBm. Sur un trajet donné, la variation de la perte de trajet sur une certaine période de temps peut être grande, ainsi une certaine marge (différence entre le niveau du signal et le niveau minimum de signal reçu) devrait être considérée. Cette marge est la quantité de signal au-dessus de la sensibilité de la radio qui devrait être reçue afin d'assurer un lien radio stable et de haute qualité pendant de mauvaises conditions atmosphériques. Une marge d'erreur de 10-15 dB fait très bien l'affaire. Pour donner un certain espace pour l'atténuation et les trajets multiples dans le signal de radio reçu, une marge de 20dB devrait être une valeur assez sûre.

Une fois que vous avez calculé le potentiel de puissance dans une direction, répétez le calcul pour l'autre direction. Substituez la puissance de transmission à celle de la deuxième radio et comparez le résultat au niveau minimum de signal reçu de la première radio.

## Exemple de calcul du potentiel de puissance

Comme exemple, nous voulons estimer la viabilité d'un lien de 5km, avec un point d'accès (AP) et un client. Le point d'accès est relié à une antenne omnidirectionnelle de 10dBi de gain, alors que le client est relié à une antenne sectorielle de 14dBi de gain. La puissance de transmission de l'AP est de 100mW (ou 20dBm) et sa sensibilité est de -89dBm. La puissance de transmission du client est de 30mW (ou 15dBm) et sa sensibilité est de -82dBm. Les câbles sont courts, avec une perte de 2dB de chaque côté.

En additionnant tous les gains, en soustrayant toutes les pertes de l'AP au client, nous obtenons:

```
  20 dBm (TX puissance Radio 1)
+ 10 dBi (Gain d'antenne Radio 1)
-  2 dB  (Perte des câbles Radio 1)
+ 14 dBi (Gain d'antenne Radio 2)
-  2 dB  (Perte des câbles Radio 2)
_________
  40 dB = Gain total
```

La perte de trajet pour un lien de 5km en considérant uniquement la perte en espace libre est:

```
Perte de trajet = 40 + 20log(5000) = 113 dB
```

Soustraire la perte de trajet du gain total

```
40 dB - 113 dB = -73 dB
```

Puisque -73dB est plus grand que la sensibilité du récepteur du client (-82dBm), le niveau du signal est juste assez important pour que le client puisse entendre le point d'accès. Nous n'avons qu'une marge de 9dB (82dB – 73dB): le lien fonctionnera bien que dans de bonnes conditions climatiques.

Ensuite, calculons le lien du client au point d'accès:

```
  15 dBm (TX tuissance Radio 2)
+ 14 dBi (Gain d'antenna Radio 2)
-  2 dB  (Perte de câbles Radio 2)
+ 10 dBi (Gain d'antenne Radio 1)
-  2 dB  (Perte de câbles Radio 1)
_________
  35 dB = Gain Total
```

Évidemment, la perte de trajet est la même pour le voyage de retour. Ainsi, notre niveau de signal reçu au point d'accès est:

```
35 dB - 113 dB = -78 dB
```

Puisque la sensibilité de réception de l'AP est de -89dBm, ceci nous laisse une marge de de 11dB (89dB - 78dB). De façon générale, ce lien fonctionnera mais pourrait probablement utiliser un peu plus de gain. En employant une antenne parabolique de 24dBi du côté du client plutôt qu'une antenne sectorielle de 14dBi, vous obtiendrez un gain additionnel de 10dBi sur les deux côtés du lien (souvenez-vous que le gain d'antenne est réciproque). Une option plus dispendieuse serait d'employer des radios de puissance plus élevée sur les deux extrémités du lien, mais le fait d'ajouter un amplificateur ou une carte avec plus de puissance à une seule extrémité n'aide pas à améliorer la qualité globale du lien.

Des outils en ligne peuvent être utilisés pour calculer le potentiel de puissance. Par exemple, le *Green Bay Professional Packet Radio's Wireless Network Link Analysis* (*http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*) est un excellent outil. La Super Edition génère un fichier pdf contenant la zone de Fresnel et le trajet des ondes radio. Les scripts de calcul peuvent même être téléchargés du site Web et être installés localement. Nous discuterons en détail d'un excellent outil en ligne dans la prochaine section **Logiciel de planification de lien**.

Le site Web de Terabeam a aussi d'excellents calculateurs disponibles en ligne: *http://www.terabeam.com/support/calculations/index.php*

## Tables pour calculer le potentiel de puissance

Pour calculer le potentiel de puissance, faites simplement une estimation de la distance de votre lien puis remplissez les tables suivantes:

### Perte d'espace libre à 2,4GHz

| Distance (m) | 100 | 500 | 1,000 | 3,000 | 5,000 | 10,000 |
|---|---|---|---|---|---|---|
| Perte (dB) | 80 | 94 | 100 | 110 | 113 | 120 |

### Gain d'antenne:

| Antenne Radio 1 (dBi) | + Antenne Radio 2 (dBi) | = Gain Total |
|---|---|---|
| | | |

### Pertes:

| Radio 1 + Perte de câbles (dB) | Radio 2 + Perte de câbles (dB) | Perte en espace libre (dB) | = Perte totale (dB) |
|---|---|---|---|
| | | | |

### potentiel de puissance pour la Radio 1 ➜ Radio 2:

| Puissance TX de Radio 1 | + Gain d'antenne | - Perte totale | = Signal | > Sensibilité de Radio 2 |
|---|---|---|---|---|
| | | | | |

### potentiel de puissance pour la Radio 2 ➜ Radio 1:

| Puissance TX de Radio 2 | + Gain d'antenne | - Perte totale | = Signal | > Sensibilité de Radio 1 |
|---|---|---|---|---|
| | | | | |

Si le signal reçu est plus grand que la force minimum de signal reçu dans les deux directions du lien, alors le lien est viable.

## Logiciel de planification de lien

Même s'il est assez simple de calculer à la main le potentiel de puissance d'un lien, il y a un certain nombre d'outils disponibles qui vous aideront à automatiser le processus. En plus de calculer la perte en espace libre, ces outils tiendront également compte de beaucoup d'autres facteurs pertinents (comme l'absorption des arbres, les effets du terrain, le climat et même l'estimation de la perte liée au trajet dans des secteurs urbains). Dans cette section, nous discuterons deux outils gratuits qui sont utiles pour la planification des liens sans fil: *Green Bay Professional Packet Radio* qui a des utilités en ligne de conception de réseau et RadioMobile.

### Conception interactive CGI

Le groupe *Green Bay Professional Packet Radio* (GBPRR) a créé une variété d'outils très utiles pour la planification de lien qui sont disponible gratuitement en ligne. Vous pouvez télécharger ces outils en ligne à *http://www.qsl.net/n9zia/wireless/page09.html*. Comme ces outils sont disponibles en ligne, ils fonctionneront avec n'importe quel navigateur Web ayant accès à accès à Internet.

Nous nous pencherons en profondeur sur le premier outil: **Analyse de Lien de réseau sans fil** (en anglais, *Wireless Network Link Analysis*). Vous le trouverez en ligne à: *http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*.

Pour commencer, entrez le canal qui sera utilisé sur le lien. Celui-ci peut être spécifié en mégahertz ou gigahertz. Si vous ne connaissez pas la fréquence,

consultez la table dans l'annexe B. Notez que le tableau présente la fréquence centrale du canal, alors que l'outil demande la fréquence transmise la plus élevée. La différence dans le résultat final est minimale, vous etes libre d'utiliser la fréquence centrale à la place. Pour trouver la fréquence transmise la plus élevée pour un canal, vous n'avez qu'à ajouter 11MHz à la fréquence centrale.

Ensuite, entrez les détails pour un côté du lien (type de ligne de transmission, le gain d'antenne et autres). Essayez de compléter autant de champs que vous connaissez ou que vous pouvez estimer. Vous pouvez également écrire la taille et l'altitude de l'antenne pour cet emplacement. Ces données seront employées pour calculer l'angle d'inclinaison de l'antenne. Pour calculer le dégagement de la zone Fresnel, vous devrez utiliser le calculateur GBPRR de la zone Fresnel.

La section suivante est très similaire, elle contient l'information sur l'autre côté du lien. Entrez toute l'information disponible dans les champs appropriés.

Finalement, la dernière section décrit le climat, le terrain et la distance du lien. Saisissez autant de données que vous connaissez ou que vous pouvez estimer. La distance du lien peut être calculée en indiquant la latitude et la longitude des deux emplacements, ou être écrite à la main.

Maintenant, cliquez sur le bouton Soumettre (*Submit*) pour un rapport détaillé du lien proposé. Ceci inclut toutes les données saisies, ainsi que la perte liée au trajet, les taux d'erreur et le temps de bon fonctionnement du lien. Quoique ces nombres soient tout à fait théoriques, ils vous donneront une idée approximative de la viabilité du lien. En ajustant les valeurs sur le formulaire, vous pouvez voir comment le fait de changer divers paramètres affectera la connexion.

En plus de l'outil de base d'analyse de lien, GBPRR offre une « super édition » qui produit un rapport PDF, ainsi qu'un nombre d'outils très utiles (y compris le calculateur de la zone Fresnel, le calculateur de distance et de direction, le calculateur de conversion de décibels, pour n'en nommer que quelques-uns). Le code source de la plupart de ces outils est également offert.

## RadioMobile

RadioMobile est un outil pour la conception et la simulation de systèmes sans fil. Il prédit la performance d'un lien radio en se basant sur l'équipement et une carte géographique numérique. C'est un logiciel du domaine public qui fonctionne sur Windows ou Linux avec l'émulateur Wine.

RadioMobile utilise un ***modèle d'élévation numérique de terrain*** pour le calcul de la couverture en indiquant la force reçue du signal à divers points le long du trajet. Il établit automatiquement un profil entre deux points dans la carte numérique montrant le secteur de couverture et la première zone Fresnel. Pendant la simulation, il vérifie la ligne de la vue et calcule la perte liée au trajet, y compris les pertes dues aux obstacles. Il est possible de créer des réseaux de différentes topologies: maître/esclave, point-à-point et point-à-multipoint.

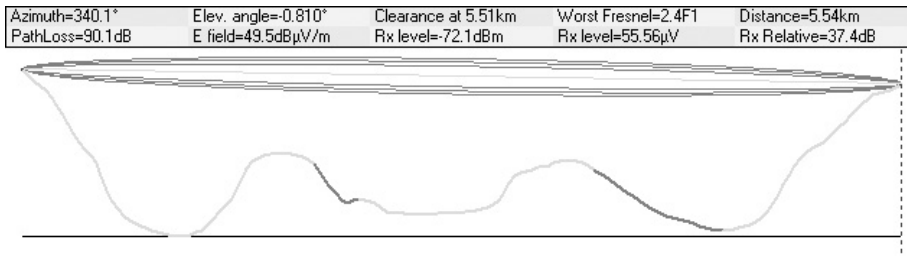


*Figure 3.9: Viabilité du lien, incluant la zone Fresnel et une estimation de la ligne de vue, en utilisant RadioMobile.*

Le logiciel calcule la région de couverture de la station de base dans un système point-à-multipoint. Cela fonctionne pour des systèmes ayant des fréquences de 20 kilohertz à 200 gigahertz. ***Les Cartes numériques d'élévation*** (ou ***digital elevation maps -DEM***, en anglais) sont disponibles gratuitement à partir de plusieurs sources et pour la majeure partie du globe. Les DEMs ne montrent pas les littoraux ou autres limites aisément identifiables, mais ils peuvent facilement être combinés en couches avec d'autres genres de données (telles que des photos aériennes ou des diagrammes topographiques) pour obtenir une représentation plus utile et plus facilement reconnaissable. Vous pouvez digitaliser vos propres cartes et les combiner avec les DEMs. Les cartes numériques d'élévation peuvent être fusionnées avec des cartes scannées, des photos satellites et des services de carte Internet (tels que Mapquest) pour produire des prédictions de couverture précises.

Vous pouvez télécharger *RadioMobile* à cette adresse:
*http://www.cplus.org/rmw/download.html*

La page principale de *RadioMobile* comporte plusieurs exemples et instructions. Elle est disponible à l'adresse suivante:
*http://www.cplus.org/rmw/english1.html*

## RadioMobile sous Linux

RadioMobile fonctionnera également en utilisant Wine sous Ubuntu Linux. Même si l'application fonctionne, quelques étiquettes de bouton peuvent être mal placées sur le cadre du bouton et rendra la lecture plus difficile.

Nous avons pu faire fonctionner RadioMobile sous Linux avec l'environnement suivant:

- IBM Thinkpad x31
- Ubuntu Breezy (v5.10), *http://www.ubuntu.com/*
- Version Wine 20050725, d'Ubuntu Universe

Il y a des instructions détaillées sur l'installation de RadioMobile sous Windows à *http://www.cplus.org/rmw/download.html*. Vous devriez suivre toutes les étapes excepté l'étape 1 (puisqu'il est difficile d'extraire un DLL à partir du fichier **`VBRUN60SP6.EXE`** sous Linux). Vous allez devoir soit copier le fichier **`MSVBVM60.DLL`** d'une machine Windows qui a déjà le Visual Basic 6 run-time installé ou simplement chercher sur Google le fichier **`MSVBVM60.DLL`** puis le télécharger.

Continuez maintenant à l'étape 2 de l'URL précédent, en veillant à ouvrir les dossiers téléchargés dans le même annuaire dans lequel vous avez placé le dossier DLL téléchargé. Notez que vous ne devez pas prendre en considération les étapes suivant l'étape 4; ce sont des étapes supplémentaires uniquement requises pour les usagers de Windows.

Finalement, vous pouvez démarrez Wine dans un terminal avec la commande suivante:

```
# wine RMWDLX.exe
```

Vous devriez voir fonctionner RadioMobile sur votre session XWindows.

## Éviter le bruit

Les bandes sans licence ISM et U-NII représentent une portion minuscule du spectre électromagnétique connu. Puisque cette région peut être utilisée sans avoir à payer des redevances, plusieurs dispositifs de consommateurs l'emploient pour un large éventail d'applications. Les téléphones sans fil, les envoyeurs vidéo analogues, le Bluetooth, les moniteurs de bébé et même les fours à micro-ondes concurrencent les réseaux informatiques sans fil pour l'usage de la bande 2,4GHz qui est très limitée. Ces signaux, comme d'autres réseaux sans fil locaux, peuvent poser des problèmes significatifs pour des liens radio de longue portée. Voici quelques étapes que vous pouvez suivre afin de réduire la réception des signaux non désirés.

- **Augmentez le gain d'antenne des deux côtés d'un lien point à point**. Les antennes ne font pas qu'ajouter du gain à un lien, mais leur directivité accrue tend à rejeter le bruit des régions autour du lien. Deux paraboliques de gain élevé qui sont pointées l'une vers l'autre vont rejeter le bruit prove-

nant de directions qui sont en dehors de la trajectoire du lien. L'utilisation d'antennes omnidirectionnelles recevra le bruit de toutes les directions.

- **N'utilisez pas un amplificateur**. Comme nous le verrons au chapitre 4, les amplificateurs peuvent empirer les problèmes d'interférence en amplifiant aléatoirement tous les signaux reçus, y compris ceux des sources d'interférence. Les amplificateurs posent également des problèmes d'interférence pour d'autres usagers de la bande qui se trouvent à proximité.
- **Employez des antennes sectorielles au lieu d'une omnidirectionnelle**. En employant plusieurs antennes sectorielles, vous pouvez réduire le bruit global reçu à un point de distribution. En organisant les canaux utilisés sur chaque antenne sectorielle, vous pouvez également augmenter la largeur de bande disponible pour vos clients.

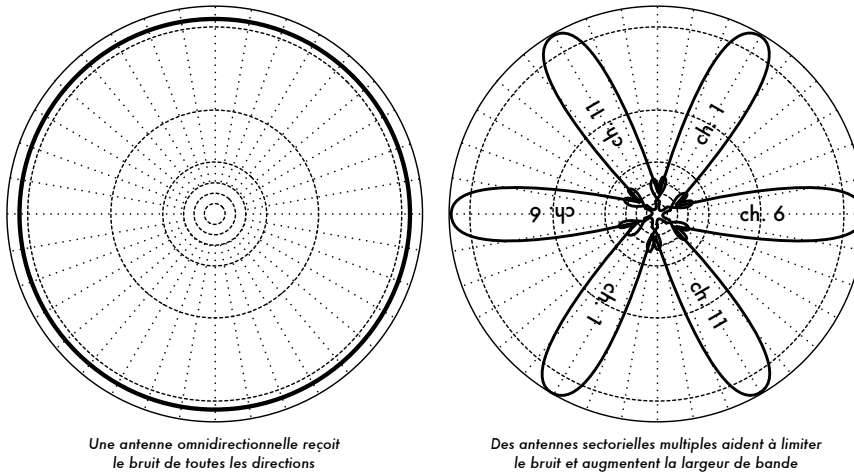


*Figure 3.10: Une seule antenne omnidirectionnelle vs multiples antennes sectorielles.*

- **Utilisez le meilleur canal disponible**. Rappelez-vous que les canaux 802.11b/g ont une largeur de 22Mhz, mais sont seulement séparés par 5MHz. Effectuez une enquête de terrain (comme détaillé au chapitre huit) et choisissez un canal qui se trouve aussi loin que possible des sources existantes d'interférence. Rappelez-vous que le paysage sans fil peut changer à tout moment lorsque des individus ajoutent des nouveaux dispositifs (téléphones sans fil, d'autres réseaux, etc...) Si votre lien a soudainement des problèmes pour envoyer des paquets, vous devrez effectuer une autre enquête et sélectionner un canal différent.
- **Utilisez des relais et des répéteurs au lieu d'un seul lien sur une longue distance**. Gardez vos liens point-à-point aussi courts que possible. Même s'il est possible de créer un lien de 12km qui passe à travers une ville, vous aurez probablement toutes sortes de problèmes d'interférence. Si vous pouvez couper ce lien en deux ou trois relais plus courts, le lien sera probablement plus stable. Évidemment ceci n'est pas possible sur

des liens ruraux à longue distance où les structures de puissance et de support ne sont pas disponibles, mais où les problèmes de bruit sont également peu probables.

- **Si possible, utilisez les bandes 5,8GHz**, **900MHz**, **ou tout autre bande sans licence**. Même si ceci n'est qu'une solution à court terme, actuellement la plupart de l'équipement installé emploie 2,4GHz. Utiliser 802.11a ou un dispositif step-up de 2,4GHz à 5,8GHz, vous permettra d'éviter cette congestion. Si vous pouvez les trouver, il existe certains anciens équipements 802.11 qui utilisent le spectre sans licence à 900MHz (malheureusement avec des débits binaires très inférieurs). D'autres technologies, telle que Ronja (*http://ronja.twibright.com/*) utilisent une technologie optique pour des liens de courte distance sans bruits.
- **Si rien de ceci ne fonctionne**, **utilisez un spectre autorisé**. Il y a des endroits où tout le spectre sans licence disponible a été employé. Dans ces cas, ce peut être une bonne idée de dépenser un peu d'argent additionnel pour de l'équipement de propriété industrielle qui emploie une bande moins congestionnée. Pour des liens de longue distance point à point qui requièrent une capacité de traitement très élevée et un temps maximum de disponibilité, cela s'avère être certainement une bonne option. Naturellement, ces dispositifs ont un prix beaucoup plus élevé comparé à l'équipement sans licence.

Pour identifier des sources de bruit, vous avez besoin d'outils qui vous montrent ce qui se produit dans le ciel à 2,4GHz. Nous verrons quelques exemples de ces outils au chapitre 6.

## Répéteurs

La composante la plus critique pour construire un liens de réseau de longue distance est la ***ligne de vue*** (***Line of Sight - LOS***). Les systèmes terrestres micro-onde ne peuvent tout simplement pas tolérer de grandes collines, arbres, ou autres obstacles sur le trajet d'un lien de longue distance. Vous devez avoir une idée claire de la configuration du terrain entre deux points avant que vous ne puissiez déterminer si un lien est viable.

Mais même s'il y a une montagne entre deux points, rappelez-vous que des obstacles peuvent parfois être transformés en atouts. Les montagnes peuvent bloquer votre signal, mais en supposant qu'il est possible d'y apporter de la puissance, elles pourront faire de très bons ***répéteurs***.

Les répéteurs sont des noeuds qui sont configurés pour rediffuser le trafic qui n'est pas destiné au noeud lui-même. Dans un réseau de maille, chaque noeud est un répéteur. Dans un réseau traditionnel d'infrastructure, certains noeuds doivent être configurés pour passer le trafic à d'autres noeuds.

Un répéteur peut utiliser un ou plusieurs dispositifs sans fil. En utilisant une seule radio (que l'on appele « ***répéteur one-arm*** »), l'efficacité globale est légèrement moins que la moitié de la largeur de bande disponible, puisque la radio peut envoyer ou recevoir des données, mais jamais faire les deux en même temps. Ces dispositifs sont meilleur marché, plus simples et ont une alimentation électrique inférieure. Un répéteur avec deux (ou plus) cartes radio peut actionner toutes les radios à pleine capacité, aussi longtemps que ceux-ci sont configurés pour utiliser des canaux qui ne se superposent pas. Naturellement, les répéteurs peuvent également assurer une connexion Ethernet pour fournir une connectivité locale.

Des répéteurs peuvent être achetés comme un ensemble complet, ou être facilement assemblés en reliant deux (ou plus) noeuds sans fil avec un câble Ethernet. Lorsque vous pensez utiliser un répéteur construit avec la technologie 802.11, rappelez-vous que les noeuds doivent être configurés pour les modes maître, administré, ou ad hoc. Généralement, les deux radios dans un répéteur sont configurées pour le mode maître, pour permettre aux multiples clients de se relier à l'un ou l'autre côté du répéteur. Mais selon votre disposition de réseau, un ou plusieurs dispositifs peuvent devoir employer un mode ad hoc ou même client.

Généralement, les répéteurs sont utilisés pour éviter des obstacles dans le trajet d'un lien de longue distance. Par exemple, il peut y avoir des bâtiments dans votre chemin, mais dans ceux-ci il y a des personnes. Il est souvent possible de se mettre d'accord avec les propriétaires des bâtiments pour fournir de la largeur de bande en échange du droit d'utiliser les toits et l'électricité. Si le propriétaire du bâtiment n'est pas intéressé, les locataires des étages supérieurs peuvent être persuadés d'installer l'équipement dans une fenêtre.

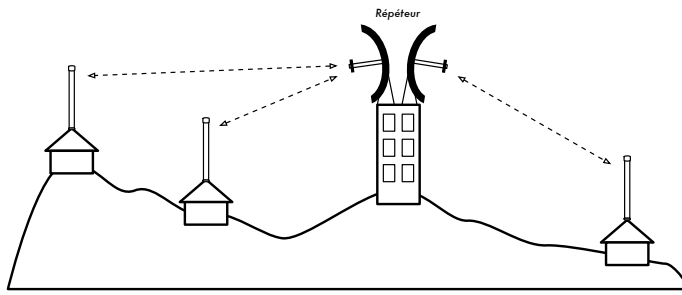


*Figure 3.11: Le répéteur transmet des paquets dans l'air entre des nœuds qui n'ont pas de ligne de vue directe.*

Si vous ne pouvez pas passer par-dessus ou à travers un obstacle, vous pouvez souvent le contourner. Plutôt que d'utiliser un lien direct, essayez une approche de sauts multiples pour éviter l'obstacle.

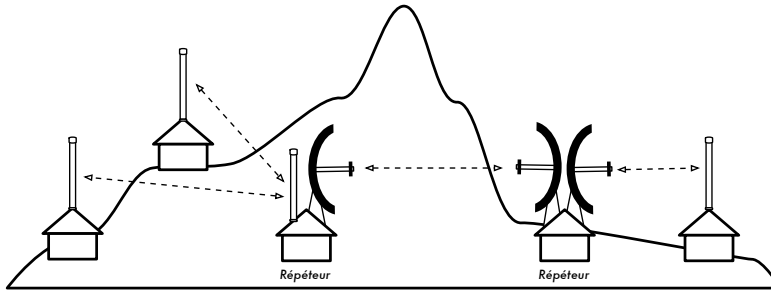


*Figure 3.12: Il n'y avait pas d'énergie disponible au dessus de la colline, mais ceci a été résout en employant de multiples de répéteurs situés autour de la base.*

Finalement, vous pouvez devoir aller vers l'arrière afin de pouvoir avancer. S'il y a un emplacement élevé de disponible dans une direction différente et que cet emplacement peut voir au delà de l'obstacle, un lien stable peut être fait par l'intermédiaire d'un itinéraire indirect.

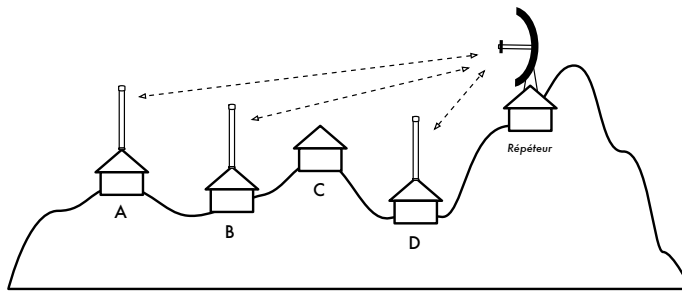


*Figure 3.13: L'emplacement D ne peut pas voir les emplacements A ou B, car l'emplacement C est dans le chemin et n'est pas intéressé à héberger un nœud. En installant un répéteur plus haut, les nœuds A, B et D peuvent communiquer. Notez qu'en fait le trafic du nœud D voyage plus loin que celui du reste du réseau avant que le répéteur puisse envoyer ces données.*

Les répéteurs dans les réseaux me font penser au principe des « six degrés de séparation ». Cette idée stipule que quiconque soit la personne que vous recherchez, vous pourrez la trouver simplement en contactant cinq intermédiaires. Les répéteurs dans les endroits élevés « voient » beaucoup d'intermédiaires, et aussi longtemps que votre noeud est dans la portée du répéteur, vous pouvez communiquer avec n'importe quel noeud que le répéteur peut atteindre.

# Optimisation du trafic

La largeur de bande est mesurée comme un débit binaire pendant un intervalle de temps. Ceci signifie qu'avec le temps, la largeur de bande disponible sur n'importe quel lien approche l'infini. Malheureusement, pour une période de temps finie, la largeur de bande fournie par une connexion de réseau quelconque n'est pas infinie. Vous pouvez toujours télécharger autant de

trafic comme vous voudrez; vous n'avez qu'à attendre suffisamment longtemps. Naturellement, les usagers humains ne sont pas aussi patients que les ordinateurs et ne sont pas disposés à attendre une quantité d'heure infinie pour que leur information traverse le réseau. C'est pour cette raison que la largeur de bande doit être contrôlée comme n'importe quelle autre ressource limitée.

Vous améliorerez de manière significative le temps de réponse et maximiserez la capacité de traitement disponible en éliminant le trafic non désiré et superflu de votre réseau. Cette section décrit beaucoup de techniques courantes pour vous assurer que votre réseau comporte uniquement le trafic qui doit le traverser.

## Cache Web

Un serveur Web proxy est un serveur sur le réseau local qui garde des copies des pages ou parties de pages Web récemment recherchées ou souvent utilisées. Quand la prochaine personne recherche ces pages, elles sont servies à partir du serveur proxy local au lieu d'Internet. Ceci a comme conséquence un accès Web sensiblement plus rapide dans la plupart des cas, tout en réduisant l'utilisation globale de largeur de bande d'Internet. Quand un serveur proxy est mis en application, l'administrateur devrait savoir que certaines pages ne peuvent pas être stockées; par exemple, des pages qui sont le résultat de scripts du côté du serveur ou tout autre contenu produit dynamiquement.

Le chargement apparent des pages Web est également affecté. Avec un lien Internet lent, une page normale commence à charger lentement, d'abord en montrant un peu de texte puis en dévoilant les graphiques un par un. Dans un réseau avec un serveur proxy, il peut y avoir un délai lorsque rien ne semble se produire, puis la page chargera presque immédiatement. Ceci se produit parce que l'information est envoyée à l'ordinateur tellement rapidement que pour reproduire la page, une quantité perceptible de temps est nécessaire. Le temps global requis pour charger la page entière peut ne prendre que dix secondes (tandis que sans serveur Proxy, il peut être nécessaire d'attendre 30 secondes afin de charger la page graduellement). Mais à moins que ceci ne soit expliqué à certains usagers impatients, ceux-ci peuvent dire que le serveur Proxy a rendu les choses encore plus lentes. C'est habituellement la tâche de l'administrateur du réseau de traiter les problèmes de perception de ses usagers.

### Produits de serveur Proxy

Il y a un certain nombre de serveurs Web Proxy disponibles. Ce sont les progiciels le plus généralement utilisés:

- «**Squid**». Le logiciel libre Squid est le standard de facto dans les universités. Il est libre, fiable, facile d'utilisation et peut être amélioré (par exemple, en ajoutant des filtres de contenu et un blocage de publicité). Squid produit des rapports graphiques qui peuvent être analysées en utilisant un logiciel tel qu'Awstats, ou Webalizer, tous deux étant de source ouverte et produisant de bons rapports graphiques. Dans la plupart des cas, il est plus facile de l'installer en tant qu'élément de la distribution qu'en le téléchargeant de *http://www.slivre-cache.org/* (la plupart des distributions de Linux telles que Debian, ainsi que d'autres versions d'Unix telles que NetBSD et FreeBSD viennent avec Squid). Un bon guide de configuration Squid peut être trouvé à *http://squid-docs.sourceforge.net/latest/book-full.html*.
- **Serveur Proxy de Microsoft Proxy 2.0**. Il n'est pas disponible pour de nouvelles installations parce qu'il a été remplacé par le serveur de Microsoft ISA et n'est plus soutenu. Il est néanmoins employé par quelques établissements, bien qu'il ne devrait probablement pas être considéré pour de nouvelles installations.
- **Serveur ISA de Microsoft**. Le serveur d'ISA est un très bon logiciel de serveur Proxy, bien que trop dispendieux pour ce qu'il fait. Cependant, avec des remises pour institutions universitaires il peut être accessible à quelques établissements. Il produit ses propres rapports graphiques, mais ses fichiers logs peuvent également être analysés avec des logiciels analyseurs populaires tel que Sawmill (*http://www.sawmill.net/*). Les administrateurs d'un emplacement avec MS ISA devraient passer suffisamment de temps afin d'obtenir une configuration correcte; autrement le serveur MS ISA lui-même peut devenir un usager de largeur de bande considérable. Par exemple, une installation par défaut peut facilement consommer plus de largeur de bande que ce que le site a employé auparavant, parce que les pages courantes avec des dates d'échéance courtes (tels que des sites de nouvelles) sont continuellement mises à jour. Par conséquent il est important que le prétraitement/chargement (*pre-fetching*) soit correctement configuré, pour qu'il puisse avoir lieu principalement durant la nuit. Le serveur ISA peut également être associé à des produits de filtrage tels que WebSense. Pour plus d'information, visitez le lien suivant: *http://www.microsoft.com/isaserver/ et http://www.isaserver.org/*.

## Empêcher les usagers de contourner le serveur Proxy

Bien que la mise en échec de la censure d'Internet et de la politique restrictive d'accès de l'information puisse être un effort politique louable, les applications Proxy et les pares feu sont des outils nécessaires dans les milieux où la largeur de bande est extrêmement limitée. Sans eux, la stabilité et la rentabilité du réseau sont menacées par les usagers légitimes eux-mêmes. Des techniques pour éviter un serveur proxy peuvent être trouvées à *http://www.antiproxy.com/*. Ce site est utile pour que les administrateurs puissent voir comment leur réseau peut faire face à ces techniques.

Pour renforcer l'usager du serveur cache, vous pourriez simplement considérer d'instaurer une politique d'accès de réseau et de faire confiance à vos usagers. Dans la disposition ci-dessous, l'administrateur doit espérer que ses utilisateurs n'évitront pas le serveur Proxy.

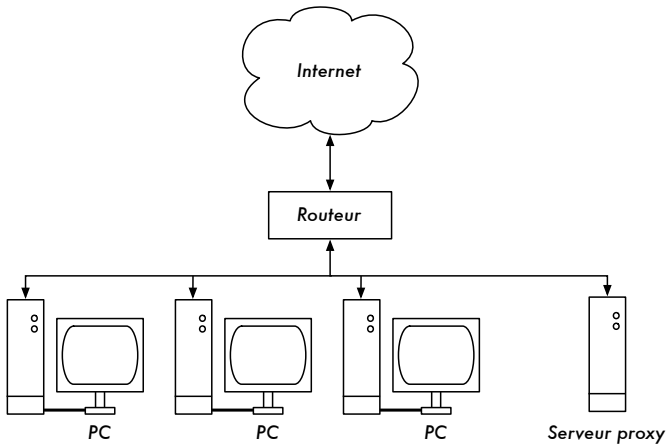


*Figure 3.14: Ce réseau repose sur la confiance que ses usagers configureront correctement leurs ordinateurs pour utiliser le serveur mandataire.*

Dans ce cas-ci l'administrateur emploie généralement une des techniques suivantes:

- **Ne pas donner l'adresse de la passerelle par défaut à travers DCHP**. Ceci peut fonctionner pendant un certain temps, mais les usagers qui veulent contourner le serveur mandataire peuvent trouver ou deviner l'adresse de la passerelle par défaut. Une fois que cela se produit, la façon de contourner le serveur mandataire est rapidement répandue.
- **Employer des politiques de domaine ou de groupe**. Ceci est très utile pour configurer les configurations correctes de serveur mandataire pour Internet Explorer sur tous les ordinateurs dans le domaine, mais ce n'est pas très utile pour empêcher que le serveur proxy soit contourné parce qu'il se base sur le registre d'un usager au domaine NT. Un usager avec un ordinateur Windows 95/98/ME peut annuler son identification réseau puis éviter le serveur proxy et une personne qui connaît un mot de passe local d'un usager sur son ordinateur Windows NT/2000/XP peut s'identifier localement et faire la même chose.
- **En prieres et querelles avec les usagers**. Ceci ne constitue jamais une situation optimale pour un administrateur de réseau.

La seule manière de s'assurer que les serveurs proxy ne soient pas évités est d'utiliser une configuration correcte de réseau, en utilisant une des trois techniques décrites ci-dessous.

## Pare-feu

Une manière plus fiable de s'assurer que les ordinateurs ne dévient pas le serveur proxy peut être mise en application en utilisant un pare-feu. Le pare-feu peut être configuré pour permettre l'entrée uniquement au serveur Proxy, par exemple pour faire des demandes HTTP à Internet. Tous les autres ordinateurs sont bloqués, comme illustré dans le diagramme ci-dessous.

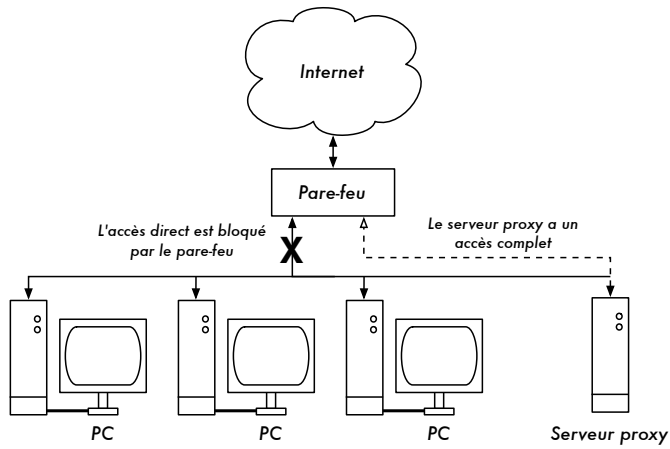


*Figure 3.15: Le pare-feu empêche les ordinateurs d'accéder directement à Internet, mais permet l'accès via le serveur proxy.*

Le fait de compter sur un pare-feu, comme dans le diagramme ci-dessus, peut être suffisant ou pas, selon la façon dont il est configuré. S'il ne fait que bloquer l'accès du LAN du campus au ports 80 des serveurs Web, des usagers intelligents trouveront des manières de le contourner. En outre, ils pourront employer des protocoles gourmands en bande passante tels que Kazaa.

## Deux cartes réseau

Peut-être la méthode la plus fiable est d'installer deux cartes réseau sur le serveur proxy et de relier le réseau du campus à Internet comme montré ci-dessous. De cette façon, la disposition du réseau rend physiquement impossible d'atteindre Internet sans passer par le serveur mandataire.

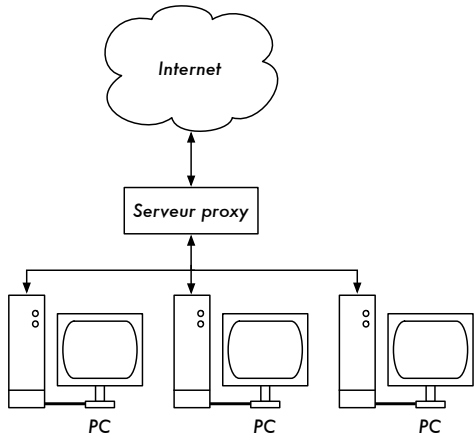


*Figure 3.16: Le seul chemin vers Internet est à travers le serveur proxy .*

Le serveur proxy dans ce schéma ne devrait pas avoir le IP fowarding activé, à moins que les administrateurs sachent exactement ce qu'ils veulent laisser passer.

Un grand avantage à cette configuration de réseau est qu'il est possible d'utiliser une technique connue en anglais sous le nom de « ***transparent proxying*** » (ou détournement du trafic à l'insu de l'utilisateur). Utiliser un transparent *proxying* signifie que les demandes Web de l'usager sont automatiquement renvoyées au serveur proxy sans avoir à configurer manuellement les navigateurs Web pour l'utiliser. Ceci force efficacement à ce que tout le trafic Web soit stocké localement, ce qui élimine beaucoup de possibilités d'erreur des usagers, et fonctionnera même avec les dispositifs qui ne soutiennent pas l'usage d'un Proxy manuel. Pour plus de détails au sujet de la configuration d'un transparent proxy avec Squid, visitez les sites suivants:

- *http://www.squid-cache.org/Doc/FAQ/FAQ-17.html*
- *http://en.tldp.org/HOWTO/mini/TransparentProxy-2.html*

## Routage réglementé

Une façon d'empêcher que les usagers puissent contourner le serveur Proxy avec de l'équipement Cisco est de réglementer le routage. Le routeur de Cisco dirige d'une manière transparente des demandes Web vers le serveur proxy. Cette technique est employée à l'Université de Makerere. L'avantage de cette méthode est que si le serveur proxy tombe en panne, les politiques de routage peuvent être temporairement enlevés, permettant aux clients de se connecter directement à Internet.

## Sites Web miroirs

Si le site Web n'est pas trop grand, et avec la permission du propriétaire ou de l'administrateur de ce site, il est possible de le copier à un serveur local durant la nuit. Ceci devrait être considéré pour les sites Web importants qui renferment un intérêt particulier pour une organisation ou qui sont très populaires parmi les usagers. Bien que ceci puisse être utile, il présente quelques pièges potentiels. Par exemple, si le site qui est dupliqué contient des programmes CGI ou tout autre contenu dynamique qui exigent de l'interaction de l'usager, ceci poserait des problèmes. Un exemple est un site Web qui demande aux personnes de s'inscrire en ligne à une conférence. Si quelqu'un s'enregistre en ligne sur un serveur dupliqué (et le programme miroir fonctionne bien), les organisateurs du site ne recevront pas l'information de la personne enregistrée.

Puisque dupliquer un site peut violer des droits de copyright, cette technique devrait seulement être employée avec la permission du site concerné. Si le site possèede ***rsync***, il pourrait être copié en utilisant cette commande. C'est probablement la manière la plus rapide et la plus efficace de maintenir le contenu du site synchronisé. Si le serveur Web à distance n'exécute pas rsync, le logiciel recommandé à employer est un programme appelé ***wget***. Il fait partie de la plupart des versions d'Unix/Linux. Une version de Windows peut être trouvée à *http://xoomer.virgilio.it/hherold/* ou dans le paquet d'outils gratuit de Cygwin Unix ( *http://www.cygwin.com/* ).

Il est possible d'utiliser un script qui fonctionne toutes les nuits sur un serveur Web local et qui fasse ce qui suit:

- Changer le répertoire racine du serveur Web: par exemple, **`/var/www/`** sur Unix, ou **`C:\Inetpub\wwwroot`** sur Windows.
- Copier un site Web en utilisant la commande:

```
wget --cache=off -m http://www.python.org
```

Le site Web dupliqué se trouvera dans un répertoire **`www.python.org`**. Le serveur Web devrait maintenant être configuré pour servir le contenu de ce répertoire comme un hôte virtuel basé sur un nom (*Name-based virtual host*). Installez un serveur local DNS pour falsifier une entrée à ce site. Pour que ceci fonctionne, les ordinateurs clients devraient être configurés pour utiliser le serveur local DNS comme DNS primaire (ceci est toujours recommandé parce que la cache d'un serveur local DNS accélère les temps de réponse Web).

## Pré-actualiser le site dans la cache en utilisant wget

Au lieu d'installer un site Web miroir comme décrit à la section précédente, une meilleure approche est de peupler le proxy cache en utilisant un processus automatisé. Cette méthode a été décrite par J. J. Eksteen et J. P. L. Cloete du CSIR à Pretoria, Afrique du Sud, dans un article intitulé ***Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies*** (disponible à l'adresse *http://www.isoc.org/inet97/ans97/cloet.htm*). Voici comment ils décrivent le fonctionnement de ce processus:

> *«Un processus automatique récupère la page initiale d'un site et un nombre spécifié de pages supplémentaires (en suivant récursivement le HTML sur les pages récupérées) à travers l'utilisation d'un proxy. Au lieu d'écrire les pages récupérées sur le disque local, le processus miroir rejette les pages récupérées. Ceci est fait afin de conserver les ressources du système ainsi que pour éviter des possibles conflits de droits d'auteur. En utilisant le proxy comme intermédiaire, il est garanti que les pages récupérées se trouveront dans la cache du proxy comme si un client avait accédé à cette page. Quand un client accède à la page récupérée, celle-ci lui est servie à partir de la cache et non du lien international congestionné. Ce processus peut être exécuté dans des périodes où le réseau est peu utilisé afin de maximiser l'usage de largeur de bande et de ne pas concurrencer d'autres activités d'accès.»*

La commande suivante (programmée pour fonctionner durant la nuit une fois par jour ou par semaine) est tout ce dont nous avons besoin (elle doit être répétée pour chaque site qui a besoin d'être pré-actualisé).

```
wget --proxy-on --cache=off --delete after -m http://www.python.org
```

Explication:

- **-m** : Copie le site au complet. wget commence à *www.python.org* et suit tous les hyperliens, c'est à dire qu'il télécharge toutes les sous-pages.
- **--proxy-on** : S'assure que wget utilise le serveur mandataire. Ceci n'est pas nécessaire dans les applications utilisant un *transparent proxy*.
- **--cache=off** : S'assure que le nouveau contenu est récupéré d'Internet et non du serveur mandataire local.
- **--delete after** : Élimine la copie miroir. Le contenu miroir reste dans la cache proxy s'il y assez d'espace disque et que les paramètres de la cache du serveur proxy sont corrects.

En outre, wget a beaucoup d'autres options; par exemple, fournir un mot de passe pour les sites Web qui les exigent. À l'aide de cet outil, Squid devrait

être configuré avec un espace de disque suffisant pour contenir tous les sites pré-actualisés et plus (pour l'usage normal de Squid impliquant des pages autres que celles pré-actualisée). Heureusement, l'espace disque devient de plus en plus meilleur marché et les tailles de disque sont bien plus grandes qu'auparavant. Cependant, cette technique peut être employée seulement avec quelques sites choisis. Ces sites ne devraient pas être trop grands afin que le processus puisse finir avant le début des heures de travail et on devrait toujours garder un oeil sur l'espace disque disponible.

## Hiérarchies de cache

Lorsqu'une organisation a plus d'un serveur proxy , les proxy peuvent mettre en commun l'information de cache entre eux. Par exemple, si une page Web existe dans le cache du serveur A, mais non dans celui du serveur B, un usager connecté par l'intermédiaire du serveur B pourrait obtenir l'objet cache du serveur A par l'intermédiaire du serveur B. Le ***Protocole Inter-Cache*** (***ICP***) et le ***Protocole de routage CARP*** (en anglais «*Cache Array Routing Protocol*» -*CARP*) peuvent partager l'information de cache. Le CARP est considéré le meilleur des deux. Squid supporte les deux protocoles et le serveur de MS ISA supporte CARP. Pour plus d'information, voir le site: *http://squid-docs.sourceforge.net/latest/html/c2075.html*. Ce partage d'information de cache réduit l'utilisation de largeur de bande dans les organismes où plus d'un serveur mandataire est employé.

## Spécifications proxy

Sur un réseau de campus universitaire, il devrait y avoir plus d'un serveur proxy, pour des raisons de performance et de redondance. Avec les disques bon marché et les grandes capacités disponibles aujourd'hui, des serveurs proxy puissants peuvent être construits, avec 50 gigaoctets ou plus d'espace disque assignés au cache. La performance des disques est importante, donc les disques SCSI les plus rapides auraient une meilleure performance (bien qu'une cache basée sur un IDE est mieux que rien du tout). RAID (*Redundant Array of Independent Disks)* ou l'usage de miroirs n'est pas recommandée.

On recommande également qu'un disque séparé soit consacré au cache. Par exemple, un disque peut être réservé au cache et un deuxième pour le système d'exploitation et la journalisation. Squid est conçu pour utiliser autant de mémoire RAM qu'il peut obtenir parce qu'il est beaucoup plus rapide de récupérer des données de la mémoire RAM que du disque dur. Pour un réseau de campus, la mémoire RAM devrait être de 1GB ou plus:

- Indépendamment de la mémoire exigée pour le logiciel d'exploitation et d'autres applications, Squid exige 10 MB de RAM pour chaque 1 GB de

disque cache. Par conséquent, s'il y a 50 GB d'espace disque assigné au cache, Squid exigera une mémoire supplémentaire de 500 MB.

- L'ordinateur exigera également 128 MB pour Linux et 128 MB pour X-windows. Un autre 256 MB devrait être ajouté pour d'autres applications et pour que tout puisse fonctionner facilement.
- Rien n'augmente autant la performance d'une machine que d'installer une grande quantité de mémoire, parce que ceci réduit la nécessité d'utiliser le disque dur. La mémoire est mille fois plus rapide qu'un disque dur. S'il y a assez de RAM disponible, les logiciels d'exploitation modernes maintiennent des données fréquemment consultées dans la mémoire. On utilise le fichier de page du disque dur comme zone de mémoire supplémentaire quand ils n'y a pas assez de RAM.

## Cache de DNS et optimisation

Les serveurs DNS de cacheseule ne font autorité sur aucun nom de domaine, ils ne font que stocker les résultats des demandes des clients, de la même façon qu'un serveur proxy stocke les pages Web populaires pendant un certain temps. Les adresses DNS sont stockées jusqu'à ce que leur ***temps de vie*** (en anglais *Time to Live -TTL*) expire. Ceci réduira la quantité du trafic DNS sur votre connexion Internet, parce que la cache DNS peut satisfaire plusieurs demandes localement. Naturellement, les ordinateurs des clients doivent être configurés pour utiliser le nom de serveur cache-seule en tant que leur serveur DNS. Quand tous les clients utilisent ce serveur DNS en tant que serveur principal, il remplira rapidement la cache d'adresses IP de noms, de sorte que les requêtes de noms précédemment lancées puissent rapidement obtenir réponse. Les serveurs DNS qui font autorité pour un domaine agissent également en tant que cache de l'association nom-adresse des hôtes de ce domaine.

### Serveur Bind (*named*)

Bind est le programme standard de facto utilisé pour les services de nom sur Internet. Lorsque Bind est installé et fonctionnel, il agira en tant que serveur cache (aucune autre configuration n'est nécessaire). Bind peut être installé à partir d'un paquet Debian ou RPM. L'installation à partir d'un paquet est habituellement la méthode la plus facile. Sur Debian, entrez au clavier:

```
apt-get install bind9
```

En plus de sa fonction de cache, Bind peut également héberger des zones d'autorités, agir comme un esclave pour zones d'autorités, implanter une *split horizon* et presque tout ce qui est possible avec le protocol DNS.

## dnsmasq

Le serveur **dnsmasq** est une alternative de serveur de cache DNS. Il est disponible pour BSD et la plupart des distributions Linux ou encore à l'adresse suivante: *http://freshmeat.net/projects/dnsmasq/*. Le grand avantage de dnsmasq est sa flexibilité: il agit facilement en tant que serveur proxy cache DNS ainsi qu'en tant que source d'autorité pour des hôtes et des domaines sans avoir recours à des fichiers de configuration de zone compliqués. Des mises à jour peuvent être faites à une zone sans même avoir à redémarrer le service. Il peut également servir de serveur DHCP et intègre le service DNS à celui de DHCP. Il est très léger, stable et extrêmement flexible. Bind est probablement un meilleur choix pour de très grands réseaux (plus qu'une centaine de noeuds), mais la simplicité et la flexibilité de dnsmasq le rendent attrayant pour les réseaux de petite à moyenne taille.

## Windows NT

Pour installer le service DNS sur Windows NT4: choisissez le panneau de configuration Réseau > Services > Ajoutez > Serveur DNS de Microsoft. Insérez le CD de Windows NT4 lorsque le système le demande. La configuration d'un serveur de cache uniquement dans NT est décrite dans l'article Knowledge Base 167234. En voici un extrait:

> *« Installez simplement DNS et entrez dans le gestionnaire de noms de domaines (Domain Name System Manager). Cliquez sur DNS dans le menu, choisissez Nouveau Serveur et saisissez l'adresse IP de l'ordinateur où vous avez installé DNS. Vous avez maintenant un serveur DNS de cache uniquement».*

## Windows 2000

Pour installer le service DNS: Démarrer > Paramètres > Panneau de configuration > Ajout/Suppression de programmes > Ajouter/Supprimer des composants Windows > Services de mise en réseau > Détails > Domain Name System (DNS). Ensuite, démarrez DNS MMC (Démarrer > Programmes > Outils Administratifs > DNS). Dans le menu Action choisir « Connecter à l'Ordinateur… » Dans la fenêtre de Sélection d'Ordinateur Cible, activez « l'Ordinateur Suivant » et entrez le nom du serveur DNS que vous voulez en cache uniquement. S'il y a un .[point] dans le gestionnaire DNS (ceci se fait par défaut), cela signifie que le serveur DNS pense qu'il est le serveur DNS racine d'Internet. Il ne l'est certainement pas. Pour que tout puisse fonctionner, supprimez le «.»[Point].

## DNS divisé et serveur miroir

Le but d'un DNS divisé (***split DNS*** ou ***split horizon*** en anglais) est de présenter une vision différente de son domaine vu de l'interne ou de l'externe. Il

y a plus d'une façon de faire un DNS divisé; mais pour des raisons de sécurité, on recommande que vous ayez deux serveurs de contenu DNS séparés: l'interne et l'externe (chacun avec différentes bases de données).

Le DNS divisé peut permettre à des clients d'un réseau de campus de voir des adresses IP du domaine du campus comme adresses locales IP RFC1918, alors que le reste d'Internet verra les mêmes noms sous une adresse IP différente. Ceci est rendu possible à deux zones sur deux serveurs DNS différents pour le même domaine.

Une des zones est employée par les clients internes du réseau et l'autre par des usagers sur Internet. Par exemple, dans le réseau suivant, l'usager au sein du campus Makerere verra *http://www.makerere.ac.ug/* résolu comme 172.16.16.21, tandis qu'un usager ailleurs sur Internet le verra résolu comme 195.171.16.13.

Le serveur DNS sur le campus dans le diagramme ci-dessus a un fichier de zone pour makerere.ac.ug et est configuré comme s'il faisait autorité pour ce domaine. En outre, il sert de serveur DNS cache pour le campus de Makerere et tous les ordinateurs sur le campus sont configurés pour l'utiliser en tant que serveur DNS.

Les enregistrement DNS pour le serveur DNS du campus ressembleraient à ceci:

```
makerere.ac.ug
www     CNAME   webserver.makerere.ac.ug
ftp     CNAME   ftpserver.makerere.ac.ug
mail    CNAME   exchange.makerere.ac.ug
mailserver      A       172.16.16.21
webserver       A       172.16.16.21
ftpserver       A       172.16.16.21
```

Mais il y a un autre serveur DNS sur Internet qui est en réalité l'autorité pour le domaine *makerere.ac.ug* domain. Les entregistrements DNS pour cette zone externe ressembleront à ceci:

```
makerere.ac.ug
www     A 195.171.16.13
ftp     A 195.171.16.13
mail    A 16.132.33.21
        MX mail.makerere.ac.ug
```

Le DNS divisé ne dépend pas de l'usage d'adresses RFC 1918. Un fournisseur de service internet (ISP) africain pourrait, par exemple, héberger des sites Web au nom d'une université mais également créer un miroir de ces mêmes sites Web en Europe. Toutes les fois que les clients de cet ISP accèdent au site Web, ils obtiennent l'adresse IP de l'ISP africain et le trafic demeure donc dans le même pays. Lorsque les visiteurs d'autres pays

accèdent à ce site Web, ils obtiennent l'adresse IP du serveur Web miroir en Europe. De cette façon, les visiteurs internationaux n'encombrent pas la connexion du VSAT de l'ISP en visitant le site Web de l'université. Ceci devient une solution attrayante car l'hébergement Web près du réseau fédérateur Internet est devenu très bon marché.

# Optimisation des liens Internet

Comme cité précédemment, la capacité de traitement du réseau jusqu'à 22Mbps peut être réalisée en utilisant du matériel standard, sans licence, 802.11g. Cette quantité de largeur de bande sera probablement au moins un ordre de grandeur plus haut que celle fournie par votre lien d'Internet et devrait pouvoir soutenir confortablement plusieurs usagers Internet simultanés.

Mais si votre connexion Internet principale est fournie via un lien VSAT, vous rencontrerez quelques problèmes de performance si vous vous fiez aux paramètres TCP/IP par défaut. En optimisant votre lien VSAT, vous pouvez améliorer de manière significative les temps de réponse lors de vos requêtes vers les serveurs d'Internet.

## Facteurs TCP/IP qui affectent une connexion satellite

Un VSAT est souvent imagé comme étant « un long et large tuyau de données ». Cette limite se rapporte aux facteurs qui affectent la performance de TCP/IP sur n'importe quel réseau qui a une largeur de bande relativement grande, mais une latence élevée. La plupart des connexions Internet en Afrique et autres régions du monde en voie de développement sont par l'intermédiaire de VSAT. Par conséquent, même si une université obtient sa connexion par l'intermédiaire d'un ISP, cette section pourrait s'appliquer si la connexion ISP est réalisée par l'intermédiaire d'un VSAT. La latence élevée dans les réseaux satellites est due à la grande distance du satellite ainsi qu'à la vitesse constante de la lumière. Cette distance augmente d'environ 520 ms le temps d'aller-retour d'un paquet (RTT) comparé à un RTT de l'Europe aux États-Unis (environ 140 ms).

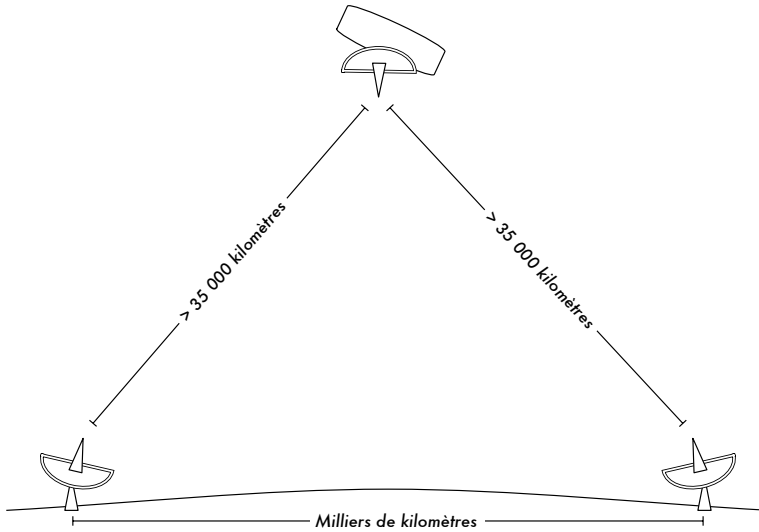


*Figure 3.17: Étant donnée la vitesse de la lumière et les longues distances impliquées, la confirmation de réception d'un seul paquet «ping» peut prendre plus de 520 ms sur un lien VSAT.*

Les facteurs qui ont un impact plus significatif sur la performance TCP/IP sont les ***longs temps de propagation***, un ***produit delai x bande passante élevé*** et les ***erreurs de transmission***.

D'une manière générale, un réseau satellite devrait utiliser des systèmes d'exploitation ayant une implantation moderne de TCP/IP supportant les extensions du RFC 1323:

- L'option ***window scale*** pour permettre de grandes tailles de fenêtre TCP (plus grandes que 64KB).
- ***Réception sélective*** (*Selective acknowledgement -SACK* en anglais) afin de permettre une récupération plus rapide des erreurs de transmissions.
- Horodatage pour calculer les valeurs RTT et l'expiration du temps de retransmission pour le lien en usage.

## Temps d'aller-retour élevé («*round-trip time*» -RTT)

Les liaisons satellites ont un RTT moyen d'environ 520ms au premier saut. TCP emploie le mécanisme *slow-start* au début d'une connexion pour trouver les paramètres appropriés de TCP/IP pour cette connexion. Le temps passé dans l'étape *slow-start* est proportionnel au RTT et pour un lien satellite ceci signifie que le TCP reste dans un mode slow-start pendant plus longtemps que dans d'autres cas. Ceci diminue dramatiquement la capacité de traitement des connexions TCP de courte durée. On peut le constater

dans le fait que le téléchargement d'un petit site Web prend étonnamment beaucoup temps, alors qu'un grand fichier est transféré à des débits acceptables après un court moment.

En outre, quand des paquets sont perdus, TCP entre dans la phase de contrôle de congestion et, à cause du RTT élevé, il reste plus longtemps dans cette phase, réduisant de ce fait le rendement des connexions TCP de courte et de longue durée.

## Produit délai-bande passante élevé

La quantité de données en transit sur un lien à un moment donné est le produit de la largeur de bande et du RTT. En raison de la latence élevée du lien satellite, le produit *délai-bande passante* est grand. TCP/IP permet à l'hôte à distance d'envoyer une certaine quantité de données à l'avance sans attendre de confirmation. Une confirmation est habituellement exigée pour toutes les données entrantes sur une connexion TCP/IP. Cependant, on permet toujours à l'hôte à distance d'envoyer une certaine quantité de données sans confirmation, ce qui est important pour réaliser un bon taux de transfert sur les connexions ayant un produit *délai-bande passante* élevé. Cette quantité de données s'appelle la ***Taille de la fenêtre TCP***. Dans les réalisations modernes de TCP/IP, la taille de la fenêtre est habituellement de 64KB.

Sur les réseaux satellites, la valeur du produit *délai-bande passante* est importante. Pour utiliser le lien dans toute sa capacité, la taille de la fenêtre de la connexion devrait être égale au produit *délai-bande passante*. Si la taille maximale de fenêtre permise est de 64KB, la capacité de traitement maximum réalisable par l'intermédiaire du satellite est (taille de la fenêtre) /RTT, ou 64KB / 520 ms. Ceci donne un débit maximum de 123KB/s, ce qui représente 984 Kbps, indépendamment du fait que la capacité du lien peut être beaucoup plus grande.

Chaque en-tête de segment TCP contient un champ appelé ***fenêtre annoncée*** qui indique combien d'octets additionnels de données le récepteur est prêt à accepter. La fenêtre annoncée est la place qui est encore libre dans le tampon. On ne permet pas à l'expéditeur d'envoyer des octets au-delà la fenêtre annoncée. Pour maximiser la performance, les tailles des tampons de l'expéditeur et du récepteur devraient au moins être égales au produit *délai-bande passante*. Dans la plupart des réalisations modernes de TCP/IP, cette taille de buffer a une valeur maximum de 64KB.

Pour surmonter le problème des versions de TCP/IP qui ne dépassent pas la taille de fenêtre au delà de 64KB, une technique connue sous le nom de «***TCP acknowledgment spoofing***» peut être employée (voir la section « proxy d'amélioration de performance », ci-dessous).

## Les erreurs de transmission

Dans les implantations les plus anciennes de TCP/IP, la perte de paquet est toujours considérée comme conséquence d'une congestion (au lieu d'erreurs de lien). Quand ceci se produit, TCP effectue l'action d'éviter la congestion en exigeant trois acquittements positifs (ACK) dupliqués ou en entrant en phase slow-start dans le cas où le temps d'attente ait expiré. En raison de la longue valeur de RTT, une fois que cette phase de contrôle de congestion est commencée, le lien satellite TCP/IP prendra un temps plus long avant de revenir au niveau de capacité de traitement précédent. Par conséquent, les erreurs sur un lien satellite ont un effet plus sérieux sur la performance TCP que sur des liens de faible latence. Pour surmonter cette limitation, des mécanismes tels que l'***Acquittement Sélectif*** (***SACK***) ont été développés. Le SACK indique exactement les paquets qui ont été reçus, permettant à l'expéditeur de retransmettre uniquement les segments qui sont absents en raison des erreurs de lien.

L'article sur les détails d'implantation de TCP/IP sur Microsoft Windows 2000 affirme:

> *«Windows 2000 introduit la prise en charge d'une fonctionnalité de performances disponible comme Acquittement Sélectif (SAK). SAK est particulièrement important pour des connexions utilisant de grandes tailles de fenêtre TCP.»*

SAK est une caractéristique standard de Linux et BSD depuis un certain temps. Assurez-vous que tant votre routeur Internet comme votre ISP à distance soutiennent SACK.

## Considérations pour les universités

Si un site a une connexion de 512 Kbps à Internet, les configurations par défaut TCP/IP sont probablement suffisantes, parce qu'une taille de fenêtre de 64 KB peut remplir jusqu'à 984 Kbps. Mais si l'université a plus de 984 Kbps, elle ne pourrait pas dans certains cas obtenir la pleine largeur de bande du lien disponible dû aux facteurs du «long et large tuyau de donnée» abordés plus haut. Ce que ces facteurs impliquent vraiment est qu'ils empêchent qu'un ordinateur remplisse toute la largeur de bande. Ce n'est pas une mauvaise chose pendant le jour, parce que beaucoup de gens emploient la largeur de bande. Mais si, par exemple, il y a de grands téléchargements programmés la nuit, l'administrateur pourrait vouloir que ces téléchargements se servent de la pleine largeur de bande, et les facteurs du «long et large tuyau de donnée» pourraient être un obstacle. Ceci peut également devenir critique si une quantité significative de votre trafic de réseau est routé à travers un tunnel unique ou une connexion VPN jusqu'à l'autre extrémité du lien VSAT.

Pour plus d'informations, voir *http://www.psc.edu/networking/perf_tune.html*.

## Proxy d'amélioration deperformance («*Performance-enhancing proxy*» -PEP)

L'idée d'un proxy d'amélioration de performance proxy est décrite dans le RFC 3135 (voir *http://www.ietf.org/rfc/rfc3135*) et pourrait être un serveur proxy avec un grand disque cache qui a des extensions RFC 1323 entre autres caractéristiques. Un ordinateur portable a une session TCP avec PEP chez l'ISP. Ce PEP, et celui qui se trouve chez le fournisseur de satellite, communiquent entre eux en utilisant différentes sessions TCP ou encore leur propre protocole propriétaire. Le PEP du fournisseur de satellite obtient les fichiers du serveur web. De cette façon, la session TCP se divise et donc les caractéristiques du lien qui ont un effet sur la performance du protocole (les facteurs du tuyeau long et large) sont évités (à travers le TCP *acknowledgment spoofing* par exemple). En plus, PEP se sert du proxying et du pré-telechargement pour accélérer davantage l'accès au web.

Un tel système peut être construit à partir de rien en utilisant par exemple Squid ou encore en achetant des solutions économiques offertes par plusieurs vendeurs.

# 4
# Antennes et lignes de transmission

L'émetteur qui produit l'énergie RF[1] pour l'antenne est habituellement situé à une certaine distance des bornes d'antenne. Le lien de connexion entre les deux est la **ligne de transmission** RF. Son but est de transporter l'énergie RF d'un endroit à l'autre et de le faire aussi efficacement que possible. Du côté du récepteur, l'antenne est responsable d'attraper tous les signaux de radio dans le ciel et de les passer au récepteur avec un minimum de distorsion de sorte que la radio puisse décoder le signal convenablement. C'est pour ces raisons que le câble RF a un rôle très important dans les systèmes de radio: il doit maintenir l'intégrité des signaux dans les deux directions.

Il y a deux catégories principales de lignes de transmission: les câbles et les guides d'ondes. Les deux sont très efficaces pour transporter de l'énergie RF à 2,4 GHz.

## *Câbles*

Les câbles RF sont, pour des fréquences supérieures à la fréquence HF, presque exclusivement des câbles coaxiaux (ou ***coax*** en en abrégé, dérivé des mots « *d'une axe commun* »). Les câbles coaxiaux se composent d'un ***conducteur*** de cuivre entouré par un matériel non-conducteur nommé ***diélectrique*** ou simplement ***isolation***. Le matériel diélectrique est entouré par un bouclier de fils tressés qui empêchent une connexion électrique. le câble coax est également protégé par une gaine externe qui est généralement faite à partir d'un matériel PVC. Le conducteur intérieur transporte le signal RF et

**1.** Radio Fréquence. Voir le chapitre 2 pour une discussion sur les ondes électromagnétiques.

le bouclier externe empêche le signal RF de rayonner dans l'atmosphère tout en empêchant également les signaux extérieurs de faire interférence sur le signal porté par le noyau. Un autre fait intéressant est que le signal électrique voyage toujours le long de la couche externe du conducteur central: plus le conducteur central est grand, mieux le signal circulera. Ceci s'appelle « l'effet pelliculaire ».

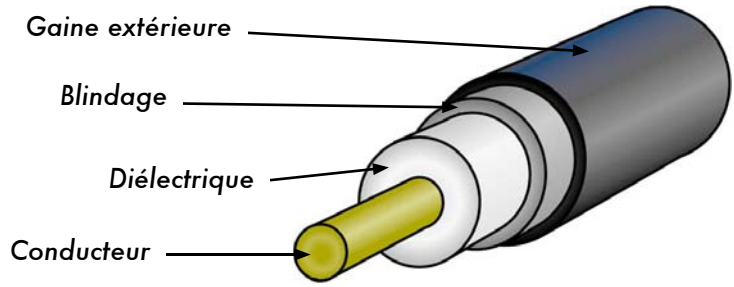


*Figure 4.1: Câble coaxial avec gaine extérieure, bouclier, matériel diélectrique et conducteur.*

Même si la construction coaxiale est efficace pour contenir le signal au sein du noyau, on observe une certaine résistance à la circulation électrique: pendant que le signal voyage au sein du noyau, il perd de sa force. Ceci est connu en tant que phénomène d'***atténuation***, et pour les lignes de transmission il est mesuré en décibels par mètre (***dB/m***). Le taux d'atténuation est une fonction de la fréquence du signal et de la construction physique du câble lui-même. À mesure que la fréquence du signal augmente, son atténuation le fera également. Évidemment, nous devons réduire au minimum, autant que possible, l'atténuation du câble en le maintenant très court et en employant des câbles de haute qualité.

Voici quelques points à considérer au moment de choisir un câble pour être utilisé avec des dispositifs micro-ondes:

1. « Plus c'est court, mieux c'est! »: ceci est la première règle à suivre au moment d'installer un câble. Comme la perte d'énergie n'est pas linéaire, si vous doublez la longueur du câble, vous pourrez perdre beaucoup plus que le double d'énergie. De la même manière, réduire la longueur du câble de la moitié donnera à l'antenne plus que le double d'énergie. La meilleure solution est de placer l'émetteur le plus près possible de l'antenne, même si ceci suppose de le placer sur une tour.
2. « Moins c'est cher, pire c'est! »: la deuxième règle d'or est que l'argent que vous investissez au moment d'acheter un câble de qualité n'est pas vain. Les câbles peu dispendieux sont faits pour être utilisés à de faibles fréquences, comme la fréquence VHF. Les micro-ondes exigent des

câbles d'une qualité supérieure. Toutes les autres options ne sont qu'une charge factice.[2]

3. Éviter toujours les RG-58. Ils sont conçus pour les réseaux Ethernet, les CB ou radio de VHF et non pour les micro-ondes.
4. Éviter également les RG-213. Ils sont conçus pour les radios CB et HF. Dans ce cas, le diamètre du câble n'implique ni grande qualité ni faible atténuation.
5. Lorsque c'est possible, employez des câbles ***Heliax*** (également nommés "mousse") pour relier l'émetteur à l'antenne. Quand ceux-ci ne sont pas disponibles, employez le meilleur câble LMR que vous pouvez trouver. Les câbles Heliax ont un conducteur central solide ou tubulaire et un conducteur externe solide ondulé qui leur permet de fléchir. Les câbles Heliax peuvent être construits de deux façons: en utilisant l'air ou la mousse comme matériel diélectrique. Les câbles diélectriques à air sont les plus chers et garantissent une perte minimum d'énergie, mais ils sont très difficiles à manipuler. Les câbles diélectriques en mousse causent une perte d'énergie légèrement plus élevée mais sont moins chers et plus faciles à installer. Un procédé spécial est exigé au moment de souder les connecteurs afin de garder le câble diélectrique en mousse sec et intact. LMR est une marque de câble coax disponible sous différents diamètres qui fonctionne bien avec des fréquences micro-ondes. Comme alternative aux câbles Heliax, on utilise généralement les LMR-400 et LMR-600.
6. Autant que possible, employez des câbles qui ont été pré-sertis et examinés dans un laboratoire approprié. L'installation de connecteurs sur des câbles peut être une tâche ardue, et il est difficile de la faire correctement même avec les outils appropriés. À moins que vous ayez accès à un équipement qui vous permette de vérifier le câble que vous avez réalisé (tel un analyseur de spectre et un générateur de signal ou un réflectomètre temporel), le dépannage d'un réseau utilisant un câble fait maison peut être difficile.
7. Ne maltraitez pas votre ligne de transmission. Ne marchez jamais sur un câble, ne le pliez pas trop et n'essayez pas de débrancher un connecteur en tirant directement sur le câble. Tous ces comportements peuvent changer la caractéristique mécanique du câble et donc son impédance, provoquer un court-circuit entre le conducteur intérieur et le bouclier, voir même briser la ligne. Ces problèmes sont difficiles à repérer et à reconnaître et peuvent produire un comportement imprévisible sur le lien radio.

---

**2.** Une charge factice est un dispositif qui absorbe l'énergie RF sans la rayonner. Imaginez un radiateur qui fonctionne aux radio fréquences.

# Guides d'ondes

Au-dessus de 2 GHz, la longueur d'onde est assez courte pour permettre un transfert d'énergie efficace et pratique par différents moyens. Un guide d'ondes est un tube conducteur par lequel l'énergie est transmise sous forme d'ondes électromagnétiques. Le tube agit en tant que frontière qui confine les ondes en son intérieur. L'effet pelliculaire empêche tous les effets électromagnétiques d'émaner hors du guide. Les champs électromagnétiques sont propagés par le guide d'ondes au moyen de réflexions contre ses murs intérieurs, qui sont considérés comme des conducteurs parfaits. L'intensité des champs est plus grande au centre le long de la dimension X et doit diminuer à zéro en arrivant aux murs car l'existence de n'importe quel champ parallèle aux murs sur la surface ferait entrer un courant infini dans un conducteur parfait. Naturellement, les guides d'ondes ne peuvent pas acheminer d'énergie RF de cette façon.

Les dimensions X, Y et Z d'un guide d'ondes rectangulaire sont représentées dans la figure suivante:

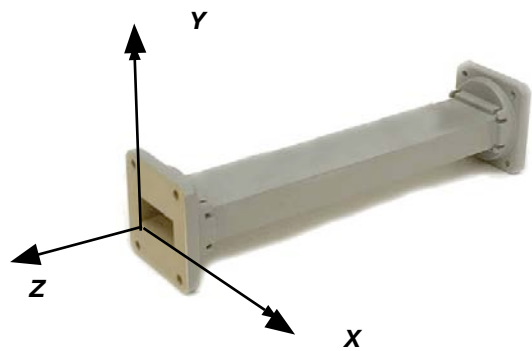


*Figure 4.2: Les dimensions X, Y, et Z d'un guide d'onde rectangulaire.*

Il y a un nombre infini de manières par lesquelles les champs électriques et magnétiques peuvent s'ordonner dans un guide d'ondes pour des fréquences au-dessus de la fréquence de coupure basse. Chacune de ces configurations de champ s'appelle un ***mode***. Les modes peuvent être séparés en deux groupes généraux. Un groupe, nommé ***TM*** (transverse magnétique), a un champ magnétique entièrement transversal à la direction de propagation mais une composante du champ électrique dans la direction de la propagation. L'autre groupe, nommé ***TE*** (transverse électrique) a un champ électrique entièrement transversal mais une composante de champ magnétique dans la direction de la propagation.

Le mode de propagation est identifié par deux lettres suivies de deux numéros. Par exemple, TE 10, TM 11, etc... Le nombre de modes possibles aug-

mente avec la fréquence pour une taille donnée de guide et il n'y a qu'un mode possible, nommé le ***mode dominant***, pour la plus basse fréquence transmissible. Dans un guide rectangulaire, la dimension critique est X. Cette dimension doit être plus élevée que 0,5 λ à la plus basse fréquence à être transmise. Dans la pratique, la dimension Y est habituellement égale à 0,5 X pour éviter la possibilité d'opérer dans un autre mode que le dominant. D'autres formes de guide peuvent être employées, la plus importante étant la forme circulaire. Dans ce dernier cas, nous appliquons plus ou moins les mêmes considérations que pour les guides rectangulaires. Les dimensions des longueurs d'onde pour les guides rectangulaires et circulaires sont indiquées dans la table suivante, où X est la largeur d'un guide rectangulaire et r est le rayon d'un guide circulaire. Toutes les figures s'appliquent au mode dominant.

| Type de guide | Rectangulaire | Circulaire |
|---|---|---|
| Longueur d'onde de coupure | **2X** | **3,41r** |
| Plus longue longueur d'onde transmise avec peu d'atténuation | **1,6X** | **3,2r** |
| Plus courte longueur d'onde avant que le prochain mode devienne possible | **1,1X** | **2,8r** |

L'énergie peut être présentée dans ou extraite à partir d'un guide d'ondes au moyen d'un champ électrique ou magnétique. Le transfert d'énergie se produit typiquement au moyen d'une ligne coaxiale. Deux méthodes possibles existent pour coupler une ligne coaxiale: utiliser le conducteur intérieur de la ligne coaxiale ou former une boucle. Une sonde qui est simplement une prolongation courte du conducteur intérieur de la ligne coaxiale peut être orientée de sorte qu'elle soit parallèle aux lignes électriques de la force. Une boucle peut être agencée de telle sorte qu'elle joigne certaines des lignes magnétiques de la force. Le point auquel l'accouplement maximum est obtenu dépend du mode de la propagation dans le guide ou la cavité. L'accouplement est maximum quand le dispositif d'accouplement est dans le champ le plus intense.

Si un guide d'ondes est laissé ouvert à une extrémité, il rayonnera l'énergie (c'est-à-dire qu'il peut être employé comme antenne plutôt que comme ligne de transmission). Ce rayonnement peut être augmenté en élargissant le guide d'ondes pour former une antenne cornet. Plus loin dans ce chapitre, nous verrons un exemple d'une antenne pratique de guide d'ondes pour les réseaux sans fil.

| Câble Type | Noyau | Diélectrique | Bouclier | Gaîne |
|---|---|---|---|---|
| RG-58 | 0,9 mm | 2,95 mm | 3,8 mm | 4,95 mm |
| RG-213 | 2,26 mm | 7,24 mm | 8,64 mm | 10,29 mm |
| LMR-400 | 2,74 mm | 7,24 mm | 8,13 mm | 10,29 mm |
| 3/8" LDF | 3,1 mm | 8,12 mm | 9,7 mm | 11 mm |

Voici une table contrastant les tailles de diverses lignes courantes de transmission. Choisissez le meilleur câble que vous pouvez vous permettre avec la plus faible atténuation possible à la fréquence que vous avez l'intention d'employer pour votre lien sans fil.

# Connecteurs et adaptateurs

Les connecteurs permettent à un câble d'être relié à un autre câble ou à une composante de la chaîne RF. Il y a une grande variété d'assortiments et de connecteurs conçus pour aller de pair avec diverses tailles et types de lignes coaxiales. Nous décrirons quelques-unes des plus populaires.

Les ***connecteurs BNC*** ont été développés vers la fin des années 40. BNC est l'acronyme de *Bayonet Neill Concelman* en honneur aux inventeurs: Paul Neill et Karl Concelman. Le BNC est un connecteur miniature qui permet un raccordement rapide des câbles. Il comporte deux crochets de baïonnette sur le connecteur femelle et le raccordement est réalisé avec un quart de tour de l'écrou d'accouplement. En principe, les connecteurs BNC sont appropriés pour la terminaison des câbles coaxiaux miniatures et subminiatures (RG-58 à RG-179, RG-316, etc...) Ils offrent une performance acceptable jusqu'à quelques gigahertz. On les retrouve généralement sur des équipements d'essai et sur les câbles coaxiaux Ethernet 10base2.

Les ***connecteurs TNC*** ont également été inventés par Neill et Concelman, et ils sont une variation filetée du BNC. En raison d'une meilleure interconnexion offerte par le connecteur fileté, les connecteurs TNC fonctionnent bien à environ 12GHz. TNC est l'acronyme de *Threaded Neill Concelman* (Nelly Concelmann fileté).

Les connecteurs de ***type N*** (encore une fois pour Neill, bien que parfois attribué à la "marine", *Navy* en Anglais) ont été à l'origine développés pendant la deuxième guerre mondiale. Ils sont utilisables jusqu'à 18 gigahertz, et très couramment utilisés pour des applications micro-ondes. Ils sont disponibles pour presque tous les types de câble. Les joints de prise/câble et de prise/douille sont imperméables à l'eau fournissant de ce fait, un collier efficace.

***SMA*** est un acronyme pour la version A de SubMiniature, et il a été développé dans les années 60. Les connecteurs SMA sont des unités subminiatures de précision qui fournissent un excellent rendement électrique jusqu'à 18 gigahertz. Ces connecteurs à haut rendement ont une taille compacte et une longévité mécanique exceptionnelle.

Le nom ***SMB*** dérivé de SubMiniature B, la deuxième conception subminiature. Le SMB est une plus petite version du SMA avec un accouplement par encliquetage. Il offre une capacité de large bande à 4 gigahertz avec une conception de connecteur à encliquetage.

Les connecteurs ***MCX*** ont été introduits dans les années 80. Tandis que les MCX utilisent un contact intérieur et un isolateur de dimensions identiques aux SMB, le diamètre extérieur de la prise est 30% plus petit que celui des SMB. Cette série fournit aux concepteurs une bonne option dans le cas où le poids et l'espace physique sont limités. Les MCX fournissent une capacité de large bande à 6 gigahertz et une conception de connecteur à encliquetage.

En plus de ces connecteurs standard, la plupart des dispositifs WiFi emploient une variété de connecteurs propriétaires. Souvent, ceux-ci sont simplement des connecteurs standard à micro-ondes avec les pièces centrales du conducteur inversées ou le fil coupé dans une direction opposée. Ces pièces sont souvent intégrées dans un système de micro-ondes en utilisant un câble *jumper* court appelé ***queue de cochon*** (*pigtail* en anglais) qui convertit le connecteur qui n'est pas standard en quelque chose de plus robuste et couramment disponible. En voici une liste non exhaustive:

Le ***RP-TNC***.Il s'agit d'un connecteur TNC avec les genres inversés. Ils sont le plus souvent trouvés dans les équipements Linksys comme le WRT54G.

L'***U.FL*** (aussi connu sous l'acronyme ***MHF***). L'U.FL est un connecteur breveté par Hirose, alors que le MHF est un connecteur mécaniquement équivalent. C'est probablement le plus petit connecteur à micro-ondes actuellement sur le marché. L'U.FL/MHF est typiquement employé pour relier une carte radio de mini-PCI à une antenne ou à un plus grand connecteur (tel qu'un N ou un TNC).

La série ***MMCX***, qui se nomme également MicroMate, est une des plus petites lignes de connecteurs RF et a été développée dans les années 90. MMCX est une série micro-miniature de connecteur avec un mécanisme de verrouillage automatique acceptant une rotation de 360 degrés permettant la flexibilité. Les connecteurs MMCX sont généralement trouvés sur les cartes radio PCMCIA construites par Senao et Cisco.

Les connecteurs ***MC-Card*** sont encore plus petits et plus fragiles que les MMCX. Ils ont un connecteur externe fendu qui se brise facilement après un

certain nombre d'interconnexions. Ceux-ci sont généralement trouvés sur les équipements de Lucent/Orinoco/Avaya.

Les adaptateurs, qui s'appellent également adaptateurs coaxiaux, sont des connecteurs courts à deux côtés qui sont utilisés pour joindre deux câbles ou composantes qui ne peuvent pas être reliés directement. Les adaptateurs peuvent être utilisés pour relier ensemble des dispositifs ou des câbles de différents types. Par exemple, un adaptateur peut être utilisé pour brancher un connecteur SMA à un BNC. Les adaptateurs peuvent également être utilisés pour joindre des connecteurs du même type mais qui ne peuvent pas être directement unis en raison de leur genre. Par exemple un adaptateur très utile est celui qui permet de joindre deux types de connecteurs N, ayant des connecteurs femelles des deux côtés.

*Figure 4.3: Un adaptateur baril N femelle.*

## Choisir un connecteur convenable

1. «La question de genre.» Pratiquement tous les connecteurs ont un genre bien défini qui consiste soit en une extrémité mâle ou une extrémité femelle. Habituellement les câbles ont des connecteurs mâles sur les deux extrémités alors que les dispositifs RF (c.-à-d. les émetteurs et les antennes) ont des connecteurs femelles. Les dispositifs tels que les coupleurs directionnels et les dispositifs de mesure de ligne peuvent avoir des connecteurs mâle et femelles. Assurez-vous que chaque connecteur mâle dans votre système joint un connecteur femelle.
2. «Moins c'est mieux!» Essayez de réduire au minimum le nombre de connecteurs et d'adaptateurs dans la chaîne RF. Chaque connecteur introduit une certaine perte additionnelle d'énergie (jusqu'à quelques dB pour chaque raccordement, selon le type de connecteur utilisé!)
3. «Achetez, ne construisez pas!» Comme nous l'avons mentionné précédemment, essayez dans la mesure du possible d'acheter des câbles qui sont déjà terminés avec les connecteurs dont vous avez besoin. Souder des connecteurs n'est pas une tâche facile et réaliser un bon travail est pratiquement impossible avec des petits connecteurs comme les U.FL et MMCX. Même la terminaison des câbles "mousse" n'est pas tâche facile.

4. N'utilisez pas un BNC pour des fréquences de 2,4GHz ou plus. Utilisez un type de connecteur N (ou SMA, SMB, TNC, etc.)
5. Les connecteurs à micro-ondes sont des pièces faites avec précision, et peuvent facilement être endommagés suite à un mauvais traitement. En règle générale, vous devez tourner la douille externe pour serrer le connecteur, tout en laissant le reste du connecteur (et du câble) immobile. Si d'autres pièces du connecteur se tordent en serrant ou desserrant, des dégâts peuvent facilement se produire.
6. Ne marchez pas sur les connecteurs et ne les laissez pas tomber sur le sol lorsque vous déconnectez des câbles (ceci survient plus souvent que vous pouvez l'imaginez, particulièrement lorsque vous travaillez sur une antenne au dessus d'un toit).
7. N'utilisez jamais des outils comme des pinces pour serrer les connecteurs. Utilisez toujours vos mains. En cas d'utilisation extérieure, rappelez-vous que les métaux augmentent de taille à des températures élevées et réduisent de taille à de basses températures: un connecteur qui a été trop serré peut se dilater en été et se briser en hiver.

# *Antennes et modèles de propagation*

Les antennes sont une composante très importante des systèmes de communication. Par définition, une antenne est un dispositif utilisé pour transformer un signal RF voyageant sur un conducteur en une onde électromagnétique dans l'espace. Les antennes présentent une propriété connue sous le nom de ***réciprocité***, ce qui signifie qu'une antenne maintiendra les mêmes caractéristiques pendant la transmission et la réception. La plupart des antennes sont des dispositifs résonnants et fonctionnent efficacement sur une bande de fréquence relativement étroite. Une antenne doit être accordée à la même bande de fréquence que le système par radio auquel elle est reliée, autrement la réception et la transmission seront altérées. Lorsqu'un signal est introduit dans une antenne, l'antenne émettra un rayonnement distribué dans l'espace d'une certaine manière. On nomme ***modèle de rayonnement*** toute représentation graphique de la distribution relative à la puissance rayonnée dans l'espace.

## Glossaire de termes d'antenne

Avant de nous pencher sur des antennes spécifiques, il y a quelques termes communs qui doivent être définis et expliqués:

## Impédance d'entrée

Pour un transfert efficace d'énergie, l'***impédance*** de la radio, l'antenne et le câble de transmission les reliant doivent être identiques. Des émetteurs-récepteurs et leurs lignes de transmission sont typiquement conçus pour une impédance de 50 Ω. Si l'antenne a une impédance différente à 50 Ω, il y a alors un déséquilibre et un circuit d'assortiment d'impédance est nécessaire. Si n'importe laquelle de ces composantes est mal adaptée, l'efficacité de transmission sera moins bonne.

## Perte de retour

La ***perte de retour*** est une autre manière d'exprimer le déséquilibre. C'est un rapport logarithmique mesuré en dB qui compare la puissance reflétée par l'antenne à la puissance qui est introduite dans l'antenne de la ligne de transmission. Le rapport entre le ROS ou Rapport d'Onde Sationnaire (*SWR-Standing Wave Ratio* en anglais) et la perte de retour est le suivant:

$$\text{Perte de retour (en dB)} = 20\log_{10}\frac{\text{ROS}}{\text{ROS-1}}$$

Tandis que de l'énergie sera toujours reflétée de nouveau dans le système, une perte de retour élevée entraînera un rendement inacceptable de l'antenne.

## Largeur de bande

La ***largeur de bande*** d'une antenne se rapporte à la gamme de fréquences sur laquelle celle-ci peut fonctionner convenablement. La largeur de bande de l'antenne est le nombre d'hertz pour lequel l'antenne montrera un ROS inférieur à 2:1.

La largeur de bande peut également être décrite en termes de pourcentage de la fréquence centrale de la bande.

$$\text{Largeur de bande} = 100 \times \frac{F_H - F_L}{F_C}$$

...Où $F_H$ est la fréquence plus élevée de la bande, $F_L$ est la fréquence la plus basse de la bande et $F_C$ est la fréquence centrale de la bande.

De cette façon, la largeur de bande est à fréquence relative constante. Si la largeur de bande était exprimée en unités absolues de fréquence, elle serait

différente en fonction de la fréquence centrale. Les différents types d'antennes présentent différentes limitations de largeur de bande.

## Directivité et Gain

La ***directivité*** est la capacité d'une antenne à focaliser l'énergie dans une direction particulière au moment de transmettre ou de recueillir l'énergie provenant d'une direction particulière au moment de recevoir. Si un lien sans fil est fixe aux deux extrémités, il est possible d'utiliser la directivité d'antenne pour concentrer le faisceau de rayonnement dans la direction voulue. Dans une application mobile où l'émetteur-récepteur n'est pas fixe, il peut être impossible de prévoir où l'émetteur-récepteur sera, et donc l'antenne devrait, dans la mesure du possible, rayonner dans toutes les directions. Une antenne omnidirectionnelle devrait être utilisée dans ce cas.

Le ***gain*** n'est pas une quantité qui peut être définie en termes de quantité physique tel que le Watt ou l'Ohm, c'est plutôt un rapport sans dimensions. Le gain est donné en référence à une antenne standard. Les deux antennes de référence les plus communes sont l'antenne isotrope et l'antenne dipôle à demi onde résonnante. L'antenne isotrope rayonne aussi bien dans toutes les directions. Les vraies antennes isotropes n'existent pas mais elles fournissent des modèles théoriques utiles et simples d'antenne et nous servent d'outil de comparaison pour les vraies antennes. Dans la vraie vie, toute antenne rayonnera plus d'énergie dans une direction que dans une d'autre. Puisque les antennes ne peuvent pas créer d'énergie, la puissance totale rayonnée est identique à celle d'une antenne isotrope. N'importe quelle énergie additionnelle rayonnée dans les directions favorisées est également compensée par moins d'énergie rayonnée dans toutes les autres directions.

Le gain d'une antenne dans une direction donnée est la quantité d'énergie rayonnée dans cette direction comparée à l'énergie qu'une antenne isotrope rayonnerait dans la même direction avec la même puissance d'entrée. Habituellement nous sommes uniquement intéressés par le gain maximum, qui est le gain dans la direction dans laquelle l'antenne rayonne la majeure partie de la puissance. On écrit **3dBi**, le gain d'une antenne de 3dB comparé à une antenne isotrope. Le dipôle à demi-onde résonnante peut être un standard utile pour comparer à d'autres antennes à une fréquence donnée ou à une bande très étroite de fréquences. Comparer le dipôle à une antenne sur une gamme de fréquences exige un certain nombre de dipôles de différentes longueurs. Un gain d'antenne de 3dB comparé à une antenne de dipôle s'écrit **3dBd**.

La méthode qui consiste à mesurer le gain en comparant l'antenne testée à une antenne standard connue, ayant un gain calibré, est connue comme la technique de ***transfert de gain***. Une autre méthode pour mesurer le gain est la méthode des trois antennes, où la puissance transmise et reçue sur les

bornes d'antenne est mesurée entre trois antennes arbitraires à une distance fixe connue.

## Diagramme de rayonnement

Le ***diagramme de rayonnement*** ou ***diagramme d'antenne*** décrit la force relative du champ rayonné dans diverses directions de l'antenne, à une distance constante. Le modèle de rayonnement est aussi un modèle de réception puisqu'il décrit également les propriétés de réception de l'antenne. Le modèle de rayonnement est tridimensionnel, mais habituellement les modèles de rayonnement mesurés sont une tranche bidimensionnelle du modèle tridimensionnel, dans les plans verticaux ou horizontaux. Ces mesures de modèle sont présentées dans un format ***rectangulaire*** ou ***polaire***. La figure suivante montre un diagramme de rayonnement aux coordonnées rectangulaires d'une antenne Yagi à dix éléments. Le détail est de bonne qualité mais il est difficile de visualiser le comportement d'antenne dans différentes directions.

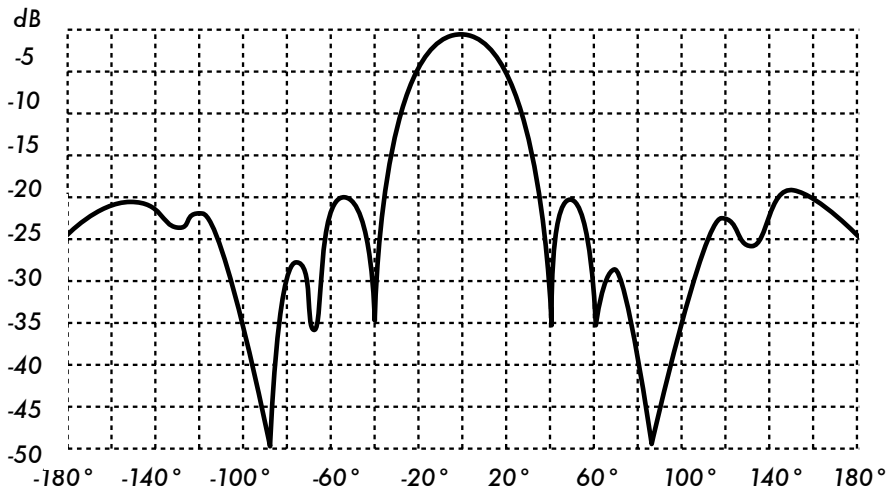


*Figure 4.4: Un diagramme de rayonnement aux coordonnées rectangulaires d'une antenne Yagi.*

Les systèmes de coordonnées polaires sont employés presque universellement. Dans un graphique de coordonné polaire, les points sont situés par projection le long d'un axe tournant (rayon) à une intersection avec un des cercles concentriques. Ce qui suit est un diagramme de rayonnement polaire de la même antenne Yagi à 10 éléments.

Les systèmes de coordonnées polaires peuvent être divisés en deux classes: linéaire et logarithmique. Dans le système de coordonnées linéaires, les cercles concentriques sont équidistants et sont gradués. Une telle grille

peut être employée pour préparer un diagramme de rayonnement linéaire de la puissance contenue dans le signal. Pour rendre plus facile la comparaison, les cercles concentriques équidistants peuvent être remplacés par des cercles convenablement placés représentant la réponse en décibel, référencée à 0 dB au bord externe du diagramme de rayonnement. Dans ce genre de graphique les lobes mineurs sont supprimés. Les lobes avec des crêtes de plus de 15 dB ou très au-dessous du lobe principal disparaissent en raison de leur petite taille. Cette grille améliore les traçages dans lesquelles l'antenne a une directivité élevée et de petits lobes mineurs. La tension du signal, plutôt que la puissance, peut également être tracés sur un système de coordonnées linéaire. Dans ce cas-ci, la directivité sera également augmentée et les lobes mineurs seront supprimés, mais pas au même degré que dans la grille linéaire de puissance.

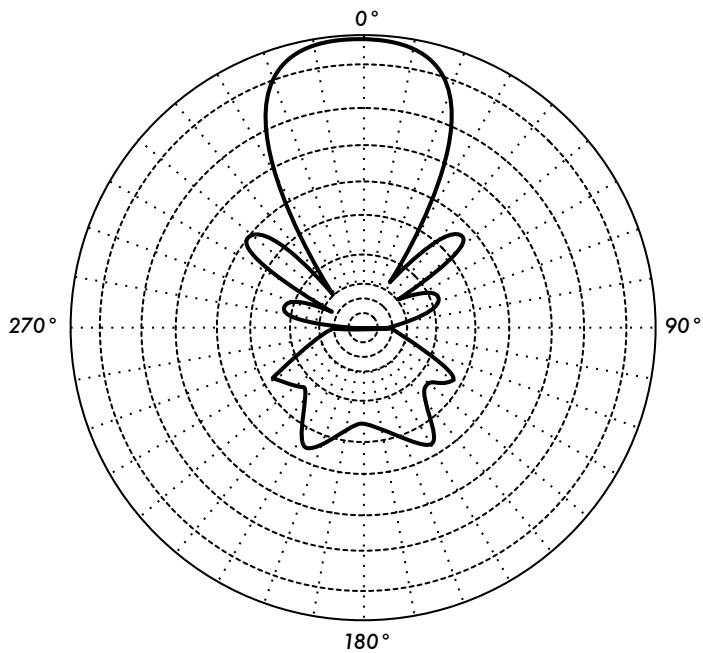


*Figure 4.5: Un diagramme polaire linéaire de la même antenne yagi.*

Dans les systèmes en coordonnées logarithmiques les lignes de grille concentriques sont espacées périodiquement selon le logarithme de la tension dans le signal. Différentes valeurs peuvent être employées pour la constante logarithmique de la périodicité et ce choix aura un effet sur l'aspect des modèles tracés. Généralement les références 0 dB pour le bord externe du diagramme sont employées. Avec ce type de grille, de lobes de 30 ou 40 dB au-dessous du lobe principal sont encore distinguables. L'espacement entre les points à 0 dB et -3 dB est plus grand que l'espacement entre -20 dB et -23 dB, qui est plus grand que l'espacement entre 50 dB et 53 dB.

L'espacement correspond donc ainsi à la signification relative de tels changements dans la performance de l'antenne.

Une balance logarithmique modifiée souligne la forme du faisceau principal tout en comprimant des lobes latéraux de niveau très bas (>30 dB) vers le centre du modèle.

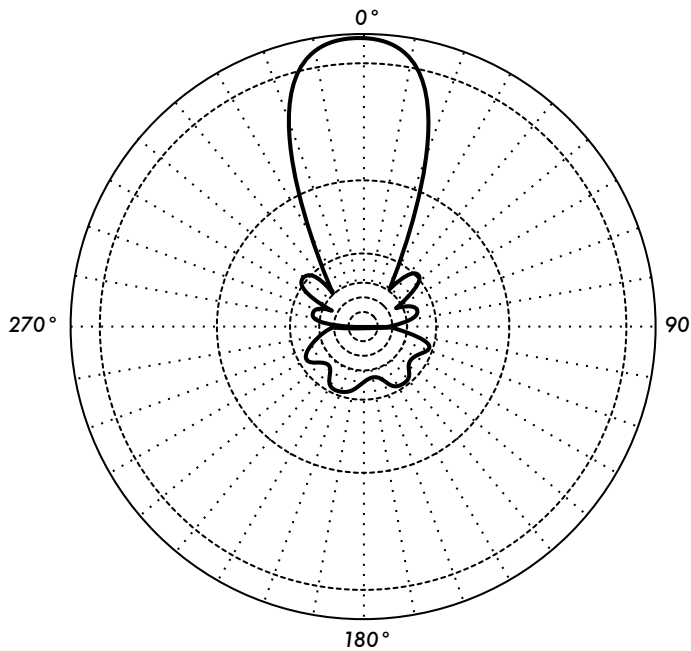


*Figure 4.6: Traçage polaire logarithmique*

Il y a deux genres de diagramme de rayonnement: ***absolu*** et ***relatif***. Des diagrammes de rayonnement absolus sont présentés dans les unités absolues de la force ou de la puissance de champ. Des diagrammes de rayonnement relatifs se retrouvent dans les unités relatives de la force ou de la puissance de champ. La plupart des mesures d'un diagramme de rayonnement font référence à l'antenne isotrope et la méthode de transfert de gain est alors employée pour établir le gain absolu de l'antenne.

Le motif de rayonnement dans la région près de l'antenne n'est pas identique au motif à de grandes distances. Le terme champ-proche se rapporte au modèle de champ qui existe près de l'antenne, alors que le terme champ-lointain se rapporte au modèle de champ à de grandes distances. Le champ-lointain s'appelle également champ de rayonnement et c'est celui qui a généralement plus d'intérêt. Habituellement, c'est la puissance rayonnée qui nous intéresse, c'est pourquoi les modèles d'antenne sont habituellement mesurés dans la région du champ-lointain. Pour la mesure des modèles, il est impor-

tant de choisir une distance suffisamment grande pour être dans le champ-lointain, bien loin du champ-proche. La distance minimum permise dépend des dimensions de l'antenne par rapport à la longueur d'onde. La formule admise pour cette distance est:

$$r_{min} = \frac{2d^2}{\lambda}$$

Où $r_{min}$ est la distance minimum de l'antenne, d la plus grande dimension de l'antenne, et λ est la longueur d'onde.

## Largeur du lobe

Par ***largeur du lobe*** d'une antenne, on entend habituellement la largeur du lobe à demi-puissance. L'intensité maximale de rayonnement est trouvée et alors les points de chaque côté de la crête qui représentent la moitié de la puissance de l'intensité maximale sont localisés. La distance angulaire entre points de demi-puissance est définie comme largeur du lobe. Comme la moitié de la puissance exprimée en décibels est -3dB, la largeur du lobe à demi puissance est parfois désignée sous le nom de la largeur du lobe 3dB. On considère habituellement autant les largeurs de lobe horizontales que les verticales.

Si nous considérons que la plupart de la puissance rayonnée n'est pas divisé en lobes latéraux, le gain directif est donc inversement proportionnel à la largeur du lobe: si la largeur du lobe diminue, le gain direct augmente.

## Lobes latéraux

Aucune antenne ne peut rayonner toute l'énergie dans une direction voulue. Une partie est inévitablement rayonnée dans d'autres directions. Ces plus petites crêtes sont désignées sous le nom de ***lobes latéraux***, généralement présentées en dB en dessous du lobe principal.

## Zéro

Dans un diagramme de rayonnement d'antenne, une zone ***zéro*** est une zone dans laquelle la puissance rayonnée efficace est à un minimum. Un zéro a souvent un angle étroit de directivité comparé à celui du lobe principal. Ainsi, le zéro est utile à plusieurs fins, telle que la suppression des signaux d'interférence dans une direction donnée.

## Polarisation

La ***polarisation*** est définie comme étant l'orientation du champ électrique d'une onde électromagnétique. La polarisation est en général décrite par une ellipse. La polarisation linéaire et la polarisation circulaire sont deux cas spéciaux de polarisation elliptique. La polarisation initiale d'une onde radio est déterminée par l'antenne.

Avec la polarisation linéaire, le vecteur de champ électrique reste tout le temps dans le même plan. Le champ électrique peut laisser l'antenne dans une orientation verticale, une orientation horizontale ou dans un angle entre les deux. Le rayonnement ***verticalement polarisé*** est légèrement moins affecté par des réflexions dans le chemin de transmission. Les antennes omnidirectionnelles ont toujours une polarisation verticale. Avec la polarisation horizontale, de telles réflexions causent des variations dans la force du signal reçu. Les antennes horizontales sont moins sensibles aux interférences causées par les humains car celles-ci sont généralement polarisées verticalement.

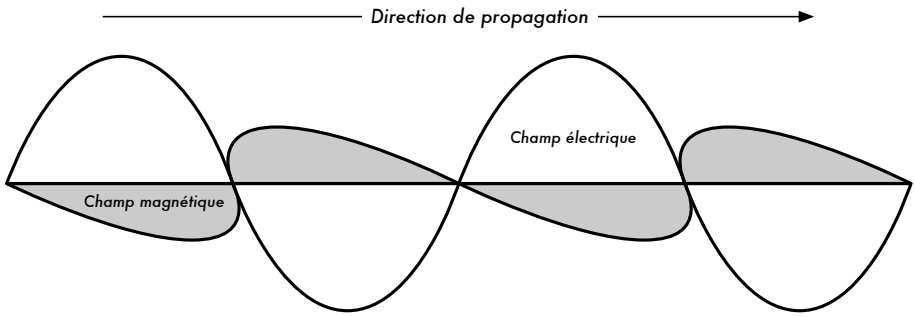


*Figure 4.7: L'onde sinusoïdale électrique se déplace en direction perpendiculaire par rapport à l'onde magnétique dans la direction de la propagation*

Dans la polarisation circulaire, le vecteur de champ électrique semble tourner avec le mouvement circulaire autour de la direction de la propagation, faisant un plein tour pour chaque cycle RF. Cette rotation peut être réalisée à droite ou à gauche. Le choix de la polarisation est l'un des choix de conception disponibles pour le concepteur du système RF.

## Déséquilibre de polarisation

Afin de transférer la puissance maximum entre une antenne de transmission et une antenne de réception, les deux antennes doivent avoir la même orientation spatiale, le même sens de polarisation et le même rapport axial.

Lorsque les antennes ne sont pas alignées ou n'ont pas la même polarisation, il y aura une réduction de transfert de puissance entre elles. Cette réduction de transfert de puissance réduira l'efficacité globale du système.

Lorsque les antennes de transmission et de réception sont toutes deux linéairement polarisées, une déviation de l'alignement physique de l'antenne entraînera une perte par déséquilibre de polarisation, ce qui peut être calculé en utilisant la formule suivante:

$$\text{Perte (dB)} = 20 \log (\cos \theta)$$

...Où θ est la différence dans l'angle d'alignement entre les deux antennes. Pour 15° la perte est approximativement de 0,3dB, pour 30° nous perdons 1,25dB, pour 45° nous perdons 3dB et pour 90° nous avons une perte infinie.

En résumé, plus le déséquilibre dans la polarisation entre une antenne de transmission et de réception est grand, plus la perte apparente est grande. En pratique, un déséquilibre de 90° dans la polarisation est un déséquilibre important mais non infini. Certaines antennes, telles que les yagis ou les antennes de bidon, peuvent simplement être tournées 90° pour assortir la polarisation à l'autre extrémité du lien. Vous pouvez employer l'effet de polarisation à votre avantage sur un point pour diriger le lien. Utilisez un outil de surveillance pour observer l'interférence des réseaux adjacents, et tournez une antenne jusqu'à ce que vous perceviez le plus bas signal reçu. Puis, placer votre lien en ligne et orientez l'autre extrémité afin d'équilibrer la polarisation. Cette technique peut parfois être employée pour établir des liens stables même dans les environnements de radio bruyants.

### Rapport avant-arrière

Il est souvent utile de comparer le ***rapport avant-arrière*** des antennes directionnelles. C'est le rapport de la directivité maximum d'une antenne à sa directivité dans la direction opposée. Par exemple, quand le modèle de rayonnement est tracé sur une échelle relative en dB, le rapport avant-arrière est la différence en dB entre le niveau du rayonnement maximum dans la direction vers l'avant et le niveau du rayonnement à 180 degrés.

Ce nombre n'a aucune importance pour une antenne omnidirectionnelle mais il vous donne une idée de la quantité de puissance dirigée vers l'avant sur une antenne directionnelle.

## Types d'Antennes

On peut réaliser un classement des différentes antennes selon les caractéristiques suivantes:

- **Fréquence et taille**. Les antennes utilisées pour les HF sont différentes des antennes utilisées pour les VHF, qui sont à leur tour différentes des antennes utilisées pour les micro-ondes. Puisque la longueur d'onde varie fréquences, les antennes doivent avoir des tailles différentes afin de ray-

onner des signaux à la bonne longueur d'onde. Nous sommes particulièrement intéressés par les antennes fonctionnant dans la gamme des micro-ondes, particulièrement dans les fréquences de 2,4 gigahertz et de 5 gigahertz. À 2,4 gigahertz la longueur d'onde est de 12,5cm alors qu'à 5 gigahertz elle est de 6cm.

- **Directivité**. Les antennes peuvent être omnidirectionnelles, sectorielles ou directives. Les a***ntennes omnidirectionnelles*** rayonnent approximativement le même modèle tout autour de l'antenne dans un modèle complet de 360°. Les types d'antennes omnidirectionnelles les plus populaires sont le ***dipôle*** et le ***ground plane***. Les ***antennes sectorielles*** rayonnent principalement dans un secteur spécifique. Le faisceau peut être aussi large que 180 degrés ou aussi étroit que 60 degrés. Les ***antennes directionnelles*** sont des antennes pour lesquelles la largeur de faisceau est beaucoup plus étroite que dans les antennes sectorielles. Elles ont un gain plus élevé et sont donc employées pour des liens de longue distance. Les types d'antennes directives sont les Yagi, les biquad, les cornets, les hélicoïdales, les antennes patch, les antennes paraboliques, et plusieurs autres.
- **Construction physique**. Des antennes peuvent être construites de plusieurs façons différentes, allant des simples fils aux antennes paraboliques en passant par les boîtes de conserve.

Lorsque nous considérons des antennes appropriées pour un usage WLAN de 2,4 GHz, une autre classification peut être employée:

- **Application**. Les points d'accès tendent à faire des réseaux point-à-multipoint, tandis que les liens à distance sont point-à-point. Ces deux types de réseaux requièrent différents types d'antennes pour arriver à leur but. Les noeuds qui sont employés pour l'accès multipoint utiliseront probablement des antennes omnidirectionnelles qui rayonnent également dans toutes les directions ou des antennes sectorielles qui focalisent sur un petit secteur. Dans le cas d'un réseau point–à-point, les antennes sont utilisées pour relier deux endroits ensemble. Les antennes directionnelles sont le meilleur choix pour ce type d'application.

Nous allons vous présenter une brève liste de type d'antennes courantes pour la fréquence de 2,4 gigahertz avec une courte description ainsi que des informations de base sur leurs caractéristiques.

## Antenne ground-plane d'un quart de longueur d'onde

L'antenne groud-plane d'un quart de longueur d'onde se construit très facilement et elle est utile quand la taille, le coût et la facilité de la construction sont importants. Cette antenne est conçue pour transmettre un signal verticalement polarisé. Elle consiste en un élément d'un quart d'onde comme une moitié dipolaire et de trois ou quatre éléments de surface d'un quart de

longueur d'onde plié de 30 à 45 degrés vers le bas. Cet ensemble d'éléments, appelés les radiaux, est connu comme la base planaire (ground plane). C'est une antenne simple et efficace qui peut capturer un signal provenant de toutes les directions également. Pour augmenter le gain, le signal peut être aplani pour ôter le focus du dessus et du dessous et fournir plus de focus sur l'horizon. La largeur de faisceau verticale représente le degré d'aplanissement dans le focus. Ceci est utile dans une situation Point-à-Multipoint, si toutes les autres antennes sont également à la même hauteur. Le gain de cette antenne est de l'ordre de 2 – 4 dBi.

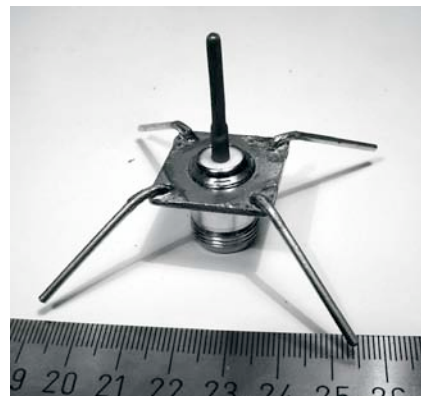


*Figure 4.8: Antenne groud-plane d'un quart de longueur d'onde.*

## Antenne Yagi

Une Yagi de base se compose d'un certain nombre d'éléments droits, chacun mesurant approximativement une demi longueur d'onde. L'élément actif d'une Yagi est l'équivalent d'une antenne dipolaire à demi onde à alimentation centrale. Parallèlement à l'élément actif et approximativement à 0,2 - 0,5 fois la longueur d'onde, de chaque côté se trouvent les tiges ou les fils droits appelés les réflecteurs et les directeurs ou simplement les éléments passifs. Un réflecteur est placé derrière l'élément conduit et est légèrement plus long que la moitié d'une longueur d'onde; un directeur est placé devant l'élément conduit et est légèrement plus court que la moitié d'une longueur d'onde. Une Yagi typique a un réflecteur et un ou plusieurs directeurs. L'antenne propage l'énergie de champ électromagnétique dans la direction qui va de l'élément conduit vers les directeurs et est plus sensible à l'énergie de champ électromagnétique entrant dans cette même direction. Plus une Yagi a de directeurs, plus le gain est grand. La photo suivante montre une antenne Yagi avec 6 directeurs et un réflecteur.

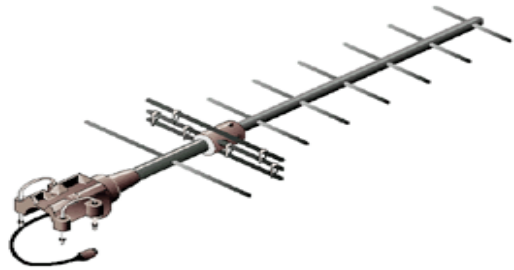

*Figure 4.9: Une antenne Yagi.*

Les antennes Yagi sont principalement utilisées pour des liens point-à-point. Elles ont un gain de 10 à 20 dBi et une largeur de faisceau horizontal de 10 à 20 degrés.

## Antenne cornet

L'antenne cornet (*horn*) tient son nom de son aspect caractéristique en forme de cornet. La partie évasée peut être à angle droit, rectangulaire, cylindrique ou conique. La direction du rayonnement maximum correspond à l'axe du cornet. Elle est facilement alimentée avec un guide d'ondes, mais peut être alimentée avec un câble coaxial et une transition appropriée. Les antennes cornet sont généralement utilisées comme élément actif dans une antenne parabolique. Le cornet est pointée vers le centre du réflecteur. L'utilisation d'une antenne cornet, plutôt qu'une antenne dipolaire ou n'importe quel autre type d'antenne au point focal du réflecteur, réduit au minimum la perte d'énergie autour des bords du réflecteur. À 2,4 gigahertz, une antenne cornet faite avec une boîte de conserve a un gain de l'ordre de 10 à 15 dBi.

*Figure 4.10: Antenne cornet faite à partir d'une boîte de conserve.*

## Antenne parabolique

Les antennes basées sur des réflecteurs paraboliques sont le type le plus commun d'antennes directives quand un gain élevé est exigé. Leur avantage

principal réside dans le fait qu'elles peuvent être construites afin de disposer d'un gain et d'une directivité aussi grands que souhaités. L'inconvénient principal est que ce type d'antenne est difficile à installer et se retrouve souvent à la merci du vent.

Les paraboles, jusqu'à un mètre, sont habituellement faits de matériel solide. L'aluminium est fréquemment employé pour l'avantage qu'il confère par rapport à son poids, sa longévité et ses bonnes caractéristiques électriques. L'effet du vent s'accroît rapidement avec la taille de la parabole et peut rapidement devenir un grave problème. Des paraboles d'une surface refléchissante employant un maillage ouvert sont fréquemment employés. Ceux-ci ont un moins bon rapport avant-arrière mais sont plus sûrs et plus facile à construire. Le cuivre, l'aluminium, le laiton, l'acier galvanisé et le fer peuvent être utilisés lors de la construction d'une parabole maillée.

*Figure 4.11: Un réflecteur d'antenne parabolique solide.*

## BiQuad

L'antenne BiQuad peut se construire facilement et offre une bonne directivité et un bon gain pour des communications point-à-point. Elle se compose de deux carrés de la même taille d'un quart de longueur d'onde comme élément de rayonnement et d'un plat ou d'une grille métallique comme réflecteur. Cette antenne a une largeur de faisceau d'environ 70 degrés et un gain de l'ordre de 10-12 dBi. Elle peut être employée en tant qu'antenne autonome ou comme conducteur pour un réflecteur parabolique. La polarisation est telle qu'en regardant l'antenne de l'avant, si les carrés sont placés côte à côte, la polarisation est verticale.

*Figure 4.12: Une BiQuad.*

### Autres antennes

Il existe plusieurs autres types d'antennes et de nouvelles sont créés suivant l'avancement technologique.

- Antennes de secteur ou sectorielles: elles sont largement répandues en infrastructure de téléphonie cellulaire et sont habituellement construites en ajoutant un plat réflécteur à un ou plusieurs dipôles mis en phase. Leur largeur de faisceau horizontale peut être aussi large que 180 degrés, ou aussi étroite que 60 degrés, alors que la verticale est habituellement beaucoup plus étroite. Des antennes composées peuvent être construites à l'aide de plusieurs antennes sectorielles pour avoir une portée horizontale plus grande (antenne multisectorielle).

Antennes panneau ou *patch*: ce sont des panneaux solides plats utilisés pour une couverture intérieure avec un gain de jusqu'à 20 dB.

## Théorie de réflexion

La propriété de base d'un réflecteur parabolique parfait est qu'il convertit une vague sphérique irradiant d'une source placée au foyer en une onde plane. Réciproquement, toute l'énergie reçue par la parabole d'une source éloignée est reflétée à un seul point au centre. La position du foyer, ou la longueur focale, est donnée par la formule suivante:

$$f = \frac{D^2}{16 \times c}$$

...Où D est le diamètre du plat et c est la profondeur de l'antenne parabolique en son centre.

La taille du réflecteur est le facteur le plus important puisqu'elle détermine le gain maximum qui peut être réalisé à la fréquence donnée et à la largeur de faisceau résultante. Le gain et la largeur de faisceau obtenus sont montrés dans la formule suivante:

$$\text{Gain} = \frac{(\pi \times D)^2}{\lambda^2} \times n$$

$$\text{Largeur du Faisceau} = \frac{70\ \lambda}{D}$$

... où D est le diamètre du réflecteur et n est l'efficacité. L'efficacité est déterminée principalement par l'efficacité de l'illumination du réflecteur par la source, mais également par d'autres facteurs. Chaque fois que le diamètre du réflecteur est doublé, le gain est quadruplé, soit 6 dB de plus. Si les deux stations doublent la taille de leurs plats, la force du signal peut être augmentée de 12 dB, un gain très substantiel. Une efficacité de 50% peut être supposée lorsque l'antenne est faite à la main.

Le rapport F/D (longueur focale / diamètre du réflecteur) est le facteur fondamental régissant la conception de la source. Le rapport est directement lié à la largeur de faisceau de la source nécessaire pour illuminer le réflecteur efficacement. Deux réflecteur du même diamètre mais de différentes longueurs focales exigent une conception différente de la source si nous désirons que tous les deux soient illuminés efficacement. La valeur de 0,25 correspond à la parabole habituelle plan-focal dans lequel le foyer est dans le même plan que le bord du réflecteur.

# *Amplificateurs*

Comme nous l'avons mentionné précédemment, les antennes ne créent pas réellement de puissance. Elles dirigent simplement toute la puissance disponible dans un modèle particulier. En utilisant un ***amplificateur de puissance***, vous pouvez employer la puissance DC afin d'augmenter votre signal disponible. Un amplificateur s'installe entre un radio émetteur et une antenne, ainsi qu'à un câble additionnel qui se relie à une source d'énergie. Les amplificateurs peuvent fonctionner à 2,4 GHz et peuvent ajouter plusieurs watts de puissance à votre transmission. Ces dispositifs peuvent sentir quand une radio transmet et, lorsque ceci se produit, ils s'allument rapidement pour amplifier le signal. Lorsque la transmission prend fin, ils s'éteignent. En réception, ils ajoutent également de l'amplification au signal avant de l'envoyer à la radio.

Malheureusement, le fait d'ajouter simplement des amplificateurs ne résoudra pas comme par magie tous vos problèmes de gestion de réseau. Nous ne traiterons pas longuement des amplificateurs de puissance au sein de ce livre car leur emploi soulève un certain nombre d'inconvénients significatifs:

- **Ils sont chers**. Les amplificateurs doivent fonctionner à des largeurs de bande relativement larges à 2,4 GHz, et doivent commuter assez rapidement pour fonctionner avec les applications Wi-Fi. Ces amplificateurs existent mais coûtent plusieurs centaines de dollars par unité.
- **Vous aurez besoin d'au moins deux amplificateurs**. Alors que les antennes fournissent un gain réciproque qui bénéficie les deux côtés d'un raccordement, les amplificateurs fonctionnent mieux pour amplifier un signal transmis. Si vous n'ajoutez qu'un amplificateur à la fin d'un lien avec un gain d'antenne insuffisant, celle-ci pourra probablement être entendue mais ne pourra pas entendre l'autre extrémité.
- **Ils ne fournissent aucune directivité additionnelle**. Ajouter un gain à une antenne fournit des avantages de gain et de directivité aux deux fins du lien. Elles améliorent non seulement la quantité disponible de signal, mais tendent à rejeter le bruit provenant d'autres directions. Les amplificateurs amplifient aveuglément les signaux désirés et les interférences, et peuvent empirer les problèmes d'interférence.
- **Les amplificateurs produisent du bruit pour les autres utilisateurs de la bande**. En augmentant votre puissance de rendement, vous créez une source plus forte de bruit pour les autres utilisateurs de la bande sans licence. Ceci ne pose peut-être pas de problème pour les zones rurales, mais peut certainement en poser pour des secteurs plus peuplés. Au contraire, ajouter un gain d'antenne améliorera votre lien et peut réellement diminuer le niveau de bruit pour vos voisins.
- **L'utilisation des amplificateurs n'est probablement pas légale**. Chaque pays impose des limites de puissance à l'utilisation du spectre sans licence. Ajouter une antenne à un signal fortement amplifié fera probablement dépasser le lien des limites légales.

L'utilisation des amplificateurs est souvent comparée au voisin sans gêne qui veut écouter sa radio en dehors de sa maison et tourne donc le volume au maximum. Il pourrait même « améliorer » la réception en plaçant des haut-parleurs en-dehors de la fenêtre. À présent, ce voisin peut certes écouter sa radio mais il en va de même pour tout le monde vivant dans le voisinage. Nous venons d'illustrer ce qui se produit avec un seul utilisateur, mais que se produit-il lorsque les autres voisins décident de faire de même avec leurs radios? L'utilisation des amplificateurs pour un lien sans fil cause approximativement le même effet à 2,4 GHz. Votre lien peut «mieux fonctionner» pour le moment mais vous aurez des ennuis lorsque d'autres utilisateurs de la bande décideront également d'utiliser des amplificateurs.

En utilisant des antennes de gain plus élevé plutôt que des amplificateurs, vous évitez tous ces problèmes. Les antennes coûtent beaucoup moins cher que les amplificateurs et vous pouvez améliorer un lien en changeant simplement l'antenne à une extrémité. Le fait d'employer des radios plus sensibles et un câble de bonne qualité aide également de manière significative pour les liaisons de longue distance. Comme ces techniques sont peu susceptibles de poser des problèmes pour les autres utilisateurs de la bande, nous vous recommandons de les considérer avant de penser à ajouter des amplificateurs.

# Conception pratique d'antennes

Le coût des antennes à 2,4 GHz a chuté depuis l'introduction du 802.11b. Les conceptions novatrices emploient des pièces plus simples et peu de matériaux pour obtenir un gain impressionnant avec très peu de machinerie. Malheureusement, la disponibilité de bonnes antennes est encore limitée dans plusieurs régions du monde, et leur coût d'importation est souvent prohibitif. Alors que concevoir une antenne peut être un processus complexe passible d'erreurs, la construction d'antennes à l'aide de composantes disponibles localement est non seulement simple mais peut aussi devenir une expérience amusante. Nous allons vous présenter quatre modèles pratiques d'antennes qui peuvent être construites à peu de frais.

## Antenne parabolique ayant une clef sans fil USB comme source

La conception d'antenne probablement la plus simple est l'utilisation d'une parabole pour diriger la sortie d'un dispositif sans fil USB (mieux connu dans le milieu du réseau sans fil comme ***USB dongle***). En plaçant l'antenne interne dipolaire présente dans les clefs sans fil USB au foyer de la parabole, vous pouvez obtenir un gain significatif sans avoir besoin de souder ou même d'ouvrir le dispositif sans fil lui-même. Plusieurs types de plats paraboliques peuvent fonctionner y compris les antennes paraboliques, les antennes de télévision et même les ustensiles de cuisine en métal (tel qu'un wok, un couvercle rond ou un tamis). En prime, il est possible d'employer le câble USB qui est peu coûteux et sans perte afin d'alimenter l'antenne, éliminant du même coup le besoin de câbles trop coûteux comme le câble coaxial ou heliax.

Pour construire une clef USB parabolique, vous devrez trouver l'orientation et la position du dipôle à l'intérieur de la clef. La plupart des dispositifs orientent le dipôle pour que celui-ci soit parallèle au bord court de la clef mais d'autres le dispose de manière perpendiculaire au bord court. Soit vous ouvrez la clef pour voir par vous-même, soit vous essayez simplement la clef dans les deux positions pour voir ce qui fournit le plus de gain.

Pour examiner l'antenne, dirigez-la vers un point d'accès à plusieurs mètres de distance et reliez la clef USB à un ordinateur portable. En utilisant le pilote de l'ordinateur portable ou un outil tel que Netstumbler (voir le chapitre six), observez la force du signal reçu de votre point d'accès. Maintenant, déplacez lentement la clef par rapport au plat parabolique tout en observant la mesure de la force du signal. Vous devriez voir une amélioration significative de gain (20 dB ou plus) lorsque vous trouvez la position appropriée. Le dipôle lui-même est typiquement placé à 3-5 centimètres de l'arrière du plat, quoique ceci puisse changer en fonction de la forme de la parabole. Essayez diverses positions tout en observant la force du signal jusqu'à ce que vous trouviez l'emplacement optimum.

Une fois que le meilleur emplacement est trouvé, fixez solidement la clef en place. Vous devrez imperméabiliser la clef et le câble si l'antenne est utilisée à l'exterieur. Utilisez un composé de silicone ou un morceau de tuyauterie de PVC pour protéger les éléments électroniques des intempéries. Vous retrouverez plusieurs conceptions paraboliques de source USB ainsi que diverses idées à l'adresse suivante: *http://www.usbwifi.orcon.net.nz/*.

## Omni colinéaire

Il est très simple de construire cette antenne: elle n'exige qu'un morceau de fil de fer, une douille N et une plaque métallique carrée. Elle peut être employée pour une couverture de courte distance point-à-multipoint intérieure ou extérieure. La plaque a un trou au milieu pour y visser le châssis de la douille de type N. Le fil de fer est soudé à la broche centrale de la douille N et dispose de spirales pour séparer les éléments actifs en phases. Deux versions de l'antenne sont possibles: une avec deux éléments en phase et deux spirales et une autre avec quatre éléments en phase et quatre spirales. Pour l'antenne courte le gain sera d'autour de 5 dBi, alors que pour l'antenne à quatre éléments, le gain sera de 7 à 9 dBi. Nous décrirons uniquement comment construire l'antenne longue.

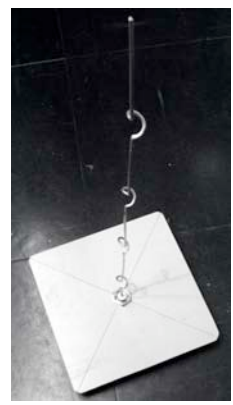

*Figure 4.13: L'antenne omni colinéaire complète*

## Liste de composantes

- Un connecteur femelle de type N à visser
- 50 centimètres de fil de cuivre ou en laiton de 2 millimètres de diamètre
- Une plaque métallique carrée de 10x10 centimètres ou plus

*Figure 4.14: Plaque d'aluminium de 10 cm x 10 cm*

## Outils requis

- Règle
- Pinces
- Lime
- Étain et fer à souder
- Perceuse avec un ensemble de mèches pour métal (incluant une mèche de1,5 centimètre de diamètre)
- Un morceau de tuyau ou une perceuse avec un diamètre de 1 cm
- Étau ou pince
- Marteau
- Clé anglaise

## Construction

1. Redressez le fil de fer en utilisant l'étau ou la pince.

*Figure 4.15: Rendez le fil de fer aussi droit que possible.*

2. Avec un marqueur, tracez une ligne à 2,5 centimètres à partir d'une extrémité du fil. Sur cette ligne, pliez le fil à 90 degrés à l'aide de la pince et du marteau.

*Figure 4.16: Frapper doucement sur le fil pour faire une courbe fermée.*

3. Tracez une autre ligne à une distance de 3,6 centimètres de la courbe. En utilisant la pince et le marteau, pliez de nouveau l'excédent de fil dans cette deuxième ligne à 90 degrés dans la direction opposée à la première courbe mais dans le même plan. Le fil devrait ressembler à un « Z ».


*Figure 4.17: Plier le fil en forme de « Z ».*

4. Nous tordrons maintenant la partie « Z » du fil pour faire une boucle d'un centimètre de diamètre. Pour ce faire, nous emploierons le tuyau ou la perceuse et courberons le fil autour d'un de ceux-ci, avec l'aide de l'étau et des pinces.


*Figure 4.18: Courber le fil autour de la perceuse pour faire une boucle.*

La boucle ressemblera à ceci:

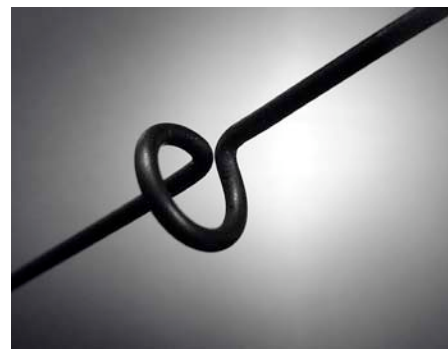

*Figure 4.19: La boucle complète.*

5. Vous devriez faire une deuxième boucle à une distance de 7,8 centimètres de la première. Les deux boucles devraient avoir la même direction de rotation et devraient être placées du même côté du fil. Faites une troisième et quatrième boucle suivant le même procédé, à la même dis-

tance de 7,8 centimètres l'une de l'autre. Coupez le dernier élément en phase à une distance de 8,0 centimètres à partir de la quatrième boucle.

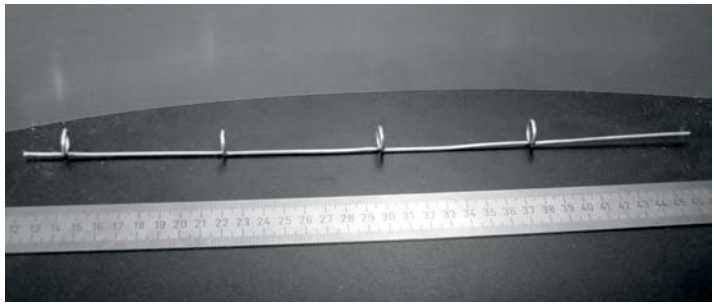

*Figure 4.20: Essayer de le maintenir le plus droit que possible*

Si les boucles ont été faites correctement, il devrait être possible de traverser toutes les boucles avec un tuyau tel qu'illustré à la suite.

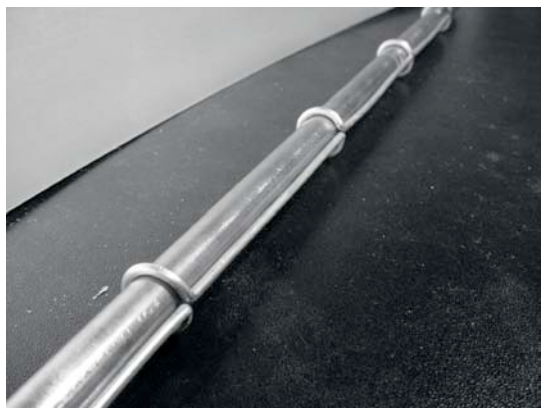

*Figure 4.21: L'insertion d'un tuyau peut aider à redresser le fil.*

6. Avec un marqueur et une règle, dessinez les diagonales du plat métallique trouvant son centre. Avec une mèche de petit diamètre, faites un trou pilote au centre de la plaque. Augmentez le diamètre du trou en utilisant des mèches avec des diamètres plus grands.

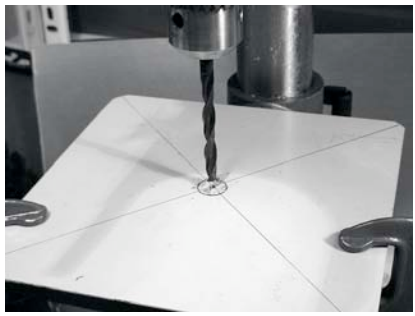

*Figure 4.22: Percer un trou dans la plaque métallique.*

Le trou devrait être exactement adapté au connecteur N. Employez une pince si nécessaire

.

*Figure 4.23: Le connecteur N doit entrer parfaitement dans le trou.*

7. Pour avoir une impédance d'antenne de 50 Ohms, il est important que la surface visible de l'isolateur interne du connecteur (le secteur blanc autour de la broche centrale) soit au même niveau que la surface de la plaque. Pour ce faire, coupez 0,5 centimètre d'un tuyau de cuivre avec un diamètre externe de 2 centimètres et placez-le entre le connecteur et la plaque.

*Figure 4.24: Ajouter un tuyau de cuivre comme entretoise aide à obtenir une impédance d'antenne de 50 Ohms.*

8. Vissez l'écrou au connecteur pour le fixer fermement à la plaque à l'aide de la clé anglaise.

*Figure 4.25: Fixez étroitement le connecteur N à la plaque.*

9. Lissez avec la lime le côté du fil qui est à 2,5 centimètres de la première boucle. Soudez le fil à environ 0,5 centimètre à l'extrémité lisse avec l'aide de l'étau ou de la pince.

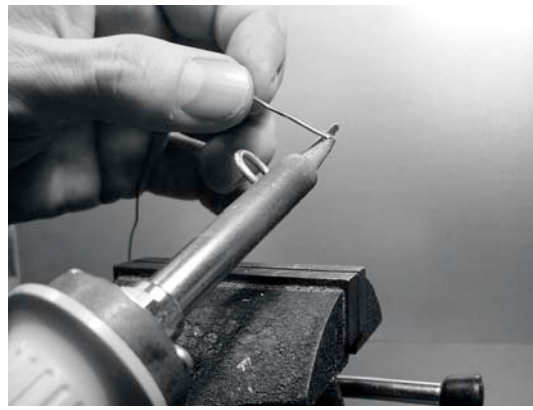

*Figure 4.26: Ajouter un peu d'étain à l'extrémité du fil avant de le souder.*

10. Avec le fer à souder, étamez la broche centrale du connecteur. En maintenant le fil vertical avec les pinces, soudez l'extrémité à laquelle vous avez ajouté l'étain dans le trou de la broche centrale. La première boucle devrait se situer à 3,0 centimètres de la plaque.


*Figure 4.27: La première boucle devrait commencer à 3,0 centimètres de la surface de la plaque.*

11. Nous allons maintenant étirer les boucles en étendant la longueur verticale totale du fil. Pour ce faire, nous utiliserons l'étau et les pinces. Vous devriez étirer le câble de sorte que la longueur finale de la boucle soit de 2,0 centimètres.

*Figure 4.28: Étirer les boucles. Procédez en douceur et essayer de ne pas érafler la surface du fil avec les pinces.*

12. Répétez la même procédure pour les autres trois boucles en étirant leur longueur à 2,0 centimètres.

*Figure 4.29: Répétez la même procédure «d'étirement» pour les boucles restantes.*

13. L'antenne devrait finalement mesurer 42,5 centimètres du plat au sommet.

*Figure 4.30: L'antenne finale devrait mesurer 42,5 cm de la plaque à l'extrémité du fil.*

14. Si vous avez un Analyseur de Spectre avec un Générateur de Piste et un Coupleur Directionnel, vous pouvez vérifier la courbe de la puissance reflétée de l'antenne. L'image ci-dessous montre l'affichage de l'analyseur de spectre.

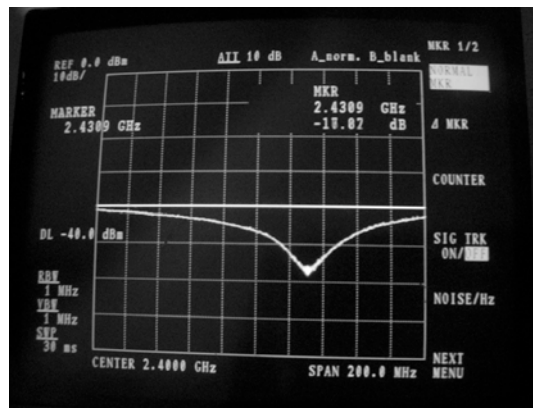


*Figure 4.31: Un traçage du spectre de la puissance reflétée de l'antenne colinéaire omnidirectionnelle.*

Si vous avez l'intention d'utiliser cette antenne à l'extérieur, vous devrez la protéger contre les intempéries. La méthode la plus simple est de l'enfermer dans un grand morceau de tuyau de PVC fermé avec des couvercles. Coupez un trou au fond pour la ligne de transmission et scellez l'antenne avec du silicone ou de la colle de PVC.

## Cantenna

Cette antenne, parfois nommée Cantenna, utilise une boîte de conserve comme guide d'ondes et un fil court soudés à un connecteur N comme sonde pour la transition du câble coaxial vers le guide d'ondes. Elle peut être facilement construite en recyclant une boîte de conserve de jus ou tout autre aliment et ne coûte que le prix du connecteur. C'est une antenne directionnelle utile pour les liens points-à-points de courte à moyenne distance. Elle peut également être employée comme source pour une plaque ou une grille parabolique.

Notez que ce ne sont pas toutes les boîtes de conserves qui peuvent être utilisées pour construire ce type antenne. Certaines contraintes dimensionnelles s'appliquent:

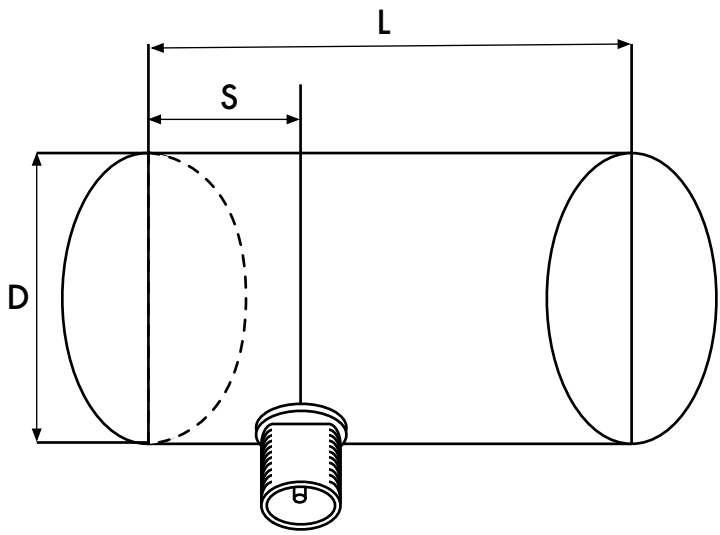


*Figure 4.32: Contraintes dimensionnelles de la Cantenna*

1. Les valeurs acceptables pour le diamètre D de l'alimentation sont entre 0,60 et 0,75 fois la longueur d'onde dans l'air pour une fréquence désignée. À 2,44 gigahertz, la longueur d'onde λ est de 12,2 centimètres donc le diamètre de la boîte de conserve devrait être dans la gamme de 7,3 - 9,2 centimètres.
2. T La longueur L de la boîte de conserve devrait préférablement être d'au moins 0,75 $\lambda_{G,}$ où $\lambda_G$ est la longueur d'onde du guide et est donnée selon la formule suivante:

$$\lambda_G = \frac{\lambda}{\sqrt{(1 - (\lambda / 1{,}706D)^2)}}$$

Pour D = 7,3 centimètres, nous avons besoin d'une boîte de conserve d'au moins 56,4 centimètres, alors que pour D = 9,2 centimètres nous avons besoin d'une boîte de conserve d'au moins 14,8 centimètres. Généralement plus le diamètre est petit, plus la boîte de conserve devrait être longue. Pour notre exemple, nous utiliserons les boîtes d'huile qui ont un diamètre de 8,3 centimètres et une taille d'environ 21 centimètres.

3. La sonde pour la transition du câble coaxial au guide d'ondes devrait être placée à une distance S du fond de la boîte de conserve. Ainsi:

$$S = 0,25\ \lambda_G$$

Sa longueur devrait être de 0,25 λ, ce qui correspond à 3,05 centimètres à 2,44 GHz.

Le gain pour cette antenne sera de l'ordre de 10 à 14 dBi, avec une largeur de faisceau d'environ 60 degrés.


*Figure 4.33: Une cantenna finalisée.*

## Liste des composants

- Un connecteur femelle de type N à visser
- 4 centimètres de fil de cuivre ou de laiton de 2 millimètres de diamètre
- Une boîte d'huile de 8,3 centimètres de diamètre et 21 centimètres de hauteur


*Figure 4.34: Composantes requises pour une cantenna.*

## Outils requis

- Ouvre-boîte
- Règle
- Pinces
- Lime
- Fer à souder
- Étain
- Perceuse avec un ensemble de mèches pour métal (avec une mèche de 1,5 centimètres de diamètre)
- Étau ou pince
- Clé anglaise
- Marteau
- Poinçon

## Construction

1. À l'aide de l'ouvre-boîte, enlevez soigneusement la partie supérieure de la boîte de conserve.


*Figure 4.35: Faîtes attention aux rebords tranchants lorsque vous ouvrez la boîte de conserve.*

Le disque circulaire a un bord très tranchant. Faites attention en le manipulant! Videz la boîte de conserve et lavez-la avec du savon. Si cette boîte contient de l'ananas, des biscuits ou tout autre festin savoureux, partagez le avec un ami.

2. Avec la règle, mesurez 6,2 centimètres à partir du fond de la boîte de conserve et marquez un point. Faites attention de bien mesurer à partir du côté intérieur du fond. Utilisez un poinçon (ou une perceuse avec une petite mèche ou un tournevis Phillips) et un marteau pour marquer le point. Ceci facilitera un perçage précis du trou. Faites attention de ne pas changer la forme de la boîte de conserve en y insérant un petit bloc de bois ou de tout autre objet avant de frapper dessus.


*Figure 4.36: Marquez le trou avant de percer.*

3. Avec une mèche de petit diamètre, faites un trou pilote. Augmentez le diamètre du trou en augmentant le diamètre de la mèche. Le trou devrait parfaitement s'adapter au connecteur N. Utilisez la lime pour lisser le

bord du trou et pour enlever toute trace de peinture afin d'assurer un meilleur contact électrique avec le connecteur.

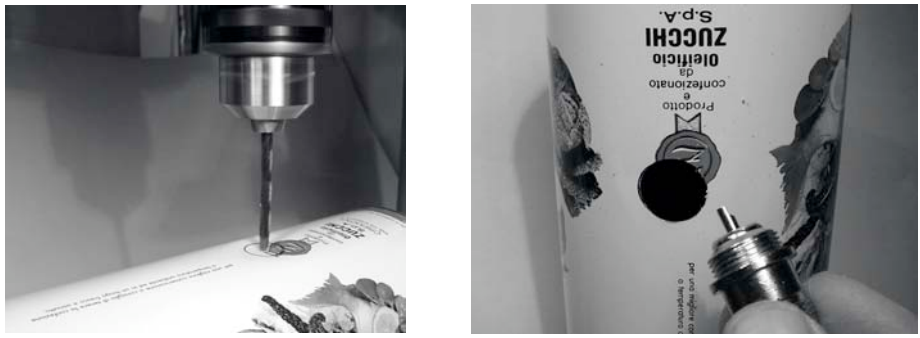


*Figure 4.37: Percez soigneusement un trou pilote, puis utilisez une mèche plus grande pour terminer le travail.*

4. Lissez avec la lime une extrémité du fil. Étamez le fil à environ 0,5 centimètre à la même extrémité à l'aide de l'étau.

*Figure 4.38: Ajouter de l'étain à l'extrémité du fil avant de souder.*

5. Avec le fer à souder, étamez la broche centrale du connecteur. En maintenant le fil vertical à l'aide des pinces, soudez le côté auquel vous avez ajouté l'étain dans le trou de la broche centrale.

*Figure 4.39: Soudez le fil à la pièce dorée du connecteur N.*

6. Insérez une rondelle et vissez doucement l'écrou sur le connecteur. Coupez le fil à 3,05 centimètres mesurés à partir de la partie inférieure de l'écrou.

*Figure 4.40: La longueur du fil est cruciale.*

7. Dévissez l'écrou du connecteur en laissant la rondelle en place. Insérez le connecteur dans le trou de la boîte de conserve. Vissez l'écrou sur le connecteur de l'intérieur de la boîte de conserve.

*Figure 4.41: Assemblez l'antenne.*

8. Utilisez les pinces et la clé anglaise pour visser fermement l'écrou sur le connecteur. Vous avez terminé!

*Figure 4.42: Votre cantenna terminée.*

Comme pour d'autres conceptions d'antenne, vous devrez l'imperméabiliser si vous souhaitez l'employer dehors. Le PVC fonctionne bien pour lune antenne faîte à partir d'une boîte de conserve. Insérez toute la boîte de conserve dans un grand tube de PVC et scellez les extrémités avec des couvercles et de la colle. Vous devrez percer un trou dans le côté du tube pour placer le connecteur N sur le côté de la boîte de conserve.

## Cantenna comme source d'une parabole

Comme avec la clef USB parabolique, vous pouvez employer la cantenna comme conducteur pour un gain sensiblement plus élevé. Montez la boîte de conserve sur l'antenne parabolique avec l'ouverture de la boîte pointant le

centre du plat. Employez la technique décrite dans l'exemple de l'antenne clef USB (en observant comment la puissance du signal change dans le temps) pour trouver l'endroit optimum pour placer la boîte de conserve selon le réflecteur que vous employez.

En employant un cantenna bien construite avec une antenne parabolique correctement réglée, vous pouvez réaliser un gain global d'antenne de 30 dBi ou plus. Plus la taille des antennes paraboliques augmente, plus il y a gain et directivité potentiels de l'antenne. Avec des antennes paraboliques très grandes, vous pouvez réaliser un gain sensiblement plus élevé.

Par exemple, en 2005, une équipe d'étudiants universitaires a établi avec succès un lien allant du Nevada à l'Utah aux États-Unis. Le lien a atteint une distance de plus de 200 kilomètres! Ils ont utilisé une antenne parabolique de 3,5 mètres pour établir un lien 802.11b qui a fonctionné à 11Mbps sans utiliser d'amplificateur. Des détails au sujet de cette réalisation peuvent être trouvés à l'adresse suivante: *http://www.wifi-shootout.com/*.

## NEC2

L'abréviation ***NEC2*** représente le ***Code numérique Électromagnétique*** (version 2) qui est un logiciel libre de modélisation d'antennes. Le NEC2 vous permet de construire un modèle 3D d'antenne, puis analyse la réponse électromagnétique de l'antenne. Le logiciel a été développé il y a plus de dix ans et a été compilé pour fonctionner sur plusieurs différents systèmes informatiques. Le NEC2 est particulièrement efficace pour analyser des modèles de grille métallique, mais possède également une certaine capacité de modélisation de surface.

La conception de l'antenne est décrite dans un fichier texte, puis on construit le modèle en utilisant cette description. Le logiciel NEC2 décrit l'antenne en deux parties: sa ***structure*** et un ordre des ***commandes***. La structure est simplement une description numérique qui explique où se situent les différentes pièces de l'antenne et la façon dont les fils sont connectés. Les commandes indiquent au logiciel NEC où la source RF est connectée. Une fois que ceux-ci sont définis, l'antenne de transmission est alors modélisée. En raison du théorème de réciprocité le modèle de transmission de gain est le même que celui de réception, ainsi modéliser les caractéristiques de transmission est suffisant pour comprendre totalement le comportement de l'antenne.

Une fréquence ou une gamme de fréquences du signal RF doit être indiquée. L'important élément suivant est la caractéristique du terrain. La conductivité de la terre change d'un endroit à l'autre mais dans plusieurs cas elle joue un rôle essentiel au moment de déterminer le modèle de gain d'antenne.

Pour faire fonctionner le logiciel NEC2 sur Linux, installez le paquet NEC2 à partir de l'URL ci-dessous. Pour le lancer, tapez **`nec2`** puis les noms des fichiers d'entrée et de sortie. Il est également intéressant d'installer le paquet **`xnecview`** pour le traçage du modèle de vérification et de rayonnement de structure. Si tout va bien, vous devriez avoir un fichier contenant le résultat. Celui-ci peut être divisé en diverses sections mais pour une idée rapide de ce qu'il représente, un modèle de gain peut être tracé en utilisant **`xnecview`**. Vous devriez voir le modèle attendu, horizontalement omnidirectionnel, avec une crête à l'angle optimum de sortie. Les versions Windows et Mac sont également disponibles.

L'avantage du NEC2 est que nous pouvons avoir une idée de la façon dont fonctionne l'antenne avant de la construire et de la façon dont nous pouvons modifier sa conception afin d'obtenir un gain maximum. C'est un outil complexe qui exige un peu de de temps pour apprendre son fonctionnement, mais c'est un instrument d'une valeur inestimable pour les concepteurs d'antenne.

Le logiciel NEC2 est disponible sur le site de Ray Anderson (en anglais seulement), "*Unofficial NEC Archives*" à *http://www.si-list.org/swindex2.html*.

Des documents en ligne (en anglais seulement) peuvent être trouvés sur le site "*Unofficial NEC Home Page*" à *http://www.nittany-scientific.com/nec/*.

# 5
# Matériel réseau

Au cours des dernières années, l'intérêt croissant pour le matériel sans fil de gestion de réseau a apporté une variété énorme d'équipements peu coûteux sur le marché. En fait il y en a tellement, qu'il serait impossible de tous les cataloguer. Au sein de ce chapitre, nous nous concentrerons sur les fonctionnalités des attributs qui sont souhaitables pour un composant réseau sans fil et nous verrons plusieurs exemples d'outils commerciaux et de bricolages maisons qui ont bien fonctionné par le passé.

## *Sans fil, avec fil*

Malgré l'appellation « sans fil », vous serez fort probablement surpris d'apprendre combien de câbles sont requis pour la construction d'un simple lien point à point sans fil. Un noeud sans fil se compose de plusieurs éléments qui doivent tous être reliés entre eux à l'aide d'un câblage approprié. Vous aurez évidemment besoin d'au moins un ordinateur connecté à un réseau Ethernet et un routeur ou pont sans fil relié au même réseau. Les composantes munies d'un module radio doivent être reliées aux antennes, toutefois elles doivent parfois être connectées à une interface avec un amplificateur, un parafoudre ou tout autre dispositif. Beaucoup de composantes exigent une alimentation électrique, soit par l'intermédiaire d'un circuit principal AC ou à l'aide d'un transformateur DC. Toutes ces composantes emploient diverses sortes de connecteurs, ainsi qu'une grande variété de modèles et de gabarits de câbles.

Multipliez maintenant la quantité de câbles et de connecteurs par le nombre de noeuds que vous déploierez et vous vous demanderez bien pourquoi on désigne ceci comme une connexion sans fil. Le diagramme suivant vous donnera une certaine idée du câblage exigé pour un lien typique point à point. Notez que ce diagramme n'est pas à l'échelle et ne représente pas nécessairement le meilleur choix de conception réseau. Mais il vous présentera plusieurs composantes courantes que vous retrouverez très probablement sur le terrain.

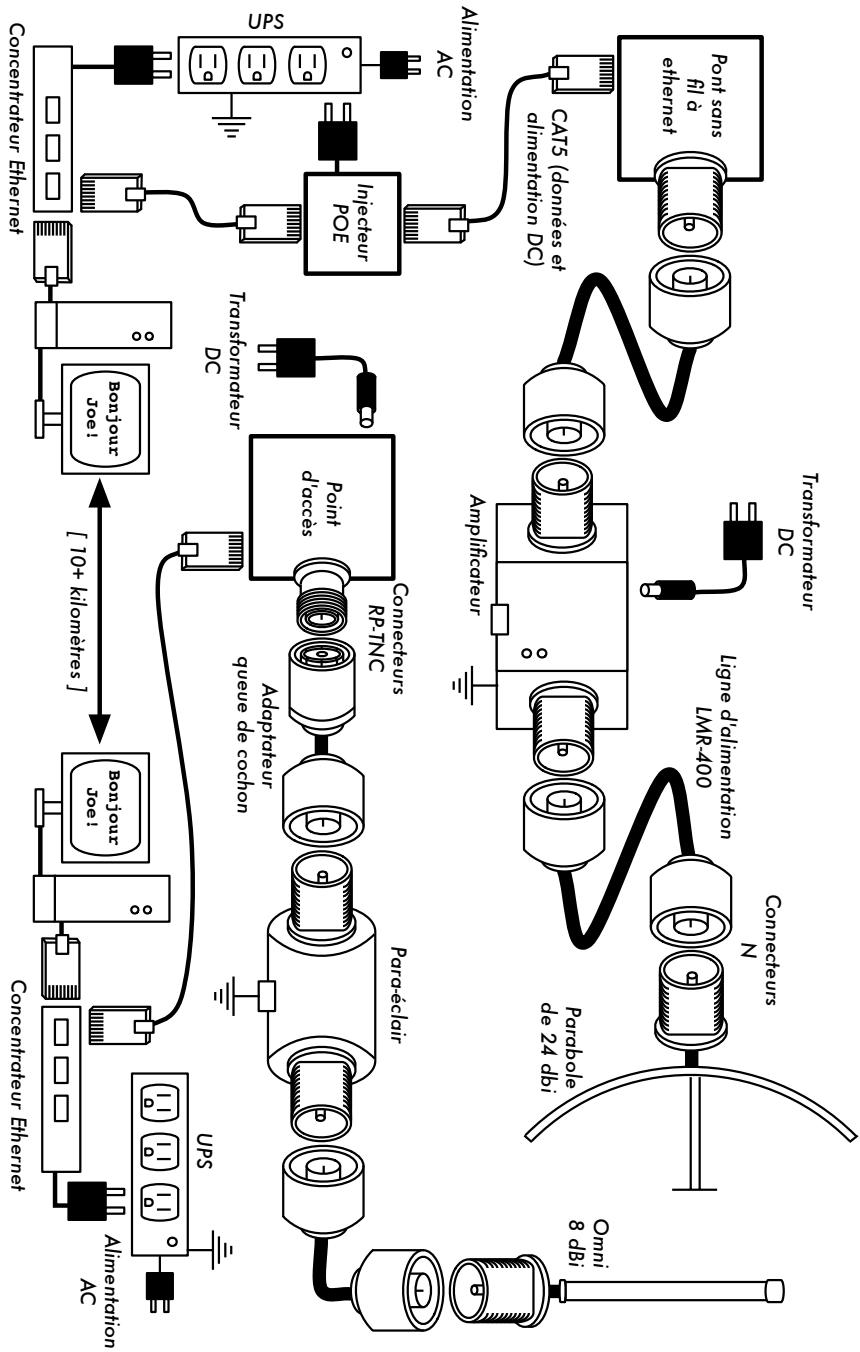


*Figure 5.1: Composantes Interconnectées*

Tandis que les composantes réelles utilisées vont varier d'un noeud à l'autre, chaque installation incorporera les pièces suivantes:

1. Un ordinateur ou réseau connecté à un commutateur Ethernet.
2. Un dispositif qui puisse connecter ce réseau à un dispositif sans fil (un routeur sans fil, un pont ou un répéteur).
3. Une antenne connectée via une source de signal radio ou intégrée dans le dispositif sans fil lui-même.
4. Des composantes électriques qui comprennent des sources d'énergie, des conditionneurs et des parafoudres.

Le choix du matériel devrait être déterminé en établissant les conditions requises pour le projet, en déterminant le budget disponible et en vérifiant que le projet est faisable en utilisant les ressources disponibles (prévoir également des pièces de rechange et des coûts récurrents d'entretien). Tel que discuté au cours du premier chapitre, il est critique d'établir la portée de votre projet avant de prendre toute décision d'achat.

# Choisir des composantes sans fil

Malheureusement, dans un monde de concurrence entre les fabricants de matériel informatique et de budgets limités, le prix est souvent le facteur décisif. Le vieux dicton: "vous obtenez ce dont vous avez payé pour" est souvent vrai lorsque arrive le moment d'acheter des équipements de haute technologie mais ne devrait pas être considéré comme une vérité absolue. Le prix est important dans n'importe quelle décision d'achat et il est essentiel de comprendre en détail ce que vous obtenez pour votre argent afin que vous puissiez faire un choix qui s'adapte à vos besoins.

Au moment de comparer les équipements sans fil qui conviennent à votre réseau, soyez certains de considérer les variables suivantes:

- **Interopérabilité**. L'équipement que vous désirez acquérir peut-il fonctionner avec des équipements provenant d'autres fabricants? Si ce n'est pas le cas, est-ce un facteur important pour ce segment de votre réseau? Si l'équipement en question supporte un protocole libre (tel que le 802.11b/g), il sera alors probablement interopérable avec l'équipement provenant d'autres fabricants.
- **Portée**. Comme nous avons vu dans le chapitre 4, la portée n'est pas quelque chose d'inhérent à un élément particulier de l'équipement. La portée d'un dispositif dépend de l'antenne reliée à celui-ci, du terrain, des caractéristiques du dispositif à l'autre extrémité du lien et à d'autres facteurs. Plutôt que de compter sur une estimation de portée (souvent médio-

cre) fournie par le fabricant, il est plus utile de connaître ***la puissance de transmission*** de la radio ainsi que le ***gain d'antenne*** (si une antenne est incluse). Avec cette information, vous pouvez calculer la portée théorique telle que décrite dans le chapitre 3.

- **Sensibilité du module radio**. Quelle est la sensibilité du dispositif radio à un débit donné? Le fabricant devrait fournir cette information au moins aux vitesses les plus rapides et les plus lentes. Ceci peut être employé comme mesure de la qualité du matériel et permet de calculer le coût du lien. Comme nous avons vu dans le chapitre trois, une basse valeur est meilleure pour quantifier la sensibilité de la radio.
- **Débit**. Les fabricants indiquent systématiquement le débit le plus élevé possible comme "vitesse" de leur équipement. Gardez en tête que le débit total de la radio (par exemple 54Mbps) n'est jamais l'estimation réelle du rendement du dispositif (par exemple, environ 22 Mbps pour le 802.11g). Si l'information sur le rapport de rendement n'est pas disponible pour le dispositif que vous êtes en train d'évaluer, vous pouvez approximativement diviser la « vitesse » du dispositif par deux et y soustraire environ 20%. Si vous doutez, effectuez un test de rendement sur une unité d'évaluation avant d'acheter en grande quantité l'équipement qui n'a aucune estimation officielle du rapport de rendement.
- **Accessoires requis**. Pour maintenir les prix bas, les fournisseurs omettent souvent les accessoires qui sont nécessaires pour un usage normal. Le prix inclut-il tous les adaptateurs de puissance? (Les approvisionnements DC sont en général inclus ; les injecteurs de puissance pour Ethernet ne le sont habituellement pas. Vérifiez aussi les tensions d'entrée car l'équipement offert a souvent une alimentation électrique de type nord-américain). Qu'en est-il des queues de cochon, des adaptateurs, des câbles, des antennes et des cartes radio? Si vous avez l'intention de les employer à l'extérieur, le dispositif inclut-il une boîte imperméable?
- **Disponibilité**. Pourrez-vous remplacer facilement les composantes brisées? Pouvez vous commander la pièce en grandes quantités? Votre projet l'exige-t-il? Quelle est la durée de vie projetée de ce produit particulier en termes de temps de fonctionnement sur le terrain et de disponibilité future du produit chez le fournisseur?
- **D'autres facteurs**. Soyez sûr que votre équipement possède les caractéristiques particulières à vos besoins. Par exemple, le dispositif inclut-il un connecteur d'antenne externe? Si oui, de quel type? Y a-t-il des limites d'usage ou de rendement imposées par le logiciel et si oui, quel est le prix pour augmenter ces limites? Quelles sont les dimensions du dispositif? Quelle quantité d'énergie consomme-t-il? Permet-il le POE comme source d'énergie? Le dispositif fournit-il du chiffrage, NAT, outils de surveillance de bande passante ou autres caractéristiques nécessaires pour la conception de votre réseau?

En répondant à ces questions, vous pourrez prendre des décisions d'achats intelligentes au moment de choisir le matériel de gestion de réseau. Il est peu probable que vous puissiez répondre à chacune des questions avant d'acheter l'équipement, mais si vous mettez des priorités dans vos questions et poussez le vendeur à y répondre avant de réaliser l'achat, vous ferez bon usage de votre budget et établirez un réseau avec des composantes qui correspondent à vos besoins.

# Solutions commerciales vs. DIY (Faîtes-le vous-même)

Votre projet de réseau se composera certainement de composantes achetées chez des fournisseurs ainsi que de pièces originaires ou même fabriquées localement. Ceci est une vérité économique de base dans la plupart des régions du monde. Actuellement, la distribution globale de l'information est tout à fait insignifiante comparée à la distribution globale des marchandises. Dans plusieurs régions, l'importation de chaque composante requise pour établir un réseau est prohibitive du point de vue des coûts, sauf pour les budgets les plus importants. Vous pouvez économiser considérablement de l'argent, à court terme, en trouvant des sources locales pour les pièces et le travail et en important uniquement les composantes qui doivent être achetées.

Naturellement, il y a une limite à la quantité de travail qui peut être effectuée par un individu ou un groupe dans un temps donné. Pour le dire d'une autre façon, en important de la technologie, vous échangez de l'argent contre de l'équipement qui peut résoudre un problème particulier dans une quantité de temps comparativement courte. L'art de construire une infrastructure de télécommunications locale se situe dans le bon équilibre entre argent et effort requis pour résoudre un problème donné.

Quelques composantes, tels que les cartes radio et les lignes d'alimentation d'antenne sont de loin trop complexes pour envisager de les fabriquer localement. D'autres composantes, telles que les antennes et les tours, sont relativement simples et peuvent être construites localement pour une fraction du coût d'importation. Entre ces extrêmes, nous retrouvons les dispositifs de communication eux-mêmes.

En employant des éléments disponibles comme les cartes radio, les cartes mères et d'autres composantes, vous pouvez construire des dispositifs qui fournissent des caractéristiques comparables (ou même supérieures) à la plupart des conceptions commerciales. La combinaison de matériel libre et

de logiciel libre peut fournir des solutions robustes et sur mesure à un très bas prix.

Ceci ne veut pas dire que l'équipement commercial est inférieur à une solution maison. En fournissant des "solutions clé en main", les fabricants nous font non seulement économiser du temps d'élaboration mais peuvent également permettre à des personnes relativement peu qualifiées d'installer et de maintenir l'équipement. Les principaux avantages des solutions commerciales sont qu'elles fournissent ***appui*** et ***garantie*** (habituellement limitée) pour leurs équipements. Elles fournissent également une ***plateforme cohérente*** qui mène à des installations de réseau très stables et souvent interchangeables.

Si une pièce d'équipement ne fonctionne pas, est difficile à configurer ou rencontre des problèmes, un bon fabricant saura vous aider. En règle générale, si l'équipement présente un défaut lors d'une utilisation normale (excepté des dommages extrêmes tel que la foudre), le fabricant le remplacera. La plupart fourniront ces services pendant un temps limité comme faisant partie du prix d'achat, et nombreux sont ceux qui offrent un service de support et une garantie pour une période prolongée pour des frais mensuels. En fournissant une plateforme cohérente, il est simple de garder des pièces de rechange en main et d'échanger celles qui présentent un problème sans avoir recours à un technicien pour configurer l'équipement sur place. Naturellement, tout ceci implique que l'équipement aura un coût initial comparativement plus élevé que les composantes disponibles localement.

Du point de vue d'un architecte de réseau, les trois plus grands risques cachés des solutions commerciales sont: ***rester pris avec un fournisseur***, les ***produits discontinués***, et les ***coûts constants des licences***.

Il peut être onéreux de se laisser attirer par les nouvelles « caractéristiques » des différents dispositifs, surtout si cela détermine le développement de votre réseau. Les fabricants fourniront fréquemment des dispositifs qui sont incompatibles de par leur conception avec ceux de leurs concurrents et ils essaieront, dans leurs publicités, de vous convaincre que vous ne pouvez pas vivre sans eux (indépendamment du fait que le dispositif contribue à la solution de votre problème de transmission ou pas). Si vous commencez à compter sur ces dispositifs, vous déciderez probablement de continuer d'acheter l'équipement du même fabricant à l'avenir. Ceci est le principe même de « rester pris avec un fournisseur ». Si une institution importante utilise une quantité significative d'équipement de propriété industrielle, il est peu probable qu'elle l'abandonnera simplement pour avoir recours à un fournisseur différent. Les équipes de vente le savent (et en effet, plusieurs se fondent sur ce principe) et l'emploient comme stratégie lors de la négociations des prix.

En plus du principe de « rester pris avec un fournisseur », le fabricant peut décider de discontinuer un produit, indépendamment de sa popularité. Ceci pour s'assurer que les clients, déjà dépendants des dispositifs de propriété industrielle de ce fabricant, achèteront le tout dernier modèle (qui est presque toujours plus cher). Les effets à long terme de ces deux stratégies sont difficiles à estimer au moment de la planification d'un projet de réseau mais devraient être gardées à l'esprit.

Finalement, si une pièce particulière d'équipement emploie un code informatique de propriété industrielle, vous pourriez avoir à renouveler une licence sur une base continue. Le coût de ces licences peut changer selon les dispositifs fournis, le nombre d'utilisateurs, la vitesse de connexion ou d'autres facteurs. Si les frais de licence sont impayés, l'équipement est conçu pour cesser simplement de fonctionner jusqu'à ce qu'un permis valide et payé soit fourni! Soyez certains de comprendre les limites d'utilisation pour n'importe quel équipement que vous achetez y compris les coûts continus des licences.

En utilisant un équipement générique qui soutient les normes ouvertes et les logiciels libres, vous pouvez éviter certains de ces pièges. Par exemple, il est très difficile de « rester pris avec un fournisseur » qui emploie des protocoles ouverts (tels que TCP/IP sur 802.11a/b/g). Si vous rencontrez un problème avec l'équipement ou le fournisseur, vous pouvez toujours acheter un équipement qui soit interopérable avec ce que vous avez déjà acheté d'un fournisseur différent. C'est pour ces raisons que nous recommandons d'employer des protocoles de propriété industrielle et le spectre sous licence seulement dans les cas où l'équivalent ouvert ou libre (tel que le 802.11a/b/g) n'est techniquement pas accessible.

De même, alors que différents produits peuvent toujours être discontinués à tout moment, vous pouvez limiter l'impact que ceci aura sur votre réseau en employant des composantes génériques. Par exemple, une carte mère particulière peut devenir indisponible sur le marché, mais vous pouvez avoir un certain nombre de cartes mères en main qui accomplirons efficacement la même tâche. Plus tard dans ce chapitre, nous verrons quelques exemples de la façon dont nous devons employer ces composantes génériques pour établir un noeud sans fil complet.

Évidemment, il ne devrait y avoir aucun coût de licence associé à un logiciel libre (excepté un fournisseur offrant un service d'appui prolongé ou tout autre service, sans facturer l'utilisation du logiciel lui-même). Certains fournisseurs ont profité du cadeau que les programmeurs de logiciels libres ont offert au public, en vendant le code sur une base de licences continues, violant de ce fait les termes de distribution déterminés par les auteurs originaux. Il serait sage d'éviter de tels fournisseurs et de soupçonner tout « logiciel gratuit» qui vient avec des frais de licence.

L'inconvénient d'utiliser le logiciel libre et le matériel générique est clairement la question du service de support. Car si des problèmes avec le réseau surgissent, vous devrez résoudre ces problèmes vous-même. Ceci est souvent accompli en consultant les ressources et les moteurs de recherche en ligne gratuits et en appliquant un correctif de code directement. Si vous n'avez pas de membre dans votre équipe qui soit assez compétent pour fournir une solution à votre problème de communication, alors lancer un projet de réseau peut prendre un temps considérable. Naturellement, le fait de simplement payer pour résoudre le problème ne garantit pas non plus qu'une solution sera trouvée. Même si nous fournissons beaucoup d'exemples sur comment effectuer une grande partie du travail par vous-même, ce travail peut représenter pour vous un véritable défi. Vous devrez trouver l'équilibre entre les solutions commerciales et DIY (Faîtes-le vous-même) qui convient à votre projet.

En bref, définissez toujours la portée de votre réseau d'abord, identifiez ensuite les ressources disponibles pour résoudre le problème et le choix des équipements en découlera naturellement. Prenez en considération tant les solutions commerciales que les composantes libres, tout en maintenant à l'esprit les coûts à long terme des deux.

# Produits sans fil professionnels

Il y a beaucoup d'équipements sur le marché pour les liens longue distance point-à-point (P2P). La plupart de ces équipements sont prêts à être installés, seuls les câbles d'antenne doivent être joints et scellés. Si nous pensons installer un lien longue distance, nous devons considérer trois facteurs principaux: la distance totale du lien, le temps requis pour le faire fonctionner et, naturellement, les besoins en vitesse du lien.

La plupart des produits commerciaux couramment disponibles pour des liens de longue portée emploient maintenant la technologie OFDM et fonctionnent dans la bande ISM de 5,8 gigahertz. Quelques produits emploient des normes ouvertes mais la plupart emploient un protocole de propriété industrielle. Ceci signifie que pour établir un lien, les radios des deux côtés devront provenir du même fabricant. Pour des liens critiques c'est une bonne idée de choisir un système qui utilise un équipement identique des deux côtés du lien. De cette façon, il n'est nécessaire de conserver en stock qu'une seule pièce de rechange qui pourra remplacer l'un ou l'autre côté du lien. Il y a quelques bons produits sur le marché qui utilisent un équipement différent à l'une ou l'autre extrémité du lien. Il est possible d'employer ceux-ci tant et aussi longtemps que le travail est réalisé méticuleusement, dans le cas contraire il sera nécessaire de conserver des pièces de rechange pour les deux types de radios.

Nous ne faisons aucune campagne publicitaire pour un certain type de radio ni une plainte au sujet de l'une ou l'autre. Nous ne présentons que quelques notes qui résultent de plus de cinq ans d'expérience sur le terrain partout dans le monde avec des produits commerciaux sans licence. Il n'y a malheureusement aucune façon de passer en revue chaque produit, de fait, seulement quelques favoris sont énumérés ci-dessous.

## Communications Redline

*Redline* a été lancé sur le marché pour la première fois avec sa ligne de produits AN-50. *Redline* a été le premier produit point-à-point disponible avec des débits au-dessus de 50 Mbps que les petits opérateurs pouvaient réellement se permettre. Ce produit emploie seulement 20 mégahertz de spectre par canal. Il y a trois modèles différents disponibles dans la ligne AN-50. Les trois ont le même ensemble de caractéristiques de base, seule la largeur de bande change. Le modèle standard a un rendement de sortie de 36 Mbps, le modèle économique, 18 Mbps et la version complète, 54 Mbps. Les commandes de largeur de bande sont mises à jour à travers un logiciel et peuvent être ajoutées dans le système à mesure que la demande en débit augmente.

Les radios *Redline* se composent d'une unité pour l'intérieur, d'une unité pour l'extérieur et d'une antenne. Les unités d'intérieur s'ajustent à une étagère standard de 19 pouces et occupent 1U. L'unité extérieure s'assemble sur le même support qui tient l'antenne en place. Cette unité extérieure est la radio. Les deux unités sont reliées par un câble coaxial. Le câble employé est de type RG6 ou RG11 de *Beldon*. C'est le même câble utilisé pour des installations de télévision par satellite. Il est peu coûteux, facilement trouvable et élimine le besoin de câbles coûteux à faibles pertes, tels que les séries *Times Microwave LMR* ou *Andrew Corporation Heliax*. En outre, placer la radio aussi près de l'antenne permet de réduire la perte due au câble au minimum.

Il y a deux caractéristiques à noter sur les radios *Redline*. La première est le ***Mode Général d'Alignement***, qui met en marche un signal sonore qui change de tonalité à mesure que la technique de modulation change. Un « bip-bip » plus rapide signifie une connexion plus rapide. Ceci permet un alignement beaucoup plus facile car le lien peut, la plupart du temps, être aligné à partir de ces seules tonalités. Seul un accord final sera nécessaire et une application graphique fonctionnant sous Windows est disponible pour aider en ce sens. L'autre caractéristique est une touche **Test**. Chaque fois que des changements radio sont faits sans avoir la certitude qu'ils sont corrects, appuyer sur la touche **Test** au lieu de la touche **Sauvegarder** rendra les nouveaux changements actifs pendant cinq minutes. Après ces cinq minutes, la configuration retourne à nouveau à ce qu'elle était avant d'appuyer sur la touche **Test**. Ceci nous permet d'essayer les changements et si les

choses ne fonctionnent pas et que le lien tombe, celui-ci reviendra après cinq minutes. Une fois que les changements ont été essayés, confirmez-les simplement dans votre configuration et appuyez sur le bouton **Sauvegarder** au lieu du bouton **Test**.

*Redline* propose d'autres modèles. Le AN-30 a quatre ports T1/E1, en plus d'une connexion Ethernet de 30 Mbps. Le AN-100 suit la norme 802.16a et le prochainement disponible *RedMax* promet une conformité avec WiMax.

Pour plus d'informations sur les produits Redline Communications, visitez le site Web suivant: *http://www.redlinecommunications.com/*.

## Alvarion

Un des grands avantages à travailler avec des produits Alvarion est son réseau de distribution mondial très bien établi. Ils ont également une des plus grandes parts du marché mondial pour toutes sortes de matériel sans fil de connectivité à Internet. On trouve des distributeurs et des revendeurs dans la plupart des régions du monde. Pour des liens de plus longue distance, deux produits attirent notre intérêt: la série VL, et *Link Blaster*.

Même si la série VL est un système point-à-multipoint, un seul client radio connecté à un seul point d'accès fonctionnera convenablement pour un lien point-à-point. Le seul point à considérer est le fait d'utiliser une antenne directionnelle au point d'accès, à moins qu'il soit prévu qu'un autre lien se relie à ce point d'accès dans le futur. Il y a deux vitesses disponibles pour la série VL, 24 Mbps et 6 Mbps. Le budget, les exigences de temps et de vitesse guideront la décision du choix de CPE à employer.

Le *Link Blaster* est très semblable à un *Redline AN-50*. Ceci est dû au fait qu'il en est un. Très rapidement après que le *Redline AN-50* soit apparu sur le marché, un accord OEM entre les deux compagnies a été signé et le *Link Blaster* est né. Bien que l'unité d'intérieur soit dans une boîte différente et que les antennes soient marquées différemment, l'électronique à l'intérieur des unités est identique. Le *Link Blaster* est plus coûteux qu'un *Redline*; la différence de prix suppose une conception plus solide et un niveau additionnel de support après vente. Il est souvent plus facile pour un revendeur d'Alvarion de trouver des produits de revendeurs de *Redline*. Ceci devra être étudié localement. Il peut être avantageux de dépenser plus d'argent pour avoir un produit localement disponible et qui dispose d'un service de support après vente.

Alvarion a certains produits point-à-point de 2,4 gigahertz disponibles. La plupart de leurs produits se retrouvent dans la bande ISM de 2,4 GHz qui utilise le Spectre dispersé à saut de fréquences (*Frequency Hopping Spread Spectrum -FHSS*) et qui créera beaucoup de bruit pour l'étalement du spec-

tre en séquence directe locale (*Direct Sequence Spread Spectrum -DSSS*) sur la même tour. Si on prévoit un système de distribution basé sur le DSSS, alors un *backhaul* FHSS ne sera pas une option efficace.

Pour plus d'information sur les produits Alvarion, visitez le site Web suivant: *http://www.alvarion.com/*.

## Communications de données Rad

La ligne de produits *Rad Airmux* est relativement nouvelle sur le marché et a un grand potentiel. *L'Airmux 200* est une radio de 48 Mbps qui emploie le câble CAT5 et détient un des meilleurs prix par rapport à d'autres solutions commerciales sur le marché. Les unités sont petites et faciles à manipuler sur une tour. Le seul désavantage que l'on peut noter est l'absence d'un système local de distribution dans les pays en voie de développement. Il y a deux modèles disponibles dans la ligne *Airmux*. L'un utilise des antennes internes et l'autre utilise des antennes externes.

L'expérience avec les radios *Airmux* au début de l'an 2005 montre qu'un défi se pose par rapport aux réglages temporels. Ceci ne devient évident que lorsque la distance du lien est à plus de 12 milles, soit 19 kilomètres et ce, peu importe le type d'antenne employée. Jusqu'à ce que ce problème soit réglé, ces radios ne devraient être employées que pour des liens au-dessous de 19 kilomètres. Si cette recommandation est suivie, ces radios fonctionnent très bien, particulièrement si nous considérons leur prix.

Pour obtenir plus d'informations sur les produits *Rad Data Communications*, visitez le site Web suivant: *http://www.rad.com/*.

## Systèmes Cisco

Les solutions sans fil de Cisco ont deux grands avantages. Elles ont un réseau très bien établi de distribution ainsi qu'un support et des personnes formées presque partout dans le monde. On trouve des distributeurs et des revendeurs partout. Ceci peut être d'une aide précieuse à l'heure de se procurer un équipement et encore plus si l'équipement se brise et a besoin d'être remplacé. L'autre grand avantage est que les solutions Cisco emploient des normes ouvertes pour la plupart de leurs pièces. La majeure partie de leurs équipements suit les normes 802.11a/b/g.

L'expérience prouve qu'il est plus difficile de comprendre leurs outils de configuration disponibles sur le Web que ceux trouvés dans plusieurs autres produits et que l'équipement coûte plus cher que d'autres solutions non commerciales et basées sur des normes ouvertes.

Vous trouverez plus d'information sur Cisco sur le site Web suivant: *http://www.cisco.com/*.

## En voulez-vous d'autres?

Il y a actuellement beaucoup plus de solutions disponibles sur le marché et de nouvelles arrivent tout le temps. Les bonnes solutions sont fournies par des compagnies comme *Trango Broadband* (*http://www.trangobroadband.com/*) et *Waverider Communications* (*http://www.waverider.com/*). Au moment de choisir quelle solution employer, rappelez-vous toujours des trois facteurs principaux: distance, temps pour la mise en fonctionnement et vitesse. Soyez certains de vérifier que les radios fonctionnent sur une bande sans licence là où vous les installez.

## Protecteurs professionnels contre la foudre

La foudre est le seul prédateur naturel pour les équipements sans fil. Celle-ci peut endommager l'équipement de deux façons différentes: par coups directs ou coups d'induction. Les coups directs surviennent lorsque la foudre frappe réellement la tour ou l'antenne. Les coups d'induction sont causés lorsque la foudre tombe tout près de la tour. Imaginez un éclair chargé négativement. Puisque les charges se repoussent, cet éclair éloignera les électrons dans les câbles, créant du courant sur les lignes. Cet évènement génère beaucoup plus de courant que ce que l'équipement par radio peut supporter. L'un ou l'autre type de foudre détruira généralement tout équipement non protégé.

*Figure 5.2: Tour avec un gros conducteur de terre en cuivre.*

La protection des réseaux sans fil contre la foudre n'est pas une science exacte et il n'y a aucune garantie que l'équipement ne subisse pas de coup de foudre, même si toutes les précautions sont prises. Plusieurs méthodes aideront cependant à prévenir les deux types de foudres: directes et d'induction. Même s'il n'est pas nécessaire d'employer toutes les méthodes de protection contre la foudre, le fait d'employer plus d'une méthode aidera à protéger davantage l'équipement. La quantité de foudre historiquement observée dans use zone donnée sera le guide le plus important au moment d'évaluer ce qui doit être fait.

Commencez à la base de la tour. Rappelez-vous que la base de la tour est sous la terre. Après que la fondation de la tour soit créée, mais avant de remblayer le trou, un large anneau de câble de terre tressé devrait être installé et étendu sous la terre pour en ressortir près de la tour. Le fil devrait être de type *American Wire Gauge* (*AWG*) #4 ou plus large. En outre, une tige de mise à terre de secours devrait être installée sous le sol et le câble de terre devrait aller de cette tige au conducteur à partir de l'anneau enterré.

Il est important de noter que tous les types d'acier ne conduisent pas l'électricité de la même manière. Certains sont de meilleurs conducteurs électriques et les différents revêtements extérieurs peuvent également avoir un impact sur la façon dont la tour d'acier conduit le courant électrique. L'acier inoxydable est l'un des pires conducteurs et les revêtements à l'épreuve de la rouille, comme la galvanisation ou la peinture, diminuent la conductivité de l'acier. C'est pour cette raison qu'un câble de terre tressé va de la base au sommet de la tour. La base doit être correctement unie aux conducteurs à partir de l'anneau et de la tige de terre de secours. Une tige contre la foudre devrait être attachée au sommet de la tour et sont bout devrait être en pointe. Plus cette pointe est fine et pointue, plus la tige sera efficace. Le câble de terre provenant de la base doit être relié à cette tige. Il est très important de s'assurer que le câble de terre est relié au métal. Tout revêtement, tel que la peinture, doit être retiré avant de connecter le câble. Une fois que la connexion est établie, le tout peut être peint, couvrant le câble et les connecteurs au besoin pour sauver la tour de la rouille et de toute autre corrosion.

La solution ci-dessus décrit l'installation de base du système de mise à terre. Elle assure la protection pour la tour elle-même contre les coups directs de la foudre et met en place le système de base auquel tout le reste devra se connecter.

La protection idéale aux coups d'induction surprise est l'installation de tube à décharge de gaz aux deux extrémités du câble. Ces tubes doivent être directement reliés au câble de terre installé sur la tour s'il se trouve à l'extrémité la plus élevée. L'extrémité inférieure doit être reliée à quelque chose d'électriquement sûr, comme un plat de terre ou un tuyau de cuivre plein

d'eau. Il est important de s'assurer que le tube à décharge extérieure est protégé contre les intempéries. Plusieurs tubes pour les câbles coaxiaux sont protégés contre les intempéries, alors que la plupart des tubes pour le câble CAT5 ne le sont pas.

Dans le cas où les tubes à décharge de gaz ne seraient pas employés et le câblage serait coaxial, la fixation d'une extrémité du câble au revêtement du câble et l'autre extrémité au câble de terre installé sur les tours assurera une certaine protection. Ceci peut fournir un chemin pour les courants d'induction, et si la charge est assez faible, elle n'affectera pas le fil conducteur du câble. Même si cette méthode n'est pas aussi bonne que la protection que nous offrent les intercepteurs de gaz, elle est préférable à ne rien faire du tout.

# Créer un point d'accès à l'aide d'un ordinateur

À la différence des systèmes d'exploitation tels que Microsoft Windows, le système d'exploitation GNU/Linux donne à l'administrateur réseau la capacité d'avoir plein accès aux couches du modèle OSI. Il est possible d'accéder et de travailler sur des paquets réseau à n'importe quel niveau, de la couche liaison de données à la couche application. Des décisions de routage peuvent être prises en se basant sur n'importe quelle information contenue dans un paquet réseau, de l'adresse du port de routage au contenu du segment de données. Un point d'accès Linux peut agir en tant que routeur, pont, pare-feu, concentrateur VPN, serveur d'application, moniteur réseau ou pratiquement n'importe quel autre rôle dans le domaine de la gestion de réseau. C'est un logiciel libre et qui n'exige aucun frais de licence. GNU/Linux est un outil très puissant qui peut remplir une grande variété de rôles au sein d'une infrastructure de réseau.

Ajoutez une carte et un dispositif sans fil Ethernet à un PC équipé de Linux et vous obtiendrez un outil très flexible qui peut vous aider à fournir de la bande passante et à contrôler votre réseau à de très faibles coûts. L'équipement peut être un ordinateur portable ou de bureau recyclé, ou un ordinateur embarqué tel qu'un équipement de réseau *Linksys WRT54G* ou *Metrix*.

Dans cette section, vous verrez comment configurer Linux pour les situations suivantes:

- Un point d'accès sans fil avec Masquerading/NAT et une connexion par câble à Internet (aussi nommée  passerelle sans fil).

- Un point d'accès sans fil faisant office de pont transparent. Le pont peut être utilisé comme point d'accès simple ou comme répéteur avec deux radios.

Considérez ces recettes comme point de départ. À partir de ces exemples simples, vous pouvez créer un serveur qui s'adapte avec précision à votre infrastructure de réseau.

## Prérequis

Avant de commencer, vous devriez déjà être familier avec Linux au moins d'un point de vue d'usager et être capable d'installer la distribution GNU/Linux de votre choix. Une compréhension de base de l'interface en ligne de commande (terminal) dans Linux est également requise.

Vous aurez besoin d'un ordinateur avec une ou plusieurs cartes sans fil déjà installées ainsi qu'une interface standard Ethernet. Ces exemples emploient une carte et un pilote spécifiques mais il y a plusieurs autres cartes qui devraient fonctionner tout aussi bien. Les cartes sans fil basées sur les chipsets *Atheros* et *Prism* fonctionnent particulièrement bien. Ces exemples se basent sur la version 5.10 (*Breezy Badger*) d'*Ubuntu Linux*, avec une carte sans fil fonctionnant grâce aux pilotes *HostAP* ou *MADWiFi*. Pour plus d'informations sur ces pilotes, visitez les sites Web suivants: *http://hostap.epitest.fi/* et *http://madwifi.org/*.

Le logiciel suivant est nécessaire pour accomplir ces installations. Il devrait se retrouver dans votre distribution Linux:

- Outils sans fil (commandes *iwconfig*, *iwlist*)
- Pare-feu *iptables*
- *dnsmasq* (serveur de cache DNS et serveur DHCP)

La puissance CPU exigée dépend de la quantité de travail qui doit être réalisée au delà du routage simple et NAT. Par exemple, un 133 MHz 486 est parfaitement capable de router des paquets aux vitesses sans fil. Si vous avez l'intention d'employer beaucoup de chiffrage (tel que les serveurs WEP ou VPN), vous aurez alors besoin d'une machine plus rapide. Si vous voulez également installer un serveur de cache (tel que Squid, voir le chapitre trois) vous aurez alors besoin d'un ordinateur avec beaucoup d'espace disque et de mémoire RAM. Un routeur typique qui travaille uniquement avec NAT fonctionne avec aussi peu de RAM que 64 MB et de stockage.

En construisant un dispositif pour faire partie de votre infrastructure de réseau, gardez à l'esprit que les disques durs ont une durée de vie limitée comparé à la plupart des autres composants. Vous pouvez souvent employer

un disque à état solide, tel qu'un disque flash, au lieu du disque dur. Celui-ci peut être une clé USB flash drive (en supposant que votre ordinateur s'initialisera à partir de l'USB), ou une carte flash compacte utilisant un adaptateur CF à IDE. Ces adaptateurs sont tout à fait accessibles et permettront à une carte CF d'agir comme un disque dur IDE standard. Ils peuvent être employés dans n'importe quel ordinateur qui supporte les disques durs IDE. Puisqu'ils n'ont aucune pièce mobile, ils fonctionneront pendant plusieurs années à une gamme de températures beaucoup plus élevées que ce qu'un disque dur peut tolérer.

## Scénario 1: Point d'accès avec mascarade

Celui-ci est le plus simple des scénarios et est particulièrement utile dans les situations où vous souhaitez un seul point d'accès pour le bureau. Ceci est plus facile dans les situations où:

1. Il y a déjà un coupe-feu et une passerelle exécutant Linux, et vous n'avez qu'à ajouter une interface sans fil.
2. Vous avez un vieil ordinateur de bureau ou portatif disponible et remis à neuf, et vous préférez l'employer comme point d'accès.
3. Vous avez besoin de plus de puissance en termes de surveillance, journalisation et/ou sécurité que ce que la plupart des points d'accès commerciaux peuvent fournir, mais n'êtes pas prêts à faire des folies en dépensant pour un point d'accès d'entreprise.
4. Vous voudriez qu'une seule machine agisse en tant que 2 points d'accès (et coupe-feu) de sorte que vous puissiez offrir un accès réseau à l'Intranet sécurisé ainsi qu'un accès ouvert pour les invités.

### Configurer les interfaces

Configurez votre serveur pour que eth0 soit connecté à Internet. Utilisez l'outil de configuration graphique fourni avec votre distribution.

Si votre réseau Ethernet utilise DHCP, vous pouvez essayer la commande suivante:

```
# dhclient eth0
```

Vous devriez recevoir une adresse IP et une passerelle par défaut. Ensuite, configurez votre interface sans fil en mode Master et donnez-lui le nom de votre choix:

```
# iwconfig wlan0 essid "my network" mode Master enc off
```

La commande **enc off** désactive le chiffrage WEP. Pour rétablir WEP, ajoutez une série de clés hexadécimales de la longueur correcte:

```
# iwconfig wlan0 essid “my network” mode Master enc 1A2B3C4D5E
```

Comme alternative, vous pouvez également utiliser une série lisible en commençant avec un “s”:

```
# iwconfig wlan0 essid “my network” mode Master enc “s:apple”
```

Donnez ensuite à votre interface sans fil une adresse IP dans un sous réseau privé, mais assurez-vous que ce n'est pas le même sous réseau que celui de votre adaptateur d'Ethernet:

```
# ifconfig wlan0 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255 up
```

## Configurer la mascarade dans le noyau de Linux

Afin de pouvoir traduire des adresses entre deux interfaces sur l'ordinateur, nous devons habiliter le masquerading (NAT) dans le noyau Linux. Premièrement nous chargeons le module pertinent de noyau:

```
# modprobe ipt_MASQUERADE
```

Ensuite nous désactivons toutes les règles existantes du pare-feu pour nous assurer que celui-ci ne bloque pas l’envoi de paquets entre les deux interfaces. Si vous avez un pare-feu activé, assurez-vous de savoir comment rétablir les règles existantes plus tard.

```
# iptables -F
```

Activez la fonction NAT entre les deux interfaces:

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Pour finir, nous devons indiquer au noyau de faire suivre les paquets d’une interface à l’autre:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Dans les distributions Linux basées sur Debian comme Ubuntu, ce changement peut aussi se réaliser en éditant le fichier **/etc/network/options**, et en changeant:

```
ip_forward=no
```

En

```
ip_forward=yes
```

Puis réinitialiser les interfaces de réseau à l'aide de la commande:

```
# /etc/init.d/network restart
```

Ou

```
# /etc/init.d/networking restart
```

## Configurer la mascarade dans le noyau de Linux

Afin de pouvoir traduire des adresses entre deux interfaces sur l'ordinateur, nous devons habiliter le masquerading (NAT) dans le noyau Linux. Premièrement nous chargeons le module pertinent de noyau:

```
# modprobe ipt_MASQUERADE
```

Ensuite nous désactivons toutes les règles existantes du pare-feu pour nous assurer que celui-ci ne bloque pas l'envoi de paquets entre les deux interfaces. Si vous avez un pare-feu activé, assurez-vous de savoir comment rétablir les règles existantes plus tard.

```
# iptables -F
```

Activez la fonction NAT entre les deux interfaces:

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Pour finir, nous devons indiquer au noyau de faire suivre les paquets d'une interface à l'autre:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Dans les distributions Linux basées sur Debian comme Ubuntu, ce changement peut aussi se réaliser en éditant le fichier **/etc/network/options**, et en changeant:

```
ip_forward=no
```

En

```
ip_forward=yes
```

Puis réinitialiser les interfaces de réseau à l'aide de la commande:

```
# /etc/init.d/network restart
```

Ou

```
# /etc/init.d/networking restart
```

## Configurer le serveur DHCP

À présent, nous devrions avoir un point d'accès fonctionnel. Nous pouvons le tester en se connectant au réseau sans fil «*my network*» (mon réseau) à l'aide d'un autre ordinateur en lui donnant une adresse dans la même plage d'adresses que notre interface sans fil sur le serveur (10.0.0.0/24 si vous avez suivi les exemples). Si vous avez activé WEP, soyez sûr d'employer la même clef que celle que vous avez indiquée sur l'AP.

Afin de faciliter la connexion au serveur et de ne pas avoir à saisir manuellement les adresses IP sur les postes clients, nous allons configurer un serveur DHCP pour distribuer automatiquement des adresses aux clients sans fil.

Pour ce faire, nous emploierons le programme dnsmasq. Comme son nom l'indique, il fournit un serveur de cache DNS ainsi qu'un serveur DHCP. Ce programme a été spécialement développé pour être utilisé avec des pare-feu fonctionnant en NAT. Avoir un serveur de cache DNS est particulièrement utile si votre connexion Internet a une grande latence et/ou une faible bande passante, tel que les connexions VSAT ou d'accès par ligne commutée (*dial-up)*. Ceci signifie que plusieurs requêtes DNS peuvent être résolues localement, éliminant une grande partie du trafic sur Internet tout en permettant une connexion beaucoup plus rapide pour les utilisateurs.

Installez dnsmasq avec votre gestionnaire de paquetage. Si dnsmasq n'est pas disponible sous forme de paquet, téléchargez le code source et installez-le manuellement. Il est disponible à: *http://thekelleys.org.uk/dnsmasq/doc.html*.

Afin d'activer dnsmasq nous n'avons qu'à taper quelques lignes du fichier de configuration de dnsmasq, **`/etc/dnsmasq.conf`**.

Le fichier de configuration est bien documenté, et propose de nombreuses options pour différents types de configuration. Pour activer le serveur DHCP nous devons éliminer les commentaires et/ou taper deux lignes.

Trouvez les lignes qui commencent par:

```
interface=
```

...et assurez-vous qu'elles stipulent:

```
interface=wlan0
```

...changez wlan0 par le nom de votre interface sans fil. Puis, trouvez les lignes qui commencent par:

```
#dhcp-range=
```

Éliminez le commentaire de la ligne et éditez-la pour y mettre les adresses que vous utilisez, par exemple:

```
dhcp-range=10.0.0.10,10.0.0.110,255.255.255.0,6h
```

Puis, sauvegardez le fichier et lancez dnsmasq:

```
# /etc/init.d/dnsmasq start
```

Vous devriez à présent pouvoir vous connecter au serveur comme point d'accès et d'obtenir une adresse IP grâce à DHCP. Ceci doit vous permettre de vous connecter à Internet à travers le serveur.

### Ajouter plus de sécurité: configurer un pare-feu

Une fois qu'il est installé et testé, vous pouvez ajouter des règles supplémentaires de pare-feu en utilisant n'importe quel outil pare-feu inclus dans votre distribution. Voici quelques applications qui vous permettront de configurer votre pare-feu:

- ***firestarter*** – un client graphique pour *Gnome* qui requiert que votre serveur fonctionne sur *Gnome*
- ***knetfilter*** – un client graphique pour *KDE* qui requiert que votre serveur fonctionne sur *KDE*
- ***Shorewall*** – un ensemble de programmes et de fichiers de configuration qui rendront plus facile la configuration du pare-feu iptables. Il y aussi d'autres interfaces pour *shorewall*, tel que *webmin-shorewall*
- ***fwbuilder*** - un puissant outil graphique, mais un peu complexe qui vous permettra de créer des règles iptables sur un autre ordinateur que votre serveur pour ensuite les transférer à celui-ci. Ceci n'exige pas un bureau graphique sur le serveur et il s'agit d'une bonne option pour la sécurité.

Une fois que tout est correctement configuré, assurez-vous que toutes les configurations sont reflétées dans le programme de démarrage du système. De cette façon, vous ne perdrez pas vos changements si l'ordinateur doit être redémarré.

## Scénario 2: Faire du point d'accès un pont transparent

Ce scénario peut être employé pour un répéteur de deux radios et pour un point d'accès connecté à Ethernet. Nous utilisons un pont au lieu de routeur lorsque nous voulons que les deux interfaces sur ce point d'accès partagent le même sous réseau. Ceci peut être particulièrement utile pour les réseaux

à multiples points d'accès où nous préférons avoir un seul pare-feu central et peut-être un serveur d'authentification. Puisque tous les clients partagent le même sous-réseau, ils peuvent facilement travailler avec un seul serveur DHCP et un pare-feu sans avoir besoin de relai DHCP.

Par exemple, vous pourriez installer un serveur selon le premier scénario, mais utiliser deux interfaces câblées Ethernet au lieu d'une câblée et d'une sans fil. Une interface serait votre connexion Internet et l'autre se connecterait à un commutateur (*switch*). Connectez ensuite autant de points d'accès que vous le désirez au même commutateur, configurez-les en tant que ponts transparents et tout le monde aura à traverser le même pare-feu et utiliser le même serveur DHCP.

Cependant, la simplicité des ponts suppose un coût au niveau de l'efficacité. Comme tous les clients partagent le même sous-réseau, le trafic sera répété dans tout le réseau. Ceci ne cause habituellement aucun désavantage pour les petits réseaux, mais à mesure que le nombre de clients augmente, une plus grande quantité de bande passante sans fil sera gaspillée pour le trafic de transmission du réseau.

## Configuration initiale

L'installation initiale d'un point d'accès configuré en tant que pont est semblable à celle d'un point d'accès avec mascarade mais sans la nécessité de dnsmasq. Suivez les instructions initiales d'installation de l'exemple précédent.

En outre, le paquet ***bridge-utils*** est exigé pour installer un pont. Ce paquet existe pour Ubuntu et d'autres distributions Debian, ainsi que pour Fedora Core. Assurez-vous qu'il soit installé et que la commande **`brctl`** soit disponible avant de procéder.

## Configurer les interfaces

Sur Ubuntu ou Debian la configuration des interfaces se réalise en éditant le fichier: **`/etc/network/interfaces`**.

Ajoutez une section comme la suivante, mais changez le nom des interfaces et des adresses IP en conséquence. L'adresse IP et le masque réseau doivent être les mêmes que ceux de votre réseau existant. Cet exemple suppose que vous construisez un répéteur sans fil avec deux interfaces sans fil, wlan0 et wlan1. Dans cet exemple, l'interface wlan0 sera un client pour le réseau nommé "office" et wlan1 créera un réseau appelé «repeater».

Ajouter les commandes suivantes à: **`/etc/network/interfaces`**

```
auto br0
iface br0 inet static
  address 192.168.1.2
  network 192.168.1.0
  netmask 255.255.255.0
  broadcast 192.168.1.255
  gateway 192.168.1.1
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid “office” mode Managed
  pre-up iwconfig wlan1 essid “repeater” mode Master
  bridge_ports wlan0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
```

Commentez toute autre ligne qui fait référence à wlan0 ou à wlan1 pour vous assurer qu'elles n'interfèrent pas avec votre configuration.

La syntaxe pour configurer des ponts par l'intermédiaire du fichier **interfaces** est spécifique aux distributions Debian, et les détails pour installer le pont sont fournis par un couple de scripts: **/etc/network/if-pre-up.d/bridge** et **/etc/network/if-post-down.d/bridge**.

La documentation pour ces programmes est disponible dans: **/usr/share/doc/bridge-utils/**.

Si ces programmes n'existent pas sur votre distribution (telle que Fedora Core), voici une configuration alternative pour **/etc/network/interfaces** qui donnera le même résultat mais avec un peu plus de tracas:

```
iface br0 inet static
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid “office” mode Managed
  pre-up iwconfig wlan1 essid “repeater” mode Master
  pre-up brctl addbr br0
  pre-up brctl addif br0 wlan0
  pre-up brctl addif br0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
  post-down brctl delif br0 wlan0
  post-down brctl delif br0 wlan1
  post-down brctl delbr br0
```

## Mise en marche du pont

Une fois que le pont est défini en tant qu'interface, il suffit de taper la commande suivante pour le mettre en marche:

```
# ifup -v br0
```

Le “-v” signifie *verbose output* et vous informera de ce qui se passe.

Sur Fedora Core (c.-à-d. les distributions non-Debian) vous aurez quand même à donner une adresse IP à votre pont et à ajouter une route par défaut au reste du réseau:

```
#ifconfig br0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
#route add default gw 192.168.1.1
```

Vous devriez maintenant être en mesure de connecter un ordinateur portable sans fil à ce nouveau point d’accès et de le connecter à Internet (ou au moins au reste de votre réseau) à travers cet ordinateur.

Si vous désirez avoir plus d’informations sur votre pont et ce qu’il fait, jetez un coup d’œil à la commande brctl. Essayez par exemple la commande suivante:

```
# brctl show br0
```

Ceci devrait vous donner de l’information sur ce que fait votre pont.

## Scénario 1 & 2: la manière facile

Au lieu d'installer votre ordinateur comme point d'accès à partir de zéro, vous pouvez utiliser une distribution Linux créée à cette fin. Ces distributions peuvent rendre le travail aussi simple que de démarrer votre ordinateur équipé d’une interface sans fil à partir d’un CD. Pour plus d’information, voyez la section suivante, « les systèmes d'exploitation conviviaux avec la technologie sans fil ».

Comme vous pouvez le voir, il est facile de créer un point d'accès à partir d’un routeur standard Linux. Utiliser Linux vous donne sensiblement plus de contrôle sur la façon dont les paquets sont routés à travers votre réseau et propose des options qui ne sont pas disponibles sur un équipement pour consommateurs.

Par exemple, vous pourriez commencer par l'un ou l'autre des deux exemples ci-dessus et mettre en application un réseau sans fil privé où les utilisateurs sont authentifiés en utilisant un navigateur web standard. En utilisant un portail captif tel que *Chillispot*, les identifications des utilisateurs peuvent être vérifiées sur une base de données existante (par exemple, un serveur de domaine Windows accessible via RADIUS). Cette configuration peut permettre un accès préférentiel aux utilisateurs enregistrés dans la base de données, tout en fournissant un niveau très limité d'accès pour le grand public.

Une autre application populaire est la vente de temps de connexion. Dans ce modèle, les utilisateurs doivent acheter un ticket avant d'accéder au réseau. Ce ticket fournit un mot de passe qui est valide pour une quantité de temps limitée (en général un jour). Quand le ticket expire, l'utilisateur doit en acheter d'autres. Ce système de vente de tickets est disponible sur les équipements de réseau commercial relativement cher, mais peut être mis en place en utilisant des logiciels libres tel que Chillispot et phpMyPrePaid. Nous verrons plus en détail la technologie de portails captifs et du système de tickets dans la section **Authentification** du chapitre six.

## Systèmes d'exploitation conviviaux avec la technologie sans fil

Il y a un certain nombre de systèmes d'exploitation libres qui fournissent des outils utiles pour travailler avec les réseaux sans fil. Ceux-ci ont été conçus pour être employés avec des ordinateurs recyclés ou tout autre matériel de gestion de réseau (plutôt que sur un ordinateur portable ou un serveur) et sont bien configurés et optimisés pour construire des réseaux sans fil. Certains de ces projets incluent:

- **Freifunk**. Basé sur le projet OpenWRT (*http://openwrt.org/*), le progiciel Freifunk offre un support OLSR facile pour les points d'accès de consommateurs basés sur MIPS, tel que les Linksys WRT54G / WRT54GS / WAP54G, Siemens SE505, et autres. En flashant simplement (c.-à-d. réécrire sa mémoire flash) un de ces APs avec le progiciel Freifunk, vous pouvez rapidement construire une maille OLSR autonome. Freifunk n'est actuellement pas disponible pour l'architecture x86. Il est maintenu par Sven Ola du groupe sans fil Freifunk à Berlin. Vous pouvez télécharger les *firmware* à l'adresse suivante: *http://www.freifunk.net/wiki/FreifunkFirmware*.
- **Metrix Pebble**. Le projet Pebble Linux a été lancé en 2002 par Terry Schmidt du groupe *NYCwireless*. C'était à l'origine une version dépouillée de la distribution Debian Linux qui inclut un pare-feu sans fil, des outils de gestion de réseau et de routage. Depuis 2004, *Metrix Communication* a prolongé le projet Pebble pour y inclure des pilotes mis à jour, de la surveillance de bande passante et un outil de configuration web. Le but du Pebble Metrix est de fournir une plateforme complète pour le développement sans fil. Il fonctionne sur les architectures x86 avec au moins 64MB de mémoire flash ou de disque dur. Vous pouvez le télécharger à l'adresse suivante: *http://metrix.net/metrix/howto/metrix-pebble.html*.
- **m0n0wall**. Basé sur FreeBSD, m0n0wall est un très petit paquet mais pare-feu complet qui fournit des services AP. Il se configure à partir d'une interface web et le système complet de configuration est stocké dans un simple fichier XML. Sa taille minuscule (moins de 6 MB) le rend attrayant pour une utilisation dans les systèmes embarqués très petits. Son but est

de fournir un pare-feu sécuritaire et, en tant que tel, il n'inclut pas d'outils utilisateurs (il n'est pas possible de se connecter à l'ordinateur en dehors du réseau). En dépit de cette limitation, c'est un choix populaire pour les équipements sans fil, en particulier ceux qui ont une certaine connaissance de FreeBSD. Vous pouvez le télécharger sur: *http://www.m0n0.ch/*.

Toutes ces distributions sont conçues pour s'adapter à des ordinateurs à stockage limité. Si vous employez un disque flash de grande capacité ou un disque dur, vous pouvez certainement installer un OS plus complet (tel qu'Ubuntu ou Debian) et utiliser l'ordinateur comme routeur ou point d'accès. De toute façon, vous devrez probablement investir une quantité non négligeable de temps pour vous assurer que tous les outils nécessaires sont inclus, afin de ne pas installer des paquets inutiles. En employant un de ces projets comme point de départ pour créer un noeud sans fil, vous économiserez considérablement de temps et d'efforts.

## Le Linksys WRT54G

Un des points d'accès actuellement les plus populaires chez les consommateurs est le Linksys WRT54G. Ce point d'accès comporte deux connecteurs externes d'antenne RP-TNC, un commutateur Ethernet quatre ports et une radio 802.11b/g. Il se configure à partir d'une simple interface web. Même s'il n'est pas conçu comme solution extérieure, il peut être installé dans une boîte ou un tuyau en plastique pour un coût relativement peu élevé. Actuellement, le WRT54G se vend environ $60.

En 2003, des bidouilleurs se sont rendus compte que le micrologiciel (*firmware*) qui se vendait avec le WRT54G était en fait une version de Linux. Ceci a entraîné un vif intérêt pour la création de *firmwares alternatifs* qui peuvent augmenter de manière significative les possibilités du routeur. Certains de ces nouveaux *firmwares* incluent un support du mode radio client, des portails captifs et réseau maillé (*mesh*). Deux *firmwares* alternatifs populaires pour le WRT54G sont OpenWRT (*http://openwrt.org/*) et Freifunk (*http://www.freifunk.net/wiki/FreifunkFirmware*).

Malheureusement, en automne 2005, Linksys a lancé la version 5 du WRT54G. Cette nouvelle version est équipée de beaucoup moins de mémoire RAM et de stockage flash sur la carte mère, ce qui rend presque impossible le fonctionnement de Linux (de fait, il fonctionne avec VxWorks, un système d'exploitation beaucoup plus petit dont la personnalisation est plus compliquée). Puisque le WRT54G v5 ne peut pas faire fonctionner les *firmwares* Linux personnalisés, il devient une alternative moins attrayante pour les constructeurs de réseau. Linksys a également sorti le WRT54GL, qui est essentiellement le WRT54G v4 (qui fonctionne avec Linux) à un prix légèrement plus élevé.

D'autres points d'accès Linksys fonctionnent également sous Linux, y compris le WRT54GS et le WAP54G. Même si ceux-ci ont également des prix relativement bas, les caractéristiques de l'équipement peuvent changer à tout moment. Il est difficile de savoir de quelle version du matériel il s'agit sans ouvrir l'emballage, il est de fait risqué de les acheter dans un magasin et pratiquement impossible de passer une commande en ligne. Même si le WRT54GL fonctionne sous Linux, Linksys a clairement dit qu'il ne compte pas vendre ce modèle en grand volume et est resté imprécis sur la durée durant laquelle ce matériel sera proposé à la vente.

Si vous pouvez vous procurer une version précédente de WRT54Gs ou WRT54GLs, ceux-ci sont des routeurs maniables et peu coûteux. Avec des *firmwares* personnalisés, ils peuvent être configurés pour fonctionner en tant que nœud d'un réseau maillé ou en mode client et fonctionnent très bien comme solution bon marché côté client. Même si le nouveau modèle v5 fonctionnera en tant que point d'accès, il ne peut être configuré comme client et a des évaluations de performances partagées comparées au v4 et aux autres modèles précédents.

Pour plus d'information visitez un de ces sites Web:

- *http://linksysinfo.org/*
- *http://seattlewireless.net/index.cgi/LinksysWrt54g*

# 6
# Sécurité

Dans un réseau câblé traditionnel, le contrôle d'accès est très simple: si une personne à un accès physique à un ordinateur ou à un concentrateur du réseau, alors elle peut utiliser (ou abuser) des ressources de ce réseau. Tandis que les mécanismes de logiciel sont une composante importante en sécurité de réseau, la limitation de l'accès physique aux appareils du réseau est le mécanisme ultime de contrôle d'accès. Si tous les terminaux et composantes du réseau sont uniquement accessibles par des individus de confiance, alors le réseau est probablement fiable.

Les règles changent de manière significative avec les réseaux sans fil. Même si la portée apparente de votre point d'accès peut sembler n'être que de quelques centaines de mètres, un usager avec une antenne à haut gain peut se servir du réseau à une distance de plusieurs pâtés de maison. Un usager non autorisé peut être détecté, mais il est impossible de retracer l'endroit où il se trouve. Sans transmettre un seul paquet, un usager malicieux peut même enregistrer toutes les données du réseau sur un disque. Ces données peuvent plus tard être employées pour lancer une attaque plus sophistiquée contre le réseau. Il ne faut jamais supposer que les ondes radio «s'arrêtent» simplement au bord de votre ligne de propriété.

Naturellement, même dans les réseaux câblés, il n'est jamais tout à fait possible de faire totalement confiance à tous les usagers du réseau. Les employés contrariés, les usagers connaissant peu les réseaux et les erreurs simples de la part d'usagers honnêtes peuvent causer des complications significatives au fonctionnement du réseau. En tant qu'architecte de réseau, votre but devrait être de faciliter la communication privée entre les usagers légitimes. Même si une certaine quantité de contrôle d'accès et d'authentification soit nécessaire dans n'importe quel réseau, vous aurez échoué dans votre travail si les usagers légitimes ont de la difficulté à utiliser le réseau pour communiquer.

Un vieil adage dit que la seule manière de rendre un ordinateur complètement sécuritaire est de le débrancher, l'enfermer dans un coffre-fort, détruire la clef et d'enterrer le tout dans le béton. Un tel système peut être complètement « sécuritaire » mais est inutile à la communication. Lorsque vous prenez des décisions de sécurité pour votre réseau, vous ne devez jamais

oublier ceci: le réseau existe afin que ses usagers puissent communiquer entre eux. Les considérations de sécurité sont importantes, mais ne devraient pas barrer la route aux usagers du réseau.

# Sécurité physique

En installant un réseau, vous établissez une infrastructure dont les gens dépendront. Le réseau doit donc être fiable. Pour plusieurs installations, les pannes se produisent souvent en raison du trifouillage humain, accidentel ou pas. Les réseaux sont physiques, des câbles et des boîtes, c'est-à-dire des choses qui sont facilement déplacées et manipulées. Dans plusieurs installations, les gens ne sauront reconnaître l'équipement que vous aurez installé, ou encore, la curiosité les mènera à expérimenter. Ils ne se rendront pas compte de l'importance d'un câble qui va à un port. On pourraient déplacer un câble Ethernet afin d'y connecter un ordinateur portatif pendant 5 minutes ou déplacer un commutateur parce qu'il est dans leur chemin. Une prise pourrait être enlevée d'une barre de puissance parce que quelqu'un a besoin de ce réceptacle. Assurer la sécurité physique d'une installation est primordial. Les avertissements et les écriteaux ne seront utiles que pour certains, ceux qui peuvent lire ou parler votre langue. Placer les choses à l'écart et y limiter l'accès est le meilleur moyen d'empêcher les accidents ou le bricolage inopportun.

Au sein d'économies moins développées, les attaches et les boîtiers ne seront pas faciles à trouver. Cenpendant, vous devriez pouvoir trouver des alimentations électriques qui fonctionneront aussi bien. Les boîtiers personnalisés sont également faciles à fabriquer et devraient être considérés essentiels à n'importe quelle installation. Dans les pays du sud, il est souvent économique de payer un maçon pour faire des trous et installer un conduit, ce qui serait une option couteuse dans le monde développé. Du PVC peut être inséré dans des murs de ciment pour passer un câble d'une pièce à l'autre, ce qui évite de faire des trous chaque fois qu'un câble doit être passé. Pour isoler, des sachets en plastique peuvent être placés dans le conduit autour des câbles.

L'équipement de petite taille devrait être monté au mur et l'équipement plus grand devrait être placé dans un cabinet ou dans un coffret.

## Commutateurs

Les commutateurs, les concentrateurs ou les points d'accès intérieurs peuvent, à l'aide d'une prise murale, être vissés directement sur un mur. Il est préférable de placer cet équipement aussi haut que possible afin d'éviter qu'une personne ne touche au dispositif ou à ses câbles.

## Câbles

Les câbles devraient être cachés et attachés. Il est préférable d'enterrer les câbles plutôt que de les laisser pendre dans la cour où ils pourraient être utilisés pour suspendre des vêtements ou simplement être accrochés par une échelle, etc. Pour éviter la vermine et les insectes, vous devez trouver un conduit électrique en plastique. Ce sera une mince dépense qui vous évitera des ennuis. Le conduit devrait être enterré à environ 30 cm de profondeur (sous la glace dans le cas des climats froids). Il est également intéressant d'acheter un conduit plus grand que nécessaire de sorte que de futurs câbles puissent y être placés. Il est également possible de trouver un conduit pour câbles en plastique qui peut être utilisé à l'intérieur des bâtiments. Si non, des attaches de câble simples, clouées au mur peuvent être utilisées pour fixer le câble et pour s'assurer qu'il ne traîne pas là où il pourrait être accroché, pincé ou coupé.

## Puissance

Il est préférable d'avoir des barres de puissance enfermées à clef dans un coffret. Si ce n'est pas possible, placez la barre de puissance sous un bureau ou sur le mur et utilisez de la bande adhésive toilée imperméable (*duct tape* en anglais, un ruban adhésif robuste) pour fixer la prise dans le réceptacle. Sur l'UPS et la barre de puissance, ne laissez pas de réceptacles vides. Au besoin, placez du ruban adhésif pour les couvrir. Les gens ont tendance à employer le réceptacle le plus accessible: rendez-les donc difficiles à utiliser. Si vous ne le faites pas, vous pourriez trouver un ventilateur ou une lumière branchée à votre UPS. Même s'il est bien d'avoir de la lumière, il est encore mieux de voir votre serveur fonctionner!

## Eau

Protégez votre équipement contre l'eau et l'humidité. Dans tous les cas, veillez à ce que votre équipement, y compris votre UPS, est à au moins 30 cm de la terre, pour éviter les inondations. Essayez en outre de placer un toit sur votre équipement, de sorte que l'eau et l'humidité ne pénètrent pas dessus. Dans des climats humides, il est important de s'assurer que l'équipement ait la ventilation appropriée afin que l'humidité puisse être éliminée. Les petits cabinets doivent avoir de la ventilation, sans quoi l'humidité et la chaleur risquent de dégrader voire détruire votre équipement.

## Mâts

L'équipement installé sur un mât est souvent sécuritaire face aux voleurs. Néanmoins, pour décourager les voleurs et pour maintenir votre équipement sécuritaire par rapport au vent, il est conseillé d'avoir des assemblages spé-

ciaux qui vont au delà de l'ingénierie. L'équipement devrait être peint d'une couleur mate, blanche ou grise pour refléter le soleil et le rendre ennuyeux et inintéressant. Les antennes plates sont beaucoup plus subtiles et moins intéressantes que les paraboliques et devraient donc être choisie de préférence. Toute installation placée au mur exige une échelle pour l'atteindre. Essayez de choisir un endroit bien éclairé mais non proéminent pour mettre l'équipement. Évitez en outre les antennes qui ressemblent à des antennes de télévision, car ce sont des articles qui attireront l'intérêt des voleurs. Une antenne WiFi sera inutile au plus commun des voleurs.

# Menaces pour le réseau

Une différence critique entre Ethernet et la technologie sans fil est que les réseaux sans fil sont construits dans un ***milieu partagé***. Ils ressemblent plus étroitement aux vieux concentrateurs (*hub*) de réseau qu'aux commutateurs (switch) modernes, du fait que chaque ordinateur connecté au réseau « voit » le trafic de tout autre usager. Pour surveiller tout le trafic de réseau sur un point d'accès, on peut simplement synthoniser le canal qui est employé, placer la carte réseau dans le mode moniteur et prendre note de chaque trame. Ces données peuvent avoir beaucoup de valeur pour une oreille indiscrète (des données telles que le courriel, la voix ou des extraits de clavardages). Elles peuvent également fournir des mots de passe et d'autres données ayant une valeur importante, menaçant davantage le réseau. Nous le verrons plus tard dans ce chapitre, ce problème peut être atténué par l'utilisation du chiffrement.

Un autre problème sérieux avec les réseaux sans fil est que ses usagers sont relativement ***anonymes***. Même s'il est vrai que chaque dispositif sans fil possède une adresse MAC fournie par le fabriquant, ces adresses peuvent souvent être changées avec un logiciel. Même avec l'adresse MAC en main, il peut être très difficile de localiser l'emplacement d'un usager sans fil. Les effets par trajets multiples, les antennes à haut gain et les caractéristiques considérablement variables des transmetteurs radio empêchent de déterminer si un usager sans fil malveillant s'assied dans la salle contiguë ou se trouve dans un immeuble à plusieurs kilomètres de distance.

Même si le spectre sans licence fournit d'énormes économies à l'usager, il a l'effet secondaire malheureux de rendre très simple les attaques par ***déni de service*** (*Denial of Service- DoS* en anglais). Une personne malveillante peut causer des problèmes significatifs sur le réseau, simplement en mettant en marche un point d'accès à puissance élevé, un téléphone sans fil, un transmetteur vidéo ou tout autre dispositif à 2,4GHz. Plusieurs autres dispositifs réseau sont également vulnérables à d'autres formes d'attaques par déni de service, tels que les attaques de désassociassions et la corruption de la table ARP.

Voici plusieurs catégories d'individus qui peuvent poser des problèmes sur un réseau sans fil:

- ***Usagers involontaires***. Puisque de plus en plus de réseaux sans fil sont installés dans des secteurs très peuplés, il est courrant que des usagers d'ordinateur portatif s'associent accidentellement au mauvais réseau. Lorsque leur réseau préféré n'est pas disponible, la plupart des clients sans fil choisiront simplement n'importe quel autre réseau sans fil disponible. L'usager peut alors se servir de ce réseau comme d'habitude, en ignorant complètement qu'il peut être en train de transmettre des données de valeur sur le réseau de quelqu'un d'autre. Les personnes malveillantes peuvent même tirer profit de ceci en installant des points d'accès dans des endroits stratégiques, pour essayer d'attirer des usagers inconscients et pour saisir leurs données.

  Le premier pas pour éviter ce problème est d'instruire vos usagers et souligner l'importance de se connecter uniquement à des réseaux connus et fiables. Plusieurs clients sans fil peuvent être configurés pour se connecter seulement à des réseaux fiables ou pour demander la permission avant de joindre un nouveau réseau. Comme nous le verrons plus tard dans ce chapitre, les usagers peuvent se connecter sans risque à des réseaux publics ouverts en employant un chiffrement fort.

- ***Wardrivers***. Le phénomène du « *wardriving* » tire son nom du film populaire « Jeux de guerre » de 1983 sur des pirates informatiques. Le but des wardrivers est de trouver l'endroit physique des réseaux sans fil. Habituellement, ils conduisent autour d'une zone donnée avec un ordinateur portatif, un GPS et une antenne omnidirectionnelle, notant le nom et l'endroit de tous les réseaux qu'ils trouvent. Ces notations sont alors combinées avec les notations d'autres *wardrivers* et sont transformées en cartes graphiques localisant toute trace de réseau sans fil d'une ville particulière.

  La grande majorité des *wardrivers* ne constituent probablement aucune menace directe pour les réseaux, mais les données qu'ils assemblent pourraient être d'intérêt pour ceux qui désirent détruire un réseau donné. Par exemple, un point d'accès non protégé détecté par un *wardriver* pourrait être situé à l'intérieur d'un bâtiment stratégique, tel qu'un bureau gouvernemental ou corporatif. Une personne malveillante pourrait employer cette information pour accéder illégalement à ce réseau. On pourrait argumenter qu'un tel AP ne devrait jamais avoir été installé en premier lieu, mais le *wardriving* rend le problème encore plus urgent. Comme nous le verrons plus tard dans ce chapitre, les wardrivers qui emploient le programme de grande diffusion NetStumbler peuvent être détectés avec des programmes tels que Kismet. Pour plus d'informations sur le *wardriving*, visitez les sites Web tels que: *http://www.wifimaps.com/*, *http://www.nodedb.com/* ou *http://www.netstumbler.com/*.

- ***Points d'accès illicites***. Il y a deux classes générales de points d'accès illicites: ceux incorrectement installés par les usagers légitimes et ceux installés par les personnes malveillantes qui ont l'intention de rassembler des données d'autrui ou de nuire au réseau. Dans le cas le plus simple, un usager légitime du réseau peut vouloir une meilleure couverture sans fil pour son bureau, ou encore trouver que les restrictions de sécurité au réseau sans fil corporatif sont trop difficiles de satisfaire. En installant un point d'accès peu coûteux sans permission, l'usager ouvre le réseau entier et le rend susceptible de subir des attaques potentielles de l'intérieur. Même s'il est possible d'identifier les points d'accès non autorisés sur votre réseau câblé, il est extrêmement important de mettre en place une politique claire les interdisant.

  Il peut être très difficile de traiter avec la deuxième classe de point d'accès illicite. En installant une AP de haute puissance qui emploie le même ESSID comme réseau existant, une personne malveillante peut duper des personnes et les mener à utiliser leur équipement et noter ou même manipuler toutes les données qui passent à travers lui. Or, si vos usagers ont été formés pour employer un chiffrage fort, ce problème est sensiblement réduit.

- ***Oreilles indiscrètes***. Tel que mentionné précédemment, l'écoute clandestine est un problème très difficile à traiter sur les réseaux sans fil. En utilisant un outil de surveillance passif (tel que Kismet), une oreille indiscrète peut noter toutes les données d'un réseau à une grande distance, sans que personne ne puisse détecter leur présence. Des données mal chiffrées peuvent simplement être notées et déchiffrées plus tard, alors que des données non codées peuvent facilement être lues en temps réel.

  Si vous avez de la difficulté à convaincre les autres de l'existence de ce problème, vous pourriez vouloir faire une démonstration à l'aide d'outils tels qu'Etherpeg (*http://www.etherpeg.org/*) ou Driftnet (*http://www.ex-parrot.com/~chris/driftnet/*). Ces outils observent un réseau sans fil pour des données graphiques, telles que des fichiers GIF et JPEG. Tandis que d'autres usagers naviguent sur Internet, ces outils montrent tous les graphiques trouvés dans un collage graphique. J'utilise souvent des outils de ce type comme démonstration en parlant de la sécurité sans fil. Même si vous pouvez dire à un usager que leur courriel est vulnérable sans chiffrement, rien ne fait passer mieux le message que de leur montrer les images qu'ils sont en train de regarder dans leur navigateur Web.

  Même si elle ne peut être complètement éliminée, l'application appropriée du chiffrement fort découragera l'écoute clandestine.

Le but de cette introduction est de vous donner une idée des problèmes qui peuvent survenir en créant un réseau sans fil. Plus tard dans ce chapitre,

nous examinerons les outils et les techniques qui vous aideront à atténuer ces problèmes.

# Authentification

Avant de pouvoir avoir accès aux ressources de réseau, les usagers devraient d'abord être ***authentifiés***. Dans un monde idéal, chaque usager sans fil aurait un identificateur qui est unique, inchangeable et qui ne peut pas être personnifié par d'autres usagers. Ceci s'avère être un problème très difficile à résoudre dans le vrai monde.

Ce que nous avons de plus semblable à un identificateur unique est l'adresse MAC. Celle-ci est un nombre de 48-bit qui a été donné par le fabricant à chaque dispositif sans fil et Ethernet. En utilisant le ***filtrage mac*** sur nos points d'accès, nous pouvons authentifier des usagers en nous basant sur leurs adresses MAC. Avec ce dispositif, le point d'accès garde une table interne d'adresses MAC qui ont été approuvées. Quand un usager sans fil essaye de s'associer au point d'accès, l'adresse MAC du client doit se trouver sur la liste d'adresses approuvées sans quoi l'association sera refusée. Comme alternative, l'AP peut garder une table de "mauvaises" adresses MAC et accorder l'accès à tous les dispositifs qui ne sont pas sur cette liste.

Malheureusement, ce n'est pas un mécanisme idéal de sécurité. Maintenir des tables d'adresses MAC sur chaque dispositif peut être encombrant, exigeant de tous les dispositifs de client d'avoir leur adresse MAC enregistrée et téléchargée aux APs. Pire encore, les adresses MAC peuvent souvent être changées par un logiciel. En observant des adresses MAC en service sur un réseau sans fil, une personne malveillante peut s'approprier de l'une d'entre-elles afin de s'associer à l'AP. Même si le filtrage MAC empêchera les usagers involontaires et la plupart des curieux d'accéder au réseau, il ne pourra pas à lui seul empêcher toutes les attaques éventuelles.

Les filtres MAC sont utiles pour limiter temporairement l'accès des clients qui agissent avec malveillance. Par exemple, si un ordinateur portatif a un virus qui envoie de grandes quantités de pourriel ou tout autre trafic, son adresse MAC peut être ajoutée à la table de filtre pour arrêter le trafic immédiatement. Ceci vous donnera le temps nécessaire pour retracer l'usager et régler le problème.

Un autre dispositif populaire d'authentification sans fil est le ***réseau fermé***. Dans un réseau typique, les APs annonceront leur ESSID plusieurs fois par seconde, permettant aux clients sans fil (ainsi que des outils tels que NetStumbler) de trouver le réseau et de montrer sa présence à l'usager. Dans un réseau fermé, l'AP ne transmet pas l'ESSID et les usagers doivent savoir le nom complet du réseau avant que l'AP permette l'association. Ceci

empêche les usagers occasionnels de découvrir le réseau et de le choisir dans leur client sans fil.

Ce dispositif pose un certain nombre d'inconvénients. Forcer les usagers à saisir l'ESSID complet avant de se connecter au réseau favorise les erreurs ce qui se traduit souvent en appels et en plaintes. Puisque le réseau n'est évidemment pas présent dans des outils tel que le NetStumbler, ceci peut empêcher que vos réseaux apparaissent sur les cartes de wardriving. Mais cela signifie également que d'autres concepteurs de réseaux ne pourront pas trouver facilement votre réseau et ne sauront pas spécifiquement que vous utilisez déjà un canal donné. Un voisin consciencieux peut exécuter une enquête d'emplacement, ne détecter aucun réseau voisin, et installer son propre réseau sur le même canal que vous utilisez. Ceci causera des problèmes d'interférence tant pour vous que pour votre voisin.

En conclusion, employer des réseaux fermés n'ajoute pas grand chose à la sécurité globale de votre réseau. En utilisant des outils de surveillance passifs (tels que Kismet), un usager habile peut détecter les trames envoyées par vos clients légitimes à l'AP. Ces trames contiennent nécessairement le nom du réseau. Un usager malveillant peut alors employer ce nom pour s'associer au point d'accès comme le ferait un usager normal.

Le chiffrement est probablement le meilleur outil que nous avons pour authentifier les usagers sans fil. Avec un chiffrement fort, nous pouvons donner une identité unique à un usager de sorte qu'il soit très difficile de la corrompre et employer cette identité pour déterminer les futurs accès au réseau. Le chiffrement a également l'avantage de préserver la confidentialité en empêchant les oreilles indiscrètes d'observer facilement le trafic du réseau.

La méthode de chiffrement généralement la plus appliquée sur les réseaux sans fil est le ***chiffrement WEP*** (l'acronyme WEP signifie en anglais ***wired equivalent privacy*** ou confidentialité équivalente au réseau filaire en français). Ce type de chiffrement fonctionne pratiquement avec tout l'équipement 802.11a/b/g. WEP emploie une clef 40-bit partagée pour chiffrer des données entre le point d'accès et le client. La clef doit être entrée sur l'AP ainsi que sur chacun des clients. Avec le chiffrement WEP activé, les clients sans fil ne peuvent s'associer à l'AP jusqu'à ce qu'ils emploient la clef correcte. Une oreille indiscrète écoutant un réseau auquel le WEP est activé verra le trafic et les adresses MAC, mais les données utiles de chaque paquet seront chiffrées. Ceci fournit un assez bon mécanisme d'authentification tout en ajoutant un peu de confidentialité au réseau.

Le WEP n'est certainement pas la solution de chiffrement la plus forte disponible actuellement. Ceci est dû au fait que la clef WEP est partagée par tous les usagers. Si la clef est compromise (par exemple si un usager donne le mot de passe à un ami ou si un employé est mis à la porte) alors changer

le mot de passe peut être très difficile puisque tous les APs et dispositifs de client doivent également être changés. Ceci signifie aussi que les usagers légitimes du réseau peuvent toujours écouter le trafic des autres clandestinement, puisqu'ils connaissent tous la clef partagée.

La clef elle-même est souvent très mal choisie rendant possible le piratage sans être connecté. Pire encore, l'implantation du WEP elle-même est souvent défectueuse dans plusieurs applications, ce qui rend encore plus facile d'abîmer certains réseaux. Même si les fabricants ont mis en application un certain nombre d'extensions à WEP (tel que de plus longues clefs à rotation rapide), ces prolongements ne font pas partie de la norme, et ne seront pas interopérables entre les équipements de différents fabricants. En mettant à jour les progiciels les plus récents pour tous vos dispositifs sans fil, vous pouvez empêcher certaines des premières attaques trouvées dans WEP.

WEP peut toujours être un outil utile d'authentification. En supposant que vos utilisateurs sont assez fiables pour ne pas donner le mot de passe, vous pouvez être certain que vos clients sans fil sont légitimes. Même s'il est possible de déchiffrer le WEP, ceci est encore au-delà de la compétence de la plupart des usagers. Le WEP est extrêmement utile pour rendre sécuritaire des liens point à point de longue distance, même des réseaux généralement ouverts. En employant WEP sur un tel lien, vous découragerez d'autres de s'associer au lien et ils emploieront probablement d'autres APs disponibles à la place. Le WEP est l'équivalent d'un écriteau « défense d'entrer » pour votre réseau. N'importe qui détectant le réseau verra qu'une clef est exigée, ce qui indique du fait même qu'ils ne sont pas les bienvenus.

La plus grande force du chiffrement WEP est son interopérabilité. Afin d'être conforme aux normes, tous les dispositifs sans fil fonctionnent avec un WEP de base. Même si ce n'est pas la méthode la plus forte disponible, c'est certainement le dispositif le plus couramment mis en application. Nous verrons d'autres techniques de chiffrement plus avancées plus tard dans ce chapitre.

Pour plus de détails sur le chiffrement WEP, voir les documents suivants:

- *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*
- *http://www.cs.umd.edu/~waa/wireless.pdf*
- http://www.crypto.com/papers/others/rc4_*ksaproc*.ps

Un autre protocole d'authentification de la couche de liaison est l'***Accès Protégé Sans fil*** (***Wi-Fi Protected Access -WPA*** en anglais). Le WPA a spécifiquement été créé pour traiter les problèmes que pose le chiffrement WEP que nous avons cités précédemment. Il fournit un schéma de chiffrement sensiblement plus fort et peut employer une clef privée partagée, des clefs uniques assignées à chaque utilisateur ou même des certificats SSL pour

authentifier le client et le point d'accès. L'authentification est vérifiée en utilisant le protocole 802.1X, qui peut consulter une base de données d'une tierce partie telle que RADIUS. En utilisant le Protocole Principal Temporel d'Intégrité (du sigle en anglais TKIP), des clefs peuvent rapidement être modifiées ce qui réduit la probabilité qu'une session particulière puisse être déchiffrée. De façon générale, le WPA fournit une authentification et une confidentialité sensiblement meilleures que le WEP standard.

La difficulté que pose actuellement le WPA est que l'interopérabilité entre les fournisseurs est encore très faible. Le WPA exige un équipement de point d'accès de dernière génération et des progiciels mis à jour sur tous les clients sans fil, ainsi qu'une quantité substantielle de configuration. Si vous installez un réseau dans un emplacement où vous contrôlez la plateforme entière d'équipements, le WPA peut être idéal. En authentifiant les clients et les APs, il résout le problème des points d'accès illicites et fournit plusieurs avantages significatifs par rapport au chiffrement WEP. Mais dans la plupart des installations de réseau où l'équipement est très varié et la connaissance des usagers sans fil est limitée, l'installation de WPA peut rapidement devenir un cauchemar. Pour toutes ces raisons, là où le chiffrement est effectivement employé, le WEP continue à être utilisé.

## Portails captifs

Un outil d'authentification couramment utilisé sur les réseaux sans fil est le ***portail captif***. Un portail captif emploie un navigateur Web standard pour donner à un usager sans fil l'occasion de présenter son accréditation pour l'ouverture de la session. Il peut également être employé pour présenter à l'usager une certaine information (telle qu'une Politique d'Utilisation Acceptable) avant d'accorder l'accès total. Du fait qu'ils emploient un navigateur Web au lieu d'un programme personnalisé d'authentification, les portails captifs fonctionnent avec pratiquement tous les ordinateurs portatifs et les logiciels d'exploitation. Les portails captifs sont typiquement employés sur des réseaux ouverts sans d'autres méthodes d'authentification (tels que les filtres WEP ou MAC).

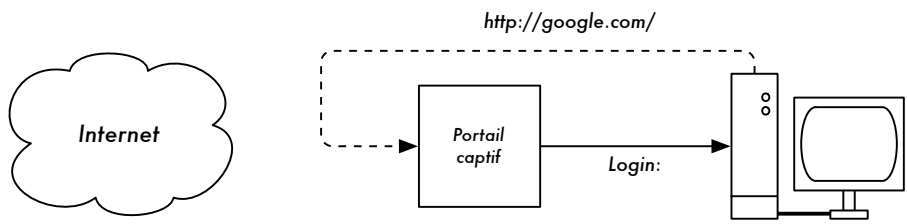


*Figure 6.1: L'usager veut aller sur page Web et est redirigé.*

Pour commencer, un usager sans fil ouvre son ordinateur portatif et choisit un réseau. Son ordinateur demande un bail DHCP, qui est accordé. L'usager emploie alors son navigateur Web pour visiter n'importe quel site sur Internet.

Au lieu de recevoir la page demandée, on présente un écran d'ouverture à l'usager. Cette page peut exiger de celui-ci qu'il entre un nom d'usager et un mot de passe, qu'il clique simplement sur un bouton d' « ouverture », qu'il saisisse les chiffres d'un ticket prépayé ou qu'il entre toute autre accréditation exigée par les administrateurs de réseau. L'usager entre alors son accréditation qui est vérifiée par un point d'accès ou un autre serveur sur le réseau. Tout autre accès au réseau est bloqué jusqu'à ce que ses accréditations soient vérifiées.

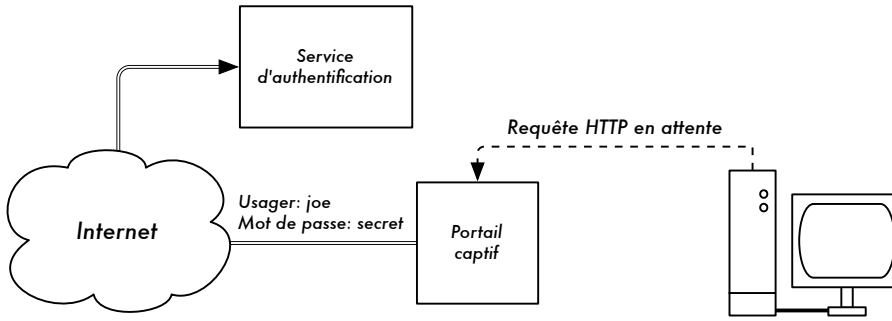


*Figure 6.2: Les accréditations de l'usager sont vérifiées avant de lui permettre un accès complet. Le serveur d'authentification peut être le point d'accès lui-même, un autre ordinateur sur le réseau local ou un serveur n'importe où sur Internet.*

Une fois authentifié, on permet à l'usager d'avoir accès à toutes les ressources du réseau et, normalement, on le redirige au site qu'il avait demandé au début.

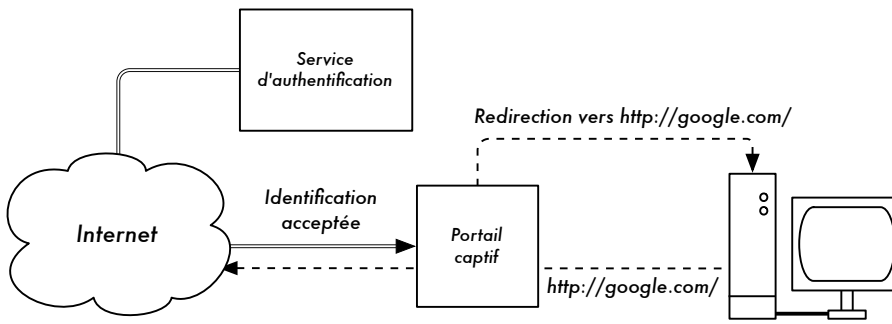


*Figure 6.3: Une fois authentifié, l'usager peut avoir accès au reste du réseau.*

Les portails captifs ne fournissent aucun chiffrement pour les usagers sans fil. Ils comptent plutôt sur les adresses MAC et IP comme unique identification. Puisque ceci n'est pas nécessairement très sécuritaire, on demandera à l'usager de s'authentifier à nouveau périodiquement. Ceci peut ce faire automatiquement en réduisant au minimum une fenêtre flottante ou pop-up spéciale du navigateur lorsque l'utilisateur entre pour la première fois.

Puisqu'ils ne fournissent pas de chiffrement fort, les portails captifs ne sont pas un très bon choix pour les réseaux qui doivent être fermés pour ne permettre l'accès qu'à des usagers fiables. Ils conviennent davantage aux cafés, aux hôtels et autres endroits d'accès publics utilisés par des usagers occasionnels de réseau.

Dans des installations de réseau publiques ou semi-publiques, les techniques de chiffrement telles que le WEP et le WPA sont inutiles. Il n'y a simplement aucune manière de distribuer des clefs publiques ou partagées aux membres du grand public sans compromettre la sécurité de ces clefs. Dans ces installations, une application plus simple telle qu'un portail captif fournit un niveau de service qui se trouve entre un service complètement ouvert et un service complètement fermé.

NoCatSplash et Chillispot sont deux logiciels libre de portails captifs.

# NoCatSplash

Si vous devez simplement fournir à des usagers d'un réseau ouvert de l'information et une Politique d'Utilisation Acceptable, jetez un coup d'oeil à NoCatSplash. Il est disponible en ligne à l'adresse suivante: *http://nocat.net/download/NoCatSplash/*.

NoCatSplash fournit à vos usagers une page de présentation (ou page *splash*) personnalisable, exigeant qu'ils cliquent sur un bouton d' « ouverture » avant d'employer le réseau. Ceci est utile pour identifier les opérateurs du réseau et montrer les règles pour l'accès au réseau.

NoCatSplash en est écrit en C et fonctionnera sur à peu près tous les systèmes d'exploitation du type Unix, incluant Linux, BSD et même les plateformes embarquées telles qu'OpenWRT. Il présente un fichier simple de configuration et peut servir n'importe quel fichier HTML personnalisé comme page de présentation. Il fonctionne typiquement directement sur un point d'accès, mais également sur un routeur ou un serveur proxy. Pour plus d'informations, visitez l'adresse suivante: *http://nocat.net/*.

## D'autres projets de points chauds populaires

NoCatSplash n'est qu'une application de portail captif. Il existe également plusieurs autres créations de source libre qui offrent une gamme diverse de fonctionnalités. En voici certaines:

- Chillispot (*http://www.chillispot.org/*). Chillispot est un portail captif conçu pour authentifier à l'aide d'une base de données d'accréditations d'usagers existante telle que RADIUS. Combiné avec l'application phpMyPrePaid, l'authentification basée sur les tickets prépayés peut être installée très fac-

ilement. Vous pouvez télécharger phpMyPrePaid à l'adresse suivante: *http://sourceforge.net/projects/phpmyprepaid/*.

- WiFi Dog (*http://www.wifidog.org/*). WiFi Dog fournit un paquet d'authentification de portail captif très complet dans un très petit espace (typiquement sous 30 kb). Du point de vue de l'usager, il n'exige aucun support pop-up ou Javascript, ce qui lui permet de fonctionner sur une plus grande variété de dispositifs sans fil.
- m0n0wall (*http://m0n0.ch/wall/*). Comme nous l'avons vu au chapitre cinq, m0n0wall est un système d'exploitation embarqué complet basé sur FreeBSD. Il inclue un portail captif avec support RADIUS, ainsi qu'un navigateur Web PHP.

# Protection des renseignements personnels

La plupart des usagers ignorent que leur courriel, leurs clavardages et même leurs mots de passe privés sont souvent envoyés « dans l'espace libre » sur des douzaines de réseaux non fiables avant d'arriver à leur destination finale sur Internet. Même s'ils se trompent, les usagers espèrent toujours que leurs renseignements personnels seront protégés lorsqu'ils utilisent des réseaux informatiques.

Cette protection peut être réalisée même sur des réseaux qui ne sont pas fiables comme des points d'accès publics et Internet. La seule méthode efficace prouvée pour protéger les renseignements personnels est l'utilisation d'un ***chiffrement bout à bout*** fort.

Les techniques de chiffrement telles que WEP et WPA essayent d'aborder la question de la protection des renseignements personnels à la couche deux, la couche liaison. Même si ceci offre une protection contre les oreilles indiscrètes dans une connexion sans fil, la protection finit au point d'accès. Si le client sans fil emploie des protocoles peu sécuritaires (tels que le POP ou un simple SMTP pour recevoir et envoyer des courriels), alors des usagers en dehors de l'AP peuvent toujours se connecter à la session et voir les données personnelles. Comme cité précédemment, le WEP souffre également du fait qu'il emploie une clef privée partagée. Ceci signifie que les usagers légitimes sans fil peuvent s'écouter clandestinement les uns les autres puisqu'ils connaissent tous la clef privée.

En employant le chiffrement avec l'hôte distant de la connexion, les usagers peuvent habilement éluder le problème. Ces techniques fonctionnent bien même sur des réseaux publics peu fiables où les oreilles indiscrètes écoutent et manipulent probablement des données venant du point d'accès.

Afin d'assurer une protection des renseignements personnels, un bon chiffrement bout à bout devrait présenter les caractéristiques suivantes:

- ***Authentification vérifiée de l'hôte distant***. L'usager devrait pouvoir savoir sans aucun doute que l'hôte distant est bien ce qu'il prétend être. Sans authentification, un usager pourrait transmettre des données privées à tout ceux qui prétendraient être le service légitime.
- ***Méthodes fortes de chiffrement***. L'algorithme du chiffrement devrait être minutieusement examiné par le public et ne devrait pas être facilement déchiffré par un tiers. Il n'y a aucune sécurité par l'obscurité et le chiffrement fort est encore plus fort quand l'algorithme est largement connu et sujet à l'examen des pairs. Un bon algorithme avec une clef assez grande et protégée fournit un chiffrement qui sera peu susceptible d'être brisé malgré tout les efforts réalisés à l'aide de la technologie actuelle.
- ***Cryptographie à clef publique***. Même si ce n'est pas une condition absolue pour le chiffrement bout à bout, l'utilisation de la cryptographie à clef publique au lieu d'une clef partagée peut assurer que les données d'un usager demeurent privées, même si la clef d'un autre usager du service est compromise. Elle résout également certains des problèmes de la distribution de clefs aux usagers sur des réseaux peu fiables.
- ***Encapsulation des données***. Un bon mécanisme de chiffrement bout à bout protège autant de données que possible. Ceci peut aller de chiffrer une simple transaction de courriel à l'encapsulation de tout le trafic IP, y compris des consultations de DNS et d'autres protocoles de support. Certains outils de chiffrement fournissent simplement un canal sécuritaire que d'autres applications peuvent utiliser. Ceci permet aux usagers d'exécuter n'importe quel programme de leur choix en ayant toujours la protection du chiffrement fort, même si les programmes eux-mêmes ne la soutiennent pas.

Prenez en compte que les lois concernant l'utilisation du chiffrement sont considérablement différentes d'un endroit à l'autre. Certains pays considèrent le chiffrement comme des munitions et peuvent exiger un permis, bloquer des clefs privées ou même interdire complètement son utilisation. Avant de mettre en application n'importe quelle solution utilisant le chiffrement, soyez sûr de vérifier que l'usage de cette technologie est autorisé dans votre région.

Dans les sections suivantes, nous verrons certains outils spécifiques qui peuvent offrir une bonne protection pour les données de vos usagers.

## Couche de sécurité SSL

La technologie de chiffrement bout à bout la plus largement disponible est la ***couche de sécurité SSL***. Elle est pratiquement installée dans tous les navigateurs Web et emploie la cryptographie à clef publique et une ***infrastructure à clef publique*** (***PKI***) fiable pour rendre plus sécuritaire la communication de données sur le Web. Toutes les fois que vous visitez un URL Web qui commence par https, vous employez la couche de sécurité SSL.

L'implantation SSL établie dans les navigateurs Web inclut une collection de certificats provenant de sources fiables, appelée les ***autorités de certificats*** (***CA***). Ces certificats sont des clefs cryptographiques qui sont employées pour vérifier l'authenticité des sites Web. Quand vous passez en revue un site Web qui emploie SSL, le navigateur et le serveur échangent d'abord des certificats. Le navigateur vérifie alors que le certificat fourni par le serveur correspond avec son nom d'hôte DNS, qu'il n'a pas expiré et qu'il est signé par une Autorité de Certification digne de confiance. De façon optionnelle, le serveur vérifie l'identité du certificat du navigateur. Si les certificats sont approuvés, le navigateur et le serveur négocient alors une clef principale de session en utilisant les certificats précédemment échangés pour la protéger. Cette clef est alors employée pour chiffrer toutes les communications jusqu'à ce que le navigateur se déconnecte. Ce genre d'encapsulation des données est connu sous le nom de ***tunnel***.

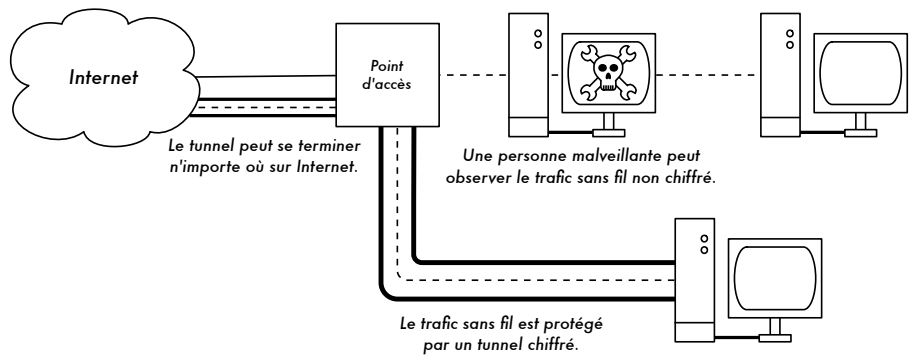


*Figure 6.4: Les oreilles indiscrètes doivent rompre un chiffrement fort pour surveiller le trafic au sein d'un tunnel chiffré. La conversation à l'intérieur de ce tunnel est identique à n'importe quelle autre conversation non chiffrée.*

L'usage de certificats avec un PKI protège non seulement la communication contre les oreilles indiscrètes, mais empêche également les ***attaques de l'homme au milieu*** (en anglais, ***man-in-the-middle -MITM***). Dans une attaque de l'homme au milieu, un usager malveillant intercepte toute la communication entre le navigateur et le serveur. En présentant des certificats faux au navigateur et au serveur, l'usager malveillant pourrait poursuivre simultanément deux sessions chiffrées. Puisque l'usager malveillant connaît le

secret des deux connexions, il est trivial d'observer et de manipuler des données passant entre le serveur et le navigateur.

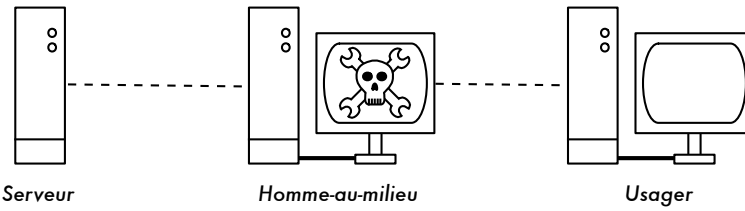


*Figure 6.5: L'homme au milieu controle efficacement tout ce que l'usager voit et peut enregistrer ou manipuler tout le trafic. Sans infrastructure a clef publique pour vérifier l'authenticité des clefs, le chiffrement fort, employé seul, ne peut pas protéger contre ce genre d'attaque..*

L'utilisation d'une bonne PKI empêche ce genre d'attaque. Afin de réussir son coup, l'usager malveillant devrait présenter un certificat au client qui est signé par une Autorité de Certificats fiable. À moins qu'une AC ait été compromise (ce qui est très peu probable) ou que l'usager ait été dupé et accepte le faux certificat, une telle attaque est impossible. C'est pourquoi il est extrêmement important que les usagers comprennent que le fait d'ignorer des avertissements sur des certificats expirés ou faux est très dangereux, particulièrement en utilisant des réseaux sans fil. En cliquant sur le bouton "ignorez", les usagers ouvrent leurs portes à plusieurs attaques potentielles.

SSL est non seulement employé pour naviguer sur le Web. Il est possible de rendre plus sécuritaires les protocoles de courriel peu sûrs tels que IMAP, POP et SMTP en les enveloppant dans un tunnel SSL. La plupart des clients de courriel actuels soutiennent IMAPS et POPS (IMAP et POP sécuritaires) ainsi que le SMTP protégé avec SSL/TLS. Si votre serveur de courriel ne fournit pas le support SSL, vous pouvez toujours le rendre plus sécuritaire avec SSL en employant un programme comme Stunnel (*http://www.stunnel.org/*). SSL peut être employé pour rendre plus sécuritaire presque n'importe quel service qui fonctionne sur TCP.

## SSH

La plupart des personnes pensent à SSH comme remplacement sécuritaire de **`telnet`**, de la même façon que **`scp`** et **`sftp`** sont les contreparties sécuritaires de **`rcp`** et **`ftp`**. Mais SSH est plus qu'un *shell* (ligne de commande) distant chiffré. Comme le SSL, il emploie une forte cryptographie à clef publique pour vérifier le serveur à distance et pour chiffrer des données. Au lieu d'une PKI, il emploie une cache d'empreinte de clefs (*fingerprint key* en anglais) qui est vérifiée avant qu'une connexion soit autorisée. Il peut employer des mots de passe, des clefs publiques ou d'autres méthodes pour l'authentification des usagers.

Beaucoup de gens ne savent pas que SSH peut également agir en tant que tunnel de chiffrement tout usage ou même un chiffrement Web proxy. En établissant d'abord une connexion SSH à un site fiable près d'un (ou sur un) serveur à distance, des protocoles peu sûrs peuvent être protégés contre l'écoute clandestine et les attaques.

Tandis que cette technique peut être un peu avancée pour plusieurs usagers, les architectes de réseau peuvent employer SSH pour chiffrer le trafic à travers des liens peu fiables, tels que les liens point-à-point sans fil. Puisque les outils sont librement disponibles et fonctionnent sur le TCP standard, n'importe quel usager instruit peut mettre en application des connexions SSH sans l'intervention d'un administrateur en fournissant son propre chiffrement bout à bout.

OpenSSH (*http://openssh.org/*) est probablement la version la plus populaire sur les plateformes de type Unix. Les versions libres telles que Putty (*http://www.putty.nl/*) et WinSCP (*http://winscp.net/*) sont disponibles pour Windows. OpenSSH fonctionnera également sur Windows dans l'environnement Cygwin (*http://www.cygwin.com/*). Ces exemples supposent que vous employez une version récente d'OpenSSH.

Pour établir un tunnel chiffré d'un port sur l'ordinateur local à un port d'hôte distant, utilisez le commutateur **-L**. Par exemple, supposez que vous voulez expédier du trafic Web proxy sur un lien chiffré au serveur squid à squid.example.net. Redirigez le port 3128 (le port de proxy par défaut) avec la commande suivante:

```
ssh -fN -g -L3128:squid.example.net:3128 squid.example.net
```

Les commutateurs **-fN** ordonnent à ssh de s'exécuter en tâche de fond après s'être connecté. Le commutateur **-g** permet à d'autres usagers sur votre segment local de se connecter à l'ordinateur local et à l'utiliser pour le chiffrement sur les liens de non-confiance. OpenSSH emploiera une clef publique pour l'authentification si vous en avez établie une ou demandera le mot de passe de l'hôte distant. Vous pouvez alors configurer votre navigateur Web pour vous connecter au port local 3128 comme son service web proxy. Tout le trafic Web sera alors chiffré avant d'être transmis à l'hôte distant.

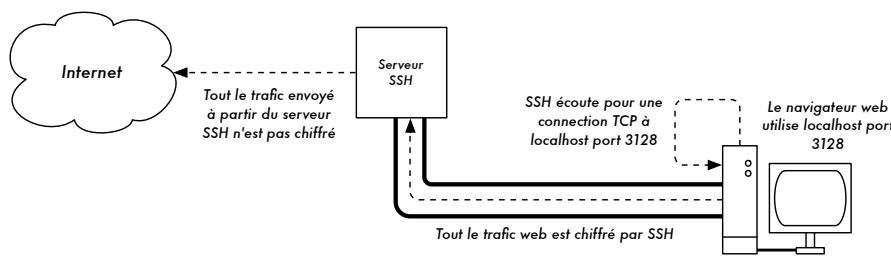


*Figure 6.6: Le tunnel SSH protège le trafic Web au delà du serveur SSH lui-même.*

SSH peut également agir en tant que proxy dynamique SOCKS4 ou SOCKS5. Ceci vous permet de créer un chiffrement Web proxy, sans avoir à installer squid. Notez que ce n'est pas un proxy à antémémoire; il chiffre simplement tout le trafic.

```
ssh -fN -D 8080 remote.example.net
```

Configurez votre navigateur web pour utiliser SOCKS4 ou SOCKS5 sur le port local 8080 et voilà, vous pourrez sortir.

SSH peut chiffrer des données sur n'importe quel port TCP, y compris des ports utilisés pour le courriel. Il peut même comprimer les données le long du chemin ce qui peut diminuer la latence sur des liens de basse capacité.

```
ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net
```

Le commutateur **-C** met en marche la compression. En spécifiant commutateur **-L** plusieurs fois, vous pouvez ajouter autant de règles de redirection de port que vous le souhaitez. Notez qu'afin d'utiliser un port plus bas que 1024, vous devez avoir des privilèges de superutilisateur (*root*) sur l'ordinateur local.

Ceux-ci ne sont que quelques exemples de la flexibilité de SSH. En mettant en application des clefs publiques et en employant l'agent ssh de redirection, vous pouvez automatiser la création de tunnels chiffrés dans tout votre réseau sans fil et ainsi protéger vos communications avec un chiffrement et une authentification solides.

## OpenVPN

OpenVPN est une implantation VPN gratuite et de source ouverte basée sur le chiffrement SSL. Il y a des implantations de client OpenVPN pour un éventail de systèmes d'exploitation, comprenant Linux, Windows 2000/XP (et plus récent), OpenBSD, FreeBSD, NetBSD, Mac OS X et Solaris. Étant un VPN, il encapsule tout le trafic (y compris DNS et tout autre protocole) dans un tunnel chiffré; et non un seul port TCP. La plupart des personnes le trouvent considérablement plus facile à comprendre et à configurer qu'IPsec.

OpenVPN présente également quelques inconvénients, tels qu'une latence assez élevée. Une certaine quantité de latence est inévitable puisque tout chiffrement/déchiffrement se réalise dans l'espace utilisateur mais à l'aide d'ordinateurs relativement nouveaux aux deux extrémité du tunnel il est possible de la réduire au minimum. Malgré qu'on puisse employer des clefs partagées traditionnelles, OpenVPN se démarque vraiment lorsqu'on l'utilise avec des certificats SSL et une Autorité de Certificat. OpenVPN présente

plusieurs avantages qui le rendent une bonne option pour fournir de la sécurité bout à bout.

- Il est basé sur un protocole de chiffrement robuste qui a fait ses preuves (SSL et RSA)
- Il est relativement facile à configurer
- Il fonctionne sur plusieurs plateformes différentes
- Il est bien documenté
- Il est gratuit et de source ouverte

Comme SSH et SSL, OpenVPN doit simplement se connecter à un port TCP de l'hôte distant. Une fois cette connexion établie, il peut encapsuler toutes les données de la couche de gestion de réseau ou même de la couche de liaison. Vous pouvez l'employer pour créer des connexions VPN robustes entre différents ordinateurs ou l'utiliser simplement pour connecter des routeurs sur des réseaux sans fil peu fiables.

La technologie VPN est un domaine complexe et dépasse un peu la portée de cet ouvrage. Il est important de comprendre comment les VPNs s'accommodent dans la structure de votre réseau afin d'assurer la meilleure protection sans ouvrir votre organisation à des problèmes involontaires. On retrouve plusieurs bonnes ressources en ligne qui se penchent sur la question de l'installation d'OpenVPN sur un serveur et un client. Je recommande particulièrement l'article suivant tiré du journal de Linux: *http://www.linuxjournal.com/article/7949* ainsi que le HOWTO officiel: *http://openvpn.net/howto.html*.

## Tor et Anonymiseurs

L'Internet est fondamentalement un réseau ouvert basé sur la confiance. Quand vous vous connectez à un serveur Web à travers Internet, votre trafic traverse plusieurs routeurs différents appartenant à une grande variété d'établissements, d'associations et d'individus. En principe, n'importe quel de ces routeurs ont la capacité de regarder vos données de près, voyant au moins la source et les adresses de destination et, souvent aussi, le contenu réel de données. Même si vos données sont chiffrées en utilisant un protocole sécuritaire, il est possible pour votre fournisseur Internet de surveiller la quantité de données, la source et la destination de ces données. Souvent, ceci est assez pour rassembler une image assez complète de vos activités en ligne.

La protection des renseignements personnels et l'anonymat sont importants et étroitement liés entre eux. Il y a beaucoup de raisons valides qui peuvent vous pousser à protéger votre vie privée en ***anonymisant*** votre trafic de ré-

seau. Supposez que vous voulez offrir une connectivité Internet à votre communauté locale en installant un certain nombre de points d'accès pour que les personnes puissent s'y connecter. Que vous les fassiez payer pour l'accès ou pas, il y a toujours un risque que les gens qui utilisent le réseau le fassent pour quelque chose qui n'est pas légal dans votre pays ou région. Vous pourriez affirmer que cette action illégale particulière n'a pas été effectuée par vous-même et qu'elle a pu être accomplie par n'importe quelle personne se reliant à votre réseau. On pourrait éviter le problème s'il était techniquement infaisable de déterminer où votre trafic a été dirigé réellement. Que pensez-vous de la censure en ligne? Des pages Web anonymes peuvent également être nécessaires pour éviter la censure du gouvernement.

Il y a des outils qui vous permettent d'anonymiser votre trafic de différentes manières relativement faciles. La combinaison de ***Tor*** (*http://tor.eff.org/*) et de ***Privoxy*** (*http://www.privoxy.org/*) est une manière puissante de faire fonctionner un serveur local proxy qui fera passer votre trafic Internet par un certain nombre de serveurs à travers Internet, rendant très difficile de suivre la trace de l'information. Le Tor peut être exécuté sur un ordinateur local, sous Microsoft Windows, Mac OSX, Linux et une variété de BSDs où il anonymisera le trafic du navigateur sur cet ordinateur. Tor et Privoxy peuvent également être installés sur une passerelle ou même un petit point d'accès embarqué (tel que Linksys WRT54G) où ils fournit automatiquement l'anonymat à tous les usagers de ce réseau.

Tor fonctionne en faisant rebondir à plusieurs reprises vos connexions TCP à travers un certain nombre de serveurs répandus sur Internet et en emballant l'information de routage dans un certain nombre de couches chiffrées (d'où le terme ***routage en oignon***), qui vont être « épluchées » au cours du déplacement du paquet à travers le réseau. Ceci signifie qu'à n'importe quel point donné sur le réseau, la source et les adresses de destination ne peuvent pas être liées ensemble. Ceci rend l'analyse de trafic extrêmement difficile.

Le besoin du proxy de protection de la vie privée Privoxy lié à Tor est dû au fait que dans la plupart des cas les requêtes de nom de serveur (requêtes DNS) ne sont pas passées par le serveur proxy et quelqu'un analysant votre trafic pourrait facilement voir que vous essayiez d'atteindre un emplacement spécifique (par exemple, *google.com*) du fait que vous avez envoyé une requête DNS pour traduire google.com à l'adresse IP appropriée. Privoxy se connecte à Tor comme un proxy SOCKS4a, qui emploie des noms d'hôtes (et non des adresses IP) pour livrer vos paquets à la destination souhaitée.

En d'autres termes, employer Privoxy avec Tor est une manière simple et efficace d'empêcher l'analyse de trafic de lier votre adresse IP avec les services que vous employez en ligne. Combiné avec des protocoles chiffrés sé-

curitaires (du type que nous avons vu au sein de ce chapitre), Tor et Privoxy fournissent un niveau élevé d'anonymat sur l'Internet.

# Surveillance

Les réseaux informatiques (et les réseaux sans fil en particulier) sont des inventions incroyablement divertissantes et utiles. Excepté, naturellement, quand ils ne fonctionnent pas. Vos usagers peuvent se plaindre que le réseau est « lent » ou « brisé », mais qu'est-ce que cela signifie vraiment? Sans pouvoir savoir ce qui se produit réellement, l'administration d'un réseau peut devenir très frustrante.

Afin d'être un administrateur de réseau efficace, vous devez avoir accès aux outils qui vous montrent exactement ce qui se produit sur votre réseau. Il y a plusieurs différentes classes d'outils de surveillance. Chacun vous montre un aspect différent de « ce qui se passe », de l'interaction physique par radio à la façon dont les applications des usagers interagissent les unes sur les autres. En observant comment le réseau fonctionne à travers le temps, vous pouvez avoir une idée de ce qui est « normal » pour votre réseau et même recevoir une annonce automatique lorsque les choses semblent sortir de l'ordinaire. Les outils énumérés dans cette section sont tous assez puissants et peuvent être gratuitement téléchargés à partir des adresses énumérées après chaque description.

## Détection de réseau

Les outils de surveillance sans fil les plus simples fournissent simplement une liste de réseaux disponibles avec l'information de base (telle que la force et le canal du signal). Ils vous permettent de détecter rapidement les réseaux voisins et déterminer s'ils causent de l'interférence.

- **Ceux qui sont incorporés au client**. Tous les systèmes d'exploitation modernes fournissent un appui intégré aux réseaux sans fil. Ceci inclut typiquement la capacité de détecter les réseaux disponibles, permettant à l'usager de choisir un réseau à partir d'une liste. Même s'il est garanti que pratiquement tous les dispositifs sans fil ont une capacité simple de balayage, la fonctionnalité peut changer considérablement entre les différentes applications. En général, ces outils sont uniquement utiles pour configurer un ordinateur chez soi ou au bureau. Ils tendent à fournir peu d'informations outre les noms de réseau et le signal disponible au point d'accès actuellement en service.
- **Netstumbler** (*http://www.netstumbler.com/*). C'est l'outil le plus populaire pour détecter les réseaux sans fil en utilisant Microsoft Windows. Il fonctionne avec une variété de cartes sans fil et est très facile à utiliser. Il détectera les réseaux ouverts et chiffrés mais ne peut pas détecter les ré-

seaux sans fil fermés. Il possède également un mesureur de signal/bruit qui trace les données du récepteur radio sur un graphique au cours du temps. Il peut également être intégré à une variété de dispositifs GPS pour noter l'information précise concernant l'emplacement et la force du signal. Ceci rend Netstumbler un outil accessible pour effectuer le relevé informel d'un site.

- **Ministumbler** (*http://www.netstumbler.com/*). Ministumbler, fait par les concepteurs de Netstumbler, fournit presque la même fonctionnalité que la version de Windows mais fonctionne sur la plateforme Pocket PC. Ministumbler peut fonctionner sur un PDA de poche avec une carte sans fil pour détecter des points d'accès dans une zone donnée.
- **Macstumbler** (*http://www.macstumbler.com/*). Même s'il n'est pas directement relié au Netstumbler, Macstumbler fournit en grande partie la même fonctionnalité mais pour la plateforme Mac OS X. Il fonctionne avec toutes les cartes Airport de Apple.
- **Wellenreiter** (*http://www.wellenreiter.net/*). Wellenreiter est un détecteur graphique de réseau sans fil pour Linux. Il exige Perl et GTK et fonctionne avec des cartes sans fil Prism2, Lucent, et Cisco.

## Analyseurs de protocoles

Les analyseurs de protocole de réseau fournissent beaucoup de détail au sujet de l'information traversant un réseau en vous permettant d'inspecter des paquets individuels. Pour des réseaux câblés, vous pouvez inspecter des paquets à la couche liaison ou à une couche supérieure. Pour les réseaux sans fil, vous pouvez inspecter l'information jusqu'aux trames 802.11. Voici plusieurs analyseurs populaires (et libres) de protocole de réseau:

- **Ethereal** (*http://www.ethereal.com/*). Ethereal est probablement l'analyseur de protocole le plus populaire disponible actuellement. Il fonctionne avec Linux, Windows, Mac OS X et divers systèmes BSD. Ethereal va capturer des paquets directement en provenance « du câble » et les montrer dans une interface graphique intuitive. Il peut décoder plus de 750 protocoles différents, des trames 802.11 aux paquets HTTP. Il peut rassembler des paquets fragmentés et suivre des sessions TCP entières facilement, même si d'autres données ont brisé l'échantillon. Ethereal est très utile pour dépanner des problèmes difficiles du réseau, ainsi que pour savoir exactement ce qui se produit quand deux ordinateurs conversent « sur le câble ».
- **Kismet** (*http://www.kismetwireless.net/*). Kismet est un analyseur de protocole sans fil puissant pour Linux, Mac OS X et même la distribution embarquée de Linux OpenWRT. Il fonctionne avec n'importe quelle carte sans fil qui supporte le mode moniteur passif. En plus de la détection de la pré-

sence du réseau, Kismet notera passivement chacune des trames 802.11 sur le disque ou sur le réseau dans le format standard PCAP, pour l'analyse postérieure avec des outils comme Ethereal. Kismet présente également de l'information associée au client; l'empreinte de l'équipement AP, la détection de Netstumbler et l'intégration GPS.

Puisque c'est un moniteur de réseau passif, il peut même détecter les réseaux sans fil « fermés » en analysant le trafic envoyé par les clients sans fil. Vous pouvez exécuter Kismet sur plusieurs ordinateurs à la fois et faire que ceux-ci informent à travers le réseau une interface usager centrale. Ceci permet la surveillance sans fil sur un large secteur, tel qu'un campus universitaire ou de corporation. Puisqu'il emploie le mode moniteur passif, il peut réaliser tout ceci sans transmettre aucune donnée.

- **KisMAC** (*http://kismac.binaervarianz.de/*). Kismac a été crée exclusivement pour la plateforme Mac OS X. Il fonctionne de façon très similaire à Kismet, mais avec une interface graphique Mac OS X très élaborée. C'est un module de balayage de données passif qui note l'information sur un disque de format PCAP compatible avec Ethereal. Malgré qu'il ne puisse pas fonctionner avec les cartes AirportExtreme (dues à des limitations du pilote sans fil), il le fait très bien avec une variété de cartes radio USB.
- **Driftnet** et **Etherpeg**. Ces outils décodent des données graphiques (telles que des fichiers GIF et JPEG) et les présentent dans un collage. Tel que mentionné précédemment, les outils de ce type ne sont pas très utiles pour le dépannage, mais sont très utiles pour démontrer l'insécurité des protocoles sans chiffrement. Etherpeg est disponible à l'adresse: *http://www.etherpeg.org/*, et Driftnet peut être téléchargé à l'adresse: *http://www.ex-parrot.com/~chris/driftnet/*.

## Surveillance de la largeur de bande

Le réseau est lent. Qui est en train d'accaparer toute la largeur de bande? En employant un bon outil de surveillance de la largeur de bande, vous pouvez facilement déterminer la source des problèmes d'envoie massif de pourriel et de virus. De tels outils peuvent également vous aider à projeter la future capacité dont vous aurez besoin à mesure que la largeur de bande devient trop petite pour ses usagers. Ces outils vous donneront une représentation visuelle de la façon dont le trafic circule dans tout votre réseau, y compris le trafic venant d'un ordinateur ou d'un service particulier.

- **MRTG** (*http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*). La plupart des administrateurs de réseau ont fait la connaissance de MRTG à un certain moment dans leurs voyages. Écrit à l'origine en 1995, MRTG est probablement l'application de surveillance de la largeur de bande la plus largement répandue. En utilisant Perl et C, il établit une page Web remplie de graphiques détaillant le trafic entrant et sortant d'une interface réseau

particulière. Avec MRTG, il est simple de consulter des commutateurs de réseau, des points d'accès, des serveurs et d'autres appareils en montrant les résultats sous la forme de graphiques qui changent au cours du temps.

- **RRDtool** (*http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/*). RRDtool a été développé par les mêmes personnes qui ont écrit mrtg mais c'est une application de surveillance générique plus puissante. RRD est l'abréviation en anglais de « *round-robin database* » (base de données à parcours circulaire). C'est un format de données générique qui vous permet de suivre facilement n'importe quel point de données comme un ensemble de moyennes au cours du temps. Tandis que rrdtool ne surveille pas directement les interfaces ou les dispositifs, plusieurs programmes de surveillance se basent sur lui pour stocker et montrer les données qu'ils rassemblent. Avec quelques simples scripts shell, vous pouvez surveillez facilement vos commutateurs de réseau et points d'accès et tracer la largeur de bande utilisée sous forme de graphique sur une page Web.
- **ntop** (*http://www.ntop.org/*). Ntop est utile pour une analyse historique de trafic et d'usage. Ce programme fournit un rapport détaillé en temps réel du trafic observé sur le réseau et le présente sur votre navigateur Web. Il s'incorpore à rrdtool pour faire des graphiques et des diagrammes dépeignant visuellement comment le réseau est employé. Sur les réseaux très occupés, ntop peut utiliser beaucoup de l'unité centrale de traitement et d'espace disque, mais il vous offre une vision précise de la façon dont votre réseau est employé. Il fonctionne sur Linux, BSD, Mac OS X et Windows.
- **iptraf** (*http://iptraf.seul.org/*). Iptraf est utile si vous désirez avoir un aperçu instantané de l'activité réseau sur un système Linux. C'est un utilitaire en ligne de commande qui vous donne un aperçu en quelques secondes des connexions et du flux réseau, y compris des ports et des protocoles. Il peut être très utile pour déterminer qui emploie un lien sans fil particulier, ainsi que pour voir son poids de chargement. Par exemple, en montrant une statistique détaillée de l'interruption du fonctionnement d'une interface, vous pouvez immédiatement repérer les usagers et déterminer exactement combien de largeur de bande ils emploient actuellement.

## Dépannage

Que faites-vous lorsque le réseau se brise? Si vous ne pouvez pas accéder à une page Web ou au serveur de courriel et si en cliquant sur le bouton de rechargement vous ne réglez pas le problème, alors vous aurez besoin d'isoler l'endroit exact d'où il provient. Les outils suivants vous aideront à cerner le problème de connexion.

- **ping**. Presque tout système d'exploitation (incluant Windows, Mac OS X, et naturellement, Linux et BSD) inclut une version de l'utilitaire ping. Il util-

ise des paquets ICMP pour essayer d'entrer en contact avec l'hôte indiqué et affiche combien de temps a été nécessaire pour obtenir une réponse.

Savoir quoi contacter est aussi important que de savoir comment contacter. Si vous constatez que vous ne pouvez pas vous connecter à un service particulier par votre navigateur Web (exemple: *http://yahoo.com/*), vous pourriez essayer de le contacter:

```
$ ping yahoo.com
PING yahoo.com (66.94.234.13): 56 data bytes
64 bytes from 66.94.234.13: icmp_seq=0 ttl=57 time=29.375 ms
64 bytes from 66.94.234.13: icmp_seq=1 ttl=56 time=35.467 ms
64 bytes from 66.94.234.13: icmp_seq=2 ttl=56 time=34.158 ms
^C
--- yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.375/33.000/35.467/2.618 ms
```

Faites « control-C » lorsque vous avez fini de rassembler les données. Si les paquets prennent un long moment avant de revenir, il peut y avoir congestion de réseau. Si les paquets de retour ping ont un ttl inhabituellement bas, il peut y avoir des problèmes de routage entre votre ordinateur et l'hôte distant. Mais que se passe-t-il si le ping ne retourne aucune donnée du tout? Si vous contactez un nom au lieu d'une adresse IP, vous pouvez avoir des problèmes de DNS.

Essayez de contacter une adresse IP sur Internet. Si vous ne pouvez pas y accéder, c'est peut-être une bonne idée d'essayer si vous pouvez contacter votre routeur par défaut:

```
$ ping 216.231.38.1
PING 216.231.38.1 (216.231.38.1): 56 data bytes
64 bytes from 216.231.38.1: icmp_seq=0 ttl=126 time=12.991 ms
64 bytes from 216.231.38.1: icmp_seq=1 ttl=126 time=14.869 ms
64 bytes from 216.231.38.1: icmp_seq=2 ttl=126 time=13.897 ms
^C
--- 216.231.38.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 12.991/13.919/14.869/0.767 ms
```

Si vous ne pouvez pas contacter votre routeur par défaut, alors il y a des chances que vous ne pourrez pas non plus accéder à Internet. Si vous ne pouvez même pas connecter d'autres adresses IP sur votre LAN local, alors il est temps de vérifier votre connexion. Si vous utilisez un câble Ethernet, est-il branché? Si vous travaillez avec une connexion sans fil, êtes-vous connecté au réseau sans fil approprié? Celui-ci est-il à portée?

Dépanner un réseau à l'aide de ping relève en partie de l'art mais demeure un bon outil pédagogique. Puisque vous trouverez probablement l'utilitaire

ping sur presque tous les ordinateurs sur lesquels vous travaillerez, c'est une bonne idée d'apprendre à l'utiliser de manière appropriée.

- **traceroute** et **mtr** (*http://www.bitwizard.nl/mtr/*). Tout comme ping, traceroute est trouvé sur la plupart des systèmes d'exploitation (il se nomme **tracert** dans certaines versions de Microsoft Windows). En exécutant traceroute, vous pouvez trouver où se situent les problèmes entre votre ordinateur et n'importe quel point sur l'Internet:

```
$ traceroute -n google.com
traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets
 1  10.15.6.1  4.322 ms  1.763 ms  1.731 ms
 2  216.231.38.1  36.187 ms  14.648 ms  13.561 ms
 3  69.17.83.233  14.197 ms  13.256 ms  13.267 ms
 4  69.17.83.150  32.478 ms  29.545 ms  27.494 ms
 5  198.32.176.31  40.788 ms  28.160 ms  28.115 ms
 6  66.249.94.14  28.601 ms  29.913 ms  28.811 ms
 7  172.16.236.8  2328.809 ms  2528.944 ms  2428.719 ms
 8  * * *
```

Le commutateur **-n** indique à traceroute de ne pas prendre la peine de résoudre les noms DNS, en le faisant donc fonctionner plus rapidement. Vous pouvez voir qu'au saut sept, le temps de voyage bondit à plus de deux secondes, alors que les paquets sont jetés au saut huit. Ceci pourrait indiquer un problème à ce point dans le réseau. Si vous contrôlez cette partie du réseau, il pourrait être intéressant de commencer votre effort de dépannage à ce point là.

My TraceRoute (mtr) est un programme utile qui combine ping et traceroute dans un outil simple. En exécutant mtr, vous pouvez obtenir une moyenne continue de latence et de perte de paquet à un hôte donné au lieu de la présentation momentanée offerte par ping et traceroute.

```
                           My traceroute  [v0.69]
tesla.rob.swn (0.0.0.0)        (tos=0x0 psize=64 bitpatSun Jan  8 20:01:26 2006
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                   Packets               Pings
 Host                            Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. gremlin.rob.swn               0.0%     4    1.9   2.0   1.7   2.6   0.4
 2. er1.sea1.speakeasy.net        0.0%     4   15.5  14.0  12.7  15.5   1.3
 3. 220.ge-0-1-0.cr2.sea1.speakeasy.  0.0%     4   11.0  11.7  10.7  14.0   1.6
 4. fe-0-3-0.cr2.sfo1.speakeasy.net   0.0%     4   36.0  34.7  28.7  38.1   4.1
 5. bas1-m.pao.yahoo.com          0.0%     4   27.9  29.6  27.9  33.0   2.4
 6. so-1-1-0.pat1.dce.yahoo.com   0.0%     4   89.7  91.0  89.7  93.0   1.4
 7. ae1.p400.msr1.dcn.yahoo.com   0.0%     4   91.2  93.1  90.8  99.2   4.1
 8. ge5-2.bas1-m.dcn.yahoo.com    0.0%     4   89.3  91.0  89.3  93.4   1.9
 9. w2.rc.vip.dcn.yahoo.com       0.0%     3   91.2  93.1  90.8  99.2   4.1
```

Les données seront constamment mises à jour et ramenées à une moyenne. Comme avec ping, vous devez faire « control-C » une fois que vous avez fini de regarder les données. Notez que pour exécuter mtr, vous devez avoir des privilèges de superutilisateur (*root*).

Tandis que ces outils ne révèlent pas avec précision ce qui ne fonctionne pas avec le réseau, ils peuvent vous fournir assez d'information pour savoir où vous devez continuer le dépannage.

## Test de performance

À quelle vitesse peut aller le réseau? Quelle est la capacité utilisable réelle d'un lien particulier du réseau? Vous pouvez obtenir une très bonne évaluation de votre rendement en envoyant du trafic sur votre lien et en mesurant combien de temps prend le transfert des données. Même s'il y a des pages Web disponibles qui peuvent réaliser un « test de vitesse » sur votre navigateur (tel que *http://www.dslreports.com/stest*), ces test sont très imprécis si vous êtes loin de la source de test. Pire encore, ils ne permettent pas d'examiner la vitesse d'un lien particulier, mais uniquement la vitesse de votre lien à Internet. Voici deux outils qui vous permettront d'exécuter un test de rendement sur vos propres réseaux.

- **ttcp** (*http://ftp.arl.mil/ftp/pub/ttcp/*). Tccp fait actuellement partie de la plupart des systèmes de type Unix C'est un outil simple de test de rendement de réseau qui fonctionne sur chaque côté du lien que vous désirez examiner. Le premier noeud fonctionne en mode récepteur et l'autre transmet:

```
node_a$ ttcp -r -s

node_b$ ttcp -t -s node_a
ttcp-t: buflen=8192, nbuf=2048, align=16384/0, port=5001  tcp -> node_a
ttcp-t: socket
ttcp-t: connect
ttcp-t: 16777216 bytes in 249.14 real seconds = 65.76 KB/sec +++
ttcp-t: 2048 I/O calls, msec/call = 124.57, calls/sec = 8.22
ttcp-t: 0.0user 0.2sys 4:09real 0% 0i+0d 0maxrss 0+0pf 7533+0csw
```

Après le rassemblement des données dans une direction, vous devriez renverser les rôles de transmission et réception pour examiner le lien dans l'autre direction. Il peut examiner les courants UDP et TCP et peut changer divers paramètres TCP et la grosseur des tampons pour donner au réseau un bon rendement. Il peut même employer un flux de données écrit par l'usager au lieu d'envoyer des données aléatoires. Rappelez-vous que l'afficheur de vitesse est en kilo-octets et non kilobits. Multipliez le résultat par 8 pour trouver la vitesse en kilobits par seconde.

Le seul inconvénient véritable de ttcp est qu'il n'a pas été développé durant des années. Heureusement, le code est de domaine public et est disponible gratuitement. Tout comme ping et traceroute, ttcp se trouve sur plusieurs systèmes comme outil standard.

- **iperf** (*http://dast.nlanr.net/Projects/Iperf/*). Tout comme ttcp, iperf est un outil de ligne de commande pour estimer le rendement d'une connexion réseau. Il a plusieurs des mêmes caractéristiques que ttcp, mais emploie un modèle « client » et « serveur » au lieu de « réception » et « transmission ». Pour exécuter iperf, initiez un serveur d'un côté et un client de l'autre:

```
node_a$ iperf -s

node_b$ iperf -c node_a
------------------------------------------------------------
Client connecting to node_a, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  5] local 10.15.6.1 port 1212 connected with 10.15.6.23 port 5001
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-11.3 sec   768 KBytes   558 Kbits/sec
```

  Le côté serveur continuera à écouter et à accepter des connexions de client sur le port 5001 jusqu'à ce que vous entriez la commande « control-c » pour l'arrêter. Ceci peut être plus simple si nous exécutons plusieurs tests à partir de divers endroits.

  La plus grande différence entre ttcp et iperf est que iperf est activement en cours de développement et présente plusieurs nouvelles caractéristiques (incluant le support IPv6). Il est un bon choix d'outil lors de la conception de nouveaux réseaux.

## Santé du réseau

En suivant l'information à travers le temps, vous pouvez avoir une idée globale de la santé du réseau et de ses services. Ces outils présenteront les tendances de votre réseau et informeront lorsque des problèmes se présentent. Le plus souvent ces systèmes vont s'apercevoir qu'il y a un problème avant même que la personne ait la chance d'appeler le support technique.

- **cacti** (*http://www.cacti.net/*). Comme nous l'avons vu précédemment, beaucoup d'outils emploient RRDtool comme programme moteur (backend) pour créer des graphiques qui vont présenter les données accumulées. **Cacti** est de ce type. C'est un outil PHP de gestion de réseau qui simplifie l'accumulation de données et la production de graphiques. Il stocke sa configuration dans une base de données MySQL et est intégré avec SNMP. À l'aide de cet outil, il est très facile de situer tous les dispositifs sur votre réseau et de tout surveiller: des flux de réseau à la charge de l'unité centrale de traitement. Cacti a un schéma extensible de collecte de données qui vous permet d'accumuler presque n'importe quel genre de données (tel que le signal radio, le bruit ou les usagers associés) et de

tracer le tout sur un graphique en fonction du temps. Des imagettes de vos graphiques peuvent être présentées dans une page Web, vous permettant d'observer l'état global de votre réseau d'un seul coup d'oeil.

- **SmokePing** (h*ttp://people.ee.ethz.ch/~oetiker/webtools/smokeping/*). SmokePing est un autre outil créé par Tobias Oetiker. Il s'agit d'un outil écrit en Perl qui montre la perte de paquet et la latence sur un graphique simple. Il est très utile d'exécuter SmokePing sur un hôte ayant une bonne connectivité sur l'ensemble de votre réseau. Avec le temps, il révèle des tendances qui peuvent indiquer toutes sortes de problèmes de réseau. Combiné avec MRTG ou cacti, vous pouvez observer l'effet que la congestion de réseau a sur la perte de paquet et la latence. De façon optionnelle, SmokePing peut envoyer des alertes quand certaines conditions sont réunies, par exemple, lorsque l'on distingue une perte excessive de paquet sur un lien pendant une période prolongée.
- **Nagios** (*http://www.nagios.org/*). Nagios est un outil de surveillance du service. En plus de suivre la performance de simples pings (comme avec SmokePing), Nagios peut observer la performance des services réels sur n'importe quel nombre d'ordinateurs. Par exemple, il peut périodiquement interroger votre serveur Web pour s'assurer que celui-ci renvoie une page Web valide. Si un contrôle échoue, Nagios peut en informer une personne ou un groupe via courriel, SMS ou messagerie instantannée.

  Alors que Nagios aidera sans doûte un seul administrateur à surveiller un grand réseau, il est mieux utilisé lorsque vous avez une équipe de dépannage avec des responsabilités partagées entre les différents membres. Les événements problématiques peuvent être configurés pour ignorer les problèmes passagers en envoyant des avis uniquement aux personnes qui sont responsables de réparer ce problème en particulier. Si le problème continue pendant une période prédéfinie sans être reconnu, d'autres personnes peuvent alors en être informées. Ceci permet que les problèmes provisoires soient simplement notés sans déranger personne tandis que les problèmes réels sont portés à la connaissance de l'équipe.

# 7
# Construire un noeud extérieur

Plusieurs considérations pratiques sont de mise lorsque nous songeons à installer un équipement électronique à l'extérieur. Il doit évidemment être protégé contre la pluie, le vent, le soleil et autres éléments nuisibles. On doit fournir de l'énergie et l'antenne devrait être montée à une hauteur suffisante. Sans mise à terre appropriée, la foudre, la fluctuation dans le réseau électrique principal et même un vent doux dans un climat approprié peuvent détruire vos liens sans fil. Ce chapitre vous donnera une certaine idée des problèmes pratiques que vous pouvez rencontrer en installant un équipement sans fil à l'extérieur.

## *Boîtiers à l'épreuve de l'eau*

Les boîtiers à l'épreuve de l'eau appropriés existent en plusieurs modèles. Le métal ou le plastique peuvent être employés pour créer un récipient imperméable pour l'équipement embarqué extérieur.

Naturellement, l'équipement a besoin d'énergie pour fonctionner et devra probablement se connecter à une antenne et à un câble Ethernet. Chaque fois que vous percez un boîtier à l'épreuve de l'eau, vous créez un autre endroit potentiel pour que l'eau s'infiltre à l'intérieur.

L'Association Nationale des Fabricants de Matériel Électrique (*National Electrical Manufacturers Association- NEMA*) fournit des directives pour la protection de l'appareillage électrique contre la pluie, la glace, la poussière et d'autres polluants. Un boîtier évalué comme étant ***NEMA 3*** ou mieux, convient à l'usage extérieur dans un climat approprié. Un ***NEMA 4X*** ou ***NEMA 6*** assure une excellente protection, même contre l'eau et la glace provenant

d'un tuyau. Pour les montages qui percent les boîtiers (tels que les prises de câble et connecteurs a grande tête «*bulkhead*»), NEMA assigne un grade à la protection des entrées (*Ingress Protection* – IP en anglais). Un grade de protection des entrées ***IP66*** ou ***IP67*** protégera les trous contre des jets d'eau très forts. Un bon boîtier extérieur devrait également assurer une protection UV pour empêcher que l'exposition au soleil ne brise le joint d'étanchéité, ainsi que pour protéger l'équipement à l'intérieur.

Évidemment, il se peut que ce soit un défi que de trouver des boîtiers évalués par la NEMA dans votre secteur. Souvent, les pièces disponibles localement peuvent être recyclés comme boîtiers. Un boîtier peut être construit à partir de boîtes en plastique solide ou d'extincteurs d'incendie en métal, à partir de conduits électriques utilisés dans la construction de maisons ou même à partir de récipients de nourriture en plastique. En perçant un boîtier, utilisez des garnitures de qualité ou des dispositifs de serrage comme des bagues avec une tête de câble presse-étoupe pour sceller l'ouverture. Dans le cas d'installations provisoires, on peu utiliser un composé de silicone stabilisé contre les rayons UV ou tout autre enduit d'étanchéité mais rappelez-vous que les câbles peuvent se plier avec le vent et que les joints collés peuvent éventuellement s'affaiblir et permettre à l'humidité de s'infiltrer à l'intérieur.

Vous pouvez prolonger considérablement la vie d'un boîtier en plastique en assurant une certaine protection contre le soleil. Si vous installez le boîtier à l'ombre, sous un équipement existant, un panneau solaire, ou une feuille de métal mince spécifiquement placée à cet endroit à cette fin, vous augmentez la durée de vie au boîtier ainsi qu'à l'équipement contenu à l'intérieur.

Avant de mettre n'importe quelle pièce électronique dans un boîtier scellé, soyez sûr que celui-ci rempli les conditions minimales de dissipation thermique. Si votre carte mère exige un ventilateur ou un grand radiateur, rappelez-vous qu'il n'y aura aucun courant d'air, et que le réchauffement de votre équipement électronique pourrait bien le briser. Utilisez seulement des composantes électroniques qui sont conçues pour être employées dans un environnement embarqué.

# Fournir de l'énergie

Évidemment, l'alimentation en courant continu peut être fournie simplement en faisant un trou dans votre boîtier et en y insérant un câble. Si votre boîtier est assez grand (par exemple, une boîte électrique extérieure) vous pourriez même installer une prise de courant alternatif à l'intérieur de la boîte. Cependant, les fabricants se servent de plus en plus d'une technique très utile qui élimine le besoin de trou additionnel dans le boîtier: le ***Power over Ethernet*** (***POE***) (***alimentation à travers Ethernet***).

La norme 802.3af définit une méthode pour alimenter le matériel réseau en utilisant les paires inutilisées d'un câble Ethernet standard. Il est possible d'utiliser sans risque jusqu'à 13 watts de puissance sur un câble CAT5 sans faire interférence sur la transmission de données qui est réalisée sur le même câble. Les nouveaux commutateurs Ethernet compatibles avec la norme 802.3af (appelés ***end span injectors***) fournissent directement de l'énergie aux dispositifs connectés. Les commutateurs « *end span injectors* » peuvent fournir de l'énergie sur les mêmes câbles employés pour les données (paires 1-2 et 3-6) ou sur les câbles inutilisés (paires 4-5 et 7-8). Un autre équipement, appelé ***mid span injectors***, est inséré entre les commutateurs Ethernet et le dispositif à alimenter. Ces injecteurs assurent de l'énergie sur les paires inutilisées.

Si votre routeur sans fil ou CPE fonctionne sur la norme 802.3af, vous pourriez en théorie simplement le connecter à un injecteur. Malheureusement, certains fabricants (notamment Cisco) sont en désaccord sur la polarité de la puissance, et le fait de connecter des équipements incompatibles peut endommager l'injecteur et l'équipement à alimenter. Lisez attentivement les instructions et assurez-vous que votre injecteur et équipement sans fil coïncident avec les trous et la polarité qui doivent être employées pour les alimenter.

Si votre équipement sans fil ne supporte pas l'énergie à travers Ethernet, vous pouvez toujours employer les paires inutilisées du câble CAT5 pour porter l'énergie. Vous pouvez employer ***un injecteur POE passif*** ou en construire un vous-même. Ces dispositifs connectent manuellement l'alimentation continue aux câbles inutilisés sur une extrémité du câble, et relient l'autre extrémité directement à un connecteur à cylindre inséré dans la prise de courant de l'équipement. Normalement, on peut acheter une paire de dispositifs POE passifs pour moins de 20 dollars.

Pour le faire vous-même, vous devrez savoir quelle est l'énergie requise pour que le dispositif fonctionne et fournir au moins cette valeur en courant et en tension, ainsi qu'un peu plus pour justifier la perte sur Ethernet. Vous ne devrez pas fournir trop d'énergie car la résistance du petit câble peut présenter un risque d'incendie. Voici une calculatrice en ligne qui vous aidera à calculer la chute de tension sur un câble CAT5: *http://www.gweep.net/~sfoskett/tech/poecalc.html*.

Une fois que vous connaissez l'énergie appropriée et la polarité électrique requises pour alimenter votre équipement sans fil, prenez un câble CAT5 en employant uniquement les câbles de données (paires 1-2 et 3-6). Puis, branchez simplement le transformateur aux paires 4-5 (habituellement bleues / bleues-blanches) et 7-8 (marron / marron-blanc) sur une extrémité et un connecteur cylindrique assorti à l'autre. Pour un guide complet expliquant comment construire votre propre injecteur POE à partir de zéro, visitez ce fabuleux guide de NYCwireless à l'adresse suivante: *http://nycwireless.net/poe/*.

# Considérations de montage

Dans plusieurs cas, l'équipement peut être placé à l'intérieur d'un bâtiment où il y a des fenêtres en verre ordinaire laissant passer les rayons de soleil. Le verre normal présentera peu d'atténuation tandis que le verre teinté présentera une atténuation inacceptable. Ceci simplifie considérablement les questions de montage, d'énergie et de protection contre les intempéries. Par contre, cela est utile uniquement dans les secteurs peuplés.

En montant des antennes sur des tours, il est très important d'employer des supports et de ne pas monter les antennes directement sur la tour. Ces supports seront utiles entre autres pour la séparation et l'alignement de l'antenne ainsi que pour sa protection.

Le support doit être assez fort pour soutenir le poids de l'antenne et pour la tenir en place les jours venteux. Rappelez-vous que les antennes peuvent agir comme des petites voiles et peuvent appliquer beaucoup de force sur leur support les jours où le vent est fort. Au moment du calcul estimatif de la résistance du vent, on doit prendre en considération toute la surface de la structure de l'antenne ainsi que la distance du centre de l'antenne au point d'attachement au bâtiment. Les grandes antennes telles que les paraboles ou les panneaux sectoriels de gain élevé peuvent affronter une charge considérable de vent. Si nous utilisons une antenne parabolique avec des fentes ou constituée de treillis au lieu d'une surface pleine, nous pourrons réduire la charge du vent sans trop d'effet sur le gain de l'antenne. Soyez sûrs que les supports et la structure sont solides, dans le cas contraire vos antennes vont se désaligner avec le temps (ou pire, tomber complètement de la tour!)

Les supports doivent être suffisamment éloigné de la tour afin de pouvoir aligner l'antenne mais sans qu'il ne devienne trop difficile de l'atteindre si un service de réparation ou de maintenance est requis.

Le tuyau de support d'entretoise où l'antenne sera installée doit être circulaire. De cette façon on peut pivoter l'antenne sur le tuyau pour l'aligner. Deuxièmement, le tuyau doit également être vertical. S'il est monté sur une tour conique, le support d'entretoise devra être conçu pour tenir compte de ceci. Ceci peut être fait en utilisant différentes longueurs d'acier ou en employant des combinaisons de tiges filetées et de plaques d'acier.

*Figure 7.1: Une antenne avec un support d'entretoise étant élevée sur une tour*

Puisque l'équipement sera dehors pendant toute sa durée de vie, il est important d'être certain que l'acier utilisé est protégé contre les intempéries. L'acier inoxydable est souvent trop cher pour être employé dans l'installation d'une tour. La galvanisation à chaud est préférée, mais peut ne pas être disponible partout. Peindre l'acier avec une bonne peinture anti-rouille fonctionnera également. Si cette dernière option est choisie, il sera important de faire une inspection annuelle et de repeindre si nécessaire.

## Tours haubanées

Une tour haubanée sur laquelle il est facile de grimper est un excellent choix pour plusieurs installations. Cependant, pour les structures très grandes, une tour autoportante pourrait être exigée.

Pour faciliter l'installation des tours haubanées, une poulie attachée au dessus du mât sera très utile. Le mât sera fixé à la section inférieure déjà en place, alors que les deux sections de la tour sont attachées avec un joint articulé. Une corde passant par la poulie facilitera l'élévation de la prochaine section. Lorsque la section console est verticale, assujettissez-la à la section inférieure du mât. Celle-ci (appelé sur le marché, mât de charge) peut alors être enlevée, et l'opération peut être répétée, s'il y a lieu. Serrez les câbles à hauban soigneusement, en vous assurant que vous employez la même tension à tous les points d'ancrage appropriés. Choisissez les points de sorte que les angles, vus du centre de la tour, soient aussi également espacés que possible.

*Figure 7.2: Un tour haubanée qui peut être grimpée.*

## Tours autoportantes

Les tours autoportantes sont chères mais parfois nécessaires, en particulier quand une plus grande hauteur est requise. Elles peuvent être aussi simple qu'un poteau lourd enterré dans un bloc en béton ou aussi compliquées qu'une tour professionnelle de radio.

*Figure 7.3: Une tour autoportante simple.*

Une tour existante peut parfois être employée pour des abonnés, bien que les antennes de transmission de station AM devraient être évitées car la structure entière est opérationnelle. Les antennes de station FM sont acceptables à condition qu'il y ait au moins quelques mètres de distance entre les antennes. Vous devez considérer que même si les antennes de transmission adjacentes peuvent ne pas faire interférence avec votre connexion sans fil, une FM de haute puissance peut faire interférence avec votre câblage Ethernet. Toutes les fois que vous utilisez une tour à plusieurs antennes, soyez très scrupuleux au sujet de lui offrir une mise à la terre appropriée et considérez l'emploi d'un câble blindé.

*Figure 7.4: Une tour beaucoup plus compliquée.*

## Montages sur le toit

Sur les toits plats, il est possible d'utiliser des montages pour antennes qui ne pénètrent pas le sol. Ils consistent en un trépied monté à une base en métal ou en bois. La base est alors soutenue par des briques, des sacs de

sables, des cruches d'eau ou n'importe quel objet qui soit lourd. Le fait d'employer un tel montage « traîneau » élimine la nécessité de percer le toit avec des boulons de fixation évitant ainsi les fuites potentielles.

*Figure 7.5: Cette base de métal peut être soutenue avec des sacs de sable, des pierres ou des bouteilles d'eau pour rendre la plateforme stable sans avoir à percer le toit.*

Lorsqu'une structure existe déjà, telles que des cheminées ou les côtés des bâtiments, on peut utiliser des montages sur les murs ou des assemblages avec des courroies. Si les antennes doivent être montées à environ 4 mètres au-dessus du toit, la meilleure solution peut être une tour qui peut être grimpée afin de permettre un accès plus facile à l'équipement et pour empêcher le mouvement de l'antenne pendant des vents forts.

## Métaux différents

Pour réduire au minimum la corrosion électrolytique quand deux métaux différents sont en contact humide, leur potentiel électrolytique devrait être aussi semblable que possible. Employez de la graisse diélectrique sur la connexion entre deux métaux différents pour empêcher tout effet d'électrolyse.

Le cuivre ne devrait jamais toucher le matériel galvanisé directement sans une protection appropriée à la jonction. Une perte d'eau à partir du cuivre contient des ions qui enlèveront la couverture galvanisée (de zinc) de la tour. L'acier inoxydable peut être employé comme matériel amortisseur, mais n'oubliez pas que ce matériel n'est pas un très bon conducteur. S'il est employé comme isolant entre le cuivre et les métaux galvanisés, la superficie de la zone de contact devrait être large et l'acier inoxydable devrait être mince. Un composé à joint devrait également être employé pour couvrir la connexion afin que l'eau ne puisse pas passer entre les métaux différents.

## Protéger les connecteurs micro-ondes

L"humidité dans les connecteurs est probablement le bris le plus fréquent d'un lien radio. Soyez certain de serrer les connecteurs fermement mais, pour ce faire, n'utilisez jamais une clé ou tout autre outil. Rappelez-vous que les métaux se dilatent et se contractent avec les changements de température et un connecteur qui a été trop serré peut se casser à l'extrémité lorsque des changements climatiques extrêmes surviennent.

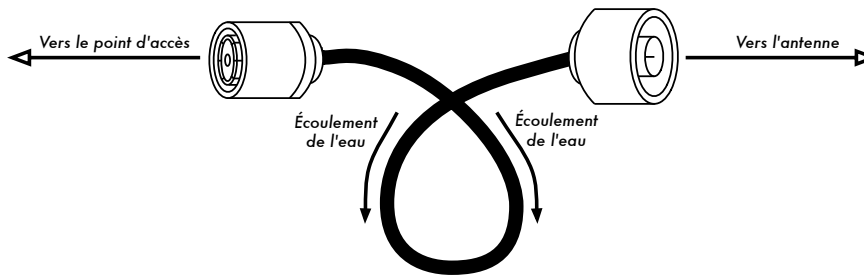


*Figure 7.6: Une boucle d'égouttement éloigne l'eau de la pluie des connecteurs.*

Une fois serrés, les connecteurs devraient être protégés en appliquant une couche de ruban électrique, puis une couche de ruban d'étanchéité, puis une couche différente de ruban électrique sur le dessus. Le mastic protège le connecteur contre l'infiltration de l'eau, et la couche de ruban électrique protège le mastic contre les rayons ultraviolets (UV). Les câbles devraient avoir une boucle supplémentaire d'égouttement pour empêcher l'eau d'entrer à l'intérieur de l'émetteur-récepteur.

# *Sécurité*

Lorsque vous travaillez en hauteur, utilisez toujours un harnais solidement attaché à la tour. Si vous n'avez jamais travaillé sur une tour, payez un professionnel pour le faire à votre place. Au-dessus d'une certaine hauteur, plusieurs pays exigent une formation spéciale pour que les personnes puissent travailler sur des tours.

Évitez de travailler sur des tours pendant des vents forts ou des orages. Grimpez toujours avec une autre personne et uniquement lorsqu'il y a beaucoup de lumière. Rappelez-vous qu'il est **extrêmement** dangereux de travailler dans l'obscurité. Accordez-vous beaucoup de temps pour accomplir le travail avant le coucher du soleil. Si vous manquez de temps, rappelez-vous que la tour sera là le lendemain et que vous pourrez alors y retravailler après une bonne nuit de sommeil.

# Aligner les antennes sur un lien à longue distance

Le secret pour aligner avec succès des antennes sur un lien à longue distance est la communication. Si vous changez trop de variables en même temps (par exemple, une équipe commence à agiter une antenne tandis que l'autre essaie de faire une lecture de la force du signal), alors le processus prendra toute la journée et vous n'obtiendrez probablement pas d'antennes correctement alignées.

Vous aurez deux équipes. Dans le meilleur des cas, chaque équipe devrait avoir au moins deux personnes: une pour prendre des lectures de signal et pour communiquer avec le site distant, l'autre pour manoeuvrer l'antenne. Vous devez prendre en considération les points suivants lorsque vous travaillez sur des liens à longue distance.

1. **Examinez tout l'équipement en avance**. Vous ne voulez pas bricoler l'équipement une fois sur le terrain. Avant de séparer l'équipement, branchez tout et connectez chaque antenne et câbles pour vous assurer que vous pouvez établir une connexion entre les dispositifs. Vous devriez pouvoir retourner à cet état (dont nous savons qu'il fonctionne) en allumant simplement le dispositif, sans devoir ouvrir une session ou changer un paramètre. C'est le bon moment pour convenir sur la polarité de l'antenne (voir le chapitre deux si vous ne comprenez pas ce qu'est la polarité).
2. **Emmenez un équipement de communication de secours**. Même si les téléphones mobiles sont habituellement assez bons pour travailler dans les villes, la réception mobile peut être mauvaise ou inexistante dans les zones rurales. Apportez une radio FRS ou GMRS à haute puissance ou une radio amateur si vos équipes ont les permis requis. Travailler à distance peut être très frustrant si vous demandez constamment à l'autre équipe « pouvez-vous m'entendre maintenant? ». Sélectionnez vos voies de transmission et examinez vos radios (y compris les batteries) avant de vous séparer.

3. **Emmenez un appareil photo**. Prenez le temps de documenter l'endroit de chaque emplacement, y compris les points de repère et les obstacles environnants. Plus tard, ceci peut être très utile pour déterminer la viabilité d'un autre lien à cet endroit sans avoir à y aller en personne. Si c'est votre première visite à l'emplacement, notez également les coordonnées GPS et l'altitude.

4. **Commencez par faire une estimation de l'orientation et de l'altitude appropriées**. Pour commencer, les deux équipes devraient employer la triangulation (en utilisant des coordonnées GPS ou une carte) pour avoir une idée approximative de la direction vers où pointer l'antenne. Utilisez une boussole pour aligner approximativement l'antenne vers l'orientation désirée. Les grands points de repère sont également utiles pour indiquer une direction. C'est encore mieux si vous pouvez utiliser des jumelles pour voir l'autre extrémité. Une fois que vous avez fait votre conjecture, prenez une lecture de la force du signal. Si vous êtes suffisamment proche et avez fait une bonne estimation, vous pourriez déjà capter le signal.

5. **Si tout le reste échoue, construisez votre propre point de repère**. Il peut être difficile de faire une estimation de l'emplacement de l'autre extrémité d'un lien sur certains types de terrains. Si vous établissez un lien dans un secteur avec peu de points de repère, aidez-vous d'un point tel qu'un cerf-volant, un ballon, la lumière d'un projecteur, une flamme ou même un signal de fumée. Vous n'avez pas nécessairement besoin d'un GPS pour avoir une idée de la direction où diriger votre antenne.

6. **Examinez le signal dans les deux directions, mais seulement une à la fois**. Une fois que les deux extrémités ont trouvé leur meilleur emplacement, l'extrémité avec l'antenne qui a le gain le plus bas doit fixer cette dernière. En utilisant un bon outil de surveillance (tel que Kismet, Netstumbler ou un outil inclus dans un bon client sans fil), l'équipe avec l'antenne qui a le plus haut gain devrait la déplacer lentement et horizontalement tout en observant le mesureur de signal. Une fois que la meilleure position est trouvée, essayez de changer la hauteur de l'antenne. Après que la meilleure position possible soit trouvée, fixez l'antenne fermement à cet endroit et demandez à l'autre équipe de commencer à bouger de façon circulaire. Répétez ce processus quelques fois jusqu'à ce que la meilleure position pour les deux antennes soit trouvée.

7. **Ne touchez pas l'antenne lorsque vous faites une lecture**. Votre corps affectera le modèle de rayonnement de l'antenne. Lorsque vous faites une lecture de la force du signal, ne touchez pas à l'antenne et ne vous tenez pas dans le chemin du signal. Il en va de même pour l'équipe de l'autre côté du lien.

8. **N'ayez pas peur si vous ne trouvez pas le meilleur signal**. Comme nous l'avons vu dans le chapitre quatre, les modèles de rayonnement

incorporent beaucoup de petits lobes latéraux de sensibilité en plus d'un lobe principal beaucoup plus grand. Si votre signal reçu est étrangement petit, vous avez peut-être trouvé un lobe latéral. Continuez de bouger lentement au delà de ce lobe pour voir si vous pouvez trouver le lobe principal.

9. **L'angle de l'antenne peut paraître complètement erroné**. Le lobe principal d'une antenne rayonne souvent légèrement à un côté ou à l'autre du point mort visuel de l'antenne. Ne vous inquiétez pas de l'apparence de l'antenne; vous devez vous occuper de trouver la meilleure position pour recevoir le plus grand signal possible.
10. **Vérifiez une deuxième fois la polarisation**. Il peut être frustrant d'essayer d'aligner une parabole pour découvrir que l'autre équipe utilise une polarisation opposée. Encore une fois, ceci devrait être convenu avant de partir de la base d'origine, mais si un lien reste obstinément faible, une deuxième vérification n'est jamais de trop.
11. **Si rien ne fonctionne, vérifiez toutes les composantes une par une**. Les dispositifs sur les deux extrémités du lien sont-ils allumés? Touts les câbles et connecteurs sont-ils correctement branchés, sans aucune pièce endommagée ou suspecte? Comme nous l'avons souligné au chapitre huit, une technique de dépannage appropriée vous fera gagner du temps et vous évitera bien des frustrations. Travaillez lentement et communiquez bien votre statut avec l'autre équipe.

En travaillant méthodiquement et en communiquant bien, vous pouvez accomplir le travail d'alignement des antennes à haut gain en peu de temps. Si le travail est réalisé correctement, ceci devrait être amusant!

# Protection contre la foudre

L'énergie est le plus grand défi pour la plupart des installations dans les pays en voie de développement. Là où il y a des réseaux électriques, ceux-ci sont souvent mal contrôlés, la tension électrique fluctue dramatiquement et les installations sont sensibles à la foudre. Une bonne protection contre les fluctuations de la tension est essentielle non seulement pour protéger votre équipement sans fil mais également tout équipement connecté à lui.

## Fusibles et disjoncteurs

Les fusibles sont primordiaux, mais très souvent négligés. Dans les zones rurales et même dans plusieurs zones urbaines des pays en voie de développement, il est très difficile de trouver des fusibles. En dépit du coût supplémentaire, il est toujours prudent d'employer des disjoncteurs. Il est possible qu'il soit nécessaire de les importer, mais on ne devrait pas passer

outre cette option. Trop souvent, des fusibles remplaçables sont enlevés pour les remplacer par n'importe quel élément moins coûteux. Dans un cas récent, tout l'équipement électronique d'une station de radio rurale a été détruit lorsqu'un éclair est passé par le circuit n'ayant aucun disjoncteur ou même un fusible pour le protéger.

## Comment faire une mise à terre

Faire une mise à terre appropriée ne devrait pas être un travail compliqué. Afin de réussir une mise à terre, vous devez accomplir deux choses: fournir un court-circuit dans le cas où une foudre tomberait et fournir un circuit pour que l'excès d'énergie puisse être dispersé.

La première étape consiste à protéger l'équipement contre un coup de foudre direct ou proche, alors que la seconde fournit un chemin pour absorber l'énergie excessive qui causerait autrement une accumulation de charge électrostatique. La charge électrostatique peut significativement détériorer la qualité du signal en particulier sur des récepteurs sensibles (par exemple, les VSATs). Il est simple de créer un court-circuit. L'installateur doit simplement faire le chemin le plus court à partir de la surface conductrice la plus élevée (un paratonnerre) jusqu'au sol. Lorsqu'une foudre frappe le paratonnerre, l'énergie suit le chemin le plus court et s'écartera ainsi de l'équipement. Ce câble de terre devrait être en mesure de supporter une haute tension (c.-à-d. que vous avez besoin d'un câble épais, comme un câble de cuivre tressé calibre 8).

Pour faire la mise à terre de l'équipement, montez un paratonnerre au-dessus de l'équipement sur une tour ou toute autre structure. Employez alors un câble conducteur épais pour connecter le paratonnerre à quelque chose qui a une bonne mise à terre. Les tuyaux de cuivre souterrains peuvent faire de bonnes mises à terre (dépendamment de leur profondeur, de l'humidité, la salinité, la quantité de métal et la teneur organique du sol). Dans plusieurs endroits en Afrique occidentale, les tuyaux ne sont pas encore enterrés, et l'équipement de mise à terre précédent est souvent inadéquat étant donné la mauvaise conductivité du sol (typique des climats arides et des sols tropicaux). Il y a trois manières faciles de mesurer l'efficacité du sol:

1. La moins précise est de brancher simplement un UPS de bonne qualité ou une barre de puissance ayant un indicateur détecteur de sol (Une diode électroluminescente, en anglais: *light-emitting diode* ou LED). Cette LED émet une lumière lorsqu'elle est parcourue par un courant électrique. Une mise à terre efficace dispersera de très faibles quantités d'énergie au sol. Certains emploient même ceci pour pirater de la lumière car cette énergie ne fait pas tourner le compteur électrique!

2. Prenez une douille et une ampoule de basse puissance en watts (30 watts), connectez un câble à la terre et le deuxième au courant positif. Si la mise à terre fonctionne, l'ampoule devrait briller légèrement.
3. La manière la plus sophistiquée est de simplement mesurer l'impédance entre le circuit positif et la terre.

Si votre mise à terre n'est pas efficace, vous devrez soit enterrer un poteau à une plus grande profondeur (où le sol est plus moite et a plus de matière organique et de métaux) ou rendre la terre plus conductrice. Une approche courante où il y a peu de sol est de creuser un trou d'un mètre de diamètre et deux mètres de profondeur et d'y laisser glisser un morceau de métal fortement conducteur qui a une certaine masse. On utilise généralement du plomb mais ça peut être n'importe quel morceau lourd de métal pesant 500 kilogrammes ou plus, tel qu'une enclume en acier ou une roue en fer. Remplissez alors le trou de charbon de bois en y mélangeant du sel, puis recouvrez-le avec de la terre. Imbibez le secteur et le charbon de bois et le sel se répandront autour du trou et feront un secteur conducteur entourant le plomb, améliorant ainsi l'efficacité de la terre.

Si vous employez un câble de radio, celui-ci aussi peut être employé pour faire la mise à terre de la tour. Cependant, une installation de qualité doit séparer la prise de terre de la tour du câble de radio. Pour la mise à terre du câble, épluchez un peu le câble au point le plus proche de la terre avant qu'il n'entre dans le bâtiment, attachez alors un câble de terre à partir de ce point, soit en soudant ou à l'aide d'un connecteur très conducteur. Ce joint doit être ensuite imperméabilisé.

## Stabilisateurs et régulateurs de puissance

Il y a beaucoup de marques de stabilisateurs de puissance, mais la plupart sont numériques ou électromécaniques. Ces derniers sont meilleur marché et beaucoup plus courants. Les stabilisateurs électromécaniques prennent la puissance à 220V, 240V ou 110V et utilisent cette énergie pour faire tourner un moteur qui produit toujours la tension désirée (normalement 220V). Ceci est normalement efficace, mais ces unités offrent peu de protection contre la foudre ou d'autres fluctuations subites de tension. Ils grillent souvent après le premier éclair. Une fois brûlés, ils peuvent être fusionnés à une certaine (habituellement fausse) tension de sortie.

Les régulateurs numériques régulent l'énergie en utilisant des résistances et d'autres composantes à état solide. Ils sont plus chers, mais sont beaucoup moins susceptibles de brûler.

Autant que possible, employez un régulateur numérique. Ils sont plus chers mais offrent une meilleure protection au reste de votre équipement. Soyez

certains de vérifier toutes les composantes de votre système d'alimentation (y compris les stabilisateurs) après que la foudre soit tombée.

# Énergie solaire et éolienne

Les applications décrites dans ce chapitre emploient la tension DC. Le courant DC – pour Direct Current en anglais (courant continu en français) a une polarité. Le fait de confondre la polarité va très probablement endommager immédiatement et irréversiblement votre équipement! Nous supposerons que vous savez manipuler un multimètre numérique (DMM) pour vérifier la polarité. Les tensions DC qui sont employées dans les applications décrites ne sont pas dangereuses lorsque vous touchez les conducteurs. Cependant, de grandes batteries d'acide de plomb peuvent fournir des courants très élevés. Un câble qui crée un court-circuit entre les bornes commencera immédiatement à rougir et à brûler son isolation. Pour empêcher le feu, il doit y avoir un fusible près de la borne positive de la batterie à tout moment. De cette façon, le fusible grillera avant les câbles.

Les batteries acide-plomb contiennent de l'acide sulfurique pouvant causer des brûlures graves. Elles libèrent de l'hydrogène lorsqu'elles sont chargées ou ont un court-circuit entre les bornes et ceci survient même si ce sont des batteries acide-plomb scellées. Une aération appropriée est nécessaire pour empêcher les explosions, particulièrement si les batteries utilisées sont du type ouvertes (*flooded cell type*, en anglais). Il est important de protéger ses yeux avec des lunettes de sûreté en manipulant ces batteries. J'ai déjà rencontré un « expert » en batterie qui en a fait exploser trois pendant sa carrière. Le plomb est toxique; assurez-vous de vous débarrasser de vos batteries usagées correctement. Ceci peut être difficile dans les pays où il n'existe aucune infrastructure de recyclage.

## Systèmes d'énergie autonomes

Il peut y avoir plusieurs situations où vous voulez installer un noeud sans fil dans une zone où le réseau électrique responsable de fournir l'énergie principale est instable ou simplement non existant. Ceci peut être le cas d'un relai sans fil isolé ou d'un pays en voie de développement où le réseau électrique fait souvent défaut.

Un système d'alimentation autonome consiste fondamentalement en une batterie qui stocke l'énergie électrique qui est produite par un générateur éolien, solaire et/ou à carburant. On y retrouve aussi les circuits électroniques qui contrôlent le processus de chargement/déchargement.

Lorsque nous concevons un système à énergie solaire ou éolienne, il est important de choisir un dispositif qui dépense un minimum d'énergie. Chaque

watt qui est gaspillé du côté du consommateur cause des coûts élevés du côté de la source d'énergie. Une plus grande consommation d'énergie signifie que de plus grands panneaux solaires et des batteries plus encombrantes seront nécessaires pour fournir l'énergie suffisante. En choisissant un équipement convenable qui puisse nous faire économiser de l'énergie, on économise du même coup beaucoup d'argent et on évite bien des ennuis. Par exemple, un lien de longue distance n'a pas nécessairement besoin d'un amplificateur fort qui dépense beaucoup d'énergie. Une carte Wi-Fi avec une bonne sensibilité de réception et une zone Fresnel qui a un espace libre d'au moins 60%, fonctionnera mieux qu'un amplificateur et économisera également de l'énergie. Une affirmation bien connue des radioamateurs s'applique ici aussi: le meilleur amplificateur est une bonne antenne. D'autres mesures pour réduire la consommation d'énergie incluent: réduire la vitesse de l'unité centrale de traitement, réduire la puissance de transmission à une valeur minimale nécessaire pour fournir un lien stable, augmenter la longueur des intervalles de la balise WiFi (*beacon*) et éteindre le système pendant les périodes où il n'est pas utilisé.

La plupart des systèmes solaires autonomes fonctionnent à 12 ou 24 volts. On devrait utiliser de préférence un dispositif sans fil qui fonctionne sur la tension DC à 12 volts que la plupart des batteries acide-plomb fournissent. Transformer la tension fournie par la batterie à AC ou employer une tension à l'entrée du point d'accès différente de la tension de la batterie causera une perte inutile d'énergie. Un routeur ou point d'accès qui accepte une tension DC de 8-20 volts est parfait.

La plupart des points d'accès bon marché ont un régulateur de tension à mode commuté à l'intérieur et fonctionnent sur une gamme de tension sans souffrir de modifications et sans se réchauffer (même si le dispositif a été fabriqué avec une alimentation d'énergie de 5 ou 12 volts).

**AVERTISSEMENT:** Le fait de faire fonctionner votre point d'accès avec une alimentation d'énergie autre que celle fournie par votre fabricant annulera certainement toute garantie et pourra endommager votre équipement. Même si la technique suivante fonctionnera normalement comme décrit, rappelez-vous que si vous l'essayez, vous le faites à vos risques et périls.

Ouvrez votre point d'accès et cherchez, près de l'entrée DC, deux condensateurs relativement grands et un inducteur (un tore avec un câble de cuivre enroulé autour de lui). S'ils sont présents, le dispositif a une entrée à mode commuté et la tension d'entrée maximale devrait être légèrement en dessous de la tension imprimée sur les condensateurs. Habituellement l'estimation de ces condensateurs est de 16 ou 25 volts. Prenez en compte qu'une alimentation d'énergie non régulée a une ondulation et peut introduire une tension beaucoup plus élevée dans votre point d'accès que peut suggérer la tension typique qui y est imprimée. Ce n'est donc pas une bonne idée de connecter

une alimentation d'énergie non régulée à 24 volts à un dispositif avec un condensateur à 25 Volt. Évidemment, le fait d'ouvrir votre dispositif annulera toute garantie existante. N'essayez pas d'actionner un point d'accès à une tension plus élevée s'il n'a pas de régulateur à mode commuté. Il se réchauffera, fonctionnera incorrectement ou brûlera.

Le populaire Linksys WRT54G fonctionne à n'importe quelle tension entre 5 et 20 volts DC et consomme environ 6 watts, mais a un commutateur Ethernet intégré. Avoir un commutateur est naturellement plaisant et utile, mais il consomme de l'énergie supplémentaire. Linksys offre également un point d'accès Wi-Fi nommé WAP54G qui consomme uniquement 3 watts et peut exécuter des progiciels d'OpenWRT et de Freifunk. Les systèmes 4G Accesscube consomment environ 6 watts une fois équipés d'une interface WiFi simple. Si le 802.11b est suffisant, les cartes mini-PCI avec le chipset d'Orinoco fonctionnent très bien tout en consommant une quantité minimale d'énergie.

Une autre stratégie importante pour économiser de l'énergie est d'employer des câbles d'alimentation DC courts, épais et de bonne qualité. Ceci limitera au minimum la perte de tension.

## Calculer et mesurer la consommation d'énergie

La conception d'un système autonome commence toujours par le calcul de la consommation d'énergie. La manière la plus facile de mesurer votre dispositif est une alimentation de laboratoire qui comporte un mesureur de tension et un ampèremètre. La tension nominale fournie par une batterie acide-plomb varie normalement entre 11 volts (vide) et environ 14,5 volts (durant la charge et à la charge complète). Vous pouvez régler la tension à l'alimentation de laboratoire et voir la quantité de courant que le dispositif consomme à différentes tensions. Si une alimentation de laboratoire n'est pas disponible, la mesure peut être effectuée en employant la fourniture incorporée au dispositif. Coupez un câble qui va à l'entrée DC de votre dispositif et insérez un **ampèremètre**. Notez que l'ampèremètre pourra se brûler ou brûler votre alimentation d'énergie s'il est appliqué entre la borne positive et négative car il se comporte comme un simple câble entre les sondes; créant de ce fait un court-circuit. Beaucoup d'ampèremètres ont une entrée sans fusibles, manipulez-les donc avec grand soin car ils peuvent facilement s'endommager.

La quantité d'énergie consommée peut se calculer à l'aide de la formule suivante:

```
P = U * I
```

P étant l'énergie en Watts, U étant la tension en Volts et I étant le courant en Ampère. Par exemple:

```
6 Watts = 12 Volts * 0,5 Ampère
```

Le résultat est l'estimation de consommation du dispositif. Si le dispositif de l'exemple fonctionne pendant une heure, il consommera seulement 6 watts/heure (Wh), respectivement 0,5 ampère/heure (Ah). Ainsi le dispositif consommera 144 Wh ou 12 Ah par jour.

Pour simplifier les choses, j'emploierai l'estimation de tension nominale des batteries pour des calculs et ne tiendrai pas compte du fait que la tension fournie par la batterie change selon sa quantité de charge. Les batteries sont évaluées à leur capacité Ah; il est donc plus facile de calculer en utilisant l'Ah au lieu de Wh. Une batterie d'un grand camion a en général 170 Ah - une batterie de camion chargée à 100% fera donc fonctionner donc le dispositif pour environ 340 heures pendant un cycle de décharge à 100%.

## Caractéristiques de décharge - Principes de base

Une batterie acide-plomb de 12 volts qui fournit de l'énergie à un consommateur fournit une tension selon sa charge. Quand la batterie est 100% chargée, elle a une tension de sortie de 12,8 volts qui chute rapidement à 12,6 volts sous tension. Etant donné que la batterie doit fournir un courant constant, la tension de sortie est maintenant linéaire, passant de 12,6 volts à 11,6 volts sur une longue période. À moins de 11,6 volts, la tension de sortie chute rapidement au cours du temps. Puisque la batterie fournit approximativement 95% de son énergie dans cette chute de tension linéaire, l'état de la charge pourrait être estimé en mesurant la tension pendant son utilisation. Le postulat est que la batterie est 100% complète à 12,6 volts et a une charge de 0% à 11,6 volts. Ainsi, en mesurant une batterie qui est actuellement déchargée, son état peut être estimé avec un multimètre numérique. Par exemple une lecture de 12,5 volts correspond à une charge de 90%, 12,3 volts correspond à une charge de 70%, etc...

Les batteries acide-plomb se dégradent rapidement lorsque les cycles de charge descendent à 0%. La batterie d'un camion perdra 50% de sa capacité de conception en moins de 50 - 150 cycles si elle est entièrement chargée et déchargée pendant chaque cycle. À une charge de 0% la batterie a toujours 11 volts sur les bornes sous tension. Ne déchargez jamais une batterie acide-plomb de 12 volts en dessous de cette valeur car ceci lui fera perdre une quantité énorme de capacité de stockage. Le fait de la décharger à 0 volts la détruira complètement. Pour éviter ceci, un circuit de débranchement de basse tension (en anglais, *low voltage disconnect circuit -LVD*) devrait être utilisé pour construire un système d'alimentation à batterie. Durant l'usage du cycle, il n'est pas recommandé de décharger une batterie de

camion sous 70%. Vous augmenterez significativement sa longévité en évitant de la décharger sous 80%. En conséquence, une batterie de camion de 170 Ah n'a qu'une capacité utilisable de 34 à 51 Ah!

Une batterie de voiture ou de camion devrait rester sous tension au delà de 12,3 volts. Dans de rares cas, il peut être permis d'aller en dessous de cette valeur; par exemple, pour une longue période inattendue de mauvais climat. Ceci est tolérable si la batterie est entièrement chargée après un tel incident. Charger à 100% prend assez de temps car le processus de charge ralentit en approchant la fin du chargement même s'il y a abondamment d'énergie à la source. Une source d'énergie faible qui peut rarement effectuer un charge complète et ainsi, user les batteries rapidement. C'est pour cette raison que l'on recommande de charger agressivement afin de maintenir les coûts d'utilisation bas. Un régulateur de charge solaire ou éolien ou un chargeur de batterie automatique (avec des caractéristiques de charge avancées) vous aidera à économiser de l'argent. Le meilleur choix est la caractéristique IUIa et le second, la caractéristique IU.

Les batteries de démarrage sont les batteries les moins coûteuses disponibles, mais elles peuvent ne pas être la meilleure option. Il y a des batteries solaires spéciales sur le marché qui sont conçues pour l'usage dans les systèmes solaires. Elles permettent des cycles de recharge plus profonds (en dessous de 50% de charge, selon le type) et ont un faible courant d'auto décharge. Les batteries acide-plomb scellées sont plus chères mais leur manipulation est plus sécuritaire.

Les batteries de camion ou de voiture qui portent la mention ***exemptes d'entretien*** devraient avoir un courant d'auto décharge négligeable. Cependant, les batteries exemptes d'entretien ont toujours besoin d'entretien. Le niveau du fluide d'électrolyte doit être vérifié fréquemment, particulièrement dans les climats chauds. S'il y a perte d'électrolyte, de l'eau distillée doit être employée pour remplir le fluide. Le fait de négliger celà, ruinera la batterie.

Trop charger vos batteries les détruiront aussi! Le courant de charge dans un système de batterie protégé doit être régulé. Un chargement excessif et illimité détruira la batterie. Si la tension dans la batterie est trop haute, la composante d'eau de l'acide sulfurique va succomber à la pression de l'électrolyse, créant une atmosphère qui contient une quantité concentrée d'oxygène. L'oxygène est très corrosif et détruira les connecteurs internes.

## Conception d'un système protégé par batterie

Les choses sont moins compliquées s'il y a un réseau électrique principal instable disponible qui accomplit son travail de temps en temps. Dans ce

cas, tout ce dont nous avons besoin est d'un chargeur automatique correct qui soit capable de charger entièrement une batterie d'une taille suffisante. Il serait souhaitable d'avoir un chargeur en mode commuté avec un large intervalle de tension d'entrée et des caractéristiques de chargement sophistiquées. Ceci pourra offrir une protection contre les changements de tension du réseau électrique. Les chargeurs bon marché qui ont un simple transformateur pourraient ne jamais charger complètement votre batterie si la tension du réseau électrique est trop faible. Un chargeur simple conçu pour 230 volts AC fournira de peu à aucun courant de charge lorsqu'il est mis en opération à 200 volts ou moins. Il ne réalisera jamais une charge complète, même s'il fonctionne pendant une longue période de temps. D'autre part, il brûlera si la tension est un peu plus forte que prévu; ou il ruinera tout simplement les batteries après un certain temps. Dans plusieurs situations, se munir d'un stabilisateur de tension AC empêchera votre chargeur de brûler à cause d'une haute tension excessive.

Un système protégé par batterie ressemble à ceci:

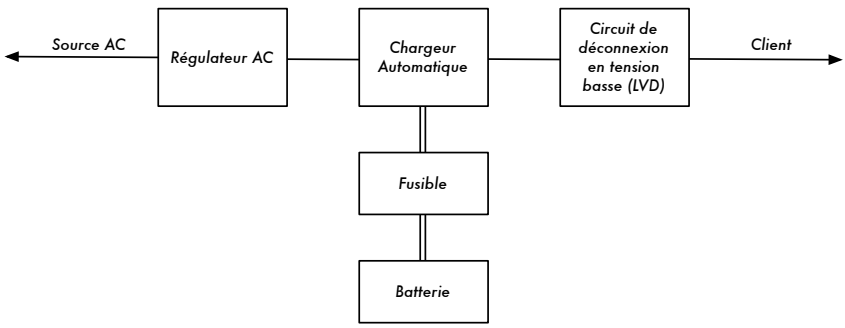


*Figure 7.7: Un système complet de protection batterie.*

Supposons que notre dispositif consomme 7 Watts à 12 Volts. Nous avons besoin du service 24 heures par jour; le dispositif consommera donc:

```
168 Wh = 24h * 7 W
```

À 12 Volt, le courant en ampères serait:

```
14 Ah = 168 Wh / 12 Volt
```

À présent, supposons qu'occasionnellement nous vivons une situation où le réseau électrique fait défaut pendant une semaine.

```
98 Ah = 14 Ah/jour* 7 jours
1176 Wh = 98 Ah * 12 Volt
```

Si nous permettons que notre batterie se décharge du 100% au 30%, consommant donc 70% de sa capacité, nous avons besoin d'une capacité de stockage de:

```
140 Ah = 98 ah / 0,7
```

Une batterie de camion a cette taille.

Normalement, l'énergie est de retour pendant 5 heures par jour, le système fonctionnera donc 19 heures sur batterie.

```
133 Wh = 19h * 7 Watt
```

Charger et décharger une batterie n'est jamais efficace à 100%. Comme il y aura de la perte d'énergie dans la batterie, nous devrons la charger avec plus d'énergie que celle que nous obtiendrons. L'efficacité du chargement/déchargement est habituellement de l'ordre de 75%.

```
177,4 Wh = 133 Wh / 0,75
```

Nous désirons charger la batterie complètement et atteindre une charge complète en 5 jours.

Considérons l'efficacité de charge:

```
166 Wh = 148 Wh / 0,75
```

Nous la convertissons en Ah:

```
14,8 Ah = 177,4 Wh / 12 Volt
```

Considérons le temps de charge:

```
2,96 A = 14,8 Ah / 5h
```

Tandis que nous chargeons, le point d'accès/routeur consomme toujours de l'énergie.  7 Watts est égal à 0,6 Ampère à 12 Volts:

```
3,56 A = 2,96 A + 0,6 A
```

Nous devrions considérer que le processus de charge ralentit lorsqu'il s'approche à la fin de la période de charge. Il vaudrait mieux avoir un courant de charge initial plus élevé que ce que nous avons calculé pour réaliser une charge de 100%. Un temps de charge de 5 heures est très peu, un chargeur IUIa à 8 ampères ou plus serait donc un bon investissement.

Comme l'électrolyte est vérifié fréquemment, même une batterie bon marché de camion peut avoir une durée de vie de 5 ans. N'oubliez pas d'utiliser un circuit de débranchement de basse tension. Ce n'est pas une erreur de surdimensionner un système à un certain degré. Peu importe si le système est bien conçu, la batterie sera éventuellement usée et devra être remplacée. En général, il est plus rentable de surdimensionner la source d'énergie plutôt que les batteries.

## Conception d'un système à énergie solaire ou éolienne

La quantité d'énergie que vous pouvez consommer avec un système à alimentation solaire ou éolienne dépend du secteur où vous vous trouvez ainsi que la période de l'année. Habituellement, des autorités compétentes en conditions climatiques pourront vous renseigner sur l'énergie de rayonnement du soleil ou de la vitesse du vent. Ces entités rassemblent ce genre d'information au cours des années et peuvent vous dire ce que vous devez prévoir pour chaque période de l'année. Des programmes de simulation et de calcul pour les systèmes solaires sont disponibles, PVSOL étant un programme commercial (et coûteux). Une version démo est disponible dans plusieurs langues.

Calculer exactement combien d'énergie un système à alimentation solaire produira à un certain endroit requiert beaucoup de travail. Le calcul doit considérer des facteurs tels que la température, le nombre d'heures de soleil, l'intensité du rayonnement, les réflexions dans l'environnement, l'alignement des panneaux solaires et ainsi de suite. Un programme de simulation avec les données climatiques est un bon point de départ mais n'oubliez pas que dans la vraie vie, quelque chose d'aussi banal comme la saleté sur les panneaux solaires peut complètement fausser les résultats de votre calcul théorique.

Il est difficile de faire une estimation de la quantité d'énergie produite par un générateur éolien s'il y a des obstacles autour de lui. L'approche empirique serait de mesurer la vitesse du vent réelle à l'emplacement sur une année; ce qui est plutôt impraticable.

Ceci devrait être un guide pratique. Si ni les programmes informatiques luxueux ni les données climatiques détaillées ne sont disponibles dans votre pays, je vous suggère d'établir un système pilote. Si la batterie ne se charge pas suffisamment, il est temps d'augmenter le nombre ou la taille des panneaux solaires. Tel que mentionné auparavant, il est très important de maintenir la consommation d'énergie au minimum afin d'éviter des coûts élevés inattendus.

Si votre système doit avoir un temps de fonctionnement de 100%, vous devrez commencer par considérer la pire période de l'année. Vous devez décider si le système aura besoin d'une capacité de stockage surdimension-

née ou d'une source d'énergie surdimensionnée afin de fournir de l'énergie pendant des périodes plus calmes. Il peut être beaucoup moins coûteux de charger manuellement le système à l'aide d'un générateur fonctionnant avec du carburant durant de longues périodes de calme.

La combinaison du vent et de l'énergie solaire semble raisonnable dans des secteurs où les différentes saisons fournissent de l'énergie éolienne lorsque l'énergie solaire est faible. Par exemple, en Allemagne le soleil fournit seulement 10% de l'énergie en hiver en comparaison avec l'été. Au printemps et à l'automne, il n'y a pas beaucoup d'énergie solaire non plus, mais le climat est très venteux. Des batteries de grande taille sont nécessaires puisqu'il est possible que ni les panneaux solaires ni les générateurs de vent puissent fournir suffisamment d'énergie pendant l'hiver.

Dans de telles conditions, un système conçu pour fonctionner 100% du temps a besoin d'une marge de sûreté correcte et beaucoup de capacité de stockage. La charge devrait se faire complètement aussi souvent que possible pendant les périodes de bonnes conditions climatiques. En fin de compte, les panneaux solaires peuvent devoir être remplacés tous les 25 ans; tandis qu'une batterie dans un système qui n'a pas suffisamment d'énergie de chargement peut avoir besoin d'un remplacement chaque année!

## Circuit

Un système autonome solaire consiste en:

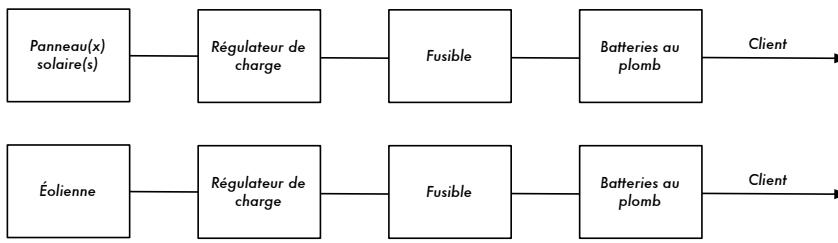


*Figure 7.8: Un système à énergie solaire ou éolienne.*

Si on combine l'énergie solaire et éolienne, les deux systèmes sont connectés à la même batterie.

## Énergie éolienne

Un générateur éolien est une option évidente lorsqu'un système autonome est conçu pour un transmetteur sans fil à installer sur une colline ou une montagne. Un point à prendre en considération avec l'énergie éolienne est que la vitesse du vent, dans un endroit entourés d'objets, sera suffisamment forte qu'en hauteur, au-dessus de ces objets. La vitesse moyenne du vent au

cours de l'année devrait être d'au moins 3 à 4 mètres par seconde et le générateur de vent devrait être 6 mètres plus haut que les autres objets sur une distance de 100 mètres. Un endroit trop loin de la côte manque habituellement d'énergie éolienne suffisante pour soutenir un système d'alimentation par le vent.

## Énergie solaire

Dans la plupart des cas, un système employant uniquement des panneaux solaires est la meilleure solution. Il est habituellement très facile de trouver un endroit approprié pour les panneaux solaires. De plus, ils ne contiennent aucune pièce mécanique mobile qui ait besoin d'entretien.

Il est important pour un système solaire que les panneaux soient montés avec le meilleur alignement et angle vers le soleil. Le meilleur angle peut changer au cours de l'année et dépend de l'endroit de l'emplacement. C'est une bonne idée de tenir compte du fait que la poussière, les feuilles ou les oiseaux peuvent se poser sur un panneau solaire. L'angle optimum de montage peut être très horizontal, ce qui cause plus de saleté sur le panneau solaire et requiert un nettoyage fréquent.

Il ne doit pas y avoir d'ombre sur le panneau solaire durant le jour, car les panneaux solaires se composent d'un certain nombre de piles solaires qui sont connectés en guirlande (*daisy chain*). Une chaîne est aussi forte que son maillon le plus faible. Si quelque chose couvre complètement la cellule d'un panneau solaire, une feuille par exemple, le panneau solaire entier ne produira aucune énergie. Même l'ombre d'un câble réduira de manière significative la quantité d'énergie produite par le système solaire!

## Régulateurs de charge

Les régulateurs de charge pour les générateurs éoliens sont différents des régulateurs pour les panneaux solaires. Si le système offre l'énergie éolienne et solaire alors deux régulateurs sont nécessaires. Chaque régulateur doit être directement connecté aux bornes de la batterie (par l'intermédiaire d'un fusible, naturellement!).

## Influence du suivi du point de puissance maximale

Les fabricants de panneaux solaires sont optimistes au moment de calculer la puissance maximale d'énergie de leurs panneaux. La puissance qui est efficacement produite par un panneau est donc sensiblement inférieure à celle indiquée sur la fiche technique. La puissance maximum d'énergie est uniquement réalisée à une certaine tension, à une température de panneau de 20 degrés Celsius et à un rayonnement de soleil de 1000 watts par mètre

carré. Ceci n'est pas réaliste puisqu'un panneau solaire devient vraiment chaud sous un rayonnement de 1000 watts par mètre carré. Une haute température réduit la génération efficace d'énergie d'un panneau. Il n'y a pas grand chose qui puisse être faite à ce sujet, à part le fait de maintenir à l'esprit qu'un panneau n'atteint jamais la puissance d'énergie indiquée par les fabricants.

Dans un système autonome, ce qui doit principalement être considéré est l'influence de la tension de sortie du panneau. Si un régulateur de charge simple est employé, la tension dans le panneau chute et atteint le niveau de la tension de la batterie. Un panneau solaire semble avoir une meilleure efficacité à 18 volts - il peut produire 1 ampère à 300 Watt/m à 30 degrés Celsius. Ce point d'efficacité meilleure s'appelle ***Point de Puissance Maximale- PPM*** (en anglais, *Maximum Power Point- MPP*).

En conséquence, un panneau va produire:

```
18 Watt = 18 Volt * 1 Ampere
```

If this panel is connected to a battery at 12,3 Volt the current will be slightly higher than in the MPP, maybe 1,1 Ampere, but the panel voltage will drop down to the level of the battery:

```
18 Watt = 18 Volt * 1 Ampère
```

Si ce panneau est connecté à une batterie à 12,3 volts, le courant sera légèrement plus haut que dans le PPM, peut-être 1,1 Ampère, mais la tension de panneau chutera jusqu'à atteindre le niveau de la batterie:

```
13,5 Watt = 12,3 Volt * 1,1 Ampère
```

L'efficacité dans notre exemple serait uniquement de 75% avec un régulateur de charge simple. Ce problème pourrait être résolu en employant un régulateur solaire avec un suivi du Point de Puissance Maximale. Un régulateur PPM bien conçu atteint une efficacité de 90%. Un système avec un régulateur simple peut ne jamais réaliser plus de 70% de l'estimation de puissance indiquée par le fabricant.

## Accroître la capacité de la batterie et du panneau solaire

Si vous voulez combiner deux batteries (ou plus) pour augmenter la capacité, interconnectez-les de façon parallèle, c.-à-d. connectez ensemble les deux bornes positives avec un câble épais. Il doit y avoir un fusible dans le câble près de chaque borne positive. Connectez ensemble les bornes néga-

tives sans fusibles. De la même façon, pour interconnecter les panneaux solaires, les fusibles ne sont pas nécessaires.

## Circuits de déconnexion à faible voltage

Vos consommateurs (votre point d'accès, routeur sans fil ou tout autre dispositif) seront connectés au régulateur de charge. La plupart des régulateurs de charge viennent avec un circuit de déconnexion à faible voltage. Le circuit de déconnexion à faible voltage ne devrait jamais s'éteindre, autrement il y a un sérieux problème de conception ou le circuit est endommagé. S'il y a deux régulateurs ou plus dans le système qui ont un circuit de déconnexion à faible voltage, connectez alors les consommateurs à un seul régulateur. Dans le cas contraire, les régulateurs pourraient être endommagés.

## Calcul

Le calcul d'un panneau solaire n'est pas très différent de celui du système protégé par batteries (tel qu'expliqué ci-haut). Évidemment, le temps où il n'y a aucune énergie disponible pour charger les batteries peut être très long et il n'y a aucune source de courant fixe qui pourrait être utilisée dans le calcul.

Un système bien conçu devrait pouvoir recharger entièrement une batterie vide en quelques jours dans de bonnes conditions climatiques tout en fournissant de l'énergie aux consommateurs.

# 8
# Dépannage

La façon dont vous établissez l'infrastructure de soutien pour votre réseau est aussi importante que le type d'équipement que vous employez. Contrairement aux connexions câblées, les problèmes avec un réseau sans fil sont souvent invisibles et peuvent demander plus de compétence et de temps afin de les diagnostiquer et de les résoudre. L'interférence, le vent et de nouvelles obstructions physiques peuvent rendre défectueux un réseau qui fonctionnait depuis longtemps. Ce chapitre détaille une série de stratégies pour vous aider à créer une équipe qui peut soutenir votre réseau efficacement.

## *Créer votre équipe*

Chaque village, compagnie ou famille a des individus qui sont intrigués par la technologie. Ce sont, entre autres, ceux que l'on retrouve à bricoler un câble, à réparer une télévision brisée ou à souder un nouveau morceau à une bicyclette. Ces personnes prendront de l'intérêt au sujet de votre réseau et voudront en apprendre autant que possible. Bien que ces personnes soient des ressources de valeur inestimable, vous devez éviter de former et donner toute la connaissance spécialisée du réseau sans fil à une seule personne. Si cette personne est votre unique spécialiste et perd l'intérêt ou trouve un travail mieux rémunéré ailleurs, elle partira en emportant toute la connaissance avec elle.

Il peut également y avoir beaucoup d'adolescents jeunes et ambitieux ou de jeunes adultes qui seront intéressés et auront le temps d'écouter, d'aider et de se renseigner sur le réseau. Encore une fois, ces personnes peuvent être très utiles et peuvent apprendre rapidement, mais l'équipe de projet doit concentrer son attention sur ceux qui sont le mieux placés pour soutenir le réseau dans les prochains mois et années. Les jeunes adultes et les adolescents iront à l'université ou trouveront un emploi, particulièrement les jeunes

ambitieux qui sont ceux qui tendent à vouloir être impliqués. Ces jeunes ont également peu d'influence dans la communauté où un individu plus âgé est susceptible d'être plus en mesure de prendre les décisions qui affectent directement le réseau dans l'ensemble. Quoique ces individus pourraient avoir moins de temps pour apprendre et pourraient sembler être moins intéressés, leur participation et une formation appropriée au sujet du système peuvent s'avérer essentiels.

Par conséquent, une stratégie principale lorsque nous créons une équipe de soutien est d'équilibrer et de distribuer la connaissance parmi ceux qui sont mieux placés pour soutenir le réseau à long terme. Vous devriez impliquer les jeunes, mais ne les laissez pas capitaliser à eux seuls l'utilisation ou la connaissance de ces systèmes. Trouvez et formez des personnes qui sont engagées au sein de la communauté, qui ont des racines dans la communauté et qui peuvent être motivées. Une stratégie complémentaire est de compartimenter les fonctions et les tâches, et de documenter toutes les méthodologies et procédures. De cette façon, les gens peuvent être formés facilement et être remplacés avec peu d'effort.

Par exemple dans un projet, l'équipe de formation a choisi un jeune diplômé d'université intelligent qui était revenu à son village. Il était très motivé et a appris rapidement. Comme il a appris si rapidement, on lui a enseigné plus que ce qui avait été prévu, en le rendant ainsi capable de traiter une variété de problèmes, de réparer un ordinateur à refaire le câblage Ethernet. Malheureusement, deux mois après le lancement du projet, il a reçu une offre d'emploi du gouvernement et a quitté la communauté. Même un meilleur salaire n'aurait pas pu le convaincre de rester puisque la perspective d'un travail stable au gouvernement était trop attirante. Toute la connaissance au sujet du réseau et comment le soutenir est partie avec lui. L'équipe de formation a dû revenir sur place pour recommencer une formation. La prochaine stratégie fut de diviser les fonctions et de former des personnes qui seraient enracinées dans la communauté de manière permanente: des personnes qui avaient une maison, des enfants et qui avaient déjà un emploi. La formation de trois personnes prend trois fois plus de temps que le temps dépensé dans la formation du jeune diplômé d'université, mais la communauté pourra retenir cette connaissance beaucoup plus longtemps.

Avec ceci nous voulons dire que le fait de choisir par vous-même la personne qui devrait être impliquée dans votre projet, n'est peut être pas la meilleure approche. Il est souvent mieux de trouver une organisation locale ou un administrateur local et de travailler avec eux afin de trouver l'équipe technique adéquate. Les valeurs, l'histoire, la politique locale et beaucoup d'autres facteurs seront importants pour eux, alors que complètement inaccessibles pour les personnes qui ne sont pas de cette communauté. La meilleure approche est de préparer votre partenaire local, lui fournir des critères cohérents, de vous assurer qu'il les comprend et d'établir des limites strictes.

Ces limites devraient tenir compte du népotisme et du patronage, tout en considérant la situation locale. Il peut être impossible de dire que vous ne pouvez pas employer un parent, mais il est mieux de fournir des moyens de contrôle et d'équilibre. Lorsqu'un candidat est un parent, il devrait y avoir des critères clairs et une deuxième autorité qui appuie cette candidature. Il est également important que ce soit le partenaire local qui ait cette autorité et non les organisateurs du projet, ce qui pourrait compromettre leur capacité de gestion. Ils seront mieux placés pour juger qui travaillera mieux avec eux. S'ils sont bien préparés dans ce processus, alors vos conditions devraient être satisfaites.

Le dépannage et le support de la technologie est un art abstrait. La première fois que vous regardez une peinture abstraite, celle-ci peut ne représenter pour vous qu'un ensemble d'éclaboussures aléatoires de peinture. Après avoir réfléchi sur la composition pendant un certain temps, vous pourriez commencer à apprécier le travail dans l'ensemble et la cohérence « invisible » peut devenir très réelle. Un débutant qui regarde un réseau sans fil peut voir les antennes, les câbles et les ordinateurs, mais il peut avoir besoin d'un certain temps pour apprécier le but du réseau « invisible ». Dans des secteurs ruraux, les personnes de la localité ont souvent besoin d'un grand travail de compréhension avant qu'ils n'apprécient un réseau invisible qui a été installé dans leur village. Par conséquent, une approche par étapes est nécessaire pour aider ces personnes à soutenir des systèmes technologiques. La meilleure méthode est la participation. Une fois que les participants sont choisis et sont engagés sur le projet, faites-les participer autant que possible. Laissez-les « conduire ». Donnez-leur le sertisseur ou le clavier et montrez-leur comment effectuer le travail. Même si vous n'avez pas le temps d'expliquer chaque détail et même si cela est plus long, ils doivent être impliqués physiquement et voir non seulement ce qui a été fait afin de bien apprécier le travail effectué.

On enseigne la méthode scientifique dans pratiquement toutes les écoles occidentales. Plusieurs personnes l'apprennent avant même d'entrer dans une classe de science de secondaire. Présentée simplement, elle consiste à prendre un ensemble de variables puis de les éliminer lentement à travers des tests binaires jusqu'à ce qu'il ne reste qu'une ou seulement quelques possibilités. Avec ces possibilités à l'esprit, vous pouvez compléter l'expérience. Vous devez alors examiner l'expérience pour voir si sa portée est semblable au résultat prévu. Si elle ne l'est pas, vous devez recalculez votre résultat prévu et réessayer. Le villageois rural typique a peut-être une première connaissance du concept, mais n'aura probablement pas eu l'occasion de résoudre des problèmes complexes. Même s'il est au courant de la méthode scientifique, il ne pensera peut-être pas à l'appliquer pour résoudre des problèmes réels.

Cette méthode est très efficace, bien que longue. On peut aller plus vite en faisant des suppositions logiques. Par exemple, si un point d'accès fonctionnant depuis longtemps arrête soudainement de fonctionner après un orage, alors vous pouvez supposer que le problème est relié à l'alimentation d'énergie et donc sauter la majeure partie du processus scientifique. On devrait enseigner les gens chargés du support technologique de dépanner en utilisant cette méthode, car il y aura des périodes où le problème ne sera ni connu ni évident. Des arbres de décision ou des organigrammes simples peuvent être faits pour tester ces variables et pour essayer de les éliminer afin d'isoler le problème. Naturellement, ces diagrammes ne devraient pas être suivis aveuglément.

Il est souvent plus facile d'enseigner cette méthode en utilisant un problème non technologique d'abord. Par exemple, faites développer à votre étudiant un procédé de résolution de problèmes sur quelque chose de simple et de familier, comme une télévision à batteries. Commencez par abîmer la télévision. Donnez-lui une batterie qui n'est pas chargée. Débranchez l'antenne. Insérez un fusible brisé. Testez l'étudiant en lui indiquant clairement que chaque problème montrera des symptômes spécifiques et indiquez le chemin quant à la façon de procéder. Une fois qu'il a réparé la télévision, faites lui appliquer ce procédé à un problème plus compliqué. Dans un réseau, vous pouvez changer une adresse IP, changer ou détruire des câbles, employer un faux SSID ou orienter l'antenne dans une fausse direction. Il est important que votre étudiant développe une méthodologie et un procédé pour résoudre ces problèmes.

# Technique de dépannage appropriée

Aucune méthodologie de dépannage ne peut complètement couvrir tous les problèmes que vous rencontrerez lorsque vous travaillerez avec des réseaux sans fil. Mais souvent, les problèmes découlent d'une ou de quelques erreurs communes. Voici quelques points simples à retenir qui peuvent faire que votre dépannage va dans la bonne direction.

- **Ne paniquez pas.** Si vous dépannez un système, cela signifie qu'il fonctionnait à un certain moment, probablement très récemment. Avant de commencer à faire des changements, examinez la scène et évaluez exactement ce qui est brisé. Si vous pouvez commencer à travailler à partir des journaux(*log*) d'historiques ou de statistiques, c'est encore mieux. Soyez sûr de rassembler l'information d'abord, ainsi vous pouvez prendre une décision avertie avant de faire des changements.
- **Est-ce branché?** Cette étape est souvent négligée jusqu'à ce que beaucoup d'autres avenues soient explorées. Des prises peuvent accidentellement (ou intentionnellement) être débranchées très facilement. Le câble est-il relié à une bonne source d'énergie? L'autre extrémité est-elle reliée à

votre dispositif? La lumière de puissance est-elle allumée? Ceci peut sembler idiot, mais vous vous sentirez encore plus idiot si vous perdez beaucoup de temps à vérifier une ligne d'alimentation d'antenne pour vous rendre compte qu'un AP a été débranché pendant tout ce temps. Faites-moi confiance, ce problème se produit beaucoup plus souvent que la plupart d'entre nous voudrait bien l'admettre.

- **Quelle a été la dernière chose à être modifiée?** Si vous êtes la seule personne avec l'accès au système, quel est le dernier changement que vous avez réalisé? Si d'autres ont accès à lui, quel est le dernier changement qu'ils ont fait et quand? Quand a été la dernière fois que le système a fonctionné? Souvent, les changements dans le système ont des conséquences fortuites qui ne sont pas notées immédiatement. Revenez en arrière et défaites ce changement pour voir quel effet ceci a sur le problème.
- **Faites une sauvegarde.** Ceci s'applique aussi bien avant que vous n'observiez qu'il y a un problème qu'après. Si vous faites un changement compliqué de logiciel à un système et que vous avez fait une sauvegarde, vous pouvez rapidement revenir à l'état précédent et recommencer si nécessaire. En dépannant des problèmes très complexes, avoir une configuration qui fonctionne partiellement peut être bien mieux qu'avoir un désordre qui ne fonctionne pas du tout (et que vous ne pouvez pas facilement reconstituer de mémoire).
- **Le connu comme étant bon.** Cette idée s'applique au matériel, aussi bien qu'au logiciel. Un « ***connu comme étant bon*** » (***known good*** en anglais) est n'importe quel composante que vous pouvez remplacer dans un système complexe pour vérifier que ses contreparties sont dans de bonnes conditions de travail. Par exemple, vous pouvez transporter un câble Ethernet fonctionnel et testé dans votre trousse à outils. Si vous suspectez des problèmes avec un câble sur le terrain, vous pouvez facilement échanger ce câble par « connu comme étant bon » et voir si les choses s'améliorent. Ceci est beaucoup plus rapide et est moins susceptible de causer des erreurs que de sertir un nouveau câble et vous indique immédiatement si le changement règle le problème. De même, vous pouvez également transporter une batterie de secours, un câble d'antenne ou un CD-ROM avec une dernière configuration effective pour le système. En réparant des problèmes compliqués, sauvegarder votre travail à un point donné vous permet de retourner à ce « connu comme étant bon » même si le problème n'est pas encore complètement résolu.
- **Changez une variable à la fois.** Lorsque vous sentez la pression de remettre un système en fonctionnement, il est tentant de vouloir changer beaucoup de variables immédiatement. Si vous le faites et que vos changements semblent régler le problème, alors vous ne comprendrez pas exactement ce qui a mené au problème en premier lieu. Pire encore, vos

changements peuvent régler le problème original, mais mener à des conséquences plus fortuites qui brisent d'autres parties du système. En changeant vos variables une par une, vous pouvez comprendre avec précision ce qui a mal tourné en premier lieu et voir les effets directs des changements que vous faites.

- **Ne l'abîmez pas.** Si vous ne comprenez pas entièrement comment fonctionne le système, n'ayez pas peur d'appeler un expert. Si vous n'êtes pas certain qu'un changement particulier n'endommagera pas une autre partie du système, alors trouvez quelqu'un avec plus d'expérience ou trouvez un moyen d'examiner votre changement sans causer plus de dommages. Mettre une pièce de monnaie au lieu d'un fusible peut résoudre le problème immédiat mais peut également causer un incendie dans le bâtiment.

Il est peu probable que les gens qui conçoivent votre réseau seront à l'appel vingt-quatre heures par jour pour régler les problèmes lorsqu'ils surgissent. Votre équipe de dépannage devra avoir de bonnes qualités de dépannage mais peut ne pas être assez compétente pour configurer un routeur à partir de zéro ou pour sertir une partie d'un LMR-400. Il est souvent beaucoup plus efficace d'avoir un certain nombre de composantes de secours et de former votre équipe pour pouvoir échanger la partie cassée en entier. Ceci peut signifier avoir un point d'accès ou un routeur préconfiguré dans un coffret verrouillé, simplement marqué et stocké avec les câbles et les alimentations d'énergie de secours. Votre équipe peut échanger la composante brisée et l'envoyer à un expert pour sa réparation ou commander une autre composante de secours. Si les pièces de secours sont maintenues sous clef et sont remplacées une fois utilisées, vous épargnerez du temps à tout le monde.

# Problèmes courants de réseau

Souvent, les problèmes de connectivité naissent de composantes brisées, de climat défavorable ou de simples problèmes de configurations. Une fois que votre réseau est connecté à Internet ou ouvert au grand public, des menaces considérables proviendront des utilisateurs du réseau eux-mêmes. Que les menaces soient bénignes ou pure malveillance, elles auront toutes un impact sur votre réseau si celui-ci n'est pas correctement configuré. Cette section se penche sur quelques problèmes communs identifiés dès que votre réseau est utilisé par des êtres humains réels.

## Sites Web hébergés localement

Si une université héberge son site Web localement, les visiteurs du site Web de l'extérieur du campus et du reste du monde concurrenceront le personnel de l'université pour la largeur de bande d'Internet. Ceci inclut l'accès automatisé des moteurs de recherche qui vont ***balayer*** périodiquement votre site au complet. Une solution à ce problème est d'employer un DNS divisé (*split*

*DNS*) et un site miroir. L'université reflète une copie de ses sites Web à un serveur, par exemple à une compagnie d'hébergement européenne et utilise un DNS divisé pour diriger tous les usagers de l'extérieur du réseau de l'université vers le site miroir alors que les usagers sur le réseau de l'université accèdent au même site localement. Des détails à propos de l'installation de cette solution sont présentés au chapitre trois.

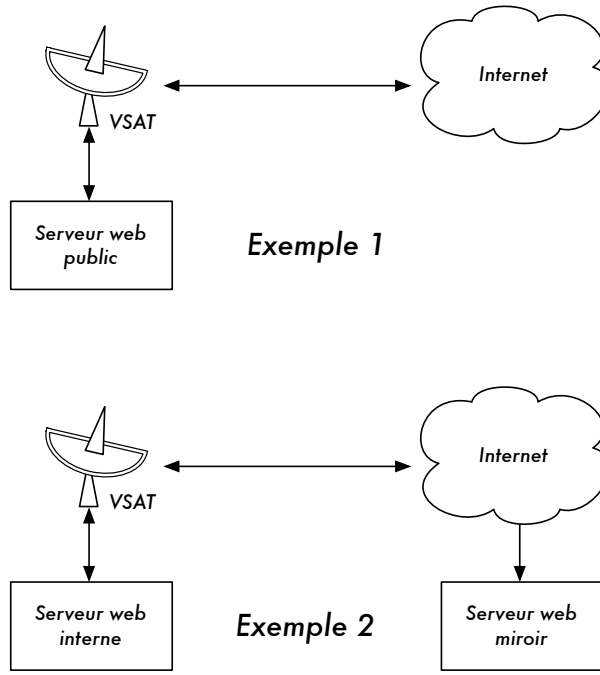


*Figure 8.1: Dans l'exemple 1, tout le trafic de site Web venant d'Internet doit traverser le VSAT. Dans l'exemple 2, le site Web public est hébergé dans un service européen rapide, alors qu'une copie est gardée sur un serveur internet pour un accès local très rapide. Ceci améliore la connexion VSAT et réduit le temps de chargement pour les usagers du site Web.*

## Serveur mandataire ouvert

Un serveur mandataire (*proxy*) devrait être configuré pour accepter seulement des connexions provenant du réseau de l'université, pas du reste de l'Internet. Ceci s'explique par le fait que les gens partout ailleurs voudront se connecter et employer des serveurs mandataires ouverts pour une variété de raisons, tel qu'éviter de payer la largeur de bande internationale. La manière de configurer ceci dépend du serveur mandataire que vous employez. Par exemple, vous pouvez indiquer la plage d'adresses IP du réseau du campus dans votre fichier **`squid.conf`** comme seul réseau qui peut employer Squid. Alternativement, si votre serveur mandataire se trouve derrière un

pare-feu, vous pouvez configurer celui-ci pour ne permettre la connexion au port du serveur mandataire qu'aux hôtes internes.

## Hôtes en mode relais ouvert

Un serveur de courriel mal configuré sera trouvé par des personnes sans scrupules sur Internet et employé comme hôte en mode relais ouvert pour envoyer des courriels non sollicités. Ceci est réalisé afin de cacher la vraie source de ce type de courrier électronique en évitant ainsi de se faire attraper. Pour tester un hôte en mode relais ouvert, l'essai suivant devrait être effectué sur votre serveur de courriel (ou sur le serveur SMTP qui agit en tant qu'hôte en mode relais ouvert sur le périmètre du réseau du campus). Utilisez ***telnet*** pour ouvrir une connexion au port 25 du serveur en question (avec quelques versions Windows de telnet, il peut être nécessaire de tapper « set local_echo » avant que le texte ne soit visible):

```
telnet mail.uzz.ac.zz 25
```

Puis, si une conversation de ligne de commande interactive peut avoir lieu (comme dans l'exemple suivant), le serveur est un hôte en mode relais ouvert:

```
MAIL FROM: spammer@waste.com
250 OK - mail from <spammer@waste.com>
RCPT TO: innocent@university.ac.zz
250 OK - rcpt to spammer@waste.com
```

Au lieu de cela, la réponse après le premier MAIL FROM devrait être quelque chose comme ce qui suit:

```
550 Relaying is prohibited.
```

Un test en ligne ainsi que de l'information sur le problème sont disponibles sur les sites tels que *http://www.ordb.org/*. Puisque ceux qui envoient des courriels non sollicités ont automatisé des méthodes pour trouver les serveurs en mode relais ouvert, un établissement qui ne protège pas ses systèmes de courriel sera très probablement trouvé et abusé. La configuration du serveur de courriel pour ne pas être serveur en mode relais ouvert consiste à indiquer les réseaux et hôtes qui ont la permission de transmettre du courriel à travers lui dans le MTA (par exemple, Sendmail, Postfix, Exim ou Exchange). Ceci sera probablement la plage d'adresses IP du réseau du campus.

## Réseautage pair à pair

L'abus de largeur de bande par des programmes de partage de fichier pair-à-pair (*peer-to-peer - P2P*) tels que Kazaa, Morpheus, WinMX et BearShare peut être empêché avec les manières suivantes:

- **Rendez impossible l'installation de nouveaux programmes sur les ordinateurs du campus.** Il est possible d'empêcher l'installation de programmes tels que Kazaa en ne donnant pas aux usagers réguliers l'accès administratif aux postes de travail PC. Beaucoup d'établissements normalisent également la structure du bureau, en installant le système d'exploitation requis sur un ordinateur, puis en y installant alors toutes les applications nécessaires d'une manière optimale. L'ordinateur est également configuré d'une manière qui empêche les usagers d'installer toute nouvelle application. Une image du disque de cet ordinateur est alors copiée à tous les autres ordinateurs en utilisant un logiciel tel que Partition Image (voir le site: *http://www.partimage.org/*) ou Drive Image Pro (voir le site: *http://www.powerquest.com/*).

  De temps en temps, les usagers peuvent réussir à installer un nouveau logiciel ou à endommager le logiciel sur l'ordinateur (par exemple, en le faisant figer souvent). Quand ceci se produit, un administrateur peut simplement remettre l'image du disque, remettant le système d'exploitation et tous les logiciels sur l'ordinateur exactement comme indiqué.

- **Le blocage de ces protocoles n'est pas une solution.** Kazaa et d'autres protocoles sont assez intelligents pour éviter les ports bloqués. Par défaut, Kazaa utilise le port 1214 pour la connexion initiale. Cependant, s'il n'est pas disponible, il essayera d'employer les ports 1000 à 4000. Si ceux-ci sont bloqués, il utilise le port 80, se faisant passer pour du trafic web. C'est pour cette raison que les ISPs ne le bloquent pas mais l' « étrangle », en utilisant un gestionnaire de largeur de bande (voir le chapitre trois).

- **Si la limitation du débit n'est pas une option, changez la disposition du réseau.** Si le serveur mandataire et celui de courriel sont configurés avec deux cartes de réseau (comme décrit dans le chapitre trois) et que ces serveurs ne sont pas configurés pour faire suivre (*ip forward*) les paquets, tout le trafic poste à poste (p2p) serait bloqué. Ceci bloquerait également tous les autres types de trafic, tels que Microsoft NetMeeting, SSH, VPN et tous les autres services qui n'ont pas été spécifiquement autorisés par le serveur mandataire. Dans les réseaux à faible largeur de bande, on peut décider que la simplicité de cette conception sera supérieure aux inconvénients. Une telle décision peut être nécessaire, mais ne devrait pas être prise à la légère. Les administrateurs réseau ne peuvent simplement pas prévoir de quelles façons innovatrices les usagers feront usage du réseau. Si vous bloquez tout accès de façon préventive, vous empêcherez les usagers de se servir de tous les services que votre ser-

veur mandataire ne soutient pas (même les services à faible largeur de bande). Même si ceci peut être souhaitable dans les circonstances à largeur de bande extrêmement faible, on ne devrait jamais le considérer comme une bonne politique d'accès en général.

## Programmes qui s'installent par eux-mêmes (à partir d'Internet)

Il y a des programmes qui s'installent automatiquement et continuent par après à utiliser la largeur de bande, par exemple: le dénommé Bonzi-Buddy, le Réseau Microsoft et quelques genres de vers. Certains programmes sont des logiciels espions qui envoient des informations sur les habitudes de navigation d'un usager à une compagnie quelque part sur Internet. Ces programmes sont évitables dans une certaine mesure par l'éducation des usagers et la restriction des ordinateurs afin d'empêcher l'accès administratif aux usagers réguliers. Dans d'autres cas, il y a des solutions logicielles pour trouver et enlever ces programmes problématiques, tels que Spychecker (*http://www.spychecker.com/*), Ad-Aware (*http://www.lavasoft.de/*) ou xp-antispy (*http://www.xp-antispy.de/*).

## Mises à jour Windows

Les derniers systèmes d'exploitation Microsoft Windows supposent qu'un ordinateur avec une connexion LAN a un bon lien à Internet et télécharge automatiquement des correctifs de sécurité, de bogues et des améliorations de fonctionnalités à partir du site Web de Microsoft. Ceci peut consommer massivement la largeur de bande sur un lien Internet dispendieux. Les deux approches possibles pour résoudre ce problème sont les suivantes:

- **Désactivez les mises à jour de Windows sur tous les ordinateurs.** Les mises à jour de sécurité sont très importantes pour les serveurs, mais il est discutable que les postes de travail dans un réseau privé protégé tel qu'un réseau de campus en aient réellement besoin.
- **Installez un serveur de mise à jour de logiciel.** C'est un programme gratuit de Microsoft qui vous permet de télécharger toutes les mises à jour de Microsoft durant la nuit sur un serveur local et de distribuer les mises à jour aux postes de travail clients à partir de ce serveur. De cette façon, les mises à jour de Windows n'emploient aucune largeur de bande sur le lien Internet pendant le jour. Malheureusement, tous les ordinateurs client doivent être configurés pour utiliser le serveur de mise à jour de logiciel pour que ceci puisse avoir un effet. Si vous avez un serveur flexible de DNS, vous pouvez également le configurer pour répondre aux demandes pour *windowsupdate.microsoft.com* et diriger l' « *updater* » vers votre serveur de mise à jour. C'est un bon choix seulement pour les grands ré-

seaux et peut sauver des quantités incalculables de largeur de bande Internet.

Le blocage du site de mises à jour de Windows sur le serveur mandataire n'est pas une bonne solution car le service de mise à jour de Windows (mises à jour automatiques) continue à réessayer plus agressivement et si tous les postes de travail font cela, le serveur mandataire aura à supporter une lourde charge. L'extrait ci-dessous provient du fichier de journal du serveur mandataire (fichier journal d'accès de Squid) où on a bloqué les fichiers Microsoft cabinet (.cab).

Une grande partie du fichier de journal Squid ressemble à ceci:

```
2003.4.2 13:24:17 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
  *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:18 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:18 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab HEAD 0
2003.4.2 13:24:19 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:19 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:20 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab HEAD 0
```

Même si ceci peut être tolérable si nous avons peu d'ordinateurs clients, le problème prend de l'ampleur de manière significative si des hôtes sont ajoutés au réseau. Plutôt que de forcer le serveur mandataire à répondre à des requêtes qui échoueront toujours, il est plus raisonnable de réorienter les clients de mise à jour de logiciel à un serveur local de mise à jour.

## Programmes qui supposent un lien de grande largeur de bande

En plus des mises à jour de Windows, beaucoup d'autres programmes et services supposent que la largeur de bande n'est pas un problème et la consomment donc pour des raisons que l'usager ne pourrait pas prévoir. Par exemple, les paquets d'anti-virus (comme le Norton AntiVirus) font des mises à jour périodiques automatiques et directement de l'Internet. Il est préférable que ces mises à jour soient distribuées à partir d'un serveur local.

D'autres programmes, tels que le RealNetworks video player, téléchargent automatiquement des mises à jour et des annonces puis envoie sur un serveur les habitudes d'utilisation. D'autres mini applications apparemment inof-

fensives (comme les gadgets de Konfabulator et Dashboard) sondent continuellement des hôtes d'Internet pour de l'information de mise à jour. Celles-ci peuvent êtres des requêtes qui demandent une faible largeur de bande (comme des mises à jour sur le climat ou des nouvelles) ou des requêtes qui exigent une très grande largeur de bande (telles que les webcams). Il peut être nécessaire de limiter ou bloquer totalement ce genre d'applications.

Les dernières versions de Windows et Mac OS X ont également un service de synchronisation de temps. Ceci maintient l'horloge de l'ordinateur précise en la connectant à des serveurs de temps sur Internet. Il est préférable d'installer un serveur de temps local et de distribuer le temps précis à partir de celui-ci, plutôt que d'occuper le lien Internet avec ces requêtes.

## Trafic de Windows sur le lien à Internet

Les ordinateurs Windows communiquent les uns avec les autres par l'intermédiaire de ***NetBIOS*** et de ***Server Message Block*** (***SMB***). Ces protocoles fonctionnent sur TCP/IP ou d'autres protocoles de transport. C'est un protocole qui fonctionne en tenant des élections pour déterminer quel ordinateur sera le ***navigateur principal***. Le navigateur principal est un ordinateur qui garde une liste de tous les ordinateurs, ressources partagées et imprimantes que vous pouvez voir dans le ***Voisinage réseau*** ou ***Favoris réseau***. L'information sur les ressources partagées disponibles est également transmise à intervalles réguliers.

Le protocole SMB est conçu pour des réseaux LAN et pose des problèmes quand l'ordinateur Windows est connecté à l'Internet. À moins que le trafic SMB soit filtré, il tendra également à se disperser sur le lien Internet, gaspillant ainsi la largeur de bande de l'organisation. Les mesures suivantes pourraient être prises afin d'empêcher ceci:

- **Bloquez le trafic sortant de SMB/NetBIOS sur le routeur périphérique ou pare-feu.** Ce trafic la largeur de bande Internet et pire encore, pourra poser un risque potentiel de sécurité. Beaucoup de vers sur Internet et d'outils de pénétration cherchent activement des SMB ouverts afin d'exploiter ces connexions pour gagner un plus grand accès à votre réseau.
- **Installez ZoneAlarm sur tous les postes de travail (pas le serveur).** Une version gratuite peut être trouvée à *http://www.zonelabs.com/*. Ce programme permet à l'usager de déterminer quelles applications peuvent établir des connexions à Internet et quelles ne peuvent pas. Par exemple, Internet Explorer doit se connecter à Internet mais pas Windows Explorer. ZoneAlarm peut empêcher que Windows Explorer se connecte.
- **Réduisez les ressources partagées du réseau.** Idéalement, seul le serveur de fichiers devrait avoir des ressources partagées. Vous pouvez utiliser un outil tel que le SoftPerfect Network Scanner

(*http://www.softperfect.com/*) pour identifier facilement toutes les ressources partagées de votre réseau.

## Vers et virus

Les vers et les virus peuvent produire d'énormes quantités de trafic. Le ver W32/Opaserv, par exemple, même s'il est vieux, est encore répandu. Il est distribué à partir des ressources partagées de Windows et est détecté par d'autres sur Internet parce qu'il essaye de s'étendre davantage. Il est donc essentiel que la protection anti-virus soit installée sur tous les ordinateurs. En outre, il est essentiel de former l'usager au sujet d'exécuter des pièces jointes et de répondre à du courriel non sollicité. En fait, ce devrait être une politique qu'aucun poste de travail ou serveur fournissent des services inutilisés. Un ordinateur ne devrait pas avoir de ressources partagées à moins que ce soit un serveur de fichiers; et un serveur ne devrait pas exécuter des services inutiles non plus. Par exemple, les serveurs de Windows et d'Unix exécutent généralement un service de serveur web par défaut. Ceci devrait être désactivé si ce serveur a une fonction différente; moins un ordinateur exécute de services, moins il y a de chances qu'il soit exploité.

## Boucle d'expédition de courriel

De temps en temps, un simple usager commettant une erreur peut poser un problème. Par exemple, un usager dont le compte d'université est configuré pour expédier tout le courrier à son compte de Yahoo. L'usager part en vacances. Tous les courriels que cet étudiant reçoit sont encore expédiés à son compte Yahoo qui a une capacité de jusqu'à 2 MB. Lorsque le compte Yahoo est complet, il commence à rebondir les courriels au compte de l'université, qui les expédient immédiatement à nouveau au compte Yahoo. On forme ainsi une boucle d'expédition de courriel qui pourrait envoyer des centaines de milliers de courriels dans les deux sens, produisant ainsi un trafic massif capable de détruire des serveurs de courriel.

Il existe des dispositifs dans les programmes de serveur de courriel qui peuvent identifier de telles boucles et qui devraient être activés par défaut. Les administrateurs doivent également faire attention de ne pas désactiver ces dispositifs par erreur ou de ne pas installer un expéditeur SMTP qui modifie les en-têtes de courriel de telle manière que le serveur de courriel ne puisse pas identifier la boucle de courriel.

## Grands téléchargements

Un usager peut commencer plusieurs téléchargements simultanés ou télécharger de grands fichiers comme des images ISO de 650MB. De cette

façon, un simple usager peut épuiser la majeure partie de la largeur de bande. Les solutions à ce genre de problème se situent dans la formation, le téléchargement sans connexion et la surveillance (y compris la surveillance en temps réel, tel que décrit au chapitre six). Le téléchargement sans connexion peut être réalisé par au moins deux manières:

- À l'université de Moratuwa, un système a été mis en application en utilisant la redirection URL. Les usagers entrant à **ftp://** URLs accèdent à une liste annuaire dans laquelle chaque fichier a deux liens: un pour le téléchargement normal et l'autre pour télécharger sans connexion. Si le lien sans connexion est choisi, le fichier indiqué est mis en attente pour le téléchargement postérieur et l'usager reçoit un courriel lorsque le téléchargement est complet. Le système garde une cache des fichiers téléchargés récemment et recherche ces fichiers immédiatement lorsqu'ils sont redemandés. La file d'attente de téléchargement est classée par la taille du fichier. Par conséquent, les petits fichiers sont téléchargés d'abord. Comme une certaine largeur de bande est assignée à ce système même pendant des heures de pointe, les usagers qui demandent de petits fichiers peuvent les recevoir en quelques minutes, parfois plus rapidement qu'avec un téléchargement en ligne.
- Une autre approche serait de créer une interface Web où les usagers entrent l'URL du fichier qu'ils désirent télécharger. Ceci est alors téléchargé durant la nuit en utilisant un ***cron job*** ou une tâche programmée. Ce système fonctionnerait uniquement pour les usagers qui ne sont pas impatients et qui savent quelles tailles de fichier seraient problématiques pour le téléchargement pendant les heures de travail.

## Envoie de fichiers de grande taille

Lorsque les usagers doivent transférer des fichiers de grande taille à des collaborateurs ailleurs sur Internet, ils devraient être entraînés pour planifier le téléchargement. Dans Windows, un téléchargement à un serveur FTP à distance peut être réalisé en utilisant un script de commandes FTP (sauvegardé comme **`c:\ftpscript.txt`**) ressemblant à ceci:

```
open ftp.ed.ac.uk
gventer
mysecretword
delete data.zip
binary
put data.zip
quit
```

Pour l'exécuter, écrivez ceci à partir de l'invite de commande:

```
ftp -s:c:\ftpscript.txt
```

Sur des ordinateurs Windows NT, 2000 et XP, la commande peut être sauvegardée dans un fichier tel que **`transfer.cmd`** et programmé pour fonctionner durant la nuit en utilisant les Tâches Planifiées (Démarrer ➜ Paramètres ➜ Panneau de configuration ➜ Tâches Planifiées). Dans Unix, il est possible d'obtenir le même résultat en utilisant ***at*** ou ***cron***.

## Usagers s'envoyant des fichiers les uns aux autres

Les usagers doivent souvent s'envoyer des fichiers de grande taille. Si le destinataire est local, envoyer ces fichiers via Internet est un gaspillage de largeur de bande. Un point de partage de fichiers devrait être créé sur le serveur local de Windows/samba/web Novell afin que l'usager puisse y placer le fichier de grande taille et que d'autres puissent y avoir accès.

Alternativement, un front-end web peut être écrit pour un serveur web local pour accepter un fichier de grande taille et pour le placer dans un espace de téléchargement. Après l'avoir téléchargé au serveur web, l'usager reçoit un URL pour le fichier. Il peut alors donner ce URL à ses collaborateurs locaux ou internationaux. Ceux-ci pourront ainsi télécharger le fichier en accédant à cet URL. C'est ce que l'Université de Bristol a fait avec leur système FLUFF. L'université offre un service pour le téléchargement de fichiers de grande taille (FLUFF) disponible à: *http://www.bristol.ac.uk/fluff/*. Ces fichiers peuvent être consultés par n'importe qui ayant reçu son emplacement. L'avantage de cette approche est que les usagers peuvent offrir l'accès à leurs fichiers à des usagers externes, tandis que la méthode de partage de fichiers peut fonctionner seulement pour des usagers du réseau du campus. Un système comme ceci peut facilement être mis en application avec un script CGI utilisant Python et Apache.

# 9
# Études de Cas

Peu importe la planification requise afin d'établir un lien ou un noeud, vous devrez inévitablement plonger dans le travail et installer quelque chose. C'est le moment de vérité qui démontre jusqu'à quel point vos évaluations et prévisions s'avèrent précises.

Il est rare que tout aille précisément comme prévu. Même après avoir installé votre 1er, 10e ou 100e noeud, vous trouverez que les choses ne fonctionnent pas toujours comme vous pouviez l'avoir prévu. Ce chapitre décrit certains de nos plus mémorables projets de réseau. Que vous soyez sur le point de vous embarquer sur votre premier projet sans fil ou que vous soyez un expert dans le domaine, il est rassurant de se rappeler qu'il y a toujours plus à apprendre.

## *Conseil général*

Les économies des pays en voie de développement sont très différentes de celles du monde développé, et donc un processus ou une solution conçue pour un pays plus développé peut ne pas convenir en Afrique occidentale ou en Asie méridionale. Spécifiquement, le coût de matériaux localement produits et le coût du travail seront négligeables, tandis que les marchandises importées peuvent être beaucoup plus chères une fois comparées à leur coût dans le monde développé. Par exemple, on peut fabriquer et installer une tour pour une dixième du coût d'une tour aux États-Unis, mais le prix d'une antenne pourrait être le double. Il sera plus facile de répliquer les solutions qui profitent des avantages concurrentiels locaux, à savoir main d'oeuvre à prix réduit et matériaux qui peuvent être trouvés localement.

Trouver l'équipement adéquat est une des tâches les plus difficile dans les marchés des pays en voie de développement. Comme le transport, la communication et les systèmes économiques ne sont pas développés, il peut

être difficile ou même impossible de trouver les matériaux ou les équipements appropriés. Ceci est, par exemple, le cas des fusibles ; en remplacement, on peut trouver un câble à combustion à un certain ampérage qui puisse les substituer. Trouver des produits de remplacement locaux pour des matériaux encourage également l'esprit d'entreprise locale, de propriété et peut faire économiser de l'argent.

## Pièces d'équipement

Il est facile de trouver des plastiques bon marché dans les pays en voie de développement, mais ceux-ci sont faits de matériaux médiocres et sont minces. La plupart du temps, il ne sont pas convenables pour contenir l'équipement. La tuyauterie de PVC est plus résistante et est faite pour être imperméable. En Afrique occidentale, le PVC le plus ordinaire est trouvé dans la tuyauterie, avec une mesure de 90 mm à  220 mm. Les points d'accès tels que le Routerboard 500 et 200 peuvent s'ajuster dans une telle tuyauterie et avec des couvercles vissés aux extrémités, ils deviennent des boîtiers imperméables très robustes. Ils ont également l'avantage supplémentaire d'être aérodynamiques et sans intérêt pour les passants. L'espace qui est laissé tout autour de l'équipement assure une circulation d'air adéquate. De plus, il est souvent conseillé de laisser un trou d'échappement au fond du boîtier de PVC, même si j'ai constaté que laisser des trous ouverts peut souvent devenir un problème. Il y a eu un cas où des fourmis ont décidé de nicher 25 mètres au-dessus de la terre à l'intérieur du tube PVC où était installé le point d'accès. Afin de protéger le trou d'échappement de possibles infestations, il est conseillé de le couvrir en utilisant un treillis métallique fait à partir de matériel localement disponible.

## Mâts d'antenne

La récupération de matériaux usagés est devenue une industrie importante pour les pays les plus pauvres. Des vieilles voitures aux télévisions, n'importe quel matériel qui a une valeur sera démonté, vendu ou réutilisé. Par exemple, vous verrez des véhicules démontés pièces par pièces, jour après jour. Le métal ainsi obtenu est classé puis rangé dans un camion pour le vendre. Les ouvriers locaux qui travaillent avec le métal seront déjà familiers avec la façon de faire des mâts de télévision à partir de métal de rebut. Avec quelques adaptations rapides, ces mêmes mâts peuvent être utilisés pour les réseaux sans fil.

Le mât typique est un poteau de 5 mètres, composé d'un tuyau de 30 mm de diamètre qui est planté dans le ciment. Il est préférable de construire le mât en deux parties, avec un mât démontable qui s'ajuste à une base qui a un diamètre légèrement plus grand. De façon alternative, le mât peut être fait avec des bras solidement cimentés dans un mur. Ce projet est facile mais exige l'utilisation d'une échelle et donc une certaine attention est suggérée.

Il est possible d'augmenter la taille de ce type de mât de plusieurs mètres avec l'utilisation de câbles hauban. Pour renforcer le poteau, plantez trois lignes avec une distance de 120 degrés et une déclinaison d'au moins 33 degrés à partir de l'extrémité de la tour.

## Importance d'impliquer la communauté locale

La participation de la communauté est impérative pour assurer le succès et la durabilité d'un projet. Faire participer la communauté dans un projet peut être le plus grand défi, mais si la communauté n'est pas impliquée la technologie ne servira pas leurs besoins et elle ne sera pas acceptée. D'ailleurs, une communauté pourrait avoir peur et renverser une initiative. Indépendamment de la complexité de l'entreprise, un projet réussi requiert du support et de l'appui de ceux à qui elle servira.

Une stratégie efficace pour gagner de l'appui est de trouver une personne influente et respectée avec de bonnes intentions. Trouvez la personne ou les personnes les plus susceptibles d'être intéressées par le projet. Vous devrez souvent faire participer ces personnes comme conseillers ou membres du comité de coordination. Ces personnes auront déjà la confiance de la communauté, sauront qui il faut approcher et pourront parler la langue de la communauté. Prenez votre temps et soyez sélectif au moment de trouver les personnes adéquates pour votre projet. Aucune autre décision n'affectera votre projet davantage que le fait d'avoir dans votre équipe des personnes de la communauté efficaces et de confiance.

Faites attention en choisissant vos alliés. Une réunion « de la municipalité » est souvent utile pour décerner la politique, les alliances et les inimitiés locales en jeu. Ensuite, il est plus facile de décider avec qui s'allier et qui éviter. Essayez de ne pas générer de l'enthousiasme sans garantie. Il est important d'être honnête, franc et de ne pas faire de promesses que vous ne pouvez pas garder.

Dans les communautés en grande partie illettrées, concentrez vous sur les services numériques analogues tels qu'Internet pour des stations de radio, l'impression d'articles et de photos en ligne et d'autres applications non-textuelles. N'essayez pas de présenter une technologie à une communauté sans comprendre les applications qui serviront réellement à cette communauté. Souvent la communauté aura peu d'idée de la façon dont les nouvelles technologies aideront leurs problèmes. Fournir simplement de nouveaux dispositifs est inutile sans comprendre la façon dont la communauté en bénéficiera.

En recueillant l'information, vérifiez les données qu'on vous donne. Si vous voulez connaître le statut financier d'une compagnie ou d'une organisation, demandez une facture d'électricité ou de téléphone. Ont-ils payé leurs fac-

tures? Parfois, les bénéficiaires potentiels compromettront leurs propres valeurs dans l'espoir de gagner des fonds ou de l'équipements. Le plus souvent, les associés locaux qui vous font confiance seront très francs, honnêtes et utiles.

Un autre piège habituel est ce que j'appelle le syndrome « de parents divorcés » où les ONGs, les donneurs et les associés ne connaissent pas les engagements des uns et des autres avec le bénéficiaire. Des bénéficiaires astucieux peuvent gagner de belles récompenses en laissant les ONGs et les donneurs leur offrir de l'équipement, de la formation et des fonds. Il est important de savoir quelle autre organisation est impliquée afin de savoir comment leurs activités pourraient affecter les vôtres. Par exemple, j'ai, par le passé, conçu un projet pour une école rurale au Mali. Mon équipe a installé un système de source ouverte avec des ordinateurs usagés et a passé plusieurs jours à former des personnes pour apprendre à l'employer. Le projet a été considéré comme un succès, mais peu de temps après l'installation, un autre donneur est arrivé avec des ordinateurs Pentium 4 neufs avec Windows XP. Les étudiants ont rapidement abandonné les vieux ordinateurs et ont fait la file pour utiliser les nouveaux ordinateurs. Il aurait été préférable de négocier avec l'école à l'avance, pour connaître leur engagement au projet. S'ils avaient été francs, les ordinateurs qui reposent maintenant et sont inutilisés pourraient avoir été installés dans une autre école où ils pourraient être employés.

Dans plusieurs communautés rurales des économies sous-développées, la loi et les politiques sont faibles et les contrats peuvent n'avoir aucun sens. Il est souvent nécessaire de trouver d'autres assurances. C'est dans ces cas où les services prépayés sont idéaux, car ils n'exigent aucun contrat légal. L'engagement est assuré par l'investissement des fonds avant que le service ne soit offert.

Le fait d'acheter exige également que ceux impliqués investissent eux-mêmes dans le projet. Un projet devrait demander la participation réciproque de la communauté.

Par-dessus tout, l'option «non-intéressé» devrait toujours être évaluée. Si on ne peut pas avoir d'allié et une communauté d'achat, le projet devrait considérer de choisir une communauté ou un bénéficiaire différent. Il doit y avoir une négociation ; l'équipement, l'argent et la formation ne peuvent pas être des cadeaux. La communauté doit être impliquée et doit également contribuer.

*—Ian Howard*

# Étude de cas: traverser la brèche à l'aide d'un simple pont à Tombouctou

Le but ultime des réseaux est de connecter des personnes ensemble, ce qui implique toujours une composante politique. Le coût d'Internet dans les économies moins développées est haut et la solvabilité est faible, ce qui s'ajoute aux défis politiques. Essayer de superposer un réseau à un réseau humain disfonctionnel est presque impossible à long terme. Ainsi, mettre en place un projet sur une base sociale instable menace son existence. C'est à ce moment que le bas prix et la mobilité d'un réseau sans fil peuvent être avantageux.

L'équipe de l'auteur a été invitée par des bailleurs de fonds à déterminer comment connecter à Internet une station radio rurale avec un très petit télécentre (deux ordinateurs) à Tombouctou, la capitale du désert du Mali. Tombouctou est largement connue comme étant un avant-poste dans la région la plus éloignée du monde. À cet endroit, l'équipe a décidé de mettre en application un modèle nommé le ***modèle sans fil parasite***. Ce modèle prend une source sans fil d'un réseau existant et étend ce réseau à un site client en utilisant un simple pont réseau. Ce modèle a été choisi parce qu'il n'exige aucun investissement significatif de la part de l'organisation qui soutient l'initiative. Tandis qu'il a ajouté une source de revenu pour le télécentre, il n'a ajouté aucun coût opérationnel significatif. Cette solution a permis que le site client obtienne une connexion Internet bon marché; cependant pas aussi rapide et fiable qu'une solution dédiée. En raison des comportements opposés d'utilisation d'un bureau et d'un télécentre, il n'y a eu aucun ralentissement du réseau qui puisse être perceptible pour l'une ou l'autre des parties. Dans une situation idéale, il aurait été préférable d'encourager le développement du télécentre en un petit fournisseur Internet. Cependant, on a considéré que ni le télécentre ni le marché étaient prêts pour cela. Comme c'est souvent le cas, il y avait de sérieuses préoccupations quant à la durabilité du télécentre une fois que les bailleurs de fonds sont partis. Ainsi, cette solution a réduit au minimum l'investissement initial tout en accomplissant deux buts: d'abord, elle a offert une connexion Internet au bénéficiaire ciblé, une station de radio, à un coût accessible. Ensuite, elle a ajouté une petite source additionnelle de revenu pour le télécentre tout en n'augmentant pas ses coûts opérationnels ni en ajoutant de la complexité au système.

## Les gens

Même en étant un endroit éloigné, Tombouctou a un nom de renommée mondiale. Devenue un symbole de région éloignée, beaucoup de projets ont voulu « planter un drapeau » dans les sables de cette ville du désert. Il y a donc un certain nombre d'activités de technologies de l'information et de la

communication (TIC) dans le secteur. La dernière fois que nous avons compté, il y avait 8 connexions satellites à Tombouctou dont la plupart servait des intérêts particuliers, excepté deux fournisseurs nationaux, SOTELMA et Ikatel. Ils utilisent actuellement le VSAT pour connecter leurs réseaux téléphoniques au reste du pays. Ce télécentre a employé une connexion X.25 à un de ces telcos, qui transmet ensuite cette connexion à Bamako. En comparaison à d'autres villes éloignées du pays, Tombouctou a un certain nombre de personnel TIC qualifié, trois télécentres existants et le télécentre nouvellement installé à la station de radio. À un certain degré, la ville est saturée d'Internet, excluant la viabilité de tous intérêts privés ou commerciaux.

## Choix de conception

Dans cette installation, le site client est à seulement 1 kilomètre à vol d'oiseau. Deux points d'accès Linksys modifiés avec OpenWRT et configurés pour fonctionner en mode pont ont été installés. L'un d'eux a été installé sur le mur du télécentre et l'autre à 5 mètres sur le mât de la station de radio. Les seuls paramètres de configuration exigés sur les deux dispositifs étaient le ssid et le canal. On a utilisé de simples antennes à panneau de 14 dBi (*http://hyperlinktech.com/*). Du côté Internet, le point d'accès et l'antenne ont été attachés à l'aide de prises de ciment et de vis sur le côté du bâtiment, face au site client. Sur celui-ci, un mât d'antenne existant a été employé. Le point d'accès et l'antenne ont été montés en utilisant des anneaux de tuyau.

Pour débrancher le client, le télécentre débranche simplement le pont de leur côté. Éventuellement, il sera possible d'installer un site additionnel qui aura également son propre pont au télécentre de sorte que le personnel puisse le débrancher advenant que le client ne paie pas. Même si cela semble rustique, cette solution est efficace et réduit le risque que le personnel commette une erreur en réalisant des changements dans la configuration du système. Avoir un pont consacré à une seule connexion a également simplifié l'installation au site central, car l'équipe d'installation pouvait choisir le meilleur endroit pour connecter les sites clients. Bien que ce ne soit pas la meilleure solution de placer des ponts sur un réseau (au lieu de router le trafic du réseau), lorsque la connaissance de la technologie est faible et que l'on veut installer un système très simple, ceci peut être une solution raisonnable pour de petits réseaux. Les ponts font que les systèmes installés au site à distance (la station radio) apparaissent simplement connectés au réseau local.

## Modèle financier

Dans ce cas-ci, le modèle financier est simple. Le télécentre charge des honoraires mensuels, environ 30$ par ordinateur connecté à la station radio. Ceci était plusieurs fois moins cher que l'alternative. Le télécentre est situé dans la cour du bureau du maire, donc le client principal du télécentre est le

personnel du maire. Ceci était important car la station de radio n'a pas voulu concurrencer pour la clientèle du télécentre et le système de la station radio a été principalement prévu pour le personnel de celle-ci. L'installation rapide d'un pont a réduit les coûts et cette sélection des clients a pu soutenir le coût d'Internet sans concurrencer le télécentre, son fournisseur. Le télécentre a également la capacité de débrancher facilement la station radio s'ils ne payent pas. Ce modèle a également permis le partage des ressources du réseau. Par exemple, la station de radio a une nouvelle imprimante laser, alors que le télécentre a une imprimante couleur. Puisque les systèmes clients sont sur le même réseau, les clients peuvent imprimer à l'un ou à l'autre endroit.

## Formation

Pour soutenir ce réseau, très peu d'entraînement a été requis. Le personnel du télécentre a été formé pour installer l'équipement et pour résoudre des problèmes de base, tel que redémarrer les points d'accès et comment remplacer l'unité si celle-ci ne fonctionne plus. Ceci permet à l'équipe de l'auteur d'envoyer simplement une pièce de rechange et d'éviter ainsi un voyage de deux jours à Tombouctou.

## Sommaire

L'installation a été considérée comme une solution provisoire, tandis que l'on cherchait une solution plus complète. Même si on peut la considérer comme un succès, elle n'a pas encore mené à établir davantage d'infrastructures physiques. Elle a tout de même apporté les TICs à une station radio et a renforcé les relations locales entre les clients et les fournisseurs.

À cette heure, l'accès Internet est encore une entreprise coûteuse à Tombouctou. La politique locale et la concurrence des initiatives subventionnées sont mises en cause; cependant, cette solution simple s'est avérée être un cas d'utilisation idéal. L'équipe a investi plusieurs mois d'analyse et de pensée critique pour en arriver là, mais il semble que la solution la plus simple a fourni le plus d'avantages.

*—Ian Howard*

# *Étude de cas: un terrain d'expérimentation à Gao*

Gao se trouve à une journée en voiture de Tombouctou dans le Mali oriental. Cette ville rurale, ressemblant plus à un grand village, repose sur le fleuve Niger juste avant que celui-ci ne plonge vers le sud et traverse le Niger et le

Nigeria. La ville s'incline légèrement vers le fleuve et a peu de bâtiments de plus de deux étages. En 2004, un télécentre a été installé à Gao. Le but du projet était de fournir des informations à la communauté dans l'espoir que celle-ci, en étant plus informée, ait des citoyens avec une meilleure santé et meilleure éducation.

Le centre fournit des informations via CD-ROMs, films et radio, mais la source d'information la plus riche pour le centre est Internet. C'est un télécentre standard avec 8 ordinateurs, une imprimante, scanner, fax, téléphone tout-en-un ainsi qu'un appareil photo numérique. Un petit bâtiment de deux pièces a été construit pour loger le télécentre. Il est situé un peu en dehors du centre-ville, l'endroit n'est idéal pour attirer des clients, mais l'emplacement a été choisi en raison de propriétaire favorable au projet. Le site a reçu des fonds pour toute la construction requise, ainsi que l'équipement et la formation initiale. L'intention était que le télécentre soit autonome financièrement après un an.

Plusieurs mois après son ouverture, le télécentre attirait peu de clients. Il utilisait un modem téléphonique pour se connecter à un fournisseur Internet de la capitale. Comme cette connexion était trop lente et peu fiable, le bailleur de fonds a financé l'installation d'un système VSAT. Il y a maintenant un certain nombre de systèmes VSAT disponibles dans la région; la plupart de ces services sont tout récemment devenus disponibles. Auparavant, les seuls systèmes disponibles étaient les systèmes de bande C (qui couvrent une zone plus grande que la bande Ku). Récemment, la fibre a été étendue dans presque chaque tunnel et canal souterrain de l'ensemble de l'Europe et elle a supplanté ainsi les services plus chers par satellite. En conséquence, les fournisseurs réorientent maintenant leurs systèmes VSAT vers de nouveaux marchés, y compris l'Afrique centrale, occidentale et l'Asie du sud. Ceci a mené un certain nombre de projets à utiliser les systèmes satellites pour se connecter à Internet.

Suite à l'installation du VSAT, la connexion offrait 128 Kbps de téléchargement en aval et 64 Kbps en amont, et coûtait environ 400$ par mois. Comme le site ne réussissait pas à gagner assez de revenu afin de pouvoir payer ce coût mensuel élevé, le télécentre a demandé de l'aide. Une entreprise privée, qui avait été formée par l'auteur, a été engagée pour installer un système sans fil. Ce système partagerait la connexion entre trois clients: un deuxième bénéficiaire, une station radio, et le télécentre, chacun payant 140$. Cet arrangement a permis de couvrir collectivement les coûts du VSAT et le revenu supplémentaire du télécentre et de la station de radio couvrirait le service de support et l'administration du système.

## Les gens

Bien qu'étant partants et enthousiastes, l'équipe de l'auteur n'a pas réalisé l'installation. Au lieu de cela, nous avons encouragé le télécentre à engager une entreprise locale pour le faire. Nous avons rassuré le client en lui garantissant que nous nous occuperions de la formation et du support à l'entreprise locale dans la réalisation de cette installation. La prémisse de cette décision était de décourager une dépendance à court terme d'une ONG. et d'établir plutôt une confiance et des rapports entre les fournisseurs de service locaux et leurs clients. Cette conception s'est avérée fructueuse. Cette approche a pris beaucoup plus de temps pour l'équipe de l'auteur, peut-être deux fois plus, mais cet investissement a déjà commencé à générer des profits. De nouveaux réseaux sont en cours d'installation et l'auteur et son équipe sont maintenant de retour à la maison en Europe et en Amérique du Nord.

## Choix de conception

On a initialement pensé qu'une connexion fédératrice se ferait à la station radio qui avait déjà une tour de 25 mètres. Cette tour serait employée pour retransmettre à d'autres clients, évitant l'installation de tours aux sites client, car cette tour se dressait au-dessus de tous les obstacles de la ville. Pour ce faire, trois approches ont été discutées: installer un point d'accès en mode répéteur, utiliser le protocole WDS ou employer un protocole de routage maillé. Un répéteur n'était pas souhaitable car il introduirait de la latence (due au problème des répéteurs one-armed) à une connexion déjà lente. Les connexions VSAT doivent envoyer des paquets à partir de et vers le satellite, ce qui représente souvent un retard allant jusqu'à 3000 ms pour un voyage aller-retour. Pour éviter ce problème, on a décidé d'employer une radio pour se connecter aux clients et une deuxième radio pour la connexion dédiée vers Internet. À des fins de simplification, on a décidé de faire ce lien avec un simple pont de sorte que le point d'accès à la station de radio paraisse être sur le même LAN physique que le télécentre.

Dans un environnement de test, cette approche a fonctionné, mais dans la réalité, sa performance a été médiocre. Après plusieurs changements différents, y compris remplacer les points d'accès, le technicien a décidé qu'il doit y avoir un problème de logiciel ou d'équipement affectant cette conception. Le technicien a alors décidé de placer le point d'accès au télécentre directement en employant un petit mât de 3 mètres et ne pas employer un site de retransmission à la station de radio. Dans cette conception, les sites clients exigent également de petits mâts. Bien que tous les sites pouvaient se connecter, ces connexions étaient parfois trop faibles et avaient une perte massive de paquets.

Plus tard, pendant la saison de poussière, ces connexions sont devenues plus erratiques et même moins stables, même si les sites clients se trouvaient de 2 à 5 kilomètres de distance et utilisaient le protocole 802.11b. L'hypothèse de l'équipe a alors été que les tours de chaque côté étaient trop courtes, bloquant ainsi la zone de Fresnel. Après avoir débattu de plusieurs théories, l'équipe s'est rendue compte que le problème se trouvait à la station de radio: la fréquence radio était de 90,0 mégahertz, plus ou moins comme la fréquence de la connexion à haute vitesse Ethernet (100BT). Durant la transmission, le signal FM (à 500 watts) consommait complètement le signal sur le câble Ethernet. À cet effet, soit un câble blindé est exigé, soit la fréquence du lien Ethernet doit être changée. Les mâts ont donc été élevés et à la station de radio, la vitesse Ethernet a été changée à 10 Mbps. Ceci a changé la fréquence sur le câble à 20 mégahertz et a ainsi évité l'interférence de la transmission FM. Ces changements ont résolu les deux problèmes, augmentant la force et la fiabilité du réseau. L'avantage d'employer ici un réseau maillé ou le WDS serait que les sites client pourraient se connecter à l'un ou l'autre point d'accès, directement au télécentre ou à la station de radio. Par la suite, le fait d'enlever la dépendance de la station radio comme répéteur pourrait probablement rendre l'installation plus stable à long terme.

## Modèle financier

Le système satellite utilisé à ce site a coûté approximativement 400$ par mois. Pour plusieurs projets de TIC pour le développement, il est difficile de gérer ce coût mensuel élevé. Normalement, ces projets peuvent acheter l'équipement et payer la mise en place d'un réseau sans fil, mais les la plupart ne sont pas en mesure de couvrir le coût du réseau après une courte période (incluant les coûts récurrents d'Internet et les coûts opérationnels). Il est nécessaire de trouver un modèle où les coûts mensuels pour un réseau peuvent être couverts par ceux qui l'utilisent. Pour la plupart des télécentres ou stations de radio, ceci est simplement trop cher. Souvent, l'unique solution est de partager les coûts avec d'autres usagers. Pour rendre Internet plus accessible, ce site a utilisé une connexion sans fil pour partager Internet avec la communauté, permettant à un plus grand nombre d'organismes d'y accéder tout en réduisant le coût par client.

Généralement au Mali, une communauté rurale a seulement quelques organismes ou compagnies qui pourraient avoir les moyens de payer pour une connexion Internet. Là où il y a peu de clients et le coût de connexion Internet est élevé, le modèle développé par cette équipe a inclus les ***clients ancres***: des clients solides et qui présentent un risque faible. Dans cette région, les ONGs (organismes non gouvernementaux) étrangères, les agences des Nations Unies et les grandes entreprises commerciales sont sont les rares qui se qualifient.

Parmi les clients choisis pour ce projet, se trouvaient trois clients ancres. Ceux-ci ont collectivement payé le coût mensuel entier de la connexion satellite. Un deuxième bénéficiaire, une station radio de la communauté a également été connectée. Tout revenu provenant des bénéficiaires a contribué à créer un fond pour couvrir de futurs coûts, mais il n'a pas été tenu en compte en raison de la faible marge économique de ces deux services communautaires. Les clients qui ne paient pas peuvent être débranchés et peuvent reprendre le service lorsqu'ils sont en mesure de le payer.

## Formation requise: qui, quoi et pour combien de temps

L'entreprise locale a enseigné au technicien du télécentre les fondements de support réseau, lequel était assez rudimentaire. Pour tout autre travail qui sortait de la routine, tel qu'ajouter un nouveau client, un consultant externe était employé. Il n'est donc pas impératif d'enseigner au personnel du télécentre comment offrir du support au système dans sa totalité.

## Leçons apprises

En partageant sa connexion, le télécentre est maintenant autonome financièrement et, de plus, trois autres sites ont accès à Internet. Bien que cela prenne plus de temps et peut-être plus d'argent, cela vaut la peine de trouver le talent local approprié et de les encourager à établir des rapports avec les clients. Un fournisseur local pourra fournir le suivi et l'appui requis pour maintenir et développer un réseau. Cette activité construit une expertise locale et crée également de la demande, ce qui permettra aux projets TIC suivants de construire sur cette base.

*—Ian Howard*

# *Étude de cas: Spectropolis, New York*

En septembre 2003 et octobre 2004, NYCwireless a produit Spectropolis. Cet événement a célébré la disponibilité des réseaux sans fil (Wi-Fi) ouverts dans le bas Manhattan et a exploré ses implications pour l'art, la communauté et l'espace public partagé. Spectropolis est le premier festival d'arts sans fil du monde et a été envisagé comme une manière d'introduire la nature technocentriste de Wi-Fi à une forme plus accessible. L'idée était de créer une manière, pour le résidant moyen et les visiteurs de New York, de «voir» et «sentir» les signaux sans fil qui imprègnent la ville (particulièrement le Wi-Fi gratuit que NYCwireless fournit dans plusieurs parcs de la ville) et qui sont autrement invisibles.

L'idée de Spectropolis est venue d'une série de discussions qui se sont déroulées durant l'hiver de l'année 2003 entre Dana Spiegel, qui était à ce

moment membre de NYCwireless et Brooke Singer, une artiste indépendante de New Media et professeur adjointe de SUNY Purchase.

Spectropolis a eu lieu au City Hall Park, un point d'accès sans fil de connexion à Internet gratuit bien connu à la ville de New York. Le festival a présenté des oeuvres d'art de 12 artistes internationaux. Chaque oeuvre d'art intégrait et se servait d'une ou de plusieurs formes de technologie sans fil, incluant entre autres Wi-Fi, Bluetooth, Radio, GPS. Chaque oeuvre devait explorer comment les technologies sans fil affectent nos expériences urbaines quotidiennes. Les oeuvres ont été exhibés à l'extérieur, dans le parc, pendant trois jours. Les artistes montraient et expliquaient leurs travaux aux visiteurs du parc.

En plus des oeuvres d'art, Spectropolis a offert cinq ateliers et trois panels de discussions. Les ateliers ont offert un regard de près aux technologies de communication sans fil et une occasion de participer et de mettre les mains à l'oeuvre. Les ateliers ont visé à instruire le public technique et non technique et à démystifier une gamme de technologies à travers des présentations.

Les panels ont exploré les implications à grande échelle des technologies sans fil pour la société, les politiques publiques, l'activisme et l'art. Chaque panel s'est concentré sur un secteur particulier d'influence de la technologie sans fil qu'ensuite un certain nombre de leaders reconnus commentaient.

Pour l'évènement, un espace ouvert dans le parc public a été choisi, principalement parce que cet emplacement nous offrait l'opportunité d'attirer un grand nombre de participants en situant l'événement dans un espace que plusieurs personnes traversent pendant les jours de travail ainsi que durant la fin de semaine. Un des buts de l'événement était d'attirer les résidents locaux et les personnes qui, autrement, n'assisteraient pas à un événement technologique. Pendant le temps que Spectropolis était au City Hall Park, des milliers de personnes sont venus chaque jour, et plusieurs se sont attardées à regarder une ou plusieurs œuvres d'art.

Du point de vue de la visibilité, tenir Spectropolis dans un espace public extérieur était important. Le trafic de personnes dans le secteur a certainement contribué à attirer un certain nombre de personnes dans le parc qui autrement ne seraient pas venues à l'événement. En outre, la ville de New York a une longue tradition d'exhibition d'art en espaces extérieurs, toutefois cet art est presque entièrement sculptural dans la forme et conçu pour faire partie du paysage mais non pas pour être interactif. Le fait de sortir d'un musée ou d'une galerie de nouveaux medias d'art hautement interactifs dans un espace public extérieur a créé une discordance dans les attentes des personnes.

## Pourquoi Spectropolis est important

Spectropolis est une tentative de donner à la technologie sans fil et en particulier au Wi-Fi une vie au delà du courriel et de la navigation web. Les oeuvres d'art interactives présentées chez Spectropolis veulent attirer l'attention au delà de « l'usage au travail » qui est associé au Wi-Fi par le grand public. En présentant des technologies sans fil par l'intermédiaire du « jeu » et de « l'exploration », Spectropolis élimine une grande partie de la crainte reliée au sujet des nouvelles technologies et permet aux personnes de considérer les implications plus importantes qu'ont les technologies sans fil sur leurs vies, sans s'alourdir du « comment » de la technologie en soi.

Spectropolis est un événement unique parce qu'il se concentre sur l'impact social des technologies sans fil, par opposition aux technologies elles-mêmes. La grande majorité des personnes ont peur d'expérimenter avec la technologie (ceci est plus courrant chez les adultes que chez les enfants) ou ne sont simplement pas intéressés. Même si Wi-Fi et les technologies de téléphonie mobile ont eu des percées significatives dans la société en général, ceci a été réalisé par l'entremise de deux activités sociales bien établies: parler au téléphone et accéder à l'Internet (courriel, web, IM, etc...)

De plus, Spectropolis met un visage sur la nature éthérée des signaux sans fil. Le fait que le Wi-Fi soit disponible dans un parc peut être indiqué par des signes et des autocollants sur des fenêtres mais ce n'est pas la même chose que de créer des objets tangibles sous forme d'oeuvres d'art qui puisse rendre ce concept aussi concret que puisse l'être les services publics offerts par le parc tels les bancs, les arbres et l'herbe. Le Wi-Fi dans les espaces publics ne devrait pas être considéré comme une ressource restreinte à une certaine communauté mais plutôt une ressource publique qui peut être partagée et appréciée par tous, tout comme l'ombre d'un grand arbre.

## Organisations participantes

NYCwireless, par l'entremise de Dana Spiegel, a été en charge de produire Spectropolis. NYCwireless est une organisation sans but lucratif qui préconise et permet la croissance de l'accès sans fil gratuit et public à Internet dans la ville de New York City et ses environs. NYCwireless, fondé en 2001, est une organisation de volontaires avec sept membres du conseil, cinq groupes de travail en intérêts spéciaux et approximativement soixante membres actifs.

NYCwireless a travaillé en partenariat avec d'autres organismes locaux et individus marquants de la communauté New York Arts ayant travaillé de manière volontaire pour produire l'événement. Spectropolis a été commandité par *Alliance for Downtown New York* (DTA), une compagnie du regroupement *Business Improvement District* (*BID*). Le DTA commandite égale-

ment un certain nombre de point d'accès sans fil gratuits et publics au centre-ville de New York, y compris le point d'accès sans fil au *City Hall Park* où s'est tenu Spectropolis. Le *Lower Manhattan Cultural Council* (*LMCC*), une organisation de financement et promotion des arts a commandité le processus de sélection des œuvres d'art à être exposées à Spectropolis. Le LMCC a été le siège d'un certain nombre de réunions et a supervisé le processus d'invitation et d'évaluation des artistes et de leurs travaux en préparation à l'événement. De plus, d'autres personnes ont contribué à Spectropolis en y dédiant une quantité de temps significative: Wayne Ashley (conservateur, LMCC), Yury Gitman (conservateur), Jordan Silbert (producteur) et Jordan Schuster (producteur).

## Appréciation de la communauté

La communauté locale a bien reçu Spectropolis. Les groupes de personnes principales qui ont assisté à l'événement ont été: des chercheurs et partisans dans le domaine des technologies sans fil, des artistes et le grand public.

Pour mener le projet de l'avant et générer de l'intérêt, nous avons contactés les artistes locaux et les communautés universitaires locales. Nous avons reçu un grand nombre de courriels demandant de l'information pour assister à l'évènement de personnes de la zone et du reste du continent (principalement des États-Unis et du Canada). Quelques enthousiastes des communications sans fil ont même voyagé de l'Europe afin d'être présents. La communauté universitaire locale était particulièrement intéressée, participant avec des étudiants de NYU, SUNY, New School, Parsons et d'autres écoles voisines. Pendant l'événement, nous avons même eu des personnes qui sont venus avec leurs propres projets et les ont installés.

Nous avons également envoyé un communiqué de presse aux médias locaux et sites Web pour informer la communauté générale de la ville de New York de l'événement. Même si avant l'événement nous n'avions pas été contactés par quiconque du grand public, plusieurs personnes qui n'avaient jamais manipulé d'équipement sans fil se sont inscrites dans nos ateliers et nos panels. Les résidents locaux et les visiteurs sont venus à l'évènement principalement pour expérimenter avec les œuvres d'art. Nous avons reçu la visite de milliers de personnes chaque jour qui ont expérimenté avec au moins quelques unes des œuvres.

En plus de l'art, un certain nombre de personnes nous a posé des questions sur la technologie sans fil en général et spécifiquement sur le Wi-Fi public. Plusieurs de ces personnes ont été dirigées vers la cabine d'information de NYCwireless qui a été installée au milieu du parc. Un certain nombre de personnes a également parlé directement aux artistes (nous nous attendions à ceci, c'est pourquoi nous avons tenu que les artistes montrent leur propre

travail au public) au sujet des travaux qu'ils ont créés, la façon dont ils ont travaillé et pourquoi l'artiste a créé cette œuvre.

Pour un certain nombre de participants, Spectropolis était leur premier contact avec le Wi-Fi comme une chose autre plus vaste qu'une technologie Internet. Beaucoup ont été surpris par le fait que les technologies sans fil pouvaient être bien plus que seulement un appel téléphonique mobile ou une page Web dans un café et étaient heureux d'apprendre les usages alternatifs de Wi-Fi explorés par les œuvre d'arts. Parfois, le rapport entre les signaux sans fil et les oeuvres d'art étaient cachés et obscurs -- comme Sonic Interface d'Akitsugu Maebayashi. Dans d'autres travaux, comme Upper Air réalisé par DSP Music Syndicate, l'œuvre d'art a été conçue pour soutenir l'existence de la technologie sans fil et explorait le rapport de la technologie avec l'observateur et l'art.

Quelques oeuvres, tels que Jabberwocky par Eric John Paulos et Elizabeth Goodman se sont servies de la technologie pour explorer les rapports sociaux dans les environnements urbains. Ces travaux étaient importants et significatifs parce qu'ils ont reliés la technologie sans fil à quelque chose qui est clairement une expérience humaine, telle que localiser une personne dans une foule. Dans Jabberwocky en particulier, le téléspectateur est forcé de voir également les limites de la technologie sans fil et de se servir des capacités humaines pour compléter les lacunes.

Dessins GPS, un atelier tenu par Jeremy Wood, présentait le résultat du concept humains + technologie comme quelque chose de plus grand que la somme de ses parties. Wood a conduit des groupes de personnes autour du centre-ville de la ville de New York afin de créer des dessins à grande échelle grâce à leurs déplacements. Cette œuvre d'art a davantage personnalisé l'expérience des technologies sans fil que n'importe quel autre projet.

Tous ces projets ont forcé les participants à réévaluer leurs rapports avec leurs technologies. En plus de présenter sous une nouvelle lumière la portée publique des réseaux sans fil, Spectropolis a fait réfléchir sur la façon dont ces technologies enrichissent et imprègnent nos vies. En parlant avec des artistes après l'événement, tous ont été étonnés de constater jusqu'à quel point les personnes étaient engagées. Les personnes qui ont interagi avec les oeuvres d'art ont une meilleure compréhension de la nature, autrement éphémère, des signaux sans fil. Pour les visiteurs de l'événement, Spectropolis a rendu les concepts abstraits de spectre et de réseaux sans fil publics beaucoup plus concrets et leur a offert une façon de comprendre ces concepts d'une manière dont le simple fait d'utiliser un téléphone mobile ou un ordinateur portable Wi-Fi ne pourrait pas. C'est dans ce sens que Spectropolis a été un vrai succès.

## Projets

*Spectropolis* a présenté les projets et artistes suivants:

- **WiFi Ephemera Cache** par Julian Bleecker,
- **UMBRELLA.net** par Jonah Brucker-Cohen et Katherine Moriwaki
- **Microrardio Sound Walk** par free103point9 Transmission Artists
- **Urballoon** par Carlos J. Gomez de Llarena
- **Bikes Against Bush** par Joshua Kinberg
- **InterUrban** par Jeff Knowlton et Naomi Spellman
- **Hotspot Bloom** par Karen Lee
- **Sonic Interface** par Akitsugu Maebayashi
- **Jabberwocky** par Eric John Paulos et Elizabeth Goodman
- **Upper Air** par The DSP Music Syndicate
- **Twenty-Four Dollar Island** par Trebor Scholz
- **Text Messaging Service** et **Following 'The Man of the Crowd'** par Dodgeball + Glowlab

## Planification

La planification de *Spectropolis* a commencé environ un an avant que l'évènement ait lieu. Au départ, des représentants de NYCwireless, LMCC et DTA, ainsi que les producteurs et les conservateurs, se sont rencontrés sur une base mensuelle pour établir le plan et pour produire l'événement. Le coût de production de Spectropolis a été d'environ 11 000$ dollars américains.

Vous pouvez trouver plus d'information dans le site web de Spectropolis 2004: *http://www.spectropolis.info/* et à mon *Blog Wireless Community* à: *http://www.wirelesscommunity.info/spectropolis*.

*—Dana Spiegel*

# *Étude de cas: la quête d'un Internet abordable dans le Mali rural*

Pendant plusieurs années, la communauté du développement international n'a cessé de promouvoir l'idée d'éliminer la brèche digitale, cet abîme invisi-

ble qui isole les pays en voie de développement de l'abondance d'information et de nouvelle technologie (TIC) des pays développés. L'accès aux outils de l'information et de communications a démontré avoir un impact important sur la qualité de vie. Pour plusieurs donneurs las de soutenir des activités traditionnelles de développement pendant des décennies, l'installation d'un télécentre dans les pays en voie de développement semble comme un effort réalisable et valable. Comme l'infrastructure n'existe pas, ceci est beaucoup plus cher dans les pays en voie de développement qu'en Occident. D'ailleurs, peu de modèles ont montré comment soutenir ces activités. Afin d'aider à atténuer une partie du coût d'une connexion Internet dans les secteurs ruraux du monde développé, l'équipe de l'auteur a favorisé l'utilisation de systèmes sans fil. En novembre 2004, un projet affilié a demandé à l'équipe de l'auteur de réaliser une initiative pilote d'implantation d'un système sans fil à un télécentre récemment établi dans le Mali rural à 8 heures de 4x4 au sud-ouest de Bamako, la capitale.

Cette ville rurale, située à la limite d'une réserve retenant l'eau du barrage Manitali qui fournit l'énergie au tiers du pays. L'avantage de cet endroit est que l'énergie hydroélectrique est beaucoup plus stable et disponible que l'énergie générée par le diesel. Comme l'énergie générée par le diesel est beaucoup moins stable, certaines communautés rurales sont chanceuses de ne pas avoir du tout accès à l'électricité.

La ville a également la chance de se situer au sein d'une des régions les plus fertiles du pays, dans la « ceinture du coton », la récolte qui rapporte le plus d'argent au Mali. On a cru que cet emplacement présenterait moins de difficultés que d'autres secteurs ruraux au Mali pour établir un télécentre autonome financièrement. Cependant, comme plusieurs expérimentations, celle-ci s'est avérée pleine de défis.

Du point de vue technologique, c'était une tâche simple. En 24 heures, l'équipe a installé un réseau 802.11b sans fil qui partage la connexion Internet VSAT des télécentres avec 5 autres services locaux: la Mairie, le Gouverneur, le Service de santé, le Conseil municipal et le Service consultatif de la communauté.

Ces clients avaient été choisis pendant une mission de reconnaissance deux mois auparavant. Durant cette visite, l'équipe avait interviewé les clients potentiels et avait déterminé quels clients pourraient être connectés sans avoir à faire des installations compliquées ou dispendieuses. Le télécentre lui-même est hébergé à la station radio de la communauté. Les stations de radio sont généralement de bons emplacements pour accueillir les réseaux sans fil au Mali rural car elles sont souvent bien situées, offrent l'électricité et la sécurité et des personnes qui comprennent au moins les fondements de la transmission par radio. Elles sont également des espaces naturels de rencontre dans un village. Fournir Internet à une station radio fait que celle-ci

puisse offrir de meilleures informations à ses auditeurs. De plus, pour une culture qui est principalement orale, la radio s'avère être le moyen le plus efficace de fournir des informations.

De la liste de clients ci-dessus, vous noterez que les clients étaient tous gouvernementaux ou paragouvernementaux. Ceci s'est avéré être un mélange difficile étant donnée l'animosité et le ressentiment considérable existant entre les divers niveaux du gouvernement. Il y avait des conflits continuels concernant les impôts et autres sujets fiscaux. Heureusement le directeur de la station de radio, le promoteur du réseau, était très dynamique et a été en mesure de relever la plupart de ces problèmes politiques.

## Choix de conception

L'équipe technique a déterminé que le point d'accès serait installé à 20 mètres au-dessus de la tour de la station de radio, juste au-dessous des dipôles de la radio FM et à une hauteur qui ne ferait pas interférence à la couverture des sites clients, dont la plupart se trouvent dans une dépression de terrain similaire à un bol. L'équipe s'est alors concentrée sur la façon de connecter chaque site client à ce site. Une antenne omnidirectionnelle de 8 dBi (de Hyperlinktech, *http:///hyperlinktech.com/*) suffirait pour fournir une couverture à tous les clients. L'antenne choisie avait une inclinaison vers le bas de 15 degrés, ce qui garantissait que les deux clients se trouvant à moins d'un kilomètre pourraient quand même recevoir un signal fort. Certaines antennes ont une largeur de faisceau très étroite et « surpassent » donc certains sites qui se trouvent à proximité. Des antennes à panneau ont aussi été considérées, il en aurait fallu au moins deux ainsi qu'une deuxième radio ou un diviseur de canaux. Cela ne semblait pas nécessaire pour ce genre d'installation. Le calcul trigonométrique suivant montre comment calculer l'angle entre l'antenne du site client et l'antenne de base de la station.

```
tan(x) = différence d'élévation
       + Hauteur de l'antenne de base de la station
       - Hauteur de l'antenne CPE
       / Distance entre les sites

     tan(x) = 5m + 20m - 3m / 400m
          x = tan-1 (22m / 400m)
          x =~ 3 degrés
```

En plus de l'équipement du télécentre (4 ordinateurs, une imprimante laser, un commutateur de 16 ports), la station de radio elle-même a un poste de travail Linux installé dans le cadre du projet de l'auteur pour l'édition audio. Un petit commutateur a été placé dans la station de radio et un câble Ethernet a été installé à travers la cour du télécentre dans un tuyau en plastique enterré à 5 centimètres.

À partir du commutateur principal, deux câbles ont été installés jusqu'à un point d'accès Mikrotik RB220. Le RB220 a deux ports Ethernet, un qui se connecte au VSAT à travers un câble croisé et l'autre qui se connecte au commutateur central de la station de radio. Le RB 220 est logé dans un boîtier de PVC et l'antenne omnidirectionnelle de 8 dBi (*Hyperlink Technologies*) est installée directement au-dessus du couvercle de PVC.

Le RB220, exécute un dérivé de Linux, Mikrotik version 2.8.27, qui contrôle le réseau et fournit le DHCP, coupe-feu, cache DNS et route le trafic au VSAT en employant NAT. Le Mikrotik vient avec une ligne de commande puissante et une interface graphique relativement amicale et complète. C'est un petit ordinateur x86, conçu pour être utilisé comme point d'accès ou ordinateur embarqué. Ces points d'accès ont une capacité POE, deux ports Ethernet, un port mini-PCI, deux fentes PCMCIA, un lecteur CF (qui est employé pour sa NVRAM), tolèrent les changements de température et soutiennent une variété de systèmes d'exploitation x86. En dépit du fait que le logiciel Mikrotik exige des licences, il y avait déjà une partie essentielle d'installée au Mali et le système avait une interface graphique puissante et amicale bien supérieure à celle d'autres produits. C'est en raison des facteurs ci hauts mentionnés que l'équipe a accepté d'employer ces systèmes, y compris le logiciel Mikrotik pour contrôler les réseaux. Le coût total du RB220, avec une licence de niveau 5, Altheros mini-pci a/b/g et POE a été de 461$ dollars. Vous pouvez trouver ces pièces en ligne chez Mikrotik à *http://www.mikrotik.com/routers.php#linx1part0*.

Le réseau a été conçu pour s'adapter à l'expansion, en isolant les divers sous-réseaux de chaque client ; des sous-réseaux privés de 24 bits ont été établis. L'AP a une interface virtuelle sur chaque sous-réseau et réalise tout le routage et le coupe-feu sur la couche IP. Note: ceci ne fournit pas un coupe-feu à la couche réseau, ce qui signifie qu'en utilisant un sniffer réseau comme le tcpdump il est possible de voir tout le trafic sur le lien sans fil.

Comme le réseau semblait présenter peu de risques au niveau de la sécurité et afin de limiter l'accès exclusivement aux abonnés, un contrôle d'accès de niveau MAC a été employé. Pour cette première phase, un système plus complet de sécurité a été laissé pour être mis en application à l'avenir, lorsqu'il y aura plus de temps disponible pour trouver une interface plus simple pour contrôler l'accès. Les usagers ont été encouragés à employer des protocoles sécuritaires, tels que https, pops, imaps etc.

Le projet affilié a installé un système VSAT (DVB-S) bande C. Ces systèmes satellites sont normalement très fiables et sont souvent employés par les ISPs. C'est une unité grande et coûteuse, dans ce cas-ci le plat était de 2,2 mètres de diamètre et coûtait approximativement 12.000$ dollars en comprenant l'installation. Il est également coûteux de le faire fonctionner, le coût d'une connexion à débit descendant de 128 kbps et à débit montant de 64

kbps s'élève à approximativement 700$ dollars par mois. Cependant, ce système a plusieurs avantages si on le compare à un système Ku, entre autres: une plus grande résistance au mauvais climat, des taux inférieurs de contention (partage de la bande passante entre différents usagers) et elle est plus efficace pour le transfert de données.

L'installation de ce VSAT n'était pas idéale car le système exécutait Windows et que les usagers pouvaient rapidement changer certaines configurations, y compris le fait d'ajouter un mot de passe au compte par défaut. Comme le système n'avait aucun UPS ou batterie de support, lorsqu'une panne d'électricité se produisait, le système redémarrait et attendait l'introduction d'un mot de passe qui avait été oublié depuis. Pour rendre cette situation encore pire, comme le logiciel VSAT n'a pas été configuré pour se restaurer automatiquement, ceci causait des pannes inutiles qui auraient pu être évitées avec l'usage d'un UPS, une configuration appropriée du logiciel VSAT en service Windows et en limitant l'accès physique au modem. Comme tous les propriétaires d'un nouvel équipement, la station radio a voulu le montrer, par conséquent il n'a pas été caché de la vue. Il aurait été préférable de garder l'équipement invisible en le protégeant dans un espace derrière des portes de verre.

Le système sans fil était assez simple. Tous les sites client choisis étaient à moins de 2 kilomètres de la station radio. Chaque site avait un endroit à partir duquel il était possible de voir physiquement la station radio. Au site client, l'équipe a choisi d'employer des CPE commerciaux. En se basant sur le prix, le choix suivant a été fait: ponts Powernoc 802.11b, antennes plates SuperPass de 7 dBi et adaptateurs POE faits maison. Pour faciliter l'installation du CPE et de l'antenne plate, ceux-ci ont été montés sur un petit morceau de bois qui a été installé sur le mur extérieur du bâtiment faisant face à la station radio.

Dans certains cas, le morceau de bois était un bloc à angles pour optimiser la position de l'antenne. À l'intérieur, un POE fait à partir d'un amplificateur de signal de télévision (12V) a été employé pour alimenter les unités. Aux sites client, il n'y avait pas de réseaux locaux, l'équipe a donc également dû installer des câbles et des commutateurs pour fournir Internet à chaque ordinateur. Dans certains cas, il a été nécessaire d'installer des adaptateurs Ethernet et leurs pilotes (ceci n'avait pas été déterminé pendant l'évaluation). Puisque les réseaux du client étaient simples, on a décidé qu'il serait plus facile de faire des ponts réseaux. Advenant le besoin, l'architecture IP pourrait permettre une future partition et l'équipement CPE supporte le mode STA. Nous avons utilisé un pont PowerNOC CPE qui a coûté 249$ dollars (disponible à *http://powernoc.us/outdoor_bridge.html*).

Le personnel local a été impliqué durant l'installation du réseau sans fil. Ils ont appris de tout, allant du câblage à l'emplacement d'une antenne. Un programme de formation intensif d'une durée de plusieurs semaines a suivi l'installation. Le but était d'enseigner au personnel aussi bien les tâches quotidiennes que le dépannage de base de réseau.

Un jeune diplômé universitaire qui était revenu à la communauté a été choisi pour offrir le support au système, excepté pour l'installation de câble réalisée par le technicien de la station de radio qui a rapidement appris cette tâche. Les réseaux Ethernet câblés sont très semblables aux réparations et aux installations des câbles coaxiaux que le technicien de la station de radio exécutait déjà régulièrement. Le jeune universitaire a également requis peu de formation. L'équipe a dépensé la majeure partie de son temps à l'aider à apprendre comment soutenir les éléments de base du système et du télécentre. Peu après l'ouverture du télécentre, des étudiants se sont inscrits pour suivre une formation de 20 heures qui incluait également l'usage d'Internet pour uniquement 40$ dollars par mois, ce qui constituait toute une affaire si on comparait ce montant aux 2$ dollars par heure exigée pour avoir accès à Internet. Le fait d'offrir cette formation représentait un revenu significatif et constituait une tâche pour laquelle le jeune universitaire était bien préparé.

Malheureusement, ce que d'une certaine façon était prévisible a eu lieu. Le jeune universitaire est parti pour la capitale, Bamako, après avoir reçu une offre d'emploi du gouvernement. Ceci laissa le télécentre abandonné, son membre le plus capable techniquement et le seul qui avait été formé pour soutenir le système était parti. La majeure partie de la connaissance pour faire fonctionner le télécentre et le réseau s'est en allée avec lui. Après délibération, l'équipe a déterminé qu'il serait préférable de ne pas former un autre jeune mais plutôt de se concentrer sur le personnel local permanent, en dépit du fait que leur expérience technique était limitée. Ceci a pris beaucoup plus de temps, nos instructeurs ont dû retourner pour un total de 150 heures de formation. Chaque fonction a été enseignée à plus d'une personne et les tâches de support du télécentre ont été divisées parmi le personnel.

La formation ne s'est pas arrêtée là. Une fois que les services communautaires furent connectés, il fut également nécessaire de leur fournir l'accès. En effet, bien que les autorités aient participé, celles-ci, incluant le maire, n'employaient pas le système. Comme l'équipe s'est rendue compte qu'il était important de s'assurer que les décideurs emploient le système, elle a fourni une formation pour eux et leur personnel. Ceci a éliminé une partie de la mystique du réseau et a fait que les décideurs de la ville s'impliquent.

Après la formation, le programme a fait un suivi du site et a commencé à fournir des résultats, évaluant les manières dont ce modèle pourrait être amélioré. Les leçons apprises de ce projet ont été appliquées à d'autres sites.

## Modèle financier

Le télécentre communautaire avait déjà été établi comme activité sans but lucratif et avait l'obligation de s'autofinancer avec la vente de ses services. Le système sans fil a été inclus comme source supplémentaire de revenu parce que les projections financières initiales pour le télécentre indiquaient qu'il serait difficile de payer la connexion VSAT.

En se basant sur la recherche et en consultant la station radio responsable de la gestion du télécentre, plusieurs clients ont été choisis. La station de radio a négocié des contrats avec un certain appui de leur partenaire financier. Pour cette première phase, les clients ont été choisis en se basant sur la facilité d'installation et la solvabilité. Les clients ont été invités à payer des frais d'abonnement, comme nous le décrirons plus tard.

Décider combien charger pour le service a été une activité importante qui a exigé consultation et une expertise que la communauté n'avait pas. L'équipement a été payé avec une concession pour aider la communauté, mais les clients devaient payer une cotisation d'abonnement, ce qui servait à assurer leur engagement. Celle-ci équivalait à un mois de prestation du service.

Afin de déterminer le coût mensuel pour la même portion de largeur de bande, nous avons commencé avec la formule suivante:

```
VSAT + salaires + dépenses (électricité, fournitures) =
revenu du télécentre + revenu des clients sans fil
```

Nous avons estimé que le télécentre devait gagner environ 200$ à 300$ dollars par mois. Les dépenses totales ont été estimées à 1050$ dollars par mois, divisées de la façon suivante: 700$ pour le VSAT, 100$ pour les salaires, 150$ pour l'électricité, et environ 100$ pour des fournitures. Pour équilibrer cette équation, les clients sans fil devaient apporter un revenu d'environ 750$ dollars. Ceci s'élevait approximativement à 150$ par client, ce qui semblait tolérable pour ceux-ci et semblait faisable, mais requérait d'un bon climat et ne laissait pas de place pour des complications.

Comme ceci devenait chaque fois plus compliqué, nous avons consulté des experts en affaires qui ont modifié la formule comme suit:

```
Dépenses mensuelles + amortissement + fonds de sécurité
= revenu total
```

Les experts en affaires ont rapidement mis l'emphase sur le besoin d'amortissement de l'équipement, ce que l'on pourrait également qualifier de « fonds de réinvestissement » ou fonds pour des imprévus, pour s'assurer que le réseau puisse continuer à fonctionner même si un client ne paie pas ou si certains équipements se brisent. Ceci donnait environ 150$ par mois pour l'amortissement (équipement évalué à environ 3.000$ dollars, amorti sur 24 mois) et la valeur d'un client pour manquement de paiements, à 100$. Ajoutez un autre 10% pour considérer la dévaluation de la monnaie (80$ ) , et cela équivaut à des dépenses de 1380$ dollars par mois. En essayant de mettre en application ce modèle, on a finalement déterminé que l'amortissement serait un concept trop difficile pour une communauté qui ne considère pas que les clients ne puissent ne pas payer. Ainsi, les deux formules ont été employées, la première par le télécentre et la seconde pour notre analyse interne.

Comme on s'est rapidement rendu compte, les paiements réguliers ne font pas partie de la culture dans le Mali rural. Dans une société agraire, tout est saisonnier, tel est donc aussi le cas pour le revenu. Ceci signifie que le revenu de la communauté fluctue beaucoup, et d'autant plus que les établissements publics impliqués avaient aussi de longs cycles budgétaires avec peu de flexibilité. Bien que théoriquement le budget pour payer le service soit disponible, cela peut prendre plusieurs mois avant que les paiements soient faits. D'autres complications fiscales ont également surgi. Par exemple, le maire a signé et utilisé les impôts de la radio pour payer son abonnement. Ceci n'a naturellement pas contribué au cash-flow. Malheureusement, les fournisseurs de VSAT ont peu de flexibilité ou de patience car ils ont une largeur de bande limitée et n'ont de la place que pour ceux qui peuvent payer.

La gestion du cash-flow est devenue notre principal souci. D'abord, le revenu prévu dans les projections financières a prouvé que même avec des perspectives optimistes, il serait non seulement problématique pour eux de trouver assez d'argent à temps pour payer les cotisations d'abonnement, mais il serait également difficile d'obtenir l'argent à la banque de Bamako. Les routes près du village peuvent être dangereuses étant donné le nombre de contrebandiers de la Guinée et les rebelles qui surveillent les chemins de la Côte d'Ivoire. Comme il avait été projeté, le télécentre n'a pas été en mesure de payer pour son service et celui-ci a été suspendu, ce qui a également suspendu le paiement de leurs clients.

Avant que le projet puisse trouver des solutions à ces problèmes, le coût du VSAT avait déjà commencé à creuser une dette pour le télécentre. Après plusieurs mois, étant donné les problèmes techniques ainsi que les inquiétudes soulevées dans cette analyse, le VSAT de bande C a été remplacé par un système de bande Ku meilleur marché. Bien que moins dispendieuse, elle a été suffisante pour la taille du réseau. Ce système coûtait

seulement 450$ dollars ce qui, en ignorant les marges d'amortissement et de sûreté, rendait le réseau accessible. Malheureusement, étant donné le manque de paiements, le réseau n'a pas été en mesure de payer pour la connexion VSAT après la période initiale qui avait été subventionnée.

## Conclusions

Construire un réseau sans fil est relativement facile, mais le faire fonctionner relève plus d'un problème administratif que d'un problème technique. Un modèle de paiement qui considère le réinvestissement et le risque est une nécessité ; dans le cas contraire, le réseau sera un échec. Dans ce cas-ci, le modèle de paiement n'était pas approprié car il ne s'est conformé ni aux cycles fiscaux des clients, ni aux attentes sociales. Une analyse appropriée de risque aurait conclu qu'un paiement mensuel de 700$ dollars (ou même de 450$ dollars) laissait une marge trop étroite entre le revenu et les dépenses pour compenser pour des défauts fiscaux. D'un autre côté, une demande élevée et les besoins en éducation ont limité l'expansion du réseau.

Après la formation, le réseau a fonctionné pendant 8 mois sans problèmes techniques significatifs. Puis, une montée importante de puissance provoquée par un éclair a détruit une grande partie de l'équipement à la station, y compris le point d'accès et le VSAT. En conséquence, actuellement le télécentre ne fonctionne pas et cette formule a été considérée une solution peu convenable.

*—Ian Howard*

# *Étude de cas: déploiements commerciaux en Afrique de l'Est*

Ce chapitre décrit les déploiements commerciaux sans fil en Tanzanie et au Kenya en mettant l'emphase sur les solutions techniques qui fournissent une disponibilité de 99,5% en accès Internet et connexion de données dans les pays en voie de développement. Contrairement aux projets consacrés à l'accès ubiquiste, nous nous sommes concentrés sur l'offre de services aux organisations, généralement celles avec des besoins critiques de communication internationale. Je décrirai deux approches commerciales radicalement différentes en rapport à la connectivité de données sans fil tout en faisant une récapitulation des leçons principales apprises en dix ans de travail en Afrique de l'Est.

## Tanzanie

En 1995, avec Bill Sangiwa, j'ai fondé CyberTwiga, un des premiers ISPs en Afrique. Les services commerciaux ont commencé au milieu de l'année 1996, et se sont limités au trafic de courriel dialup à travers un lien SITA de 9,6 kbps (coûtant plus de 4000$ dollars par mois!). Nous sentant frustrés par les services erratiques de PSTN, et encouragés par un déploiement réussi d'un réseau de 3 nœuds point à multipoint (PMP) par l'autorité des ports de la Tanzanie, nous avons commencé des pourparlers avec une compagnie locale de téléphones mobiles pour placer une station base de PMP sur leur mât central. Vers la fin de l'année 1998, en connectant plusieurs sociétés à ce système privé WiLan de 2,4 gigahertz, nous avons validé le marché et notre capacité technique pour fournir des services sans fil.

Comme les concurrents déployaient aussi des réseaux de 2,4 gigahertz, deux faits se sont produit: un marché sain pour des services sans fil est né, mais étant donné le bruit RF à 2,4 gigahertz, la qualité du réseau a diminué. Notre fusion avec la compagnie de téléphones mobiles au milieu de l'an 2000 a inclus des plans pour un réseau sans fil dans tout le pays construit sur l'infrastructure de téléphonie mobile existante (des tours et des liens de transmission) et des attributions de propriété industrielle de spectre RF.

Comme l'infrastructure était en place (les tours cellulaires, les liens de transmission, etc...), la conception et le déploiement du réseau de données sans fil furent assez simples. La capitale de la Tanzanie, Dar es Salaam, est un endroit très plat, et comme l'associé de téléphones mobiles travaillait avec un réseau analogique, les tours étaient très hautes. Une compagnie associée au Royaume-Uni, Tele2, avait débuté des opérations avec l'équipement Breezecom (maintenant Alvarion) à 3,8/3,9 gigahertz, nous avons donc suivi leur exemple.

Vers la fin de l'an 2000, nous avions établi une couverture dans plusieurs villes, employant des circuits de transmission E1 fractionnés pour le transport (backhaul). Dans la plupart des cas la petite taille des villes connectées a justifié l'utilisation d'une seule station base omnidirectionnelle PMP ; seulement dans la capitale commerciale, Dar es Salaam, des stations base de trois secteurs ont été installées. Les limites de largeur de bande ont été configurées directement sur les radios des clients lesquels avaient normalement une seule adresse IP publique. Les routeurs feuille (leaf) à chaque station base envoyaient le trafic aux adresses IP statiques des clients, en évitant que le trafic de diffusion envahisse le réseau. Les pressions du marché ont maintenu les prix assez bas, à environ 100$ dollars par mois pour 64 kbps, mais à ce moment-là (vers la 2e moitié de l'an 2000) les ISPs pouvaient fonctionner avec des taux de contentions très impressionnants et avantageux. Les applications qui consomment beaucoup de largeur de bande telles que le partage de fichiers entre pairs (P2P), voix et ERPs n'existaient

tout simplement pas en Afrique de l'Est. Avec les frais excessivement élevés des appels internationaux, les organismes ont rapidement changé le fax pour le courriel, même si le coût de l'achat de leur équipement sans fil était de l'ordre de 2000$ à 3000$ dollars.

Les capacités techniques ont été développées localement, exigeant une formation outre-mer pour le personnel uniquement pour des sujets tels que SNMP et UNIX. En plus d'améliorer les qualifications de la compagnie, ces opportunités de formation ont fidélisé le personnel. Nous avons dû concurrencer au sein d'un marché de TIC très limité avec des compagnies internationales d'extraction d'or, l'ONU et d'autres agences internationales.

Pour assurer la qualité aux sites client, nous avons engagé une entreprise locale de radio et de télécommunications de premier niveau et le progrès des installations était contrôlé de manière très stricte avec des cartes de travail. Les températures élevées, la lumière du soleil équatorial tenace, la pluie et la foudre plaçaient les composantes extérieures sous des conditions extrêmes ; l'intégrité du câblage RF était essentielle.

Les clients manquaient souvent de personnel compétent dans le domaine des TIC, ce qui obligeait nos employés à configurer plusieurs types d'équipement réseau et différentes topologies.

L'infrastructure et les obstacles de régulation ont souvent empêché les opérations. La compagnie de téléphones mobiles contrôlait étroitement les tours, de sorte que s'il y avait un problème technique à une station base, des heures et même des jours pourraient passer avant que nous puissions y avoir accès. En dépit des générateurs de secours et des systèmes UPS à chaque site, le courant électrique a toujours été problématique. Pour la compagnie de téléphones mobiles, l'approvisionnement électrique aux stations base était moins critique. Leurs abonnés n'avaient qu'à s'associer à une station de base différente tandis que nos abonnés au service de données sans fil perdaient la connexion.

Du côté de la régulation, la plus grande interruption a eu lieu lorsque l'autorité de télécommunications a décidé que notre opération était responsable de perturber les opérations du satellite sur la bande C pour le pays en entier et nous a ordonné de déconnecter notre réseau.

En dépit des données qui démontraient que nous n'étions pas responsables de ce problème, le régulateur a réalisé une saisie de notre équipement qui a reçu une importante publicité. Naturellement l'interférence a persisté, et plus tard il a été déterminé qu'elle émanait du radar d'un bateau russe impliqué dans des activités spatiales. Nous avons tranquillement engagé des pourparlers avec le régulateur, lequel nous a finalement récompensé avec 2 x 42 mégahertz de spectre privé dans les bandes de 3,4/3,5 gigahertz. Les clients

se sont connectés à travers les modems téléphoniques pendant le mois que nous avons reconfiguré les stations de base et installé le nouveau CPE.

Finalement le réseau a grandi jusqu'à atteindre environ 100 noeuds et fournissait une bonne connectivité, sans être excellente, à 7 villes à travers plus de 3000 Km de liens de transmission. La seule fusion avec l'opérateur de téléphones mobiles a rendu ce réseau faisable ; l'ampleur du marché Internet/données à lui seul n'aurait pas justifiée la construction d'un réseau de données de ces dimensions ni les investissements requis pour des fréquences privées. Malheureusement, l'opérateur de téléphones mobiles a pris la décision de se retirer du marché d'Internet au milieu de l'an 2002.

## Nairobi

Au début de l'an 2003, j'ai été approché par une compagnie kenyane, AccessKenya, qui compte avec un fort appui du Royaume-Uni et un support technique pour concevoir et déployer un réseau sans fil à Nairobi et ses environs. Nous avons eu l'avantage de compter sur de formidables professionnels en réseautage et commerce, un équipement sans fil amélioré, les progrès en interconnexion de réseaux, et un plus grand marché afin de concevoir un réseau de haute disponibilité qui répondait aux contraintes de régulation.

Notre conception du réseau a été déterminée par deux facteurs de régulation. À ce moment-là au Kenya, les services Internet avaient une licence différente de celle des opérateurs de réseau public de données, et une même compagnie ne pouvait pas obtenir les deux licences. En transmettant le trafic de multiples ISPs concurrents ou usagers corporatifs, le réseau devait fonctionner avec une totale neutralité. En outre, les fréquences privées, à savoir les 3,4/3,5 gigahertz, n'ont pas été assignées exclusivement à un seul fournisseur, et nous avons été préoccupés par l'interférence et la capacité technique et/ou volonté politique du régulateur pour faire respecter la loi. D'autre part, le spectre à 3,4/3,5 gigahertz était dispendieux, coûtant environ 1000 dollars américains par mégahertz par an par station de base. C'est-à-dire qu'une station de base utilisant 2 x 12 mégahertz impliquait le paiement de licences pour un montant de 10 000 dollars par an. Comme Nairobi est un endroit montagneux avec un bon nombre d'arbres et de grandes vallées, les réseaux sans fil à large bande ont exigé beaucoup de stations de base. Les dépenses reliées aux licences n'avaient pas de sens. En revanche, les fréquences de 5,7/5,8 gigahertz étaient soumises seulement à des frais annuels d'environ 120$ dollars américains par radio déployée.

Pour répondre à la première exigence de régulation nous avons choisi de fournir des services à l'aide de tunnels VPN point à point, et non pas par l'intermédiaire d'un réseau de routes IP statiques. Une ISP nous fournirait une adresse IP publique à leur NOC. Notre réseau réalisait une conversion d'IP

de publique à privée, et le trafic passait par notre réseau dans un espace IP privé. Au site client, une conversion d'IP privé à publique avait lieu, ce qui fournissait toutes les adresses routables requises au réseau de l'usager.

La sécurité et le chiffrage contribuaient à la neutralité du réseau et la flexibilité constituait un avantage compétitif de notre réseau. La largeur de bande était limitée au niveau du tunnel VPN. En nous basant sur l'expérience opérative de notre compagnie affiliée du Royaume-Uni, VirtualIT, nous avons choisi Netscreen (qui fait à présent partie de Juniper Networks) en tant que fournisseur pour les routeurs coupe-feu VPN.

Notre critère pour l'équipement sans fil à bande large éliminait les dispositifs à haut rendement. Les facteurs comme la forme, la fiabilité et la facilité d'installation et de gestion étaient plus importants que le rendement. En 2003 et jusqu'à maintenant, toutes les connexions internationales d'Internet vers le Kenya étaient portées par satellite. Avec des coûts 100 fois plus élevés que la fibre optique, la connectivité par satellite a mis un plafond financier sur la quantité de largeur de bande achetée par les usagers. Nous avons considéré que la majeure partie de notre population d'usagers requérait d'une capacité de l'ordre de 128 à 256 kbps. C'est pour cette raison que nous avons choisi la plateforme Canopy récemment présentée par Motorola, la jugeant en conformité avec notre modèle d'affaires et de réseau.

Broadband Access, Ltd, est devenu disponible en juillet 2003, lançant le réseau « Blue » (bleu). Nous avons démarré modestement: avec une seule station base. Nous voulions que l'expansion de notre réseau obéisse à la demande, plutôt que de compter sur la stratégie de construire de grands tuyaux pour ensuite espérer les remplir.

Canopy et les améliorations provenant de tierces parties tels que les stations de base omnidirectionnelles, nous ont permis d'accroître notre réseau au même rythme qu'augmentait le trafic, ce qui a atténué les dépenses initiales de capital. Nous savions que la compensation viendrait lorsque le réseau augmenterait de taille et qu'à ce moment-là nous devrions sectoriser le trafic et réaligner les radios des clients. La courbe douce d'apprentissage d'un petit réseau a payé de grands dividendes plus tard. Le personnel technique était de plus en plus familier avec les questions de support d'un réseau simple, plutôt que de devoir traiter celles-ci en plus d'équipements RF et d'une topologie logique complexes. Le personnel technique a assisté à deux jours de sessions de formation offerts par Motorola.

Avec une conception typique point à multipoint, des stations de base liées à un service central par l'intermédiaire d'un réseau fédérateur à micro-ondes à grande vitesse Canopy, le réseau a été déployé sur les toits des bâtiments et non sur des tours d'antennes. Tous les baux stipulaient l'accès pour le personnel à l'approvisionnement d'énergie 24 heures par jour et 7 jours par se-

maine, en protégeant l'exclusivité de nos fréquences de radio. D'un autre côté, nous n'avons pas voulu limiter les propriétaires d'offrir de l'espace sur leurs toits aux concurrents tant et aussi longtemps qu'ils garantissaient que nos services ne seraient pas interrompus.

Les installations sur les toits fournissaient beaucoup d'avantages: l'accès physique illimité et sans restrictions causées par la nuit ou la pluie, ce qui permettait d'atteindre le but d'une disponibilité du réseau de 99,5%. Les grands bâtiments ont également hébergé beaucoup de grands clients et il a été possible de les connecter directement au cœur de notre réseau micro-ondes. Les installations sur les toits avaient le désavantage de recevoir un trafic humain plus important: les personnes responsables de maintenir l'équipement d'air climatisé ou réparant les fuites du toit pouvaient occasionnellement endommager le câblage. En conséquence, toutes les stations de base ont été installées avec deux ensembles de câblage pour tous les éléments du réseau, un primaire et un de rechange.

La prospection de sites confirmait la disponibilité d'un chemin libre pour les ondes radio et pour les besoins des clients. L'équipe de prospection notait les coordonnées de chaque client via GPS et portait un télémètre laser pour déterminer la taille des obstacles. Après avoir reçu le paiement pour l'équipement, des personnes étaient engagées pour effectuer les installations toujours sous la surveillance du personnel technique. Canopy a l'avantage que les CPE et les éléments des stations de bases sont légers, de sorte que la présence de plusieurs personnes n'était pas nécessaire dans la plupart des installations. Câbler les unités Canopy était également simple, avec des câbles UTP pour l'extérieur connectant les radios directement aux réseaux des clients. Tout cela permettait la réalisation d'une installation complète et adéquate en moins d'une heure et l'équipe engagée n'avait pas besoin de formation avancée ou d'outils spéciaux.

Comme nous avons compilé des centaines de positions GPS de nos clients, nous avons commencé à travailler étroitement avec une compagnie de topographie pour inclure ces emplacements dans des cartes topographiques. Celles-ci sont devenues l'outil principal de planification pour l'emplacement de stations bases.

Notez que l'architecture de tunnel VPN point à point, avec ses couches physiques et logiques séparées, a exigé que les clients achètent tant la largeur de bande sans fil comme l'équipement VPN. Afin de contrôler étroitement la qualité, nous avons catégoriquement refusé de permettre à des clients de fournir leurs propres équipements ; ils ont dû nous l'acheter afin d'avoir des garanties de service et d'équipement. De cette façon, chaque client a reçu le même paquet. Généralement, les installations coûtaient environ 2500$ dollars américains et les coûts mensuels pour une largeur de bande de 64 à 128 kbps étaient de l'ordre de 500$ à 600$ dollars. Un avantage de l'appro-

che du tunnel VPN était que nous pouvions empêcher le trafic d'un client dans le réseau logique (par exemple, si leur réseau avait été attaqué par un ver ou s'ils ne payaient pas une facture) tandis que la couche radio demeurait intacte et maniable.

Lorsque le réseau est passé d'une seule station de base à dix stations, et que le service a été étendu jusqu'à la ville de Mombasa, la disposition du réseau RF et les routeurs ont été configurés avec fallover ou hotswap avec redondance. Afin de maintenir le réseau stable dans le cadre d'un approvisionnement électrique erratique, chaque station base a exigé des investissements importants en inverseurs et un équipement dual UPS de conversion. Après un certain nombre de problèmes avec les clients que nous avons attribués aux pannes électriques (rupture de connexions VPN), nous avons simplement inclus un petit UPS dans notre installation de base.

Ajouter un analyseur de spectre portatif à notre investissement de capital initial était coûteux, mais énormément justifié pour l'opération du réseau. Cet outil nous permet de retracer des opérateurs malhonnêtes, confirmer les caractéristiques de fonctionnement de l'équipement et vérifier la couverture RF afin d'améliorer nos performances.

Le fait de prêter une attention toute particulière à la surveillance nous a permis de perfectionner la performance du réseau et de rassembler des données historiques de grande valeur. Celles-ci étaient représentées graphiquement grâce à MRTG ou Cacti (comme décrit au chapitre six). On obtenait des données sur le vacillement (jitter), RSSI et le trafic permettant de détecter des opérateurs malhonnêtes ou une détérioration potentielle des câbles/connecteurs, ainsi que la présence de vers dans les réseaux du client. Il n'était pas rare que des clients prétendent que leur service avait été interrompu pendant des heures ou des jours et exigent un remboursement. La surveillance historique permettait de vérifier ou infirmer ces réclamations.

Le réseau « Blue » en Tanzanie comprend un certain nombre de leçons sur comment améliorer les technologies RF et réseau.

## Leçons apprises

Pendant des années à venir les circuits satellites fourniront toute la connectivité Internet internationale en Afrique de l'Est. Plusieurs groupes ont présenté des propositions pour offrir la connectivité à travers la fibre sous-marine, ce qui revitalisera les télécommunications lorsque ceci se produira. Comparé aux régions par fibre, les coûts de largeur de bande en Afrique de l'Est demeureront très hauts.

En conséquence, les réseaux sans fil de large bande n'ont pas besoin de se concentrer sur le rendement pour fournir des services Internet. Au lieu de cela, l'accent devrait être mis sur la fiabilité, la redondance et la flexibilité.

La fiabilité pour nos réseaux sans fil était notre point de vente principal. Du côté du réseau, ceci se traduisait en investissements considérables dans la substitution d'infrastructure, telle que l'énergie de secours et l'attention aux détails tels que le sertissage de câbles et le câblage en soi. Les raisons les plus courantes pour qu'un client perde la connectivité étaient des questions de câblage ou de sertissage tandis qu'il n'y avait essentiellement aucun problème relié à la radio. Un avantage concurrentiel principal de notre procédé d'installation de client est que nous obligions le personnel engagé à adhérer de façon stricte aux spécifications. C'est pour cette raison que les sites clients bien gérés restaient connectés pendant des centaines de jours sans aucune panne non programmée du réseau. Nous avons contrôlé notre infrastructure autant que possible (c.-à-d. sur les toits des bâtiments).

Même si les alliances potentielles avec les fournisseurs de téléphones mobiles cellulaires semblaient attrayantes, notre expérience nous a montré qu'elles soulèvent plus de problèmes qu'elles n'en résolvent. En Afrique de l'Est, les entreprises d'Internet produisent une fraction du revenu généré par la téléphonie mobile et sont donc marginales par rapport aux compagnies de téléphones mobiles. Essayer de faire fonctionner un réseau sur une infrastructure qui ne vous appartient pas est, du point de vue du fournisseur de téléphones mobiles, un geste de bonne volonté, ce qui rendra impossible de respecter les engagements de service.

Mettre en marche des réseaux de grande redondance, avec une capacité de basculement (failover) ou de remplacement à chaud (hotswap), est une proposition dispendieuse en Afrique. Néanmoins, les routeurs centraux et l'équipement VPN à notre point central de présence étaient entièrement redondants, configurés pour un failover consistant et pour être testés de façon routinière. Pour les stations base nous avons pris la décision de ne pas installer les routeurs duels, mais avons gardés des routeurs de rechange en stock. Nous avons jugé que dans le pire des scénarios, le fait de ne pas avoir de réseau pendant 2 à 3 heures (une chute du réseau à une heure du matin un dimanche sous la pluie) semblerait acceptable pour les clients. De même, les membres du personnel qui travaillaient les fins de semaine ont eu accès à un compartiment de secours contenant des éléments de rechange pour les équipements des clients, tels que des radios et des alimentations électriques.

La flexibilité a été prise en compte dans la conception logique du réseau et dans son infrastructure RF. L'architecture de tunnel VPN point à point développée à Nairobi était extraordinairement flexible pour répondre aux besoins des clients ou du réseau. Comme simple exemple, les connexions des

clients pouvaient être programmées pour s'arrêter pendant les heures de moindre trafic pour permettre de réaliser un back up en dehors du site. Nous pouvions également vendre des liens multiples à des destinations séparées, augmentant le retour de nos investissements de réseau tout en offrant de nouveaux services à nos clients (comme la télésurveillance des caméras CCTV).

Par rapport au RF nous avions assez de spectre pour projeter une expansion ou pour mettre en place un réseau sur une fréquence alternative en cas d'interférence. Avec le nombre de plus en plus important de stations base, probablement le 80% de nos clients étaient à la portée de deux stations de base de sorte que si une station de base était détruite nous pouvions rapidement restituer le service.

La séparation des couches logiques et RF du réseau « Blue » a présenté un niveau additionnel de complexité et de coût. En considérant qu'à long terme les technologies de radio avanceront plus rapidement que les techniques d'interconnexion de réseaux, la séparation des réseaux, en théorie, nous donne la flexibilité de remplacer le réseau RF existant sans perturber le réseau logique. Nous pouvons également installer différents réseaux de radio en conformité avec les nouvelles technologies (Wimax) ou les besoins des clients, tout en maintenant le réseau logique.

En conclusion, on doit se rendre à l'évidence que les réseaux sophistiqués que nous avons déployés seraient parfaitement inutiles sans notre engagement persistant au service à la clientèle. C'est après tout pour cela que nous sommes payés.

## Pour plus d'information

- Broadband Access, Ltd. *http://www.blue.co.ke/*
- AccessKenya, Ltd. *http://www.accesskenya.com/*
- VirtualIT *http://www.virtualit.biz/*

*—Adam Messer, Ph.D.*

# Annexe A: Ressources

Nous recommandons les ressources suivantes (en anglais seulement) pour en apprendre davantage sur les divers aspects du réseautage sans fil. Pour plus de liens et de ressources, visitez notre site Web à: *http://wndw.net/.*

## Antennes et conception d'antennes

- Cushcraft technical papers on antenna design and radio propagation, *http://www.cushcraft.com/comm/support/technical-papers.htm*
- Free antenna designs, *http://www.freeantennas.com/*
- Hyperlink Tech, *http://hyperlinktech.com/*
- Pasadena Networks LLC, *http://www.wlanparts.com/*
- SuperPass, *http://www.superpass.com/*
- Unofficial NEC-2 code archives, *http://www.si-list.org/swindex2.html*
- Unofficial NEC-2 radio modeling tool home page, *http://www.nittany-scientific.com/nec/*
- USB WiFi dish designs, *http://www.usbwifi.orcon.net.nz/*

## Outils de dépannage pour réseaux

- Cacti network monitoring package, *http://www.cacti.net/*
- DSL Reports bandwidth speed tests, *http://www.dslreports.com/stest*
- Ethereal network protocol analyzer, *http://www.ethereal.com/*
- Iperf network performance testing tool, *http://dast.nlanr.net/Projects/Iperf/*
- iptraf network diagnostic tool, *http://iptraf.seul.org/*
- MRTG network monitoring and graphing tool, *http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*
- My TraceRoute network diagnostic tool, *http://www.bitwizard.nl/mtr/*
- Nagios network monitoring and event notification tool, *http://www.nagios.org/*
- Ntop network monitoring tool, *http://www.ntop.org/*

- RRDtool round robin database graphing utility, *http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/*
- SmokePing network latency and packet loss monitor, *http://people.ee.ethz.ch/~oetiker/webtools/smokeping/*
- SoftPerfect network analysis tools, *http://www.softperfect.com/*
- Squid transparent http proxy HOWTO, *http://en.tldp.org/HOWTO/mini/TransparentProxy-2.html*
- ttcp network performance testing tool, *http://ftp.arl.mil/ftp/pub/ttcp/*

## Sécurité

- AntiProxy http proxy circumvention tools and information, *http://www.antiproxy.com/*
- Anti-spyware tools, *http://www.spychecker.com/*
- Driftnet network monitoring utility, *http://www.ex-parrot.com/~chris/driftnet/*
- Etherpeg network monitoring utility, *http://www.etherpeg.org/*
- Introduction to OpenVPN, *http://www.linuxjournal.com/article/7949*
- Lavasoft Ad-Aware spyware removal tool, *http://www.lavasoft.de/*
- OpenSSH secure shell and tunneling tool, *http://openssh.org/*
- OpenVPN encrypted tunnel setup guide, *http://openvpn.net/howto.html*
- Privoxy filtering web proxy, *http://www.privoxy.org/*
- PuTTY SSH client for Windows, *http://www.putty.nl/*
- Sawmill log analyzer, *http://www.sawmill.net/*
- Security of the WEP algorithm, *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*
- Spyware prevention for Windows XP (German), *http://www.xp-antispy.de/*
- Stunnel Universal SSL Wrapper, *http://www.stunnel.org/*
- TOR onion router, *http://tor.eff.org/*
- Weaknesses in the Key Scheduling Algorithm of RC4, *http://www.crypto.com/papers/others/rc4_ksaproc.ps*
- Windows SCP client, *http://winscp.net/*
- Your 802.11 Wireless Network has No Clothes, *http://www.cs.umd.edu/~waa/wireless.pdf*
- ZoneAlarm personal firewall for Windows, *http://www.zonelabs.com/*

## Optimisation de la bande passante

- Cache heirarchies with Squid,
  *http://squid-docs.sourceforge.net/latest/html/c2075.html*
- dnsmasq caching DNS and DHCP server,
  *http://thekelleys.org.uk/dnsmasq/doc.html*
- Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies,
  *http://www.isoc.org/inet97/ans97/cloet.htm*
- Fluff file distribution utility, *http://www.bristol.ac.uk/fluff/*
- Microsoft Internet Security and Acceleration Server,
  *http://www.microsoft.com/isaserver/*
- Microsoft ISA Server Firewall and Cache resource site,
  *http://www.isaserver.org/*
- Pittsburgh Supercomputing Center's guide to Enabling High Performance Data Transfers, *http://www.psc.edu/networking/perf_tune.html*
- RFC 3135: Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations, *http://www.ietf.org/rfc/rfc3135*
- Squid web proxy cache, *http://squid-cache.org/*

## Réseaux maillés sans fil

- Champaign-Urbana Community Wireless Network software,
  *http://cuwireless.net/download*
- Freifunk OLSR mesh firmware for the Linksys WRT54G,
  *http://www.freifunk.net/wiki/FreifunkFirmware*
- MIT Roofnet Project, *http://pdos.csail.mit.edu/roofnet/doku.php*
- OLSR mesh networking daemon, *http://www.olsr.org/*
- Real-time OLSR topology viewer,
  *http://meshcube.org/nylon/utils/olsr-topology-view.pl*

## Systèmes d'exploitation et pilotes pour périphériques sans fil

- HostAP wireless driver for the Prism 2.5 chipset, *http://hostap.epitest.fi/*
- m0n0wall wireless router OS, *http://m0n0.ch/wall/*
- MadWiFi wireless driver for the Atheros chipset, *http://madwifi.org/*

- Metrix Pebble wireless router OS, *http://metrix.net/metrix/howto/metrix-pebble.html*
- OpenWRT wireless router OS for Linksys access points, *http://openwrt.org/*
- Pebble Linux, *http://nycwireless.net/pebble/*

## Logiciels pour les technologies sans fil

- Chillispot captive portal, *http://www.chillispot.org/*
- Interactive Wireless Network Design Analysis Utilities, *http://www.qsl.net/n9zia/wireless/page09.html*
- KisMAC wireless monitor for Mac OS X, *http://kismac.binaervarianz.de/*
- Kismet wireless network monitoring tool, *http://www.kismetwireless.net/*
- MacStumbler wireless network detection tool for Mac OS X, *http://www.macstumbler.com/*
- NetStumbler wireless network detection tool for Windows and Pocket PC, *http://www.netstumbler.com/*
- NoCatSplash captive portal, *http://nocat.net/download/NoCatSplash/*
- PHPMyPrePaid prepaid ticketing system, *http://sourceforge.net/projects/phpmyprepaid/*
- RadioMobile radio performance modeling tool, *http://www.cplus.org/rmw/*
- Terabeam wireless link calculation tools, *http://www.terabeam.com/support/calculations/index.php*
- Wellenreiter wireless network detection tool for Linux, *http://www.wellenreiter.net/*
- WiFiDog captive portal, *http://www.wifidog.org/*
- Wireless Network Link Analysis tool by GBPRR, *http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*

## Information générale sur les technologies sans fil

- DefCon long distance WiFi shootout, *http://www.wifi-shootout.com/*
- Homebrew wireless hardware designs, *http://www.w1ghz.org/*
- Linksys wireless access point information, *http://linksysinfo.org/*
- Linksys WRT54G resource guide, http://seattlewireless.net/index.cgi/LinksysWrt54g
- NoCat community wireless group, *http://nocat.net/*

- POE guide by NYCWireless, *http://nycwireless.net/poe/*
- Ronja optical data link hardware, *http://ronja.twibright.com/*
- SeattleWireless community wireless group, *http://seattlewireless.net/*
- SeattleWireless Hardware comparison page, *http://www.seattlewireless.net/HardwareComparison*
- Stephen Foskett's Power Over Ethernet (PoE) Calculator, *http://www.gweep.net/~sfoskett/tech/poecalc.html*

## Fournisseurs de logiciels de réseautage

- Alvarion wireless networking equipment, *http://www.alvarion.com/*
- Cisco wireless networking equipment, *http://www.cisco.com/*
- Metrix outdoor wireless networking kits, *http://metrix.net/*
- Mikrotik wireless network equipment, *http://www.mikrotik.com/routers.php#linx1part0*
- PowerNOC outdoor wireless networking equipment, *http://powernoc.us/outdoor_bridge.html*
- RAD Data Communications networking hardware, *http://www.rad.com/*
- Redline Communications WiMax wireless networking equipment, *http://www.redlinecommunications.com/*
- Trango wireless networking hardware, *http://www.trangobroadband.com/*
- WaveRider wireless hardware, *http://www.waverider.com/*

## Services de consultation en réseautique

- Access Kenya ISP, *http://www.accesskenya.com/*
- Broadband Access Ltd. wireless broadband carrier, *http://www.blue.co.ke/*
- Virtual IT outsourcing, http://www.virtualit.biz/
- wire.less.dk consultancy and services, *http://wire.less.dk/*

## Formation et éducation

- Association for Progressive Communications wireless connectivity projects, *http://www.apc.org/wireless/*
- International Network for the Availability of Scientific Publications, *http://www.inasp.info/*
- Makere University, Uganda, *http://www.makerere.ac.ug/*

- Radio Communications Unit of the Abdus Salam International Center for Theoretical Physics, *http://wireless.ictp.trieste.it/*
- World Summits on Free Information Infrastructures, *http://www.wsfii.org/*

## Liens divers

- Cygwin Linux-like environment for Windows, *http://www.cygwin.com/*
- Graphvis graph visualization tool, *http://www.graphviz.org/*
- ICTP bandwidth simulator, *http://wireless.ictp.trieste.it/simulator/*
- ImageMagick image manipulation tools and libraries, *http://www.imagemagick.org/*
- NodeDB war driving map database, *http://www.nodedb.com/*
- Open Relay DataBase, *http://www.ordb.org/*
- Partition Image disk utility for Linux, *http://www.partimage.org/*
- RFC 1918: Address Allocation for Private Internets, *http://www.ietf.org/rfc/rfc1918*
- Spectropolis NYC art project, *http://www.spectropolis.info/*
- Ubuntu Linux, *http://www.ubuntu.com/*
- wget web utility for Windows, *http://xoomer.virgilio.it/hherold/*
- WiFiMaps war driving map database, *http://www.wifimaps.com/*

## Livres

- *802.11 Networks: The Definitive Guide, 2nd Edition*. Matthew Gast, O'Reilly Media. ISBN #0-596-10052-3
- *802.11 Wireless Network Site Surveying and Installation.* Bruce Alexander, Cisco Press. ISBN #1-587-05164-8
- The *ARRL Antenna Book, 20th Edition.* R. Dean Straw (Editor), American Radio Relay League*.* ISBN #0-87259-904-3
- The *ARRL UHF/Microwave Experimenter's Manual*. American Radio Relay League*.* ISBN #0-87259-312-6
- *Building Wireless Community Networks, 2nd Edition.* Rob Flickenger, O'Reilly Media. ISBN #0-596-00502-4
- *Deploying License-Free Wireless Wide-Area Networks.* Jack Unger, Cisco Press. ISBN #1-587-05069-2
- *How To Accelerate Your Internet: A practical guide to Bandwidth Management and Optimisation using Open Source Software*. *http://bwmo.net/*

- TCP/IP Illustrated, Volume 1. W. Richard Stevens, Addison-Wesley. ISBN #0-201-63346-9
- *Wireless Hacks, 2nd Edition*. Rob Flickenger and Roger Weeks, O'Reilly Media. ISBN #0-596-10144-9

# *Annexe B: Allocations des canaux*

Les tableaux suivants présentent le numéro des canaux et les fréquences centrales utilisées pour les standards 802.11a et 802.11b/g. Notez que même si toutes ces fréquences sont dans les bandes sans licence ISM et U-NII, tous les canaux ne sont pas disponibles dans tous les pays. Plusieurs régions imposent des restrictions à certains canaux sur la puissance de rendement et l'usage intérieur/extérieur. Ces règlements changeant rapidement, vous devez toujours vous renseigner sur la réglementation locale avant de déployer votre équipement sans fil.

Notez que ces tableaux montrent la fréquence centrale pour chaque canal. Les canaux ont une largeur de 22MHz pour le standard 802.11b/g et de 20MHz pour le standard 802.11a.

| 802.11b / g | | | |
|---|---|---|---|
| Chaîne # | Fréquence centrale (GHz) | Chaîne # | Fréquence centrale (GHz) |
| 1 | 2,412 | 8 | 2,447 |
| 2 | 2,417 | 9 | 2,452 |
| 3 | 2,422 | 10 | 2,457 |
| 4 | 2,427 | 11 | 2,462 |
| 5 | 2,432 | 12 | 2,467 |
| 6 | 2,437 | 13 | 2,472 |
| 7 | 2,442 | 14 | 2,484 |

| 802.11a | |
|---|---|
| Chaîne # | Fréquence centrale (GHz) |
| 34 | 5,170 |
| 36 | 5,180 |
| 38 | 5,190 |
| 40 | 5,200 |
| 42 | 5,210 |
| 44 | 5,220 |
| 46 | 5,230 |
| 48 | 5,240 |
| 52 | 5,260 |
| 56 | 5,280 |
| 60 | 5,300 |
| 64 | 5,320 |
| 149 | 5,745 |
| 153 | 5,765 |
| 157 | 5,785 |
| 161 | 5,805 |