Réseaux sans fil dans les pays en développement

Deuxième édition

Un guide pratique pour la planification et la construction des infrastructures de télécommunications 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
Deuxième édition en français, Janvier 2009

ISBN: 978-0-9778093-9-4

Table des matières

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.

- **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. 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*).

- **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*

- **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.

- **Laura M. Drewett** est une co-fondatrice de Adapted Consulting Inc, une entreprise sociale qui se spécialise dans l'adaptation de la technologie et de solutions d'affaires pour le monde en développement. Depuis que Laura a vécu pour la première fois au Mali dans les années 1990 et écrit sa thèse sur les programmes d'éducation des filles, elle s'est efforcée de

trouver des solutions durables pour le développement. En tant qu'expert dans la durabilité des projets TIC projets dans les environnements des pays en développement, elle a conçu et géré des projets pour une diversité de clients en Afrique, au Moyen-Orient et en Europe de l'Est. Laura est titulaire d'un baccalauréat ès arts avec distinction en affaires étrangères et Français de l'Université de Virginie et un certificat de maîtrise en gestion de projet de la George Washington University School of Business.

- **Alberto Escudero-Pascual et Louise Berthilson** sont les fondateurs de IT+46, une société suédoise de consultance mettant l'accent sur les technologies de l'information dans les régions en développement. IT+46 est internationalement connue pour la promotion et l'implementation de l'infrastructure Internet sans fil dans les zones rurales d'Afrique et d'Amérique latine. Depuis 2004, l'entreprise a formé plus de 350 personnes dans 14 pays et a publié plus de 600 pages de documentation sous Licence Creative Commons. Plus d'informations peuvent être trouvées à partir de *http://www.it46.se/*

- **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*.

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

- **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.

- **Gina Kupfermann** est une ingénieur diplômé en gestion de l'énergie et est titulaire d'un diplôme en ingénierie et en affaires. Outre son métier de contrôleur financier, elle a travaillé pour plusieurs projets communautaires auto-organisés et des organizations à but non lucratif. Depuis 2005, elle est membre du conseil exécutif de l'association pour le développement des réseaux libres, l'entité juridique de *freifunk.net*.
- **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.
- **Juergen Neumann** (*http://www.ergomedia.de/*) a commencé à travailler avec la technologie de l'information en 1984 et depuis lors, a été la recherche de moyens pour déployer les TIC de manière utile pour les organisations et la société. En tant que consultant en matière de stratégie et d'implémentation des TICs, il a travaillé pour les grandes entreprises allemandes et internationales et de nombreux projets à but non lucratif. En 2002, il co-fonda *www.freifunk.net*, une campagne pour diffuser les connaissances et le réseautage social sur les réseaux libres et ouverts. Freifunk est globalement considéré comme l'un des plus grands succès parmi les projets communautaires dans ce domaine.
- **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.

- **Frédéric Renet** est co-fondateur de solutions techniques pour Adapted Consulting, Inc. Frédéric a été impliqué dans les TIC depuis plus de 10 ans et a travaillé avec des ordinateurs depuis son enfance. Il a commencé sa carrière dans les TIC au début des années 1990 avec un système de babillard électronique (BBS) sur un modem analogique et a depuis continué à créer des systèmes qui améliorent la communication. Plus récemment, Frédéric a passé plus d'une année à IESC/Geekcorps au Mali en tant que consultant. À ce titre, il a conçu de nombreuses solutions innovantes pour la radio FM, les laboratoires d'informatique des écoles, et des systèmes d'éclairage pour les communautés rurales.
- **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.

Appuis

- **Lisa Chan** (*http://www.cowinanorange.com/*)**:** l'éditrice principale.
- **Casey Halverson** (*http://seattlewireless.net/~casey/*) a réalisé une révision technique et a fourni différentes suggestions.
- **Jessie Heaven Lotz** (*http://jessieheavenlotz.com/*) a mis à jour plusieurs illustrations de cette édition.
- **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.
- **Catherine Sharp** (*http://odessablue.com/*) a offert son appui pour l'édition.
- **Lara Sobel** a conçu la couverture pour la seconde édition de WNDW. Elle est une artiste vivant actuellement à Seattle, WA.
- **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.

A propos du guide de l'énergie solaire

Le matériel de base utilisé pour le chapitre sur l'énergie solaire a été traduit et développé par Alberto Escudero-Pascual. En 1998, l'organisation Ingénierie sans frontières (Fédération espagnole) avait publié la première version d'un manuel intitulé "Manual de Energía Solar Fotovoltaica y Cooperación al Desarrollo ". Le manuel avait été rédigé et publié par les membres de l'ONG et des experts de l'Institut de l'énergie solaire de l'université polytechnique de Madrid.

Curieusement, aucun des membres de l'équipe de rédaction n'avait gardé aucune copie du document en format électronique et aucune autre édition n'avait été réalisée. Près de dix années se sont écoulées à partir de cette première édition, et ce document est un effort pour sauvegarder et étendre le manuel.

Dans le cadre de cette opération de sauvetage, Alberto tient à remercier les coordonnateurs de la première édition originale ainsi que ses mentors pendant ses années d'université: Miguel Ángel Eguido Aguilera, Mercedes Montero Bartolomé y Julio Amador. Ce nouveau travail est sous licence Creative Commons Attribution-ShareAlike 3.0. Nous espérons que ce document devienne un nouveau point de départ pour de nouvelles éditions, y compris des nouvelles contributions par la communauté.

Cette seconde édition étendue du guide d'énergie solaire a reçu une contribution précieuse de Frédéric Renet et Louise Berthilson.

Remerciements spéciaux

Le groupe central voudrait remercier les organisateurs de la conférence WSFII pour avoir facilité l'espace, le support fourni et également 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, Antoine Tonon Guillemot, Jean-Philippe Dionne. La deuxième traduction française a été réalisée par Antoine B. Bagula et Pascal Morin. La coordination de cet effort collectif a été développée à travers l'initiative WiLAC, *http://www.wilac.net*.

La publication de ce travail a été soutenue par le Centre de Recherche pour le Développement International du Canada, *http://www.idrc.ca/*. Un soutien supplémentaire a été fourni par *NetworktheWorld.org*.

IDRC CRDI

The Abdus Salam International Centre for Theoretical Physics

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 récemment 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.

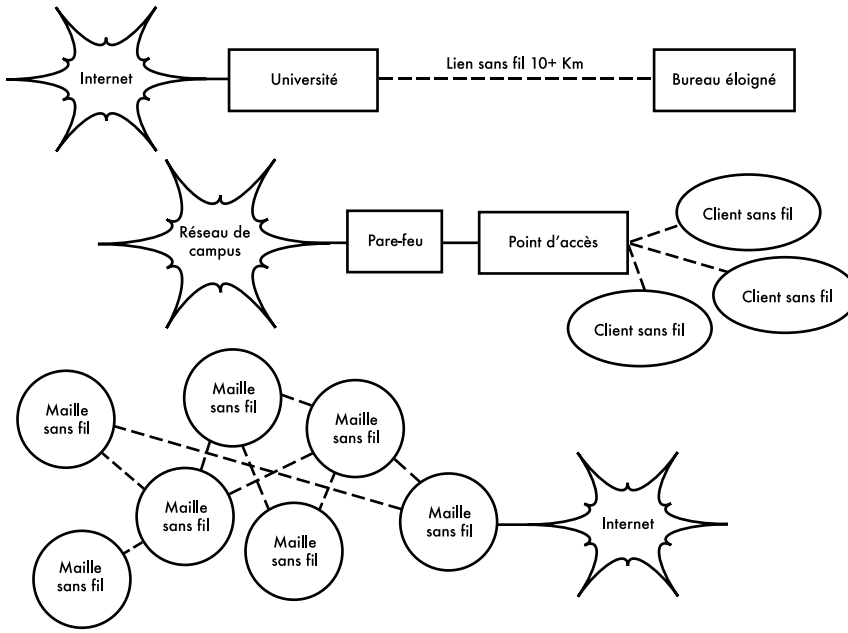


Figure 1.1: Quelques exemples de réseaux sans fil.

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***), soit ***étalement de spectre à séquence directe***, 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 *mobiles*. 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 213.***

Dois-je installer un câble électrique jusqu'en haut de la tour? ***Page 252.***

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 219.***

Pour combien de temps mon point d'accès peut fonctionner à l'aide d'une batterie? ***Page 240.***

Gestion

Comment puis-je surveiller et gérer des points d'accès à distance à partir de mon bureau? ***Page 177.***

Que dois-je faire si le réseau fait défaillance? ***Page 177, 269.***

Quels sont les problèmes les plus fréquents que l'on doit affronter avec les réseaux sans fil et comment puis-je les résoudre? ***Page 269.***

Distance

Quelle est la portée de mon point d'accès? ***Page 68.***

Existe-t-il une formule qui me permette de connaître la portée d'un point d'accès donné? ***Page 69.***

Comment puis-je savoir si un emplacement éloigné peut se connecter à Internet à l'aide d'un lien sans fil? ***Page 68.***

Le manufacturier dit que mon point d'accès à une portée de 300 m. Est-ce vrai? ***Page 68.***

Comment puis-je fournir une connectivité sans fil à plusieurs clients éloignés et dispersés partout dans la ville? ***Page 53.***

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 127.***

Puis-je utiliser la technologie sans fil pour me connecter à un site éloigné et partager une connexion centrale unique à Internet? ***Page 52.***

Mes liens sans-fil semblent trop longs. Puis-je placer un répéteur au milieu pour les améliorer? ***Page 78.***

Sinon, dois-je utiliser un amplificateur? ***Page 115.***

Installation

Comment puis-je installer mon AP pour usage interne sur le toit de ma demeure près de l'antenne? ***Page 251.***

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 266.***

Puis-je construire un mât d'antenne tout seul? Quelle hauteur puis-je atteindre? ***Page 253.***

Pourquoi mon antenne fonctionne beaucoup mieux si je la place dans une autre direction? ***Page 12.***

Quel canal dois-je utiliser? ***Page 15.***

Les ondes de radio traversent-elles les édifices et les arbres? Qu'arrive t-il avec les personnes? ***Page 16.***

Les ondes de radio pourront-elles traverser une colline qui se trouve dans son chemin? ***Page 17.***

Comment puis-je construire un réseau maillé? ***Page 57.***

Quel type d'antenne est le mieux adapté pour mon réseau? ***Page 103.***

Puis-je construire un point d'accès en utilisant un vieil ordinateur? ***Page 148.***

Comment puis-je installer Linux sur mon AP? Pourquoi devrais-je le faire? ***Page 156.***

Coûts

Comment puis-je savoir si un lien sans fil est possible avec un petit montant d'argent? ***Page 283.***

Quel est le meilleur AP pour le plus faible coût? ***Page 139.***

Comment puis-je attirer des clients et les facturer pour l'utilisation de mon réseau sans fil? ***Page 167, 192.***

Partenaires et Clients

Si je suis un fournisseur de connexions, dois-je toujours avoir recours à un service FAI? Pourquoi? ***Page 27.***

Avec combien de clients puis-je couvrir mes coûts? ***Page 283.***

Mon réseau sans fil peut supporter combien de clients? ***Page 65.***

Comment faire pour que mon réseau sans fil soit plus rapide? ***Page 80.***

Ma connexion Internet est-elle aussi rapide qu'elle pourrait l'être? ***Page 91.***

Sécurité

Comment puis-je protéger mon réseau sans fil des accès non autorisés? ***Page 159.***

Est-ce vrai qu'un réseau sans fil est toujours peu sécuritaire et ouvert aux attaques de pirates informatiques? ***Page 162.***

Comment puis-je voir ce qui se déroule sur mon réseau? ***Page 178.***

Information et licence

Quels autres livres puis-je lire pour améliorer mes connaissances en réseaux sans fil? ***Page 376.***

Où puis-je trouver plus d'informations en ligne? ***Page 371,*** *http://wndw.net/****.***

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
O = 1/5 mètres
O = 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**.

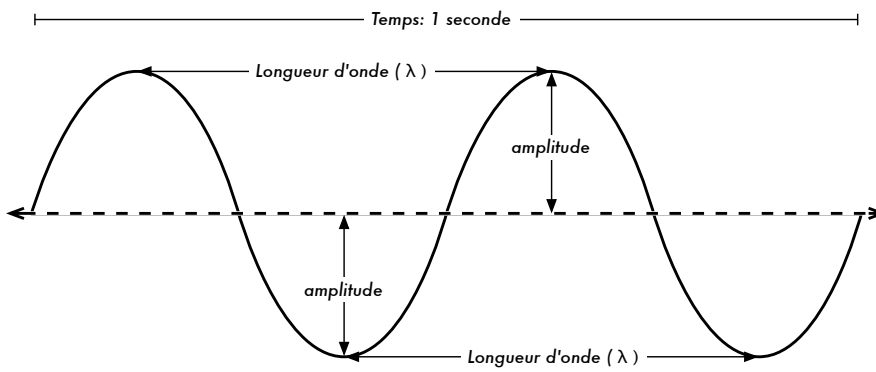


Figure 2.1: Longueur d'onde, amplitude, et fréquence. Pour cette onde, la fréquence est de 2 cycles par seconde, ou 2 Hz.

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.

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 (μs), 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	μ
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:

$$
\begin{aligned}
f &= 2{,}4\ \text{GHz} \\
&= 2\ 400\ 000\ 000\ \text{cycles / seconde}
\end{aligned}
$$

$$
\begin{aligned}
\text{Longueur d'onde lambda } (\lambda) &= c / f \\
&= 3*10^{8} / 2{,}4*10^{9} \\
&= 1{,}25*10^{-1}\ \text{m} \\
&= 12{,}5\ \text{cm}
\end{aligned}
$$

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.

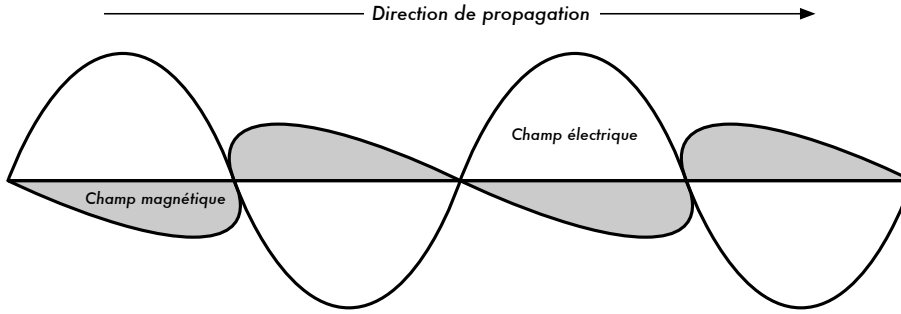


Figure 2.2: Les deux composantes complémentaires d'une onde électromagnétique: son champ électrique son champ magnétique. La polarisation décrit l'orientation du champ électrique.

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.

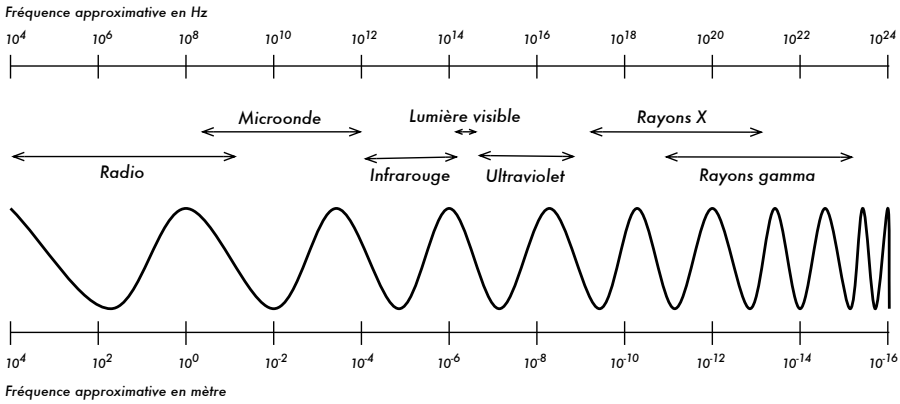


Figure 2.3: Le spectre électromagnétique.

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, ou ***débit binaire***, 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.

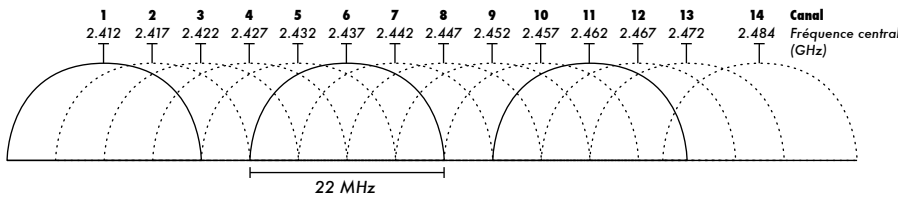


Figure 2.4: Canaux et centre de fréquences pour le standard 802.11b. Notez que les chaînes 1,6 et 11 ne se superposent pas.

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 matériau quelconque, elles en sortent généralement affaiblies ou amorties. La puissance qu'elles vont perdre va dépendre de leur fréquence et naturellement du matériau. 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].

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.

---

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.

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 2,4 GHz. Une façon simple de mesurer l'absorption du plastique à 2,4 GHz 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 2,4 GHz, une grille de métal avec une maille d'un centimètre agira de la même façon qu'une plaque de métal.

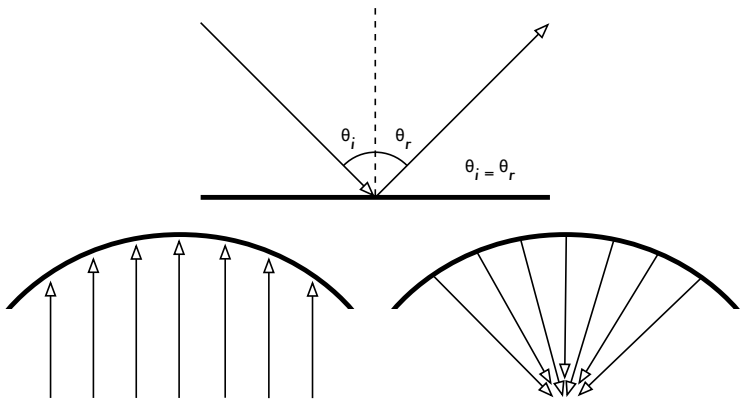


Figure 2.5: Réflexion d'ondes radio. L'angle d'incidence est toujours égal à l'angle de réflexion. Une antenne parabolique utilise cet effet afin de conduire dans une même direction les ondes radio éparpillées sur sa surface.

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.

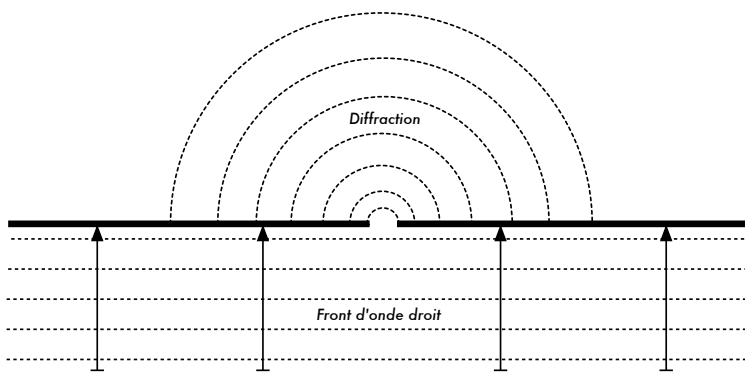


Figure 2.6: Diffraction à travers une ouverture étroite.

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.

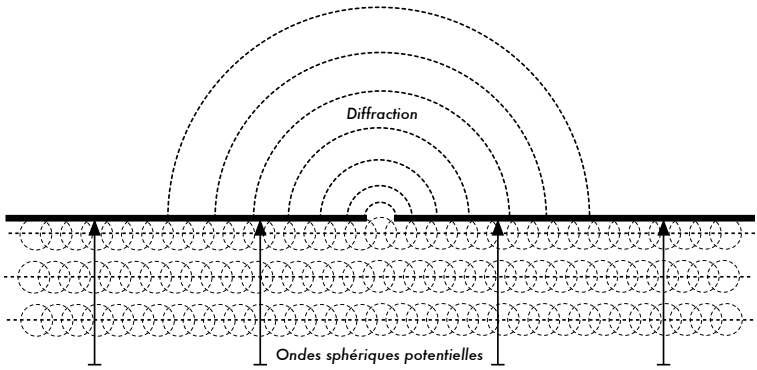


Figure 2.7: Le principe Huygens.

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.

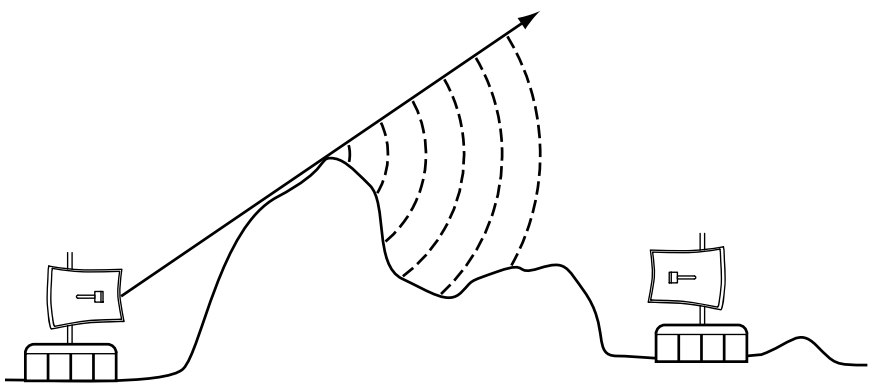


Figure 2.8: Diffraction sur le sommet d'une montagne.

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.

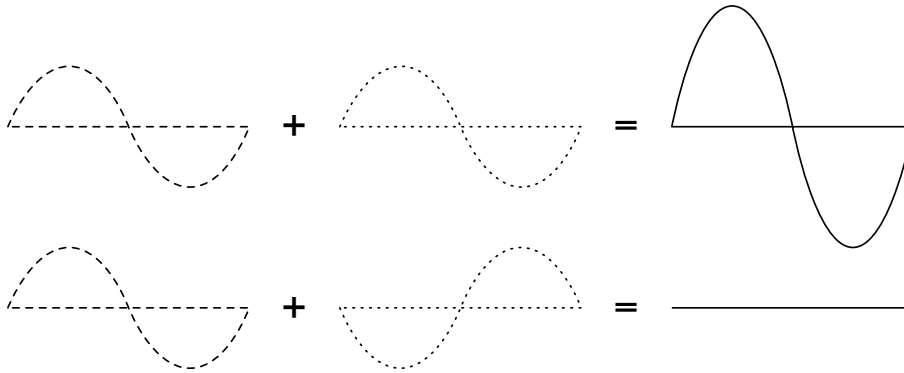


Figure 2.9: Interférence constructive et destructive.

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.

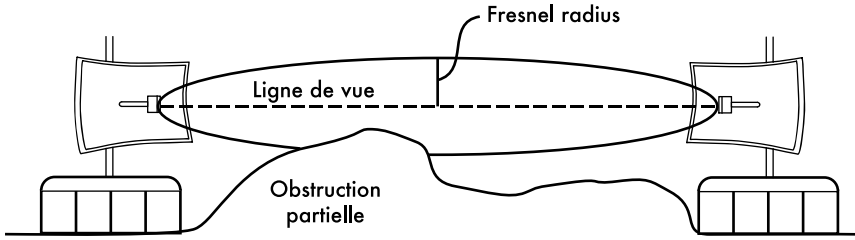


Figure 2.10: La zone Fresnel est partiellement bloquée sur ce lien, même si la ligne de vue apparaît clairement.

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
```

Ceci est un comportement exponentiel.

---

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.

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 l'achat d'équipement ou la prise de décision sur une plate-forme matérielle, vous devez avoir une idée claire de la nature de votre problème de communication. Très probablement, vous lisez ce livre parce que vous avez besoin d'interconnecter des réseaux informatiques afin de partager des ressources et, à terme, accéder a l'Internet. La conception du réseau que vous choisissez d'implémenter doit s'adapter au problème de communication que vous essayez de résoudre. Avez-vous besoin de connecter un site distant à une connexion Internet au coeur de votre campus? Est il probable que la taille de votre réseau augmente afin d'inclure plusieurs sites distants? La plupart de vos composantes réseau seront-elles installées à des endroits fixes, ou votre réseau croîtra-t-il jusqu'à inclure des centaines d'ordinateurs portables mobiles et d'autres périphériques?

Dans ce chapitre, nous commencerons par un examen des concepts réseaux relatifs au protocole TCP/IP, la famille principale des protocoles réseaux utilisés actuellement sur l'Internet. Ensuite, nous verrons des exemples illustrant la façon dont d'autres ont construit des réseaux sans fil pour résoudre leurs problèmes de communication, y compris les schémas de la structure essentielle du réseau. Enfin, nous présenterons plusieurs méthodes communément utilisées pour obtenir une circulation efficace de vos informations à travers votre réseau et le reste du monde.

La mise en réseau 101

TCP/IP fait référence à la suite des protocoles qui rendent possible les conversations sur le réseau Internet. Comprendre TCP/IP vous permet d'implémenter des réseaux de pratiquement n'importe quelle taille et finalement faire partie intégrante du réseau Internet.

Si vous êtes déjà confortable avec les éléments essentiels du réseautage TCP/IP (y compris l'adressage, le routage, les commutateurs, les pare-feu et routeurs), vous voulez peut être passer à la **conception du réseau physique** à la **Page 51**. Nous allons maintenant passer en revue les notions de base du réseautage Internet.

Introduction

Venise en Italie est une ville fantastique pour s'y perdre. Les routes ne sont que des sentiers qui traversent l'eau en des centaines d'endroits et ne suivent jamais une simple ligne droite. Les agents de courrier postal de Venise sont parmi les plus hautement qualifiés du monde, spécialisés dans la livraison à un seul ou deux des six *sestieri* (districts) de Venise. Ceci est nécessaire en raison du complexe agencement (layout) de cette ville antique. Plusieurs personnes trouvent que la localisation de l'eau et du soleil dans Venise est beaucoup plus utile qu'essayer de trouver un nom de rue sur une carte.

Figure 3.1: Un autre type de masque réseau.

Imaginez un touriste qui arrive à trouver le masque en papier mâché comme souvenir et veut l'avoir livré du studio à S. Polo dans Venise à son bureau à Seattle aux Etats-Unis. Cela peut paraître comme une tâche ordinaire (voire trivial), mais voyons ce qui se passe réellement.

L'artiste emballe d'abord le masque dans une boîte d'expédition avec adresse de son bureau à Seattle aux Etats-Unis. Il le remet ensuite à un employé postal qui y associe certains formulaires officiels et l'envoie à un hub central de traitement de colis pour les destinations internationales. Après plusieurs jours, le colis passe la douane Italienne et est embarqué sur un vol transatlantique, à destination d'une centrale de traitement de colis aux Etats-Unis. Une fois passé la douane aux États-Unis, le colis est envoyé au point de distribution régionale pour le nord-ouest des États-Unis, puis le centre de traitement postal de Seattle. Finalement, le colis est acheminé par camionnette de livraison sur un parcours qui l'amène à la bonne adresse, la bonne rue, et dans le bon quartier. L'agent au bureau accepte le colis et le met dans la bonne boîte aux lettres. Une fois arrivé, le colis est récupéré et le masque est enfin lui-même reçu.

L'agent du bureau de Seattle ne sait ni ne se fout de la façon d'arriver au sestiere de S. Polo dans Venise. Son travail est tout simplement d'accepter les colis tels qu'arrivés et les livrer à la bonne personne. De même, le transporteur

postal à Venise n'a pas besoin de s'inquiéter de la façon d'arriver dans le bon quartier à Seattle. Son travail consiste à ramasser les colis de son quartier et les acheminer vers le hub le plus porche de la chaîne de livraison.

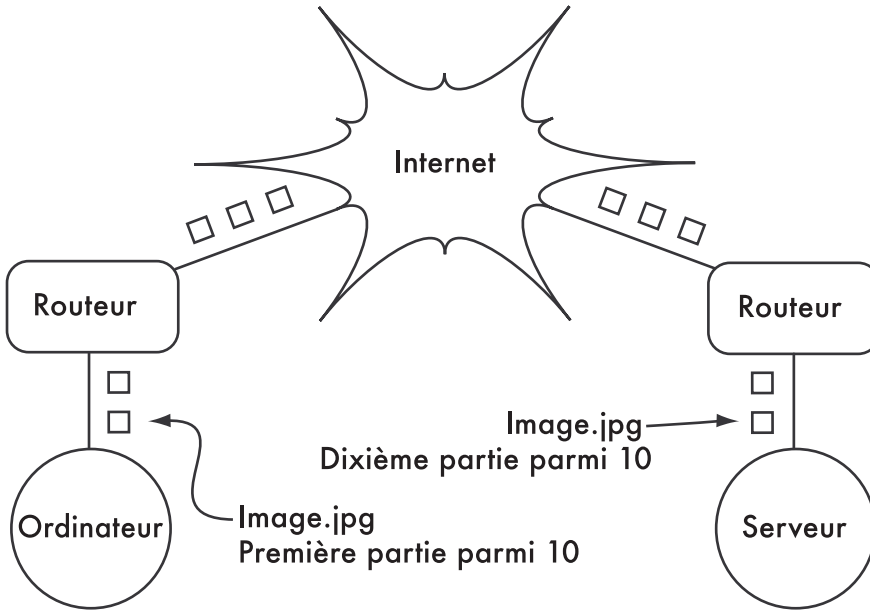


Figure 3.2: Réseautage Internet. Les paquets sont transmis entre les routeurs jusqu'à ce qu'ils atteignent leur destination finale.

Cela est très similaire à la façon dont le routage Internet fonctionne. Un message est divisé en des nombreux ***paquets*** qui sont marqués avec leur source et destination. L'ordinateur envoie ensuite ces paquets vers un ***routeur***, qui décide où les envoyer ensuite. Le routeur n'a besoin que de garder une trace d'une poignée de routes (par exemple, comment arriver au réseau local, le meilleur itinéraire à quelques autres réseaux locaux, et une route à une passerelle vers le reste de l'Internet). Cette liste des routes possibles est appelée la ***table de routage***. Quand les paquets arrivent au routeur, l'adresse de destination est examinée et comparée à celle qui est à l'intérieur de la table de routage. Si le routeur n'a pas de route explicite à la destination en question, il envoie le paquet à l'adresse correspondante la plus proche qu'elle peut trouver, ce qui est souvent sa propre passerelle Internet (via la ***route par défaut***). Et le prochain routeur fait la même chose, et ainsi de suite, jusqu'à ce que le paquet arrive finalement à destination.

Les colis peuvent faire leur chemin à travers le système postal international puisque nous avons mis en place un schéma d'adressage normalisé pour les colis. Par exemple, l'adresse de destination doit être écrite lisiblement sur le devant du colis et doit inclure tous les renseignements essentiels (tels que le nom du destinataire, adresse, ville, pays et code postal). Sans cette information, le colis sont soit renvoyés à l'expéditeur ou sont perdus dans le système.

Les colis peuvent circuler à travers le réseau Internet parce que nous nous sommes convenus sur un schéma d'adressage et un protocole de transmission des paquets. Ces protocoles de communication standard permettant d'échanger l'information à l'échelle globale.

Communications coopératives

La communication n'est possible que lorsque les participants parlent une langue commune. Mais une fois que la communication devient plus complexe qu'une simple conversation entre deux personnes, le protocole devient tout aussi important que le langage. Toutes les personnes dans un auditorium peuvent parler anglais, mais sans la mise en place d'un ensemble de règles pour établir qui a le droit d'utiliser le microphone, la communication des idées d'une personne à toute la salle est presque impossible. Maintenant, imaginez un auditoire aussi vaste que le monde entier, plein de tous les ordinateurs qui existent. Sans un ensemble commun de protocoles de communication réglementant quand et comment chaque ordinateur peut parler, l'Internet serait un mess chaotique où chaque machine tente de parler à la fois.

Les gens ont développé un certain nombre de modules de communications pour résoudre ce problème. Le plus connu d'entre eux est le ***modèle OSI***.

Le modèle OSI

La norme internationale pour l'interconnexion de systèmes ouverts (OSI, *Open Systems Interconnection*) est définie par le document ISO/ IEC 7498-1, tel que décrit par l'organisation Internationale pour la Standardisation et la Commission électrotechnique internationale. Le standard complet est disponible sous la publication "ISO/IEC 7498-1:1994," qui est disponible à partir de *http://standards.iso.org/ittf/PubliclyAvailableStandards/*.

Le modèle OSI répartit le trafic réseau en un certain nombre de ***couches***. Chaque couche est indépendante des couches voisines, et chacune s'appuie sur les services fournis par la couche au dessous d'elle, tout en offrant de nouveaux services à la couche au dessus. L'abstraction entre les couches rend facile la conception des ***piles de protocoles*** élaborés et très fiables, tels que la pile omniprésente ***TCP/IP***. Une pile de protocole est une implémentation réelle d'un module de communications en couches. Le modèle OSI ne définit pas les protocoles qui seront utilisés dans un réseau, mais simplement délègue chaque "tache" de communications à une seule couche dans une hiérarchie bien définie.

Alors que la spécification ISO/IEC 7498-1 décrit en détails comment les couches doivent interagir les uns avec les autres, elle laisse les détails d'implémentation réelle au fabricant. Chaque couche peut être implémentée en matériel (plus commun pour les couches inférieures) ou en logiciel. Tant que l'interface entre les couches adhère à la norme, les gens qui implémentent sont libres d'utiliser tous les moyens qui leur sont disponibles pour construire leur pile de protocole. Cela signifie que n'importe quelle couche donnée du fabricant A peut fonctionner avec la même couche du fabricant B (en supposant que les spécifications pertinentes sont implémentées et interprétées correctement).

Voici un bref aperçu des sept couches du modèle de réseau OSI:

Couche	Nom	Description
7	Application	La ***couche application*** est la couche à laquelle la plupart des utilisateurs réseaux sont exposés, et est le niveau ou la communication humaine se passe. HTTP, FTP, et SMTP sont tous des protocoles de couche d'application. L'utilisateur humain se situe au-dessus de cette couche interagissant avec l'application.
6	Présentation	La ***couche présentation*** traite de la représentation des données avant qu'elles n'atteignent la couche application. Cela inclut le codage MIME, la compression de données, les contrôles de formatage, l'ordonnancement des octets, etc.
5	Session	La ***couche session*** gère la session de communications logique entre les applications. NetBIOS et RPC sont deux exemples d'une cinquième couche de protocole.
4	Transport	La ***couche transport*** fournit une méthode pour parvenir à atteindre un service particulier sur un noeud du réseau donné. TCP et UDP sont des exemples de protocoles qui fonctionnent à cette couche. Certains protocoles de la couche transport (comme TCP) garantissent que toutes les données sont arrivées à la destination, et sont rassemblées et remises à la couche suivante dans le bon ordre. UDP est un protocole "orienté sans connexion" couramment utilisé pour la vidéo et le streaming audio.
3	Réseau	IP (Internet Protocol) est le protocole de la ***couche réseau*** le plus commun. C'est la couche où le routage se passe. Les paquets peuvent quitter le réseau liaison locale et être retransmis sur d'autres réseaux. Les routeurs implémentent cette fonction sur un réseau en utilisant au moins deux interfaces réseau ; une sur chacun des réseaux qui doivent être interconnectés. Les nœuds sur l'Internet sont accessibles par leur adresse globale IP unique. ICMP est un autre protocole réseau critique. C'est un protocole spécial qui offre différents messages de gestion nécessaires pour le bon fonctionnement du protocole IP. Cette couche est également parfois dénommée ***couche Internet***.

Couche	Nom	Description
2	Liaison des données	Lorsque deux ou plusieurs nœuds partagent le même support physique (par exemple, plusieurs ordinateurs branchés dans un hub ou une salle pleine d'appareils sans fil en utilisant tous le même canal radio), ils utilisent la ***couche liaison de données*** pour communiquer. Ethernet, Token Ring, ATM, et les protocoles de réseau sans fil (802.11a/b/g) sont des exemples communs des protocoles de la couche liaison des données. La communication sur cette couche est dite à liaison-locale, car tous les noeuds connectés sur cette couche communiquent les uns avec les autres directement. Cette couche est parfois connue sous le nom de ***couche Media Access Control*** (***MAC***). Sur le modèle de réseaux Ethernet, les noeuds sont référencés par leurs ***adresses MAC***. Il s'agit d'un nombre unique de 48 bits attribué à chaque dispositif réseau quand il est fabriqué.
1	Physique	La ***couche physique*** est la couche inférieure du modèle OSI. Elle se réfère au support physique réel où les communications ont lieu. Cela peut être un câble en cuivre de type CAT5, un faisceau de fibre optique, des ondes radios, ou n'importe quel autre moyen de transmission de signaux. Les câbles coupés, la fibre coupée, et l'interférence des fréquences radios RF sont tous des problèmes de la couche physique.

Dans ce modèle, les couches sont numérotées de un à sept, avec sept étant la couche supérieure. Ceci vise à renforcer l'idée que chaque couche se fonde sur et dépend des couches inférieures. Imaginez le modèle OSI comme un bâtiment, avec la fondation à la couche un, les autres couches comme les étages successifs, et le toit à la septième couche. Si vous supprimez une seule couche, l'édifice ne tiendra pas. Similairement, si le quatrième étage prend feu, alors personne ne peut passer dans les deux directions.

Les trois premières couches (physique, liaison de données, et réseau) toutes apparaissent “sur le réseau”. C'est-à-dire que l'activité de ces couches est déterminée par la configuration de câbles, les commutateurs, les routeurs et autres dispositifs similaires. Un commutateur réseau ne peut distribuer des paquets qu’en utilisant des adresses MAC. Ainsi il a besoin d’implémenter simplement les couches un et deux. Un simple routeur ne peut acheminer les paquets qu’en utilisant seulement leur adresse IP. Il a ainsi besoin d’implémenter les couches un à trois. Un serveur web ou un ordinateur portable exécutent des applications. Il doit donc implémenter l'ensemble des sept couches. Certains routeurs avancés peuvent implémenter la couche quatre et au-dessus pour leur permettre de prendre des décisions fondées sur le contenu de haut niveau d’un paquet tel que le nom d'un site web, ou les pièces jointes d'un e-mail.

Le modèle OSI est reconnu internationalement, et est largement considéré comme le modèle de réseau complet et définitif. Il fournit un cadre pour les fabricants et les gens qui implémentent les protocoles réseau qui peut être utilisé pour construire des dispositifs réseaux pouvant interagir dans à peu près n'importe quelle partie du monde.

Le modèle OSI peut paraître inutilement complexe du point de vue d'un ingénieur ou un dépanneur de réseau. En particulier, les gens qui construisent et maintiennent les réseaux TCP/IP ont rarement besoin de faire face à des problèmes au niveau des couches session ou présentation. Pour la majorité des implémentations de réseau Internet, le Modèle OSI peut être simplifié en une petite collection de cinq couches.

Le modèle TCP/IP

À la différence du modèle OSI, le modèle TCP/IP n'est pas une norme internationale et ses définitions varient. Néanmoins, il est souvent utilisé comme un modèle pragmatique pour la compréhension et le dépannage de réseaux Internet. La grande majorité de l'Internet utilise TCP/IP. Ainsi nous pouvons faire des hypothèses sur les réseaux qui les rendent plus facile à comprendre. Le modèle de réseautage TCP/IP décrit les cinq couches suivantes:

Couche	Nom
5	Application
4	Transport
3	Internet
2	Liaison des données
1	Physique

En termes du modèle OSI, les couches cinq à sept sont intégrés dans la couche supérieure (la couche application). Les quatre premières couches dans les deux modèles sont identiques. Beaucoup d'ingénieurs de réseau pensent de tout ce qui est au dessus de la couche quatre comme

"juste des données" qui varient d'application à application. Comme les trois premières couches sont inter-opérables entre la quasi-totalité des fabricants de matériel, et la couche quatre fonctionne entre tous les hôtes utilisant TCP/IP, et tout ce qui est au-dessus de la couche quatre tend à s'appliquer à des applications spécifiques, ce modèle simplifié fonctionne bien lors de la construction et le dépannage des réseaux TCP/IP. Nous allons utiliser le modèle TCP/IP lors de l'examen des réseaux dans ce livre.

Le modèle TCP/IP peut être comparé à une personne livrant une lettre à un édifice de bureaux au centre ville. Elle 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.

Les protocoles Internet

TCP/IP est la pile de protocoles la plus couramment utilisée sur le réseau Internet. L'acronyme signifie ***Transmission Control Protocol*** (***TCP***) et ***Internet Protocol*** (***IP***), mais en fait, il se réfère à toute une famille de protocoles de communications connexes. TCP/IP est également appelé la ***suite de protocoles Internet***, et elle opère sur les couches trois et quatre du modèle TCP/IP.

Dans cette discussion, nous allons nous concentrer sur la version quatre du protocole IP (IPv4) car c'est la version la plus largement déployée sur le réseau Internet.

Adressage IP

Dans un réseau IPv4, l'adresse est un nombre de 32 bits, normalement présenté comme quatre nombres de 8-bit exprimés sous forme décimale et séparés par des points. 10.0.17.1, 192.168.1.1, ou 172.16.5.23 sont des exemples d'adresses IP.

Si vous avez énuméré toutes les adresses IP possible, elles vont de 0.0.0.0 à 255.255.255.255. Cela donne un total de plus de quatre milliards d'adresses IP possibles (255 x 255 x 255 x 255 = 4 228 250 625), bien que bon nombre de ces adresses sont réservées à des fins spéciales et ne devraient pas être attribuées aux ordinateurs hôtes. Chaque adresse IP utilisable est un identifiant unique qui distingue un noeud réseau d'un autre noeud.

Les réseaux interconnectés doivent se mettre d'accord sur un plan d'adressage IP. Les adresses IP doivent être uniques et ne peuvent généralement pas être utilisées sur l'Internet à des endroits différents en même temps, sinon, les routeurs ne connaîtraient pas la meilleure façon d'acheminer les paquets aux noeuds.

Les adresses IP sont assignées par une autorité centrale de numérotation qui détermine une méthode de numérotation logique et cohérente. Cela permet de s'assurer que les adresses dupliquées ne sont pas utilisées par les différents réseaux. L'autorité attribue des larges blocs d'adresses consécutives à un petit nombre d'autorités, qui à leur tour cèdent des petits blocs consécutifs à l'intérieur de ces fourchettes à d'autres autorités, ou à leurs clients. Ces groupes d'adresses sont appelés sous-réseaux, ou des ***subnets***. Les grands sous-réseaux peuvent être subdivisés en des sous-réseaux plus petits. Un groupe d'adresses relatives est considéré comme un ***espace d'adressage***.

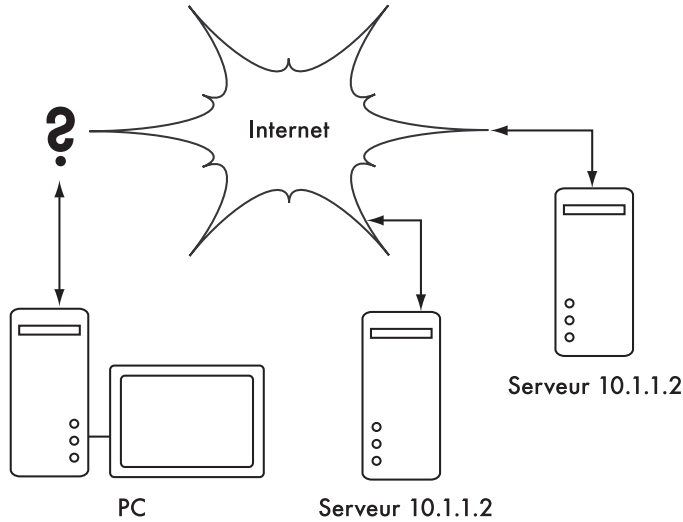


Figure 3.3: Sans adresses IP uniques, un routage sans ambiguïté est impossible. Si le PC demande une page Web à partir de 10.1.1.2, quel serveur va-t-il atteindre?

Sous réseaux

Par application d'un ***masque de sous réseau*** (aussi appelé ***masque de réseau***, ou simplement ***netmask***) à une adresse IP, vous pouvez définir logiquement à la fois l'hôte et le réseau auquel il appartient. Traditionnellement, les masques de sous réseau sont exprimés au moyen d'une forme décimale avec points, un peu comme une adresse IP. Par exemple, 255.255.255.0 est un masque réseau commun. Vous trouverez ce type de notation utilisé lors de la configuration des interfaces, la création des routes, etc. Toutefois, les masques de sous réseau sont plus succinctement exprimés en utilisant la ***notation CIDR*** qui énumère simplement le nombre de bits dans le masque après la barre oblique (/). Ainsi, /24 est une notation simplifiée de 255.255.255.0. CIDR est l'abréviation de ***Classless Inter-Domain Routing***, et est défini dans RFC1518[1].

Un masque de sous réseau détermine la taille d'un réseau donné. En utilisant un masque de réseau /24, 8 bits sont réservés pour les hôtes (32 bits total - 24 bits de masque réseau = 8 bits pour les hôtes). Ceci conduit à un maximum de 256 adresses d'hôtes possible (2^8 = 256). Par convention, la première valeur est considérée comme ***l'adresse réseau*** (.0 ou 00000000), et la dernière valeur est considérée comme ***l'adresse de diffusion*** (.255 ou 11111111). Ceci laisse 254 adresses disponibles pour les hôtes réseau.

Les masques de sous réseau fonctionnent par application du ET logique (en anglais logical AND) à un nombre IP de 32 bits. En notation binaire, le bits "1" dans le masque représentent la partie de l'adresse de réseau, et les bits "0" représentent la partie de l'adresse hôte. Une opération ET logique est effectuée pour comparer deux bits. Le résultat est "1" si les deux bits comparés sont 1.

---

1. RFC est une abréviation pour une demande de commentaires (en anglais *Request For Comments*). Les RFC sont une série numérotée de documents publiés par la Société Internet pour documenter les idées et concepts liés aux technologies de l'Internet. Pas tous les RFC ne sont des normes. Les RFC peuvent être consultées en ligne sur *http://rfc.net/*

Sinon, le résultat est "0". Voici tous les résultats possibles résultant de la comparaison binaire de deux bits.

Bit 1	Bit 2	Résultats
0	0	0
0	1	0
1	0	0
1	1	1

Pour comprendre comment un masque de réseau est appliqué à une adresse IP, if faut d'abord convertir tout en binaire. Le masque réseau 255.255.255.0 en binaire contient vingt-quatre bits de valeur "1" :

```
255       255       255       0

11111111.11111111.11111111.00000000
```

Lorsque ce masque réseau est combiné avec l'adresse IP 10.10.10.10, nous pouvons appliquer un ET logique à chacun des bits pour déterminer l'adresse réseau.

```
   10.10.10.10: 00001010.00001010.00001010.00001010
 255.255.255.0: 11111111.11111111.11111111.00000000
                ----------------------------------
    10.10.10.0: 00001010.00001010.00001010.00000000
```

Il en résulte le réseau 10.10.10.0/24. Ce réseau est constitué des hôtes 10.10.10.1 à 10.10.10.254, avec 10.10.10.0 comme adresse réseau et 10.10.10.255 comme adresse de diffusion. Les masques de sous réseau ne se limitent pas à des octets entiers. On peut également préciser des masques de sous réseau comme 255.254.0.0 (ou /15 CIDR). Il s'agit d'un grand bloc, contenant 131.072 adresses, allant de 10.0.0.0 à 10.1.255.255. Il pourrait encore être subdivisé, par exemple, en 512 sous-réseaux de 256 adresses chacun. Le premier serait 10.0.0.0-10.0.0.255, puis 10.0.1.0-10.0.1.255, et ainsi de suite jusqu'à 10.1.255.0-10.1.255.255. Sinon, il pourrait être divisé en 2 blocs de 65536 adresses, ou 8192 blocs de 16 adresses, ou dans bien d'autres façons. Il pourrait même être subdivisé en un mélange de différentes tailles de blocs, aussi longtemps qu'aucun d'entre eux ne se chevauchent, et chacun est une valeur de sous réseau dont la taille est une puissance de deux.

Alors que de nombreux netmasks sont possibles, les netmasks communément utilisés sont:

CIDR	Décimales	# des hôtes
/30	255.255.255.252	4
/29	255.255.255.248	8
/28	255.255.255.240	16
/27	255.255.255.224	32
/26	255.255.255.192	64
/25	255.255.255.128	128
/24	255.255.255.0	256
/16	255.255.0.0	65 536
/8	255.0.0.0	16 777 216

Avec chaque réduction de la valeur CIDR, l'espace d'adressage est doublé. Souvenez vous que deux adresses IP au sein de chaque réseau sont toujours réservées pour l'adresse réseau et l'adresse de diffusion.

Il existe trois netmasks qui ont des noms spéciaux. Un réseau /8 (avec un masque de réseau de 255.0.0.0) définit un réseau de **Classe A**. Un réseau /16 (255.255.0.0) est de **Classe B**, et un réseau /24 (255.255.255.0) est appelé de **Classe C**. Ces noms ont existé bien avant la notation CIDR, mais sont encore souvent utilisées pour des raisons historiques.

Adresses IP globales

Vous étés-vous déjà demandé qui contrôle la répartition de l'espace IP? Les ***adresses IP routables globalement*** sont attribuées et distribuées par les ***Regional Internet Registrars*** (***RIR***) aux fournisseurs d'accès. Les fournisseurs de services Internet alors allouent des plus petits blocs IP à leurs clients selon leurs exigences. Presque tous les utilisateurs d'Internet obtiennent leurs adresses IP d'un fournisseur de services Internet.

Les 4 milliards d'adresses IP disponibles sont administrés par l'***Internet Assigned Numbers Authority*** (***IANA***, *http://www.iana.org/*). L'IANA a divisé ce grand espace en sous-réseaux, généralement des sous-réseaux /8 avec 16 millions d'adresses chacun. Ces sous-réseaux sont déléguées à l'un des cinq regional Internet registrars (RIRs), qui ont l'autorité sur de vastes régions géographiques.

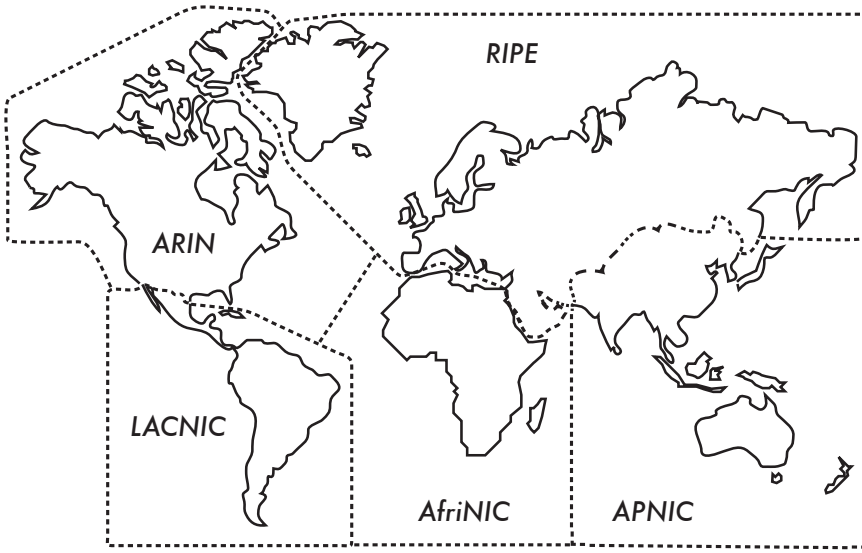


Figure 3.4: L'autorité pour les assignations d'adresse IP est déléguée aux cinq Regional Internet Registrars.

Les cinq RIR sont:

- African Network Information Centre (AfriNIC, *http://www.afrinic.net/*)
- Asia Pacific Network Information Centre (APNIC, *http://www.apnic.net/*)
- American Registry for Internet Numbers (ARIN, *http://www.arin.net/*)
- Regional Latin-American and Caribbean IP Address Registry (LACNIC, *http://www.lacnic.net/*)
- Réseaux IP européens (RIPE NCC, *http://www.ripe.net/*)

Votre fournisseur de services Internet vous allouera un espace d'adresse IP routable globalement à partir du pool d'adresses qui lui a été alloué par votre RIR. Le système de registre garantit que les adresses IP ne sont pas réutilisées dans n'importe quelle partie du réseau n'importe où dans le monde.

Une fois qu'un accord a été trouvé sur l'assignation d'adresses IP, il est possible de passer des paquets entre les réseaux et participer au réseau Internet. Le processus de passer les paquets entre les réseaux est appelé ***routage***.

Les adresses IP statiques

Une adresse IP statique est une assignation d'adresse qui ne change jamais. Les adresses IP statiques sont importantes car les serveurs utilisant ces adresses peuvent avoirs des mappages DNS pointant vers ces serveurs et généralement servir l'information a d'autres machines (tels que les services de messagerie, les serveurs Web, etc.)

Des blocs d'adresse IP statique peuvent être attribués par votre fournisseur de services Internet, soit sur demande ou automatiquement selon vos moyens de connexion à l'Internet.

Adresses IP dynamiques

Les adresses IP dynamique sont attribuées par un fournisseur de services Internet pour les nœuds non permanents connectant à l'Internet, comme un ordinateur à la maison qui utilise une connexion dial-up.

Les adresses IP dynamiques peuvent être attribuées automatiquement à l'aide des protocoles ***Dynamic Host Configuration Protocol*** (***DHCP***), ou ***Point-to-Point Protocol*** (***PPP***), selon le type de connexion Internet. Un noeud utilisant le protocole DHCP commence par demander du réseau une allocation d'adresse IP, et automatiquement configure son interface réseau. Les adresses IP peuvent être assignées au hasard à partir d'un pool d'adresses par votre fournisseur de services Internet, ou pourraient être attribuées en fonction d'une politique. Les adresses IP attribuées par DHCP sont valables pour un temps déterminé (appelé ***temps de location*** ou en anglais *lease time*). Le noeud doit renouveler le bail DHCP avant l'expiration du temps d'allocation. Au moment du renouvellement, le noeud peut recevoir la même adresse IP ou une autre à partir du pool d'adresses disponibles.

Les adresses dynamiques sont populaires auprès des fournisseurs de services Internet car elles leur permettent d'utiliser moins d'adresses IP que le nombre total de leurs clients. Ils ont seulement besoin d'une adresse pour chaque client qui est actif à n'importe quel moment. Les adresses IP globalement routables coûtent de l'argent, et certaines autorités spécialisées dans l'attribution des adresses (comme le RIPE, le RIR) sont très strictes sur l'usage d'adresses IP par les fournisseurs d'accès. L'allocation dynamique d'adresses permet aux fournisseurs d'accès Internet d'économiser de l'argent, et ils chargent souvent un extra à leurs clients pour une adresse IP statique.

Adresses IP privées

La plupart des réseaux privés ne nécessitent pas l'attribution d'adresses IP publiques routables globalement pour chaque ordinateur dans l'organisation. En particulier, les ordinateurs qui ne sont pas des serveurs publiques n'ont pas besoin d'être adressable à travers le réseau Internet. Pour les machines dans un réseau interne, les organisations utilisent généralement des adresses IP provenant d'un ***espace d'adressage privé***.

Il existe actuellement trois blocs d'espace d'adressage privé réservés par l'IANA: 10.0.0.0 /8, 172.16.0.0/12, et 192.168.0.0/16. Ceux-ci sont définis dans le RFC1918. Ces adresses ne sont pas destinés à être routées sur l'Internet et sont généralement uniques seulement au sein d'un organisme ou groupe d'organismes qui ont choisi de suivre le même schéma de numérotation.

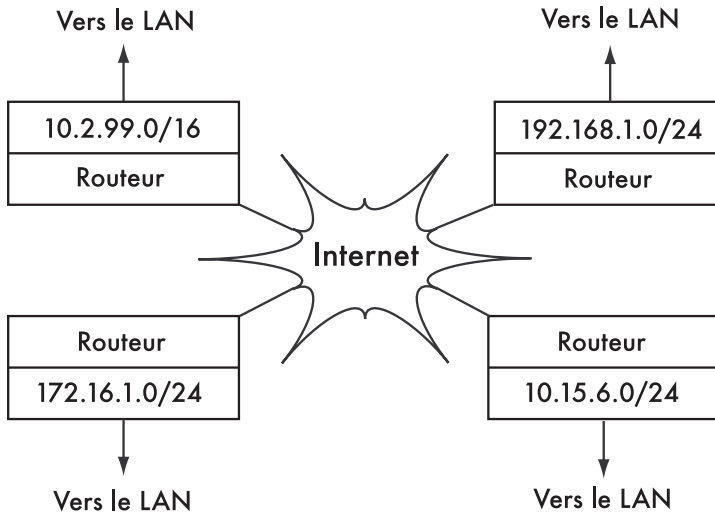


Figure 3.5: Les adresses privées RFC1918 peuvent être utilisées au sein d'un organisme, et ne sont pas routées sur le réseau Internet.

Si vous avez l'intention de relier entre eux des réseaux privés qui utilisent un espace d'adressage RFC1918, assurez-vous d'utiliser des adresses uniques à travers tous les réseaux. Par exemple, vous pouvez diviser l'espace d'adressage 10.0.0.0 /8 en des multiples réseaux de classe B (10.1.0.0/16, 10.2.0.0/16, etc.) ou des blocs d'une autre taille. Un bloc peut-être aussi assigné à un réseau en fonction de son emplacement physique (la branche principale du campus, les bureaux extérieurs un, les bureaux extérieurs deux, dortoirs, etc.). Le réseau des administrateurs à chaque emplacement peut alors diviser le réseau en plusieurs réseaux de classe C (10.1.1.0/24, 10.1.2.0/24, etc.) ou en blocs de toute autre taille logique. Dans l'avenir, si les réseaux devraient jamais être connectés (soit par une connexion physique, liaison sans fil, ou VPN), alors toutes les machines seront accessibles à partir de n'importe quel point du réseau sans avoir à renuméroter les périphériques réseau.

Certains fournisseurs d'accès à l'Internet peuvent allouer des adresses privées comme celles-ci au lieu des adresses publiques à leurs clients, bien que cela a de graves désavantages. Étant donné que ces adresses ne peuvent pas être routés sur l'Internet, les ordinateurs qui les utilisent ne sont pas vraiment "partie" de l'Internet, et ne sont pas directement accessible à partir de l'Internet. Afin de leur permettre de communiquer avec l'Internet, leur adresse personnelle doit être traduite en adresse publique. Ce processus de translation d'adresses est connu sous le nom de ***Network Address Translation*** (***NAT***), et est normalement executé au niveau de la passerelle entre le réseau privé et l'Internet. Nous verrons plus de détails sur le NAT à la **Page 44**.

Routage

Imaginez un réseau avec trois hôtes: A, B et C. Ils utilisent les adresses IP respectives 192.168.1.1, 192.168.1.2 et 192.168.1.3. Ces hôtes font partie d'un réseau /24 (leur masque de réseau est 255.255.255.0).

Pour que les deux hôtes communiquent sur un réseau local, chacun de ces hôtes doit déterminer l'adresse MAC de l'autre. Il est possible de configurer manuellement chaque hôte avec une table de correspondance entre l'adresse IP et l'adresse MAC, mais normalement le ***protocole de résolution d'adresses*** (en anglais ***ARP***, *Address Resolution Protocol*) est utilisé pour le déterminer automatiquement.

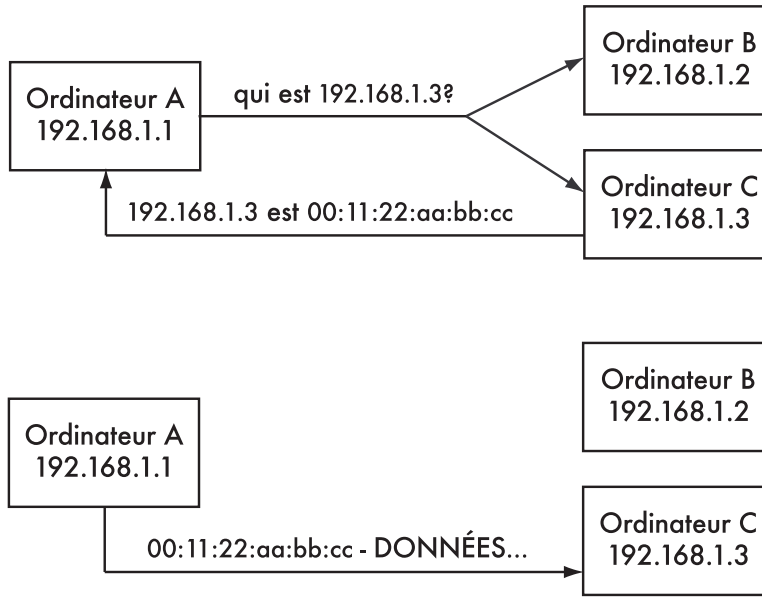


Figure 3.6: Un ordinateur doit envoyer des données à 192.168.1.3. Mais il doit d'abord demander au réseau l'adresse MAC qui correspond à 192.168.1.3.

Lorsque vous utilisez ARP, Un hôte A diffuse à tous les hôtes la question "Qui a l'adresse MAC pour l'adresse IP 192.168.1.3?". Quand l'hôte C voit une requête ARP pour son propre adresse IP, il répond avec son adresse MAC.

Considérons maintenant un autre réseau avec 3 hôtes, D, E et F, avec les adresses IP respectives 192.168.2.1, 192.168.2.2 et 192.168.2.3. Il s'agit d'un autre réseau /24, mais il n'est pas dans la même gamme que le réseau ci-dessus. Les trois hôtes peuvent atteindre directement les uns les autres (en utilisant ARP pour résoudre l'adresse IP dans une adresse MAC et envoyer des paquets à cette adresse MAC).

Maintenant, nous allons ajouter une machine hôte G. Cette machine possède deux cartes réseau, avec une carte branchée dans chaque réseau. La première carte réseau emploie l'adresse IP 192.168.1.4, et l'autre utilise 192.168.2.4. L'hôte G est maintenant liaison locale à deux réseaux, et peut router les paquets entre eux.

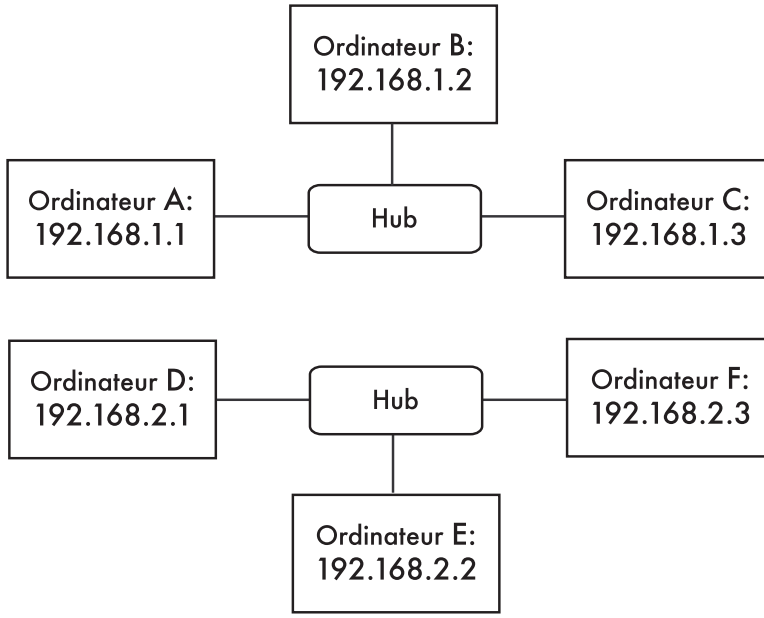


Figure 3.7: Deux réseaux IP différents

Mais que faire si les hôtes A, B, C veulent atteindre D, E et F? Ils auront besoin d'ajouter une route à l'autre réseau via le réseau hôte G. Par exemple, les hôtes A-C ajouteront un itinéraire par le biais de 192.168.1.4. Sous Linux, cela peut être accompli avec la commande suivante:

```
# ip route add 192.168.2.0/24 via 192.168.1.4
```

... et les hôtes D-F ajouteraient le texte suivant:

```
# ip route add 192.168.1.0/24 via 192.168.2.4
```

Le résultat est présenté dans la **Figure 3.8**. Notez que la route est ajoutée par l'intermédiaire de l'adresse IP sur l'hôte G qui est liaison locale aux réseaux respectifs. L'hôte A ne peut pas ajouter une route via 192.168.2.4 même si c'est la même machine physique que 192.168.1.4 (hôte G), car cette adresse IP n'est pas liaison locale.

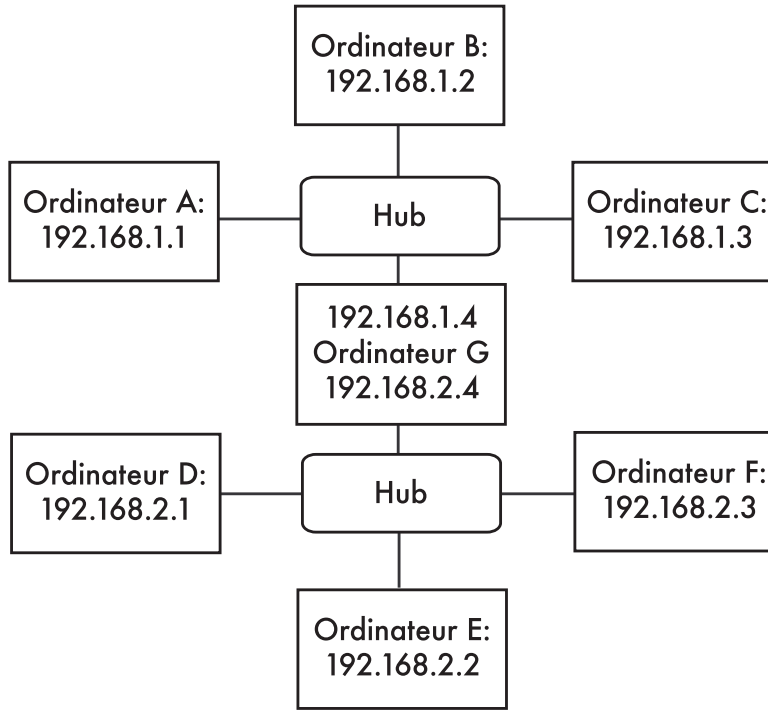
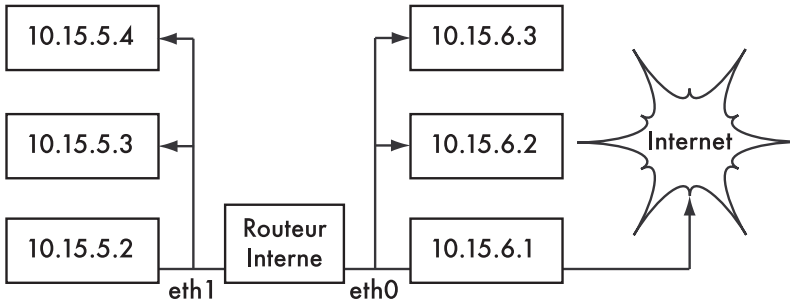


Figure 3.8: l'hôte G agit comme un routeur entre les deux réseaux.

Une route informe le système d'exploitation que le réseau désiré ne ment pas concernant le réseau liaison locale immédiat, et il doit ***acheminer*** le trafic à travers le routeur spécifié. Si l'hôte A veut envoyer un paquet à l'hôte F, il devrait d'abord l'envoyer à G. L'hôte G cherchera alors l'hôte F dans sa table de routage afin de voir s'il a une connexion directe au réseau de l'hôte F. Enfin, l'hôte G résoudra l'adresse matérielle (MAC) de l'hôte F et lui fera suivre le paquet.

Il s'agit là d'un simple exemple de routage où la destination est à un seul ***hop*** de la source. Quand les réseaux deviennent plus complexes, beaucoup de hops devront être traversés pour atteindre la destination finale. Comme il n'est pas pratique pour chaque machine sur l'Internet de connaître la route vers toutes les autres machines, nous ferons usage d'une entrée de routage connue sous le nom de la ***route par défaut*** (en anglais, *default route*) (aussi connu sous le nom de ***passerelle par défaut*** ou en anglais *default gateway*). Quand un routeur reçoit un paquet destiné à un réseau pour lequel il n'a pas de route explicite, le paquet est transmis à la passerelle par défaut.

La passerelle par défaut est typiquement le meilleur moyen de sortir de votre réseau, généralement en direction de votre fournisseur de services Internet. Un exemple d'un routeur utilisant une passerelle par défaut est illustré à la **Figure 3.9**.




```
Table de routage pour l'routeur intérieur:

Destination     Gateway      Genmask         Flags  Metric  Iface
10.15.5.0        *            255.255.255.0  U       0       eth1
10.15.6.0        *            255.255.255.0  U       0       eth0
default          10.15.6.1    0.0.0.0        UG      0       eth0
```

Figure 3.9: En l'absence de route explicite vers une destination particulière, un hôte utilise l'entrée de la passerelle par défaut dans sa table de routage.

Les routes peuvent être mises à jour manuellement, ou peuvent réagir dynamiquement aux pannes réseaux ou autres événements. Quelques exemples populaires de protocoles de routage dynamique sont RIP, OSPF, BGP, et OLSR. La configuration du routage dynamique est au-delà du champ d'application de ce livre, mais pour en savoir plus sur le sujet, voir les ressources à l'**annexe A**.

Network Address Translation (NAT)

En vue d'atteindre les hôtes sur l'Internet, les adresses RFC1918 doivent être converties en adresses IP globales publiquement routables. Ceci se fait au moyen d'une technique connue sous le nom de ***Network Address Translation*** ou ***NAT***. Un périphérique NAT est un routeur qui manipule les adresses des paquets au lieu de les acheminer simplement. Sur un routeur NAT, la connexion Internet, utilise une (ou plusieurs) adresses IP globalement routables alors que le réseau privé emploie une adresse IP venant de la gamme d'adresses privées RFC1918. Le routeur NAT permet à l'adresse globalement routable d'être partagée parmi tous les utilisateurs internes, qui tous utilisent des adresses privées. Il convertit les paquets d'une forme d'adressage à l'autre lorsque les paquets le traverse. Pour les utilisateurs du réseau, ils peuvent dire qu'ils sont directement connectés à l'Internet et ne nécessitent aucun logiciel spécial ou des pilotes. Ils utilisent simplement le routeur NAT comme leur passerelle par défaut, et adressent les paquets de la même façon. Le routeur NAT traduit les paquets sortants pour utiliser l'adresse IP globale quand ils quittent le réseau et les traduit de nouveau quand ils sont reçus à partir de l'Internet.

La conséquence majeure de l'utilisation de NAT est que les machines qui sont dans le réseau Internet ne peuvent pas accéder facilement à des serveurs au sein de l'organisme sans la mise en place des règles d'acheminement (forwarding) explicites sur le routeur. Les connexions émanant de l'espace d'adressage privé de l'organisation n'ont, en général, aucune difficulté, bien que

certaines applications (comme la Voix sur IP et certains logiciels VPN) peuvent avoir du mal à être gérées par le NAT.

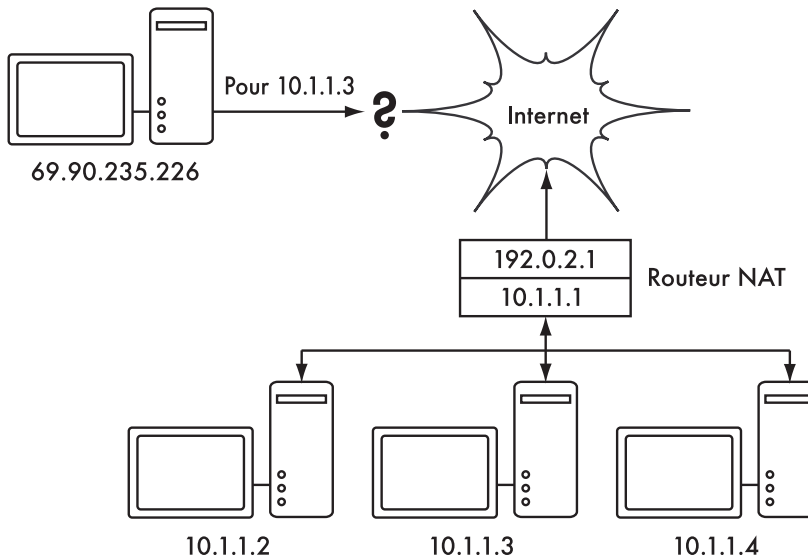


Figure 3.10: Le Network Address Translation vous permet de partager une adresse IP unique avec de nombreux hôtes internes, mais peut rendre certains services difficile à fonctionner correctement.

Selon votre point de vue, cela peut être considéré comme un bug (car cela rend plus difficile la mise en place d'une communication à double sens) ou une fonctionnalité (car cela fournit effectivement un pare-feu "libre" pour l'ensemble de votre organisation). Les adresses RFC1918 devraient être filtrées à la périphérie de votre réseau pour éviter le trafic RFC1918 accidentel ou malicieux entrant ou sortant de votre réseau. Bien que le NAT exécute certaines fonctions pare-feu, il n'est pas un remplacement d'un véritable pare-feu.

Suite de protocoles Internet

Les machines sur l'Internet utilisent le protocole Internet (IP) pour atteindre les uns avec les autres, même lorsque séparés par des nombreuses machines. Il existe un certain nombre de protocoles qui sont exécutés en liaison avec IP qui offrent des caractéristiques d'une importance critique pour l'opération du protocole IP lui-même. Chaque paquet spécifie un numéro de protocole qui identifie le paquet comme l'un de ces protocoles. Les protocoles les plus communément utilisés sont ***Transmission Control Protocol*** (***TCP***, numéro 6), ***User Datagram Protocol*** (***UDP***, le nombre 17), et ***Internet Control Message Protocol*** (***ICMP***, numéro 1). Pris en tant que groupe, ces protocoles (et autres) sont connus sous le nom de ***suite de protocoles Internet*** (en anglais *Internet Protocol Suite*), ou tout simplement ***TCP/IP***.

Les protocoles TCP et UDP introduisent le concept de numéros de port. Les numéros de port permettent à plusieurs services à être exécutés sur la même adresse IP, tout en étant distingués les uns des autres. Chaque paquet a un numéro de port source et destination. Certains numéros de port sont des normes

bien définies utilisées pour atteindre des services bien connus tels que le courrier électronique et les serveurs web. Par exemple, les serveurs web normalement ***écoutent*** sur le port TCP 80, et les serveurs de messagerie SMTP écoutent sur le port TCP 25. Quand nous disons qu'un service "écoute" sur un port (comme le port 80), cela signifie qu'il va accepter les paquets qui utilisent son IP comme adresse IP de destination et 80 comme port de destination. Habituellement les serveurs ne se soucient pas de l'adresse IP source ou le port source, même si parfois ils les utilisent pour établir l'identité de l'autre côté. Lors de l'envoi d'une réponse à de tels paquets, le serveur va utiliser sa propre adresse comme adresse IP source et 80 comme port source.

Quand un client se connecte à un service, il peut faire usage de n'importe quelle numéro de port source qui n'est pas déjà en service de son côté, mais il doit se connecter au bon port sur le serveur (par exemple, 80 pour Web, 25 pour le courrier électronique). TCP est un protocole ***orienté session*** avec des fonctionnalités de garantie de livraison et de transmission (telles que la détection - la mitigation de la congestion du réseau, les retransmissions, la réorganisation des paquets et leur réassemblage, etc.) UDP est conçu pour les flux de trafic orienté ***sans connexion***, et ne garantit pas la livraison du tout, ou dans un ordre particulier.

Le protocole ICMP est conçu pour le débogage et la maintenance de l'Internet. A la place des numéros de port, il a des ***types de messages***, qui sont aussi des nombres. Des types différents de messages sont utilisés pour demander une réponse simple à partir d'une autre ordinateur (echo request), informer l'expéditeur d'un autre paquet d'une éventuelle boucle de routage (temps dépassé), ou informer l'expéditeur d'un paquet qui ne pouvait pas être livré en raison de règles de pare-feu ou d'autres problèmes (destination inaccessible).

A présent, vous devez disposer d'une solide compréhension de l'adressage des ordinateurs sur le réseau et comment les flux d'information circule sur le réseau entre ces ordinateurs. Maintenant, nous allons avoir un bref aperçu sur la physique du matériel qui implémente ces protocoles réseau.

Ethernet

Ethernet est le nom du standard le plus populaire pour connecter ensemble les ordinateurs sur un ***réseau local*** (***LAN***). Il est parfois utilisé pour connecter les ordinateurs individuels à l'Internet, via un routeur, un modem ADSL, ou un périphérique sans fil. Toutefois, si vous connectez un seul ordinateur à Internet, vous pouvez ne pas utiliser Ethernet du tout. Le nom vient du concept physique d'éther, le support qui était une fois censé transporter les ondes lumineuses à travers l'espace libre. La norme officielle est appelée IEEE 802.3.

Le standard Ethernet le plus commun est appelé 100baseT. Il définit un débit de données avec un taux de 100 mégabits par seconde, exécutant sur des fils à paire torsadée avec des connecteurs de type MODULAR RJ-45 à l'extrémité. La topologie du réseau est en étoile, avec des commutateurs ou des hubs au centre de chaque étoile, et des noeuds terminaux (dispositifs et commutateurs supplémentaires) sur la périphérie.

Les adresses MAC

Chaque dispositif connecté à un réseau Ethernet a une adresse MAC unique, attribuée par le fabricant de la carte réseau. Sa fonction est comme celle d'une adresse IP, car elle sert d'identifiant unique qui permet aux dispositifs de parler les uns aux autres. Toutefois, la portée d'une adresse MAC est limitée à un domaine de diffusion, qui est définie comme tous les ordinateurs connectés entre eux par des câbles, les hubs, commutateurs, et les bridges, mais ne traversant pas des routeurs ou passerelles Internet. Les adresses MAC ne sont jamais utilisées directement sur l'Internet, et ne sont pas transmises à travers les routeurs.

Hubs

Les ***hubs*** Ethernet connectent plusieurs dispositifs Ethernet à paire torsadée ensemble. Ils fonctionnent sur la couche physique (la plus basse ou la première couche). Ils répètent les signaux reçus par chaque port sur tous les autres ports. Les Hubs peuvent donc être considérés comme des simples répétiteurs. Grâce à cette conception, un seul port peut transmettre à la fois avec succès. Si deux dispositifs transmettent en même temps, ils corrompent les transmissions des uns et des autres , et les deux doivent reculer et retransmettre leurs paquets plus tard. C'est ce qu'on appelle une ***collision***, et chaque hôte reste responsable pour détecter les collisions lors de la transmission, et retransmettre ses propres paquets en cas de besoin.

Lorsque des problèmes tels que les collisions excessives sont décelées sur un port, certains hubs peuvent déconnecter (***partition***) ce port pendant un certain temps pour limiter son impact sur le reste du réseau. Pendant qu'un port est partitionné, les dispositifs qui s'y rattachent ne peuvent pas communiquer avec le reste du réseau. Les réseaux a base de hub sont généralement plus robustes que les réseaux Ethernet coaxial (également connu sous le nom de 10base2 ou ThinNet), où des dispositifs fonctionnant mal peuvent désactiver l'ensemble du segment. Mais les hubs sont limités dans leur utilité, car ils peuvent facilement devenir des points de congestion sur les réseaux occupés.

Commutateurs ou switches

Un ***commutateur*** est un appareil qui fonctionne un peu comme un hub, mais fournit une connexion dédiée (ou ***commutée***) entre les ports. Plutôt que de répéter tout le trafic sur chaque port, le commutateur détermine quels sont les ports qui communiquent directement et les connectent temporairement. Les commutateurs fournissent généralement des performances beaucoup meilleures que les hubs, en particulier sur les réseaux occupés avec beaucoup d'ordinateurs. Ils ne sont pas beaucoup plus cher que les hubs, et sont en train de les remplacer dans de nombreuses situations.

Les commutateurs fonctionnent sur la couche liaison de données (la deuxième couche), car ils interprètent et agissent sur l'adresse MAC des paquets qu'ils reçoivent. Quand un paquet arrive à un port sur un commutateur, le commutateur prend note de l'adresse MAC de la source, qu'il associe a ce port. Il stocke ces informations dans une table MAC interne. Le commutateur examine ensuite l'adresse MAC de la destination dans sa table MAC et transmet le paquet sur le port

correspondant. Si l'adresse MAC de destination ne se trouve pas dans la ***table MAC***, le paquet est alors envoyé à tous les interfaces connectées. Si le port de destination correspond au source port, le paquet est filtré et n'est pas transmis.

Hubs et Commutateurs

Les hubs sont considérés comme des dispositifs peu sophistiqués, car ils rediffusent l'ensemble du trafic sur chaque port inefficacement. Cette simplicité introduit à la fois une pénalité de performance et un problème de sécurité. La performance d'ensemble est plus faible car la bande passante disponible doit être partagée entre tous les ports. Étant donné que tout le trafic est vu par tous les ports, tous les hôtes sur le réseau peuvent facilement contrôler tout le trafic réseau.

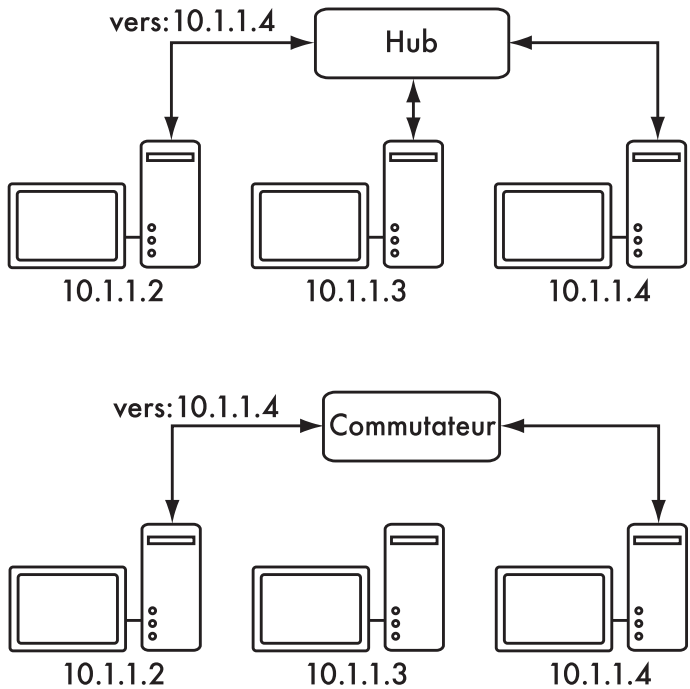


Figure 3.11: Un hub simplement répète tout le trafic sur chaque port, alors qu'un commutateur crée une connexion temporaire dédiée entre les ports qui ont besoin de communiquer.

Les commutateurs créent des connexions virtuelles entre les ports de réception et de transmission.

Il en résulte de meilleures performances parce que de nombreuses connexions virtuelles peuvent être établies en même temps. Les commutateurs plus coûteux peuvent commuter le trafic tout en inspectant le trafic à des niveaux plus hauts (à la couche transport ou application), permettre la création de réseaux locaux virtuels, et implémenter d'autres fonctions avancées.

Un hub peut être utilisé lorsque la répétition du trafic sur tous les ports est souhaitable, par exemple, lorsque vous voulez permettre explicitement une machine de surveillance à voir tout le trafic sur le réseau. La plupart des

commutateurs fournissent la fonctionnalité ***port moniteur*** qui permet de répéter sur un port affecté spécifiquement à cette fin.

Les Hubs furent une fois moins chers que les commutateurs. Toutefois, le prix de commutateurs a chuté de façon spectaculaire au cours des années. Par conséquent, les hubs anciens devraient être remplacés, des que possible, par des nouveaux commutateurs.

Les hubs et les commutateurs peuvent offrir des services ***gérés***. Certains de ces services incluent notamment la possibilité de fixer la vitesse de la connexion (10baseT, 100baseT, 1000BaseT, complète ou demi-duplex) par port, le déclenchement des triggers (ou déclencheurs) pour la surveillance des événements réseau (par exemple les changements dans l'adresse MAC et les paquets malformés), et d'habitude incluent de ***compteurs de port*** pour faciliter la comptabilité de la bande passante. Un commutateur géré qui offre des possibilités de télécharger en amont ou en aval des compteurs des bytes sur chaque port physique peut grandement simplifier la surveillance réseau. Ces services sont généralement disponibles via SNMP, ou ils peuvent être accessibles via telnet, ssh, une interface web, ou un outil de configuration personnalisée.

Routeurs et pare-feux

Alors que les hubs et les commutateurs fournissent une connectivité sur un segment de réseau local, le travail d'un routeur est de transmettre les paquets entre les différents segments de réseau. Un routeur a généralement deux ou plusieurs interfaces réseau physique. Il peut supporter différents types de médias, tels que Ethernet, ATM, DSL, ou dial-up. Les routeurs peuvent être des périphériques matériels dédiés (tels que les routeurs Cisco ou Juniper) ou ils peuvent être construits à partir d'un PC standard avec plusieurs interfaces réseau, des cartes et des logiciels appropriés.

Les routeurs sont localisés à la ***périphérie*** de deux ou plusieurs réseaux. Par définition, ils ont une connexion sur chaque réseau, et en tant que machines périphériques peuvent prendre d'autres responsabilités en plus du routage. Beaucoup des routeurs ont des fonctionnalités ***pare-feu*** qui fournissent un mécanisme de filtre ou de réorienter les paquets qui ne correspondent pas à la sécurité ou les exigences de la politique d'accès. Ils peuvent également fournir des services de translation d'adresses (NAT, Network Adress Translation).

Les routeurs varient largement en coût et capacités. Les moins coûteux et moins flexibles sont des dispositifs matériels dédiés souvent avec des fonctionnalités NAT, utilisés pour partager une connexion Internet entre quelques ordinateurs. La seconde gamme supérieure consiste en un routeur logiciel ayant un système d'exploitation exécutant sur un PC standard avec de multiples interfaces réseau. Des systèmes d'exploitation standard tels que Microsoft Windows, Linux et BSD sont tous capables de routage et sont beaucoup plus souples que les périphériques matériels à faible coût. Cependant, ils souffrent des mêmes problèmes que les ordinateurs classiques, avec de forte consommation de puissance, un grand nombre de pièces complexes et potentiellement peu fiables, et à très intense configuration.

Les dispositifs les plus coûteux sont des routeurs matériels haut de gamme dédiés, construits par des sociétés comme Cisco et Juniper. Ils ont tendance à avoir des meilleures performances, plus de fonctionnalités, et sont plus fiables

que les routeurs logiciels sur des PC. Il est aussi possible de prendre des contrats d'appui technique et de maintenance pour ces routeurs.

La plupart des routeurs modernes offrent des mécanismes pour surveiller et enregistrer les performances à distance, généralement via le Simple Network Management Protocol (SNMP) même si les dispositifs les moins chers souvent omettent cette fonctionnalité.

Autre équipement

Chaque réseau physique a une pièce d'équipement terminal associée. Par exemple, les connexions VSAT sont composées d'une antenne connectée à un terminal qui, soit se branche sur une carte dans un PC, ou se termine à une connexion Ethernet normale. Les lignes DSL utilisent un ***modem DSL*** qui fait le pont entre la ligne téléphonique et un périphérique local, soit un réseau Ethernet ou un seul ordinateur via USB. Les ***modems câbles*** font le pont entre la télévision et le câble Ethernet, ou un bus d'une carte PC interne. Certains types de circuit de télécommunication (par exemple un T1 ou T3) utilisent un CSU/DSU pour faire le pont entre le circuit et un port série ou Ethernet. Les lignes dial-up standard utilisent les modems pour connecter un ordinateur au téléphone, généralement par le biais d'une carte plug-in ou un port série. Et il existe différents types d'équipements de réseau sans fil qui connectent à une variété de radios et antennes, mais presque toujours aboutissent à un jack Ethernet.

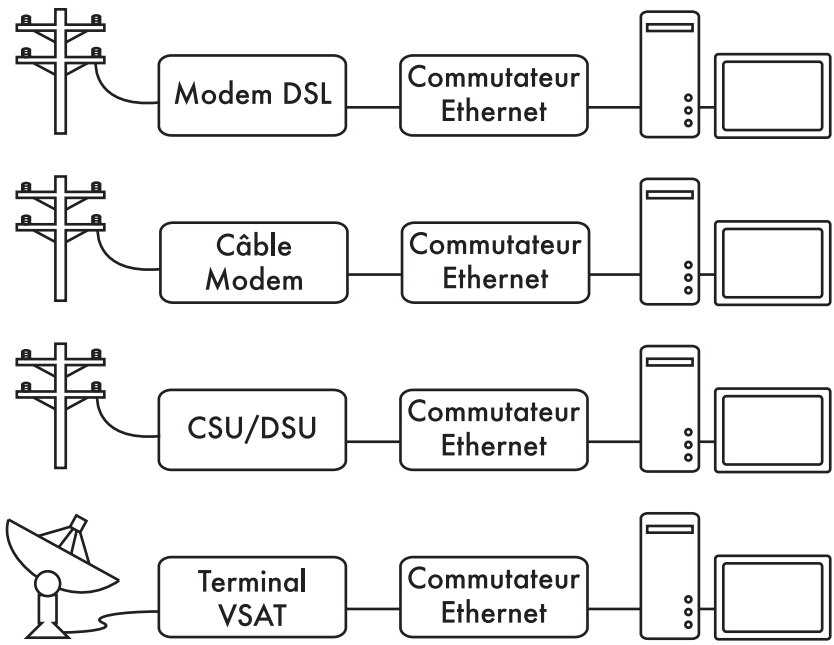


Figure 3.12: De nombreux modems ADSL, les modems câble, CSU/UAD, points d'accès sans fil, et terminaux VSAT aboutissant à un jack de réseau Ethernet.

La fonctionnalité de ces dispositifs peut varier considérablement entre fabricants. Certains fournissent des mécanismes de contrôle des performances,

alors que d'autres peuvent ne pas le prévoir. Comme en fin de compte votre connexion Internet vient de votre fournisseur de services Internet, vous devriez suivre leurs recommandations au moment de choisir l'équipement qui relie leur réseau à votre réseau Ethernet.

Assembler les pièces

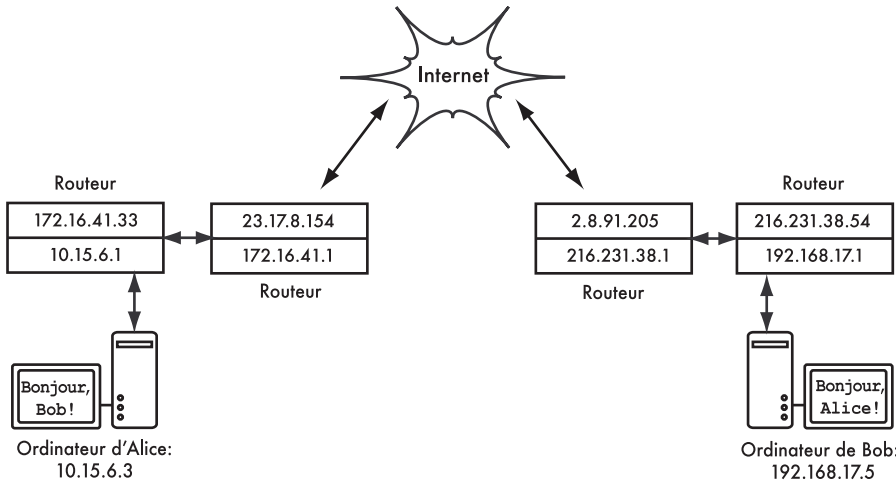


Figure 3.13: Réseautage Internet. Chaque segment de réseau a un routeur avec deux adresses IP, réalisant une «liaison locale» à deux réseaux différents. Les paquets sont expédiés entre les routeurs jusqu'à ce qu'ils atteignent leur destination finale.

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 de l'acheminement, 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 se passe sur l'Internet.

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 tous les 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.

La conception du réseau physique

Lors de la conception des réseaux sans fil, il peut sembler étrange de parler du réseau "physique". Après tout, où est la partie physique du réseau? Dans les réseaux sans fil, le support physique que nous utilisons pour communiquer est de toute évidence l'énergie électromagnétique. Mais dans le contexte de ce

chapitre, le réseau physique se réfère au problème banal de trouver là où mettre les choses. Comment avez-vous arrangé l'équipement afin que vous puissiez atteindre vos clients sans fil? S'ils remplissent les bureaux d'un immeuble ou s'étendent sur plusieurs kilomètres, les réseaux sans fil sont naturellement organisés dans ces trois configurations logiques: liaisons ***point à point***, ***point à multipoints***, et nuées ***multipoints à multipoints***. Bien que différentes parties de votre réseau puissent prendre avantage de toutes ces trois configurations, toute liaison individuelle tombera dans l'une de ces topologies.

Point à point

Généralement, les liaisons ***point à point*** fournissent une connexion Internet là où cet accès n'est pas disponible autrement. Une extrémité d'une liaison point à point disposera d'une connexion Internet, tandis que l'autre utilisera la liaison pour accéder à l'Internet. Par exemple, une université peut avoir un accès rapide à relais de trames ou une connexion VSAT dans le centre de son campus, mais ne peut pas se permettre une telle liaison pour un important bâtiment hors campus. Si le bâtiment principal a une vue claire sur le site distant, une connexion point à point peut être utilisée pour relier les deux sites. Cela peut améliorer ou même remplacer les liaisons par ligne commutée. Avec une bonne antenne et une ligne de visée claire, des liaisons point à point fiables au-delà de trente kilomètres sont possibles.

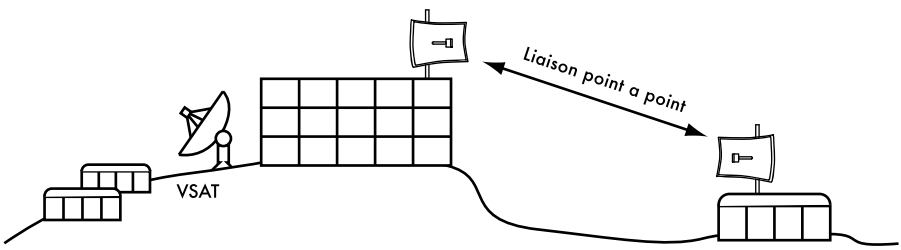


Figure 3.14: Une liaison point à point permet de relier un site distant pour partager une connexion Internet.

Bien sûr, une fois qu'une connexion point à point a été établie, beaucoup plus peut être fait pour étendre le réseau encore plus loin. Si le bâtiment dans notre exemple est au sommet d'une haute colline, il peut être en mesure d'accéder à d'autres endroits importants qui ne peuvent pas être atteints directement à partir du campus central. En installant une autre liaison point à point sur le site distant, un autre noeud peut rejoindre le réseau et faire usage de la connexion Internet centrale.

Les liaisons point à point ne doivent pas nécessairement impliquer un accès à Internet. Supposons que vous avez à vous rendre physiquement à une station distante de surveillance des conditions météorologiques située haut dans les collines afin de recueillir les données qu'elle enregistre au fil du temps. Vous pouvez vous connecter sur le site avec une liaison point à point permettant la collecte de données et la surveillance en temps réel, sans la nécessité de vous rendre sur le site. Les réseaux sans fil peuvent fournir assez de bande passante

pour transporter de grandes quantités de données (y compris audio et vidéo) entre deux points qui sont connectés, même sil n'y a pas de connexion directe à l'Internet.

Point à multipoints

L'autre agencement réseau le plus couramment rencontré est le ***point à multipoints***. Quand plusieurs nœuds communiquent avec un point d'accès central, il s'agit d'une application point à multipoints. Un ***point d'accès sans fil*** offrant une connexion à plusieurs ordinateurs portables est l'exemple typique d'un agencement réseau point à multipoints. Les portables ne communiquent pas les uns avec les autres directement, mais doivent être à portée du point d'accès afin d'utiliser le réseau.

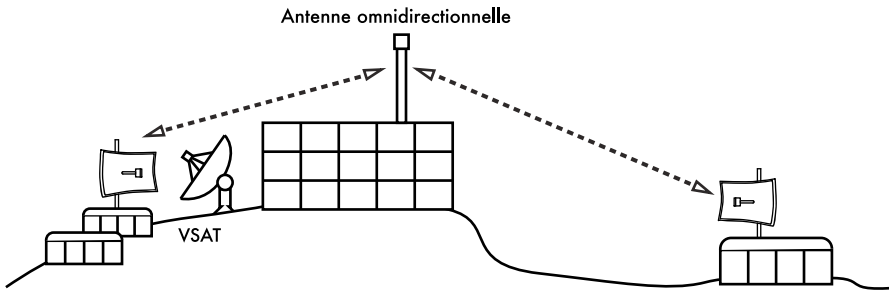


Figure 3.15: Le VSAT est maintenant partagé par de multiples sites distants. Tous les trois sites peuvent aussi communiquer directement à une vitesse beaucoup plus rapide que le VSAT.

La mise en réseau point à multipoints peut également s'appliquer à notre exemple précédent à l'université. Supposons que le bâtiment distant en haut de la colline est relié au campus central par une liaison point à point. Plutôt que de mettre en place plusieurs liaisons point à point pour distribuer la connexion Internet, une seule antenne qui est visible par plusieurs bâtiments à distance peut être utilisée. Ceci est un exemple classique d'une connexion à longue distance ***point*** (site distant sur la colline) ***à multipoints*** (de nombreux bâtiments dans la vallée ci-dessous).

Notez qu'il existe un certain nombre de problèmes de performance associés au point à multipoints sur de très longues distances. Ces problèmes seront traités plus loin dans ce chapitre. Ces liaisons sont possibles et utiles dans de nombreuses circonstances. Mais ne faites pas l'erreur classique d'installer une simple tour radio dans le milieu de la ville et espérer être en mesure de servir des milliers de clients comme vous le feriez avec une station de radio FM. Comme nous allons le voir, les réseaux de données à double sens se comportent très différemment de la radiodiffusion.

Multipoints à multipoints

Le troisième type d'agencement réseau est le ***multipoints à multipoints***, qui s'appelle également réseau ***ad hoc*** ou ***maillé***. Dans un réseau multipoints à

multipoints, il n'y a pas d'autorité centrale. Chaque noeud du réseau transporte le trafic de tous les autres en cas de besoin et tous les noeuds communiquent les uns avec les autres directement.

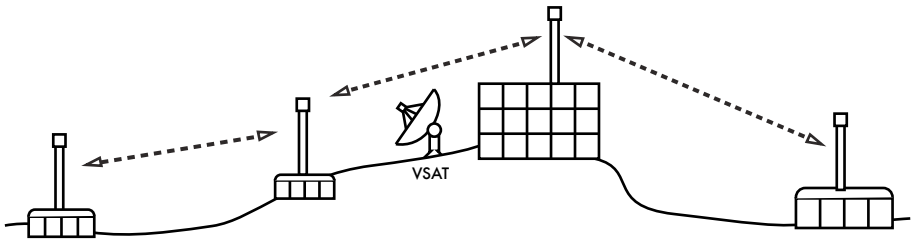


Figure 3.16: Un maillage multipoints à multipoints. Chaque point peut atteindre les autres à très grande vitesse, ou utiliser la connexion VSAT central pour accéder à l'Internet.

Le bénéfice de cet agencement réseau est que, même si aucun des nœuds n'est à portée d'un point d'accès central, les nœuds peuvent encore communiquer les uns avec les autres. Les bonnes implémentations du réseau maillé sont de type autoréparable. Ce qui signifie qu'elles détectent automatiquement les problèmes de routage et les résolvent en cas de besoin. L'extension d'un réseau maillé est aussi simple qu'ajouter des nœuds au réseau existant. Si l'un des noeuds du "nuage" se trouve être une passerelle Internet, alors cette connexion peut être partagée entre tous les clients.

Les deux grands inconvénients de cette topologie sont une complexité accrue et une baisse des performances. La sécurité dans un tel réseau est également un sujet de préoccupation puisque chaque participant porte potentiellement le trafic de tous les autres. Les réseaux multipoints à multipoints ont tendance à être difficile à dépanner en raison du grand nombre de variables qui change avec l'évolution des noeuds rejoignant et quittant le réseau. Les maillages multipoints à multipoints ont généralement une capacité inférieure aux réseaux point à point ou point à multipoints, en raison de la charge additionnelle de gestion du routage réseau et l'augmentation de contention pour les fréquences radioélectriques.

Néanmoins, les réseaux maillés sont utiles dans de nombreuses circonstances. Plus tard dans ce chapitre, nous verrons un exemple de la façon de construire un réseau multipoints à multipoints maillé utilisant un protocole de routage appelé OLSR.

Utiliser la technologie adaptée

Tous ces modèles de réseau peuvent être utilisés pour compléter les uns les autres dans un grand réseau, et peuvent évidemment faire usage des techniques de réseaux câblés traditionnels quand ceci est possible. C'est une pratique courante, par exemple, de recourir à une connexion sans fil à longue distance pour offrir un accès Internet à un endroit éloigné, puis mettre en place un point d'accès sur le site éloigné pour offrir un accès sans fil local. L'un des clients de ce point d'accès peut également jouer le rôle de nœud d'un maillage permettant une propagation organique entre les utilisateurs de portables qui tous, ultimement, utilisent la liaison point à point originale pour accéder à l'Internet.

Maintenant que nous avons une idée claire de la façon dont les réseaux sans fil sont généralement organisés, nous pouvons commencer à comprendre comment la communication est possible sur ces réseaux.

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.

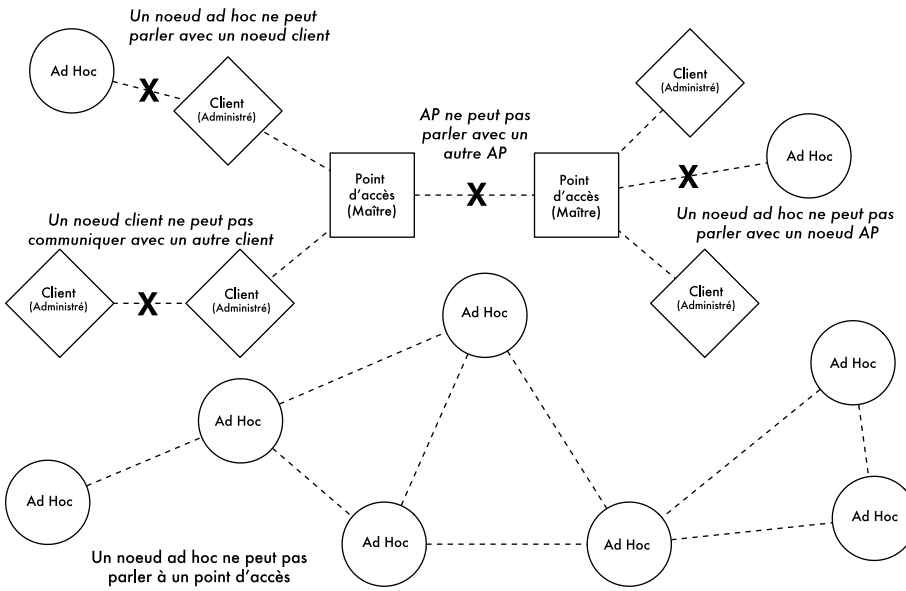


Figure 3.17: AP, Clients et nœuds Ad Hoc.

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 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 portables 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.

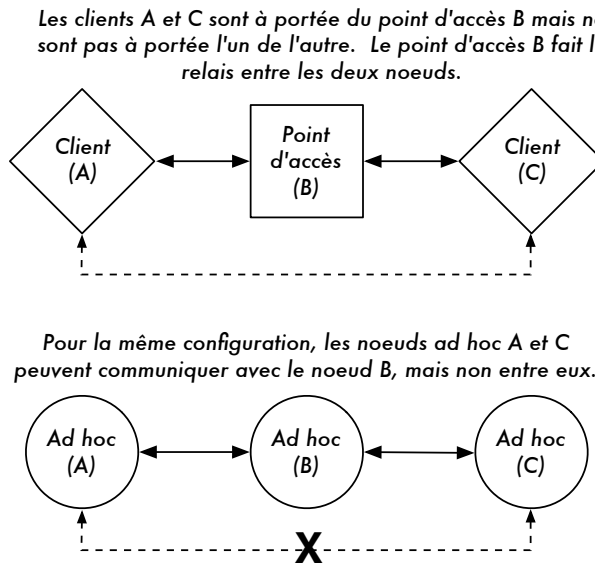


Figure 3.18: Le point d'accès B va transmettre le trafic entre les clients A et C. En mode Ad hoc, le nœud B ne transmettra pas le trafic entre A et C par défaut.

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.

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 Pyramid.

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 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 trouve 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- utilisateur; 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 Pyramid. 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`**.

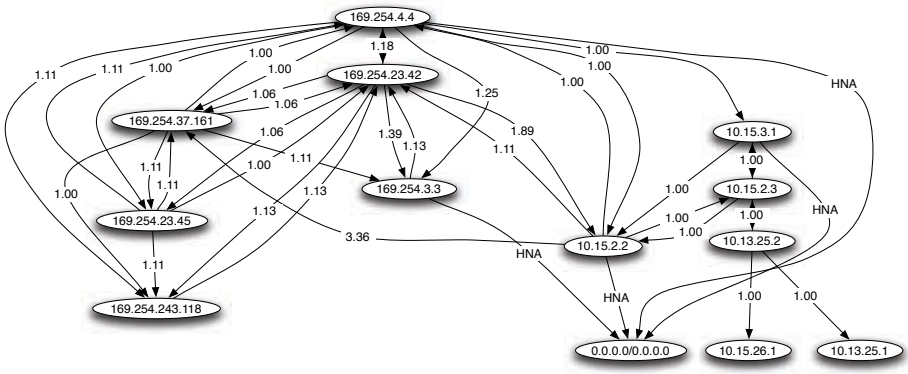


Figure 3.19: Une topologie réseau OLSR automatiquement générée.

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. De 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.

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 rapporte 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 54 Mbps de radio, mais le rendement réel sera de 22 Mbps. 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. 22 Mbps 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 - 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.
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.

Application	Largeur de bande / Usager	Notes
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.
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 5 Mbps 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 5 Mbps ou de plus de largeur de bande dans les **deux directions** avec aucune latence en absolu. Comme l'équipement sans fil 802.11g est ***demi-duplex*** (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 **10 Mbps**. 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 augmente 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:

$$L_{fsl} = 40 + 20*\log(r)$$

Où L_{fsl} ,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 dispersion 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 11 MHz 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.

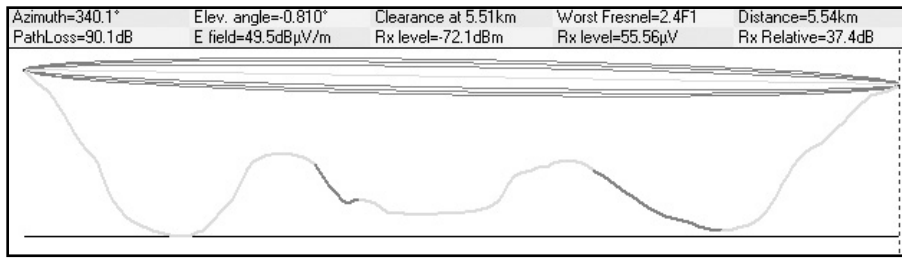


Figure 3.20: Viabilité du lien, incluant la zone Fresnel et une estimation de la ligne de vue, en utilisant RadioMobile.

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 Google Maps) 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 transmetteurs vidéo analogiques, le Bluetooth, les écoute-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 provenant 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.

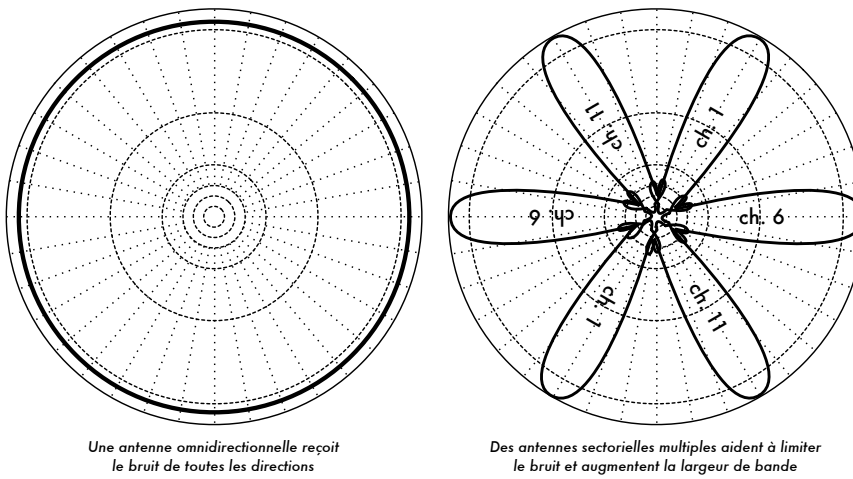


Figure 3.21: Une seule antenne omnidirectionnelle vs multiples antennes sectorielles.

- **Utilisez le meilleur canal disponible**. Rappelez-vous que les canaux 802.11b/g ont une largeur de 22 Mhz, 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 consommation 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.

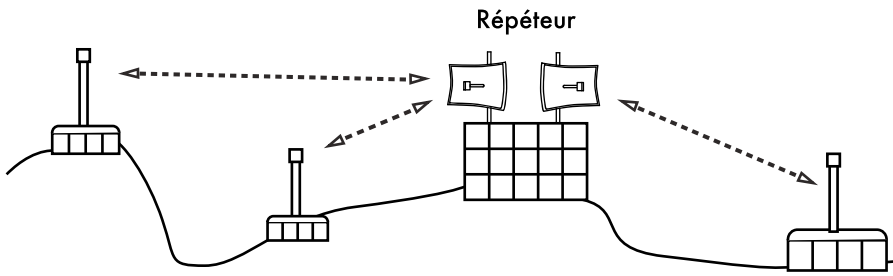


Figure 3.22: Le répéteur transmet des paquets dans l'air entre des nœuds qui n'ont pas de ligne de vue directe.

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.

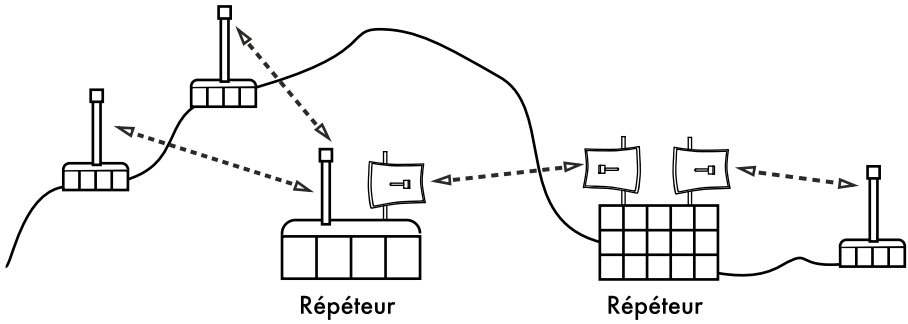


Figure 3.23: Il n'y avait pas d'énergie disponible au dessus de la colline, mais ceci a été résout en employant de multiples de répéteurs situés autour de la base.

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.

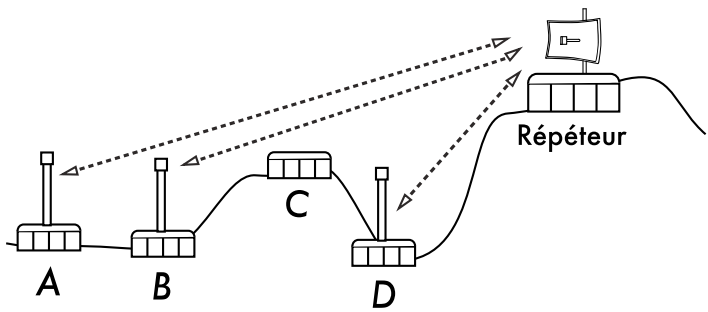


Figure 3.24: L'emplacement D ne peut pas voir les emplacements A ou B, car l'emplacement C est dans le chemin et n'est pas intéressé à héberger un nœud. En installant un répéteur plus haut, les nœuds A, B et D peuvent communiquer. Notez qu'en fait le trafic du nœud D voyage plus loin que celui du reste 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 logiciels 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 open source 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 supporté. 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 pare-feux 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'usage 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'éviteront pas le serveur Proxy.

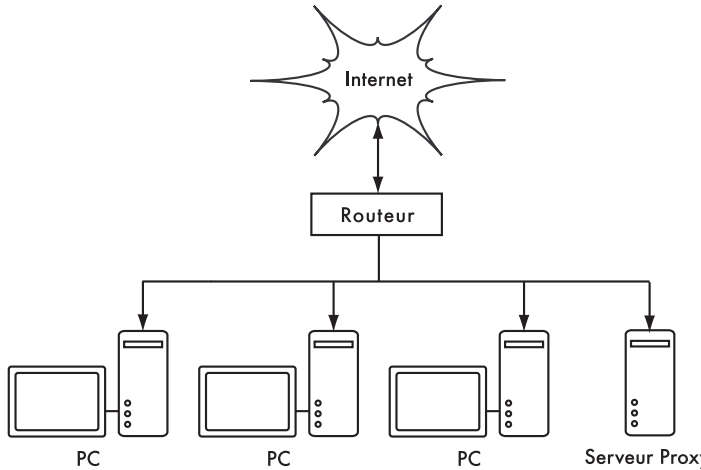


Figure 3.25: Ce réseau repose sur la confiance que ses usagers configureront correctement leurs ordinateurs pour utiliser le serveur mandataire.

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.

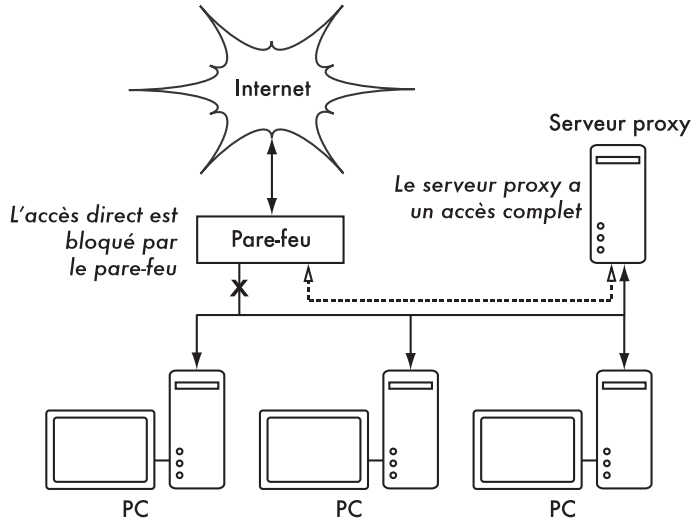


Figure 3.26: Le pare-feu empêche les ordinateurs d'accéder directement à Internet, mais permet l'accès via le serveur proxy.

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.

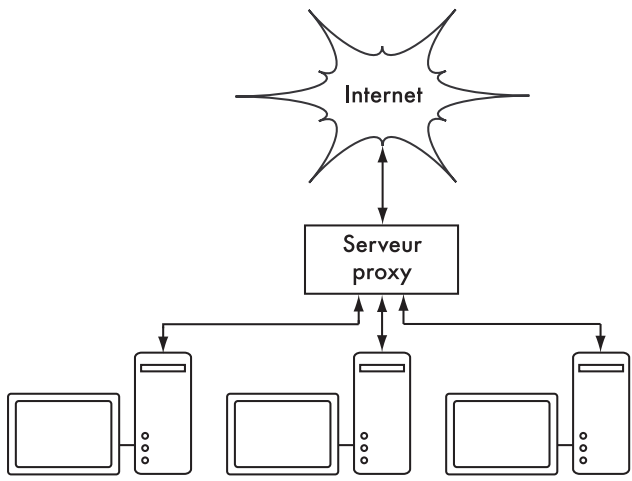


Figure 3.27: Le seul chemin vers Internet est à travers le serveur proxy .

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 supportent 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:

- h*ttp://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 possède 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 e 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 e 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 du 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 e cache proxy s'il y assez d'espace disque et que les paramètres de e 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'un cache basé 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 système 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 pagination 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 cache-seul 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 ***durée de vie*** (en anglais *Time to Live* -***TTL***) expire. Ceci réduira la quantité du trafic DNS sur votre connexion Internet, parce que e cache DNS peut satisfaire plusieurs demandes localement. Naturellement, les ordinateurs des clients doivent être configurés pour utiliser le nom de serveur cache-seul en tant que leur serveur DNS. Quand tous les clients utilisent ce serveur DNS en tant que serveur principal, il remplira rapidement e 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 (FAI) 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 FAI accèdent au site Web, ils obtiennent l'adresse IP de le FAI 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 le FAI 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 22 Mbps 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 FAI, cette section pourrait s'appliquer si la connexion FAI 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).

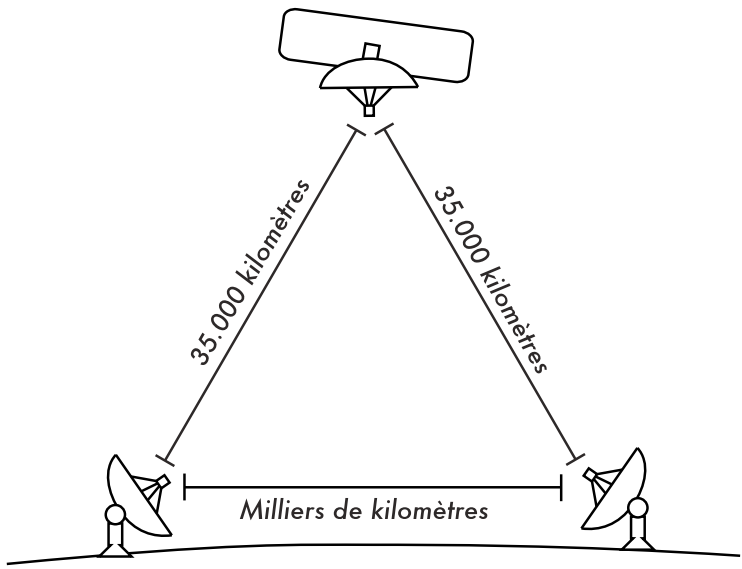


Figure 3.28: Étant donnée la vitesse de la lumière et les longues distances impliquées, la confirmation de réception d'un seul paquet «ping» peut prendre plus de 520 ms sur un lien VSAT.

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 (SACK). SACK est particulièrement important pour des connexions utilisant de grandes tailles de fenêtre TCP.»*

SACK est une caractéristique standard de Linux et BSD depuis un certain temps. Assurez-vous que tant votre routeur Internet comme votre FAI à distance supportent 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 de performance («Performance-enhancing proxy» -PEP)

L'idée d'un proxy d'amélioration de performance 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 le FAI. 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.

Plus d'informations

Alors que l'optimisation de la bande passante est une entreprise complexe et souvent difficile, les techniques présentées dans ce chapitre devraient aider à réduire les sources manifestes de gaspillage de bande passante. Pour faire le meilleur usage possible de la bande passante disponible, il sera nécessaire de définir une bonne politique d'accès, mettre en place une surveillance compréhensive et des outils d'analyse, et mettre en œuvre une architecture de réseau qui applique les limites d'usage souhaité.

Pour plus d'informations sur l'optimisation de la bande passante, voir le livre gratuit *How to Accelerate Your Internet* (*http://bwmo.net/*).

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 abrégé, dérivé des mots « *d'un 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 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 ».

---

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

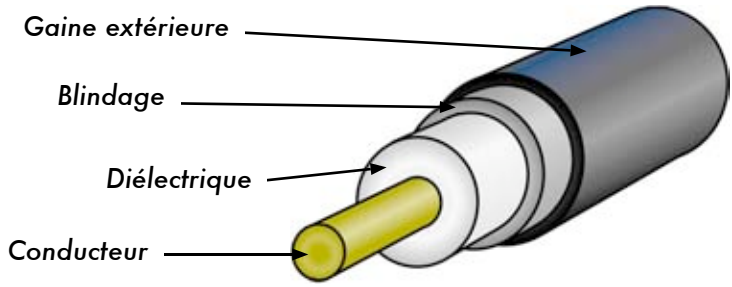


Figure 4.1: Câble coaxial avec gaine extérieure, bouclier, matériel diélectrique et conducteur.

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.

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

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.

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:

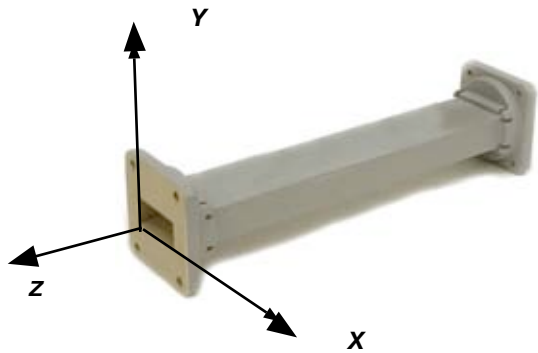


Figure 4.2: Les dimensions X, Y, et Z d'un guide d'onde rectangulaire.

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 augmente 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 12 GHz. 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 FH est la fréquence plus élevée de la bande, FL est la fréquence la plus basse de la bande et FC 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.

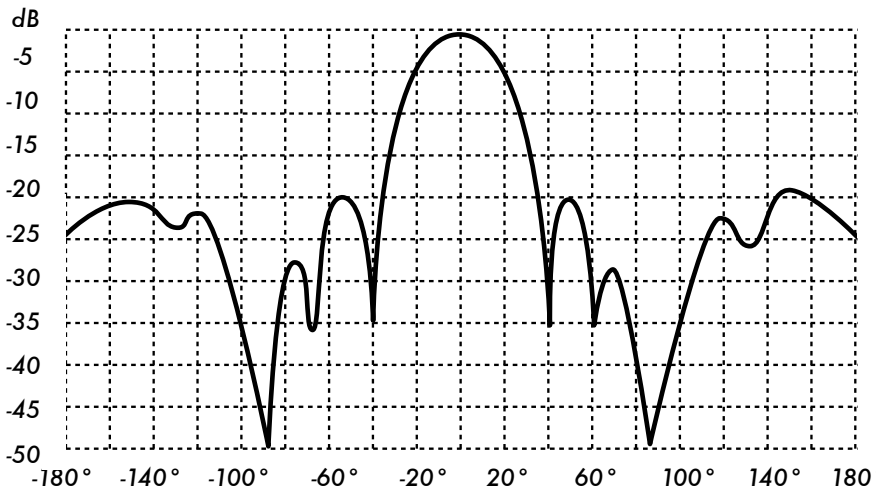


Figure 4.4: Un diagramme de rayonnement aux coordonnées rectangulaires d'une antenne Yagi.

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.

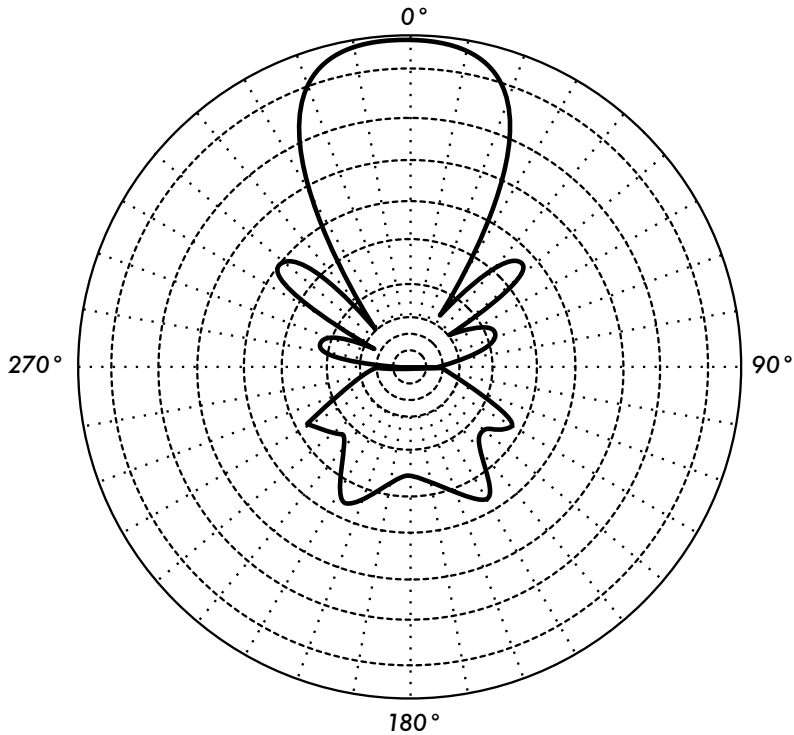


Figure 4.5: Un diagramme polaire linéaire de la même antenne yagi.

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.

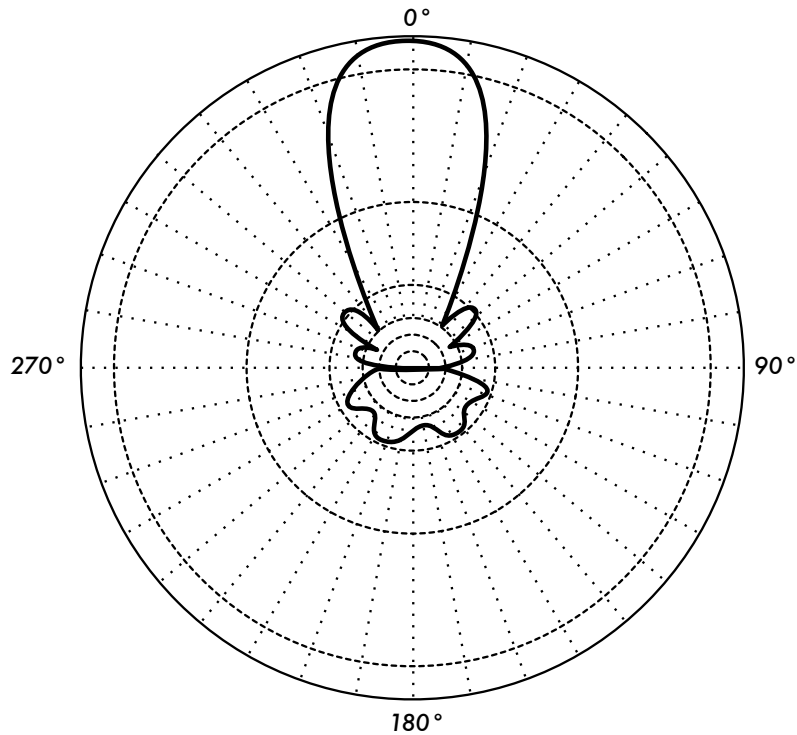


Figure 4.6: Traçage polaire logarithmique

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 important 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.

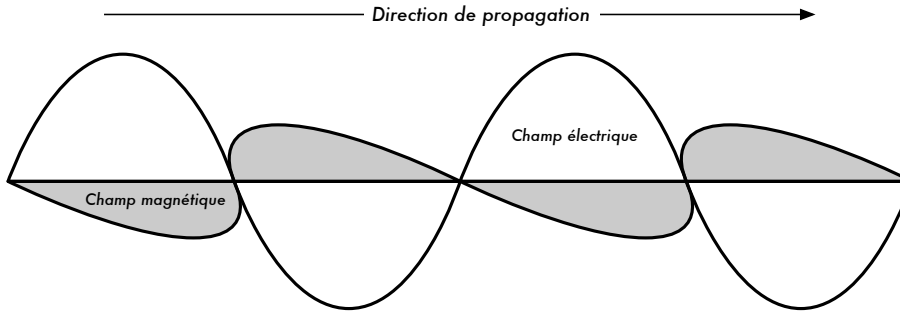


Figure 4.7: L'onde sinusoïdale électrique se déplace en direction perpendiculaire par rapport à l'onde magnétique dans la direction de la propagation

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:

```
Perte (dB) = 20 log (cos θ)
```

...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 rayonner 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.

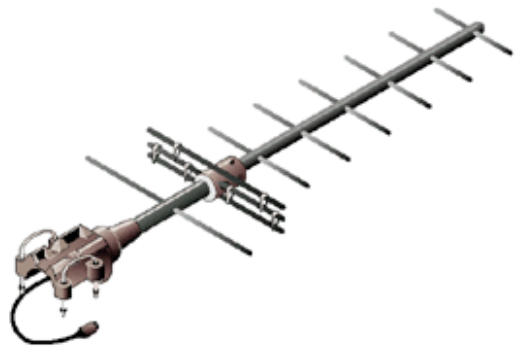


Figure 4.9: Une antenne Yagi.

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.

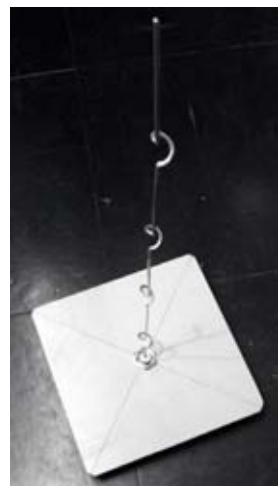


Figure 4.13: L'antenne omni colinéaire complète

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:

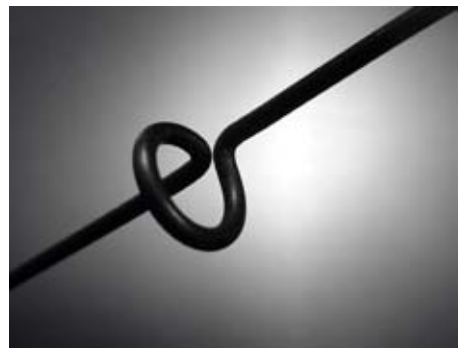


Figure 4.19: La boucle complète.

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 distance 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.

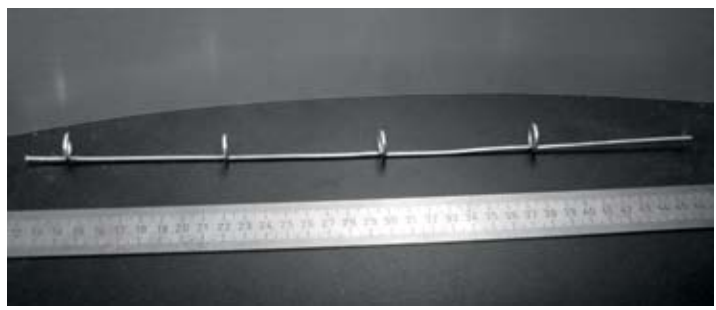


Figure 4.20: Essayer de le maintenir le plus droit que possible

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.

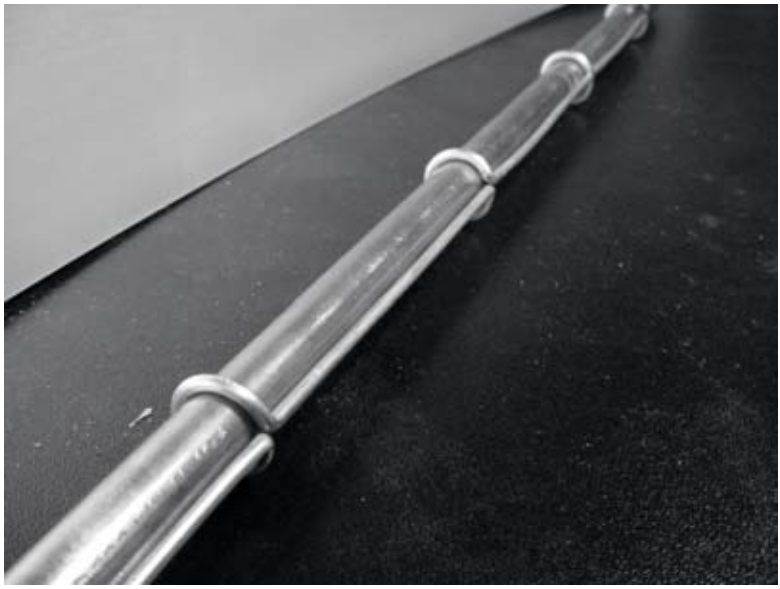


Figure 4.21: L'insertion d'un tuyau peut aider à redresser le fil.

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.

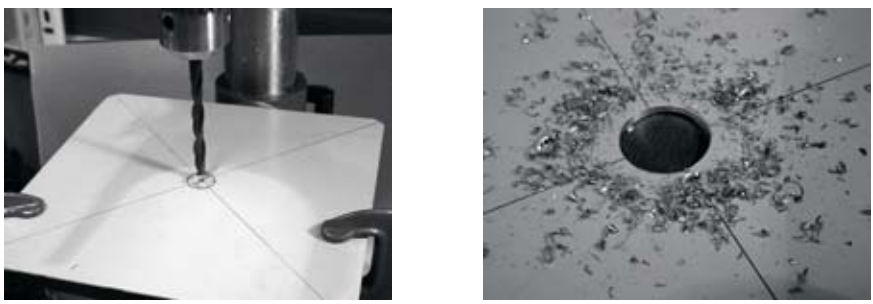


Figure 4.22: Percer un trou dans la plaque métallique.

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.

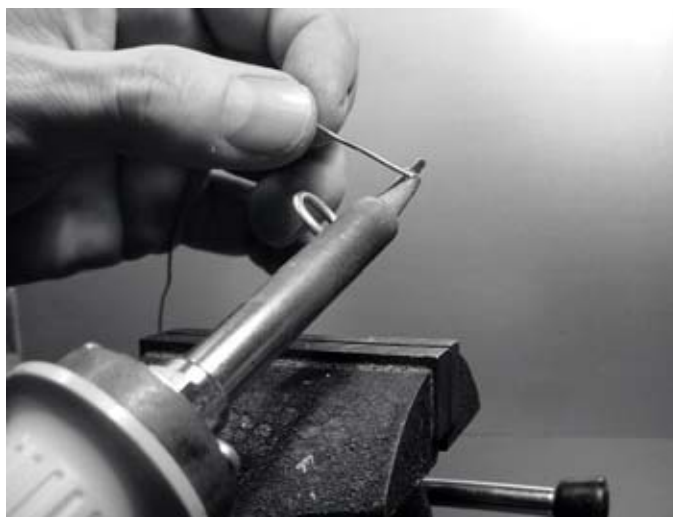


Figure 4.26: Ajouter un peu d'étain à l'extrémité du fil avant de le souder.

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.

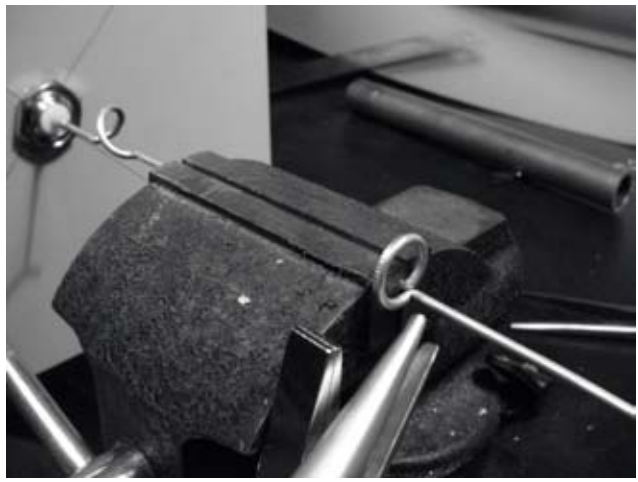


Figure 4.29: Répétez la même procédure «d'étirement» pour les boucles restantes.

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

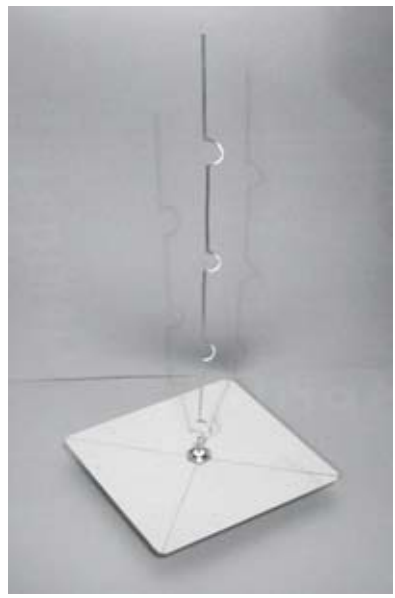


Figure 4.30: L'antenne finale devrait mesurer 42,5 cm de la plaque à l'extrémité du fil.

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.

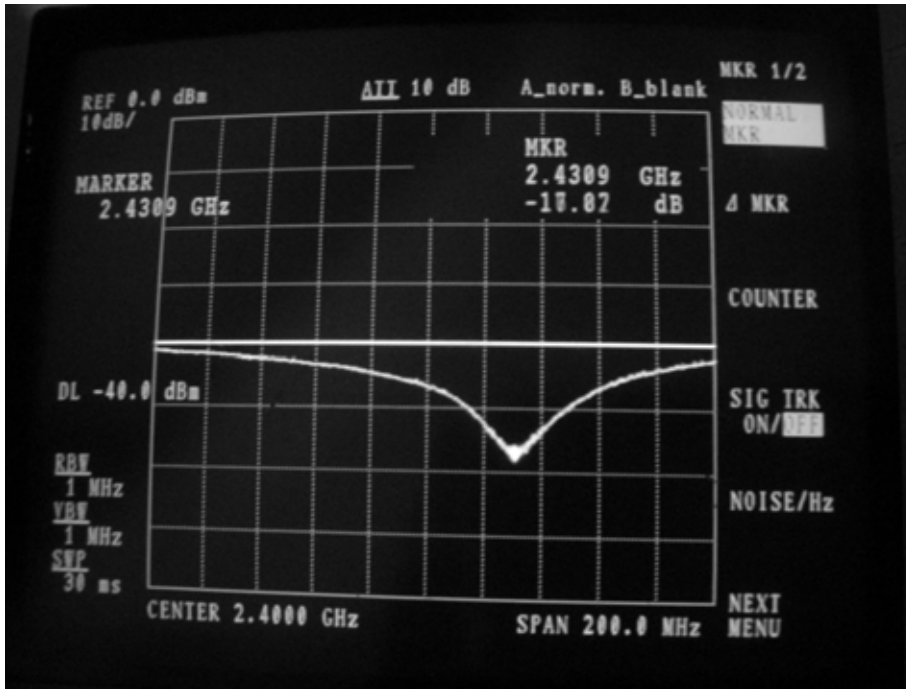


Figure 4.31: Un traçage du spectre de la puissance reflétée de l'antenne colinéaire omnidirectionnelle.

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:

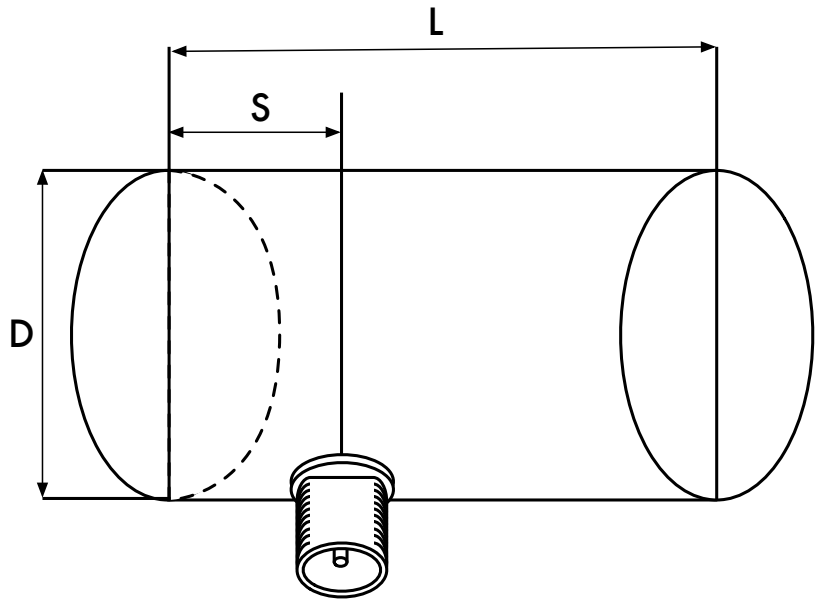


Figure 4.32: Contraintes dimensionnelles de la Cantenna

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 λ_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.

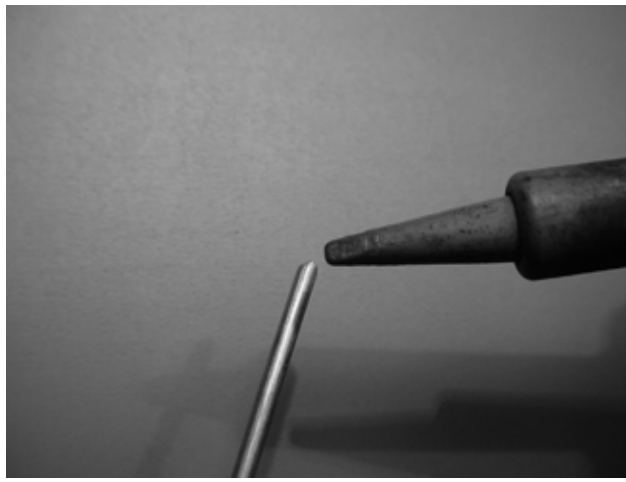


Figure 4.38: Ajouter de l'étain à l'extrémité du fil avant de souder.

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 une 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 alternatif ou à l'aide d'un transformateur continu. 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.

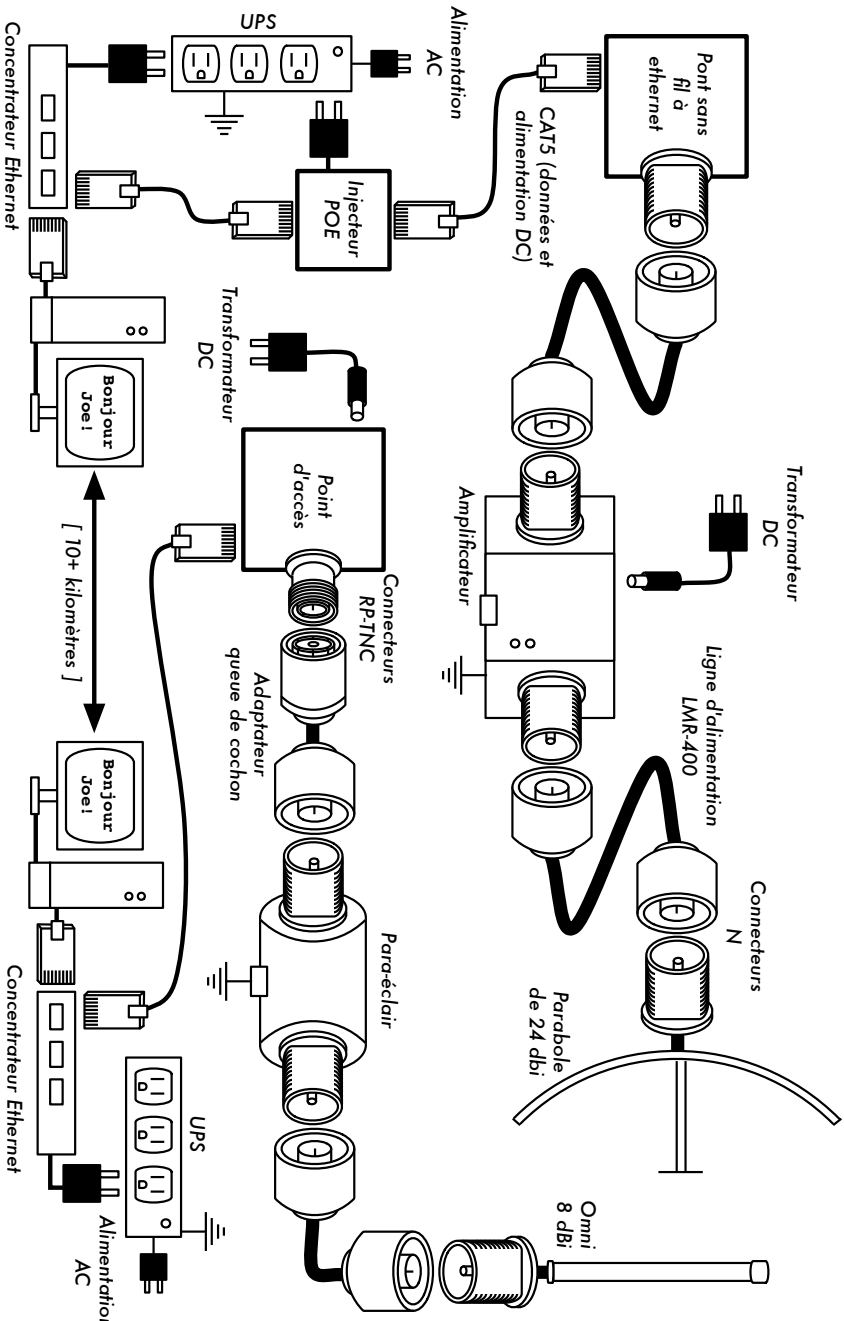


Figure 5.1: Composantes Interconnectées

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 médiocre) 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 prisonnier d'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 prisonnier d'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 prisonnier d'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 prisonnier d'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. 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 l'étalement de spectre par saut (ou évasion) de fréquence (*Frequency Hopping Spread Spectrum-FHSS*) et qui créera beaucoup de bruit pour l'étalement de spectre à séquence directe (*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 indirecte 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 une plaque 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 pare-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 portable 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 pare-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 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 Pyramid**. 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 Pyramid 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:// pyramid.metrix.netl*.
- **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 et surveillance

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 spéciaux 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 Wi-Fi*** (*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).

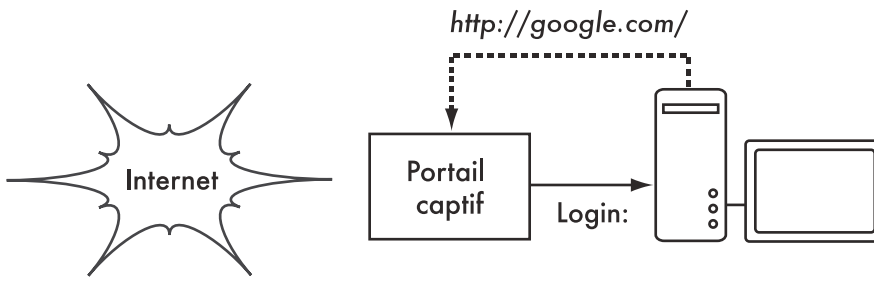


Figure 6.1: L'usager veut aller sur page Web et est redirigé.

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.

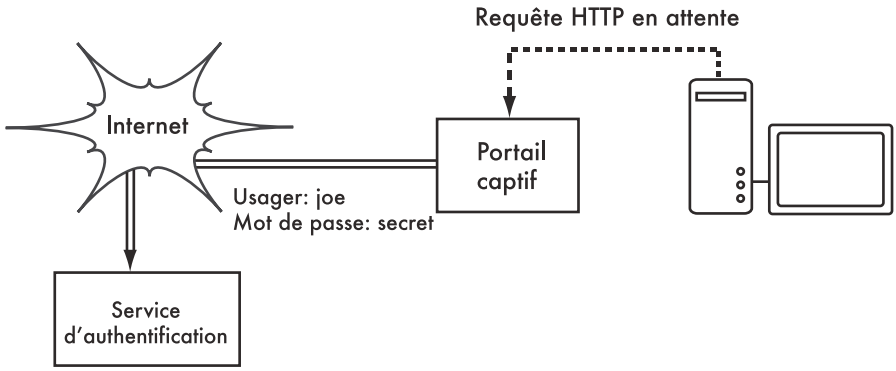


Figure 6.2: Les accréditations de l'usager sont vérifiées avant de lui permettre un accès complet. Le serveur d'authentification peut être le point d'accès lui-même, un autre ordinateur sur le réseau local ou un serveur n'importe où sur Internet.

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.

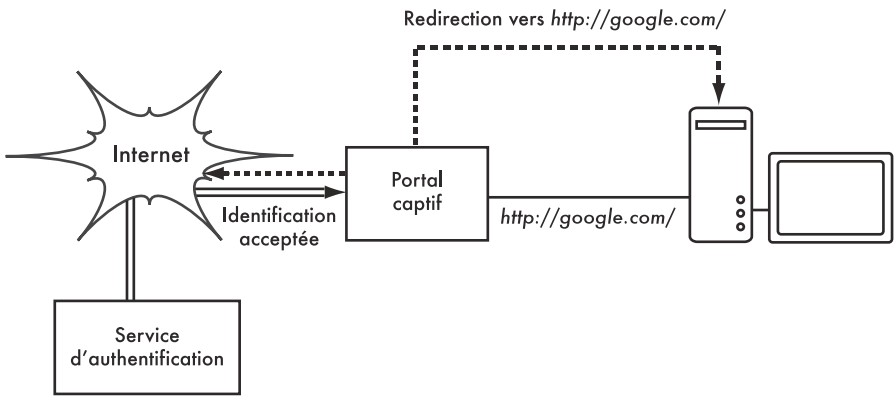


Figure 6.3: Une fois authentifié, l'usager peut avoir accès au reste du réseau.

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.

Projets points chauds populaires

- **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 facilement. 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.
- **NoCatSplash** (*http://nocat.net/download/NoCatSplash/*) fournit à vos utilisateurs une page de démarrage personnalisable, leur demandant de cliquer sur un bouton "Identification" avant d'utiliser le réseau. Ceci est utile pour identifier les opérateurs du réseau et 'afficher des règles pour l'accès au réseau. Il fournit une solution très facile dans les situations où vous avez besoin de fournir de l'information aux utilisateurs d'un réseau ouvert et une politique d'usage acceptable.

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.

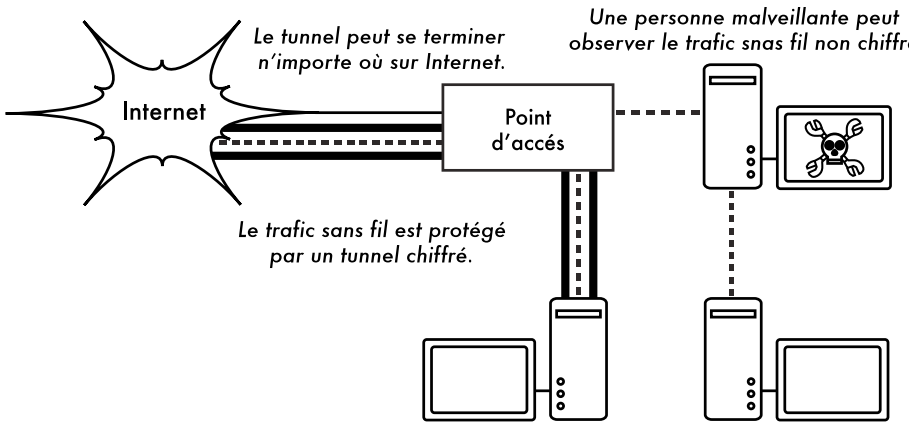


Figure 6.4: Les oreilles indiscrètes doivent rompre un chiffrement fort pour surveiller le trafic au sein d'un tunnel chiffré. La conversation à l'intérieur de ce tunnel est identique à n'importe quelle autre conversation non chiffrée.

L'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***.

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.

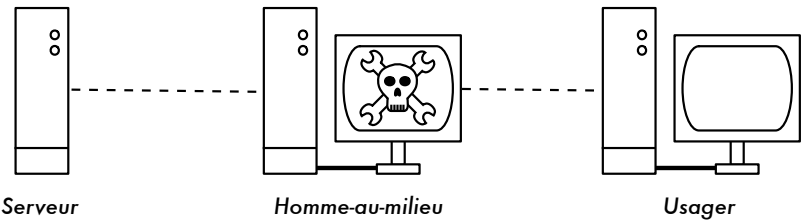


Figure 6.5: L'homme au milieu controle efficacement tout ce que l'usager voit et peut enregistrer ou manipuler tout le trafic. Sans infrastructure a clef publique pour vérifier l'authenticité des clefs, le chiffrement fort, employé seul, ne peut pas protéger contre ce genre d'attaque..

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.

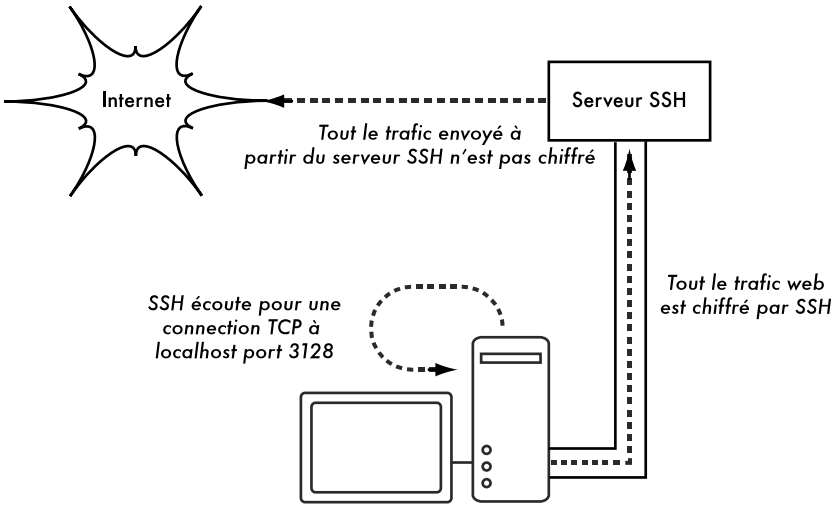


Figure 6.6: Le tunnel SSH protège le trafic Web au delà du serveur SSH lui-même.

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 réseau. 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 sécuritaires (du type que nous avons vu au sein de ce chapitre), Tor et Privoxy fournissent un niveau élevé d'anonymat sur l'Internet.

Surveillance réseau

La surveillance réseau utilise des outils d'enregistrement et d'analyse pour déterminer avec précision les flux de trafic, l'utilisation, et d'autres indicateurs de performance d'un réseau. Des bon outils de suivi vous donnent les chiffres précis et des représentations graphiques globales de l'état du réseau. Cela vous permet de visualiser précisément ce qui se passe, de sorte que vous sachiez où des ajustements pourraient être nécessaires. Ces outils peuvent vous aider à répondre à des questions critiques, telles que:

- Quels sont les services les plus populaires utilisés sur le réseau?
- Qui sont les plus grand utilisateurs du réseau?
- Quels sont les autres canaux sans fil qui sont en service dans ma région?
- Les utilisateurs installent t'ils des points d'accès sans fil sur mon réseau câbé ?
- À quel moment de la journée le réseau est il le plus utilisé?
- Quels sont les sites que vos utilisateurs fréquentent?
- Est-ce que le montant du trafic entrant ou sortant est proche de notre capacité réseau disponible?
- Existe-t-il des indications d'une situation inhabituelle réseau qui consomme la bande passante ou cause d'autres problèmes?
- Est-ce que notre fournisseur de services Internet (ISP) fournit le niveau de service que nous payons pour? Cela devrait s'exprimer en termes de bande passante disponible, perte de paquets, latence, et disponibilité globale.

  Et peut-être la question la plus importante de toutes:

- Est-ce que le modèle de trafic observé correspond à nos attentes?

Voyons comment un administrateur système typique peut faire bon usage des outils de surveillance réseau.

Un exemple effectif de surveillance réseau

Aux fins d'exemple, supposons que nous sommes en charge d'un réseau qui fonctionne depuis trois mois. Il se compose de 50 ordinateurs et trois serveurs: email, web, et des serveurs pare-feu (proxy). Alors que tout allait bien au début, les utilisateurs ont commencé à se plaindre de la lenteur du réseau et une augmentation des emails spam. Au fil du temps, les performances de l'ordinateur ralentissent très lentement (même si vous n'utilisez pas le réseau), frustrant vos utilisateurs.

Avec les plaintes fréquentes et l'usage très faible des ordinateurs, le Conseil s'interroge sur la nécessité de tant de matériel réseau. Le Conseil souhaite également avoir une preuve que la bande passante pour laquelle il paie est effectivement utilisé. En tant qu'administrateur réseau, vous êtes sur l'extrémité

de réception de ces plaintes. Comment pouvez vous diagnostiquer la baisse soudaine des performances réseau et ordinateurs et aussi justifier le matériel réseau et les coûts de la bande passante?

Surveillance du réseau local LAN (trafic local)

Pour se faire une idée de ce qui est exactement a l'origine du ralentissement, vous devriez commencer par regarder le trafic sur le réseau local. Il y a plusieurs avantages à surveiller le trafic local:

- Le dépannage est grandement simplifié.
- Les virus peuvent être détectés et éliminés.
- Des utilisateurs malveillants peuvent être détectés et controlés.
- Le matériel et ressources réseau peuvent être justifiés sur base des statistiques réelles.

Supposons que tous les commutateurs supportent le protocole ***Simple Network Management Protocol*** (***SNMP***). SNMP est un protocole de la couche application destiné à faciliter l'échange d'information de gestion entre les périphériques réseau. En attribuant une adresse IP à chaque commutateur, vous êtes en mesure de contrôler toutes les interfaces sur ce commutateur en observant l'ensemble du réseau à partir d'un seul point. Cela est beaucoup plus facile que d'activer SNMP sur tous les ordinateurs d'un réseau.

En utilisant un outil gratuit tel que MRTG (voir **Page 192**), vous pouvez surveiller chaque port sur le commutateur et présenter les données graphiquement, comme une moyenne globale au cours du temps. Les graphiques sont accessibles à partir du web. Vous êtes donc en mesure d'afficher les graphiques à partir de n'importe quelle machine à tout moment.

Avec la surveillance MRTG en place, il devient évident que le LAN interne est inondé avec beaucoup plus de trafic que la connexion Internet peut supporter, même quand le laboratoire est inoccupé. Ceci est une indication très claire que certains des ordinateurs sont infestés par un virus réseau. Après avoir installé le bon anti-virus et des logiciels anti-espions sur toutes les machines, le trafic LAN interne atteint le niveau escompté. Les machines exécutent beaucoup plus vite, les e-mails spam sont réduits, et le moral des utilisateurs remonte rapidement.

Surveillance du réseau à longue distance WAN (trafic externe)

En plus de la surveillance du réseau local interne, vous avez besoin de démontrer que la bande passante pour laquelle l'organisme paye est en fait ce qu'elle reçoit du fournisseur des services Internet. Vous pouvez le faire en contrôlant le ***trafic externe***.

Le traffic externe est généralement consideré comme tout ce qui est transmis sur un ***réseau a longue distance*** (***WAN***, *Wide Area Network*). Tout ce qui est reçu (ou envoyé à) d'un réseau autre que votre LAN interne est aussi

consideré comme trafic externe. Les avantages de la surveillance du traffic externe incluent:

- Les coûts de la bande passante Internet sont justifiés en montrant l'usage réel, et si cet usage s'accorde avec les frais de bande passante de votre FAI.
- Les besoins en capacité futures sont estimés en regardant les tendances d'usage et en prévoyant la croissance probable.
- Les Intrus de l'Internet sont détectés et filtrés avant qu'ils ne puissent causer des problèmes.

La surveillance du trafic se fait facilement avec l'usage de MRTG sur un dispositif ou SNMP est activé tel qu'un routeur. Si votre routeur ne supporte pas SNMP, alors vous pouvez ajouter un commutateur entre votre routeur et votre connection FAI et ainsi surveiller le trafic sur le port du commutateur comme vous le feriez avec un réseau local interne.

Détection de pannes de réseau

Avec des outils de surveillance en place, vous avez maintenant une mesure précise de la quantité de bande passante que l'organisme utilise. Cette mesure doit s'accorder avec les frais de la bande passante de votre fournisseur. Elle peut également indiquer le débit actuel de votre connexion si vous utilisez presque toute votre capacité disponible aux heures de pointe. Un graphique de type “sommet plat” est une indication assez claire que vous operez à pleine capacité. La **Figure 6.7** montre des sommets plats dans le trafic sortant de pointe au milieu de toutes les journées sauf le dimanche.

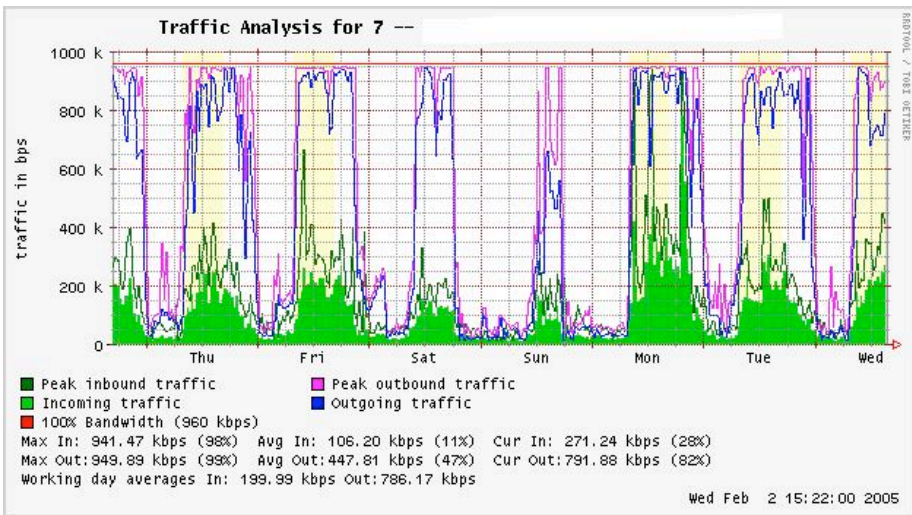


Figure 6.7: Un graphique avec un "sommet plat" est une indication de la surutlization.

Il est clair que votre connexion Internet actuelle est surutilisée aux heures de pointe provoquant un retard réseau. Après présentation de cette information au conseil d'administration, vous pouvez faire un plan pour une optimisation ulterieure de votre connexion existante (par mise à niveau de votre serveur proxy et en utilisant d'autres techniques dans ce livre) et estimer combien de temps vous devez mettre pour mettre à jour votre connexion en vue de suivre la demande . C'est également un excellent temps pour revoir votre politique opérationnelle avec le conseil d'administration et discuter des moyens pour rendre l'usage actuel conforme à cette politique.

Plus tard dans la semaine, vous recevez un appel téléphonique d'urgence dans la soirée. Apparemment, personne dans le laboratoire peut naviguer sur le Web ou envoyer un courriel. Vous vous ruez vers le laboratoire et hâtivement redémarrez le serveur proxy sans résultats. La navigation Web et le courriel ne marchent toujours pas. Vous redémarrez alors le routeur, mais toujours sans succès. Vous continuez a éliminer les zones de faute possible une par une jusqu'à ce que vous vous rendez compte que le commutateur réseau est eteint - un câble d'alimentation detaché est à blâmer. Après allumage, le réseau vit de nouveau.

Comment pouvez-vous dépanner une telle panne sans recourir à cette technique d'essai et erreur consomatrice de temps? Est-il possible d'être averti des coupures de courant à mesure qu'ils surviennent plutôt que d'attendre lorqu'un utilisateur se plaint? Une façon de le faire est d'utiliser un logiciel tel que ***Nagios*** qui continuellement sonde les périphériques réseau et vous avertit des pannes. Nagios rapportera la disponibilité des différentes machines et services, et vous alertera sur les machines qui sont arretées. En plus de l'affichage graphique de l'état du réseau sur une page web, il enverra des notifications par SMS ou e-mail, vous alertant immédiatement en cas de problèmes.

Avec une mise en place de bons outils de surveillance, vous serez en mesure de justifier le coût de l'équipement et la bande passante en démontrant effectivement comment elle est utilisée par l'organisme. Vous êtes informé automatiquement lorsque les problèmes surviennent et vous avez des statistiques historiques de performance des périphériques du réseau. Vous pouvez comparer les performances actuelles par rapport à cette historique pour verifier un comportement inhabituel, et enrayer les problèmes avant qu'ils ne deviennent critiques. Lorsque les problèmes arrivent, il est simple de déterminer la source et la nature du problème. Votre travail est plus facile, le Conseil est satisfait, et vos utilisateurs sont beaucoup plus heureux.

Surveillance de votre réseau

La gestion d'un réseau sans surveillance est similaire à la conduite d'un véhicule sans un indicateur de vitesse ou une jauge de carburant, avec vos yeux fermés. Comment avez-vous savoir à quelle vitesse vous conduisez? Est-ce que le véhicule consomme le carburant de manière aussi efficace que promis par les concessionnaires? Si vous faites une révision moteur plusieurs mois plus tard, la voiture est t'elle plus rapide ou plus efficace qu'elle ne l'était avant?

De façon similaire, comment pouvez-vous payer pour une facture d'électricité ou d'eau sans voir votre usage mensuel à partir d'un compteur? Vous

devez faire un compte de votre utilisation de la bande passante du réseau afin de justifier le coût des services et des achats de matériel, et tenir compte des tendances d'usage.

Il ya plusieurs avantages à implementer un bon système de surveillance de votre réseau:

1. **Le budget réseau et les ressources sont justifiés**. Les bon outils de surveillance peuvent démontrer sans l'ombre d'un doute que l'infrastructure du réseau (bande passante, matériel et logiciel) est adapté et capable de gérer les exigences des utilisateurs du réseau.
2. **Les intrus au réseau sont détectés et filtrés**. En regardant le trafic de votre réseau, vous pouvez détecter les assaillants et prévenir l'accès aux serveurs internes et services.
3. **Les virus réseau sont facilement détectés**. Vous pouvez être avertis de la présence de virus réseau et prendre les mesures appropriées avant qu'ils ne consomment la bande passante Internet et déstabilisent votre réseau.
4. **Le depannage des problèmes de réseau est grandement simplifié.** Plutôt que d'essayer la methode "d'essai et erreur" pour le débogage des problèmes de réseau, vous pouvez être immédiatement informé des problèmes spécifiques. Certains types de problèmes peuvent même être réparés automatiquement.
5. **La performance réseau peut être hautement optimisée.** Sans une surveillance efficace, il est impossible d'affiner vos périphériques et les protocoles pour obtenir la meilleure performance possible.
6. **La planification de la capacité est beaucoup plus facile.** Possédant une solide historique de performance, vous n'avez pas à "deviner" la quantité de bande passante dont vous aurez besoin quand votre réseau se développe.
7. **Un usage réseau approprié peut être appliqué.** Lorsque la bande passante est une ressource rare, le seul moyen d'être équitable à tous les utilisateurs, est de veiller à ce que le réseau est utilisé tel que plannifié.

Heureusement, la surveillance réseau n'a pas besoin d'être une entreprise coûteuse. Il existe de nombreux outils libres gratuitement disponibles qui vont vous montrer exactement ce qui se passe sur votre réseau en détail. Cette section vous aidera à identifier de nombreux outils précieux et la meilleure façon de les utiliser.

Le serveur de surveillance dédié

Bien que les services de surveillance peuvent être ajoutés à un serveur réseau existant, il est souvent souhaitable de consacrer une machine (ou plus si nécessaire) pour la surveillance réseau. Quelques applications (comme ntop) exigent des ressources considérables pour fonctionner, en particulier sur un

réseau sollicité. Mais la plupart des programmes d'enregistrement et de surveillance ont des exigences RAM et stockage modestes, généralement necessitant peu de resources de l'unité centrale de traitement. Comme les systèmes d'exploitation libres (comme Linux ou BSD) font un usage très efficace des ressources matérielles, ceci permet de construire un serveur de surveillance très capable avec pieces de PC recyclées. Il n'y a habituellement pas besoin d'acheter un tout nouveau serveur auquel reléguer les taches de surveillance.

L'exception à cette règle consiste en des très grandes installations. Si votre réseau comprend plus de quelques centaines de noeuds, ou si vous consommez plus de 50 Mbit/s de bande passante Internet, vous aurez besoin de distribuer les fonctions de surveillance entre quelques machines dédiées. Cela dépend en grande partie de ce que vous voulez exactement surveiller. Si vous êtes tenté de rendre compte de tous les services accessibles par adresse MAC, ceci consommera plus de ressources que simplement mesurer les flux réseau sur un port. Mais pour la majorité des installations, une seule machine dédiée a la surveillance est généralement suffisante.

Alors que la consolidation des services de contrôle dans une machine unique permettra de rationaliser l'administration et les mises à jour, elle peut également assurer une meilleure surveillance en cours. Par exemple, si vous installez les services de surveillance sur un serveur Web et ce serveur Web développe des problèmes, votre réseau peut ne pas être surveillé jusqu'à ce que le problème soit résolu.

Pour un administrateur réseau, les données collectées sur les performances du réseau sont presque aussi importantes que le réseau lui-même. Votre surveillance doit être robuste et protégée contre les pannes de service aussi bien que possible. Sans statistiques réseau, vous êtes effectivement aveugle aux problèmes du réseau.

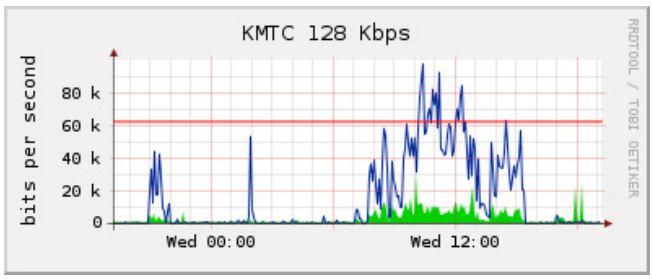


Figure 6.8: Le sondage du routeur périphérique peut vous montrer l'usage réseau d'ensemble, mais vous ne pouvez pas separer les données en donnees machines, services et utilisateurs.

Où le serveur convient dans mon réseau?

Si vous êtes uniquement intéressé par la collecte des statistiques de flux réseau a partir d'un routeur, vous pouvez le faire n'importe où sur le réseau local. Cela permet une retroaction simple sur l'utilisation, mais ne peut pas vous donner des informations détaillées sur les modes d'usage. La **Figure 6.8** montre un graphique MRTG typique produit à partir d'un routeur Internet. Alors que

l'utilisation en entrée et sortie sont claires, il n'y a pas de détail sur comment les ordinateurs, les utilisateurs, ou de protocoles utilisent la bande passante.

Pour plus de détails, le serveur de surveillance dédié doit avoir accès à tout ce qui doit être surveillé. En règle générale, cela signifie qu'il doit avoir accès à l'ensemble du réseau. Pour surveiller une connexion WAN, tel que la liaison Internet à votre fournisseur des services, le serveur de surveillance doit être en mesure de voir le trafic passant par le routeur peripherique. Pour surveiller un réseau local, le serveur de surveillance est généralement connecté à un ***port moniteur*** sur le commutateur. Si plusieurs commutateurs sont utilisés dans une installation, le serveur de surveillance peut avoir besoin d'une connexion à chacun d'entre eux. Cette liaison peut être un câble physique, ou si vos commutateurs réseau le supporte, un réseau local virtuel configuré spécifiquement pour la surveillance du trafic.

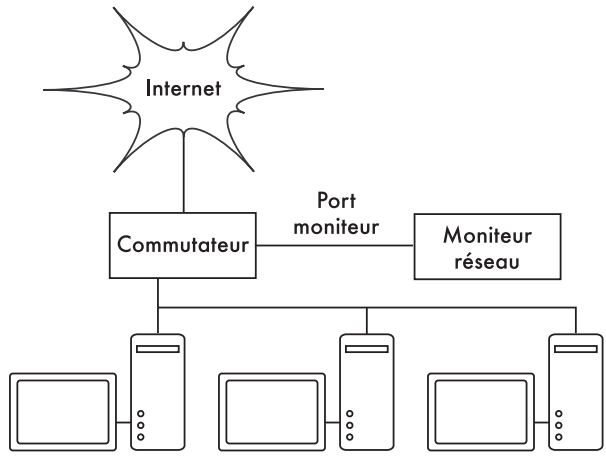


Figure 6.9: Utiliser le port moniteur sur votre commutateur pour observer le trafic traversant tous les ports du réseau.

Si la fonctionnalité port moniteur n'est pas disponible sur votre commutateur, le serveur de surveillance peut être installé entre votre réseau interne et l'Internet. Bien que cela fonctionne, il introduit un point de défaillance unique pour le réseau, car le réseau tombera en panne si le serveur de surveillance développe un problème. Il est également un goulot d'étranglement de performance potentiel si le serveur ne peut pas suivre les demandes du réseau.

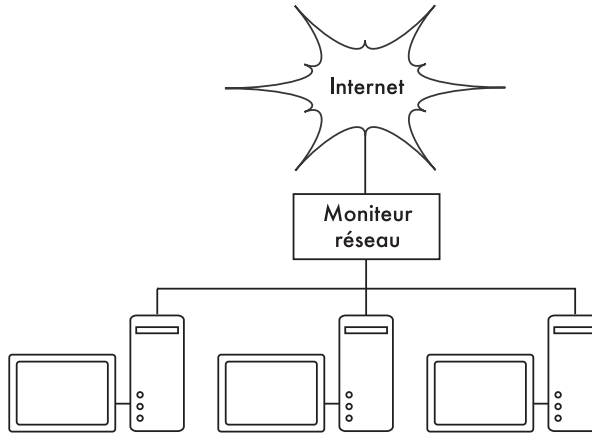


Figure 6.10: Par l'insertion d'un moniteur de réseau entre le réseau local et votre connexion Internet, vous pouvez observer tout le trafic réseau.

Une meilleure solution consiste a utiliser un simple hub (et non pas un commutateur) qui relie la machine de surveillance au réseau LAN interne, le routeur externe et la machine de surveillance. Bien que ceci introduit toujours un point supplémentaire de defaillance dans le réseau (car l'ensemble du réseau sera inaccessible si le hub tombe en panne), les hubs sont généralement considérés comme beaucoup plus fiables que les routeurs. Ils sont également très faciles à remplacer au cas où ils tombent en panne.

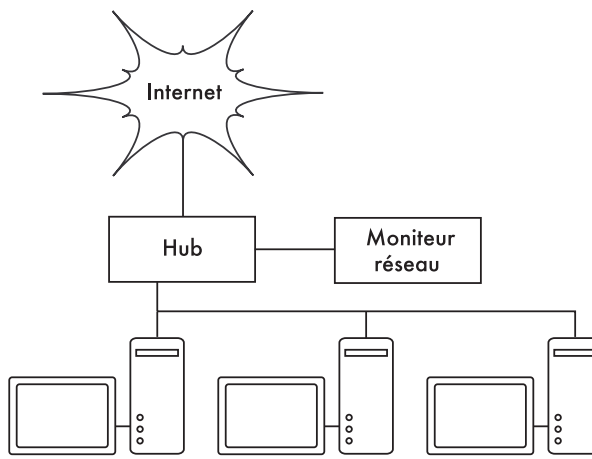


Figure 6.11: Si votre commutateur ne fournit pas de fonctionnalité port moniteur, vous pouvez insérer un hub entre votre routeur et le réseau local et connecter le serveur de surveillance au hub.

Une fois que votre serveur de surveillance est en place, vous êtes prêt à commencer la collecte de données.

Qu'est-ce qu'il faut surveiller

Il est possible de tracer n'importe quel evenement réseau et montrer sa valeur sur un graphique au fil du temps. Étant donné que chaque réseau est

légèrement différent, vous devrez décider quelle information est importante afin d'évaluer les performances de votre réseau.

Voici quelques indicateurs importants que de nombreux administrateurs de réseau généralement tracent.

Statistiques sans fil

- Le signal reçu et le bruit de tous les noeuds de la dorsale.
- Nombre de stations associées.
- Réseau x adjacents détectés et canaux .
- Retransmissions excessives.
- Débit de données radio si vous utilisez des taux d'échantillonage automatique.

Statistiques commutateur

- L'usage de la bande passante par port.
- L'usage de la bande passante ventilée par protocole.
- L'usage de la a bande passante ventilée par adresse MAC.
- Les diffusions en tant que pourcentage du nombre total de paquets .
- La perte de paquets et taux d'erreur .

Statistiques Internet

- Utilisation de la bande passante Internet par protocole et hote.
- Hits cache du serveur proxy.
- Les meilleurs 100 sites accedés.
- Les requêtes DNS.
- Le Nombre d'e-mails entrants / e-mails spam / email rebondissant.
- La taille de la file d'attente des e-mail sortants.
- Disponibilité des services crtiques (serveurs Web, serveurs de courriels, etc.).
- Les temps de Ping et taux de perte de paquets vers votre fournisseur de services Internet.
- Etat des sauvegardes .

Statistiques de santé système

- Usage memoire .
- Usage de fichiers d'échange.
- Compte de processus / processus zombie.
- Charge système .

- Tension et charge de l'Uninterruptible Power Supply (UPS).
- Température, vitesse du ventilateur, et tensions système .
- État du disque SMART .
- État du RAID array .

Vous devez utiliser cette liste comme une suggestion pour où commencer. Avec la maturité de votre réseau, vous trouverez probablement des nouveaux indicateurs clés de performance du réseau, et vous devriez les tracer aussi bien. Il existe de nombreux outils librement disponibles qui vous donneront autant de détails que vous le souhaitez sur ce qui se passe sur votre réseau. Vous devriez envisager la surveillance de la disponibilité de toute ressource où l'indisponibilite aurait des répercussions négatives sur les utilisateurs de votre réseau.

Par exemple, vos utilisateurs peuvent se connecter a des modems en ligne sur votre site afin d'avoir accès à distance à votre réseau. Si tous les modems sont utilisés, ou s'ils sont défectueux, les utilisateurs se verront refuser l'accès et probablement se plaindront. Vous pouvez prévoir et éviter ces problèmes en surveillant le nombre de modems disponibles, et par approvisionnement de capacités supplémentaires avant de tomber en manque.

N'oubliez pas de surveiller la machine de surveillance elle-même, par exemple son usage de CPU et d'espace disque, afin de recevoir un avertissement si elle devient surchargée ou défectueuse. Une machine de surveillance a court de ressources peut influer sur votre capacité à surveiller efficacement le réseau.

Types d'outils de surveillance

Nous allons maintenant nous pencher sur différentes classes d'outils de surveillance. Les outils de ***detection réseau*** écoutent les balises envoyées les par points d'accès sans fil et affichent les informations telles que le nom du réseau, la force du signal reçu, et le canal. Les outils de ***contrôle intermittent*** (*spot check*) sont conçus pour le dépannage et normalement fonctionnent interactivement pendant de courtes périodes de temps. Un logiciel tel que **`ping`** peut être considéré comme un outil spot check, car il génère du trafic en sondant une machine particulière. Des outils spot check passifs comprennent les ***analyseurs de protocole*** qui inspectent tous les paquets sur le réseau et fournissent des détails sur toute conversation réseau (y compris les adresses source et destination, le protocole d'informations, et même les données d'application). Les outils de ***tendances*** (*trending*) executent une surveillance incontrollée sur de longues périodes, et généralement imprime les résultats sur un graphique. Les outils de ***surveillance en temps*** réel réalisent une surveillance similaire mais notifients les administrateurs immédiatement s'ils détectent un problème. Les outils de ***test de débit*** vous disent la bande passante actuelle disponible entre deux points sur un réseau. Des outils de ***détection d'intrusion*** observent le traffic réseau indesirable ou inattendu et prennent les mesures appropriées (généralement refuser l'accès et/ou notifier un administrateur réseau). Enfin, des outils d'***étalonnage*** (*benchmarking*) estiment les performances maximales d'un service ou une connexion réseau.

Détection 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.

- **Outils 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 réseaux 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.

Les outils de contrôle intermittent

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.

Cette section est tout simplement une introduction aux outils de dépannage couramment utilisés. Pour plus de discussion sur les problèmes de réseau et la façon de les diagnostiquer, voir le **chapitre 9, Dépannage**.

ping

Presque tout système d'exploitation (incluant Windows, Mac OS X, et naturellement, Linux et BSD) inclut une version de l'utilitaire **`ping`**. Il utilise 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 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
```

Tapez “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 ***temps de vie*** (***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 vous connecter à 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 taper “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.

Analyseurs de protocole

Les analyseurs de protocole de réseau fournissent beaucoup de détails sur les informations qui coulent à travers un réseau en vous permettant d'inspecter les paquets individuels. Pour les réseaux câblés, vous pouvez inspecter les paquets de données sur la couche liaison ou aux couches supérieures. Pour les réseaux sans fil, vous pouvez surveiller l'information jusqu'aux trames 802.11 individuelles. Voici quelques analyseurs de protocole de réseau populaires (et libres) :

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 présence 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.

Figure 6.12 : Kismet fonctionne sur une tablette Internet de type Nokia 770

Puisque Kismet utilise le mode moniteur passif des cartes radios, il fait tout cela sans transmettre des données. Kismet est un outil précieux pour le diagnostic des problèmes de réseau sans fil.

KisMAC

http://kismac.binaervarianz.de/. ***Kismac*** a été conçu 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. Bien qu'il ne puisse pas fonctionner avec les cartes AirportExtreme (à cause des limitations du pilote sans fil), il le fait très bien avec une variété de cartes radio USB.

tcpdump

http://www.tcpdump.org/. ***tcpdump*** est un outil de ligne de commande pour la surveillance du trafic réseau. Il ne dispose pas de toutes les cloches et sifflets de wireshark mais il utilise moins de ressources. Tcpdump peut capturer et afficher toute l'information des protocoles réseau jusqu'à la couche liaison. Il peut montrer toutes les entêtes des paquets de données reçues, ou tout simplement les paquets qui correspondant à des critères particuliers. Les paquets capturés par tcpdump peuvent être chargé dans Wireshark pour analyse visuelle et d'autres diagnostics. Cela est très utile si vous souhaitez surveiller une interface sur un système distant et ramener le fichier sur votre ordinateur local pour analyse. L'outil tcpdump est disponible comme un outil standard dans les dérivés d'Unix (Linux, BSD et Mac OS X). Il existe également un portage pour Windows appelé ***WinDump*** disponible à *http://www.winpcap.org/windump/*.

Wireshark

http://www.wireshark.org/. Anciennement connu sous le nom d'Ethereal, ***Wireshark*** est un analyseur de protocole réseau libre pour Unix et Windows. Il est connu comme "l'analyseur de protocole réseau le plus populaire au monde."

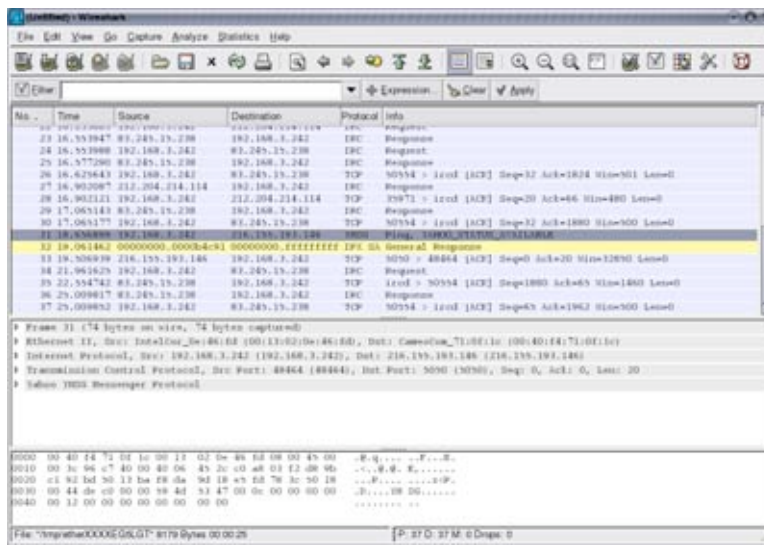


Figure 6.13 : Wireshark (ex Ethereal) est un puissant Analyseur de protocole réseau qui peut vous montrer autant de détails que vous souhaitez sur tous les paquets.

Wireshark vous permet d'examiner les données d'un réseau en direct ou à partir d'un fichier de capture sur le disque, ainsi q'une navigation interactive et un tri des données saisies. Les sommaires ainsi que l'information détaillée est disponible pour chaque paquet, y compris l'en-tête complet et les parties de données. Wireshark a plusieurs fonctionnalités puissantes, y compris un langage riche de filtrage d'affichage et la possibilité de visualiser la reconstitution d'un flux de session TCP.

Il peut être redoutable à utiliser pour les utilisateurs qui l'utilisent la première fois ou ceux qui ne sont pas familiers avec les couches OSI. Il est généralement utilisé pour isoler et analyser un trafic spécifique à destination ou en provenance d'une adresse IP, mais il peut également être utilisé comme un outil général de détection de fautes. Par exemple, une machine infectée par un ver réseau ou un virus peut être identifiée par la recherche de la machine qui est en train d'envoyer le même type de paquets TCP/IP à de grands groupes d'adresses IP.

Outils de tendance

Les outils de tendance sont utilisés pour voir comment votre réseau est utilisé sur une longue période de temps. Ils fonctionnent par surveillance périodique de votre activité réseau, et affichage d'un résumé sous forme lisible (par exemple un graphique). Les outils de tendance collectent les données et les analysent ainsi que les documentent.

Voici quelques exemples d'outils de tendance. Certains d'entre eux ont besoin d'être utilisés en combinaison avec d'autres car ils ne sont pas des programmes autonomes.

MRTG

http://oss.oetiker.ch/mrtg/. Le ***Multi Router Traffic Grapher*** (***MRTG***) surveille le volume du trafic sur les liaisons réseau en utilisant SNMP. MRTG génère des graphiques qui fournissent une représentation visuelle du trafic entrant et sortant. Ils sont généralement affichés sur une page Web.

La mise en place de MRTG peut être un peu déroutante, surtout si vous n'êtes pas familier avec SNMP. Mais une fois qu'il est installé, MRTG ne nécessite pratiquement aucun entretien, sauf si vous changez quelque chose sur le système qui est surveillé (comme son adresse IP).

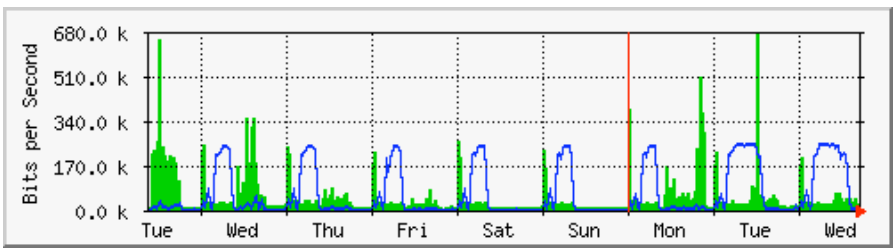


Figure 6.14 : MRTG est probablement le grapheur de flux réseau le plus largement installé.

RRDTool

http://oss.oetiker.ch/rrdtool/. ***RRD*** est l'abréviation de ***Round Robin Database***. RRD est une base de données qui stocke les informations de façon très compacte sans expansion avec le temps. ***RRDTool*** fait référence à une suite d'outils qui vous permettent de créer et de modifier les bases de données RRD, ainsi que générer des graphiques utiles pour présenter les données. Il est utilisé pour garder la trace de séries chronologiques de données (telles que la bande passante du réseau, la température de la chambre machine, ou la moyenne de la charge du serveur) et peut afficher ces données en termes de moyenne sur le temps.

Notez que RRDTool lui-même ne communique pas avec les périphériques réseau pour retrouver les données. Il s'agit simplement d'un outil de manipulation de la base de données. Vous pouvez utiliser un simple script (généralement en shell ou Perl) pour faire ce travail pour vous. RRDTool est également utilisé par de nombreuses interfaces complètes qui vous offrent une interface web conviviale pour la configuration et l'affichage. Les graphiques RRD vous donnent plus de contrôle sur les options d'affichage et le nombre d'objets disponibles sur un graphique par rapport à MRTG.

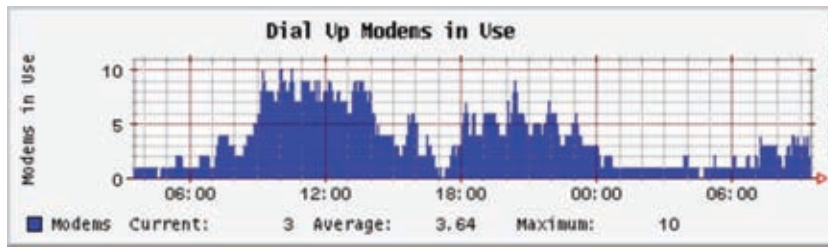


Figure 6.15 : RRDTool vous donne beaucoup de flexibilité dans la façon dont vos données réseau recueillies peuvent être affichées.

RRDTool est inclus dans la quasi-totalité des distributions Linux modernes, et peut être téléchargé à partir de *http://oss.oetiker.ch/rrdtool/*.

ntop

http://www.ntop.org/. Pour l'historique d'analyse du trafic et son usage, vous aimeriez certainement investiguer ***ntop***. 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.

Certains de ses fonctions les plus utiles comprennent :

- L'affichage du trafic peut être trié selon différents critères (source, destination, le protocole, adresse MAC, etc.).
- Statistiques de trafic regroupé par protocole et numéro de port.

- Une matrice de trafic IP qui montre les connexions entre machines.
- Flux réseau pour les routeurs ou les commutateurs qui supportent le protocole NetFlow.
- Identification du système d'exploitation hôte.
- Identification du trafic P2P.
- De nombreuses cartes graphiques.
- Perl, PHP, et API Python.

Ntop est disponible à partir de *http://www.ntop.org/* et est disponible pour la plupart des systèmes d'exploitation. Il est souvent inclus dans un grand nombre de distributions Linux populaires, y compris RedHat, Debian et Ubuntu. Pendant qu'il peut être laissé actif pour recueillir des données historiques, ntop peut être assez processeur intensif selon la quantité de trafic observée. Si vous allez l'exécuter pendant de longues périodes, vous devez surveiller l'utilisation de l'unité centrale de traitement de la machine de surveillance.

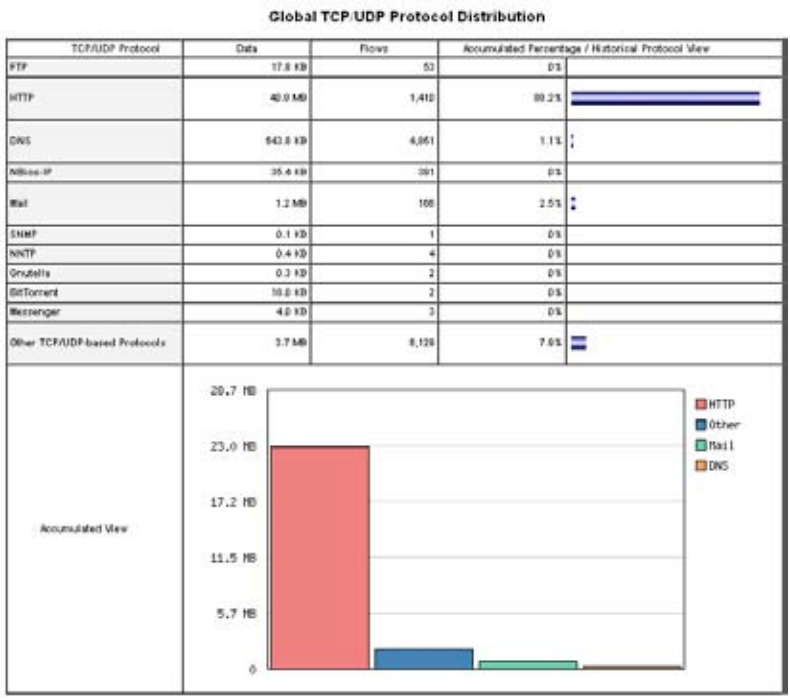


Figure 6.16 : ntop affiche une mine d'informations sur la façon dont votre réseau est utilisé par des clients et des serveurs.

Le principal inconvénient de ntop est qu'il ne fournit pas d'information instantanée, seulement des totaux et moyennes à long terme. Cela peut le rendre difficile à utiliser pour diagnostiquer un problème soudain.

Cacti

http://www.cacti.net/. ***Cacti*** est un frontal pour RRDTool. Il stocke toutes les informations nécessaires pour créer des graphiques dans une base de données MySQL. Le frontal est écrit en PHP. Cactus fait le travail de maintenance de graphiques, de sources de données, et gère la collecte des données. Il existe un support pour les dispositifs SNMP, et des scripts personnalisés peuvent facilement être écrits pour sonder virtuellement n'importe quel événement réseau concevable.

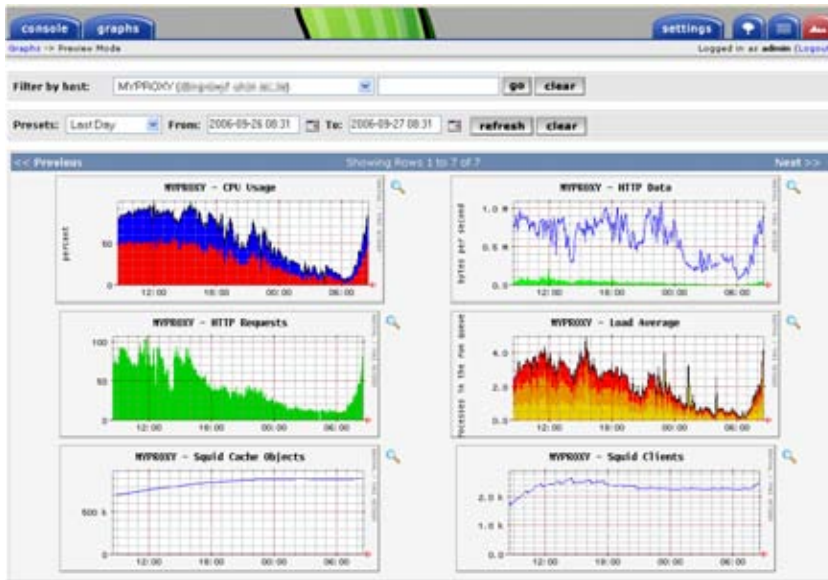


Figure 6.17 : Cacti permet de gérer le sondage de vos périphériques réseau, et peut construire des visualisations du comportement réseau très complexes et très informatives.

Cacti peut être quelque peu déroutant à configurer, mais une fois que vous utilisez la documentation et les exemples, il peut produire des graphiques très impressionnants. Il y a des centaines de modèles pour les différents systèmes disponibles sur le site web de Cacti, et son code est en développement rapide.

NetFlow

NetFlow est un protocole IP inventé par Cisco pour la collecte d'informations sur le trafic. Du site Web de Cisco, il est cité :

> *Cisco IOS NetFlow fournit efficacement un ensemble de services pour les applications IP, y compris la comptabilité du trafic réseau, la facturation basée sur l'usage réseau, la planification du réseau, la sécurité, les capacités de surveillance de déni de service (Denial of Service) et la surveillance réseau. NetFlow fournit des informations précieuses sur les utilisateurs du réseau et les applications, les temps d'usage de pointe et le routage du trafic.*

Les routeurs Cisco peuvent générer l'information NetFlow qui est disponible à partir du routeur sous la forme de paquets UDP. NetFlow est aussi moins CPU

intense sur les routeurs Cisco compare a l'usage de SNMP. Il fournit également des informations plus granulaires que SNMP, vous donnant une image plus détaillée de l'usage du port et protocole.

Cette information est recueillie par un collecteur NetFlow qui stocke et présente les données comme un agrégat au fil du temps. En analysant les flux de données, on peut dresser sur un tableau des flux de trafic et le volume de trafic dans un réseau ou sur une connexion. Il y a plusieurs collecteurs NetFlow commerciaux et libres disponibles. Ntop est un outil gratuit qui peut agir comme un collecteur et sonde NetFlow. Un autre s'appelle Flowc (voir ci-dessous).

Il peut également être souhaitable d'utiliser NetFlow comme un outil de contrôle intermittent grâce a un aperçu rapide des données au cours d'une crise réseau. Pensez à NetFlow comme une alternative à SNMP pour dispositifs Cisco. Pour plus d'informations sur NetFlow, voir *http://en.wikipedia.org/wiki/Netflow*.

Flowc

http://netacad.kiev.ua/flowc/. ***Flowc*** est un collecteur NetFlow (NetFlow voir ci-dessus) libre. Il est léger et facile à configurer. Flowc utilise une base de données MySQL pour Stocker les informations de trafic agrégées. Par conséquent, il est possible de générer vos propres rapports à partir des données en utilisant SQL, ou utiliser des générateurs de rapport inclus. Les générateurs de rapport intégrés produisent des rapports en HTML, texte ou un format graphique.

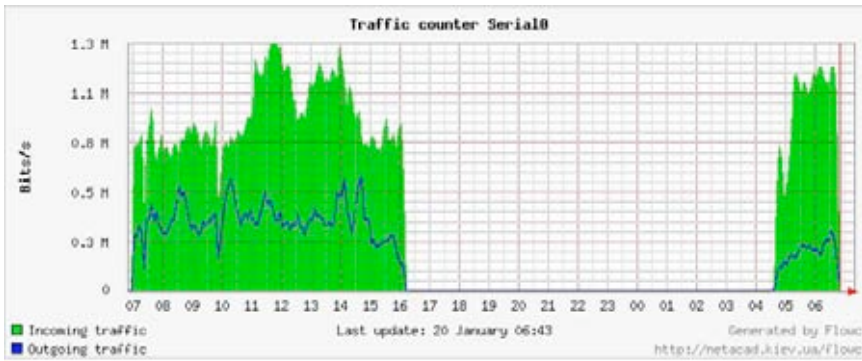


Figure 6.18 : Un diagramme typique généré par Flowc.

Le grand écart dans les données indique probablement une panne réseau. Les outils de tendance ne vont pas généralement vous aviser d'une coupure de courant, mais simplement enregistrer son occurrence. Pour être informé lorsque des problèmes de réseau surviennent, utilisez un outil de surveillance en temps réel tels que Nagios (voir **Page 202**).

SmokePing

http://oss.oetiker.ch/smokeping/. ***SmokePing*** est un outil de mesure de latence de luxe écrit en Perl. Il peut mesurer, stocker et afficher la latence, la distribution de latence et la perte de paquets sur un seul graphique. SmokePing

utilise RRDTool pour le stockage des données, et peut imprimer des graphiques très informatives qui présentent l'information sur l'état de votre connexion réseau jusqu'à la minute près.

Il est très utile d'exécuter SmokePing sur un hôte qui a une bonne connectivité à l'ensemble de votre réseau. Au fil du temps, les tendances révélées peuvent pointer a toute sorte de problèmes de réseau. Combiné avec MRTG (voir **Page 192**) ou Cacti (voir **Page 195**), vous pouvez observer l'effet que l'encombrement du réseau a sur la perte de paquets et la latence. SmokePing peut optionnellement envoyer des alertes lorsque certaines conditions sont remplies, comme par exemple lorsqu'une trop grande perte de paquets est observée sur une liaison pour une période de temps prolongé. Un exemple de SmokePing en action est illustré à la **Figure 6.19**.

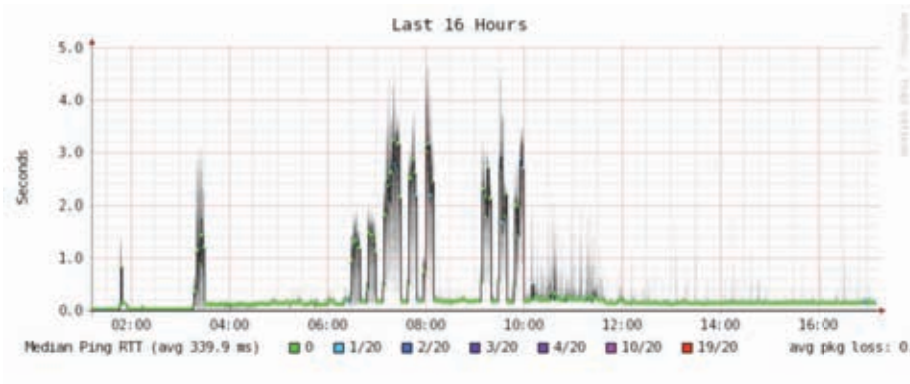


Figure 6.19 : SmokePing peut afficher simultanément la perte de paquets et la latence dans un seul graphique.

EtherApe

http://etherape.sourceforge.net/. ***EtherApe*** affiche une représentation graphique du trafic réseau. Les hôtes et les liaisons changent de taille en fonction du volume de trafic envoyé et reçu. Le changement de couleurs est utilisé pour représenter le protocole le plus utilisé. Comme avec wireshark et tcpdump, les données peuvent être saisies "off the wire" à partir d'une connexion réseau ou lues a partir d'un fichier de capture tcpdump.

EtherApe ne montre pas tout à fait autant de détails que ntop, mais ses exigences en ressources sont beaucoup plus légères.

iptraf

http://iptraf.seul.org/. ***Iptraf*** est un léger mais puissant moniteur de réseau local LAN. Il a une interface ncurses et fonctionne dans une ligne de commande shell. Iptraf prend un moment pour mesurer le trafic observe, et affiche ensuite diverses statistiques réseau, y compris les connexions TCP et UDP , l'information ICMP et OSPF, les flux de trafic, les erreurs de type IP checksum, et plus encore. Il s'agit d'un programme simple à utiliser qui consomme un minimum de ressources système.

Bien qu'il ne tienne pas de données historiques, il est très utile pour l'affichage instantané de rapport d'usage.

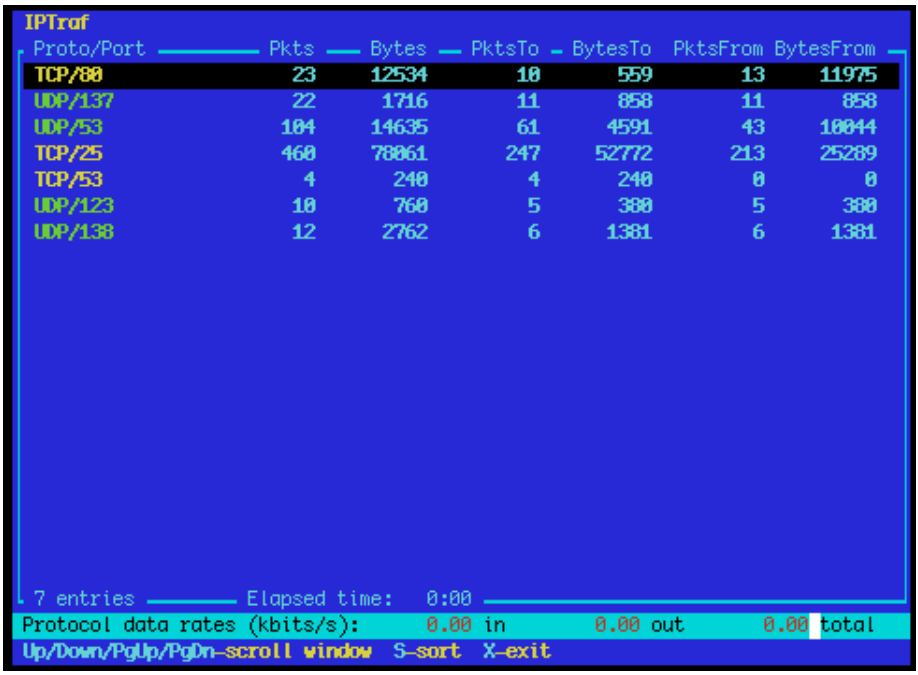


Figure 6.20 : Répartition des statistiques du trafic iptraf par port.

Argus

http://qosient.com/argus/. L'acronyme ***Argus*** dénotes ***Audit Record Generation and Utilization System***. Argus est aussi le nom du dieu de la mythologie grecque qui a des centaines d'yeux.

Du site Argus, il est cité :

> *Argus génère des flux de statistiques comme la connectivité, la capacité, demande, perte, retard, et la latence par transaction. Argus peut être utilisé pour analyser et rapporter sur le contenu des fichiers de capture de paquets ou il peut fonctionner comme un moniteur continu,'examinant les données à partir d'une interface vive; générant un journal d'audit de toutes les activités réseau vues dans le flux de paquets. Argus peut être déployé pour surveiller tous les périphériques système individuels ou l'ensemble de l'activité réseau d'une entreprise. Comme moniteur continu, Argus offre des modèles de traitement des données de type push et pull afin de permettre des stratégies souples pour la collecte des données d'audit réseau. Les clients de données Argus supportent un éventail d'opérations, telles que le tri, l'agrégation, l'archivage et l'établissement de rapports.*

Argus est constitué de deux parties : un maître collecteur qui lit les paquets à partir d'un périphérique réseau et un client qui se connecte au maître et affiche

les statistiques d'usage. Argus fonctionne sur BSD, Linux, et la plupart des autres systèmes UNIX.

NeTraMet

http://freshmeat.net/projects/netramet/. ***NeTraMet*** est un autre outil populaire d'analyse de flux. Comme Argus, NeTraMet se compose de deux parties : un collecteur qui rassemble des statistiques via SNMP, et un gestionnaire qui spécifié les flux qui doivent être surveillés. Les flux sont indiqués en utilisant un simple langage de programmation qui définit les adresses utilisées sur chaque extrémité, et peut inclure Ethernet, IP, information de protocole, ou d'autres identificateurs. NeTraMet fonctionne sur DOS et la plupart des systèmes UNIX, y compris Linux et BSD.

L'essai de débit

A quelle vitesse le réseau peut aller ? Quelle est la capacité réelle utilisable d'une liaison réseau ? Vous pouvez obtenir une très bonne estimation de votre capacité de débit en inondant la liaison avec le trafic et en mesurant le temps qu'il faut pour transférer les données.

Figure 6.21 : Des outils tels que celui-ci venant de SpeedTest.net sont jolis, mais ne vous donnent pas toujours une idée précise de la performance du réseau.

Bien qu'il existe des pages web disponibles capables de réaliser un "essai rapide" sur votre navigateur (comme *http://www.dslreports.com/stest* ou *http://speedtest.net/*), ces tests deviennent de plus en plus inexacts des que vous vous éloignez de la source d'essai. Pire encore, ils ne vous permettent pas de tester la vitesse d'une liaison donnée, mais seulement la vitesse de votre liaison à un site

particulier sur l'Internet. Voici quelques outils qui vous permettent d'effectuer des essais sur le débit de vos propres réseaux.

ttcp

http://ftp.arl.mil/ftp/pub/ttcp/. ***ttcp*** fait actuellement partie de la plupart des systèmes de type Unix C'est un outil simple de test de performance de réseau qui fonctionne sur chaque côté d'une liaison 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 debit 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.

bing

http://fgouget.free.fr/bing/index-en.shtml. Au lieu d'inonder une connexion de données et voir combien de temps prend le transfert pour compléter, ***Bing*** tente d'estimer le débit disponible d'une connexion point à point en analysant les temps aller-retour pour des paquets ICMP de différentes tailles. Bien qu'il ne soit pas toujours aussi précis comme test d'inondation, il peut fournir une bonne estimation sans transmettre un grand nombre d'octets.

Comme bing utilise l'écho des requêtes ICMP, il peut estimer la bande passante disponible sans avoir à exécuter un client à l'autre extrémité, et peut même tenter d'estimer le débit des liaisons en dehors de votre réseau. Comme il utilise relativement peu de bande passante, bing peut vous donner une idée de la performance du réseau sans courir le risque des coûts qu'un test d'inondation engagerait certainement.

Outils en temps réel

Il est souhaitable de savoir quand les gens tentent de pénétrer dans votre réseau, ou quand une partie du réseau est en panne. Comme aucun administrateur système ne peut être en train de surveiller un réseau tout le temps, il y a des programmes qui sont destinés à surveiller constamment l'état du réseau et qui peuvent envoyer des alertes lorsqu'un événement notable se produit. Voici quelques outils libres qui peuvent aider à s'acquitter de cette tâche.

Snort

Snort (*http://www.snort.org/*) est un sniffer de paquets et de journalisation qui peut être utilisé comme un système léger de détection d'intrusion réseau. Il est fondé sur des journalisations basées sur des règles et peut accomplir l'analyse de protocole, la recherche de contenu, et la correspondance des paquets. Il peut être utilisé pour détecter une variété d'attaques et de sondes, telles que les sondes furtifs des ports, les attaques CGI, les sondes SMB, des tentatives d'empreintes digitales des système d'exploitation, et de nombreux autres types de schémas de trafic anormal. Snort a une capacité d'alerte en temps réel qui peut notifier les administrateurs sur les problèmes à mesure qu'ils se produisent en utilisant une variété de méthodes.

L'installation et l'exécution de Snort n'est pas triviale, et peut exiger une machine dédiée à la surveillance avec des ressources considérables en fonction de la quantité de trafic réseau. Heureusement, Snort est très bien documenté et a une forte communauté d'utilisateurs. En implémentant un ensemble compréhensif de règles Snort, vous pouvez identifier un comportement inattendu qui, autrement, pouvait mystérieusement consommer votre bande passante Internet.

Voir *http://snort.org/docs/* pour une liste exhaustive des ressources d'installation et de configuration.

Apache : mod_security

mod_security (*http://www.modsecurity.org/*) est un moteur libre de détection d'intrusion et de prévention pour les applications web. Ce type d'outil de sécurité est également connu comme un ***pare-feu d'application web*** (en anglais *web application firewall*). Mod_security augmente la sécurité des applications web en protégeant les applications Web des attaques connues et inconnues. Il peut être utilisé seul, ou en tant que module dans le serveur web Apache (*http://www.apache.org/*).

Il existe plusieurs sources pour les règles mod_security mises à jour qui aident à protéger contre les exploitations de sécurité les plus récentes. Une excellente ressource est GotRoot, qui maintient un énorme répositoire de règles qui est mis à jour fréquemment :

http://gotroot.com/tiki-index.php?page=mod_security + rules

La sécurité des applications web est importante dans la défense contre les attaques sur votre serveur web qui pourrait entraîner le vol des données précieuses ou personnelles, ou une situation ou le serveur est utilisé pour lancer des attaques ou envoyer des spams aux autres utilisateurs de l'Internet. En plus d'être préjudiciable à l'Internet dans son ensemble, ces intrusions peuvent sérieusement réduire votre bande passante disponible.

Nagios

Nagios (*http://nagios.org/*) est un logiciel qui surveille les hôtes et services sur votre réseau, vous avisant immédiatement lorsque des problèmes se posent. Il peut envoyer des notifications par e-mail, SMS ou par exécution d'un script, et envoiera des notifications à la personne ou un groupe en fonction de la nature du problème. Nagios fonctionne sur Linux ou BSD et fournit une interface web montrant à la minute près l'état du système.

Nagios est extensible, et peut surveiller l'état de virtuellement n'importe quel événement réseau. Il effectue des contrôles en exécutant des petits scripts à intervalles réguliers, et compare les résultats des contrôles à une réponse attendue. Cela peut produire des contrôles beaucoup plus sophistiqués qu'une simple sonde réseau. Par exemple, ping (**Page 188**) peut vous dire qu'une machine est en marche, et nmap peut rapporter qu'un port TCP répond aux requêtes, mais Nagios peut actuellement retrouver une page web ou faire une demande de base de données et vérifier que la réponse n'est pas une erreur.

Nagios peut même vous avertir lorsque la bande passante, la perte de paquet, la température de la chambre machine, ou un autre indicateur de la santé réseau traverse un seuil particulier. Cela peut vous donner un avertissement sur les problèmes de réseau, vous permettant souvent de résoudre le problème avant que les utilisateurs aient la possibilité de se plaindre.

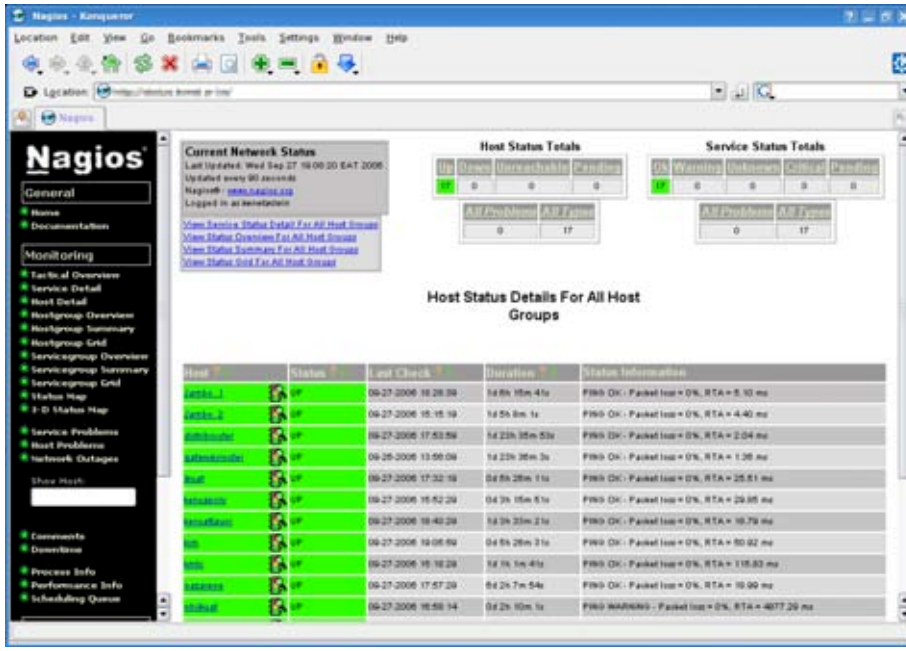


Figure 6.22 : Nagios vous tient informé du moment où une panne réseau ou rupture de service se produit.

Zabbix

Zabbix (*http://www.zabbix.org/*) est un outil de surveillance temps réel libre qui est une sorte d'hybride entre Nagios et Cacti. Il emploie une base de données SQL pour le stockage des données, a son propre logiciel graphique, et effectue toutes les fonctions que vous attendez d'un moniteur temps réel moderne (tel que la sonde SNMP et une notification instantanée des conditions d'erreur). Zabbix est distribué sous licence GNU General Public License.

Autres outils utiles

Il y a des milliers d'outils libres de surveillance réseau qui répondent à des besoins très spécialisés. Voici quelques-uns de nos favoris qui ne font pas tout à fait partie des catégories ci-dessus.

Driftnet et Etherpeg

Ces outils décodent les données graphiques (tels que les fichiers GIF et JPEG) et les affichent comme collage. Comme indiqué précédemment, les outils de ce type sont d'un usage limité en dépannage de problèmes, mais sont très utiles pour démontrer l'insécurité des protocoles non cryptés. ***Etherpeg*** est disponible à partir de *http://www.etherpeg.org/* et ***Drifnet*** peut être téléchargé à partir de *http://www.ex-parrot.com/~chris/Driftnet/*.

Figure 6.23 : Un collage web généré par Etherpeg.

ngrep

ngrep fournit la plupart des fonctionnalités de correspondance de formes GNU mais les applique au trafic réseau. Il reconnaît actuellement IPv4 et IPv6, TCP, UDP, ICMP, IGMP, PPP, SLIP, FDDI, Token Ring, et bien plus encore. Comme il fait largement usage des correspondances des expressions régulières, il s'agit d'un outil adapté aux utilisateurs avancés ou ceux qui ont une bonne connaissance des expressions régulières.

Mais vous n'avez pas nécessairement besoin d'être un expert regex pour être en mesure de faire usage du ngrep basic. Par exemple, pour afficher tous les paquets contenant la chaîne GET (probablement les requêtes HTTP), essayez ceci :

```
# ngrep -q GET
```

Les correspondances de forme peuvent être restreintes à une suite particulière de protocoles, ports, ou d'autres critères en utilisant des filtres BPF. BPF est le langage de filtrage utilisé par les outils d'inhalation de paquet (packet sniffing) communs, tels que tcpdump et snoop. Pour afficher les chaînes GET ou POST envoyées au port destination 80, utilisez cette ligne de commande :

```
# ngrep -q 'GET | POST' port 80
```

En utilisant ngrep de façon créative, vous pouvez détecter toute activité partant des virus aux e-mails de type spam. Vous pouvez télécharger ngrep sur *http://ngrep.sourceforge.net/*.

Qu'est ce qui est normal ?

Si vous êtes à la recherche d'une réponse définitive quant à ce que le modèle de votre trafic devrait ressembler, vous allez être déçu. Il n'y a pas de réponse correcte absolue à cette question, mais se basant sur certains travaux, vous pouvez déterminer ce qui est normal pour votre réseau. Bien que chaque environnement soit différent, certains des facteurs qui peuvent influencer l'apparence de vos modèles de trafic sont les suivants :

- La capacité de votre connexion Internet.
- Le nombre d'utilisateurs qui ont accès au réseau.
- La politique sociale (octet de tarification, les quotas, système d'honneur, etc.).
- Le nombre, les types, et le niveau des services offerts.
- La santé du réseau (présence de virus, les émissions excessives, boucles de routage, relais e-mail. ouverts, des attaques par déni de service, etc.).
- La compétence des utilisateurs de votre ordinateur.
- L'emplacement et la configuration des structures de contrôle (pare-feu, serveurs Proxy, caches, et ainsi de suite).

Ceci n'est pas une liste définitive, mais devrait vous donner une idée de la façon dont un large éventail de facteurs peut influer sur vos modèles de bande passante. Dans cet esprit, examinons la question des niveaux de référence.

Mise en place d'une référence

Comme chaque environnement est différent, vous devez déterminer par vous-même ce a quoi vos modèles de trafic doivent ressembler dans des situations normales. Ceci est utile car ça vous permet d'identifier les changements au fil du temps, soit soudains ou progressifs. Ces changements peuvent à leur tour indiquer un problème, ou un problème potentiel futur dans votre réseau.

Par exemple, supposons que votre réseau s'arrête et vous n'êtes pas sûr de la cause. Heureusement, vous avez décidé de conserver une représentation graphique des diffusions (broadcasts) en tant que pourcentage de l'ensemble du trafic réseau. Si ce graphique montre une augmentation soudaine de la quantité de trafic de diffusion, cela peut signifier que votre réseau a été infecté par un virus. Sans une idée de ce qui est "normal" pour votre réseau (une référence), vous ne serez pas en mesure de voir que le nombre de diffusions a augmenté, mais seulement qu'il a été relativement élevé, ce qui peut ne pas indiquer un problème.

Les graphiques de référence et les chiffres sont également utiles lors de l'analyse des effets des modifications apportées au réseau. Il est souvent très utile d'expérimenter avec de tels changements en essayant différentes valeurs possibles. Savoir ce à quoi la référence ressemble vous indiquera si vos changements ont conduit à une amélioration ou ont fait pire.

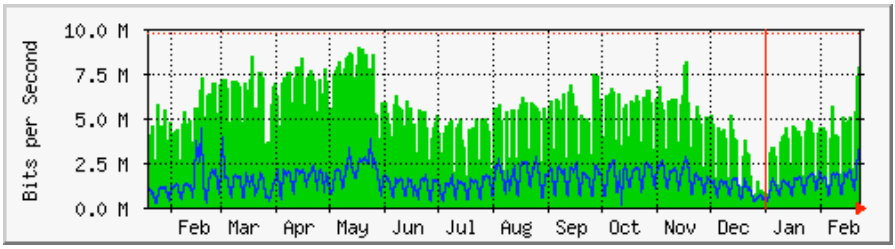


Figure 6.24 : Par la collecte de données sur une longue période de temps, vous pouvez prédire la croissance de votre réseau et apporter des modifications avant que les problèmes se développent.

Dans la **Figure 6.24**, nous pouvons voir l'effet que l'implémentation des sondes délais a eu sur l'utilisation Internet autour de la période de Mai. Si nous n'avions pas conserve une représentation graphique de l'usage de la ligne, nous ne saurions jamais ce que l'effet du changement sur le long terme a été. Lorsque vous regardez un graphique du trafic total après avoir fait les changements, ne supposez pas que simplement parce que le graphique n'a pas changé radicalement vos efforts ont été gaspillés. Vous avez peut-être enlevé l'usage frivole de votre ligne seulement pour le remplacer par un véritable trafic légitime. Vous pouvez ensuite combiner cette référence avec d'autres, disons les 100 premiers sites accédés ou utiliser la moyenne de vos vingt premiers utilisateurs, afin de déterminer si les habitudes ont simplement changé. Comme nous le verrons plus tard, MRTG, RRDTool, et Cacti sont d'excellents outils que vous pouvez utiliser pour maintenir un niveau de référence.

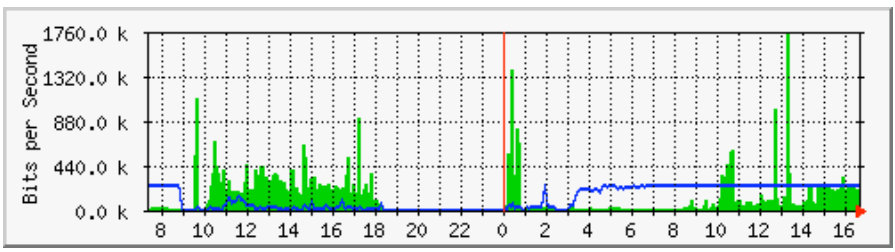


Figure 6.25 : La tendance du trafic à Aidworld enregistrée sur une seule journée.

La **Figure 6.25** montre le trafic sur un pare-feu Aidworld sur une période de 24 heures. Il n'y a apparemment rien de mal à ce graphique, mais les utilisateurs se sont plaints au sujet de la lenteur d'accès à Internet.

La **Figure 6.26** montre que l'utilisation de bande passante pour téléchargement (zone sombre) était plus élevée pendant les heures de travail sur le dernier jour que sur les jours précédents. Une période d'usage de téléchargement élevé commençait chaque matin à 03:00 et finissait normalement a 09:00. Mais le dernier jour, il était toujours en marche à 16h30. Une enquête plus poussée révéla un problème avec le logiciel de sauvegarde qui démarrait à 03:00 tous les jours.

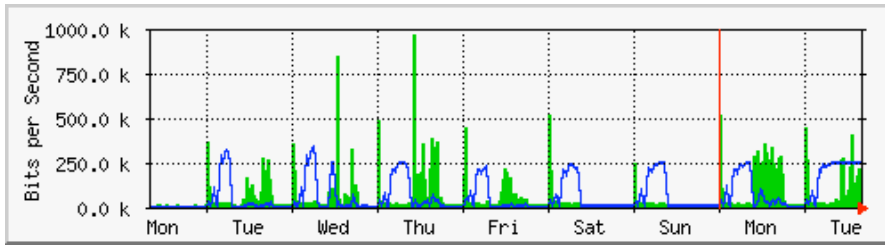


Figure 6.26 : Le même réseau connecté sur une semaine entière, révèle un problème avec les sauvegardes, ce qui a provoqué la congestion inattendu pour les utilisateurs du réseau.

La **Figure 6.27** montre les mesures de latence sur la même connexion, tel que mesuré par un logiciel appelé SmokePing. La position des points montre la latence moyenne, tandis que la fumée grise indique la répartition de latence (jitter). La couleur des points indique le nombre de paquets perdus. Ce graphique sur une période de quatre heures ne permet pas d'identifier s'il existe des problèmes sur le réseau.

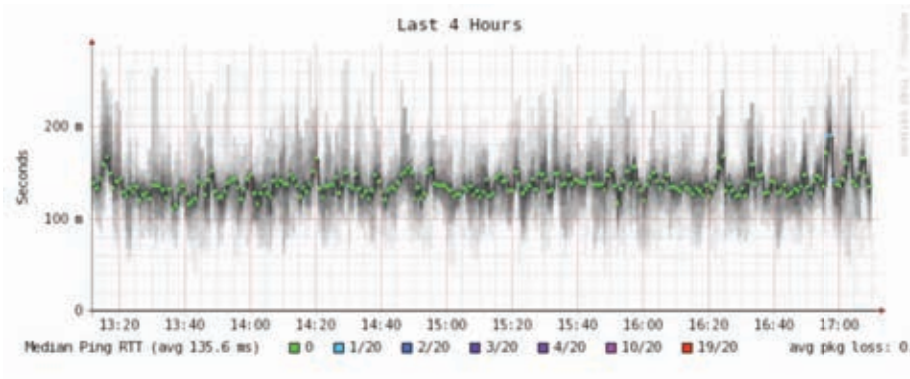


Figure 6.27 : Quatre heures de latence et de perte de paquets.

Le graphique suivant (**Figure 6.28**) présente les mêmes données sur une période de 16 heures. Cela indique que les valeurs dans le graphique ci-dessus sont proches de la normale (référence), mais qu'il y avait des augmentations importantes de latence à plusieurs reprises tôt le matin, jusqu'à 30 fois la valeur de référence. Cela indique qu'une surveillance supplémentaire doit être effectuée au cours de ces périodes tôt le matin pour établir la cause de la haute latence, ce qui est probablement un trafic lourd quelconque.

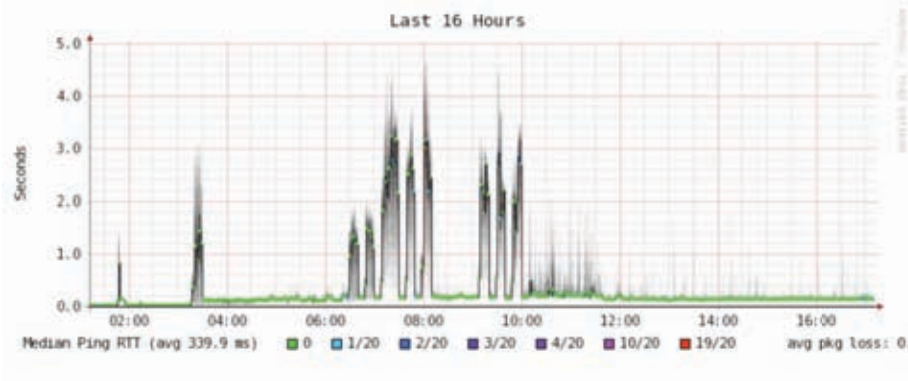


Figure 6.28 : Une plus grande propagation de la latence est révélée dans un journal de 16 heures.

La **Figure 6.29** montre que la latence du mardi était bien pire que le dimanche ou le lundi, en particulier au début de la matinée. Cela pourrait indiquer que quelque chose a changé sur le réseau.

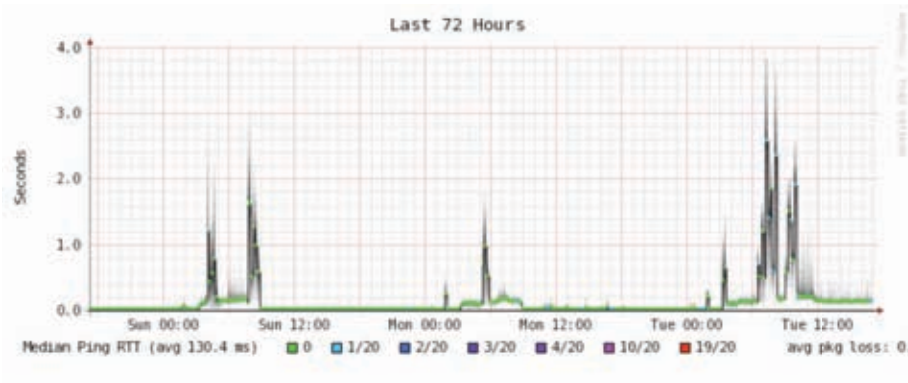


Figure 6.29 : Le zooming d'une semaine révèle une nette répétition de l'augmentation de latence et la perte de paquets dans les premières heures du jour.

Comment puis-je interpréter le graphique de trafic ?

Dans un graphique basic du flux d'un réseau (tel que celui généré par le moniteur de réseau MRTG), la zone verte indique le ***trafic entrant***, tandis que la ligne bleue indique le ***trafic sortant***. Le trafic entrant est le trafic qui provient d'un autre réseau (généralement Internet) et est adressé à un ordinateur de votre réseau. Le trafic sortant est le trafic qui provient de votre réseau, et est adressé à un ordinateur quelque part sur l'Internet. En fonction du type d'environnement réseau que vous avez, le graphique vous aidera à comprendre comment votre réseau est effectivement utilisé. Par exemple, la surveillance des serveurs révèle généralement de plus grandes quantités de trafic sortant quand les serveurs répondent à la demande (telles que l'envoi de courrier ou servir des pages web), alors que la surveillance des machines clientes pourrait révéler des montants

plus élevés de trafic entrant dans les machines quand elles reçoivent des données a partir des serveurs.

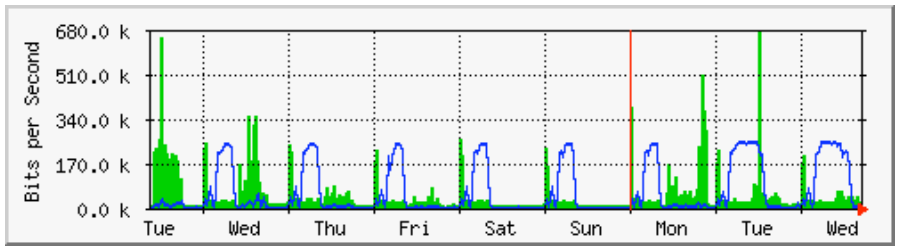


Figure 6.30 : Le graphique classique du flux réseau. La zone sombre représente le trafic entrant, tandis que la ligne représente le trafic sortant. Les arcs répétitifs du trafic sortant montrent à quel moment du soir les sauvegardes sont terminées.

Les modèles du trafic varient en fonction de ce que vous êtes en train de surveiller. Un routeur va normalement avoir plus de trafic entrant que le trafic sortant quand les utilisateurs téléchargent des données à partir d'Internet. Un excès de bande passante sortante qui n'est pas transmis par les serveurs de votre réseau peut indiquer la présence un client peer-to-peer, un serveur non autorisé, ou même un virus sur un ou plusieurs de vos clients. Il n'y a pas de paramètres qui indiquent ce que le trafic destination au trafic source devrait ressembler. C'est à vous d'établir une base de référence pour comprendre ce à quoi les modèles de trafic normaux ressemblent sur votre réseau.

Détection de surcharge réseau

La **Figure 6.31** montre une connexion Internet surchargée.

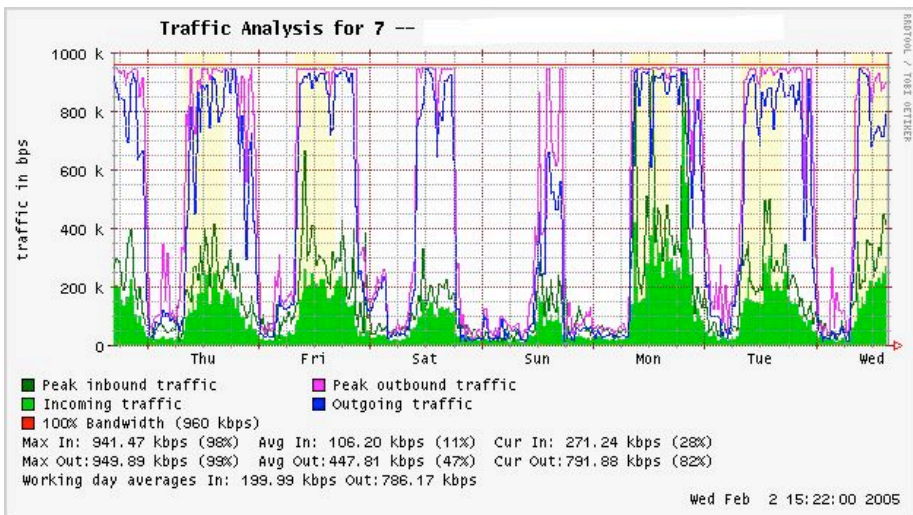


Figure 6.31 : les graphiques à sommets aplatis indiquent qu'une ligne est en train d'utiliser le maximum de bande passante disponible, et est surutilisée pendant ces périodes.

Le signe le plus évident de la surcharge est les sommets plats du trafic sortant au milieu de tous les jours. Les sommets plats (flats tops) peuvent indiquer une surcharge, même s'ils sont bien en deçà de la capacité théorique maximale de la liaison. Dans ce cas, ils peuvent indiquer que vous ne recevez pas assez de bande passante de votre fournisseur de service que vous ne l'attendiez.

Mesurer la 95e percentile

La 95e percentile est un calcul mathématique largement utilisé pour évaluer l'utilisation régulière et soutenue d'une pipe d'un réseau. Sa valeur indique la plus haute consommation de trafic pour une période donnée. Le calcul de la 95 e percentile signifie que 95% du temps, l'usage est en dessous d'un certain montant, et 5% du temps l'usage est au-dessus de ce montant. La 95e centile est une bonne valeur à utiliser pour montrer que la bande passante est effectivement utilisée au moins 95% du temps.

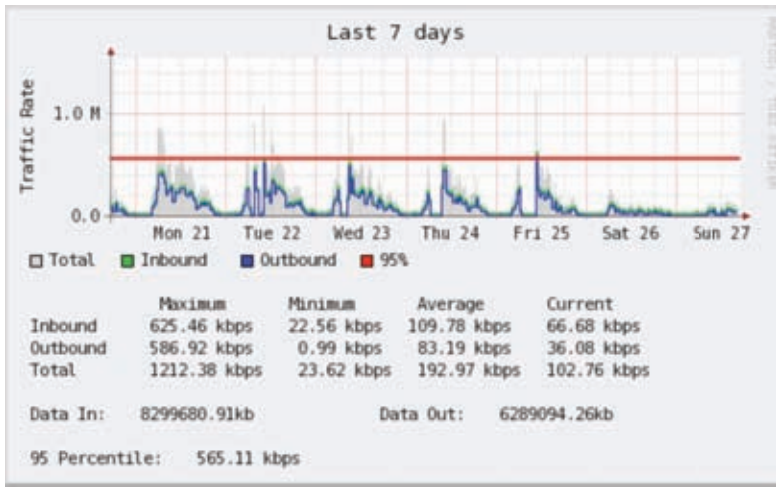


Figure 6.32 : La ligne horizontale indique le montant de la 95 e percentile.

MRTG et de Cacti calculera le 95 e percentile pour vous. Ceci est un échantillon graphique d'une connexion 960 kbps. La 95e percentile est montrée à 945 kbps après rejet de 5% du trafic le plus élevé.

Suivi de RAM et CPU usage

Par définition, les serveurs fournissent des services essentiels qui devraient toujours être disponibles. Les serveurs reçoivent et répondent aux demandes client, donnant accès à des services qui sont l'essence même d'avoir un réseau en premier lieu. Par conséquent, les serveurs doivent disposer de suffisamment de capacité matérielle pour tenir compte de la charge de travail. Cela signifie qu'ils doivent disposer de suffisamment de RAM, de stockage et la puissance de traitement nécessaire pour répondre au nombre des requêtes des clients. Sinon,

le serveur va prendre plus de temps pour répondre, ou dans le pire des cas, il peut être incapable de répondre. Étant donné que les ressources matérielles sont limitées, il est important de garder une trace de la façon dont les ressources système sont utilisées. Si un serveur de base (comme un serveur Proxy ou le serveur de messagerie) est submergé par les demandes, les temps d'accès deviennent longs. Cela est souvent perçu par les utilisateurs comme un problème de réseau.

Il y a plusieurs programmes qui peuvent être utilisés pour surveiller les ressources sur un serveur. La méthode la plus simple sur une machine Windows est de l'accès au gestionnaire des tâches (Task Manager) en utilisant la touche **Ctrl Alt + Del**, puis cliquez sur l'onglet Performance. Sur un système Linux ou BSD, vous pouvez taper **`top`** dans une fenêtre de terminal. Pour maintenir les journaux historiques de ces performances, MRTG ou RRDTool (sur **Page 192**) peuvent également être utilisés.

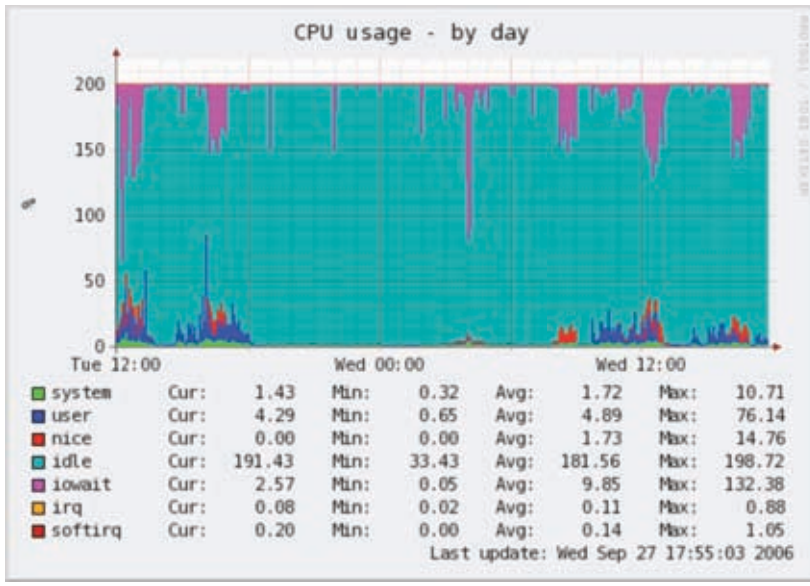


Figure 6.33 : RRDTool peut montrer des données arbitraires, telles que l'usage mémoire et CPU, exprimées en moyenne sur le temps.

Les serveurs de messagerie exigent un espace suffisant car certaines personnes peuvent préférer laisser leurs e-mails sur le serveur pendant de longues périodes de temps. Les messages peuvent s'accumuler et remplir le disque dur, en particulier si les quotas ne sont pas en service. Si le disque ou la partition utilisée pour le stockage du courrier se remplit, le serveur de messagerie ne peut pas recevoir de courrier. Si ce disque est aussi utilisé par le système, toutes sortes de problèmes du système peuvent se produire comme le système d'exploitation manque d'espace d'échange et le stockage temporaire.

Les serveurs de fichiers doivent être surveillés, même s'ils ont des gros disques. Les utilisateurs trouveront un moyen de remplir n'importe quelle taille de disque plus rapidement que vous ne le pensez. L'usage disque peut être assurée

par le recours à des quotas, ou tout simplement par la surveillance d'usage et informer les utilisateurs quand ils utilisent trop. Nagios (voir **Page 202**) peut vous avertir lorsque l'usage disque, l'utilisation CPU, ou d'autres ressources du système franchissent un seuil critique.

Si une machine ne répond plus ou est lente, et les mesures montrent que les ressources système sont fortement utilisées, ceci peut être un signe qu'une mise à niveau est nécessaire. Si l'usage du processeur est constamment supérieur à 60% du total, il peut être temps de mettre à niveau le processeur. Une faible vitesse pourrait également provenir de l'insuffisance de RAM. Assurez-vous de vérifier l'ensemble l'usage du CPU, RAM, et de l'espace disque avant de décider de mise à niveau d'un composant particulier.

Un moyen simple de vérifier si une machine a une RAM insuffisante consiste à examiner la lumière du disque dur. Quand la lumière est allumée constamment, cela signifie généralement que la machine est constamment en train d'échanger des grandes quantités de données vers et à partir du disque. Ceci est connu sous le nom d'***emballage*** (en anglais *thrashing*), et est très mauvais pour la performance. Il peut généralement être résolu par la recherche du processus qui utilise plus de RAM, et le terminer ou le reconfigurer. A défaut, le système a besoin de plus de RAM.

Vous devriez toujours déterminer si c'est plus rentable de mettre à niveau une composante individuelle ou l'achat d'une toute nouvelle machine. Certains ordinateurs sont difficiles ou impossibles à mettre à niveau, et il coûte souvent plus de remplacer des composants individuels que de remplacer l'ensemble du système. Comme la disponibilité des pièces et des systèmes varie largement dans le monde entier, assurez-vous de balancer le coût des pièces par rapport à l'ensemble du système, y compris l'expédition et les taxes lors de la détermination du coût de la mise à niveau.

7
Energie Solaire

Ce chapitre fournit une introduction aux éléments d'un ***système photovoltaïque autonome***. Le mot autonome se réfère au fait que le système fonctionne sans connexion à un réseau électrique. Dans ce chapitre, nous présentons les concepts fondamentaux de la production et du stockage de l'énergie solaire photovoltaïque et proposons une méthode pour la conception d'un système fonctionnel ayant un accès limité aux informations et aux ressources.

Ce chapitre traite seulement l'usage de l'énergie solaire pour la production directe d'électricité (***énergie solaire photovoltaïque***). L'énergie solaire peut aussi être utilisée pour chauffer des combustibles (***énergie solaire thermique***) utilisés comme source de chaleur, ou pour faire tourner une turbine génératrice d'électricité. Les systèmes d'énergie solaire thermique sortent du champ d'application du présent chapitre.

L'énergie solaire

Un système photovoltaïque est basé sur la capacité de certains matériaux à convertir l'énergie rayonnante du soleil en énergie électrique. Le montant total d'énergie solaire qui éclaire un secteur donné est connu sous le nom d'***irradiance*** (***G***) et elle est mesurée en ***watts par mètre carré*** (***W/m²***). Les valeurs instantanées sont normalement traduites en moyenne sur une période de temps, de sorte qu'il est courant de parler de l'irradiance totale par heure, par jour ou par mois.

Bien sûr, la quantité exacte de rayonnement qui arrive à la surface de la Terre ne peut pas être prédit avec une grande précision à cause des variations climatiques naturelles. Par conséquent, il est nécessaire de travailler avec des données statistiques basées sur “l'histoire solaire” d'un lieu particulier. Ces données sont recueillies par une station météorologique sur une longue période de temps et sont disponible à partir d'un certain nombre de sources, comme des tables ou des bases de données. Dans la plupart des cas, il peut être difficile de trouver des informations détaillées sur un lieu spécifique, et vous devrez travailler avec des valeurs approximatives.

Quelques organismes ont produit des cartes des valeurs moyennes de l'irradiation solaire globale quotidienne pour des régions différentes. Ces valeurs

sont connues sous le nom d'***heures d'équivalent plein soleil*** (*PSH, Pic Sun Hours*). Vous pouvez utiliser la valeur d'heures d'équivalent plein soleil de votre région pour vous simplifier les calculs. Une unité d'équivalent plein soleil correspond à un rayonnement de 1000 watts par mètre carré. Si nous trouvons qu'un endroit dispose de 4 PSH dans le pire des mois, cela signifie que, dans ce mois nous ne devrions pas nous attendre à une irradiation quotidienne de plus de 4000 W/m^2 (jour). Les heures d'équivalent plein soleil sont un moyen facile pour représenter le pire des cas d'irradiation moyenne par jour.

Des cartes PSH à basse résolution sont disponibles à partir d'un certain nombre de sources en ligne, tels que *http://www.solar4power.com/solar-power-global-maps.html*. Pour des plus amples informations, consultez un fournisseur d'énergie solaire ou une station météorologique.

Qu'en est-il de l'énergie éolienne ?

Il est possible d'utiliser une éolienne en place de panneaux solaires quand un système autonome est conçu pour être installé sur une colline ou une montagne. Pour être efficace, la vitesse moyenne du vent au cours de l'année devrait être d'au moins 3 à 4 mètres par seconde, et l'éolienne doit être à une hauteur de 6 mètres plus élevée que d'autres objets dans un périmètre de 100 mètres. Un endroit éloigné de la côte manque généralement de l'énergie éolienne suffisante pour supporter un système éolien.

De manière générale, les systèmes photovoltaïques sont plus fiables que les éoliennes car la lumière du soleil est plus disponible qu'un vent régulier dans la plupart des endroits. Cependant, les éoliennes sont en mesure de charger les batteries même la nuit, tant qu'il y a assez de vent. Il est bien entendu possible de combiner le vent avec l'énergie solaire pour couvrir les moments de couverture nuageuse prolongés ou lorsqu'il n'y a pas suffisamment de vent.

Pour la plupart des endroits, le coût d'une bonne éolienne n'est pas justifié à cause de la faible quantité d'énergie qu'elle va ajouter à l'ensemble du système. Ce chapitre se concentrera donc sur l'emploi de panneaux solaires pour la production d'électricité.

Les composantes du système photovoltaïque

Un système photovoltaïque de base est constitué de quatre composantes principales : le ***panneau solaire***, les ***batteries***, le ***régulateur*** et la ***charge***. Les panneaux sont responsables de la collecte de l'énergie du soleil et de la production d'électricité. La batterie stocke l'énergie électrique pour une utilisation ultérieure. Le régulateur veille à ce que le panneau et la batterie travaillent ensemble de façon optimale. La charge se réfère à tout dispositif qui nécessite l'énergie électrique, et est la somme de la consommation de tous les équipements électriques connectés au système. Il est important de se rappeler que les panneaux solaires et les batteries utilisent le ***courant continu*** (*DC, Direct Current*).

Il sera également nécessaire d'inclure dans votre système photovoltaïque un certain type de ***convertisseur*** si la gamme de tension de fonctionnement de votre matériel n'est pas adaptée à la tension fournie par votre batterie. Si votre équipement utilise une source de tension DC qui est différente de celle fournie par la batterie, vous aurez besoin d'utiliser un convertisseur DC/DC. Si certains de vos équipements nécessitent une alimentation en ***courant alternatif*** (*AC, Alternating Current*), vous aurez besoin d'utiliser un convertisseur DC/AC, également connu sous le nom d'***onduleur***.

Chaque système électrique devrait également intégrer différents dispositifs de sécurité dans le cas où quelque chose tournerait mal. Ces dispositifs comprennent un bon câblage, des disjoncteurs, des parafoudres, les fusibles, les tiges de sol, éclairage d'arrêt, etc.

Le panneau solaire

Le ***panneau solaire*** est composé de cellules solaires qui recueillent le rayonnement solaire et le transforme en énergie électrique. Cette partie du système est parfois dénommé ***module solaire*** ou ***générateur photovoltaïque***. Des ***matrices de panneaux solaires*** peuvent être constituées par le raccordement d'un ensemble de panneaux en série et/ou en parallèle afin de fournir une énergie nécessaire pour une charge donnée. Le courant électrique fourni par un panneau solaire varie proportionnellement à la radiation solaire. Cela varie selon les conditions climatiques, l'heure de la journée, et le temps de l'année.

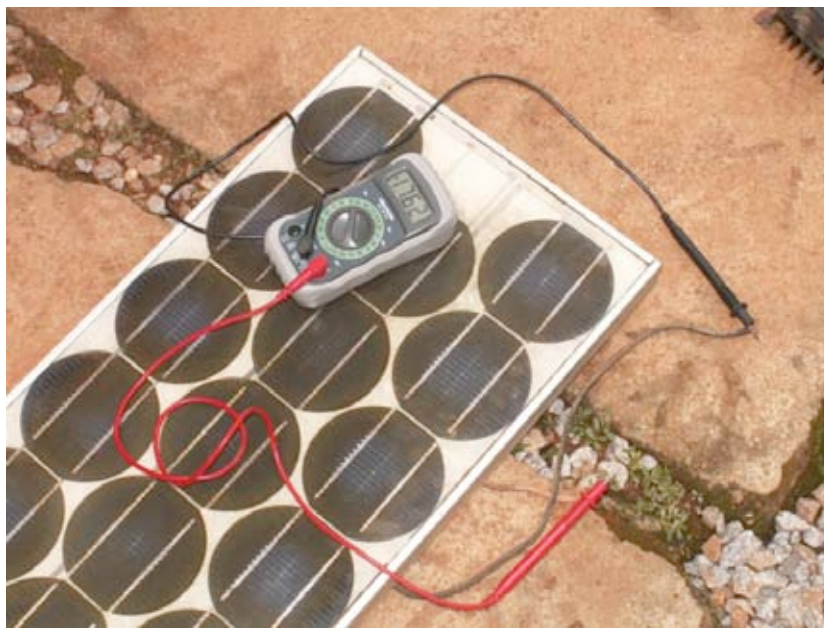


Figure 7.1: Un panneau solaire

Plusieurs technologies sont utilisées dans la fabrication de cellules solaires. Le plus commun est le silicium cristallin qui peut être soit de type monocristallin

ou polycristallin. Le silicium amorphe peut être moins cher mais est moins efficace pour convertir l'énergie solaire en électricité. Doté d'une espérance de vie réduite et d'une efficacité de transformation de 6 à 8%, le silicium amorphe est généralement utilisé pour l'équipement de faible puissance, telles que les calculatrices portatives. Les nouvelles technologies solaires, comme le ruban de silicone et le photovoltaïque en couche mince, sont actuellement en cours de développement. Ces technologies promettent une efficacité plus élevée mais ne sont pas encore largement disponibles.

La batterie

La batterie stocke l'énergie produite par les panneaux qui n'est pas immédiatement consommée par la charge. Cette énergie stockée peut ensuite être utilisée pendant les périodes de faible ensoleillement. La batterie est parfois également appelée l'***accumulateur***. Les batteries stockent l'électricité sous forme d'énergie chimique. Le type le plus commun de batteries utilisées dans les applications solaires sont les batteries au plomb-acide sans entretien, également appelées ***batteries à recombinaison de gaz*** ou ***batteries au plomb-acide à régulation par soupape*** (***VRLA*** : *Valve Regulated Lead Acid*).

Figure 7.2 : Une batterie plomb-acide à 200 Ah. La borne négative a été cassée à cause d'une pression exercé sur les bornes lors du transport.

En dehors du stockage de l'énergie, les batteries scellées au plomb-acide remplissent aussi deux fonctions importantes :

- Elles sont en mesure de fournir une puissance instantanée supérieure à ce qu'une matrice de panneaux solaires peut générer. Cette puissance instantanée est nécessaire pour démarrer certains appareils, tels que le moteur d'un réfrigérateur ou une pompe.
- Elles déterminent la tension de fonctionnement de votre installation.

Pour une petite installation dans un contexte où les contraintes d'espace sont importantes, d'autres types de batteries (tels que les batteries NiCd, NiMH ou Li-ion) peuvent être utilisés. Ces types de batteries spécialisées ont besoin d'un chargeur/régulateur spécialisé et ne peuvent remplacer directement les batteries au plomb-acide.

Le régulateur

Le ***régulateur*** (ou plus formellement, le ***régulateur de charge solaire***) assure que la batterie travaille dans des conditions appropriées. Il évite la surcharge ou surdécharge de la batterie, qui sont très préjudiciables à la vie de la batterie. Pour assurer une bonne charge et décharge de la batterie, le régulateur utilise l'***état de charge*** (*SoC, State of Charge*) de la batterie. L'état de charge est estimé sur la base de la tension réelle de la batterie. En mesurant la tension de la batterie et en étant programmé avec le type de technologie de stockage utilisée par la batterie, le régulateur peut connaître avec précision les moments où la batterie serait surchargée ou excessivement déchargée.

Figure 7.3 : Un contrôleur de charge solaire de 30 A.

Le régulateur peut inclure d'autres fonctionnalités qui ajoutent des informations précieuses et le contrôle de la sécurité de l'équipement. Ces fonctionnalités incluent notamment les ampèremètres, voltmètres, la mesure

d'Ampère-heure, les horloges, les alarmes, etc. Tout en étant pratiques, aucune de ces fonctionnalités n'est indispensable pour un système photovoltaïque fonctionnel.

Le convertisseur

L'électricité fournie par une matrice de panneaux et la batterie est de type continu à voltage fixe. La tension fournie peut ne pas correspondre à ce qui est exigé par votre charge. Un ***convertisseur continu/alternatif*** (***DC/AC***), également connu sous le nom d'***onduleur***, convertit le courant continu de vos batteries en courant alternatif. Cela se fait au prix d'une perte d'énergie pendant la conversion. Si nécessaire, vous pouvez également utiliser des convertisseurs pour obtenir un courant continu à un niveau de tension autre que celui qui est fourni par les batteries. Les convertisseurs DC/DC perdent également de l'énergie pendant la conversion. Pour un fonctionnement optimal, vous devez concevoir votre système solaire de façon à générer la tension correspondant à la charge.

Figure 7.4 : Un convertisseur DC/AC à 800 Watt.

La charge

La charge est l'équipement qui consomme l'énergie produite par votre système énergétique. La charge peut inclure du matériel de communication sans fil, des routeurs, des postes de travail, des lampes, des téléviseurs, des modems VSAT, etc. Bien qu'il ne soit pas possible de calculer avec précision la

consommation totale exacte de votre équipement, il est essentiel d'être en mesure de faire une bonne estimation. Dans ce type de système, il est absolument nécessaire d'utiliser un équipement efficient et de faible puissance pour éviter de gaspiller de l'énergie.

Assembler les pièces

Le système photovoltaïque complet intègre tous ces éléments. Les panneaux solaires génèrent de l'électricité lorsque l'énergie solaire est disponible. Le régulateur assure un fonctionnement efficace des panneaux et évite les dommages causés aux batteries. Le banc de batteries emmagasine l'énergie collectée pour une utilisation ultérieure. Les convertisseurs et onduleurs adaptent l'énergie emmagasinée pour répondre aux besoins de votre charge. Enfin, la charge consomme de l'énergie pour accomplir des tâches. Lorsque tous les éléments sont équilibrés et sont correctement entretenus, le système se maintient pendant des années.

Nous allons maintenant examiner chacune des composantes du système photovoltaïque de manière plus détaillée.

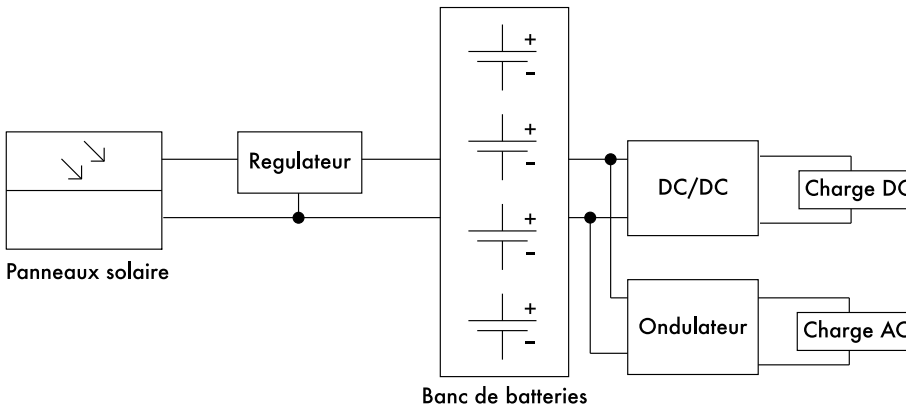


Figure 7.5 : Une installation solaire avec des charges DC et AC.

Le panneau solaire

Un panneau solaire individuel est constitué de nombreuses cellules solaires. Les cellules sont reliées électriquement pour fournir un courant et une tension particuliers. Les cellules individuelles sont encapsulées correctement pour assurer l'isolement et la protection contre l'humidité et la corrosion.

Figure 7.6 : L'effet de l'eau et la corrosion sur un panneau solaire.

Il existe différents types de modules disponibles sur le marché, selon les exigences énergétiques de votre application. Les modules les plus courant sont composés de 32 ou 36 cellules solaires de silicium cristallin. Ces cellules sont toutes de taille égale, montées en série, encapsulées entre du verre et du plastique, et utilisent une résine en polymère comme isolant thermique. La surface du module est généralement comprise entre 0,1 et 0,5 m^2. Généralement, les panneaux solaires ont deux contacts électriques, l'un positif et l'autre négatif.

Certains panneaux solaires comprennent également des contacts supplémentaires pour permettre l'installation de diodes de dérivation dans des cellules individuelles. Les ***diodes de dérivation*** servent à protéger le panneau contre un phénomène connu sous le nom de "*hot-spots*". Un hot-spot se produit lorsque certaines des cellules sont dans l'ombre alors que le reste du panneau est en plein soleil. Plutôt que de produire de l'énergie, les cellules qui sont dans l'ombre se comportent comme une charge qui favorise la dissipation de l'énergie. Dans cette situation, ces cellules peuvent expérimenter une augmentation significative de température (environ 85 à 100 °C.) Les diodes de dérivation empêchent la formation of hot-spots sur les cellules qui sont dans l'ombre mais réduisent la tension maximale du panneau. Elles ne devraient être utilisées que lorsque l'ombrage est inévitable. Une bien meilleure solution consiste à exposer l'ensemble des panneaux au soleil à chaque fois que possible.

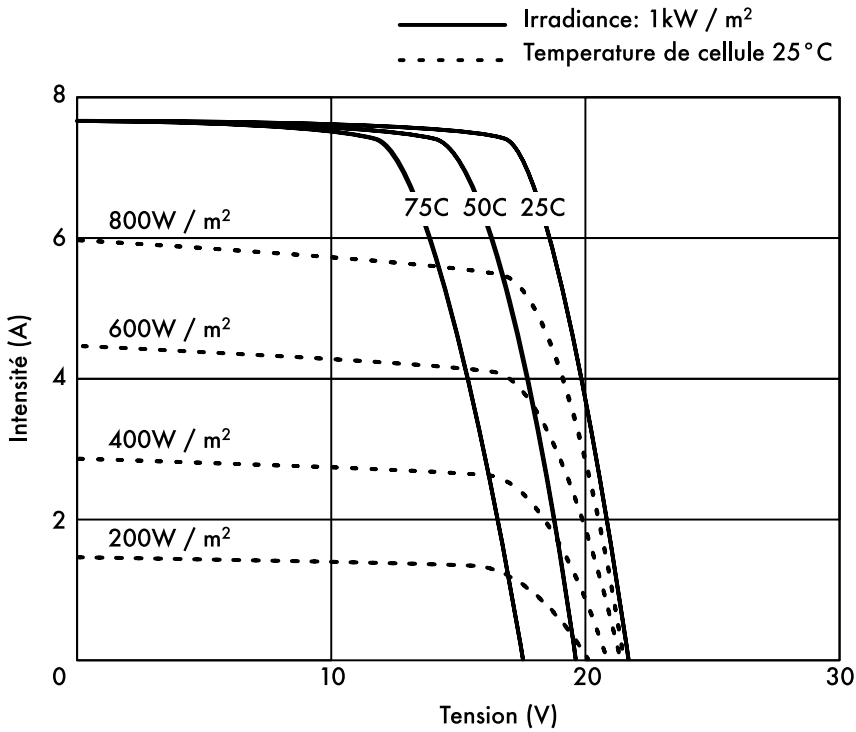


Figure 7.7 : Différentes courbes IV. L'intensité (A) change avec l'irradiance, et la tension (V) change avec des changements de la température.

La performance électrique d'un module solaire est représentée par une ***courbe caractéristique IV,*** qui représente l'intensité qui est fourni en fonction de la tension générée pour un certain rayonnement solaire.

La courbe représente l'ensemble des valeurs possibles de tension courant. Les courbes dépendent de deux facteurs principaux : la température et le rayonnement solaire reçu par les cellules. Pour un endroit donné de la cellule solaire, l'intensité générée est directement proportionnel le à l'irradiance solaire (G), tandis que la tension diminue légèrement avec une augmentation de la température. Un bon régulateur essayera de maximiser la quantité d'énergie qu'un panneau fournit en suivant le point qui fournit la puissance maximale (V x I). La puissance maximale correspond à la variation brusque de la courbe IV.

Paramètres du panneau solaire

Les principaux paramètres qui caractérisent un panneau photovoltaïque sont les suivants :

1. **Courant de court-circuit** (I_{sc}) : la valeur maximale de l'intensité fournie par le panneau lorsque les connecteurs sont court-circuités.

2. **Tension de circuit ouvert** (V_{oc}) : la tension maximale que le panneau fournit lorsque les terminaux ne sont pas connectés à une charge quelconque (un circuit ouvert). Cette valeur est normalement 22 V pour les panneaux qui vont être utilisés dans les systèmes de 12 V, et est directement proportionnelle au nombre de cellules connectées en série.

3. **Point de puissance maximale** (P_{max}) : le point où l'énergie électrique fournie par le panneau est au maximum, où $P_{max} = I_{max} \times V_{max}$. Le point de puissance maximale d'un panneau est mesuré en watts (W) ou watts-crête (W_p). Il est important de ne pas oublier que dans des conditions normales, le panneau ne fonctionnera pas comme dans des conditions de pointe car la tension de fonctionnement est fixée par la charge ou le régulateur. Les valeurs typiques de V_{max} et I_{max} doivent être un peu plus petites que les valeurs I_{sc} et V_{oc}.

4. **Facteur de remplissage** (FF, Fill factor) : la relation entre la puissance maximale que le panneau peut fournir et le produit $I_{sc} \times V_{oc}$. Cette relation vous donne une idée de la qualité du panneau car elle est une indication du type de courbe caractéristique IV. Plus le FF est proche de 1, plus un panneau peut offrir de puissance. Les valeurs communes sont d'habitude entre 0,7 et 0,8.

5. **Efficacité** (h) : le rapport entre la puissance électrique maximale que le panneau peut fournir à la charge et la puissance du rayonnement solaire (P_L) incident au panneau. Ce rapport est normalement dans la gamme d'environ 10-12% selon le type de cellules (monocristallin, polycristallin et amorphe ou de couches minces).

En tenant compte des définitions du point de puissance maximale et du facteur de remplissage, nous voyons que :

$$h = P_{max} / P_L = FF \cdot I_{SC} \cdot V_{OC} / P_L$$

Les valeurs I_{sc}, V_{oc} et le V_{Pmax} sont fournies par le fabricant et se réfèrent aux conditions normales de mesure d'irradiance G = 1000 W/m², au niveau de la mer, pour une température de cellules de Tc = 25 °C.

Les paramètres du panneau changent pour certaines conditions d'irradiance et de température. Les fabricants auront parfois des graphiques ou des tables avec des valeurs pour les conditions différant de la norme. Vous devriez vérifier les valeurs de performance pour les températures de panneau qui sont susceptibles de correspondre à votre installation.

Soyez conscients du fait que deux panneaux peuvent avoir la même W_p mais se comporter très différemment dans différentes conditions d'exploitation. Lors de l'acquisition d'un panneau, il est important de vérifier, si possible, que leurs paramètres (au moins, I_{sc} et les V_{oc}) correspondent aux valeurs promises par le fabricant.

Paramètres des panneaux pour le dimensionnement du système

Pour calculer le nombre de panneaux nécessaires pour couvrir une charge donnée, il vous suffit de connaître le courant et la tension au point de puissance maximale : I_{Pmax} et V_{Pmax}.

Vous devrez toujours être conscient que le panneau ne va pas opérer dans des conditions parfaites car la charge ou le système de régulation ne va pas fonctionner au point de puissance maximale du panneau. Vous devez assumer une perte d'efficacité de 5% dans vos calculs afin de compenser cet effet.

Interconnexion des panneaux

Une ***matrice de panneaux solaires*** est une collection de panneaux solaires qui sont électriquement interconnectés et installés sur un certain type de support. Une matrice de panneaux solaires vous permet de générer une plus grande tension et plus de courant que ce qui est possible avec un seul panneau solaire. Les panneaux sont interconnectés de manière à ce que la tension générée soit proche (mais supérieure à) du niveau de tension des batteries, et que le courant généré soit suffisant pour alimenter l'équipement et charger les batteries.

La connexion de panneaux solaires en série augmente la tension générée. La connexion de panneaux en parallèle augmente l'intensité. Le nombre de panneaux utilisés doit être augmenté jusqu'à ce que la quantité d'électricité produite dépasse légèrement les exigences de votre charge.

Il est très important que tous les panneaux dans votre matrice soient le plus identiques possible. Dans une matrice, vous devez utiliser des panneaux de la même marque et de mêmes caractéristiques car toute différence dans leurs conditions de fonctionnement aura un impact important sur le bon fonctionnement et la performance de votre système. Même les panneaux qui ont des performances identiques afficheront une certaine variation dans leurs caractéristiques due à leurs procédés de fabrication. Les caractéristiques de fonctionnement de deux panneaux du même fabricant peuvent varier jusqu'à ± 10%.

Dans la mesure du possible, c'est une bonne idée de tester la performance réelle des panneaux individuels pour vérifier leurs caractéristiques de fonctionnement avant de les assembler dans une matrice.

Comment choisir un bon panneau

Une métrique évidente à utiliser pour l'achat de panneaux solaires consiste à comparer le rapport entre la valeur nominale de puissance de crête (W_p) et le prix. Cela vous donnera une idée approximative du coût par watt pour les différents panneaux. Mais il y a aussi un certain nombre d'autres considérations à garder à l'esprit.

Si vous allez installer des panneaux solaires dans les zones géographiques où l'encrassement (de la poussière, du sable ou gravier) sera probablement un problème, il faut envisager l'achat de panneaux avec une faible affinité pour la rétention des crasses. Ces panneaux sont faits de matériaux qui augmentent la probabilité de nettoyage du panneau par le vent et la pluie.

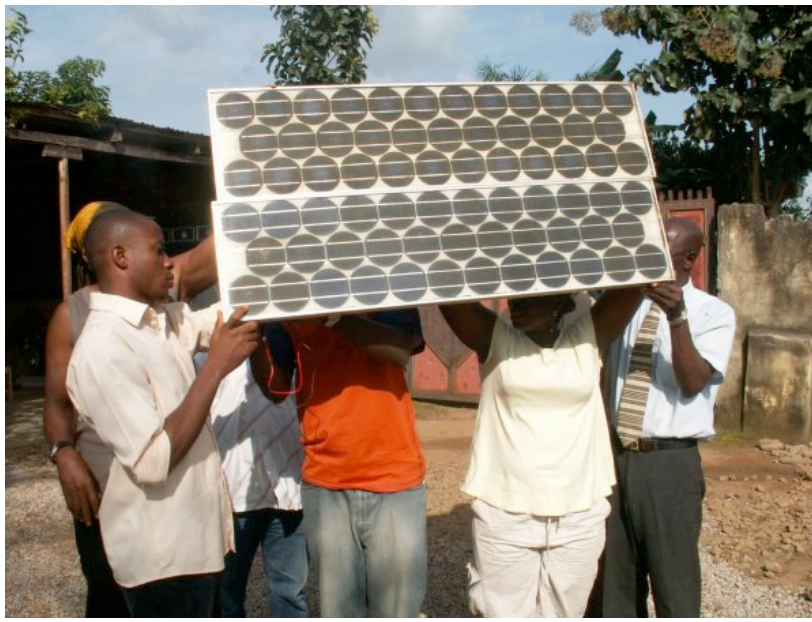


Figure 7.8 : Interconnexion des panneaux en parallèle. Le voltage reste constant pendant que le courant double (Photo : Fantsuam Foundation, Nigeria).

Il faut toujours vérifier la construction mécanique de chaque panneau. Vérifiez que le panneau est en verre trempé et que le cadre en aluminium est robuste et bien construit. Les cellules solaires à l'intérieur du panneau peuvent durer plus de 20 ans, mais elles sont très fragiles et le panneau doit les protéger contre les risques mécaniques. Il faut exiger du fabricant une garantie de qualité en termes de puissance de sortie et de construction mécanique.

Enfin, assurez-vous que le fabricant ne fournit pas seulement la puissance de crête nominale du panneau (W_p), mais aussi la variation de la puissance avec l'irradiation et la température. Cela est particulièrement important lorsque les panneaux sont utilisés dans les matrices car les variations dans les paramètres de fonctionnement peuvent avoir un grand impact sur la qualité de l'électricité produite et la durée de vie utile des panneaux.

La batterie

La batterie est le siège d'une certaine réaction chimique réversible qui stocke l'énergie électrique qui peut être récupérée plus tard en cas de besoin. Cette énergie électrique est transformée en énergie chimique lorsque la batterie est en charge, et l'inverse se produit lorsque la batterie est déchargée.

Une batterie est formée par un ensemble d'éléments ou de cellules en série. Les batteries de type plomb-acide sont composées de deux électrodes au plomb immergées dans une solution électrolytique d'eau et d'acide sulfurique. Une différence de potentiel d'environ 2 volts a lieu entre les électrodes selon la valeur instantanée de la charge de la batterie. Les batteries les plus utilisées dans les

applications solaires photovoltaïques ont une tension nominale de 12 ou 24 volts. Une batterie 12 V contient donc 6 cellules en série.

Dans un système photovoltaïque, la batterie a deux objectifs importants : fournir l'énergie électrique au système lorsque l'énergie n'est pas fournie par la matrice de panneaux solaires et stocker l'énergie excédentaire générée par les panneaux chaque fois que l'énergie est supérieure à la charge. Selon la présence ou l'absence de lumière du soleil, un processus cyclique de charge et décharge se produit dans la batterie. Pendant les heures de soleil, la matrice des panneaux produit de l'énergie électrique. L'énergie qui n'est pas consommée immédiatement est utilisée pour charger la batterie. Pendant les heures d'absence de soleil, toute demande d'énergie électrique est fournie par la batterie qui se décharge conséquemment.

Ces cycles de charge et de décharge se produisent chaque fois que l'énergie produite par les panneaux ne correspond pas à l'énergie requise pour soutenir la charge. Quand il y a suffisamment de soleil et que la charge est légère, les batteries se chargent. De toute évidence, les batteries se déchargent chaque nuit quand de l'énergie est utilisée. Les batteries se déchargent également lorsque l'irradiance est insuffisante pour couvrir les exigences de charge (en raison de la variation naturelle de conditions climatologiques, des nuages, de la poussière, etc.)

Si la batterie ne stocke pas assez d'énergie pour répondre à la demande pendant les périodes sans soleil, le système sera épuisé et ne sera pas disponible pour utilisation. D'autre part, le surdimensionnement du système (en ajoutant un trop grand nombre de panneaux et batteries) est coûteux et inefficace. Lors de la conception d'un système autonome, nous avons besoin d'un compromis entre le coût des composante et la disponibilité énergétique du système. Une façon d'y parvenir est d'estimer le nombre de jours d'autonomie requis. Dans le cas d'un système de télécommunications, le ***nombre de jours d'autonomie*** du système solaire dépend de l'importance de sa fonction dans la conception de votre réseau. Si l'équipement doit servir de répétiteur et fait partie de la dorsale de votre réseau, vous souhaiterez probablement concevoir votre système photovoltaïque avec une autonomie pouvant aller jusqu'à 5-7 jours. D'autre part, si le système solaire est responsable de la fourniture d'énergie à l'équipement client, vous pouvez probablement réduire le nombre de jours d'autonomie à deux ou trois. Dans les zones à faible éclairement, il serait nécessaire d'augmenter encore cette valeur. Dans tous les cas, il vous faudra toujours trouver le juste équilibre entre le coût et la fiabilité.

Les types de batteries

De nombreuses technologies de batteries existent et sont destinées à être utilisées dans une variété d'applications différentes. Le type le plus approprié pour les applications photovoltaïques est la ***batterie stationnaire*** conçue pour un emplacement fixe et pour des scénarios où la consommation d'énergie est plus ou moins irrégulière. Les batteries “stationnaires” peuvent supporter des cycles de décharge profonde mais elles ne sont pas conçues pour produire des courants élevés dans de brèves périodes de temps.

Les batteries stationnaires peuvent utiliser un électrolyte alcalin (tel que le nickel-cadmium) ou acide (tel que le plomb-acide). Les batteries stationnaires à base de nickel-cadmium sont recommandées pour leur grande fiabilité et leur résistance dans toutes les situations possibles. Malheureusement, elles ont tendance à être beaucoup plus coûteuses et difficile à obtenir que les batteries scellées au plomb-acide.

Dans de nombreux cas où il est difficile de trouver localement des batteries stationnaires de bonne qualité et bon marché (l'importation de batteries n'est pas bon marché), vous serez obligés d'utiliser des batteries destinées au marché automobile.

Utilisation des batteries automobiles

Les batteries automobiles ne sont pas bien adaptées aux applications photovoltaïques car elles sont conçues pour fournir un courant substantiel pour seulement quelques secondes (lors du démarrage du moteur) plutôt que le maintien d'un courant faible pendant de longues périodes de temps. Cette caractéristique de conception des batteries automobiles (aussi appelée batteries de traction) se traduit par une durée de vie effective courte lorsqu'elles sont utilisées dans les systèmes photovoltaïques. Les batteries de traction peuvent être utilisées dans de petites applications où la réduction de coût est le facteur le plus important ou si d'autres batteries ne sont pas disponibles.

Les batteries de traction sont conçues pour les véhicules et brouettes électriques. Elles sont moins coûteuses que les batteries stationnaires et peuvent servir dans une installation photovoltaïque, bien qu'elles aient besoin d'un entretien très fréquent. Ces batteries ne devraient jamais être déchargées profondément, afin d'éviter de réduire considérablement leur capacité à tenir une charge. Une batterie de camion ne doit pas être déchargée de plus de 70% de sa capacité totale. Cela signifie que vous ne pouvez utiliser qu'un maximum de 30% de capacité nominale d'une batterie plomb-acide avant qu'elle ne doive être rechargée.

Vous pouvez étendre la durée de vie d'une batterie au plomb-acide en utilisant de l'eau distillée. Un densimètre ou hydromètre peut vous aider à mesurer la densité de l'électrolyte de la batterie. Une batterie typique a une gravité spécifique de 1,28. L'ajout d'eau distillée et l'abaissement de la densité à 1,2 peuvent aider à réduire la corrosion de l'anode, au détriment de la capacité globale de la batterie. Si vous réglez la densité de l'électrolyte de la batterie, vous devez utiliser de l'eau distillée car l'eau du robinet ou l'eau de puits endommagera de façon permanente la batterie.

Etats de charge

Il existe deux états spéciaux de charge qui peuvent avoir lieu pendant la charge et décharge cyclique de la batterie. Ces états devraient tous deux être évités afin de préserver la durée de vie utile de la batterie.

Surcharge

La surcharge a lieu lorsque la batterie arrive à la limite de ses capacités. Si l'énergie est appliquée à une batterie au-delà de son point de charge maximale, l'électrolyte commence à se décomposer. Cela produit des bulles d'oxygène et d'hydrogène dans un processus connu sous le nom de gazéification. Il en résulte une perte de l'eau, l'oxydation de l'électrode positive, et dans des cas extrêmes, un risque d'explosion.

D'un autre côté, la présence de gaz évite la stratification de l'acide. Après plusieurs cycles continus de charge et de décharge, l'acide tend à se concentrer dans le bas de la batterie et réduit ainsi sa capacité effective. Le processus de gazéification agite l'électrolyte et évite la stratification.

Encore une fois, il est nécessaire de trouver un compromis entre les avantages (éviter la stratification électrolyte) et les inconvénients (perte d'eau et production de l'hydrogène). Une solution consiste à permettre une condition de surcharge légère de temps en temps. Une méthode classique consiste à permettre, pendant quelques jours, une tension de 2,35 à 2,4 Volts à une température de 25 °C pour chaque élément de la batterie. Le régulateur devrait assurer des surcharges périodiques contrôlées.

Surdécharge

De la même façon qu'il existe une limite supérieure, il y a aussi une limite inférieure à l'état de charge d'une batterie. Un déchargement au-delà de cette limite se traduira par la détérioration de la batterie. Lorsque l'approvisionnement effectif de la batterie est épuisé, le régulateur empêche toute extraction d'énergie de la batterie. Lorsque la tension de la batterie atteint la limite minimale de 1,85 volts par cellule à 25 °C, le régulateur déconnecte la charge de la batterie.

Si la décharge de la batterie est très profonde et que la batterie demeure déchargée pendant une longue période, cela entraîne trois effets : la formation de sulfate cristallisé sur les plaques de la batterie, le ramollissement de la matière active sur la plaque de batterie, et le gauchissement de la plaque. Le processus de formation de cristaux de sulfate stable s'appelle sulfatation dure. Ce phénomène est particulièrement négatif car il génère de gros cristaux qui ne prennent pas part à aucune réaction chimique et peut rendre votre batterie inutilisable.

Paramètres de batterie

Les principaux paramètres qui caractérisent une batterie sont les suivantes :

- Tension nominale, V_{NBat}. La valeur la plus commune est de 12 V.
- Capacité nominale, C_{NBat}. La quantité maximale d'énergie qui peut être extraite d'une batterie qui est entièrement chargée. Elle est exprimée en ampères-heures (Ah) ou watt-heures (Wh). La quantité d'énergie qui peut être obtenue d'une batterie dépend de la durée du processus d'extraction. La décharge d'une batterie sur une longue période produira plus d'énergie par rapport à la décharge de la même batterie sur une courte période. La capacité d'une batterie est donc spécifiée par des temps de

décharge différents. Pour les applications photovoltaïques, ce temps devrait être supérieur à 100 heures (C100).

- Profondeur maximale de décharge, DoD_{max}. A profondeur de la décharge est la quantité d'énergie extraite d'une batterie en un seul cycle de décharge. Elle est exprimée en pourcentage. L'espérance de vie d'une batterie dépend de la profondeur de sa décharge à chaque cycle. Le fabricant doit fournir des schémas relatant le nombre de cycles de charge-décharge à la durée de vie de la batterie. En règle générale, vous devriez éviter de décharger une batterie à décharge profonde au-delà de 50%. Les batteries de traction ne doivent pas être déchargées de plus de 30%.
- Capacité utile, C_{UBat}. C'est la capacité réelle (utilisable) de la batterie. Elle est égale au produit de la capacité nominale et du montant maximum de DoD. Par exemple, une batterie stationnaire de capacité nominale (C100) de 120 Ah et d'intensité de décharge de 70% a une capacité utile de (120 x 0,7) 84 Ah.

Mesure de l'état de charge de la batterie

Etat de charge	Tension batterie en 12V	Volts par cellule
100%	12,70	2,12
90%	12,50	2,08
80%	12,42	2,07
70%	12,32	2,05
60%	12,20	2,03
50%	12,06	2,01
40%	11,90	1,98
30%	11,75	1,96
20%	11,58	1,93
10%	11,31	1,89
0%	10,50	1,75

Une batterie scellée au plomb-acide de 12 V peut fournir différentes tensions selon son état de charge. Lorsque la batterie est entièrement chargée dans un circuit ouvert, la tension de sortie est d'environ 12,8 V. La tension de sortie

diminue rapidement à 12,6 V lorsque les bornes sont attachées. Comme la batterie fournit un courant constant en cours d'utilisation, la tension de la batterie diminue de façon linéaire de 12,6 à 11,6 V selon l'état de charge. Une batterie scellée au plomb-acide fournit 95% de son énergie dans cette gamme de tension. Si nous assumons qu'une batterie à pleine charge a une tension de 12,6 V lorsqu'elle est “pleine” et une tension de 11,6 V lorsqu'elle est “vide”, on peut estimer que la batterie est déchargée à 70% quand elle atteint une tension de 11,9 V. Ces valeurs ne sont qu'une approximation grossière, car elles dépendent de la vie et la qualité de la batterie, de la température, etc.

Selon cette table, et considérant que la batterie d'un camion ne devrait pas être déchargée à plus de 20% à 30%, nous pouvons déterminer que la capacité utile d'un camion qui a une batterie de 170 Ah est de 34 Ah (20%) à 51 Ah (30%). A l'aide de la même table, nous pouvons en déduire que nous devrions programmer le régulateur pour empêcher la batterie de se décharger en dessous de 12,3 V.

La batterie et le régulateur de protection

Les disjoncteurs thermomagnétiques ou encore fusibles à un temps doivent être utilisés pour protéger les batteries et l'installation contre les courts-circuits et des dysfonctionnements. Il existe deux types de fusibles : à action retardée et à action rapide. Les fusibles retardés doivent être utilisés avec des charges présentant des propriétés inductives ou capacitives, là où une surintensité peut se produire à l'allumage. Les fusibles retardés permettent le passage d'un courant plus élevé que leur seuil pour un court laps de temps. Les fusibles à action rapides fondent immédiatement si le courant qui les traverse est plus élevé que leur seuil.

Figure 7.9 : Un banc de batteries à 3600Ah avec des courants atteignant des niveaux de 45 A pendant la charge.

Le régulateur est connecté à la batterie et aux charges de sorte que deux types différents de protection doivent être pris en considération. Un fusible doit être placé entre la batterie et le régulateur afin de protéger la batterie de court-circuit en cas de défaillance du régulateur. Un deuxième fusible est nécessaire pour protéger le régulateur contre le courant induit par une charge excessive. Ce deuxième fusible est normalement intégré dans le régulateur lui-même.

Chaque fusible est caractérisé par un courant maximum et une tension utilisable maximum. Le courant maximum du fusible devrait être 20% plus grand que le courant maximal prévu. Même si les batteries produisent une faible tension, un court-circuit peut conduire à un très fort courant qui peut facilement atteindre plusieurs centaines d'ampères. Des intensités élevées peuvent causer un incendie, endommager le matériel et les batteries, voire provoquer un choc électrique à un corps humain.

Si un fusible est endommagé, il ne faut jamais le remplacer avec un fil ou un fusible destiné à des courts-circuits plus élevés. Il faut tout d'abord déterminer la cause du problème, puis remplacer le fusible par un autre qui a les mêmes caractéristiques.

Effets de température

La température ambiante a plusieurs effets importants sur les caractéristiques de la batterie :

- La capacité nominale de la batterie (que le fabricant donne habituellement pour 25 °C) augmente avec la température à la vitesse d'environ 1%/°C.
- Mais si la température est trop élevée, la réaction chimique qui a lieu dans la batterie s'accélère, ce qui peut provoquer le même type d'oxydation que celui qui a lieu au cours de la surcharge. Evidemment, ceci réduira l'espérance de vie de la batterie. Ce problème peut être compensé en partie dans des batteries de voiture en utilisant une faible densité de dissolution (une densité de 1,25 lorsque la batterie est complètement chargée).
- Quand la température est réduite, la durée de vie de la batterie augmente. Mais si la température est trop faible, vous courez le risque de geler l'électrolyte. La température de congélation dépend de la densité de la solution, qui est également liée à l'état de charge de la batterie. Plus la densité est basse, plus le risque de gel augmente. Dans les zones de basse températures, vous devez éviter un gel profond des batteries (ceci car la DoD_{max} est effectivement réduite.)
- La température modifie également le rapport entre la tension et la charge. Il est préférable d'utiliser un régulateur qui ajuste les paramètres de la tension plancher de déconnexion et reconnexion en fonction de la température. Le capteur de température du régulateur devrait être fixé à la batterie au moyen d'un ruban adhésif ou en utilisant une autre méthode simple.

- Dans des zones de température élevée, il est important de garder les batteries dans un endroit aussi frais que possible. Les batteries doivent être entreposées dans un endroit ombragé et ne jamais être exposées à la lumière directe du soleil. Il est également souhaitable de placer les batteries sur un support, afin de permettre la circulation de l'air par en dessous et d'améliorer ainsi le refroidissement.

Comment choisir une bonne batterie

Choisir une bonne batterie peut être très difficile dans les régions en voie de développement. Les batteries de grande capacité sont lourdes, volumineuses et coûteuses à l'importation. Une batterie de 200 Ah pèse environ 50 kg (120 livres) et elle ne peut pas être transportée comme bagage à main. Si vous voulez des batteries à longue durée de vie (comme 5 ans ou plus) et sans entretien, vous devez être prêt à payer le prix.

Une bonne batterie devrait toujours être accompagnée de ses spécifications techniques, y compris la capacité à différents taux de décharge (C20, C100), la température de fonctionnement, les points de tension de coupure, et les exigences pour les chargeurs.

Les batteries doivent être exemptes de fissures, d'écoulement liquide ou de tout signe de dommage, et les bornes de la batterie doivent être exemptes de corrosion. Comme des tests en laboratoire sont nécessaires pour obtenir des données complètes sur la capacité réelle et le vieillissement, attendez vous à trouver beaucoup de batteries de qualité médiocre (y compris des fausses) sur les marchés locaux. Le prix typique d'une batterie (excluant le transport et les taxes à l'importation) est de 3-4$ USD par Ah pour les batteries à plomb-acide de 12 V.

L'espérance de vie par rapport au nombre de cycles

La batterie est la seule composante d'un système solaire qui doit être amortie sur une courte période de temps et remplacée régulièrement. Vous pouvez augmenter la durée de vie utile d'une batterie en réduisant l'intensité de décharge par cycle. Même les batteries à décharge profonde auront une grande autonomie si le nombre de cycles de décharge profonde (> 30%) est réduit.

Si vous déchargez complètement la batterie tous les jours, vous aurez généralement besoin de la changer en moins d'un an. Si vous utilisez seulement 1/3 de la capacité de la batterie, elle pourra durer plus de 3 ans. Il peut être moins cher d'acheter une batterie avec une capacité 3 fois supérieure que de changer de batterie chaque année.

Le régulateur de charge

Le régulateur de charge est également connu sous le nom de contrôleur de charge, régulateur de tension, contrôleur de charge-décharge ou contrôleur de charge. Le régulateur se trouve entre la matrice de panneaux, les batteries, et votre équipement ou charges.

Rappelez-vous que la tension de la batterie, bien que toujours près de 2 V par cellule, varie en fonction de son état de charge. En surveillant la tension de la batterie, le régulateur empêche la surcharge ou la surdécharge.

Les régulateurs utilisés dans les applications solaires doivent être connectés en série : ils déconnectent la matrice de panneaux de la batterie pour éviter la surcharge, et ils déconnectent la batterie de la charge pour éviter la surdécharge. La connexion et la déconnexion est faite par le biais d'interrupteurs qui peuvent être de deux types : électromécaniques (relais) ou électroniques (transistor bipolaire, MOSFET). Les régulateurs ne doivent jamais être connectés en parallèle.

Afin de protéger la batterie contre la gazéification, l'interrupteur ouvre le circuit de charge lorsque la tension de la batterie atteint sa ***tension de deconnection haute*** (***HVD***, *high voltage disconnect*) ou son point de coupure. La ***tension de deconnection basse*** (***LVD***, *low voltage disconnect*) protège la batterie contre la surdécharge en débranchant ou en distribuant la charge. Pour prévenir les connexions et déconnexions continues, le régulateur ne raccordera pas les charges jusqu'à ce que la charge de la batterie ait atteint sa ***tension de reconnexion basse*** (***LRV***, *low reconnect voltage*).

Les valeurs typiques pour une batterie au plomb-acide de 12 V sont les suivantes :

Point de tension	Tension
LVD	11,5
LRV	12,6
Tension constante régulée	14,3
Egalisation	14,6
HVD	15,5

Le régulateurs les plus modernes sont également en mesure de déconnecter automatiquement les panneaux durant la nuit pour éviter de décharger la batterie. Ils peuvent également surcharger périodiquement la batterie pour augmenter leur durée de vie, et peuvent utiliser un mécanisme connu sous le nom de modulation de largeur d'impulsions (PWM, *pulse width modulation*) pour prévenir l'accumulation excessive de gaz.

Comme le point de fonctionnement à tension de crête de la matrice des panneaux varie avec la température et l'éclairement solaire, les nouveaux régulateurs sont capables de suivre constamment le point d'énergie maximale de la matrice solaire. Cette caractéristique est connue sous le nom de point de puissance maximale (MPPT, *maximum power point tracking*).

Paramètres du régulateur

Lors de la sélection d'un régulateur pour votre système, vous devriez au moins connaître la tension de fonctionnement et l'intensité maximale que le régulateur peut gérer. La tension de fonctionnement sera de 12, 24, ou 48 V. L'intensité maximale doit être de 20% plus élevée que l'intensité fournie par la matrice de panneaux connectés au régulateur.

Les autres fonctions et les données d'intérêt comprennent :

- Des valeurs spécifiques pour le LVD, LRV et HVD.
- Support pour la compensation en température. La tension qui indique l'état de charge de la batterie varie avec la température. Pour cette raison, certains régulateurs sont capables de mesurer la température de la batterie et corriger les différentes valeurs de coupure et les valeurs de reconnexion.
- L'instrumentation et les jauges. Les instruments les plus communs mesurent la tension des panneaux et des batteries, l'état de charge (SoC) ou la profondeur de décharge (DoD, *Depth of Discharge*). Certains régulateurs ont des alarmes spéciales pour indiquer que les panneaux ou les charges ont été déconnectées, le LVD ou HVD a été atteint, etc.

Convertisseurs

Le régulateur fournit un courant continu à une tension spécifique. Les convertisseurs et onduleurs sont utilisés pour ajuster la tension afin de répondre aux besoins de votre charge.

Convertisseurs DC/DC

Les convertisseurs DC/DC transforment une tension continue en une autre tension continue d'une valeur différente. Il existe deux méthodes de conversion qui peuvent être utilisées pour adapter la tension des batteries : conversion linéaire et conversion de commutation.

La conversion linéaire abaisse la tension des batteries par conversion de l'énergie excédentaire en chaleur. Cette méthode est très simple mais elle est de toute évidence inefficace. Généralement, la conversion de commutation fait appel à un composant magnétique pour stocker temporairement l'énergie et la transformer en une autre tension. La tension résultante peut être plus grande, inférieure, ou l'inverse (négative) de la tension d'entrée.

L'efficacité d'un régulateur linéaire diminue avec l'augmentation de la différence entre la tension d'entrée et la tension de sortie. Par exemple, si l'on veut une conversion de 12 V à 6 V, le régulateur linéaire aura une efficacité de seulement 50%. Un régulateur de commutation standard a une efficacité d'au moins 80%.

Convertisseur DC/AC ou Onduleur

Les onduleurs sont utilisés lorsque votre équipement exige une alimentation AC. Les onduleurs coupent et inversent le courant continu AC pour générer une onde carrée qui est plus tard filtrée pour approximer une onde sinusoïdale et éliminer les harmoniques indésirables. Très peu d'onduleurs produisent en réalité une onde sinusoïdale pure en sortie. La plupart des modèles disponibles sur le marché produisent ce qui est connu comme “Onde sinusoïdale modifiée”, car leur tension de sortie n'est pas une sinusoïde pure. Quand il s'agit d'efficacité, les onduleurs à Onde sinusoïdale modifiée produisent de meilleurs résultats que les onduleurs sinusoïdaux purs.

Sachez que ce ne sont pas tous les équipements qui acceptent une onde sinusoïdale modifiée comme tension d'entrée. Le plus souvent, certaines imprimantes à laser ne fonctionnent pas avec un onduleur à onde sinusoïdale modifiée. Par ailleurs, les moteurs fonctionneront mais ils consommeront plus d'énergie que quand ils sont alimentés avec une onde sinusoïdale pure. En outre, les alimentations DC ont tendance à un plus grand réchauffement et les amplificateurs audio peuvent émettre un bourdonnement sonore.

Mis à part le type d'onde, certains aspects importants des onduleurs sont les suivants :

- **Fiabilité en présence de surtensions**. Les onduleurs ont deux seuils de puissance : l'un pour la puissance continue, et un plus grand seuil pour la puissance de crête. Ils sont capables de fournir la puissance de crête pour un très court laps de temps, comme lors du démarrage d'un moteur. L'onduleur devrait aussi être en mesure de s'arrêter avec sécurité (avec un coupe-circuit ou fusible) dans le cas d'un court-circuit, ou si la puissance demandée est trop élevée.
- **Efficacité de conversion**. Les onduleurs sont plus efficaces quand ils fonctionnent entre 50% à 90% de leur puissance nominale continue. Vous devez sélectionner un onduleur qui correspond le mieux à vos exigences de charge. Le fabricant fournit généralement les performances de l'onduleur à 70% de sa puissance nominale.
- **Recharge de la batterie**. Beaucoup d'onduleurs intègrent également la fonction inverse : la possibilité de charger les batteries en présence d'une autre source de courant (réseau de distribution électrique, générateur, etc.) Ce type d'onduleur est connu comme un onduleur/chargeur.
- **Bascule automatique**. Certains onduleurs peuvent basculer automatiquement entre différentes sources d'énergie (réseau électrique, générateur, énergie solaire) en fonction des disponibilités.

Lorsque vous utilisez les équipements de télécommunications, il est préférable d'éviter d'utiliser des convertisseurs DC/AC et de les alimenter directement à partir d'une source DC. La plupart du matériel de communication peut accepter une large gamme de tensions d'entrée.

Matériel ou charge

Il devrait être évident que la consommation du système photovoltaïque augmente avec les exigences de puissance. Il est donc essentiel de faire correspondre la taille du système d'aussi près que possible à la charge attendue. Lors de la conception du système, vous devez d'abord faire une estimation réaliste de la consommation maximale. Une fois l'installation en place, la consommation maximale fixée doit être respectée afin d'éviter de fréquentes pannes de courant.

Appareils domestiques

L'usage de l'énergie solaire photovoltaïque n'est pas recommandé pour des applications à échange de chaleur (chauffage électrique, réfrigérateurs, grille-pain, etc.). Dans la mesure du possible, l'énergie doit être utilisée avec parcimonie en utilisant des appareils de faible puissance.

Matériel	Consommation (Watts)
Ordinateur portable	30-50
Lampe de faible puissance	6-10
Routeur WRAP (une radio)	4-10
Modem VSAT	20-30
PC (sans écran LCD)	20-30
PC (avec écran LCD)	200-300
Switch réseau (16 ports)	6-8

Voici quelques points à garder à l'esprit lors du choix des équipements appropriés à utiliser avec un système solaire :

- L'énergie solaire photovoltaïque est adaptée pour l'éclairage. Dans ce cas, le recours à des ampoules halogènes ou lampes fluorescentes est obligatoire. Bien que ces lampes soient les plus chères, elles ont une efficacité énergétique plus grande que les ampoules à incandescence. Les lampes à LED constituent également un bon choix car elles sont très efficaces et sont alimentées en courant continu.
- Il est possible d'utiliser l'énergie photovoltaïque pour les appareils qui nécessitent une consommation faible et constante (une TV, pour prendre un cas courant). Les petites télévisions consomment moins d'énergie que les grands téléviseurs. Considérez également qu'une télévision noir et blanc consomme environ la moitié de la puissance d'une TV couleur.

- L'énergie solaire photovoltaïque n'est pas recommandée pour toute application qui transforme l'énergie en chaleur (énergie thermique). Utilisez le chauffage solaire ou le butane comme solution de rechange.
- Les machines à laver automatiques classiques fonctionneront, mais vous devez éviter l'usage de tout programme de lavage qui nécessite le chauffage centrifuge de l'eau.
- Si vous devez utiliser un réfrigérateur, il devrait consommer le moins d'énergie possible. Il y a des réfrigérateurs spécialisés qui utilisent le courant DC bien que leur consommation puisse être assez élevée (environ 1000 Wh/jour).

L'estimation de la consommation totale est une étape fondamentale dans le dimensionnement de votre système solaire. Voici un tableau qui vous donne une idée générale de la consommation d'énergie que vous pouvez attendre de différents appareils.

Matériel de télécommunications sans fil

Economiser l'énergie en choisissant le bon matériel économise beaucoup d'argent et de peine. Par exemple, une liaison longue distance n'a pas nécessairement besoin d'un amplificateur puissant qui consomme beaucoup d'énergie. Une carte Wi-Fi avec une bonne sensibilité de réception et une zone de Fresnel dégagée au moins sur 60% fonctionnera mieux qu'un amplificateur et économisera aussi la consommation de l'énergie. Un dicton bien connu des amateurs radio s'applique ici aussi : le meilleur amplificateur est une bonne antenne. Les autres mesures visant à réduire la consommation d'énergie comprennent la régulation de la vitesse du processeur, la réduction de la puissance de transmission à la valeur minimale nécessaire pour fournir un lien stable, l'augmentation de la durée d'intervalle des transmissions de trame balise (*beacon interval*), et l'extinction du système quand il n'est pas utilisé.

Materiel	Consommation (Watts)
Linksys WRT54G (BCM2050 radio)	6
Linksys WAP54G (BCM2050 radio)	3
Orinoco WavePoint II ROR (30mW radio)	15
Soekris net4511 (sans radio)	1,8
PC Engines WRAP.1E-1 (sans radio)	2,04

Materiel	Consommation (Watts)
Mikrotik Routerboard 532 (sans radio)	2,3
Inhand ELF3 (sans radio)	1,53
Senao 250mW radio	3
Ubiquiti 400mW Radio	6

La plupart des systèmes solaires autonomes fonctionnent à 12 ou 24 volts de tension. Il est donc préferable d'utiliser, un appareil sans fil fonctionnant avec une tension continue de 12 volts, que la plupart des batteries au plomb-acide fournissent. La transformation de la tension fournie par la batterie en tension AC ou l'utilisation d'une tension à l'entrée du point d'accès qui diffère de la tension de la batterie causera une perte inutile d'énergie. Un routeur ou un point d'accès acceptant 8-20 Volts DC est parfait.

La plupart des points d'accès bon marché ont un régulateur de tension à commutateur de mode et peuvent fonctionner dans cette plage de tension sans modification ou échauffement (même si l'appareil a été livré avec une alimentation de 5 ou 12 volts).

AVERTISSEMENT : l'exploitation de votre point d'accès en utilisant une alimentation autre que celle prévue par le fabricant de votre matériel entraînera certainement l'annulation de toute garantie, et peut causer des dommages à votre équipement. Alors que la technique suivante fonctionnera généralement comme prévu, rappelez-vous que si vous l'essayez, vous le faites à vos propres risques.

Ouvrez votre point d'accès et regardez près de l'entrée d'alimentation DC pour chercher deux condensateurs relativement grands et une bobine d'inductance (un tore de ferrite avec fil de cuivre enroulé autour de celui-ci). S'ils sont présents, le dispositif a un réglage de mode d'entrée, et la tension d'entrée maximale doit être un peu au-dessous de la tension imprimée sur les condensateurs. Habituellement, le seuil de tension de ces condensateurs est de 16 ou 25 volts. Sachez qu'une source d'énergie non régulée présente une ondulation d'amplitude et peut alimenter votre point d'accès avec une tension beaucoup plus élevée que la tension standard imprimée sur l'alimentation. Ainsi, connecter une source d'alimentation non régulée de 24 volts à un dispositif à condensateurs de 25 volt n'est pas une bonne idée. Bien sûr, l'ouverture de votre dispositif annulera toute garantie. N'essayez pas d'utiliser un point d'accès à une tension plus haute que celle prévue si il ne dispose pas d'un régulateur à commutation de mode. Il va s'échauffer, mal fonctionner, ou brûler.

Les équipements utilisant les processeurs Intel x86 sont plus consommateurs d'énergie électrique comparés aux équipements basés sur les architectures RISC comme ARM ou MIPS. La plate-forme Soekris, qui utilise un processeur de type AMD ElanSC520, est une des cartes les moins consommatrices d'énergie. Une alternative au processeur AMD (ElanSC ou Geode SC1100) consiste à utiliser des équipements équipés de processeurs MIPS. Les processeurs de type

MIPS sont plus performants qu'un processeur AMD Geode mais consomment entre 20-30% plus d'énergie.

Le Linksys WRT54G est un équipement répandu qui fonctionne à une tension de 5 à 20 volts DC et consomme environ 6 Watts, mais possède un commutateur Ethernet intégré. Avoir un *switch* est bien sûr agréable et pratique, mais consomme plus. Linksys offre également un point d'accès Wi-Fi appelé WAP54G qui consomme seulement 3 Watts et peut utiliser les firmware OpenWRT et Freifunk. Les systèmes 4G Accesscube consomment environ 6 Watts quand ils sont équipés d'une seule interface WiFI. Si le standard 802.11b est suffisant, les cartes mini-PCI avec les chipset Orinoco fonctionnent très bien tout en en consommant un minimum d'énergie.

La puissance requise par l'équipement sans fil ne dépend pas seulement de l'architecture, mais aussi du nombre d'interfaces réseau, de radios, du type de mémoire/stockage et du trafic des données. En règle générale, une carte réseau sans fil à faible consommation consomme 2 à 3 W, et une carte radio à 200 mW consomme jusqu'à 3 W. Les cartes à grande puissance (comme le 400 mW Ubiquity) consomment environ 6 W. La consommation d'une station répétitrice avec deux stations de radio peut se situer entre 8 et 10 W.

Bien que la norme IEEE 802.11 intègre un mécanisme avec mode d'économie d'énergie, ce mécanisme n'est pas aussi bénéfique qu'on peut l'espérer. Le principal mécanisme d'économie d'énergie consiste à permettre aux stations de mettre périodiquement leurs cartes sans fil dans un état de “sommeil” par le biais d'un circuit temporel. Lorsque la carte sans fil se réveille, elle vérifie si une trame-balise existe indiquant des données en attente. Les économies d'énergie ont donc lieu seulement du côté client car le point d'accès a besoin de rester toujours éveillé pour envoyer des balises et stocker les données pour les clients. Les implémentations du mode d'économie d'énergie chez les différents fabricants peuvent être incompatibles entre elles, pouvant ainsi causer l'instabilité des connexions sans fil. Il est presque toujours préférable de laisser le mode d'économie d'énergie désactivé sur tous les équipements. Ceci parce que les difficultés qu'il engendre pourront sans doute l'emporter sur la maigre quantité d'énergie économisée.

Sélection de la tension

La plupart de systèmes autonomes à faible énergie utilisent une batterie à 12 V car c'est la tension opérationnelle la plus communément utilisée par les batteries scellées au plomb-acide. Lors de la conception d'un système de communication sans fil, vous avez besoin de prendre en considération la tension la plus efficace pour le fonctionnement de votre équipement. Alors que la tension d'entrée peut s'étaler sur un large éventail de valeurs, vous devez vous assurer que l'ensemble de la consommation d'énergie du système est minime.

Câblage

Le câblage est un élément important de l'installation car un câblage approprié assurera un transfert efficace de l'énergie. Certaines bonnes pratiques que vous devez considérer sont :

- Utilisez une vis pour attacher le câble aux bornes de la batterie. Les connexions lâches gaspilleront l'énergie.
- Appliquez de la vaseline ou un gel minéral sur les cosses de la batterie. La corrosion accroît la résistance électrique de la connexion, entraînant des pertes.
- Pour des faibles courants (<10 A), envisager le recours à des connecteurs de type Faston ou Anderson Powerpole. Pour les courants forts, utiliser des blocs de jonction à tige filetée.

La taille du câble est souvent donnée en *American Wire Gauge* (AWG). Au cours de vos calculs, vous aurez besoin d'une conversion entre AWG et mm^2 pour estimer la résistance du câble. Par exemple, un câble de type AWG # 6 a un diamètre de 4,11 mm et peut supporter jusqu'à 55 A. Une table de conversion, incluant une estimation de la résistance et la capacité d'intensité, est disponible à l'Annexe D. Gardez à l'esprit que l'intensité maximale peut également varier selon le type d'isolation et d'application. En cas de doute, consulter le fabricant pour des plus amples informations.

L'orientation des panneaux

La plus grande partie de l'énergie du soleil arrive en ligne droite. Le module solaire va capturer plus d'énergie s'il est en "face" du soleil, et perpendiculaire à la ligne droite entre la position de l'installation et le soleil. Bien sûr, la position du soleil est en constante évolution par rapport à la terre. Nous devons donc trouver une position optimale pour nos panneaux. L'orientation des panneaux est déterminée par deux angles, ***l'azimut a*** et ***l'inclinaison*** ou ***l'élévation ß***. L'azimut est l'angle qui mesure la déviation par rapport au sud dans l'hémisphère nord, et la déviation par rapport au nord dans l'hémisphère sud. L'inclinaison est l'angle formé par la surface du module et le plan horizontal.

Azimut

Le module doit être tourné vers l'équateur terrestre (face au sud dans l'hémisphère nord et au nord dans l'hémisphère sud), de sorte qu'au cours de la journée, le panneau capte la plus grande quantité de rayonnement possible (a = 0).

Il est très important qu'aucune partie des panneaux ne reste jamais à l'ombre. Etudiez les éléments qui entourent le panneau solaire (arbres, bâtiments, murs, d'autres panneaux, etc.) pour être sûr qu'aucune ombre ne soit projetée sur les panneaux à un moment du jour ou de l'année. Il est acceptable de tourner les panneaux de ± 20° vers l'est ou l'ouest en cas de besoin (a = ± 20°).

Inclinaison

Une fois que vous avez fixé l'azimut, le paramètre clé de vos calculs est l'inclinaison du panneau, que nous exprimerons comme l'angle bêta (ß). La hauteur maximale que le soleil atteint tous les jours va varier, atteignant son maximum le jour du solstice d'été et son minimum au solstice d'hiver. Idéalement, les panneaux devraient suivre cette variation, mais ce n'est généralement pas possible pour des raisons de coût.

Dans les installations avec des équipements de télécommunications, il est normal d'installer les panneaux avec une inclinaison fixe. Dans la plupart des scénarios de télécommunication, les demandes en énergie du système sont constantes tout au long de l'année. Fournir une énergie suffisante au cours du “pire des mois” pourra bien marcher pour le reste de l'année.

La valeur de l'angle bêta (ß) devrait permettre de maximiser le rapport entre l'offre et la demande d'énergie.

- Pour les installations à consommation énergétique constante (ou presque constante) tout au long de l'année, il est préférable d'optimiser l'installation pour capter le maximum de rayonnement durant les mois “d'hiver”. Vous devez utiliser la valeur absolue de la latitude du lieu (angle F) augmentée de 10° (ß = lFl + 10°).
- Pour les installations à faible consommation pendant l'hiver, la valeur de la latitude de l'endroit peut être utilisée comme inclinaison du panneau solaire. De cette façon, le système est optimisé pour les mois de printemps et d'automne (ß = lFl).
- Pour les installations qui ne sont utilisées que pendant l'été, vous devriez utiliser la valeur absolue de la latitude du lieu (angle F) diminué de 10° (ß = lFl - 10°). L'inclinaison du panneau ne devrait jamais être inférieure à 15° pour éviter l'accumulation de poussière et/ou l'humidité sur le panneau. Dans les régions où la neige et la glace peuvent tomber, il est très important de protéger les panneaux et les incliner à un angle de 65° ou plus.

S'il y a une augmentation considérable de consommation au cours de l'été, vous devriez considérer un arrangement pour deux inclinations fixes, une pour les mois d'été et une autre pour les mois d'hiver. Cela nécessiterait des structures de support spéciales et un horaire régulier pour changer la position des panneaux.

Comment dimensionner votre système photovoltaïque

Lors du choix d'un équipement répondant à vos besoins en électricité, vous devrez au minimum déterminer les éléments suivants :

- Le nombre et le type de panneaux solaires nécessaires pour capturer l'énergie solaire suffisante pour supporter votre charge.
- La capacité minimale de la batterie. La batterie aura besoin de stocker assez d'énergie pour fournir la puissance pendant la nuit et les jours de faible ensoleillement, et déterminera votre nombre de jours d'autonomie.
- Les caractéristiques de toutes les autres composantes (le régulateur, câblage, etc.) nécessaires pour supporter l'électricité produite et stockée.

Les calculs de dimensionnement système sont importants car l'énergie (et à terme l'argent) est gaspillée à moins que les composantes du système ne soient équilibrées. Par exemple, si nous installons plus de panneaux solaires pour produire plus d'énergie, les batteries doivent avoir une capacité suffisante pour stocker le surplus d'énergie produite. Si le banc des batteries est trop petit et la que charge n'utilise pas l'énergie quand elle est générée, alors l'énergie devra être jetée. Un régulateur utilisant une intensité de courant inférieure à celle requise, ou un seul câble simple qui est trop petit, peut être une cause de défaillance (ou même d'incendie) rendant l'installation inutilisable.

Ne jamais oublier que la capacité de production et de stockage de l'énergie photovoltaïque est limitée. Laisser allumer accidentellement une ampoule au cours de la journée peut facilement vider votre réserve avant la nuit, au point de rendre indisponible toute énergie supplémentaire. La disponibilité des "combustibles" pour les systèmes photovoltaïques (c'est-à-dire le rayonnement solaire) peut être difficile à prévoir. En fait, il n'est jamais possible d'être absolument certain qu'un système autonome va être en mesure de fournir l'énergie nécessaire à un moment donné. Les systèmes solaires sont conçus pour une certaine consommation, et si l'utilisateur dépasse les limites fixées, la fourniture d'énergie est vouée à l'échec.

La méthode de conception que nous proposons consiste à examiner les besoins en énergie et, en se basant sur ces besoins, à calculer un système capable de fonctionner le plus longtemps possible, pour être le plus fiable possible. Bien sûr, plus des panneaux et batteries sont installés, plus d'énergie pourra être collectée et stockée. Cette augmentation de la fiabilité entraînera aussi une augmentation des coûts.

Dans certaines installations photovoltaïques (telles que la fourniture de l'énergie pour les équipements de télécommunications sur une dorsale d'un réseau), le facteur fiabilité est plus important que le coût. Dans une installation client, un coût faible sera probablement le facteur le plus important. Trouver un équilibre entre le coût et la fiabilité n'est pas une tâche facile, mais quel que soit votre situation, vous devriez être en mesure de déterminer ce qui est attendu de vos choix de conception et à quel prix.

La méthode que nous utiliserons pour le dimensionnement du système est connue sous le nom de la "méthode du pire des mois". Nous calculons simplement les dimensions du système autonome de façon qu'il fonctionne dans le mois au cours duquel la demande d'énergie est la plus grande en termes d'énergie solaire disponible. C'est le mois le plus défavorable de l'année car il aura le plus grand rapport entre l'énergie demandé et l'énergie disponible.

En utilisant cette méthode, la fiabilité est prise en considération en fixant le nombre maximal de jours que le système peut fonctionner sans recevoir de rayonnement solaire (lorsque toute consommation est faite uniquement au prix de l'énergie stockée dans la batterie). Ceci est connu sous le nom de "nombre maximum de jours d'autonomie" (N), et peut être considéré comme le nombre de jours nuageux lorsque les panneaux ne recueillent aucune quantité signifiante d'énergie.

Au moment de choisir N, il est nécessaire de connaître la climatologie de l'endroit, ainsi que la destination économique et sociale de l'installation. Sera-t-elle utilisée pour éclairer les maisons, un hôpital, une usine, pour une liaison

radio, ou pour une autre application ? Rappelez-vous que quand N augmente, l'investissement dans l'équipement et l'entretien augmente aussi. Il est également important d'évaluer tous les coûts logistiques d'équipement de remplacement. Changer une batterie déchargée à partir d'une installation dans le centre d'une ville est différent de changer une batterie qui est au sommet d'un poteau de télécommunications qui se trouve à plusieurs heures ou jours de marche.

Fixer la valeur de N n'est pas une tâche facile car de nombreux facteurs entrent en cause, et beaucoup d'entre eux ne peuvent être évalués facilement. Votre expérience va jouer un rôle important dans cette partie du dimensionnement système. Une valeur couramment utilisée pour des équipements de télécommunications critiques est N = 5. Pour les équipements client à faible coût, il est possible de réduire l'autonomie à N = 3.

Dans l'Annexe E, nous avons inclus plusieurs tableaux qui faciliteront la collecte des données nécessaires pour le dimensionnement du système. Le reste de ce chapitre vous expliquera en détails les informations que vous avez besoin de collecter ou d'estimer et la façon d'utiliser la méthode du “pire des mois”.

Données à collecter

- **Latitude de l'installation**. N'oubliez pas d'utiliser un signe positif dans l'hémisphère nord et négatif dans le sud.
- **Les données de rayonnement solaire**. Pour la méthode du “pire des mois”, il suffit de connaître juste douze valeurs, une pour chaque mois. Les douze valeurs sont des valeurs moyennes mensuelles de l'irradiation quotidienne globale sur le plan horizontal (G_{dm} (0), en kWh/m² par jour). La valeur mensuelle est la somme des valeurs de l'irradiation globale pour tous les jours du mois, divisée par le nombre de jours du mois.

Si vous avez les données en joules (J), vous pouvez appliquer la conversion suivante :

$$1\ J = 2.78 \times 10^{-7}\ kWh$$

Les données d'irradiation $G_{dm}(0)$ de nombreux endroits du monde sont rassemblées dans des tableaux et bases de données. Vous devriez vérifier ces informations à partir d'une station météorologique proche de votre site d'implémentation, mais ne soyez pas surpris si vous ne trouvez pas les données en format électronique. C'est une bonne idée de demander à des entreprises qui installent des systèmes photovoltaïques dans la région, car leur expérience peut être d'une grande valeur.

Ne pas confondre “heures d'ensoleillement” avec le nombre “d'heures d'équivalent plein soleil”. Le nombre d'heures d'équivalent plein soleil n'a rien à voir avec le nombre d'heures sans nuages, mais se rapporte à la quantité quotidienne de l'irradiation. Une journée de 5 heures de soleil sans nuages n'est pas nécessairement ce nombre d'heures quand le soleil est à son apogée (au zénith).

Une heure d'équivalent plein soleil est une valeur normalisée d'un rayonnement solaire de 1000 W/m² à 25 °C. Ainsi, lorsque nous nous référons à

5 heures d'équivalent plein soleil, ceci implique un rayonnement solaire quotidien de 5000 W/m^2.

Caractéristiques électriques des composantes du système

Les caractéristiques électriques des composantes de votre système devraient être fournies par le fabricant. Il est conseillé de faire vos propres mesures pour vérifier toute déviation par rapport aux valeurs nominales. Malheureusement, l'écart par rapport aux valeurs promises peut être importante et devrait être prévue.

Voici les valeurs minimales que vous avez besoin de rassembler avant de commencer votre dimensionnement système :

Panneaux

Vous avez besoin de savoir la tension V_{Pmax} et le courant I_{Pmax} au point de puissance maximale dans des conditions normales.

Batteries

Capacité nominale (pendant 100 heures de décharge) C_{NBat}, la tension opérationnelle V_{NBat}, et soit la profondeur de décharge maximale (Maximum Depth of discharge DoD_{max}) ou la capacité utile C_{UBat}. Vous avez également besoin de connaître le type de batterie que vous envisagez d'utiliser, si elle est de type scellée au plomb-acide, gel, AGM, traction modifiée, etc. Le type de batterie est important lorsqu'il s'agit de décider des points de coupure dans le régulateur.

Régulateur

Vous avez besoin de connaître la tension nominale V_{NReg}, et le courant maximal qui peut être utilisé I_{maxReg}.

Convertisseur/Onduleur DC/AC

Si vous allez utiliser un convertisseur, vous avez besoin de connaître la tension nominale V_{NConv}, la puissance instantanée P_{IConv} et la performance à 70% de la charge maximale H70.

Equipement ou charge

Il est nécessaire de connaître la tension nominale de V_{NC} et la puissance nominale d'opération P_C pour chaque équipement alimenté par le système.

Afin de connaître l'énergie totale que notre installation va consommer, il est aussi très important de tenir compte de la durée moyenne d'utilisation de chaque charge. Est-elle constante ? Ou va-t-elle être utilisée quotidiennement, hebdomadairement, mensuellement ou annuellement ? Examinez les changements dans l'usage qui pourrait avoir une incidence sur la quantité d'énergie nécessaire (usage saisonnier, périodes de formation ou scolaires, etc.).

Les autres variables

Outre les caractéristiques électriques des composantes et de la charge, il est nécessaire de se prononcer sur deux autres éléments d'information avant d'être en mesure de dimensionner un système photovoltaïque. Ces deux décisions sont le nombre requis de jours d'autonomie et la tension de fonctionnement du système.

N, le nombre de jours d'autonomie

Vous avez besoin de vous prononcer sur une valeur pour N qui soit un compromis entre les conditions météorologiques, le type d'installation et l'ensemble des frais. Il est impossible de donner une valeur concrète de N appliquable à chaque installation, mais le tableau suivant donne quelques valeurs recommandées. Prenez ces valeurs comme une approximation grossière, et consultez un concepteur expérimenté pour parvenir à une décision finale.

Lumière du soleil	Installation domestique	Installation critique
Très nuageux	5	10
Variable	4	8
Ensoleillé	3	6

V_N, tension nominale de l'installation

Les composantes de votre système doivent être choisies pour fonctionner à une tension nominale V_N. Cette tension est généralement de 12 ou 24 Volts pour les petits systèmes, et si la puissance totale de la consommation dépasse 3 kW, la tension sera de 48 V. Le choix de V_N n'est pas arbitraire, et dépend de la disponibilité de l'équipement.

- Si l'équipement le permet, essayer de fixer la tension nominale à 12 ou 24 V. De nombreuses cartes de communication sans fil acceptent une large gamme de tension d'entrée et peuvent être utilisées sans convertisseur.
- Si vous avez besoin d'alimenter plusieurs types d'équipements qui fonctionnent à des tensions nominales différentes, vous devez calculer la tension qui minimise la consommation globale de l'énergie, y compris les pertes de conversion de puissance dans les convertisseurs DC/DC et DC/AC.

Procédure de calcul

Il existe trois étapes principales qui doivent être suivies pour calculer la taille appropriée d'un système :

1. **Calculer l'énergie solaire disponible (l'offre)**. Sur la base de données statistiques du rayonnement solaire et de l'orientation et l'inclinaison optimale des panneaux solaires, nous calculons l'énergie solaire disponible. L'estimation de l'énergie solaire disponible est faite par intervalles mensuelles qui réduisent les données statistiques à 12 valeurs. Cette estimation est un bon compromis entre la précision et la simplicité.
2. **Estimer le besoin d'énergie électrique (la demande)**. Enregistrez les caractéristiques de consommation d'énergie de l'équipement choisi ainsi que l'usage estimé. Ensuite, faites le calcul de l'énergie électrique requise sur une base mensuelle. Vous devriez envisager les fluctuations d'usage à cause des variations entre l'hiver et l'été, la saison des pluies/saison sèche, les périodes d'école/vacances, etc. Le résultat de cette estimation sera 12 valeurs de demande d'énergie, une pour chaque mois de l'année.
3. **Calculer la taille idéale du système (le résultat)**. Avec les données provenant du “pire des mois”, lorsque la relation entre l'énergie solaire demandée et l'énergie solaire disponible est la plus grande, nous calculons :

- Le courant que la matrice de panneaux doit fournir, ce qui permettra de déterminer le nombre minimal de panneaux.
- La capacité de stockage de l'énergie pour couvrir le nombre minimum de jours d'autonomie, qui permettra de déterminer le nombre requis de batteries.
- Les caractéristiques électriques du régulateur.
- La durée et les sections de câbles nécessaires pour les connexions électriques.

Le courant nécessaire dans le mois le plus défavorable

Pour chaque mois, vous avez besoin de calculer la valeur I_m, qui est le courant quotidien maximum qu'une matrice de panneaux fonctionnant à tension nominale V_N doit fournir sur une journée avec une irradiation de G_{dm} pour le mois «m», pour des panneaux inclinés à ß degrés.

L'I_m (pour le pire des mois) sera la plus grande valeur de I_m, et le dimensionnement système est basé sur les données de ce mois. Les calculs de

G_{dm}(ß) pour un certain lieu peuvent être faits sur base de G_{dm}(0) en utilisant des logiciels tels que PVSYST (*http://www.pvsyst.com/*) ou PVSOL (*http://www.solardesign.co.uk/*).

En raison des pertes du régulateur et des batteries, et du fait que les panneaux ne fonctionnent pas toujours au point de puissance maximale, le courant I_{mMAX} est calculé comme suit:

$$I_{mMAX} = 1,21\ I_m \text{ (le pire des mois)}$$

Une fois que vous avez déterminé le pire des mois, la valeur de I_{mMAX}, et l'énergie totale dont vous avez besoin E_{TOTAL} (le pire des mois), vous pouvez procéder aux calculs finaux. E_{TOTAL} est la somme de toutes les charges AC et DC en Watts. Pour calculer E_{TOTAL} voir **l'annexe E**.

Nombre de panneaux

En combinant les panneaux solaires en série et parallèle, nous pouvons obtenir la tension et le courant requis. Lorsque les panneaux sont connectés en série, la tension totale est égale à la somme des tensions individuelles de chaque module, tandis que le courant reste inchangé. Lorsque les panneaux sont connectés en parallèle, les courants sont additionnés tandis que la tension reste inchangée. Il est très important d'utiliser des panneaux ayant des caractéristiques presque identiques lors de la création d'une matrice des panneaux.

Vous devriez essayer d'acquérir des panneaux avec une tension V_{Pmax} un peu plus élevée que la tension nominale du système (12, 24 ou 48V). Rappelez-vous que vous avez besoin de fournir un peu plus de volts que la tension nominale de la batterie afin de la charger. Si vous ne trouvez pas de panneau capable de satisfaire à lui seul vos besoins, il vous faut connecter plusieurs panneaux en série pour atteindre la tension de votre choix. Le nombre de panneaux en série N_{ps} est égal à la tension nominale du système divisée par la tension d'un seul panneau, arrondi à l'entier le plus proche.

$$N_{ps} = V_N \ / \ V_{Pmax}$$

Afin de calculer le nombre de panneaux en parallèle (N_{PP}), vous devez diviser le courant I_{mMAX} par le courant d'un seul panneau au point de puissance maximale I_{Pmax}, arrondi à l'entier le plus proche.

$$N_{pp} = I_{mMAX} \ / \ I_{Pmax}$$

Le nombre total de panneaux est le résultat de la multiplication du nombre de panneaux en série (pour régler la tension) par le nombre de panneaux en parallèle (pour régler le courant).

$$N_{TOTAL} = N_{ps} \times N_{pp}$$

Capacité de la batterie ou accumulateur

La batterie détermine la tension globale du système. Elle nécessite une capacité suffisante pour fournir l'énergie pour la charge quand le rayonnement solaire n'est pas suffisant.

Pour estimer la capacité de notre batterie, nous devons d'abord calculer la capacité énergétique nécessaire pour notre système (C_{NEC} capacité nécessaire).

La capacité nécessaire dépend de l'énergie disponible durant le “pire des mois” et du nombre de jours d'autonomie (N).

$$C_{NEC}\ (Ah) = E_{TOTAL}(\text{pire des mois})(Wh) \ / \ V_N(V) \times N$$

La capacité nominale de la batterie C_{NOM} doit être plus grande que la C_{NEC} car nous ne pouvons pas décharger complètement la batterie. Pour déterminer la capacité de batterie dont nous aurons besoin, nous devons considérer l'intensité maximale de la décharge (DoD) que la batterie permet :

$$C_{NOM}(Ah) = C_{NEC}(Ah) \ / \ DoD_{MAX}$$

Pour calculer le nombre de batteries en série (N_{bs}), on divise la tension nominale de notre installation (V_N) par la tension nominale d'une seule batterie (V_{NBat}) :

$$N_{bs} = V_N \ / \ V_{NBat}$$

Régulateur

Un avertissement important : toujours utiliser les régulateurs en série, jamais en parallèle. Si votre régulateur ne supporte pas le courant requis par votre système, vous devrez acheter un nouveau régulateur avec supportant une intensité plus élevé.

Pour des raisons de sécurité, un régulateur doit être en mesure de fonctionner avec un courant I_{maxReg} d'au moins 20% supérieur à l'intensité maximale qui est prévue par la matrice de panneaux :

$$I_{maxReg} = 1.2 \ N_{pp} \ I_{PMax}$$

Onduleur DC/AC

La consommation totale d'énergie nécessaire pour l'équipement AC est calculée en incluant toutes les pertes qui sont introduites par le convertisseur DC/AC (ou onduleur). Lors du choix d'un onduleur, gardez à l'esprit que les performances de l'onduleur varient en fonction de la puissance demandée. Un onduleur a de meilleures performances lorsque les caractéristiques d'exploitation sont proches de sa puissance nominale. Utiliser un onduleur de 1500 Watt de puissance pour alimenter une charge de 25 Watt est extrêmement inefficace. Afin d'éviter ce gaspillage d'énergie, il est important de considérer non pas la puissance de crête de tous vos équipements, mais la puissance de crête des équipements susceptibles de fonctionner simultanément.

Câbles

Une fois que vous connaissez le nombre de panneaux et de batteries, ainsi que le type de régulateur et les onduleurs que vous voulez utiliser, il est nécessaire de calculer la longueur et le diamètre des câbles nécessaires pour connecter les composantes.

La longueur dépend de l'emplacement de votre installation. Vous devriez essayer de réduire au minimum la longueur des câbles entre le régulateur, les

panneaux et batteries. Utiliser des câbles courts permettra de minimiser la perte en puissance et le coût du câble.

Le diamètre est choisi sur la base de la longueur du câble et du courant maximum qu'il doit transporter. L'objectif est de minimiser les chutes de tension. Afin de calculer l'épaisseur S du câble, il est nécessaire de connaître :

- Le courant maximum I_{MC} qui va circuler dans le câble. Dans le cas du sous-système panneau batterie, c'est le I_{mMAX} calculé pour chaque mois. Dans les sous-système batterie-charge, il dépend de la manière dont les charges sont connectées.
- La chute de tension (V_a-V_b) considérée comme acceptable dans le câble. La chute de tension qui résulte de l'ajout de toutes les chutes individuelles est exprimée en pourcentage de la tension nominale de l'installation. Les valeurs maximales courantes sont les suivantes :

Composant	Chute de tension (en% de V_N)
Matrice de panneaux -> Batterie	1%
Batterie -> Convertisseur	1%
Ligne principale	3%
Ligne principale (éclairage)	3%
Ligne principale (Equipement)	5%

Chutes de tension couramment acceptables dans les câbles

La section du câble est déterminée par la loi d'Ohm :

$$S(mm^2) = r(\Omega mm^2/m)L(m)\ I_{mMAX}(A)/\ (V_a\text{-}V_b)(V)$$

Où S est la section, R est la résistivité (propriété intrinsèque du matériau : pour le cuivre, 0,01286 Ω mm² / m), et L est la longueur.

S est choisi en fonction des câbles disponibles sur le marché. Vous devriez choisir la section immédiatement supérieure à celle qui est obtenue à partir de la formule. Pour des raisons de sécurité impliquant certaines valeurs minimales, un minimum de 6 mm² de section est utilisé pour le câble qui relie les panneaux et la batterie. Pour les autres sections, ce minimum est de 4 mm².

Coût d'une installation solaire

Bien que l'énergie solaire en elle-même soit gratuite, l'équipement nécessaire pour la transformer en énergie électrique utile ne l'est pas. Vous avez non seulement besoin d'acheter du matériel pour transformer l'énergie solaire en électricité et le stocker pour utilisation, mais vous devez également maintenir et

remplacer les diverses composantes du système. Le problème du remplacement de l'équipement est souvent négligé et un système solaire est souvent mis en oeuvre sans un bon plan de maintenance.

Description	Nombre	Coût unitaire	Sous total
Panneau solaire 60W (environ 4 $ / W)	4	$300	$1.200
Régulateur de 30A	1	$100	$100
Câblage (mètres)	25	$1 / metro	$25
Batteries à décharge profonde 50 Ah	6	$150	$900
		Total:	$2.225

Afin de calculer le coût réel de votre installation, nous incluons un exemple illustratif. La première chose à faire est de calculer les coûts d'investissement initiaux.

Le calcul de notre coût d'investissement est relativement facile une fois que le système a été dimensionné. Vous avez juste besoin d'ajouter le prix de chaque pièce d'équipement et le coût de la main-d'oeuvre pour l'installation et le câblage des équipements. Pour raison de simplicité, nous n'incluons pas les frais de transport et d'installation mais ces frais ne doivent pas être négligés.

Pour connaître le coût réel de fonctionnement d'un système, nous devons estimer la durée de vie de chaque composante du système et la fréquence à laquelle vous devez le remplacer. En comptabilité, cette terminologie est connue sous le nom d'amortissement.

Notre nouvelle table ressemblera à ceci :

Description	#	Coût unitaire	Sous total	Durée de vie (années)	Coût annuel
Panneau solaire 60W	4	$300	$1.200	20	$60
Régulateur 30A	1	$100	$100	5	$20
Câblage (mètres)	25	$1 / metro	$25	10	$2,50
Batterie a cycle Profond 50Ah	6	$150	$900	5	$180
		Total:	$2.225	Coût annuel:	$262,50

Comme vous pouvez le voir, une fois que le premier investissement a été fait, un coût annuel de 262,50 $ est prévu. Le coût annuel est une estimation du capital requis par an pour remplacer les composantes du système une fois qu'elles ont atteint la fin de leur durée de vie utile.

8
La construction d'un noeud de plein air

L'installation de matériel électronique en plein air implique de nombreuses considérations d'ordre pratique. De toute évidence, le matériel doit être protégé de la pluie, du vent, du soleil, et d'autres conditions difficiles. L'énergie doit être fournie, et l'antenne doit être montée à une hauteur suffisante. L'absence d'une prise de terre appropriée, la proximité de la foudre, l'utilisation d'une alimentation fluctuante, voire même un vent léger dans certaines conditions peuvent anéantir vos connexions sans fil. Ce chapitre donne une idée des problèmes pratiques auxquels vous serez confrontés lors de l'installation d'un équipement sans fil en plein air.

Boîtiers étanches

Il existe des nombreuses variétés de boîtiers étanches appropriés. Le métal ou le plastique peuvent être utilisés pour créer un conteneur étanche pour des équipements intégrés extérieurs.

Bien sûr, l'équipement a besoin d'énergie pour pouvoir fonctionner, et aura sans doute besoin de se connecter à une antenne et un câble Ethernet. Chaque fois que vous percez un boîtier étanche, vous créez un autre endroit potentiel d'infiltration d'eau.

L'association nationale des fabricants électriques (*NEMA*, *National Electrical Manufacturers Association*) prévoit des directives pour la protection de l'équipement électrique contre la pluie, la glace, la poussière et autres contaminants. Un boîtier ayant un indice ***NEMA 3*** ou plus est mieux approprié pour l'utilisation à l'extérieur dans un climat moyen. Un boîtier ayant un indice ***NEMA 4X*** ou ***NEMA 6*** fournit une excellente protection, même contre l'eau d'arrosage et la glace. Pour les accessoires servant à pénétrer le corps des enceintes (tels que les presse-étoupe et les connecteurs à cloison), la Commission Electrotechnique Internationale (IEC, *International Electrotechnical Commission*) assigne un Indice de Protection (IP, *Ingress Protection*). Un indice de protection d'entrée ***IP66*** ou ***IP67*** pourra protéger les trous percés contre de très forts jets d'eau. Un bon boîtier extérieur devrait aussi fournir une protection

contre le rayonnement UV en vue d'empêcher la rupture du boîtier de protection suite à l'exposition au soleil ainsi que protéger l'équipement à l'intérieur.

Bien entendu, trouver des boîtiers standardisés NEMA ou IEC peut être un défi dans votre région. Souvent, le matériel disponible localement peut être reconditionné pour être utilisé comme conteneur. Le plastique robuste ou des boîtes d'arroseurs en métal, les boîtiers des conduits électriques, ou même, à la rigueur des boites d'aliments en plastique peuvent être utilisés. Quand vous percez un boîtier, utilisez des joints plats ou toriques de qualité, avec un presse-étoupe pour sceller l'ouverture. Les composés de silicone stabilisés aux UV ou d'autres produits d'étanchéité peuvent être utilisés pour des installations temporaires, mais rappelez-vous que les câbles fléchissent dans le vent et les joints collés finiront par s'affaiblir et permettre une infiltration d'humidité.

Vous pouvez prolonger considérablement la durée de vie d'un boitier en plastique en le protégeant contre le soleil. Installer le boîtier à l'ombre, que ce soit en dessous d'un équipement existant, d'un panneau solaire, ou de feuilles minces de métal conçues spécifiquement pour cet objectif, va allonger considérablement la durée de vie du boîtier et du matériel qu'il contient.

Avant d'installer un dispositif électronique dans une boîte scellée, assurez-vous qu'il a des exigences de dissipation de chaleur minimales. Si votre carte mère a besoin d'un ventilateur ou d'un grand dissipateur de chaleur, n'oubliez pas qu'il n'y aura pas de circulation d'air, et votre dispositif électronique va sans doute cuire à mort sur la tour. Utilisez seulement des composants électroniques conçues pour être utilisés dans un environnement renfermé.

Fournir l'énergie

De toute évidence, l'énergie continue peut être fournie en faisant simplement un trou dans votre boîtier pour passer un câble. Si votre boîtier est assez grand (par exemple, un boîtier électrique extérieur), vous pouvez même câbler une prise de courant alternatif à l'intérieur de la boîte. Mais les fabricants supportent de plus en plus une fonctionnalité très pratique qui élimine le besoin d'un trou supplémentaire dans la boîte: l'***Alimentation par Ethernet*** (***PoE***, *Power over Ethernet*).

Le standard 802.3af définit une méthode permettant d'alimenter en énergie les dispositifs électroniques en utilisant les paires non utilisées d'un câble Ethernet standard. Près de 13 watts de puissance peuvent être fournis sans danger sur un câble CAT5 sans interférer avec les transmissions de données sur le même câble Ethernet. De nouveaux ***switchs POE*** (***endspan***), conformes 802.3af, alimentent directement les périphériques connectés. Ces switchs peuvent fournir de l'énergie sur les mêmes fils qui sont utilisés pour les données (paires 1-2 et 3-6) ou sur les fils non utilisés (paires 4-5 et 7-8). D'autres équipements, appelés ***injecteurs POE*** (***midspan***), sont insérés entre les switchs et le dispositif qui doit être alimenté. Ces injecteurs fournissent l'énergie sur les paires inutilisées.

Si votre routeur sans fil ou CPE supporte le standard 802.3af, vous pouvez, en théorie, le connecter simplement à un injecteur. Malheureusement, certains fabricants (notamment Cisco) sont en désaccord sur la polarité de l'énergie, et la connexion de matériels non compatibles peut endommager l'injecteur et

l'équipement à alimenter. Lisez le manuel et assurez-vous que votre injecteur et équipements sans fil s'accordent sur les pins et la polarité qui doit être utilisée pour l'énergie.

Si votre équipement sans fil ne supporte pas l'alimentation par Ethernet, vous pouvez toujours utiliser les paires non utilisées dans un câble CAT5 pour le transport de l'énergie. Vous pouvez soit utiliser un ***injecteur POE passif***, ou tout simplement construire un vous-même. Ces dispositifs connectent manuellement l'énergie continue à la paire inutilisée du câble sur une de ses extrémités, et relie l'autre extrémité directement à un connecteur branché à l'alimentation de l'équipement. Une paire de dispositifs POE passifs peut généralement être achetée pour moins de 20$.

Pour créer votre propre dispositif, vous aurez besoin de connaître les besoins en énergie pour son fonctionnement et produire au moins le courant et la tension correspondante à cette énergie, plus assez pour tenir compte de la perte engendrée par le fonctionnement du câble Ethernet. Il ne faut pas non plus fournir trop d'énergie, car la résistance du petit câble peut présenter un danger de feu. Vous pouvez trouver une calculatrice en ligne qui vous permettra de calculer la chute de tension pour un type donné de CAT5 sur: *http://www.gweep.net/~sfoskett/tech/poecalc.html*

Une fois que vous connaissez la puissance et la polarité électrique nécessaires pour alimenter votre matériel sans fil, pratiquez un sertissage de câble CAT5 en utilisant uniquement les fils des données (paires 1-2 et 3-6). Il vous suffit ensuite de connecter le transformateur aux paires 4-5 (généralement bleu/bleu-blanc) et 7-8 (brun/ brun-blanc) à une extrémité, et un connecteur correspondant à l'autre.

Considérations de montage

Dans de nombreux cas, le matériel peut être situé dans un bâtiment, à condition qu'il y ait une fenêtre en verre ordinaire par laquelle les ondes traversent. Le verre normal va présenter peu d'atténuation, mais le verre teinté présentera une atténuation inacceptable. Cela simplifie considérablement le montage, les problèmes de puissance et d'étanchéité, mais est de toute évidence utile uniquement dans les zones peuplées.

Lors du montage des antennes sur des tours, il est très important d'utiliser un crochet d'écartement, et ne pas monter les antennes directement à la tour. Ces crochets ont plusieurs fonctions incluant la séparation de l'antenne, l'alignement de l'antenne et sa protection.

Les crochets d'écartement doivent être suffisamment solides pour supporter le poids de l'antenne, et aussi le tenir en place pendant les jours venteux. N'oubliez pas que les antennes peuvent agir comme des petites voiles, et peuvent faire subir beaucoup de force à leurs montures en cas de vents forts. Lors de l'estimation de la résistance au vent, la surface totale de la structure de l'antenne doit être considérée, ainsi que la distance entre le centre de l'antenne et l'endroit du point de fixation au bâtiment. Les grandes antennes telles que les antennes plates ou les antennes sectorielles à gain élevé peuvent avoir une prise au vent considérable. L'utilisation d'une antenne parabolique à fentes ou en

filet, plutôt qu'une antenne plate, permettra de réduire la prise au vent sans trop affecter le gain de l'antenne. Assurez-vous que les crochets de montage et la structure de support sont solides afin d'éviter le désalignement de votre antenne au fil du temps (ou pire, de faire tomber la tour entièrement!)

Les crochets de montage doivent être suffisamment éloignés de la tour pour permettre l'orientation, mais pas trop éloignés afin d'éviter que les antennes deviennent trop difficiles à atteindre dans le cas ou l'antenne a besoin de service ou d'entretien.

Figure 8.1 : Une antenne ayant un crochet de soutènement étant montée sur une tour

Le tuyau sur le crochet d'écartement sur lequel l'antenne sera montée doit être rond. De cette façon, l'antenne peut pivoter sur le tuyau pour le pointage. Deuxièmement, le tuyau doit être aussi vertical. S'il est monté sur une tour conique, le crochet d'écartement devra être conçu de façon à atteindre cet objectif. Cela peut être fait en utilisant différentes longueurs d'acier, ou en utilisant des combinaisons de tige filetée et des plaques d'acier.

Comme l'équipement sera à l'extérieur pour toute sa durée de vie, il est important de s'assurer que l'acier utilisé soit à l'épreuve des intempéries. L'acier inoxydable a souvent un prix trop élevé pour les installations de tour. La galvanisation à chaud est préférée, mais elle peut ne pas être disponible dans

certaines régions. Peindre tout l'acier avec une bonne peinture antirouille marche également. Quand la peinture est choisie, il sera important de planifier une inspection annuelle du montage et repeindre en cas de besoin.

Pylônes haubanés

Un pylône haubané où on peut grimper est un excellent choix pour de nombreuses installations, mais pour des très hautes structures, un pylône autoportant pourrait être nécessaire.

Lors de l'installation des pylônes haubanés, une poulie fixée au sommet d'un poteau pourra faciliter l'installation de la tour. Le poteau sera soutenu par la section basse déjà en place, tandis que les deux sections de la tour seront attachées par un joint articulé. Une corde passant par la poulie va faciliter le relèvement de la section suivante. Une fois que la section cantilever est verticale, boulonnez là à la section inférieure du poteau. Le poteau (appelée flèche de levage dans le commerce) peut alors être retiré, et l'opération peut être répétée, si nécessaire. Serrez les cordes haubanées avec soin, en veillant à ce que vous utilisiez la même tension à tous les points d'ancrage appropriés. Choisissez les points de sorte que les angles, comme on le voit à partir du centre de la tour, soient aussi régulièrement espacés que possible.

Figure 8.2 : Un pylône haubané escaladable

Pylônes autoportants

Les pylônes autoportantes sont chères, mais parfois nécessaires, en particulier quand une hauteur importante est une exigence. Celles-ci peuvent être aussi simples qu'un poteau lourd lesté dans un empilage de béton, ou aussi complexes qu'un pylône de radio professionnelle.

Figure 8.3 : Un simple mat autoportant

Un pylône existant peut parfois être utilisé pour les abonnés, même si les antennes de transmission de type AM doivent être évitées parce que l'ensemble

de la structure est actif. Les antennes de type FM sont acceptables, à condition qu'au moins quelques mètres de distance séparent les antennes. Soyez conscient que même si les antennes de transmission adjacentes peuvent ne pas interférer avec votre connexion sans fil, celles de haute puissance FM peuvent interférer avec votre réseau câblé Ethernet. A chaque utilisation d'une tour d'antenne à forte densité de population, il faut être très scrupuleux sur la bonne mise à terre et envisager l'utilisation de câble blindé.

Figure 8.4 : Une tour beaucoup plus compliquée

Les dispositifs de toit

Des dispositifs de toit non pénétrants peuvent être utilisés sur des toits plats. Ceux-ci consistent en un trépied monté sur une base en métal ou bois. La base est ensuite lestée avec des briques, des sacs de sable, des cruches d'eau, ou simplement tout ce qui est lourd. L'utilisation de cette technique élimine le besoin de percer le toit avec des boulons de montage, et ainsi éviter les fuites potentielles.

Figure 8.5 : Cette base en métal peut être soutenue par des sacs de sable, des pierres, ou des bouteilles d'eau pour créer une plateforme stable sans perforer le toit.

Un support mural ou des sangles de métal assemblées peuvent être utilisés sur des structures existantes telles que les cheminées ou les côtés d'un bâtiment. Si les antennes doivent être montées sur plus de 4 mètres au-dessus du toit, pylône escaladable peut être une meilleure solution permettant de faciliter l'accès à l'équipement et prévenir le mouvement d'antenne lors de grands vents.

Métaux non similaires

Afin de réduire au minimum la corrosion électrolytique lorsque deux métaux différents sont en contact humide, leur potentiel électrolytique devrait être aussi proche que possible. Utilisez la graisse diélectrique sur la connexion entre deux métaux de type différent afin de prévenir tout effet d'électrolyse.

Le cuivre ne doit jamais toucher directement le matériel galvanisé sans un joint de protection approprié. L'eau coulant du cuivre contient des ions qui

enlèveront la couverture galvanisée (zinc) de la tour. L'acier inoxydable peut être utilisé comme un tampon matériel, mais vous devriez être conscient que l'acier inoxydable n'est pas un très bon conducteur. S'il est utilisé comme un tampon entre le cuivre et les métaux galvanisés, la surface de contact doit être grande et l'acier inoxydable devrait être mince. Un composé mixte devrait également être utilisé pour couvrir la connexion de sorte à empêcher l'eau s'inflitrer entre les métaux non similaires.

Protéger les connecteurs micro-ondes

L'humidité dans les connecteurs est probablement la cause la plus souvent observée des pannes des liaisons radio. Assurez-vous de serrer fermement les connecteurs, mais ne jamais utiliser une clé ou d'autres outils pour le faire. Rappelez-vous que les métaux se dilatent et se contractent avec les changements de température, et un connecteur trop serré peut se briser dans des conditions météorologiques extrêmes changeantes.

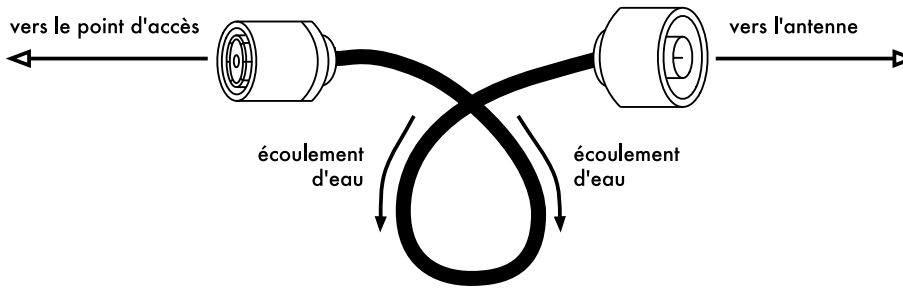


Figure 8.6 : Une boucle goutte éloigne l'eau de pluie de vos connecteurs

Une fois serrés, les connecteurs doivent être protégés en appliquant une couche de ruban électrique, puis une couche de ruban d'étanchéité, puis une autre couche de ruban électrique par dessus. L'étanchéifiant protège le connecteur contre l'infiltration d'eau, et la couche de ruban protège l'étanchéifiant des méfaits des rayons ultraviolets (UV). Les câbles doivent avoir une boucle goutte supplémentaire pour éviter une pénétration d'eau à l'intérieur de l'émetteur.

Sécurité

Utilisez toujours un harnais solidement fixé au pylône pendant le travail en hauteur. Si vous n'avez jamais travaillé sur une tour, faites appel à un professionnel pour le faire pour vous. De nombreux pays exigent une formation spéciale pour les personnes autorisées à travailler sur des pylônes au-dessus d'une certaine hauteur.

Évitez de travailler sur des pylônes au cours de vents forts ou de tempêtes. Montez toujours avec un partenaire, et seulement quand il fait bien jour. Le travail sur pylône prendra, sans doute, plus de temps que vous ne le pensez. Rappelez-vous qu'il est **extrêmement** dangereux de travailler dans l'obscurité.

Donnez-vous assez de temps pour terminer le travail bien avant le coucher du soleil. Si vous manquez de temps, rappelez-vous que la tour sera là le lendemain matin, et que vous pouvez commencer à travailler sur le problème de nouveau après une bonne nuit de sommeil.

Alignement d'antennes sur une liaison longue distance

Pour bien aligner les antennes à une grande distance, vous aurez besoin d'une sorte de retour visuel qui montre la puissance instantanée reçue à la source de l'antenne. Cela vous permet de faire de petits changements à l'alignement de l'antenne tout en vérifiant l'outil de rétroaction, et en vous arrêtant finalement quand la puissance maximale reçue a été trouvée.

La boîte à outils d'alignement d'antenne idéale se compose d'un ***générateur de signaux*** et d'un ***analyseur de fréquence*** ; de préférence l'un des deux à chaque extrémité de la liaison. L'adjonction d'un générateur de signaux à une extrémité de la liaison et d'un analyseur à l'autre vous permet d'observer la puissance reçue et de surveiller l'effet de déplacer l'antenne à différentes positions en temps réel. Une fois que le maximum a été trouvé sur une des extrémités d'une liaison point à point, le générateur et l'analyseur peuvent être échangés, et le processus répété de l'autre côté.

L'usage d'un générateur de signaux est préférable a celle d'une carte radio elle-même car le générateur de signaux peut générer un signal continu. Une carte WiFI transmet de nombreux paquets d'information en commutant l'émetteur sous tension et hors tension très rapidement. Cela peut être très à difficile à capter avec un analyseur de fréquence, surtout lorsqu'il opère dans des endroits bruyants.

De toute évidence, le coût d'un générateur de signaux calibrés et celui d'un analyseur qui fonctionne à 2,4 GHz (ou même 5 GHz si vous utilisez 802.11a) est bien au-delà du budget de la plupart des projets. Heureusement, il existe un certain nombre d'outils peu coûteux qui peuvent être utilisés en lieu et place.

Générateur de signaux économique

Il existe de nombreux émetteurs bon marché qui utilisent la bande des fréquences 2,4 GHz ISM. Par exemple, les téléphones sans fil, les écoute-bébés, et les transmetteurs de télévision miniaturisés génèrent tous un signal continu à 2,4 GHz. Les transmetteurs de télévision (parfois appelés ***expéditeurs vidéo***) sont particulièrement utiles, car ils ont souvent un connecteur d'antenne SMA et peuvent être alimentés par une petite batterie.

Les expéditeurs vidéo incluent généralement un support pour trois ou quatre canaux. Bien que ceux-ci ne correspondent pas directement aux canaux WiFI, ils permettent de tester l'extrémité basse, moyenne, ou haute de la bande des fréquences.

Pour le travail à 5 GHz, vous pouvez utiliser un transmetteur vidéo en combinaison avec un convertisseur de 2,4 GHz à 5 GHz. Ces dispositifs acceptent un signal faible de puissance 2,4 GHz et émettent des signaux

puissants de 5 GHz. Ils sont habituellement très cher (300-500 chacun), mais restent très probablement moins chers que le générateur de signaux et l'analyseur de fréquence à 5 GHz.

Quel que soit votre choix du signal source, vous aurez besoin d'un moyen d'afficher le niveau de puissance reçu à l'autre bout. Alors que le coût de la gamme d'analyseurs de fréquence de 2,4 GHz est à la baisse, ils coûtent quand même couramment quelques milliers de dollars, même pour le matériel d'occasion.

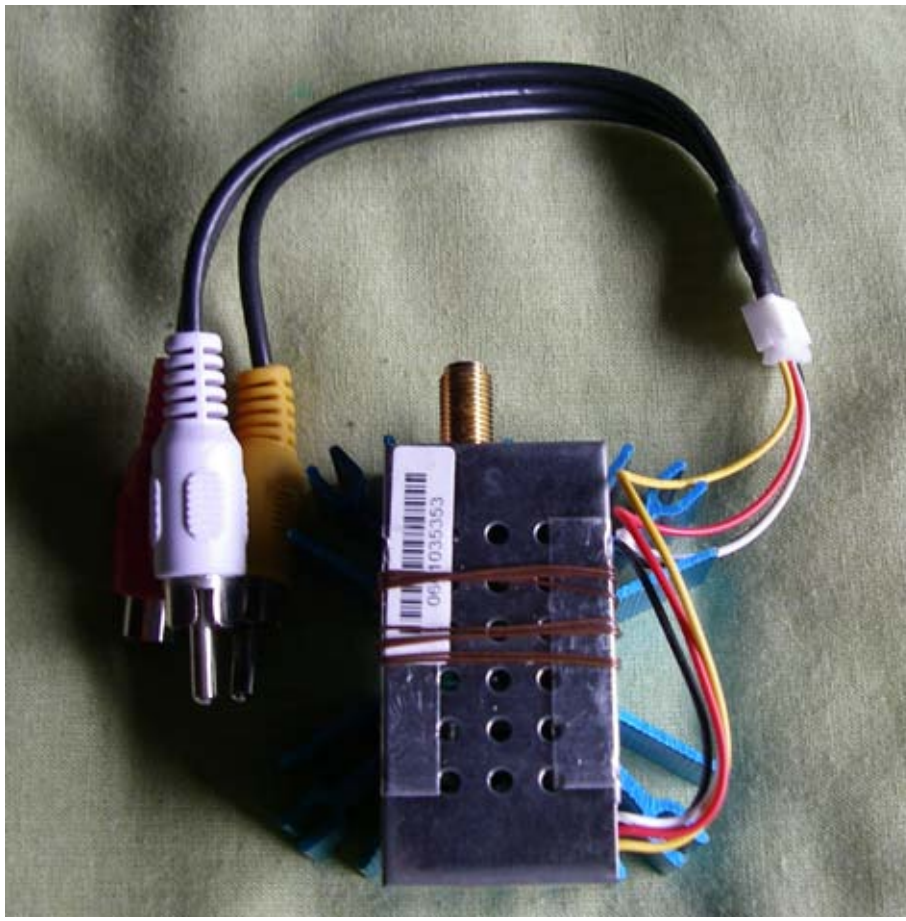


Figure 8.7 : Un expéditeur vidéo a 2.4 GHz avec un connecteur d'antenne SMA

Wi-Spy

Le Wi-Spy est un modèle d'analyseur de fréquence USB fabriqué par MetaGeek (*http://www.metageek.net/*). Il dispose d'un récepteur très sensible de petite taille (de la taille d'une clé USB).

Figure 8.8 : L'analyseur de fréquence USB Wi-Spy

La version Wi-Spy la plus récente comprend une meilleure gamme dynamique et un connecteur d'antenne externe. Elle est également fournie avec un très bon logiciel d'analyse de fréquence pour le système d'exploitation Windows appelé Chanalyzer. Elle fournit des vues instantanées, moyennes, maximales, topographiques, et spectrales.

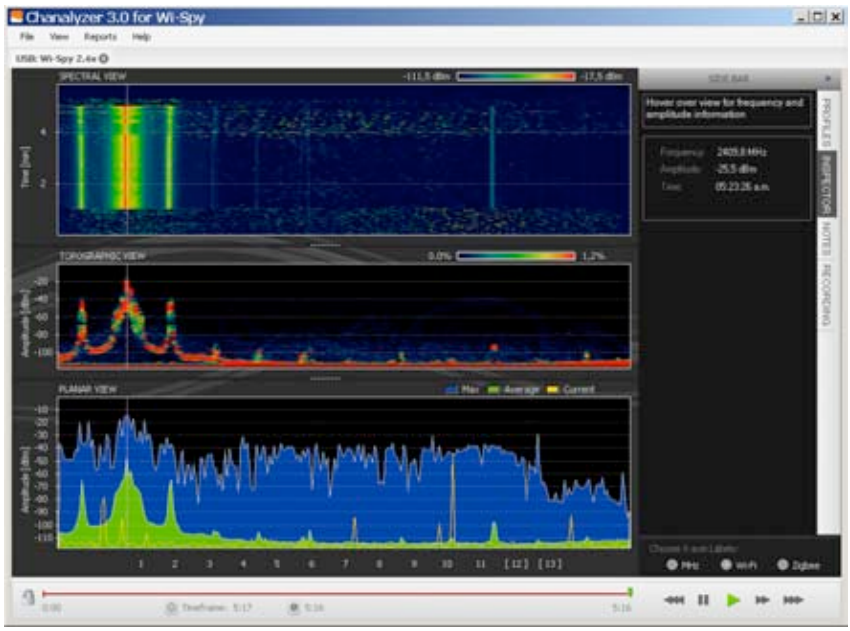


Figure 8.9 : Le motif distinctif en pic à gauche du graphe est causé par un transmetteur de télévision puissant de 2.4 GHz.

Il y a un excellent logiciel gratuit pour le système d'exploitation Mac OS X appelé EaKiu (*http://www.cookwareinc.com/EaKiu/*). En plus des vues standard, il fournit aussi une animation 3D, et ajoute le support pour de multiples dispositifs Wi-Spy.

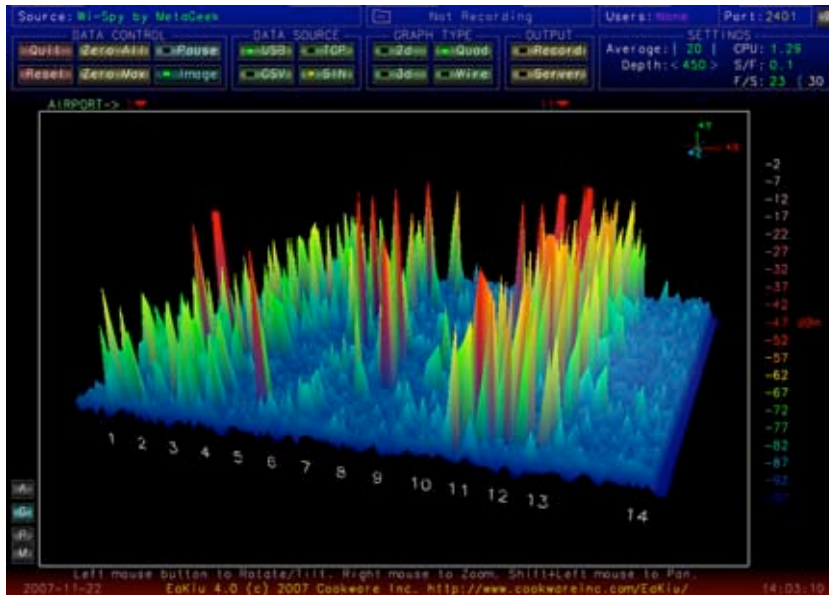


Figure 8.10 : La vue en 3D EaKiu vous laisse tourner et zoomer n'importe quelle partie du graphe en temps réel. Il y a probablement un réseau WiFI sur le canal 11, avec d'autres sources de bruit dans la bande.

Pour les utilisateurs du système d'exploitation Linux, Wi-Spy est supportée par le projet Kismet Spectrum-Tools (*http://kismetwireless.net/spectools/*). Ce package comprend les outils en ligne de commande ainsi que d'une interface graphique construite sur GTK.

Autres méthodes

Certains routeurs sans fil (comme le Mikrotik) fournissent un "outil d'alignement d'antenne" qui vous montre une barre mobile représentant la puissance reçue. Quand la barre est au maximum, l'antenne est alignée. Avec certains routeurs, vous pouvez également activer un mode rétroactif audio. Cela fait émettre au routeur un son bruyant, qui change de tonalité en fonction de la puissance reçue.

Si vous ne disposez pas d'un analyseur de fréquence Wi-Spy ou d'un dispositif qui supporte un mode d'alignement d'antenne, vous devrez utiliser le système d'exploitation pour obtenir une rétroaction sur la qualité de la liaison sans fil. Une méthode simple pour le faire sous Linux consiste à utiliser une boucle qui continuellement fait appel à la commande **`iwconfig`**. Par exemple:

```
wildnet:~# while :; do clear; iwconfig; sleep 1; done
```

Ceci affiche l'état de toutes les cartes radio dans le système en faisant des mises à jour une fois par seconde. Notez que cela ne fonctionne que sur le coté client d'une liaison sans fil. Du côté point d'accès (mode Maître), vous devez utiliser la commande **`iwspy`** pour collecter des statistiques pour l'adresse MAC du client:

```
wildnet:~# iwspy ath0 00:15:6D:63:6C:3C
wildnet:~# iwspy
ath0 Statistics collected:
 00:15:6D:63:6C:3C : Quality=21/94 Signal=-74 dBm Noise=-95 dBm
 Link/Cell/AP : Quality=19/94 Signal=-76 dBm Noise=-95 dBm
 Typical/Reference : Quality:0 Signal level:0 Noise level:0
```

Vous pouvez ensuite utiliser une boucle **`while`** (comme dans l'exemple précédent) pour mettre à jour continuellement le statut de la liaison.

```
wildnet:~# while :; do clear; iwspy; sleep 1; done
```

Procédure d'alignement d'antenne

La communication est la clé pour mener à bien l'alignement des antennes sur une très longue distance. Si vous changez trop de variables à la fois (par exemple, une équipe commence à bouger une antenne, tandis que l'autre tente de prendre une lecture du signal), alors le processus durera toute la journée et va probablement conduire à des antennes mal alignées.

Vous aurez deux équipes. Idéalement, chaque équipe doit avoir au moins deux personnes: une pour prendre la lecture du signal et les communiquer à l'autre équipe, et l'autre pour manipuler l'antenne. Gardez ceci à l'esprit lors du travail sur des liens à longue distance.

1. **Testez tous les équipements à l'avance.** Vous ne voudrez pas chipoter avec les réglages une fois que vous êtes sur le terrain. Avant de séparer l'équipement, allumez tout, connectez chaque antenne et cordon de liaison, et assurez-vous que vous pouvez établir une connexion entre les dispositifs. Vous devriez être en mesure de revenir à cet état sûr de bon fonctionnement par simple alimentation de l'appareil, sans avoir à vous authentifier ou à modifier les paramètres. Il est maintenant temps de se mettre d'accord sur la polarisation de l'antenne (voir le **Chapitre 2** si vous n'avez pas compris ce que signifie polarisation).

2. **Apportez des appareils de communication de secours.** Alors que les téléphones mobiles sont généralement assez bons pour travailler dans les villes, la réception mobile peut être mauvaise ou inexistante dans les zones rurales. Apportez une radio de haute puissance FRS ou GMRS, ou si vos équipes ont des permis de radio-amateur, utilisez une plate-forme amateur radio. Le travail à distance peut être très frustrant si vous êtes constamment obligé de demander à l'autre équipe "Pouvez-vous m'entendre maintenant?". Choisissez vos canaux de communication et testez vos radios (y compris les batteries) avant de vous séparer.

3. **Apportez un appareil photo.** Prenez le temps de documenter la situation géographique de chaque site en, incluant les repères et les obstacles. Cela peut être très utile plus tard pour déterminer la faisabilité d'une autre liaison à cet emplacement sans avoir à s'y déplacer en personne. Si c'est votre premier voyage sur le site, enregistrez les coordonnées GPS ainsi que l'altitude.

4. **Commencez par l'estimation de la bonne portée et altitude.** Pour commencer, les deux équipes devraient utiliser la triangulation (en utilisant les coordonnées GPS ou une carte) pour obtenir une idée approximative de la direction à pointer. Utilisez un compas pour aligner approximativement l'antenne au point d'incidence souhaité. Des grands repères sont également utiles pour le pointage. Si vous pouvez utiliser des jumelles pour voir l'autre bout, tant mieux. Une fois que vous avez fait votre approximation, faites une lecture de la puissance du signal. Si vous êtes assez près et vous avez fait une bonne approximation, vous pouvez déjà avoir un signal.

5. **Si tout le reste échoue, construire vos propres repères.** Certains types de terrains rendent la localisation de l'autre extrémité d'une liaison sans fil difficile. Si vous êtes en train de construire une liaison dans une zone avec peu de repères, un repérage personnel utilisant par exemple un cerf-volant, un ballon, une fusée de détresse, flammes, ou même un signal de fumée pourrait aider. Vous n'avez pas nécessairement besoin d'un GPS pour avoir une idée sur où pointer votre antenne.

6. **Tester le signal dans les deux directions, mais seulement une à la fois.** Une fois que les deux extrémités ont fait leur meilleure estimation, l'extrémité de la liaison sans fil ou l'antenne a le plus faible gain devrait mettre l'antenne en position. Utilisant un bon outil de contrôle (comme Kismet, Netstumbler, ou un bon client sans fil), l'équipe avec l'antenne à plus grand gain devrait balayer l'antenne lentement horizontalement tout en regardant la mesure du signal. Une fois que la meilleure position est trouvée, essayez de modifier l'élévation de l'antenne. Après que la meilleure position possible est trouvée, verrouiller l'antenne et contacter l'autre équipe pour qu'elle commence à réorienter lentement l'antenne. Répétez ce processus quelques fois jusqu'à ce que la meilleure position possible pour les deux antennes soit trouvée.

7. **Ne pas toucher l'antenne pour prendre une lecture.** Votre corps aura une incidence sur le rayonnement de l'antenne. Ne touchez pas l'antenne, et ne vous mettez pas dans le chemin de la visée de l'antenne quand vous prenez des mesures de la puissance du signal. Il en va de même pour l'équipe de l'autre côté de la liaison.

8. **N'ayez pas peur de dépasser le meilleur signal reçu.** Comme nous l'avons vu dans le **chapitre quatre**, les caractéristiques de rayonnement incorporent de nombreux petits lobes latéraux de sensibilité, en plus d'un beaucoup plus grand lobe principal. Si votre signal reçu est mystérieusement petit, vous pouvez avoir trouvé un lobe latéral. Continuez à balayer lentement au-delà de ce lobe pour voir si vous pouvez trouver le lobe principal.

9. **L'angle de l'antenne peut paraître complètement faux.** Le lobe principal d'une antenne rayonne souvent légèrement d'un côté ou

l'autre du centre visuel de l'antenne. Les antennes plates à alimentation offset sembleront pointer trop loin vers le bas, ou même directement vers le bas. Ne vous inquiétez pas pour l'apparence de l'antenne. Votre but est de trouver la meilleure position pour recevoir le meilleur signal possible.

10. **Tester doublement la polarisation.** Il peut être frustrant d'essayer d'aligner une antenne pour découvrir que l'autre équipe utilise une polarisation opposée. Encore une fois, ceci devrait être décidé avant de se séparer. Mais si un lien reste obstinément faible, un double contrôle ne peut pas faire de mal.

11. **Si rien ne fonctionne, vérifiez touts les composants un par un.** Est-ce que les appareils aux deux extrémités de la liaison sont allumés? Est-ce que tous les connecteurs et cordons de liaisons sont correctement connectés, est-ce qu'aucune partie n'est endommagée ou suspecte? Comme indiqué dans le **chapitre huit**, une technique de maintenance appropriée vous fera économiser du temps et épargner des frustrations. Travaillez lentement et communiquez bien votre avancement avec l'autre équipe.

En travaillant méthodiquement et en communicant bien, vous pouvez terminer le travail d'alignement des antennes à gain élevé en peu de temps. Si c'est fait correctement, ça devrait être amusant!

Protection contre la foudre et le surtension

L'alimentation en électricité représente le défi principal pour la plupart des installations dans les pays en voie de développement. Lorsque des réseaux d'alimentation existent, ils sont souvent mal gérés, délivrent un courant fluctuant énormément et sont la merci de la foudre. Une véritable protection contre la surtension est vitale pour protéger non seulement votre équipement sans-fil, mais aussi tous les matériels qui y sont reliés.

Fusibles et disjoncteurs

Les fusibles sont cruciaux, mais très souvent négligés. Dans les zones rurales, et même dans de nombreuses zones urbaines des pays en développement, les fusibles sont difficiles à trouver. Malgré le coût supplémentaire, il est plutôt toujours prudent d'utiliser des disjoncteurs. Ceux-ci peuvent devoir être importés, mais ne doivent pas être négligés. Trop souvent, les fusibles remplaçables sont supprimés et une pièce de monnaie est utilisée à la place. Dans un cas récent, l'ensemble des équipements électroniques d'une station radio en milieu rural a été détruit quand un coup de foudre est passé par le circuit, non équipé de coupe-circuit ou même d'un fusible de protection.

Comment mettre à la terre

Une prise de terre appropriée n'est pas un travail compliqué. Quand vous mettez à la terre, vous essayez d'accomplir deux choses: créer un court-circuit pour la foudre, et fournir aux excès d'énergie un circuit où se dissiper.

La première étape consiste à protéger le matériel contre un coup de foudre direct ou à proximité, alors que la seconde fournit un moyen pour dissiper l'énergie excédentaire qui, autrement, causerait une accumulation d'électricité statique. L'électricité statique peut provoquer une dégradation signifiante de la qualité du signal, en particulier sur les récepteurs sensibles (VSAT par exemple). Créer un court-circuit est simple. L'installateur doit simplement créer le chemin le plus court de la surface la plus conductrice (un paratonnerre) au sol. Lorsque la foudre touche le paratonnerre, l'énergie voyagera le long du chemin le plus court ; et ainsi donc passera au delà de l'équipement. La terre devrait être en mesure de supporter la haute tension (c'est-à-dire dont vous avez besoin d'une câble à diamètre important, comme un câble en cuivre tressé de 8 AWG).

Pour la prise de terre des équipements, monter un paratonnerre au-dessus de l'appareil sur une tour ou une autre structure. Ensuite, utilisez du câble à forte conductivité pour connecter le paratonnerre à quelque chose qui est bien mis à la terre. Les tuyaux de cuivre enterrés peuvent être très bien mis à la terre (en fonction de leur profondeur, de l'humidité, de la salinité, de la quantité de métal et de la teneur en matière organique du sol). Dans de nombreux sites en Afrique de l'Ouest, les tuyaux ne pas encore enfouis sous terre, et les précédents équipements de mise en terre sont souvent inadéquats en raison de la mauvaise conductivité du sol (typique des sols saisonnièrement arides, des sols tropicaux). Il y a trois façons simples pour mesurer l'efficacité de votre terre:

1. La moins précise consiste à simplement brancher un onduleur UPS de bonne qualité ou une multiprise qui a un indicateur de détection de terre (une lumière LED dans le circuit). Cette LED est alimentée par l'énergie qui est diffusée dans la terre. Une bonne terre dissipera une petite quantité d'énergie dans le sol. Certaines personnes utilisent cette méthode pour pirater un peu de lumière gratuite car cette énergie n'est pas prise en compte par le compteur électrique !
2. Prendre une douille et une ampoule de faible puissance (30 Watts), connecter un fil au fil de terre et le second à la phase. Si le fil de terre est bon, l'ampoule doit briller légèrement.
3. La méthode la plus complexe consiste à simplement mesurer l'impédance entre le circuit positif et la terre.

Si votre terre n'est pas efficiente, vous aurez besoin d'enterrer le socle plus profondément (le sol est plus humide là où il y a plus de matières organiques et de métaux) ou vous avez besoin de rendre le terrain plus conducteur. Une approche communément utilisée la où il y a peu de sol consiste à creuser un trou de 1 mètre de diamètre et 2 mètres de profondeur. Déposer dans le trou une pièce de métal très conductrice de masse importante. Ceci est parfois appelé un ***plomb***, mais peut être n'importe quel morceau de métal lourd de 50 kg ou plus, comme par exemple une enclume en fer ou une jante métallique. Puis

remplissez le trou avec du charbon de bois et mélangez le sel, puis ajoutez de la terre. Trempez la zone, et le charbon de bois et le sel vont diffuser autour du trou et créer une zone conductrice qui entoure le plomb en améliorant l'efficacité du sol.

Si un câble radio est utilisé, il peut aussi être utilisé pour la mise à la terre du pylône, même si une conception plus sûre consiste à séparer la terre du pylône de celle du câble. Pour la mise à la terre du câble, il suffit de dénuder un peu le câble à l'endroit le plus proche de la terre avant qu'il n'aille dans le bâtiment, puis joindre un câble de terre à partir de ce point, soit par soudure ou au moyen d'un connecteur très conducteur. Ceci doit être imperméabilisé.

Stabilisateurs et régulateurs de tension

Il existe de nombreuses marques de stabilisateurs de puissance, mais la plupart sont soit numériques ou électromécaniques. Ces derniers sont beaucoup moins chers et plus courants. Les stabilisateurs électromécaniques fonctionnent à 220V, 240V ou 110V et utilisent cette énergie pour faire tourner un moteur qui produit toujours la tension souhaitée (normalement 220V). Ceci est normalement efficace, mais ces unités offrent peu de protection contre la foudre ou d'autres hausses de tensions. Ils brûlent souvent après juste une attaque. Une fois brûlés, ils peuvent fondre et rester bloqués à une certaine (généralement mauvaise) tension de sortie.

Les régulateurs numériques servent à réguler l'énergie en utilisant des résistances et d'autres composants électroniques. Ils sont plus coûteux, mais sont beaucoup moins susceptibles d'être brûlés.

Dans la mesure du possible, utilisez les régulateurs numériques. Ils valent le coût ajouté et offrent une meilleure protection pour le reste de votre équipement. Assurez-vous d'inspecter touts les composants de votre système d'alimentation (y compris le stabilisateur), après la foudre.

9
Dépannage

La façon dont vous avez établi l'infrastructure de support de votre réseau est aussi importante que le type de matériel que vous utilisez. Contrairement aux connexions câblées, les problèmes avec un réseau sans fil sont souvent invisibles et peuvent exiger plus de compétences et plus de temps pour diagnostiquer et résoudre. L'interférence, le vent, et de nouveaux obstacles physiques peuvent entraîner une panne d'un réseau fonctionnant pourtant depuis longtemps. Ce chapitre décrit en détail une série de stratégies qui vous aideront à mettre en place une équipe qui peut maintenir efficacement votre réseau.

Mettre en place votre équipe

Chaque village, entreprise ou famille a des personnes qui sont intriguées par la technologie. Ce sont eux qu'on trouve en train d'épisser un câble de télévision, re-câbler une télévision en panne ou souder une nouvelle pièce sur un vélo. Ces personnes s'intéresseront à votre réseau et voudront apprendre le plus possible à ce sujet. Bien que ces personnes soient des ressources inestimables, vous devez éviter de donner toutes les connaissances spécialisées des réseaux sans fil à une seule personne. Si votre seul spécialiste perd intérêt ou trouve un travail plus rémunéré quelque part, il emmènera la connaissance avec lui là ou il va.

Il peut y avoir aussi de nombreux jeunes et adolescents ambitieux ou des jeunes adultes qui seront intéressés et auront le temps d'écouter, d'aider, et d'apprendre sur le réseau. Encore une fois, ils sont très utiles et apprendront rapidement, mais l'équipe du projet doit concentrer son attention sur ceux qui sont les mieux placés pour soutenir le réseau dans les mois et années à venir. Les jeunes adultes et les adolescents iront à l'université et trouveront de l'emploi, en particulier les jeunes ambitieux qui ont tendance à vouloir être impliqués. Ces jeunes ont également peu d'influence dans la communauté alors qu'une personne âgée est susceptible d'être plus capable de prendre des décisions qui affectent positivement l'ensemble du réseau. Même si ces personnes pourraient avoir moins de temps pour apprendre et sembler être moins intéressées, leur implication ainsi qu'une formation appropriée sur le système peut être critique.

Par conséquent, une stratégie clé dans la mise en place d'une équipe de maintenance est d'équilibrer et distribuer les connaissances à ceux qui sont les mieux placés pour soutenir le réseau à long terme. Vous devez faire participer les jeunes, mais ne les laissez pas monopoliser l'utilisation ou la connaissance de ces systèmes. Trouvez des personnes qui se sont engagés à la communauté, qui ont leurs racines dans la communauté, qui peuvent être motivés, et formez les. Une stratégie complémentaire consiste à compartimenter les fonctions et les devoirs, et documenter toutes les méthodes et procédures. De cette façon, les gens peuvent facilement être formés, et remplacés avec peu d'effort.

Par exemple, dans un site d'un projet, l'équipe de formation choisit un jeune diplômé universitaire qui était retourné dans son village. Il était très motivé et apprit vite. Comme il avait appris si vite, il était enseigné plus que ce qui avait été prévu, et il était en mesure de faire face à une variété de problèmes, allant de réparer un PC au câblage d'un réseau Ethernet. Malheureusement, deux mois après le lancement du projet, il s'est vu offrir un poste de fonctionnaire et a quitté la communauté. Même un meilleur salaire ne pouvait pas le garder car la perspective d'un emploi stable au gouvernement était trop séduisante. Toutes les connaissances sur le réseau et comment le maintenir partirent avec lui. L'équipe de formation a dû retourner et de commencer la formation de nouveau. La stratégie suivante fut de diviser les fonctions et former des personnes qui étaient définitivement enracinées dans la communauté: les gens qui avaient des maisons et des enfants et avaient déjà un emploi. Il avait fallu trois fois plus de temps pour enseigner trois personnes qu'il n'avait fallu pour former le jeune diplômé universitaire, mais la communauté conservera ce savoir plus longtemps.

Bien que ceci semble suggérer que vous devez choisir manuellement qui doit être impliqué, ce n'est pas souvent la meilleure approche. Il est souvent mieux de trouver un organisme partenaire local ou un gestionnaire local et travailler avec eux pour former la bonne équipe technique. Les valeurs, l'histoire, la politique locale, et de nombreux autres facteurs seront importants pour eux, tout en restant complètement incompréhensibles pour les personnes qui n'appartiennent pas à cette communauté. La meilleure approche est de donner des instructions à votre partenaire local, lui donner des critères fondés, de vous assurer qu'il comprend ces critères, et de fixer des limites fermes. Ces limites doivent inclure des règles sur le népotisme et le favoritisme, même si ces règles doivent tenir compte de la situation locale. Il peut être impossible de dire que vous ne pouvez pas embaucher des parents, mais il est préférable de prévoir un moyen de contrôle et des contrepoids. Si un candidat est parent, il devrait y avoir des critères clairs et une seconde autorité pour décider de sa candidature. Il est également important que ce pouvoir soit donné aux partenaires local et qu'il ne soit pas miné par les organisateurs du projet, ce qui compromettrait leur capacité à gérer. Ils seront mieux à même de juger qui travaillera mieux avec eux. S'ils sont bien éduqués dans ce processus, vos exigences devraient être mieux satisfaites.

Le dépannage et le support à la technique sont un art abstrait. La première fois que vous regardez une peinture abstraite, elle peut paraître comme un tas quelconque d'éclaboussures de peinture. Après avoir réfléchi sur la composition pendant un certain temps, vous pouvez parvenir à apprécier le travail dans son ensemble, et la cohérence "invisible" devient très réelle. Le néophyte à la vue

d'un réseau sans fil peut voir les antennes, des câbles et des ordinateurs, mais cela peut lui prendre un certain temps pour apprécier la raison “invisible” du réseau. Dans les zones rurales, il peut souvent falloir un énorme bond en compréhension avant que les habitants n’apprécient un réseau invisible qui est tout simplement tombé dans leur village. Par conséquent, une approche progressive est nécessaire pour permettre aux personnes de supporter les systèmes technologiques. La meilleure méthode est la participation. Une fois que les participants sont choisis et engagés au projet, impliquez les le plus possible. Laissez-les "diriger". Donnez-leur une pince à câble ou le clavier et montrez leur comment faire le travail. Même si vous n'avez pas le temps d'expliquer tous les détails et même si cela prendra plus de temps, ils doivent être impliqués physiquement et voir non seulement ce qui a été fait, mais aussi la quantité de travail qui a été faite.

La méthode scientifique est enseignée dans la quasi-totalité des écoles occidentales. Beaucoup de gens l’apprennent au moment où ils atteignent l'école secondaire dans les cours de science. Simplement dit, vous prenez un ensemble de variables, puis lentement vous éliminez ces variables par le biais de tests binaires jusqu'à ce qu’il vous reste seulement une ou seulement quelques possibilités. Avec ces possibilités à l'esprit, vous pouvez compléter votre expérience. Puis vous effectuez un test pour voir si l'expérience produit quelque chose de similaire au résultat escompté. Si non, vous recalculez votre hypothèse et essayez à nouveau. Le villageois agraire moyen peut avoir été eu des notions de ce concept, mais risque de ne pas avoir eu l'occasion de résoudre des problèmes complexes. Même s'il est familier avec la méthode scientifique, il risque de ne pas penser à l'appliquer pour résoudre des problèmes réels.

Cette méthode est très efficace, même si elle prend du temps. Elle peut être accélérée en faisant des hypothèses logiques. Par exemple, si un point d'accès qui fonctionnait depuis longtemps ne fonctionne plus après une tempête, vous pouvez soupçonner un problème d’alimentation, et par conséquent sauter la plupart des étapes de la procédure. Les personnes chargées du support technique devraient recevoir une formation de maintenance en utilisant cette méthode, car il y aura des moments où le problème n'est ni connu, ni évident. Des simples arbres de décision ou des diagrammes peuvent être établis pour tester ces variables, et essayer d'éliminer les variables pour isoler le problème. Bien entendu, ces diagrammes ne devraient pas être suivis aveuglément.

Il est souvent plus facile d'enseigner cette méthode en commençant avec un problème qui n’est pas technologique. Par exemple, vos étudiants peuvent avoir à développer une procédure de résolution d’un problème simple et familier, comme une télévision, alimentée par batterie. Commencez par le sabotage de la télévision. Donnez-leur une batterie qui n'est pas chargée. Débrancherz l'antenne. Insérez un fusible brisé. Testerz l'étudiant en montrant clairement que chaque problème peut révéler des symptômes spécifiques et montrerz la manière de procéder. Une fois qu'ils ont réparé la télévision, faites leur appliquer cette procédure à un problème plus complexe. Dans un réseau, vous pouvez changer une adresse IP, commuter ou endommager des câbles, utiliser un mauvais SSID, ou orienter l'antenne dans une mauvaise direction. Il est important qu’ils développent une méthodologie et une procédure pour résoudre ces problèmes.

Une bonne technique de dépannage

Aucune méthodologie de dépannage ne peut couvrir complètement tous les problèmes que vous allez rencontrer quand vous travaillez avec les réseaux sans fil. Mais souvent, les problèmes résultent en l'une des quelques erreurs courantes. Voici quelques points à avoir à l'esprit pour orienter votre effort de dépannage dans la bonne direction.

- **Ne pas paniquer.** Si vous êtes en train de dépanner un système, cela signifie qu'il était en train de fonctionner à un moment donné, probablement très récemment. Avant de vous précipiter et de faire des changements, faites état des lieux et évaluez exactement ce qui est endommagé. Si vous avez des journaux historiques ou des statistiques à utiliser, tant mieux. Assurez-vous de recueillir des informations en premier lieu, afin que vous puissiez prendre une décision appropriée avant de faire des changements.
- **Est-il branché?** Cette étape est souvent négligée jusqu'à ce que de nombreuses autres pistes ont été explorées. Les prises peuvent être très facilement débranchées accidentellement (ou intentionnellement). Est que la charge est relié à une bonne source d'énergie? Est-ce que l'autre extrémité est connectée à votre appareil? Est-ce que la lumière est allumée? Cela peut paraître stupide, mais vous vous sentirez plus stupide si vous passez beaucoup de temps à vérifier une ligne d'alimentation d'antenne pour réaliser après que le point d'accès a été tout ce temps débranché. Croyez-moi, ceci arrive plus souvent que la plupart d'entre nous pourraient l'admettre.
- **Quelle a été la dernière chose à être changée?** Si vous êtes la seule personne ayant accès au système, quel a été le dernier changement que vous avez fait? Si d'autres y ont accès, quel a été le dernier changement qu'ils ont fait et quand? À quand remonte la dernière fois que le système fonctionnait? Souvent, les modifications apportées au système ont des conséquences inattendues qui peuvent ne pas être remarquées immédiatement. Révisez ce changement et observez quel effet il a sur le problème.
- **Faites une sauvegarde.** Cela s'applique avant et après que vous remarquez les problèmes. Si vous réalisez un changement logiciel compliqué au système, avoir une copie de sauvegarde signifie que vous pouvez restaurer rapidement le système à ses paramètres précédents et recommencer. Lors du dépannage des problèmes très complexes, avoir une configuration qui fonctionne "à peu près" est beaucoup mieux qu'un gâchis qui ne fonctionne pas du tout (et que vous ne pouvez pas restaurer facilement de mémoire).
- **Référence KGS (Known Good State).** Cette idée s'applique au matériel, ainsi qu'au logiciel. Un produit référent est tout composant que vous pouvez remplacer dans un système complexe pour vérifier que son homologue est en bon état de fonctionnement. Par exemple, vous

pouvez transporter un câble Ethernet testé dans une trousse à outils. Si vous soupçonnez des problèmes avec un câble, vous pouvez facilement changer le câble suspect par le bon et voir si les choses s'améliorent. Cela est beaucoup plus rapide et moins sujet aux erreurs que re-sertir un câble, et vous indique immédiatement si le changement résout le problème. De même, vous pouvez également emmener avec vous une batterie de sauvegarde, un câble d'antenne, ou un CD-ROM avec une bonne configuration connue pour le système. Quand vous résolvez des problèmes compliqués, sauvegarder votre travail en un point donné vous permet de revenir à cet état connu comme bon, même si le problème n'est pas encore complètement résolu.

- **Changer une variable à la fois.** Lorsque vous êtes sous pression de remettre en service un système en panne, il est tentant de sauter en avant et changer des nombreuses variables à la fois. Si vous le faites, et que les modifications semblent résoudre le problème, alors vous n'allez pas comprendre exactement ce qui a conduit au problème en premier lieu. Pire encore, vos changements peuvent résoudre le problème mais conduire à des conséquences non intentionnelles qui endommagent d'autres parties du système. En changeant vos variables une à une, vous pouvez comprendre précisément ce qui s'est mal passé en premier lieu, et être en mesure de voir les effets directs des modifications que vous apportez.
- **Ne pas nuire.** Si vous ne comprenez pas pleinement comment un système fonctionne, n'ayez pas peur de faire appel à un expert. Si vous ne savez pas si un changement particulier va endommager une autre partie du système, alors soit cherchez quelqu'un avec plus d'expérience ou trouvez un moyen de tester vos modifications sans faire des dégâts. Mettre une pièce de monnaie en lieu et place d'un fusible peut résoudre le problème immédiat, mais peut aussi brûler le bâtiment.

Il est peu probable que les personnes qui ont conçus votre réseau seront disponibles vingt-quatre heures par jour pour résoudre vos problèmes lorsqu'ils surviennent. Votre équipe de dépannage devra avoir de bonnes compétences de dépannage, mais peut ne pas être suffisamment compétente pour configurer un routeur à partir de zéro ou sertir un morceau de LMR-400. Il est souvent beaucoup plus efficace d'avoir un certain nombre de composantes de sauvegarde à portée de main, et former votre équipe pour être en mesure d'échanger la partie endommagée entière. Cela pourrait vouloir dire avoir un point d'accès ou routeur pré configuré et mis dans un classeur verrouillé, clairement marqué et entreposé avec des câbles et alimentations de sauvegarde. Votre équipe peut remplacer des composants défectueus, et soit envoyer les pièces endommagées à un expert pour réparation ou s'arranger pour avoir une autre sauvegarde envoyée. Supposant que les sauvegardes sont conservées en toute sécurité et sont remplacées lorsqu'elles sont utilisées, cela peut épargner le temps pour tout le monde.

Les problèmes réseau communs

Souvent, les problèmes de connectivité proviennent de composantes défectueuses, des conditions météorologiques défavorables, ou une simple mauvaise configuration. Une fois que votre réseau est connecté à l'Internet ou ouvert au grand public, des menaces proviendront des utilisateurs du réseau eux-mêmes. Ces menaces peuvent aller de bénignes à la malveillance pure et simple, mais auront toutes un impact sur votre réseau s'il n'est pas correctement configuré. Cette section se penche sur certains problèmes courants une fois que votre réseau est utilisé par des êtres humains.

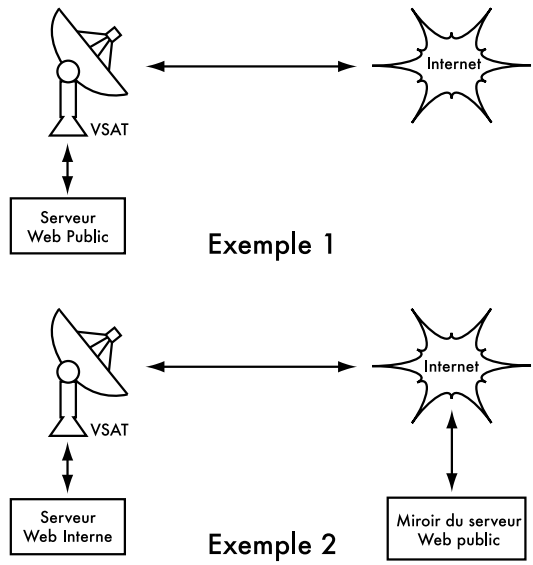


Figure 9.1 : Dans l'exemple 1, tout le trafic vers le site web venant de l'Internet doit traverser le VSAT. Dans l'exemple 2, le site web public est hébergé sur un service Européen rapide, alors qu'une copie est gardée sur un serveur local pour des accès locaux très rapides. Ceci améliore la connexion VSAT et réduit les temps de charge pour les utilisateurs du site web.

Sites hébergés localement

Si une université héberge son site Web localement, ceux qui visitent le site Web de l'extérieur du campus et le reste du monde seront en compétition pour l'usage de bande passante avec le personnel de l'université. Cela comprend l'accès automatisé à partir de moteurs de recherche qui périodiquement "aspirent" la totalité de votre site. Une solution à ce problème est d'utiliser le *split* DNS et le mirroring. L'université héberge une copie miroir de ses sites Internet à un serveur, disons, à un hébergeur européen, et utilisant le *split* DNS dirige tous les utilisateurs extérieurs au réseau universitaire sur le site miroir, tandis que les utilisateurs sur le réseau universitaire accèdent le même site localement. Les détails sur la façon de mettre en place ceci sont fournis dans **le troisième chapitre**.

Proxy ouverts

Un serveur proxy doit être configuré pour n'accepter que les connexions du réseau de l'université, pas du reste de l'Internet. Ceci parce que les gens d'ailleurs se connectent et utilisent les serveurs proxy ouverts pour des raisons diverses, comme par exemple éviter de payer pour la bande passante internationale. La façon de configurer ceci dépend du serveur proxy que vous utilisez. Par exemple, vous pouvez spécifier la gamme d'adresses IP du réseau du campus dans votre fichier **`squid.conf`** comme étant le seul réseau qui peut utiliser Squid. Alternativement, si votre serveur proxy se trouve derrière un pare-feu (Firewall), vous pouvez le configurer pour permettre seulement aux hôtes internes de se connecter au port du proxy.

Relais ouverts

Un serveur de messagerie mal configuré sera découvert par des gens sans scrupules sur l'Internet et utilisé comme un relais pour envoyer des emails en masse et des spams. Ils le feront pour cacher la véritable source du spam et éviter de se faire attraper. Pour tester un relais ouvert, le test suivant devrait être effectué sur votre serveur de messagerie (ou sur le serveur SMTP qui agit comme relais sur le périmètre du réseau de campus). Utilisez **`telnet`** pour ouvrir une connexion au port 25 du serveur en question (avec certaines versions de telnet sur les machines Windows, il peut être nécessaire de typer `set local_echo' avant que le texte ne soit visible):

```
telnet mail.uzz.ac.zz 25
```

Ensuite, si une conversation interface a lieu (par exemple, comme suit), le serveur est un hôte 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 ressembler à ceci:

```
550 Relaying is prohibited.
```

Un testeur en ligne est disponible à des sites tels que *http://spamhaus.org/*. Il y a aussi des informations sur le problème sur ce site. Comme les spammers ont conçus des méthodes automatisées pour trouver ces relais ouverts, il est presque garanti q'une institution qui ne protége pas ses systèmes de messagerie sera découverte et abusée. Configurer un serveur de messagerie pour ne pas être un relais ouvert consiste à préciser les réseaux et les hôtes qui sont autorisés à relayer le courrier à travers eux dans le ***MTA*** (par exemple, Sendmail, Postfix, Exim, ou Exchange). Ce sera probablement la gamme d'adresses IP du réseau de campus.

Partage P2P (peer-to-peer)

L'abus de bande passante par le biais des programmes de partage de fichiers peer-to-peer (P2P) tels que Kazaa, Morpheus, BitTorrent, WinMX et BearShare peut être évité par les moyens suivants:

- **Rendre impossible l'installation de nouveaux programmes sur les ordinateurs du campus.** En ne donnant pas aux utilisateurs réguliers l'accès administrateur sur les postes de travail PC, il est possible de prévenir l'installation de programmes tels que Kazaa. Beaucoup d'institutions également normalisent l'ordinateur de bureau où ils installant le système d'exploitation sur un seul PC. Ensuite, ils installent toutes les applications nécessaires sur ce PC et le configurent de manière optimale. Le PC est également configuré d'une manière qui empêche les utilisateurs d'installer des nouvelles applications. Une image disque de ce PC est alors cloné à tous les autres ordinateurs en utilisant des logiciels comme Partition Image (voir *http://www.partimage.org/*) ou Drive Image Pro (voir *http://www.powerquest.com/*).

  De temps en temps, les utilisateurs peuvent réussir à installer de nouveaux logiciels ou endommager le logiciel sur l'ordinateur (en le faisant souvent bloquer, par exemple). Lorsque cela se produit, un administrateur peut tout simplement restaurer l'image, faisant fonctionner le système d'exploitation et tous les logiciels sur l'ordinateur tel que spécifié initialement.

- **Le blocage de ces protocoles n'est pas une solution.** La raison en est que Kazaa et d'autres protocoles sont assez astucieux pour contourner les ports bloqués. Kazaa par défaut utilise le port 1214 pour la connexion initiale, mais si ce port n'est pas disponible, il va tenter d'utiliser les ports 1000 à 4000. Si ceux-ci sont bloqués, il utilise le port 80. Ceci, en fait, ressemble à du trafic Web. Pour cette raison, les ISPs ne le bloquent pas mais "l'étranglent" en utilisant des outils de gestion de bande passante.

- **Si le taux de limitation n'est pas une option, modifier la disposition du réseau.** Si le serveur proxy et les serveurs de messagerie sont configurés avec deux cartes réseau (tel que décrit dans le **chapitre trois**) et ces serveurs ne sont pas configurés pour transmettre des paquets, ceci bloquerait tout trafic P2P. Cela bloquerait également tous les autres types de trafic, tels que Microsoft NetMeeting, SSH, le logiciel VPN, et tous les autres services qui ne sont pas spécifiquement autorisés par le serveur proxy. Dans les réseaux à faible bande passante, il peut être décidé que la simplicité de ce modèle l'emporte sur les inconvénients. Une telle décision peut être nécessaire, mais ne devrait pas être prise à la légère. Les administrateurs réseau ne peuvent tout simplement pas prévoir combien novateur sera l'usage que les utilisateurs feront d'un réseau. En bloquant préventivement tous les accès, vous pourrez empêcher les utilisateurs de faire usage de tous les services (même les services à faible bande passante) que votre proxy ne permet pas. Bien que ceci puisse être souhaitable dans des circonstances extrêmes de

faible bande passante, ça ne devrait jamais être considéré comme une bonne politique d'accès en général.

Programmes qui s'installent eux-mêmes (à partir de l'Internet)

Ce sont des programmes qui sont destinés à s'installer eux-mêmes automatiquement et ensuite continuer à utiliser la bande passante, par exemple, la soi-disant Bonzi Buddy, le Microsoft Network, et certains types de vers. Certains logiciels sont des logiciels espions, qui continuellement envoient l'information sur les habitudes d'un navigateur à une compagnie quelque part sur l'Internet. La formation de l'utilisateur et le verrouillage des PC pour éviter que les utilisateurs normaux accèdent aux droits d'administration sont, dans une certaine mesure, des mesures préventives contre ces programmes. Dans d'autres cas, il existe des solutions logicielles permettant de trouver et supprimer ces programmes problème, tels que Spychecker (*http://www.spychecker.com/*) ou Ad-Aware (*http://www.lavasoft.de/*).

Des mises à jour du système d'exploitation Windows

La dernière version du système d'exploitation Microsoft Windows assume qu'un ordinateur avec une connexion réseau local (LAN) a une bonne connexion à l'Internet, et télécharge automatiquement les correctifs de sécurité, des bugs et les améliorations de fonctionnalité à partir du site Web de Microsoft. Cela peut consommer d'énormes quantités de bande passante sur un lien Internet coûteux. Les deux approches possibles à ce problème sont les suivantes:

- **Désactiver les mises à jour Windows sur tous les postes de travail PC.** Les mises à jour de sécurité sont très importantes pour les serveurs, mais la nécessité de ces mises a jour pour des postes de travail dans un réseau privé protégé comme un réseau de campus est discutable.
- **Installer un serveur de mise à jour de logiciels.** C'est un logiciel Microsoft gratuit qui vous permet de télécharger toutes les mises à jour de Microsoft pendant la nuit sur un serveur local et de distribuer ces mises à jour à des postes de travail client à partir du serveur local. De cette façon, les mises à jour Windows n'ont pas besoin d'utiliser toute la bande passante sur la connexion Internet au cours de la journée. Malheureusement, tous les ordinateurs client doivent être configurés pour utiliser le logiciel serveur de mise à jour pour que ceci ait un effet. Si vous avez un serveur DNS flexible, vous pouvez également le configurer pour répondre à des demandes de *windowsupdate.microsoft.com* et diriger le logiciel de mise à jour (updater) vers votre serveur de mise à jour. Ceci est une bonne option seulement pour les grands réseaux. Elle peut cependant économiser des énormes quantités de bande passante sur Internet.

Le blocage du site des mises à jour Windows sur le serveur proxy n'est pas une bonne solution parce que le service Windows Update (mises à jour automatiques) continue à réessayer de façon plus agressive, et si tous les postes de travail le font, ceci impose une lourde charge sur le serveur proxy. L'extrait ci-dessous provient d'un journal proxy (journal d'accès Squid), où ceci a été fait par le blocage des fichiers *cabinet* Microsoft (.cab).

Une grande partie du journal Squid se présente comme suit:

```
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
```

Bien que ceci puisse être tolérable pour quelques clients PC, le problème s'accroît significativement avec le nombre d'hôtes qui sont ajoutés au réseau. Plutôt que de forcer le serveur proxy à satisfaire les demandes qui ne échoueront toujours, il est plus logique de réorienter les mises à jour logicielles des clients vers un serveur local de mise à jour.

Programmes qui assument une connexion a grande largeur de bande

En plus des mises à jour Windows, de nombreux autres programmes et services supposent que la bande passante n'est pas un problème, et donc consomment la bande passante pour des raisons que l'utilisateur ne peut pas prévoir. Par exemple, les logiciels anti-virus (tels que Norton AntiVirus) se mettent à jour eux-mêmes automatiquement de façon périodique et directement à partir de l'Internet. Il est préférable que ces mises à jour soient distribuées à partir d'un serveur local.

D'autres programmes, comme le lecteur vidéo RealNetworks, téléchargent automatiquement les mises à jour et publicités, mais aussi envoient des statistiques d'utilisation vers un site Internet. Des applets paraissant inoffensives (comme Konfabulator et le widgets du Dashboard) sondent continuellement les hôtes Internet pour des informations à jour. Celles-ci peuvent impliquer des demandes de bande passante faibles (comme la météo ou des nouvelles), ou des demandes de bande passante très élevées (comme les webcams). Ces applications peuvent avoir besoin d'être étranglées ou bloquées totalement.

Les dernières versions de Windows et Mac OS X ont également un service de synchronisation de temps. Cela permet à l'horloge de l'ordinateur de rester précis en vous connectant à des serveurs de temps sur l'Internet. Il est plus efficace d'installer un serveur de temps local et d'effectuer la distribution de temps précis à partir de là plutôt qu'immobiliser la liaison Internet avec ces demandes.

Trafic Windows sur la liaison Internet

Des ordinateurs Windows communiquent entre eux par le biais de ***NetBIOS*** et ***Server Message Block*** (***SMB***). Ces protocoles sont au au-dessus de la couche TCP/IP ou d'autres protocoles de transport. Ce protocole fonctionne par tenue ***d'élections*** pour déterminer l'ordinateur qui sera le navigateur maître (*master browser*). Le master browser est un ordinateur qui maintient une liste de tous les ordinateurs, les partages et les imprimantes que vous pouvez voir dans le menu Voisinage réseau (*Network Neighborhood*) ou Favoris réseau (*My Network Places*). L'information sur les partages disponibles est également diffusée à intervalles réguliers.

Le protocole SMB est conçu pour les réseaux locaux et cause des problèmes lorsque l'ordinateur Windows est connecté à l'Internet. À moins que le trafic SMB soit filtré, il aura aussi tendance à se propager sur la liaison Internet, gaspillant la bande passante de l'organisation. Les étapes suivantes pourraient être prises pour prévenir ceci:

- **Bloquer le trafic SMB/NetBIOS sortant sur le périmètre du routeur ou firewall. C**e trafic consomme la bande passante Internet, et pire encore, représente un risque potentiel pour la sécurité. Beaucoup de vers Internet et outils de pénétration sondent activement les partages SMB ouverts et exploitent ces connexions pour accéder plus facilement à votre réseau.
- **Installer ZoneAlarm sur tous les postes de travail (pas le serveur).** Une version gratuite peut être trouvé sur le site *http://www.zonelabs.com/*. Ce logiciel permet à l'utilisateur de déterminer les applications qui peuvent établir des connexions à l'Internet et ceux qui ne peuvent pas. Par exemple, Internet Explorer a besoin de se connecter à Internet, mais Windows Explorer n'a pas besoin. ZoneAlarm peut empêcher Windows Explorer de le faire.
- **Réduire les partages réseau. I**déalement, seul le serveur de fichiers devrait avoir des partages. Vous pouvez utiliser un outil tel que le scanneur de réseaux SoftPerfect (disponible sur *http://www.softperfect.com/*) pour identifier facilement tous les partages dans votre réseau.

Les vers et les virus

Les vers et les virus peuvent générer d'énormes quantités de trafic. Le vers W32/Opaserv, par exemple, est toujours en vigueur, même s'il est vieux. Il se propage par le biais des partages Windows et est détecté par d'autres

personnes sur Internet car il tente de se propager davantage. Il est donc essentiel que la protection anti-virus soit installée sur tous les PC. En outre, la formation des utilisateurs sur l'exécution de pièces jointes et la réplique aux courriers électroniques non sollicités est essentielle. En fait, la politique serait qu'aucun poste de travail ou serveur n'exécute les services non utilisés. Un PC ne devrait pas avoir des partages sauf s'il s'agit d'un serveur de fichiers et un serveur ne devrait pas exécuter de services inutiles non plus. Par exemple, typiquement les serveurs Windows et Unix exécutent par défaut un serveur des services Web. Ces services devraient être désactivés si ce serveur a une fonction différente. Le moins de services un ordinateur exécute, moins il y a à exploiter.

Boucles de transfert des e-mails

Occasionnellement, un seul utilisateur faisant une erreur peut causer un problème. Par exemple, un utilisateur dont le compte de l'université est configuré pour expédier tout le courrier à son compte Yahoo. L'utilisateur va en vacances. Tous les e-mails envoyés à celui-ci pendant son absence sont encore transmis à son compte Yahoo qui peut atteindre 2 Mo seulement. Lorsque le compte Yahoo est plein, il commence à renvoyer les e-mails au compte de l'université, qui le transmet immédiatement au compte Yahoo. Une boucle de messagerie qui enverrait et retournerait des centaines de milliers d'e-mails entre le compte de l'université et le compte Yahoo se forme créant une génération massive de trafic et écroulant les serveurs de messagerie.

Il y a des fonctionnalités du programme serveur de messagerie qui peuvent reconnaître des boucles. Celles-ci devraient être activées par défaut. Les administrateurs doivent également prendre soin de ne pas désactiver cette fonctionnalité par erreur ou installer un agent de transfert SMTP qui modifie les en-têtes de courrier de manière à ce que le serveur de messagerie ne reconnaît pas la boucle de messagerie.

Gros téléchargements

Un utilisateur peut démarrer plusieurs téléchargements simultanés, ou télécharger de gros fichiers tels que des images ISO de 650MB. De cette façon, un seul utilisateur peut utiliser la plus grande partie de la bande passante. Les solutions à ce genre de problème résident dans la formation, le téléchargement hors ligne, et la surveillance (y compris la surveillance en temps réel, comme indiqué dans le **chapitre six**). Le téléchargement hors ligne peut être mis en oeuvre au moins de deux façons:

- À l'Université de Moratuwa, un système a été implémenté en utilisant la redirection d'url. Les utilisateurs accédant à une url **ftp://** arrivent sur un répertoire dans lequel chaque fichier dispose de deux liens: l'un pour le téléchargement normal, et l'autre pour le téléchargement hors ligne. Si la connexion hors ligne est sélectionnée, le fichier spécifié est main tenu dans la file d'attente pour un téléchargement ultérieur et l'utilisateur est notifié par e-mail lorsque le téléchargement est terminé. Le système assure une cache des fichiers récemment téléchargés et les récupère

immédiatement lors d'une nouvelle demande. La file d'attente de téléchargement est triée par taille. Par conséquent, les petits fichiers sont téléchargés en premier. Comme une certaine bande passante est allouée à ce système même pendant les heures de pointe, les utilisateurs demandant des petits fichiers peuvent les recevoir en quelques minutes, parfois même plus rapidement qu'un téléchargement en ligne.

- Une autre approche serait de créer une interface Web où les utilisateurs entrent l'url du fichier qu'ils veulent télécharger. Celui-ci est alors téléchargé pendant la nuit en utilisant une tâche cron (***cron job***) ou une tâche planifiée. Ce système ne fonctionne que pour les utilisateurs qui ne sont pas impatients et connaissent quelles tailles de fichier seraient problématiques pour le téléchargement au cours de la journée de travail.

Envoi de gros fichiers

Lorsque les utilisateurs ont besoin de transférer de gros fichiers aux collaborateurs qui sont ailleurs sur Internet, ils doivent être formé sur comment planifier le transfert. Dans Windows, un transfert sur un serveur FTP distant peut être fait en utilisant un fichier script FTP, qui est un fichier texte contenant des commandes FTP, semblables au suivant (enregistré sous **`c:\ftpscript.txt`**) :

```
open ftp.ed.ac.uk
gventer
mysecretword
delete data.zip
binary
put data.zip
quit
```

Pour l'exécuter, tapez ceci à partir de l'invite de commande:

```
ftp -s:c:\ftpscript.txt
```

Sur les ordinateurs Windows NT, 2000 et XP, la commande peut être sauvegardée dans un fichier tel que **`transfer.cmd`**, et planifiée pour exécution pendant la nuit en utilisant les tâches planifiées (Démarrer ➔ Paramètres ➔ Panneau de contrôles ➔ Tâches planifiées). En Unix, le même résultat peut être obtenu en utilisant **`at`** ou **`cron`**.

Les utilisateurs s'envoyant des fichiers

Les utilisateurs ont souvent besoin de s'envoyer des grands fichiers. Envoyer ces fichiers par Internet si le destinataire est local est un gaspillage de bande passante. Un partage de fichier devrait être crée sur le serveur local Windows/Samba/Web Novell, où un utilisateur peut rendre un gros fichier accessible aux autres.

Alternativement, une interface Web peut être écrite pour permettre à un serveur web local d'accepter un grand fichier et le placer dans une zone de téléchargement. Après son transfert sur le serveur Web, l'utilisateur reçoit un URL pour le fichier. Il peut alors donner cette URL à ses collaborateurs locaux et internationaux qui peuvent le télécharger lorsqu'ils accèdent à cette URL. C'est

ce que l'Université de Bristol a fait avec son système FLUFF. L'Université offre une installation pour le téléchargement de gros fichiers (FLUFF, facility for the upload of large files), disponible à partir de *http://www.bristol.ac.uk/fluff/*. Ces fichiers peuvent ensuite être accessibles à toute personne qui a reçu leur emplacement. L'avantage de cette approche est que les utilisateurs peuvent donner aux utilisateurs externes l'accès à leurs fichiers alors que la méthode de partage de fichiers ne peut fonctionner que pour les utilisateurs qui sont dans le réseau de campus. Un tel système peut facilement être mis en œuvre comme un script CGI utilisant Python et Apache.

10
Viabilité économique

La réalisation de la viabilité à long terme est peut-être l'objectif le plus difficile lors de la conception et l'exploitation des réseaux sans fil et de télécentres dans les pays en développement. Le coût prohibitif de la connectivité Internet dans de nombreux pays en développement impose une dépense d'exploitation qui rend ces modèles sensibles à la conjoncture économique et nécessite l'innovation pour atteindre la viabilité. Des progrès substantiels dans l'usage des réseaux sans fil pour les communications rurales ont été accomplis au cours des dernières années, dus en grande partie à des percées technologiques. Des liaisons à longue distance ont été construites, des modèles à bande passante élevée sont possibles et les moyens fiables d'accéder aux réseaux sont disponibles. En revanche, il y a eu moins de succès avec le développement de modèles d'affaires durables pour les réseaux sans fil et télécentres, en particulier pour les régions éloignées. Sur la base des expériences des auteurs et leurs observations des réseaux existants, ainsi que sur la connaissance des meilleures pratiques d'esprit d'entreprise, ce chapitre mettra l'accent sur la documentation des méthodes de construction durables pour les réseaux sans fil et les télécentres.

Au cours de la dernière décennie, il y a eu une croissance dans l'accès à l'Internet dans le monde en développement. La plupart des villes du monde en développement ont désormais des réseaux sans fil ou ADSL et des connexions a fibre optique à l'Internet. Ceci est une amélioration substantielle. Néanmoins, en dehors des zones urbaines, l'accès à l'Internet est encore un formidable défi. Il y a peu d'infrastructure câblée au-delà des villes principales. Par conséquent, le réseau sans fil demeure l'un des rares choix abordable pour la fourniture d'accès à Internet. Il existe maintenant des modèles éprouves d'accès rural au moyen des réseaux sans fil. En Macédoine, le projet Macedonia Connects a maintenant connecté la majorité des écoles du pays à l'Internet. Ce livre a été écrit pour ceux qui veulent connecter leurs communautés. Les modèles décrits ici sont plus petits en dimension et utilisent des concepts abordables. Notre objectif est de fournir des exemples sur la façon dont les réseaux sans fil peuvent être conçus pour permettre un accès durable là où les grands opérateurs de télécommunications n'ont pas encore installé leurs réseaux dans des régions ou

il ne serait pas économiquement possible de le faire par des modèles traditionnels.

Deux idées fausses doivent être dissipées. Tout d'abord, beaucoup de gens supposent qu'il existe un modèle d'affaires idéal, qui fonctionnera dans chaque communauté du monde en développement, et que la clé du succès est de trouver cette solution “Eurék”. Dans la pratique, ce n'est pas le cas. Chaque communauté, ville ou village est différent. Il n'existe pas de modèle qui répond aux besoins de toutes les régions du monde en développement. Malgré le fait que certains endroits peuvent être similaires en termes économiques, les caractéristiques d'un modèle d’affaires durable varient d'une communauté à l’autre. Même si un modèle peut marcher dans un village, un autre village voisin peut ne pas posséder les mêmes qualités nécessaires pour faire que ce modèle soit viable. Dans ce cas, d'autres modèles novateurs doivent être appliqués au contexte de cette communauté particulière.

Une autre fausse idée est que la viabilité a la même définition pour tous les peuples. Bien que ce terme signifie généralement que le système est construit à persister indéfiniment, ce chapitre met davantage l'accent sur les conditions économiques (et de la gestion financière) que sur les autres aspects de la viabilité. Aussi, au lieu d’utiliser un horizon indéterminé, notre modèle porte sur une période de cinq ans- la période pendant laquelle les infrastructures TIC et les technologies sans fil devraient être utiles. Ainsi, le terme viabilité sera utilisé pour encapsuler un système conçu pour persister pendant environ cinq ans ou plus.

Lors de la détermination et la mise en oeuvre du meilleur modèle pour un réseau sans fil ou télécentre, plusieurs facteurs contribuent à assurer son succès. Ce chapitre ne se veut pas un guide pour la gestion durable des réseaux sans fil. Au contraire, ce guide du “Comment faire” vise à présenter une approche qui vous permettra de trouver le modèle qui convient le mieux pour votre situation. Les outils et les informations contenus dans ce chapitre vont aider les gens qui veulent démarrer des réseaux sans fil dans le monde en développement à se poser les bonnes questions et recueillir les données nécessaires pour définir les composant les plus appropriées pour leur modèle. Gardez à l'esprit que la détermination du meilleur modèle n'est pas un processus séquentiel où chaque étape est suivie jusqu'à la fin. En fait, le processus est continu et itératif. Toutes les étapes sont intimement liées les unes aux autres, et souvent vous allez revoir les étapes plusieurs fois au cours de votre progrès.

Créer un énoncé de mission

Que voulez-vous accomplir par la mise en place de votre réseau? Ceci semble une question simple. Toutefois, de nombreux réseaux sans fil sont installés sans une vision claire de ce qu'ils font et ce qu'ils espèrent réaliser dans le futur. La première étape consiste à documenter cette vision avec la contribution de votre personnel ou équipe. Quel est le but du réseau sans fil? Qui le réseau va-t-il servir? Qu'est-ce que le réseau fait pour faire face aux besoins de la communauté et créer de la valeur? Quels sont les principes qui guident le réseau? Un bon énoncé de la mission exprime le but de votre réseau sous une forme concise, de manière

significative tout en s'articulant sur vos valeurs et services. Par-dessus tout, votre mission fournit une vision des aspirations de votre réseau sans fil.

Il est important que chaque membre de l'équipe de travail pour construire le réseau sans fil soit associé au processus de développement de votre mission, ce qui contribuera à créer un intérêt ultérieur. Cela ralliera le soutien et l'engagement non seulement de votre personnel, mais également des clients, des partenaires et des bailleurs de fonds, faisant avancer votre objectif général. Dans le monde dynamique de la technologie, les besoins des clients et le meilleur moyen de satisfaire ces besoins changent rapidement. Par conséquent, l'élaboration de votre mission est un processus continu. Après avoir défini la mission initiale avec votre équipe, vous devez effectuer des recherches pour déterminer si cette première conception s'aligne avec les réalités de votre environnement. Sur la base d'une analyse de l'environnement externe et de vos compétences internes, vous devez constamment modifier la mission tout au long du cycle de vie du réseau sans fil.

Évaluer la demande pour les offres potentielles

La prochaine étape dans l'avancement de votre modèle d'affaires consiste à évaluer la demande de la communauté pour les produits et services réseaux. Tout d'abord, identifiez les personnes, groupes et organismes dans la communauté qui ont un besoin d'information et pourraient bénéficier des offres du réseau sans fil. Les utilisateurs potentiels consisteraient en un large éventail de personnes et d'organismes qui incluent, mais ne sont pas limitées à:

- Les associations d'agriculteurs et coopératives.
- Les groupes des femmes.
- Les écoles et les universités.
- Les entreprises et les entrepreneurs locaux.
- Les cliniques de soins de santé et les hôpitaux.
- Les groupes religieux.
- Les organisations internationales et locales non gouvernementales (ONGs).
- Les agences locales et gouvernementales nationales.
- Les stations de radio.
- Les organisations dans l'industrie du tourisme.

Une fois que vous avez établi une liste de tous les groupes d'utilisateurs potentiels du réseau, vous devez déterminer leurs besoins en matière d'accès à l'information et de communication. Souvent, les gens confondent les services avec les besoins. Un agriculteur peut avoir besoin de recueillir des informations sur les prix du marché et des conditions climatiques pour améliorer son

rendement des cultures et des ventes. Peut-être la manière dont il reçoit cette information est par le biais d'Internet, mais l'agriculteur peut également recevoir ces informations par SMS sur un téléphone mobile ou par l'intermédiaire de la voix sur le protocole Internet (***VoIP***, ***Voice over Internet Protocol***). Il est important de faire la différence entre les besoins et les services parce qu'il peut y avoir diverses façons de satisfaire le besoin de l'agriculteur. Votre réseau sans fil devrait examiner la meilleure façon de satisfaire les besoins de l'agriculteur, et ainsi créer de la valeur au coût le plus bas pour l'utilisateur.

Lors de l'évaluation des besoins de la communauté, il est important de trouver comment le réseau peut créer le plus de valeur à ses utilisateurs. Par exemple, dans la petite ville de Douentza au Mali, un gestionnaire de télécentre avait évalué les bénéfices potentiels de création d'un réseau sans fil par le biais de discussions avec plusieurs organismes locaux. Il s'était entretenu avec une ONG locale qui avait besoin d'envoyer des rapports mensuels à son siège à Bamako. À ce moment-là, il n'y avait pas d'accès à l'Internet dans Douentza. Pour envoyer un e-mail de la copie du rapport, l'ONG envoyait un de ses employés à Mopti, une fois par mois. Ce qui se traduisait dans des frais de transport et hébergement, ainsi que le manque à gagner d'avoir l'employé en dehors du lieu du travail pendant plusieurs jours chaque mois. Lorsque le gestionnaire de télécentre calcula les dépenses totales mensuelles engagées par l'ONG, il était en mesure de démontrer la valeur d'une connexion Internet par le biais des économies de coûts à l'organisme.

L'assistance de la part des principaux partenaires peut également être nécessaire pour garantir la viabilité de votre réseau sans fil. Au cours de cette phase, vous devez contacter des partenaires potentiels et explorer les collaborations mutuellement bénéfiques.

Vous pouvez évaluer la demande dans votre collectivité en communiquant avec vos clients potentiels et poser des questions directement par le biais de sondages, de groupes de discussion, des entrevues ou des assemblées. Mener des recherches par le biais d'un examen de la documentation statistique, des rapports d'industrie, les recensements, les magazines, journaux et autres sources de données secondaires aidera également à vous donner une meilleure image de votre environnement local. Le but de cette collecte de données est d'obtenir une parfaite compréhension de la demande de l'information et des communications dans votre communauté afin que le réseau en cours de création réponde à ces besoins. Souvent, les réseaux sans fil qui ne réussissent pas dans le monde en développement oublient cette étape clé. L'ensemble de votre réseau devrait être fondé sur la demande dans la communauté. Si vous avez mis en place un réseau sans fil dans lequel la communauté ne trouve pas de valeur ou dont elle ne peut pas se permettre les services, il finira par échouer.

Mettre en place des incitations appropriées

Souvent, il y a peu d'incitation économique à accéder à l'Internet pour des participants dont l'économie est basée sur la subsistance. En plus, le coût d'acquisition d'un ordinateur, l'apprentissage pour l'utiliser, et l'obtention d'une

connexion Internet l'emportent de loin sur les retombées économiques qu'elle peut apporter. Il y a eu récemment quelques développements d'applications qui font face à ce manque d'incitation, tels que les systèmes d'informations boursières, les normes de qualité imposées par les pays importateurs, et des échanges de marchandises. L'accès à l'Internet devient un avantage évident dans les situations où la connaissance des prix des produits au jour le jour peut faire une différence signifiante dans le revenu.

La mise en place des incitations économiques est primordiale pour le succès du réseau. Le réseau doit fournir une valeur économique à ses utilisateurs d'une manière qui l'emporte sur son coût, ou il doit être assez bon marché pour que ses coûts soient marginaux et abordables pour ses utilisateurs. Il est crucial de concevoir un réseau avec des utilisations économiques viables et des coûts qui sont inférieurs à la valeur économique qu'il fournit. En outre, pour créer une structure d'incitation, il faut impliquer la communauté dans la création du réseau dès le début du projet, en veillant à ce que cette initiative soit organique et non pas imposée de l'extérieur. Pour commencer, vous devez essayer de répondre aux questions suivantes:

1. Quelle valeur économique ce réseau peut générer pour l'économie locale et pour qui?
2. Combien de valeur économique perceptible peut être générée?
3. Est que les obstacles présents peuvent être surmontés pour permettre la réalisation de ces retombées économiques?

En répondant à ces questions, le réseau sera en mesure d'exprimer clairement sa proposition de valeur pour ses utilisateurs. Par exemple, "En utilisant ce réseau, vous pouvez améliorer vos marges sur les ventes de 2%," ou "l'Internet vous permettra de sauver X $ en frais de téléphone et de transport par mois." Vous devez envisager comment votre réseau peut améliorer les performances, réduire les coûts, ou accroître les recettes pour ces clients.

Par exemple, s'il doit fournir les cours du marché pour l'industrie locale de maïs, le réseau devrait être situé à proximité de l'endroit où les agriculteurs apportent leur récolte pour vendre aux commerçants. Votre réseau devrait alors probablement se rattacher sur les cours du marché, fournissant chaque jour des feuilles de prix (1$ chacun), ou les terminaux pour les vendeurs et les commerçants (2$/hr). Votre réseau peut également fournir les moyens pour les agriculteurs pour en savoir plus sur les nouvelles techniques et acheter des nouveaux produits. Vous pouvez également fournir des connexions sans fil aux commerçants et leur louer des terminaux de type clients légers pour l'accès à l'Internet. Si le marché est petit, vous pourriez être en mesure de réduire les coûts en limitant l'accès aux images et aux autres services à grande consommation de bande passante. Encore une fois, savoir combien de valeur votre réseau créera pour ces marchands vous permettra d'évaluer combien ils seront en mesure de payer pour vos services.

Renseignez-vous sur la réglementation des réseaux sans fil

La réglementation sur les réseaux sans fil a également des répercussions sur le type de modèle d'affaires qui peut être mis en œuvre. Tout d'abord, cherchez à savoir si une organisation a le droit d'utiliser des fréquences de 2,4 GHz sans permis. Dans la plupart des pays du monde, la fréquence 2,4 GHz est librement utilisable, cependant certains pays restreignent l'exploitation d'un réseau ou exigent des permis coûteux pour le faire. Bien que les réseaux sans fil soient légaux en Ukraine, le gouvernement exige une licence coûteuse pour utiliser des fréquences de 2,4 GHz. Ce qui rend cet usage partagé prohibitif. Dans les faits, seuls des Fournisseurs d'Accès à Internet bien établis ont les moyens de payer les frais de licence dans ce pays. Cette restriction rend difficile pour une petite communauté de partager un réseau sans fil avec d'autres parties ou organismes potentiellement intéressés. D'autres pays, tels que la République du Mali sont plus permissifs. Comme il n'y a pas de telles restrictions sur les réseaux sans fil, la possibilité de partager la connectivité Internet dans les petites communautés est une solution viable. La leçon est de faire des recherches au début en veillant à ce que votre réseau se conforme à la législation du pays et la communauté locale. Certains gestionnaires des projets ont été forcés de fermer leurs réseaux sans fil tout simplement parce qu'ils étaient en train d'enfreindre la loi involontairement.

Vous devez également vérifier la légalité des services voix sur le protocole Internet (VoIP). La plupart des pays dans le monde en développement n'ont pas encore défini si VoIP est autorisé. Dans ces pays, rien ne vous empêche d'offrir le service VoIP. Toutefois, dans certains pays, il existe des règles complexes entourant la VoIP. En Syrie, la VoIP est interdite pour tous les réseaux, non pas seulement les réseaux sans fil. En Ukraine, la VoIP est légale pour les appels internationaux uniquement.

Analysez la concurrence

La prochaine phase de l'évaluation de votre communauté implique une analyse de la concurrence dans les réseaux sans fil. Les concurrents incluent les organismes qui offrent des produits et services similaires (par exemple, un autre fournisseur de services Internet sans fil), des organismes considérés comme des substituts ou des alternatives aux produits et services de votre réseau (par exemple, un cybercafé), et les organismes définis comme nouveaux entrants dans le marché des télécommunications sans fil. Une fois que vous avez identifié vos concurrents, vous devriez les étudier en détails. Vous pouvez obtenir des informations sur vos concurrents par le biais d'Internet, appels téléphoniques, leurs publicités et des documents de marketing, des études de leurs clients et des visites sur leur site. Créez un fichier pour chaque concurrent. L'information de concurrence recueillie peut inclure une liste des services (y compris les prix et la qualité de l'information), leur clientèle cible, les techniques de service à la clientèle, la réputation, le marketing, etc. Assurez-vous de recueillir tout ce qui

vous aidera à déterminer comment positionner votre réseau dans la communauté.

Il est important d'évaluer votre concurrence pour de nombreuses raisons. Tout d'abord, ça vous aide à déterminer le niveau de saturation du marché. Il y a eu plusieurs cas où un télécentre subventionné a été établi par un organisme donateur dans un petit village avec demande limitée, malgré le fait qu'il existait déjà localement un cybercafé local dans le coin. Dans un cas, le centre subventionné pouvait maintenir des prix bas car il n'avait pas à couvrir ses coûts. Ceci amena le cybercafé local à fermer faute de clients. Après l'arrêt du financement, le centre subventionné dût aussi fermer en raison de la faiblesse des revenus et des coûts élevés. Connaître ce qui existe déjà va vous permettre de déterminer comment votre réseau peut contribuer à la valeur de la communauté. En outre, l'analyse de la concurrence peut stimuler des idées novatrices pour votre offre de services. Existe-t-il quelque chose que vous pouvez faire mieux que les concurrents pour rendre vos services plus adaptés aux besoins de la communauté? Enfin, en analysant vos concurrents du point de vue clientèle et en comprenant leurs forces et leurs faiblesses, vous pouvez déterminer vos avantages concurrentiels au sein de la communauté. Les avantages concurrentiels sont ceux qui ne peuvent pas être facilement reproduits par la concurrence. Par exemple, un réseau sans fil qui peut exclusivement offrir une connexion Internet plus rapide qu'un concurrent est un avantage compétitif qui facilite l'utilisation par le client.

Déterminer les coûts initiaux et récurrents, la tarification

Lorsque vous prévoyez de construire et d'exploiter votre réseau sans fil, vous devez déterminer les ressources nécessaires pour démarrer votre projet et les coûts d'exploitation récurrents. Les coûts initiaux comprennent tout ce que vous devez acheter pour commencer votre réseau sans fil. Ces frais peuvent aller de l'investissement initial fait dans le matériel, les installations et l'équipement pour les points d'accès, les hubs, les commutateurs, les câbles, l'UPS, etc. aux frais d'enregistrement de votre organisme en tant qu'une entité légale. Les coûts récurrents sont ce que vous devez payer pour continuer à opérer votre réseau sans fil, y compris le coût d'accès à l'Internet, téléphone, les prêts, l'électricité, les salaires, les frais de location des bureaux, les frais d'entretien et de réparation de l'équipement, ainsi que les investissements destinés à remplacer les dysfonctionnements ou des équipements obsolètes.

Chaque pièce d'équipement finira par tomber en panne ou devenir obsolète à un moment donné, et vous devriez mettre de côté des fonds supplémentaires à cette fin.

Une méthode recommandée et courante pour faire face à ceci consiste a prendre le prix de l'appareil et de le diviser par le temps que vous estimez qu'il va durer. Ce processus est appelé ***amortissement***. Voici un exemple. Un ordinateur moyen est censé durer de deux à cinq ans. Si le coût initial d'achat de l'ordinateur était de 1000$ USD et si vous serez en mesure d'utiliser l'ordinateur pour cinq ans, votre amortissement annuel sera de 200$ USD. En d'autres

termes, pour pouvoir remplacer cet ordinateur vous allez perdre éventuellement 16,67$ USD chaque mois. Afin de rendre votre projet durable, il est d'une importance fondamentale que vous économisez de l'argent pour compenser la dépréciation du matériel de chaque mois. Conservez ces économies jusqu'à ce que vous ayez finalement a les dépenser pour le remplacement de l'équipement. Certains pays ont des lois fiscales qui déterminent la durée de l'amortissement pour les différents types de dispositifs. Dans tous les cas, vous devriez essayer d'être très réaliste sur le cycle de vie de tous les appareils mis en place et prévoir soigneusement leur amortissement.

Essayez d'évaluer tous vos frais à l'avance et faites des estimations réalistes de vos dépenses. La grille suivante (à la page suivante) montre un moyen pour classifier et faire une liste de tous vos coûts. C'est un bon outil pour structurer des coûts différents, et il va vous aider à distinguer entre les coûts initiaux et récurrents.

Il est important d'étudier tous vos frais de démarrage à l'avance et faire des estimations réalistes sur vos frais récurrents. Il est toujours préférable de budgétiser pour plus que de budgétiser pour moins des dépenses. Avec chaque projet sans fil, il y a toujours des frais imprévus, en particulier au cours de la première année de fonctionnement quand vous apprenez à mieux gérer votre réseau.

Catégories de coûts

Pour améliorer vos chances de viabilité, il est généralement préférable de maintenir la structure de coûts au plus bas pour votre réseau. En d'autres termes, garder vos dépenses aussi basses que possible. Prenez le temps de faire une étude approfondie sur l'ensemble de vos fournisseurs, en particulier les fournisseurs de services Internet, et faire le tour du marché pour les meilleures affaires en termes de qualité de service. Une fois de plus, soyez certains que ce que vous achetez auprès de fournisseurs correspond à la demande dans la communauté. Avant l'installation d'un VSAT coûteux, assurez vous qu'il y a un nombre suffisant de personnes et d'organismes dans votre communauté qui ont la volonté et la capacité de payer pour l'utiliser. En fonction de la demande pour l'accès à l'information et la capacité de payer, une méthode alternative de la connectivité peut être plus approprié. N'ayez pas peur de sortir des sentiers battus et faire preuve de créativité lorsqu'il s'agit de déterminer la meilleure solution.

Tenir vos coûts bas ne devrait pas être au détriment de la qualité. Comme le matériel de basse qualité est plus susceptible de dysfonctionnement, vous pourriez être en train de dépenser plus sur l'entretien à long terme. L'argent que vous êtes prêt à dépenser pour maintenir votre infrastructure de TIC est difficile à deviner. Plus votre infrastructure devient grande et compliquée, plus de ressources financières et de main-d'œuvre vous devez allouer à son entretien.

	Coûts Initiaux/de démarrage	Coûts récurrents
Coûts de travail	• Check up (analyses) et consultations • Coûts de développement pour programmes, tests, intégration, etc. • Coûts d'installation • Coûts de recrutement • Coûts de formation (introduction)	• Les frais de manutention/ salaires pour employés ou indépendants, y compris vous-même • Maintenance du matériel et coûts de support logiciel, hardware et équipement auxiliaire • Sécurité du personnel • Coûts de formation (perfectionnement)

	Coûts Initiaux/de démarrage	Coûts récurrents
Coûts du matériel	• Coûts d'acquisition et production (pour le matériel tel que PCs, VSAT, liaison radio matériel et logiciel) • Equipement auxiliaire (par exemple, les commutateurs, les câbles et le câblage, la génératrice, UPS, etc.) • Sécurité et protection des données • Mobilier (chaises, tables, éclairage, rideaux, carrelage et moquette) • Coûts des locaux (neufs, modification, de la climatisation, et des boîtes câblage électrique, grilles de sécurité) • Coûts légaux, tels que l'enregistrement de l'entreprise • Les premiers coûts de licence (VSAT) • Les coûts initiaux de mise sur le marché (autocollants, des affiches, vernissage d'ouverture)	• Coûts d'exploitation pour hardware et systèmes d'exploitation (accès Internet, téléphone, etc.) • Loyer ou taux de crédit • Amortissement du hardware et équipements • Frais de licence • Consommables et fournitures de bureau (par exemple, les supports de données, du papier, agrafes, trombone) • Les dépenses opérationnelles pour maintenir la protection et la sécurité des données • Les primes d'assurance • Les coûts de l'énergie et assurer l'alimentation • Les paiements de prêts, coûts du capital pour rembourser vos frais d'installation • Les coûts de publicité • Taxes locales • Services juridiques et de comptabilité.

Souvent, cette relation n'est pas linéaire mais exponentielle. Si vous avez un problème de qualité avec votre équipement une fois qu'il est mis en œuvre, cela peut vous coûter un énorme montant d'argent pour le réparer. Parallèlement, les ventes vont diminuer parce que l'équipement ne fonctionne pas. Il y a un exemple intéressant d'un important fournisseur d'accès à Internet sans fil (WISP, Wireless Internet Service Provider) qui avait plus de 3000 points d'accès en fonctionnement pendant un certain temps. Toutefois, le WISP n'avait jamais réussi à rentrer dans ses frais car il devait dépenser trop d'argent pour maintenir tous les points d'accès. En outre, la société avait sous-estimé le court cycle de vie de ces dispositifs. Le matériel TIC s'améliore et coûte moins avec le temps. Dès que la société avait investi du temps et de l'argent pour installer des coûteux points d'accès de première génération, le nouveau standard "g" apparut. Des nouveaux concurrents conçurent des meilleurs points d'accès et à moindre coût et offrirent un accès à l'Internet plus rapide pour moins d'argent. Finalement, le premier WISP avait été forcé de fermer l'entreprise, même s'il était initialement le leader du marché. Regardez le tableau ci-dessous pour obtenir une meilleure idée sur le développement rapide de normes et de l'équipement sans fil :

Protocole	Date de sortie	transfert de données standard
802.11	1997	< 1 Mbps
802.11b	1999	5 Mbps
802.11g	2003	20 Mbps
802.11a	1999, mais rares jusqu'à 2005	23 Mbps
802.11y	Juin 2008 (estimé)	23 Mbps
802.11n	Juin 2009 (estimé)	75 Mbps

Gardez à l'esprit les progrès rapides et des changements dans la technologie et réfléchissez sur comment et quand il serait temps pour vous de réinvestir dans des dispositifs nouveaux et moins chers (ou mieux) pour maintenir votre infrastructure compétitive et à jour. Comme mentionné précédemment, il est très important que vous économisiez suffisamment pour être en mesure de le faire quand c'est nécessaire.

Une fois que vous avez identifie et élaboré vos coûts, vous devriez aussi déterminer quoi et comment faire payer pour vos services. Cela est une procédure compliquée et de longue haleine à faire correctement. Ces points clés aideront lors de la prise de décisions sur les prix:

- Calculer le prix à appliquer pour couvrir tous vos coûts quand vous fournissez le service, y compris tous les frais récurrents.
- Examiner les prix de vos concurrents.
- Évaluer ce que vos clients sont prêts et sont capables de payer pour vos services, et assurez-vous que vos prix correspondent à ceci.

Il est absolument essentiel d'établir un plan financier avant de commencer. Vous avez besoin d'une liste de toutes vos dépenses initiales et récurrentes et de faire quelques calculs pour trouver si votre projet peut être viable.

Assurer le financement

Une fois que vous avez déterminé vos dépenses initiales et récurrentes et fait votre plan financier, vous savez de combien vous avez besoin pour opérer un réseau sans fil avec succès. La prochaine étape consiste à trouver et garantir le montant d'argent approprié pour démarrer et exploiter votre réseau sans fil.

La méthode la plus traditionnelle pour acquérir un financement pour les réseaux sans fil dans le monde en développement consiste en des subventions accordées par les bailleurs de fonds. Un donateur est un organisme qui met un financement et d'autres types de dons à la disposition d'un organisme ou un consortium d'organismes pour les aider à gérer des projets ou soutenir des causes. Parce que ce financement est accordé sous forme de subventions ou d'autres dons, il n'est pas supposé être remboursé par les organismes qui mettent en œuvre les projets sans fil ou par les bénéficiaires de ces projets. Ces donateurs comprennent de grands organismes internationaux comme les Nations Unies (UN, United Nations) et diverses institutions spécialisées des Nations Unies comme les Nations Unies pour le développement (PNUD) et l'organisation des Nations Unies pour l'éducation, la Science et la Culture (UNESCO, United Nations Educational, Scientific and Cultural Organization). Les agences gouvernementales qui se spécialisent dans le développement international, comme l'agence des États-Unis pour le développement international (USAID, United States Agency for International Development), le département du Royaume-Uni pour le développement International (DFID, United Kingdom's Department for International Development) et l'Agence canadienne de développement international (CIDA, Canadian International Development Agency), sont également considérés comme des donateurs. Les grandes fondations comme la Fondation Gates et la Fondation Soros Network ainsi que les entreprises privées constituent un autre type de bailleurs de fonds.

En règle générale, l'allocation des fonds implique une procédure concurrentielle ou non concurrentielle. Comme la procédure non concurrentielle est plus rare, ce chapitre mettra l'accent sur le processus concurrentiel à un niveau très élevé. La plupart des donateurs ont des procédures complexes entourant la répartition des fonds. Les auteurs de ce livre ne sont en aucun cas en train d'essayer de simplifier ce système approfondi des règles et des règlements. Les auteurs ont seulement l'intention de transmettre une compréhension générale de ce processus pour les communautés qui tentent d'établir des réseaux sans fil dans le monde en développement. Au cours de l'appel d'offres, le donateur crée une ***demande de proposition*** (***RFP***, *Request for proposal*) ou une ***demande de candidature*** (***RFA***, *Request for application*) qui sollicite des divers organismes non gouvernementaux, entreprises privées et leurs partenaires, des soumissions des propositions décrivant leurs plans pour des projets dans les limites des objectifs et les lignes directrices définis par le donateur. En réponse à cette demande de propositions ou de candidature, les

ONGs et autres organismes concourront pour les fonds par le biais de la présentation de leurs propositions. Ces propositions sont ensuite évaluées par les donateurs sur base des critères spécifiques établis. Enfin, l'organisme donateur sélectionne la proposition la plus appropriée et la meilleure pour financer le projet. Parfois, les donateurs fournissent également des fonds pour soutenir les actions d'un organisme, mais ce type de financement est plus rare que le processus de soumission concurrentiel.

Une autre façon d'avoir accès à des fonds nécessaires pour démarrer et maintenir un réseau sans fil est par ***microfinance***, ou l'octroi de prêts, d'épargne et autres services financiers de base aux plus pauvres du monde. Initié dans les années 1970 par des organismes comme ACCION International et la Banque Grameen, le microcrédit, un type de microfinance, permet aux personnes pauvres et aux entrepreneurs de recevoir des prêts de petits montants d'argent pour démarrer des petites entreprises. Malgré le fait que ces individus n'ont pas beaucoup de qualifications traditionnelles nécessaires pour obtenir des prêts comme un crédit vérifiable, des garanties ou un emploi stable, les programmes de microcrédit ont connu un grand succès dans de nombreux pays en développement. En règle générale, le processus implique un individu ou un groupe qui remplit et soumet une demande de prêt, dans l'espoir de recevoir un prêt, et le prêteur, la personne ou l'organisme qui fournit le prêt, donne de l'argent à la condition qu'il soit retourné avec intérêt.

Le recours au microcrédit pour financer les réseaux sans fil pose une contrainte. Généralement, le microcrédit implique de très petites sommes d'argent. Malheureusement, comme un grand capital est nécessaire pour l'achat du premier équipement de réseau sans fil à mettre en place, parfois un microcrédit n'est pas suffisant. Toutefois, il y a eu de nombreuses autres applications de microcrédit couronnées de succès qui ont introduit la technologie et sa valeur dans le monde en développement. L'histoire des opérateurs de téléphonie rurale en est un exemple. Ces entrepreneurs utilisent leurs micro-prêts pour acheter des téléphones mobiles et des crédits de téléphone. Ensuite, ils font louer l'usage de leurs téléphones mobiles aux membres de la communauté par appel et gagnent suffisamment d'argent pour rembourser leur dette et faire un profit pour eux-mêmes et leurs familles.

Un autre mécanisme pour trouver du financement pour démarrer un réseau sans fil est ***les business Angels***. Les investisseurs dans ce mécanisme sont généralement des personnes fortunées qui fournissent des capitaux pour le démarrage d'entreprises en échange d'un taux élevé de retour sur louent investissement. Parce que les entreprises dans lesquelles ils investissent sont des starts-up et, par conséquent, sont souvent à haut risque, les investisseurs ont tendance à exiger beaucoup plus que leur investissement. Beaucoup s'attendent à une position au conseil d'administration et peut-être un rôle dans l'organisme.

Certains anges veulent avoir une participation dans la société, tandis que d'autres préfèrent des actions de l'entreprise qui peuvent être facilement rachetables à leur valeur nominale, fournissant ainsi une sortie propre pour l'investisseur. Pour protéger leurs investissements, les anges demandent souvent aux entreprises de ne pas prendre certaines décisions sans leur approbation. En raison du risque élevé impliqué dans des marchés en

développement, il est souvent difficile de trouver des anges financiers pour aider à mettre en place un réseau sans fil, mais pas impossible. La meilleure façon de trouver des investisseurs potentiels est par le biais de votre réseau social et par la recherche en ligne.

Evaluer les forces et les faiblesses de la situation interne

Un réseau est seulement aussi bon que les personnes qui y travaillent et l'exploitent. L'équipe que vous mettez en place peut faire la différence entre la réussite et l'échec. C'est pourquoi il est important de comparer les qualifications et compétences de votre équipe, y compris ceux du personnel et des bénévoles, aux compétences nécessaires pour un projet sans fil. Tout d'abord, faites une liste de toutes les compétences requises pour exécuter un projet sans fil avec succès. Les domaines de compétence devraient inclure, entre autres, la technologie, les ressources humaines, la comptabilité, le marketing, la vente, la négociation, le juridique, et les opérations. Ensuite, identifiez les ressources locales qui remplissent ces compétences. Associez les compétences de votre équipe aux compétences qui sont nécessaires et identifiez les différences importantes.

Un outil souvent utilisé pour aider à cette autoévaluation est une analyse des forces, faiblesses, opportunités et menaces, appelé SWOT (*strengths, weaknesses, opportunities* et *threats*). Pour réaliser cette analyse, précisez vos forces et faiblesses internes, et faites de projections sur les opportunités et les menaces externes dans votre communauté. Il est important d'être réaliste et honnête sur ce que vous faites bien et ce qui vous fait défaut. Assurez-vous de faire la distinction entre là où votre organisme se trouve au début de cet effort et là où il pourrait être dans l'avenir. Vos forces et vos faiblesses vous permettront d'évaluer vos capacités internes et à mieux comprendre ce que votre organisme peut faire ainsi que ses limites. En comprenant vos forces et vos faiblesses et en les comparant à ceux de vos concurrents, vous pouvez déterminer vos avantages concurrentiels sur le marché. Vous pouvez aussi remarquer les zones où vous pouvez améliorer. Les opportunités et les menaces sont externes. Ce qui vous permet d'analyser les conditions réelles et la façon dont ces conditions influencent votre réseau.

Le diagramme ci-dessous vous aidera à faire votre propre analyse SWOT pour votre organisme. Assurez-vous de répondre aux questions posées et faites une liste de vos forces, faiblesses, opportunités et menaces dans les espaces désignés.

Forces	Faiblesses
• Qu'est-ce que vous faites bien ? • Quelles ressources uniques pouvez-vous en tirer ? • Qu'est-ce que les autres considèrent comme vos forces ? • ?	• Que pourriez-vous améliorer ? • Où avez-vous moins de ressources que les autres ? • Qu'est-ce que les autres sont susceptibles de voir comme faiblesses ? • ?
Opportunités	**Menaces**
• Quelles sont les bonnes opportunités qui s'ouvrent à vous ? • Quelles sont tendances dont vous pouvez prendre avantage ? • Comment pouvez-vous transformer vos forces en opportunités ? • ?	• Quelles sont les tendances qui peuvent vous nuire ? • Qu'est ce que votre concurrence est en train de faire ? • A quelles menaces, vos faiblesses vous exposent ? • ?

Assembler les pièces

Une fois que vous avez recueilli tous les renseignements, vous êtes prêt à mettre tout ensemble et à vous prononcer sur le meilleur modèle pour le réseau sans fil dans votre communauté. Sur la base des résultats de vos analyses externes et internes, vous devez redéfinir votre mission et vos offres de service. Tous les facteurs que vous avez étudiés au cours des étapes précédentes entrent en jeu lors de la détermination de votre stratégie globale. Il est essentiel d'employer un modèle qui se base sur les possibilités et fonctionne dans les contraintes de l'environnement local. Pour ce faire, vous devez souvent trouver des solutions novatrices pour atteindre la viabilité. En examinant plusieurs exemples et en discutant des éléments des modèles mis en oeuvre dans ces exemples, vous comprendrez mieux comment arriver à un modèle approprié.

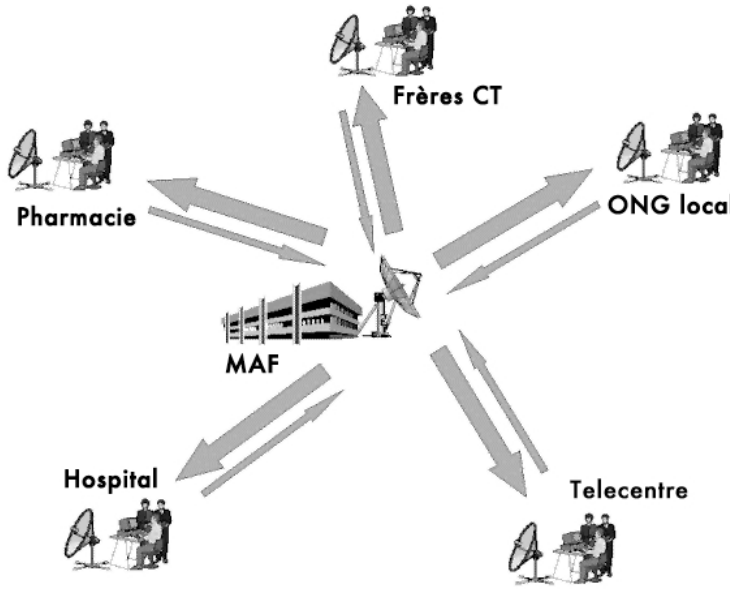


Figure 10.1 : Internet partage sur réseau sans fil

Dans la jungle lointaine de la République démocratique du Congo, il y a un hôpital rural dans un village appelé Vanga, dans la province de Bandundu. Il est tellement éloigné que les patients voyagent des semaines pour y arriver par le biais d'une combinaison de voyage à pied et par rivière. Ce village, fondé par les missionnaires baptistes en 1904, a servi d'hôpital pendant des nombreuses années. Bien qu'il soit extrêmement éloigné, il est réputé pour être un excellent établissement et a eu le soutien des missionnaires allemands et américains qui ont gardé cette installation en fonctionnement. En 2004, un projet parrainé par l'USAID a créé un télécentre dans ce village pour aider à améliorer l'éducation dans cette communauté isolée. Ce service Internet a également été largement utilisé par la classe éduquée dans la communauté et le personnel de l'hôpital. Le centre a été une grande faveur pour la communauté, offrant un accès à la connaissance du monde et allant même jusqu'à la consultation avec des collègues éloignés en Suisse, en France et au Canada. Le centre nécessitait une quasi totale subvention pour son fonctionnement et pour couvrir ses coûts, et le financement allait se terminer a la fin de l'année 2006. Bien que le centre amenait une grande valeur ajoutée à la communauté, il avait quelques lacunes, principalement techniques, économiques, et politiques qui limitaient sa viabilités. Une étude fut commandée pour examiner les options pour son avenir. Après avoir passé en revue la structure de coûts du centre, il fut déterminé qu'il était nécessaire de réduire ses coûts et rechercher de nouveaux moyens d'accroître ses recettes. Les dépenses les plus importantes étaient l'électricité et l'accès à Internet et, par conséquent, des modèles créatifs devaient être construits pour réduire les coûts du télécentre et fournir l'accès d'une manière qui soit durable.

Dans ce cas, un VSAT traditionnel a été utilisé pour la connectivité. Toutefois, ce modèle a fourni une façon unique de répondre aux moyens limites des groupes d'une communauté locale pour payer les services Internet. Des

organismes divers dans la communauté partagent l'accès à l'Internet par l'intermédiaire d'un réseau sans fil. Ils partagent également les coûts associés à cette connexion. Ce modèle fonctionne bien en raison de conditions spécifiques à savoir - la sensibilisation et la compréhension de la valeur de l'Internet par les membres clés de la communauté, les ressources nécessaires pour supporter l'accès à Internet, et un système de réglementation qui permet le partage sans fil. Dans Vanga, plusieurs organismes, y compris un hôpital, une pharmacie, plusieurs groupes missionnaires, un centre de ressource communautaire, et certains organismes sans profit, ont besoin d'accès à l'Internet et les moyens de payer pour cela. Cet arrangement permet au réseau d'organismes de disposer d'une connexion de meilleure qualité à un moindre coût. En outre, un organisme dans le village a la capacité et la volonté de gérer plusieurs aspects des opérations du réseau, y compris la facturation et la perception des payements, l'entretien technique et général de l'ensemble des opérations du réseau entier. Par conséquent, ce modèle fonctionne bien dans Vanga, car il a été adapté pour répondre à la demande de la Communauté et pour influencer les ressources économiques locales.

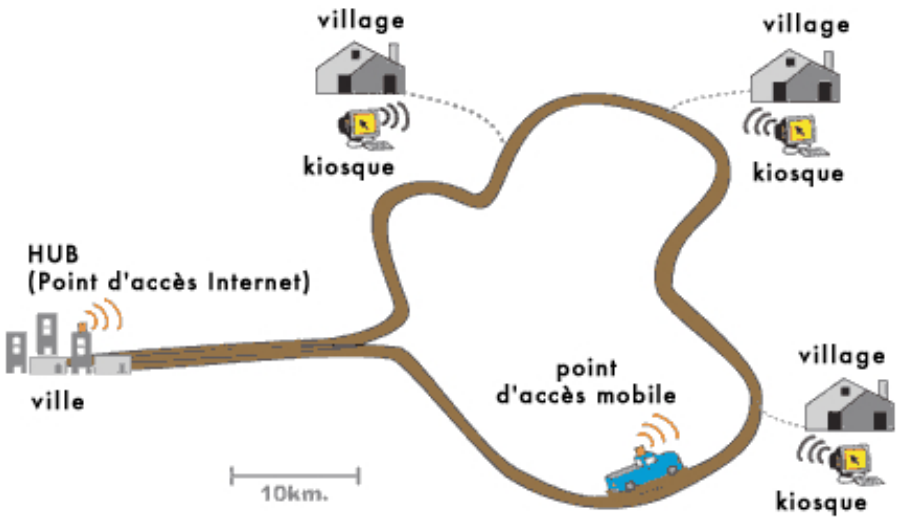


Figure 10.2 : Point d'accès Itinérant Daknet

Un autre exemple d'un modèle adapté au contexte local est celui de DakNet, de First Mile Solutions. Ce modèle a été déployé dans les villages en Inde, au Cambodge, au Rwanda, et le Paraguay. En prenant en compte le faible pouvoir d'achat des villageois, ce modèle répond à leurs besoins en matière de communication d'une façon innovatrice. Dans le modèle DakNet, il y a une franchise qui existe dans le pays, et les entrepreneurs locaux sont recrutés et formés pour opérer des kiosques équipés des antennes WiFI. A l'aide de cartes prépayées, les villageois sont capables d'envoyer et recevoir de manière asynchrone des e-mails, textes, mails et de la voix, de mener des recherches Web, et de participer au e-commerce. Ensuite, ces communications sont

stockées dans le serveur du kiosque local. Quand un bus ou une moto avec un point d'accès mobile passe près du kiosque, le véhicule reçoit automatiquement les données stockées dans le kiosque et délivre toute les données qu'il a. Une fois le véhicule atteint un centre ayant une connectivité Internet, il traite toutes les demandes, relayant les emails, les messages, et les fichiers partagés.

DakNet intègre à la fois l'accès mobile et des modèles de franchise pour apporter de la valeur aux populations dans des villages reculés. Pour qu'un tel modèle soit viable, plusieurs conditions clés doivent être présentes. Tout d'abord, un organisme de franchise doit exister pour fournir l'appui financier et institutionnel, y compris un investissement initial, le capital pour certains coûts récurrents, des conseils pour les pratiques de début, la formation en gestion, des procédures normalisés, des mécanismes d'information, et des outils de marketing. En outre, ce modèle nécessite une personne du village très motivée et dynamique, avec des compétences adéquates pour gérer une entreprise et la volonté d'accepter certaines exigences de l'organisme de franchise. Parce que ces entrepreneurs sont souvent invités à engager leurs propres ressources pour les dépenses initiales, ils ont besoin d'avoir un accès suffisant aux ressources financières. Enfin, pour s'assurer que ce modèle se soutient lui-même, il devrait y avoir une demande suffisante de l'information et de communication et peu de concurrents au sein de la communauté.

Conclusion

Aucun modèle d'affaires ne permettra à des réseaux sans fil d'être viables dans tous les environnements du monde en développement. Des modèles différents doivent être utilisés et adaptés en fonction des circonstances. Chaque communauté possède des caractéristiques uniques, et une analyse suffisante doit être menée au début d'un projet pour déterminer le meilleur modèle. Cette analyse devrait considérer plusieurs facteurs clés dans l'environnement local, y compris la demande, la concurrence, les coûts, les ressources économiques, etc. Bien qu'une planification et une exécution appropriées permettront de maximiser les chances de rendre votre réseau viable, il n'y a aucune garantie de succès. Toutefois, l'utilisation des méthodes détaillées dans ce chapitre vous aidera à garantir que votre réseau apporte de la valeur à la collectivité d'une manière qui correspond aux besoins des utilisateurs.

11
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 factures? 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: Réseau sans fil communautaire de la fondation Fantsuam

Kafanchan est une communauté de 83.000 personnes située à 200 km au nord d'Abuja, au centre du Nigéria. Kafanchan était connue comme une ville active et florissante car elle était l'un des principaux carrefours de la voie ferroviaire nationale. Quand l'industrie ferroviaire était en plein essor, près de 80% de la population de Kafanchan en dépendait d'une façon ou d'une autre. Suite à la chute complète du système ferroviaire Nigérien, la population de Kafanchan était forcée de retourner à sa source initiale de revenu, qui est l'agriculture.

Kafanchan est mal connecté en termes de téléphonie fixe et connectivité Internet. Aujourd'hui, la région ne dispose pas de téléphonie fixe (PSTN) et le GSM est juste arrivé en 2005. Toutefois, la couverture GSM est tout aussi pauvre que sa qualité de service. À l'heure actuelle, les services SMS sont le moyen le plus fiable de communication car des conversations vocales ont tendance à se couper dans le milieu et souffrent des bruits lourds.

L'accès limité à l'électricité apporte de nouveaux défis pour la population de Kafanchan. La compagnie nationale d'électricité du Nigéria, généralement connue sous le nom de NEPA (*National Electric Power Authority*), est plus communément connue par les Nigériens comme "Ne jamais s'attendre à l'électricité toujours" (*Never Expect Power Always*). En 2005, la NEPA changea son nom pour *Power Holding Company of Nigeria* (PHCN).

Kafanchan est alimenté en électricité par la NEPA sur une moyenne de 3 heures par jour. Pour les autres 21 heures, la population repose sur des générateurs diesel chers ou le kérosène pour l'éclairage et la cuisine. Quand l'électricité NEPA est disponible sur le réseau, elle fournit une tension non réglementée dans la gamme de 100-120 V pour un système conçu pour 240 V. Cette tension doit être régulée à 240 V avant que la plupart des charges puissent être connectées. Seules les ampoules peuvent être alimentées directement à la grille électrique car elles peuvent supporter cette tension basse sans dommage.

Les participants au projet

Étant donné le contexte difficile de Kafanchan, comment quelqu'un pourrait-il avoir l'idée de créer le premier fournisseur de services Internet sans fil en milieu rural au Nigéria? La fondation Fantsuam l'a fait et elle en a fait une réalité.

La fondation Fantsuam est un organisme non gouvernemental local qui a travaillé de concert avec la communauté de Kafanchan depuis 1996 pour lutter contre la pauvreté et l'inégalité à travers des programmes de développement intégré. Dans le projet Fantsuam, l'accent est mis sur la microfinance, les services TIC et le développement social dans les communautés rurales du Nigéria. Une partie de la mission Fantsuam était de devenir le premier fournisseur de services Internet sans fil en milieu rural au Nigéria en vue d'être reconnu comme chef de file dans la prestation des initiatives de développement rural, ainsi que le conducteur le plus avancé dans la connaissance de l'économie rurale au Nigéria.

Le fournisseur de services Internet sans fil de la Fondation Fantsuam, également connu sous le nom de Zittnet, est financé par le CRDI ; le centre de recherche pour le développement International du Canada. IT +46, une entreprise de consultance suédoise se concentrant sur les TIC pour le développement, a travaillé de concert avec l'équipe Zittnet pour fournir un appui technique pour les communications sans fil, la gestion de la bande passante, l'énergie solaire, les systèmes d'alimentation de secours d'énergie et les déploiements VoIP.

Objectifs

L'objectif principal de Zittnet est d'améliorer l'accès aux communications dans la zone rurale de Kafanchan par la mise en œuvre d'un réseau sans fil communautaire. Le réseau fournit l'accès Intranet et Internet à des partenaires locaux dans la communauté. Le réseau communautaire est formé par des organismes communautaires tels que les établissements d'enseignement, des institutions religieuses, les services de santé, les petites entreprises et des particuliers.

Système d'alimentation de secours

Afin de fournir un service fiable à la communauté, Zittnet avait besoin d'être équipé d'un système d'alimentation en courant stable permettant au réseau de fonctionner indépendamment de la NEPA.

Un système d'alimentation hybride constitué d'un banc de batteries à cycle profond et de panneaux solaires à 2 kW (crête) fut conçu pour Fantsuam. Le système peut se charger à partir de trois sources différentes: un générateur diesel, un panneau solaire, et la NEPA lorsque l'électricité est disponible.

Le ***centre des opérations du réseau*** (***NOC***, *Network Operation Center*) de l'organisme fonctionne complètement à partir de l'énergie solaire. Le reste des locaux Fantsuam fonctionnent à l'électricité NEPA ou un générateur via le banc de batterie en vue d'obtenir une stabilité de tension ininterrompue. La charge du NOC a été séparée du reste de la charge de Fantsuam en vue d'assurer une

source d'énergie fiable pour l'infrastructure critique du NOC, même lorsque l'énergie du banc de batteries est faible.

Figure 11.1: 24 panneaux solaires avec une puissance nominale de 80 W ont été montés sur le toit du NOC pour alimenter le système 24 / 7.

Les simulations avec les meilleures données solaires révèlent que l'état de Kaduna, où est situé Kafanchan, reçoit au moins 4 heures d'équivalent plein soleil au cours de ses pires des mois qui s'étendent de Juin à août (la saison des pluies).

Chacun des panneaux solaires (Suntech 80 W crête) fournit un courant maximal de 5 A (lorsque le rayonnement solaire est le plus élevé au cours de la journée). Dans le pire des mois de l'année, le système devrait produire pas moins de 6 kWh / jour.

Le système solaire a été conçu pour fournir une tension DC à la sortie de 12 V et 24 V DC pour correspondre à la faible tension d'entrée des serveurs et postes de travail de l'infrastructure NOC et des salles de formation.

Les panneaux solaires utilisés sont des panneaux Suntech STP080S-12/ Bb-1 ayant les spécifications suivantes:

- Tension en circuit ouvert (V_{oc}): **21,6 V**
- Tension de fonctionnement optimale (V_{mp}): **17,2 V**
- Courant de court-circuit (I_{sc}): **5 A**
- Courant d'exploitation optimum (I_{mp}): **4.65 A**
- Puissance maximale STC (P_{max}): **80 W (Crête)**

La puissance minimale de 6 kWh / jour qui alimente la NOC est utilisée pour alimenter les équipements suivants:

Périphérique	Heures/ jour	Unités	Puissance (W)	Wh
Points d'accès	24	3	15	1080
Serveurs de faible puissance	24	4	10	960
Écrans LCD	2	4	20	160
Ordinateur portable	10	2	75	1500
Lampes	8	4	15	480
Modem VSAT	24	1	60	1440
			Total:	**5620**

La consommation électrique des serveurs et des écrans LCD est basé sur les stations de calcul Inveneo à faible énergie, *http://www.inveneo.org/?q=Computingstation*.

La consommation énergétique totale du NOC est de 5,6 kWh / jour. Ce qui est inférieure à la puissance générée quotidiennement à partir de panneaux solaires dans le pire des mois.

Figure 11.2: Le NOC est construit par des briques en latérite produites localement et posées par les jeunes de Kafanchan.

Centre d'opérations du réseau

Un nouveau centre d'opérations du réseau (NOC) a été créé pour héberger le système de secours ainsi que des installations pour les serveurs. Le NOC a été conçu de façon à être exempt de poussière et doté de bonnes capacités de refroidissement pour les batteries et les onduleurs. Le NOC utilise des méthodes naturelles et est fait de matériaux disponibles localement.

Le bâtiment est composé de quatre chambres: une chambre de stockage de batterie, une salle des serveurs, un espace de travail et une salle de stockage pour le matériel.

La chambre de stockage de batterie accueille soixante dix batteries de 200 Ah à cycle profond ainsi que cinq onduleurs (l'un d'entre eux est à onde sinusoïdale pure), deux régulateurs de l'énergie solaire, des stabilisateurs de tension et des discontacteurs DC et AC. Les batteries sont empilées verticalement sur une structure en plateau métallique pour un meilleur refroidissement.

L'espace serveur contient un rack de serveurs et un ventilateur. La chambre n'a pas de fenêtres pour éviter la poussière et la surchauffe. La salle des serveurs et la chambre de batteries ont une orientation face sud pour améliorer le refroidissement naturel et aider à garder la chambre à une température appropriée.

La salle des serveurs et l'espace batterie nécessitent un refroidissement a faible coût / faible énergie comme elles ont besoin d'opérer 24x7. Pour atteindre cet objectif, les techniques de refroidissement naturel ont été introduites dans la conception du NOC: petits ventilateurs et extracteurs et murs en briques épais (double largeur) dans la direction du coucher du soleil.

Le côté sud du bâtiment accueille 24 panneaux solaires dans un espace sans ombre sur la toiture métallique. Le toit a été conçu avec une inclinaison de 20 degrés pour accueillir les groupes et de limiter la corrosion et la poussière. Des efforts supplémentaires ont été déployés pour garder les panneaux facilement accessibles pour le nettoyage et l'entretien. Le toit a également été renforcé afin d'assurer une charge supplémentaire de 150-200 kg.

L'immeuble NOC est construit avec des briques en boue de latérite de production locale. Le matériel est bon marché car il est utilisé fréquemment et provient de la couche supérieure du sol. Les briques sont produites localement à la main en utilisant une technique de pression low-tech. Le NOC est unique en son genre dans l'état de Kaduna.

Figure 11.3: Omolayo Samuel, l'un des membres du personnel de Zittnet, ne craint pas la hauteur de la tour de 45 m de hauteur, pendant qu'elle 'aligne des antennes hébergées dans le haut de la tour.

Les infrastructures physiques: Un mât de communication

La plupart des clients potentiels à Zittnet habitent entre 1 km et 10 km des locaux de Fantsuam. Pour atteindre ces clients, Fantsuam mit en place un mât de communication dans leurs locaux. En Octobre 2006, un mât de 45 m (150 pieds) de hauteur autoportant fut installé à la Fondation Fantsuam. Le mât fut équipé d'une prise de terre et une protection contre la foudre ainsi qu'une lampe de signalisation obligatoire.

Un anneau en métal fut enterré à la base de la tour, à une profondeur de 4 pieds. Tous les trois pieds du mât furent ensuite reliés au circuit de terre. Un paratonnerre fut monté au plus haut point du mât afin de protéger le matériel contre les coups de foudre. Le paratonnerre est fait de cuivre pur et est relié à l'anneau de terre à la base du mât en utilisant une bande de cuivre.

La lampe de signalisation montée à la tête du mât est une exigence de l'aviation civile. La lampe est équipée d'une cellule photoélectrique permettant une commutation automatique en fonction du niveau de lumière ambiante. De cette façon, la lampe s'allume la nuit et s'éteint au cours de la journée.

L'infrastructure de la dorsale du réseau sans fil

L'infrastructure de la dorsale du réseau sans fil est construite en utilisant des points d'accès à plusieurs bandes de type Smart Bridges et des unités client de

la série Nexus PRO TOTAL. Ces unités ont été conçues pour permettre aux fournisseurs de services et aux entreprises de créer des liaisons sans fil extérieures de type point à multipoint à haute performance. Elles sont fournies avec une antenne sectorielle intégrée à plusieurs bandes qui peut fonctionner aussi bien dans la bande des 2,4 GHz que la bande des fréquences 5.1-5.8 GHz. La série Nexus PRO TOTAL offre la qualité de service (***QoS***, *quality of service*) en terme de priorités de trafic et gestion de la bande passante par client à l'aide des extensions WMM (*WiFi Multimedia*) compatibles avec la norme IEEE 802.11e.

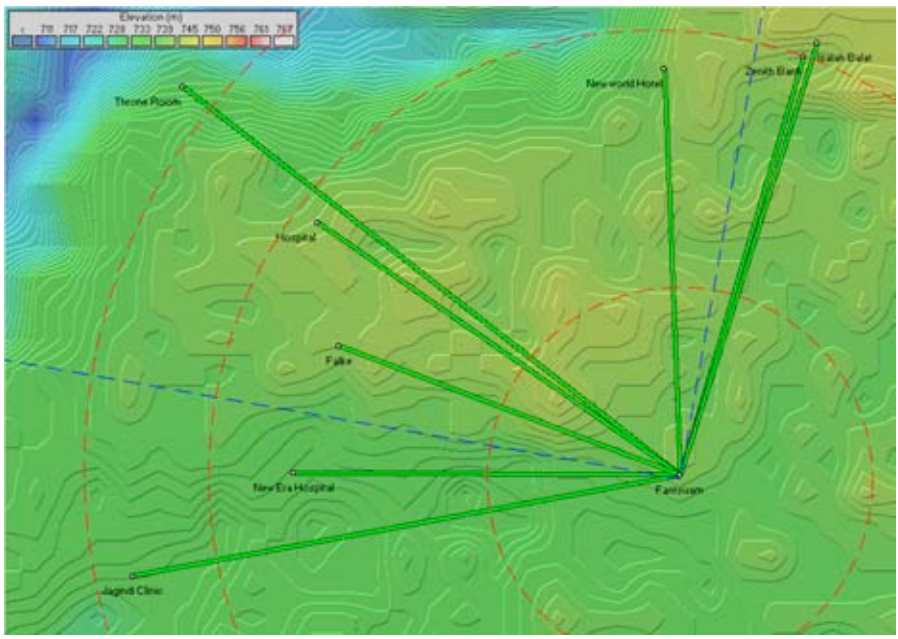


Figure 11.4: la topologie du réseau Zittnet en Octobre 2007.

Actuellement, la topologie du réseau est une topologie étoile avec deux points d'accès dans le mât de communication situé dans les locaux Fantsuam. Un point d'accès a une antenne sectorielle de 90 degrés (en lignes pointillées en bleu) et l'autre point d'accès offre une couverture omnidirectionnelle dans l'entourage (en anneaux pointillé en rouge). Les clients qui sont situés dans la zone située entre les lignes pointillées sont connectés à l'antenne sectorielle, tandis que les autres clients sont connectés à l'antenne omnidirectionnelle.

Des plans sont en cours pour étendre la dorsale du réseau sans fil par la mise en place de deux répétiteurs sans fil. Un répétiteur sera situé dans la ville de Kafanchan en utilisant une tour existante de la compagnie NITEL pour améliorer la couverture sans fil au coeur de la ville. Le second répétiteur sera mis en place dans le Kagoro Hills, un petit groupe de montagnes situées à environ 7 km de Kafanchan et à altitude d'environ 500 m par rapport à Kafanchan. Ce répétiteur va fournir une couverture à de nombreuses villes environnantes et peut être même permettre une liaison longue distance vers Abuja.

Zittnet avait connecté son premier client au début d'août 2007. Deux mois plus tard, pas moins de huit clients sont connectés à Zittnet. Ces clients comprennent:

- L'hôpital général
- New Era hôpital
- Jagindi Street Clinic (clinique de santé)
- Zenith Bank (privée)
- Isaïe Balat (café Internet)
- New World Hotel
- Throne Room Guesthouse
- Fulke

Problèmes rencontrés

Quelques problèmes qui ont été constamment présents dans l'ensemble du projet sont les suivants.

Bâtiments de faible hauteur

La plupart des locaux des clients sont des bâtiments sans étage d'une hauteur de moins de 3 mètres. Beaucoup de maisons ont des très faibles structures de toit qui rendent impossible de monter l'équipement sur le toit, comme l'accès physique n'est pas possible. Les bâtiments de faible hauteur nous forcent à monter l'équipement à une hauteur relativement faible car les clients ne peuvent pas se permettre d'investir dans les petits (10 m) mâts pour installer le matériel. La plupart des installations utilisent des réservoirs d'eau ou un simple poteau métallique de 3 m attaché à la paroi de la prémisse.

Lorsque l'équipement est monté bas, la première zone de Fresnel n'est pas claire et un débit faible est expérimenté. Bien que le paysage de Kafanchan soit très plat, la végétation sous forme d'épais manguiers bloque facilement la ligne de visée.

Les coups de foudre

Des orages lourds sont fréquents dans Kafanchan pendant la saison des pluies. En Septembre 2007, un coup de foudre à proximité endommagea les équipements montés sur un mât ainsi que son alimentation. A l'heure actuelle, le point d'accès et son injecteur PoE sont encrés à la tour elle-même. D'autres moyens doivent être investigués afin de prévenir tout dommage à l'équipement causés par une foudre environnante. L'équipe Zittnet travaille actuellement sur l'amélioration de la protection contre les surtensions en ajoutant des intercepteurs de surtension coaxiaux supplémentaires. En outre, le bouclier du câble UTP reliant le point d'accès au NOC sera encré (grounded) à l'aide de blocs de terre et des attaches.

Equipement de faible qualité

Malheureusement, un manque de produits de qualité sur le marché est un problème généralisé sur l'ensemble du continent africain. Comme la plupart des pays sous Sahariens manquent de politiques d'assurance de la qualité pour les produits importés, le marché est inondé par des articles “on marché” et de très faible qualité. Comme les produits de qualité sont difficiles à trouver, vous vous trouverez souvent en train d'acheter de la marchandise localement disponible qui peut se casser avant même sa mise en service. Comme aucune sorte de garantie n’existe pour ces petits achats, cela finit par être très coûteux. Ce problème est presque toujours présent pour des accessoires communs tels que les prises de courant, les bars de puissance, les connecteurs RJ45, le câblage CAT5, et d'autres équipements low-tech.

Modèle d’affaires

La seule alternative pour l'accès Internet dans Kafanchan est par satellite. En 2006, Fantsuam avait un abonnement pour une bande passante de 128/64 kbit/s dédiée à un coût de 1800$ USD/mois. Ce coût mensuel énorme de connectivité a été un grand fardeau pour Fantsuam et un stress constant de ne pas être en mesure de répondre à la facture mensuelle.

Comme une alternative à ce modèle "taxe forfaitaire" à haut risque, Fantsuam a mis en place un système appelé ***HookMeUP*** fourni par Koochi Communications. Le système vous propose des frais flexibles de type *Pay-As-You-Go* sur des connexions Internet VSAT pour les pays de l'Afrique sous saharienne.

Ce type de modèle d'accès se trouve généralement dans les aéroports, les hôtels ou les grandes galeries marchandes dans les pays occidentaux où les utilisateurs finaux achètent des coupons en ligne et se connectent en utilisant un code d'accès.

Le système HookMeUP offre une connexion VSAT dédiée de 512/256 kbps à Fantsuam (à partir de leur station au sol au Royaume-Uni). Fantsuam achète des coupons à Koochi communications et les revend à ses clients locaux dans Kafanchan. De cette façon, Fantsuam n'est plus bloqué avec un coût mensuel fixe, mais a seulement à payer Koochi pour la bande passante consommée. Le risque d'acheter cher la bande passante internationale au prix d’un coût plus élevé pour l'utilisateur final a été maintenant transféré au fournisseur de service Internet au lieu de l'utilisateur final.

Fantsuam Fondation agit désormais comme un revendeur de coupons de Koochi et un fournisseur d'infrastructure sans fil pour les utilisateurs finaux. Le réseau sans fil communautaire fournit désormais à la Fondation Fantsuam cinq sources de revenus:

1. Installation d'équipement pour locaux clients (une fois par client)
2. Location des équipements sans fil (coût mensuel par client)
3. Revente d’équipements sans fil (une fois par client)
4. Installation de points chauds (hotspot) sans fil dans les locaux client (une fois par client)
5. Revente de coupons (continuellement)

Le système de coupons est basé sur trois paramètres: ***temps d'accès***, ***limite de données*** et ***temps de validité***. Le paramètre qui s'épuise le premier va consommer le bon.

Temps d'accès	Limite de données (Mb)	Temps de validité	Prix (USD)	USD / h	USD / 700 MB
30 min	5	1 jour	0,80	1,60	112,00
60 min	10	5 jours	1,28	1,28	89,60
12 heures	60	14 jours	10,40	0,87	121,33
24 heures	150	30 jours	26,00	1,08	121,33
1 mois	500	1 mois	71,50	0,10	100,10
3 mois	1600	3 mois	208,00	0,10	91,00
6 mois	3500	6 mois	416,00	0,10	82,20
12 mois	7500	12 mois	728,00	0,08	67,95

Le plus grand avantage de ce système est que Fantsuam Fondation n'a plus le fardeau d'une énorme facture mensuelle de la bande passante internationale. Avoir un modèle de prix forfaitaire signifie que vous êtes obligé de vendre une certaine quantité de bande passante par mois. Avec le modèle Pay-As-You-Go (PAYG), le revenu Fantsuam pour la revente des coupons dépend de la quantité de bande passante que leurs clients consomment. Le client paie à l'avance (modèle prépayé) avec le résultat que Fantsuam n'aura jamais en fin de compte une énorme dette chez son fournisseur.

Le modèle prépayé fonctionne bien en Afrique, car les gens sont familiers avec ce modèle d'opérateurs de téléphonie mobile. Il est même utilisé par les compagnies d'électricité dans certains pays. Le modèle prépayé est apprécié par beaucoup de gens comme il les aide à garder la trace de leurs dépenses. L'une des principales limitations du modèle PAYG est le manque de flexibilité et de transparence. L'actuel système PAYG prévoit très peu de rétroaction à l'utilisateur sur la consommation de temps ou de volume. Ce n'est que lorsque l'utilisateur se déconnecte qu'il est informé du nombre de minutes qui restent à être dépensées.

Toutefois, le modèle d'affaires semble s'adapter très bien à la réalité locale de Kafanchan et de nombreuses autres communautés rurales en Afrique. Bien qu'il y ait de la place pour l'amélioration, l'avantage d'éviter les dettes est beaucoup plus élevé que les inconvénients. Avec le temps, lorsque le nombre de clients aura augmenté et qu'ils pourront compter sur un revenu mensuel substantiel provenant du réseau sans fil, ça serait bénéfique de revenir de nouveau au modèle de taxe forfaitaire.

Clients

Les clients sont libres d'utiliser l'accès Internet pour n'importe quel fin. Par exemple, Isaïe Balat revend des coupons (qu'il a achetés de Fantsuam) à ses clients. Son café Internet a 10 ordinateurs qui sont tous connectés à Zittnet. Les clients achètent des coupons chez le propriétaire avec une marge de 25% sur le prix offert par Fantsuam. En retour, les clients qui n'ont pas accès à un ordinateur connecté à Zittnet peuvent accéder au réseau par PC dans le café Internet d'Isaïe Balat.

New World Hotel est un autre client qui vise à créer un modèle d'affaires similaire, mais sur une plus grande échelle. Ils fourniront un accès Internet sans fil à l'ensemble de leurs chambres et offrent l'accès à la liaison montante Zittnet par la revente des coupons.

D'autres clients, comme l'hôpital général et Jagindi Street Clinic, utilisent l'accès Internet pour usage professionnel et privé sans revendre l'accès à ses clients.

-- Louise Berthilson

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 invisible 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, Atheros 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. Un FAI 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 semaine, 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'approche 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.

Étude de cas: Réseau maillé sans fil communautaire Dharamsala

Le Réseau maillé sans fil communautaire Dharamsala est né en Février 2005, suite à la déréglementation du WiFI pour usage extérieur en Inde. À la fin de Février 2005, le maillage a déjà connecté 8 campus.

Des tests intensifs au courant de Février 2005 ont montré que le terrain très montagneux est le plus approprié pour la mise en place des réseaux maillés. Ceci puisque les réseaux point à multipoint conventionnels ne peuvent pas surmonter les limitations associées a la ligne de visée présentées par les montagnes. La topologie en maillage fournit également une plus vaste couverture, tandis que la nature “autoréparable” du routage en maille s’est révélée essentielle dans les endroits où l'alimentation électrique est, au mieux, très erratique.

La dorsale du maillage comprend plus de 30 noeuds, partageant tous un seul canal radio. Les services Internet à large bande sont fournis à tous les membres du maillage. Le montant total de la bande passante Internet disponible en amont est de 6 Mbps. Il y a plus de 2000 ordinateurs connectés à la maille. La connexion Internet à large bande met le maillage sous une grande charge. A l'heure actuelle, le système semble gérer la charge sans aucune augmentation de la latence ou perte de paquets. Il est clair que l'évolutivité va devenir un problème si nous continuons à utiliser un seul canal radio. Pour résoudre ce problème, un nouveau maillage des routeurs supportant de canaux radio multiples est développé et testé à Dharamsala, en mettant l'accent sur des produits qui répondent à nos exigences techniques et notre viabilité économique. Les résultats initiaux sont très prometteurs.

Le maillage réseau est basé sur des déploiements récurrents d'un périphérique conçu et construit localement - connu sous le nom de ***l'Himalayan-Mesh-Router*** (*http://drupal.airjaldi.com/node/9*). Les même routeurs maillés sont installés à chaque endroit, avec différentes antennes, en fonction de la situation géographique et des besoins. Nous utilisons un large éventail d'antennes, des antennes 8 - 11 dBi omnidirectionnelles aux antennes 12 - 24 dBi directionnelles et parfois certaines antennes sectorielles à gain élevé (et coût).

Le maillage est principalement utilisé pour:

- Accès Internet.
- Applications de partage de fichiers
- Sauvegardes hors site.
- Lecture de vidéo de haute qualité à partir d’archives à distance.

Un PBX central basé sur logiciel de type voix sur Internet (ASTERISK) est installé et il fournit des services de téléphonie avancée pour les membres. Le PBX Asterisk fournit également une interface pour le réseau téléphonique a commutation de circuit PSTN. Toutefois, en raison de questions juridiques, il est actuellement utilisé uniquement pour les appels entrants dans la maille. Les

abonnés utilisent une grande variété de téléphones logiciels, ainsi que de nombreux ***adaptateurs téléphoniques analogiques*** (***ATA***s) et des téléphones IP.

Figure 11.5: Installateur Dharamsala travaillant sur une tour

La dorsale encrypté du maillage ne permet pas l'accès itinérant des appareils mobiles (ordinateurs portables et les assistants numériques personnels). Ainsi nous avons placé plusieurs points d'accès de type 802.11b à bon nombre des mêmes endroits où les routeurs maillés sont installés. Le maillage est la dorsale de ces infrastructures alors que les points d'accès fournissent l'accès aux dispositifs mobiles itinérants en cas de besoin.

L'accès à la dorsale de la maille n'est possible que par les routeurs maillés. Les clients sans fil simples n'ont pas l'intelligence nécessaire pour "parler" les protocoles de routage maillée et les politiques d'accès strictes. Le maillage est donc cryptée (WPA) et aussi "caché" afin de prévenir les appareils mobiles de le trouver ou de tenter d'y accéder. Permettre l'accès à la maille par les routeurs maillés seulement permet des politiques de contrôle d'accès strictes et l'application des limites à ***l'équipement sur prémisse client*** (***CPE***, *Client Premises Equipment*), qui est un élément crucial nécessaire à la réalisation de la sécurité bout en bout, le traffic-shaping, et qualité de service.

La consommation d'énergie d'un routeur maillé est inférieure à 4 watts. Cela rend les routeurs maillés idéaux pour usage avec de panneaux solaires. Beaucoup de routeurs maillés Dharamsala sont alimentés uniquement par de petits panneaux solaires. L'usage de l'énergie solaire en combinaison avec de petites antennes de faible puissance et des routeurs de faible consommation d'énergie est idéalement adapté aux régions sinistrées, car il est très susceptible de survivre lorsque toute autre infrastructure de communication est endommagée.

--AirJaldi, http://airjaldi.com/

Étude de cas: Mise en réseau de l'état de Mérida

La ville de Mérida se trouve au pied de la montagne la plus élevée au Venezuela, sur un plateau à environ 1600 m. Elle est la capitale de l'état de Mérida et abrite une université vielle de deux siècles avec quelques 35.000

étudiants. L'Université de Los Andes (ULA) déploya en 1989 le premier réseau informatique universitaire qui, en dépit de difficultés économiques, s'est étendu pour inclure 26 km de câble à fibre optique au dessus duquel un réseau TDM et ATM (*Asynchronous Transfer Mode*) sont construits. En 2006 un réseau Gigabit Ethernet de 50 km fut déployé au dessus du même câble à fibre optique.

Figure 11.6: Mérida est l'un des trois états montagneux du Venezuela où les Andes atteignent 5000 m de hauteur.

Néanmoins, de nombreux endroits de la ville et les villages environnants sont hors de portée de l'anneau en fibre optique. L'université dispose d'un serveur de communication avec les lignes téléphoniques permettant l'accès à distance à son réseau, mais les appels locaux sont facturés à la minute et de nombreux villages n'ont pas purement et simplement des lignes téléphoniques.

Pour ces raisons, les efforts visant à développer l'accès sans fil au réseau de l'université, sous dénomination RedULA, ont été menés dès le début. Les premières tentatives ont profité de l'existence du réseau de paquets exploité par les radios amateurs. Dès 1987, les amateurs avaient une passerelle avec une station ***haute fréquence*** (***HF***, *High Frequency*) à 300 bps pour les contacts d'outre-mer, ainsi que plusieurs stations ***très haute fréquence*** (***VHF***, *Very High Frequency*) à 1200 bps qui sillonnaient le pays.

Alors que les montagnes escarpées de la région sont un grand obstacle pour la pose des câbles et la construction des routes, elles peuvent être utiles dans le déploiement d'un réseau radio. Cette tâche est facilitée par l'existence d'un système de téléphérique, réputé le plus élevé du monde, qui relie la ville à un pic de 4765 m.

Figure 11.7: Sur son chemin vers la crête, le téléphérique passe par une gare intermédiaire appelé La Aguada, qui a une hauteur de 3450 m ainsi qu'une incroyable vue sur la ville de Mérida et d'autres villages à des distances allant jusqu'à 50 km.

Réseau radio à commutation de paquets

Les radio amateurs locaux exploitent un réseau radio à commutation de paquets. Au départ, il fonctionnait à 1200 bps, en utilisant des radios VHF amateurs FM vocales connectées à un ordinateur personnel au moyen d'un ***contrôleur de nœud terminal*** (***TNC***, *terminal node controller*). Le TNC est l'interface entre la radio analogique et les signaux numériques traités par le PC.

Le TNC déclenche les circuits Push to Talk de la radio pour passer du mode de transmission au mode de réception, effectuer la modulation /démodulation et l'assemblage/désassemblage des paquets en utilisant une variante du protocole X.25 connu sous le nom de AX.25. Les passerelles entre les radios VHF et HF radios ont été construites en attachant deux modems sur le même TNC et ordinateur. En règle générale, une passerelle devrait relier le réseau de paquets VHF local à des stations d'outre-mer par le biais de stations HF qui pourraient s'étendre sur des milliers de kilomètres, quoique à une vitesse de 300 bps seulement. Un réseau radio national à commutation de paquets a également été construit qui relaie sur les répétiteurs numériques ***digipeaters*** (les *digital repeaters* sont essentiellement des TNCs connectés à deux radios avec des antennes pointant dans des directions différentes) pour étendre le réseau de Mérida à Caracas par le biais de seulement deux de ces stations répétitrices. Les digipeaters fonctionnaient à 1200 bps permirent le partage de programmes et certains fichiers texte entre amateurs.

Phil Karn, un radioamateur avec une solide expérience dans les réseaux informatiques, a écrit le logiciel KA9Q qui implémente le protocole TCP / IP sur AX.25. En utilisant ce logiciel, nommé après son développeur, les amateurs du monde entier ont rapidement été en mesure de se connecter à l'Internet en utilisant différents types de radios. KA9Q conserve les fonctions du TNC au strict minimum, exploitant la puissance de l'ordinateur attaché au TNC pour la plupart des fonctions de traitement. Cette approche permet beaucoup plus de souplesse

et des mises à jour faciles. Dans Mérida, nous étions en mesure d'étendre la capacité du réseau à 9600 bps en utilisant des modems plus avancés, rendant possible à plusieurs radio amateurs d'accéder à l'Internet par l'intermédiaire du réseau câblé RedULA. La limite sur bande passante radio disponible dans la bande VHF met une casquette sur la vitesse de transfert de données maximale qui peut être obtenue. Pour accroître cette vitesse, il faut passer à des porteuses de fréquence plus élevée.

Les amateurs sont autorisés à utiliser des canaux larges de 100 kHz à l'aide de signaux ***ultra haute fréquence*** (***UHF***, *ultra-High Frequency*). Des radios numériques avec de modems de 19.2 Kbps doublèrent la bande passante de transmission. Un projet fut développé en utilisant cette technologie pour relier la Maison de la Science dans la ville de El Vigia à Mérida et l'Internet. Les antennes UHF furent construites à LabCom, le laboratoire de communications de ULA.

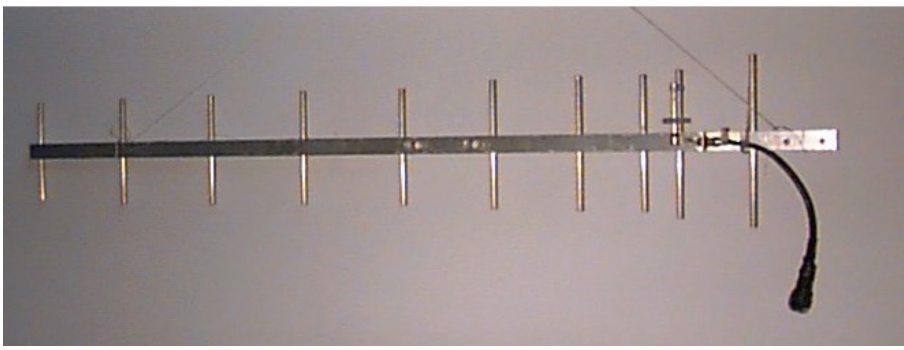


Figure 11.8: Une antenne UHF pour la radio à commutation de paquet conçue par LabCom à ULA.

Bien que El Vigia se trouve à seulement 100 km de Mérida par route, le terrain montagneux exige l'usage de deux répéteurs. L'un situé à La Aguada, à 3600 m d'altitude, et l'autre à Tusta, à 2000 m. Le projet a été financé par FUNDACITE MERIDA, une institution gouvernementale qui promeut la science et la technologie dans l'état. FUNDACITE opère aussi un pool de modems téléphone de 56 Kbps pour fournir l'accès Internet aux institutions et individus. La nécessité de disposer de deux stations répétitrices souligne les limites imposées par l'usage des porteuses de fréquence élevée, qui exigent une ligne de visée pour établir une transmission fiable. Dans la plus faible bande VHF, les signaux se réfléchissent facilement et peuvent aller au-delà des collines.

Il est parfois possible de refléter des signaux au moyen d'un ***répétiteur passif***, qui est construit par la liaison de deux antennes directionnel dos à dos avec un câble coaxial, sans radio. Ce système fut testé pour connecter ma résidence à LabCom. La distance n'est que de 11 km, mais il y a une colline au milieu qui bloque les signaux radio. Une connexion fut faite à l'aide d'un répétiteur passif pour refléter au large de La Aguada, avec les deux antennes du répétiteur pointant 40 degrés d'écart. Alors que tout cela était très excitant et certainement beaucoup moins cher que l'accès par modems téléphoniques, un support plus rapide serait de toute évidence nécessaire pour une dorsale sans fil pour connecter les villages reculés.

Ainsi, nous étudiâmes l'usage des modems de 56 kbps développés par Dale Heatherington. Ces modems sont logés dans une carte de type PI2 construit par les amateurs d'Ottawa et reliés directement à un PC utilisant Linux comme système d'exploitation de réseau. Bien que ce système fonctionne très bien, l'apparition du World Wide Web avec sa pléthore d'images et d'autres fichiers a bande passante accaparante, if fut clair que si nous dévions satisfaire les besoins des écoles et des hôpitaux, nous avions à déployer une solution à plus grande largeur de bande, au moins sur la dorsale. Cela signifiait l'usage de fréquences porteuses encore plus élevées dans la gamme micro-ondes, entraînant des coûts élevés.

Heureusement, une technologie alternative largement utilisée dans des applications militaires était en train de devenir disponible pour des usages civils à des prix abordables. Appelé ***étalement de spectre*** (*spread spectrum*), elle fut d'abord utilisé dans des applications civiles comme réseau local sans fil a courte portée, mais s'avéra très vite très utile dans les endroits a faible concentration des fréquences électromagnétiques permettant de couvrir des distances de plusieurs kilomètres.

Etalement de spectre

L'étalement de spectre utilise des signaux de faible puissance avec expansion de spectre pour couvrir toute la bande passante allouée tout en permettant un certain nombre d'utilisateurs de partager le support de communication en utilisant des codes différents pour chaque abonné.

Il y a deux manières d'accomplir cela: ***étalement de spectre à séquence directe*** (***DSSS***, *Direct Sequence Spread Spectrum*) et ***étalement de spectre à saut fréquentiel*** (***FHSS***, *Frequency hopping Spread Spectrum*).

Dans DSSS, l'information à transmettre est numériquement multipliée par une séquence des fréquences plus élevées, augmentant ainsi la bande passante de la transmission. Bien que cela puisse sembler être un gaspillage de bande passante, le système de restauration est si efficace qu'il peut décoder les signaux très faibles, permettant l'usage simultané du même spectre par plusieurs stations.

En FHSS, l'émetteur change constamment sa fréquence porteuse à l'intérieur de la bande passante allouée selon un code spécifié. Le récepteur doit connaître ce code afin de s'aligner sur la fréquence porteuse.

Les deux techniques échangent l'énergie de transmission pour la bande passante, permettant à plusieurs stations de partager une certaine partie du spectre. Nous avons étions en mesure de démontrer cette technique au cours du premier collège latino-américain sur les réseaux (EsLaRed'92) tenu à Mérida en 1992. Nous avions établi certains réseaux tests utilisant des antennes externes conçues par LabCom, permettant la transmission sur plusieurs kilomètres. En 1993, le ministère vénézuélien des télécommunications ouvrit quatre bandes à utiliser avec la DSSS:

- 400 - 512 MHz
- 806 - 960 MHz
- 2.4 - 2.4835 GHz

- 5,725 - 5,850 GHz

Dans chacun de ces groupes, la puissance maximale de l'émetteur était limitée à 1 Watt et le gain maximum de l'antenne à 6 dBi, pour une ***puissance isotrope rayonnée effective*** (***EIRP***, *effective isotropic radiated power*) de 36 dBm. Cette décision ouvrit la voie pour le déploiement d'un réseau DSSS avec une bande passante nominale de 2 Mbps dans la bande de fréquence de 900 MHz. Cette technologie répondit aux besoins émanant de la forte augmentation de l'activité World Wide Web.

Le réseau débuta à LabCom où la connexion à RedULA était disponible. LabCom abritait une antenne Yagi de fabrication interne dirigée vers un coin réflecteur à Aguada. Cela fournit un faisceau de 90 degrés, éclairant la grande partie de la cité de Mérida. Plusieurs sites abonnés, partageant tous la bande passante de valeur nominale de 2 Mbit/s, commencèrent à échanger de fichiers, y compris des images et des clips vidéo. Certains sites abonnés qui nécessitaient plus de câbles entre l'antenne et la propagation radio fréquences furent servis par usage d'amplificateurs bidirectionnels.

Ces résultats encourageants furent reportés à un groupe mis en place au centre international de physique théorique (ICTP, International Center for Theoretical Physics) à Trieste, en Italie, en 1995. Ce groupe visait à fournir la connectivité entre les centres de calcul, le bâtiment des sciences physiques, et le bâtiment de technologie à l'Université d'Ile-Ife au Nigéria. Plus tard cette année, le réseau fut mis en place par l'ICTP avec financement de l'Université des Nations Unies et fonctionne de manière satisfaisante depuis lors. Ce réseau se révèle être beaucoup plus rentable que le réseau a fibre optique initialement prévu aurait été.

De retour à Mérida, comme le nombre de sites augmenta, le débit observé par utilisateur baissa. Nous commençâmes à envisager la bande de fréquence de 2.4 GHz pour fournir une capacité supplémentaire. Cette bande peut transporter simultanément trois flots indépendants de 2 Mbit/s, mais avec une portée effective qui est plus faible que ce qui peut être réalisé dans la bande de fréquence de 900 MHz. Nous étions très occupés à la planification de l'extension de la dorsale en utilisant la bande des 2,4 GHz lorsque nous découvrîmes une compagnie débutante qui offrait une nouvelle solution qui promettait des longues distances, un débit spectaculairement plus élevé, et la possibilité de réutilisation des fréquences micro-ondes à bande étroite.

Système de livraison de services à large bande

Après avoir visité la compagnie Nashua, New Hampshire, les installations de Spike Technologies, nous étions convaincus que leur marque d'antenne et système radio étaient la meilleure solution pour les besoins de notre réseau, pour les raisons suivantes:

Leur système de livraison de services à large bande emploie une antenne sectorielle (**Figure 11.9**) avec 20 dBi de gain sur chacun d'au plus 22 secteurs indépendants. Chaque secteur transmet et reçoit sur des canaux indépendants à 10 Mbit/s full duplex, pour un débit total de 440 Mbps. La réutilisation de fréquences sur les secteurs entrelaces en fait un système spectrale ment efficace.

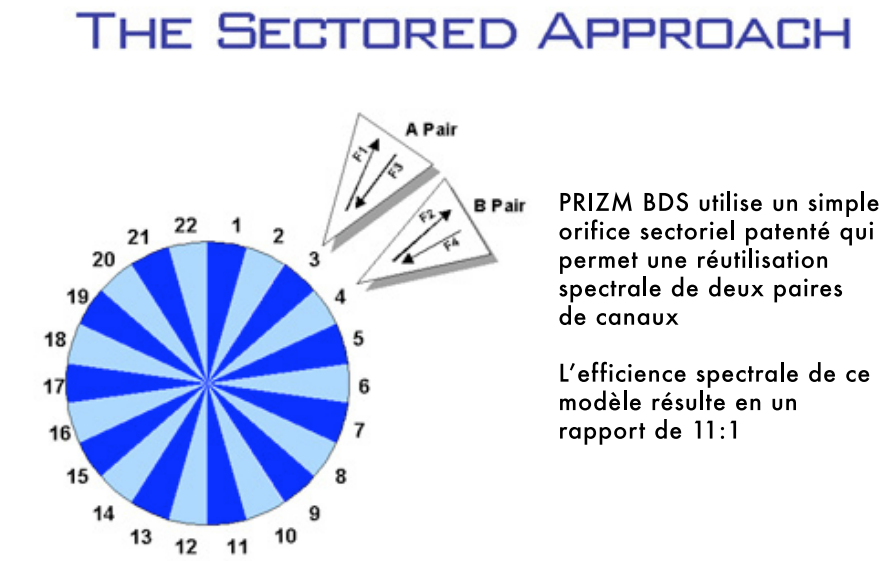


Figure 11.9: Système sectoriel full duplex à haute densité de Spike Technologies.

Les radios numériques à bande étroite peuvent fonctionner n'importe où de 1 à 10 GHz, avec une couverture allant jusqu'à 50 km. Les radios fonctionnent avec une variété de câbles modem TV, délivrant une connexion réseau local standard 10 Base-T à l'abonné. A la station de base, les secteurs sont interconnectés avec un commutateur à haute vitesse ayant une latence très faible (voir la **Figure 11.10**) permettant des applications telles que le streaming vidéo jusqu'à 30 images par seconde. Chaque secteur agit comme un réseau local Ethernet indépendant.

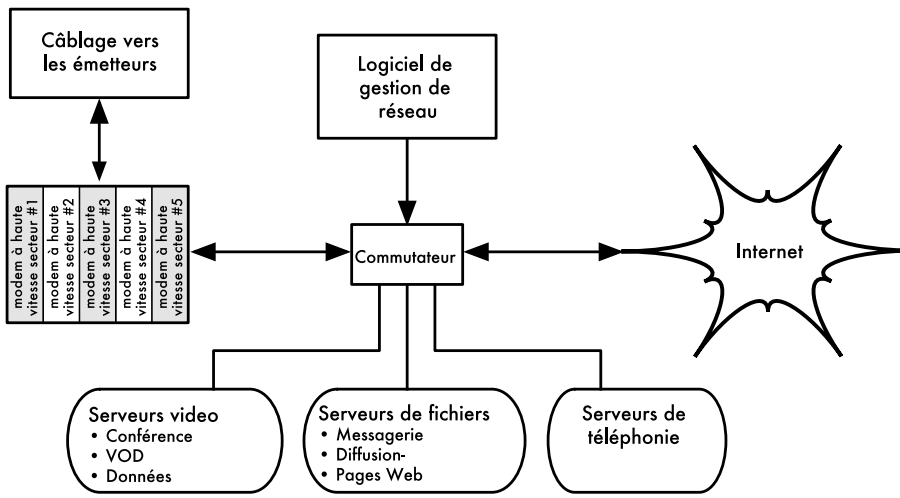


Figure 11.10 : Système d'interconnexions Spike Technologies.

Sur le site de l'abonné, une radio similaire et un modem fournissent une connexion 10BaseT à l'Ethernet local.

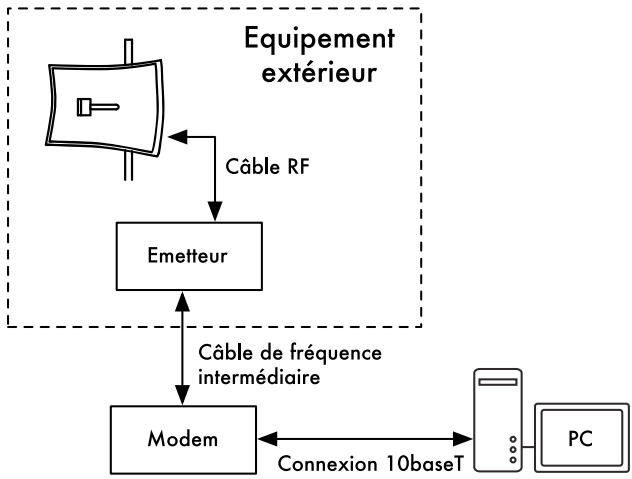


Figure 11.11: L'extrémité abonné de la liaison.

Grâce au financement du FUNDACITE, un système expérimental fut rapidement installé à Mérida, avec la station de base située juste au-dessus de la station de téléphérique de La Aguada à une altitude de 3600 m.

Figure 11.12: Installation à Mérida au-dessus de La Aguada, à 3600 mètres.

Au début, seulement 5 secteurs ont été installés, avec un faisceau de 16 degrés chacun. Le premier site abonné était dans les locaux FUNDACITE, où un système de satellite fournissait un accès Internet. Le second secteur servait le palais du gouverneur. Le secteur trois servait FUNDEM, un organisme

humanitaire de l'administration locale. Le quatrième secteur servait un pénitencier près de la ville de Lagunillas, à environ 35 km de Mérida. Le cinquième secteur transmettait au répétiteur au sommet d'une montagne, à proximité du village de La Trampa, à 40 km de La Aguada. De La Trampa, une autre liaison de 41 km étendait le réseau à la Maison de la Science dans la ville de Tovar.

Le 31 Janvier 1998, une vidéoconférence entre le pénitentiaire et le Palais de Justice à Mérida prouva qu'en dehors de l'accès à l'Internet, le système pourrait également supporter le streaming vidéo. Dans ce cas, il était utilisé pour la comparution des détenus, évitant ainsi les inconvenances et les risques de leur transport.

Le succès de l'expérimentation incita le gouvernement d'état à allouer les fonds pour un système complet pour donner accès Internet à haute vitesse au système de santé de l'état, au système éducatif, aux bibliothèques, aux centres communautaires, et plusieurs agences gouvernementales. En Janvier 1999, nous avions 3 hôpitaux, 6 établissements d'enseignement, 4 instituts de recherche, 2 journaux, 1 station de télévision, 1 bibliothèque publique, et 20 institutions sociales et gouvernementales partageant l'information et accédant à l'Internet. Un plan fut établi pour connecter 400 sites en full duplex à la vitesse de 10 Mbits/s au sein de cette année, et le financement fut déjà alloué à cette fin.

La **Figure 11.13** montre une carte de l'état de Mérida. Les lignes sombres montrent la dorsale initiale tandis que les lignes claires montrent les extensions.

Figure 11.13: Le réseau de l'état de Mérida

Parmi les nombreuses actions soutenues par le réseau, il est utile de mentionner les éléments suivants:

- **L'éducation**: les écoles ont reçu un approvisionnement sans fin de matériel de la plus haute qualité pour les élèves et les enseignants, en particulier dans les domaines de la géographie, des langues et des sciences, et comme un outil pour communiquer avec d'autres groupes qui partagent des intérêts communs. Les bibliothèques ont des cabines avec des ordinateurs avec accès Internet accessibles au grand public. Des journaux et de stations de télévision ont une source extraordinaire d'information à mettre à la disposition de leur public.
- **La santé**: L'hôpital universitaire a une liaison directe vers l'unité de soins intensifs, où un personnel de médecins spécialistes est toujours de service. Ces médecins sont disponibles pour être interrogés par leurs collègues dans des villages reculés afin de discuter des cas spécifiques. Un groupe de chercheurs de l'université est en train de développer plusieurs applications de la télémédecine sur la base du réseau.
- **La recherche**: L'observatoire astronomique de Llano del Hato, situé sur une montagne à 3600 m et 8 degrés de l'équateur sera bientôt relié, permettant aux astronomes du monde entier l'accès aux images qui y sont recueillis. Les chercheurs de terrain dans de nombreux villages bénéficieront d'un accès Internet.
- **Le gouvernement**: La plupart des organismes gouvernementaux sont déjà connectés et commencent à mettre en ligne des informations pour les citoyens. Nous nous attendons à ce que ceci ait un impact profond sur les relations entre les citoyens et le gouvernement. Les organismes humanitaires et les forces de l'ordre font un usage intensif du réseau.
- **Le divertissement et la productivité**: Pour les personnes vivant à l'extérieur de la ville, les possibilités offertes par le réseau ont un impact significatif sur la qualité de leur vie. Nous espérons que cela contribuera à inverser la tendance à l'exode rurale pour atténuer la surpopulation des zones urbaines. Les agriculteurs ont accès à l'information sur le prix commandant leurs cultures et les fournitures, ainsi que l'amélioration des pratiques agricoles.

Supercomm'98, tenue à Atlanta en Juin, cita le réseau de services à large bande de Mérida comme vainqueur du prix SUPERQuest dans la catégorie Accès à distance-8 (8-Remote Accès) comme le meilleur dans ce domaine particulier de candidats.

Formation

Depuis nos premiers efforts visant à établir un réseau informatique, nous nous sommes rendu compte que la formation est d'une importance primordiale pour les personnes impliquées dans la conception, la gestion et l'entretien des réseaux. Compte tenu de notre budget très limité, nous décidâmes que nous devions mettre en commun nos ressources avec celles d'autres personnes qui

avaient également besoin de formation. En 1990, l'ICTP organisa la première école internationale sur l'analyse et la gestion des réseaux d'ordinateurs, qui fut suivi par le professeur José Silva, et le professeur Luis Nunez de notre université. À leur retour à Mérida, ils proposèrent que nous devions émuler en quelque sorte cette activité dans notre université. À cette fin, profitant de mon congé sabbatique, je passa trois mois à Bellcore à Morristown, New Jersey, et trois mois de plus à l'ICTP aidant dans la préparation de la deuxième école sur les réseaux en 1992, où je fus rejoint par mon collègue, le Professeur Edmundo Vitale. Je passai le reste de mon congé sabbatique au SURANET à College Park, Maryland, sous la direction de Dr. Glenn Ricart. Celui-ci me présenta à Dr. Saul Hahn de l'Organisation des États américains, qui offrit une aide financière pour une activité de formation en Amérique latine. Ces expériences nous permirent de lancer la première école latino-américaine sur les réseaux (EsLaRed'92) à Mérida, à laquelle ont assisté 45 participants de 8 pays de la région, avec des instructeurs de l'Europe, les États-Unis et d'Amérique latine. Cette formation pratique dura trois semaines, et des technologies sans fil étaient accentuées.

EsLaRed'95 réunit de nouveau à Mérida avec 110 participants et 20 instructeurs. EsLaRed'97 avait 120 participants, et il fut approuvé par l'Internet Society, qui également parraina un atelier réseau en espagnol et portugais pour l'Amérique latine et les Caraïbes tenu à Rio de Janeiro en 1998 avec EsLaRed comme responsable du contenu de la formation. Maintenant, dix ans plus tard, EsLaRed continue à étendre ses efforts de formation tout au long de l'Amérique du Sud.

Remarques de conclusion

L'Internet a un impact plus profond dans les pays en développement qu'ailleurs, en raison du coût élevé des appels téléphoniques internationaux, de fax, de magazines et de livres. Ceci est évidemment exacerbé par la baisse du revenu moyen des personnes. Certains habitants dans des villages reculés qui n'ont pas de téléphones sont en train d'expérimenter une transition du 19ème au 21ème siècle grâce aux réseaux sans fil. Il est à espérer que ceci contribuera à l'amélioration des modes de vie dans les domaines de la santé, l'éducation, le divertissement et la productivité, ainsi que créer une relation plus équitable entre les citoyens et le gouvernement.

Références

- Karn, Phil, "The KA9Q Internet (TCP / IP) Package: A Progress Report", Sixth ARRL Computer Networking Conference, Redondo Beach, CA, 29 August 1987.
- Heatherington, D., "A 56 kilobaud modem RF," Sixth ARRL Computer Networking Conference, Redondo Beach, CA, 29 August 1987.
- Conatel, Comision Nacional de Comunicaciones, Ministerio de Comunicaciones y Transporte, "NORMAS PARA LA OPERACION DE SYSTEMAS DE TELECOMUNICACIONES CON TECNOLOGIA DE

BANDA ESPARCIDA (SPREAD SPECTRUM)", Caracas 17 Novembre 1993.

- International Center for Theoretical Physics, "Programme of Training and System Development on Networking and Radiocommunications, Trieste, Italy, 1996, *http://www.ictp.trieste.it/*
- Escuela Latinoamericana de Redes, *http://www.eslared.org.ve/*

--Ermanno Pietrosemoli

Étude de cas: Chilesincables.org

Les technologies récentes de transmission de données sans fil permettent la création des réseaux à grande vitesse, des réseaux séparés géographiquement à un coût relativement faible. Si ces réseaux sont construits autour de l'idée de la suppression des restrictions à l'accès aux données, nous les appelons des ***réseaux libres*** (*free networks*). Ces réseaux peuvent apporter de grands avantages à tout utilisateur, indépendamment de sa condition politique, économique, ou sociale. Ce type de réseau est une réponse directe au modèle commercial souvent restrictif qui gouverne une grande partie de notre société occidentale moderne.

Pour promouvoir les réseaux libres, les technologies sans fil doivent être adaptées et utilisées le mieux possible. Ceci est réalisé par des groupes de pirates informatiques qui font de la recherche, l'investigation, le développement et l'implémentation des projets, ainsi que permettre un accès libre à la connaissance acquise.

Chilesincables.org s'efforce de promouvoir et organiser des réseaux libres sans fil en Chili de manière professionnelle. Pour ce faire, nous fournissons une formation sur les aspects juridiques et techniques de mise en réseau sans fil, en encourageant l'adaptation des nouvelles technologies par le biais d'une recherche appropriée et en stimulant l'adaptation de ces technologies pour répondre aux besoins spécifiques des communautés chiliennes et de la société.

Description de la technologie

Nous employons une variété de technologies sans fil, y compris le IEEE 802.11a/b/g. Nous sommes aussi en train d'investiguer les dernières innovations dans le domaine, comme le WiMAX. Dans la plupart des cas, le matériel a été modifié afin d'accepter des antennes externes construites localement qui répondent à la réglementation des télécommunications locales.

Même si une majorité de matériel sans fil disponible sur le marché correspond à nos objectifs, nous encourageons l'utilisation et l'exploration d'un petit nombre de fournisseurs qui permettent un meilleur contrôle et une adaptation à nos besoins (sans nécessairement augmenter les prix). Il s'agit notamment de Wi-Fi avec les cartes offertes par les chipsets Atheros, Prism, Orinoco, et Ralink, ainsi que certains modèles de points d'accès fabriqué par Linksys, Netgear, et Motorola. La communauté des pirates informatiques a mis au point un firmware qui offre de nouvelles fonctionnalités sur cet équipement.

Pour la dorsale du réseau lui-même, nous employons des systèmes d'exploitation libres, y compris GNU/Linux, FreeBSD, OpenBSD, et Minix. Ceci correspond à nos besoins dans les domaines de routage ainsi que la mise en œuvre des services tels que les proxies, le web et les serveurs FTP, etc.

En outre, ils partagent la philosophie de notre projet consistant en une technologie libre avec le logiciel libre.

Utilisations et applications

Les réseaux mis en œuvre permettent les tâches suivantes:

- Transfert de données via FTP ou des serveurs web.
- Les services VoIP.
- Streaming audio et vidéo.
- Messagerie instantanée.
- Exploration et implémentation de nouveaux services tels que LDAP, la résolution de nom, de nouvelles méthodes de sécurité, etc.
- Services fournis par les clients. Les utilisateurs sont libres d'utiliser l'infrastructure réseau afin de créer leurs propres services.

Administration et maintenance

L'unité opérationnelle du réseau est le ***noeud***. Chaque noeud permet aux clients de s'associer au réseau et obtenir des services réseau de base. En outre, chaque nœud doit être associé à au moins un autre noeud, par convention. Cela permet au réseau de grandir et de rendre plus de services disponibles à chaque client.

Un noeud est maintenu par un administrateur qui est un membre de la communauté commis aux tâches suivantes:

- Le maintien d'une disponibilité suffisante (plus de 90%).
- Fourniture des services de base (généralement l'accès à Internet).
- Garder les clients à jour sur les services du noeud (par exemple, comment obtenir l'accès au réseau). Ceci est généralement fourni par un portail captif.

L'administration générale du réseau (en particulier, les tâches liées au déploiement de nouveaux nœuds, la sélection des sites, la topologie du réseau, etc.) est effectuée par le conseil d'administration de la communauté, ou par des techniciens formés à cet effet.

Chilesincables.org est actuellement en train d'acquérir le statut juridique, une étape qui permettra la réglementation de ses procédures administratives internes et l'officialisation de la communauté dans notre société.

Formation et renforcement des capacités

Chilesincables.org considère la formation de ses membres et ses clients comme étant d'une importance vitale pour les raisons suivantes:

- Le spectre radio doit être conservé aussi clair que possible afin de garantir la qualité des connexions sans fil. Par conséquent, la formation en techniques de communication radio est essentielle.
- L'emploi de matériaux et de méthodes approuvées par la réglementation actuelle est une exigence pour le développement normal des activités.
- Afin de se conformer aux standards Internet, l'ensemble de nos administrateurs réseau sont formés en réseau TCP/IP.
- Pour assurer la continuité des opérations du réseau, la connaissance de la technologie de réseau doit être transférée aux utilisateurs.

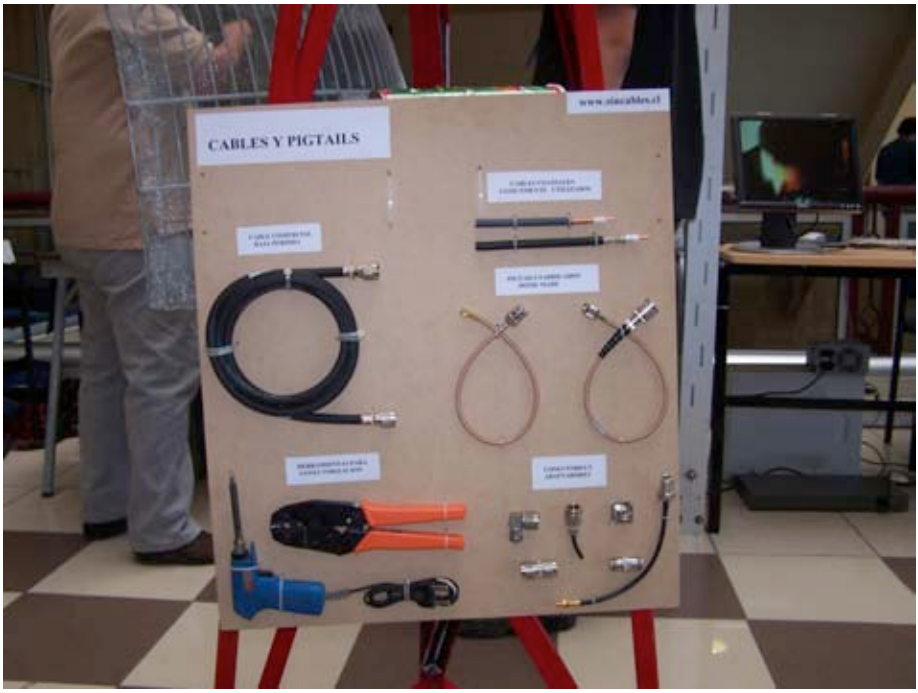
À l'appui de ces principes, Chilesincables.org entreprend les activités suivantes:

- **Atelier d'antenne**. Les participants sont formés à la construction d'antennes, et introduits aux concepts de base de communication radio.
- **Atelier Systèmes d'exploitation**. La formation sur la mise en œuvre de routeurs et autres dispositifs basés sur GNU/Linux ou d'autres logiciels tels que m0n0wall ou pfsense. Les concepts de base des réseaux sont également enseignés.
- **Promotion et publicité**. Les événements dans les différentes communautés qui poursuivent les mêmes objectifs que les nôtres sont promus. Il s'agit notamment des ateliers dans les collèges, des conférences, des rencontres du logiciel libre, etc.
- **Mise à jour du matériel**. Chilesincables.org maintient un certain nombre de documents à libre accès et du matériel mis à la disposition des personnes intéressées à une activité spécifique.

Les images sur les pages suivantes présentent un bref compte rendu des activités dans notre communauté.

Figure 11.14: Atelier antenne à fente omnidirectionnelle. Dans cette session, les participants apprirent la construction d'antennes et la théorie associée.

Figure 11.15: Un de nos membres du personnel enseignant la mise en œuvre d'un routeur m0nowall dans l'administration d'un noeud.



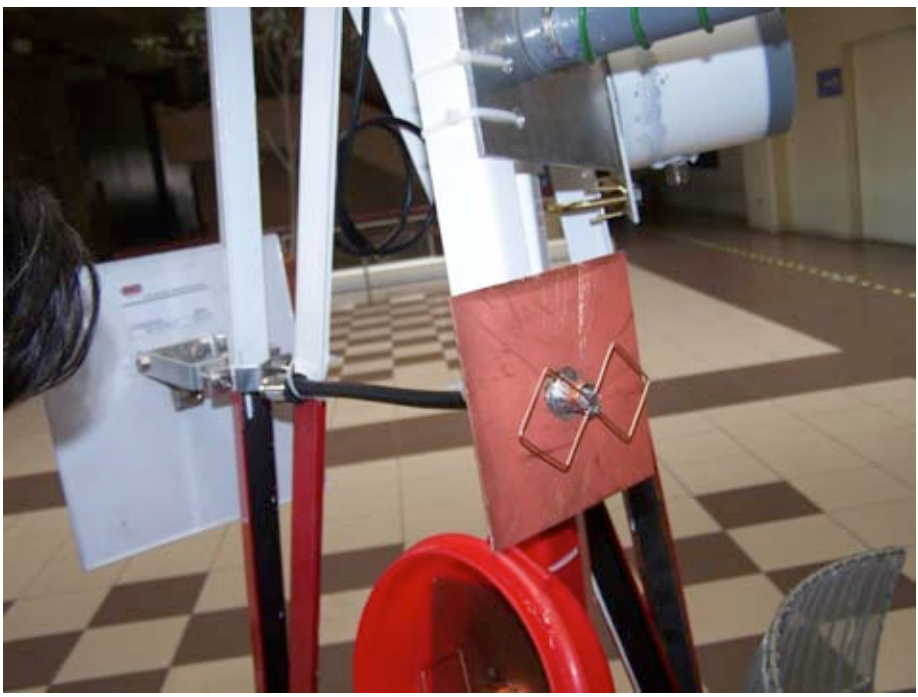


Figure 11.16: Détail de la minitour avec des échantillons d'antennes, câbles et nattes.

Figure 11.17: Station sans fil et antenne parabolique utilisées pour la transmission de Santiago-2006 FLISOL via le streaming vidéo.

Figure 11.18: Situation de l'autre bout de la liaison.

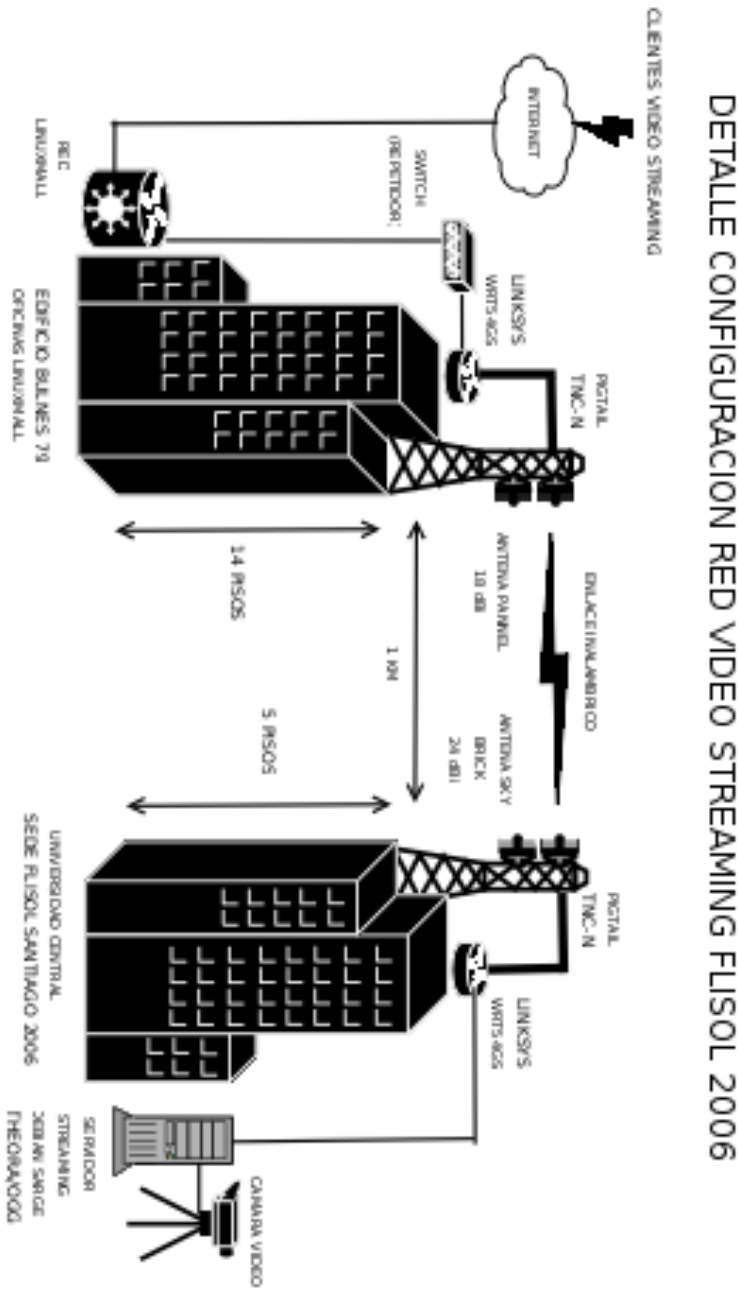


Figure 11.19: Schéma représentant la transmission en streaming video Santiago-2006 FLISOL utilisant des logiciels libres. La vitesse de transmission sans fil réalisée était de 36 Mbit/s à 1 km.

Figure 11.20 : Le nœud Quiani. C'est l'un des noeuds les plus élevés du monde. Il est situé à une altitude de 4000 m, environ 2000 km au nord de la capitale du pays.

Figure 11.21: Un nœud dans le sud de Santiago, constitué d'une tour de 15 m, une antenne de type Trevor Marshall 16 +16 et 30 clients. Le noeud est connecté à un noeud de la ville a plus de 12 km de distance.

Figure 11.22: Vue panoramique d'un noeud du haut de la tour.

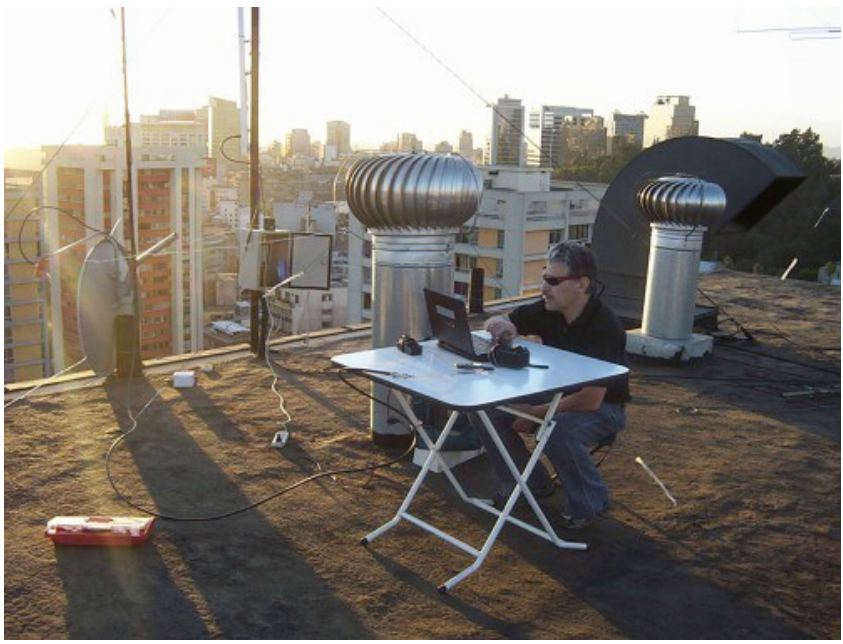


Figure 11.23: Nœud de la ville relié au nœud au sud de Santiago. Notez l'antenne parabolique utilisée pour le backhaul et l'antenne sectorielle pour connecter les clients.

Figure 11.24: Implémentation d'un noeud sur un château d'eau dans Batuco, région métropolitaine, fournissant le backhaul pur le télécentre de Cabrati.

Figure 11.25: Atelier sur les antennes Yagi organisé par notre communauté. Les participants construisent leurs propres antennes.

Crédits

Notre communauté est composée d'un groupe d'associés bénévoles engagés dont certains sont dignes d'être cités:

Felipe Cortez (Pulpo), Felipe Benavides (Colcad), Mario Wagenknecht (Kaneda), Daniel Ortiz (Zaterio), Cesar Urquejo (Xeuron), Oscar Vasquez (Machine), Jose de San Martin (Packet), Carlos Campano (Campano), Christian Vasquez (fondu), Andres Peralta (Cantenario), Ariel Orellana (Ariel), Miguel Bizama (Picunche), Eric Azua (M. Floppy), David Paco (Dpaco), Marcelo Jara (Alaska).

--Chilesincables.Org

Étude de cas: 802.11 longue distance

Grâce à une topographie favorable, le Venezuela a déjà des liens de réseau sans-fil à longue portée, comme celle de 70 km de long exploitée par FUNDACITE Mérida entre Pico Espejo et Canagua.

Pour tester les limites de cette technologie, il est nécessaire de trouver une voie dégagée avec une ligne de visée non obstruée et un dégagement d'au moins 60% de la première zone de Fresnel.

Tout en regardant le terrain au Venezuela, à la recherche d'un tronçon à haute altitude aux extrémités et un terrain bas entre les deux, je me concentrai d'abord sur la région de Guyana. Bien que beaucoup de terrains élevés s'y trouvent, en particulier le fameux "tepuys" (une mesas haute avec des murs raides), il y avait toujours des obstacles dans le milieu du terrain.

Mon attention fut portée vers la cordelière des Andes, dont les pentes raides (surgissant brusquement de la plaine) se révélaient adéquates à la tâche. Depuis plusieurs années, je voyageais à travers les zones faiblement peuplées à cause de ma passion pour le vélo de montagne. Dans ma tête, je conservais un dossier de l'adéquation des différents endroits pour les communications longue distance.

Pico del Aguila est un endroit très favorable. Il a une altitude de 4200 m et est à environ deux heures de route de ma ville de Mérida. Pour l'autre extrémité, je localisai enfin la ville d'El Baul, dans l'état de Cojedes. En utilisant le logiciel gratuit Radio Mobile (disponible à l'*http://www.cplus.org/rmw/english1.html*), je trouvai qu'il n'y avait pas d'obstruction de la première zone de Fresnel (couvrant 280 km) entre Pico del Aguila et El Baul.

Plan d'action

Une fois satisfait de l'existence d'une trajectoire convenable, nous nous sommes penchés sur l'équipement nécessaire pour atteindre l'objectif. Nous utilisions des cartes Orinoco pendant un certain nombre d'années. Avec une puissance de sortie de 15 dBm et un seuil de réception de -84 dBm, elles sont robustes et fiables. La perte en espace libre pour 282 km est de 149 dB. Donc, nous aurions besoin d'antennes de 30 dBi aux deux extrémités et même celles-ci laisseraient très peu de marge pour d'autres pertes.

D'autre part, le routeur sans fil populaire Linksys WRT54G est sous Linux. La communauté logicielle libre a écrit plusieurs versions de firmware pour Linux qui permettent une personnalisation complète de tous les paramètres de transmission. En particulier, le firmware OpenWRT permet l'ajustement du temps de réponse de la couche MAC ainsi que la puissance de sortie. Un autre firmware, DD-WRT, a une interface graphique et un utilitaire très pratique d'enquête de site. En outre, le Linksys peut être situé plus près de l'antenne qu'un ordinateur portable. Nous avons donc décidé d'utiliser une paire de ces boîtes. L'un a été configuré comme un ***point d'accès*** (***AP***, *Access Point*) et l'autre en tant que client. Le WRT54G peut fonctionner à 100 mW de puissance de sortie avec une bonne linéarité, et peut même être poussé jusqu'à 200 mW. Mais à cette valeur, la non linéarité est très grave et des faux signaux sont générés, ce qui devrait être évité. Bien que ce soit des équipements pour consommateurs et très bon marché, après des années d'utilisation, nous étions confidents que cela pourrait servir notre objectif. Bien sûr, nous avons conservé un ensemble de rechange à portée de main, juste au cas où.

En fixant la puissance de sortie à 100 mW (20 dBm), nous avons pu obtenir un avantage de 5DB par rapport à la carte de Orinoco. Par conséquent, nous nous sommes fixés pour une paire de WRT54GS.

Etude du site Pico del Aguila

Le 15 Janvier 2006, je suis allé à Pico Águila afin de vérifier sur site si ce que la Radio Mobile avait signalé était approprié. L'azimut vers El Baul est de 86°, mais comme la déclinaison magnétique est de 8° 16', notre antenne doit pointer vers une porteuse magnétique de 94°.

Malheureusement, quand j'ai regardé vers 94°, j'ai trouvé la ligne de visée obstruée par un obstacle qui n'avait pas été montré par le logiciel, en raison de la limitation de la résolution des cartes numériques d'élévation qui sont librement disponibles.

J'ai roulé mon vélo de montagne pendant plusieurs heures pour examiner la zone environnante à la recherche d'une voie claire vers l'Est. Plusieurs endroits prometteurs ont été identifiés, et pour chacun d'eux, j'ai pris des photos et enregistré les coordonnées à l'aide d'un GPS pour traitement ultérieur avec le logiciel Radio Mobile. Cela m'a conduit à affiner mon chemin de sélection, résultant en celui représenté par la **Figure 11.26** en utilisant Google Earth:

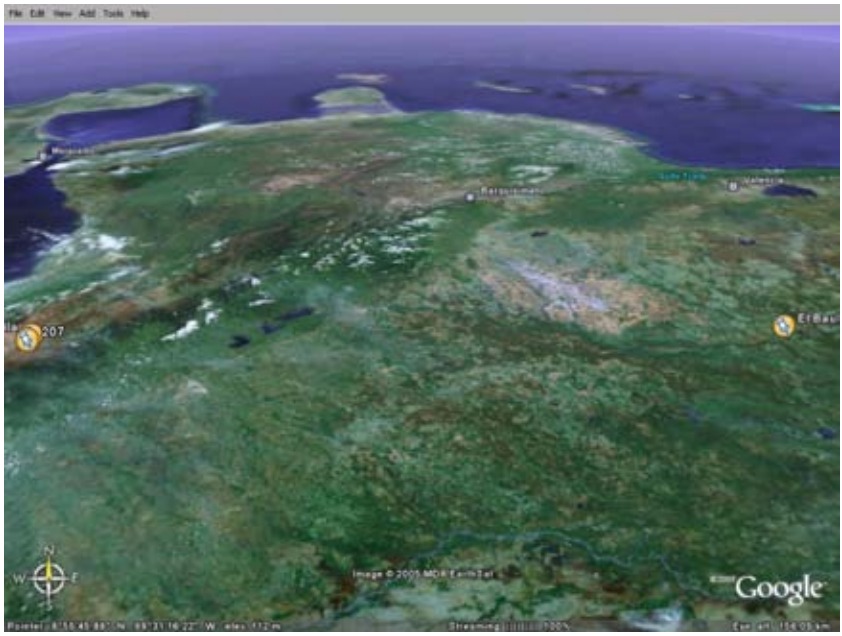


Figure 11.26: Vue de la liaison de 280 km de lien. Le lac Maracaibo est à l'ouest, et la Péninsule de Paraguana est vers le Nord.

Le profil Radio obtenu avec Radio Mobile est montré dans la **Figure 11.27**:

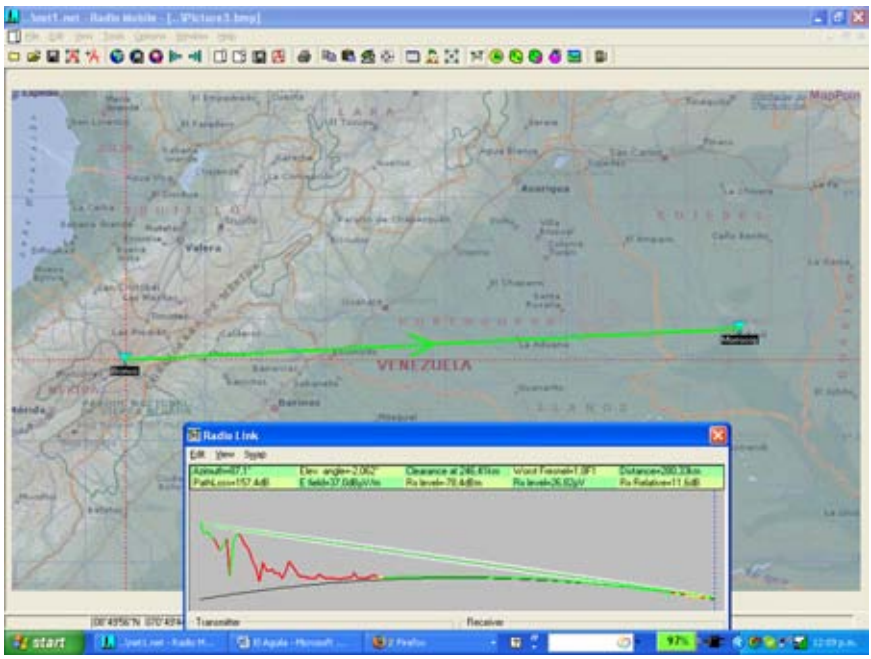


Figure 11.27: Plan et profil du projet de chemin entre Pico Aguila, et la colline Morrocoy, près de la ville de El Baul.

Les détails de la liaison sans fil sont affichés par la **Figure 11.28:**

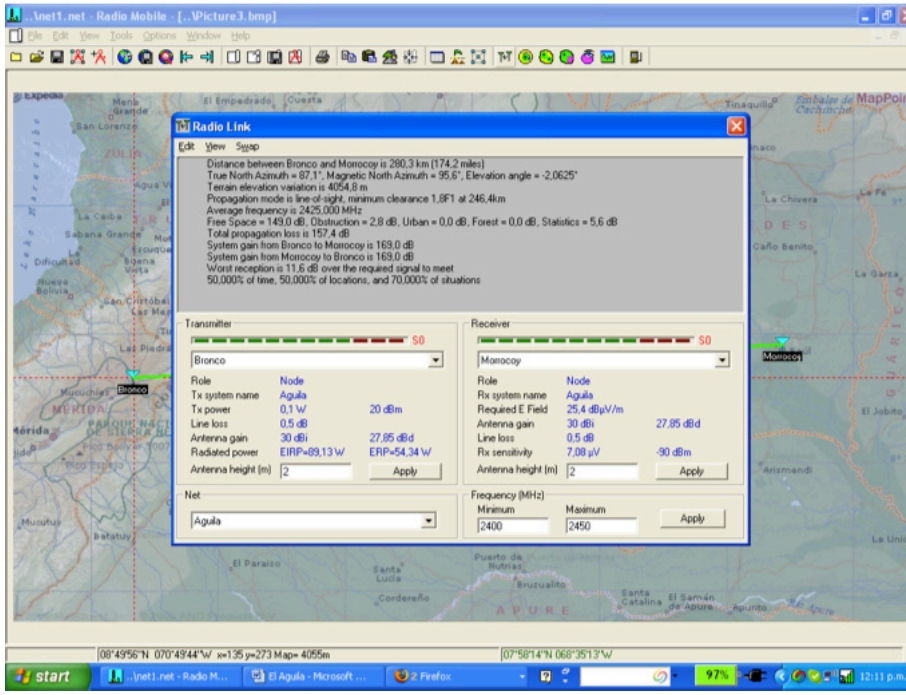


Figure 11.28: Détails de Propagation de la liaison de 280 km.

Afin de parvenir à une marge raisonnable d'environ 12 dB pour la liaison, il nous fallait des antennes d'au moins 30 dBi de gain à chaque extrémité.

Antennes

Les antennes à gain élevé pour la bande des 2.4 GHz ne sont pas disponibles au Venezuela. Les coûts d'importation sont considérables, ce qui nous a plutôt décidé de recycler des réflecteurs paraboliques (anciennement utilisés pour le service par satellite) et remplacer l'alimentation avec une conçu pour la bande des 2,4 GHz. Nous avons prouvé le concept à l'aide d'une antenne plate de 80 cm. Le gain a été beaucoup trop faible, de sorte que nous avons essayé un réflecteur offset de 2,4 m. Ceci donna suffisamment de gain, mais avec certaines difficultés dans le pointage du faisceau de 3,5°. L'offset de 22.5° signifiait que l'antenne semblait être orientée vers le bas quand elle était alignée horizontalement.

Plusieurs tests ont été réalisés en utilisant divers cantennas et une antenne Yagi de 12 dBi comme alimentation. Nous avons pointé l'antenne à une station de base du réseau sans fil de l'université qui était situé à 11 km sur une montagne de 3500 m. Le site de test se trouve à 2000 m et donc l'angle d'élévation est de 8°. A cause du décalage de l'alimentation, nous avions pointe l'antenne parabolique de 14° vers le bas, comme on peut le constater dans la figure suivante:

Figure 11.29: Réflecteur d'alimentation offset de 2,4 m avec une antenne de 12 dBi à son foyer, tourné 14° vers le bas. L'élévation réelle est de 8° vers le haut.

Nous étions en mesure d'établir un lien avec la station de base à Aguada, mais nos efforts pour mesurer le gain de l'installation en utilisant Netstumbler ne furent pas couronnés de succès. Il y avait trop de fluctuation sur les valeurs de puissance reçues du trafic réel.

Pour une mesure signifiante du gain, nous avions besoin d'un générateur de signaux et un analyseur de fréquences. Ces instruments ont également été nécessaires pour la visite sur terrain afin d'aligner correctement les antennes.

En attendant l'équipement requis, nous avons cherché une antenne à être utilisée à l'autre extrémité, et aussi un système de pointage mieux adapté au faisceau radio étroit.

En Février 2006, je me suis rendu à Trieste pour prendre part à la formation annuelle des réseaux sans fil dans laquelle j'ai été assistant depuis 1996. Pendant que j'étais là, j'ai mentionné le projet à mon collègue Carlo Fonda qui a immédiatement été ravi et impatient de participer.

La collaboration entre le collège sur les réseaux pour les pays d'Amérique latine (**EsLaRed**) et le Centre international de physique théorique Abdus Salam (**ICTP**) remonte à 1992, lorsque le premier collège sur les réseaux a eu lieu à Mérida avec le soutien de l'ICTP. Depuis lors, les membres des deux institutions ont collaboré à plusieurs activités. Certaines d'entre elles incluent un séminaire annuel de formation sur les réseaux sans fil (organisée par l'ICTP) et un autre sur les réseaux informatiques (organisée par EsLaRed) tenues dans plusieurs pays d'Amérique latine. En conséquence, il n'a pas été difficile de persuader Dr. Sandro Radicella, le chef de la section Aéronomie et Laboratoire de propagation

radio a ICTP, pour supporter le voyage de Carlo Fonda au Venezuela au début d'avril afin de participer à l'expérience.

De retour à la maison, j'ai trouvé une antenne parabolique maillée de 2,75 m à alimentation centrale installée dans une parcelle voisine. M. Ismael Santos gracieusement prêta son antenne pour l'expérience.

La **Figure 11.30** montre le démontage du réflecteur maillé.

Figure 11.30: Carlo et Ermanno démontent l'antenne satellite fournie par M. Ismael Santos.

Nous avons échangé les alimentations pour celles à 2,4 GHz, et pointé l'antenne à un générateur de signaux qui était situé au sommet d'une échelle à quelques 30 mètres de distance. Avec un analyseur de fréquence, nous avons mesuré la durée maximale du signal et localisé l'objectif (*focus*). Nous avons également mis en évidence la boresight à la fois pour l'alimentation centrale et les antennes de décalage (*offset antennas*).

Ceci est montré dans la **Figure 11.31**:

Figure 11.31: Trouver le focus de l'antenne avec une alimentation de 2,4 GHz

Nous avons également comparé la puissance du signal reçu à la sortie avec la puissance de sortie d'une antenne commerciale de 24 dBi. Cela produisit une différence de 8 dB. Ce qui nous a amené à croire que le gain global de notre antenne a été d'environ 32 dBi. Bien sûr, il y a une certaine incertitude associée à cette valeur. Nous étions en train de recevoir des signaux de réception, mais la valeur s'accordait avec le calcul de dimension de l'antenne.

Sondage sur le site El Baul

Une fois que nous étions satisfaits avec le bon fonctionnement et la visée des deux antennes, nous avons décidé de faire une étude de site à l'autre extrémité de la liaison El Baul. Carlo Fonda, Gaya Fior et de Ermanno Pietrosemoli atteignirent le site le 8 avril. Le lendemain, nous avons trouvé une colline (sud de la ville) avec deux tours de télécommunications appartenant à deux opérateurs de téléphonie cellulaire et une appartenant au maire de El Baul. La colline de Morrocoy est environ 75 m au-dessus de la zone qui l'entoure, à environ 125 m au-dessus du niveau de la mer. Elle offre une vue dégagée vers El Aguila. Il existe un chemin de terre au sommet, un must pour notre objet, étant donné le poids de l'antenne.

Exécution de l'expérience

Le mercredi 12 avril, Javier Triviño et Ermanno Pietrosemoli voyagèrent vers Baul avec l'antenne offset chargée sur le toit d'un camion à quatre roues motrices. Tôt le matin du 13 avril, nous avons installé l'antenne et l'a pointée à un relèvement compas de 276°, étant donné que la déclinaison est de 8° et donc la véritable Azimut est de 268°.

Dans le même temps, l'autre équipe (composée par Carlo Fonda et de Gaya Fior d'ICTP, avec l'assistance de Franco Bellarosa, Lourdes Pietrosemoli et José Triviño) roula vers la zone étudiée précédemment a Pico del Aguila dans une camionnette Bronco qui transportait l'antenne maillée de 2,7 m.

Figure 11.32: Pico del Aguila et ses environs avec la camionnette Bronco.

Le mauvais temps est commun à une altitude de 4100 m au-dessus du niveau de la mer. L'équipe de la Aguila était en mesure d'installer et pointer l'antenne maillée avant que le brouillard et la neige aient commencé. La **Figure 11.33** montre l'antenne et le câble utilisé pour viser le faisceau radio de 3°.

L'alimentation pour le générateur de signaux était fournie à partir du camion au moyen d'un 12 VDC vers un onduleur 120 VAC. À 11 heures du matin dans El Baul, nous étions en mesure d'observer un signal de -82 dBm à la fréquence convenue de 2450 MHz à l'aide d'un analyseur de spectre. Pour être certain que nous avions trouvé la bonne source, nous demandâmes à Carlo d'éteindre le signal. En effet, la trace sur l'analyseur montra seulement du bruit. Cela confirma que nous étions en train de voir réellement le signal qui venait de quelque 280 km de distance.

Après avoir tourné le générateur de signaux de nouveau, nous effectuâmes un ajustement en hauteur et azimut aux deux extrémités. Une fois que nous étions satisfaits d'avoir atteint le signal reçu maximum, Carlo enleva le générateur de signaux et le remplaça par un routeur sans fil Linksys WRT54G configuré comme un point d'accès. Javier remplaça l'analyseur de notre côté par un autre WRT54G configuré comme un client.

Figure 11.33: Viser l'antenne à El Águila.

En une fois, nous commençâmes à recevoir des "balises", mais les paquets ping ne passaient pas.

Cela était prévisible car le temps de propagation de l'onde radio sur une liaison de plus de 300 km est de 1 ms. Il faut au moins 2 ms à un accusé de réception pour accéder l'émetteur.

Heureusement, le firmware OpenWRT permet l'adaptation du temps de réponse (ACK timing). Après que Carlo aie ajustée pour l'augmentation des 3 ordres de grandeur de délai au-dessus de ce qui est prévu pour une liaison Wi-Fi standard, nous commençâmes à recevoir des paquets avec un délai d'environ 5 ms.

Figure 11.34: Installation d'antenne a El Bau. L'altitude réelle était de 1° vers le haut car l'antenne avait un décalage de 22,5°.

Nous procédâmes au transfert de plusieurs fichiers PDF entre les ordinateurs portables de Carlo et de Javier. Les résultats sont présentés dans la **Figure 11.35**.

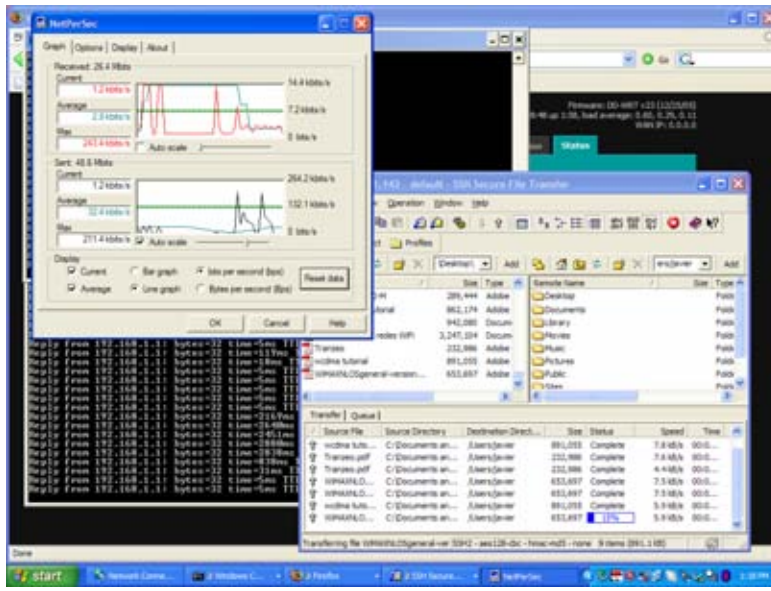


Figure 11.35: Capture d'écran de l'ordinateur portable de Javier montrant les détails de transfert de fichiers PDF à partir de l'ordinateur portable de Carlo a 280 km de distance, en utilisant deux routeurs sans fil WRT54G, et sans amplificateurs.

Notez le temps ping de quelques millisecondes.

Figure 11.36: Javier Triviño (à droite) et Ermanno Pietrosemoli rayonnant à cause de l'antenne d' El Baul.

Figure 11.37: Carlo Fonda au site d'Aguila site

Mérida, Venezuela, le 17 avril 2006

Un an après cette expérience, nous avons trouvé le temps et les ressources pour la répéter. Nous avons utilisé des antennes commerciales de 30 dBi ainsi q'un couple de routeurs sans fil qui avaient été modifiés par le groupe TIER dirigé par le Dr Eric Brewer de l'Université de Berkeley.

Le but de la modification de la norme WiFi MAC est de la rendre apte à des applications longue distance par le remplacement du contrôle d'accès de type CSMA par celui du type TDMA. Ce dernier est mieux adapté pour les longues distances de type point à point car il ne nécessite pas une réception des réponses ACK. Cela élimine la nécessité d'attendre les 2 ms de temps de propagation aller-retour sur la liaison de 300 km de distance.

Le 28 avril 2007, une équipe formée par Javier Triviño, Torres et José Francisco Torres installa l'une des antennes au site d'El Aguila. L'autre équipe, formée par Leonardo González V., G. Leonardo González, Alejandro González et Ermanno Pietrosemoli, installa l'autre antenne à El Baul.

Une liaison solide fut mise en place rapidement en utilisant les routeurs Linksys WRT54G. Cela permit la transmission vidéo à un débit mesuré de 65 kbps. Avec les routeurs TDMA, le débit mesuré était de 3 Mbit/s dans chaque direction. Cela produisit un débit total de 6 Mbit /s comme prévu par les simulations faites à Berkeley.

Peut-on faire mieux?

Ravis de ces résultats, qui ouvrent la voie à vraiment des liaisons longue distance à large bande bon marché , la deuxième équipe se déplaça vers un autre emplacement déjà identifié à 382 km de El Aguila, dans un endroit appelé Platillón. Platillón est à 1500 m au-dessus du niveau de la mer et il a une première zone de Fresnel vers El Aguila (situé à 4200 m au-dessus du niveau de la mer) dégagée. Le chemin proposé est illustré par la **Figure 11.38**:

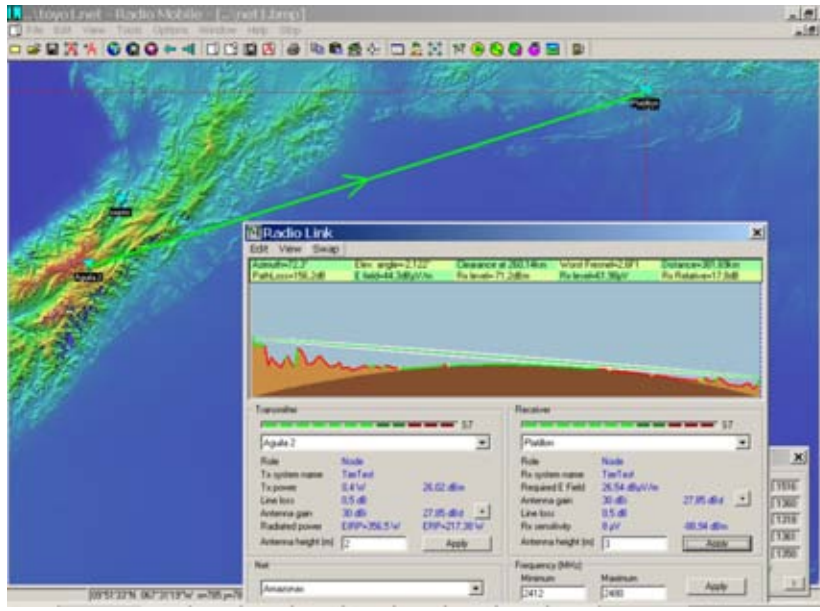


Figure 11.38: Carte et profil du chemin de 380 km.

Encore une fois, la liaison a rapidement été mise en place avec le Linksys et les routeurs fournis par TIER. La liaison Linksys montra environ 1% de perte de paquets, avec une moyenne de temps aller-retour de 12 ms. L'équipement TIER n'a révélé aucune perte de paquets, avec un temps de propagation au-dessous de 1 ms. Cela permit la transmission vidéo, mais la liaison n'était pas stable. Nous remarquâmes des fluctuations de signal qui souvent interrompaient la communication.

Toutefois, lorsque le signal reçu était d'environ -78 dBm, le débit mesuré était un total de 6 Mbit /s bidirectionnel avec les routeurs TIER implémentant TDMA.

Figure 11.39: L'équipe d' El Aguila, José Torres (à gauche), Javier Triviño (centre), et Francisco Torres (à droite)

Bien que d'autres essais devaient être effectués afin de déterminer les limites d'un débit stable, nous sommes convaincus que le Wi-Fi a un grand potentiel de propagation à longue distance pour les communications à large bande. Il est particulièrement bien adapté pour les zones rurales ou le spectre de fréquences n'est pas encore surpeuplé et l'interférence n'est pas un problème, à condition qu'il y ait une bonne ligne de visée radio.

Remerciements

Nous tenons à exprimer notre gratitude à M. Ismael Santos pour le prêt de l'antenne maillée installée à El Aguila et à l'ingénieur Andrés Pietrosemoli pour l'approvisionnement des joints d'échafaudage spéciaux utilisés pour le transport et l'installation des antennes.

Nous aimerions également remercier le Centre international de physique théorique Abdus Salam pour supporter le voyage de Carlo Fonda de l'Italie au Venezuela.

Figure 11.40: L'équipe de Platillon. De gauche à droite: V. Leonardo González, Leonardo González G., Ermanno Pietrosemoli et Alejandro González.

En 2006, l'expérience a été réalisée par Ermanno Pietrosemoli, Javier Triviño de EsLaRed, Carlo Fonda, et de Gaya Fior de l'ICTP. Avec l'aide de Franco Bellarosa, Pietrosemoli Lourdes, et José Triviño.

Pour les expériences de 2007, Dr Eric Brewer de l'Université de Berkeley a fourni les routeurs sans fil avec la couche MAC modifiée pour les liaisons longues distances, ainsi que le soutien enthousiaste de son collaborateur, Sonesh Surana. RedULA, CPTM, Dirección de Servicios ULA Universidad de los Andes, Mérida et FUNDACITE contribuèrent à cet essai.

Ce travail a été financé par le CIA-CRDI.

Références

- Fundación Escuela Latinoamericana de Redes, Latin American Networking School, *http://www.eslared.org.ve/*
- Abdus Salam International Centre for Theoretical Physics, *http://wireless.ictp.it*
- OpenWRT Open Source firmware for Linksys, *http://openwrt.org/*
- Fundacite Mérida, *http://www.funmrd.gov.ve/*

--Ermanno Pietrosemoli

Annexes

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 hierarchies 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 Pyramid wireless router OS, *http://pyramid.metrix.net/*
- 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/*
- 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*
- 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

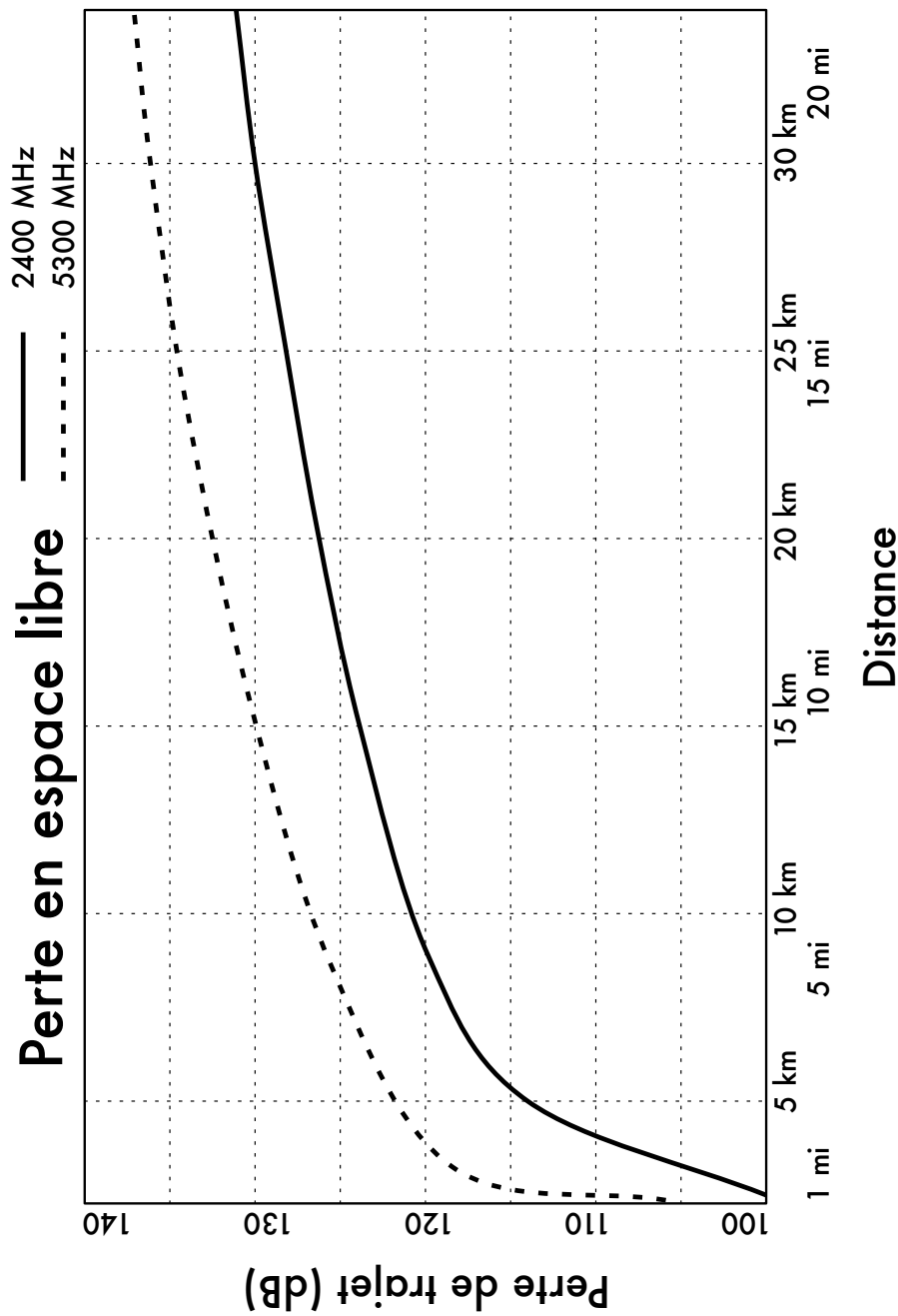
Les tableaux suivants présentent le numéro des canaux et les fréquences centrales utilisées pour les standards 802.11a et 802.11b/g. Notez que même si toutes ces fréquences sont dans les bandes sans licence ISM et U-NII, tous les canaux ne sont pas disponibles dans tous les pays. Plusieurs régions imposent 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

Annexe C: Perte de trajet



Annexe D: Tailles des câbles

AWG, diamètre, capacité d'intensité, et résistance à 20 ° C. Ces valeurs peuvent varier d'un câble à câble. En cas de doute, consulter les spécifications du fabricant.

Jauge AWG	Diamètre (mm)	Ohms / Mètre	Ampères Maximum
0000	11,68	0,000161	302
000	10,40	0,000203	239
00	9,27	0,000256	190
0	8,25	0,000322	150
1	7,35	0,000406	119
2	6,54	0,000513	94
3	5,83	0,000646	75
4	5,19	0,000815	60
5	4,62	0,001028	47
6	4,11	0,001296	37
7	3,67	0,001634	30
8	3,26	0,002060	24
9	2,91	0,002598	19
10	2,59	0,003276	15

Annexe E: Dimensionnement solaire

Utilisez ces tables pour recueillir les données nécessaires pour estimer la taille requise de votre système d'énergie solaire.

Données générales

Nom du site	
Latitude du site (°)	

Données d'irradiation

$G_{dm}(0)$, en kWh / m^2 par jour

Jan	Fev	Mar	Avr	Mai	Juin	Juil	Août	Sep	Oct	Nov	Déc

Le mois de pire irradiation	

Fiabilité et tension opérationnelle du système

Jours d'autonomie (N)	
Tension nominale (V_{NEquip})	

Caractéristiques des composants

Panneaux solaires	
Tension @ puissance maximale (V_{pmax})	
Intensité @ puissance maximale (I_{pmax})	
Type de panneau / modèle et puissance (W_p)	

Batteries	
Capacité nominale @ 100 H (C_{NBat})	
Tension nominale (V_{NBat})	
Profondeur maximale de décharge (DoD_{MAX}) ou capacité utilisable (C_{UBat})	

Régulateur	
Tension nominale (V_{NReg})	
Intensité maximum (I_{maxReg})	

Convertisseur DC/AC (si nécessaire)	
Tension nominale (V_{NConv})	
Puissance instantanée (P_{IConv})	
Performance @ 70% de charge	

Charges

Estimation de l'énergie consommée par les charges (DC)				
Mois de plus grande consommation				
Description	# d'unités	x Puissance Nominale	x Usage Heures / jour	= Energie (Wh / jour)
E_{TOTAL} DC				

Estimation de l'énergie consommée par les charges (AC)				
Mois de plus grande consommation				
Description	# d'unités	x Puissance Nominale	x Usage Heures / jour	= Energie (Wh / jour)
E_{TOTAL} AC (avant le convertisseur)				
E_{TOTAL} AC (après le convertisseur) = E_{TOTAL} AC / 70%				

Trouver le pire des mois

Nom du site												
Latitude du site (°)												
Tension nominale de l'installation V_N												
(Mois)	J	F	M	A	M	J	J	A	S	O	N	D
Inclinaison ß												
G_{dm} (ß) (kWh/m² × jour)												
E_{TOTAL} (DC) (Wh/jour)												
E_{TOTAL} (AC) (Wh/jour)												
E_{TOTAL} (AC + DC)=												
I_m (A) = E_{TOTAL} (Wh/jour) × 1kW/m²/ (G_{dm}(ß) x V_N)												

Résumé du pire des mois	
Le pire des mois	
I_m (A)	
I_{mMAX} (A) = 1.21 x I_m	
E_{TOTAL} (AC + DC)	

Les calculs finaux

Panneaux		
Panneaux en série (N_{PS})	$N_{PS} = V_N / V_{Pmax} =$	
Panneaux en parallèle (N_{PP})	$N_{PP} = I_{mMAX} / I_{Pmax} =$	
Nombre total de panneaux	$N_{TOT} = N_{PS} \times N_{PP} =$	

Batteries		
Capacité nécessaire (C_{NEC})	E_{TOTAL}(le pire des mois) / V_N x N	
Capacité nominale (C_{NOM})	C_{NEC} / DoD_{MAX}	
Nombre de batteries en série (N_{BS})	V_N / V_{NBAT}	

Câbles			
	Panneaux > Batteries	Batteries > Convertisseur	Ligne principale
Chute de tension ($V_a - V_b$)			
Epaisseur (Section) $r \times L \times I_{mMAX} / (V_a - V_b)$			

Pour le calcul d'épaisseur du câble, r = 0,01286 Ω mm²/m (pour le cuivre) et L est la longueur en mètres.

Glossaire

0–9

802.11. Alors que 802.11 est un protocole sans fil de plein droit, il est souvent utilisé pour designer une famille de protocoles utilisée principalement pour les réseaux locaux sans fil. Les trois variantes populaires de cette famille de protocoles comprennent 802.11b, 802.11g et 802.11a. Voir aussi: ***Wi-Fi***.

A

AC. voir ***courant alternatif***.

Accumulateur. Un autre nom pour une ***batterie***.

adresse de diffusion. Dans les réseaux IP, l'adresse de diffusion est utilisée pour envoyer des données à tous les hôtes dans le sous réseau local. Dans les réseaux Ethernet, l'adresse MAC de diffusion est utilisée pour envoyer des données à toutes les machines dans le même domaine de collision.

adresse MAC. Un nombre unique de 48 bits attribué à chaque dispositif réseau quand il est fabriqué. L'adresse MAC est utilisée pour les communications liaison locale.

adresse réseau. La plus petite adresse IP dans un sous réseau. L'adresse de réseau est utilisée dans les tables de routage pour spécifier la destination à être utilisée lors de l'envoi de paquets vers un groupe logique d'adresses IP.

advertised window. La partie d'une entête TCP qui spécifie le nombre supplémentaire d'octets de données que le récepteur est prêt à accepter.

ajustement de fenêtre (window scale). Une amélioration de TCP définie par le RFC1323 permettant des tailles de fenêtre TCP de plus de 64 ko.

amortissement. Une technique comptable utilisée pour gérer le coût de remplacement et de l'obsolescence de l'équipement au fil du temps.

amplificateur. Un dispositif utilisé pour augmenter la puissance transmise d'un dispositif sans fil.

amplitude. La distance du milieu d'une onde à l'extrême de l'un de ses sommets.

analyseur de protocole. Un programme de diagnostic utilisé pour observer et désassembler des paquets d'un réseau. Les analyseurs de protocole fournissent le plus grand détail possible sur les différents paquets.

analyseur de spectre. Un dispositif qui fournit une représentation visuelle du spectre électromagnétique. Voir aussi: ***Wi-Spy***

anonymat. Dans les réseaux informatiques, les communications qui ne peuvent pas être liées à un individu unique sont traitées d'anonymes. Le choix entre l'anonymat et la responsabilité dans les communications est un débat en cours, et les règles sur les communications anonymes varient largement dans le monde entier. Voir aussi: ***authentifié***

antenne dipôle. Le modèle le plus simple d'antenne omnidirectionnelle.

antenne directionnelle. Une antenne qui rayonne très fortement dans une direction particulière. Les exemples d'antennes directionnelles comprennent l'antenne Yagi, l'antenne plate et les antennes de guides d'ondes. Voir aussi: ***antenne sectorielle***, ***antenne omnidirectionnelle***.

antenne isotrope. Une antenne hypothétique qui distribue sa puissance de façon uniforme dans toutes les directions. Elle est approximée par un dipôle.

antenne sectorielle. Une antenne qui rayonne principalement dans une région spécifique. Le faisceau peut être aussi large que 180 degrés, ou aussi étroit que 60 degrés. Voir aussi: ***antenne directionnelle, antenne omnidirectionnelle***

antenne omnidirectionnelle. Une antenne qui rayonne à peu près également dans toutes les directions dans le plan horizontal. Voir aussi: ***antenne directionnelle, antenne sectorielle***.

AP voir ***point d'accès***.

Argus voir ***Audit Record Generation and Utilization System***.

ARP Voir ***Address Resolution Protocol***.

association. Une radio 802.11 radio est associée à un point d'accès quand elle est prête à communiquer avec le réseau. Cela signifie qu'elle est réglée au bon canal, est à portée du point d'accès, et utilise le SSID correct et d'autres paramètres d'authentification, etc.

atténuation. La réduction de la puissance disponible de la radio quand elle absorbée le long d'une ligne, comme à travers les arbres, les murs, les bâtiments, ou d'autres objets. Voir aussi: ***perte en espace libre, dispersion***.

at. Un utilitaire Unix qui permet l'exécution chronométrée, spontanée des programmes. Voir aussi: ***cron***.

Audit Record Generation and Utilization System (Argus). Un outil libre de surveillance réseau utilisé pour le suivi des flux entre les hôtes. Argus est disponible à partir de *http://www.qosient.com/argus*.

authentifié. Un utilisateur du réseau qui a prouvé son identité à un service ou un périphérique (comme un point d'accès) sans l'ombre d'un doute, le plus souvent par des moyens cryptographiques. Voir aussi: ***anonymat***.

Azimut. L'angle qui mesure la déviation par rapport au sud dans l'hémisphère nord, et la déviation par rapport au nord dans l'hémisphère sud. Voir aussi: ***inclinaison***.

B

bail. Dans DHCP, les adresses IP sont attribuées pour une période de temps limitée, connue sous le nom bail ou temps d'allocation. Quand ce délai expire, les clients doivent demander une nouvelle adresse IP au serveur DHCP.

Bande ISM. ISM est l'Abréviation d'industriel, Scientifique et médical. La bande ISM est un ensemble de fréquences radio mis de coté par l'UIT pour l'usage libre.

bande passante. Une mesure de gammes de fréquences, généralement utilisée pour les communications numériques. Le terme bande passante est également couramment utilisé de façon interchangeable avec la capacité pour se référer à un débit de données maximal théorique d'une ligne de communication numérique. Voir aussi: ***capacité***, ***canal***, ***débit***.

Base de données Round Robin (DRR). Une base de données qui stocke les informations d'une manière très compacte de façon à ne pas s'étendre au fil du temps. C'est le format de données utilisé par RRDTool et d'autres outils de surveillance réseau.

batterie. Un dispositif utilisé pour le stockage de l'énergie dans un système photovoltaïque. Voir aussi: ***panneau solaire***, ***régulateur de charge***, ***convertisseur***, ***onduleur***.

batterie au plomb-acide à régulation par soupape (VRLA, Valve Regulated Lead Acid) voir ***batteries au plomb acide***.

Batteries au plomb acide sans entretien voir ***batteries au plomb acide***.

batteries de traction voir ***batteries au plomb acide***.

batteries au plomb acide. Batteries composée de deux électrodes en plomb immergé dans une solution électrolytique de l'eau et d'acide sulfurique. Voir aussi: ***batteries à recombinaison***.

Batteries à recombinaison voir ***batteries au plomb acide***.

batteries stationnaires. Les batteries destinées pour un emplacement fixe et à être utilisées dans les scénarios où la consommation d'énergie est plus ou moins irrégulière. Les batteries stationnaires peuvent avoir des cycles de décharge profonde mais elles ne sont pas conçues pour produire des courants élevés dans de brèves périodes de temps. Voir aussi: ***batteries au plomb acide***.

BGAN voir ***Broadband Global Acces Network***.

bien connu. Dans le dépannage, le bien connu est un composant qui peut être substitue pour vérifier que son homologue est en bon état de fonctionnement.

bilan de liaison (link budget). La quantité d'énergie radio disponible pour surmonter les pertes liaison. La communication devrait être possible si le bilan est supérieur à la perte liaison, la sensibilité minimale de la radio de réception et les obstacles.

boucles de redirection. Une configuration de routage erronée où les paquets sont redirigés cycliquement entre deux ou plusieurs routeurs. La défaillance catastrophique du réseau est évitée en utilisant la valeur TTL sur tous les paquets, mais la transmission des boucles doit être réglée pour une bonne exploitation du réseau.

bridge-utils. Un logiciel Linux qui est nécessaire pour créer des ponts Ethernet 802.1d. *http://bridge.sourceforge.net/*

bridge. Un appareil réseau qui relie deux réseaux au niveau de la couche liaison de données. Les bridges ne font pas de routage de paquets au niveau de la couche réseau. Ils ne font que répéter les paquets entre deux réseaux à liaisons locales. Voir aussi: ***routeur*** et ***transparent bridging firewall***.

Broadband Global Access Network (BGAN). Un des nombreux standards utilisés pour l'accès Internet par satellite. Voir aussi: ***Digital Video Broadcast (DVB-S)*** et ***Very Small Aperture Terminal (VSAT)***.

C

cache DNS. En installant un serveur DNS sur votre réseau local, les requêtes DNS pour l'ensemble d'un réseau peuvent être mis en cache localement afin d'améliorer les temps de réponse. Cette technique est appelée e cache DNS.

cache transparent. Une méthode de mise en œuvre d'un cache de site web qui ne requiert pas de configuration sur les clients web. Les demandes Web sont redirigés en silence vers la mémoire cache qui fait la demande au nom du client. Les caches transparents ne peuvent pas utiliser l'authentification. Ce qui rend impossible à mettre en œuvre la comptabilité du trafic au niveau utilisateur. Voir aussi: ***cache de site web***, ***Squid***.

Cacti (*http://www.cacti.net/*). Un outil de surveillance basé web écrit en PHP.

canal. Une gamme de fréquences bien définie utilisée pour les communications. Les canaux 802.11 utilisent 22 MHz de bande passante, mais sont séparés par seulement 5 MHz. Voir aussi: ***Annexe B***.

capacité du canal. Le montant maximum d'informations qui peut être envoyé en utilisant une bande passante donnée. Voir aussi: ***bande passante***, ***débit***, ***débit de données***.

capacité. Le trafic théorique maximal fourni par une ligne de communication numérique. La capacité est souvent utilisée de façon interchangeable avec la bande passante.

Capacité nominale (C_N). Le montant maximal de l'énergie qui peut être extraite d'une batterie entièrement chargée. Elle est exprimée en ampères-heures (Ah) ou Watt-heure (Wh).

Capacité utile (C_U). La charge utile d'une batterie. Elle est égale au produit de la capacité nominale et la profondeur maximale de la décharge.

Carte d'élévation numérique (DEM). Les données qui représentent la hauteur du terrain pour une location géographique donnée. Ces cartes sont utilisées par des logiciels tels que Radio Mobile pour modéliser la propagation électromagnétique.

CA voir ***Certificate Authority***.

cellule. Les panneaux solaires sont constitués de plusieurs cellules individuelles reliées électriquement pour fournir une valeur d'intensité et de tension donnée. Les batteries sont également composées de cellules individuelles connectées en série, chacune d'elle contribuant pour environ 2 volts à la tension de la batterie.

Certificate Authority. Une entité de confiance qui émet les clés cryptographiques. Appelée aussi ***Autorité de Certification*** en français. Voir aussi: ***Public Key Infrastructure***, ***SSL***.

charge. Matériel qui consomme de l'énergie dans un système photovoltaïque. Voir aussi: ***batterie***, ***panneaux solaires***, ***régulateur***, ***convertisseur***, ***onduleur***.

Cible (target). l'action à prendre dans netfilter une fois qu'un paquet correspond à une règle. Certaines cibles netfilter possibles sont ACCEPT, DROP, LOG, et REJECT.

CIDR voir ***Classless Inter-Domain Routing***.

Classless Inter-Domain Routing. CIDR a été développé pour améliorer l'efficacité du routage sur la dorsale Internet en permettant l'agrégation du routage et des masques de réseau de taille arbitraire. Le CIDR remplace l'ancien schéma d'adressage à base de classes. Voir aussi: ***réseaux de Classe A, B, C***.

Clients affermis (anchor clients). Les clients d'un système d'abonnement qui sont fiables et peuvent être considérés comme à faible risque.

client. Une carte radio 802.11 en mode géré. Les clients sans fil joindront un réseau créé par un point d'accès, et automatiquement changent de canal pour lui correspondre. Voir aussi: ***point d'accès, maillage***.

coaxial. Un câble rond (coaxial) avec un fil central entouré par un diélectrique, un conducteur extérieur, et une gaine isolante dure. Les câbles d'antenne sont généralement composés de câbles coaxiaux. Coaxial est une abréviation pour "d'axe commun".

code électromagnétique numérique (NEC2). Un logiciel de modélisation d'antenne gratuit qui vous permet de créer une antenne dans le modèle 3D et ensuite analyser sa réponse électromagnétique. *http://www.nec2.org/*

collision. Sur un réseau Ethernet, une collision se produit lorsque deux périphériques connectés au même segment physique essaient de transmettre en même temps. Lorsque des collisions sont détectées, les dispositifs retardent leur retransmission pour une courte période choisie au hasard.

commutateur (ou ***switch***). Un appareil réseau qui fournit une connexion dédiée temporaire entre les dispositifs communiquant. Voir aussi: ***hub***.

compteurs de ports. Les commutateurs et routeurs gérés fournissent des statistiques pour chaque port réseau appelés compteurs de ports. Ces statistiques peuvent inclure les paquets entrants et sortants, les octets, de même que les erreurs et les retransmissions.

condition de correspondance. Dans netfilter, une condition de correspondance définit les critères qui déterminent la destination ultime d'un paquet. Les paquets peuvent être comparés sur base de l'adresse MAC, l'adresse IP source ou destination, numéro de port, le contenu des données, ou une autre propriété.

conducteur. Un matériel qui permet le flux de l'énergie électrique ou thermique sans beaucoup de résistance. Voir aussi: ***diélectrique***, ***isolant***.

connecteur BNC. Un connecteur de câble coaxial qui se sert d'une baïonnette de type "connexion rapide". Les connecteurs BNC sont généralement disponibles sur les câbles coaxiaux de type 10base2.

connecteur N. Un connecteur micro-onde robuste qu'on trouve couramment sur les composants réseau de plein air, telles que les antennes et les points d'accès extérieur.

connecteur TNC. Un connecteur micro-onde fileté, robuste et commun.

contrôles. Dans le NEC2, les contrôles déterminent la source RF dans un schéma d'antenne. Voir aussi: ***structure***.

conversion par commutation. Une méthode de conversion de tension DC qui utilise un composant magnétique pour stocker temporairement l'énergie et la transformer en une autre tension. La conversion de commutation est beaucoup plus efficace que la conversion linéaire. Voir aussi: ***conversion linéaire***.

conversion linéaire. Une méthode de conversion de tension qui abaisse la tension

en convertissant l'excès énergétique en chaleur. Voir aussi: ***conversion par commutation***.

convertisseur DC/AC. Un dispositif qui convertit la tension DC en tension AC qui est plus convenable pour de nombreux appareils. Également connu sous le nom d'**onduleur**.

convertisseur DC/DC. Un dispositif qui modifie la tension d'une source d'alimentation DC. Voir aussi: ***conversion linéaire***, ***conversion par commutation***.

convertisseur. Un appareil utilisé pour convertir les signaux DC en signaux DC ou AC de tension différente. Voir aussi: ***onduleur***.

coordonnées polaires linéaires. Un système graphique avec des cercles concentriques gradués et également espacés, représentant une valeur absolue sur une projection polaire. Ces graphiques sont généralement utilisés pour représenter les caractéristiques de rayonnement d'antenne. Voir aussi: ***coordonnées polaires logarithmiques***.

coordonnées polaires logarithmiques. Un système graphique avec des cercles concentriques gradués et également espacés, représentant une valeur absolue sur une projection polaire. Ces graphiques sont généralement utilisés pour représenter les caractéristiques de rayonnement d'antenne. Voir aussi: ***coordonnées polaires linéaires***.

couche application. La couche la plus haute dans les modèles de réseau OSI et TCP/IP.

couche Internet voir ***couche réseau***.

couche liaison de données. La deuxième couche présente à la fois dans les modèles OSI et TCP/IP. Dans cette couche, les communications se produisent directement entre les noeuds. Sur les réseaux Ethernet, elle est aussi parfois appelée la couche MAC.

couche MAC voir ***couche liaison de données***.

couche Media Access Control voir ***couche liaison de données***.

couche physique. La couche inférieure à la fois dans les modèles OSI et TCP/IP. La couche physique est le support concret utilisé pour les communications, tels que le câble en cuivre, la fibre optique, ou les ondes radio.

couche présentation. La sixième couche du modèle de réseau OSI. Cette couche s'occupe de la représentation des données, telles que l'encodage MIME ou la compression de données.

couche réseau. Également appelée couche Internet. Il s'agit de la troisième couche des modèles OSI et TCP/IP, où opère IP et le routage Internet a lieu.

couche session. Cinquième couche du modèle OSI. La couche session logique gère les connexions entre les applications.

couche transport. La troisième couche des modèles OSI et TCP/IP, qui fournit une méthode permettant d'atteindre un service particulier sur un noeud du réseau. Des exemples de protocoles qui fonctionnent à cette couche sont TCP et UDP.

Courant Alternatif (AC). Un courant électrique qui varie dans le temps d'une manière cyclique. Le courant alternatif est généralement utilisé pour l'éclairage et les appareils. Voir aussi: ***Courant Continu (DC)***.

Courant Continu (DC). Un courant électrique qui reste constant dans le temps. Le courant continu est généralement utilisé pour des équipements de réseau, tels que les points d'accès et routeurs. Voir aussi: ***Courant Alternatif***.

courbe caractéristique IV. Un graphique représentant le courant qui est fourni en fonction de la tension générée pour une certaine radiation solaire.

cron. Un utilitaire sous Unix qui permet une exécution chronométrée et répétitive des programmes. Voir aussi: ***at***.

Cryptographie à clé publique (Public Key Cryptography). Une forme de cryptage utilisée par le protocole SSL, SSH, et les autres programmes populaires de sécurité. La cryptographie à clé publique, parfois appelée aussi cryptographie asymétrique, permet l'échange d'informations sur un réseau non sécurisé sans la nécessité de distribuer une clé secrète.

D

dB voir ***Décibel***.

DC voir ***Courant Continu***.

débit de données. La vitesse à laquelle les radios 802.11 échangent des symboles, qui est toujours plus élevé que le débit

disponible. Par exemple, le débit nominal de données de la norme 802.11g est de 54 Mbits/s tandis que le débit maximum est d'environ 20 Mbps. Voir aussi: ***débit***.

débit. La quantité réelle d'information par seconde traversant une connexion réseau, sans tenir compte de surcharges de protocole.

décalage de polarisation. Un état où une antenne de transmission et celle de réception n'utilisent pas la même polarisation, résultant en une perte de signal.

Décalage (lag). Terme utilisé pour décrire un réseau à forte latence.

décibels (dB). Une unité de mesure logarithmique qui exprime l'ampleur de l'énergie par rapport à un niveau de référence. Les unités couramment utilisées sont le dBi (décibels par rapport à un radiateur isotrope) et le dBm (décibels par rapport à un milliwatt).

déconfiture ou effondrement (Thrashing). L'état ou un ordinateur a épuisé la mémoire RAM disponible et doit utiliser le disque dur pour le stockage temporaire, ce qui réduit grandement les performances du système.

Déni de service (DoS). Une attaque sur les ressources du réseau, généralement par inondation d'un réseau avec du trafic ou l'exploitation d'un bug dans une application ou un protocole de réseau.

Dépréciation. Une méthode comptable utilisée pour économiser de l'argent pour couvrir une éventuelle rupture des équipements.

Détection réseau. Outils de diagnostic réseau qui permettent d'afficher des informations sur les réseaux sans fil, tels que le nom de réseau, canal, et la méthode de cryptage utilisée.

DHCP voir ***Dynamic Host Configuration Protocol***.

Diagramme d'antenne (antenna pattern). Un graphique qui décrit la force relative d'un champ de radiation dans différentes directions à partir d'une antenne. Voir aussi: ***diagramme rectangulaire***, ***diagramme polaire***, ***coordonnées linéaire polaires***, ***coordonnées logarithmique polaires***.

diélectrique. Un matériau non-conducteur qui sépare les fils conducteurs a l'intérieur d'un câble.

Digital Video Broadcast (DVB-S). Un des nombreux standards utilisés pour l'accès Internet par satellite. Voir aussi: ***Broadband Global Access Network (BGAN)*** et ***Very Small Aperture Terminal (VSAT)***.

diodes de dérivation. Une fonctionnalité qu'on trouve sur certains panneaux solaires qui empêche la formation de points chauds sur les cellules dans l'ombre, mais réduit la tension maximale du panneau.

directivité. La capacité d'une antenne à concentrer l'énergie dans une direction lors de la transmission, ou de recevoir de l'énergie à partir d'une direction lors de la réception.

Direct Sequence Spread Spectrum DSSS (étalement de spectre à séquence directe). Un schéma de modulation radio utilisé par la norme 802.11b.

Diversité d'antenne. Une technique utilisée pour surmonter les multiples interférences en utilisant deux ou plusieurs antennes de réception séparées physiquement.

diversité voir ***diversité d'antenne***.

dnsmasq. Un serveur cache DNS et DHCP libre, disponible à partir de *http://thekelleys.org.uk/*.

DNS voir ***Domain Name Service***.

Domain Name Service (DNS). Le protocole le plus largement utilisé pour faire correspondre les adresses IP à des noms.

DoS voir ***déni de service***.

DSSS voir ***Direct Sequence Spread Spectrum (étalement de spectre à séquence directe)***.

DVB-S voir ***Digital Video Broadcast***.

Dynamic Host Configuration Protocole (DHCP). Un protocole utilisé par les hôtes pour déterminer automatiquement leurs adresses IP.

E

écoute. Les programmes qui acceptent les connexions sur un port TCP sont dit être à l'écoute sur ce port.

élévation voir ***inclinaison***.

transmetteur vidéo (***video sender***). Un émetteur vidéo de 2,4 GH qui peut être

utilisé comme un générateur de signaux peu coûteux.

encryptage bout à bout. Une connexion cryptée négociée par les deux extrémités d'une session de communication. Quand il est utilisé sur des réseaux non sécurisés (tels que l'Internet), l'encryptage bout à bout peut fournir une meilleure protection que la couche de liaison.

encryptage de la couche liaison. Une connexion encryptée entre les dispositifs liaison locale, typiquement un client sans fil et un point d'accès. Voir aussi: ***encryptage bout à bout***.

énergie solaire photovoltaïque. Le recours à des panneaux solaires pour collecter l'énergie solaire pour produire de l'électricité. Voir aussi: ***énergie solaire thermique***.

énergie solaire thermique. Energie recueillie à partir du soleil sous forme de chaleur. Voir aussi: ***énergie solaire photovoltaïque***.

CPE, Client Premises Equipment. Un équipement réseau (comme un routeur ou passerelle) qui est installé à un emplacement client.

espace d'adressage privé. Un ensemble d'adresses IP réservés indiqué dans RFC1918. L'espace d'adressage privé est fréquemment utilisé au sein d'un organisme en liaison avec la translation d'adresses réseau (NAT). L'espace d'adressage privé réservé inclut 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16. Voir aussi: ***NAT***.

espace d'adressage. Un groupe d'adresses IP qui résident tous dans le même sous réseau logique.

espion. Quelqu'un qui intercepte les données du réseau comme les mots de passe, e-mail, données vocales, ou les chat en ligne.

ET logique. Une opération logique qui s'évalue comme vraie si tous les éléments faisant l'objet d'une comparaison s'évaluent aussi comme vrai. Voir aussi: ***OU logique***.

étalonnage (benchmarking). Evaluation de la performance maximale d'un service ou un périphérique. Etalonner une connexion réseau implique généralement une inondation de la liaison par du trafic et une mesure du débit réel observé, à la fois à la transmission et la réception.

état de charge (SOC, State of Charge). La charge actuelle d'une batterie déterminée par la tension et le type de batterie.

EtherApe. Un outil de visualisation réseau libre. Disponible sur *http://etherape.sourceforge.net/*.

Ethereal voir ***Wireshark***.

Extended Service Set Identifier (ESSID). Le nom utilisé pour un identificateur de réseau 802.11. Voir aussi: ***réseau fermé***.

F

filter. La table par défaut utilisée par le système pare-feu Linux netfilter. Cette table est utilisée pour la détermination du trafic qui doit être accepté ou refusé.

filtrage MAC. Une méthode de contrôle d'accès basée sur l'adresse MAC de dispositifs de communication.

filtre de paquet (packet filter). Un pare-feu qui fonctionne sur la couche Internet en inspectant la source et destination des adresses IP, les numéros de port, et les protocoles. Les paquets sont soit autorisés ou rejetés selon les règles de filtrage de paquets.

firestarter. Une interface graphique pour la configuration des pare-feux Linux. Il est disponible à partir de *http://www.fs-security.com/*.

flush. Pour supprimer toutes les entrées dans une table de routage ou une chaîne netfilter.

frauder (spoof). Emprunter l'identité d'un périphérique réseau, un utilisateur ou un service.

fréquence. Le nombre d'ondes complètes qui traversent un point fixé au cours d'une période de temps. Voir aussi: ***longueur d'onde***, ***Hertz***.

front-to-back ratio. Le rapport de la directivité maximale d'une antenne à sa directivité dans la direction opposée.

full duplex. Matériel de communication qui permet d'envoyer et de recevoir en même temps (comme un téléphone). Voir aussi: ***half duplex***.

fusible retardé. Un fusible qui permet à un courant plus élevé que son seuil de passer pour un court laps de temps. Voir aussi: ***fusible rapide***.

fusible rapide. Un type de fusible qui saute immédiatement si le courant est plus élevé que son seuil. Voir aussi: ***fusible retardé***.

fwbuilder. Un outil graphique qui vous permet de créer des scripts iptables sur une machine distincte de votre serveur, puis de les transférer sur le serveur plus tard. *http://www.fwbuilder.org/*.

G

Gain d'antenne. La puissance concentrée dans le sens de la plus grande radiation d'une antenne, généralement exprimée en dBi. Le gain d'antenne est réciproque, ce qui signifie que l'effet de gain est présent lors de la transmission ainsi que la réception.

gain. La capacité d'un composant radio (tel qu'une antenne ou amplificateur) pour augmenter la puissance d'un signal. Voir aussi: ***Decibel***.

gazéification. La production de bulles d'oxygène et d'hydrogène qui se produit quand une batterie est surchargée.

générateur de signaux. Un émetteur qui émet continuellement à une fréquence spécifique.

générateur photovoltaïque voir ***panneaux solaires***.

H

half duplex. Matériel de communication qui peut envoyer ou recevoir, mais jamais les deux à la fois (comme une radio portable). Voir aussi: ***full duplex***.

Heliax. Un câble coaxial de haute qualité qui a un conducteur solide ou à centre tubulaire avec un conducteur extérieur solide ondulé qui lui permet de fléchir. Voir aussi: ***câble coaxial***

Hertz (Hz). Une mesure de ***fréquence*** dénotant un certain nombre de cycles par seconde.

Heures d'équivalent plein soleil (PSH, Pic Sun Hours). Valeur moyenne quotidienne de l'irradiation pour une zone donnée.

HF (High Frequency). Les ondes radio de 3 à 30 MHz sont appelées HF. Les réseaux de données construits sur HF peuvent fonctionner à très longue portée, mais avec une très faible capacité.

hop. Les données qui traversent une connexion réseau. Un serveur web peut être à plusieurs hops de votre ordinateur local car les paquets sont transmis de routeur à routeur pour éventuellement atteindre leur destination finale.

hotspot. Un endroit qui donne l'accès Internet par Wi-Fi, généralement au moyen d'un portail captif.

hub. Un dispositif réseau Ethernet qui réplique toutes les données reçues sur tous les ports connectés. Voir aussi: ***commutateur***.

Hz voir ***Hertz***

I

IANA voir ***Internet Assigned Numbers Authority***.

ICMP voir ***Internet Control Message Protocol***.

ICP voir ***Inter-Cache Protocol***.

impédance. Le quotient de la tension sur le courant d'une ligne de transmission constituée d'une résistance et une réactance. L'Impédance de charge doit correspondre à l'Impédance de source pour obtenir un transfert de puissance maximum (50Ω Pour la plupart du matériel de communication).

inclinaison. L'angle qui marque l'écart par rapport à un plan horizontal. Voir aussi: ***azimut***.

Infrastructure à clé publique (PKI, Public Key Infrastructure). Un mécanisme de sécurité utilisé en conjonction avec la cryptographie à clé publique pour empêcher la possibilité des attaques Man-In-The-Middle. Voir aussi: ***certificate authority***.

injecteur POE passif voir ***Power over Ethernet***.

injecteur end span. Un dispositif 802.3af POE qui fournit de l'électricité via le câble Ethernet. Un commutateur Ethernet qui fournit de l'électricité sur chaque port est un exemple d'un injecteur end span. Voir aussi: ***injecteur mid span***.

injecteur mid span. Un dispositif Power over Ethernet inséré entre un commutateur Ethernet et le dispositif destiné à être alimenté. Voir aussi: ***injecteurs end span.***

Inter-Cache Protocol (ICP). Un protocole de haute performance utilisé pour les communications entre caches Web.

interférence constructive. Lorsque deux ondes identiques fusionnent et sont en phase, l'amplitude de l'onde résultante est le double de celle de l'une des composantes. C'est ce qu'on appelle l'interférence constructive. Voir aussi: ***interférence destructive***.

Interférence destructive. Lorsque deux ondes identiques fusionnent et sont exactement en opposition de phase, l'amplitude de l'onde résultante est égale à zéro. C'est ce qu'on appelle Interférence destructrice. Voir aussi: ***interférence constructive***.

Internet Assigned Numbers Authority (IANA). L'organisme qui administre les diverses parties critiques de l'infrastructure d'Internet, y compris l'attribution des adresses IP, les serveurs de noms racine, et les numéros des services des protocoles.

Internet Control Message Protocol (ICMP). Un protocole de couche réseau utilisé pour informer les noeuds sur l'état du réseau. ICMP est une partie de la suite de protocoles Internet. Voir aussi: ***Internet protocol suite***.

Internet protocol suite (TCP/IP) (Suite de protocoles Internet). La famille de protocoles de communication qui composent l'Internet. Certains de ces protocoles comprennent TCP, IP, ICMP, UDP etc. Également appelée la ***suite de protocoles TCP/IP***, ou tout simplement ***TCP/IP***.

IP (Internet Protocol). Le protocole de la couche réseau le plus connu. IP définit les hôtes et les réseaux qui constituent l'Internet global.

iproute2. Les outils avancés de routage de Linux utilisés pour l'ajustage du trafic (traffic shaping) et d'autres techniques avancées. Disponible à partir de *http://linux-net.osdl.org/*

iptables. La commande de base utilisée pour manipuler les règles pare-feu ***netfilter***.

IP voir ***Internet Protocol***.

irradiance. Le montant total de l'énergie solaire qui éclaire une zone donnée, en W/m^2.

Isolant voir ***diélectrique***.

K

knetfilter. Une interface graphique pour configurer les pare-feux Linux. Disponible à partir de *http://venom.oltrelinux.com/*.

L

lambda (λ) voir ***longueur d'onde***.

LAN voir ***Local Area Network***.

largeur de faisceau. La distance angulaire entre les points de chaque côté du lobe principal d'une antenne où la puissance reçue est la moitié de celle du lobe principal. La largeur de faisceau d'une antenne est généralement indiquée à la fois pour les plans horizontaux et verticaux.

latence. Le temps qu'il faut pour un paquet pour traverser une connexion réseau. Elle est souvent faussement utilisée de façon interchangeable avec Round Trip Time (RTT), car la mesure de la RTT d'une connexion à longue distance est triviale par rapport à la mesure de la latence réelle. Voir aussi: ***Round Trip Time***.

liaison locale. Les périphériques réseau qui sont connectés au même segment physique et communiquent les uns avec les autres directement sont en liaison locale. Une liaison locale ne peut pas traverser les limites d'un routeur sans utiliser un type d'encapsulation comme un ***tunnel*** ou un ***VPN***.

ligne de transmission RF. La connexion (généralement coaxial, Heliax, ou un guide d'onde) entre une radio et une antenne.

Ligne de visée (LOS, Line of Sight). Si un personne debout en un point A a une vue dégagée du point B, alors le point A a une ligne de visée claire au point B.

lobes latéraux. Aucune antenne n'est en mesure de rayonner toute l'énergie dans une direction préférée. Une partie de cette énergie est rayonnée inévitablement dans d'autres directions. Ces petits pics sont considérés comme des lobes latéraux.

Local Area Network (LAN). Un réseau (Ethernet en général) utilisé au sein d'un organisme. La partie d'un réseau qui existe juste derrière un routeur du fournisseur d'accès est généralement considéré comme faisant partie du réseau local. Voir aussi: ***WAN***.

longueur d'onde. La distance mesurée à partir d'un point d'une onde à la partie équivalente sur la suivante, par exemple a partir du haut d'une crête à l'autre. Aussi appelé lambda (λ).

LOS voir ***Ligne de visée***.

M

maillage. Un réseau sans hiérarchisation où chaque noeud sur le réseau porte le trafic de tous les autres en cas de besoin. Les bonnes implémentations des réseaux maillés sont autoréparables. Ce qui signifie qu'elles peuvent détecter les problèmes de routage et les fixer en cas de besoin.

Man-In-The-Middle (MITM). Une attaque de réseau ou un utilisateur malveillant intercepte toutes les communications entre un client et un serveur, permettant l'information à être copiée ou modifiée.

masque de réseau voir ***netmask***.

masque de sous-réseau (subnet mask) voir ***masque de réseau (netmask)***.

matériel géré. Un matériel réseau qui fournit une interface d'administration, des compteurs de port, SNMP, ou d'autres éléments interactifs est dit géré.

matrice de panneaux solaires. Un ensemble de panneaux solaires câblés en série et/ou en parallèle afin de fournir l'énergie nécessaire pour une charge donnée.

MC-Card. Un très petit connecteur micro-onde trouvé sur le matériel Lucent / Orinoco / Avaya.

méthode des pires mois. Une méthode de calcul des dimensions d'un système photovoltaïque autonome de sorte qu'il fonctionne dans le mois au cours duquel la demande d'énergie est plus grande par rapport à l'énergie solaire disponible. C'est le pire des mois de l'année car c'est le mois ayant le plus grand ratio entre l'énergie demandée et l'énergie disponible.

MHF voir ***U.FL***.

microfinance. La mise à disposition de petits prêts, d'épargne et autres services financiers aux gens les plus pauvres du monde.

milliwatts (mW). Une unité de puissance représentant un millième de Watt.

MITM voir ***Man-In-The-Middle***.

MMCX. Un très petit connecteur micro-onde qu'on trouve couramment sur les équipements fabriqués par Senao et Cisco.

Mode ad hoc. Un mode radio utilisé par les dispositifs 802.11. Il permet la création d'un réseau sans un point d'accès. Les réseaux maillés utilisent souvent des radios en mode ad hoc. Voir aussi: ***mode de gestion***, ***mode maître***, ***mode moniteur***.

mode dominant. La fréquence la plus basse qui peut être transmise par une guide d'ondes d'une taille donnée.

mode géré. Un mode radio utilisé par les dispositifs 802.11 qui permet à la radio à se joindre à un réseau créé par un point d'accès. Voir aussi: ***mode maître***, ***mode ad-hoc***, ***mode moniteur***.

mode infrastructure voir ***mode maître***.

Modèle réseau OSI. Un modèle populaire de réseau de communication défini par le standard ISO/IEC 7498-1. Le modèle OSI se compose de sept couches interdépendantes, allant de la physique à la couche application. Voir aussi: ***modèle réseau TCP/IP***.

modèle réseau TCP/IP. Une simplification populaire du modèle réseau OSI qui est utilisée avec des réseaux Internet. Le protocole TCP/IP se compose de cinq couches interdépendantes, allant de la physique à la couche application. Voir aussi: ***modèle réseau OSI***.

mode maître. Un mode radio utilisé par les dispositifs 802.11 ou la radio permet de créer des réseaux tout comme le fait un point d'accès. Voir aussi: ***mode géré***, ***mode ad-hoc***, ***mode moniteur***.

mode moniteur. Un mode radio utilisé par les dispositifs 802.11 qui ne sont pas habituellement utilisés pour les communications qui permettent à la radio de suivre passivement le trafic. Voir aussi: ***mode maître***, ***mode géré***, ***mode ad-hoc***.

module solaire voir ***panneau solaire***.

multipoints à multipoints voir ***maille***.

multi route. Le phénomène de la réflexion d'un signal qui atteint son objectif en utilisant des routes différentes, et donc à des moments différents.

Multi Router Trafic Grapher (MRTG). Un utilitaire libre utilisé pour produire des

graphiques de statistiques de trafic. Disponible sur *http://oss.oetiker.ch/mrtg/*.

mW voir ***milliwatt***.

My TraceRoute (MTR). Un outil de diagnostic réseau utilisé comme une alternative au programme ***traceroute***. *http://www.bitwizard.nl/mtr/*. Voir aussi: ***traceroute/ tracert***.

N

Nagios (*http://nagios.org/*) Un outil de surveillance en temps réel qui se connecte et notifie un administrateur de services et pannes réseau.

nat. La table utilisée dans le système pare-feu Linux netfilter pour la traduction d'adresses réseau.

natte. Un câble micro-ondes court qui convertit un connecteur non-standard en quelque chose de plus robuste et plus couramment disponible.

NAT voir ***Network Address Translation (traduction d'adresses réseau)***.

navigateur maître. Sur les réseaux Windows, le navigateur maître est l'ordinateur qui tient à jour une liste de tous les ordinateurs, les actions et les imprimantes qui sont disponibles dans le voisinage réseau ou les Favoris réseau.

NEC2 voir ***Code électromagnétique numérique***.

NetBIOS. Un protocole de couche session utilisé par les réseaux Windows pour le partage de fichiers et d'imprimantes. Voir aussi: ***SMB***.

netfilter. Le module de filtrage de paquets dans les noyaux Linux modernes est connu sous le nom de nettfilter. Il emploie la commande iptables pour manipuler les règles de filtrage. *http://netflter.org/*.

netmask (masque de réseau). Un netmask est un nombre de 32 bits qui divise les 16 millions d'adresses IP disponibles en petits morceaux, appelés sous-réseaux. Tous les réseaux IP utilisent les adresses IP en combinaison avec des netmasks pour regrouper logiquement les hôtes et les réseaux.

NeTraMet. Un utilitaire libre d'analyse de flux réseau disponible sur *http://freshmeat.net/projets/netramet/*.

Network Address Translation (NAT, traduction d'adresses réseau). NAT est une technologie de réseau qui permet à plusieurs ordinateurs de partager une seule adresse IP routable globalement. Bien que le NAT peut aider à résoudre le problème de l'espace d'adressage IP limité, il crée un défi technique pour les services à deux sens, tels que la Voix sur IP.

ngrep. Un utilitaire de sécurité réseau libre utilisé pour trouver les expressions régulières dans les données. Disponible gratuitement à partir de *http://ngrep.sourceforge.net/*.

noeud. Tout appareil capable d'envoyer et de recevoir des données sur un réseau. Les points d'accès, les routeurs, des ordinateurs et des ordinateurs portables sont tous des exemples de noeuds.

nombre de jours d'autonomie (N). Le nombre maximum de jours qu'un système photovoltaïque peut fonctionner sans recevoir un apport significatif d'énergie solaire.

notation CIDR. Une méthode utilisée pour définir un masque réseau en précisant le nombre de bits présents. Par exemple, le masque réseau 255.255.255.0 peut être spécifié par /24 en notation CIDR.

ntop. Un outil de surveillance réseau qui fournit des détails sur les connexions et le protocole utilisés sur un réseau local. *http://www.ntop.org/*.

null. Dans un modèle de rayonnement d'antenne, un null est une zone dans laquelle la puissance rayonnée effective est à un niveau minimum.

nulling. Un cas spécifique d'interférence multi-route où le signal à l'antenne de réception est annulé par l'interférence destructive de signaux réfléchis.

O

onde mécanique. Une onde qui se produit lorsqu'un certain support ou objet est en balancement périodique. Voir aussi: ***onde électromagnétique***.

onde électromagnétique. Une onde qui se propage à travers l'espace sans avoir besoin d'un moyen d'un support de propagation. Il contient une composante électrique et une composante magnétique. Voir aussi: ***onde mécanique***.

onduleur voir ***convertisseur DC/AC***.

OU logique. Une opération logique qui évalue comme vrai si l'un des éléments comparés est également évalué comme vrai. Voir aussi: ***ET logique***.

Outils de test de débit. Outils de mesure de la bande passante disponible entre deux points sur un réseau.

outils de test intermittent (spot check tools). Des outils de surveillance réseau qui sont exécutés uniquement en cas de nécessité pour diagnostiquer un problème. Ping et traceroute sont des exemples d'outils de test intermittent.

P

Paire torsadée non blindé voir ***UTP***.

panneau solaire. La composante d'un système photovoltaïque utilisée pour convertir le rayonnement solaire en électricité. Voir aussi: ***batterie***, ***régulateur de charge***, ***convertisseur***, ***onduleur***.

paquet. Les messages envoyés entre les ordinateurs sur les réseaux IP sont divisés en petits morceaux appelés paquets. Chaque paquet comprend une source, une destination, et d'autres informations de routage qui sont utilisés pour router le paquet vers sa destination finale. Les paquets sont rassemblés de nouveau à l'autre extrémité par le protocole TCP (ou un autre protocole) avant d'être passés à l'application.

pare-feu. Un routeur qui accepte ou refuse le trafic basé sur certains critères. Les pare-feux sont un outil de base utilisé pour protéger des réseaux entiers contre le trafic indésirable.

partition. Une technique utilisée par les hubs du réseau pour limiter l'impact des ordinateurs qui transmettent excessivement. Les hubs vont temporairement retirer l'ordinateur abusif (il le partitionne) du reste du réseau, et le reconnecter à nouveau après quelque temps. Un partitionnement excessif indique la présence d'une consommation excessive de bande passante provenant, par exemple, d'un client peer-to-peer ou un virus réseau.

passerelle par défaut. Quand un routeur reçoit un paquet à destination d'un réseau pour lequel il n'a pas de route explicite, le paquet est transmis à la passerelle par défaut. La passerelle par défaut répète le processus, peut-être en envoyant le paquet à sa propre passerelle par défaut, jusqu'à ce que le paquet atteigne sa destination finale.

périphérie (edge). Le lieu où un réseau d'un organisme joint un autre réseau. Les périphéries sont définies par la location du routeur externe qui agit souvent comme un pare-feu.

Perte de Retour. Un ratio logarithmique mesuré en dB qui compare l'énergie réfléchie par l'antenne à l'énergie qui est introduite dans l'antenne par la ligne de transmission. Voir aussi: ***impédance***.

perte de route. Perte de signal radio en raison de la distance entre les stations de communication.

perte en espace libre. Diminution de puissance résultant de l'étalement géométrique de l'onde lors de sa propagation dans l'espace. Voir aussi: ***atténuation***, ***perte d'espace libre***, ***annexe C***.

pile de protocoles. Un ensemble de protocoles réseau interdépendants qui fournissent des couches de fonctionnalités. Voir aussi: ***modèle réseau OSI*** et ***modèle réseau TCP/IP***.

ping. Un utilitaire de diagnostic réseau utilisant l'echo ICMP et les messages réponses pour déterminer le temps aller-retour à un réseau hôte. Ping peut être utilisé pour déterminer l'emplacement des problèmes de réseau en "Pingant" les ordinateurs sur le chemin entre la machine locale et la destination finale.

PKI voir ***Public Key Infrastructure***.

plate-forme cohérente. Les coûts de maintenance peuvent être réduits en utilisant une plate-forme cohérente, avec le même matériel, logiciel, et firmware pour de nombreux composants dans un réseau.

plomb. Une lourde pièce de métal enfouie dans la terre pour améliorer la conductivité d'un terrain.

PoE voir ***Power over Ethernet***.

point-à-multipoints. Un réseau sans fil où plusieurs noeuds connectent à un emplacement central. L'exemple classique d'un réseau point-à-multipoints est un point d'accès à un bureau avec plusieurs ordinateurs portables l'utilisant pour accéder

à l'Internet. Voir aussi: ***point à point***, ***multipoints-à-multipoints***.

point à point. Un réseau sans fil composé de deux stations seulement, généralement séparés par une grande distance. Voir aussi: ***point-à-multipoints***, ***multipoints-à-multipoints***.

point chaud. Dans les systèmes photovoltaïques, un point chaud se produit quand une cellule unique d'un panneau solaire est dans l'ombre ; la faisant jouer le rôle de charge résistive plutôt que de produire de l'électricité.

Point d'accès (AP). Un dispositif qui crée un réseau sans fil habituellement connecté à un réseau câble Ethernet. Voir aussi: ***CPE***, ***mode maître***.

Point de puissance maximum (P_{max}). Le point où l'énergie électrique fournie par un panneau solaire est au maximum.

point d'accès illégitime (rogue access point). Un point d'accès non autorisé mal installé par les utilisateurs légitimes ou par une personne malveillante qui a l'intention de recueillir des données ou endommager le réseau.

Point-to-Point Protocol (PPP). Un protocole réseau utilisé généralement sur les lignes série (comme une connexion dial-up) pour fournir la connectivité IP.

polarisation circulaire. Un champ électromagnétique ou le vecteur du champ électrique semble tourner avec un mouvement circulaire de ans la direction de ans propagation, faisant un tour complet pour chaque cycle RF. Voir aussi: ***polarisation linéaire, polarisation horizontale, polarisation verticale***.

polarisation horizontale. Un champ électromagnétique avec la composante électrique se déplaçant dans une direction linéaire horizontale. Voir aussi: ***polarisation verticale***, ***polarisation circulaire, polarisation linéaire***.

polarisation linéaire. Un champ électromagnétique ou le vecteur du champ électrique reste sur le même plan. L'orientation peut horizontale, verticale, ou à un angle entre les deux. Voir aussi: ***polarisation circulaire, polarisation verticale, polarisation horizontale***.

polarisation verticale. Un champ électromagnétique dont la composante électrique se déplace dans un mouvement linéaire vertical. La plupart d'appareils électroniques des consommateurs sans fil utilisent la polarisation verticale. voir aussi: ***polarisation horizontale, polarisation circulaire, polarisation linéaire***.

polarité inversée (RP). Connecteurs micro-onde propriétaires basés sur un connecteur standard mais avec les genres inversés. Le RP-TNC est probablement le plus commun des connecteurs à polarité inversée, mais d'autres (tels que la RP-SMA et RP-N) sont également monnaie courante.

polarisation. La direction de la composante électrique d'une onde électromagnétique à la sortie de l'antenne de transmission. Voir aussi:***polarisation linéaire, polarisation circulaire***.

polar plot. Un graphique où les points sont localisés par projection le long d'un axe de rotation (rayon) à une intersection avec l'un de plusieurs cercles concentriques. Voir aussi: ***rectangular plot***.

politique. Dans netfilter, la politique est l'action à prendre par défaut au cas ou aucune des règles de filtrage ne s'appliquent. Par exemple, la politique par défaut pour toute chaîne peut être configurée pour ACCEPT ou DROP.

portail captif. Un mécanisme utilisé pour rediriger, de façon transparente, les navigateurs Web vers un nouvel emplacement. Les portails captifs sont souvent utilisés pour l'authentification ou pour interrompre une session en ligne d'un utilisateur (par exemple, pour afficher une charte d'utilisation).

port moniteur. Sur un commutateur géré, un ou plusieurs ports peuvent être configurés pour recevoir le trafic envoyé à tous les autres ports. Cela vous permet de connecter un serveur moniteur de trafic au port pour observer et analyser les formes de trafic.

Power over Ethernet (PoE). Une technique utilisée pour la fourniture d'alimentation continue à des périphériques utilisant le câble de données Ethernet. Voir aussi: ***injecteurs end span***, ***injecteurs mid span***.

PPP voir ***Point to Point Protocol***.

Principe de Huygens. Un modèle d'onde qui propose un nombre infini de fronts d'onde le long de tout point d'un front d'onde avançant.

Privoxy (*http://www.privoxy.org/*). Un proxy web qui offre l'anonymat par le biais des filtres. Privoxy est souvent utilisé en conjonction avec Tor.

Profondeur maximale de la décharge(DoD$_{max}$). La quantité d'énergie extraite d'une batterie en un seul cycle de décharge, exprimée en pourcentage.

Protocole de résolution d'adresses (ARP, Address Resolution Protocol). Un protocole très utilisé sur les réseaux Ethernet pour traduire les adresses IP en adresses MAC.

protocole orienté session. Un protocole réseau (tel que TCP) qui exige initialisation avant échange des données ainsi qu'un certain nettoyage après que l'échange de données soit terminée. Les protocoles orientés session offrent généralement une correction d'erreur et le réassemblage de paquets alors que les protocoles orientés non connexion ne le font pas. Voir aussi: ***protocole orienté non connexion***.

protocole orienté non connexion. Un protocole de réseau (comme UDP) qui n'exige pas d'initiation de session ou sa maintenance. Typiquement, les protocoles orientés non connexion exigent moins de surcharge que les protocoles orientés session, mais ne fournissent pas généralement la protection des données ou le réassemblage de paquets. Voir aussi: ***protocole orienté session***.

proxy anonyme. Un service réseau qui cache la source ou la destination des communications. Les proxy anonymes peuvent être utilisés pour protéger la vie privée des utilisateurs du réseau et réduire l'exposition d'un organisme à une responsabilité juridique liée aux actions de ses utilisateurs.

proxy transparent. Un proxy cache installé afin que les requêtes web des utilisateurs soient automatiquement transmises au serveur proxy, sans qu'il soit nécessaire de configurer manuellement des navigateurs Web pour l'utiliser.

PSH voir ***Heures d'équivalent plein soleil***.

puissance. La quantité d'énergie dans un certain laps de temps.

R

Radiation pattern voir ***antenna pattern***.

radio. La partie du spectre électromagnétique dans laquelle les ondes peuvent être générés par l'application d'un courant alternatif à une antenne.

réciprocité. La capacité d'une antenne de maintenir les mêmes caractéristiques, peu importe si elle fonctionne en mode transmission ou réception.

rectangular plot. Un graphique où les points sont situés sur une simple

grille Voir aussi: ***polar plot***.

Redirection (forwarding). Quand les routeurs reçoivent les paquets qui sont destinés à un autre hôte ou réseau, ils envoient ces paquets au routeur le plus proche de la destination finale. Ce processus se nomme redirection.

régulateur de charge d'énergie solaire voir ***régulateur***.

régulateur. La composante d'un système photovoltaïque qui assure que la batterie fonctionne dans des conditions appropriées. Elle évite la surcharge et la surdécharge, qui sont très préjudiciables à la vie de la batterie. Voir aussi: ***panneau solaire***, ***batterie***, ***charge***, ***convertisseur***, ***onduleur***.

Regional Internet Registrars. Les 4 milliards d'adresses IP disponibles sont gérées administrativement par l'IANA. L'espace a été divisé en grands sous réseaux, qui sont délégués à l'un des cinq registres Internet régionaux, chacun ayant autorité sur une grande zone géographique.

répéteur "one-arm". Un répéteur sans fil qui utilise une seule radio à débit significativement réduit. Voir aussi: ***répéteur***.

répéteur. Un noeud qui est configuré pour la rediffusion du trafic qui n'est pas destiné pour le noeud lui-même, souvent utilisé pour étendre la portée utile d'un réseau.

Request for Comments (RFC). Les RFCs sont une série numérotée de documents publiés par la Société Internet pour documenter des idées et des concepts liés aux technologies de l'Internet. Pas tous les RFC sont des normes, mais beaucoup sont soit approuvés explicitement par l'IETF ou éventuellement deviennent des normes de

fait. Les RFC peuvent être consultées en ligne à *http://rfc.net/*.

réseau à conduit long et grand. Une connexion réseau (telle que VSAT), qui a une grande capacité et latence. Pour atteindre les meilleures performances possibles, TCP/IP doit être ajusté au trafic sur de telles liaisons.

réseau fermé. Un point d'accès qui ne diffuse pas son SSID, souvent utilisé comme mesure de sécurité.

réseau privé virtuel (VPN). Un outil utilisé pour relier deux réseaux dans un réseau non sécurisé (comme l'Internet). Les VPN sont souvent utilisés pour connecter les utilisateurs distants à un réseau d'une organisation en cas de voyage ou de travail à la maison. Les VPN utilisent une combinaison de cryptage et de tunnelling pour sécuriser tout le trafic réseau, quelle que soit l'application utilisée. Voir aussi: ***tunnel***.

réseaux de Classe A, B, C. Depuis quelque temps, l'espace d'adressage IP a été allouée en blocs de trois tailles différentes. Il s'agit de la classe A (environ 16 millions d'adresses), classe B (environ 65 mille adresses), et de la classe C (255 adresses). Alors que le CIDR a remplacé l'allocation à base de classes, ces classes sont encore souvent mentionnées et utilisées à l'intérieur des organisations en utilisant l'espace d'adressage privé. Voir aussi: ***notation CIDR***.

RIR voir ***Regional Internet Registrars***

Round Trip Time (RTT). Le temps qu'il faut pour un paquet pour être reconnu à partir de l'autre extrémité d'une connexion. Fréquemment confondue avec ***latence***.

Routable globalement (globally routable). Une adresse délivrée par un fournisseur de services Internet ou RIR qui est accessible à partir de n'importe quel point sur l'Internet. En IPv4, il y a environ quatre milliards d'adresses IP possibles, mais qui ne sont pas toutes routables globalement.

routage. Le processus de transmission de paquets entre les différents réseaux. Un dispositif qui le fait s'appelle un routeur.

routage oignon. Un outil de protection de l'anonymat (tels que Tor), qui fait rebondir vos connexions TCP répétitivement à travers un certain nombre de serveurs répartis sur l'ensemble de l'Internet, en enveloppant l'information dans un certain nombre de couches encryptées.

routage proactif. Une implémentation d'un maillage où chaque noeud connaît l'existence de chaque autre noeud de la nuée du maillage ainsi que les nœuds qui peuvent être utilisés pour router le trafic vers ces noeuds. Chaque noeud maintient une table de routage couvrant l'ensemble de la nuée du maillage. Voir aussi: ***routage réactif***.

routage réactif. Une implémentation d'un maillage où les routes sont calculées seulement lorsqu'il est nécessaire d'envoyer des données à un noeud spécifique. Voir aussi: ***routage proactif***.

route par défaut. Une route réseau qui pointe vers la passerelle par défaut.

routeur. Un appareil qui transmet les paquets entre les différents réseaux. Le processus de transmission de paquets au prochain hop est appelé le routage.

RP-TNC. Une version commune de micro-connecteur TNC propriétaire ayant des genres inversés. Le RP-TNC se trouve souvent sur les équipements fabriqués par Linksys.

RP voir ***polarité inversée (Reverse polarity)***.

RRDTool. Une suite d'outils qui vous permettent de créer et de modifier les bases de données RRD, ainsi que de générer des graphiques utiles pour présenter les données. RRDTool est utilisée pour garder une trace de séries chronologiques de données (telles que la bande passante du réseau, la température de la salle machine, la charge du serveur ou les moyennes) et peut afficher que les données en moyenne plus de temps. RRDTool est disponible à partir de *http://oss.oetiker.ch/rrdtool/*.

RRD voir ***base de données Round Robin***.

rsync (*http://rsync.samba.org/*). Un utilitaire libre de transfert de fichiers utilise pour la maintenance des sites miroirs.

RTT voir ***Round Trip Time***.

S

SACK voir ***Selective Acknowledgment***.

Selective Acknowledgment. Un mécanisme utilisé pour surmonter les

déficiences de TCP sur des réseaux à haute latence tels que les VSAT.

scattering. La perte de signal due à des objets dans le chemin entre deux sommets. Voir aussi: ***perte en espace libre***, ***atténuation***.

Secure Sockets Layer (SSL). Une technologie de cryptage bout a bout intégrée dans virtuellement tous les clients web. SSL utilise la cryptographie à clé publique et une infrastructure à clé publique de confiance pour sécuriser les communications de données. Chaque fois que vous visitez un site Web qui commence par https, vous utilisez SSL.

Service Set ID (SSID) voir ***Extended Service Set Identifier***.

Shorewall (*http://shorewall.net/*). Un outil de configuration utilisé pour la mise en place des pare-feux netfilter sans la nécessité d'apprendre la syntaxe d'iptables.

Simple Network Management Protocol (SNMP). Un protocole destiné à faciliter l'échange d'information de gestion entre les périphériques réseau. SNMP est généralement utilisé pour sonder les commutateurs réseau et les routeurs afin de recueillir des statistiques d'exploitation.

site-wide web cache. Alors que tous les navigateurs modernes fournissent un cache de données locales, les grandes entreprises peuvent améliorer leur efficience par l'installation d'un web cache global tel que Squid. Un web cache global conserve une copie de toutes les demandes faites à partir d'un organisme, et sert la copie locale sur les demandes ultérieures. Voir aussi: ***Squid***.

SMA. Un petit connecteur micro-onde fileté.

SMB (Server Message Block). Un protocole réseau utilisé dans Windows pour fournir des services de partage des fichiers. Voir aussi: ***NetBIOS***.

SMB voir ***Server Message Block***

SmokePing. Un outil de mesure de latence qui mesure, stocke et affiche la latence, la distribution de latence et la perte de paquets, toutes sur un graphe unique. SmokePing est disponible à partir de *http://oss.oetiker.ch/smokeping/*.

SNMP voir ***Simple Network Management Protocol***.

Snort (*http://www.snort.org/*). Un système de détection d'intrusion très populaire et libre. Voir aussi: ***système de détection d'intrusion***.

SoC voir ***état de charge.***

sous-réseaux. Un sous-ensemble d'une gamme de réseaux IP défini par le masques réseaux (netmasks).

Spectre électromagnétique. La très large gamme de fréquences possible de l'énergie électromagnétique. Les parties du spectre électromagnétique comprennent la radio, micro-ondes, la lumière visible, et les rayons X.

spectre voir ***spectre électromagnétique***.

split horizon DNS. Une technique utilisée pour fournir des réponses différentes à des requêtes DNS basé sur l'origine de la demande. Split horizon est utilisé pour diriger les utilisateurs internes vers un ensemble de serveurs qui diffèrent de ceux des utilisateurs de l'Internet.

Squid. Un cache proxy web libre très populaire. Il est flexible, robuste, plein de fonctionnalités, et s'adapte pour supporter des réseaux de n'importe quelle taille. *http://www.squid-cache.org/*.

SSID voir ***Extended Service Set Identifier***.

SSL voir ***Secure Sockets Layer***.

stateful inspection. Règles pare-feu qui considèrent l'état d'un paquet. L'état ne fait pas partie du paquet transmis sur l'Internet mais est déterminé par le pare-feu lui-même. Les connexions nouvelles, établies et autres peuvent être prises en considération lors du filtrage des paquets. Stateful inspection est parfois appelé suivi de connexion (*connection tracking*).

structure. Dans NEC2, une description numérique de l'endroit où les différentes parties de l'antenne sont situés, et la façon dont les fils sont connectés. Voir aussi: ***contrôles***.

Support partagé. Un réseau à liens locaux où chaque noeud peut observer e trafic de tout autre nœud.

surcharge. L'état de la batterie lorsque la charge est appliquée au-delà de la limite de la capacité de la batterie. Si l'énergie est appliquée à une batterie au-delà de son point de charge maximale, l'électrolyte commence à se décomposer. Des régulateurs permettront un petit temps de surcharge de la batterie pour éviter la gazéification, mais retireront la puissance avant que la batterie soit endommagée.

surdécharge. Le déchargement d'une batterie au-delà de sa profondeur maximale de décharge qui entraîne une détérioration de la batterie.

sursouscription. Permettre plus d'utilisateurs que la bande passante maximale disponible peut supporter.

surveillance en temps réel. Un outil de surveillance qui effectue la surveillance sans contrôle pendant de longues périodes et notifie les administrateurs immédiatement lorsque des problèmes se posent.

Système de Détection d'Intrusion (IDS, Intrusion Detection System). Un logiciel qui veille sur le trafic réseau, à la recherche de formes de données ou comportements suspects. Un IDS peut faire une entrée de journal, notifier un administrateur réseau, ou agir directement en réponse au trafic.

système photovoltaïque autonome voir ***système photovoltaïque***.

système photovoltaïque. Un système énergétique qui génère l'énergie électrique à partir du rayonnement solaire et la stocke pour un usage ultérieur. Un système photovoltaïque autonome le fait sans aucune connexion à un réseau électrique. Voir aussi: ***batterie***, ***panneaux solaires***, ***régulateur de charge***, ***convertisseur***, ***onduleur***.

T

table de routage. Une liste des réseaux et des adresses IP tenu par un routeur afin de déterminer comment les paquets devraient être transmis. Si un routeur reçoit un paquet d'un réseau qui ne figure pas dans sa table de routage, le routeur utilise sa passerelle par défaut. Les routeurs fonctionnent dans la couche réseau. Voir aussi: bridge et passerelle par défaut.

table MAC. Un commutateur réseau doit assurer le suivi des adresses MAC utilisées sur chaque port physique afin de distribuer des paquets efficacement. Cette information est conservée dans une table appelée la table MAC.

Taille de fenêtre TCP (TCP window size). La taille de la fenêtre TCP. Le paramètre TCP qui définit la quantité de données qui peut être envoyée avant qu'un accuse de réception ACK ne soit renvoyée par la destination. Par exemple, une taille de fenêtre de 3000 signifierait que deux paquets de 1500 octets chacun seront envoyés, après lesquels la destination soit accusera réception (ACK) de ces paquets ou demandera une retransmission.

tcpdump. Un outil libre de capture et d'analyse de paquet disponible sur *http://www.tcpdump.org/*. Voir aussi: ***WinDump*** et ***Wireshark***.

TCP/IP voir ***suite de protocoles Internet***.

TCP voir ***Transmission Control Protocol***.

Temporal Key Integrity Protocol (TKIP). Un protocole de cryptage utilisé en conjonction avec WPA pour améliorer la sécurité d'une session de communication.

tendances (trending). Un type d'outil de surveillance qui effectue la surveillance sans contrôle sur de longues périodes, et imprime les résultats sur un graphique. Les outils de tendances vous permettent de prédire le comportement futur de votre réseau. Ceci vous aide à planifier les mises à jour et des changements.

tension nominale (V_N). La tension de fonctionnement d'un système photovoltaïque, généralement de 12 ou 24 volts.

Time To Live (TTL). Une valeur TTL agit comme une date limite ou un frein de secours signalant un moment où les données doivent être rejetées. Dans les réseaux TCP/IP, le TTL est un compteur qui commence à une certaine valeur (comme 64) et est décrémenté à chaque hop routeur. Si la durée de vie atteint zéro, le paquet est jeté. Ce mécanisme permet de réduire les dommages causés par des boucles de routage. Dans DNS, le TTL définit le temps qu'un enregistrement de zone (zone record) doit être conservé avant d'être actualisé. Dans Squid, le TTL définit combien de temps un objet en cache peut être conservé avant qu'il ne soit de nouveau extrait du site d'origine.

TKIP voir ***Temporal Key Integrity Protocol***.

Tor (*http://www.torproject.org/*). Un outil de routage oignon qui fournit une bonne protection contre l'analyse du trafic.

traceroute/tracert. Un utilitaire de diagnostic réseau omniprésent souvent utilisé en conjonction avec ping pour déterminer l'emplacement des problèmes de réseau. La version Unix est appelée

traceroute, tandis que la version Windows est tracert. Les deux utilisent les requêtes d'écho ICMP avec des valeurs de TTL croissantes pour déterminer les routeurs qui sont utilisés pour se connecter à un hôte distant, et également afficher les statistiques de latence. Une autre variante est tracepath, qui fait appel à une technique similaire avec des paquets UDP. Voir aussi: ***mtr***.

trafic entrant. Paquets réseau qui proviennent de l'extérieur du réseau local (généralement l'Internet) et sont attachés à une destination à l'intérieur du réseau local. Voir aussi: ***traffic sortant***.

trafic externe. Trafic réseau qui provient de, ou qui est destiné à une adresse IP en dehors de votre réseau interne, comme le trafic Internet.

trafic sortant. Des paquets de réseau qui ont pour origine le réseau local et sont destinés à une adresse en dehors du réseau local (typiquement quelque part sur l'Internet). Voir aussi: ***trafic entrant***.

transfert de gain. Comparaison d'une antenne sous test avec une antenne standard de type connu, qui a un gain calibré.

Transmission Control Protocol (TCP). Un protocole orienté session qui fonctionne sur la couche transport offrant le réassemblage de paquets, l'évitement de congestion, et une livraison de données fiable. TCP est un protocole intégré utilisé par de nombreuses applications Internet, y compris HTTP et SMTP. Voir aussi: ***UDP***.

transmission de puissance. La quantité d'énergie fournie par l'émetteur radio, avant tout gain d'antenne ou des pertes en ligne.

transparent bridging firewall. Une technique pare-feu qui introduit un pont qui transmet les paquets de façon sélective sur base des règles pare-feu. Un bénéfice d'un pont transparent est qu'il ne nécessite pas d'adresse IP. Voir aussi: ***bridge***.

TTL voir ***Time To Live***.

tunnel. Une forme d'encapsulation de données qui encapsule une pile de protocoles dans un autre. Cela est souvent utilisé en conjonction avec le cryptage pour protéger les communications contre une indiscrétion potentielle, tout en éliminant la nécessité de supporter l'encryptage de l'application elle-même. Les tunnels sont souvent utilisés conjointement avec les ***VPN***.

types de messages. Plutôt que des numéros de port, le trafic ICMP utilise des types de messages pour definir l'information en cours d'envoi. Voir aussi: ***ICMP***.

U

UDP (User Datagram Protocol). Un protocole sans connexion (de la couche de transport) couramment utilisé pour la vidéo et le streaming audio.

UDP voir ***User Datagram Protocol***.

U.FL. Un très petit connecteur micro-onde couramment utilisé sur des cartes radio de type mini-PCI.

Utilisateurs non intentionnels. Les utilisateurs de portables qui, accidentellement, sont associés au mauvais réseau sans fil.

Unshielded Twisted Pair (UTP). Câble utilisé pour l'Ethernet 10BaseT et 100baseT. Il est composé de quatre paires de fils torsadées.

UTP voir ***Unshielded Twisted Pair*** (paire torsadée non blindée).

V

Very Small Aperture Terminal (VSAT). Un des nombreux standards utilisés pour l'accès Internet par satellite. Le VSAT est la technologie par satellite la plus largement déployée en Afrique. voir aussi: ***Broadband Global Access Network (BGAN)*** et ***Digital Video Broadcast (DVB-S)***.

Vitesse. Un terme générique utilisé pour désigner la réactivité d'une connexion réseau. Un réseau à "grande vitesse" doit présenter une faible latence et une capacité plus que suffisante pour transporter le trafic de ses utilisateurs. Voir aussi: ***largeur de bande, capacité*** et ***latence***.

VoIP (Voice over IP). Une technologie qui offre des caractéristiques de type téléphonie sur une connexion Internet. Les exemples de clients VoIP populaires incluent Skype, Gizmo Project, MSN Messenger et iChat.

VPN voir ***Virtual Private Network***.

VRLA voir ***batterie au plomb acide à valve régulée***.

VSAT voir ***Very Small Aperture Terminal***.

W

WAN voir ***Wide Area Network***.

War drivers. Les amateurs sans fil qui sont intéressés par trouver l'emplacement physique des réseaux sans fil.

WEP voir ***Wired Equivalent Privacy***.

wget. Un outil de ligne de commande libre pour le téléchargement de pages Web. *http://www.gnu.org/software/wget/*

Wide Area Network (WAN). Toute technologie réseau à longue distance. Généralement, les lignes louées, relais de trames (Frame Relay), ADSL, réseaux câblés, et les lignes satellite implémentent tous des réseaux à longue distance. Voir aussi: ***LAN***.

Wi-Fi Protected Access (WPA). Un ***cryptage de couche de liaison*** assez puissant, supporté par la plupart d'équipements Wi-Fi.

Wi-Fi. Une marque déposée appartenant à l'alliance Wi-Fi. Elle est utilisée pour se référer à diverses technologies de réseau sans fil (y compris les normes 802.11a, 802.11b et 802.11g). Wi-Fi est l'abréviation de ***Wireless Fidelity***.

wiki. Un site Web qui permet à tout utilisateur de modifier le contenu de n'importe quelle page. L'un des wikis le plus populaire est *http://www.wikipedia.org/*

WinDump. La version Windows de tcpdump. Elles est disponible à partir de *http://www.winpcap.org/windump/*

Wired Equivalent Privacy (WEP). Un protocole de ***cryptage de la couche liaison*** quelque peu inviolable qui est supporté par pratiquement tous les équipements 802.11a/b/g.

Wireless Fidelity voir ***Wi-Fi***.

wireshark. Un analyseur de protocole réseau pour Unix et Windows. *http://www.wireshark.org/*

Wi-Spy. Un outil peu coûteux d'analyse de spectre de 2,4 GHz disponible sur *http://www.metageek.net/*.

WPA voir ***Wi-Fi Protected Access***

Z

Zabbix (*http://www.zabbix.org/*). Un outil de surveillance en temps réel qui se connecte et notifie un administrateur de système sur les pannes de service et les pannes réseau.