RÉSEAUX SANS FIL DANS LES PAYS EN DÉVELOPPEMENT

Un guide pratique pour la planification et la construction des infrastructures de télécommunications à bas prix

RÉSEAUX SANS FIL DANS LE MONDE EN DÉVELOPPEMENT

Troisième édition

Réseaux sans fil dans le monde en développement

Pour plus d'informations sur ce projet, veuillez visiter http://wndw.net

Première édition, Janvier 2006
Deuxième édition, Décembre 2007
Troisième édition, Février 2013

Comme nous l'avons découvert, le monde en développement des réseaux sans fil est tout autour de nous. Les auteurs de ce livre ont inclus des projets en Amérique du Nord, en Europe, en Asie, en Amérique du Sud, en Inde et en Afrique. Nous sommes arrivés à la conclusion que la plupart des lieux ont le potentiel de trouver les réseaux sans fil intérieurs et extérieurs à coûts abordables utiles. Nous espérons que vous apprécierez le contenu de ce livre et l'utiliserez comme point de départ d'un projet sans fil dans votre communauté. Le livre et le fichier PDF sont publiés sous une licence Creative Commons Attribution-ShareAlike 3.0. Cela permet à quiconque de faire des copies, et même de les vendre pour un profit, aussi longtemps que le crédit approprié est donné aux auteurs et que les ouvrages dérivés sont mis à disposition dans les mêmes conditions.

Toutes copies ou travaux dérivés doivent inclure un lien visible vers notre site, http://wndw.net/.

Voir http://creativecommons.org/licenses/by-sa/3.0/ pour plus d'informations sur ces termes.

ISBN-13: 978-1497541108

LICENCE

AVANT-PROPOS

Cette troisième version de ce livre a commencé comme un BookSprint organisé en Septembre 2011 dans la belle ville de Copenhague par Sebastian Buettrich, qui en est un des auteurs.
Une équipe de base de huit personnes a ensuite complété cette version du livre au cours des mois suivants menant à sa publication en Mars 2013.

Pendant le projet, le groupe de base a activement sollicité les contributions et commentaires de la communauté des réseaux sans fil dans le monde entier. Vous pouvez fournir vos propres commentaires ou des questions techniques auprès des auteurs sur notre page Facebook :
https://www.facebook.com/groups/wirelessu

Ce livre est disponible en eBook pour votre appareil mobile. Il est téléchargeable gratuitement sur le site http://wndw.net/ (résolution haute et basse disponible). Il peut aussi être commandé comme un livre imprimé à partir du site http://www.lulu.com/
Nous donnons une copie à chaque étudiant qui suit un cours de formation sans fil offert par toutes les institutions avec lesquelles nous travaillons telles que le Centre international de physique théorique (en anglais International Centre for Theoretical Physics ICTP), le Centre pour les ressources de démarrage réseau (en anglais Network Startup Resource Center NSRC), l'Institut asiatique de technologie (en anglais Asian Institute of Technology AIT) l'Internet Society (ISOC) et AirJaldi, pour n'en citer que quelques-uns. Et nous vous encourageons grandement à vous inscrire à un cours local.
Pour plus d'informations sur les prochaines formations ou si vous souhaitez organiser un cours dans votre région, veuillez s'il vous plaît contacter l'éditeur, Jane Butler par courriel électronique a l'adresse suivante:
janesbutler@networktheworld.org

Si vous envisagez un projet sans fil et vous avez besoin d'un exemplaire de ce livre et ne pouvez ni le télécharger car vous avez une bande passante limitée, ou si vous n'avez pas les moyens de le commander en ligne, veuillez s'il vous plaît envoyez un e-mail à Jane ou envoyer un message sur Facebook et nous vous enverrons un exemplaire imprimé.

Contributeurs de base

Jane Butler est l'éditrice principale de cette version du livre.
Jane est actuellement président de la Fondation privée appelée networktheworld.org qui encourage et appuie la croissance de la connectivité Internet dans le monde, principalement en soutenant des projets sans fil et la formation http://wirelessu.org. Elle est également à la tête de la collaboration industrielle et de la sensibilisation de l'University College London. Jane est titulaire d'un baccalauréat spécialisé en ingénierie, et est un ingénieur agréé et membre de l'Institution de l'électronique et de la technologie.
Elle peut être contactée par courriel électronique à l'adresse
janesbutler@networktheworld.org

L'éditrice tient à remercier le groupe des contributeurs de base qui sont énumérés ci-dessous

Ermanno Pietrosemoli . Ermanno est actuellement chercheur dans le laboratoire des Télécommunications/TIC pour le développement du Centre international de physique théorique de Trieste, en Italie. Il est également président de la Fundación Escuela Latinoamericana de Redes " EsLaRed ", une organisation à but non lucratif qui fait la promotion des TIC en Amérique latine par la formation et les projets de développement. EsLaRed a reçu de l'Internet Society, le Prix Jonathan B. Postel pour les services en 2008. Ermanno a déployé des réseaux de communication de données sans fil en se concentrant sur la technologie à faible coût, et a participé à la planification et la construction de réseaux de données sans fil en Argentine, en Colombie, en Équateur, en Italie, au Lesotho, au Malawi, au Maroc, au Mexique, au Nicaragua, au Pérou, au Trinidad, aux Etats-Unis et au Venezuela. Il a publié plusieurs articles relatifs à la communication de données sans fil présenté dans des nombreuses conférences et est co-auteur et auteur technique du livre "Réseau sans fil pour le monde en développement" disponible gratuitement sur http://wndw.net. Ermanno est titulaire d'une maîtrise de l'Université de Stanford et a été professeur de télécommunications à l'Universidad de los Andes au Venezuela de 1970 à 2000. Ermanno peut être atteint par courriel électronique à l'adresse ermanno@ictp.it

Marco Zennaro. Marco a reçu une maîtrise en génie électronique de l'Université de Trieste en Italie. Il a ensuite défendu une thèse de doctorat sur le sujet «Wireless Sensor Networks pour le développement : Potentialités et

questions ouvertes" à KTH -Royal Institute of Technology, Stockholm, en Suède. Ses intérêts de recherche se focalisent sur l'utilisation des TIC pour le développement (en anglais ICT4D). Il s'intéresse en particulier aux réseaux sans fil et l'utilisation des réseaux de capteurs pour les pays en développement. Marco a organisé des conférences sur les technologies sans fil dans plus de 20 pays différents. Lorsqu'il ne voyage pas, il est le rédacteur en chef de wsnblog.com. Marco peut être atteint par courriel électronique à l'adresse mzennaro@ictp.it

Carlo Fonda est un membre de l'unité des communications radio du Centre international Abdus Salam de physique théorique de Trieste, en Italie. Carlo peut être atteint par courriel électronique à l'adresse cfonda@ictp.it

Stephen Okay. Steve est un geek-à-tout-faire (en anglais geek-of-all-trades) ayant plus de 20 ans d'expérience dans les systèmes/programmation réseau et d'administration avec une passion particulière pour les réseaux et les logiciels libres/ouverts. Il a déployé des réseaux sans fil au Laos, au Malawi, en Italie et aux États-Unis. Il est co-fondateur d'Inveneo et a enseigné dans les ateliers sur la voix sur Internet (VoIP) et des réseaux sans fil dans des nombreux établissements à travers le monde. Il vit et hack à San Francisco, en Californie. Steve peut être atteint par courriel électronique à l'adresse steve@inveneo.org

Corinna " Elektra " Aichele. Elektra a travaillé sur des protocoles de réseaux maillés pour la communauté Freifunk en Allemagne. Avant d'inventer le protocole de routage pour les réseaux maillés sans fil B.A.T.M.A.N en 2006, elle a travaillé sur l'amélioration du protocole de routage OLSR. Elle est l'une des personnes derrière le dispositif Mesh-Potatoe, un routeur WiFi matériel ouvert robuste ayant un port FXS . Elle fait partie de la communauté Villagetelco, qui s'efforce de déployer des réseaux maillés pour la VoIP et les données. Elle vit dans une maison solaire à Berlin, en Allemagne. La philosophie derrière ses idées sur la communication omniprésente pour tous se résume en ceci: «Le fait que vous parlez dans votre tête ne signifie pas que vous pensez - mais seulement que vous vous parlez à vous-même".
Elektra peut être atteinte par courriel électronique à l'adresse
elektra@villagetelco.org.
http://villagetelco.org
http://open-mesh.net/

Sebastian Buettrich. Sebastian est gestionnaire du laboratoire de recherche de l'Université IT de Copenhague, http://pit.itu.dk. Il travaille avec les systèmes systèmes embarqués/pervasifs, la technologie sans fil, les logiciels open gratuits/libres et l'énergie solaire pour construire des réseaux, des systèmes, des compétences et créer la capacité en tant que gestionnaire, développeur, architecte, consultant et enseignant. Le travail de Sebastian s'est focalisé sur (mais sans s'y limiter) les pays en développement et les communautés, en particulier en Asie et en Afrique. Un de ses intérêts actuels est d'aider à développer les réseaux de campus pour la recherche et l'éducation, en mettant l'accent sur l'intégration mondiale et la durabilité. Ses affiliations actuelles secondaires sont : http://www.nsrc.org - le Centre de démarrage réseau de ressources http://wire.less.dk - ONG et de la société co- fondée avec Tomas Krag http://wirelessU.org - un groupe de professionnels dévoués qui travaillent à un, à dimension humaine, inclusive http://wndw.net/ société de l'information à l'échelle mondiale -
Co- auteur de la mise en réseau sans fil dans le livre monde en développement . Sébastien est titulaire d'un doctorat en physique quantique de l'Université technique de Berlin en Allemagne, avec un accent sur l'optique, la spectroscopie radio, les systèmes photovoltaïques et de la programmation scientifique. Il aime et joue de la musique, et est fasciné et engagé avec le texte, la langue et la poésie sous de nombreuses formes.
Sebastian peut être atteint par courriel électronique à l'adresse
sebastian@less.dk

Jim Forster . Jim est un passionné de l'expansion de l'Internet. Il a commencé sa carrière avec Cisco en 1988 quand il était tout petit et y a passé 20 ans, la plupart du temps travaillant dans le développement du logiciel IOS et l'architecture des systèmes puis ensuite comme un ingénieur distingué. Jim a commencé à travailler sur des projets et des politiques visant à améliorer l'accès à Internet dans les pays en développement pendant qu'il était chez Cisco. Présentement, il est engagé dans des efforts à but lucratif et non lucratif visant à étendre les communications en Afrique et en Inde. Jim est un des fondateurs de networktheworld.org, une fondation dédiée à l'amélioration des communications et de l'Internet, en particulier en Afrique et en Inde. Il siège sur plusieurs conseils d' administration, y compris Range Networks/ OpenBTS et Inveneo aux États-Unis, Esoko Networks au Ghana, et AirJaldi en Inde.
Jim peut être atteint par courriel électronique à l'adresse
jforster@networktheworld.org

Klaas Wierenga . Klaas travaille dans le groupe de recherche et de développement avancée de Cisco Systems, où il se focalise sur les problèmes d'identité, la sécurité et la mobilité, souvent en collaboration avec la communauté de la recherche et de l'éducation . Il est co-auteur du livre Cisco Press "Building the Mobile Internet ". Avant de joindre Cisco, il a travaillé à SURFnet, le réseau de recherche et d'éducation néerlandais, où il créa le service d'itinérance WiFi global dans le milieu universitaire appelé eduroam. Il est aussi le président du groupe de travail Mobilité de TERENA, l'association européenne de réseaux de recherche et d'éducation. Klaas participe dans un nombre de groupes de travail de l'IETF dans les domaines de l'identité, la sécurité et de la mobilité et préside le groupe de travail abfab qui traite de l'identité fédérée pour des applications non-web. Il peut être atteint par courriel électronique à l'adresse klaas@wierenga.net.

Eric Vyncke . Depuis 1997, Eric a travaillé comme ingénieur distingué de Cisco dans le domaine de la sécurité aidant les clients à déployer des réseaux sécurisés. Depuis 2005, Eric a également été actif dans le domaine de l'IPv6. Notamment, il co-préside le Conseil IPv6 belge et dispose d'un site bien connu pour la surveillance des déploiements IPv6 : http://www.-vyncke.org/ipv6status/ Il est également professeur associé à l'Université de Liège en Belgique. Il participe à plusieurs groupes de travail de l'IETF traitant de sécurité ou de l'IPv6 .Eric peut être atteint par courriel électronique à l'adresse eric@vyncke.org.

Bruce Baikie. Bruce est un membre du groupe Broadband for Good d'Inveneo où il occupe le poste de directeur principal des initiatives pour la bande passante large. Il met à profit sa vaste expérience dans les secteurs de l'énergie et des télécommunications ainsi que 16 ans chez Sun Microsystems en tant qu'expert de l'industrie des télécommunications pour conseiller sur l'implémentation des projets ICT4D solaires. Ses domaines d'expertise comprennent: le réseautage sans fil, les centres edo-data, les systèmes d'alimentation de télécommunications DC, et l'énergie solaire. Bruce a publié de nombreux documents et articles sur les opérations des centres de données verts et l'énergie solaire dans le domaine d'ICT4D. Sa formation comprend un B.S. en génie mécanique de l'Université technologique du Michigan et des études supérieures en commerce international de l'Université du Wisconsin. Bruce est également un conférencier invité sur l'énergie solaire ICT4D au Centre international Abdus Salam de physique théorique de Trieste, en Italie. Au cours de ces deux dernières années, Bruce a guidé des

étudiants en ingénierie de l'Illinois Institute of Technology, l'Université de Colorado- Boulder, l'Université d'État de San Francisco, et l'Université d'État de San Jose dans la conception ICT4D et des projets en Haïti, Afrique de l'Ouest, et la Micronésie. Bruce peut être atteint par courriel électronique à l'adresse bruce@green-wifi.org

Laura Hosman . Laura est Professeur assistant en sciences politiques de l'Illinois Institute of Technology (IIT). Avant de joindre ITI, Professeur Hosman a occupé des positions de recherche postdoctorale à l'Université de California, Berkeley et l'Université de Southern California (USC) . Elle est détentrice d'un doctorat en économie politique et politique publique de l'USC. Ses recherches actuelles portent sur le rôle de l'information et de la technologie de la communication (TIC) dans les pays en développement, en particulier en termes de ses effets potentiels sur les facteurs socio-culturels, le développement humain et la croissance économique. Son travail se concentre sur deux domaines principaux : Partenariats public-privé et la TIC dans l'éducation, avec un accent sur les pays en développement. Son blog, donnant un aperçu sur ses expériences sur le terrain, se trouve sur l'url http://ict4dviewsfromthefield.wordpress.com

Michael Ginguld . Michael est Fondateur, Directeur-Stratégie et des Opérations de Rural Broad Band Pvt. Ltd. Il est également Co-fondateur et PDG d'AirJaldi Research and Innovation. Michael est né et a grandi dans le kibboutz de Kissufim en Israël. Il a plus de 20 ans d'expérience de travail dans les projets TIC, développement communautaire et rural de l'Inde, l'Indonésie, le Cambodge, le Népal et Israël. Michael a travaillé dans le secteur à but lucratif et non lucratif avec les organisations de base de démarrage, des groupes de défense des droits, des grandes ONG internationales et des entreprises commerciales travaillant dans les pays en développement. Michael a vécu et travaillé à Dharamsala entre 1998 et 2002 et est retourné en Inde au début de 2007 pour participer à une initiative de connectivité rurale qui a finalement conduit à la création de AirJaldi Research and Innnovation, une organisation à but non lucratif dédiée à la recherche et développent et renforcement de capacité dans le domaine des réseaux sans fil en 2007, et de RBB, une organisation à but lucratif travaillant sur la conception, le déploiement et la gestion des réseaux ruraux à large bande dans les zones rurales en 2009. Michael est titulaire d'un baccalauréat ès sciences en Economie Agricole de l'Université hébraïque de Jérusalem en Israël, d'une maîtrise en études du développement de l' Institut d'études sociales de La Haye au

Pays-Bas, et d'une maîtrise en administration publique de la Kennedy School of Government de l'Université de Harvard, Cambridge aux USA. Michael est basé à Dharamsala, Himachal Pradesh en Inde. Il peut être atteint par courriel électronique à l'adresse Michael@airjaldi.net.

Emmanuel Togo. Emmanuel est du Ghana. Il a obtenu son premier diplôme en informatique et physique de l'Université du Ghana en 1999. Il travaille actuellement en tant que chef de l'unité de réseautage des systèmes informatiques de l'université du Ghana (UGCS). Il est également un membre fondateur de l'équipe technique du réseau GARNET travaillant à construire le réseau national de recherche et d'éducation au Ghana. L'objectif actuel d'Emmanuel est la conception et le déploiement d'un réseau campus WiFi abordable à grande échelle au Ghana. Emmanuel peut être atteint par courriel électronique à l'adresse ematogo@ug.edu.gh

The Open Technology Institute, (qui a fourni une étude de cas), renforce les individus et les communautés à travers la recherche de politiques, l'apprentissage et l'innovation technologique.

Soutien Technique

L'équipe de rédaction tient tout particulièrement à souligner le soutien de notre illustrateur technique, Paolo Atzori, qui a pendant plusieurs mois travaillé sans relâche pour assurer que le livre a quelques illustrations merveilleuses ainsi que précises et facile à lire. Il a aussi veillé à ce que nous soyons en mesure de publier avec succès plusieurs versions du livre en format haute et basse résolution.

Paolo Atzori. Paolo a étudié l'architecture à Venise et à Rome ainsi que les arts médiatiques en Cologne. Après avoir travaillé comme architecte à Viennes, Paolo a collaboré avec l'Académie des Arts et Médias de Cologne (KHM). Il travailla ensuite au NABA de Milan où Il fut nommé directeur de la maîtrise en conception environnemental numérique et conseiller du programme de doctorat de la Planetary Collegium, M-Node. Il a créé de nombreux projets théâtraux et artistiques, introduisant des nouvelles représentations de l'espace caractérisé par la dynamique de l'omniprésence et de l'interaction. Paolo a également organisé des expositions dédiées aux arts numériques, des programmes éducatifs dirigés, et a publié des articles et des essais sur la culture numérique. Il a vécu et travaillé à Venise, Rome, New

York, Viennes, Cologne, Bruxelles, et Tel Aviv. Il vit depuis 2005 à Trieste, en Italie avec sa partenaire Nicole et leurs enfants Alma et Zeno.
En 2011, il fonda avec Nicole Leghissa l'Agence « hyphae» .
http://hyphae.org
http://vimeo.com/groups/xtendedlab/videos
http://www.xtendedlab.com/
http://www.khm.de/ ~ Paolo

Les auteurs et éditeurs des versions antérieures du livre

Rob Flickenger. Rob a écrit et édité plusieurs livres sur les réseaux sans fil et Linux, y compris «Wireless Hacks» (O'Reilly) et «How To Accelerate Your Internet» (http://bwmo.net/). Il est fier d'être un hacker, amateur scientiste fou, et promoteur de réseaux gratuits partout.

Laura M. Drewett est un co-fondateur de Adapted Consulting Inc., une entreprise sociale qui se spécialise dans l'adaptation de solutions technologiques et commerciales pour les pays 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. Laura est titulaire d'un baccalauréat ès arts avec distinction en affaires étrangères et en français de l'Université de Virginie et d'une maîtrise en gestion de projet de l'École de commerce de l'Université George Washington.

Alberto Escudero - Pascual et Louise Berthilson sont les fondateurs d'IT +46, une société de conseil suédoise mettant l'accent sur la technologie de l'information dans les régions en développement.Plus d'informations peuvent être trouvées à l'url http://www.it46.se/

Ian Howard. Après un tour du monde pendant sept ans comme parachutiste de l'armée canadienne, Ian Howard a décidé d'échanger son arme pour un ordinateur. Après avoir terminé un diplôme en sciences de l'environnement à l'Université de Waterloo, il a écrit dans une proposition, « la technologie sans fil a la possibilité de combler la dividende numérique. Les pays pauvres, qui n'ont pas d'infrastructure pour l'inter connectivité comme nous, vont maintenant être en mesure de créer une infrastructure sans fil. » Comme récompense, Geekcorps l'envoya au Mali comme Gestionnaire de programme de Geekcorps Mali, où il dirigea une équipe chargée d'équiper

des stations de radio avec des interconnexions sans fil et conçut des systèmes de partage de contenu.

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

Tomas Krag passe ses journées à travailler avec wire.less.dk, une organisation à but non lucratif basée à Copenhague, qu'il a fondé avec son ami et collègue Sebastian Buttrich au début de 2002. wire.less.dk est spécialisée dans les solutions de réseaux sans fil communautaires et met un accent particulier sur les réseaux sans fil à faible coût pour les pays en développement. Tomas est également un associé de la Tactical Technology Collective http://www.tacticaltech.org, une association à but non lucratif basée à Amsterdam pour « renforcer les mouvements et réseaux sociaux technologiques dans les pays en développement et en transition, ainsi que promouvoir une utilisation des nouvelles technologies efficace, consciente et créative par la société civile ». Actuellement, la plupart de son énergie va dans le Wireless Roadshow (http://www.thewirelessroadshow.org), un projet qui soutient des partenaires de la société civile dans les pays en développement dans la planification, la construction et la maintenance de solutions de connectivité basées sur le spectre sans licence, la technologie ouverte et la connaissance ouverte .

Gina Kupfermann est 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 divers projets communautaires auto-organisés et des organisations à but non lucratif. Depuis 2005, elle est membre du conseil exécutif de l'association de développement de réseaux libres, l'entité juridique de freifunk.net

Adam Messer. Initialement formé en tant que scientifique en insectes, Adam Messer s'est métamorphosé en professionnel des télécommunications après qu'une conversation fortuite en 1995 l'aie emmené à démarrer l'une des premières sociétés de fournisseurs de services Internet de l'Afrique. Pionnier des services de données sans fil en Tanzanie, Messer a travaillé pendant 11 ans en Afrique orientale et australe dans les communications vocales et données pour les startups et les opérateurs de téléphonie mobile multinationales . Il habite maintenant à Amman, en Jordanie.

Juergen Neumann (http://www.ergomedia.de) a commencé à travailler avec la technologie de l'information en 1984 et depuis lors, a été à la recherche de moyens pour déployer les TIC de manière utile pour les organisations et la société. En tant que consultant pour la stratégie et la mise en œuvre des TIC, il a travaillé pour de grandes entreprises allemandes et internationales et des nombreux projets à but non lucratif. En 2002, il co-fonda www.freifunk.net, pour la diffusion des connaissances et le réseautage social sur les réseaux libres et ouverts. Freifunk est globalement considéré comme l'un des projets communautaires les plus efficaces dans ce domaine.

Frédéric Renet est un co-fondateur des solutions techniques chez 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 dans le début des années 1990 avec un système de bulletin de bord 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'un an à l'IESC/Geekcorps au Mali en tant que consultant. À ce titre, il a conçu de nombreuses solutions innovatrices pour la bande de radiodiffusion FM, des laboratoires informatiques de l'école et les systèmes d'éclairage pour les communautés rurales.

Contents

INTRODUCTION

Ce livre a pour objectif de donner aux individus le pouvoir de construire des réseaux DIY (Faites-le vous-même) en utilisant des technologies sans fil. Il a été rédigé par un groupe de fanatiques (geeks) du réseautage qui ont participé à la conception, le déploiement et l'exploitation de réseaux sans fil depuis un certain temps, chacun d'entre eux participant activement à l'expansion de la portée de l'Internet partout dans le monde.

Nous croyons que les individus peuvent avoir une importante participation dans la construction de leurs propres infrastructures de communication et en même temps influencer la grande communauté autour d'eux en s'assurant que les réseaux deviennent moins coûteux et disponibles. Nous espérons non seulement vous convaincre que c'est possible, mais aussi vous montrer comment nous l'avons fait, en vous donnant les informations et les outils dont vous auriez besoin pour démarrer un projet de réseau dans votre communauté locale. En offrant aux individus de votre communauté locale un accès à l'information moins coûteux et facile, ils bénéficieront directement de ce que l'Internet a à offrir. Le temps et les efforts fournis pour l'accès au réseau mondial de l'information se traduit en valeur à l'échelle locale. De même, le réseau devient de plus en plus valable aussi longtemps que beaucoup plus de gens y sont connectés.

Les communautés qui sont connectés à l'Internet à haute vitesse ont une voix dans un marché global où les transactions se font à travers le monde à la vitesse de la lumière. Partout dans le monde, les gens se rendent compte que l'accès à Internet leur donne une voix pour discuter de leurs problèmes, de la politique, ainsi que tout ce qui est important dans leur vie, d'une manière que le téléphone et la télévision ne peuvent tout simplement pas rivaliser. Ce qui jusque récemment semblait comme de la science-fiction est en train de devenir une réalité, et cette réalité est en train de se construire sur des réseaux sans fil.

Le Pays d'AIPOTU

Maintenant passons un moment à regarder un pays fictif dans le monde en développement appelé 'AIPOTU'. Aipotu a été connecté à Internet simplement par des liens VSAT coûteuses pour un moment très long.

Une nouvelle liaison de télécommunication optique sous-marine est finalement arrivée à la côte d'Aipotu.

En partant de zéro, AIPOTU a maintenant un défi de déployer une infra-

structure de communication couvrant tout un pays.
Aujourd'hui, la méthode de choix est probablement une stratégie à trois niveaux. D'abord et avant tout, AIPOTU devrait essayer d'établir des lignes à fibre optiques partout où cela est possible. Les lignes de fibre offrent la possibilité de transporter un «océan de bande passante». Le coût de la fibre optique est très faible, compte tenu de sa capacité. En améliorant les émetteurs-récepteurs optiques, la capacité d'une ligne de fibre optique peut être améliorée sans poser un nouveau câble. Si AIPOTU peut se permettre d'établir une connexion fibre pour chaque famille, il n'y a aucune raison de ne pas le faire. Cela rendrait notre modèle à trois niveaux inutile et nous pourrions nous arrêter là.
Cependant, il y a probablement des zones d'AIPOTU qui ne peuvent pas se permettre des lignes de fibre optiques.
Le deuxième niveau que les gens d'AIPOTU peuvent utiliser pour connecter les villages isolés ou des petites villes est d'utiliser des liaisons point-à-point à grande vitesse entre les points élevés.
Il est possible d'établir des liaisons à haut débit (40 Mbps) de 30 km ou plus entre les pilonnes de 30 mètres de hauteur sur un terrain plat.
Si les sommets des montagnes, collines ou des bâtiments élevés sont disponibles, des liaisons encore plus longues pourraient être établies. Les experts en technologie de réseau d'AIPOTU n'ont pas à trop se soucier de la technologie sans fil utilisée au-dessus de leurs pilonnes- le coût consiste principalement dans la construction des pilonnes, une protection appropriée contre la foudre, les alimentations en courant, l'alimentation de secours et la protection contre le vol, plutôt que dans le matériel sans fil actuel et les antennes.
De même que la technologie d'émetteurs-récepteurs optiques, les émetteurs-récepteurs sans fil continuent aussi à avancer.
Cependant une liaison sans fil sera toujours de plusieurs ordres de grandeur inférieure à la capacité de la fibre optique. Le troisième défi pour AIPOTU est de résoudre le problème du dernier kilomètre (en anglais last mile): distribution d'accès à tous les ménages, aux bureaux, aux installations de production et autres.
Pas trop longtemps, la méthode de choix était de déployer les fils de cuivre, mais actuellement un meilleur choix existe.
Ce troisième volet de notre modèle de réseau appartient clairement au domaine de la technologie de réseau sans fil .

Bût de ce livre

L'objectif global de ce livre est de vous permettre de construire une technologie de communication accessible dans votre communauté locale, en faisant le meilleur usage de toutes les ressources disponibles. En utilisant un équipement peu onéreux, vous pouvez construire des réseaux de données à grande vitesse qui seront capables de connecter des zones éloignées entre-elles, fournir un accès réseau à large bande dans les zones sans service téléphonique et finalement connecter vos voisins et vous-même à l'Internet global. En utilisant des sources de matériaux locales et fabriquant vous-même certaines parties, vous pouvez construire des liaisons de réseau fiables avec un budget très restreint et travaillant avec votre communauté locale, vous pouvez construire une infrastructure de télécommunication profitable à tous ceux qui y participent.

Ce livre n'est pas un guide pour configurer le sans fil pour votre ordinateur 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 utilisées comme une épine dorsale pour les grands réseaux sans fil ainsi que la résolution du problème du dernier kilomètre.

Avec ces objectifs à l'esprit, 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 incluse dans ce livre présente les expériences de divers groupes dans la construction de ces réseaux, les ressources qui y ont été investies, ainsi que résultats de ces expériences.

Il est également important de noter que toutes les ressources, les techniques et les méthodologies de conceptions décrites dans ce livre sont valables dans n'importe quelle partie du monde.

Il y a beaucoup de zones rurales à travers le monde entier qui ne sont pas connectées à l'Internet pour des raisons de coût, la géographie, la politique et autres. Le déploiement du réseautage sans fil peut souvent conduire à résoudre ces problèmes et ainsi étendre la connectivité à ceux qui n'ont pas encore été connectés.

Il y a beaucoup de projets de réseaux communautaires émergents partout.

Ainsi, si vous vivez au Royaume-Uni, Kenya, au Chili, en Inde ou ailleurs, ce livre peut être un guide pratique utile.

Depuis les toutes premières expériences à la fin du XIX siècle, le sans-fil a été un domaine des technologies de communication en évolution rapide.

Bien que nous fournissions des exemples spécifiques sur la façon de construire des liaisons de données à haute vitesse, les techniques décrites dans ce livre ne sont pas destinées à remplacer l'infrastructure filaire existant (comme les systèmes téléphoniques ou la dorsale à fibre optique). Au contraire, ces techniques visent à augmenter les systèmes existants, et fournir la connectivité dans les zones où le déploiement de la fibre ou un autre câble physique serait impraticable. Nous espérons que vous trouverez ce livre utile pour résoudre vos défis de communication.

Intégration du sans-fil dans votre réseau existant

Si vous êtes un administrateur de réseau, vous pouvez vous demander comment le sans-fil peut s'intégrer dans votre infrastructure réseau existante. Le sans-fil peut servir à des nombreux titres, en commençant par une simple extension (comme un câble Ethernet de plusieurs kilomètres) jusqu'à un point de distribution (comme un grand hub). Voici quelques exemples de la façon dont votre réseau peut bénéficier de la technologie sans fil.

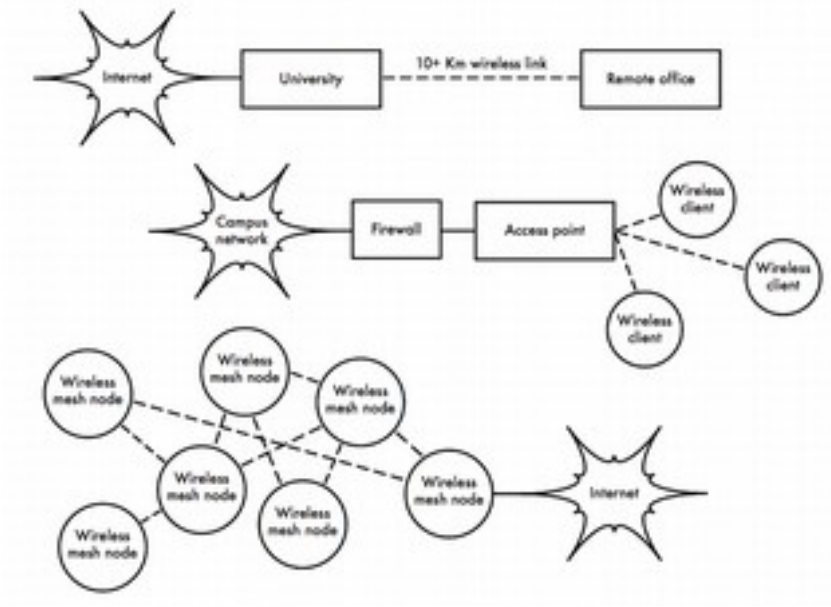


Figure I 1: Quelques exemples de réseautage sans fil.

Comment ce livre est organisé

Ce livre contient 4 sections principales dénommées -

Physique
Réseautage
Planification et de déploiement
Entretien, surveillance et soutenabilité

A la fin de ce livre, vous trouverez un glossaire ainsi que les appendices et les études de cas. Dans les quatre sections principales, il y a des chapitres rédigés par des experts qui ont une expérience théorique et pratique de ces sujets. Il y a un large éventail de sujets dans les chapitres qui ont été sélectionnés comme étant la clé vous permettant de démarrer et étendre un déploiement sans fil véritable dans votre propre communauté.

Une autre ressource que vous pourriez trouver utile se trouve sur la page Web ci-dessous:
http://wtkit.org/groups/wtkit/wiki/820cb/download_page.html

Cette page Web contient l'ensemble des documents de présentation utilisés par ces mêmes experts clés pour offrir des cours de formation de réseau sans fil dans le monde entier.
En outre, tous les experts clés qui ont écrit ce livre consultent régulièrement notre page Facebook. Ainsi lorsque vous planifiez votre déploiement sans-fil, veuillez s'il vous plaît poster des questions sur notre page - nous répondrons rapidement.
https://www.facebook.com/groups/wirelessu/

PHYSIQUE

1. 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 toute autre connexion réseau : votre navigateur Internet, courriel électronique et autres applications fonctionnent de la même façon. Mais comparées au câble Ethernet, les ondes radio ont des propriétés inattendues. Par exemple, il est très facile de voir le chemin pris par un câble Ethernet : localisez la prise sortant de votre ordinateur, suivez le câble jusqu'à l'autre extrémité, et vous l'avez trouvé! Vous pouvez également être certain que l'utilisation de plusieurs câbles Ethernet les uns à côté 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 ? Qu'advient-il lorsque ces ondes rebondissent sur les objets dans la salle ou sur d'autres bâtiments s'il s'agit d'un lien extérieur? Comment plusieurs cartes sans fil peuvent être utilisées dans la même secteur sans interférer les uns avec les autres ? Afin de construire des liaisons sans fil stables et à haut débit, il est important de comprendre comment les ondes radio se comportent dans le monde réel .

Qu'est-ce qu'une onde ?

Nous sommes tous familiers avec les vibrations ou des oscillations sous diverses formes : une pendule, un arbre se 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 de façon périodique, avec un certain nombre de cycles par unité de temps. Ce genre d'onde est parfois appelée une onde **mécanique**, puisqu'elle est définie par le mouvement d'un objet ou de son milieu de propagation. Quand des telles oscillations voyagent (c'est-à-dire quand l'oscillation ne reste pas attaché à un seul endroit), nous parlons 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 ensuite les lèvres du chanteur pour entreprendre un voyage, à la vitesse du son. Une pierre plongeant dans un lac cause une perturbation qui se déplace ensuite à travers le lac comme une onde.

Une onde a une certaine **vitesse**, **une fréquence et une longueur d'onde.**

Celles-ci sont reliées par une relation simple :

*Vitesse = Fréquence * Longueur d'onde*

La longueur d'onde (parfois appelée **lambda**, λ) est la distance séparant deux crêtes successives d'une onde périodique (ou, de manière plus technique, d'un point au point suivant qui est dans la même phase), par exemple à partir du sommet d'une crête à l'autre. La fréquence est le nombre d'ondes entières qui passent par un point fixe en une période de temps. La vitesse est mesurée en mètres/seconde, la fréquence est mesurée en cycles par seconde (ou Hertz, représenté par le symbole **Hz**), et la longueur d'onde est mesurée en mètres . Par exemple, si onde se déplace sur l'eau à un mètre par seconde, et elle oscille cinq fois par seconde, alors chaque one aura une longueur de vingt centimètres:

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

Les vagues ont également une caractéristique dénommée amplitude. C'est la distance entre le centre d'une onde et l'extrémité d'une de ses crêtes, et peut être illustrée comme étant la "hauteur" d'une vague d'eau. La fréquence, la longueur d'onde et l'amplitude sont illustrées dans la figure RP 1.

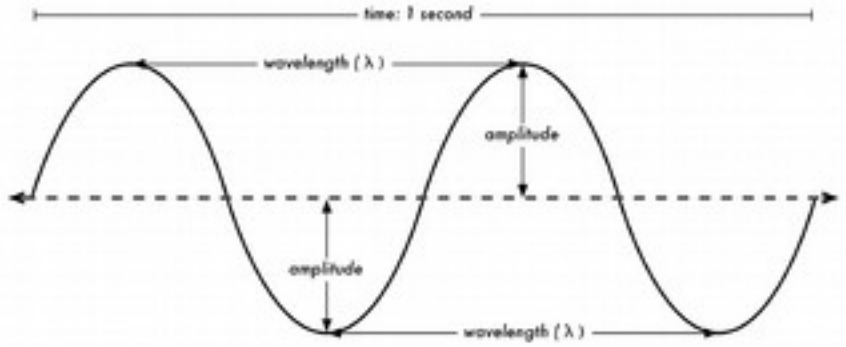


Figure RP 1: Figure RP 1 : Longueur d'onde, amplitude et fréquence. Pour cette onde, la fréquence est de 2 cycles par seconde, ou 2 Hz, alors que la vitesse est de 1 m/s.

Les ondes dans l'eau sont faciles à visualiser. Il suffit de laisser tomber une

pierre dans le lac et vous verrez les ondes se déplaçant dans 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?". Pour comprendre cela, vous devez comprendre les forces électromagnétiques.

Les forces électromagnétiques

Les forces électromagnétiques sont les forces entre les charges et les courants électriques. 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 chargées, mais ce sont les électrons qui sont responsables de l'essentiel de ce que nous avons besoin de connaître sur la façon dont les ondes radios se comportent. Regardons ce qui se passe dans un morceau de fil de fer droit vertical dans lequel nous enfonçons les électrons d'un bout à l'autre et vice-versa. A un moment donné, le dessus du fil est chargé négativement – tous les électrons y sont recueillis. Ceci crée un champ électrique le long du fil à partir de l'extrémité chargée positivement à celle chargée négativement. L'instant suivant, tous les électrons ont tous été conduits à l'autre extrémité, et le champ électrique va dans l'autre sens. Lorsque ceci se produit de façon répétitive, les vecteurs de champ électrique (représentés par des 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 (à cause des deux pôles différemment chargés, le plus et le moins, qui sont créés dans le fil de fer vertical droit), ou plus communément une ***antenne dipôle***. C'est la forme la plus simple d'antenne omnidirectionnelle. Le champ électrique mobile est communément appelé une onde électromagnétique car il y a aussi un champ magnétique y associé.
Un champ électrique mobile, comme une onde, accompagne toujours avec un champ magnétique - vous ne trouverez pas l'un sans l'autre. Pourquoi est-ce le cas ? Un champ électrique est créé par des objets chargés électriquement.
Un champ électrique mobile est produit par le déplacement des objets char-

gés électriquement, comme décrit ci-dessus pour une antenne dipôle.
Partout où les charges électriques se déplacent, elles causent un champ magnétique.

Ceci est mathématiquement formulé dans les équations de Maxwell:
https://en.wikipedia.org/wiki/Electromagnetic_0eld#Mathematical_description

Étant donné que les composantes électriques et magnétiques sont liées ensemble de cette façon, nous parlons d'un champ électromagnétique. Dans le réseautage sans fil pratique, nous nous concentrons sur la composante électrique, mais il y avoir toujours aussi une composante magnétique.
Revenons à la relation:

$$Vitesse = Fréquence * Longueur\ d'onde$$

Dans le cas des ondes électromagnétiques, la vitesse c c'est la vitesse de la lumière.

$$c = 300{,}000\ km / s = 300.000.000\ m / s = 3 * 108\ m / s$$
$$c = f * \lambda$$

Les ondes électromagnétiques diffèrent des ondes mécaniques en ce qu'elles ne requièrent aucun support pour se propager. Les ondes électromagnétiques se propagent même à travers le vide parfait. La lumière des étoiles est un bon exemple : elle nous parvient à travers l'espace vide.

Symboles du système international d'unités.

En physique, mathématiques et ingénierie, les nombres sont souvent exprimés par des puissances de dix. Nous utiliserons également ces termes et les symboles utilisés pour les représenter, par exemple le gigahertz (GHz), centimètre (cm), microsecondes (μs), et ainsi de suite.
Ces symboles font partie du système international de mesure **SI** (http://www.bipm.org/utils/common/pdf/si_brochure_8_en.pdf),ce ne sont pas des abréviations et ne devraient pas être modifiés.
La conversion majuscule/minuscule est importante et ne doit pas être altérée.

Symboles SI

atto	10^{-18}	1/1000000000000000000	a
femto	10^{-15}	1/1000000000000000	f
pico	10^{-12}	1/1000000000000	p
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}	1000	k
mega	10^{6}	1000000	M
giga	10^{9}	1000000000	G
tera	10^{12}	1000000000000	T
peta	10^{15}	1000000000000000	P
exa	10^{18}	1000000000000000000	E

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

$$f = 2.4\ GHz = 2400000000\ cycles/seconde$$
$$Longueur\ d'onde\ (\lambda) = c/f = 3 * 10^{8} / 2{,}4 * 10^{9} = 1{,}25 * 10^{-1}\ m = 12{,}5\ cm$$

La fréquence et par conséquent la longueur d'onde déterminent globalement le comportement d'une onde électromagnétique. Elle régit les dimensions des antennes que nous construisons ainsi que les interactions avec les objets qui sont dans le chemin de propagation, y compris les effets biologiques des êtres vivants. Les standards sans fil se distinguent bien sûr par plus que juste leur fréquence de fonctionnement - par exemple, les standards 802.11b, 802.11g, 802.11n et 802.16 peuvent tous travailler à 2,4 GHz, mais ils sont cependant très différents les uns des autres. Les techniques de modulation, les techniques d'accès aux médias, et d'autres ca-

ractéristiques pertinentes des normes de communication sans fil seront discutés dans le chapitre intitulé **Principes de base des télécommunications**.
Cependant, les caractéristiques de base des ondes électromagnétiques de pouvoir pénétrer les objets, parcourir des longues distances, et autres sont seulement déterminées par la physique. L'onde électromagnétique ‘’ne sait pas ou ne se soucie pas” de la modulation, du standard ou la technique qu’elle utilise. Ainsi, alors que différentes normes peuvent utiliser des techniques avancées pour faire face à l’absence de la ligne de mire (NLOS Non Line of Sight), aux chemins multiples et autres, elles ne peuvent toujours pas permettre une onde de traverser un mur si le mur absorbe la fréquence respective. Par conséquent, une compréhension des idées de base de fréquence et longueur d'onde aide beaucoup dans le travail sans fil pratique.

Phase

Plus loin dans ce chapitre, nous allons parler de concepts reliés à l’interférence, les chemins multiples et les zones de Fresnel. Pour comprendre cela, nous aurons besoin de connaître la phase d'une onde, ou plutôt, les différences de phase entre les ondes. En regardant l'onde sinusoïdale présentée par la figure 1 RP, imaginez maintenant que nous avons deux de ces ondes en mouvement. Celles-ci peuvent être exactement dans la même position : Lorsque l'une est à sa crête, l'autre est également a atteint sa crête. Dans ce cas, nous dirions qu’elles sont en phase, ou leur différence de phase est nulle. Cependant, une one pourrait également se déplacer dans le sens opposé d’un autre, elle pourrait, par exemple, atteindre sa crête au point où l'autre onde est à zéro. Dans ce cas, nous avons un différence de phase. Cette différence de phase peut être exprimée en fractions de longueur d'onde comme par exemple λ / 4, ou en degrés comme par exemple 90 ° - avec un cycle complet de l'onde étant de 360 degrés. Une différence de phase de 360 degrés est le même que celui de 0 degrés : pas de différence de phase.

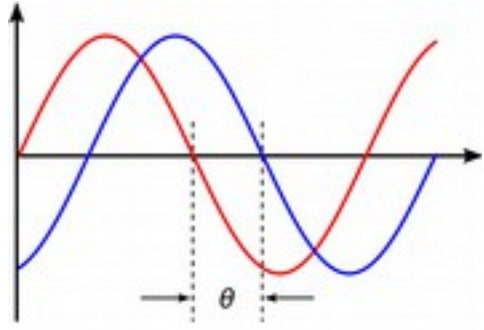


Figure RP 2: Différence de phase entre deux ondes.

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 de fer), les électrons ne peuvent se déplacer que vers le haut ou vers le bas, pas de travers (parce qu'il n'y a pas d'espace pour se déplacer) et donc des champs électriques pointent uniquement vers le haut ou vers le bas, verticalement. Le champ abandonnant le fil et voyageant comme une onde a une polarisation linéaire strict (et dans ce cas, verticale). Si nous déposons l'antenne à plat sur une surface, nous trouverions une polarisation linéaire horizontale.

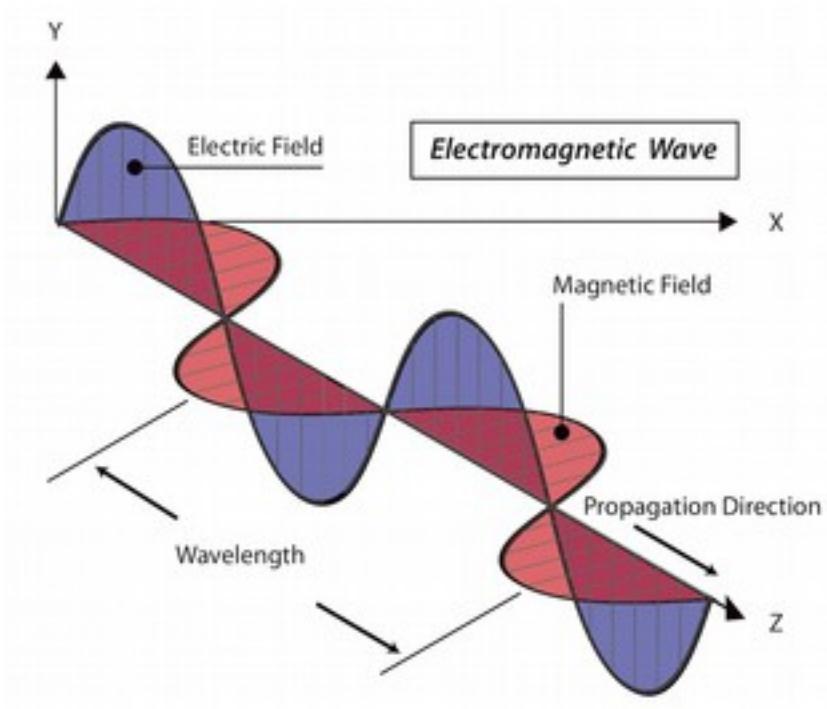


Figure RP 3: Onde magnétique polarizée verticalement

La polarisation linéaire n'est juste qu'un cas particulier, et n'est jamais tout à fait parfaite: en général, nous aurons toujours certaines composantes du champ pointant aussi vers d'autres directions.

Si nous combinons deux dipôles alimentés par le même signal, nous pouvons générer une onde polarisée circulairement, dans laquelle le vecteur champ électrique continue à tourner perpendiculairement à la trajectoire de l'onde. Le cas le plus général est la polarisation elliptique, dans laquelle la valeur maximale du vecteur champ électrique diffère dans les directions verticales et horizontale. Comme on peut l'imaginer, la polarisation devient importante lors de l'alignement des antennes. Si vous ignorez la polarisation, vous courrez le risque d'obtenir un signal très faible même si vous avez les meilleures antennes. On dit que cette polarisation est en déséquilibre (polarization mismatch en anglais).
De de la même façon, la polarisation peut également être utilisée de manière intelligente en vue de garder deux liaisons sans fil indépendantes et sans interférence, même si elles utilisent les mêmes extrémités (ou même si elles partagent le même relecteur) et donc la même trajectoire: si une liaison est polarisée verticalement et l'autre horizontalement, elles resteront indépendantes l'une de l'autre. L'application des polarisations différentes est un moyen pratique de doubler les débits de données sur une liaison utilisant une seule fréquence. Les antennes utilisées dans ce type d'application doivent être soigneusement construites afin de rejeter la polarisation ''indésirables", c'est à dire une antenne destinée à une polarisation verticale ne doit pas recevoir ou transmettre aucun signal polarisé horizontalement et vice versa. Nous disons qu'ils doivent avoir un grand rejet de ''polarisation croisée"(cross polarization en anglais).

Le spectre électromagnétique

Les ondes électromagnétiques couvrent une large gamme de fréquences (et par conséquent, les longueurs d'onde).
Cette gamme de fréquences ou de longueurs d'onde s'appelle 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 $7.5 * 10^{14}$ Hz et $3.8 * 10^{14}$ Hz, correspondant aux longueurs d'onde comprises entre 400 nm (Violet/bleu) et 800 nm (rouge).
Nous sommes également régulièrement exposés à d'autres régions du spectre électromagnétique, y compris le courant alternatif (CA) ou réseau électrique à 50/60 Hz, la radio AM et FM, l'ultraviolet (à des fréquences plus élevées que celles de la lumière visible), l'infrarouge (à des fréquences inférieures à celles de la lumière visible), Les rayons X, et bien d'autres .

Le terme Radio est utilisé pour la partie du spectre électromagnétique dans laquelle les ondes peuvent être transmises en appliquant un courant alternatif à une antenne. Ceci est valable pour la gamme des fréquences allant de 30 kHz à 300 GHz, mais dans le sens le plus étroit du terme, la limite supérieure de fréquence serait d'environ 1 GHz, au-dessus de laquelle on parle de micro-ondes et des ondes millimétriques. Quand on parle de radio, beaucoup de gens pensent de la radio FM, qui utilise une fréquence autour de 100 Mhz .Entre la radio et l'infrarouge, se trouve la région des micro-ondes - avec des fréquences d'environ 1 GHz à 300 GHz, et des longueurs d'onde de 30 cm à 1 mm. L'usage le plus populaire des micro-ondes pourrait être le four à micro-ondes, qui de fait utilise exactement la même région électromagnétique (plage d'ondes) que les normes sans fil dont il est question dans ce livre.
Cette région se situe dans les bandes électromagnétiques ouvertes pour usage général sans licence générale. Cette région est appelée bande ISM, signifiant une bande Industrielle, Scientifique et Médicale.

La plupart des autres parties du spectre électromagnétique sont étroitement contrôlées par la législation par licences, ces dernières constituant un facteur économique important.
Dans de nombreux pays, le droit d'utiliser des parties du spectre électromagnétique a été vendu à des entreprises de communication pour des millions de dollars.
Dans la plupart des pays, les bandes ISM ont été réservées pour un usage sans licence et donc n'exigent aucun payement quand elles sont utilisées.

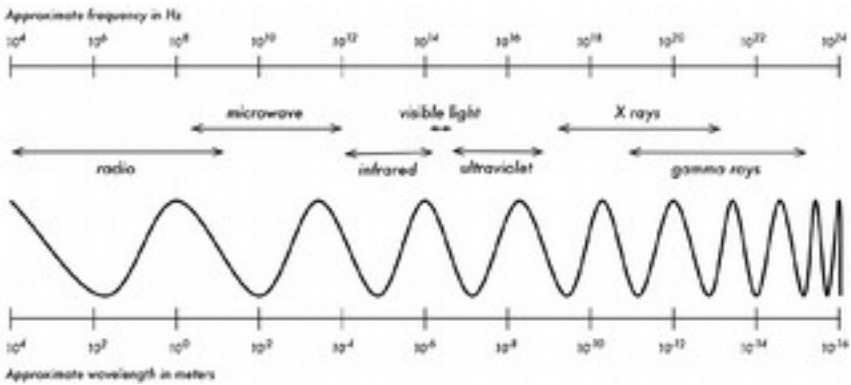


Figure RP 4: Le spectre électromagnétique.

Les fréquences les plus intéressants pour nous vont de 2400 à 2495 GHz, utilisées par les normes sans fil 802.11b et 802.11g (correspondant aux longueurs d'onde d'environ 12,5 cm), ainsi que les fréquences allant de 5,150 à 5,850 GHz (correspondant aux longueurs d'onde de l'ordre de 5 à 6 cm), utilisées par la norme sans fil 802.11a.

La norme 802.11n peut fonctionner dans l'une de ces deux bandes de fréquence. Referez-vous au chapitre intitulé ''Famille Wifi" pour un aperçu des normes et des fréquences. En outre, vous pouvez trouverez plus d'information sur la partie radio du spectre électromagnétique dans le chapitre intitulé ''Spectre Radioélectrique".

Largeur de bande

"Largeur de bande" est un terme que vous rencontrerez souvent en physique de la radio physique. La largeur de bande est simplement une mesure de la gamme de fréquence. Si une plage de 2,40 GHz à 2,48 GHz est utilisée par un périphérique, alors la largeur de bande serait 0,08 GHz (ou plus communément 80 MHz).

Il est facile de voir que la largeur de bande que nous définissons dans ce livre est étroitement liée à la quantité de données que vous pouvez y transmettre - plus il y a de l'espace dans la fréquence, plus des données que vous pouvez y inclure à un moment donné. Le terme largeur de bande est souvent utilisé pour quelque chose que nous devrions plutôt appeler taux de transmission de données, comme quand nous disons "ma connexion Internet a 1 Mbps de largeur de bande" pour signifier qu'elle peut transmettre des données à 1 mégabit par seconde.

Ce que vous pouvez transmettre exactement dans un signal physique dépendra de la modulation, du codage et d'autres techniques. Par exemple, la norme 802.11g utilise la même bande passante que la norme 802.11b, cependant, elle est transmet plus de données dans ces mêmes gammes de fréquence allant jusqu'à 5 fois plus de bits par seconde.
Un autre exemple que nous avons mentionné: vous pouvez doubler votre débit de données en ajoutant une seconde liaison ayant une polarisation perpendiculaire à celle d'une liaison radio existante. Dans ce cas, la fréquence et la bande passante n'ont pas changé, mais le débit de données est doublé.

Les fréquences et canaux

Penchons-nous un peu plus près sur l'utilisation de la bande 2,4 GHz dans la norme 802.11b.
Le spectre est divisé en parties de taille égale réparties sur la bande en canaux. Notez que les canaux sont de 22 MHz de largeur, mais ne sont séparés que par 5 MHz. Cela signifie que les canaux adjacents se chevauchent et peuvent interférer les uns avec les autres . Ceci est représenté visuellement dans la Figure RP 5.

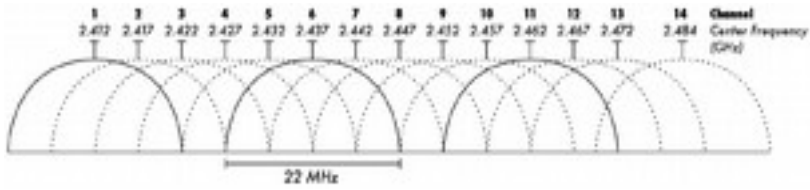


Figure RP 5: Canaux et fréquences centrales pour la norme 802.11b. Notez que les canaux 1, 6 et 11 ne se chevauchent pas.

Comportement des ondes radio

Il y a quelques règles simples qui peuvent s'avérer extrêmement utiles lors d'une planification initiale d'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 objets;
• plus courte est la longueur d'onde, plus de données celle-ci pourra transporter.

En dépit de la simplicité de ces règles, il est facile de les comprendre grâce a des exemples.

Les ondes plus longues voyagent plus loin

Les ondes de plus grande longueur d'onde ont tendance à voyager plus loin que les ondes à plus courte longueur d'onde. À titre d'exemple, les stations de radio AM ont une diffusent plus loin que les stations FM, qui utilisent une fréquence 100 fois plus élevée. A puissance égale, les émetteurs de plus basses fréquences ont tendance à atteindre des distances beaucoup plus grandes que les émetteurs à haute fréquence.

Les ondes plus longues contournent les obstacles

Une onde sur l'eau qui a une longueur de 5 mètres ne sera pas affectée par un morceau de bois de 5 mm flottant sur l'eau.
Si au contraire, le morceau de bois était de 50 mètres (par exemple un bateau), il modifierait le comportement de l'onde. La distance qu'une onde peut parcourir dépend de la relation entre la longueur de l'onde et la taille des obstacles sur son chemin de propagation. Il est plus difficile de visualiser le déplacement des ondes ''à travers" des objets solides, mais tel est le cas des ondes électromagnétiques. Les ondes de grande longueur d'onde (et conséquemment de fréquence inférieure) ont tendance à mieux pénétrer les objets que les ondes de courte longueur d'onde) (et donc de fréquence plus élevée). Par exemple, la radio FM (88-108 MHz) peut diffuser à travers les bâtiments et autres obstacles facilement, tandis que les ondes courtes (telles que celles utilisées par les téléphones GSM fonctionnant à 900 MHz ou 1800 MHz) ont plus de difficulté à pénétrer les bâtiments. Ceci est en partie dû à la différence de niveaux de puissance entre les radios FM et GSM, mais est également en partie à cause de la longueur d'onde plus courte des signaux GSM. Aux fréquences beaucoup plus élevées, la lumière visible ne passe pas à travers un mur ou même un morceau de bois de 1 mm - comme nous le savons tous, à travers l'expérience pratique. Mais le métal arrêtera tout type d'onde électromagnétique.

Les ondes plus courtes peuvent transporter plus de données
Le plus vite les ondes oscillent ou battent, le plus d'informations elles transporteront - chaque oscillation ou cycle pourrait être utilisé par exemple pour transporter un bit numérique, un '0 ' ou un '1', un ''oui" ou un ''non". Ainsi, le débit de données s'ajuste à la bande passante, et peut être encore amélioré par une modulation avancée et des techniques d'accès aux médias telles que l'OFDM et le MIMO (en anglais Multiple Input, Multiple Output).

Le principe de Huygens Il y a un autre principe qui peut être appliqué à tous les types d'ondes et qui est extrêmement utile pour comprendre la propagation des ondes radio. Ce principe est connu comme le **principe de Huygens,** en hommage à Christiaan Huygens, un mathématicien hollandais, physicien et astronome, de 1629 à 1695.
Imaginez que vous prenez un petit morceau de bâton et le plongez verticalement à la surface d'un lac immobile, causant ainsi une dance et oscillation de l'eau.
Les ondes abandonneront le centre du bâton - l'endroit où vous l'avez

plongé – en créant des cercles. Maintenant, chaque fois que des particules d'eau se balancent et dansent, elles provoqueront leurs particules voisines à faire de même : à partir de tout point de perturbation, une nouvelle onde circulaire va émerger. Ceci est, sous une forme simple, le principe d'Huygens. Dans les mots de wikipedia.org :
''Le principe d'Huygens est une méthode d'analyse qui s'applique aux problèmes de propagation des ondes dans la limite lointaine de son champ. Il reconnaît que chaque point d'un front d'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 des ondes permet de mieux comprendre une variété de phénomènes d'ondes, comme la diffraction. Ce principe est vrai pour les ondes radio ainsi que des ondes sur l'eau, pour le son et la lumière, mais la longueur d'onde de la lumière est beaucoup trop courte pour permettre aux êtres humains d'effectivement voir leurs effets directement. Ce principe nous aidera à comprendre la diffraction ainsi que des zones de Fresnel, et le fait que parfois nous semblons être en mesure de transmettre dans des coins, sans aucune ligne de vue. Penchons-nous maintenant sur ce qui se passe aux ondes électromagnétiques quand ils se propagent.

Absorption

Lorsque les ondes électromagnétiques passent à travers 'quelque chose' (certains matériaux), elles en sortent généralement affaiblies ou atténuées.
Ce qu'elles perdent en puissance dépendra 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 filtre une bonne partie de l'intensité lumineuse et la plupart du rayonnement ultraviolet. Souvent, un coefficient d'absorption est utilisé pour décrire l'impact d'un matériau sur le rayonnement .
Pour les micro-ondes, les deux principaux matériaux absorbants sont:
Métal . Les électrons peuvent se déplacer librement dans les métaux, et sont facilement capables d'osciller et ainsi absorber l'énergie d'une onde de passage.
Eau . Les micro-ondes font que les molécules d'eau se bousculent, capturant de ce fait une partie de l' énergie de l'onde. Pour les fins pratiques du réseautage sans fil, nous pouvons très bien considérer le métal et l'eau

comme des matériaux absorbeurs parfaits : nous ne serons pas en mesure de passer à travers eux (bien que des couches minces d'eau vous permettent le passage d'une certaine puissance). Ces matériaux sont à la micro-onde ce qu'est un mur de brique est à la lumière. Quand nous parlons de l'eau, nous devons nous rappeler qu'elle existe sous différentes formes : la pluie, le brouillard et la brume, des nuages bas et autres. L'eau sous toutes ses formes se présentera comme obstruction dans le chemin des liaisons radio. Elles ont une forte influence sur ces liaisons, et dans de nombreux cas, un changement climatique peut rompre une liaison radio. Quand on parle du métal, gardez à l'esprit qu'il peut se trouver dans des endroits inattendus: il peut être caché dans les murs (par exemple, les grilles métalliques dans le béton) ou être sous forme d'une couche mince de métal sur les types modernes de verre (verre teinté, verre coloré).

Cependant en dépit de sa minceur, la couche de métal pourrait être suffisante pour absorber de manière significative une onde 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. Le vieux bois sec mort est plus ou moins transparent tandis que le bois frais et humide absorbera beaucoup l'onde. Les matériaux plastiques et leurs similaires n'absorbent pas généralement beaucoup d'énergie radio, mais cela varie en fonction de la fréquence et du type de matériau. Enfin, parlons un peu de nous-mêmes: les humains. Notre constitution physique (ainsi que celle des animaux) est en grande partie faite d'eau. En ce qui concerne le réseautage, nous pouvons aussi bien être décrits comme des grands sacs d'eau, avec la même forte absorption des ondes.

Orienter un point d'accès dans un bureau de sorte que son signal doit passer par à travers plusieurs personnes est une erreur fondamentale lors de la conception des réseaux de bureaux. Ceci est également vrai pour les hotspots, des 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: le métal et les surfaces d'eau sont les principales sources de réflexion pour les ondes radio. Les règles de réflexion sont très simples : l'angle d'incidence d'une onde radio sur une surface plane est égal à son angle de réflexion.

Notez que dans le contexte d'une onde radio, un grille dense de métal est

perçue de la même façon qu'une surface solide, tant et aussi longtemps que la distance entre les barreaux est petite comparativement à la longueur d'onde. A 2,4 GHz, une grille d' un métal d'un centimètre agira de la même façon qu'une plaque métallique. Bien que les règles de réflexion soient assez simples, les choses peuvent devenir très compliquées quand vous imaginez un intérieur de bureau avec beaucoup, beaucoup de petits objets métalliques de formes variées et compliquées. La même chose vaut pour les situations extérieures urbaines : regardez autour de vous dans la ville et essayer de repérer tous les objets métalliques. Ceci explique pourquoi les effets par trajet multiples (c.-à-d. les signaux atteignant leur cible le long des chemins différents, et donc à des moments différents) jouent un rôle important dans le domaine du réseautage sans fil. Les surfaces d'eau où les vagues et les ondulations changent tout le temps sont effectivement l'objet d'une réflexion très compliquée qui est plus ou moins impossible à calculer et prévoir avec précision.

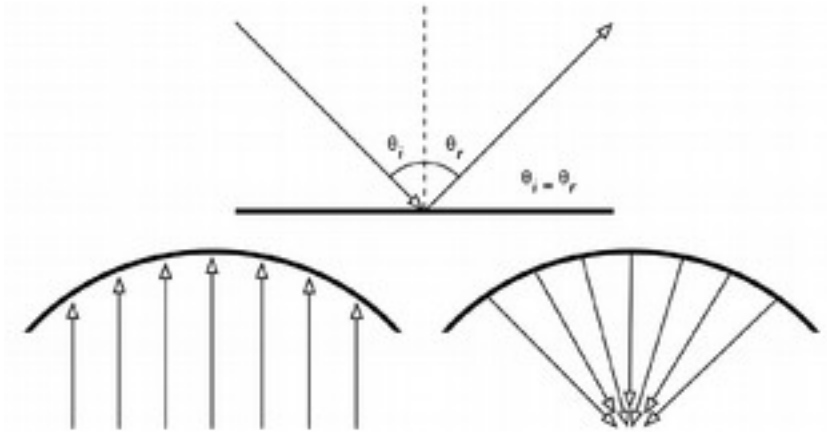


Figure RP 6: Réflexion des ondes radio. L'angle d'incidence est toujours égal à l'angle de réflexion. Une surface métallique parabolique utilise cet effet pour concentrer les ondes radio éparpillées autour d'elle dans une même direction.

Il faut aussi ajouter que la polarisation a un impact : les ondes de polarisation différente seront en général reflétées différemment.
Nous utilisons la réflexion à notre avantage dans la construction d'antennes: par exemple, nous installons des antennes paraboliques énormes derrière notre émetteur/récepteur de radio en vue de collecter et regrouper le signal radio en un seul point, le point focal.

Diffraction

La diffraction est le repli apparent des ondes lorsqu'elles frappent un objet. C'est l'effet de ''ondes tournant les coins". Imaginez une onde se propageant sur l'eau en un front d'onde droit, exactement comme une vague qui se forme une plage océanique.
Maintenant, plaçons une barrière solide, disons une clôture en bois massif, dans sa voie de manière à la bloquer. Nous avons taillé une ouverture en fente étroite dans ce mure, telle une petite porte. A partir de cette ouverture, une onde circulaire va se former, et elle atteindra naturellement des points qui ne sont pas en ligne droite derrière cette ouverture, mais également de chaque côté de celle-ci. Si vous regardez ce front d'onde – qui pourrait tout aussi bien être une onde électromagnétique - comme étant un faisceau de lumière (une ligne droite), il serait difficile d'expliquer comment elle peut atteindre des points qui devraient être masqués par un obstacle. Quand nous le modélisons comme un front d'onde, le phénomène devient logique.

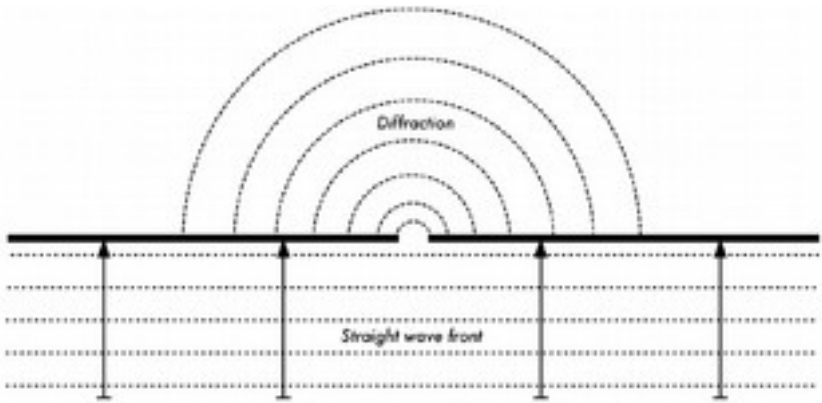


Figure RP 7: Diffraction par une ouverture étroite.

Le principe de Huygens fournit un modèle pour comprendre ce comportement. Imaginez qu'à un instant donné, chaque point d'un front d'onde peut être considérée comme le point de départ d'une ''ondelette" sphérique. Cette idée a ensuite été étendue par Fresnel, mais la question de savoir si elle décrit adéquatement le phénomène reste encore un sujet de débat.
Mais pour les fins de ce livre, le modèle d'Huygens décrit l'effet très bien.

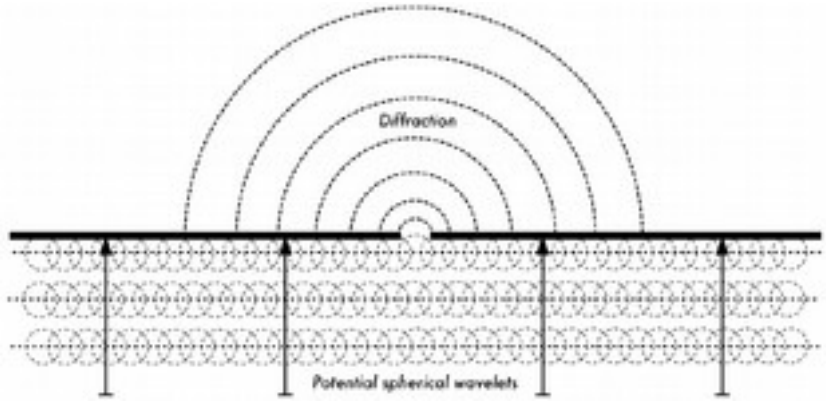


Figure RP 8: Le principe d'Huygens.

A cause de l'effet de diffraction, les ondes vont se replier autour des coins ou se propager à travers une ouverture dans une barrière. Les longueurs d'onde de la lumière visible sont beaucoup trop petites pour que les humains puissent observer leurs effets directement. Ayant une longueur d'onde de plusieurs centimètres, les micro-ondes montreront les effets de diffraction quand les ondes frappent des murs, les sommets des montagnes et autres obstacles. C'est comme si l'obstruction change la direction de l'onde en la faisant ''tourner" les coins.

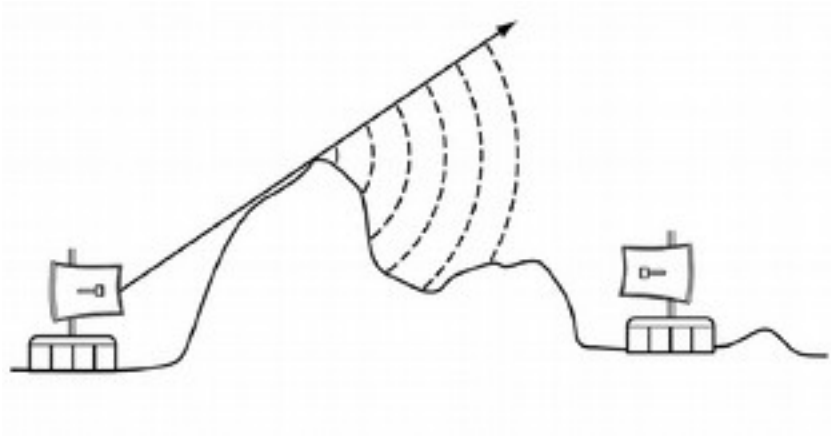


Figure RP 9: Diffraction sur un sommet de montagne.

Notez que la diffraction s'obtient au dépend de l'énergie : l'énergie de l'onde diffractée est significativement inférieure à celle du front d'onde qui l'a causé. Mais dans certaines applications très spécifiques, vous pouvez profiter de l'effet de diffraction pour contourner les obstacles.

Interférence

L'interférence est l'un des termes et phénomènes les plus mal compris dans le réseautage sans fil. Interférence est souvent blâmée quand nous sommes trop paresseux pour trouver le vrai problème, ou quand un régulateur veut arrêter le fonctionnement du réseau de quelqu'un pour des raisons commerciales. Ainsi, pourquoi tous les malentendus? C'est surtout parce que tout en utilisant le même mot, différentes personnes expriment des choses différentes. Un physicien et un ingénieur en télécommunications utiliseront le mot ''Interférence" de manières très différentes. La vue du physicien sera concentrée sur le ''comportement des ondes". L'ingénieur en télécommunications va parler de " ... tout bruit qui est dans la voie de l'onde". Les deux points de vue sont pertinents dans le sans fil, et il est important d'être en mesure de connaître les deux et faire la différence. Commençons par le point de vue des physiciens : Lorsque vous travaillez avec des ondes, un plus un ne fait pas nécessairement deux. Ça peut également faire zéro.

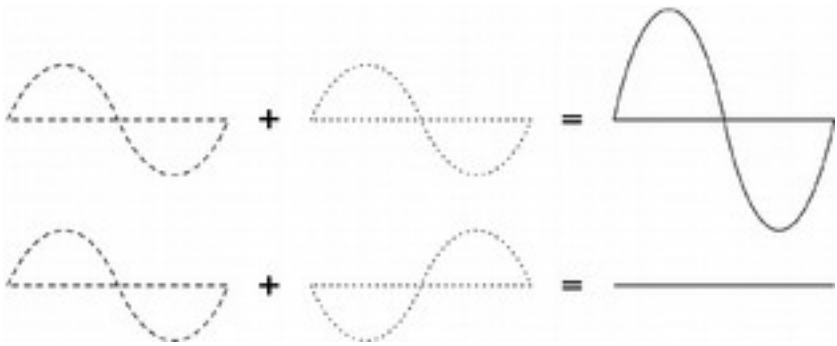


Figure RP 10: Interférence constructive et destructive.
onstructive and destructive.

Cela est facile à comprendre quand vous dessinez deux ondes sinusoïdales et ajoutez leurs amplitudes. Lorsque le différence de phase est nulle, les deux crêtes coïncident, vous aurez les résultats maximum (1 + 1 = 2).
Ceci s'appelle une **interférence constructive**.

Lorsque le différence de phase est de 180 degrés, ou λ / 2, une crête coïncide avec une vallée, vous aurez une annihilation complète ((1 + (-) 1 = 0) - **interférence destructive** .
Vous pouvez effectivement essayer ceci avec des ondes sur l'eau et deux petits bâtons pour créer des ondes circulaires - vous verrez que là où les deux ondes se croisent, il y aura des secteurs de crêtes d'ondes plus élevées et d'autres qui restent presque plats et calmes. Pour que les trains d'ondes entières s'additionnent ou s'annulent parfaitement, elles doivent avoir exactement la même longueur d'onde et une relation de phase fixe. Vous pouvez voir des exemples évidents d'interférence en action quand vous regardez la façon dont les antennes sont disposées dans ce qu'on appelle des réseaux de faisceaux (en anglais beamforming arrays), afin de produire une interférence constructive maximale dans les directions où vous voulez le signal et une interférence destructive (pas de signal) là où le signal n'est pas voulu.
Techniquement, cela est réalisé par une combinaison de dimensionnement physique et le contrôle des déphasages.
De manière simplifiée, imaginez que vous avez trois antennes - et vous ne voulez pas que la troisième antenne puisse capter le signal de la première et deuxième antenne. Vous pouvez ainsi placer la troisième antenne à une position où les signaux provenant de la première et deuxième antenne s'annulent.
Ayons maintenant un regard sur la façon dont le mot interférence est généralement utilisé : dans un sens plus large, pour toute perturbation par d'autres sources de radio fréquence, tout bruit provenant, par exemple, des canaux voisins ou les fournisseurs de service concurrents. Ainsi, quand les réseauteurs sans fil parlent d'interférence, ils font typiquement référence à toutes ces sortes de perturbations par d'autres réseaux, ainsi que les autres sources de micro-ondes opérant exactement à la même fréquence et même phase ou non. Ce genre d'interférence est l'une des principales sources de difficulté à l'établissement des liaisons sans fil, en particulier en milieux urbains ou les espaces fermés (comme une salle de conférence) où des nombreux réseaux peuvent se faire concurrence dans un même spectre de fréquence. Cependant, l'interférence de ce genre est souvent surestimée : par exemple, imaginez que vous deviez établir une liaison point à point qui doit traverser une zone surpeuplée du centre-ville pour atteindre sa cible de l'autre côté de la ville.
Un tel faisceau très directionnel traversera le brouillard electrique (an anglais electric smog) du centre urbain sans aucun problème.

Vous pouvez imaginer cela comme deux faisceaux de lumière vert et rouge qui se croisent dans un angle de 90 degrés : alors que les deux faisceaux se chevauchent dans une certaine zone, l'une n'aura quasiment aucun impact sur l'autre.
En règle générale, la gestion du spectre et la coexistence est devenue un problème majeur en particulier dans les environnements denses à l'intérieur et les zones urbaines.

La ligne de vue

Le terme ligne de vue (dont l'abréviation est LOS en anglais pour Line Of Sight) est assez facile à comprendre quand on parle de la lumière visible : si nous pouvons voir un point B à partir du point A où nous sommes, nous avons la ligne de mire. Il suffit de dessiner une ligne droite de A à B, et si rien ne se trouve dans le chemin, nous avons la ligne de vue. Les choses deviennent un peu plus compliquées quand nous avons affaire à des micro-ondes.
Rappelez-vous que la plupart des caractéristiques de propagation des ondes électromagnétiques varient avec leur longueur d'onde. C'est également le cas pour l'élargissement des ondes pendant leur propagation. La lumière a une longueur d'onde d'environ 0,5 micromètres et tel qu'utilisés dans les réseaux sans fil les micro-ondes ont une longueur d'onde de quelques centimètres.
Par conséquent, leurs faisceaux sont beaucoup plus large - elles ont besoin de plus d'espace, pour ainsi dire. Notez que les faisceaux de la lumière visible s'élargissent de la même façon, et si vous les laissez se propager assez longtemps, vous pouvez voir les résultats en dépit de leur courte longueur d'onde. En pointant un laser bien focalisé vers la lune, son faisceau va s'élargir 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 couteux et une paire de jumelles. Plutôt que de pointer vers la Lune, pointer vers une montagne lointaine ou une structure inoccupée (comme un château d'eau). Le rayon de votre faisceau augmentera à mesure que la distance augmente. Cela est dû à la diffraction. La ligne de vue dont nous avons besoin afin d'établir une connexion sans fil optimale d'un point A au point B est plus que juste une ligne fine - sa forme ressemble plus à celle d'un cigare, une ellipsoïde.
Sa largeur peut être décrite par le concept des zones de Fresnel - voir la section suivante pour une explication.

Vous y trouverez également l'abréviation NLOS (an anglais Non Line of Sight), qui est le plus souvent utilisé pour décrire et annoncer des technologies qui permettent de traiter avec des ondes qui atteignent le récepteur à travers de trajectoires multiples (chemins multiples) ou la diffraction.

Elle ne signifie pas qu'un faisceau électromagnétique unique va ''dans les coins" (autrement que par la diffraction) ou ''traverse les obstacles" mieux que celui d'autres technologies.
Par exemple, vous pouvez appeler les espaces blancs une technologie NLOS, comme leurs fréquences basses (plus grandes longueurs d'onde) leur permettent de pénétrer des objets et utiliser la diffraction beaucoup mieux que les transmissions comparables à 2,4 GHz ou 5 GHz.

Comprendre les zones de Fresnel

La théorie exacte des zones de Fresnel (prononcez en anglais « Fray-nell") est assez compliquée. Cependant, le concept est assez simple à comprendre: nous savons par le principe d'Huygens qu'une nouvelle onde circulaire prend naissance à partir de chaque point d'un front d'onde.
Nous savons aussi à partir de ce principe que les faisceaux de micro-ondes s'élargissent à mesure qu'ils quittent l'antenne.
Finalement, par ce principe nous savons que les ondes d'une même fréquence peuvent interférer les unes avec les autres.

La théorie de la zone de Fresnel s'occupe simplement d'une ligne de A à B, ainsi que la contribution de l'espace autour de cette ligne dans ce qui arrive au point B.
Certaines ondes voyagent directement de A à B, tandis que d'autres se déplacent en dehors de cet axe et atteignent le récepteur par réflexion.
Par conséquent, leur trajet est plus long, introduisant un décalage de phase entre le faisceau direct et indirect.
Chaque fois que le décalage de phase est d'une demi-longueur d'onde, vous obtenez une interférence destructive: les signaux s'annulent.
En adoptant cette approche vous trouverez que lorsque la longueur du trajet réfléchi est plus supérieure à celle du trajet direct par moins d'une une demi-longueur d'onde, les réflexions s'ajouteront au signal reçu.
Inversement, lorsque la longueur du trajet réfléchi est supérieure à la celle du trajet direct par plus d'une demi- longueur d'onde, sa contribution diminuera la puissance reçue.

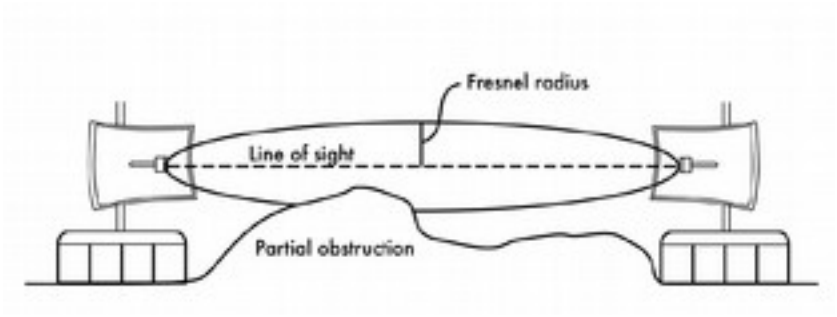


Figure RP 11: La zone de Fresnel est partiellement obstruée sur cette liaison, bien que la ligne de vue visuelle apparaisse clairement.

Notez qu'il y a beaucoup de zones de Fresnel possibles, mais nous sommes principalement préoccupés par la première zone, parce que les contributions de la seconde zone sont négatives.
Les contributions de la troisième zone sont à nouveau positives, mais il n'y a aucun moyen pratique de profiter de cette zone sans les pénalités relatives à la deuxième zone de Fresnel.
Si la première zone de Fresnel est partiellement obstruée par un obstacle, par exemple un arbre ou un bâtiment, le signal arrivant à l'autre extrémité serait diminué. Lors de l'établissement des liaisons sans fil, il faut donc être sûr que la première zone est maintenue libre de toute obstruction. En pratique, il n'est strictement pas nécessaire que l'ensemble de cette zone soit dégagée.
En réseautage sans fil, nous visons à dégager environ 60 pour cent du rayon de la première zone de Fresnel. Voici une formule pour calculer le rayon de la première zone de Fresnel :

$$r = 17.31 \sqrt{\left(\frac{(d_1 * d_2)}{(f * d)}\right)}$$

où r est le rayon de la zone en mètres, d_1 et d_2 sont les distances de l'obstacle aux extrémités de la liaison en mètres, d est la distance de la liaison totale en mètres, et f est la fréquence exprimée en MHz.

Le premier rayon de la zone de Fresnel peut également être calculé directement à partir de la longueur d'onde :

$$r = \sqrt{\left(\frac{\lambda * d_1 * d_2}{d}\right)}$$

avec toutes les variables en mètres.

Il est évident que la valeur maximale de la première zone de Fresnel se trouve exactement au milieu de la trajectoire et cette valeur peut être obtenue en fixant les valeurs $d_1 = d_2 = d/2$ dans les formules précédentes.
Notez que les formules vous donnent le rayon de la zone de Fresnel en son centre, pas la hauteur par rapport au sol.
Pour calculer la hauteur par rapport au sol, vous devez tirer le résultat à partir d'une ligne tracée directement entre les sommets des deux pilonnes. Par exemple, calculons la taille de la première zone de Fresnel au milieu d'une liaison de 2 km de longueur transmettant à 2,437 GHz (canal 6 de la norme 802.11b):

$$r = 17.31 \sqrt{\left[\frac{(1000 * 1000)}{(2437 * 2000)}\right]}$$

$$r = 17.31 \sqrt{\left(\frac{1000000}{4874000}\right)}$$

r = 7.84 mètres

En supposant que nos deux pilonnes avaient une hauteur de dix mètres, la première zone de Fresnel passerait juste à 2,16 mètres au-dessus du sol au milieu de la liaison. Mais de quelle hauteur devrait une structure localisée à ce point pour pouvoir libérer 60% de la zone de Fresnel?

*r = 0,6 * 7,84 mètres*
r = 4,70 mètres

En soustrayant 10 mètres au résultat, nous pouvons voir qu'une structure de 5,3 mètres de haut au centre de la liaison bloquerait moins de 40% de la première zone de Fresnel.
Ceci est normalement acceptable, mais pour améliorer la situation, nous aurons besoin de placer les antennes plus haut, ou changer la direction de la liaison pour éviter l'obstacle .

Energie

Toute onde électromagnétique transporte de l'énergie - nous pouvons le sentir que lorsque nous profitons (ou souffrons) de la chaleur du soleil. La quantité d'énergie divisée par le temps pendant lequel nous la mesurons est appelée puissance.
La puissance P se mesure en W (watts) et est d'une importance cruciale pour le fonctionnement d'une liaison sans fil: vous avez besoin d'une certaine puissance minimale pour qu'un récepteur puisse donner un sens au signal. Nous reviendrons sur les détails de la puissance de transmission, des pertes, des gains et de la sensibilité de la radio dans le chapitre sur les *Antennes/lignes de transmission*. Ici, nous allons discuter brièvement de la façon dont la puissance P est définie et mesurée. Le champ électrique est mesuré en V/m (différence de potentiel par mètre) et la puissance contenue dans ces champs est proportionnel au carré du champ électrique :

$$P \sim E^2$$

Pratiquement, nous mesurons la puissance en watts au moyen d'une certaine forme de récepteur, par exemple une antenne et un voltmètre, wattmètre, oscilloscope, analyseur de spectre ou encore une carte radio et un ordinateur portable. Observer la puissance d'un signal revient à observer le carre du signal en volts divisée par la résistance électrique.

Calcul avec le dB

L'utilisation des décibels (dB) est de loin la technique la plus importante pour le calcul de la puissance. Il n'y a pas de nouvelle physique cachée dans ceci - c'est n'est qu'une méthode pratique pour rendre les calculs beaucoup plus simples.
Le décibel est une unité sans dimension, qui définit une relation entre deux mesures de puissance. Il est défini par:

$$dB = 10 * Log (P_1/P_0)$$

où P_1 et P_0 peuvent être deux valeurs quelconques que vous voulez comparer. Typiquement, dans notre cas, ce sera 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 son deux fois plus fort qu'un autre si celui-ci a un signal physique dix fois plus puissant.
Un autre exemple, tout à fait proche à notre domaine d'intérêt est l'absorption.
Supposons qu'un mur se trouve dans le chemin de notre liaison sans fil, et chaque mètre du mur consomme la moitié du signal disponible.
Le résultat serait :

0 mètres = 1 (signal complet)
1 m = 1/2
2 mètres = 1/4
3 mètres = 1/8
4 mètres = 1/16
n mètres = $1/2^n = 2^{-n}$

Ce comportement est exponentiel. Mais une fois que nous avons appliqué l'astuce de l'application du logarithme (log), les choses deviennent beaucoup plus faciles : au lieu de prendre une valeur à la nième, nous multiplions simplement par n.
Au lieu de multiplier des valeurs, nous les additionneront.
Voici quelques valeurs couramment utilisées qui sont importantes à retenir:

+3 dB = double puissance
-3 dB = moitié de la puissance
+10 dB = ordre de grandeur (10 fois plus de puissance)
-10 dB = un dixième puissance

En plus des mesures sans dimension comme les dBs, il existe un certain nombre de définitions qui sont basées sur une certaine valeur de base P_0. Les plus pertinentes pour nous sont:

dBm relatif à P_0 = 1 mW
dBi relatif à une antenne isotrope idéale

Une antenne isotrope est une antenne hypothétique qui répartit la puissance uniformément dans toutes les directions. L'antenne qui l'y ressemble le plus est le dipôle, mais une antenne isotrope parfaite ne peut être construire en réalité. Le modèle isotrope est cependant utile pour décrire le gain relatif de puissance d'une antenne réelle.
Une autre convention commune (bien que moins pratique) pour exprimer le pouvoir est en **milliwatts**.

Voici les niveaux de puissance équivalente, exprimés en milliwatts et dBm:

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

Pour plus de détails sur le dB, veuillez-vous référer à la leçon sur les mathématiques du dB du kit de formation sans fil:
http://wtkit.org/sandbox/groups/wtkit/wiki/820cb/attachments/ebdac/02-dB_Math-v1.12_with-notes.pdf

Physique dans le monde réel

Ne vous inquiétez pas si les concepts de ce chapitre semblent représenter un véritable défi.
Comprendre comment les ondes radio se propagent et interagissent avec le l'environnement est un champ d'étude complexe en soi.
La plupart des personnes trouvent qu'il est difficile de comprendre un phénomène qu'elles ne peuvent même pas voir de leurs propres yeux.
A présent, vous devriez comprendre que les ondes radio ne se propagent pas seulement suivant un chemin droit prévisible.
Pour rendre les réseaux de communication fiables, vous devrez être en mesure de calculer combien de puissance est nécessaire pour parcourir une distance donnée, et prédire comment les ondes se déplacent le long du trajet.

2. TELECOMMUNICATIONS DE BASE

Le but de tout système de télécommunications est d'utiliser un canal de communication pour transférer l'information de l'émetteur vers le récepteur. L'information est transmise par un signal, qui consiste en une certaine quantité physique qui change avec le temps. Le signal peut être une tension proportionnelle à l'amplitude de la voix comme dans la téléphonie simple, une séquence d'impulsions de lumière dans la fibre optique, ou une onde radioélectrique irradiée par une antenne.
Pour les signaux analogiques, ces variations sont directement proportionnels à certaines grandeurs physiques comme le son, la lumière, la température, la vitesse du vent, etc. L'information peut également être transmise par des signaux numériques binaires, qui auront seulement deux valeurs, une valeur un numérique et une valeur zéro numérique.
Tout signal analogique peut être converti en un signal numérique en utilisant un échantillonnage approprié suivi par un codage.
La fréquence d'échantillonnage doit être au moins deux fois la fréquence maximale du signal pour pouvoir transférer toutes les informations contenues dans un signal.
Les signaux aléatoires sont imprévisibles et ne peuvent être décrits que par des moyens statistiques. Le bruit est un signal aléatoire classique caractérisé par sa puissance moyenne et sa distribution de fréquence.
Un signal peut être caractérisé par son comportement dans le temps ou par ses composantes fréquentielles qui constituent son spectre.

Quelques exemples de signaux sont présentés dans la Figure 1 TB .

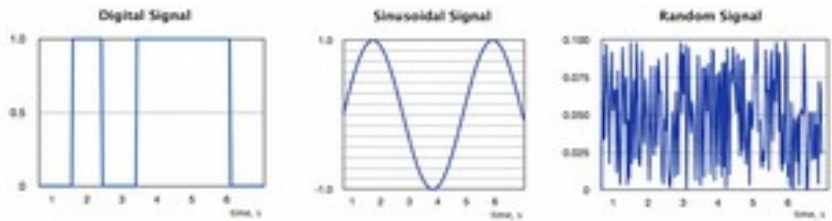


Figure TB 1: Exemples de signaux

Tout signal périodique contient plusieurs composantes sinusoïdales, toutes ces composantes étant des multiples de sa fréquence de base qui est l'inverse de la période du signal.

Ainsi, un signal peut être caractérisé soit par un diagramme de son amplitude par rapport au temps, appelé une forme d'onde, ou par un diagramme des amplitudes de ses composantes fréquentielles, appelé spectre.

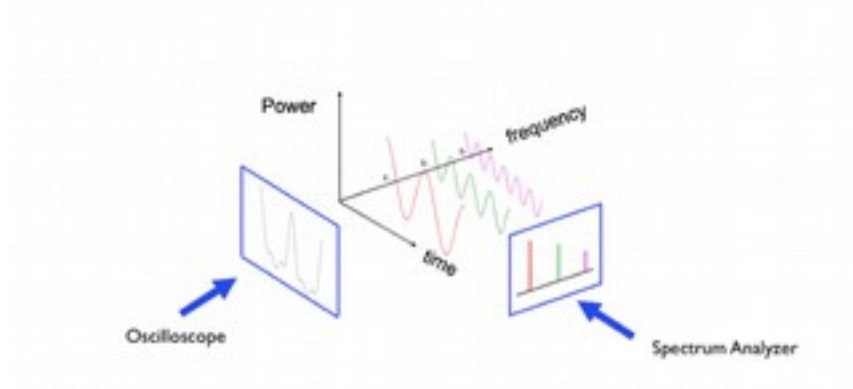


Figure TB 2: Formes d'onde, spectre et filtres

La figure TB 2 montre comment un même signal peut être représenté sous deux angles différents.
La forme d'onde peut s'obtenir par un instrument appelé un oscilloscope, alors que le spectre peut être obtenu en utilisant ce qu'on appelle un analyseur de spectre.
La distribution spectrale relaie une information importante sur le signal et permet une compréhension intuitive de la notion de filtrage des signaux électriques.
Dans l'exemple illustré, le signal est constitué par la superposition de trois composantes sinusoïdales de fréquence f_1, f_2 et f_3. Si nous passons ce signal à travers un dispositif qui supprime les composantes f_2 et f_3, la sortie sera une sinusoïdale pure de fréquence f_1. Nous appelons cette opération ''filtrage passe-bas", car elle élimine les hautes fréquences.
En revanche, nous pouvons soumettre le signal à un ''filtre passe-haut", un dispositif qui va filtrer les signaux f_1 et f_2 laissant seulement un signal sinusoïdal de fréquence f_3. D'autres combinaisons donnant naissance à une variété de filtres sont possibles.

Comme aucun dispositif physique ne peut transmettre l'infinité des fréquences du spectre radioélectrique, chaque signal passant par un dispositif subira toujours dans une certaine mesure un filtrage.
La largeur de bande d'un signal est la la différence entre la plus haute et la plus basse fréquence qu'il contient et s'exprime en Hz (nombre de cycles par seconde). Pendant son passage à travers le canal de communication, le signal est soumis à des interférences causées par d'autres signaux et est également affecté par le bruit électrique toujours présent dans toute composante électrique ou optique. L'interférence intra-canal (en anglais Intra-channel) provient du même canal que celui de notre signal.
L'interférence co-canal (en anglais Co-channel) est due à l'imperfection des filtres conduisant à l'incapacité de filtrer des signaux provenant des canaux adjacents.
Par conséquent, le signal reçu sera toujours une réplique déformée du signal transmis, à partir de laquelle l'information originale doit être récupérée par des moyens appropriés pour combattre l'effet d'interférence et du bruit.
Par ailleurs, le signal reçu sera soumis à l'atténuation et délai qui augmentent avec la distance entre l'émetteur et le récepteur.

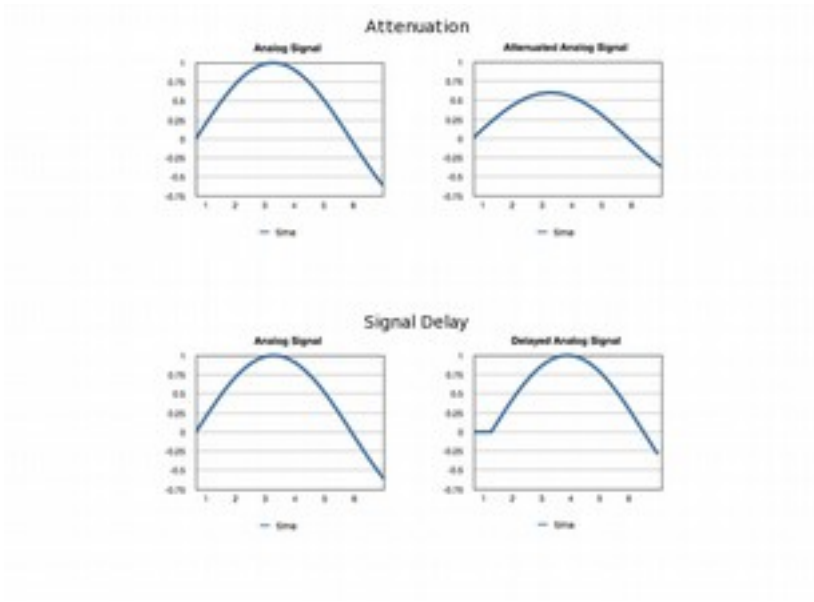


Figure TB 3: Atténuation et délai

Bien qu'il soit relativement simple de restaurer l'amplitude du signal au moyen d'un amplificateur électrique, les composants de l'amplificateur vont ajouter du bruit supplémentaire au signal, de sorte qu'à des très longues distances où le signal reçu est faible, l'amplificateur produit un signal qui est tellement brouillé avec le bruit que l'information originalement transmise ne sera plus récupérable.

Une façon de résoudre ce problème consiste à convertir la quantité continue porteuse de l'information en une séquence de symboles très simples qui peuvent être plus facilement reconnaissables, même à grande distance.
Par exemple, le drapeau d'un navire est un moyen commode de distinguer la nationalité du navire, même à des distances où les lettres sur la coque du navire ne peuvent être lues. Cette technique a été étendue pour le transfert généralisé des messages en attribuant à chaque lettre de l'alphabet différentes positions des drapeaux, dans une forme précoce de télécommunications longue distance utilisant des signaux digitaux ou numériques.

La limitation de cette méthode est évidente; pour être capable de distinguer entre, disons, 26 symboles correspondant à chaque lettre de l'alphabet, on doit être très proche du navire qui est en train de communiquer.
D'autre part, si l'on code chaque lettre de l'alphabet dans une séquence de seulement deux symboles, ces symboles peuvent être distingués à beaucoup plus longue distance, par exemple le point et les traits du système télégraphique.
Le processus de transformation d'un signal analogique continu dans un signal discontinu numérique est appelé une conversion analogique-numérique (ADC en anglais), et inversement, il faut avoir un convertisseur numérique- analogique (DAC en anglais) à l'extrémité réceptrice pour retrouver l'information originale.
C'est la raison pour laquelle les systèmes de télécommunications les plus modernes utilisent des signaux numériques binaires pour transmettre toutes sortes d'informations de façon plus robuste.
Le récepteur doit seulement faire la distinction entre deux symboles possibles, ou en d'autres termes entre les deux valeurs possibles du bit reçu (digit binaire ; en anglais binary digit).

Par exemple, le CD a remplacé le disque en vinyle, et la télévision analogique est en train d'être remplacée par la télévision numérique.

Les signaux numériques peuvent utiliser moins de largeur de bande, comme en témoigne la ‘’dividende numérique” actuellement exploitée dans de nombreux pays, qui consiste en une largeur de bande qui a été rendue disponible grâce à la transition de la transmission analogique au numérique dans la radiodiffusion télévisuelle.
Bien que dans le processus de conversion de l'analogique au système d'information numérique, il y a toujours une certaine perte d'information, nous pouvons concevoir le système de manière à rendre cette perte négligeable.

Figure TB 4: L'image sous-échantillonnée

Par exemple, dans un appareil photo numérique, nous pouvons choisir le nombre de bits utilisés pour enregistrer l'image.

Plus le nombre de bits (proportionnelle à la quantité de mégapixels) sera, meilleure sera l’image rendue, mais plus de mémoire sera utilisée et plus de temps sera nécessaire pour transmettre l'image.
Ainsi, les systèmes de communication les plus modernes traitent avec des signaux numériques, bien que la variable d'origine que nous voulons transmettre puisse être analogique, comme la voix.

On peut démontrer que tout signal analogique peut être reconstruit à partir d'échantillons discrets si la fréquence d'échantillonnage est au moins deux fois aussi élevée que la fréquence la plus élevée du signal.

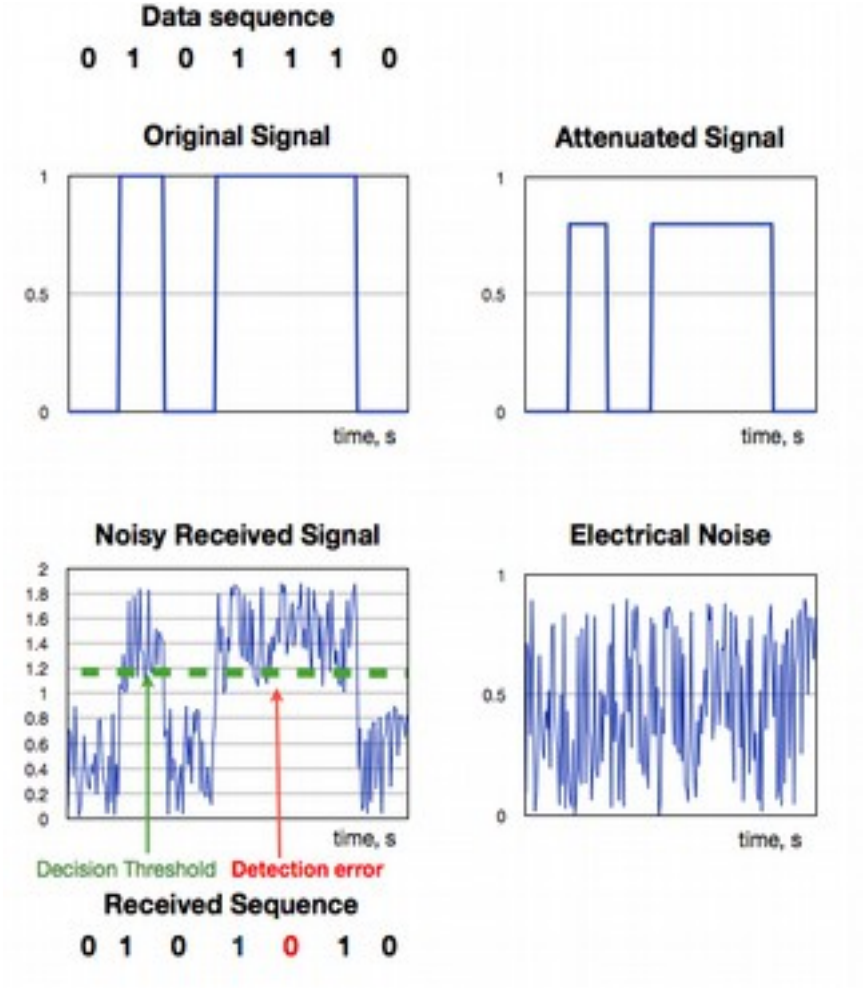


Figure TB 5: détection d'un signal brouillé

Ensuite, chaque échantillon est codé sur autant de bits que nécessaire pour obtenir la précision désirée. Ces bits peuvent maintenant être stockés ou transmis de manière efficace, puisque pour la récupération de l'information il faut faire la distinction entre seulement les deux états, et non parmi les nuances infinies d'un signal analogique. Ceci est illustré dans la figure TB 5, où les données d'origine se composent de la séquence 0 1 0 1 1 1 0. Les 0 sont représentés comme zéro volt et les 1 comme 1 V. Lorsque le signal se déplace vers le récepteur, son amplitude diminue.

Cet effet qui est appelé ''atténuation" est représenté dans la figure.
De même, il y aura aussi un délai associé au signal lorsqu'il se déplace de l'émetteur vers le récepteur. La variabilité du délai du signal reçu est appelé jitter (en anglais).
Si l'atténuation, le bruit ou le jitter (ou leur combinaison) est suffisamment sévère, cela peut provoquer une erreur de détection. Un amplificateur peut être utilisée pour surmonter l'atténuation, mais le bruit électrique toujours présent dans le système va s'ajouter au signal reçu.
Le signal reçu brouillé est donc tout à fait différent du signal original, mais dans un système numérique, nous pouvons encore récupérer les informations contenues par échantillonnage du signal reçu au bon moment et en comparant la valeur au moment de l'échantillonnage avec une tension de seuil approprié. Dans cet exemple, le bruit de signal reçu a une crête de 1,8 V, ainsi nous pourrions choisir une tension de seuil de 1,1 V. Si le signal reçu est supérieur au seuil, le détecteur émettra une valeur 1 numérique, sinon, il va afficher un 0 numérique. Dans ce cas, nous pouvons voir qu'en raison de l'effet du bruit, le cinquième bit a été détecté de façon erronée comme un zéro. Les erreurs de transmission peuvent également survenir si la période d'échantillonnage du signal est différente de celle des données originales (différence entre les taux d'horloge), ou si l'horloge du récepteur n'est pas assez stable (jitter).
Tout système physique aura une limite supérieure dans les fréquences qui transmettent fidèlement (la largeur de bande du système), les fréquences élevées seront bloquées, de sorte que la hausse et la chute brusque de la tension seront lissées lors du passage du signal par le canal. Par conséquent, nous devons nous assurer que chacun des éléments du système a une largeur de bande suffisante pour traiter le signal. D'autre part, plus la largeur de bande du système de réception est élevée, plus sera la quantité de bruit qui affectera le signal reçu.

Modulation

La robustesse du signal numérique est également exemplifiée par le fait qu'il était choisi pour les premiers essais de transmission radio.
Marconi démontra la faisabilité de la transmission à longue distance, mais assez vite se rendit compte qu'il y avait un besoin de partager le support de communication différents utilisateurs.
Ceci était réalisé en assignant des fréquences porteuses différentes qui étaient modulées par le message de chaque utilisateur.

La modulation consiste en un schéma qui modifie l'amplitude, la fréquence ou la phase de la porteuse en fonction de l'information que l'on veut transmettre.
L'information originale est récupérée à la destination par le canal d'une démodulation correspondante du signal reçu.

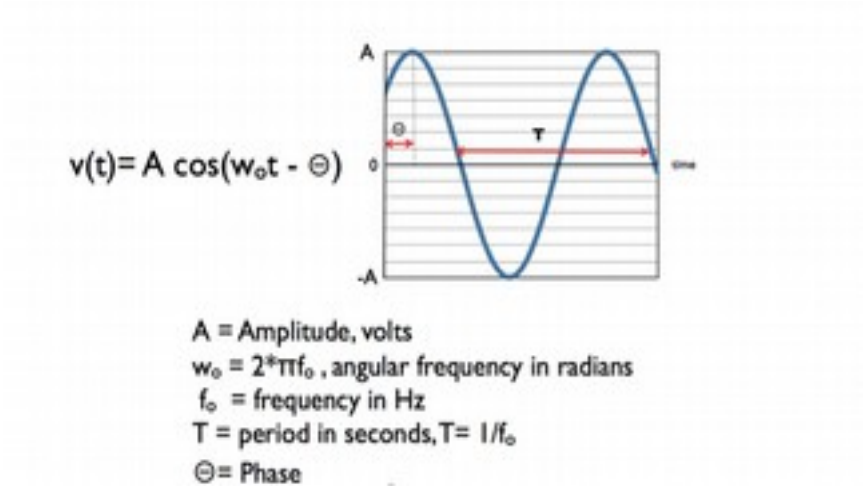


Figure TB 6: Signal porteur sinusoïdal.

La Figure TB 6 montre un signal porteur avec une amplitude **A**, une phase **θ**, et une fréquence $\mathbf{f_0}$ qui est l'inverse de la période **T**.

La combinaison des différents schémas de modulation a entraîné une pléthore de techniques de modulation dépendant de l'aspect que l'on veut optimiser: robustesse par rapport au bruit, quantité d'informations transmises par seconde (capacité de la liaison en bits/seconde) ou efficacité spectrale (nombre de bits/seconde par Hertz).
Par exemple, le **BPSK** (en anglais Binary Phase Shift Keying), est une technique de modulation très robuste mais qui transmet un seul bit par symbole, tandis que le **256 QAM** (en anglais Quaternary Amplitude Modulation) vous permet de transporter 8 bits par symbole, multipliant ainsi par un facteur de huit la quantité d'informations transmises par seconde, mais pour distinguer correctement entre les 256 symboles transmis, le signal reçu doit être très fort en comparaison du bruit (un rapport très élevé est S/N -Signal/Noise est requis).

La mesure ultime de la qualité de la transmission numérique est le **BER**(en anglais Bit Error Rate) qui correspond à la fraction de bits décodés par erreur. Les valeurs typiques de BER se situent entre 10^{-3} et 10^{-9}. La modulation permet également de choisir quelle gamme de fréquence nous souhaitons utiliser pour une transmission donnée.
Toutes les fréquences ne sont pas créées égales et le choix de la fréquence porteuse est déterminée par des contraintes juridiques, commerciales et techniques.

Multiplexage et duplexage

En général, le partage d'un canal parmi les utilisateurs différents est appelé multiplexage . Ceci est illustré dans la figure TB 7.

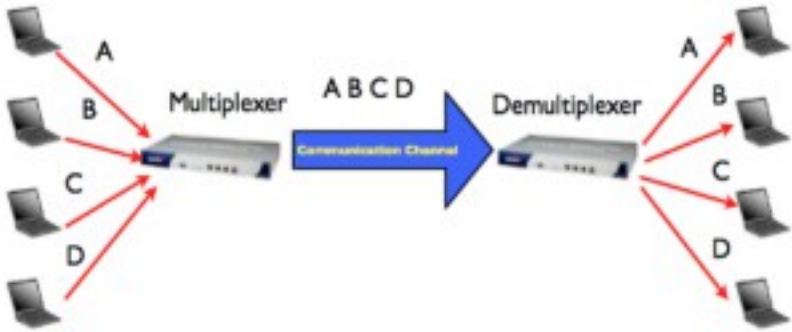


Figure TB 7: Multiplexage

L'attribution des fréquences porteuses différentes à différents utilisateurs est appelée **FDMA** (en anglais Frequency Division Multiple Access).

Une autre technique consiste à attribuer des créneaux temporels différents à différents utilisateurs, dans ce qui est connu comme le **TDMA** (en anglais Time Division Multiple Access), ou même différents codes à différents utilisateurs dans le **CDMA** (en anglais Code Division Multiple Access) où les différents utilisateurs sont reconnus au niveau du récepteur par le code mathématique particulier qui leur est assigné : Voir Figure 8 TB.

En utilisant deux ou plusieurs antennes simultanément, on peut tirer avantage de différents affaiblissements introduits dans les différents chemins vers le récepteur établissant ainsi une différence parmi les utilisateurs dans ce qui est connu comme **SDMA** (en anglais Space Division Multiple Access), une technique employée dans le systèmes **MIMO** (en anglais Multiple Input Multiple Output) qui ont gagné en popularité ces derniers temps.

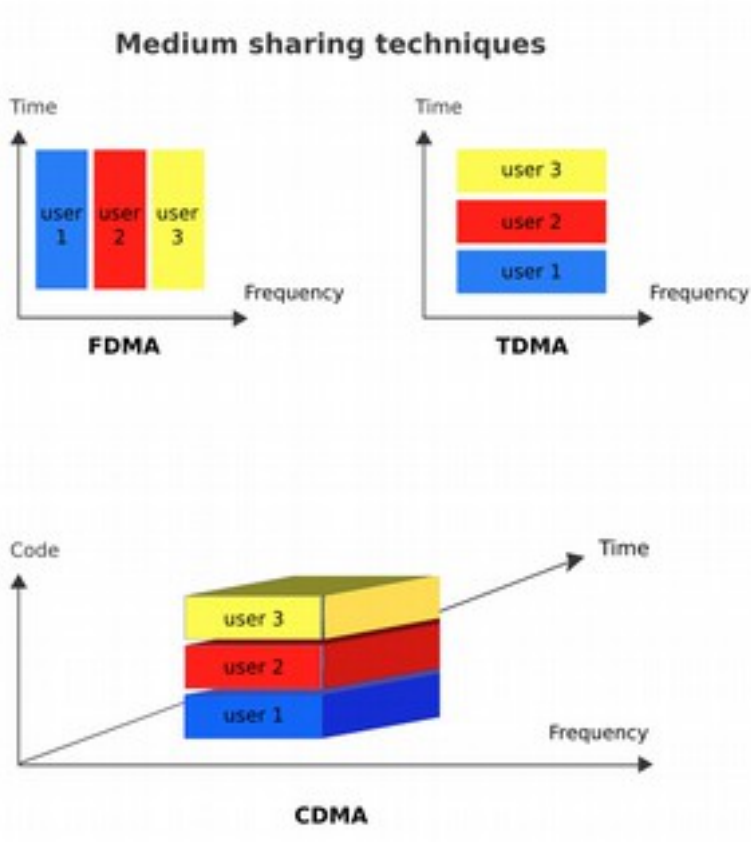


Figure TB 8: Techniques de partage du support de communication

La plupart des systèmes de communication transmettent des informations dans les deux directions, par exemple de la station de base à l'abonné dans ce qu'on appelle la liaison descendante (en anglais ***downlink***), et à partir de l'abonné à la station de base sur la liaison montante (en anglais ***uplink***).

Pour ce faire, le canal doit être partagé entre les deux directions conduisant respectivement au **FDD** (en anglais Frequency Division Duplexing) et **TDD** (en anglais Time Division Duplexing).

Conclusions

Le système de communication doit surmonter le bruit et l'interférence en vue d'établir une reproduction appropriée du signal au récepteur.
La capacité du canal de transmission en bits/seconde est proportionnelle à la largeur de bande en Hz et au logarithme du rapport signal/bruit.
La modulation permet d'adapter le signal au canal et permettre à plusieurs signaux de partager le même canal. Les schémas de modulation plus élaborés permettent un taux de transmission plus élevé, mais nécessitent un rapport S/N élevé. Le canal peut être partagée par plusieurs utilisateurs qui occupent des fréquences différentes, différents intervalles de temps, des codes différents, ou en prenant avantage de différentes caractéristiques de propagation dans ce qui s'appelle multiplexage spatial.
Pour plus d'informations et diapositives couvrant ce sujet, veuillez s'il vous plaît visitez
http://wtkit.org/groups/wtkit/wiki/820cb/download_page.html

3. LICENSE ET REGLEMENTATION

Il y a un certain nombre de domaines où les lois et régulations nationales et internationales peuvent influencer votre capacité à créer des réseaux sans fil. Étant donné que ces régulations varient d'un pays à l'autre, il est impossible de donner une vue d'ensemble des régulations applicables dans votre région. Il est également utile de noter qu'il peut y avoir une énorme différence dans les lois existantes et la façon dont elles sont réglementées en pratique.
En d'autres termes, il peut y avoir des pays où l'utilisation du spectre 2,4 GHz / 5 GHz pour le déploiement du sans-fil à l'extérieur est techniquement illégale, mais où tout le monde le fait quand même. En règle générale, si d'autres personnes sont en train d'établir des réseaux similaires à ce que vous voulez, contactez-les pour savoir quelles sont les obstacles juridiques qu'ils peuvent avoir rencontré. Si ces réseaux sont très largement déployés dans votre pays, alors vous n'avez probablement pas besoin de trop vous inquiéter. D'autre part, il est toujours conseillé de demander conseil localement aux fournisseurs de matériel, les experts sans fil ou d'autres qui sont venus avant vous, avant de consacrer du temps et des ressources pour l'établissement d'un réseau sans fil. Quoi que vous fassiez, il est important que vous preniez les lois et réglementations locales en considération.

Des exemples des types de réglementation pertinents

Chaque pays peut avoir des règles différentes, et chaque scénario peut provenir à travers différents types de règlements. Les domaines où les régulations peuvent être pertinentes comprennent les licences d'utilisation des fréquences radio spécifiques, les règles concernant le droit d'installer des tours pour les antennes, la puissance maximale permise et les règles d'octroi de licences de télécommunications qui limitent votre capacité à fournir un accès Internet à d'autres.
Les types de questions juridiques qui valent (ou ne valent pas) la peine d'être considérées lors de la planification d'un réseau sans fil comprennent:

- L'octroi de licences du spectre de fréquence
- Les licences ISP/Télécommunications
- Le permis pour les tours d'antennes
- La puissance de transmission et les limites de gain d'antenne
- La Certification de l'équipement
- Les conditions d'utilisation des ISP

Licences de spectre

La plupart des pays considèrent le spectre de radio fréquence (RF) comme une propriété exclusive de l'Etat. Le spectre RF est une ressource nationale, un peu comme l'eau, la terre, le gaz et les minéraux. Cependant, contrairement à ces derniers, la fréquence radio est réutilisable. L'objectif de gestion du spectre est d'atténuer la pollution du spectre radioélectrique et de maximiser le bénéfice du spectre radioélectrique utilisable. La première phrase de la constitution de l'Union internationale des télécommunications (UIT) reconnaît pleinement ''le droit souverain de chaque état de réglementer ses télécommunications". La gestion efficace du spectre nécessite une réglementation aux niveaux national, régional et mondial.

La licence est une façon ordonnée de gérer qui, quand, où et comment le spectre est utilisé. Le spectre sans fil libre a été fixé autour de la bande de 2,4 GHz. En Juin 2003, l'UIT rendit disponible la bande 5 GHz pour le déploiement sans licence de la technologie. La bande des 900 MHz, libre aux Etats-Unis, est actuellement utilisée pour les téléphones GSM en Europe occidentale et dans de nombreux pays en développement. Chaque pays a le droit souverain de réglementer ses télécommunications et d'interpréter le régulations radio internationales. Les gouvernements définissent les règles et conditions d'utilisation des fréquences . (tire de Wikipedia ''Gestion du spectre").

Les technologies décrites dans ce livre (principalement) utilisent une tranche du spectre sans licence dénommée ISM (en anglais Industrial, Scientific and Medical radio bands).

Les fréquences **radioélectriques** dans les bandes ISM ont été utilisées à des fins de communication, bien que ces dispositifs opérant dans ces fréquences puissent être sujets à des interférences provenant de sources qui n'ont pas des fins de communication. Les bandes ISM sont définies par l'UIT -R (Secteur des radiocommunications de l'UIT) à 2,4 et 5 GHz.

L'utilisation individuelle de ces bandes par différents pays peut différer en raison des variations dans les régulations nationales de la radio. Comme les dispositifs de communication utilisant les bandes ISM doivent tolérer toute interférence de matériel ISM, les opérations sans licence sont typiquement autorisées à utiliser ces bandes, puisque l'exploitation sans licence doit de toute façon généralement tolérer les interférences provenant d'autres dispositifs.

Aux États-Unis, la FCC (en anglais Federal Communications Commission) établit l'étalement de spectre (en anglais spread spectrum) sans licence d'abord dans les bandes ISM à travers les règles adoptées le 9 mai 1985.

Beaucoup d'autres pays ont adopté ces réglementations FCC plus tard, permettant l'utilisation de cette technologie dans de nombreux pays. (tiré de Wikipedia ‘’ISM Band”).

Licences ISP/Télécommunications

Dans certains pays, une licence ISP serait nécessaire avant de déployer une infrastructure de réseau pour le partage de réseaux sur les espaces publics. Dans d'autres pays, cela serait nécessaire seulement pour opérer des réseaux commerciaux.

Permis pour tours d’antennes

Lors du déploiement des réseaux extérieurs à longue distance, il est souvent nécessaire de construire une tour pour l'antenne. De nombreux pays ont des règlements concernant la construction de ces tours de l'antenne si elles sont plus que 5 ou 10 mètres au-dessus du toit ou au sol.

Limites de puissance de transmission

Lors de l’établissement des limites de puissance de transmission, les organismes de réglementation utilisent généralement la puissance isotrope rayonnée équivalente (EIRP en anglais), car c'est la puissance réellement émise par l'antenne.

Les limites de puissance peuvent aussi être imposées sur la puissance de sortie des dispositifs. À titre d'exemple, la FCC impose certaines règles relatives à la puissance rayonnée par l'antenne, selon que le déploiement est le point -à-multipoint (PtMP en anglais) ou point à point (PtP en anglais).

Elle impose également certaines règles relatives à la puissance maximale transmise par la radio.

Quand une antenne omnidirectionnelle est utilisée, la FCC considère automatiquement que la liaison est un PtMP.

Dans la configuration d'une liaison 2.4 GHz PtMP, la FCC limite la PIRE à 4 watts et la limite de puissance pour la radiation intentionnelle à 1 Watt. Les choses sont plus compliquées dans la bande des 5 GHz. La bande radio U-NII (en anglais Unlicensed National Information Infrastructure (U-NII)) fait partie du spectre de fréquences radio utilisé par les périphériques IEEE- 802.11a et par de nombreux fournisseurs de services Internet sans fil. Il opère sur trois gammes:

U-NII Low (U- NII -1): 5,15-5,25 GHz.Les régulations exigent l'utilisation d'une antenne intégrée. La puissance est limitée à 50 mW.

U- NII Mid (U- NII -2): 5,25-5,35 GHz. Les régulations permettent une antenne installée par l'utilisateur, sous réserve de sélection dynamique de fréquence (DFS, ou évitement radar) .

La puissance est limitée à 250 mW.
U-NII Worldwide: de 5,47 à 5,725 GHz. Utilisation à la fois extérieure et intérieure, sous réserve de sélection dynamique de fréquence (DFS, ou évitement radar) . La puissance est limitée à 250 mW.
Ce spectre a été ajouté par la FCC en 2003 en vue ''d'aligner les bandes de fréquences utilisées par les périphériques U- NII aux États-Unis avec des bandes utilisées dans d'autres parties du monde".
La FCC a actuellement mis une limitation provisoire sur les opérations dans les canaux qui se chevauchent dans la bande 5600-5650 MHz.
U- NII Upper (U- NII -3): de 5,725 à 5,825 GHz.
Parfois appelée U- NII/ISM en raison du chevauchement avec la bande ISM. Les régulations permettent une antenne installée par l'utilisateur. La puissance est limitée à 1W. Les fournisseurs de service sans fil utilisent généralement la bande 5,725 à 5,825 GHz. (tiré de *Wikipedia* ''U- NII").
Pour le déploiement PtP dans la bande 5 GHz, la PIRE maximale autorisée est considérablement élevée, car une antenne à gain élevé produit un faisceau très étroit et donc l'interférence causée aux autres utilisateurs est considérablement inférieure à la topologie PtMPt.

Certification de l'équipement

Les gouvernements peuvent exiger une certification formelle qu'un équipement radio donnée conforme aux normes techniques spécifiques et réglementations locales.
Ceci est souvent désigné comme ***homologation***, et le processus doit être effectué par un laboratoire indépendant agréé par le gouvernement du pays. L'équipement certifié est autorisé à fonctionner sans une licence individuelle. Il est à noter que la certification ne peut s'appliquer qu'à l'état d'usine d'origine des équipements radio. Par exemple, changer l'antenne sur un point d'accès sans fil aux États-Unis annule la certification FCC.

Termes de fonctionnement ISP

Plusieurs fournisseurs de service Internet (ISPs) incluent dans leurs ''termes de fonctionnement" une clause qui interdit aux utilisateurs de partager une connexion Internet avec d'autres utilisateurs. Il peut aussi y avoir des connexions commerciales qui n'ont pas ces limitations. Il est important de noter que ce n'est pas une question juridique, mais une clause du contrat avec le fournisseur d'accès, et la conséquence en cas de violation de celle-ci consiste généralement en une coupure de la connexion Internet.

4. SPECTRE RADIO

Qu'est-ce que le spectre électromagnétique ?

Il n'y a pas une définition unique du spectre électromagnétique.
Du point de vue technique, le spectre est tout simplement la gamme des ondes électromagnétiques qui peuvent être utilisées pour transmettre des informations. Cependant du point de vue pratique, les aspects économiques et politiques, ainsi que la technologie qui est réellement utilisée pour transmettre des informations par le biais de ces ondes jouent un rôle essentiel.
Par exemple, lorsque pour la première en 1902, grâce aux ondes, Marconi envoya son ''message télégraphie sans fil" à travers l'Atlantique, il utilisa la totalité du spectre disponible pour envoyer quelques bits/s sur une superficie de plusieurs milliers de kilomètres carrés. Avec l'émetteur initial utilisé pour cette réalisation qui occupa toutes les fréquences que les récepteurs existants étaient capable de recevoir, personne d'autre ne pouvait utiliser la radio pour communiquer dans un rayon de quelque 3500 km de la station de transmission en Angleterre. Ainsi, si d'autres utilisateurs voulaient envoyer des messages dans la même zone, ils auraient eu besoin de coordonner leurs transmissions dans différents ''créneaux horaires" pour partager le milieu de transmission (spectre). Cette technique est appelée ''TDMA" (en anglais Time Division Multiple Access). Les utilisateurs situés à des distances beaucoup plus grandes au-delà de 3500 km de l'émetteur de Marconi pouvaient utiliser le spectre de nouveau, puisque la puissance des ondes radio diminue à mesure que nous nous éloignons de l'émetteur.
La réutilisation du spectre dans différentes zones géographiques est appelé ''SDMA" (en anglais Space Division Multiple Access).
Plus tard, Marconi fut capable de construire un émetteur qui pouvait limiter les émissions à une seule gamme de fréquences et un récepteur qui pourrait être ''réglé" pour recevoir dans une gamme de fréquence particulière.
Ainsi, de nombreux utilisateurs localisés dans la même région/zone pouvaient transmettre simultanément (dans l'espace) et au même moment.
Ainsi le ''FDMA" (en anglais Frequency Division Multiple Access) démarra et la radio devint un moyen pratique de communication, et le seul qui était disponible pour communiquer avec un navire dans les mers.
La coordination des fréquences attribuées aux différents utilisateurs fut attribuée à des agences nationales créées à cet effet, mais puisque les ondes radio ne peuvent pas être stoppées par les frontières nationales, des accords in-

ternationaux étaient ont été nécessaires. L'organisation internationale qui fut créée pour réguler la transmission de télégrammes entre les différents pays fut aussi chargée de l'allocation de l'usage du spectre électromagnétique. Aujourd'hui, l'union on internationale des télécommunications, UIT, est l'organisation internationale la plus ancienne chargée de formuler des recommandations sur les fréquences à utiliser pour différents services pour ses 193 membres nationaux. L'utilisation du spectre pour les applications militaires posa un nouveau problème ; le ''brouillage" qui consiste en une interférence intentionnelle introduite par l'ennemi pour perturber la communication. Pour éviter le brouillage, une nouvelle technique fut développée dans laquelle l'information devant être transmise était combinée avec un code mathématique spécial dont seuls les récepteurs ayant sa connaissance pouvaient interpréter l'information. Le signal codé était transmis à faible puissance, mais en utilisant un très large intervalle de fréquences pour rendre le brouillage plus difficile. Cette technique fut plus tard adapté aux applications civiles dans ce qu'on appelle le ''CDMA" (en anglais Code Division Multiple Access), l'une des saveurs de la communication à étalement de spectre, largement utilisée dans les systèmes de communication modernes. En résumé, le spectre peut être partagé entre plusieurs utilisateurs en attribuant des créneaux horaires, des intervalles de fréquences différentes, des zones différentes dans l'espace, ou des codes différents. Une combinaison de ces méthodes est utilisée dans les derniers systèmes cellulaires. Outre les questions de souveraineté et de sa défense, des grands intérêts économiques et politiques jouent un rôle déterminant dans la gestion du spectre, qui doit également être constamment mis à jour pour profiter des progrès de la technologie des communications.

Les ingénieurs en télécommunications continuent de trouver des moyens plus efficaces pour transmettre des informations à l'aide du temps, de la fréquence et de la diversité dans l'espace en utilisant des techniques de modulation et de codage de plus en plus avancées. L'objectif est d'accroître ''efficacité spectrale" définie comme la quantité de bits par seconde (bit/s) pouvant être transmis dans chaque Hz de largeur de bande par kilomètre carré. Par exemple, les premières tentatives pour fournir des services de téléphonie mobile furent effectuées en utilisant un émetteur puissant idéalement localisé pour couvrir toute une ville. Cet émetteur (appelé une station de base dans ce contexte), divisa la bande de fréquence allouée en 30 canaux, par exemple, de sorte à permettre seulement 30 conversations simultanées dans toute la ville. En conséquence, le service était très cher et accessible seulement aux personnes extrêmement riches. Cette situation a prévalu pendant

de nombreuses années, jusqu'à ce que les progrès de la technologie électronique permirent l'implémentation d'un schéma permettant de profiter de la ‘’diversité dans l'espace". Au lieu d'utiliser un seul émetteur puissant pour couvrir une cité entière, la région devant être servie était divisée en de nombreuses "cellules", chacune d'elles étant desservie par un émetteur de faible puissance. Ainsi, les cellules qui sont suffisamment distantes les unes des autres peuvent utiliser les mêmes canaux sans interférence, dans ce qui est connu comme la ‘’ réutilisation des fréquences”. Dans le système cellulaire, les 10 premiers canaux doivent utiliser la bande de fréquences 1 et les 10 canaux suivants la bande de fréquences 2 alors que les 10 canaux restants utilisent la bande de fréquences 3. Ceci est représenté par la figure 1 RS où les couleurs correspondent à des bandes de fréquences différentes. Notez que la répétition des couleurs se produit seulement à des distances assez lointaines pour éviter les interférences. Si l'on divise la cité par exemple en 50 cellules, nous pouvons maintenant avoir 10X50 = 500 utilisateurs simultanés dans la même cité au lieu de 30. Par conséquent, en ajoutant des cellules de petites dimensions (caractérisées par une puissance d'émission plus faible), nous pouvons augmenter le nombre de canaux disponibles jusqu'à ce que nous atteignons une limite imposée par l'interférence .

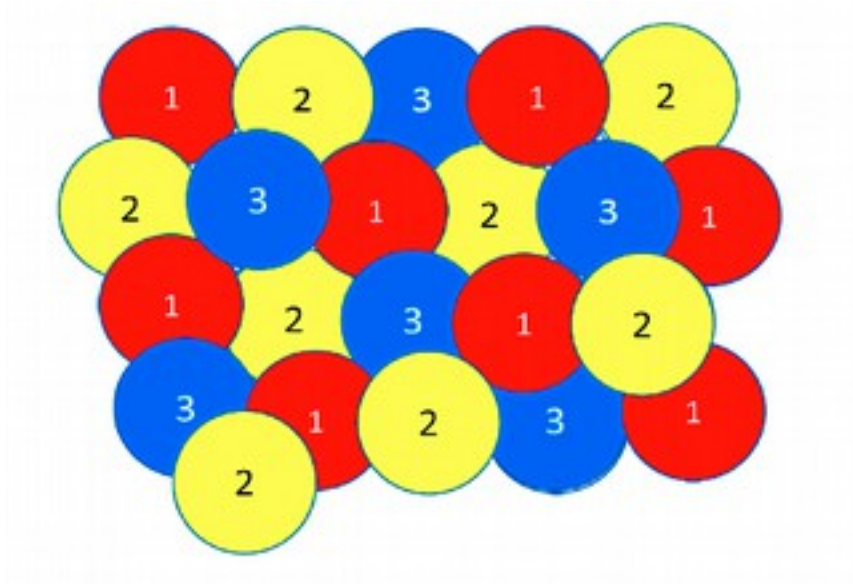


Figure RS 1: Le partage cellulaire du spectre.

Cet exemple montre qu'une utilisation intelligente des ressources existantes

peut considérablement accroître leur utilité.
Bien que la principale utilisation du spectre soit pour des fins de communication, il y a aussi d'autres utilisations, comme la cuisson de la nourriture dans les fours à micro-ondes, les applications médicales, les commandes d'ouverture des garages, etc.
Ainsi, certaines bandes de fréquences sont allouées à ces fins dans ce qui est connu comme les bandes ISM (en anglais Industrial, Scientific and Medical). Cette utilisation du spectre est généralement pour les applications à courte distance. Une percée s'est produite en 1985, lorsque la FCC (en anglais Federal Commission of Communications), l'agence qui supervise le spectre aux États-Unis, étendit l'utilisation de ce spectre aux applications de communications à condition que la puissance d'émission soit maintenue à un niveau très faible de minimiser les interférences.
Les gens pouvaient utiliser librement ces bandes ''sans licence" sans aucune demande de permis préalable, à condition que l'équipement utilisé ait été certifié par un laboratoire agréé qui assurerait sa conformité avec les mesures de mitigation d'interférences.

Plusieurs fabricants ont commencèrent à prendre avantage de cette opportunité pour fournir du matériel qui pouvait être utilisé pour permettre aux ordinateurs de communiquer sans câbles, et certains réseaux de données sans fil couvrant des zones géographiques importantes furent construites avec ce matériel mais le point tournant s'est produit après l'approbation en 1997 de la norme IEEE 802.11 (IEEE signifiant en anglais Institute of Electrical and Electronics Engineers), qui fut la base de ce qui est connu sous le nom WiFi.
L'existence d'une norme qui garantit l'interopérabilité des équipements produits par différents fabricants alimenta une croissance du marché impressionnante qui, à son tour conduisit à une concurrence qui favorisa une baisse spectaculaire du coût des appareils.

En particulier, la partie de la bande ISM entre 2400 et 2483 MHz est aujourd'hui disponible dans la plupart des pays du monde sans une demande préalable de licence et est largement utilisée par les ordinateurs portables, les tablettes électroniques, les téléphones intelligents et même des appareils photographiques. Il est important de souligner le rôle du spectre sans licence dans le succès énorme de l'accès Internet par WiFi à haut débit.

Des nombreux aéroports, hôtels et cafés partout dans le monde offrent l'ac-

cès WiFi Internet gratuit sur leurs prémisses, et des réseaux communautaires sans fil à faible coût couvrant des zones géographiques considérables ont été construits aussi bien en milieu rural qu'urbain, grâce à la disponibilité du spectre gratuit. Les opérateurs de téléphonie mobile, qui ont à payer plus cher les licences de fréquences pour utiliser le spectre, étaient tout à fait hostiles à cette compétition apparemment injuste.

Mais quand ils commencèrent à offrir les téléphones intelligents, qui font un usage intensif de l'Internet, ils se rendirent compte assez vite que le déchargement du trafic sur le WiFi était dans leur meilleur intérêt, car il diminuait le trafic dans leur réseau de distribution (connu sous le nom de backhaul en anglais). Ainsi, maintenant ils encouragent leurs clients à utiliser le WiFi partout où il est disponible et n'utiliser le service de téléphonie cellulaire plus cher seulement qu'en dehors de portée de tout point d'accès WiFi.

Ceci est un exemple remarquable de l'utilité du spectre sans licence même pour les opérateurs de télécommunications traditionnels qui ont souvent exercé des pressions contre elle.

Comment se fait l'arbitrage du spectre ?

Actuellement, les principales méthodes pour avoir accès à une bande de fréquences donnée sont les ventes aux enchères et le soi-disant ''concours de beauté".
La méthode de vente aux enchères est simple; les parties intéressées font une offre pour un morceau donné du spectre; quiconque commet la somme plus élevée obtient le droit d'utiliser les fréquences.
En théorie, cette méthode garantit que l'arbitrage sera transparent.
Dans la pratique, cela a souvent été contourné et il y a eu des cas où des puissants intérêts commerciaux acquièrent des fréquences seulement pour éviter leur utilisation par la compétition, résultant ainsi à des très précieuses bandes de fréquences restant inutilisées.
Aussi il y a la tentation de la part des gouvernements à utiliser cette méthode comme un moyen de générer des revenus pas nécessairement dans le meilleur intérêt public. À titre d'exemple, en l'an 2000, il y avait des ventes aux enchères dans plusieurs pays d'Europe pour l'arbitrage du spectre pour les téléphones mobiles qui entraîna un revenu total de 100 milliards d'euros dans les coffres des gouvernements.
La méthode du ''concours de beauté" consiste à avoir les parties intéressées

soumettre des propositions sur la façon dont ils ont l'intention d'utiliser le spectre.
Un comité de l'organisme de réglementation du spectre décide alors laquelle parmi ces propositions répond mieux aux objectifs publics. Cette méthode repose sur l'objectivité, la compétence technique et l'honnêteté des membres du comité de décision qui n'est pas toujours garantie.

Dans de nombreux pays, il existe des règles pour l'arbitrage du spectre qui exigent la rétrocession des bandes de fréquences qui ont été acquises mais qui n'ont pas été utilisées. Cependant leur application est souvent absente en raison des grands intérêts économiques qui sont affectés.

Figure RS 2: Un véhicule spécial pour la surveillance du spectre dans Montevideo, en Uruguay.

La figure RS 2 montre une photographie d'un véhicule de surveillance du spectre dans Montevideo, en Uruguay et la Figure 3 RS montre une photographie du même genre d'équipement utilisé à Jakarta, en Indonésie.

Figure RS 3: La "Police du spectre" au travail dans Jakarta.

Notez que le spectre gratuit utilisé dans les bandes sans licence ne peut empêcher les problèmes d'interférence, en particulier dans les zones très encombrées. Néanmoins il a connu un succès fantastique pour les applications à courte distance dans les villes et aussi pour les applications longues distance dans les zones rurales. Il est donc conseillé de rechercher de nouvelles formes de répartition du spectre, en tenant compte des besoins des nombreux intervenants et trouver un équilibre entre eux.
Un mécanisme d'allocation dynamique du spectre semble être le meilleur choix compte tenu des avancées technologiques qui ont rendent celui-ci viable aujourd'hui. À titre d'exemple, la méthode actuelle de répartition du spectre est similaire au système ferroviaire où voies ferroviaires peuvent rester inutilisées pendant un temps considérable tandis que l'allocation dynamique du spectre s'apparente au système d' autoroute qui peut être utilisé à tout moment par les différents utilisateurs.

Les problèmes politiques

Ce n'est pas exagéré de pointer l'importance du spectre comme un facilitateur de communications. La télévision et la radio ont une forte influence pour façonner la perception du public sur toute question et ont été utilisés ouvertement pour la propagande politique (Il a été dit que l'élection du président Kennedy des États-Unis était principalement attribuable à sa cam-

pagne télévisée). Pendant la guerre froide, la voix de l'Amérique, Radio Moscou et Radio Havane de Cuba étaient des moyens très efficaces pour influencer un auditoire mondial. Des exemples plus récents incluent l'influence de CNN et Al Jazeera dans l'interprétation publique du Printemps arabe. Le spectre utilisé dans les deux sens de communications a également fait l'objet d'interventions de l'État, notamment en cas de troubles politiques. D'autre part, les intérêts économiques jouent également un rôle essentiel dans la diffusion ; la société de consommation repose lourdement sur la radio et la télévision pour créer des besoins artificiels ou pencher les consommateurs vers une marque particulière.
Nous pouvons conclure que le spectre électromagnétique est une ressource naturelle dont l'utilité est fortement conditionnée par des facteurs technologiques, économiques et politiques.

Explosion de la demande de spectre

Avec la croissance du nombre de tablettes et des téléphones intelligents, les opérateurs télécoms sont en train d'essayer d'accéder à de nouvelles bandes de fréquences, mais la façon traditionnelle d'arbitrer le spectre se confronte à une impasse. Gardez à l'esprit que le spectre est utilisé pour les émissions radio et télévisées, les communications par satellite, le contrôle du trafic aérien, la géolocalisation (en anglais Global Systems postioning -GPS), ainsi que pour les besoins militaires, la police et ainsi que pour d'autres fins gouvernementaux. Traditionnellement, la demande en spectre supplémentaire a été satisfaite grâce aux progrès de l'électronique permirent l'utilisation de fréquences élevées à un coût abordable. Les fréquences élevées sont bien adaptées pour les transmissions à haute vitesse, mais elles sont caractérisées par une portée limitée et sont très atténuées par des murs et autres obstacles ainsi que par la pluie.Ceci est illustré par la comparaison de la couverture d'une station de de radiodiffusion AM à celle d'une radiodiffusion FM: la plus grande couverture de la station AM est due à l'utilisation des fréquences plus basses. D'autre part, les stations FM peuvent utiliser des largeurs de bandes plus grandes et comme conséquence elles peuvent t offrir une meilleure qualité audio au détriment d'une couverture plus limitée. Les opérateurs cellulaires actuels utilisent des fréquences encore plus élevées, généralement supérieures à 800 MHz. En conséquence, les fréquences de radiodiffusion télévisuelles sont convoités par les fournisseurs de téléphonie cellulaire, car en utilisant des fréquences inférieures, ils auraient besoin de moins de stations de base, et feraient d'énormes économies dans le déploie-

ment, l'exploitation et les coûts de maintenance .
C'est pourquoi ces fréquences sont communément appelés ‘’propriétés au bord de la mer”. les techniques pour une utilisation plus efficace du spectre par le biais de méthodes de modulation et de codage avancées ont eu le plus grand impact en permettant plus de bits/s par Hz de largeur de bande disponible. Ceci, à son tour, a été possible grâce aux grands progrès de l'électronique (fabrication circuits intégrés les plus avancés) qui ont rendu économiquement possible l’implémentation de la modulation sophistiquée requise et techniques de codage. Selon les calculs effectués en 1948 par Claude Shannon – le père des télécommunications modernes, une ligne téléphonique typique pouvait porter jusqu'à 30 kbit/s.
Mais cela n'a été possible que dans les années 90 quand les circuits intégrés implémentant les techniques nécessaires étaient effectivement construits.
En particulier, la transition vers la radiodiffusion télévisée terrestre numérique, qui est plus efficace dans l'utilisation du spectre par rapport à la transmission analogique, a libéré une partie du spectre dans les soi-disant ‘’espaces blancs”, les fréquences qui devraient être mises en jachère entre les chaînes de télévision analogiques pour éviter les interférences.

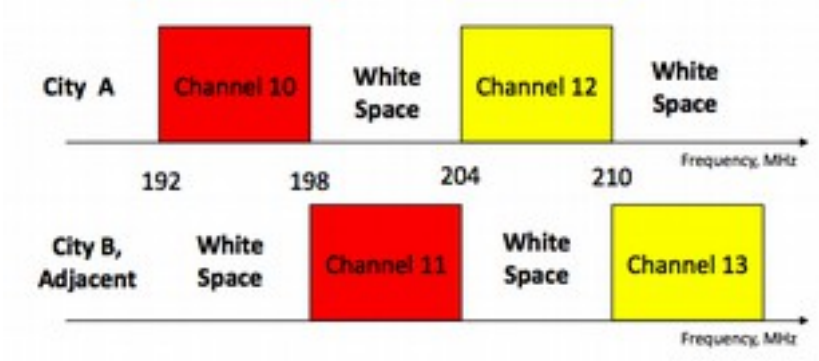


Figure RS 4: Exemple d’arbitrage de canaux TV dans deux cités qui sont suffisamment proches pour que les transmissions de l'une puissent atteindre l'autre. Les espaces blancs sont laissés en jachère pour minimiser les interférences .

Dans la radiodiffusion télévisée analogique traditionnelle, les canaux adjacents ne peuvent pas être utilisés en même temps, parce que le signal d'un canal peut ‘’déborder” sur les deux canaux adjacents et causer une interférence. Ceci est similaire à la réservation centrale utilisée dans les autoroutes pour séparer la circulation dans les deux sens afin d' éviter les collisions.
Ainsi, un "espace blanc" doit être laissé entre deux canaux contiguës de télé-

vision analogique pour éviter les interférences.
La télévision numérique est beaucoup plus efficace dans l'utilisation du spectre, et plusieurs canaux de télévision numérique peuvent opérer dans la même bande de fréquence anciennement utilisée par un canal analogique unique sans ``débordement" dans les canaux adjacents. Ainsi, dans les endroits où la télévision analogique est remplacée par la télévision numérique une '' dividende numérique dividende" est en cours de récolte. En conclusion, le concept d'espace blanc peut être appliqué à trois différentes tranches de fréquences :

- Le spectre qui a été attribuée à la diffusion TV, mais qui n'est pas en cours d'utilisation. Cela vaut particulièrement pour le pays en développement, où il n'y a pas d'incitation économique pour les opérateurs de télévision à utiliser tous les canaux de télévision disponibles.
- Le spectre qui doit être laissé libre entre deux canaux de TV analogue pour éviter les interférences.
- Le spectre qui a été récupéré à la suite de la transition de l'analogique vers la télévision numérique terrestre, qui est plus efficiente en spectre. Cela s'applique actuellement aux pays développés, mais s'appliquera rapidement aux pays en développement.

Au cours des 20 dernières années, il y a eu une croissance énorme de la demande pour plus de spectre pour les services de communications mobiles, dont les services de données demandent beaucoup plus de largeur de bande que la voix et l'utilisation croissante de la vidéo présente un défi supplémentaire. Il n'est pas étonnant que les opérateurs de télécommunications partout dans le monde cherchent à ce qu'une partie de ces ''espaces blancs" leur soient alloués pour satisfaire leurs besoins.
D'autre part, les opérateurs de télévision sont très réticents à concéder tout spectre à ceux qui sont maintenant devenus leurs concurrents directs.

La raréfaction du spectre ou la thésaurisation de fréquences?

Bien que le spectre disponible soit actuellement totalement attribué pour les pays développés, des nombreuses études indépendantes ont montré que son utilisation simultanée effective constitue une infime fraction du total.
Ceci est dû à la manière dont le spectre a été initialement administré et aussi parce que souvent le spectre est utilisé de façon intermittente.

Par exemple, certaines stations d'émissions télévisées ne transmettent pas 24 heures par jour. En conséquence, une nouvelle façon plus radicale d'utiliser le spectre a été suggérée où au lieu d'allouer le spectre de façon exclusive à une organisation donnée, le nouveau paradigme d'allocation dynamique du spectre propose d'utiliser n'importe quel spectre qui est disponible dans une certain endroit à un moment donné et passer à une autre fréquence dès que le brouillage est détecté dans une bande donnée.
Une analogie peut être faite à expliquer ce concept: la façon actuelle d'allouer le spectre est similaire à un système de chemin de fer. Les voies ferrées ne sont jamais utilisées 100 % du temps. Une utilisation plus efficace de la même quantité de terrain peut être réalisée avec une autoroute où des nombreux utilisateurs différents peuvent partager le même chemin selon leurs besoins actuels. Bien sûr, l'implémentation de l'accès dynamique au spectre exige des nouvelles technologies et des nouvelles lois. Des nombreux intérêts acquis combattent cet accès alléguant le risque d'interférence. Le problème clé est de savoir comment déterminer quand une tranche particulière du spectre est très utilisé dans un endroit particulier et comment passer rapidement à une nouvelle bande de fréquence quand un utilisateur existant de priorité plus élevée est détecté. La technologie pour accomplir cet exploit a déjà été démontrée et définie dans la nouvelle norme IEEE 802.22 récemment approuvée, ainsi que dans les deux autres qui sont actuellement en considération.

IEE 802.22

Stimulé par le succès impressionnant du WiFi (dû principalement à l'utilisation du spectre ouvert sans licence), l'IEEE a créé un groupe de travail chargé d'adresser les exigences d'un réseau sans fil régional.
Le défi était de développer une technologie appropriée pour la transmission longue distance qui pourrait être utilisée dans différents pays (avec des très différentes allocations de spectre). Ainsi, ils se concentrèrent sur les fréquences actuellement allouées à la radiodiffusion télévisée qui s'étendent approximativement de 50 à 800 MHz.
Nulle part, ce spectre est tout le temps utilisé dans son intégralité, donc il y des ''espaces blancs", les régions en jachère qui pourraient être ''re-exploitée" et mis à profit pour des communications bidirectionnelles. Dans les zones rurales du monde entier, mais spécialement dans les pays en développement il y a de grandes portions du spectre actuellement sous-utilisées . Il est prévu que la norme IEEE 802.22 permettra un accès dynamique du spectre d'une manière similaire à la norme IEEE 802.11 (WiFi), permettant l'accès ouvert

au spectre.
Evidemment, tout le spectre ne sera pas ouvert à la fois, un processus graduel est nécessaire à mesure que les nombreux obstacles techniques, juridiques, économiques et politiques sont résolus, mais il ne fait aucun doute que c'est la tendance et que la norme IEE 802.22 ouvre la voie pour le futur de l'allocation des fréquences .
Afin d'évaluer la disponibilité d'un canal de fréquence donnée à un moment donné, deux méthodes sont envisagées: détection de canal et l'utilisation d'une base de données des utilisateurs primaires dans une zone géographique donnée à un moment donné.
La détection de canal signifie qu'avant toute tentative d'utilisation d'un canal, les stations de base vont écouter le canal. S'il est utilisé, ils essayeront de nouveau et répéteront la procédure jusqu'à ce qu'un canal libre soit trouvé. Cette procédure est répétée à intervalles réguliers pour tenir compte de la possibilité de stations s'éveillant à tout moment. Cette méthode devrait suffire pour l'allocation dynamique du spectre. Néanmoins les détenteurs actuels du spectre ont réussi à convaincre les régulateurs de l'application de la deuxième méthode, qui est beaucoup plus compliquée et impose une complexité supplémentaire et des coûts en équipement du consommateur.
La seconde méthode consiste en la construction d'une base de données de toutes les stations de transmission titulaires existantes, avec leur position et leur zone de couverture respective, afin d'établir une zone ‘’ans limite” dans un canal donné.
Une nouvelle station voulant transmettre doit d'abord déterminer sa position exacte (ainsi elle doit disposer d'un récepteur GPS ou d'autres moyens pour déterminer son emplacement géographique), puis interroger la base de données afin de s'assurer que son emplacement actuel n'est pas dans la zone interdite du canal qu'elle est en train d'essayer d'utiliser. Pour interroger la base de données, elle doit avoir accès à Internet par un autre moyen (par ADSL en anglais asymétrique Digital Subscriber Line, par câble, par satellite, ou Cellulaire) en plus de la radio de norme 802.22 (qui ne peut pas être utilisée jusqu'à ce que la canal soit confirmé comme utilisable).
Ainsi cela ajoute un fardeau supplémentaire considérable dans le matériel de la station qui se traduit en des coûts supplémentaires, en dehors du coût de la construction et la maintenance de la base de données. Aux États-Unis, la FCC (Federal Communications Commission, l'organisme de réglementation de spectre) a été en train de promouvoir la construction de la base de données des utilisateurs enregistrés et a autorisé 10 entreprises privées différentes de construire, exploiter et entretenir ces référentiels de données.

En outre, des essais de la norme ont été conduits. Au Royaume-Uni, l'OFCOM (le régulateur du spectre) est en train de conduire des essais de la norme IEE 802.22 en se concentrant sur la méthode de base de données après avoir écarté la méthode de détection de spectre pour la mitigation des interférences. Bien que le IEEE 802.22 est la norme officiellement agréée qui a reçu le plus de publicité, il y a plusieurs candidats concurrents qui sont en train en exploration en vue de tirer parti des espaces blancs TV pour fournir des services de communication bidirectionnels, parmi ceux-ci, il y a:

IEEE 802.11af

Cet amendement tire profit de l'énorme succès de la norme IEEE 802.11 en adaptant la même technologie pour fonctionner dans les bandes de fréquences allouées à la transmission télévisée, diminuant ainsi l'encombrement du spectre de la bande 2,4 GHz et offrant une plus grande couverture à cause de l'utilisation des fréquences de transmission inférieures. Les détails du IEEE 802.11af sont encore en cours de discussion par le groupe de travail correspondant IEEE 802.11.

IEEE 802.16h

Cet amendement de la norme 802.16 a été ratifiée en 2010 et décrit le mécanisme pour implémenter le protocole dans les applications en exploitation non coordonnée, avec licence ou sans licence. Bien que la plupart des déploiements ont été dans la bande des 5 GHz, il peut également s'appliquer aux fréquences de la bande de télévision et peut bénéficier des déploiements significatifs des systèmes WiMAX (en anglais Wireless Microwave Access) dans de nombreux pays .

L'avantage pour les pays en développement

Il est à noter que dans les pays en développement, le spectre attribué aux émissions de télévision n'est que partiellement utilisé.
Ceci représente une occasion magnifique d'introduire les services des réseautage de données sans fil dans les canaux qui ne sont pas actuellement alloués, et commencer à récolter les bénéfices de la norme 802.22 dans un environnement plus favorable, où la détection de spectre et le changement de fréquence agile requis pour partager le spectre surpeuplé dans les pays développés peut être évité. L'utilité des fréquences plus basses pour la transmission bidirectionnelle des données a été prouvée par le déploiement avec succès des systèmes cellulaires CDMA (en anglais Code Division Modulation

Access) dans la bande des 450 MHz, localisée en plein milieu des fréquences attribuées à la télévision, dans les zones rurales comme la Patagonie Argentinne, actuellement desservie par ‘’Cooperativa Telefonica de Calafate, en brief COTECAL” . COTECAL offre les services vocaux et données aux clients à des distances allant jusqu'à 50 km de la station de base, dans la belle région représentée dans la figure suivante:

Figure RS 5: Région desservie en services voix et données par COTECAL, en Calafate et El Chalten, en Argentine.

Il y a donc une opportunité pour les parties prenantes de faire pression pour l’implémentation des solutions basées sur des périphériques de bandes de télévision à un stade précoce, pendant que les problèmes de transition vers le numérique sont à l'étude . Cela aidera à assurer que intérêts commerciaux d’un petit nombre ne l'emportent pas sur les intérêts de la société en large. Les activistes/ lobbyistes devraient insister sur la nécessité de la transparence dans le processus d'attribution des fréquences et la responsabilisation de l'administration du spectre dans leur pays ou région. En outre, il est important que ceux qui souhaitent déployer des réseaux acquièrent une compréhension de l'utilisation réelle du spectre par les titulaires de spectre dans

chaque région de leur pays.
Le contrôle du spectre nécessite des instruments couteux et une courbe d'apprentissage abrupte pour les utiliser, mais récemment un appareil à cout abordable et facile à utiliser est devenu disponible. Il permet une analyse de la bande des fréquences comprises entre 240 MHz et 960 MHz, qui englobe la partie supérieure de la bande de télévision. Les détails de ce matériel ouvert basé sur l'analyseur de spectre RF Explorer pour la bande de télévision supérieure se trouvent sur :
http://www.seeedstudio.com/depot/rf-explorermodel-wsub1g -p- 922.html
La Figure RS 6 montre le RF Explorer pour la bande des fréquences 2,4 GHz en train d'être utilisé pour tester une antenne construite par les participants de la formation sans fil de l'atelier de formation sans fil de l'ICTP en 2012 à Trieste, en Italie.

Figure RS 6 : Les participants en provenance d'Albanie, du Népal, du Malawi et l'Italie testent une antenne avec l'analyseur de spectre RF Explorer à Trieste, en février 2012.

Cet instrument à faible coût ouvre la voie à une large participation de la population dans la mesure de l'utilisation réelle du spectre de leur propre pays qui nous espérons peut aboutir à une meilleure gestion du spectre.
Pour plus des informations supplémentaires, voir:
http://www.apc.org/en/faq/citizens-guide-airwaves

5. ANTENNES/LIGNES DE TRANSMISSION

L'émetteur qui génère l'énergie RF que l'antenne utilise est généralement situé à une certaine distance des bornes de l'antenne. La liaison qui connecte les deux est **la ligne de transmission RF**. Son but est de transporter l'énergie RF d'un endroit à un autre et de le faire aussi efficacement que possible. Du côté du récepteur, l'antenne est responsable de recueillir tous les signaux radio dans l'air et de les passer au récepteur avec le minimum de distorsion de sorte que la radio puisse décoder le signal convenablement. Pour ces raisons, le câble RF joue un rôle très important dans les systèmes de radio : il doit maintenir l'intégrité des signaux dans les deux directions.

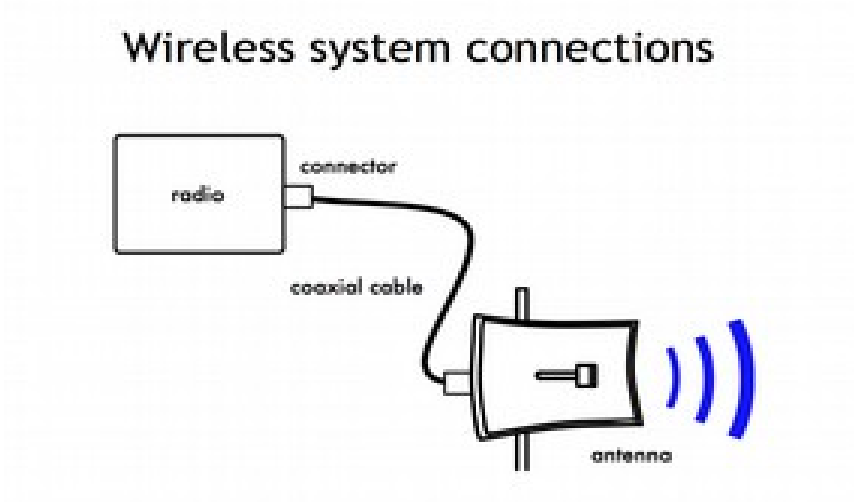


Figure ATL 1: Radio, Ligne de transmission et Antenne

La ligne de transmission la plus simple qu'on peut envisager est le bifilaire (ou en anglais twin lead) constitué de deux conducteurs séparés par un diélectrique ou isolant. Le diélectrique peut être constitué d'air ou une matière plastique comme celle utilisée pour les lignes de transmission plates utilisées dans les antennes de télévision. Une ligne de transmission bifilaire ouverte à une extrémité ne saura pas rayonner parce que le courant dans chaque conducteur a la même valeur mais une direction opposée, de sorte que les champs créés en un point donné à une certaine distance de la ligne s'annulent.

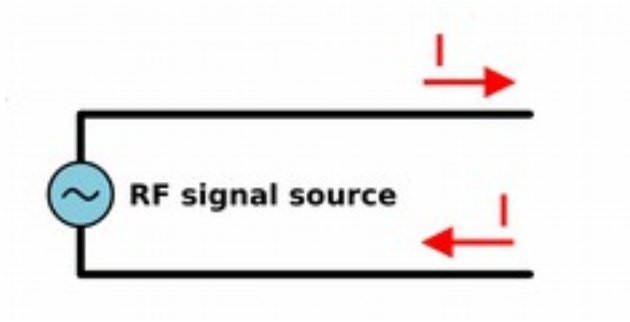


Figure ATL 2 : Ligne de transmission bifilaire

Si nous plions les extrémités ouvertes de la ligne de transmission dans des directions opposées, les courants génèreront des champs électriques qui sont en phase et se renforcent les uns les autres. Ils vont donc rayonner et se propager à distance. Nous avons maintenant une antenne à l'extrémité de la ligne de transmission.

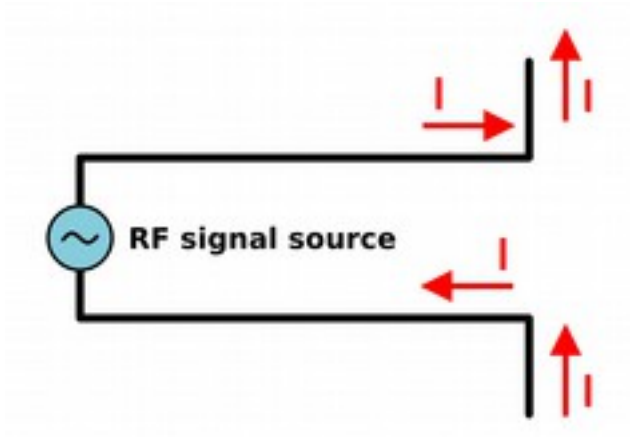


Figure ATL 3 : Antenne à partir de la ligne de transmission.

La longueur de la partie courbée de la ligne de transmission déterminera la caractéristique de l'antenne. Si cette longueur correspond à un quart d'une longueur d'onde, nous aurons une antenne dipôle demi-onde avec un gain de 2,15 dBi. Le fonctionnement de la ligne de transmission bifilaire qui vient d'être décrite est fortement affecté par n'importe quel métal dans sa proximité.

Ainsi une meilleure solution est de confiner les champs électriques au moyen d'un conducteur externe qui protège le conducteur intérieur. Ceci constitue un câble *coaxial*. Alternativement, un tube métallique creux de dimensions appropriées pourra aussi transporter l'énergie RF dans ce qui est connu comme un *guide d'ondes*.

Câbles

Les câbles coaxiaux (ou coax en abrégé, dérivé des mots ‘’d’un axe commun”) sont presque exclusivement utilisés pour des fréquences plus élevées que les fréquences HF. Les câbles coaxiaux ont un fil conducteur interne qui est entouré d'un matériel diélectrique non-conducteur appelé diélectrique, ou tout simplement isolation. Le diélectrique est ensuite entouré d’un bouclier protecteur qui est souvent en fils tressés. Le diélectrique empêche la formation d’une connexion électrique entre le noyau interne et le bouclier protecteur. Finalement, le câble coaxial est protégé par une gaine extérieure qui est généralement faite de matériel PVC. Le conducteur interne transporte le signal RF et le bouclier externe empêche le signal RF de rayonner dans l'atmosphère tout en empêchant aussi les signaux extérieurs d'interférer avec le signal porté par le noyau interne. Un autre fait intéressant est que le signal électrique à haute fréquence se déplace uniquement le long de la couche extérieure d'un conducteur, le matériau de l'intérieur ne contribuant pas à la conduction. Par conséquent, plus large est le conducteur interne, meilleur sera la conduction du signal.
C'est ce qu'on appelle ‘’effet pelliculaire” (en anglais skin effect).

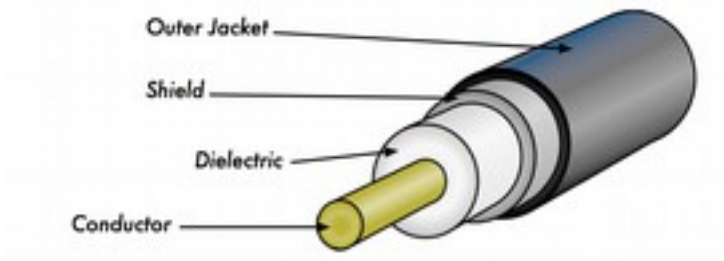


Figure ATL 4: câble coaxial avec gaine extérieure, bouclier, matériel diélectrique et conducteur interne.

Même si la construction coaxiale est bonne pour transporter le signal, il y a toujours une résistance à la circulation électrique: pendant que le signal se déplace, il perd de sa puissance. Cette détérioration est connue sous le nom d'**atténuation**, et elle se mesure en décibels par mètre (dB/m) pour les lignes de transmission. Le taux d'atténuation est fonction de la fréquence du signal et la construction physique du câble lui-même. A mesure que la fréquence du signal augmente, son atténuation fera de même. Evidemment, nous devons minimiser l'atténuation du câble autant que possible en maintenant le câble très court et en utilisant des câbles de haute qualité.
Voici quelques points à considérer lors du choix d'un câble pour une utilisation avec des appareils à micro-ondes :
1. ''Le plus court sera le mieux" : La première règle lorsque vous installez un morceau de câble est d'essayer de le maintenir le plus court possible. Comme la perte d'énergie n'est pas linéaire, si vous doublez la longueur du câble, vous allez perdre beaucoup plus que le double de la puissance. De la même manière, la réduction de la longueur du câble de moitié vous donne plus de deux fois d'énergie à l'antenne. La meilleure solution est de placer l'émetteur le plus proche possible de l'antenne, même si cela signifie le placer sur une tour.
2. ''Le moins coûteux est le pire! " La deuxième règle d'or est que tout l'argent que vous investissez dans l'achat d'un câble de bonne qualité est une bonne affaire. Les câbles bon marché peuvent être utilisés à de basses fréquences, telles que le VHF. Les micro-ondes nécessitent une disponibilité des câbles de haute qualité.
3. ''Eviter le RG-58". Il est destiné aux réseautages Ethernet, au CB ou Radio VHF, pas pour les micro-ondes .
4. ''Eviter le RG-213 ou RG -8". Ils sont destinés aux CB et la radio HF. Dans ce cas, même si le diamètre est grand, l'atténuation est significative à cause l'utilisation d'un isolant peu coûteux.
5. ''Quand c'est possible, utilisez le câble LMR le plus nominale ou l'équivalent que vous pouvez trouver". Le LMR est une marque de câble coaxial disponible en différents diamètres qui fonctionne bien à des fréquences micro-ondes. Les plus couramment utilisés sont le LMR- 400 et le LMR- 600. Les câbles Heliax sont également très bons, mais sont coûteux et difficile à utiliser.
6. ''Quand c'est possible, utilisez des câbles qui sont pré-sertis et testés dans un laboratoire approprié. L'installation des connecteurs aux câbles est une affaire délicate qui est difficile à faire correctement, même avec les outils spécifiques. Ne jamais marcher sur un câble, trop le plier, ou essayer de dé-

brancher un connecteur en tirant sur le câble directement.
Tous ces comportements peuvent changer la caractéristique mécanique du câble et donc son impédance, court-circuiter le noyau interne et le bouclier extérieur, ou même briser la ligne.
7. '' Ces problèmes sont difficiles à suivre et à reconnaître et peuvent conduire à des comportements imprévisibles sur la liaison radio".
8. ''Pour des très courtes distances, un câble mince de bonne qualité peut être suffisant car il n'introduira pas trop d'atténuation".

Guides d'ondes

Au-dessus de 2 GHz, la longueur d'onde est suffisamment courte pour permettre un transfert d'énergie pratique et efficient par des moyens différents. Un guide d'ondes est un tube conducteur à travers lequel l'énergie est transmise sous forme d'ondes électromagnétiques. Le tube agit comme une barrière qui confine les ondes en son intérieur. Le phénomène de la cage de Faraday empêche les effets électromagnétiques de se manifester en dehors du guide d'onde. Les champs électromagnétiques se propagent à travers le guide d'ondes à l'aide des réflexions sur ses parois intérieures, qui sont considérés comme des conducteurs parfaits. L'intensité des champs est plus grande au centre du guide d'onde le long de l'axe X, et doit être réduite à zéro sur les parois externes parce que l'existence de n'importe quel champ parallèle aux parois sur la surface provoquerait la circulation d'un courant infini dans un conducteur parfait. Les axes X, Y et Z d'un guide d'onde rectangulaire peuvent être vus dans la figure suivante:

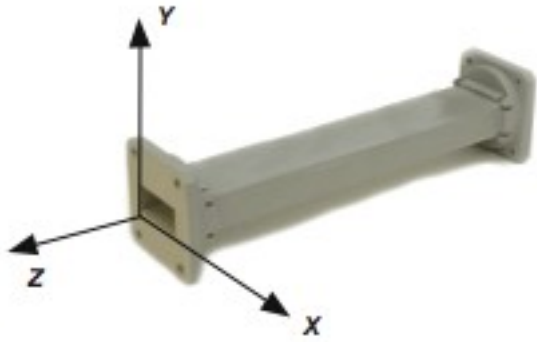


Figure ATL 5: Les axes X, Y, et Z d'un guide d'onde rectangulaire.

Il y a un nombre infini des façons dont les champs électrique et magnétique peuvent s'arranger dans un guide d'onde pour des fréquences supérieures à une limite inférieure. Chacune de ces configurations de champ est appelé un mode. Les modes peuvent se subdiviser en deux groupes généraux. Un groupe, désigné TM (en anglais Transverse Magnetic), dont le champ magnétique est entièrement transversal à la direction de propagation, mais qui possède une composante électrique dans la direction de propagation. L'autre type, désigné TE (en anglais Transverse Electric) a son champ électrique totalement transversale, mais possède une composante du champs magnétique dans la direction de propagation . Le mode de propagation s'identifie par les lettres de groupe suivies par deux indices numériques. Par exemple, TE 10, TM 11, etc. Pour une taille de guide d'onde donnée, le nombre de modes possibles augmente avec la fréquence, et pour la fréquence la plus basse pouvant être transmise il existe seul mode, dénommé mode dominant. Dans un guide d'onde de forme rectangulaire, la dimension critique est X. A la fréquence de transmission la plus basse, cette dimension doit être supérieure à 0,5 fois la longueur d'onde λ. En pratique, la dimension Y est habituellement d'environ 0,5 fois X pour éviter toute possibilité d'opération dans un mode différent du mode dominant. Des formes transversales autres que le rectangle peuvent être utilisées, le plus important étant le tube circulaire. Les mêmes considérations similaires au cas rectangulaire s'appliquent pour ces formes. Le tableau suivant présente les dimensions de longueurs d'onde pour les guides rectangulaires et circulaires. Dans ce tableau, le X est la largeur d'un guide d'onde rectangulaire et le r est le rayon d'un guide d'onde circulaire. Toutes les figures s'appliquent au mode dominant.

Type de guide	rectangulaire	circulaire
Limite de longueur d'onde	2X	3.41r
La plus longue longueur d'onde transmise avec peu d'atténuation	1.6X	3.2r
La plus courte longueur d'onde avant que le mode prochain devienne possible.	1.1X	2.8r

L'énergie peut être introduite ou extraite d'un guide d'ondes soit au moyen du champ électrique ou du champ magnétique. Le transfert d'énergie passe typiquement par une ligne coaxiale. Les deux méthodes possibles pour le couplage à une ligne coaxiale consistent soit à utiliser le conducteur intérieur de la ligne coaxiale, ou former une boucle.

Une sonde qui est simplement une courte prolongation du conducteur intérieur de la ligne coaxiale peut être orientée de façon qu'elle soit parallèle à des lignes électriques de la force. Une boucle peut être agencée de manière à joindre certaines lignes magnétiques de la force. Le point auquel l'accouplement maximum est obtenu dépend du mode de propagation dans le guide ou la cavité. L'accouplement est maximal lorsque 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 utilisé comme antenne plutôt que comme ligne de transmission). Ce rayonnement peut être amélioré en élargissant le guide d'ondes pour former une antenne cornet pyramidale. Il y a dans l'annexe A, dénommée la construction de l'antenne, des exemples pratiques d'antennes guide d'ondes pour le WiFI.

Connecteurs et adaptateurs.

Les connecteurs permettent un câble à être connecté à un autre câble ou à une composante de la chaîne RF. Il y a une grande variété de d'assortiments et de connecteurs conçus pour aller de pair avec différents tailles et types de câbles coaxiaux. Nous allons décrire quelques-uns des plus populaires.

Les **connecteurs BNC** ont été développés à la fin des années 40. Le BNC signifie en anglais Bayonet Neill Concelman, nommé d'après ceux qui l'ont inventé : Paul Neill et Carl Concelman.

La gamme de produits BNC consiste en un connecteur miniature de connexion/déconnexion rapide. Il dispose de deux crochets baïonnette sur le connecteur femelle, et le raccordement se fait avec seulement un quart de tour de l'écrou d'accouplement.

Les connecteurs BNC sont parfaitement appropriés pour la terminaison des câbles coaxiaux miniatures et subminiatures (RG- 58 à RG-179, RG -316, etc.). Ils se trouvent le plus souvent sur les équipements d'essai et le câbles coaxiaux Ethernet 10base2.

Les **connecteurs TNC** ont également été inventés par Neill et Concelman, et consistent en une variation filetée du BNC. Grâce à une meilleure interconnexion fournie par le raccord fileté, les connecteurs TNC fonctionnent à environ 12 GHz . TNC est l'acronyme de Threaded Neill Concelman (Neill Concelman fileté).

Les connecteurs **Type N** (encore une fois pour Neill, bien que parfois attribué à la "Marine", Navy en anglais) ont été initialement développées au cours de la Seconde Guerre mondiale. Ils sont utilisables jusqu'à 18 GHz, et très couramment utilisés pour les applications micro-ondes.

Ils sont disponibles pour presque tous les types de câble.
Tant la fiche de prise/ câble que celle de prise/douille sont censées être étanches, fournissant de ce fait un collier efficace. Néanmoins, pour une utilisation à l'extérieur, ils doivent être enveloppés dans un ruban auto agglomérant pour empêcher l'infiltration de l'eau. **SMA** est un acronyme pour la version A de SubMiniature, et a été développé dans les années 60. Les connecteurs SMA sont des unités subminiatures de précision qui fournissent une performance électrique excellente jusqu'à 18 GHz. Ces connecteurs filetés à haute performance sont de taille compacte et ont une durabilité mécanique exceptionnelle.
Le nom **SMB** dérive de SubMiniature B, la deuxième conception subminiature. Le SMB est une version réduite du SMA avec un accouplement pour encliquetage. Il offre une capacité de large à 4 GHz avec une conception de connecteur à encliquetage.
Les connecteurs **MCX** ont été introduits dans les années 80. Alors que le MCX utilise un contact intérieur et un isolateur de dimensions identiques aux SMB, le diamètre extérieur de la prise est de 30% plus petit que celui du SMB. Cette série fournit aux concepteurs des bonnes options dans le cas où le poids et l'espace physique sont limités. Le MCX offre une capacité de large bande à 6 GHz avec une conception de connecteur à encliquetage.
En plus de ces connecteurs standards, la plupart des appareils Wi-Fi utilisent une variété des connecteurs propriétaires.
Souvent, ce sont simplement des connecteurs micro-ondes normaux avec les parties de conducteur central inversées, ou le fil coupé dans la direction opposée.
Ces parties sont souvent intégrées dans un système micro-ondes à l'aide d'un jumper court et flexible appelé pigtail qui convertit le connecteur non standard en quelque chose de plus robuste et plus couramment disponible. Certains de ces connecteurs incluent:
RP-TNC. Il s'agit d'un connecteur TNC avec les genres inversés.
U.FL (également connu sous le nom MHF). C'est peut-être le plus petit connecteur micro-ondes largement utilisé actuellement. Le U.FL/MHF est généralement utilisé pour connecter une carte radio mini-PCI à une antenne ou un plus grand connecteur (tels que les connecteurs N ou TNC) à l'aide d'un câble mince dans ce qui est connu comme pigtail. La série **MMCX**, qui est aussi appelé MicroMate, est l'une des plus petites lignes de connecteurs RF qui a été développée dans les années 90. Le MMCX est une série de connecteurs microminiature ayant un mécanisme de verrouillage automatique permettant une rotation de 360 degrés pour plus de flexibilité.

Les connecteurs MC -Card sont encore plus petits et plus fragiles que les MMCX. Ils ont un connecteur externe fendu qui se casse facilement après un certain nombre d'interconnexions.
Les adaptateurs sont des dispositifs courts, a double face qui sont utilisés pour relier deux câbles ou des composants qui ne peuvent pas être reliés directement. Par exemple, un adaptateur peut être utilisé pour connecter un connecteur SMA à un BNC. Les adaptateurs peuvent être aussi utilisés pour relier des connecteurs du même type mais de genres différents.

Figure ATL 6 : Un adaptateur baril N femelle.

Par exemple, un adaptateur très utile est celui qui permet de relier deux types de connecteurs N, ayant des prises femelles des deux côtés.

Choisir le bon connecteur

''La question de genre." La plupart des connecteurs ont un genre bien défini. Les connecteurs mâles ont une enveloppe ou manche externe (souvent avec un fil intérieur) destiné à entourer le corps du connecteur femelle. Ils ont normalement une broche qui s'insère dans la prise correspondante du connecteur femelle, qui a une enveloppe filetée sur la surface externe ou deux struds de baïonnette faisant saillie à partir d'un cylindre.
Faites attention aux connecteurs à polarité inverse pour lesquels le mâle possède une douille intérieure et la femelle une broche intérieure. Habituellement les câbles sont dotés de connecteurs mâles aux deux extrémités, tandis que les dispositifs RF (c'est-à-dire les émetteurs et antennes) ont des connecteurs femelles. Les parafoudres, les coupleurs directionnels et des dispositifs de mesure de ligne ont deux connecteurs mâles et femelles.

Assurez-vous que chaque connecteur mâle dans votre système se marie à un connecteur femelle.
‘’Moins c’est mieux." Essayez de réduire le nombre de connecteurs et adaptateurs dans la chaîne RF. Chaque connecteur introduit une certaine perte supplémentaire (jusqu'à un dB pour chaque connexion, selon le connecteur).
‘’ Achetez, ne construisez pas.” Comme 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, réaliser ce travail correctement est presque impossible pour les petits connecteurs comme l’U.FL et le MMCX . Même la terminaison des câbles ‘’mousse” n'est pas une tâche facile.
‘’N’utilisez pas le BNC pour des fréquences de 2,4 GHz ou plus.” Utilisez des connecteurs de type N (ou SMA, SMB, TNC, etc.).
Les connecteurs micro-ondes sont des pièces faites avec précision et peuvent être facilement endommagé suite à un mauvais traitement. En règle générale, vous devez faire tourner la douille extérieure pour serrer le connecteur, tout en laissant le reste du connecteur (et du câble) stationnaire .
Si d'autres parties du connecteur se tordent en serrant ou desserrant, des dégâts peuvent facilement se produire.
‘’Ne jamais marcher sur les connecteurs ou les laisser tomber par terre lors de la déconnexion des câbles (cela arrive plus souvent que vous pouvez imaginer, surtout lorsque l'on travaille sur un mât sur un toit). ’Ne jamais utiliser des outils comme des pinces pour serrer les connecteurs”. Toujours utiliser vos mains.
Lorsque vous travaillez à l'extérieur, n'oubliez pas que les métaux se dilatent à haute températures et se contracte à basse température : un connecteur trop serré peut se plier en été ou même briser en hiver.

Diagrammes de rayonnement d’antennes

Les antennes sont une composante très importante de systèmes de communication. Par définition, une antenne est un dispositif permettant de transformer un signal RF voyageant sur une ligne de transmission en une onde électromagnétique dans l'espace libre.
Les antennes ont une propriété connue sous le nom de réciprocité, qui signifie qu'une antenne conservera les mêmes caractéristiques, peu importe que ça soit en émission ou en réception. Toutes les antennes fonctionnent efficacement sur une bande de fréquences relativement étroite.

Une antenne doit être accordée sur la même bande de fréquence que le système de radiocommunication auquel il est relié, sinon la réception et la transmission seront compromises (altérées).
En radiodiffusion, nous pouvons fonctionner avec des antennes de réception inefficientes, parce que les émetteurs sont très puissants.
Mais dans les communications bidirectionnelles, nous devons avoir des antennes dimensionnées de façon appropriée.
Lorsqu'un signal est introduit dans une antenne, l'antenne émet un rayonnement qui est diffusé dans l'espace d'une certaine manière.
Une représentation graphique de la distribution relative de la puissance rayonnée dans l'espace est appelé diagramme de rayonnement.

Glossaire des termes d'antenne

Avant de parler antennes spécifiques, il y a quelques termes communs qui doivent être définis et expliqués:

Impédance d'entrée

Pour un transfert d'énergie efficient, l'impédance de la radio, l'antenne, et le câble de transmission qui les relient doivent être la même. Les émetteurs et leurs lignes de transmission sont généralement conçus pour 50 Ω d'impédance. Si l'antenne présente une impédance de différente de 50 Ω, il y aura un déséquilibre et des réflexions auront lieu à moins qu'un circuit d'adaptation d'impédance soit inséré. Quand l'une de ces composantes est mal adaptée, l'efficacité de la transmission en souffrira.

Perte de retour

La perte de retour est une autre façon d'exprimer le déséquilibre. Il s'agit d'un rapport logarithmique mesuré en dB qui compare la puissance Pr reflétée par l'antenne à la puissance Pi qui est introduite dans l'antenne par la ligne de transmission:

$$Perte\ de\ retour\ (en\ dB) = 20\ log_{10}\ Pi/Pr$$

Bien que de l'énergie sera toujours reflétée de nouveau dans le système, une grande perte de retour résultera en une performance inacceptable pour l'antenne. L'interaction entre l'onde qui se propage de l'émetteur vers l'antenne et l'onde réfléchie par l'antenne vers l'émetteur crée ce qui est connu comme une onde stationnaire.

Ainsi une autre façon de mesurer la différence d'impédance se fait au moyen du rapport d'onde stationnaire (ROS) (en anglais Voltage Standing Wave Ratio or VSWR) définie par :

$$\textit{Perte de retour (en dB)} = 20 \log_{10} (ROS+1/ROS -1)$$

Dans une ligne de transmission parfaitement équilibrée, le ROS = 1.
Dans la pratique, nous nous efforçons de maintenir un ROS inférieur à 2.

Largeur de bande

La largeur de bande d'une antenne se rapporte à la gamme de fréquences F_H – F_L dans laquelle l'antenne peut fonctionner correctement. La largeur de bande de l'antenne est le nombre de Hz pour laquelle l'antenne répond à certaines exigences, comme présentant un gain de moins de 3 dB du gain maximum ou un ROS inférieur à 1,5. La largeur de bande peut également être décrite en termes de pourcentage de la fréquence centrale de la bande.

$$\textit{Largeur de bande} = 100 (F_H - F_L)/F_C$$

...où F_H est la plus haute fréquence dans la bande, F_L est la plus faible fréquence dans la bande, et F_C est la fréquence centrale de la bande. De cette façon, la largeur de bande est constante par rapport à la fréquence. Si la largeur de bande passante 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 lors de la transmission ou de recueillir l'énergie provenant d'une direction particulière lors de la réception. Si une liaison sans fil utilise des locations fixes dans les deux sens, 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 n'est pas fixe, il peut être impossible de prédire où l'émetteur sera, et donc l'antenne devrait idéalement rayonner aussi bien que possible dans toutes les directions.
Une antenne omnidirectionnelle est utilisée dans ces applications.

Le **gain** ne peut pas être défini en termes d'une quantité physique telle que le Watt ou l'Ohm, mais plutôt comme un rapport sans dimension.

Le gain s'exprime par référence à une antenne standard.
Les deux antennes de référence les plus communes sont l'antenne isotrope et l'antenne dipôle à demi-onde.
L'antenne isotrope rayonne aussi bien dans toutes les directions. Les antennes isotropes réelles n'existent pas, mais elles fournissent des modèles d'antenne théoriques simples et utiles permettant de comparer les antennes réelles. Toute antenne véritable rayonnera plus d'énergie dans certaines directions que dans d'autres.
Comme les antennes ne peuvent pas créer de l'énergie, la puissance totale rayonnée est identique à celle d'une antenne isotrope. Toute énergie supplémentaire rayonnée dans le sens favorisé est également compensée par moins d'énergie rayonnée dans une autre direction. 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 lorsqu'elle est alimentée par la même puissance d'entrée. Habituellement, nous sommes seulement intéressés par le gain maximum, qui est le gain dans la direction dans la quelle l'antenne rayonne la majeure partie de la puissance, la soit disant ''ligne de visée'' ou ''boresight'' en anglais.
Un gain d'antenne de **3 dB** par rapport à une antenne isotrope serait écrit que **3 dBi**. L'antenne dipôle à demi-onde peut constituer une référence utile pour la comparaison aux autres antennes à une fréquence donnée ou sur une bande très étroite de fréquences.
Contrairement à l'isotrope, elle est très facile à construire et parfois les fabricants expriment le gain par rapport au dipôle a demi-onde au lieu de la isotrope. Un gain d'antenne de 3 dB par rapport à une antenne dipôle s'exprimerait comme 3 dBd. Comme une antenne dipôle à demi-onde a un gain de 2,15 dBi, nous pouvons trouver la gain dBi de n'importe quelle antenne en ajoutant 2,15 à son gain dBd.
La méthode de mesure de gain d'une antenne en comparant l'antenne testée à une antenne de référence connue, ayant un gain calibré, est techniquement connue sous le nom de technique de transfert de gain.

Diagramme de rayonnement

Le diagramme de rayonnement ou diagramme d'antenne décrit la force relative du champ rayonné par l'antenne dans différentes directions à une distance constante.
Le diagramme de rayonnement est aussi un modèle de réception car il décrit aussi les propriétés de réception de l'antenne, comme une conséquence de la réciprocité.

Le diagramme de rayonnement est tridimensionnel, mais généralement les diagrammes de rayonnement publiés sont une tranche bidimensionnelle du modèle tridimensionnel, dans les plans horizontaux et verticaux.
Ces mesures des modèles sont présentées soit sous un format rectangulaire ou polaire.
La figure suivante montre un diagramme de rayonnement aux coordonnées rectangulaires d'une antenne Yagi typique à dix éléments.
Le détail est de bonne qualité mais il est difficile de visualiser le comportement de l'antenne dans différentes directions.

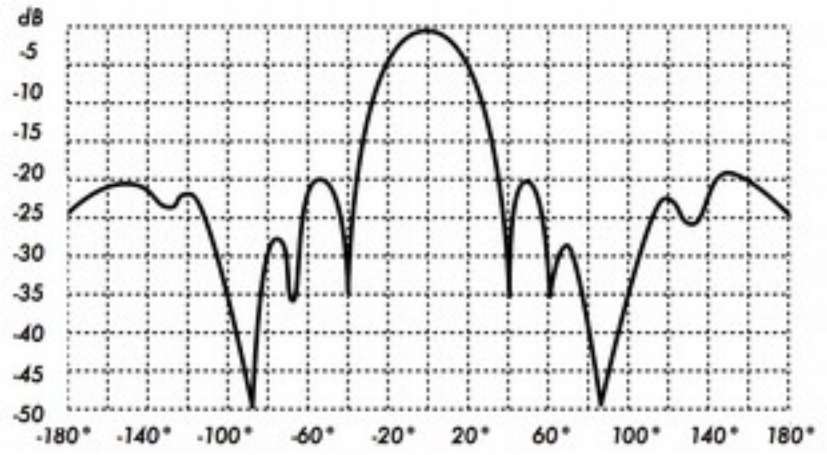


Figure ATL 7 : Un diagramme de rayonnement aux coordonnées rectangulaire du d'une antenne Yagi.

Les systèmes de coordonnées polaires sont utilisés presque universellement. Dans un graphique de coordonnées polaires, les points sont situés par projection le long d'un axe tournant (rayon) à une intersection avec un des nombreux cercles concentriques qui représentent le gain correspondant en décibel référencé à 0 dB au bord externe du diagramme de rayonnement.

Cette représentation permet de mieux appréhender la distribution radiale de la puissance de l'antenne.
La figure ATL 8 représente un diagramme polaire de la même antenne Yagi à 10 éléments.

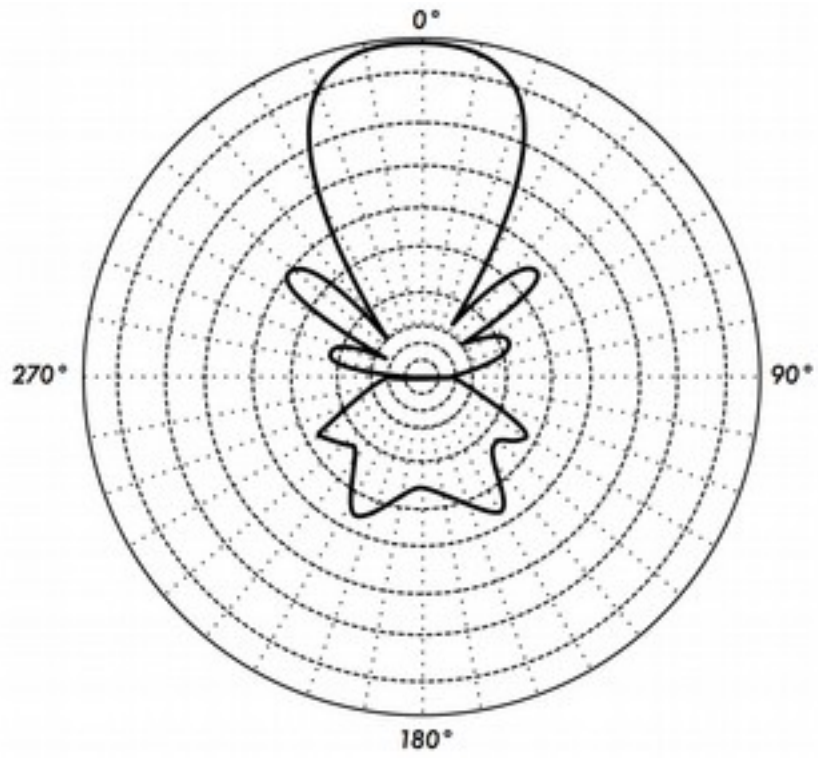


Figure ATL 8: Le diagramme de rayonnement polaire de la même antenne.

Le diagramme du champ qui existe à proximité de l'antenne est différent de celui à une certaine distance, celui qui est intéressant.
Le champ éloigné (en anglais far-field) est aussi appelé le champ de rayonnement.
Pour la mesure du diagramme de rayonnement, il est important de choisir une distance suffisamment grande.
La distance minimale permissible dépend des dimensions de l'antenne par rapport à la longueur d'onde. La formule acceptée pour cette distance est:

$$R_{min} = 2d^2/\lambda$$

où R_{min} est la distance minimale par rapport à l'antenne, d est la plus grande dimension de l'antenne, et λ est la longueur d'onde.

Largeur du lobe.

La largeur du lobe d'une antenne sous-entend généralement la largeur de lobe à demi-puissance. L'intensité de rayonnement maximale est trouvée, puis les points de chaque côté de la crête qui représentent la moitié de la puissance sont localisés. La distance angulaire entre les points demi-puissance est définie comme largeur de lobe. Comme la moitié de la puissance exprimée en décibels est de -3 dB, la moitié de la puissance de largeur de lobe est parfois désigné sous le nom de largeur de lobe 3 dB.

On considère habituellement autant les largeurs de faisceaux horizontales que verticales.

En supposant que la plupart de la puissance rayonnée n'est pas divisée en lobes latéraux, le gain directif est donc inversement proportionnel à la largeur de lobe : si la largeur du lobe diminue, le gain augmente.

Une antenne à gain très élevé peut avoir une largeur de lobe de quelques degrés et devra être pointée avec beaucoup d'attention afin de ne pas rater la cible. La largeur de lobe est définie par les points de demi-puissance et détermine à son tour la zone de couverture.

La zone de couverture fait référence à l'espace géographique ``illuminée" par l'antenne et elle est définie approximativement par l'intersection de la largeur du lobe avec la surface de la terre. Sur une station de base, il est généralement souhaitable de maximiser la zone de couverture, mais parfois il faut recourir à l'inclinaison (en anglais downtilting) de l'antenne, soit mécaniquement ou électriquement, en vue de fournir des services aux clients qui sont très proches de la station de base et donc en dessous de la largeur de lobe d'une antenne qui n'a pas été l'objet d'inclinaison (downtilting).

Cet inclinaison pourrait être atteint en inclinant l'antenne mécaniquement, mais souvent le lobe peut être dirigé en changeant la phase du signal appliqué aux différents éléments de l'antenne dans ce qui est connu comme l'inclinaison (downtilting) électriquement.

Lobes latéraux

Aucune antenne n'est capable de rayonner toute son énergie dans une direction privilégiée. Un peu de cette énergie est inévitablement rayonnée dans d'autres directions.

Ces plus petites crêtes sont dénommées lobes latéraux, généralement presentés en dB en dessous du lobe principal.

Dans la conception d'antenne, un équilibre doit être trouvé entre le gain et des lobes latéraux.

Zéro

Dans un diagramme de rayonnement d'antenne, un zéro est une zone dans laquelle la puissance effective rayonnée est au minimum. Un zéro a souvent un angle de directivité étroite par rapport à celui du lobe principal. Ainsi, le zéro est utile pour plusieurs fins, tels que la suppression de signaux d'interférences dans une direction donnée.

Polarisation

La polarisation est définie comme étant l'orientation du champ électrique d'une onde électromagnétique. La polarisation initiale d'une onde radio est déterminée par l'antenne. La plupart des antennes sont soit polarisées verticalement ou horizontalement.

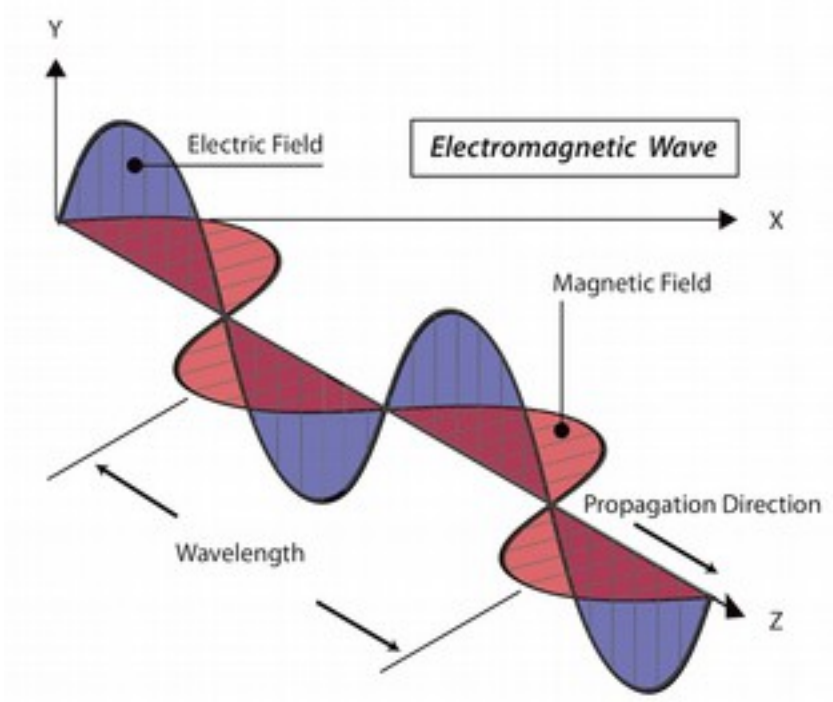


Figure ATL 9: Le champ électrique est perpendiculaire au champ magnétique, tous deux sont perpendiculaires à la direction de propagation

La polarisation de l'antenne d'émission et de réception doit correspondre, autrement une très grosse perte sera encourue.

Certains systèmes modernes profitent de polarisation pour transmettre deux signaux indépendants à la même fréquence, séparés par la polarisation. La polarisation est en général décrite par une ellipse.
La polarisation linéaire et la polarisation circulaire sont deux cas particuliers de polarisation elliptique. Avec la polarisation linéaire, le vecteur champ électrique reste dans le même plan tout le temps.
Le champ électrique peut laisser l'antenne dans une orientation verticale, une orientation horizontale, ou un certain angle entre les deux.
Le rayonnement verticalement polarisé est un peu moins affecté par des réflexions dans la voie de transmission. Les antennes omnidirectionnelles ont normalement une polarisation verticale. Les antennes horizontales sont moins susceptibles de capter des interférences causées par l'homme car celles-ci sont normalement polarisées verticalement.
En polarisation circulaire, le vecteur champ électrique semble tourner avec le mouvement circulaire autour de la direction de 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

Pour transférer la puissance maximale entre une antenne émettrice et une antenne réceptrice, les deux antennes doivent avoir la même orientation spatiale et le même sens de polarisation.
Lorsque les antennes ne sont pas alignées ou n'ont pas la même polarisation, il y aura une réduction du transfert de puissance entre elles. Cette réduction du transfert de puissance réduira l'efficacité globale du système. Lorsque les antennes émettrice et réceptrice sont toutes deux à polarisation linéaire, une déviation de l'alignement physique de l'antenne se traduira par une perte par déséquilibre de polarisation, qui peut être déterminée par la formule suivante:

$$Perte\ (dB) = 20 \log10\ (\cos \theta)$$

... où θ est la différence dans l'angle de polarisation entre les deux antennes. Pour 15°, la perte est d'environ 0,3 dB, pour 30°nous perdons 1,25 dB, pour 45°nous perdons 3 dB et pour 90°nous avons une perte infinie.
En résumé, plus le décalage de polarisation entre une antenne émettrice et réceptrice est grand, plus grande sera la perte. En pratique, un décalage de polarisation de 90°est un assez grand mais pas infini.

Certaines antennes, comme les Yagis ou les cantennas, peuvent simplement être soumises à une rotation de 90°pour assortir (correspondre) à la polarisation de l'autre extrémité de la liaison.
Vous pouvez utiliser l'effet de polarisation à votre avantage sur une liaison point-à-point.
Utilisez un outil de surveillance pour observer l'interférence de réseaux adjacents, et tourner une antenne jusqu'à ce que vous perceviez le signal le plus bas. Ensuite, activez votre liaison et orientez l'autre extrémité pour équilibrer la polarisation.
Cette technique peut parfois être utilisée pour établir des liaisons stables, même dans les environnements de radio bruyants.
Le décalage de polarisation peut être exploité pour envoyer deux signaux différents sur la même fréquence dans le même temps, permettant ainsi de doubler le débit de la liaison sans fil.
Des antennes spéciales qui a alimentation duales peuvent être utilisées à cette fin. Elles ont deux connecteurs RF qui se fixent sur deux radios indépendantes. Le vrai le débit est un peu inférieur au double du débit d'une antenne unique en raison de l'interférence inévitable de polarisation croisée.

Rapport avant-arrière

Il est souvent utile de comparer le rapport avant- arrière des antennes directionnelles.
C'est le rapport entre la directivité maximale d'une antenne et sa directivité dans la direction opposée.
Par exemple, lorsque le diagramme 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 de rayonnement à 180 degrés. Ce nombre n'a aucune importance pour une antenne omnidirectionnelle, mais il est tout à fait pertinente lors de la construction d'un système avec répétiteurs, dans lequel le signal envoyé en arrière va interférer avec le signal utile et doit être minimisé.

Ouverture d'antenne.

L'"ouverture" électrique d'une antenne réceptrice est définie par la section croisée d'une antenne parabolique qui fournirait la même puissance à une charge adaptée. Il est facile de voir que la grille parabolique a une ouverture très similaire à un paraboloïde solide.
L'ouverture d'une antenne est proportionnelle à son gain.
Par réciprocité, l'ouverture est la même pour l'antenne émettrice.

Notez que le concept d'ouverture n'est pas facilement visualisable dans le cas d'une antenne filaire dans laquelle l'espace physique est négligeable.

Dans ce cas, l'ouverture de **l'antenne doit être déduite de la formule du gain.**

Types d'antennes

Une classification d'antennes peut être basée sur :

La fréquence et la taille.
Antennes utilisées pour le HF sont différentes des antennes utilisées pour le VHF, qui sont à leur tour différentes des antennes utilisées pour les micro-ondes.
Puisque la longueur d'onde varie avec la fréquence, les antennes doivent avoir différentes tailles pour pouvoir émettre des signaux à la longueur d'onde correcte.
Nous sommes particulièrement intéressés par les antennes fonctionnant dans la gamme des micro-ondes, particulièrement dans les fréquences de 2,4 GHz et 5 GHz. À 2,4 GHz, la longueur d'onde est de 12,5 cm, alors qu'à 5 GHz elle est de 6 cm.

Directivité.
Les antennes peuvent être omnidirectionnelles, sectorielle ou directive. Les antennes omnidirectionnelles rayonnent à peu près le même signal tout autour de l'antenne dans un angle de 360°.
Les types d'antennes omnidirectionnelles les plus populaires sont le dipôle et les antennes à base planaire (en anglais 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 ou directives** sont des antennes dont la largeur du faisceau est beaucoup plus étroite que celle des antennes sectorielles. Elles ont le gain le plus élevé et sont donc utilisées pour les liaisons longues distances.
Les types d'antennes directives comprennent les antennes Yagi, le biquadratique, l'antenne cornet, l'antenne hélicoïdal, l'antenne patch, l'antenne parabolique, et bien d'autres.

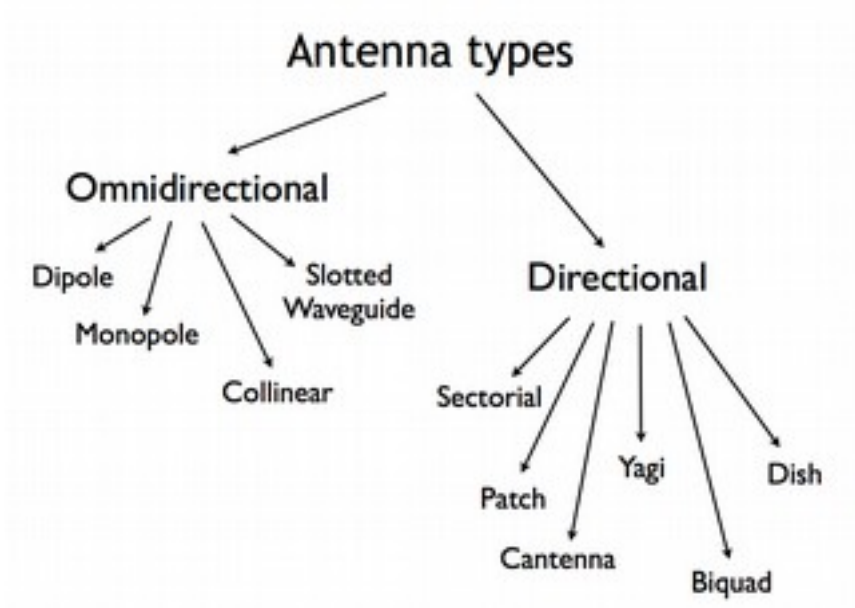


Figure ATL 10: Types d'antennes.

Construction physique.
Les antennes peuvent être construites de plusieurs façons différentes, allant des fils simples aux antennes paraboliques en passant par des boites de conserve.
Lorsque nous considérons des antennes qui sont appropriées pour l'utilisation WLAN à 2.4 GHz, une autre classification peut être utilisée :

Application.
Les points d'accès ont tendance à produire des réseaux point-à- multipoint, tandis que les liaisons à distance ou les dorsales sont point-à-point. Chacun de ces types de réseaux suggère l'utilisation de différents types d'antennes.
Les nœuds qui sont utilisés pour l'accès multipoint utiliseront probablement des antennes omnidirectionnelles qui rayonnent dans toutes les directions, ou plusieurs antennes sectorielles, chacune focalisant dans un petit secteur.
Dans le cas du point-à-multipoint, les antennes sont utilisées pour relier deux locations simples.

Les antennes directives sont le meilleur choix pour ce type d'applications.

Nous allons vous présenter une liste brève d'antennes courantes pour la fréquence 2,4 GHz ainsi qu'une brève description et des informations de base sur leurs caractéristiques.

Antenne à base plane d'un quart de longueur d'onde.

L'antenne à base plane d'un quart de longueur d'onde est de conception très simple et est utile lorsque la taille, le coût et la facilité de construction sont importants. Cette antenne est conçue pour transmettre un signal polarisé verticalement. Elle consiste en un élément actif d'un quart de longueur d'onde et trois ou quatre éléments de surface d'un quart de longueur d'onde courbés de 30 à 45 degrés vers le bas. Cet ensemble d'éléments, appelés radiaux, est connue comme une base plane (en anglais ground plane).

Figure ATL 11 : Antenne à base plane d'un quart de longueur d'onde.

C'est une antenne simple et effective qui peut capturer un signal provenant de toutes les directions de façon égale. Le gain de cette antenne est de l'ordre de 2 à 4 dBi.

Antenne Yagi- Uda

Une antenne Yagi de base ou plus correctement une antenne Yagi-Uda se compose d'un certain nombre d'éléments droits/rectilignes, chacun mesurant environ la moitié d'une longueur d'onde. L'élément conduit ou actif d'une antenne Yagi est l'équivalent d'une antenne dipôle demi-onde à alimentation centrale.

Parallèlement à l'élément actif, et aux environs de 0,2 à 0,5 fois la longueur d'onde de part et d'autre de celle-ci se trouvent des tiges ou fils droits appelés réflecteurs et directeurs, ou simplement des éléments passifs. Un réflecteur est placé derrière l'élément actif et est légèrement plus long que la moitié d'une longueur d'onde. Les directeurs sont placés devant l'élément actif et sont légèrement plus courts que la moitié de la longueur d'onde. Une antenne Yagi typique a un réflecteur et un ou plusieurs directeurs. L'antenne Yagi propage l'énergie du champ électromagnétique dans la direction allant de l'élément actif vers les éléments directeurs et est plus sensible à l'énergie du champ électromagnétique dans cette même direction. Le plus d'éléments directeurs a une antenne Yagi, plus sera son gain.
Voici la photo d'une antenne Yagi avec 5 directeurs et un réflecteur. Les antennes Yagi sont souvent mises dans une boite radôme cylindrique pour la protection contre les intempéries.

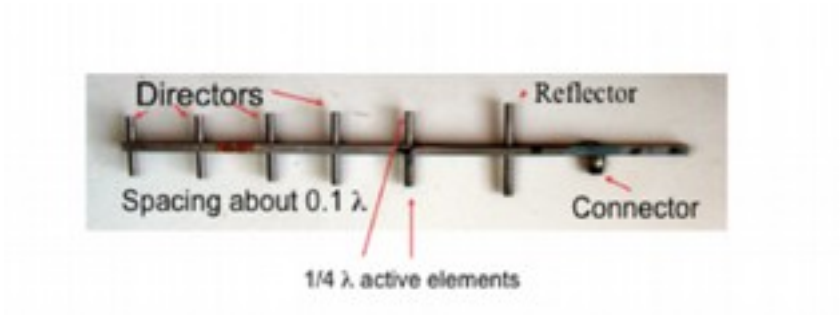


Figure ATL 12: Yagi- Uda

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

Antenne cornet

L'antenne cornet tire son nom de son apparence caractéristique évasée en forme de cornet. La partie évasée peut être de forme carrée, rectangulaire, cylindrique ou conique. La direction du rayonnement maximum correspond à l'axe du cornet. Elle est facilement alimentée par un guide d'onde, mais elle peut être alimentée par un câble coaxial et une transition appropriée. Alors qu'il est fastidieux de construire de vous-même à la maison une antenne cornet, une boîte de conserve cylindrique de dimensions appropriées aura des caractéristiques similaires.

Figure ATL 13: Alimentation cornet faite à partir d'une boîte de conserve.

Les antennes cornets sont couramment utilisées comme élément actif dans une antenne parabolique. Le cornet est dirigé vers le centre du réflecteur.

L'utilisation d'un cornet au point focal de la parabole plutôt qu'une antenne dipôle ou tout autre type d'antenne, minimise la perte de l'énergie aux extrémités du réflecteur de l'antenne parabolique. A 2.4 GHz, une antenne cornet simple faite avec une boîte de conserve a un gain de l'ordre de 10 dBi.

Antenne parabolique

Les antennes basées sur des réflecteurs paraboliques sont le type le plus commun d'antennes directives quand un gain élevé est nécessaire. L'avantage principal est qu'elles peuvent être construites pour avoir le gain et la directivité aussi grands que nécessaire.
L'inconvénient principal est que les grandes paraboles sont difficiles à installer et sont susceptibles d'avoir une grande charge de vent. Des randomes peuvent être utilisés pour réduire la charge de vent ou la dérive, ainsi que pour la protection contre le vent.

Figure ATL 14: Une antenne parabolique solide.

Des antennes paraboliques allant jusqu'à un mètre sont généralement faits de matériaux solides. L'aluminium est fréquemment utilisé pour l'avantage qu'il confère par rapport à son poids, sa durabilité et ses bonnes caractéristiques électriques.
La dérive s'accroit rapidement avec la taille de la parabole et peut rapidement devenir un grave problème. Les antennes paraboliques qui ont une surface réfléchissante à maillage ouvert sont fréquemment utilisées.
Celles-ci ont un rapport avant-arrière moins bon, mais sont plus sûrs et plus faciles à construire.
Le cuivre, l'aluminium, le laiton, l'acier galvanisé et l'acier sont des matériaux convenables pour le maillage.

Antenne biQuad
L'antenne biQuad est simple à construire et offre une bonne directivité et un bon gain pour les communications point- à-point. Elle consiste en deux carrés de la même taille d'un quart de longueur d'onde comme éléments rayonnants et d'une plaque ou une grille métallique comme réflecteur. Cette antenne a une largeur de faisceau d'environ 70 degrés et un gain de l'ordre de 10 à 12 dBi. Elle peut être utilisée comme antenne autonome ou comme alimentation pour une antenne parabolique. La polarisation est telle qu'en regardant l'antenne à partir de l'avant, si les carrés sont placés côte à côte, la polarisation est verticale.

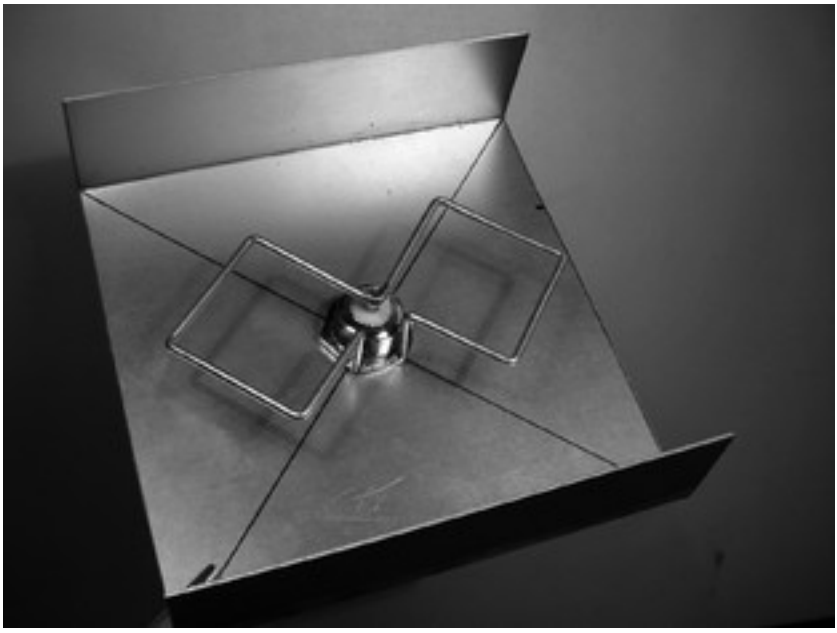


Figure ATL 15: Une antenne biQuad.

Antennes à log périodiques (an anglais Log Periodic Antennas)
Les antennes à log périodiques ont un gain modéré sur une bande de fréquence large. Elles sont souvent utilisées dans des analyseurs de spectre pour des fins de test et sont également populaires comme antennes de réception télévisée, car elles peuvent couvrir du canal 2 au canal 14. Ces antennes sont utilisées dans les périphériques d'espaces blancs qui nécessitent la capacité de travailler dans les canaux largement différents.

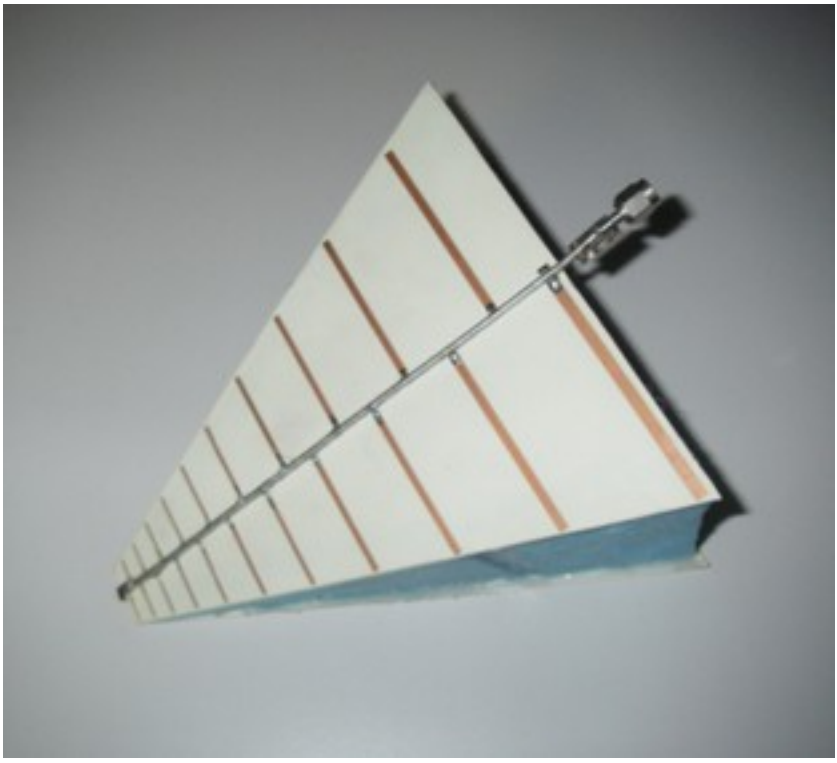


Figure ATL 16: Antenne à log périodique.

D'autres antennes.
Il existe plusieurs autres types d'antennes et de nouvelles sont créées suite aux progrès technologiques.

Antennes de secteur ou sectorielles : Elles sont largement utilisées dans l'infrastructure de téléphonie cellulaire et sont généralement construites en ajoutant une plaque réfléchissante 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, tandis que la verticale est généralement beaucoup étroite. Des antennes composites 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 allant jusqu'à 23 dBi

Théorie de réflexion

La propriété de base d'un réflecteur parabolique parfait est qu'il convertit une onde sphérique irradiant à partir d'une source ponctuelle placée au foyer en une onde plane. Inversement, toute l'énergie reçue par l'antenne parabolique à partir d'une source distante est réfléchie en un seul point au foyer de la parabole. La position du foyer ou longueur focale est donnée par:

$$f = D^2/16c$$

... où D est le diamètre de la parabole et c est la profondeur de la parabole en son centre. La taille de la parabole est le facteur le plus important, car elle détermine le gain maximal qui peut être atteint à une fréquence donnée et la largeur de faisceau résultante. Le gain et la largeur de faisceau obtenu sont données par:

$$Gain = ((3{,}14\ D)^2/\lambda^2\ )\ n$$

$$Largeur\ de\ faisceau = 70\ \lambda\ /\ D$$

... où D est le diamètre de la parabole et n est l'efficacité.

L'efficacité est déterminée principalement par l'efficacité de l'illumination de l'antenne par la source, mais aussi par d'autres facteurs. Chaque fois que le diamètre d'une parabole double, le gain est quadruplé soit 6 dB de plus.
Si les deux stations communicantes doublent la taille de leurs paraboles, la force du signal peut être augmentée de 12 dB, un gain très substantiel.
Une efficacité de 50% peut être obtenue lorsque l'antenne est faite à la main. Le rapport F/D (longueur focale/diamètre de la parabole) est le facteur fondamental qui régit la conception de l'alimentation d'une antenne.
Ce rapport est directement lié à la largeur de faisceau de l'alimentation nécessaire pour illuminer l'antenne efficacement. Deux antennes de même diamètre mais de longueurs focales différentes exigent une conception différente de l'alimentation si nous voulons que les deux soient illuminées efficacement. La valeur de 0,25 correspond à une antenne parabolique commune à plan focal où le foyer se trouve dans le même plan que le bord de la parabole. L'illumination optimale d'une antenne parabolique est un compromis entre la maximisation du gain et la minimisation des lobes latéraux.

Amplificateurs

Comme mentionné précédemment, les antennes ne créent réellement pas de puissance. Elles dirigent tout simplement toute puissance disponible dans une configuration particulière.
Un amplificateur de puissance vous permet d'utiliser la puissance DC pour augmenter votre signal disponible. Un amplificateur relie l'émetteur radio et l'antenne et possède un câble supplémentaire qui se connecte à une source d'alimentation. Il y a des amplificateurs disponibles qui fonctionnent à 2,4 GHz qui peuvent ajouter plusieurs watts de puissance à votre transmission.
Ces appareils détectent quand une radio est en train de transmettre et quand cela se produit, ils s'allument et amplifient le signal. Ils s'éteignent ensuite de nouveau lorsque la transmission se termine.
Lors de la réception, ils ajoutent également une amplification au signal avant de l'envoyer à la radio. Malheureusement, une addition simple des amplificateurs ne va pas magiquement résoudre tous vos problèmes réseau.
Nous n'allons pas discuter des amplificateurs en détail dans ce livre, car leur utilisation soulève un certain nombre d'inconvénients signifiants:

- • **Ils sont coûteux**. Les amplificateurs doivent fonctionner à des largeurs de bande relativement grandes à 2,4 GHz, et doivent commuter assez rapidement pour fonctionner avec les applications Wi –Fi.
- • **Ils ne fournissent aucune directivité supplémentaire**. Les antennes à gain élevé non seulement améliorent la quantité disponible de signal mais ont aussi tendent à rejeter le bruit provenant d'autres directions. Les amplificateurs amplifient aveuglément non seulement les signaux désirés mais aussi les signaux parasites, et peuvent ainsi empirer les problèmes d'interférence.
- • **Les amplificateurs génèrent du bruit pour les autres utilisateurs de la bande.** En augmentant votre puissance de sortie, vous créez une grande source de bruit pour les autres utilisateurs de la bande sans licence. En revanche, l'ajout de gain d'antenne permettra d'améliorer votre liaison et cela peut réellement diminuer le niveau de bruit pour vos voisins.
- • **L'utilisation des amplificateurs est souvent illégale.** Chaque pays impose des limites de puissance sur l'utilisation du spectre sans licence.

- L'ajout d'une antenne à un signal hautement amplifié est susceptible de causer un dépassement des limites légales sur la liaison. Les antennes coûtent beaucoup moins que les amplificateurs, et peuvent améliorer une liaison en changeant simplement l'antenne à une extrémité. L'utilisation des radios les plus sensibles et des câbles de bonne qualité contribue également sur les liaisons sans fil à longue distance de façon significative.

Ces techniques ne sont pas susceptibles de causer des problèmes pour les autres usagers de la bande. Ainsi, nous recommandons leur utilisation avant d'ajouter des amplificateurs. Des nombreux fabricants offrent des versions haute puissance de leurs radios WiFi à la fois aux fréquences de 2 et s et 5 GHz, avec des amplificateurs intégrés. Ceci est mieux que les amplificateurs externes, mais ne présumez pas qu'il est toujours intelligent d'utiliser la version haute puissance car pour de nombreuses applications, le couplage de la puissance standard à une antenne à gain élevé est en fait mieux.

Conceptions d'antennes pratiques

Le coût des antennes à 2.4 GHz a considérablement chuté avec l'augmentation de la popularité du WiFi.Des conceptions innovatrices utilisent des pièces plus simples et moins de matériaux pour réaliser un gain impressionnant avec relativement peu d'usinage. Malheureusement, la disponibilité des bonnes antennes est encore limitée dans certaines régions du monde, et leur importation peut être coûteuse. Alors que la conception d'une antenne peut être un processus complexe et une source d'erreurs, la construction d'antennes à partir de composants disponibles localement est très simple, et peut être très amusant. Dans l'annexe A sur la construction de l'antenne, nous présentons certaines conceptions pratiques d'antennes qui peuvent être construites pour très peu d'argent.

Mesures d'antennes

Les instruments d'antennes de précision nécessitent des instruments et des installations coûteux Il est donc conseillé d'obtenir les valeurs de paramètres de l'antenne directement à partir d'un fabricant de renom. Une chambre non-résonante (en anglais anechoic) est nécessaire pour effectuer des mesures d'antenne précises, autrement les réflexions vont provoquer des mesures fausses. La glace affecte la performance de toutes les antennes dans une certaine mesure et le problème devient plus grave à des fréquences plus élevées. L'impédance dans l'espace libre est de 377 ohms.

Si l'air entourant immédiatement les éléments dipolaires est remplacé par de la glace qui a une impédance inférieure à l'air, alors la correspondance de l'impédance et les diagrammes de rayonnement de l'antenne vont changer. Ces changements s'empirent progressivement à mesure que la charge de la glace augmente. Les éléments d'antenne sont généralement enfermés dans un boîtier de protection en plastique (radôme). Ceci permet d'obtenir un espace d'air entre les éléments du boîtier et la glace de sorte que l'impédance inférieure de la couche de glace a seulement un petit effet sur les radiateurs. Le désaccord est fortement réduit mais la déformation du diagramme de rayonnement peut encore se produire (le désaccord réduit la largeur de bande passante utilisable de l'antenne). Pour une épaisseur de glace donnée, la déviation par rapport aux valeurs de rendement nominal s'empire avec l'augmentation de la fréquence. Dans les zones où le givrage sévère et une neige mouillée sont communs, il est prudent d'installer un radôme complet sur les antennes paraboliques solides, utiliser des antennes panneaux au lieu de réflecteurs cornet, et rester loin des grilles paraboliques.

Figure ATL 17: L'effet de la glace sur une antenne grille parabolique

RÉSEAUTAGE

6. RÉSEAUTAGE

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 à 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 vous connecter à un site distant au cœur de votre campus ? Est-il probable que votre réseau va croître en vue d'inclure plusieurs sites distants? Est que la plupart des composantes réseau seront installées dans des endroits fixes ou votre réseau croîtra-il jusqu'à inclure des centaines d'ordinateurs portables et d'autres périphériques?
Dans ce chapitre, nous passerons en revue les concepts réseaux définissant le protocole TCP/IP qui constitue la famille principale des protocoles actuellement utilisés sur l'Internet. Ensuite, nous allons examiner les options matérielles qui sont susceptibles de former la couche physique sous-jacente à votre réseau TCP/IP. Finalement nous examinerons quelques exemples de configurations sans fil. Ceci vous fournira une très bonne préparation au chapitre intitulé planification du déploiement présenté plus loin dans ce livre. Le TCP/IP fait référence à la suite de protocoles qui rendent possible les communications sur le réseau Internet. La compréhension du TCP/IP vous permettra de construire des réseaux de virtuellement n'importe quelle taille et ultimement faire partie intégrante du réseau Internet. Cette édition du livre comprend maintenant une introduction à l'IPv6 qui est le nouveau système d'adressage de l'Internet. Comme il est très probable que vous déploierez des réseaux utilisant l'IPv6, il est fortement recommandé de vous familiariser avec la façon dont cela fonctionne et comment l'IPv6 peut coexister avec les anciens réseaux IPv4 qui continueront à exister sur l'Internet pendant encore un certain temps.

Introduction

Venise en Italie est une ville fantastique pour s'y perdre. Les routes ne sont que des sentiers pédestres qui traversent l'eau dans 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. Ils sont spécialisés dans la livraison dans seulement un ou deux des six districts (en Italien sestieri) de Venise.
Cela est nécessaire en raison du complexe agencement de cette ville antique.

Beaucoup de gens 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. Imaginez un touriste qui arrive à trouver le masque en papier mâché comme un souvenir et veut l'avoir livré du studio à San Polo dans Venise à son bureau à Londres au Royaume-Uni.
Cela peut paraitre une tâche ordinaire (ou même triviale), mais regardons ce qui se passe réellement.

Figure NG 1: Un autre type de masque réseau.

L'artiste emballe d'abord le masque dans une boîte d'expédition avec l'adresse de sa maison. Ensuite, il le remet à un employé postal qui y attache certains formulaires officiels et l'envoie à un poste central de traitement de colis pour les destinations internationales. Après plusieurs jours, le colis passe la douane italienne et est embarqué sur un vol à destination du Royaume-Uni et arrive dans un dépôt central de traitement des importations à l'aéroport de Heathrow.

Une fois passé la douane, le colis est envoyé à un point de distribution dans la ville de Londres, puis au centre de traitement postal local du district de Camden où vit le touriste. Finalement, le colis est acheminé par camionnette de livraison pour l'amener à la bonne maison sur la bonne rue dans Camden. Un membre de la famille accepte et signe pour le paquet de la livraison reçu du chauffeur de la camionnette, et ensuite le laisse dans le studio du touriste qui un peu plus tard le déballe dans la joie. L'agent du bureau de triage de Camden ne connaît ni ne se soucie de la façon d'arriver dans le district/sestiere de San Polo de Venise. Son travail consiste simplement à accepter les paquets à leur arrivée et les livrer à la bonne personne dans Camden.

Similairement, l'employé des postes à Venise n'a pas besoin de s'inquiéter sur la façon de se rendre à la bonne adresse dans Londres. Son travail consiste à accepter des paquets de son quartier et les transmettre au plus proche centre suivant dans la chaîne de livraison. Ceci est très similaire à la façon dont le routage Internet fonctionne.

Un message est subdivisé dans de nombreux paquets individuels qui sont étiquetés avec leur source et destination. Ensuite, l'ordinateur envoie ces paquets à un routeur qui décide où les envoyer dans la suite. Le routeur a besoin de garder seulement une trace d'une poignée de routes (par exemple, comment arriver au réseau local, la meilleure route à quelques autres réseaux locaux et une route vers une passerelle vers le reste de l'Internet). Cette liste de routes possibles est appelée la table de routage. Lorsque les paquets arrivent au routeur, l'adresse de destination est examinée et comparée à sa table de routage interne.

Si le routeur n'a pas de route explicite vers la destination en question, il envoie le paquet à l'adresse correspondance la plus proche qu'il peut trouver, qui est souvent sa propre passerelle Internet (par la route par défaut). Et le routeur suivant fait la même chose et cela se répète jusqu'à ce que le paquet arrive finalement à sa destination. Les colis peuvent trouver leur chemin à travers le système postal international seulement parce que nous avons mis en place un système normalisé d'adressage des colis.

Par exemple, l'adresse de destination doit être écrite lisiblement sur le devant de l'emballage, et comprend tous les renseignements essentiels (comme le nom du destinataire, l'adresse de la rue, la ville, le pays, le code postal).

Sans cette information, les colis sont soit retournés à l'expéditeur ou sont perdus dans le système.

Les paquets peuvent circuler à travers le réseau Internet mondial parce que nous nous sommes convenus sur un schéma commun d'adressage et un protocole pour la transmission des paquets.
Les protocoles de communication standard rendent possible l'échange des informations à l'échelle globale.

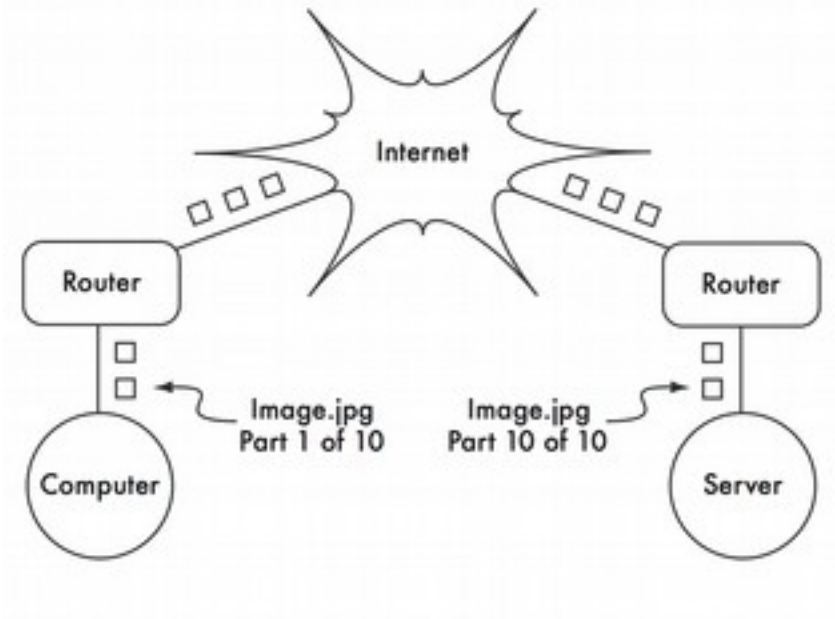


Figure NG 2 : Réseautage Internet. Les paquets sont transmis entre les routeurs jusqu'à ce qu'ils atteignent leur destination finale.

Communications coopératives.

Une communication n'est possible que lorsque les participants parlent un langage commun. 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 une salle peuvent parler anglais, mais sans la mise en place d'un ensemble de règles pour déterminer qui a le droit d'utiliser le microphone, la communication des idées d'un individu à l'ensemble de la salle est presque impossible.

Maintenant, imaginez un auditorium aussi grand que le monde, plein de tous les ordinateurs qui existent.
Sans un ensemble commun de protocoles réglementant quand et comment chaque ordinateur peut communiquer, l'Internet deviendrait un désordre chaotique où toutes les machines tenteraient de communiquer en même temps. Un certain nombre de modèles de communication ont été développés pour résoudre ce problème. Le plus connu d'entre eux est le modèle OSI.

Le modèle OSI

La norme internationale pour l'interconnexion des systèmes ouverts (en anglais Open Systems Interconnection ou en abrégé OSI) est définie par le document ISO/IEC 7498-1, tel que décrit par l' Organisation internationale de normalisation et la Commission électrotechnique internationale. La norme complète est disponible comme publication ``ISO/IEC 7498-1:1994" disponible
sur http://standards.iso.org/ittf/PubliclyAvailableStandards/.
Le modèle OSI divise le trafic du 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 en dessous d'elle, tout en offrant de nouveaux services à la couche au-dessus d'elle. L'abstraction entre les couches rend facile la conception des piles de protocoles élaborés et très fiables, telles que l'omniprésent TCP/IP. Une pile de protocoles est une implémentation effective d'un modèle de communication en couches. Le modèle OSI ne définit pas les protocoles qui seront utilisés dans un réseau particulier, mais simplement délègue chaque tâche de communication à une seule couche dans une hiérarchie bien définie.
Bien que la spécification ISO/IEC 7498-1 explique comment les couches doivent interagir les unes avec les autres, elle laisse les détails réels d'implémentation au fabricant. Chaque couche peut être implémentée en matériel (plus fréquent pour les couches inférieures) ou en logiciel. Tant que l'interface entre les couches adhère à la norme, les développeurs sont libres d'utiliser tous les moyens disponibles pour construire leur pile de protocole.
Cela signifie que toute couche donnée du fabricant A peut fonctionner avec la même couche du constructeur B (en supposant que les spécifications pertinentes sont implémentées et interprétées correctement).

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

Couche	Nom	Description
7	Application	La **couche application** est la couche à laquelle la plupart des utilisateurs du réseau sont exposés. C'est le niveau où la communication humaine passe. HTTP, FTP et SMTP sont tous des protocoles de la couche 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 HTML et MIME, la compression de données, les contrôles de mise en forme, l'ordre des octets, etc.
5	Session	La **couche session** gère la session de communication logique entre les applications. RPC est un exemple d'une cinquième couche de protocole.
4	Transport	La **couche transport** fournit une méthode pour parvenir à atteindre un service particulier sur un nœud de réseau donné. TCP, UDP et SCTP sont des exemples de protocoles qui fonctionnent à cette couche. Certains protocoles de couche transport (tels que TCP) garantissent que toutes les données arrivent à destination, et sont rassemblées et est 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. Il ne vérifie pas l'arrivée de paquets de données.
3	Réseau	IP (le protocole Internet) est le protocole de couche réseau le plus commun. C'est la couche où le routage se produit. Les paquets peuvent quitter le réseau liaison locale et être retransmis sur d'autres réseaux. Les routeurs implémentent cette fonction sur un réseau en ayant au moins deux interfaces de réseau ; une sur chacun des réseaux à interconnecter. Les nœuds sur Internet sont accessibles par leur adresse globale IP unique. ICMP est un autre protocole réseau critique. C'est un protocole spécial qui fournit divers messages de gestion nécessaires au bon fonctionnement du protocole IP. Cette couche est également parfois appelée la couche Internet.
2	Liaison	Lorsque deux ou plusieurs nœuds partagent le même support physique (par exemple, plusieurs ordinateurs connectés à un concentrateur (en anglais hub) ou une salle pleine de dispositifs sans fil en utilisant le même canal radio) ils utilisent la **couche liaison** des données pour communiquer. Des exemples courants de protocoles de liaison de données sont Ethernet, Token Ring, ATM, et les protocoles de réseau sans fil (IEEE 802.11a/b/g). La communication sur cette couche est dite liaison locale, car tous les nœuds connectés à cette couche communiquent directement entre eux. Cette couche est parfois connue comme la couche **Media Access Control (MAC)**. Sur les réseaux Ethernet, les nœuds sont référencés par leur adresse MAC. Il s'agit d'un nombre unique de 48 bits attribué à chaque périphérique réseau quand il est fabriqué.
1	Physique	La **couche physique** est la couche la plus basse du modèle OSI, et se réfère au support physique réel où les communications ont lieu. Il peut s'agir d'un câble CAT5 de cuivre, d'un faisceau de fibres optiques, des ondes hertziennes, ou n'importe quel autre moyen capable de transmettre des signaux. Les câbles coupés, la fibre cassée, et les interférences RF sont tous des problèmes de la couche physique.

Les couches de ce modèle sont numérotés de un à sept, avec sept étant au sommet. Ceci vise à renforcer l'idée que chaque couche s'appuie 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 successives et le toit à la couche sept. 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 sens. Toutes les trois premières couches (physique, liaison de données et réseau) sont visibles ``sur le réseau". C'est-à-dire que l'activité de ces couches est déterminée par la configuration des câbles, les commutateurs, les routeurs, et des dispositifs similaires. Un commutateur réseau ne peut distribuer des paquets qu'en utilisant des adresses MAC. Ainsi il a besoin d'implémenter seulement les couches un et deux. Un simple routeur ne peut acheminer les paquets qu'en utilisant seulement leur adresse IP. Il a donc besoin d'implémenter uniquement les couches un à trois. Un serveur web ou un ordinateur portable exécutent des applications. Ainsi Il doit implémenter toutes les 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 l'information de plus haut niveau dans 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 définitif et complet. Il fournit un cadre qui peut être utilisé par les fabricants et les gens qui implémentent des protocoles réseau pour construire des dispositifs réseaux pouvant interagir dans n'importe quelle partie du monde. Du point de vue d'un ingénieur réseau ou un testeur, le modèle OSI peut sembler inutilement complexe. En particulier, les gens qui construisent et maintiennent des réseaux TCP/IP ont rarement besoin de faire face à des problèmes au niveau des couches de session ou de présentation. Pour la majorité des implémentations réseau Internet, le modèle OSI peut être simplifié en une petite collection de cinq couches.

Le modèle TCP/IP

Contrairement au 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 des réseaux Internet. La grande majorité de l'Internet utilise le protocole TCP/IP. Ainsi nous pouvons faire des hypothèses sur les réseaux qui les rendent plus faciles à comprendre.

Le modèle de réseautage TCP/IP décrit les cinq couches suivantes:

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

En termes de 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 interopérables entre la quasi-totalité des fabricants de matériel, et la couche quatre fonctionne entre tous les hôtes utilisant le protocole 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. Dans ce livre, nous allons utiliser le modèle TCP/IP lors de l'examen des réseaux. Le modèle TCP / IP peut être comparé à une personne livrant une lettre à une édifice de bureaux au centre-ville. La personne devra tout d'abord interagir avec la rue (la couche physique), faire attention au trafic sur cette route (la couche liaison de données), tourner à la jonction appropriée pour rejoindre une autre route et arriver à la bonne adresse (la couche Internet), aller à l' étage correcte et le numéro de chambre appropriées (la couche transport) et finalement lui remettre la lettre ou à un réceptionniste qui la lui remettra (la couche application). Une fois qu'ils ont transmis le message au réceptionniste, le porteur du message est libre d'aller sur son chemin. Les cinq couches peuvent être facilement mémorisées en utilisant le mnémonique anglais ``Please Don't Look In the Attic", qui bien sûr signifie ``physique/liaison de données/ Internet /Transport /Application.".

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 se réfère à toute une famille de protocoles de communication connexes. TCP/IP est également appelé suite de protocoles Internet, et il opère sur les couches trois et quatre du modèle TCP/IP. Dans cette discussion, nous allons nous concentrer sur la version six du protocole IP (IPv6) car depuis 2012, c'est la version à déployer en parallèle avec la version quatre précédente (IPv4). En 2012, environ la moitié du contenu de l'Internet est disponible avec une meilleure expérience utilisateur en utilisant Ipv6. La version précédente est aussi décrite dans ce chapitre parce que un certain contenu ancien et certaines anciennes applications (Skype en 2012) exigent encore l'IPv4. Et en effet, des nombreux réseaux auxquels vous pourriez avoir à vous connecter auront encore la vielle technologie IPv4 déployée pour encore quelques années à venir.
Outre la longueur de l'adresse, IPv4 et IPv6 sont très similaires: ce sont des protocoles de réseau sans fil opérant sur la même couche de liaison de données (WiFi, Ethernet ...) et qui desservent les mêmes protocoles de transport (TCP, SCTP, UDP ...). Dans ce livre, quand IP est décrit sans version, cela signifie qu'il s'applique aux deux versions. Un réseau à double pile est un réseau qui opère IPv6 et IPv4 à la fois et en même temps. Il est prévu que les réseaux doubles seront la norme au moins jusqu'en 2020 quand l'unique-IPv6 deviendra la norme.

Adressage IPv6

L'adresse IPv6 est un nombre de 128 bits, habituellement exprimé en plusieurs nombres hexadécimaux. Afin de rendre cette adresse lisible, elle est écrite en portions de 32 bits ou 4 chiffres hexadécimaux séparés par deux points ``:". Le nombre hexadécimal devrait être écrit en minuscules, mais peut aussi être écrit en majuscules.

Un exemple d'une adresse IPv6 est:
2001:0db8:1234:babe:0000:0000:0000:0001
Cette adresse correspond à :

2001	0db8	1234	babe	0	0	0	1

Comme ces adresses sont assez longues, il est courant de supprimer le 0 initial dans chaque portion, de sorte que la même adresse peut aussi s'écrire:

2001:db8:1234:babe:0:0:0:1

Cette adresse peut encore être simplifiée en regroupant un bloc de portions consécutifs de `0' dans la forme abrégée ``::''. La même adresse devient alors :

2001: dbB8 : 1234: babe::1

Il existe quelques adresses IPv6 spécifiques:

- :: 1 (ou 0000:00000:0000:0000:0000:0000:0000:0001) représente l'adresse de bouclage destinée a être utilisée par un nœud lorsque le nœud veut s'envoyer des paquets à lui-même;
- :: (tous zéro) est l'adresse non spécifiée destinée à être utilisée par un nœud quand il ne connaît pas son adresse globale, par exemple à son démarrage.

Les préfixes IPv6

Les nœuds IPv6 sur la même liaison ou le même réseau partage le même préfixe IPv6, qui est défini comme étant la partie la plus significative de l'adresse IPv6.
La longueur du préfixe est généralement de 64 bits sur un réseau local.
Ainsi, notre adresse habituelle de 2001:dbB8:babe::1 peut être écrite comme 2001:db8:1234:babe::1/64 (la longueur du préfixe est ajoutée à la fin de l'adresse après un ``/'').
La définition de la longueur du préfixe sur une adresse divise effectivement l'adresse en deux parties: le préfixe lui-même et l'identifiant d'interface (an anglais Interface identifier IID).

2001	db8	1234	babe	0	0	0	0
Préfixe				Identifiant d'interface			

Sur un réseau LAN ou WLAN, la longueur du préfixe doit être 64 bits sinon certains protocoles ne fonctionneront pas correctement.
Tous les nœuds sur le même réseau LAN ou WLAN partagent habituellement le même préfixe mais leur identifiant d'interface doit être unique pour éviter toute confusion. L'analogie avec une adresse postale dans les grandes villes, c'est que le préfixe est le nom de la rue et l'identifiant d'interface est le numéro de la maison. La longueur de préfixe peut être différente sur les liaisons qui n'appartiennent ni au réseau LAN ou au réseau WLAN.

Le réseau lui-même est identifié par le préfixe sans aucun identifiant d'interface mais avec la longueur de préfixe comme par exemple: 2001: db8:1234:babe::/64

Adressage IPv4

Dans un réseau IPv4, l'adresse est un nombre de 32 bits normalement décrit par quatre nombres de 8 bits 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 IPv4. Si vous auriez énuméré toutes les adresses IPv4 possible, elles vont de 0.0.0.0 à 255.255.255.255. Cela donne un total de plus de quatre milliards d'adresses IPv4 possibles (255 x 255 x 255 x 255 = 4228250625), bien que beaucoup d'entre elles sont réservées à des fins particulières et ne devraient pas être attribuées aux ordinateurs hôtes.
Quelques adresses IPv4 spéciales incluent:

- 127.0.0.1 représente l'adresse de bouclage (similaire à :: 1 pour l'IPv6) ;
- 0.0.0.0 représente l'adresse non spécifiée (similaire à :: pour IPv6).

Sous-réseaux IPv4

En appliquant un masque de sous-réseau (également appelé un masque réseau, ou tout simplement le netmask en anglais ou même préfixe) à une adresse IPv4, vous pouvez définir logiquement à la fois un ordinateur 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 IPv4. Par exemple, 255.255.255.0 est un masque réseau commun. Vous trouverez cette notation utilisée lors de la configuration des interfaces réseau, la création de 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 Classeless Inter-Domain Routing et est défini dans le document RFC1518. Un masque de sous-réseau détermine la taille d'un réseau donné. L'utilisation d'un masque /24 signifie que 8 bits sont réservés pour les ordinateurs hôtes (32 bits au total - 24 bits de masque = 8 bits pour les ordinateurs hôtes). Ceci conduit à un maximum de 256 adresses d'ordinateurs hôtes possibles (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).
Cela laisse 254 adresses disponibles pour les ordinateurs hôtes de ce réseau. Les masques de sous-réseau fonctionnent par application du ET logique à une adresse IPv4 de 32 bits.
En notation binaire, les bits ``1" dans le masque indiquent la partie adresse réseau et les bits ``0" indiquent la partie adresse de l'ordinateur hôte.
Un ET logique est appliqué pour comparer deux bits. Le résultat est ``1" si les bits comparés ont tous deux une valeur binaire égale à ``1".
Dans le cas contraire, le résultat est ``0". Voici l'ensemble des résultats possibles résultant d'une comparaison ET binaire entre deux bits.

Bit1	Bit2	Résultat
0	0	0
0	1	0
1	0	0
1	1	1

Pour comprendre comment un masque réseau est appliqué à une adresse IPv4, il faut d'abord convertir tout en binaire. Le masque de 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 IPv4 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 ordinateurs 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 sont pas limités à des octets entiers.

On peut également spécifier des masques de sous-réseau sous la forme 255.254.0.0 (ou /15 CIDR). Il s'agit d'un grand bloc d'adresses, contenant les 131 072 adresses allant de 10.0.0.0 à 10.1.255.255. Il pourrait être subdivisé, par exemple en 512 sous-réseaux de 256 adresses chacun. La première serait 10.0.0.0-10.0.0.255, alors 10.0.1.0-10.0.1.255, et ainsi de suite jusqu'à 10.1.255.0-10.1.255.255. Alternativement, ce bloc d'adresses pourrait être divisé en deux blocs de 65 536 adresses, ou 8192 blocs de 16 adresses, ou en d'autres nombreuses façons. Il pourrait même être subdivisé en un mélange de blocs de différentes tailles, aussi longtemps qu'aucun d'entre eux ne se chevauchent et que chaque bloc est un sous-réseau valide dont la taille est une puissance de deux. Alors que de nombreux masques de réseau sont possibles, les masques réseau communs comprennent:

CIDR	Décimal	# d'ordinateurs 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

A chaque réduction de la valeur CIDR, l'espace d'adressage IPv4 est doublé. Souvenez-vous que deux adresses IPv4 au sein de chaque réseau sont toujours réservées pour les adresses de réseau et de diffusion. Il existe trois masques de réseau communs qui ont des noms spéciaux.

Un réseau /8 (avec un masque 255.0.0.0) définit un réseau de classe A. Un réseau /16 (avec un masque 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 utilisés pour des raisons historiques.

À bien des égards, comme vous pouvez déjà le voir la planification de l'IPv6 est plus facile que celle de l'IPv4.

Adresses IP globales

Les réseaux interconnectés doivent s'accorder sur un plan d'adressage IP pour les adresses IPv6 et IPv4. Les adresses IP doivent être uniques et ne peuvent généralement pas être utilisées en différents endroits sur Internet en même temps. Sinon, les routeurs ne seraient pas capables de connaître la meilleure façon d'acheminer les paquets vers ces adresses.

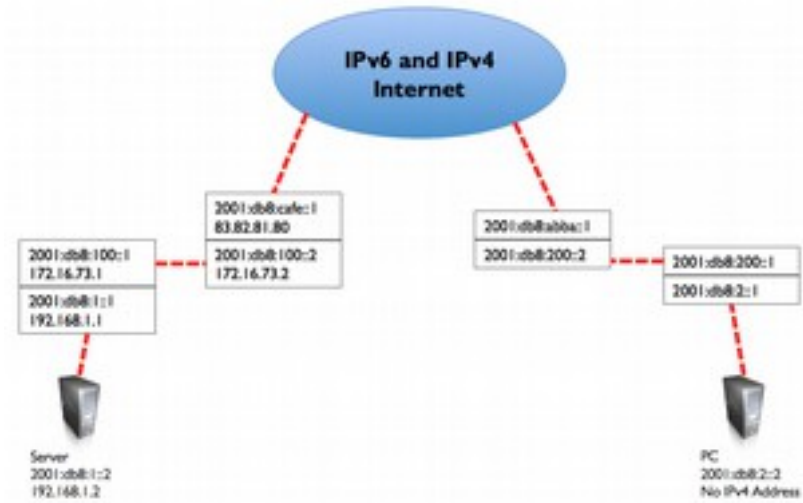


Figure NG 3: Avec des adresses IP uniques, un routage global ambigu est impossible. Si le PC demande une page Web à partir de 2001:db8:1::2, il atteindra le bon serveur.

Afin de conserver les adresses IP uniques et globalement routables, elles sont attribuées par une autorité centrale d'adressage qui fournit une méthode constante et cohérente d'adressage. Cela garantit que les adresses dupliquées ne sont pas utilisées par des réseaux différents.L'autorité attribue de grands blocs d'adresses consécutives à des autorités inferieures, qui à leur tour attribuent petits blocs consécutifs au sein de ces gammes à d'autres autorités, ou à leurs clients. Les groupes d'adresses sont appelés sous-réseaux ou les préfixes comme nous l'avons déjà mentionné. Un groupe d'adresses correspondantes à ces préfixes est désigné comme un espace d'adressage. Les adresses IPv4 et IPv6 sont toutes administrées par l'Internet Assigned Numbers Authority (IANA, http://www.iana.org/).

L'IANA a divisé ces espaces d'adressage dans de grands sous-réseaux, et ces sous-réseaux sont délégués à l'un des cinq registres régionaux Internet (en anglais regional Internet registries RIR), qui ont reçu l'autorité sur de vastes zones géographiques.
Les adresses IP sont attribuées et distribuées par les registraires Internet régionaux (RIR) aux fournisseurs de services Internet (ISPs). L'ISP attribue ensuite des petits blocs IP à leurs clients selon les besoins. Virtuellement, tous les utilisateurs Internet obtiennent leurs adresses IP à partir d'un ISP.

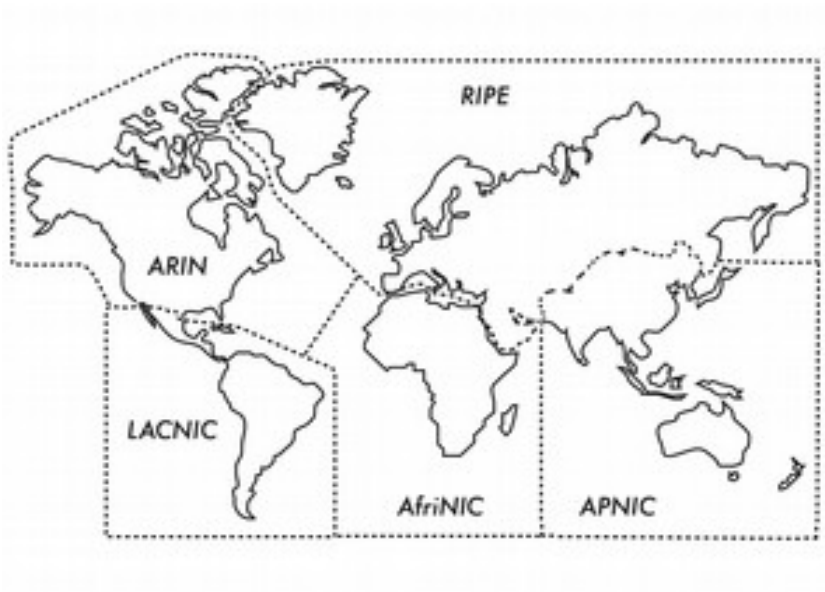


Figure NG 4: L'autorité pour l'attribution des adresses IP est déléguée aux cinq Regional Internet Registrars (RIR).

Les cinq RIR sont :

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

Votre ISP vous attribuera un espace d'adressage IP routable globalement à partir du pool d'adresses qui lui a été attribué 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 qu'un accord a été obtenu sur l'assignation d'adresses IP, il est possible de passer des paquets entre les réseaux et de participer au réseau Internet. Le processus de passer des paquets entre les réseaux s'appelle routage.

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 avoir des mappages DNS pointant vers elles et typiquement servir des informations à d'autres machines (tels que les services de messagerie, serveurs Web, etc.)
Des blocs d'adresses IP statiques peuvent être attribués par votre ISP, soit par demande ou automatiquement selon vos moyens de connexion à l'Internet.

Les adresses IP dynamiques

Les adresses IP dynamiques sont attribuées par un fournisseur de services Internet pour les nœuds non -permanents se connectant à l'Internet, tels qu'un ordinateur personnel connecté par dial-up ou un ordinateur portable se connectant au moyen d'une connexion sans fil hotspot. Les adresses IP dynamiques peuvent être attribuées automatiquement en utilisant le protocole Dynamic Host Configuration Protocol (DHCP) ou le Protocole Point-to-Point (PPP), selon le type de connexion Internet.

Un nœud utilisant DHCP commence par solliciter du réseau une allocation d'adresse et automatiquement configure son interface réseau. Les adresses IP peuvent être attribuées de manière aléatoire à partir d'un pool par votre ISP, ou 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 nœud doit renouveler la location DHCP avant l'expiration du temps de location. Au moment du renouvellement, le nœud peut recevoir la même adresse IP ou une autre dans le pool d'adresses disponibles.

Bien que DHCP fonctionne pour IPv6 et IPv4, IPv6 a un autre mécanisme de base qui est plus communément utilisé pour l'attribution d'adresse.

Ce mécanisme s'appelle Stateless Address Auto-Configuration (SLAAC) qui est le mécanisme par défaut sur les routeurs et les ordinateurs hôtes IPv6.
Le SLAAC ne nécessite pas de serveur DHCP.
Le routeur envoie des messages appelés Router Advertisement (RA) à intervalles réguliers à tous les réseaux W/LAN qui sont connectés. Ces messages contiennent le préfixe de 64 bits à être utilisé sur ce W/LAN.
Les ordinateurs hôtes alors génèrent leurs 64 bits identifiant d'interface (en général un nombre aléatoire ou un nombre basé sur leur adresse MAC - voir plus loin) et construisent leurs adresses de 128 bits par concaténation du préfixe de 64 bits de la RA et le 64 bits identifiant d'adresse (IID) nouvellement créé.
Les adresses dynamiques sont populaires auprès des fournisseurs de services Internet, car ces adresses dynamiques leur permet d'utiliser moins d'adresses IP par rapport au nombre total de clients connectés.
Ils ont seulement besoin d'une adresse pour chaque client qui est actif à tout moment donné. Les adresses IP routables globalement coûtent de l'argent, et il y a maintenant une pénurie d'adresses IPv4.
L'attribution d'adresses dynamiques permet aux fournisseurs de service Internet d'économiser de l'argent, et ils chargent souvent un extra à leurs clients pour une adresse IP statique.

Adresses IPv4 privées

Vers 2000, il était devenu clair qu'il n'y aurait pas assez d'adresses IPv4 pour tout le monde.
C'est la raison pour laquelle IPv6 a été spécifié et développé.
Mais il y avait aussi une astuce temporaire comme la plupart des réseaux privés n'exigeaient pas d'attribution des adresses IPv4 publics routable globalement pour tous ordinateurs d'une organisation.
En particulier, les ordinateurs qui ne sont pas des serveurs publics n'ont pas besoin d'être adressables sur le réseau Internet.
Les organisations utilisent généralement des adresses IPv4 de l'espace d'adressage privé pour les machines qui sont sur le réseau interne.
Il existe actuellement trois blocs d'espace d'adressage privé réservés by l'IANA : 10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16. Ces blocs sont définis dans le document RFC1918.
Ces adresses sont pas destinées à être routées sur Internet et sont généralement uniques seulement dans une organisation ou groupe d'organisations qui choisissent de suivre le même schéma d'adressage.

Cela signifie que plusieurs organisations distinctes peuvent utiliser les mêmes adresses pour autant qu'ils n'interconnectent pas leurs réseaux directement.

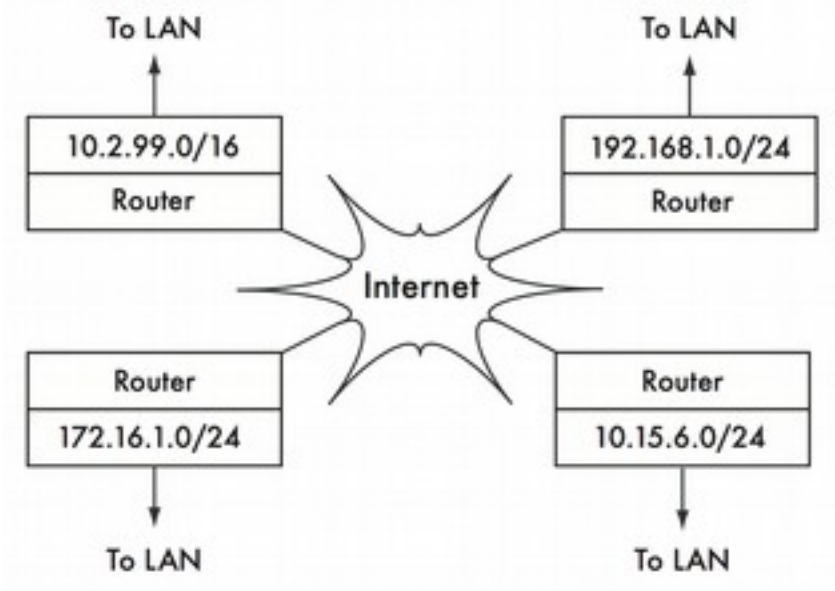


Figure NG 5 : Les adresses privées RFC1918 peuvent être utilisées dans une organisation et ne sont pas routées sur le réseau Internet.

Si jamais vous avez l'intention de connecter entre eux les réseaux privés qui utilisent l'espace d'adressage RFC1918, veillez utiliser des adresses uniques à travers tous ces réseaux.

Par exemple, vous pourriez diviser l'espace d'adresses 10.0.0.0/8 en plusieurs réseaux de classe B (10.1.0.0/16, 10.2.0.0/16, etc.).
Un bloc peut être attribué à chaque réseau en fonction de son emplacement physique (la branche du campus principal, premier bureau d'opération, deuxième bureau d'opération, dortoirs, et ainsi de suite).
Les administrateurs de réseau à chaque emplacement peuvent alors diviser le réseau plus loin dans plusieurs réseaux de classe C (10.1.1.0/24, 10.1.2.0/24, etc.) ou en blocs de toute autre taille logique.

Ainsi dans l'avenir, si les réseaux doivent toujours être connectés (soit par une connexion physique, une liaison sans fil, ou VPN), alors toutes les machines seront accessible à partir de n'importe quel point du réseau sans avoir à reconfigurer les périphériques réseau.
Certains fournisseurs de services Internet peuvent attribuer des adresses privées comme celles-ci à la place d'adresses publiques à leurs clients, même si cela a des inconvénients graves.
Étant donné que ces adresses ne peuvent pas être routés sur l'Internet, les ordinateurs qui les utilisent ne font pas vraiment ``partie" de l'Internet, et ne sont pas directement accessibles à partir de celui-ci.
En vue de leur permettre de communiquer avec l'Internet, leurs adresses privées doivent être traduits en adresses publiques.
Ce processus de traduction est connue comme la traduction d'adresses réseau (en anglais network address translation NAT) et est normalement effectué sur la passerelle entre le réseau privé et l'Internet.
Nous allons examiner le NAT en détail plus loin dans ce chapitre.
Comme il existe un très grand nombre d'adresses IPv6, il n'est pas nécessaire d'avoir des adresses privées IPv6, bien qu'il existe des adresses locales uniques (en anglais Unique Local Adresses ULA) qui sont adaptées aux réseaux non connectés tels que les laboratoires.

Découvrir les voisins

Imaginez un réseau avec trois ordinateurs hôtes: H_A, H_B, H_C.
Ils utilisent respectivement les adresses IP A, B et C.
Ces ordinateurs hôtes font partie du même sous-réseau/préfixe.
Pour communiquer sur un réseau local, deux ordinateurs hôtes doivent déterminer les adresses MAC des uns aux autres.
Il est possible de configurer manuellement chaque ordinateur hôte avec une table de correspondance entre une adresse IP et une adresse MAC.
Cependant, il est plus facile de découvrir dynamiquement l'adresse MAC d'un voisin à travers le protocole de découverte de voisins (en anglais Neighbour Discovery Protocol NDP) dans IPv6 et le protocole de résolution d'adresse (en anglais Address Resolution Protocol ARP) en IPv4. NPD et ARP fonctionnent d'une manière très similaire.

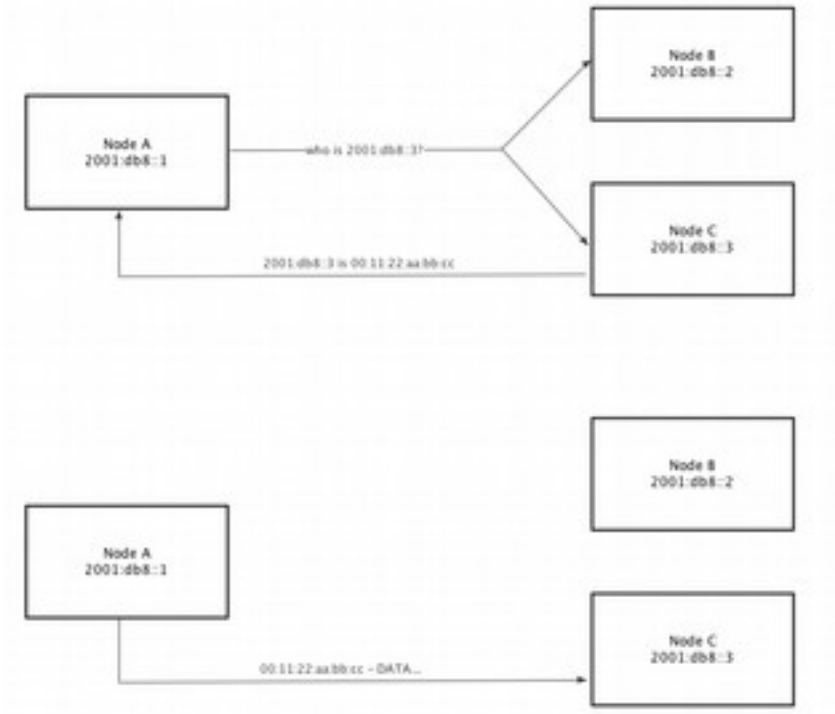


Figure NG 6 : Nœud IPv6 A, 2001:db8::1 doit envoyer des données à 2001:db8::3 dans le même réseau (préfixe 2001:db8::/ 64) . Mais le nœud doit d'abord demander l'adresse MAC correspondante de 2001:db8::3.

En utilisant NPD, le nœud A multi diffuse à certains hôtes la question ``Qui a l'adresse MAC de l'adresse IPv6 2001:DB8::3 ?".

Lorsque le nœud C voit un message Neighbor Association (NS) pour son propre adresse IPv6, il répond avec son adresse MAC dans un message Neighbor Adverstisement (NA).

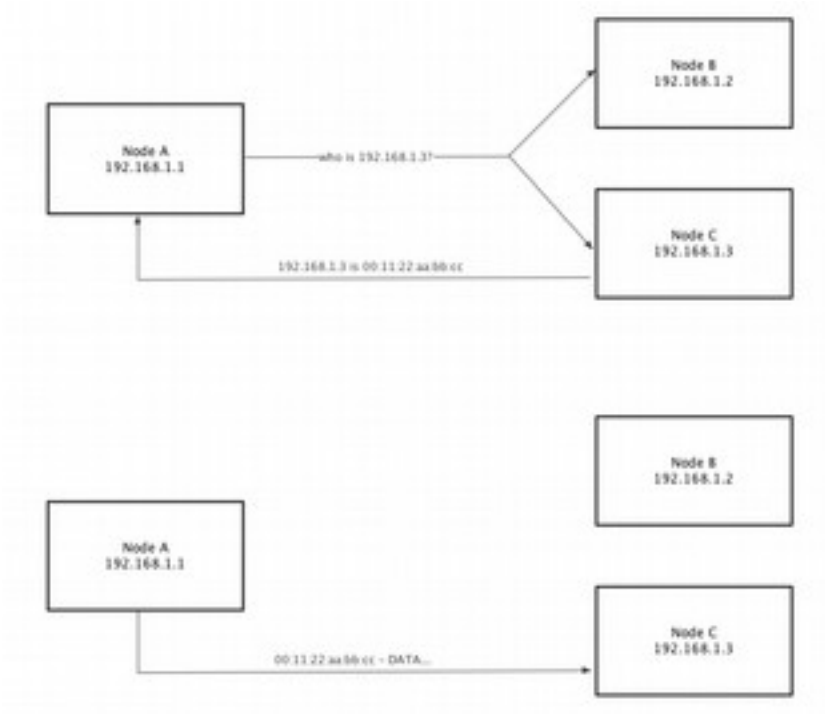


Figure NG 7: Le nœud IPv4 nœud A, 192.168.1.1, doit envoyer des données à 192.168.1.3 dans le même sous-réseau (192.168.1.0/24). Mais le nœud doit d'abord demander à l'ensemble du réseau l'adresse MAC correspondant à 192.168.1.3.

Lors de l'utilisation d'ARP, le nœud A diffuse à tous les ordinateurs hôtes la question ``Qui a l'adresse MAC pour l'adresse IPv4 192.168.1.3?".
Lorsque le nœud C voit une requête ARP pour son propre adresse IPv4, il répond avec son adresse MAC.
Le nœud B verra également la requête ARP mais ne répondra car 192.168.1.3 n'est pas son adresse. Ceci est très similaire à NDP pour IPv6, sauf qu'un nœud IPv4 ne dispose que d'une seule adresse IPv4. Aussi, ARP diffuse la demande. Cela signifie qu'il est reçu par tous les nœuds IPv4 dans le réseau. Ceci conduit à une plus grande utilisation du processeur hôte que dans le cas du NDP dans IPv6 qui multi diffuse à seulement certains ordinateurs hôtes.

Routage IP à des non- voisins

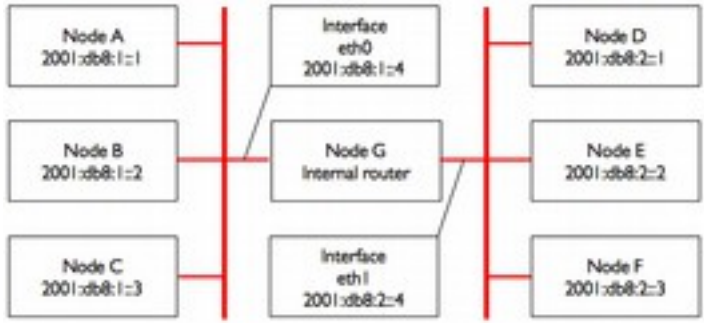


Figure NG 8 : Deux réseaux IPv6 distincts.

Considérons maintenant un autre réseau avec 3 nœuds, D, E, et F, avec les adresses IPv6 respectives 2001:db8:2::1, 2001:db8:2::2, et 2001:db8:2::3. Ceci est un autre réseau /64, mais il n'est pas dans la même gamme d'adresses que le réseau sur le côté gauche. Tous les trois hôtes peuvent s'atteindre directement (premièrement, utiliser NPD pour résoudre l'adresse IPv6 en une adresse MAC, puis envoyer les paquets à cette adresse MAC). Maintenant, nous allons ajouter le nœud G. Ce nœud a deux cartes réseau (également appelées interfaces), avec une branchée dans chaque réseau. La première carte réseau utilise l'adresse IPv6
2001:db8:1::4 sur l'interface eth0 et l'autre interface eth1 utilise l'adresse IPv6 2001:db8:2::4. Le nœud G est maintenant liaison-local pour les deux réseaux, et peut transmettre les paquets entre elles: le nœud G peut acheminer des paquets entre les deux réseaux. Il est donc appelé un routeur ou parfois une passerelle.
Mais que faire si les hôtes A, B, et C veulent atteindre les hôtes D, E, et F ? Ils ont besoin de savoir qu'ils doivent utiliser le nœud G et ils devront ajouter une route à l'autre réseau via l'ordinateur hôte G. Par exemple, les ordinateurs hôtes A-C ajouteraient une route statique via 2001:db8:1::4.
Sous Linux, cela peut être accompli avec la commande suivante :

 # Ip -6 route add 2001:db8:2::/64 via 2001:db8:1::4

... et les hôtes D-F ajouteraient ce qui suit:

 # Ip -6 route add 2001:db8:1::/64 via 2001:db8:2::4

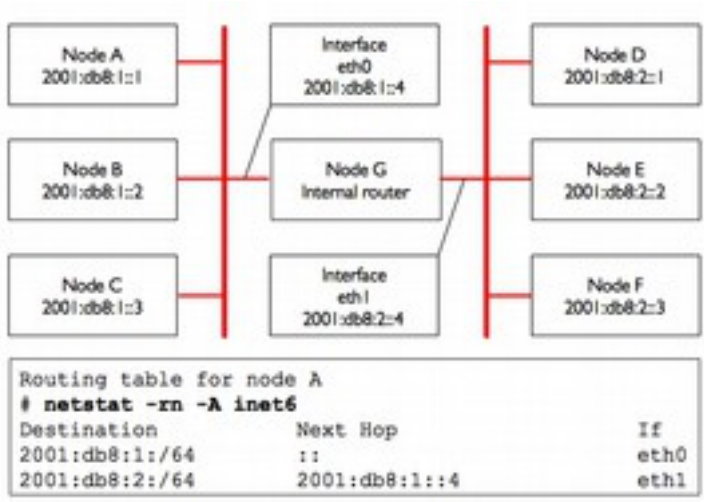


Figure NG 9 : Le nœud G agit comme un routeur entre les deux réseaux, d'autres ordinateurs hôtes utilisent des routes statiques.

Le résultat pour le nœud A est représenté dans la Figure NG 9.

Notez que la route est ajoutée via l'adresse IPv6 sur l'hôte G qui est liaison-locale au réseau respectif.
L'hôte A ne pouvait pas ajouter une route via 2001:db8:2::4, même si c'est la même machine physique que 2001:db8:1::4 (nœud G) car cette adresse IPv6 n'est pas liaison-locale.

L'adresse du saut suivant (next hop) peut être saisi soit comme une adresse globale (2001:db8 :2 ::4) ou une adresse liaison-locale (fe80:: ...) mais il est généralement plus facile de configurer une route statique avec une adresse globale.

Dans IPv6, le routeur G envoie également une sollicitation et des annonces de routage (router advertisements) périodiques contenant sa propre adresse liaison-locale permettant ainsi à tous les nœuds utilisant la configuration automatique sans-état ou le DHCP automatiquement d'ajouter une route par défaut via l'adresse liaison-locale du routeur comme indiqué dans la figure NG 10 .

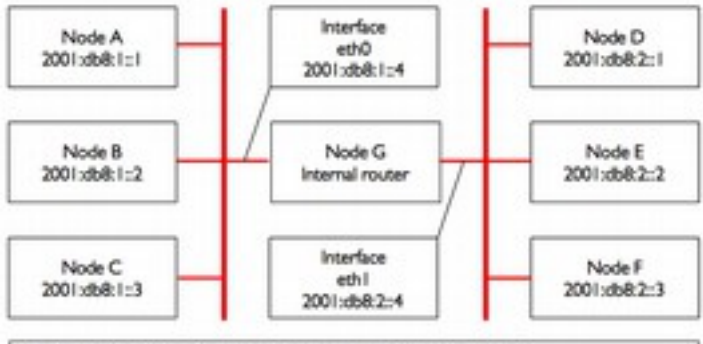


Figure NG 10 : Le noeud G agit comme un routeur entre les deux réseaux, les hôtes utilisent la configuration automatique d'adresses sans état.

Ceci est un exemple de routage très simple, où la destination est a seulement un saut unique de la source. Comme les réseaux deviennent plus complexes, beaucoup de sauts doivent être traversés pour atteindre la destination ultime. Comme il n'est pas pratique pour chaque machine sur l'Internet de connaître la route vers chaque autre machine, nous faisons usage d'une entrée de routage connu comme la route par défaut (également connu sous le nom de passerelle par défaut). Lorsqu'un routeur reçoit un paquet destiné à un réseau pour lequel il ne dispose pas de route explicite, le paquet est transmis à sa passerelle par défaut. La passerelle par défaut est généralement la meilleure route de sortie de votre réseau, généralement en direction de fournisseur des services Internet. Un exemple d'un routeur qui utilise une passerelle par défaut est illustré par la figure NG 11. La figure NG 11 montre la table de routage (qui est l'ensemble de toutes les routes) du routeur interne G qui comprend les deux réseaux directement connectés 2001:db8:1::/64 et 2001:db8:2::/64 ainsi que d'une route à tous les autres ordinateurs hôtes sur Internet ::/0.
Un nœud utilise toujours la route la plus spécifique, c'est la route qui correspond au préfixe le plus long vers la destination. Dans la figure NG 11, l'interface eth0 sera utilisée pour la destination 2001:db8:1::1 (longueur correspondante /64) plutôt que le moins spécifique :: /0 (longueur correspondante de 0).

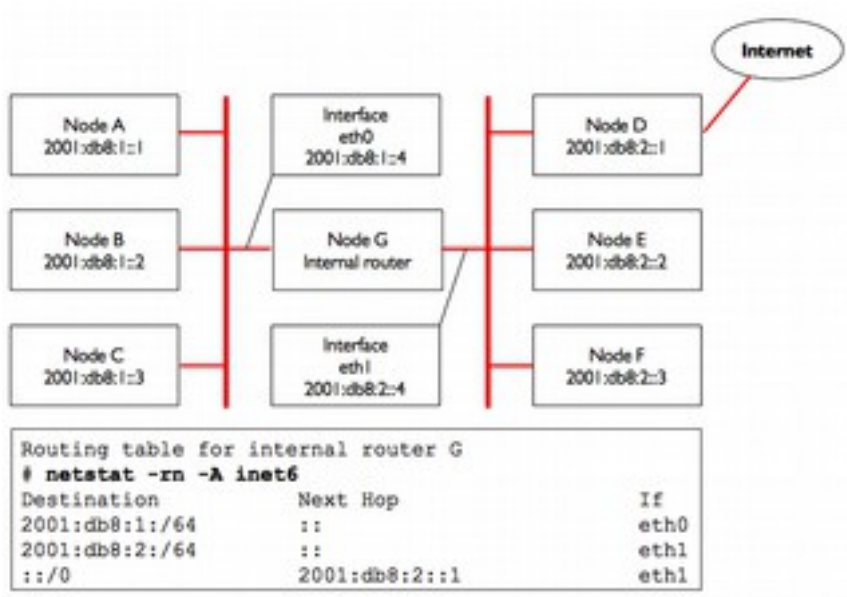


Figure NG 11: Le noeud G est le routeur interne et utilise le routeur Internet .

Une route informe le système d'opération (en anglais Operating system OS) que le réseau désiré ne se trouve pas sur le réseau liaison-locale immédiat et qu'il doit transmettre 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 au nœud G. Le nœud G chercherait ensuite l'hôte F dans sa table de routage pour voir s'il dispose d'une connexion directe au réseau de F. Enfin, l'ordinateur hôte G résoudrait l'adresse MAC de l'hôte F et lui transmettrait le paquet.
Les routes peuvent être mises à jour manuellement ou peuvent réagir dynamiquement aux pannes réseau et autres événements.

Quelques exemples de routage dynamique populaire incluent les protocoles RIP, OSPF, et BGP.
La configuration du routage dynamique est au-delà de la portée de ce livre mais pour lire davantage sur le sujet, referez-vous aux ressources dans l'annexe F.
L'IPv4 se comporte exactement de la même manière que représenté sur la figure NG 12.

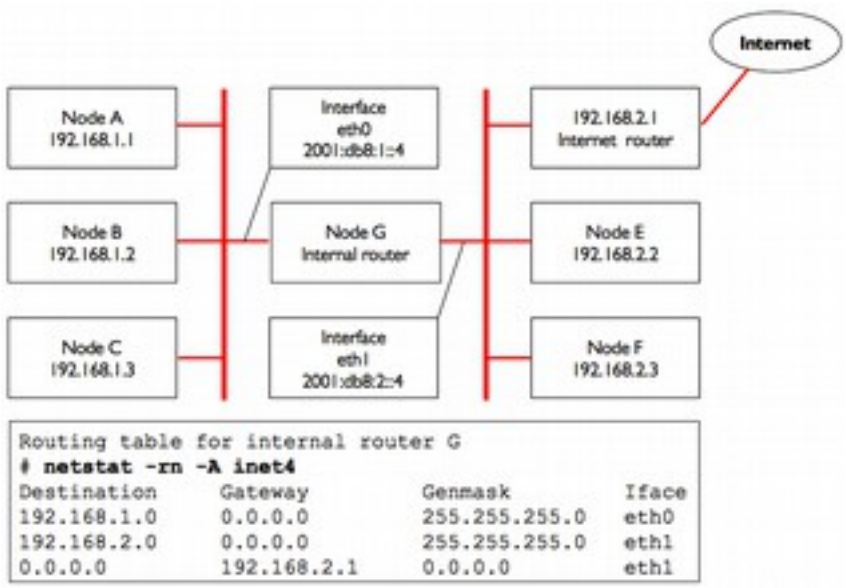


Figure NG 12 : Le nœud G est le routeur Internet sur ce réseau Ipv4.

Comme indiqué précédemment, la plupart des réseaux et l'Internet lui-même sont à double pile et tous les hôtes et les routeurs ont deux adresses IPv4 et IPv6.
Cela signifie aussi que les nœuds auront des routes pour IPv4 et des routes pour Ipv6.
Par exemple, l'ensemble de toutes les routes sur le noeud G des figures précédentes seront:

 # Netstat- rn -A inet6

destination	*Next Hop*	*If*
2001:db8:1:/64	*::*	*eth0*
2001:db8:2:/64	*::*	*eth1*
::/0	*2001:db8:2::1*	*eth1*

 # Netstat- rn -A inet4

Destination	*Gateway*	*Genmask*	*Iface*
192.168.1.0	*0.0.0.0*	*255.255.255.0*	*eth0*
192.168.2.0	*0.0.0.0*	*255.255.255.0*	*eth1*
0.0.0.0	*192.168.2.1*	*0.0.0.0*	*eth1*

Network Address Translation (NAT) pour IPv4

Pour atteindre les hôtes sur l'Internet, les adresses privées doivent être converties en des adresses globales IPv4 publiquement routables.

Ceci se réalise au moyen d'une technique connue sous le nom Network Address Translation ou NAT.

Un dispositif NAT est un routeur qui manipule les adresses des paquets à la place de les acheminer tout simplement.

Sur un routeur NAT, la connexion Internet utilise une (ou plusieurs) adresses IPv4 globalement routables, tandis que le réseau privé utilise une adresse IPv4 du pool d'adresses privées RFC1918.

Le routeur NAT permet de partager l'adresse globale entre tous les utilisateurs internes, qui utilisent tous des adresses privées.

Il convertit les paquets d'une forme d'adressage a une 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 passerelle par défaut, adressent les paquets comme les routeurs le feraient normalement.

Le routeur NAT traduit les paquets sortants pour utiliser une adresse IPv4 globale et les traduit à nouveau lors de leur réception à partir de l'Internet. La conséquence majeure de l'utilisation du NAT est que les machines sur l'Internet ne peuvent pas atteindre facilement des serveurs au sein de l'organisation sans la mise en place des règles d'acheminement explicites sur le routeur.

Les connexions émanant de l'espace d'adressage privé n'ont généralement aucun problème, bien que certaines applications (telles que la voix sur IP et certains logiciels VPN) peuvent être gérées difficilement par le NAT.

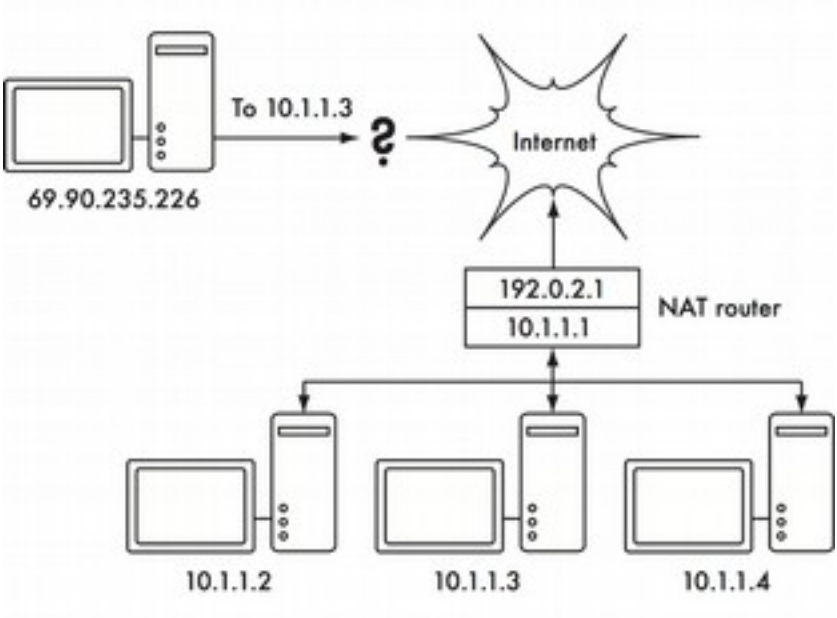


Figure NG 13: La translation d'adresse réseau vous permet de partager une adresse IPv4 unique avec beaucoup d'hôtes internes, mais peut rendre difficile l'exécution de certains services.

Dépendant du point de vue, cela peut être considéré comme un bug (car cela rend plus difficile la mise en place d'une communication bidirectionnelle) ou une fonctionnalité. Les adresses RFC1918 doivent être filtrées a la périphérie de votre réseau pour éviter le trafic RFC1918 accidentel ou malicieux d'entrer ou sortir de votre réseau.
Bien que le NAT effectue certaines fonctions pare-feu, ce n'est pas un remplacement pour un véritable pare-feu car actuellement la plupart des attaques se produisent quand un utilisateur interne visite certains sites Web au contenu hostile (appelé malware pour logiciels malveillants).

Suite des protocoles Internet

Les machines sur l'Internet utilisent le protocole Internet (IP) pour atteindre les uns les autres, même quand elles sont séparées par des nombreuses machines intermédiaires.
Il existe un certain nombre de protocoles qui sont exécutés conjointement avec IP.

Ces protocoles offrent des fonctionnalités qui sont aussi critiques pour les opérations normales que le protocole IP lui-même. Chaque paquet spécifie un numéro de protocole identifiant le paquet comme appartenant à un de ces protocoles.

Les protocoles les plus couramment utilisés sont le transmission control protocol (TCP, numéro 6), User Datagram Protocol (UDP, numéro 17), et l'Internet Control Message Protocol (ICMP, numéro 1 pour IPv4 et numéro 58 pour IPv6) . Pris en tant que groupe, ces protocoles (et d'autres) sont connus sous le nom de suite de protocoles Internet (en anglais Internet protocol suite) ou tout simplement TCP/IP en abrégé. 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 se distinguant les uns des autres. Chaque paquet possède un numéro de port source et destination. Certains numéros de port sont des normes bien définies, utilisées pour accéder à des services bien connus tels que les serveurs de messagerie et Web. Par exemple, les serveurs Web écoutent normalement sur le port TCP 80 pour le trafic non sécurisé et sur le port TCP 443 pour le trafic crypté/sécurisé. Les serveurs de temps NTP écoutent sur le port UDP 123 tandis que les serveurs de noms de domaine DNS écoutent sur le port UDP 53 et les serveurs de messagerie SMTP écoute sur le port TCP 25. Quand nous disons que le service ``écoute" sur un port (comme le port 80), cela signifie qu'il va accepter les paquets utilisant son IP comme adresse IP de destination et 80 comme le port de destination.

Habituellement, les serveurs ne se soucient pas de l'adresse IP source ou le port source, bien que parfois ils vont les utiliser pour établir l'identité de l'autre côté. Lors de l'envoi d'une réponse à ces paquets, le serveur va utiliser sa propre adresse IP comme adresse IP source et 80 comme port source. Lorsqu'un client se connecte à un service, il peut utiliser n'importe quel 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 le web, 25 pour le courrier électronique). Le protocole TCP est un protocole orienté session offrant une livraison et une transmission garantie et ordonnée et des fonctions de contrôle (telles que la détection et la mitigation de la congestion du réseau, les retransmissions, la réorganisation des paquets et leur réassemblage, etc.)

UDP est conçu pour les flux d'informations orienté sans connexion, et ne garantit pas du tout ni la livraison ou un ordre particulier mais peut être si rapide qu'il est souvent utilisé pour les protocoles en temps réel telles que la synchronisation, la voix ou la vidéo.

Le protocole ICMP est conçu pour le débogage et la maintenance sur l'Internet.
A la place des numéros de port, il a types de messages, qui sont également des nombres. Des messages de types de messages différents sont utilisés pour solliciter une réponse simple d'un autre ordinateur (echo request), informer l'expéditeur de l'arrivée d'un autre paquet, d'une boucle de routage possible (temps dépassé) ou informer l'expéditeur qu'un paquet qui n'a pas pu être livré à cause des règles pare-feu ou d'autres problèmes (destination inaccessible). A présent, vous devriez avoir une solide compréhension de l'adressage des ordinateurs sur le réseau et comment les flux d'information circulent sur le réseau entre ces ordinateurs. Maintenant, nous allons avoir un bref aperçu sur le matériel physique sous-jacent à ces protocoles réseau.

Matériel physique

Ethernet

Ethernet est le nom de la norme la plus populaire pour connecter ensemble les ordinateurs sur un **réseau local (LAN)**. Il est parfois utilisé pour connecter des ordinateurs individuels à l'Internet, par le biais d' un routeur, un modem ADSL ou un dispositif sans fil. Toutefois, si vous connectez un seul ordinateur à Internet, vous pouvez ne pas du tout utiliser Ethernet. Le nom vient du concept physique de l'éther qui est le milieu qui était autrefois censé transporter des ondes lumineuses dans l'espace libre. La norme officielle est appelé IEEE 802.3. Le 100baseT également connu en anglais sous le nom de Fast Ethernet est la norme Ethernet la plus largement déployée. Elle définit un débit de données de 100 mégabits par seconde (d'où le 100), exécutant sur des fils à paire torsadée (d'où le T) avec des connecteurs modulaires de type 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 nœuds terminaux (appareils et commutateurs supplémentaires) sur la périphérie. Les serveurs sont également connectés à l'aide du Gigabit Ethernet qui a un débit de 1 gigabit par seconde. De plus en plus, le Gigabit Ethernet remplace le Fast Ethernet dans de nombreux réseaux de nos jours car la demande pour la vidéo haut volume et d'autres applications à grand débit de données deviennent plus fréquentes.

Les adresses Medium Access Control (MAC)

Chaque dispositif connecté à un réseau Ethernet ou WiFi possède une adresse MAC unique, attribué par le fabricant de la carte réseau.

Elle sert d'identifiant unique qui permet aux dispositifs de communiquer entre eux. Toutefois, la portée d'une adresse MAC est limitée à un domaine de diffusion, qui est défini comme l'ensemble des ordinateurs reliés entre eux par des câbles, des concentrateurs, des commutateurs, et des bridges, mais ne traversant pas les routeurs ou des passerelles Internet. Les adresses MAC ne sont jamais utilisées directement sur l'Internet et ne passent pas à travers les routeurs. Les adresses MAC pour les réseaux WiFi IEEE 802.11 sont de 48 bits long et ressemblent à ceci: 00:01c:c0:17:78:8c ou 40:6c:8f:52:59:41; la dernière adresse MAC, les premiers 24 bits 40:6c:8f indique que cette adresse a été attribuée par Apple.

Hubs

Les concentrateurs Ethernet (hubs) connectent plusieurs périphériques Ethernet à paires torsadées ensemble. Ils opèrent au niveau de la couche physique (la couche la plus basse ou la première). Ils répètent les signaux reçus par chaque port sur tous les autres ports. Les concentrateurs peuvent donc être considérés comme des répéteurs simples. En raison de cette conception, seulement un seul port peut transmettre à la fois avec succès. Si deux dispositifs transmettent en même temps, ils vont corrompre les transmissions des uns les autres, et les deux doivent reculer et retransmettre leurs paquets plus tard. C'est ce qu'on appelle une collision, et chaque hôte est chargé de détecter et d'éviter les collisions avant transmission, et retransmettre ses propres paquets au moment opportun. Lorsque des problèmes tels que des collisions excessives sont détectées sur un port, certains hubs peuvent déconnecter (partitionner) ce port pendant un certain temps afin de limiter son impact sur le reste du réseau. Pendant qu'un port est partitionné, les dispositifs qui lui sont attachés ne peuvent pas communiquer avec le reste du réseau. Les hubs sont d'utilité limitée car ils peuvent facilement devenir des points de congestion sur les réseaux occupés. Ainsi de nos jours, ils ne sont plus normalement déployés sur les réseaux. Il est seulement important de noter qu'un point d'accès WiFi agit comme un hub du côté radio.

Commutateurs (Switches)

Un commutateur est un dispositif 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 relie ensemble temporairement.

Il peut y avoir plusieurs de ces connexions de port temporaires en même temps. Les commutateurs offrent généralement de meilleures performances que les hubs, en particulier sur les réseaux occupés avec de nombreux ordinateurs. Ils ne sont pas beaucoup plus cher que les hubs, et les remplacent dans la plupart des situations. Les commutateurs opèrent au niveau de la couche de liaison de données (deuxième couche), car ils interprètent et agissent sur l'adresse MAC des paquets qu'ils reçoivent. Quand un paquet arrive à un port d' un commutateur, le commutateur prend note de l'adresse MAC de la source qu'il associe à ce port . Il stocke ces informations dans une table MAC interne souvent connue dénommée en anglais content addressable memory (CAM) table.
Ensuite, le commutateur examine l'adresse MAC de destination dans sa table MAC, et transmet le paquet uniquement vers le port correspondant. Si l'adresse MAC de destination est introuvable dans la table MAC, le paquet est alors envoyé à l'ensemble des interfaces connectées dans l'espoir d'atteindre la bonne MAC.

Hubs vs commutateurs

Les hubs sont considérés comme des dispositifs peu sophistiqués, car ils rediffusent l'ensemble du trafic sur chaque port. Cette simplicité introduit à la fois une pénalité de performance et un problème de sécurité. La performance globale est plus faible, car la largeur de bande disponible doit être partagée entre tous les ports. Comme tout le trafic est vu par tous les ports, tout hôte du réseau peut facilement contrôler tout le trafic réseau. Les commutateurs créent des connexions virtuelles temporaires entre les ports de réception et de transmission.
Cela donne de meilleures performances car de nombreuses connexions virtuelles peuvent être réalisées simultanément. Les commutateurs les plus coûteux peuvent commuter le trafic tout en inspectant les paquets de données à des niveaux plus élevés (la couche transport ou la couche d'application), permettant la création de réseaux locaux virtuels, et l'implémentation d'autres fonctionnalités avancées.
Un hub peut être utilisé lorsque la répétition du trafic sur tous les ports est souhaitable, par exemple, lorsque vous souhaitez explicitement autoriser une machine de contrôle à voir l'ensemble du trafic sur le réseau.
La plupart des commutateurs offrent des fonctionnalités de moniteur de port qui permettent la répétition sur un port qui a été spécifiquement assigné à cette fin.
Les hubs furent une fois moins coûteux que les commutateurs.

Cependant, le prix de commutateurs a diminué de façon spectaculaire au cours des années. Par conséquent, chaque fois que possible les anciens hubs des réseaux doivent être remplacés avec de nouveaux commutateurs.

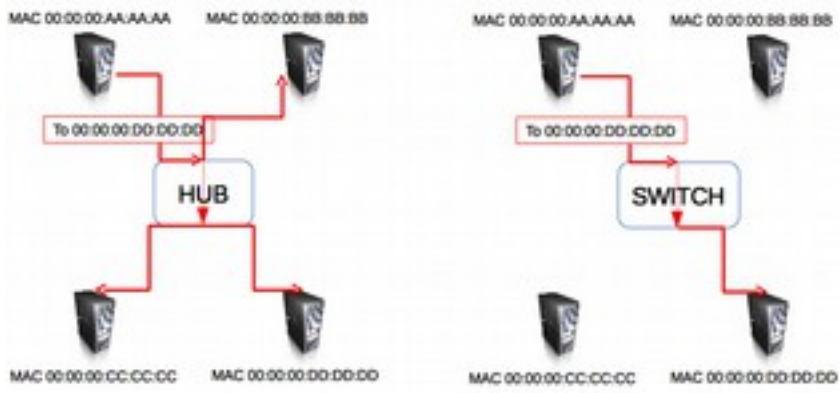


Figure NG 14 : Un hub simplement répète tout le trafic sur chaque port, tandis qu'un commutateur établit une connexion temporaire dédiée entre les ports qui ont besoin de communiquer.

Aussi bien les hubs tout comme les commutateurs peuvent offrir des services gérés. Certains de ces services incluent la possibilité de régler la vitesse de liaison (10 Base-T, 100baseT, 1000baseT, full et half-duplex) par port, activer les déclencheurs (en anglais triggers) pour surveiller les événements réseau (comme les changements d'adresse MAC ou les paquets malformés), et d'habitude comprend les compteurs de port pour une comptabilisation facile de la largeur de bande.
Un commutateur géré qui fournit le nombre d'octets en upload ou download pour chaque port physique peut grandement simplifier la surveillance du 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.

Les routeurs et les pare-feu.

Alors que les hubs et les commutateurs fournissent une connectivité sur un segment de réseau local, le travail d'un routeur est de transmettre des paquets entre les différents segments du réseau.

Un routeur a généralement deux ou plusieurs interfaces de réseau physiques. Il peut inclure le support pour différents types d'interfaces réseau, tels qu'Ethernet, WiFi, fibre optique, DSL, ou dial-up.
Les routeurs peuvent être des dispositifs dédiés ou ils peuvent être faits d'un PC standard avec plusieurs cartes réseau 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, ils peuvent prendre d'autres responsabilités en plus du routage. Beaucoup de routeurs ont des fonctionnalités pare-feu qui fournissent un mécanisme pour filtrer ou rediriger les paquets qui ne correspondent pas à la sécurité ou aux exigences de la politique d'accès.

Ils peuvent aussi fournir des services de translation d'adresses réseau (NAT) pour l'IPv4. Les routeurs varient considérablement en coût et capacités.
Les routeurs les moins coûteux et moins flexibles sont des dispositifs matériels dédiés, souvent ayant des fonctionnalités NAT, utilisés pour partager une connexion Internet entre quelques ordinateurs. Les marques bien connues incluent Linksys, D -Link, Netgear.

La seconde gamme supérieure consiste en un routeur logiciel ayant un système d'exploitation opérant sur un PC standard avec plusieurs interfaces réseau. Les systèmes d'exploitation standards tels que Microsoft Windows, Linux, BSD sont tous capables de routage, et sont beaucoup plus souples que les périphériques à faible coût.
Cela est souvent appelé Partage de connexion Internet.
Cependant, ces routeurs souffrent des mêmes problèmes que les ordinateurs classiques charterisés par une forte consommation d'énergie, un grand nombre de composantes complexes et potentiellement non fiables, et une configuration plus complexe. 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 une bien meilleure performance, plus de fonctionnalités, et sont plus fiables que les routeurs logiciels sur PC.

Il est également possible d'acheter des contrats de support technique et de maintenance pour ces routeurs.
La plupart des routeurs modernes offrent des mécanismes de surveillance et suivi de performance à distance, généralement via le Simple Network Management Protocol (SNMP), bien que les dispositifs les moins coûteux omettent souvent cette fonctionnalité.

Autre équipement

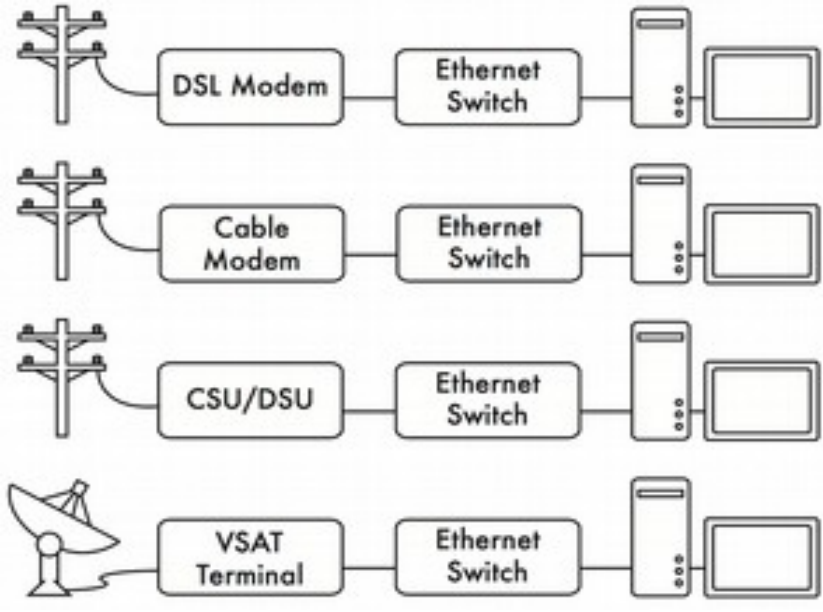


Figure NG 15 : Beaucoup de modems DSL, câbles modem, points d'accès sans fil et terminaux VSAT aboutissant à une prise Ethernet .

Chaque réseau physique a une pièce d'équipement terminal associé. Par exemple, les connexions VSAT sont constituées d'une antenne parabolique reliée à un terminal qui soit se branche sur une carte à l'intérieur d'un PC, ou se termine à une connexion Ethernet standard.
Les lignes DSL utilisent un modem DSL qui relie la ligne téléphonique à un périphérique local, soit un réseau Ethernet ou un seul ordinateur via USB. Les câbles modems font le pont entre le câble de télévision et le câble Ethernet ou un bus d'une carte interne du PC.
Les lignes dialup standard utilisent des modems pour connecter un ordinateur au téléphone, généralement par l'intermédiaire d'une carte plug-in ou un port série . Et il existe de nombreux types d'équipements de réseau sans fil qui se connectent à une grande variété de radios et d'antennes, mais presque toujours aboutissant à une prise Ethernet. La fonctionnalité de ces dispositifs peut varier considérablement entre fabricants.
Certains fabricants offrent des mécanismes de contrôle de performance, tandis que d'autres ne peuvent pas.

Comme votre connexion Internet vient finalement de votre fournisseur de services, vous devez suivre leurs recommandations au moment de choisir l'équipement qui leur réseau à votre réseau Ethernet.

Mettre le tout ensemble

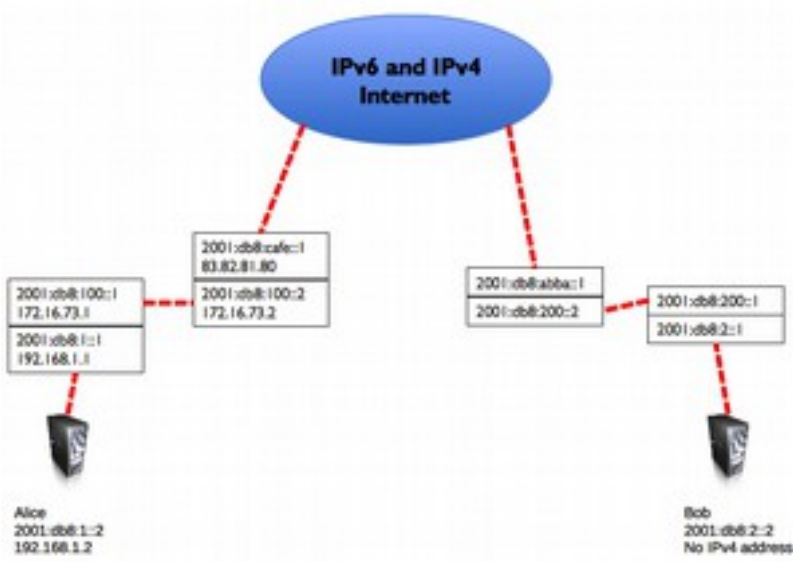


Figure NG 16 : Réseautage Internet. Chaque segment du réseau a un Routeur avec deux adresses IP, le rendant ``liaison local" à deux réseaux différents.

Les paquets sont transmis entre les routeurs jusqu'à ce qu'ils atteignent leur destination finale. Une fois que tous les nœuds du réseau ont une adresse IP, ils peuvent envoyer des paquets de données à l'adresse IP de n'importe quel autre nœud. Grâce à l'utilisation du routage et du forwarding, ces paquets peuvent atteindre des nœuds sur les réseaux qui ne sont pas physiquement connectés au nœud d'origine.
Ce processus décrit beaucoup de ce ``qui se passe" sur Internet. Dans cet exemple, vous pouvez voir le chemin que les paquets prennent quand Alice discute avec Bob à l'aide d'un service de messagerie instantanée. Chaque ligne pointillée représente un câble Ethernet, une liaison sans fil, ou tout autre type de réseau physique. Le symbole de nuage est couramment utilisé pour se substituer à "Internet ", et représente un nombre quelconque d'autres réseaux IP intervenants.

Aussi longtemps que les routeurs expédient le trafic IP vers la destination finale, ni Alice ou Bob n'ont besoin de se préoccuper de la façon dont ces réseaux fonctionnent.
N'eut été les protocoles Internet et la coopération de tout le monde sur le net, ce type de communication serait impossible.
Dans la figure NG 16, Alice est une pile double qui a des adresses IPv4 et IPv6, et Bob n'a que des adresses IPv6. Ils communiquent en utilisant IPv6 qui est la version IP commune entre eux .

La conception du réseau physique

Il peut sembler étrange de parler du réseau ``physique" lors de la construction des réseaux sans fil. Après tout, où est la partie physique du réseau ? Dans les réseaux sans fil, le support physique que nous utilisons pour la communication est de toute évidence l'énergie électromagnétique. Mais dans le contexte de ce chapitre, le réseau physique se réfère au problème banal de l'endroit où mettre les choses.

Comment organisez-vous l'équipement afin d' atteindre vos clients sans fil ? Qu'ils remplissent un immeuble de bureaux ou s'étendent sur des nombreux miles, les réseaux sans fil sont naturellement classifiés dans ces trois configurations logiques: les liaisons point -à-point, des liaison point-à-multipoint et les nuages multipoint-à-multipoint.
Alors que les différentes parties de votre réseau peuvent profiter de ces trois configurations, toute liaison individuelle va tomber dans un de ces topologies.

Point- à-point

Les liaisons point- à-point fournissent typiquement une connexion Internet lorsqu'un tel accès n'est pas disponible autrement. Un côté d'une liaison point -à-point aura une connexion Internet, tandis que l'autre utilise la liaison pour accéder à l'Internet. Par exemple, une université peut avoir un relais de trame (frame relais) rapide ou une connexion VSAT au milieu du campus, mais ne peut pas se permettre une telle connexion pour un bâtiment important juste en dehors du campus. Si le bâtiment principal a une vue non obstruée sur le site distant, une connexion point -à-point peut être utilisée pour relier les deux ensemble. Cela peut augmenter ou même remplacer des liaisons dial-up existantes.
Avec les antennes appropriées et une ligne de vue dégagée, des liaisons point -à-point fiables de plus de trente kilomètres sont possibles.

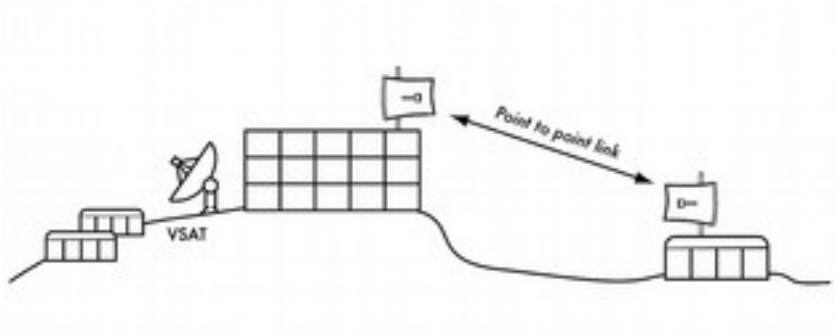


Figure NG 17 : Une liaison point -à-point permet à un site distant de partager une connexion Internet centrale.

Bien sûr, une fois qu'une seule connexion point-à-point a été établie, beaucoup plus peut être fait pour étendre le réseau davantage. Si dans notre exemple, le bâtiment à distance se trouve au sommet d'une haute colline, il peut être en mesure d'accéder à d'autres endroits importants qui ne seraient pas accessibles directement à partir du campus central.
En installant une autre liaison point -à-point sur le site distant, un autre nœud peut rejoindre le réseau et faire usage de la connexion Internet centrale. Les liaisons point -à-point ne doivent pas nécessairement impliquer l'accès à l'Internet. Supposons que vous avez-vous rendre physiquement à une station de surveillance météorologique à distance, dans les collines, afin de recueillir les données enregistrées au fil du temps. Vous pouvez vous connecter sur le site avec une liaison point-à-point, permettant la collecte et le suivi des données de se produire en temps réel, sans besoin de déplacement effective vers le site. Les réseaux sans fil peuvent fournir suffisamment de largeur de bande pour transporter de grandes quantités de données (y compris audio et vidéo) entre deux points qui sont connectés entre eux, même s'il n'y a pas de connexion directe à Internet.

Point-à-multipoint

Un autre agencement réseau le plus couramment rencontré est le point-à-multipoint. Chaque fois que plusieurs nœuds communiquent avec un point d'accès central, il s'agit d'une application point-à-multipoint. L'exemple typique d'un schéma de point-à-multipoint est l'utilisation d' un point d'accès sans fil fournissant une connexion à plusieurs ordinateurs portables.
Les ordinateurs portables ne communiquent pas directement entre eux, mais doivent être à portée du point d'accès pour utiliser le réseau.

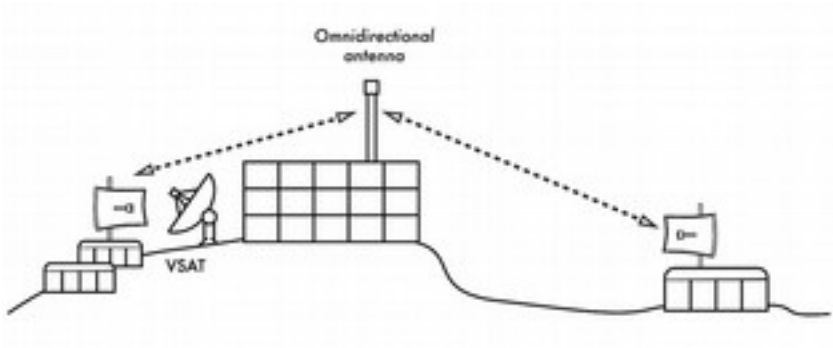


Figure NG 18 : Le VSAT central est désormais partagé par des multiples sites distants. Tous les trois sites peuvent également communiquer directement à des vitesses beaucoup plus rapides que celle du VSAT .

Le réseautage point-à-multipoint peut également s'appliquer à notre exemple précédent de l'université. Supposons que le bâtiment isolé au sommet de la colline est relié au campus central avec une liaison point-à-point. Plutôt que de mettre en place plusieurs liaisons point -à-point pour distribuer la seule connexion Internet, une antenne unique visible à partir de plusieurs bâtiments distants peut être utilisée. Ceci est un exemple classique d'une connexion étendue point (site distant sur la colline) à multipoint (plusieurs bâtiments dans la vallée ci-dessous). Notez qu'il existe un certain nombre de problèmes de performances quand on utilise le point-à-multipoint sur de très longue distances. Ceci sera abordé dans le chapitre intitulé Planification du déploiement. Ces liaisons sont possibles et utiles dans de nombreuses circonstances. Mais ne commettez pas l'erreur classique d'installer un seul tour radio de grande puissance dans le milieu de la ville et s'attendre à être en mesure de servir des milliers de clients, comme vous le feriez avec une station de radio FM. Comme nous le verrons, les réseaux de données bidirectionnels se comportent très différemment de la radio diffusion.

Multipoint -à-multipoint

Le troisième type de configuration du réseau est le multipoint-à-multipoint, qui est également dénommé un réseau ad- hoc ou un réseau maillé.
Dans un réseau multipoint-à-multipoint, il n'y a aucune autorité centrale. Chaque nœud du réseau achemine le trafic de tous les autres en fonction des besoins, et tous les nœuds communiquent directement les uns avec les autres.

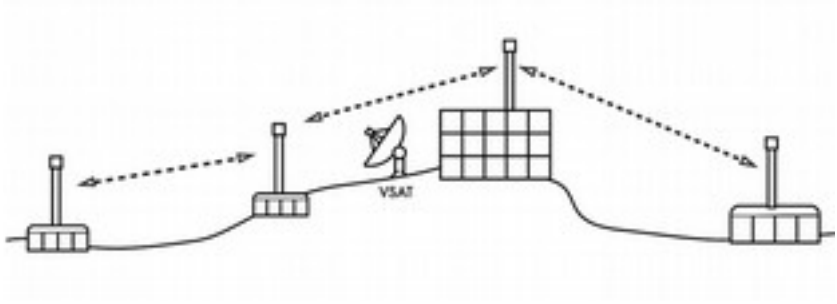


Figure NG 19: Un maillage multipoint-à-multipoint . Chaque point peut atteindre tous les autres à très grande vitesse. De même, n'importe lequel d'entre ces points peut utiliser le point d'accès central pour une connexion VSAT pour l' Internet.

L'avantage de cette configuration du réseau est que, même si aucun des nœuds n'est à portée d'un point d'accès central, ils peuvent toujours communiquer les uns avec les autres.
Le bonnes implémentations de réseau maillé sont auto-guérissant, ce qui signifie qu'ils détectent automatiquement les problèmes de routage et les fixent au besoin.
L'extension d'un réseau maillé est aussi simple que l'ajout de nœuds. Si l'un des nœuds dans le ``nuage" se trouve être une passerelle Internet, alors cette connexion peut être partagée entre tous les clients. Parmi les inconvénients de cette topologie on trouve une complexité accrue et des performances moindres. La sécurité dans un tel réseau est également un sujet de préoccupation, étant donné que chaque participant porte potentiellement le trafic de tous les autres.
Les réseaux multipoint -à-multipoint ont tendance à être difficiles à dépanner en raison du grand nombre de variables changeantes avec des nœuds joignant et quittant le réseau.
Les réseaux multipoint-à-multipoint ont généralement une capacité réduite par rapport au point-à-point ou aux réseaux point-à-multipoint, en raison de la charge supplémentaire de la gestion du routage de réseau et l'augmentation de contention dans le spectre radio.
Néanmoins, les réseaux maillés sont utiles dans de nombreuses circonstances. Pour plus d'informations à leur sujet veuillez s'il vous plaît lire le chapitre intitulé maillage réseau.

Utilisez la technologie qui s'adapte

Tous ces modèles de réseau peuvent être utilisés pour compléter les unes les autres dans un grand réseau. En outre, ils peuvent utiliser des techniques de réseautage câblées traditionnelles chaque fois que possible. Les réseaux câblés ont encore souvent des capacités de largeur de bande plus élevées que le sans fil. Elles devraient donc être utilisées quand c'est approprié ou abordable. Cependant en regardant le sans fil, c'est une pratique courante, par exemple, de recourir à une liaison sans fil à longue distance pour offrir un accès Internet à un endroit éloigné, puis établir un point d'accès sur le site éloigné pour fournir un accès sans fil local. L'un des clients de ce point d'accès peut aussi jouer le rôle d'un nœud d'un maillage permettant une propagation organique entre les utilisateurs des portables qui tous, ultimement, utilisent la liaison point-à-point originale pour accéder à Internet. Ceci est juste un des scénarios communs du déploiement sans fil. Il y a beaucoup d'autres. 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 .

7. FAMILLE WIFI

IEEE 802 : Qu'est-ce que c'est, et pourquoi devrais-je m'en occuper?

Les premiers jours du réseautage furent dominés par les réseaux câblés seulement (si vous ne considérez pas la dorsale micro-onde longue distance que l'ancienne compagnie AT&T avait installé à travers les États-Unis). Maintenant, des nombreux réseaux sont construits en utilisant la solution câblée et le sans fil. Typiquement les réseaux câblés, ou plus habituellement de nos jours, les réseaux en fibre ont une plus grande capacité que le sans fil. Mais la pose de la fibre est beaucoup plus coûteuse et prend du temps. Ainsi, très souvent les réseaux commencent par le sans fil et à mesure que leur utilisation augmente, les réseaux en fibre commencent à être déployés. Dans les réseaux d'accès (ceux qui sont à proximité des utilisateurs) ou dans les environnements urbains denses, souvent le sans-fil est aussi plus pratique. Donc il est très important quand vous commencez à penser à déployer des réseaux sans fil dans votre région ou votre communauté, votre réseau pourrait constituer la base de la croissance future du réseautage de votre région.

Un aspect des réseaux câblés et sans fil qui est important à comprendre consiste dans les différentes normes qui existent aujourd'hui, ainsi que les nouvelles normes en cours d'élaboration. Les normes sans fil sont à la base de nombreux produits sans fil. Elles assurent l'interopérabilité et la facilité d'utilisation par ceux qui conçoivent, déploient et gèrent des réseaux sans fil. Nous avons déjà abordé ce sujet dans le chapitre intitulé Radio Spectrum. Les normes utilisées dans la grande majorité des réseaux émanent du groupe de travail IEEE 802 de l'Association de normalisation IEEE. **IEEE 802** fait référence à une famille de normes IEEE qui traite des réseaux locaux et les réseaux métropolitains. Plus précisément, les normes IEEE 802 sont limitées à des réseaux transportant des paquets de taille variable. (En revanche, dans les réseaux à relais de cellules, les données sont transmises dans des petites unités, de taille uniforme appelées cellules). Le nombre 802 était tout simplement le prochain numéro libre que IEEE pouvait affecter, quoique le ``802" est parfois associé à la date ou la première réunion a eu lieu en Février 1980. Les services et les protocoles spécifiés par la norme IEEE 802 correspondent aux deux couches inférieures (liaison de données et physique) du modèle de référence OSI en sept couches.

En fait, IEEE 802 divise la couche liaison de données OSI en deux sous- couches

nommées Logical Link Control (LLC) et Media Access Control (MAC). La famille des normes IEEE 802 est maintenue par le Comité IEEE 802 de normalisation LAN/MAN (en anglais IEEE 802 LAN/MAN Standards Committee LMSC). Les normes les plus utilisées sont pour la famille Ethernet, Token Ring, LAN sans fil, Bridging et Virtual Bridged LANs. Un groupe de travail individuel fournit la direction à suivre pour chaque région. Les groupes de travail sont répertoriés dans le tableau ci-dessous.

Nom	Description
IEEE 802.1	Bridging et de gestion de réseau
IEEE 802.3	Ethernet
IEEE 802.11 a /b/g /n	LAN (WLAN) sans fil
IEEE 802.15	PAN sans fil
IEEE 802.15.1	certification Bluetooth
IEEE 802.15.2	coexistence IEEE 802.15 et IEEE 802.11
IEEE 802.15.3	PAN sans fil à haut débit
IEEE 802.15.4	PAN sans fil à débit réduit par exemple Zigbee
IEEE 802.15.5	Réseaux maillés pour WPAN
IEEE 802.15.6	Body Area Network
IEEE 802.16	Broadband Wireless Access (base de WiMAX)
IEEE 802.16.1	Service de distribution multipoint local
IEEE 802,18	Réglementation Radio TAG
IEEE 802,19	coexistence TAG
IEEE 802.20	Mobile Broadband Wireless Access
IEEE 802.21	Support Handoff indépendant
IEEE 802.22	Réseaux régionaux sans fil
IEEE 802.23	Groupe de travail des services d'urgence
IEEE 802.24	Smart Grid TAG
IEEE 802.25	Omni- Range Area Network

La norme 802.11

802.11 est la norme dont nous sommes le plus intéressés comme elle définit le protocole pour les réseaux locaux (LAN) sans fil. Les amendements 802.11 sont si nombreux que dans les dernières années ils ont commencé à utiliser deux lettres au lieu d'une. (802.11z – l'amendement DLS - a donné lieu à 802.11aa, ab, ac, .., etc.). Voici un tableau des variantes de 802.11, leurs fréquences et leurs couvertures approximatives.

Protocole 802.11	Version	Fréquence	Largeur de bande	Débit de données par Stream	Portée intérieure approximative		Portée extérieure approximative	
		(GHz)	(MHz)	(Mbit/s)	(m)	(ft)	(m)	(ft)
-	Juin 1997	2,4	20	1; 2	20	66	100	330
a	Sept. 1999	5	20	6;9;12; 18; 24; 36; 48; 54	35	115	120	390
b	Sept. 1999	2,4	20	1; 2; 5,5; 11	35	115	140	460
g	Juin 2003	2,4	20	6;9;12;18;24; 36; 48; 54	38	125	140	460
n	Oct. 2009	2,4/5	20	7,2; 14,4; 21,7; 28,9; 43,3; 57,8; 65; 72,2	70	230	250	820
			40	15; 30; 45; 60 ; 90; 120; 135; 150				
ac	Nov. 2011	5	20	Jusqu'à 87,6				
			40	Jusqu'à 200,0				
			80	Jusqu'à 433,3				
			160	Jusqu'à 866,7				

En 2012, l'IEEE a publié la norme 802.11-2012 qui regroupe tous les amendements précédents. Le document est librement téléchargeable sur: http://standards.ieee.org/findstds/standard/802.11-2012.html

La planification du déploiement des réseaux sans fil 802.11

Avant que des paquets de données puissent être acheminés et routés peuvent sur l'Internet, les couches un (physique) et deux (liaison de données) doivent être connectées. Sans une connectivité liaison locale, les nœuds du réseau ne peuvent pas communiquer les uns aux autres et acheminer les paquets. Pour assurer la connectivité physique, les périphériques réseau sans fil doivent fonctionner dans la même partie du spectre radio. Cela signifie que les radios 802.11a communiqueront avec les radios 802.11a à environ 5 GHz, et les radios 802.11b/g communiqueront avec d'autres radios 802.11b/g à environ 2,4 GHz. Mais un dispositif 802.11a ne peut pas interagir avec un dispositif 802.11b/g, car ils utilisent des gammes complètement différentes du spectre électromagnétique.

Plus spécifiquement, les interfaces sans fil doivent s'accorder sur un canal commun. Si une carte radio 802.11b est réglée sur le canal 2 tandis que l'autre est réglée sur le canal 11, les radios ne peuvent pas communiquer entre elles. Les fréquences centrales de chaque canal pour les standards 802.11a et 802b/g sont reprises en Annexe B: Allocation des canaux. Lorsque les deux interfaces sans fil sont configurées pour utiliser le même protocole sur le même canal radio, alors elles sont prêtes à négocier la connectivité dans la couche liaison de données.

Chaque dispositif 802.11a/b/g peut fonctionner dans l'un des quatre modes possibles :

1. Mode maître (en anglais Master, aussi appelé AP ou mode infrastructure). Ce mode est utilisé pour créer un service qui ressemble à un point d'accès traditionnel. L'interface sans fil crée un réseau avec un nom spécifique (appelé le SSID) et un canal, et offre des services réseau de sur ce canal. En mode maître, les interfaces sans fil gèrent toutes les communications relatives au réseau (authentification des clients sans fil, gestion de la contention sur le canal, répétition de paquets, etc.). Les interfaces sans fil en mode maître ne peuvent pas communiquer avec les interfaces qui leur sont associées en mode géré.
2. Mode géré (en anglais Managed). Ce mode est parfois aussi appelé mode client. Les interfaces sans fil en mode géré joindront un réseau créé par un maître, et changeront automatiquement leur canal pour assurer la correspondance avec celui du maître. Elles présentent ensuite les informations d'identification nécessaires au maître et si elles sont acceptées, elles sont dites être associées au maître. Les interfaces en mode géré ne communiquent pas directement entre elles. Elles ne pourront communiquer qu'avec un maître associé.
3. Mode Ad-hoc. Ce mode crée un réseau multipoint-à-multipoint où il n'y a pas de nœud maître unique ou AP. En mode ad-hoc, chaque interface sans fil communique directement avec ses voisins. Les nœuds doivent être à la portée des autres pour communiquer, et doivent s'entendre sur un nom de réseau et le canal à utiliser. Le mode Ad - hoc est souvent aussi appelé réseautage maillé et vous pouvez trouver des détails sur ce type de réseaurage dans le chapitre intitulé maillage réseau.
4. Mode moniteur (en anglais monitor). Ce mode est utilisé par certains outils (tels que Kismet) pour écouter passivement tout le trafic radio sur un canal donné.

En mode moniteur, les interfaces sans fil ne transmettent pas de données. Ce mode est utile pour analyser les problèmes sur une liaison sans fil ou observer l'utilisation du spectre dans le secteur local. Le mode moniteur n'est pas utilisé pour les communications normales.

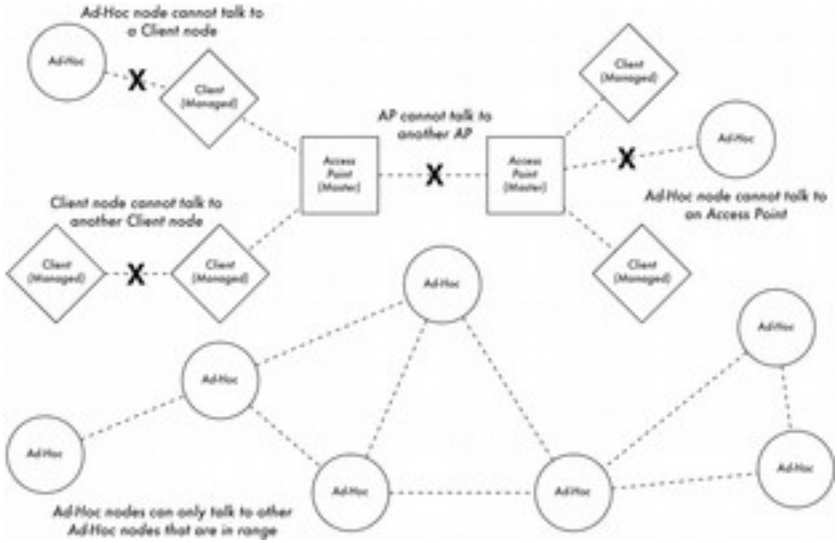


Figure WF 1: AP, clients et nœuds ad hoc.

Lors de la réalisation d'une liaison point-à-point ou point-à-multipoint, une radio fonctionne généralement en mode maître, tandis que l'autre/les autres fonctionne(nt) en mode géré. Dans un maillage multipoint-à-multipoint, les radios fonctionnent tous en mode ad-hoc pour qu'elles puissent communiquer entre elles directement. Il est important de garder ces modes à l'esprit lorsque vous concevez votre réseau. Rappelez-vous que les clients en mode gérés ne peuvent pas communiquer directement entre eux. Il est donc probable que vous ayez besoin d'un site répéteur élevé en mode maître ou ad-hoc. Le mode Ad- hoc est plus flexible mais il présente un certain nombre de problèmes de performances par rapport à l'utilisation des modes maître/gérés .

La norme 802.22

Vous êtes- vous jamais demandé pourquoi l'un des plus grands utilisateurs de spectre sans fil dans presque tous les pays sur la terre, ne s'est jamais

investi dans les affaires de communications bidirectionnelles ? Non ? Eh bien, demandez-vous pourquoi le secteur de la diffusion télévisée n'a jamais voulu faire les communications bidirectionnelles. La réponse simple est que ce n'était pas leur ligne d'affaires. Ce qu'ils faisaient était plutôt d'obtenir l'accès au spectre et utiliser le meilleur spectre (`` spectre de front de mer") entre le DC et la lumière du jour .. et presque gratuitement pour démarrer. Avec le remplacement de la télévision analogique par la télévision numérique, une partie de ce ``spectre de front de mer" est mise à disposition du réseautage sans fil. Et dans certaines parties du monde où la télévision n'a pas connu un grand déploiement, ces mêmes parties du spectre radio sont disponibles pour les réseaux sans fil aussi. La nouvelle technologie sans fil est communément appelé TVWS (Les espaces blancs TV, en anglais TV White Spaces) et bien qu'étant relativement nouvelle au moment de l'écriture de ce livre, cette technologie est utilisée dans beaucoup d'essais pour le sans fil à large bande en milieu rural.
De *wikipedia* -
Connu officieusement sous le nom de Super Wi-Fi, le **IEEE 802.22** est une norme sans fil pour les réseaux sans fil régionaux (en anglais Wireless Regional Area Netwoks) qui utilise des espaces blancs dans le spectre des fréquences de télévision . Le développement de la norme WRAN IEEE 802.22 est destiné à utiliser les techniques de radio cognitive (CR) pour permettre le partage du spectre géographique inutilisé qui était alloué à la diffusion télévisée, sur une base de non interférence, afin d'offrir un accès à large bande aux zones d'accès difficile et à faible population, qui sont typiques des milieux ruraux. Il est donc opportun et a le potentiel pour une large applicabilité à travers le monde.
Les réseaux **WRANs IEEE 802.22** sont conçus pour fonctionner dans les bandes de diffusion TV tout en assurant qu'aucune interférence préjudiciable n'est causée à l'opération titulaire, à savoir, la télévision numérique et télédiffusion analogique ainsi que des dispositifs autorisés de faible puissance tels que les microphones sans fil. La norme a été finalement publiée en Juillet 2011.

Technologie du 802.22 ou TVWS

Les premières ébauches de la norme 802.22 spécifient que le réseau devrait fonctionner dans une topologie point à multipoint (P2M) . Le système sera composé des stations de base (BS) et équipement de prémisse client (en anglais Customer Premise Equipment CPE). Les CPE seront attachés à une BA via une liaison sans fil.

Une caractéristique clé des stations de base WRAN 802.22 est qu'elles seront capables d'effectuer la détection du spectre disponible. L'institut des ingénieurs électroniciens et électriciens (en anglais Institute of Electrical and Electronics Engineers IEEE), ensemble avec la FCC aux États-Unis ont adopté une approche centralisée pour la détection du spectre disponible. Plus précisément chaque station de base (BS) serait équipée d'un récepteur GPS qui permettrait de reporter sa position. Cette information sera renvoyée aux serveurs centralisés qui répondraient avec les informations sur les chaînes de télévision libres qui sont disponibles et les bandes de garde dans la zone de la station de base. Les autres propositions permettraient la détection du spectre local uniquement, où la BS déciderait par elle-même des canaux qui sont disponibles pour la communication. C'est ce qu'on appelle la détection distribuée. Dans la détection distribuée, Les CPE détecteraient le spectre et enverraient des rapports périodiques a la station de base sur ce qu'ils ont détecté. Avec l'information acquise, la station de base évaluera si un changement est nécessaire dans le canal utilisé ou si au contraire elle devrait continuer à transmettre et recevoir dans le même canal. Une combinaison des deux approches est également envisageable. Ces mécanismes de détection sont principalement utilisés pour identifier le cas d'une transmission titulaire/primaire et s'il y a moyen d'éviter d'interférer avec elle. Cela signifie que la couche physique doit être capable de s'adapter à différentes conditions et être flexible pour sauter d'un canal à l'autre sans erreurs de transmission ou perdre des clients (CPE). Cette flexibilité est également requise pour ajuster dynamiquement la largeur de bande ainsi que les schémas de modulation et de codage. L'OFDMA (en anglais Orthogonal Frequency Division Multiple Access) est le schéma de modulation pour la transmission en téléchargement en amont tout comme en aval. Avec l'OFDMA, il sera possible d'atteindre cette adaptation rapide qui est nécessaire aussi bien pour les stations de base et que les CPE.

En utilisant un seul canal de télévision (une chaîne de télévision a une bande passante de 6 MHz, dans certains pays, elles peuvent être 7 ou 8 MHz), the taux de transmission maximal en bits qui peut être atteint est d'approximativement 19 Mbit/s à une distance de 30 km. La vitesse atteinte et la distance maximale correspondante ne sont pas suffisantes pour répondre aux exigences de la norme. Il existe une fonctionnalité appelée agrégation de canaux (en anglais canal bonding) qui traite de ce problème. L'agrégation des canaux utilise plus d'un canal de transmission/réception. Ceci permet au système d'avoir une bande passante plus élevée qui sera reflétée par une meilleure performance du système.

Résumé

Comme nous pouvons le voir, les normes pour les services câblés et sans fil sont pour la plupart incorporé dans le groupe de travail IEEE 802. En ce moment, la famille 802.11 des normes et du matériel WiFi 802.11 est de loin le plus largement manufacturée et utilisée pour les liaisons sans fil à l'intérieur et à l'extérieur. Le chapitre intitulé ``Sélection et configuration du matériel" traite des équipements beaucoup plus en détail. La nouvelle norme 802.22 est appelé à jouer un rôle croissant dans des nombreux réseaux sans fil ruraux (et urbains). La libération du spectre sans licence actuellement utilisé pour la diffusion télévisée permettra que cela se produise. Cependant les normes et les différents groupes impliqués dans cette norme sont encore dans un état primaire, comme le sont aussi les organismes du monde entier impliqués dans la réallocation du spectre. L'équipement disponible est encore très nouveau et les déploiements sont rares et largement séparés.
Dans les 2-3 prochaines années, il est prévu que ceci changera significativement et la prochaine révision de ce livre pourrait bien contenir des études de cas et des informations sur le déploiement à partager sur les réseaux basés sur la norme 802.22.

En attendant il y a un projet intéressant en cours en Ecosse dans le Royaume-Uni qui déploie des réseaux 802.22 TVWS.
Vous pouvez avoir plus d'informations sur le projet sur la page web:
http://www.wirelesswhitespace.org/projects.aspx

8. RÉSEAUX MAILLÉS

Introduction

Les réseaux maillés sont basés sur le réseautage multipoint-à-multipoint (m2m). Dans la nomenclature de la norme IEEE 802.11, le réseautage m2m est dénommé ``ad-hoc" ou en mode ``IBSS". La plupart des réseaux sans fil d'aujourd'hui sont basées sur la communication point -à-point (P2P) ou point-à-multipoint (P2M).

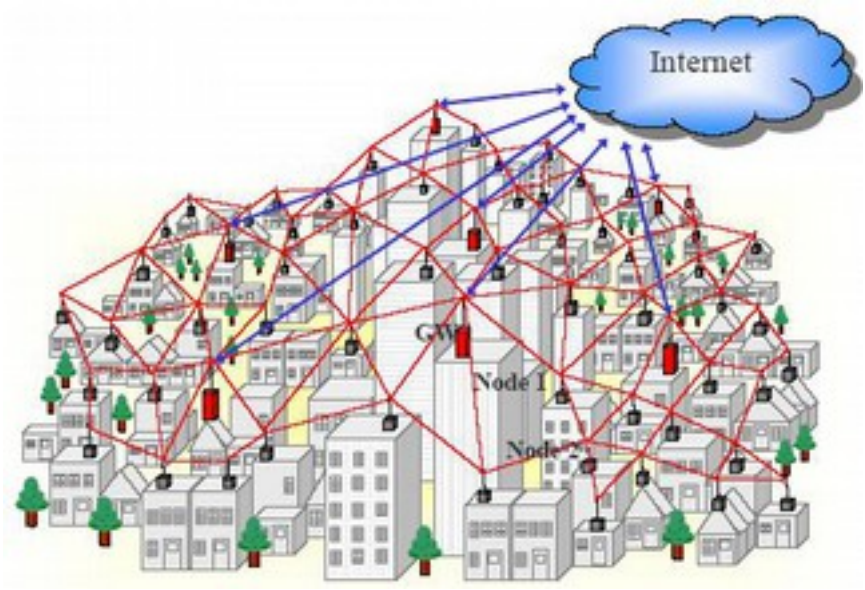


Figure MN 1 : Un réseau maillé métropolitain, fournissant une connectivité locale et l'accès à l'Internet via plusieurs passerelles Internet.

Un hotspot Wi-Fi typique fonctionne en mode infrastructure P2M qui consiste en un point d'accès (avec une radio fonctionnant en mode maître) attaché à une ligne DSL ou un autre réseau câblé à grande échelle.
Dans un hotspot, le point d'accès agit comme une station maîtresse qui distribue l'accès Internet à ses clients.
Cette topologie hub-and-spoke est aussi généralement utilisée pour le service téléphonique mobile (2G ou 3G).

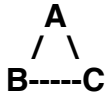
Les téléphones mobiles se connectent à une station de base P2M - sans la présence d'une station de base, les téléphones mobiles ne peuvent pas communiquer entre elles. Si vous faites un appel de plaisanterie à un ami qui est assis de l'autre côté de la table, votre téléphone envoie des données à la station de base de votre fournisseur de services qui peut être à une distance d'un mile – ensuite la station de base renvoie les données vers le téléphone mobile de votre ami.
Dans une région éloignée sans stations de base, un téléphone GSM est inutile comme un dispositif de communication, tout simplement parce que les radios GSM sont conçues de telle manière à ce qu'elles ne peuvent pas communiquer directement entre elles. Ceci est différent de postes de radio analogiques qui peuvent communiquer les uns avec les autres suivant le modèle m2m tant qu'ils se trouvent à portée.
Une radio sans fil est par défaut un support de diffusion, et toute station quelconque qui peut transmettre et recevoir peut communiquer suivant le modèle m2m. En ce qui concerne le défi technologique, l'implémentation des réseaux m2m est beaucoup plus exigeante que celle du p2m et p2p. Les stratégies pour implémenter la coordination de l'accès au canal sont plus complexes. Par exemple, il n'y a pas d'autorité centrale pour attribuer les intervalles de temps d'émission. Comme il n'y a pas de gestion centralisée, les stations m2m doivent s'entendre mutuellement sur les paramètres de coordination de la cellule tels que, similairement au MAC, le cell-id de la cellule sans fil. Le fait que le 802.11 nomme le mode m2m de WiFi ``ad-hoc" suggère que la direction IEEE pensait d'un réseau m2m comme étant une solution provisoire spontanée, sous- optimale.
La communication multipoint-à-multipoint est en fait plus polyvalente/versatile et peut être beaucoup plus efficace que la communication point-à-point ou point-à-multipoint: la communication m2m comprend la capacité de communiquer p2p et p2m, parce le p2p et p2m sont seulement des sous-ensembles du m2m.
Un réseau composé de seulement deux appareils multipoint-à-multipoint communique simplement en p2p :

A--B

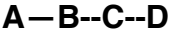
Un réseau de trois dispositifs maillés A, B, C peut former une topologie comme ci-dessous. Par exemple :

A--B--C

où A peut communiquer uniquement avec B et C ne peut communiquer seulement avec B, alors que B peut communiquer avec A et C. B, en fait, communique suivant le modèle p2m.
Sans routage, A et C ne peuvent pas communiquer entre eux en mode 802.11 ad-hoc.
En ajoutant un protocole de routage, A peut automatiquement savoir que derrière B, il y a C et vice-versa, et que B peut être utilisé comme un relais de communication permettant à tous les nœuds de communiquer les uns avec les autres.
Dans ce cas, B jouera un rôle similaire à un point d'accès en mode infrastructure 802.11. Les cartes WiFi configurées comme clients de mode infrastructure ne peuvent pas communiquer directement.
Elles auront donc toujours besoin le point d'accès B comme un relais.
Si les trois dispositifs se déplacent, la topologie peut former un maillage complet, où chaque nœud peut communiquer avec tous les autres nœuds directement:



Dans ce cas, relayer le trafic n'est pas nécessaire étant donné que les liaisons sont toutes assez bonnes. En mode infrastructure, la communication directe n'est pas possible.
Tout le trafic entre les clients doit être relayé par le point d'accès. Si nous ajoutons maintenant un nœud D au petit exemple de topologie and chaîne, tous les dispositifs peuvent communiquer entre eux si c'est un maillage.



D'autre part, ce ne serait pas possible si le réseau est un réseau en mode infrastructure et B est un point d'accès. C et D seraient tous deux clients du mode infrastructure, et comme déjà mentionné précédemment, les clients de mode infrastructure ne peuvent pas communiquer directement les uns avec les autres.
Ainsi le client D ne pouvait pas joindre le réseau de mode infrastructure, car il est hors de portée du point d'accès B alors qu'il serait encore dans la couverture du client C.

L'impact des routes à relais multiplessur la largeur de bande

Les réseaux maillés ayant des dispositifs à une seule radio constituent un moyen peu coûteux pour établir un réseau sans fil omniprésent, mais cela demande un compromis. Avec seulement une interface sans fil dans chaque dispositif, les radios doivent opérer dans le même canal. Le simple transfert des données sur une route allant de nœud A à B en passant par C réduit de moitié la largeur de bande disponible. Quand A envoie des données à B, B et C doivent garder le silence. Tandis que B est en train de transmettre des données à C, A doit rester silencieux aussi - et ainsi de suite. Notez que la même chose est vraie si deux clients connectés à un point d'accès dans le mode infrastructure veulent communiquer entre eux. Si nous supposons que toutes les liaisons sans fil dans la chaîne maillée ABCD fonctionnent à la même vitesse, la communication entre A et D serait à peu près 1/3 de la vitesse d'une liaison simple, étant donné que A et D peuvent utiliser la capacité du réseau de façon exclusive. L'impact sur la largeur de bande peut être atténué ou évité en utilisant des dispositifs à plusieurs radios, étant donné qu'ils fonctionnent sur des fréquences différentes qui n'interfèrent pas les uns avec les autres. En dépit du compromis sur la largeur de bande, les dispositifs de réseaux mailles a radio simple ont encore leurs mérites. Ils sont moins couteux, moins complexes et consomment moins d'énergie que les dispositifs multi-radio. Cela peut être important si les systèmes sont alimentés par énergie solaire ou éolien ou nécessitent une batterie de secours. Si les liaisons sans fil dans un réseau à trois sauts (une chaîne avec 4 nœuds comme ci-dessus) fonctionnent à 12 Mbit chacune, la largeur de bande totale de bout en bout pourrait encore offrir assez de largeur de bande pour saturer une liaison Internet de 2 Mbits en téléchargement en amont.

Résumé

Le réseautage maillé étend la gamme de dispositifs sans fil pour permettre le relais du trafic en des sauts multiples. Par le biais du routage dynamique, les maillages peuvent être auto-recouvrant en cas de défaillance d'un nœud et permettre une croissance organique si plusieurs nœuds sont ajoutés. Si les nœuds du maillage n'ont qu'une seule radio, le bénéfice de la couverture s'obtient au prix d'une réduction de la largeur de bande. Il y a un exemple d'un réseau maillé réel dont vous pouvez trouver plus d'informations sur le déploiement sur la page web : http://code.google.com/p/afrimesh/

Figure MN 2: Capture d'écran du réseau maillé Villagetelco à Bo-Kaap en Afrique du Sud.

Les protocoles de routage pour les réseaux maillés

Les protocoles de routage pour les réseaux maillés sans fil doivent être conçus en gardant à l'esprit les défis de la communication radio. Les liaisons sans fil et la topologie d'un réseau maillé sont intrinsèquement instables. Les dispositifs peuvent s'allumer et s'éteindre, la largeur de bande disponible varie et les liaisons sont souvent erronées avec perte de paquets.

Un protocole de routage maillé doit être résilient contre les erreurs de routage, même si les messages de routage du protocole sont retardés ou perdus. En même temps, la largeur de bande de communication disponible et la performance de calcul des nœuds du maillage est limitée et ne devrait pas être gaspillé dans les décisions de protocole et congestion de trafic. En 2005, lorsque la première édition du livre WNDW a été écrite, il n'y avait pratiquement que quelques protocoles de routage utilisables pour les réseaux maillés. Dans les éditions précédentes, ce chapitre a été porté sur le protocole OLSR. À l'époque, le démon OLSR n'était pas livré avec une configuration de travail par défaut, de sorte qu'il était nécessaire de patauger dans la profondeur du fichier de configuration olsrd.conf pour savoir quelle était la meilleure configuration de l'algorithme de routage.

La situation a un peu changé depuis 2005.

Il y a maintenant un certain nombre de protocoles et des implémentations de réseaux maillés et toutes les implémentations qui sont mentionnées dans ce chapitre sont disponibles sous forme de paquets d'installation pour OpenWRT.
Les développeurs des protocoles maillés sont en concurrence dans un défi d'offrir le meilleur protocole de routage maillé.
I l y a maintenant un événement annuel pour les développeurs de protocole maillé qui a lieu une fois par an.
Ça s'appelle ``Battlemesh", www.battlemesh.org
La plupart des protocoles de routage maillé (BABEL, BATMAN, OLSR, BMX, BMX6) prennent soin de maintenir des tables de routage IPv4 et IPv6 dans un nœud de maillage en ajoutant, en mettant à jour et en supprimant des routes.
Ces protocoles de maillage utilisent le routage IP.
Ce sont des protocoles de maillage de couche 3 comme IP représente la troisième couche du modèle OSI des couches réseaux. Batman-adv (anced) est un protocole relativement nouveau qui fonctionne sur la seconde couche du modèle de réseautage.
C'est donc un protocole de maillage de couche 2. Pour les couches supérieures (y compris la couche IP), Batman-adv fait apparaître tout le maillage comme un commutateur, où toutes les connexions sont liaison locale. Un maillage Batman -adv est transparent aux couches supérieures du modèle de réseautage.
Cela simplifie de beaucoup la configuration d'un réseau maillé, car il est possible d'utiliser le DHCP, mDNS ou MAC bridging avec Batman -adv. Batman-adv est un module du noyau Linux, qui est livré avec les sources officielles du noyau Linux.
Les protocoles de routage maillé doivent aussi gérer l'annonce et la sélection des passerelles vers les réseaux externes comme l'Internet.
Un problème courant avec les mécanismes de sélection de la passerelle est que le protocole de routage peut décider de commuter entre passerelles trop souvent - par exemple, parce que l'un des chemins de routage vers une passerelle est juste devenu un peu meilleur que l'autre.
Ceci est ennuyeux car il peut causer des battements de passerelle et conduire en des séances de connexion interrompues fréquemment.
S'il y a plus d'une passerelle Internet dans le maillage, l'utilisation d'une méthode avancée pour la sélection de la passerelle est fortement recommandée.

Qu'en est-il du 802.11s ?

Le calendrier de lancement (en anglais roadmap) du 802.11s est d'étendre un réseau jusqu'à 32 nœuds. Selon Wikipedia, il utilise HWMP (en anglais Hybrid Wireless Mesh Protocol) comme protocole de routage par défaut, avec la possibilité d'utiliser d'autres protocoles de routage.
Citation: ``HWMP est inspiré par une combinaison d'AODV (RFC 3561 [2]) et the routage basé sur des structures arborescentes".
Comme le 802.11s est relativement nouveau, il n'a pas été sujet à beaucoup d'expérience pratique jusqu'à ce jour.

Périphériques et firmware pour les systèmes embarqués

Ce ne sont pas tous les périphériques WiFi qu'on trouve sur le marché qui sont adaptés pour les réseaux maillés.
En 2005, lorsque la première édition de ce livre a été écrite, l'une des recommandations claire en matériel de réseautage maillé était l'usage du routeur Linksys WRT54G combiné avec le firmware Freifunk.
Alors que le WRT54G(L) est toujours sur le marché, il ne vaut plus la peine d'être recommandé.[1] OpenWRT est à la fois un environnement de développement de logiciel très polyvalent pour les développeurs et un firmware pour les utilisateurs avancés de Linux. L'ancien firmware Freifunk est basé sur la version dépassée d'OpenWRT appelée ``White Russian". ``White Russian" supportait seulement des dispositifs avec des chipsets Broadcom avec un pilote sans fil binaire propriétaire et est basé sur la version Linux 2.4. Il a été évincé par les versions d'OpenWRT ``Kamikaze" et ``Backfire" (dernière version). Avec ``Kamikaze" et ``Backfire", OpenWRT a obtenu le soutien de nombreux chipsets, des architectures de processeur et des périphériques sans fil. Les protocoles de routage maillés mentionnés avant sont disponibles sous forme de paquets d'installation pour OpenWRT. Quelques communautés de réseautage ouvert ont développé leurs propres images du firmware OpenWRT personnalisés avec

1. 1. Quoique le WRT54GL est toujours disponible sur le marché à des prix de 60 US $, il est très coûteux. La version 4.0 de WRT54G a été vendue comme version 1.0 de WRT54-GL par Linksys en 2005, après que Linksys ait introduit la version 5 de WRT54G 5.0 qui n'était pas compatible Linux. La version 5.0 de WRT54G ne dispose que de la moitié du stockage Wash et la capacité de mémoire RAM. Le modèle WRT54G est le routeur WiFi à durée de production la plus longue. Avec le montant d'argent que vous avez besoin de dépenser pour acquérir un routeur Linksys WRT54GL en 2011, vous pouvez acheter deux ou trois routeurs similaires d'autres marques mais qui sont plus rapides en termes de CPU et le débit de données.

Kamikaze et Backfire. Cependant, ils sont principalement conçus pour répondre à leurs préférences et exigences locales et de supportent un nombre limité de dispositifs. Comme ils sont souvent localisés, ils peuvent être d'une utilité limitée pour le grand public. OpenWRT dispose d'un système de gestion du logiciel, qui vient à la rescousse.
Il est typique pour OpenWRT d'installer des logiciels dans le routeur après qu'il ait été installé.
Il existe maintenant un méta-logiciel nommé ``lucifreifunk-community" qui convertit automatiquement une image OpenWRT en un firmware de réseautage maillé communautaire.
Le nombre de dispositifs qui peuvent être convertis en un routeur maillé a considérablement augmenté. D'autre part, le processus de conversion d'un firmware OpenWRT en un firmware de maillage via le système de gestion de logiciel est malheureusement souvent sujet à plus d'erreurs.
Certains fabricants des routeurs WiFi sont en train de fournir des équipements avec OpenWRT comme leur firmware d'usine : Mesh-Potato, Dragino MS-12, Allnet 0305.

Figure MN 3: Routeur WiFi maillé de l'extérieur Mesh-Potato avec VoIP (avec un port FXS pour connecter des combinés téléphoniques analogiques) . www.villagetelco.org

Le Mesh-Potato est un dispositif extérieur de faible puissance conçu pour un réseau maillé avec un port FXS (téléphone analogique), permettant de brancher un combiné téléphonique analogique et faire des appels téléphoniques via le maillage.
Le Mesh Potato est livré avec un firmware de maillage qui utilise le protocole maillé de couche trois BATMAN. Un second firmware nommé SECN (en anglais Small enterprise/campus network) est aussi disponible pour le Mesh-Potato. Il utilise le protocole maillé de couche deux BATMAN-ADV.
Mais ces dispositifs ne sont pas les seuls qui devraient être considérés pour l'achat. OpenWRT supporte une très large gamme des routeurs sans fil. Le remplacement du firmware d'usine par OpenWRT est souvent assez facile. Encore une fois, la gamme des dispositifs disponibles est tellement diversifiée qu'il n'y a pas une méthode de mise à jour unique qui fonctionne pour toute la gamme de matériel qui pourrait être décrite. La table du matériel supporté par OpenWRT est énorme et il ne cesse de s'élargir: http://wiki.openwrt.org/toh/start
Ce site devrait être votre point de départ avant d'aller acheter du matériel. Pour le moment, si vous êtes à la recherche d'un routeur basé sur un chipset qui supporte la norme 802.11n en mode ad-hoc, ma recommandation porte sur des dispositifs qui sont supportés par le port AR7XXX de OpenWRT.
Notez que les fabricants de matériel peuvent changer les chipsets des dispositifs sans le préciser explicitement. Les révisions nouvelles du matériel ne sont pas garanties de fonctionner à moins que quelqu'un les a testé et rapporté le test dans le wiki OpenWRT. Les dispositifs notables qui peuvent être flashés avec OpenWRT sont les unités extérieures produites par Ubiquity et les dispositifs SoHO produits par TP-Link. TP-Link produit plusieurs dispositifs SoHO à faible coût avec des chipsets de type Atheros ar71xx (802.11n).
Le TP-Link MR3220 (802.11n single stream) et MR3420 (802.11n double stream) disposent d'un CPU de 400 MHz MIPS 24kc, un port USB 2.0, un port commutateur à 4 ports de 100 Mbit, un port WAN, une mémoire flash de 4 Mo et 32 Mo de RAM.
Les prix commencent à environ 30 $ US. Comme les dispositifs TP-Link disposent d'un port USB 2.0, il est possible d' ajouter une autre interface WiFi via le dongle WiFi USB. En fait, le USB 2.0 ajoute des nombreuses possibilités, comme l'ajout de l'espace de stockage supplémentaire, le support audio, webcams, etc.

Figure MN 4: routeurs extérieurs de bricolage basés sur le circuit imprimé provenant de routeurs SOHO (Photo montrant deux dispositifs basés sur le TP-Link WR741 et le WR941 et un basé sur un routeur Fonera)

Un autre firmware qui au départ devait être comme une alternative au firmware WRT54G est le DD-WRT. Le DD-WRT est un firmware conçu pour les utilisateurs finaux. Il ne supporte que le protocole de routage OLSR.

Problèmes fréquemment observés

Les problèmes typiques de communication multipoint à multipoint sont soit liés à la couche physique de la radio ou la couche MAC. Les suggestions IEEE 802.11 sur le mode multipoint-à-multipoint ne sont pas à la hauteur de la tâche. Les principaux défis sont les suivants:

Coordination d'accès au canal, à savoir les problèmes de nœud caché et nœud exposé.

Pour en revenir à notre petite maille de topologie ABC, il peut arriver que A et C commencent à envoyer des données à B en même temps parce qu'ils ne s'entendent pas l'un et l'autre. Ceci résulte dans une collision sur le site de B. Le protocole 802.11 dispose d'un mécanisme pour mitiger ce problème : le RTS/CTS (en anglais request to send, clear to send). Avant qu'un noeud m2m n'envoie les données, il demande du temps d'antenne en envoyant un paquet court appelé RTS, afin de réserver le canal. Il attend jusqu'à ce qu'il reçoive un signal CTS. Donc A envoie un paquet RTS court et B envoie un paquet court CTS. De cette façon, C détecte qu'il y aura une transmission d'un nœud caché avec lequel il ne doit pas interférer.

Cependant, le mécanisme RTS/CTS actuel du protocole 802.11 fonctionne bien seulement pour des routes à deux sauts. Sur des routes plus longues, il peut arriver que plusieurs stations envoient des signaux RTS, entraînant l'arrêt de transmission de tous les nœuds en attente d'un signal CTS. C'est ce qu'on appelle un ``RTS broadcast storm'' en anglais. Pour les réseaux maillés de taille considérable, il n'est pas recommandé d'utiliser le mécanisme RTS/CTS.

Synchronisation de la minuterie

Les concepteurs du protocole ad-hoc 802.11 avaient pensé qu'il serait intelligent que les périphériques WiFi soient capables de synchroniser leurs horloges de temporisation MAC en envoyant des signatures de temps dans les balises (en anglais beacons).

Cependant des fausses signatures de temps peuvent provenir des erreurs et elles déclenchent souvent des conditions de course (en anglais race conditions) dans le matériel, les pilotes et le protocole ad-hoc 802.11, qui n'a pas été conçu pour faire face à ces problèmes. Les tentatives infructueuses de synchronisation d'horloge se traduisent souvent par la division cellulaire (voir ci-dessous). Il y a quelques hacks qui ont été introduits pour résoudre le problème.La meilleure solution est de désactiver entièrement la synchronisation de la minuterie. Cependant la synchronisation de la minuterie se fait souvent dans l'interface matérielle sans fil ou le firmware d'une interface. OpenWRT a un truc (hack) pour désactiver la synchronisation de la minuterie en utilisant les cartes Atheros 802.11abg qui fonctionnent avec le pilote Madwifi . Si vous utilisez un noyau Linux récent, certains pilotes sans fil (à savoir ath9k) qui sont souvent utilisés pour les dispositifs maillés sont assez robustes pour contrer les problèmes de temporisation en mode adhoc.

Toutefois, cela n'est pas utile si le périphérique WiFi est livré avec un micro-programme de source binaire fermé qui n'est pas prêt à faire face aux problèmes de la minuterie. Il n'y a pas beaucoup que nous pouvons faire à ce sujet, à part utiliser les pilotes/firmwares/chipsets qui sont connus pour fonctionner de manière fiable.

Fractionement de cellule IBSS

Ceci est un problème typique de la manière dont le 802,11 suggère l'implémentation du mode m2m. Les dispositifs Ad-hoc peuvent ne pas s'entendre sur une certaine identité d'une cellule (IBSS-ID). Si elles ne parviennent pas à s'entendre sur l'utilisation d'une certaine identité d'une (cell-id), ils deviennent des cellules sans fil logiquement séparés. Il s'agit d'un véritable ``show stopper'', parce que les dispositifs sans fil ne seront pas en mesure de communiquer les uns avec les autres. Le problème est lié à des problèmes de synchronisation de la minuterie. Depuis la version Linux 2.6.31, il est possible de configurer manuellement le IBSS-ID. Cette fonctionnalité est également disponible dans OpenWRT.

9. SÉCURITÉ POUR LES RESEAUX SANS FIL

Introduction

Alors que le spectre sans licence permet d'énormes économies de coûts pour l'utilisateur, il présente un mauvais effet secondaire où les refus/dénis de service (DoS) sont trivialement simples. En allumant simplement un point d'accès de haute puissance, un téléphone sans fil, un émetteur vidéo ou tout autre dispositif opérant dans la fréquence 2,4 GHz, une personne malveillante pourrait causer des problèmes importants sur le réseau. Beaucoup de dispositifs réseaux sont aussi vulnérables à d'autres formes d'attaques par déni de service telles que le ``dissassociation flooding" ou les débordements de la table ARP. Il existe plusieurs catégories de personnes qui peuvent causer des problèmes sur un réseau sans fil:

Les utilisateurs non intentionnels.
Les zones densément peuplées telles que les centres villes et les campus universitaires peuvent conduire à une densité de points d'accès sans fil. Dans ces zones peuplées, il est courant pour les utilisateurs de ordinateurs portables de s'associer accidentellement au mauvais réseau. La plupart des clients sans fil choisiront simplement n'importe quel réseau sans fil disponible, souvent celui qui a le signal le plus fort quand leur réseau préféré n'est pas disponible. L'utilisateur peut alors utiliser ce réseau comme d'habitude, ignorant complètement qu'il peut être en train de transmettre des données sensibles sur le réseau de quelqu'un d'autre. Des personnes malicieuses peuvent même tirer profit de ceci en installant des points d'accès dans des endroits stratégiques pour essayer d'attirer les utilisateurs non avertis et capturer leurs données.
La première étape pour éviter ce type de problème est d'éduquer vos utilisateurs, et souligner l'importance de se connecter uniquement aux réseaux connus et fiables. Beaucoup de clients sans fil peuvent être configurés pour se connecter uniquement aux réseaux fiables, ou pour demander la permission avant de joindre un nouveau réseau. Comme nous le verrons plus loin dans ce chapitre, les utilisateurs peuvent se connecter en toute sécurité à des réseaux publics ouverts en utilisant un encryptage solide.

Wardrivers.
Le phénomène du `` war driving" en anglais tire son nom du film populaire de piratage informatique ``war game" de 1983. Les ``war drivers" sont intéressés à trouver l'emplacement physique des réseaux sans fil. Habituellement, Ils conduisent autour d'une zone donnée avec un ordinateur portable, un GPS et une antenne omnidirectionnelle, enregistrant le nom et l'emplacement de tous les réseaux qu'ils trouvent.
Ces rapports sont ensuite combinés avec les rapports d'autres war drivers pour donner des cartes graphiques localisant toute trace de réseau sans fil d'une ville particulière. La grande wardrivers ne posent probablement pas de menace directe pour les réseaux, mais les données qu'ils collectent pourrait être d'intérêt pour un pirate de réseau. Par exemple, il peut être évident qu'un point d'accès non protégé détecté par un war driver est situé dans un bâtiment sensible, comme un bureau gouvernemental ou un siège social. Une personne malicieuse pourrait utiliser cette information pour accéder illégalement au réseau dans ce bâtiment. Sans doute, un tel point d'accès n'aurait jamais dû être installé en premier lieu, mais le ``war driving" rend le problème d'autant plus urgent. Comme nous le verrons dans ce chapitre, les war drivers qui utilisent le logiciel populaire NetStumbler peuvent être détectés avec des programmes tels que Kismet . pour plus d'd'informations sur le ``war driving", consultez les page web http://wigle.net/, http://www.-nodedb.com/, ou http://www.stumbler.net/.

Points d'accès illicites.
Il existe deux catégories générales de points d'accès illicites: Ceux incorrectement installés par les utilisateurs légitimes, et ceux installés par des personnes malicieuses qui ont l'intention de recueillir des données ou endommager le réseau . Dans le cas le plus simple, un utilisateur légitime du réseau peut vouloir une meilleure couverture sans fil dans son bureau, ou il pourrait trouver des restrictions de sécurité sur le réseau sans fil de l'entreprise trop difficiles à respecter. En installant sans autorisation un point d'accès bon marché, l'utilisateur ouvre le réseau entier à des attaques potentielles de l'intérieur. Même s'il est possible d'identifier les points d'accès non autorisés sur votre réseau câblé, mettre en place une politique claire les interdisant est une première étape très importante. La deuxième catégorie de points d'accès illicites peut être très difficile à traiter. En installant un point d'accès de haute puissance qui utilise le même ESSID qu'un réseau existant, une personne malicieuse peut duper des personnes et les emmener à utiliser leur équipement, et enregistrer ou même manipuler toutes les données qui le

traverse. Encore une fois, si vos utilisateurs sont formés pour utiliser un encryptage solide, ce problème est significativement réduit.

Les écoutes indiscrètes (en anglais eavesdroping).
Comme mentionné précédemment, l'écoute indiscrète est un problème très difficile à traiter dans les réseaux sans fil. En utilisant un outil de surveillance passive (tel que Kismet), un écouteur indiscret peut enregistrer toutes les données du réseau à partir d'une grande distance sans jamais faire connaître sa présence. Les données faiblement encryptées peuvent tout simplement être enregistrées et déchiffrées plus tard, alors que les données non encryptées peuvent être facilement lues en temps réel. Si vous avez des difficultés à convaincre les autres de ce problème, vous pourriez peut-être avoir besoin de démontrer des outils tels que Drifnet (http://www.ex-parrot.com/~chris /driftnet/). Driftnet montres un réseau sans fil pour les données graphiques, tels que les fichiers GIF et JPEG. Pendant que les autres utilisateurs naviguent sur Internet, ces outils affichent tout simplement tous les graphes trouvés dans un collage graphique. Même si vous pouvez dire à un utilisateur que son courriel est vulnérable sans encryptage, rien ne fait mieux passer le message que lui montrer les images qu'il est en train de regarder avec son navigateur Web. Encore une fois, même si elle ne peut pas être complètement évitée, l'application appropriée d'un cryptage solide découragera l'écoute indiscrète.

Protéger le réseau sans fil

Dans un réseau câblé traditionnel, le contrôle d'accès est relativement simple : Si une personne a un accès physique à un ordinateur ou à un concentrateur de réseau, elle peut utiliser (ou abuser) des ressources du réseau. Bien que les mécanismes logiciels soient un élément important de la sécurité de réseau, limiter l'accès physique aux dispositifs du réseau est le mécanisme ultime de contrôle d'accès. Autrement dit, si tous les terminaux et les composantes du réseau sont physiquement accessibles uniquement aux personnes fiables, le réseau peut probablement être fiable. Les règles changent significativement avec les réseaux sans fil. Alors que la portée apparente de votre point d'accès peut sembler être de seulement quelques centaines de mètres, un utilisateur avec une antenne à haut gain peut être en mesure d'utiliser le réseau à une distance de plusieurs pâtés de maison.
Si un utilisateur non autorisé est détecté, il est impossible de simplement ``retracer le câble" à son emplacement.

Sans transmettre un seul paquet, un utilisateur vil suffisamment talentueux peut capturer et enregistrer le trafic sur un réseau sans fil sur un disque. Ces données peuvent plus tard être utilisées pour lancer une attaque plus sophistiquée contre le réseau. Il ne faut jamais supposer que les ondes radio tout simplement "s'arrêtent" au bord de votre propriété, ou à l'intérieur de votre bâtiment. La sécurité physique des réseaux sans fil est limitée à la prévention de la compromission des composants actifs, des câbles et l'alimentation en courant.

Là où l'accès physique au réseau ne peut être empêché, nous devons compter sur des moyens électroniques pour contrôler l'accès à l'infrastructure sans fil en vue de permettre seulement les personnes et les systèmes autorisés à utiliser le réseau sans fil. Mais rappelez-vous que même si un certain degré de contrôle d'accès et d'authentification est nécessaire dans n'importe quel réseau, vous avez échoué dans votre travail si les utilisateurs légitimes ont difficile à utiliser le réseau pour communiquer. Enfin, il n'est généralement pas raisonnable de faire entièrement confiance à tous les utilisateurs du réseau sans fil, mêmement pour les réseaux câblés. Des employés mécontents, les utilisateurs du réseau sans non éduqués, ainsi que des simples erreurs de la part des utilisateurs honnêtes peuvent causer des dommages significatifs aux opérations réseau. En tant qu'architecte de réseau, votre objectif est de faciliter une communication privée entre les utilisateurs légitimes du réseau et entre les utilisateurs et les services légitimes. Il y a un vieux dicton qui dit que la seule façon de sécuriser complètement un ordinateur est de le débrancher, le verrouiller dans un coffre-fort, détruire la clé, et enterrer le tout dans du béton. Alors qu'un tel système pourrait être complètement ``sécurisé", il deviendrait inutile pour la communication. Lorsque vous prenez des décisions en matière de sécurité pour votre réseau, rappelez-vous que pardessus tout, le réseau existe afin que ses utilisateurs puissent communiquer les uns avec les autres. Les considérations de sécurité sont importantes, mais ne devraient pas barrer la route aux utilisateurs du réseau. Une simple règle de pouce pour savoir si oui ou non le réseau est en train de barrer la route à ses utilisateurs consiste à compter combien de temps vous ou les autres travailleurs passent pour aider les gens à se connecter au réseau. Si les utilisateurs réguliers ont à plusieurs reprises des problèmes pour simplement accéder s au réseau, même après qu'ils aient été formés et entraînés sur la façon de le faire, il est possible que les procédures d'accès soient trop encombrantes et leur revue serait en ordre. Prenant tout ceci en compte, notre objectif est de fournir une sécurité physique et un contrôle d'accès adéquats afin de protéger la communication sans sacrifier la facilité d'usage du réseau.

La sécurité physique pour les réseaux sans fil

Lors de l'installation d'un réseau, vous construisez une infrastructure dont les gens dépendent. Des mesures de sécurité existent pour s'assurer que le réseau est fiable. Les réseaux sans fil ont des composantes physiques, telles que des câbles et des boîtiers, qui sont facilement perturbés. Dans des nombreuses installations, les gens ne comprendront pas le but de l'équipement installé, ou la curiosité peut les entraîner à expérimenter. Ils peuvent ne pas réaliser l'importance d'un câble connecté à un port. Quelqu'un peut débrancher un câble Ethernet afin qu'il puisse connecter son ordinateur portable pendant 5 minutes, ou déplacer un interrupteur car il est dans son chemin. Une fiche peut être retirée d'une prise de courant parce que quelqu'un a besoin de cette prise. Assurer la sécurité physique d'une installation est primordial. Les signes et les écriteaux ne seront utiles qu'à ceux qui savent lire votre langue. Placer les choses à l'écart et limiter l'accès est le meilleur moyen d'assurer que les accidents et le tripatouillage ne se produisent pas.

Des attaches et boitiers appropriés peuvent ne pas être facile à trouver dans votre localité. Vous devriez être capable de trouver les fournitures électriques qui fonctionnent tout aussi bien. Les boîtiers de commande sont également faciles à fabriquer et doivent être considérés indispensables à toute installation. Il est souvent rentable de payer un maçon faire des trous et installer les conduits. Le PVC peut être encastré dans les murs en ciment pour le passage du câble d'une pièce à l'autre. Cela évite la nécessité de faire des nouveaux trous à chaque fois qu'un câble doit être passé. Des sachets en plastique peuvent être placés dans le conduit autour des câbles pour l'isolation. L'équipement de petite dimension devrait être monté sur le mur et les grands équipements devrait être mis dans un cabinet ou un coffret.

Les commutateurs

Les commutateurs, les concentrateurs ou les points d'accès d'intérieur peuvent être vissés directement sur un mur à l'aide d'une prise. Il est préférable de mettre cet équipement aussi haut que possible pour réduire le risque que quelqu'un soit en mesure de toucher l'appareil ou ses câbles sans effort significatif.

Les câbles

À tout le moins, les câbles doivent être cachés et attachés. Il est possible de trouver un conduit de câbles en matière plastique qui peut être utilisé dans

des bâtiments. Si vous ne pouvez pas le trouver, les attaches de câbles simples peuvent être clouées au mur pour fixer le câble. Cela permettra de s'assurer que le câble ne traîne pas là où il peut être accroché (en anglais snagged), pincé ou coupé. Lors de la fixation du câble au mur, il est important de ne pas clouer ou visser dans le câble lui-même. Le câble contient de nombreux fils minuscules sur lesquels les données du réseau traversent. Clouer à travers le câble l'endommagera et le rendre inutile pour transmettre des données.
Veillez également à ne pas trop plier ou tordre le câble car cela pourrait aussi bien l'endommager. Il est préférable d'enfouir les câbles, plutôt que les laisser traîner dans la cour. Les câbles traînant peuvent être utilisés pour le séchage des vêtements, ou peuvent être accrochés par une échelle, etc. Pour éviter la vermine et les insectes, utilisez un conduit électrique en plastique. La mince dépense vaudra bien le cout des ennuis. Le conduit doit être enterré à environ 30 cm de profondeur, ou en dessous du niveau de la glace dans les climats froids. Ça vaut la peine de faire un investissement supplémentaire d'acheter un conduit plus grand que nécessaire à y placer des câbles futurs. Considérez l'étiquetage du câble enfui dans la terre avec un signe ``appeler avant de creuser'' pour éviter des futures pannes accidentelles.

Alimentation

Il est préférable d'avoir des barres d'alimentation enfermées a clef dans un coffret. Si cela n'est pas possible, placez la barre d'alimentation sous un bureau ou sur le mur et utilisez un ruban adhésif (ou Ruban gaffer, un ruban adhésif fort) pour sécuriser la fiche dans le réceptacle. Ne laissez pas de récipients vides sur l'onduleur et la barre d'alimentation. Au besoin couvrez les avec du ruban adhésif. Comme les gens ont tendance à utiliser le réceptacle plus accessible, rendez ceux-ci qui sont critiques difficile à utiliser. Si vous ne le faites pas, vous pourrait trouver un ventilateur ou la lumière branché sur votre onduleur ; même s'il est agréable d'avoir la lumière, il est plus agréable de garder votre serveur opérationnel.

L'eau

Protégez votre équipement contre l'eau et de l'humidité. Dans tous les cas, assurez-vous que votre équipement, y compris votre onduleur est à au moins 30 cm du sol, pour éviter les dommages causés par l'inondation. Aussi essayer d'avoir un toit au-dessus de votre équipement, pour éviter la pénétration de l'eau et l'humidité.

Dans des climats humides, il est important que l'équipement aie une bonne ventilation en vue de s'assurer que l'humidité soit évitée. Les petits cabinets ont besoin d'avoir de ventilation, sinon l'humidité et la chaleur peuvent dégrader ou endommager votre équipement.

Les mâts

L'équipement installé sur un mât est souvent à l'abri des voleurs. Néanmoins, afin de dissuader les voleurs et de protéger votre équipement contre les vents, il est bon d'aller au-delà des mesures d'ingénierie des montures. Peindre l'équipement en blanc terne ou gris permet de refléter le soleil et le fait apparaître simple et sans intérêt. Les antennes panneaux sont souvent préférés car elles sont beaucoup plus subtils e et moins intéressantes que les paraboles.
Toute installation murale devrait être suffisamment élevée pour exiger une échelle pour l'atteindre. Essayez de choisir des endroits bien éclairés, mais pas des endroits proéminents pour placer l'équipement. Aussi, évitez des antennes qui ressemblent à des antennes de télévision, car ce sont des éléments qui attireront l'intérêt des voleurs alors qu'une antenne wifi sera inutile au plus commun des voleurs.

L'authentification et le contrôle d'accès

En parlant d'authentification, un certain nombre de termes connexes comme identité (numérique), autorisation, intimité, etc. surgissent. Donc, avant d'entrer dans l'authentification propre, nous devons introduire une certaine terminologie, sans chercher à être exhaustif. L'identité numérique est l'entité électronique qui est une représentation d'une entité physique, comme une personne ou un dispositif.
L'authentification est le processus de vérification de l'affirmation selon laquelle une entité (électronique) est autorisée à agir au nom d'une entité (physique) donnée connue. En d'autres termes, l'authentification est le processus de prouver que l'entité physique correspond à une certain entité électronique. L'autorisation, à son tour, est le processus d'établissement des droits de l'identité pour accéder à certaines ressources ou à effectuer certaines tâches.
Finalement, la confidentialité est une question complexe. Elle a à voir avec le droit d'une personne de ne pas avoir ses données personnelles et son comportement connus par des partis qui n'en ont pas strictement besoin pour fournir le service demandé par les utilisateurs.

Ainsi, par exemple, il est raisonnable pour un magasin de liqueur de savoir que le client est au-dessus d'un certain âge avant de lui vendre des boissons alcoolisées, mais pas de connaître le nom du client, et des tierces personnes ne devraient avoir aucune connaissance de la transaction du tout. La confidentialité est particulièrement préoccupante dans un monde dans lequel les utilisateurs utilisent de plus en plus des réseaux et des services en dehors de leur milieu familial. Sans payer une attention appropriée aux aspects de la confidentialité, il est trop facile de tracer le comportement et le mouvement d'utilisateurs. Il est à noter qu'il existe une balance entre l'authentification et la confidentialité. La vérification de l'identité d'un utilisateur en elle-même envahit la confidentialité de l'utilisateur. La partie authentifiant connait qui utilise cette ressource à un moment et un endroit donné, mais le défi est de minimiser la quantité d'informations sur un utilisateur et le nombre de parties qui sont au courant de cette information. Dans le cadre de ce livre, nous sommes principalement intéressés par les techniques de contrôle d'accès au réseau. En d'autres termes, nous voulons être en mesure de décider qui (identité authentifiée) arrive à accéder à quoi (autorisation) sans sacrifier la confidentialité. L'authentification se fait généralement par la preuve de la connaissance d'un secret (un mot de passe, une signature), la possession d'un jeton ou d'une caractéristique (un certificat, un empreinte digitale) ou les deux. Le contrôle d'accès est souvent nécessaire pour s'assurer que seuls les utilisateurs autorisés peuvent utiliser le réseau afin d'éviter l'épuisement des ressources rares et/ou pour le respect des règles et règlements.

En plus des réseaux d'accès contrôlé, il peut aussi y avoir des réseaux ouverts avec un accès limité ou pour un temps limité. Mais en raison de la nécessité pour les organisations de contrôler l'accès à leurs ressources limitées et aussi des lois anti- terroristes, ils deviennent moins omniprésents. Au fil des années, un certain nombre de techniques ont été utilisées pour contrôler l'accès à des réseaux sans fil. Par la suite, elles ont été pour la plupart abandonnées en raison de problèmes de sécurité ou d'évolutivité comme le WiFi est devenu de plus en plus populaire.

Filtrage Mac

L'accès à un réseau Wi-Fi peut être basé sur l'adresse MAC. C'est le nombre de 48 bits attribué par le fabricant à chaque dispositif sans fil et Ethernet, et qui est censé être unique et persistant. En utilisant le filtrage mac sur nos points d'accès, nous pouvons authentifier les utilisateurs en fonction de leur adresse MAC.

Par cette fonction, le point d'accès garde une table interne d'adresses MAC approuvées. Quand un utilisateur sans fil tente de s'associer au point d'accès, l'adresse MAC du client doit être dans la liste approuvée, sinon l'association sera refusée. Alternativement, le point d'accès peut conserver une table d'adresses MAC connues ``mauvaises", et permettre tous les dispositifs qui ne sont pas sur la liste.
Malheureusement, ceci n'est pas un mécanisme de sécurité idéal. Maintenir les tables MAC sur chaque dispositif peut être encombrant, exigeant de tous les dispositifs clients d'avoir leurs adresses MAC enregistrées et téléchargées aux points d'accès. Pire encore, les adresses MAC peuvent souvent être modifiées dans le logiciel.
En observant les adresses MAC utilisées sur un réseau sans fil, un attaquant déterminé peut usurper l'identité d'une adresse MAC approuvée et s'associer avec succès au point d'accès.
Alors que le filtrage MAC empêche les utilisateurs non intentionnels et même des individus les plus curieux d'accéder au réseau, le filtrage MAC seul ne peut pas empêcher les attaques de pirates déterminés. Les filtres MAC sont utiles pour limiter temporairement l'accès aux clients de mauvaise conduite. Par exemple, si un ordinateur portable a un virus qui envoie de grandes quantités de spam ou autre trafic, son adresse MAC peut être ajoutée à la table de filtrage pour arrêter le trafic immédiatement. Ceci peut faire gagner du temps pour traquer l'utilisateur et fixer le problème.

Réseaux fermés

Le mode appelé réseau fermé est une autre ``caractéristique d'authentification '' des réseaux WiFi qui fut populaire à un moment donné. Dans un réseau typique, Les points d'accès diffuseront leur ESSID plusieurs fois par seconde, permettant aux clients sans fil (ainsi que des outils tels que NetStumbler) de trouver le réseau et indiquer sa présence à l'utilisateur. Dans un réseau fermé, le point d'accès (AP) ne balise pas l'ESSID (``ESSID caché"), et les utilisateurs doivent connaître le nom complet du réseau avant que l'AP permette l'association. Cela empêche les utilisateurs occasionnels de découvrir le réseau et le sélectionner dans leur client sans fil . Il y a un certain nombre d'inconvénients à cette fonction. Forcer les utilisateurs à taper l'ESSID complet avant la connexion au réseau est sujet aux erreurs et conduit souvent à des appels de support et des plaintes. Puisque le réseau n'est évidemment pas présent dans les outils d'étude de site comme NetStumbler, cela peut empêcher vos réseaux d'apparaître sur les ``war driving" cartes.

Mais cela signifie aussi que d'autres constructeurs de réseau ne peuvent pas aussi trouver votre réseau facilement votre réseau, et en particulier ne sauront pas que vous utilisez déjà un canal donné.
Un voisin consciencieux peut effectuer une étude de site, trouver qu'il n y a pas de réseaux à proximité, et installer son propre réseau sur le même canal que vous utilisez. Cela entraînera des problèmes d'interférence à la fois pour vous et votre voisin.
Enfin, l'utilisation des réseaux fermés n'ajoute finalement que peu à votre sécurité globale du réseau. En utilisant des outils de surveillance passive (comme Kismet), un utilisateur malveillant peut détecter les trames envoyées de vos clients légitimes à l'AP.
Ces trames contiennent nécessairement le nom du réseau.
L'utilisateur malveillant peut alors utiliser ce nom pour s'associer au point d'accès, comme un utilisateur normal le ferait.
L'encryptage est probablement le meilleur outil dont nous disposons pour authentifier les utilisateurs sans fil. Grâce à un cryptage solide, nous pouvons identifier de manière unique un utilisateur d'une manière qui est très difficile à falsifier, et ensuite utiliser cette identité pour déterminer l'accès au réseau. Le cryptage a également l'avantage l'ajout d'une couche de confidentialité en empêchant les écoutes indiscrètes d'observer le trafic réseau facilement. Le cryptage est la technique qui est utilisée pour authentifier des utilisateurs dans la plupart des déploiements actuels.

WEP

La première méthode de cryptage largement utilisée sur les réseaux WiFi était le cryptage WEP. WEP est l'acronyme de Wired Equivalent Privacy, et est supporté par la quasi-totalité des équipements 802.11a/b/g . Incidemment, c'est un abus de langage complet car la confidentialité que le WEP fournit n'est en aucune façon équivalente à celle des connexions câblées. WEP utilise une clé de 40 bits partagé pour crypter les données entre le point d'accès et le client. La clé doit être introduite dans les APs ainsi que dans chacun des clients.
Avec WEP activé, les clients sans fil ne peuvent pas s'associer avec le point d'accès jusqu'à ce qu'ils utilisent la bonne clé.
Un écouteur indiscret espionnant un réseau WEP activé saura toujours voir le trafic et les adresses MAC, mais la partie donnée(en anglais payload) de chaque paquet est crypté. Cela a fourni un mécanisme d'authentification tout en ajoutant un peu de confidentialité sur le réseau. WEP n'est définitivement pas la solution de cryptage la plus puissante disponible.

Pour une chose, la clé WEP est partagée entre tous les utilisateurs.
Si la clé est compromise (par exemple, si un utilisateur dit un ami ce que le mot de passe est, ou si un employé est chassé du travail) changer le mot de passe peut être très difficile car tous les points d'accès et périphériques clients ont besoin d'être changé.
Ceci aussi signifie aussi que les utilisateurs légitimes du réseau peuvent encore espionner le trafic des autres car ils connaissent tous la clé partagée.
La clé elle-même est souvent mal choisie, rendant les tentatives de craquage hors ligne possibles.
Mais le plus important est que le WEP lui-même est cassé, permettant un accès illégal au réseau très facile. Donc WEP ne devrait plus être utilisé.

Pour plus de détails sur l'encryptage WEP, voir ces documents :
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
http://www.cs.umd.edu/ ~ waa / wireless.pdf

Réseaux sans fil " commutés "

Une différence essentielle entre les réseaux Ethernet commutés modernes et le sans-fil est que les réseaux sans fil sont construits sur un support partagé.
Ils ressemblent davantage aux anciens concentrateurs de réseau qu'aux commutateurs modernes, par le fait que chaque ordinateur connecté au réseau peut ``voir" le trafic de tous les autres utilisateurs.
Pour surveiller tout le trafic réseau sur un point d'accès, on peut simplement se mettre sur le canal utilisé, mettre la carte réseau en mode moniteur, et enregistrer chaque trame de données.
Ces données peuvent être directement utiles pour un écouteur indiscret (y compris les données telles que le courrier électronique, les données vocales, ou l'historique des conversations en ligne).
Elles peuvent également fournir des mots de passe et d'autres données sensibles, permettant ainsi de compromettre le réseau d'avantage.
Le WPA et le 802.1X sont conçus pour faire que le réseau sans fil se comporte comme un réseau commuté plutôt qu'un réseau partagé.

WPA

Le WiFi Protected Access ou WPA est un autre protocole d'authentification de couche liaison de données. WPA a été créé spécifiquement pour adresser les problèmes connus du WEP mentionné précédemment.
WPA a été conçu pour être une solution compatible provisoire pendant que la norme 802.11i complète (WPA2) était en développement.

WPA et WPA2 peuvent fonctionner sous le parapluie de la norme 802.1X pour l'authentification sans fil (voir ci-dessous), mais aussi beaucoup dans le même mode que le WEP, avec une clé partagée entre tous les clients et l'AP, dénommé le mode Pre Shared Key (PSK) (l'alliance WiFi appelle le WPA-PSK au nom de ``WPA Personal" à l'opposé de ``WPA Enterprise" qui est utilisé en combinaison avec le 802.1X).
Dans l'ensemble, WPA fournit une authentification et une confidentialité significativement meilleures que le WEP standard, principalement en s'appuyant sur la Temporary Key Integrity Protocol (TKIP) qui continuellement et automatiquement change le cryptage entre les clients et les points d'accès.

Malheureusement précisément la compatibilité ascendante de TKIP a donné lieu à certains vecteurs d'attaque contre le TKIP permettant de décrypter certains paquets cryptés, qui à leur tour peuvent être manipulés pour d'autres attaques.
Plus d'informations peuvent être trouvées dans les articles suivants :
http://dl.aircrack -ng.org/breakingwepandwpa.pdf
http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf
La conséquence de ces découvertes est qu'il est sage de passer à la prochaine génération de protocoles d'accès WiFi sécurisé : WPA2.

WPA2-PSK

WPA2 est la norme IEEE 802.11i complète. La principale différence avec le WPA est l'utilisation du Advanced Encryption System (AES) au lieu de TKIP ; une norme de cryptage qui (jusqu'à présent) n'a pas été brisée. Ainsi, l'utilisation de WPA2 avec AES peut être considéré comme fiable pour l'instant!

Résumé

L'inconvénient majeur de chacune de ces trois dernières méthodes d'authentification est que, quel que soit le niveau de cryptage, elles sont encore construites sur la notion de secret commun partagé entre tous les clients et le point d'accès. EIles ne permettent pas d'identifier les utilisateurs individuels et en toute franchise, un secret partagé par potentiellement des dizaines de milliers d'utilisateurs peut difficilement être considéré comme un secret. Un autre problème sérieux avec les réseaux sans fil dont l'accès est contrôlé par l'une des méthodes mentionnées, est que ses utilisateurs sont relativement anonymes.

S'il est vrai que chaque dispositif sans fil comprend une adresse MAC unique qui est fournie par le fabricant, comme mentionné plus tôt, ces adresses MAC peuvent souvent être modifiées par logiciel. Et même si l'adresse MAC est connue, il peut être très difficile de localiser où un utilisateur sans fil se trouve physiquement. Les effets multi-trajets, des antennes à gain élevé, et des caractéristiques très variables de l'émetteur radio, il peut être impossible de déterminer si un utilisateur sans fil est assis dans la chambre à côté ou s'il se trouve dans un immeuble d'appartements à une distance d'un mile. Les préoccupations concernant la sécurité, la responsabilisation et l'évolutivité ont conduit à la montée de ce qu'on appelle communément le réseautage basé sur l'identité.

Réseautage basé sur l'identité

En réseautage basé sur l'identité, des utilisateurs individuels sont authentifiés plutôt que de secrets partagés entre plusieurs utilisateurs. Généralement, le système d'authentification vérifie les informations d'identification utilisateur contre une sorte de base de données ou un répertoire d'entreprise. Communément en utilisant le protocole RADIUS, un protocole conçu à l'origine pour contrôler l'accès à des pools de modems dial-in mais suffisamment polyvalent pour servir comme un protocole de contrôle d'accès générique pour l'accès au réseau.

Les portails captifs

Un outil d'authentification couramment utilisé sur les réseaux sans fil est le portail captif . Un portail captif utilise un navigateur Web standard pour donner à un utilisateur sans fil l'occasion de présenter son accréditation pour l'ouverture de la session. Il peut également être utilisé pour présenter des informations (comme une politique d'utilisation acceptable) à l'utilisateur avant d'accorder l'accès total (d'avantage d'accès). En utilisant un navigateur Web au lieu d'un programme personnalisé pour l'authentification, les portails captifs fonctionnent avec pratiquement tous les ordinateurs portables et systèmes d'exploitation. Les portails captifs sont généralement utilisés sur des réseaux ouverts sans d'autres méthodes d'authentification (tels que les filtres WEP ou MAC). Pour commencer, un utilisateur sans fil ouvre le navigateur web de son ordinateur portable qui le dirige vers le portail. Il est ensuite invité à accepter la politique d'utilisation ou répondre à d'autres questions telles que la saisie d'un nom d'utilisateur et mot de passe, et cliquez sur un bouton " login", ou peut-être taper des chiffres d'un ticket prépayé.

L'utilisateur entre ses informations d'identification, qui sont vérifiés par le point d'accès ou un autre serveur sur le réseau.
Tout autre accès au réseau est bloqué jusqu'à ce que ces informations d'accès soient vérifiées. Après vérification, l'ordinateur portable de l'utilisateur recevra un bail DHCP.
Ils peuvent ensuite utiliser leur navigateur Web pour aller sur n'importe quel site sur Internet.

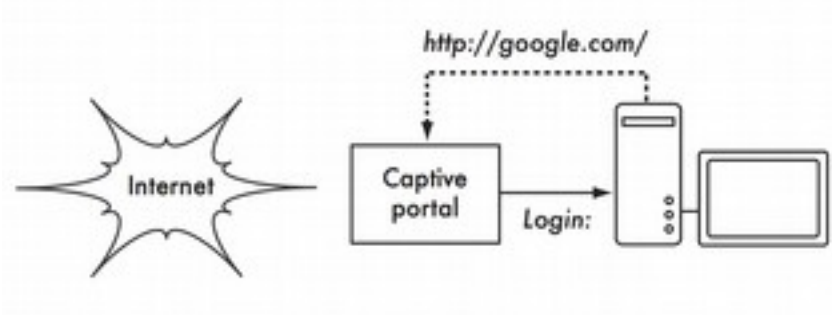


Figure SWN 1 : L'utilisateur demande une page Web et est redirigé.

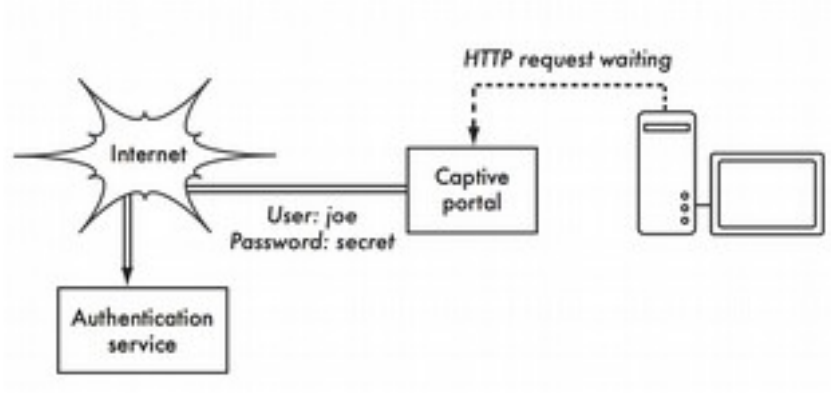


Figure SWN 2 : les informations d'identification de l'utilisateur sont vérifiées avant qu'un accès total soit accordé. Le serveur d'authentification peut être le point d'accès lui-même, une autre machine sur le réseau local ou sur un serveur n'importe où sur Internet.

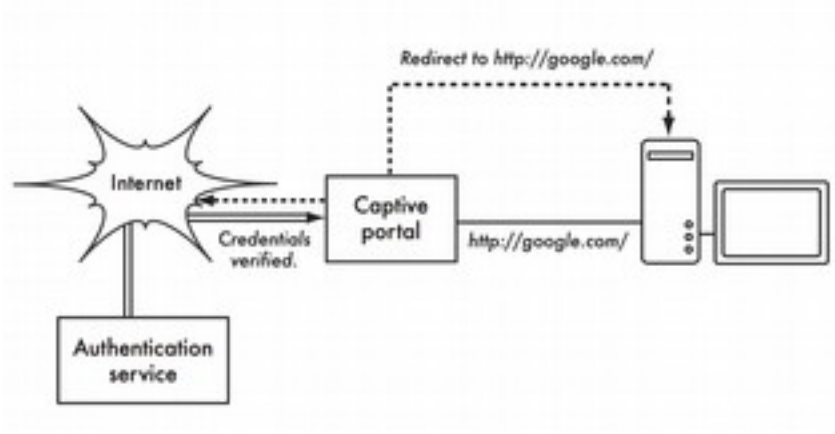


Figure SWN 3 : Après l'authentification, l'utilisateur est autorisé à accéder au reste du le réseau et est généralement redirigé vers le site d'origine demandé - dans ce cas Google.

Les portails captifs ne fournissent aucun cryptage pour les utilisateurs sans fil. Plutôt en s'appuyant sur l'adresse MAC et IP du client comme un identifiant unique, qui peut être usurpé facilement, de nombreuses implémentations exigeront de l'utilisateur de garder ouverte une fenêtre flottante ou pop-up du navigateur.

Comme similairement à la sécurité basée MAC ou WEP, les portails captifs ne fournissent pas de protection contre l'écoute indiscrète (ils utilisent un support partagé) et sont vulnérables aux détournements de session, les portails captifs ne sont pas un très bon choix pour les réseaux qui doivent être verrouillés pour ne permettre l'accès qu'à des utilisateurs fiables. Ils sont beaucoup plus adaptés aux cafés, hôtels et autres lieux d'accès public utilisés par usagers occasionnels.

Un autre inconvénient des portails captifs est qu'ils reposent sur l'utilisation d'un navigateur pour l'authentification. Ceci peut être très contre-intuitif pour les utilisateurs qui tentent simplement de vérifier leur e-mail ou envoyer un message instantané, pour ne pas mentionner le fait que beaucoup de dispositifs sans fil tels que des capteurs, des imprimantes et des caméras n'ont pas un navigateur intégré. Dans les paramètres de réseaux publics ou semi- publics, les techniques de cryptage telles que WEP et WPA sont effectivement inutiles. Il n'y a tout simplement aucun moyen de distribuer des clés publiques ou partagées aux membres du grand public sans compromettre la sécurité de ces clés.

Dans ces situations, une application simple comme un portail captif fournira un niveau de service qui se trouve quelque part entre un service complètement ouvert et un service complètement fermé.

De nombreux vendeurs et les projets open source existent qui fournissent les fonctionnalités de portail captif, pour n'en nommer que quelques-uns:

- CoovaChilli, CoovaAP (http://coova.org/CoovaChilli/), Coova est le successeur du projet Chillispot qui n'est plus activement maintenu. Coova permet l'utilisation d'une authentification RADIUS dans le back-end.
- WiFidog (http://www.wi0dog.org/), WiFi Dog offre un ensemble très complet d'authentification de portail captif dans très peu d'espace (généralement sous 30kb). Du point de vue utilisateur, il ne nécessite pas de pop-up ou le support du javascript, ce qui lui permet de fonctionner sur une plus grande variété de dispositifs sans fil .
- M0n0wall, pfSense (http://m0n0.ch/wall/), m0n0wall est un système d'exploitation embarqué complet basé sur FreeBSD. Il comprend un portail captif avec support RADIUS, ainsi que d'un serveur web PHP.
-

De nombreux fournisseurs généraux de réseautage offrent une certaine forme de portails captifs intégrés, par exemple, Microtik, Cisco, Aruba, Aptilo.

802.1X

En entreprise et dans les déploiements campus, le modèle le plus courant d'authentification du réseau sans fil est celui basé sur le IEEE 802.1X.
Le 802.1X est un protocole de couche 2 qui peut être utilisé à la fois pour l'authentification du réseau câblé et du sans fil et en fait comporte un certain nombre de technologies.
Le 802.1X décrit l'interaction entre le dispositif client (suppliant 802.1X) et le point d'accès ou un commutateur (authentificateur) ainsi que celle entre le Point d'accès ou le commutateur et un serveur RADIUS backend (serveur d'authentification) qui vérifie à son tour les accréditations (en anglais credentials?) de l'utilisateur contre un annuaire d'entreprise (ou fichier plat d'ailleurs).

Enfin, le 802.1X décrit comment transporter les informations d'identification (accréditations) du suppliant au serveur d'authentification de façon transparente jusqu'à l'authentificateur ou de tout autre dispositif dans la voie en s'appuyant sur l'Extensible Authentication Protocol (EAP).
Le cryptage entre le suppliant et l'authentificateur peut être fait en utilisant des clés WEP rotatives, WPA avec TKIP ou WPA2 avec AES.

Pour les raisons mentionnées dans le paragraphe sur le WEP, WPA-PSK et WPA2-PSK, la combinaison WPA2 avec AES est fortement recommandée.

Probablement la caractéristique la plus intéressante du 802.1X est l'utilisation d' EAP. L'EAP définit une manière générique pur encapsuler les informations d'identification et de les transporter d'un suppliant (logiciel client) à un serveur d'authentification (serveur RADIUS).
Les méthodes dites EAP définissent comment les méthodes d'authentification spécifiques peuvent être encapsulées dans EAP.
Il existe des méthodes EAP pour tous types courants de méthodes d'authentification tels que les certificats, les cartes SIM, le nom d'utilisateur/mot de passe, mots de passe uniques et jetons matériels.
A cause des problèmes de clés ou de distribution de jetons lors de la distribution des jetons ou des certificats et leur révocation, la grande majorité des déploiements à grande échelle utilisent ce qu'on appelle les méthodes EAP tunnellisées : authentification par nom d'utilisateur/mot de passe en utilisant un tunnel TLS pour le serveur d'authentification à travers lequel le nom d'utilisateur réel et mot de passe sont transmis.
L'identité de l'utilisateur utilisé pour l'enveloppe TLS (TLS-enveloppe) est généralement de forme anonymous@domain (c'est ce qu'on appelle l'identité extérieure), tandis que l'identité interne (à l'intérieur du tunnel TLS) est de la forme username@domain.
Cette distinction est particulièrement intéressante pour l'itinérance (en anglais roaming) à d'autres réseaux d'organisations.

Il est possible de transporter les informations d'authentification d'un utilisateur sur Internet tout en révélant seulement son organisation mère (la partie domaine), mais ceci est le sujet du paragraphe suivant.
Donc ce qui se passe dans une authentification 802.1X typique avec une méthode EAP- tunnellisée est le suivant:

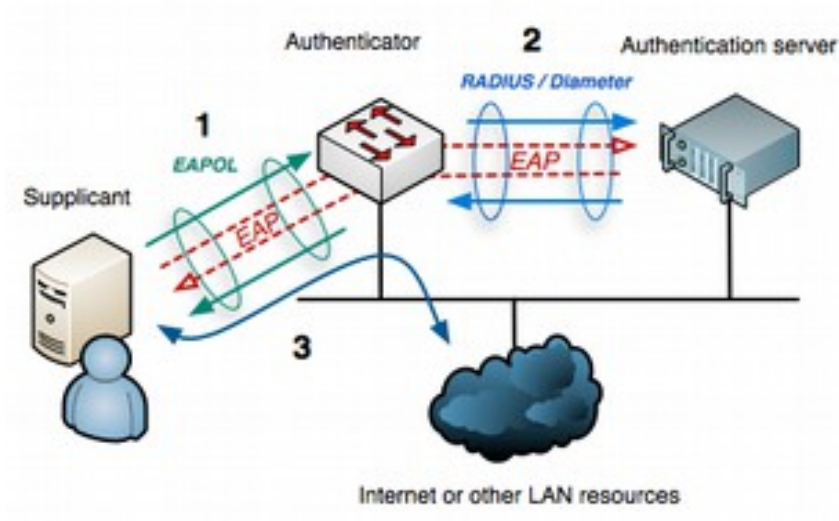


Figure SWN 4 : L'utilisation de 802.1X avec EAP tunnellisé pour l'accès au réseau (avec la courtoisie de SURFnet)

Les clients associés avec le point d'accès (authentificateur).
Le point d'accès demande du client (suppliant) de s'authentifier.
Le client envoie un message EAP contenant un paquet TLS avec une identité externe anonymous@domain et à l'intérieur du paquet TLS username @domain et le mot de passe pour le point d'accès sur la liaison 802.11(EAP over LAN ou EAPoL).
Le point d'accès reçoit le message EAP, l'encapsule dans RADIUS et l'envoie au serveur RADIUS de l'organisation (serveur d'authentification) .
Le serveur RADIUS décapsule le message EAP et vérifie les informations d'identification utilisateur contre une sorte de backend comme un fichier plat, un LDAP directory, un Active Directory ou quelque chose d'autre.
Si les informations d'identification sont valides, le serveur RADIUS renvoie un message d'acceptation d'accès RADIUS au point d'accès. Le point d'accès donne au client l'accès au réseau local sans fil. Le client effectue une demande DHCP, obtient une adresse IP et il est connecté au réseau. Il y a un certain nombre de méthodes EAP tunnelisées qui fonctionnent essentiellement de la même façon. Les différences sont dans le support de systèmes d'exploitation, la vulnérabilité au dictionnaire et aux attaques de type man-in -the-middle et si elles nécessitent un stockage de mots de passe en plein texte dans le backend.

Les méthodes EAP les plus largement déployées aujourd'hui sont les EAP-TTLS (EAP Tunnelled Transport Layer Security) et PEAP (Protected EAP). Il y a eu des implémentations incompatibles de PEAP en raison de désaccords entre les partisans du PEAP (Apple, Cisco et Microsoft) résultant en un grande absorption de TTLS.
Le fait que ces incompatibilités sont en grande partie résolues et le manque de support natif pour le TTLS dans un certain nombre de systèmes d'exploitation courants (variantes d'Apple iOS et MS Windows) ont entraîné une augmentation de l'absorption de PEAP. L'EAP-FAST est une méthode EAP récente qui gagne du terrain est en raison de ses propriétés de sécurité. L'EAP-FAST a également été choisie comme base pour la nouvelle méthode EAP tunnellissee (TEAP) qui va être développée et que l'IETF s'attend à être la seule a être approuvée.

Itinérance inter-organisationnelle

Une propriété intéressante de RADIUS est que ses messages peuvent être proxy vers d'autres serveurs RADIUS. Cela signifie qu'il est possible pour une organisation de permettre à chacun des utilisateurs d'accéder au réseau en authentifiant au serveur RADIUS de son organisme d'attache.
Lorsque le serveur RADIUS de l'organisation A reçoit une demande d'authentification venant d'anonymous@organisationB.org, il peut transmettre la demande au serveur RADIUS de l'organisation B au lieu de vérifier les informations d'identification localement.
Le serveur RADIUS de l'organisation B à son tour peut vérifier les informations d'identification et envoyer de l'acceptation d'accès en retour au serveur RADIUS de l'organisation A indiquant alors au point d'accès de permettre l'accès à l'utilisateur. Ce soi-disant accès fédéré permet la création de déploiements très larges et évolutives tout en permettant en même temps les différentes organisations d'appliquer leurs propres politiques d'authentification pour leurs utilisateurs.
Alors que le proxying RADIUS est certainement possible dans les déploiements portail captif, il brille définitivement dans un environnement 802.1X/EAP. En utilisant EAP, les informations d'identification peuvent être protégées de façon que seule l'organisation mère de l'utilisateur soit en mesure de les voir.
De cette façon, les grands déploiements peut être faits sans la fuite des informations d'identification et sans avoir à enseigner aux utilisateurs d'entrer leurs informations d'identification secrets dans chaque site Web qu'ils trouvent en face d'eux.

A titre d'exemple, eduroam, la fédération d'accès sans fil itinérante dans l'éducation, qui au lieu d'avoir des connexions RADIUS directs entre les organisations, étend le concept ci-dessus légèrement en construisant un système hiérarchique de serveurs nationaux et internationaux RADIUS, permettant à des millions d'étudiants d'avoir accès à plus de 5000 réseaux de campus dans de nombreux pays sur tous les continents à l'exception de l'Antarctique.

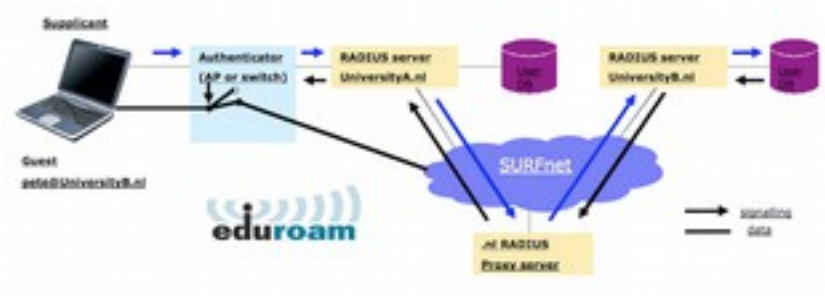


Figure SWN 5 : L'infrastructure eduroam pour l'itinérance à l'échelle mondiale dans le milieu universitaire.

Encryptage de bout en bout

Il convient de noter que, alors que WEP, WPA-PSK et WPA2-PSK utilisent des techniques de cryptage pour fournir un contrôle d'accès et protéger contre l'écoute indiscrète, ils ne protègent que le trafic sans fil entre le client et le point d'accès, pas sur la partie câblée de la voie de communication. Afin de protéger la communication contre toute manipulation intempestive ou l'écoute clandestine, le cryptage de bout en bout est nécessaire. La plupart des utilisateurs sont parfaitement inconscients que leur email privé, conversations chat, et même les mots de passe sont souvent envoyés ``en clair" sur des dizaines de réseaux non fiables avant d'arriver à leur destination finale sur l'Internet. Cependant aussi erronés qu'ils soient, les utilisateurs espèrent encore généralement une confidentialité lors de l'utilisation des réseaux informatiques. La confidentialité est possible même sur des réseaux non sécurisés tels que les points d'accès publics et de l'Internet. La seule méthode efficace éprouvée pour protéger la confidentialité est l'utilisation d'un cryptage solide de bout en bout. Ces techniques fonctionnent bien, même sur réseaux publics non sécurisés, où les écouteurs indiscrets sont à l'écoute et peut-être même manipulent des données en provenance

d'un point d'accès. Pour assurer la confidentialité des données, un bon encryptage de bout en bout doit fournir les fonctionnalités suivantes:

Authentification vérifiée de l'extrémité distante.
L'utilisateur doit être en mesure de savoir sans aucun doute que l'extrémité distante est bien celle qu'elle prétend être. Sans authentification, un utilisateur pourrait fournir des données sensibles à toute personne qui prétend être le service légitime.

Méthodes d'encryptage fort.
L'algorithme d'encryptage doit résister à un test public, et ne doit pas être facilement décryptable par un tiers. Il n'y a pas de sécurité dans l'obscurité, et un encryptage solide est encore plus fort lorsque l'algorithme est largement connu et soumis à une revue par des pairs.
Un bon algorithme avec une clé suffisamment large et protégée peut fournir un encryptage qui est peu susceptible d'être brisé par aucun effort pendant note existence en utilisant la technologie actuelle. Méfiez-vous des vendeurs de produits qui vous assurent que leur cryptage propriétaire utilisant des algorithmes de secrets commerciaux sont mieux que les algorithmes ouverts testés par des pairs.

Cryptographie à clé publique.
Bien que n'étant pas une exigence absolue pour le cryptage de bout-à-bout, l'utilisation de la cryptographie à clé publique à la place d'une clé partagée peut faire en sorte que les données d'un individu restent privées, même si la clé d'un autre utilisateur du service est compromise. Elle résout également certains problèmes liés à la distribution des clés aux utilisateurs sur des réseaux non sécurisés.

Encapsulation des données.
Un bon mécanisme de cryptage de bout-à-bout protège autant des données que possible. Cela peut aller de l'encryptage d'une transaction électronique unique à l'encapsulation du trafic IP, y compris les recherches DNS et d'autres protocoles. Certains outils de cryptage offrent simplement un canal sécurisé que d'autres applications peuvent utiliser. Cela permet aux utilisateurs d'exécuter n'importe quel programme qu'ils aimeraient tout en jouissant de la protection d'un cryptage solide, même si les programmes eux-mêmes ne le supportent pas. Soyez conscients que les lois concernant l'utilisation du cryptage varient considérablement d'un endroit à l'autre.

Certains pays traitent le cryptage comme des munitions, et peuvent exiger un permis, séquestrer des clés privées, ou même interdire complètement leur utilisation. Avant d'implémenter toute solution qui implique l'encryptage, assurez-vous de vérifier que l'utilisation de cette technologie est autorisée dans votre région.
Dans les sections suivantes, nous allons jeter un œil sur quelques outils spécifiques qui peuvent fournir une bonne protection pour les données de vos utilisateurs.

TLS

La technologie d'encryptage de bout-à-bout la plus largement disponible est le Transport Layer Security, connu simplement comme TLS (ou son prédécesseur SSL: Secure Sockets Layer). Intégré dans pratiquement tous les navigateurs web et des nombreuses autres applications, TLS utilise la cryptographie à clé publique et une clé publique d'infrastructure fiable (PKI) pour sécuriser les communications de données sur le web.
Chaque fois que vous visitez un URL Web qui commence par https, vous utilisez TLS. L'implémentation TLS qui est intégrée dans les navigateurs Web comprend une collection de certificats d'organisations appelé les autorités de certification (en anglais Certificate Authorities CA). Un CA valide l'identité des utilisateurs réseau et/ou les fournisseurs de service et assure qu'ils sont ce qu'ils prétendent être et délivre un certificat pour ainsi dire. Plutôt que de réaliser ceci par un document de fantaisie signé approprié pour l'encadrement mural, cela se fait à travers l'échange de clés cryptographiques. Par exemple, quelqu'un qui veut un certificat pour son site Web soumet une demande de certificat (en anglais Cerificate Request CR), encodé (``signé") avec une clé cryptographique spécifiquement créée pour la signature de la demande de certificat. Il soumet cette demande à l'autorité compétente, qui alors ``signe" la demande avec sa propre clé. Ceux-ci sont encodés dans le certificat avec le nom exact
du site pour lequel le demandeur veut que le certificat soit valide. Par exemple du point de vue du certificat, WWW.AIPOTU.GOV n'est pas le même qu'AIPOTU.GOV. Chaque site nécessiterait son propre certificat à présenter à un navigateur pour effectuer des transactions HTTPS authentifiés. Si le propriétaire du domine AIPOTU.GOV a seulement un certificat délivré pour AIPOTU.GOV et pas aussi WWW.AIPOTU.GOV, un utilisateur accédant à l'adresse ``WWW" recevra un avertissement pour un certificat non valide pour ce site.
Cela peut être déroutant pour certains utilisateurs et, au fil du temps, les

emmener à espérer des avertissements des certificats TLS venant de leur navigateur comme normaux quand la vérité est tout à fait l'opposée. Lorsque vous accédez à un site Web qui utilise TLS, le navigateur et le serveur échangent premièrement des certificats. Le navigateur vérifie ensuite que le certificat fourni correspond au nom DNS de l'ordinateur que le navigateur connait être le serveur, que le certificat n'a pas expiré ou a été révoqué et qu'il a été signé par une autorité de certification de confiance. Le serveur vérifie optionnellement la validité du certificat du navigateur. Si les certificats sont approuvés, les deux parties négocient alors une clé de session maîtresse en utilisant les certificats précédemment échangés pour protéger la session qui est en train d'être établie.
Cette clé est ensuite utilisée pour encrypter les communications jusqu'à ce que le navigateur se déconnecte.
Ce type d'encapsulation des données est connu comme un tunnel.

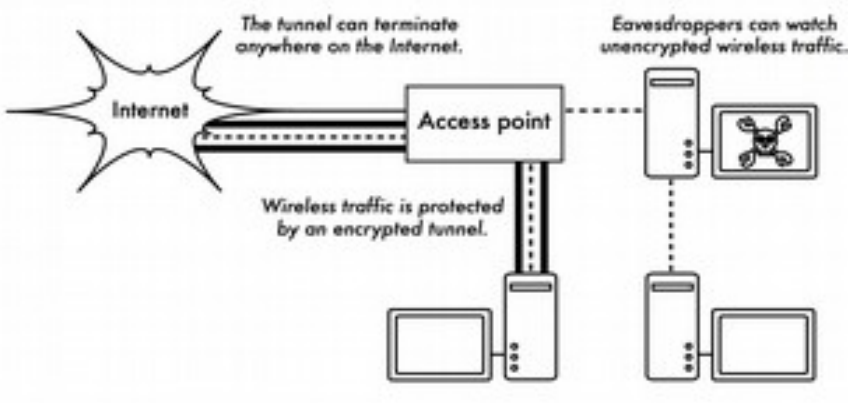


Figure SWN 6 : Les écouteurs indiscrets doivent briser un cryptage solide pour surveiller le trafic des données sur un tunnel encrypté. La conversation à l'intérieur du tunnel est identique à toute autre conversation qui n'est pas cryptée.

L'utilisation de certificats avec une PKI protège la communication non seulement contre les oreilles indiscrètes, mais est également utilisé pour prévenir contre la soi-disant attaque Man-in- the-Middle (MitM).
Dans une attaque MitM, un utilisateur malicieux intercepte toute communication entre un client et un serveur.

En présentant des certificats contrefaits à la fois au client et serveur, un utilisateur malicieux pourrait effectuer deux sessions encryptées simultanément. Comme l'utilisateur connaît le secret sur les deux connexions, il est trivial d'observer et de manipuler les données étant transmises entre le client et le serveur.

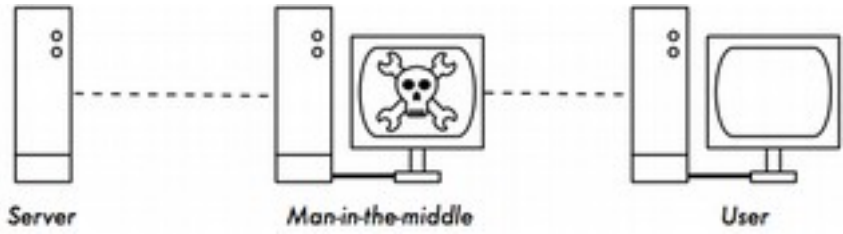


Figure SWN 7 : L'attaque man-in-the-middle contrôle effectivement tout ce que l'utilisateur voit, et peut enregistrer et manipuler tout le trafic. Sans une infrastructure à clé publique pour vérifier l'authenticité des clés, l'encryptage solide seul ne peut pas fournir une protection contre ce genre d'attaque.

L'utilisation d'un bon PKI peut significativement réduire les risques de ce type d'attaque. Pour réussir, l'utilisateur malveillant devrait être en possession d'un certificat signé par une autorité CA fiable qu'il peut présenter au client pour accepter comme authentique. Cela n'est possible que s'il peut tromper l'utilisateur final pour l'accepter ou si le CA est compromis. Les autorités de certification portent un fardeau spécial pour protéger leurs systèmes et réseau contre l'accès non autorisé et les utilisateurs malicieux.
Si un CA devait être compromis, l'attaquant qui l'a compromis pourrait mener des attaques MiTM sur l'un des utilisateurs essayant de se connecter aux systèmes avec un certificat émis par cette autorité de certification. Il pourrait également délivrer des certificats contrefaits en réponse à des demandes de certificats légitimes, garantissant ainsi sa capacité d'intercepter ou d'interférer avec les communications cryptées entre les utilisateurs du navigateur et les serveurs. Tandis que la compromission de CA compromis fut une fois considérée comme très improbable, au moment de la rédaction de ce document, il y a eu un certain nombre d'incidents qui révèlent que ce n'est plus le cas.
Les entreprises dont la principale activité était d'agir comme autorité de certification commerciale ont fait faillite à la suite d'avoir leurs systèmes compromis et des certificats contrefaits délivrés sous leur nom.

En Septembre 2011, l'autorité de certification DigiNotar a été attaquée par des pirates, forçant tous ses certificats à être révoqués, ceci l'envoyant en faillite. Ces compromissions n'étaient pas le travail des criminels informatiques sophistiqués utilisant des attaques sophistiquées exotiques, mais simplement le manque de sécurité de leur infrastructure globale et les politiques et procédures de sécurité. Finalement, il est bon de souligner que TLS est utilisé non seulement pour la navigation web. Les protocoles de courrier électronique non sécurisés comme IMAP, POP et SMTP peuvent être sécurisés en les enveloppant dans un tunnel TLS. La plupart des clients de messagerie modernes soutiennent IMAPS et POPS (IMAP et POP sécurisés) ainsi que le SMTP protégé par TLS. Si votre serveur de messagerie n'a pas de support TLS, vous pouvez toujours le sécuriser avec TLS en utilisant un logiciel comme Stunnel (http://www.stunnel.org/). TLS peut être utilisé pour sécuriser efficacement n'importe quel service qui fonctionne sur TCP.

SSH

La plupart des gens pensent de SSH comme remplacement sécurisé de telnet, juste comme SCP et SFTP sont les homologues sécurisés de RCP et FTP. Mais SSH est beaucoup plus qu'un remote shell crypté. Par exemple, il peut aussi agir comme un tunnel crypté à usage général, ou même un crypteur proxy web. En établissant d'abord une connexion SSH à un emplacement approuvé près (ou même sur) un serveur distant, les protocoles non sécurisés peuvent être protégés contre l'écoute et l'attaque. Comme TLS, il utilise une cryptographie à clé publique forte pour vérifier le serveur distant et encrypter les données. Au lieu d'une PKI, il utilise une cache clé empreinte digitale (en anglais key fingerprint cache) qui est vérifiée avant que la connexion est autorisée.

Il peut utiliser des mots de passe et des clés publiques pour l'authentification de l'utilisateur, et, par son support pour le système Pluggable Authentication Modules (PAM), il peut également supporter d'autres méthodes d'authentification. Bien que cette technique puisse être un peu avancée pour des nombreux utilisateurs, les architectes des réseaux peuvent utiliser SSH pour encrypter le trafic sur les liaisons non fiables, comme les liaisons sans fil point à point. Comme les outils sont disponibles gratuitement et fonctionnent avec le TCP standard, tout utilisateur instruit peut implémenter ses propres connexions SSH, en fournissant son propre encryptage de bout-à-bout sans intervention d'un administrateur. OpenSSH (http://openssh.org/) est probablement l'implémentation la plus populaire sur les plates-formes Unix.

Des implémentations libres tels que Putty (http://www.putty.nl/) et WinSCP (http://winscp.net/) sont disponibles pour Windows .
OpenSSH fonctionne également sur Windows sous le logiciel Cygwin (http://www.cygwin.com/). Ces exemples supposent que vous utilisez une version plus récente d'OpenSSH.

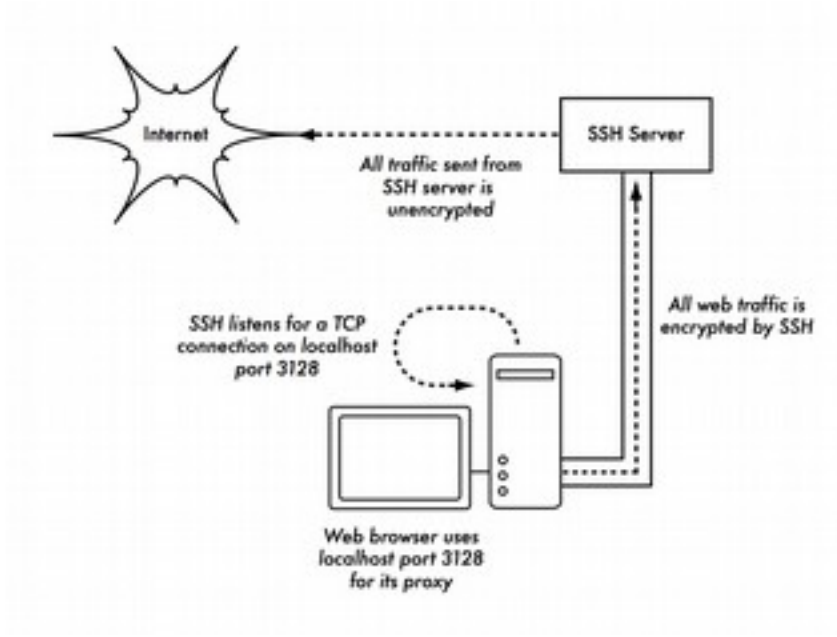


Figure SWN 8 : Le tunnel SSH protège le trafic web jusqu'au serveur SSH lui-même.

Pour établir un tunnel crypté à partir d'un port sur la machine locale à un port d'hôte distant, utilisez le commutateur -L . Par exemple, supposez que vous voulez transférer le trafic de proxy web sur une liaison cryptée au serveur squid sur l'hôte squid.example.net .
Redirigez le port 3128 (le port proxy par défaut) en utilisant cette commande :

ssh –fN -g -L3128:squid.example.net:3128 squid.example.net

Les commutateurs -fN instrusent ssh de s'exécuter en tâche de fond après s'être connecté.

Le commutateur –g permet à d'autres utilisateurs sur votre segment local de se connecter à la machine locale et l'utiliser pour l'encryptage sur les liaisons non sécurisées. OpenSSH utilise une clé publique pour l'authentification si vous en avez établi une, ou il vous demandera votre mot de passe sur le côté opposé. Vous pouvez ensuite configurer votre navigateur Web pour se connecter au port local 3128 comme son service web proxy.
Tout le trafic web sera alors crypté avant la transmission vers le côté distant. SSH peut également agir comme un SOCKS4 dynamique ou un proxy SOCKS5. Ceci vous permet de créer un encryptage proxy web, sans la nécessité d'installer squid. Notez que ce n'est pas un proxy à antémémoire, il crypte tout 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 vous partez. SSH peut encrypter les données sur n'importe quel port TCP, notamment les ports utilisés pour le courrier électronique. Il peut même compresser les données en cours de route, ce qui peut diminuer la latence sur les liaisons de faible capacité:

ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net

Le commutateur- C met en marche la compression. Vous pouvez ajouter autant de règles de redirection de port que vous le souhaitez en spécifiant le commutateur -L plusieurs fois. Notez qu'afin d'utiliser un port local inférieur à 1024, vous devez avoir les privilèges du superviseur (root) sur la machine locale. Ceux-ci ne sont que quelques exemples de la flexibilité de de SSH. En mettant en application des clés publiques et en utilisant l'agent ssh de redirection, vous pouvez automatiser la création de tunnels cryptés dans tout votre réseau sans fil et ainsi protéger vos communications avec un cryptage et une authentification solides.

OpenVPN

OpenVPN est une implémentation de VPN qui est basée sur l'encryptage SSL avec à la fois une édition commerciale ainsi qu'une édition Open Source ``communautaire". Il y a des implémentations client OpenVPN pour un large éventail des systèmes d' exploitation dont Linux, Window 2000/XP et ses versions plus récentes, OpenBSD, FreeBSD, NetBSD et Mac OS X.

De nombreux utilisateurs trouvent plus facile de comprendre et configuree OpenVPN que les VPNs de type IPSec. OpenVPN a cependant certains inconvénients, tels qu'une latence assez élevée du trafic sur le tunnel VPN. Une certaine latence est inévitable puisque tout cryptage/décryptage est effectué dans l'espace utilisateur. Cependant, l'utilisation d'ordinateurs relativement nouveaux à chaque extrémité du tunnel peut minimiser ces effets. Malgré qu'on peut utiliser des clés partagées traditionnelles pour l'authentification, OpenVPN se démarque vraiment quand on l'utilise avec des certificats SSL et une autorité de certification.
OpenVPN présente de nombreux avantages qui en font une bonne option pour la sécurité de bout-à-bout.
Certaines de ces raisons sont:

- il est basé sur un protocole de cryptage éprouvé et robuste (SSL et RSA).
- Il est relativement facile à configurer.
- Il fonctionne sur plusieurs plateformes différentes.
- Il est bien documenté. Une version Open-Source ``Communautaire" est maintenue en plus d'une version commerciale payable.

OpenVPN doit se connecter à un seul port TCP ou UDP de l'hôte distant. Une fois cette connexion établie, il peut encapsuler toutes les données jusqu'à la couche de gestion réseau couche ou même jusqu'à la couche de liaison de données si votre solution l'exige.
Vous pouvez l'utiliser pour créer des connexions VPN robustes entre des machines individuelles, ou simplement l'utiliser pour connecter des routeurs de réseau sur des réseaux sans fil non sécurisés. La technologie VPN est un champ complexe, et aller dans plus des détails est au-delà de la portée de cette section. Il est important de comprendre comment les VPNs s'accommodent dans la structure de votre réseau afin d'assurer la meilleure protection possible sans exposer votre organisation à des problèmes involontaires.

Il y a beaucoup de bonnes ressources en ligne qui traitent de l'installation d'OpenVPN sur un serveur et le client.
Nous vous recommandons cet article du Linux Journal :
http://www.linuxjournal.com/article/7949 ainsi que le HOWTO officiel :
http://openvpn.net/howto.html

Tor & Anonymiseurs

L'Internet est fondamentalement un réseau ouvert basé sur la confiance. Lorsque vous vous connectez à un serveur web sur Internet, votre trafic traverse plusieurs routeurs différents appartenant à une grande variété d'institutions, des entreprises et des particuliers. En principe, l'un de ces routeurs a la capacité d'examiner de près vos données, voyant les adresses source et destination, et très souvent aussi le contenu réel des données. Même si vos données sont cryptées en utilisant un protocole sécurisé, il est possible pour votre fournisseur d'accès Internet de surveiller la quantité de données transférées, ainsi que la source et la destination de ces données. Souvent, cela est suffisant pour reconstituer une image assez complète de vos activités en ligne. La confidentialité et l'anonymat sont importants, et sont étroitement liées entre eux. Il y a beaucoup de raisons valables qui peuvent vous pousser à protéger votre vie privée par anonymisation de votre trafic réseau. Supposons 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 chargiez pour l'accès ou non, il y a toujours le risque que les gens utilisent le réseau pour quelque chose qui n'est pas légal dans votre pays ou région.

Vous pouvez plaider avec le système juridique que cette action illégale particulier n'était pas perpétré par vous-même, mais qu'elle aurait pu être perpétrée par quiconque qui se connecterait à votre réseau.

Le problème serait soigneusement évité s'il était techniquement impossible de déterminer où votre trafic était réellement dirigé.

Et que dire de la censure en ligne ?

La publication de pages Web de façon anonyme peut aussi être nécessaire pour éviter la censure gouvernementale.

Il existe des outils qui vous permettent d'anonymiser votre trafic de manière relativement facile.

La combinaison de Tor (http://www.torproject.org/) et Privoxy (http://www.privoxy.org/) est un moyen puissant pour faire fonctionner un serveur proxy local qui fera passer votre trafic Internet à travers un certain nombre de serveurs à travers l'Internet, rendant très difficile de suivre la trace de l'information.

Tor peut être exécuté sur un ordinateur local, sous Microsoft Windows, Mac OSX, Linux, ainsi que diverses versions BSD, où il anonymizera le trafic du navigateur sur cette machine particulière.

Tor et Privoxy peuvent également être installés sur un serveur de passerelle, ou même un petit Point d'accès intégré (tel qu'un Linksys WRT54G) où il fournit l'anonymat à tous les utilisateurs du réseau automatiquement.
Tor fonctionne en faisant rebondir vos connexions TCP plusieurs fois à travers un certain nombre de serveurs répartis à travers l'Internet, enveloppant l'information de routage dans un certain nombre de couches encryptées (d'où le terme de routage en oignon), qui sont ``épluchées" au cours du déplacement du paquet à travers le réseau. Cela signifie qu'en tout point donné du réseau, les adresses source et destination ne peuvent pas être liées ensemble. Ceci rend l'analyse du trafic extrêmement difficile.
La nécessité du proxy de confidentialité Privoxy dans le contexte de Tor est due au fait que les requêtes du serveur de noms (requêtes DNS) dans la plupart des cas ne passent pas à travers le serveur proxy, et quelqu'un analysant votre trafic serait en mesure de facilement voir que vous essayez d'atteindre un site spécifique (par exemple google.com) par le fait que vous avez envoyé une requête DNS pour traduire google.com en une adresse IP appropriée. Privoxy se connecte à Tor comme proxy socks4a, qui utilise les noms d'hôte (pas les adresses IP) pour faire arriver vos paquets à la destination prévue. En d'autres mots, utiliser Privoxy avec Tor est un moyen simple et efficace pour prévenir l'analyse du trafic de lier votre adresse IP aux services que vous utilisez en ligne. Combiné avec des protocoles cryptés sécurisés (tels que ceux que nous avons vu dans ce chapitre), Tor et Privoxy fournissent un niveau élevé de l'anonymat sur Internet.

PLANIFICATION ET DEPLOIEMENT

10. PLANIFICATION DU DEPLOIEMENT

Estimation de la capacité

Pour estimer la capacité, il est important de comprendre que la vitesse mentionée d'un dispositif sans fil (le taux de transfert des données) se réfère au taux auquel les radios peuvent échanger des symboles, et non pas le débit utilisable que vous pourrez observer.
Le débit (en anglais throughput) est également désigné en tant que capacité de canal, ou simplement largeur de bande (bien que ce terme soit différent de la bande passante radio). - La largeur de bande-débit se mesure en Mbps, alors que la largeur de bande radio se mesure en MHz. Par exemple, une liaison 802.11g simple peut utiliser 54 Mbps radios, mais elle ne fournira seulement que jusqu'à 22 Mbps de débit réel.
Le reste conssiste en un surplus (overhead) dont les radios 802.11g ont besoin pour coordonner leurs signaux. Il convient de noter que le débit est une mesure de bits au cours du temps. 22 Mbps signifie qu'un maximum de 22 mégabits de données peuvent être transferées d'une extrémité de la liaison à l'autre dans chaque seconde donnée.
Si les utilisateurs tentent de passer plus de 22 mégabits a travers la liaison, cela prendra plus d'une seconde . Comme les données ne peuvent pas être transferées immédiatement, elles sont placées dans une file d'attente (en anglais queue) puis transmises aussi rapidement que possible. Cette file d'attente augmente le temps nécessaire pour les bits les plus récemment mis dans la file d'attente de traverser la liaison. Le temps pris par les données de traverser une liaison s'appelle latence et une latence élevée est communément designée sous le nom de décalage (en anglais lag).
Votre liaison pourra finalement envoyer tout le trafic en file d'attente, mais probablement vos utilisateurs probablement se plaindront avec l'augmentation du décalage.
De quelle capacité de traitement vos usagers ont réellement besoin? Ceci va dépendre du nombre d'usagers que vous avez et comment ceux-ci utilisent la liaison sans fil.
Différentes applications Internet requièrent des capacités de traitement différentes.

Application	Exigence/Usager	Notes

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.
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 vidéo	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 vidéo 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)	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 implémentiez une mise en forme du trafic (bandwith shaping).

Pour estimer la capacité de traitement nécessaire pour votre réseau, multipliez le nombre prévu d'usagers par les exigences des applications 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 de pointe 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. 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 en conséquence doubler la capacité de traitement exigée, pour faire un total de 10 Mbps. Vos liens sans fil doivent fournir cette capacité chaque seconde, sans quoi les conversations auront un délai.Comme tous 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 5 à 10 est tout à fait courant. Très probablement, vous procéderez à une surévaluation lorsque vous établirez votre infrastructure de réseau. En surveillant soigneusement le débit 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.

Calcul du bilan de liaison

Le processus pour déterminer si une liaison est viable s'appelle calcul du bilan de liaison. Un système de communication de base se compose de deux radios, chacune avec son antenne associée, les deux séparées par le chemin à couvrir suivant la Figure DP 1 ci-dessous.

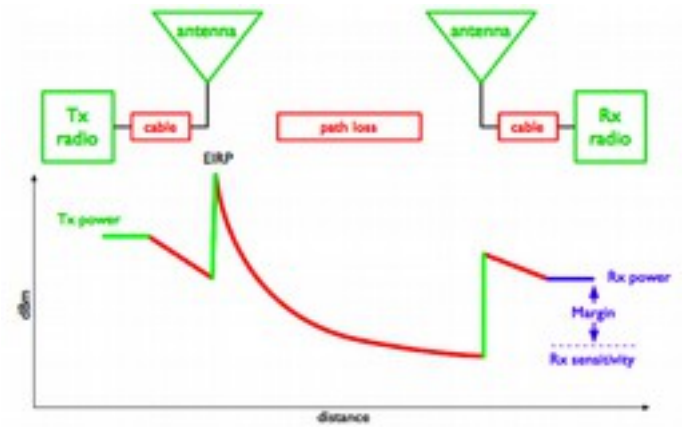


Figure DP 1: Les composantes d'un système de communication de base.
Afin d'avoir une communication entre les deux, les radios exigent qu'un

signal minimum provenant des antennes soit fourni à leurs ports d'entrée.
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). Dans un tel système, certains paramètres peuvent être modifiés (l'équipement utilise) alors que d'autres sont fixes (la distance entre les radios).
Commençons par examiner les paramètres qui peuvent être modifiés.

1. Les caractéristiques de l'équipement à considérer lors du calcul du bilan de la liaison sont:

Puissance de transmission (TX). Elle est exprimée en milliwatts ou en dBm. 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. Un exemple est fourni ici-bas qui montre qu'en utilisant le protocole 802.11g, il y a une différence de 5 dB en puissance de sortie quand vous utilisez 6Mbs ou 54Mbs.

SYSTEM INFORMATION	
Processor Specs	Atheros MIPS 4KC, 180MHz
Memory Information	16MB SDRAM, 4MB Flash
Networking Interface	1 X 10/100 BASE-TX (Cat. 5, RJ-45) Ethernet Interface

REGULATORY / COMPLIANCE INFORMATION	
Wireless Approvals	FCC Part 15.247, IC RSS210, CE
RoHS Compliance	YES

RADIO OPERATING FREQUENCY 2412-2462 MHz

TX SPECIFICATIONS			
	DataRate	TX Power	Tolerance
802.11b	1Mbps	20 dBm	+/-1dB
	2Mbps	20 dBm	+/-1dB
	5.5Mbps	20 dBm	+/-1dB
	11Mbps	20 dBm	+/-1dB
802.11g OFDM	6Mbps	20 dBm	+/-1dB
	9Mbps	20 dBm	+/-1dB
	12Mbps	20 dBm	+/-1dB
	18Mbps	20 dBm	+/-1dB
	24Mbps	20 dBm	+/-1dB
	36Mbps	18 dBm	+/-1dB
	48Mbps	16 dBm	+/-1dB
	54Mbps	15 dBm	+/-1dB

RX SPECIFICATIONS			
	DataRate	Sensitivity	Tolerance
802.11b	1Mbps	-95 dBm	+/-1dB
	2Mbps	-94 dBm	+/-1dB
	5.5Mbps	-93 dBm	+/-1dB
	11Mbps	-90 dBm	+/-1dB
802.11g OFDM	6Mbps	-92 dBm	+/-1dB
	9Mbps	-91 dBm	+/-1dB
	12Mbps	-89 dBm	+/-1dB
	18Mbps	-88 dBm	+/-1dB
	24Mbps	-84 dBm	+/-1dB
	36Mbps	-81 dBm	+/-1dB
	48Mbps	-75 dBm	+/-1dB
	54Mbps	-72 dBm	+/-1dB

Figure DP 2 : Datasheet d'Ubiquiti Bullet2

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. Des valeurs typiques sont : les antennes paraboliques ont un gain de 19-24 dBi, les antennes omnidirectionnelles ont 5-12 dBi et les antennes sectorielles ont un gain approximatif de 12-15 dBi.
Niveau minimum de signal reçu (RSL), ou simplement la sensibilité du récepteur. Le RSL minimum est toujours exprimé en dBm négatif (- dBm) et consiste en 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 spécifications du RSL devraient être fournies par le fabricant de l'équipement. Dans la fiche du fabricant (datasheet) présenté ci-haut, vous pouvez voir qu'il y a une différence de 20 dB de sensibilité du récepteur, avec -92dBm à 6Mbs et -72dBm à 54 Mbs. N'oubliez pas qu'une différence de 20 dB signifie a rapport de 100 en termes de puissance.
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 y compris les connecteurs est assez faible, dans la gamme de 2 ou 3 dB. Il est préférable d'avoir des câbles aussi courts que possible.

2. 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***.

Perte en espace libre
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 sera le signal reçu à cause de 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 une fréquence du signal

générique f, l'équation pour la perte en espace libre est:

$$L_{fsl} = 32.40 + 20*log_{10}(D) + 20*log_{10}(f)$$

Où L_{fsl},la perte de signal, est exprimée en dB et D est en kilomètres et f est en MHz. En dessinant un graphe de la perte en espace libre en fonction de la distance, on obtient une figure comme celle-ci-bas. Ce qui est observable est que la différence entre l'usage du 2400 MHz et le 5300 MHz est de 6 dB en termes de perte en espace libre.Ainsi une fréquence supérieure produit une grande perte en espace libre qui est souvent compensée par un plus grand gain pour les antennes paraboliques. Pour les mêmes dimensions d'antenne, une antenne parabolique opérant à 5 GHz est plus puissante de 6 dB qu'une antenne opérant à 2.4 GHz.

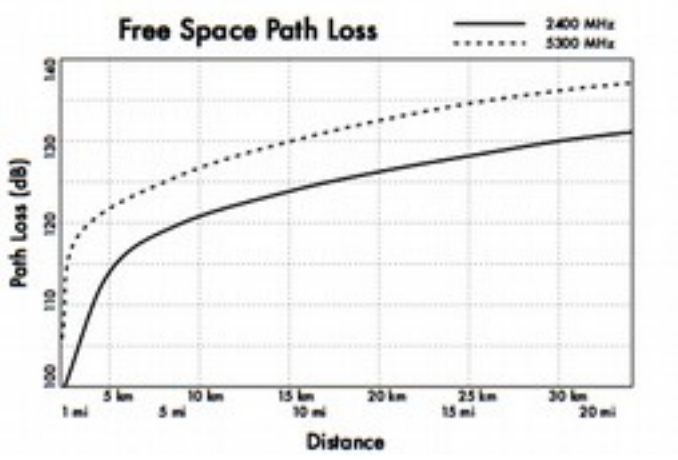


Figure DP 3 : Graphe de calcul de la perte en espace libre

Atténuation

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.

Diffusion

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*), ou dispersion du signal. Dans certains cas les signaux reflétés s'ajoutent et ne posent aucun problème. Quand ils s'ajoutent en opposition de phase, le signal reçu est presque nul. Dans certains cas, le signal reçu à l'antenne de réception peut être annulé par les signaux reflétés. Ceci est connu sous le nom d'***annulation*** (en anglais «*nulling*»). Il existe une technique simple appelée ***diversification d'antenne*** qui est utilisée pour résoudre le problème des trajets multiples. Elle consiste à ajouter une deuxième antenne à la radio.

Le phénomène des trajets multiples est en fait très localisé. Si deux signaux s'ajoutent en opposition de phase à une position, ils ne feront pas de même à la deuxième position proche. 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 dispositifs commerciaux, on emploie la diversité de commutation d'antenne: il y a des antennes multiples 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 recouvrir le signal de façon similaire à la perte de signal. La mise de tous ces paramètres ensemble conduit au calcul du bilan de liaison.

Si vous utilisez des radios différentes de chaque côté de la liaison, vous devriez calculer la perte de trajet deux fois, une fois pour chaque direction (en utilisant pour chaque calcul des valeurs appropriées de la puissance de transmission TX et de réception RX et du gain de l'antenne de transmission TX et de réception RX).

En additionnant tous les gains et soustrayant toutes les pertes, ceci 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	

En soustrayant la perte de trajet du Gain Total, ceci donne:

Gain total - Perte de trajet = Niveau du signal au côté récepteur de la liaison.

Si le niveau du signal résultant 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'utiliser.
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 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 une liaison radio stable et de haute qualité pendant des mauvaises conditions atmosphériques.
Une marge de 10-15 dB est acceptable. Pour tenir compte de l'atténuation et les trajets multiples dans le signal de radio reçu, une marge de 20dB devrait être une valeur assez rassurante.
Une fois que vous avez calculé le bilan de la liaison 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 bilan de liaison

Comme exemple, nous voulons estimer la viabilité d'une liaison 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.

Commençons par calculer le bilan de liaison du point d'accès AP vers le client comme illustré par la Figure DP 4.

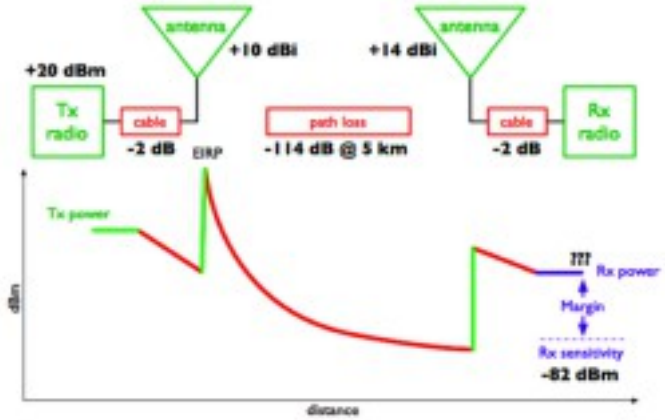


Figure DP 4 : Calcul du budget de liaison de AP vers le client

En additionnant tous les gains et en soustrayant toutes les pertes de l'AP vers le 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 une liaison de 5km, considérant la perte en espace libre, est de -114dB.
La soustraction de la perte de trajet du gain total donne:

40 dB - 114 dB = -74 dB

Puisque -74dB 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 8dB (82dB – 74dB) qui fonctionnera probablement bien dans de bonnes conditions climatiques mais n'est pas assez pour protéger la liaison contre les conditions climatiques extrêmes. Ensuite, calculons le lien du client vers le point d'accès, comme illustré ici-bas:

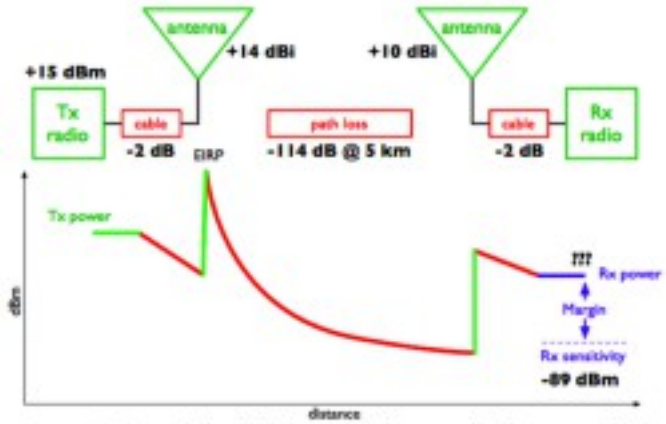


Figure DP 5: Calcul du bilan de liaison du client vers l'AP.

15 dBm	*(TX puissance Radio 1)*
+14 dBi	*(Gain d'antenne Radio 1)*
-2 dB	*(Perte des câbles Radio 1)*
+10 dBi	*(Gain d'antenne Radio 2)*
-2 dB	*(Perte des câbles Radio 2)*
35 dB =	*Gain total*

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

35 dB - 114 dB = -79 dB

Puisque la sensibilité de réception de l'AP est de -89dBm, ceci nous laisse une marge de de 10dB (89dB - 79dB).
De façon générale, cette liaison fonctionnera probablement bien. 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 de la liaison (souvenez-vous que le gain d'antenne est réciproque).
Une option plus coûteuse serait d'utiliser des radios de puissance plus élevée sur les deux extrémités de la liaison. Cependant, notez que 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 de la liaison.

Tables pour calculer le bilan de liaison.

Pour calculer le bilan de liaison, faites simplement une estimation de la

distance de votre liaison, et ensuite remplissez les tables suivantes:

Perte d'espace libre à 2,4GHz

Distance (m)	100	500	1000	3000	5000	10 000
Perte (dB)	80	94	100	110	113	120

Gain d'antenne:

Antenne Radio 1	+ Antenne Radio 2	= Gain Total

Pertes:

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

Budget de liaison pour la liaison Radio 1 ➔ Radio 2:

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

Budget de liaison pour la liaison Radio 2 ➔ Radio 1:

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

Si le signal reçu a une puissance plus grande que la puissance minimum de réception du signal dans les deux directions de la liaison ainsi que tout bruit sur le trajet, alors la liaison est viable.

Logiciel de planification de liaison

Même s'il est assez simple de calculer à la main le potentiel de puissance d'une liaison, il y a un certain nombre d'outils disponibles qui vous aideront 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 par les arbres, les effets du terrain, le climat et même l'estimation de la perte de trajet en milieux urbains). La plupart d'outils commerciaux sont très coûteux et sont souvent destinés pour l'usage sur un matériel spécifique.
Dans cette section, nous discuterons un outil gratuit appelé RadioMobile.

RadioMobile

RadioMobile est un outil pour la conception et la simulation de systèmes sans fil. Il prédit la performance d'une liaison radio en se basant sur l'équipement et une carte géographique numérique. C'est un logiciel du domaine public mais pas de source ouverte (en anglais open source). 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. Un exemple est montré dans la Figure DP 6 ci-dessous.

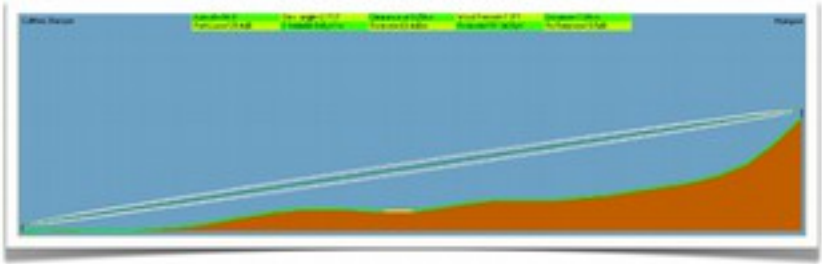


Figure DP 6 : Simulation Radio Mobile montrant une élévation numérique de terrain et la première zone de Fresnel.

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. 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 allant de 100 KHz à 200 GHz. Les cartes numériques d'élévation numériques (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 figures de

prédiction précises. Il y a deux versions de RadioMobile : une version sous Windows et une version en ligne utilisant une interface Web.
Voici les différences principales entre les deux.

Version Web :
• elle peut fonctionner sur n'importe quelle machine (Linux, Mac, Windows, tablette, téléphone, etc .)
• elle ne nécessite pas de gros téléchargements. Comme elle fonctionne en ligne, les données sont stockées sur le serveur et seules les données nécessaires sont téléchargées .
• elle enregistre les sessions. Si vous exécutez une simulation et vous vous connectez après un certain temps, vous pourrez toujours retrouver votre simulation et les résultats.
• Elle est plus facile à utiliser, surtout pour les débutants.
• elle nécessite une connexion. Il n'est pas possible d'exécuter une simulation si vous êtes déconnecté.
• comme elle a été développée pour la communauté des radioamateurs, elle ne peut fonctionner que pour certaines bandes de fréquences. A titre d'exemple, il n'est pas possible de simuler des liaisons à 5.8GHz, mais seulement à 5.3GHz. C'est assez bon d'un point de vue pratique, mais vous devez garder cela à l'esprit.

Version de Windows :
• elle peut fonctionner en mode hors connexion. Une fois que les cartes sont téléchargées, il n'y a pas besoin d'être en ligne pour lancer la simulation.
• on peut utiliser un GPS externe pour obtenir la position exacte de la station. Bien que cela n'est pas souvent utilisé, ça pourrait parfois être utile.
• elle fonctionne sur Windows (elle fonctionne sous Linux mais pas directement).
• elle nécessite de gros téléchargements. Si votre largeur de bande passante est limitée, télécharger de nombreuses cartes pourrait être un problème. La version en ligne nécessite des téléchargements plus petits.
• elle n'est pas conviviale, surtout pour les débutants.
La page Web principale de RadioMobile, avec des exemples et des tutoriels, est disponible à l'adresse: http://www.cplus.org/rmw/english1.html
Suivez les instructions pour installer le logiciel sur Windows.
RadioMobile en ligne
Pour utiliser la version en ligne de RadioMobile vous devez d'abord créer

un compte. Aller à: http://www.cplus.org/rmw/rmonline.html et créer un nouveau compte. Vous recevrez un email de confirmation dans quelques minutes et vous serez prêt à l'utiliser. La simulation d'une liaison exige quelques étapes qui nécessitent de suivre le menu sur la gauche, de haut en bas comme le montre la Figure DP 7 ci-dessous.

Figure DP 7 : Préparation pour simuler une liaison en utilisant RadioMobile.

La première étape est de cliquer sur « New Site ». Il vous sera présenté une carte, similaire à Google Maps. Vous pouvez zoomer sur la carte pour trouver l'emplacement de votre premier site. Faites glisser le repère orange et le placer dans la position souhaitée. Une fois que vous avez terminé, cliquez sur « Submit ». Donnez à l'emplacement un nom significatif, et cliquez sur « Add to My Sites ». Ainsi, vous serez en mesure d'utiliser cet emplacement pour la simulation.
Répétez la même procédure pour le second site. Une fois que vous avez au moins deux sites, vous pouvez passer à l'étape suivante. L'interface ne vous permettra pas d'entrer directement les coordonnées du site.
Ainsi vous pourriez vouloir entrer un emplacement approximative pour le curseur et puis ensuite corriger la valeur des coordonnées dans le tableau.
La deuxième étape consiste à entrer des informations sur la liaison: les caractéristiques de l'équipement, les antennes, etc.
Cliquez sur « New Link » dans le menu de gauche. Sélectionnez les deux sites à partir des menus déroulants. Donnez un nom significatif pour la liai-

son et entrez les informations sur l'équipement utilisé. La sensibilité du récepteur est exprimée en microvolts, alors que nous utilisons habituellement dBm. Pour traduire de microvolts en dBm, voici quelques exemples :

- 90dBm vaut 7,07 microvolts
- 85dBm vaut 12,6 microvolts
- 80dBm vaut 22,4 microvolts
- 75dBm vaut 39,8 microvolts
- 70dBm vaut 70,7 microvolts

Il est très important de choisir une fréquence que la version en ligne de RadioMobile peut gérer.
Voici les fréquences les plus importantes pour les liaisons WiFi :
Utilisez 2300 MHz pour les liaisons 2.4 GHz et 5825 MHz pour les liaisons 5.8 GHz.
Une fois que vous avez entré toutes les informations, cliquez sur « Submit ». En peu de temps, un écran similaire à la Figure DP 8 ci-dessous vous sera présenté.

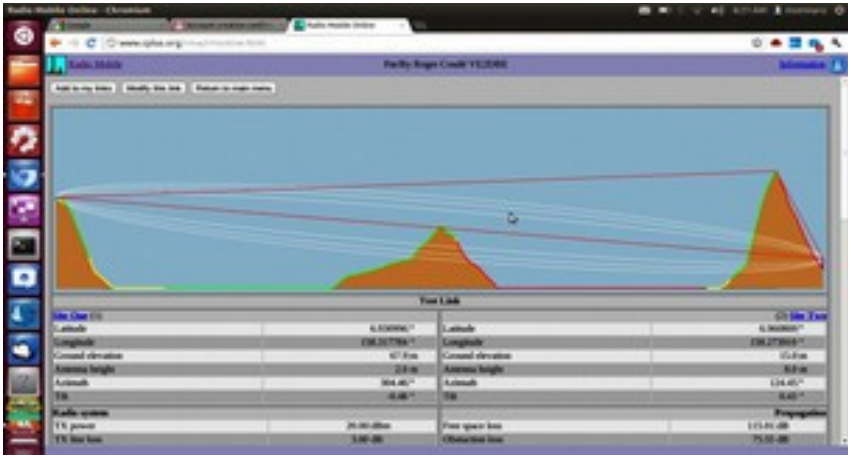


Figure DP 8 : Résultat de la simulation.

Cette page contient toutes les informations nécessaires pour vérifier si la liaison est viable ou non. Elle donne des informations sur : la longueur de la liaison, l'azimut, l'élévation et l'inclinaison que vous devriez donner aux antennes, la perte en espace libre, la perte en espace totale, y compris la perte statistique et, plus important encore, le niveau du signal reçu. Avec la

sensibilité du récepteur que vous avez entré, il vous sera présenté une marge d'évanouissement qui vous permettra de déterminer si la liaison est viable ou non. Si vous êtes satisfait du résultat en haut de la page, vous devez cliquer sur « Add to my sites » et la liaison sera enregistrée. Si vous n'êtes pas satisfait et que vous souhaitez simuler une configuration d'équipement différent, cliquez sur « Modify this link » .

Radio Mobile pour Windows en quelques étapes simples

Ceci est un guide abrégé pour commencer à utiliser RadioMobile après l'installation. Chaque paramètre qui n'est pas spécifié ici peut être laissé à la valeur par défaut et modifié par la suite si nécessaire .

Étape 1 : télécharger les cartes numériques d'élévation (DEMs) de votre zone d'intérêt. choisir le format de SRTM.

Étape 2 : créer une carte. Dans « File » → « Map properties », choisissez le milieu de votre zone d'intérêt comme coordonnées de votre carte et une taille en km assez grande pour englober tous points. Utilisez 514X514 pixels pour le moment. Vous pouvez ajouter un autre type de carte (comme celle des routes) à la carte DEM si vous le souhaitez.

Étape 3: Créer des systèmes. Dans « File » → « Network properties » → « Systems ». Chaque système est une combinaison de la puissance TX, la sensibilité RX et du gain d'antenne . Sélectionnez antenne omni même si votre antenne est directionnelle, mais insérez le gain réel .

Étape 4 : créer des unités. Chaque unité a un nom et une position géographique. Vous pouvez utiliser degrés, minutes, secondes ou degrés et fractions, mais assurez-vous de sélectionner le bon hémisphère (N ou S, E ou W).

Étape 5: Attribuer des rôles : sélectionner la rubrique « Network properties » dans le menu «File». Ensuite, allez à l'onglet «Membership» où vous serez autorisé à modifier le système et le rôle de chaque unité. Activez chaque unité dans la liste en la cochant. Attribuez un nom à votre réseau et dans l'onglet «parameters» réglez la fréquence minimale et maximale de fonctionnement exprimée en MHz.

Étape 6 : Visualisez votre réseau sur la carte. Selectionez «View» → «Show networks» → «All»

Étape 7: obtenez le profil et pointez au bilan liaison . «Tools»→«Radio link». Vous pouvez passer à la vue détaillée qui vous donne une description textuelle du résultat e de la simulation .

Étape 8: Visualisez la couverture : cliquez sur « Tools » → « Radio coverage » → « Single polar » pour obtenir la couverture de chaque station.

A ce stade, le type d'antenne devient pertinent. Si ce n'est pas une omni vous devez modifier la configuration de l'antenne et l'orientation de l'axe de visée (direction où le faisceau est dirigé) .

Utilisation de Google Earth pour obtenir un profil d'élévation

Google Earth est une application de cartographie très populaire. Elle peut être utilisée pour obtenir le profil d'élévation entre deux points, et donc déterminer l'existence (ou pas) de la ligne de visée optique. La ligne de visée radioélectrique peut être dérivée de l'optique en ajoutant l'effet de la courbure de la terre (en utilisant le rayon modifié de la terre) et les exigences de dégagement de la première zone de Fresnel.

La procédure est la suivante :

Installer Google Earth sur votre appareil, lancez l'application et zoom sur la carte afin que vous puissiez voir les deux points que vous souhaitez lier.

1. Dans le menu supérieur, cliquez sur « Add path ».
2. Cliquez pour définir le premier point, puis pour le deuxième point.
3. Donnez à la connexion un nom (« Liaison », par exemple) et cliquez sur OK dans la fenêtre pop-up.
4. La connexion apparaît dans le menu à gauche.
5. Cliquez à droite sur le nom de la connexion ("Link" dans notre exemple)
6 .Sélectionnez «Show elevation profile »
7. Le profil d'altitude apparaît au bas de l'écran.
8 .Si vous vous déplacez le long du profil, vous verrez une flèche rouge indiquant là où le point est dans la carte.

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'utilisent 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 liaisons 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'une liaison point à point. Les antennes ne font pas qu'ajouter du gain à une liaison, mais l'augmenta-

tion de leur directivité tend à rejeter le bruit dans les régions autour de la liaison. Deux antennes paraboliques de gain élevé qui pointent l'une vers l'autre vont rejeter le bruit provenant de directions qui sont en dehors de la trajectoire de la liaison. Les antennes omnidirectionnelles recevront le bruit provenant de toutes les directions.

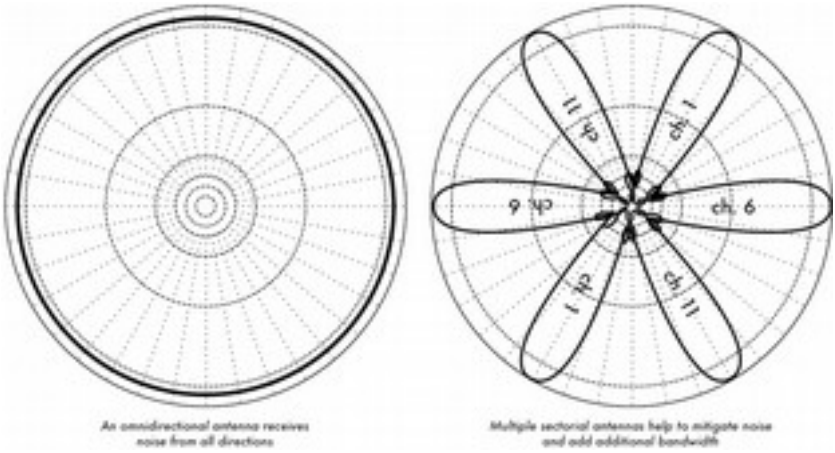


Figure DP 9 : Une seule antenne omnidirectionnelle vs multiples antennes sectorielles.

• **Employez des antennes sectorielles** au lieu d'une omnidirectionnelle. En employant plusieurs antennes sectorielles, vous pouvez réduire le bruit global reçu en un point de distribution donné. En organisant les canaux utilisés sur chaque antenne sectorielle, vous pouvez également augmenter la largeur de bande disponible pour vos clients.

• **N'utilisez pas un amplificateur**. 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.

• **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 petits sauts** et des répéteurs au lieu d'une seule liaison sur une longue distance. Gardez vos liens point-à-point aussi courts que possible. Même s'il est possible de créer une liaison de 12km qui traverse 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.** Même si ceci n'est qu'une solution à court terme, actuellement la plupart d'équipements installés utilisent la bande de 2,4GHz. En utilisant le
802.11a, vous éviterez cette congestion.

• **Si rien de ceci ne fonctionne, utilisez un spectre autorisé**. Il y a des endroits où tout le spectre sans licence disponible a été utilisé. Dans ces cas, ça peut être une bonne idée de dépenser une somme d'argent supplémentaire pour obtenir une licence correspondante et déployer un équipement qui opère dans une bande moins encombrée. Pour des liaisons de longue distance point à point qui requièrent un débit 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.

Récemment, l'équipement opérant dans les bandes de 17GHz et 24GHz est devenu disponible. Même s'il est plus coûteux, cet équipement offre une plus grande largeur de bande et dans beaucoup de pays, ces bandes sont sans licence.

Pour identifier des sources de bruit, vous avez besoin d'outils qui vous révèlent ce qui se passe dans l'air à 2,4GHz. Nous verrons quelques exemples de ces outils dans les chapitres sur **gestion réseau** et **maintenance et dépannage.**

Répéteurs

La composante la plus critique pour construire une liaison de réseau de longue distance est la ligne de vue (en anglais Line of Sight – **LOS**).

Les systèmes micro-onde terrestres ne peuvent tout simplement pas tolérer de grandes collines, arbres, ou autres obstacles sur le trajet d'une liaison de

longue distance.
Vous devez avoir une idée claire de la configuration du terrain entre deux points avant que vous ne puissiez déterminer si une liaison 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 soit possible d'y apporter de l'énergie électrique, elles pourront faire de très bons sites répéteurs. Les répéteurs sont des nœuds qui sont configurés pour rediffuser le trafic qui n'est pas destiné au nœud lui-même. Dans un réseau maillé, chaque nœud est un répéteur.
Dans un réseau infrastructure traditionnel, certains nœuds doivent être configurés pour faire passer le trafic à d'autres nœuds.
Un répéteur peut utiliser un ou plusieurs dispositifs sans fil. Lors de l'utilisation d'une seule radio (en anglais « one-arm repeater »), l'efficacité globale est légèrement inférieure à la moitié de la largeur de bande disponible, puisque la radio peut envoyer ou recevoir des données, mais ne jamais faire les deux en même temps. Ces dispositifs sont meilleur marché, plus simples et ont des exigences de consommation électriques inferieures.
Un répéteur à deux (ou plus) cartes radio peut opérer toutes les radios à pleine capacité, aussi longtemps que celles-ci sont configurées pour utiliser des canaux qui ne se superposent pas.
Naturellement, les répéteurs peuvent également fournir une connexion Ethernet pour une connectivité locale.
Des répéteurs peuvent être achetés comme une solution matérielle complète, ou être facilement assemblés en reliant deux (ou plus) nœuds sans fil avec un câble Ethernet.
Lorsque vous pensez utiliser un répéteur construit avec la technologie 802.11, rappelez-vous que les nœuds 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 à des multiples clients de se connecter à l'un ou l'autre côté du répéteur.
Mais selon votre configuration réseau, un ou plusieurs dispositifs peuvent exiger un mode ad hoc ou même client.

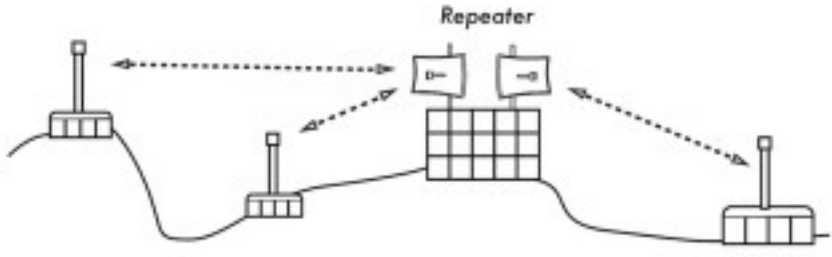


Figure DP 10 : Le répéteur transmet des paquets dans l'air entre des nœuds qui n'ont pas de ligne de vue directe.

Généralement, les répéteurs sont utilisés pour éviter des obstacles dans le trajet d'une liaison de longue distance. Par exemple, il peut y avoir des bâtiments dans votre trajet, mais dans ceux-ci, il y a des personnes. Il est souvent possible de faire des accords avec les propriétaires des bâtiments pour leur 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 sur une fenêtre. Si vous ne pouvez pas passer par-dessus ou à travers un obstacle, vous pouvez souvent le contourner. Plutôt que d'utiliser une liaison directe, essayez une approche à sauts multiples pour éviter l'obstacle.

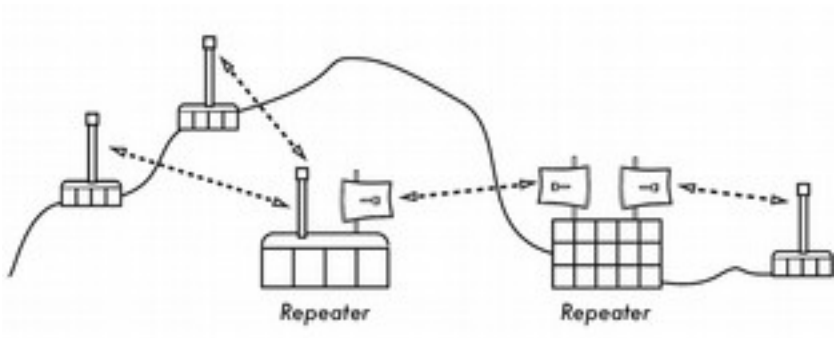


Figure DP 11: Il n'y avait pas d'énergie électrique disponible au-dessus de la colline, mais ceci a été résolu en utilisant de multiples sites répéteurs situés autour de la base.

Finalement, vous devrez peut-être envisager de réculer pour pouvoir avancer. ' Si il ya un site élevé disponible dans une direction différente, et que ce site peut voir au-delà de l'obstacle, une liaison stable peut être établie par l'intermediaire d'un intinéraire indirect.

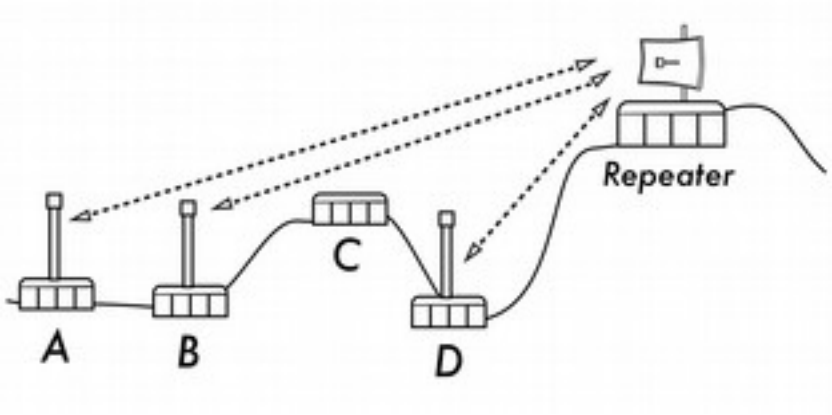


Figure DP 12 : Le site D ne peut pas voir les sites A ou B, car le site C est dans le chemin et n'est pas interessé d'héberger un nœud répéteur. En installant un répéteur plus haut, les nœuds A, B, et D peuvent communiquer les uns avec les autres. Notez qu'en fait le trafic du nœud D voyage plus loin que celui du reste du réseau avant que le répéteur transmette ses données.

La planification du déploiement de l'IPv6

Comme nous l'avons mentionné dans le chapitre intitulé réseau, la plupart des régions du monde ont soit épuisé ou presque épuisé leurs adresses IPv4. Par conséquent, il est important que vous considériez dans votre planification le déploiement des réseaux IPv6.

Il est entendu qu'au moment de l'écriture de ce livre, il ya encore de nombreux sites et services qui sont encore disponibles uniquement sous IPv4. Ainsi, afin de devenir un leader dans le déploiement de l'IPv6, vous devez être capable d'interconnecter avec les réseaux IPv4 existants ainsi qu'enseigner et guider vos utilisateurs et développeurs sur la facon de gérer IPv6 et IPv4 ensemble.

En prenant la direction du déploiement Pv6 dans votre réseau, vous serez à l'avant-garde de l'Internet et reconnu comme quelqu'un qui est prêt à connaître et supporter la prochaine génération de réseaux.

Lors de la préparation pour IPv6, voici quelques mesures que vous pouvez prendre pour vous aider à vous diriger dans la bonne direction.
1. N'achetez pas des routeurs, firewalls et autres équipements IP qui traitent les paquets IPv4 dans le matériel à pleine vitesse alors que les paquets IPv6 sont traités plus lentement dans le logiciel ou pire encore qui ne supportent pas IPv6 du tout. La grande majorité des périphériques réseau disponibles supportent IPv6 . RIPE a préparé quelques conditions pour être ajoutés à n'importe quel appel d'offres pour s'assurer que l'IPv6 est inclus:
http://www.ripe.net/ripe/docs/current -ripe-documents/ripe-554
Vous pouvez également rechercher le logo IPv6 Ready sur les fiches de données de dispositifs .
2. Lors du déploiement des nouveaux logiciels, assurez-vous qu'ils supportent IPv6 .
3. Quand vous discutez de votre liaison backhaul avec un fournisseur d'accès local, vérifiez qu'il a déployé ou prévoit de déployer et offrir des services IPv6. Si ce n'est pas le cas, discutez avec lui comment vous pouvez coopérer et interconnecter votre réseau IPv6 avec lui. Le coût de l'IPv6 devrait être inclus dans le coût global; ce qui signifie que vous n'aurez rien à payer de plus pour obtenir IPv6. L'accord de niveau de service (SLA) pour IPv6 doit être identique (débit, latence, temps de réponse, etc.) que pour IPv4. Il existe plusieurs techniques de transition IPv4/IPv6 qui peuvent être déployées .
Voici quelques URLs que vous pouvez consulter pour vous donner des informations à jour sur ceci :
http://www.petri.co.il/ipv6-transition.htm
http://en.wikipedia.org/wiki/IPv6_transition_mechanisms
http://www.6diss.org/tutorials/transitioning.pdf

Il y a plus d'informations sur la croissance de l'IPv6 et la carence des adresses IPv4 disponibles dans cet article publié à la fin de 2012.

http://arstechnica.com/business/2013/01/ipv6-takes-one-step-forward-ipv4-two-steps-back-in-2012/

Il ya aussi un projet financé par la CE appelé 6Deploy qui offre des services de formation et de helpdesk pour les ingénieurs réseau qui commencent des déploiements IPv6. Il est fortement recommandé que vous les contactez pour discuter de votre projet.
http://www.6deploy.eu/index.php?page=home

11. SÉLECTION ET CONFIGURATION MATÉRIEL

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.

Avec et Sans 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 nœud 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 courant continu.
Toutes ces composantes utilisent 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 nœuds que vous déploierez et vous vous demanderez bien pourquoi on désigne ceci comme une connexion sans fil.
Le diagramme de la page suivante 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 présente plusieurs composantes courantes que vous retrouverez très probablement sur le terrain.

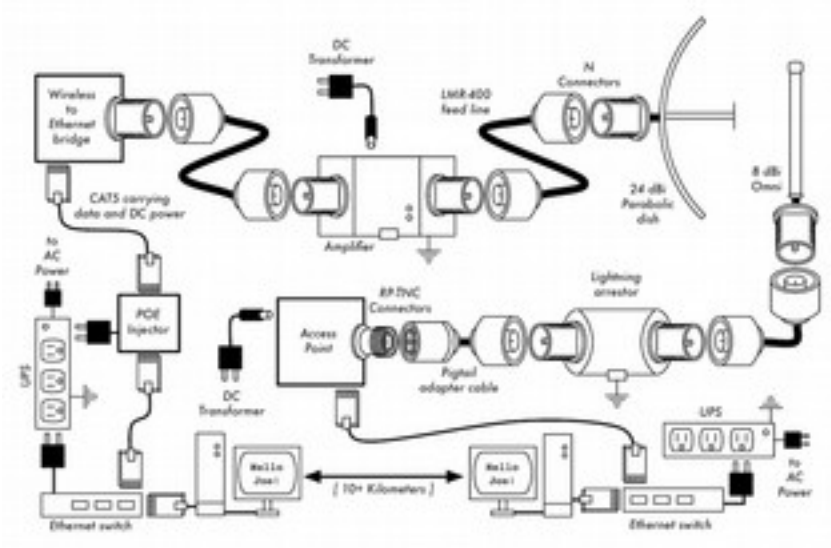


Figure HW 1 : Composantes et connecteurs communs pour une liaison sans fil point à point.

Tandis que les composantes réelles utilisées vont varier d'un nœud 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 exigences du 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 dans les autres chapitres de ce livre, 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. Ceci n'est pas quelque chose d'inhérente 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 semi fictive estimation de portée 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 lors des calculs du bilan de liaison dans le chapitre sur la planification du déploiement.

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 compléter un calcul du bilan de liaison. Quand il s'agit de sensibilité de la radio, une petite valeur est meilleure.

Débit. Les fabricants indiquent systématiquement le débit le plus élevé possible comme "vitesse" de leur équipement.

Gardez en tête que le débit radio symbolique (par exemple 54Mbps) n'est jamais une estimation réelle du rendement du dispositif (par exemple, environ 22 Mbps pour le 802.11g). Si l'information sur le débit 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 débit sur une unité d'évaluation avant d'acheter une grande quantité d'équipement qui n'a aucune estimation officielle de débit.

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? Par exemple, les approvisionnements DC sont en général inclus ; les injecteurs Power over Ethernet (PoE) 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 pigtails, 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 défectueuses ? Pouvez-vous commander une pièce en grandes quantités si votre projet l'exige? 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?

Consommation énergétique. Pour les installations à distance, la consommation d'énergie est le problème le plus critique . Si les appareils doivent être alimentés par des panneaux solaires, il est très important de choisir celles qui exigent la plus petite énergie possible. Le coût des panneaux solaires et des batteries peut être beaucoup plus élevé que le coût des dispositifs sans fil. Ainsi une faible consommation d'énergie peut entraîner un budget global beaucoup plus faible.

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 débit imposées par le logiciel et si oui, quel est le prix pour augmenter ces limites? Quelles sont les dimensions du dispositif? Permet-il le PoE comme source d'énergie?

Le dispositif fournit-il l'encryptage des données, le NAT, les outils de surveillance de bande passante ou autres caractéristiques critiques 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 réseautage. 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 mieux 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 des pièces d'origine locale ou même fabriquées localement. Ceci est une vérité économique de base dans la plupart des régions du monde. Au stade actuel de la technologie humaine, la distribution globale de l'information est tout à fait triviale 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 pouvez échanger de l'argent contre de l'équipement qui peut résoudre un problème particulier dans un temps comparativement court. L'art de construire une infrastructure de télécommunications locale se trouve dans une bonne balance entre l'argent et l'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 sur le marché local 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 implémentations 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 « faites-le vous-même ». 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 réparer, un bon fabricant saura vous assister. 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 site. Naturellement, tout ceci implique que l'équipement aura un coût initial comparativement plus élevé que les composantes disponibles sur le marché local.
Du point de vue d'un architecte de réseau, les trois plus grands risques cachés des solutions commerciales sont: *rester prisonnier d'un fournisseur*, la discontinuité des *produits*, et les *coûts continuels des licences*. Il peut être onéreux de permettre au leurre des nouvelles « caractéristiques » mal-définies de conduire 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).

Quand 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 propriétaire, il est peu probable qu'elle l'abandonnera simplement pour utiliser 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 combinaison avec le 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 propriétaires de ce fabricant, achèteront le tout dernier modèle (qui est presque toujours plus cher). Les effets à long terme de ces deux stratégies (rester prisonnier d'un fournisseur et discontinuité des produits) 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 propriétaire, vous pourriez avoir à renouveler une licence pour utiliser ce code 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, certains équipements sont conçus pour simplement cesser 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 continuels des licences.

En utilisant un équipement générique qui supporte 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 utilise 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 chez un autre fournisseur qui soit interopérable avec ce que vous avez déjà acheté. C'est pour ces raisons que nous recommandons d'utiliser des protocoles propriétaires 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 utilisant 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 accompliront la même tâche efficacement.
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). Occasionnellement, il y a eu des vendeurs qui ont profité du cadeau que les programmeurs de logiciels libres ont offert au public, en vendant le code sur une base de licences continuelles, violant de ce fait les termes de distribution déterminés par les auteurs originaux. Il serait sage d'éviter de tels fournisseurs et d'être sceptique envers 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.

Quand des problèmes 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 membres de votre équipe qui soient assez compétents et assez dévoués pour fournir une solution à votre problème de communication, alors lancer un projet de réseau peut prendre un temps considérable. Naturellement, le simple fait de « jeter de l'argent sur le problème » ne garantit pas non plus qu'une solution sera trouvée. Alors que 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 une balance entre les solutions commerciales et DIY (Faîtes-le vous-même) qui conviennent à votre projet.

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

Lors de l'examen qui l'équipement à utiliser, n'oubliez pas de comparer la distance utile espérée, la fiabilité et le débit, en plus du prix.

Et enfin, assurez-vous que les radios que vous achetez fonctionnent dans la bande sans licence où vous les installez, ou que vous avez un budget et l'autorisation de payer pour les licences appropriées si vous devez utiliser un spectre sous licence.

Protection professionnelle contre la foudre

La foudre est un prédateur naturel pour les équipements sans fil. Une carte montrant la répartition mondiale de la foudre pendant la période 1995-2003 est présentée ci-dessous.

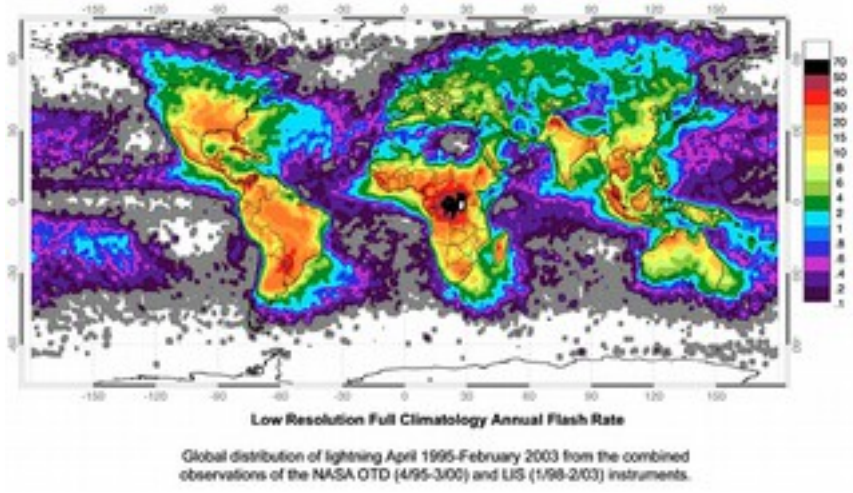


Figure HW 2 : Répartition mondiale de la foudre de 1995 à 2003

La foudre peut attaquer ou endommager l'équipement de deux façons différentes: 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 entre elles, cet éclair causera les électrons dans les câbles de s'éloigner de la foudre, créant du courant sur les lignes. Cet évènement génèrera beaucoup plus de courant que ce que l'équipement par radio peut supporter. L'un ou l'autre typede foudre détruira généralement tout équipement non protégé.

Figure HW 3: 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 foudres directes et d'induction. Alors qu'il n'est pas nécessaire d'utiliser toutes les méthodes de protection contre la foudre, le fait d'utiliser 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 creusée, 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 ou 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 tressé 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 tubes 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.

Configuration du point d'accès

Cette section fournit une procédure simple pour la configuration de base des points d'accès et des clients WiFi en passant en revue les principaux paramètres et en analysant leurs effets sur le comportement du réseau.
La section proposera également quelques trucs et astuces et conseils de dépannage pratiques.

Avant de commencer

Lorsque vous recevez de nouveaux équipements sans fil, prenez un certain temps pour vous familiariser avec ses principales caractéristiques et assurez-vous que :

- Vous téléchargez ou autrement obtenez tous **les manuels utilisateurs** et **fiches techniques** de spécification disponibles pour les périphériques que vous allez déployer.
- Si vous avez des périphériques d'occasion, assurez-vous de recevoir des informations complètes sur leur configurations actuelle ou dernière configuration connue - (par exemple mot de passe, adresses IP, etc.)
- Vous devriez déjà avoir un plan en main pour le réseau que vous allez déployer (y compris le **budget de liaison**,la **topologie du réseau**, **les canaux et les paramètres IP**).
- Etes prêt à prendre des notes écrites de tous les paramètres que vous allez appliquer (spécialement les **mots de passe** !)
- Faites des sauvegardes de fichiers de la dernière bonne configuration connue.

Contact avec le dispositif

Dans un premier temps, il est important que vous appreniez la signification de tous les voyants lumineux (LEDs) sur l'appareil. La figure ci-dessous montre la face avant typique d'un point d'accès, avec plusieurs LED allumés.

Figure HW 4 : Le devant d'un point d'accès typique.

Les LEDs indiquent généralement :

- Présence d'énergie électrique
- Ports actifs / trafic (couleur jaune / vert)
- Etat d'erreur (couleur rouge)
- Intensité du signal reçu (les barres du LED, parfois à plusieurs couleurs; certains dispositifs peuvent même être configurés pour allumer chaque LED à des seuils spécifiques de chaque, par exemple Ubiquiti).

Parfois, des significations différents sont associées au même LED en utilisant différentes couleurs et différents dynamiques (par exemple le LED est allumé/éteint /clignotant à différentes vitesses).
Vous devez identifier les différents ports et interfaces de l'appareil :

- Interfaces radio, parfois appelés réseaux locaux sans fil (WLANs). Elles devraient avoir un ou plusieurs connecteurs d'antenne ou des antennes (ou des antennes non détachables).
- Une ou plusieurs interfaces Ethernet :
- Un ou plusieurs ports pour réseau local (LAN)
- Un port pour la liaison montante (également appelé WAN)
- L'alimentation en entrée (5, 6, 7, 5, 12V ou autre, généralement DC). Il est vraiment (vraiment) important que l'alimentation corresponde à la tension! Parfois, l'énergie est fournie à l'appareil via le même câble UTP qui transporte les données Ethernet: c'est ce qu'on appelle Power-over- Ethernet (PoE) .
- Bouton d'alimentation (pas toujours présent) .
- Bouton de réinitialisation (souvent «cachée» dans un petit trou, peut être pressé en utilisant un trombone déplié).

Le bouton de réinitialisation peut avoir des effets différents (allant d'un simple redémarrage à une réinitialisation d'usine complète) si pressé brièvement vs pour un temps plus long.
Il peut prendre 30 secondes ou plus pour déclencher une réinitialisation complète.

REMARQUE : La réinitialisation complète (c.-à-d. réinitialiser aux paramètres d'usine)d' un dispositif qui est dans un état inconnu peut être une tâche pénible !

Soyez sûr de garder des notes écrites de paramètres critiques tels que l'adresse IP de l'appareil et le masque de réseau, et le nom d'administrateur et mot de passe.
La figure suivante montre un point d'accès Linksys commun avec alimentation en entrée, les ports réseau, le bouton de réinitialisation et deux antennes.

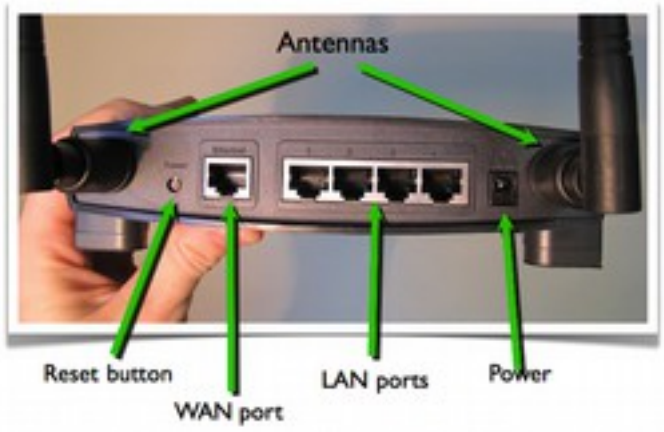


Figure HW 5 : Point d'accès Linksys

Interfaces utilisateur

Vous pouvez interagir (par exemple donner des commandes et modifier les paramètres) avec le point d'accès de plusieurs manières, en fonction du matériel que vous utilisez. Les manières possibles sont les suivantes:

- Interface utilisateur graphique (page web).
- Interface utilisateur graphique (logiciel d'application propriétaire).
- Une interface en ligne de commande (telnet, ssh)
- Interface logiciel embarqué dans le système (quand l'AP/client est un ordinateur ou un smartphone avec un écran et son propre système d'exploitation).

Les interfaces utilisateur : l'interface graphique (page web)

Ce système est utilisé dans les point d'accès Linksys, Ubiquiti et la plupart des point d'accès moderne. Une fois que vous êtes connecté à l'AP, vous interagissez avec le dispositif en utilisant un navigateur normal .

Avantages : elle fonctionne avec la plupart des navigateurs et systèmes d'exploitation.
Inconvénients : l'interface statique ne reflète pas les changements immédiatement, mauvaise rétroaction, peut être incompatible avec certains navigateurs, exige une configuration TCP/IP fonctionnel.
Certaines implémentations récentes (par exemple, Ubiquiti ci-dessous) sont très bons et utilisent des fonctionnalités web dynamiques modernes pour fournir la rétroaction et des outils avancés.

Figure HW 6 : interface utilisateur Ubiquiti.

Les interfaces utilisateur : l'interface graphique (logiciel d'application)
Dans ce cas, vous avez besoin d'un logiciel spécial pour interagir avec le dispositif.

Ce système est utilisé dans les points d'accès Mikrotik (appelé WinBox), Apple (appelé Utilitaire Airport), Motorola (appelé Canopy), et beaucoup d'anciens points d'accès.

Avantages: interfaces généralement puissants et attrayants ; permettent une configuration en lot de plusieurs périphériques.
Inconvénients : solutions propriétaires, le plus souvent disponibles pour un seul système d'exploitation, le logiciel doit être préinstallé avant de commencer la configuration. Mikrotik WinBox, ci-dessous, est une solution très puissante et peut gérer de grands réseaux.

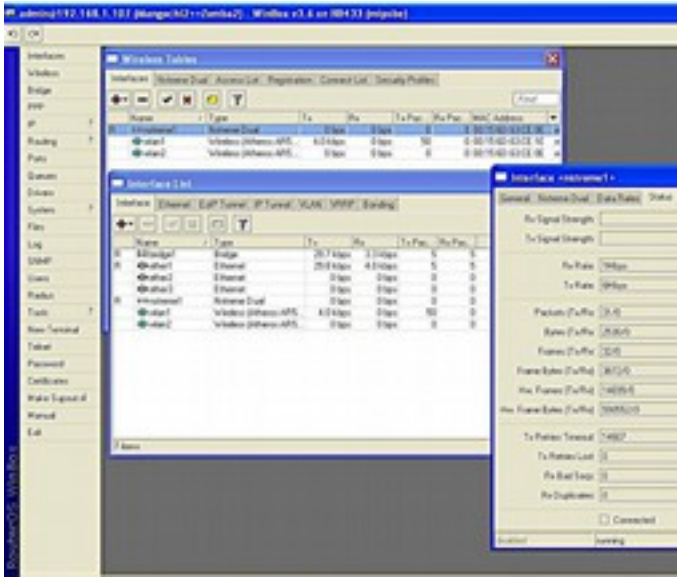


Figure HW 7: Mikrotik WinBox .

Les interfaces utilisateur: l'interface en ligne de commande (parfois appelé shell)
Dans ce cas, vous vous connectez à l'appareil en utilisant une connexion série ou Ethernet, via telnet ou ssh. ssh est beaucoup plus sûr que telnet du point de vue de la sécurité (ce dernier devrait être évité si possible). La configuration est réalisée avec des commandes exécutées sur le système d'exploitation hôte, habituellement un variante de Linux ou un système d'exploitation propriétaire, comme indiqué sur la page suivante. Ce système est utilisé par Mikrotik (appelé RouterOS), Ubiquiti (appelé AirOS), les points d'accès haut de gamme (Cisco) et des points d'accès incorporés dans les ordinateurs portables.
Avantages : très puissant car il peut être scripté.
Inconvénients: difficile à apprendre.

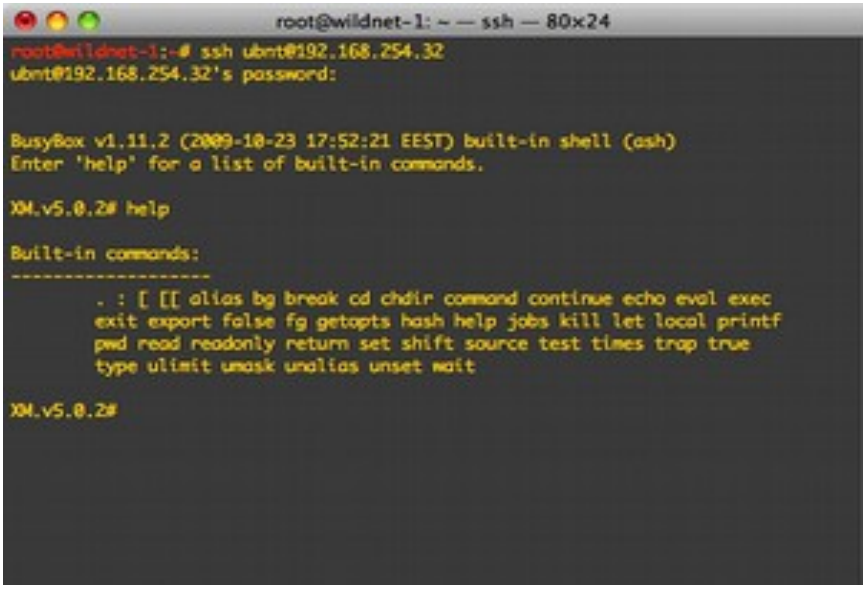


Figure HW 8 : Command Line Interface .

Configurer le point d'accès

Avant de configurer l'AP, n'oubliez pas de :

- Commencez à partir d'un état connu, ou réinitialiser l'appareil aux paramètres d'usine (toujours une bonne idée!) .
- La connexion à l'appareil via Ethernet est généralement plus facile que via réseau sans fil. La plupart des appareils avec une interface web ont une configuration IP par défaut sur le réseau 192.168.0.0, mais ce n'est pas une règle! Lisez le manuel.
- Si convenable, mettre à jour le firmware à la dernière version stable (mais attention !)
- Changer le nom d'utilisateur par défaut admin et le mot de passe d'abord!
- Changez le nom de l'appareil avec quelque chose qui l'identifie clairement (par exemple, quelque chose comme « AP_conference_room_3» ou «hotspot_public_area») .

  Cela vous aidera à reconnaître l'AP à l'avenir lorsque vous vous vous y connectez sur le réseau .
- La mise à jour du firmware est souvent une procédure risquée.

Avant de tenter de le faire, assurez-vous de prendre toutes les précautions comme - raccordement de l'appareil et l'ordinateur à un onduleur, et puis ne pas effectuer la mise à jour du firmware en faisant d'autres tâches sur l'ordinateur, et vérifier que vous avez une image binaire valide du firmware, lire attentivement les instructions ! Si la procédure échoue, vous pouvez vous retrouver avec un appareil inutilisable qui ne peut être récupéré (la soi-disant «brique») .

• N'oubliez pas d'écrire (et stocker dans un endroit sûr) tous ces paramètres, en particulier le nom d'utilisateur administrateur/mot de passe.

Configurer l'AP - couche IP

Si vous êtes à l'aise avec ce que vous faites, vous pouvez effectuer la configuration IP après la configuration sans fil pour éviter la reconfiguration et la reconnexion de votre PC ou ordinateur portable. Mais de cette façon, si vous faites une erreur à la fois dans une configuration filaire et sans fil, vous pouvez vous retrouver avec un AP inaccessible . Nous aimerions vous conseillons vivement de suivre les étapes de configuration critique une à la fois, de vérifier l'état de l'appareil après chaque étape. N'oubliez pas d'écrire (et stocker dans un endroit sûr) tous les paramètres IP!

Configurez l'interface Ethernet de l'AP selon la configuration de votre réseau filaire :

• Adresse IP/masque de réseau/passerelle ou DHCP

• Adresse(s) DNS

• Revérifier les nouveaux paramètres et de les appliquer (parfois vous pouvez avoir à redémarrer l'AP)

• Maintenant, vous pouvez avoir besoin de reconfigurer votre PC /ordinateur portable pour la correspondance avec la nouvelle configuration Ethernet, et se reconnecter à l'AP.

Configurer l'AP - couche physique

• Configurer le mode : **maître** (ou **point d'accès** ou **station de base**). Le mode de l'appareil peut généralement être configuré comme : "maître" (également appelé " point d'accès " ou " station de base " ou "BS"), " client " (également appelé " géré " ou "station" ou " poste client " ou " CPE "), " moniteur ", " WDS " (Wireless Distribution System), et rarement d'autres variantes.

• Configurez le SSID (Service Set Identifier, le nom du réseau sans fil créé par l'AP, jusqu'à 32 caractères de longueur) : il est préférable de choisir un nom significatif. Rappelez-vous que «la sécurité par obfuscation n'est pas une sécurité réelle», ainsi un SSID caché ou faux n'ajoute pas beaucoup de sécurité à votre réseau .
• Configurer le canal sans fil, selon les réglementations locales et le résultat de l'étude du site.
• Ne pas utiliser un canal qui est déjà occupé par un autre point d'accès ou d'autres sources d'énergie RF. Vous devriez déjà avoir prévu le canal à l'avance, au cours de la phase de conception. Le choix du meilleur canal est parfois une tâche difficile, et vous devrez peut-être effectuer une étude du site avec des outils logiciels (sniffers sans fil) ou analyseurs de spectre matériel (comme le WiSpy de MetaGeek et l'AirView de Ubiquiti) .
• Configurer la puissance de transmission et la vitesse du réseau (ces valeurs peuvent également être configurées comme «automatique» dans certains appareils). La valeur de puissance d'émission est également soumise à la réglementation locale. Vérifier à l'avance la puissance maximale permise par la loi et essayez toujours d'utiliser la valeur minimale qui correspond à vos besoins, afin d' éviter les interférences avec d'autres réseaux (le vôtre ou autres).

Le choix de la vitesse du réseau est limitée aux valeurs fournies par les normes 802.11a/b/g/n (jusqu'à 54 Mbps), mais certains fournisseurs créé des extensions aux normes (souvent appelé modes « turbo ») de 100 Mbps ou plus. Ces modes ne sont pas standards et peuvent ne pas être capables d'inter-opérer avec des équipements d'autres fournisseurs.

La configuration des modes en «compatibilité descendante » (tels que le soutien 802.11b sur les réseaux 802.11g) réduira le débit global disponible de vos clients les plus rapides. Le point d'accès doit envoyer le préambule à un rythme plus lent pour les clients 802.11b, et les communications réelles entre le client et l'AP se produiront aux vitesses 802.11b. Cela prend plus de temps, et ralentit les clients 802.11g qui sont autrement plus rapides.

Configurer l'AP - sécurité

Les paramètres de sécurité sont souvent un choix difficile, et il peut être difficile de concilier une bonne protection contre les utilisateurs non intentionnels avec un accès facile pour les utilisateurs autorisés.

Les besoins de sécurité plus complexes nécessiteront une configuration plus complexe et des logiciels supplémentaires.
Configurer les fonctions de sécurité du réseau :

- Pas d'encryptage (tout le trafic est en clair)
- WEP (Wired Equivalent Privacy), clés de 40 ou 104 bits, il est imparfait et donc obsolète.
- WPA / WPA2 (WiFi Protected Access) : PSK, TKIP et EAP
- Activer ou désactiver (cacher) la diffusion SSID (« balise »). Cacher le SSID et le filtrage MAC n'ajoutent pas beaucoup de sécurité, et sont difficiles à maintenir et une source de problèmes pour les utilisateurs inexpérimentés du réseau.
- Activer ou désactiver une liste de contrôle d'accès (basée sur les adresses MAC des clients). Le filtrage MAC est une mesure de sécurité faible: - Un client malveillant peut capturer des paquets et de découvrir les adresses MAC qui ont le droit de s'associer, il peut alors modifier sa propre adresse MAC à l'une des celles qui sont reconnues et «tromper» le point d'accès.
-

Pour plus d'informations sur la façon de concevoir la sécurité de votre réseau sans fil, veuillez s'il vous plaît lire le chapitre intitulé La sécurité dans les réseaux sans fil .

Configurer l'AP - routage / NAT

Les fonctionnalités d'une couche IP avancée et de configuration de routage sont souvent incluses dans les points d'accès modernes.
Cela peut inclure des fonctionnalités pour le routage et traduction d'adresses réseau (NAT), en plus du pontage de base.

La configuration IP avancée comprend :

- Le routage statique
- Le routage dynamique
- NAT (masquerading, port forwarding)
- Pare-feu
- Certains points d'accès peuvent également agir en tant que serveurs des fichiers et serveurs d'impression (le disque dur externe et imprimantes peuvent être connectés via USB).

Configurer l'AP - avancé

Un peu plus de réglages avancés peuvent être disponibles pour votre AP, selon le modèle / fournisseur / firmware / etc.

- Intervalle de balise (Beacon)
- Le mécanisme RTS/CTS . RTS/CTS (ready to send, clear to send) peut contribuer à atténuer le problème de nœuds cachés (clients qui peuvent « entendre » l'AP, mais pas les autres clients, créant ainsi des interférences) .
- La fragmentation. La configuration de la fragmentation peut être utilisée pour augmenter les performances dans le cas des zones de faible signal, celles de couverture marginale, ou des liaisons longues.
- Robustesse à l'interférence
- Extensions fournisseurs aux normes WiFi
- Autres paramètres pour les liaisons longue distance (10 à 100 km) et une meilleure sécurité.

Configurez le client

La configuration du côté client est beaucoup plus simple :

- Configurer le mode : client (ou géré, station, station de client, CPE)
- Configurez le SSID du réseau à joindre
- Le canal, la vitesse et d'autres paramètres se règlent automatiquement en fonction du point d'accès.
- Si WEP ou WPA est activé sur l'AP, vous devrez entrer le mot de passe correspondant (la clé)
- Les clients peuvent aussi avoir des paramètres supplémentaires (souvent propriétaires). *Par exemple, certains clients peuvent être configurés pour s'associer uniquement avec un AP ayant une adresse MAC spécifiée .*

Conseils - travailler à l'extérieur

- Vous devriez essayer de configurer les périphériques (les deux points d'accès et clients) à l'avance et dans un endroit confortable comme un laboratoire.

Le travail à l'extérieur est plus difficile et peut conduire à des erreurs (Configuration « sur site » = difficulté) .

• Si vous devez configurer des périphériques à l'extérieur, assurez-vous que la batterie de votre ordinateur portable est suffisamment chargé, d'avoir toutes les informations nécessaires avec vous (sur papier, pas uniquement en format électronique !) et d'avoir un bloc-notes pour prendre des notes. Une bonne documentation est primordiale pour les maintenances futures sur terrain.

Dépannage

• Organiser votre travail en étapes logiques et les suivre.

• Lisez le manuel, étudier la signification des paramètres et réglages, conduisez des tests et des expériences (n'ayez pas peur!) .

• En cas de problèmes, réinitialiser aux paramètres d'usine et essayez à nouveau.

• Si le problème persiste, essayez à nouveau en changeant un paramètre/réglage à la fois.

• Ca ne fonctionne toujours pas ? Essayez de rechercher sur le web des mots-clés pertinents (nom de l'appareil, etc.), recherchez dans les forums et sur les sites du fabricant/fournisseur.

• Mettez à jour le firmware à la dernière version .

• Si vous avez encore des problèmes, essayez avec un autre client/AP pour vérifier si vous avez un problème matériel avec l'original.

12. INSTALLATION INTÉRIEURE

Introduction

Les éditions précédentes de ce livre ont mis un grand accent sur les réseaux étendus sans fil comme moyen de relier les communautés entre elles et à l'Internet.
Toutefois, avec la disponibilité des points d'accès Wi-Fi à bas prix et la prolifération des appareils portables munis des capacités WiFi, WiFi est devenu une norme de fait pour l'accès au réseau intérieur dans les entreprises et les écoles.
Ce chapitre présente les principaux points de discussion dans le choix et l'installation de réseaux WiFi à l'intérieur.

Préparations

Avant d'installer un réseau local sans fil, c'est une bonne idée de prendre le temps de réfléchir un peu sur:

• Qu'est-ce que vous envisagez de faire avec le réseau sans fil?
Est-ce une addition au réseau câblé ou son remplacement ? Allez-vous exécuter sur le réseau des applications qui ne sont pas tolérants aux délais ou sensibles aux variations de largeur de bande (comme la voix et la vidéoconférence).
• La différence principale entre le sans-fil intérieur et extérieur est l'absorption et la réflexion des ondes radio par le bâtiment lui-même. Quelles sont les caractéristiques du bâtiment dont vous devez prendre compte? Est-ce que les murs contiennent du métal, de l'eau ou du béton lourd? Est-ce que les fenêtres contiennent du métal (par exemple, un revêtement métallique ou grilles métalliques) ? Est-ce que le bâtiment est long et étiré ou compact ?
• Espérez-vous des utilisateurs qui seront essentiellement statiques ou vont-ils se déplacer beaucoup? Et quand ils se déplaceront, il est important d'avoir un transfert intercellulaire (en anglais handover) sans interruption (ce qui signifie, un transfert aussi rapide que vous ne verrez pas l'interruption d'un appel vocal) ?
• Y a-t-il de bons endroits pour accrocher les points d'accès ? Est-ce les prises des câbles et d'électricité pour les points d'accès sont

facilement accessibles? L'électricité est- elle stable? Sinon, même les points d'accès intérieurs pourraient avoir besoin d'une alimentation solaire/batterie stable et/ou un UPS.

• Y a-t-il des sources d'interférence, comme les points d'accès ad hoc provenant des utilisateurs, les dispositifs Bluetooth, micro-ondes ?

Exigences de largeur de bande

La première étape dans la conception d'un réseau sans fil à l'intérieur est de déterminer la nécessité en termes de nombre d'utilisateurs simultanés que le réseau peut supporter, le nombre et le type de dispositifs et le type d'applications qu'ils exécutent. Il est également important de comprendre la distribution des utilisateurs.

Les amphithéâtres ou les salles de réunion ont des profils d'utilisation différents des couloirs.

Un réseau sans fil qui est à peine utilisé et qui doit supporter un faible nombre d'utilisateurs est facile à déployer et ne pourra pas expérimenter des ennuis facilement. Le problème commence lorsque le nombre d'utilisateurs et leur utilisation du réseau augmente.

Ce chapitre se concentre donc sur les réseaux sans fil à haute densité. La table suivante vous donne une idée de l'exigence de largeur de bande pour certaines applications typiques:

Surfer sur le web:	500 - 1000 kb/s
audio:	100 - 1000 kb/s
streaming video:	1 - 4 Mb/s
partage des fichiers:	1 - 8 Mb/s
périphérique de sauvegarde:	10 - 50 Mb/s

Les installations typiques dans un environnement de bureau sont dimensionnées pour supporter 20-30 utilisateurs par cellule et ont environ 1 point d'accès par 250-500 mètres carrés. Cependant, comme mentionné précédemment, dépendant des caractéristiques de l'environnement, ceci peut ne pas être suffisant. Dans un environnement dense, il peut y avoir jusqu'à 1 appareil sur une surface de 20 mètres carrés. En fin de compte, vous devez calculer le débit nécessaire par couvrir votre zone.

Donc, si vous avez disons 10 utilisateurs dans une zone de 100 mètres carrés, dont 8 sont en train de surfer le web et 2 sont à regarder la vidéo en ligne, vous aurez besoin de: 8 * 1000 kb/s + 2 * 4000 kb/s = 16000 kb/s pour la zone de 100 mètres carrés ou 160 kb/s par mètre carré.

Les fréquences et les débits de données

Les solutions sans fil 2.4 GHz et 5 GHz diffèrent par quelques points essentiels. La bande de 2,4 GHz a une meilleure portée et moins d'atténuation et est supportée par la plupart des dispositifs dans fil. Le principal inconvénient de la bande 2,4 GHz est qu'il n'y a que 3 canaux qui ne se chevauchent pas, ce qui limite considérablement le nombre de points d'accès qui peuvent être placés dans une certaine zone. Ceci est regrettable car la fabrication de plus petites cellules (conçues pour avoir des points d'accès diffusant avec moins de puissance) est la meilleure façon de fournir plus de débit par zone.
Remarque: parfois le chevauchement léger de 4 canaux est conseillé, mais la recherche montre qu'en fait, ceci diminue la performance. En général, la performance se dégrade rapidement avec le chevauchement des canaux (interférence co-canal) . La bande des 5 GHz, d'autre part a une portée pire, mais a dans la plupart des zones géographiques autour de 20 canaux. Ce qui la rend beaucoup plus facile à déployer sans interférence entre canaux adjacents. Le choix de la norme WiFi est un autre élément important, étant donné que le débit moyen en Mo/s pour les technologies les plus courantes est de:

11b:	**7.2 Mb/s**
11g:	**25 Mb/s**
11a:	**25 Mb/s**
11n:	**25 - 160 Mb/s**

Il convient de noter que le rendement baisse lorsque, par exemple, à la fois des dispositifs 802.11b et 11g sont desservis par le même point d'accès. Dans un réseau où les machines clientes utilisent une combinaison de norme 802.11g et 11b, le point d'accès fonctionnera vers le bas de sa capacité à des vitesses inférieures. La bande de 5 GHz est un choix préféré pour les réseaux de grande performance et grande densité. Comme vous voulez de toute façon limiter la couverture de chaque point d'accès à une

petite zone bien définie, l'atténuation du signal par des murs, etc. est un avantage plutôt qu'un problème. Le déploiement de la bande 2,4 GHz pour la majorité des dispositifs combiné avec la bande 5 GHz pour les ``dispositifs importants" est à considérer aussi.

Points d'accès choix et placement

Quand il s'agit de choisir les points d'accès (PA) sans fil d'intérieur, il y a essentiellement deux choix architecturaux : point d'accès ``basés contrôleur" et ``clients plats". Les clients plats sont des points d'accès autonomes qui ont toute l'intelligence à bord pour gérer un réseau WiFi (choix SSID, méthode de cryptage, de routage/commutation, etc.).
La solution basée sur un contrôleur de l'autre côté comporte de points d'accès qui disposent de fonctionnalité minimale pour offrir un service sans fil avec un contrôleur central commun pour tous les points d'accès à un emplacement .
Le contrôleur central a aussi toute l'intelligence et tout le trafic venant des points d'accès qui lui est adressé. Le choix entre l'une des deux architectures est un compromis entre le coût, la facilité de gestion et l'évolutivité. En général, on peut dire que plus l'environnement est complexe et plus la taille est grande, plus cela devient attrayant d'implémenter une solution basée sur un contrôleur. Les points d'accès doivent en général être placés dans les zones à forte densité d'utilisateurs. Le signal débordera probablement suffisamment pour aussi desservir les zones moins denses. Malheureusement, la performance globale du système sera principalement déterminée par les clients, et non les points d'accès, de sorte que le placement des points d'accès, bien qu'importante, ne peut pas beaucoup influencer la performance de l'ensemble du système. D'autres sources radio opérant dans les bandes WiFi ont une très forte influence sur la performance du réseau WiFi. Ainsi, en général, les points d'accès doivent, autant que possible, être si possible isolés des autres sources radio en utilisant les murs, les plafonds et les gens comme «boucliers». Il est possible d'utiliser des antennes externes afin d'améliorer la performance. Les antennes omnidirectionnelles sont les plus couramment utilisées et elles fournissent une zone de couverture plus ou moins circulaire autour du point d'accès. Cependant, dans la plupart des cas à l'intérieur, les points d'accès seront installés sur les murs, les plafonds ou les colonnes, et les antennes omnidirectionnelles sont un mauvais choix, si vous regardez où vont les ondes radio, et où les utilisateurs sont.

Ainsi, dans les cas où le point d'accès n'est pas au centre de la zone à couvrir, des antennes directives sont une alternative.
Certains hôtels et salles de conférence, par exemple, placent des petites antennes directionnelles dans les coins de grands espaces ouverts ou suspendus pour fournir un couloir pour la couverture du signal dans les grands espaces. Gardez à l'esprit que les nombreuses réflexions généralement rencontrées dans un environnement intérieur rendent difficile d'essayer de contrôler totalement une couverture spécifique.
Les points d'accès peuvent être montés sur le plafond, sur les murs ou des meubles, chacun ayant des caractéristiques différentes. Le montage au plafond donne une bonne couverture globale, le montage mural souvent approche les points d'accès aux utilisateurs et les points d'accès placés sous les tables ou les chaises ou dans les meubles peuvent utiliser l'isolement naturel pour créer de petites cellules ayant peu d'interférences avec les points d'accès voisins, mais il pourrait y avoir des préoccupations au sujet de la possibilité d'effets nocifs du rayonnement émis .
Enfin, pour les réseaux exigeant vraiment une grande performance, les points d'accès avec la technologie d'antenne adaptative à puce pourrait être une option. Ils s'obtiennent à un prix, mais offrent l'avantage d'adapter le signal radio à l'emplacement des utilisateurs dynamiquement - ils dirigent les ondes radio là où elles sont nécessaires, à tout moment dans le temps.

SSID et architecture réseau

Les réseaux d'intérieur sont susceptibles de servir de nombreux utilisateurs simultanés. Les grands complexes comme un campus universitaire sont généralement constitués de plusieurs bâtiments, chacun avec son propre réseau intérieur et des réseaux extérieurs entre eux. Il est donc important de réaliser un bon plan pour vos SSIDs. Notez que le SSID définit le domaine de diffusion de couche 2 du réseau. La planification SSID doit aller de pair avec votre architecture de couche 3 du réseau. Si vous souhaitez que les utilisateurs de se déplacent de manière transparente sur l'ensemble de la zone couverte par votre réseau sans fil, à l'intérieur tout comme au-delà même d'un bâtiment, tous les points d'accès devraient offrir le même SSID, par exemple «UniversityWireless», ou «eduroam» pour une université qui veut participer au service d'itinérance mondiale qu'EDUROAM offre. Toutefois, les utilisateurs qui restent dans un SSID ne nécessitent pas ou demandent un nouveau bail DHCP, vous aurez donc à accommoder tous les utilisateurs dans un sous-réseau de couche 3.

Pour un grand campus, cela pourrait exiger un grand sous-réseau plat pour tous les utilisateurs sans fil.
C'est une situation de compromis - vous pouvez avoir soit d'énormes sous-réseaux avec une itinérance transparente, ou une architecture de sous-réseau plus gérable avec des SSID distincts tels que ``Bibliothèque", ``LectureHall", ``Cafétéria '', ...

Après installation

Maintenant que l'infrastructure est en place, il est important de s'assurer que tout fonctionne comme prévu et reste comme cela. Cela peut se faire sous la forme d' une étude de site, mesurant l'intensité des signaux et le débit. Mais à la fin la raison principale pour installer un réseau sans fil est de servir ses utilisateurs. Ainsi l'écoute des plaintes des utilisateurs ou leurs problèmes est tout aussi important.
La demande change constamment et il en va de même de l'état-de l'art. Il est important de garder à l'esprit les besoins des utilisateurs et les adapter aux mises à niveau prévues de la technologie que vous déployez.

13. INSTALLATION A L'EXTERIEUR

Bien que la technologie Wi-Fi a été conçue pour des réseaux locaux, son impact dans les pays en développement est plus dramatique dans les applications longue distance .

Dans les pays développés, les câbles à fibres optiques offrant de grandes largeurs de bande ont été installés pour satisfaire les besoins de communication de la plupart des villes. La pénétration de la fibre optique dans le monde en développement n'est pas aussi grande et est loin d'être suffisante pour couvrir les besoins. Et le coût de son expansion souvent ne répond pas à l'objectif de retour sur investissement (en anglais return of investment (ROI)) dans un délai de temps raisonnable des compagnies de téléphone. Les technologies sans fil, d'autre part, ont eu beaucoup plus de succès dans les pays en développement et la possibilité d'accroître la pénétration en utilisant les réseaux sans fil est énorme.

Les opérateurs télécoms ont installé des liaisons radio à micro-ondes traditionnelles dans la plupart des pays. Il s'agit d'une technologie mûre qui offre une grande fiabilité et une disponibilité atteignant 99,999 %. Toutefois, ces systèmes coûtent plusieurs milliers de dollars et exigent un personnel spécialement formé pour l'installation. Les systèmes par satellite se sont révélés bien adaptés pour le trafic de diffusion comme la télévision et pour certaines autres applications. Cependant, des solutions satellites sont encore coûteuses pour le trafic bidirectionnel, tandis que le WiFi est rentable du point de vue coût pour des réseaux point-à-point externes ainsi que les réseaux d'accès typiques (point-à-multipoint) où une station de base (BS) est au service de nombreux clients/CPEs. Dans ce chapitre, nous allons nous concentrer sur les liaisons externes point-a-point de point de longue distance. Deux obstacles importants doivent être surmontés avant d'appliquer WiFi sur des longues distances: les restrictions du bilan énergétique et les limites temporelles de synchronization.

Les autres limitations pour l'utilisation de WiFi sur des longues distances consistent dans l'exigence d'une ligne de mire entre les point extrêmes de la liaison longue distance et la vulnérabilité aux interférences dans la bande sans licence. La première limitation peut souvent être traitée en prenant avantage des élévations de terrain ou en utilisant des tours pour surmonter des obstacles tels que la courbure de la terre et pour obtenir un dégagement de la zone de Fresnel .

La ligne de mire n'est pas nécessaire pour les applications intérieures car les stations sont très rapprochées et la plupart des obstacles peuvent être franchis par les réflexions sur les murs, le plafond, etc. Mais pour les applications longue distance, la ligne de mire est absolument essentielle. La deuxième limitation est moins prononcée dans les zones rurales et peut être atténuée par une migration vers la bande des 5 GHz qui est moins encombrée. Le problème du bilan énergétique peut être résolu en utilisant des antennes à gain élevé et une radio puissante et très sensible attachée directement à l'antenne pour éviter la perte de câble RF. La limitation temporelle a à voir avec les techniques d'accès aux médias. WiFi utilise un procédé d'accès aléatoire pour partager le support de communication. Ce support est donc soumis à des collisions qui ne peuvent être détecté par air. Ainsi l'émetteur s'appuie sur la réception d'un accusé de réception pour chaque trame reçue avec succès. Si, après un certain laps de temps, appelé « ACKTimeout », la trame de reconnaissance reconnaître trame n'est pas reçue, l'émetteur enverra à nouveau la trame. Comme l'émetteur n'enverra pas une nouvelle trame avant que la reconnaissance de la trame précédente ne soit reçue, l'ACKTimeout doit être court. Ceci fonctionne bien dans le scénario initial prévu pour le WiFi (réseaux à l'intérieur) où le temps de propagation de 33,3 microsecondes par kilomètre est négligeable, mais ne marche pas pour des liaisons sur quelques kilomètres. Bien que de nombreux dispositifs WiFi ne contiennent pas de dispositions pour modifier l'ACKTimeout, le nouvel équipement destiné à des applications

extérieures (ou des tierces firmware tels que Open WRT) vous donnera cette possibilité, souvent au moyen d'un champ «distance» d'une interface utilisateur graphique (en anglais Graphical User Interface (GUI)). La modification de ce paramètre permettra un débit raisonnable, qui de toute façon diminuera proportionnellement à la distance. La fenêtre de contention «slot-time» doit également être augmentée pour s'adapter à de plus longues distances.

D'autres fabricants ont choisi de passer de l'accès aléatoire à l'accès multiple avec division temporelle (en anglais Time Division Multiple Access (TDMA)). Le TDMA divise l'accès à un canal donné en des multiples tranches de temps, et affecte ces tranches à chaque nœud sur le réseau. Chaque nœud transmet uniquement dans la tranche qui lui a été affectée, évitant ainsi les collisions. Dans une liaison point-à-point cela donne un grand avantage car les reconnaissances (ACKs) ne sont pas nécessaires parce que les stations prennent des tours pour transmettre et recevoir. Bien que cette méthode soit beaucoup plus efficace, elle n'est pas conforme à la norme WiFi. Ainsi plusieurs fabricants l'offrent comme protocole propriétaire, en option à côté de la norme WiFi. Le WiMAX ainsi que les protocoles propriétaires (comme Mikrotik Nstreme, ou Ubiquiti AirMAX) utilisent TDMA pour éviter ces problèmes de synchronisation des ACKs . La norme 802.11 définit la sensibilité du récepteur comme le niveau de signal reçu qui est nécessaire pour garantir un BER (taux d'erreur binaire) en-dessous de 10^{-5} . Ceci permet de déterminer la quantité d'énergie par bit requise pour surmonter le bruit ambiant ainsi que le bruit généré par le récepteur lui-même. Quand le nombre de bits/seconde transmis augmente, plus de puissance sera nécessaire au récepteur pour fournir la même énergie par bit. Par conséquent, la sensibilité du récepteur diminue à mesure que le débit de l'émetteur augmente de sorte à maintenir le même rapport signal/bruit comme la distance augmente le débit diminue, ou alternativement, pour des distances plus longues il faut choisir des débits plus faibles pour compenser la réduction de la puissance du signal avec la distance.

Que faut-il pour une liaison longue distance ?

Il y a quatre aspects qui doivent être pris en considération pour adapter les dispositifs WiFi aux longues distances : augmenter la portée dynamique de la radio; augmenter le gain de l'antenne; diminuer la perte de câble d'antenne, et prendre des dispositions pour le temps de propagation du signal.

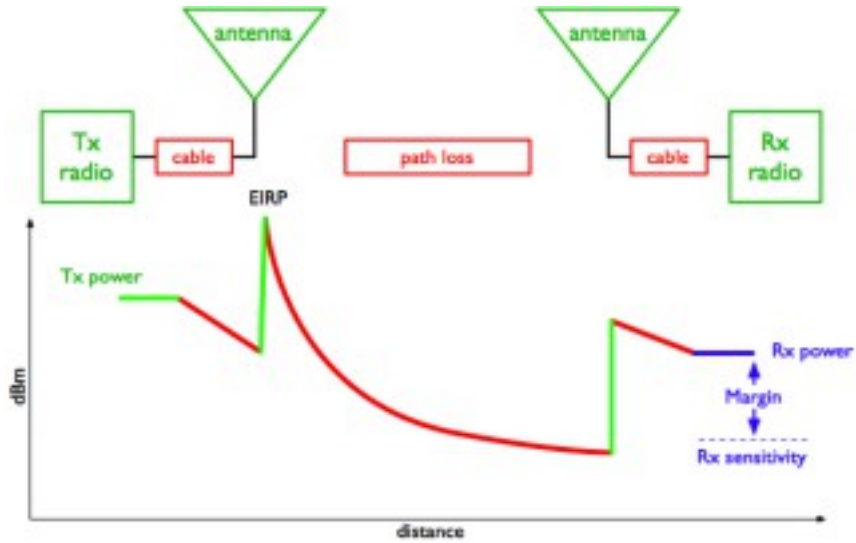


Figure OI 1: Puissance en dBm en fonction de la distance dans une liaison radio (bilan de puissance) .

Le graphique ci-dessus montre le niveau de puissance à chaque point d'une liaison sans fil. L'émetteur fournit une certaine quantité d'énergie. Une petite quantité est perdue en atténuation dans le câble RF entre l'émetteur et l'antenne ou dans le guide d'ondes. L'antenne concentre ensuite l'énergie, offrant un gain. A ce point, la puissance est à la valeur maximale possible pour la liaison. Cette valeur est appelée puissance rayonnée isotrope équivalente (Equivalent Isotropic Radiated Power (EIRP)) car elle correspond à la puissance que l'émetteur devrait émettre si l'antenne n'avait pas de gain. Entre les antennes d'émission et de réception, il y a les pertes en espace libre et d'environnement qui augmentent avec la distance entre les points extrêmes de la liaison.
L'antenne de réception fournit un certain gain supplémentaire. Ensuite, il

existe une petite quantité de perte entre l'antenne réceptrice et la radio réceptrice.
Si la quantité d'énergie reçue à l'autre extrémité est supérieure à la sensibilité de la radio réceptrice, la liaison est possible. L'augmentation de la puissance de transmission peut conduire à des violations de la réglementation du pays. Augmenter le gain de l'antenne est de loin le moyen le plus efficace pour améliorer la portée. Assurez-vous que la radio à utiliser dispose de connecteurs pour une antenne externe (certains appareils ont une antenne intégrée ou autrement une antenne non amovible).
La diminution des pertes dans les câbles d'antenne est toujours une issue importante, et la façon la plus radicale de l'atteindre est de placer la radio en dehors, directement reliée à l'antenne, en utilisant une boîte résistante aux intempéries. Souvent, cela prête à alimenter la radio avec le PoE (Power over Ethernet).
L'amélioration de la sensibilité du récepteur implique la sélection d'un modèle avec une meilleure performance, ou se contenter d'une vitesse de transmission plus faible où la sensibilité est plus élevée.
Bien que les antennes à gain élevé peuvent être coûteuses, on peut trouver dans de nombreux pays des antennes satellitaires qui ne sont plus utilisées et peuvent être modifiées pour les bandes WiFi. Dans un monde parfait, nous devrions utiliser les antennes à gain plus élevé avec les radios les plus fortes et les plus sensibles possibles. Mais un certain nombre de considérations pratiques rendent cela impossible. Les amplificateurs introduisent une faiblesse supplémentaire. En plus, ils pourraient violer la puissance maximale permise par les règlements locaux et ajouter du bruit à la réception. Ils doivent donc être évités. Les émetteurs à haute puissance sont disponibles auprès de nombreux fabricants qui offrent jusqu'à 1 W de puissance de sortie. Ils pourraient être utilisés à la place d'amplificateurs dans les pays où cela est légal. En général, il est préférable d'utiliser des antennes à gain élevé qu'un émetteur de grande puissance. Un gain d'antenne élevé aidera à la fois en émission et en réception résultant en un double impact dans le bilan de liaison.
Il causera également moins d'interférences aux autres utilisateurs et recevra moins d'interférences provenant d'autres utilisateurs et limitera les effets de trajets multiples.
Cependant, un gain d'antenne élevé implique une largeur de faisceau très étroit, ce qui signifie que des techniques d'alignement spéciales sont nécessaires.

L'alignement de l'antenne

Pour de courtes distances, lorsque l'antenne correspondante est visible, la procédure d'alignement de l'antenne se réduit à pointer l'antenne dans la direction de l'antenne correspondante, à la fois dans le plan horizontal (azimut) et dans le plan vertical (élévation). Cela devrait suffire pour établir la connexion.
Une fois que la connexion est faite, un réglage fin peut être obtenu par lecture du niveau de la force du signal reçu (en anglais le Receiver Signal Strength Level (RSSL)) dans la radio locale.
Cette valeur est fournie par l'interface utilisateur, et peut également être obtenue en utilisant des logiciels comme netstumbler.
La procédure consiste à déplacer l'antenne dans le plan horizontal par petites étapes en lisant le RSSL. Ne touchez pas l'antenne lors de la lecture puisque votre corps aura une incidence sur la mesure.
Une fois que vous êtes satisfait de la valeur maximale obtenue, la procédure est répétée dans le plan vertical, en déplaçant l'antenne d'abord et haut et ensuite vers le bas jusqu'à ce qu'une valeur maximale de la puissance reçue soit obtenue, point auquel les boulons qui fixent l'antenne sont serrés.
C'est tout ce qui est nécessaire pour aligner un dispositif client à un point d'accès ou une station de base.
Si vous avez une liaison point à point, la même procédure doit être répétée à l'autre extrémité de la liaison.
Pour les longues distances et lorsque l'autre extrémité de la liaison n'est pas visible, quelques étapes supplémentaires sont nécessaires. En premier lieu, la direction horizontale (de palier) pour aligner l'antenne doit être obtenue à partir des coordonnées des points d'extrémité.
Ensuite, une boussole est utilisée pour déterminer la direction dans laquelle l'antenne doit viser. Gardez à l'esprit qu'en général, il y a une différence entre le palier magnétique palier mesuré par le compas et le palier géographique obtenu à partir des coordonnées des points d'extrémité ou à partir d'une carte. Cette différence est appelée la déclinaison magnétique. Elle peut être très importante dans certains endroits et doit être prise en compte pour aligner correctement l'antenne.

La Figure OI 2 montre une différence de 8 ° entre le nord magnétique indiqué par le compas et le nord géographique ou vrai nord indiqué par la plaque de cuivre.

Figure OI 2: Différence entre le nord magnétique et géographique à El Baul, Venezuela en 2006 .

Gardez à l'esprit que le fer et d'autres métaux magnétiques auront une incidence sur la lecture de la boussole. Ainsi restez loin de ceux-ci au moment de la mesure. Si l'antenne doit être montée dans une tour d'acier, il pourrait être impossible d'obtenir une lecture précise à proximité. Au lieu de cela, il faut s'éloigner d'une certaine distance, utiliser la boussole pour déterminer la direction dans laquelle l'antenne doit viser, puis essayer de localiser un objet facilement reconnaissable qui peut être utilisé comme une référence pour orienter l'antenne plus tard. Comme l'ouverture du faisceau d'une antenne très directive pourrait être de seulement quelques degrés, après alignement avec la boussole, nous devons procéder à un réglage fin pour le bon alignement de l' antenne par mesure de la force du signal reçu.

Malheureusement, le RSSL indiqué par le logiciel de la radio ne fonctionnera qu'après qu'un paquet approprié soit reçu de façon satisfaisante et décodé. Et cela ne se produira que lorsque l'antenne est bien alignée. Ainsi, nous avons besoin d'un instrument qui permet de révéler la force du signal reçu de manière indépendante de la modulation qu'elle pourrait avoir. L'instrument nécessaire pour cette tâche est l'analyseur de spectre.

Il y a une grande variété d'analyseurs de spectre sur le marché, certains d'entre eux coûtant des milliers de dollars, mais si nous sommes seulement intéressés dans les bandes WiFi, on peut faire avec des solutions peu coûteuses comme celles-ci:

" RF Explorer" propose des dispositifs peu coûteux pour plusieurs bandes de fréquences. Le " RF Explorateur modèle 2.4G " sur http://www.seeedstudio.com/depot/-p-924.html?cPath=174 coûte 120 $ et est une unité autonome qui peut mesurer des signaux de 2,4 à 2,485 GHz, avec une sensibilité de -105 dBm. Il dispose d'un connecteur SMA pour l'antenne et est par conséquent bien adapté pour l'alignement de l'antenne.

" WiSpy " est un analyseur de spectre dans un dongle USB qui se fixe à un ordinateur portable. Vous aurez besoin des modèles avec connecteur SMA RP. Il en existe un de 2,4 GHz à prix modéré et un autre qui couvre à la fois les bandes de 2.4 et 5 GHz vendus pour 600 $ sur www.metageek.net.
« Ubiquiti Networks» sur www.ubnt.com vendait des analyseurs de spectre à dongle USB de la bande 2,4 GHz à 70 $.
Malheureusement, ils semblent avoir abandonné ce produit après intégration des fonctionnalités de l'analyseur de spectre dans leurs radios de la série M .
Ainsi, lors de l'utilisation de ces radios, vous pouvez profiter de leur outil d'alignement " AirView ". En principe une de ces radios peu coûteuses comme le " Bullet M " qui est livré avec un connecteur N mâle peut également être utilisée pour aligner des antennes pour d'autres radios dans les bandes 2,4 et 5 GHz. Malheureusement, le signal modulé numériquement transmis par les radios WiFi n'est pas bien adapté pour l'alignement de l'antenne, car sa puissance est répartie sur la largeur de bande de 20 MHz.
Pour l'alignement de l'antenne, une seule fréquence avec une puissance de sortie stable est nécessaire. Ce type de signal est produit par un générateur de signal de micro-ondes, mais ces générateurs de signaux sont très coûteux. Le " RF Explorateur modèle 2.4G " intègre un générateur de signal de 2,4 GHz, mais la puissance de sortie maximale de 1 dBm n'est pas bien adapté pour l'alignement d'antenne sur longues distances.
Au lieu de cela, nous avons redéfini des dispositifs appelés « émetteurs vidéo ", destinés à transmettre les signaux vidéo, pour jouer le rôle de puissantes sources individuelles de signaux de fréquence à micro-ondes en l'absence de modulation. Ils sont disponibles à la fois pour le 2,4 GHz et les bandes 5 GHz avec une puissance de sortie jusqu'à 33 dBm.

Pour nos fins, il est nécessaire d'acheter un modèle avec un connecteur d'antenne afin que nous puissions connecter notre propre antenne. Il y a beaucoup de vendeurs à choisir, voir par exemple :
http://www.lightinthebox.com/Popular/Wi0_Video_Transmitter.html

Comme un exemple de liaison de longue distance utilisant des dispositifs WiFi modifiés, nous pouvons parler d'une expérience réalisée en Avril 2005 au Venezuela entre Pico del Aguila (8,83274638 ° N, 70,83074570 ° W, 4100 m d'altitude) et El Baul (8,900000 ° N, 68,2000000 ° E, 70m d'altitude). En utilisant le logiciel Radio Mobile, nous constatons que la distance à El Baul est de 280 km, l'azimut est de 97 °, l'angle d'élévation de l'antenne est de -2,0 °, et l'endroit où le faisceau est plus proche du sol se situe à 246 km, où il libère 1,7 fois la première zone de Fresnel à la fréquence de 2,412 GHz.
La Figure OI 3 illustre la résultats du logiciel.

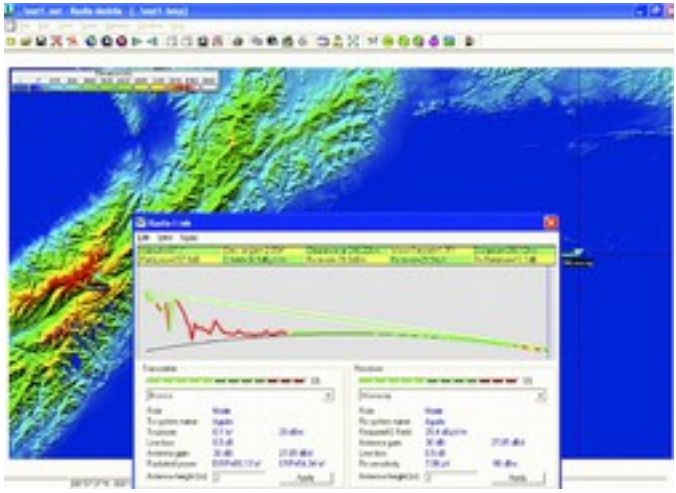


Figure OI 3: Profil d'une liaison de 280 km sur laquelle les dispositifs WiFi standard avec le firmware OpenWRT permettant l'augmentation des ACKTimeout ont été utilisés pour transférer des fichiers à environ 65 kb/s en Avril 2006 entre Pico del Aguila et El Baul au Venezuela.

Notez que la courbure de la terre est tout à fait évidente, et a été évitée parce que l'une des stations était à 4100 m d'altitude et l'autre à 70 m.
La fréquence était de 2412 MHz, la puissance de sortie de 100 mW, et un gain d'antenne d'environ 30 dBi. Le video streaming a été transmis avec succès en dépit de la bande passante limitée.
Un an plus tard l'expérience a été répétée avec le même équipement WiFi mais avec des antennes commerciales de 32 dBi aux deux extrémités et des résultats similaires ont été obtenus.

Enfin, un autre type de firmware mis au point par le groupe TIER à l'Université de l'Université de Berkeley qui implémente TDD (Time Division Duplexing) fut testé. Il montra un débit bidirectionnel remarquable de 6 Mbit/s avec le matériel de la norme 802.11b.

Le déplacement du site distant sur une colline élevée de 1400 m appelé Platillon (9,88905350 ° N, 67,50552400 ° W), fournit une liaison longue distance expérimentale sur 380 km où l'expérience a été répétée avec succès comme décrit dans la section Études de cas dans ce livre.
Ceci peut être illustré à l'aide d'une version en ligne de la radio mobile, disponible sur http://www.cplus.org/rmw/rmonline.html, qui est plus simple à utiliser, même si elle a une certaine limitation par rapport à la version téléchargeable. Il faut vous inscrire sur le site, entrez les coordonnées des points sur lesquels la liaison radio doit être établie, les valeurs de puissance pour les radios et les gains d'antennes et hauteur, et le logiciel ira chercher les données pertinentes d'altitude nécessaires pour effectuer la simulation de la liaison.

Gardez à l'esprit que seules les fréquences d'amateurs radio sont prises en charge dans la version web, donc le 2.3 GHz devrait être utilisé au lieu de 2,4 GHz, mais les résultats sont assez proches et validés par l'expérience sur le terrain.
Dans la figure OI 4, nous montrons les résultats de la simulation radio mobile en ligne pour cette expérience qui peut être reproduite par le lecteur comme un exercice .

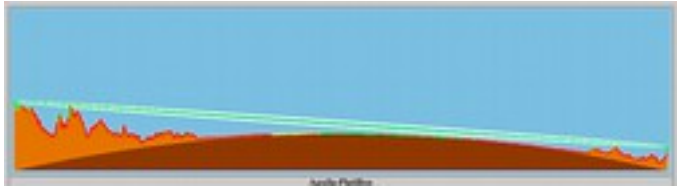


Figure OI 4: Profil d'un test de 380 km à 2,4 GHz réalisé en Avril et Août 2007 au Venezuela.

Notez que la courbure de la terre est d'autant plus perceptible sur le trajet de 380 km, mais la hauteur des points d'extrémité combinée avec le terrain plat entre ces points permet un dégagement suffisant de la première zone de Fresnel .

La Figure OI 5 montre les valeurs numériques de la simulation radio mobile en ligne:

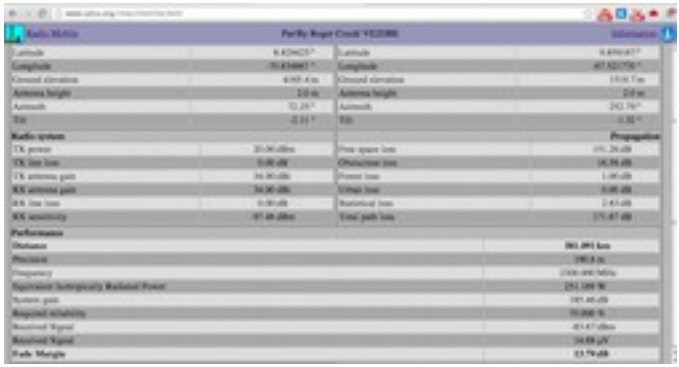


Figure OI 5: Résultats de la simulation radio mobile en ligne pour la liaison de 380 km entre Aguila et Platillon.

14. ENÉRGIE HORS RÉSEAU

Ce chapitre fournit une introduction aux systèmes photovoltaïques autonomes. Les systèmes autonomes fonctionnent sans connexion à un réseau électrique en place. Ce chapitre présente les concepts de base de la production et du stockage de l'énergie solaire photovoltaïque. Nous allons également fournir une méthode pour la conception d'un système solaire ayant un accès limité à l'information et aux ressources. Ce chapitre ne traite que des systèmes solaires pour la production directe d'électricité (énergie solaire photovoltaïque). Les systèmes d'énergie solaire thermique sont au-delà de la portée de ce chapitre.

Energie solaire

Un système photovoltaïque est basé sur la capacité des panneaux photovoltaïques de pouvoir convertir directement le rayonnement solaire en énergie électrique. Le montant total de l'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, jour ou mois.

La quantité de rayonnement qui arrive sur la surface de la terre varie en raison de variations climatiques naturelles et dépend de l'emplacement. Par conséquent, il est nécessaire de travailler avec des données statistiques sur la base de l ' « histoire solaire » d'un lieu particulier. Pour beaucoup d'endroits, il peut être difficile d'obtenir des informations détaillées. Nous aurons besoin de travailler avec des valeurs approximatives dans ces cas.Quelques organisations produisent des cartes qui continent les valeurs moyennes de l'irradiation globale quotidienne pour différentes régions. Ces valeurs sont connues sous le nom d'heures d'équivalent plein soleil (PSH, Pic Sun Hours en anglais). Vous pouvez utiliser la valeur de PSH de votre région pour simplifier vos calculs. Une unité d'équivalent plein soleil correspond à un rayonnement de 1000 watts par mètre carré pour une durée d'une heure. Si une zone a 4 PSH par jour dans le pire des mois, cela signifie que nous pouvons nous attendre à une irradiation journalière de 4000 Wh/m2.

Des cartes à basse résolution et des outils de calcul du PSH sont disponibles à partir d'un certain nombre de sources en ligne tels que :

http://re.jrc.ec.europa.eu/pvgis/apps4/pvest.php?map= africa &lang=en

Pour plus d'informations, consultez un fournisseur local d'énergie solaire ou station météo.

Qu'en est -il de l'énergie éolienne ?

Quand un système autonome est conçu pour l'installation sur une colline ou une montagne, Il est possible d'utiliser une éolienne en place de panneaux solaires. Pour être efficace, la vitesse moyenne du vent au courant 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 habituellement de l'énergie éolienne suffisante pour soutenir un système éolien. D'une manière générale, les systèmes photovoltaïques sont plus fiables que les éoliennes, comme la lumière du soleil est plus disponible qu'un vent régulier dans beaucoup d'endroits.
Cependant, les éoliennes sont en mesure de recharger les batteries même pendant la nuit, aussi longtemps qu'il y a suffisamment de vent. Il est bien entendu possible d'utiliser le vent en combinaison avec l'énergie solaire pour couvrir les moments de couverture nuageuse prolongée ou lorsqu'il y a pas suffisamment de vent. Il existe un projet qui utilise à la fois la production d'énergie solaire et éolienne dans les Highlands et les îles d'Ecosse. Pour plus d'informations sur ce projet, consultez le lien :
http://www.wirelesswhitespace.org/projects/wind-firenewable-energybasestation.aspx
Cependant, pour la plupart des endroits le coût d'une bonne éolienne n'est pas justifiée a cause de la faible quantité d'énergie qu'elle va ajouter à l'ensemble du système . Ce chapitre se concentrera donc sur l'utilisation de panneaux solaires pour la production électrique .

Composants du système photovoltaïque

Un système photovoltaïque de base se compose de quatre éléments principaux: le panneau solaire, les batteries, le régulateur, et la charge.
Le panneau produit de l'électricité. La batterie stocke l'énergie électrique. Le régulateur protège la batterie contre une charge excessive et la décharge. La charge se réfère à tout dispositif qui nécessite une alimentation électrique. Il est important de rappeler que les panneaux solaires et batteries produisent du courant continu (CC). Si la plage de tension de fonctionnement de votre matériel n'est pas adaptée à la tension fournie par la batterie, il sera également nécessaire d'inclure un certain type de convertisseur.
Si l'appareil que vous souhaitez alimenter utilise une tension continue différente de celle fournie par la batterie, vous devrez utiliser un convertisseur DC /DC. Si une partie de votre équipement nécessite une alimentation secteur, vous devrez 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 câblage approprié, des disjoncteurs, parafoudres, fusibles, des tiges de sol, éclairage d'arrêt, etc.

Le panneau solaire

Le panneau solaire est composé de cellules solaires qui recueillent le rayonnement solaire et la transforment en énergie électrique. Cette partie du système est parfois appelé un module solaire ou un générateur photovoltaïque. Des matrices de panneaux solaires peuvent être constituées par la connexion d'un ensemble de panneaux en série et /ou en parallèle dans le but de fournir l'énergie nécessaire pour une charge donnée. Le courant électrique fourni par un panneau solaire varie proportionnellement à la radiation solaire. Cela variera en fonction des conditions climatiques, l'heure de la journée, et le moment de l'année.

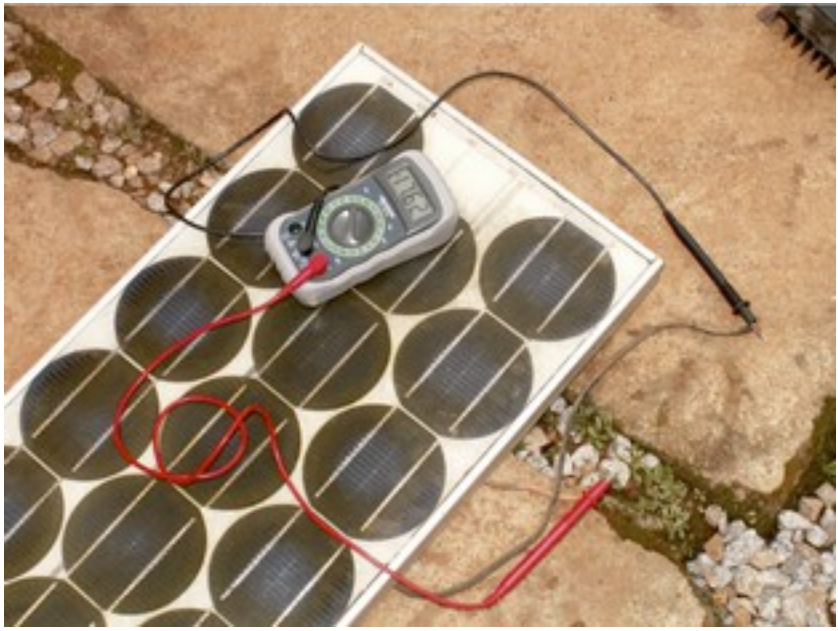


Figure OGP 1: Un panneau solaire

Plusieurs technologies sont utilisées dans la fabrication de cellules solaires. Le plus commun est le silicium cristallin, et peut être soit monocristallin ou poly cristallin.

Le silicium amorphe peut être moins couteux, mais est moins efficace dans la conversion de l'énergie solaire en électricité. Ayant une espérance de vie réduite et une efficacité de transformation de 6 à 8 %, le silicium amorphe est généralement utilisé pour les équipements de faible puissance, tels 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 des rendements plus élevés 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. L'énergie ainsi stockée peut ensuite être utilisée pendant des périodes de faible ensoleillement. La batterie est également parfois appelée l'accumulateur. Les batteries stockent l'électricité sous forme d'énergie chimique.

Le type le plus commun de batteries utilisées dans des applications solaires sont les batteries au plomb-acide sans entretien, également appelés batteries à recombinaison ou batteries VRLA (valve regulated lead acid en anglais).

Figure OGP 2: Une batterie plomb- acide 200 Ah. La borne négative a été cassée à cause d'une pression exercée sur les bornes pendant le transport.

En plus du stockage de l'énergie, les batteries scellées au plomb-acide servent également deux fonctions importantes :

• Elles sont capables de fournir une puissance instantanée supérieure à ce qu'une matrice de panneaux peut générer. Cette puissance instantanée est nécessaire pour démarrer certains appareils, tels que le moteur d'un réfrigérateur ou d'une pompe.
• Elles déterminent la tension de fonctionnement de votre installation.
Pour une petite installation d'énergie dans un contexte où les contraintes d'espace sont importantes, d'autres types de batteries (comme NiCd, NiMH ou Li-ion) peuvent être utilisés .
Ces types de batteries 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 fonctionne dans des conditions appropriées. Il permet d'éviter la surcharge de la batterie ou la surdécharge, qui sont tous deux très préjudiciable à la durée de 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 en anglais) de la batterie. L'état de charge est estimée 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 les moments précis où la batterie serait surchargée ou excessivement déchargée.

Figure OGP 3: Un régulateur de charge solaire 30 ampères.

Le régulateur peut inclure d'autres fonctionnalités qui ajoutent des informations précieuses ainsi que le contrôle de la sécurité de l'équipement. Ces fonctionnalités incluent notamment les ampèremètres, voltmètres, la mesure d'ampère-heure, des horloges, alarmes, etc.
Tout en étant pratique, aucune de ces caractéristiques n'est indispensable pour un système photovoltaïque fonctionnel.

Le convertisseur

L'électricité fournie par une matrice de capteurs et la batterie est de type continu à une tension fixe. La tension fournie peut ne pas correspondre à ce qui est requis par votre charge.
Un convertisseur continu/alternatif (DC / AC), également connu sous le nom onduleur convertit le courant continu de vos batteries en courant alternatif. Cela se fait au prix d'une perte d'énergie lors de la conversion .
Si nécessaire, vous pouvez également utiliser des convertisseurs pour obtenir un courant continu a 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 sorte que la tension continue générée correspond à la charge.

Figure OGP 4: Un convertisseur (onduleur) de 800 Watt DC/AC.

La charge

La charge est l'équipement qui consomme l'énergie produite par votre système d'énergie. La charge peut inclure l'équipement de communications sans fil, les routeurs, les postes de travail, les lampes, téléviseurs, modems VSAT, etc. Bien qu'il ne soit pas possible de calculer précisément la consommation totale exacte de votre équipement, il est essentiel d'être capable de faire une bonne estimation. Dans ce type de système, il est absolument nécessaire d'utiliser des équipements efficients et de peu de puissance pour éviter de gaspiller l'énergie.

Assembler les pièces

L'installation photovoltaïque complète intègre l'ensemble de ces composantes. Les panneaux solaires produisent de l'électricité lorsque l'énergie solaire est disponible. Le régulateur assure le fonctionnement le plus efficace des panneaux et évite d'endommager les batteries.
Le banc des batteries emmagasine l'énergie pour une utilisation ultérieure.
Les convertisseurs et onduleurs adaptent l'énergie stockée pour correspondre aux besoins de votre charge.
Enfin, la charge consomme l'énergie stockée pour faire le travail. Lorsque tous les éléments sont en équilibre et sont correctement entretenus, le système se maintient pendant des années.

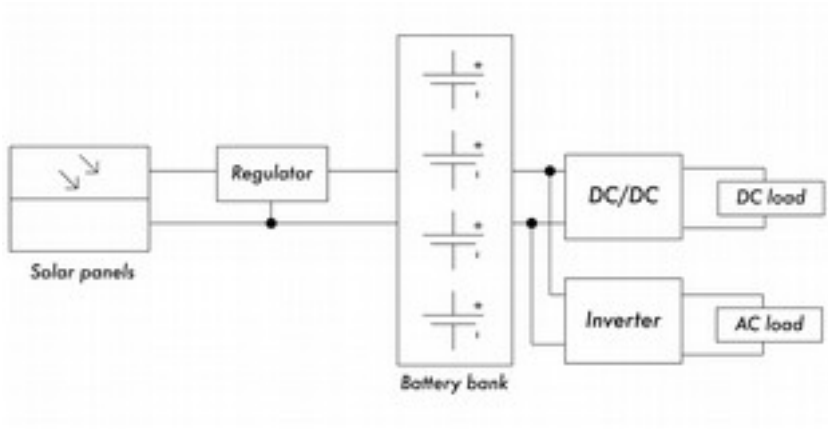


Figure OGP 5: Une installation solaire avec des charges DC et AC.

Nous allons maintenant examiner chacun des composantes individuelles de l'installation photovoltaïque de manière plus détaillée.

Le panneau solaire

Un panneau solaire individuel est composé de nombreuses cellules solaires . Les cellules sont reliées électriquement pour fournir une valeur particulière de courant et de tension. Les cellules individuelles sont bien encapsulées pour fournir une isolation et une protection contre l'humidité et la corrosion .

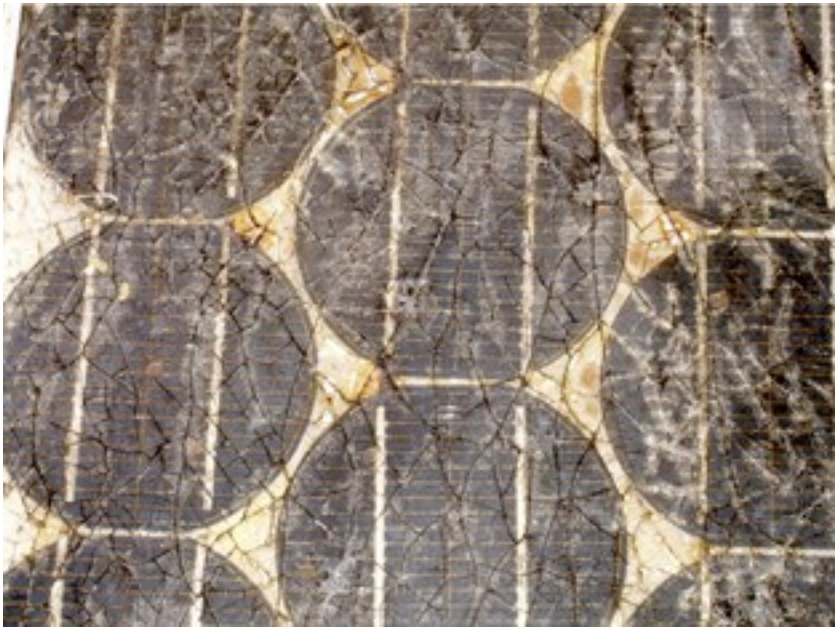


Figure OGP 6: The effect of water and corrosion in a solar panel

Il existe différents types de modules disponibles sur le marché, selon les exigences énergétiques de votre application. Les modules les plus courants sont constitués de 32 ou 36 cellules solaires de silicium cristallin. Ces cellules sont toutes de taille égale, montées en série , et encapsulées entre du verre et de la matière plastique, et utilisent une résine en polymère (EVA) comme isolant thermique. La surface du module est typiquement comprise entre 0,1 et 0,5 m^2. Les panneaux solaires ont généralement deux contacts électriques, l'un positif et l'autre négatif. Certains panneaux 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 en anglais sous le nom «hot-spots» .

Un hot-spot se produit lorsque certaines des cellules sont dans l'ombre tandis 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 dissipe de l'énergie.
Dans cette situation, ces cellules peuvent expérimenter une augmentation significative de température (environ 85 à 100 ºC). Les diodes de dérivation empêchent la formation des 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 plus meilleure solution consiste à exposer l'ensemble du panneau au soleil autant que possible.

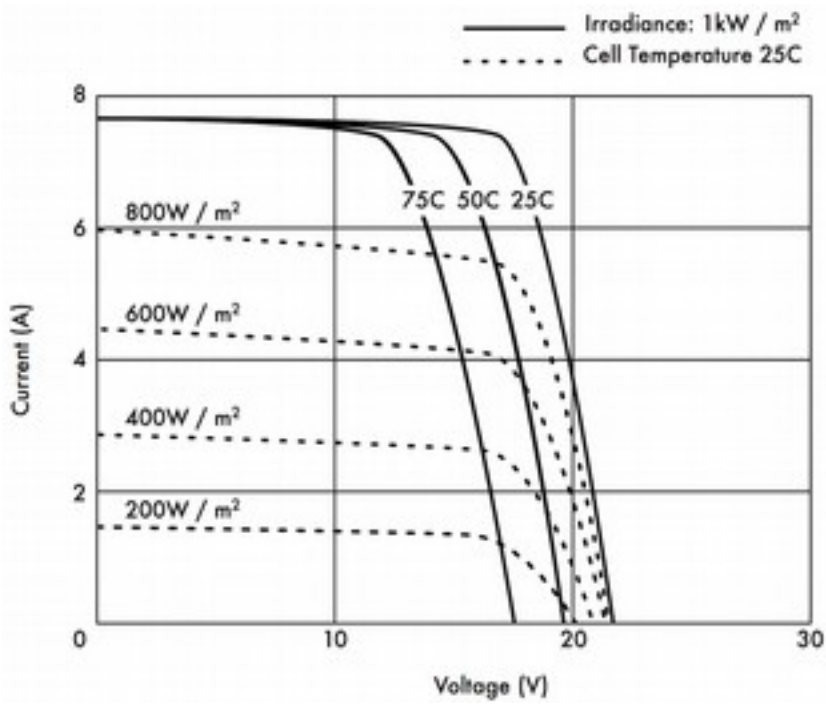


Figure OGP 7: Différentes courbes IV . L'intensité du courant (A) varie avec l'irradiance, et la tension (V) varie avec la température.

La performance électrique d'un module solaire est représentée par la courbe caractéristique IV, qui représente l'intensité du courant qui est fournie 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 du courant générée est directement proportionnelle à l'irradiance solaire (G) , tandis que la tension diminue légèrement avec l'augmentation de la température.
Un bon régulateur essayera de maximiser la quantité d'énergie par un panneau 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 :

1. **Curant de court-circuit (I_{SC}):** le courant maximum fourni par le panneau lorsque les connecteurs sont court-circuitées .
2. **Tension de circuit ouvert (V_{OC})**: la tension maximale que le panneau fournit lorsque les bornes ne sont pas connectées à une charge quelconque (un circuit ouvert). Cette valeur est normalement de 22 V pour des 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(Pmax)**: le point où l'énergie 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 fonctionne pas dans les 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} devraient être un peu plus petites que les valeurs I_{SC} et de V_{OC}.
4. **Facteur de remplissage (FF)** : le rapport entre la puissance maximale que le panneau peut effectivement fournir et le produit I_{SC} .V_{OC}. Ce rapport vous donne une idée de la qualité du panneau , car c'est une indication du type de courbe caractéristique IV .
   Plus le FF est proche de 1, plus un panneau peut fournir d'énergie. Les valeurs communes sont généralement 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 d'environ 10 à 12 %, selon le type de cellules (monocristallin, polycristallin, amorphe ou un film mince).

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

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

Les valeurs de l'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/m^2 , au niveau de la mer, pour une température de cellules de Tc = 25 º C.
Les paramètres du panneau changent pour certaines conditions d'irradiance et de température. Les fabricants devront parfois inclure des graphiques ou des tableaux avec des valeurs pour des conditions différant de la norme.
Vous devez vérifier les valeurs de rendement à des températures de panneaux qui sont susceptibles de correspondre à votre installation.
Soyez conscient 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 ses paramètres (au moins , I_{SC} et V_{OC}) correspondent aux valeurs promises par le fabricant.

Paramètres du panneau 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 devez toujours être conscient que le panneau ne va pas fonctionner dans des conditions parfaites comme la charge ou le système de régulation ne va pas toujours fonctionner au point de puissance maximale du panneau . Vous devez assumer une perte d'efficacité de 5 % dans vos calculs pour compenser cela.

Interconnexion des panneaux

Une matrice de panneaux solaires est un ensemble de panneaux solaires qui sont électriquement interconnectés et installés sur un certain type de support. L'utilisation d'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 entre eux de manière à ce que la tension générée soit proche (mais supérieur à) du niveau de

tension des batteries, et que le courant généré soit suffisant pour alimenter les équipements et charger les batteries. La connexion de panneaux solaires en série augmente la tension générée. La connexion des panneaux en parallèle augmente l'intensité du courant. Le nombre de panneaux utilisés devrait être augmenté jusqu'à ce que la quantité d'énergie produite dépasse légèrement les exigences de votre charge. Il est très important que tous les panneaux dans votre matrice soient aussi identiques que possible. Dans une matrice, vous devez utiliser des panneaux de la même marque et de mêmes caractéristiques parce que toute différence dans leurs conditions d'exploitation aura un grand impact sur le bon fonctionnement et la performance de votre système. Même les panneaux qui ont des performances identiques afficheront habituellement une certaine variation dans leurs caractéristiques due à leurs procédés de fabrication. Les caractéristiques de fonctionnement réelles des deux panneaux d'un 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.

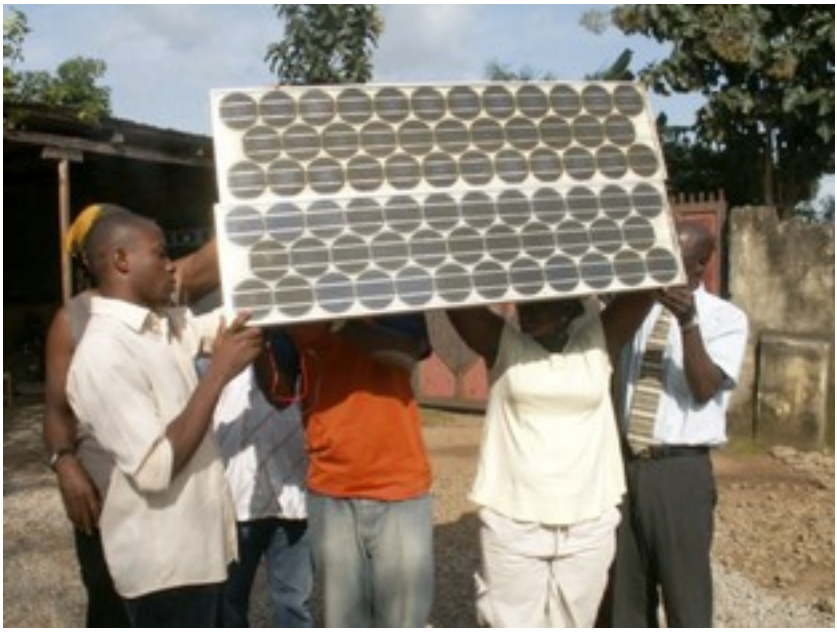


Figure OGP 8: Interconnexion des panneaux en parallèle. La tension reste constante tandis que les courant double . (Photo: Fondation Fantsuam, Nigeria)

Comment choisir un bon panneau

Une métrique évidente à utiliser lors de l'achat de panneaux solaires consiste à comparer le rapport de la puissance de crête nominale (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 (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. 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 la 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 alimentation du panneau (W_p), mais aussi la variation de la puissance avec l'irradiation et la température.

Ceci 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'énergie électrique générée 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 composantes 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.

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}. La 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

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.

Etat de charge	Tension batterie à 12V	Volts par cellule
100%	12.7	2.12
90%	12.5	2.08
80%	12.42	2.07
70%	12.32	2.05
60%	12.2	2.03
50%	12.06	2.01
40%	11.9	1.98
30%	11.75	1.96
20%	11.58	1.93
10%	11.31	1.89

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'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 le court-circuit 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 OGP 9: Un banc de batteries à 3600Ah avec des courants atteignant des niveaux de 45 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 une 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 court-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. 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 une composante 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.

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	Consommation (Watts)
Ordinateur portable	30-50
Lampe de faible puissance	6-10
Routeur WRAP (une radio)	4-10
Modem VSAT	15-30
PC (sans écran LCD)	20-30
PC (avec écran LCD)	200-300
Switch réseau (16 ports)	6-8

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 (en anglais *beacon interval*), et l'extinction du système quand il n'est pas utilisé.

La plupart des systèmes solaires autonomes fonctionnent à 12 ou 24 volts de tension. Il est donc préférable 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.

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.

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 : tailles des cables.

Gardez à l'esprit que l'intensité qui définit la capacité 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 = |F| + 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 = |F|).
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 = |F| - 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-telle 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/m^2 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 PC 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 applicable 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 Im, qui est le courant quotidien maximum qu'une matrice de panneaux fonctionnant à tension nominale VN 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 Gdm(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 ETOTAL 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.

$$N_{ps} = V_N / Vpmax$$

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 (capacité nécessaire CNEC).

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

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

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 IMC qui va circuler dans le câble. Dans le cas du sous-système panneau batterie, c'est le ImMAX calculé pour chaque mois. Dans les sous-système batterie-charge, il dépend de la manière dont les charges sont connectées.
- La chute de tension (Va-Vb) 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 :

Composante	Chute de tension (en % de VN)
Matrice de panneaux ->Batterie	1,00%
Batterie -> Convertisseur	1,00%
Ligne principale	3,00%
Ligne principale (éclairage)	3,00%
Ligne principale (Equipement)	5,00%

Chutes de tension couramment acceptables dans les câbles

La section du câble est déterminée par la loi d'Ohm :
$S(mm^2) = r(\Omega mm^2/m)L(m)\ I_{mMAX}(A)/\ (V_a-V_b)(V)$

Où S est la section, R est la résistivité (propriété intrinsèque du matériau : pour le cuivre, 0,01286 Ω mm^2 / 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 mm^2.

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 œuvre 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/mètre	$25
Batteries à décharge profonde 50 Ah	6	$900	$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'œuvre 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	Nombre	Coût unitaire	Sous total	Durée de vie (années)	Coût par an:
Panneau solaire 60W	4	$300	$1,200	20	$60
Régulateur 30A	1	$100	$100	5	$20
Câblage (mètres)	25	$1/mètre	$25	10	$2.50
Batterie à 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.

MAINTENANCE, DÉPANNAGE, ET DURABILITÉ

15. MAINTENANCE ET DÉPANNAGE

Introduction

La façon dont vous établissez 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. Nous décrivons également un nombre des techniques de dépannage standards qui ont fait leurs preuves dans la résolution des problèmes réseaux en général.

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, ré-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 passer 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 où 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.

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. Bientôt, il devint un expert en IT et en connaissances réseaux ainsi que le réseau local. 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 se vit offrir un poste de fonctionnaire et quitta 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 dut retourner et de recommencer la formation de nouveau, cette fois avec des locaux qui étaient censés rester dans le village. Bien que la réformation fut beaucoup plus longue, la communauté était garantie que le savoir et les connaissances acquises resteraient dans la communauté plus longtemps. 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. A la vue d'un réseau sans fil, le néophyte 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. Débranchez l'antenne. Insérez un fusible brisé.
Testez l'étudiant en montrant clairement que chaque problème peut révéler des symptômes spécifiques et montrez 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.

Techniques appropriées 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 défectueux, 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 qui surgissent une fois que votre réseau est utilisé.

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.

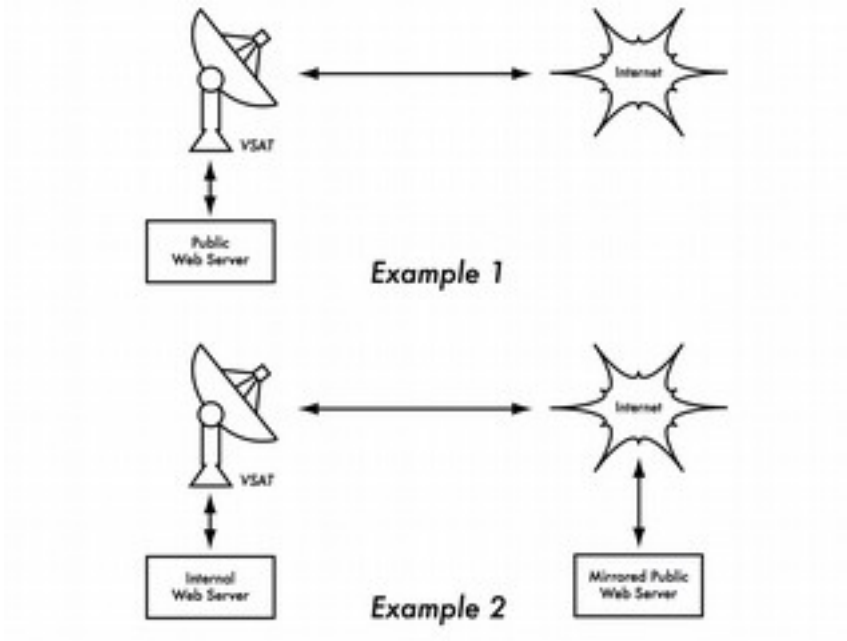


Figure MT 1: Dans l'exemple 1, tout le trafic vers le site web venant de l'Internet doit traverser le VSAT. Dans l'exemple 2, le site web public est hébergé sur un service Européen rapide, alors qu'une copie est gardée sur un serveur local pour des accès locaux très rapides. Ceci améliore la connexion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

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 s**quid.conf** comme étant le seul réseau qui peut utiliser Squid.

Alternativement, si votre serveur proxy se trouve derrière un parefeu (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://www.mailradar.com/openrelay/ ou http://www.checkor.com/

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) 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 des applications qui demandent une grande bande passante. 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.

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

Il ya des programmes qui sont destinés à s'installer eux-mêmes automatiquement et ensuite continuer à utiliser la bande passante. Certains logiciels sont des logiciels espions (Spyware en anglais), 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 problematiques, tels que Spychecker (http://www.spychecker.com/).

Mises à jour du système d'exploitation Windows

Les systèmes d'exploitation Microsoft Windows assument 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 une liaison Internet coûteuse.
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.

Programmes qui assument une connexion à 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. C'est plus efficace d'installer un serveur de temps local et d'effectuer la distribution de temps précis à partir de ce serveur plutôt qu'immobiliser la liaison Internet avec ces demandes.

Les vers et les virus

Les vers et les virus peuvent générer d'énormes quantités de trafic. 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 retransmet immédiatement au compte Yahoo. Une boucle de messagerie se forme qui enverrait et retournerait des centaines de milliers d'e-mails entre le compte de l'université et le compte Yahoo générant un trafic massif 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.
Le téléchargement hors ligne peut se faire 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://** accèdent 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 maintenu dans une file d'attente pour un téléchargement ultérieur et l'utilisateur est notifié par e-mail lorsque le téléchargement est terminé. Le système maintient une cache des fichiers récemment téléchargés et les récupèrent 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.

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/Mac, où un utilisateur peut rendre un gros fchier 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 cet 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 (en anglais FLUFF, facility for the upload of large files), disponible à partir de http://www.bris.ac.uk/it-services/applications/fluff/.

Il ya aussi des outils tels que SparkleShare (http://sparkleshare.org/) et LipSync (https://github.com/philcryer/lipsync) qui sont des logiciels a sources ouvertes que vous pouvez installer et configurer vous même pour faire la même chose.
Il y'a aussi des nouveaux services en-ligne gratuits tels que Google Drive qui peuvent etre configurés pour le partage des fichiers et l'édition courante de ces fichiers. Considérez l'utilisation de rsync (http://rsync.samba.org/) pour les utilisateurs qui veulent s'envoyer des fichiers larges similaires ou les memes regulierement.
Rsync est plus un protocole de synchronisation plutot qu'un simple protocole de transfert de fichier. Au lieu de simplement transferer un fichier du début à la fin, Rsync vérifie avec le serveur rsync sur l'hôte destination pour s'assurer si le fichier envoyé existe déjà.
Si c'est le cas, les deux parties comparent leurs copies et l'expéditeur transmet à la destination seulement les différences entre les deux fichiers.
For example, if a 10 MB database of research data only has 23 KB of new data vs. the last version, only the 23 KB of changes will be transmitted.
Rsync can also use the SSH protocol, providing a secure transport layer for sync actions.

Par exemple, si une base de données de 10 MB de données de recherche a seulement 23 KB de nouvelles données par rapport à la dernière version, seules les 23 KB de changements seront transmises.
Rsync peut également utiliser le protocole SSH fournissant une couche de transport sécurisée pour les actions de synchronisation.

Localisation des fautes et reportage.

Le dépannage n'est seulement que la moitié de la tâche de résolution des problèmes sur un réseau sans fil. Une fois qu'un problème a été diagnostiqué et localisé, il doit être documenté de façon permanente afin que d'autres qui travaillent sur le réseau soit maintenant ou dans l'avenir, soient en mesure d'apprendre de l'incident.
Tenir un registre des problèmes et des incidents qui se produisent est aussi un bon moyen de suivre et de résoudre les problèmes à long terme qui peuvent se produire, par exemple, une fois tous les quelques mois, mais en suivant un modèle précis. Vous pouvez également réduire la complexité et la frustration associée à la resolution d'un problème si vous gardez un journal de toutes les modifications apportées au réseau.
Le journal de bord est l'endroit où vous et votre équipe écrivez chaque modification apportée à un système ainsi que la date et le moment où la modification a ete a été effectuée . Par exemple:

23 Juillet 10:15 Changement de route par défaut sur la machine alpha de 123.45.67.89 à 123.56.78.1 parce votre ISP en amont a déplacé notre passerelle.

Avec le développement de votre réseau, envisagez d'installer un système de suivi des fautes comme JIRA ou Bugzilla pour aider à mieux garder trace de qui a travaillé sur ce problème et ce qui s'est passé lors de ce travail. Cela fournit une histoire sur le problème qui a été adressé et comment le problème a été fixé et fournit une méthode ordonnée pour l'attribution des tâches et aider à prévenir les cas ou une personne n'enfreigne le travail de l'autre pendant que tous deux tentent de résoudre le même problème.
Les systèmes de billetterie des problèmes sont un sujet qui pourrait remplir un livre entier. Ainsi nous ne les mentionneront ici que brièvement pour vous en faire prendre conscience. Comme ils peuvent aussi être très complexes à implementer, un journal de bord peut suffire pour des réseaux simples.

16. SURVEILLANCE RÉSEAU

Introduction

La surveillance du réseau est l'utilisation d'outils d'exploitation et d'analyse pour déterminer avec précision les flux de trafic et autres indicateurs de performance sur un réseau. De bons outils de surveillance produisent les chiffres précis et les représentations graphiques globales de l'état du réseau. Cela vous permet de visualiser précisément ce qui se passe afin que vous sachiez là où des ajustements peuvent être nécessaires .Ces outils peuvent vous aider à répondre à des questions essentielles, telles que :

- Quels sont les services les plus populaires utilisés sur le réseau?
- Qui sont les plus grands utilisateurs du réseau ?
- Quels sont les autres canaux sans fil utilisés dans ma région?
- Les utilisateurs installant des points d'accès sans fil sur mon réseau câblé privé?
- À quel moment de la journée le réseau est-il plus utilisés?
- Quels sont les sites que vos utilisateurs fréquentent?
- Est-ce que La quantité de trafic entrant ou sortant est-elle proche de la capacité disponible du réseau?
- Y at-il des indications d'une situation inhabituelle du réseau qui consomme de la bande passante ou cause d'autres problèmes ?
- Est-ce que notre Fournisseur de Services Internet (FSI) pourvoit le niveau de service que nous payons?
- Cela devrait répondre en termes de bande passante disponible, la perte de paquets, la latence et la disponibilité globale.
- Et peut-être la question la plus importante de toutes:
- Est-ce que les modèles de trafic observées correspondent-ils à nos attentes?

Outils de suivi et de mesurés sont programmes extrêmement importants à avoir en main pour vérifier la santé de votre réseau et diagnostiquer ou résoudre les problèmes .Tout au long des chapitres précédents du présent ouvrage nous l'avons mentionné ou donné de brefs exemples de l'utilisation de certains outils pour les tâches spécifiques comme configuration et installation, dépannage, collecte de statistiques et données de mesures de la santé de votre réseau, etc.

Cette section traite de certains de ces outils d'une manière plus détaillée. Il convient de noter que ce n'est en aucun cas une liste exhaustive de tous les outils disponibles pour les réseaux câblés et sans fil.
Il est également important de réaliser que les outils de diagnostic et de suivi changent comme tous les autres logiciels et le matériel.
Rester à jour sur les dernières versions, des erreurs dans les versions existantes, de nouveaux outils dans le domaine, etc. peuvent être en soi un travail presqu'à temps plein.
Dans ce livre, nous n'avons pas mentionné certains outils qui n'étaient plus activement maintenu entre l'édition précédente et celle-ci. Les outils présentés dans cette section sont tous en cours de développement au moment de la redaction de ce livre, mais il appartient au lecteur de déterminer si un outil particulier est adapté à leur situation.

Exemple de surveillance du réseau

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

Un exemple efficace de surveillance du réseau

Pour cet exemple, supposons que nous sommes en charge d'un réseau qui a fonctionné pendant trois mois. Il est composé de 50 ordinateurs et de trois serveurs: email, web, et les serveurs proxy. Alors qu'au départ les choses vont bien, les utilisateurs commencent à se plaindre de faible vitesses du réseau et une augmentation en spams.
Comme le temps passe, les performances de l'ordinateur ralentit pour une exploration (même si vous n'utilisez pas le réseau), ce qui provoque beaucoup de frustrations pour vos utilisateurs.
Avec des plaintes fréquentes et très faible utilisation de l'ordinateur, le Comité s'interroge sur la nécessité de tant de matériel réseau.
Le Comité souhaite également la preuve que la bande passante qu'ils paient est effectivement utilisé . En tant qu'administrateur réseau, vous êtes sur le récepteur final de ces plaintes.Comment peuvez-vous diagnostiquer la chute brutale des performances du réseau et de l'ordinateur et aussi justifier le matériel réseau et les coûts de bande passante?

Maintenance du LAN (trafic local)

Pour avoir une idée de ce qui est exactement l'origine du ralentissement, vous devriez commencer par regarder le trafic sur le réseau local.

Il ya plusieurs avantages à surveiller le trafic local :

1 . Le dépannage est grandement simplifié. Les virus peuvent être détectés et éliminés.
2 . Des utilisateurs malveillants peuvent être détectés et examinés.
3 . Le matériel et les ressources réseaux peuvent être justifiés par des statistiques réelles.

Supposons que tous les commutateurs soutiennent le Simple Network Management Protocol (SNMP). SNMP est un protocole de couche d'application conçu pour faciliter l'échange d'informations de gestion entre périphériques réseau.
En attribuant une adresse IP pour chaque commutateur, vous êtes capable de surveiller toutes les interfaces sur ce commutateur en observant l'ensemble du réseau à partir d'un seul point. C'est beaucoup plus facile que de permettre SNMP sur tous les ordinateurs d'un réseau.

En utilisant un outil gratuit comme MRTG, http://oss.oetiker.ch/mrtg/, vous pouvez contrôler chaque port du commutateur et présenter les données sous forme graphique, comme une moyenne globale au fil du temps. Les graphiques sont accessibles depuis le web, donc vous êtes en mesure d'afficher les graphiques de n'importe quelle machine à tout moment. Avec MRTG surveillance en place, il devient évident que le réseau local interne est inondé avec beaucoup plus de trafic que la connexion Internet peut prendre en charge même si le laboratoire est inoccupé.
Ceci est une indication assez clair que certains ordinateurs sont infestés par un virus de réseau.
Après l'installation de bon anti-virus et anti-logiciels espions sur toutes les machines, le trafic LAN interne s'installe à des niveaux attendus. Les machines fonctionnent beaucoup plus rapidement, les spams sont réduits et le moral des utilisateurs s'améliore rapidement.

Surveillance du WAN (trafic externe)

En plus de regarder le trafic interne sur le LAN, vous devez démontrer que la bande passante payé par l'organisation est en fait ce qu'elle reçoit de leur Fournisseur de Services Internet (FSI).

Vous pouvez y parvenir en surveillant le trafic externe. Trafic externe est généralement classé comme une chose envoyée sur un réseau étendu (WAN).

Tout ce qui est reçu d' (ou envoyé à) un réseau autre que votre LAN interne est qualifié comme trafic externe.
Les avantages de la surveillance du trafic externe comprennent :
Coûts de bande passante Internet sont justifiés en montrant l'utilisation réelle, et si cette utilisation est d'accord avec les frais de bande passante de votre FSI.
Besoins en capacité futures sont estimés en regardant les tendances d'utilisation et de prédire les modèles de croissance probables. Les intrus de l' Internet sont détectés et filtré avant qu'ils ne causent des problèmes.
La surveillance de cette circulation se fait facilement à l'aide de MRTG sur un dispositif SNMP activé, tel qu'un routeur.
Si votre routeur ne prend pas en charge SNMP, vous pouvez ajouter un commutateur entre votre routeur et votre connexion du FSI, et surveiller le trafic du port comme vous le feriez avec un LAN interne.

Détection des pannes de réseau

Grâce à des outils de surveillance en place, vous avez maintenant une mesure précise de la bande passante utilisée par l'organisation. Cette mesure devrait être en accord avec les frais de bande passante de votre FSI.
Elle peut aussi indiquer le débit réel de votre connexion si vous êtes proche de votre capacité disponible aux heures de pointe .
Un "Flat top" (sommet stationnaire) graphique est une indication assez claire que vous opérez à pleine capacité.
La figure NM 1 suivante montre les sommets stationnaires dans le trafic sortant en pointe au milieu de chaque jour, sauf le dimanche.
Il est clair que votre connexion Internet actuelle est plus utilisé aux heures de pointe, causant le décalage du réseau.
Après avoir présenté ces informations au Comité, vous pouvez faire un plan pour optimiser davantage la connexion existante (par la mise à niveau de votre serveur proxy et l'utilisation d'autres techniques dans ce livre) et estimer le temps nécessaire pour la mise à niveau de votre connexion pour faire face à la demande.
C'est aussi une excellente occasion de revoir votre politique opérationnelle avec le Comité et discuter des moyens pour mettre l'utilisation réelle en conformité avec cette politique.

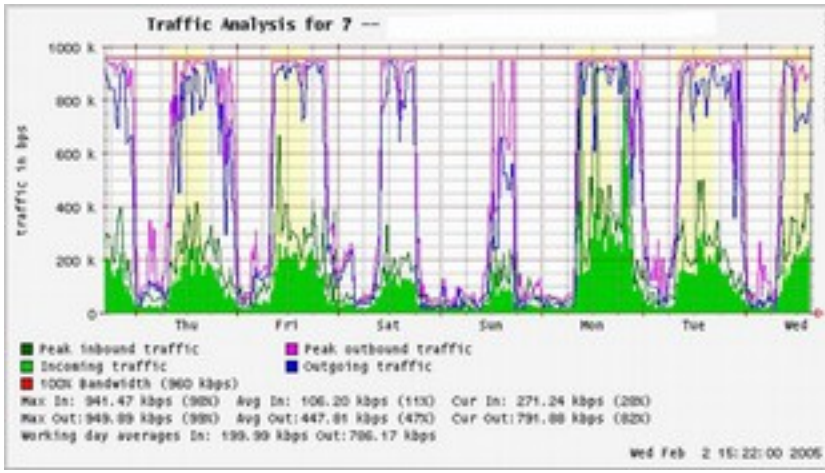


Figure NM 1: Un graphique avec un «sommet plat» est une indication de surutilisation.

Plus tard dans la semaine, vous recevez un appel téléphonique d'urgence dans la soirée. Apparemment, personne dans le laboratoire ne peut naviguer sur le Web ou envoyer un courriel. Vous vous précipitez pour le laboratoire et redémarrer le serveur proxy à la hâte sans résultats. Parcourir et email sont toujours discontinues . Ensuite vous redémarrez le routeur mais toujours sans succès. Vous continuez à éliminer les possible zones de failles un par un jusqu'à ce que vous vous rendez compte que le commutateur de réseau est éteint - un câble d'alimentation en vrac est à blâmer.
Après la mise sous tension, le réseau functionne de nouveau.
Comment pouvez-vous résoudre cette panne sans ce temps d'essai et erreur? Est-il possible d'être notifié de pannes quand ils se produisent plutôt que d'attendre qu'un utilisateur se plaint? Une façon de faire est d'utiliser un programme tel que Nagios (http://www.nagios.org/) qui sonde continuellement les dispositifs de réseau et vous avertit des cas de pannes. Nagios rapportera la disponibilité des différentes machines et services et vous alertera sur des machines qui ne fonctionnent plus.
En plus d'afficher l'état du réseau graphiquement sur une page web, il va envoyer des notifications par SMS ou e-mail, vous alertant immédiatement en cas de problème.
Avec de bons outils de surveillance en place, vous serez en mesure de justifier le coût de l'équipement et de la bande passante en démontrant bien comment il est utilisé par l'organisation.

Vous êtes averti automatiquement en cas de problème et vous avez des statistiques historiques de la façon dont les périphériques réseau sont performants. Vous pouvez vérifier les performances actuelles contre cette histoire de trouver un comportement inhabituel et éviter les problèmes avant qu'ils ne deviennent critiques.
Lorsque des problèmes surviennent, 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.

La surveillance de votre réseau

Gérer un réseau sans surveillance est similaire à la conduite d'un véhicule sans un compteur de vitesse ou une jauge de carburant.
Comment savez-vous vitesse à quelle vous roulez?
Est-ce que la voiture consomme le carburant de manière efficiente comme promis par les concessionnaires?
Si vous faites une révision du moteur plusieurs mois plus tard, la voiture est plus rapide ou plus efficace qu'elle ne l'était avant?
De même, comment pouvez-vous payer pour une facture d'électricité ou d'eau sans voir votre consommation mensuelle à partir d'un compteur?
Vous devez avoir un compte de l'utilisation de bande passante de votre réseau afin de justifier le coût des services et les achats de matériel et pour tenir compte des tendances d'utilisation.
Il y'a plusieurs avantages à implémenter un bon système de surveillance pour votre réseau:

- Le budget et les ressources réseau sont justifiées. De bons outils de surveillance peuvent démontrer sans aucun doute que l'infrastructure du réseau (bande passante, le matériel et les logiciels) est adaptée et capable de gérer les besoins des utilisateurs du réseau.
- Les intrus sont détectés et filtrés. En regardant le trafic de votre réseau, vous pouvez détecter les attaquants et empêcher l'accès aux serveurs et aux services internes importants.
- Virus de réseau sont facilement détectés. Vous pouvez être averti de la présence de virus de réseau et prendre les mesures appropriées avant qu'ils consomment de la bande passante Internet et déstabilisent votre réseau.
- Dépannage des problèmes de réseau est grandement simplifié. Plutôt que de tenter «essais et erreurs» pour déterminer les pro-

blèmes de réseau, vous pouvez être informé instantanément des problèmes de spécifiques. Certains types de problèmes peuvent même être résolus automatiquement.
• Performances réseau peut être hautement optimisé. Sans une surveillance efficace, il est impossible d'affiner vos dispositifs et protocoles pour atteindre la meilleure performance possible.
• Planification de la capacité est beaucoup plus facile. Avec l'historique solide de records de performance, vous n'avez pas à «deviner» la quantité de bande passante dont vous aurez besoin comme votre réseau grandit.
• L'utilisation appropriée du réseau peut être renforcée. Lorsque la bande passante est une ressource rare, la seule façon d'être équitable à tous les utilisateurs est de s'assurer que le réseau est utilisé conformément à son objectif.

Heureusement, la surveillance du réseau n'a pas besoin d'être une entreprise coûteuse. Il y'a beaucoup des outils libre et gratuitement disponibles qui peuvent vous montrer exactement ce qui se passe sur votre réseau en détail. Cette section vous aidera à identifier de plusieurs outils précieux et la meilleure façon de les utiliser.

Le serveur dédié à la surveillance

Alors que les services de contrôle peuvent être ajoutées à un serveur de réseau existant, il est souvent souhaitable de consacrer une machine (ou plus, si nécessaire) à la surveillance du réseau. Certaines applications (comme ntop http://www.ntop.org/) exigent des ressources considérables afin de fonctionner, en particulier sur un réseau occupé. Mais la plupart des programmes d'enregistrement et de surveillance ont de modeste exigences de RAM et du stockage, généralement avec peu de puissance CPU nécessaire. Puisque les systèmes d'exploitation libre (comme Linux ou BSD) font usage très efficient de ressources matérielles, c'est possible de mettre en point un serveur capable de surveillance à partir de pièces recyclés d'un PC. Il n'est généralement pas nécessaire d'acheter un nouveau serveur pour le reléguer à des tâches de surveillance. L'exception à cette règle est dans le cas de très grandes installations. Si votre réseau comprend plus de quelques centaines de nœuds ou si vous consommez plus de 50 Mbps de bande passante Internet, vous aurez probablement besoin de séparer les fonctions de surveillance à quelques machines dédiées. Cela dépend en grande partie de ce que vous souhaitez surveiller.

Si vous tentez de considérer tous les services accessibles par adresse MAC, cela consommera beaucoup plus de ressources que la simple mesure de flux réseau sur un port de commutateur. Mais pour la plupart des installations, une seule machine dédiée à la surveillance est généralement suffisant. Alors que la consolidation des services de surveillance à une seule machine permet de rationaliser l'administration et les mises à jour, il peut également assurer une meilleure surveillance continue. Par exemple, si vous installez des services de surveillance sur un serveur Web et ce serveur Web développe des problèmes, votre réseau ne pourra plus être surveillé jusqu'à ce que le problème soit résolu. Pour un administrateur réseau, les données recueillies sur les performances du réseau sont presque d'égale importance au réseau lui-même. Votre surveillance devrait être robuste et protégé contre les interruptions de service aussi bien que possible. Sans statistiques de réseau, vous êtes effectivement aveugle concernant les problèmes du réseau.

Comment le serveur s'intègre-t-il dans votre réseau?

Si vous êtes uniquement intéressé par la collecte de statistiques de flux de réseau à partir d'un routeur, vous pouvez le faire de n'importe où sur le LAN. Ceci fournit des informations simples sur l'utilisation mais ne peut pas vous donner des détails complets sur les modes d'utilisation. La figure NM 2 ci-dessous montre un graphique typique MRTG généré à partir du routeur Internet. Bien que l'utilisation entrants et sortants sont clairs, il n'y a pas de détails sur les ordinateurs, les utilisateurs ou les protocoles utilisant la bande passante.

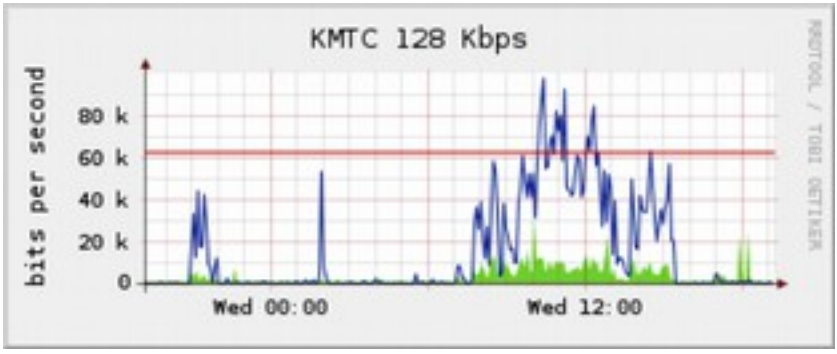


Figure NM 2: Le sondage du routeur périphérique vous montre l'usage d'ensemble du réseau mais vous ne pouvez pas décomposer les données en données machines, services et les utilisateurs.

Pour plus de détails, le serveur dédié à la surveillance doit avoir accès à tout ce qui doit être contrôlé. Typiquement, cela signifie qu'il doit avoir accès à l'ensemble du réseau.
Pour surveiller une connexion WAN, comme le lien Internet de votre FSI, le serveur de surveillance doit être en mesure de voir le trafic passant par le routeur de bord.
Pour surveiller un réseau local, le serveur de surveillance est typiquement raccordé à un port de moniteur sur le commutateur. Si plusieurs détecteurs sont utilisés dans une installation, le serveur de surveillance peut avoir besoin d'une connexion à tous ces détecteurs.
Cette connexion peut être soit un câble physique ou si vos commutateurs de réseau prennent cela en charge, un VLAN est spécialement configuré pour la surveillance du trafic.

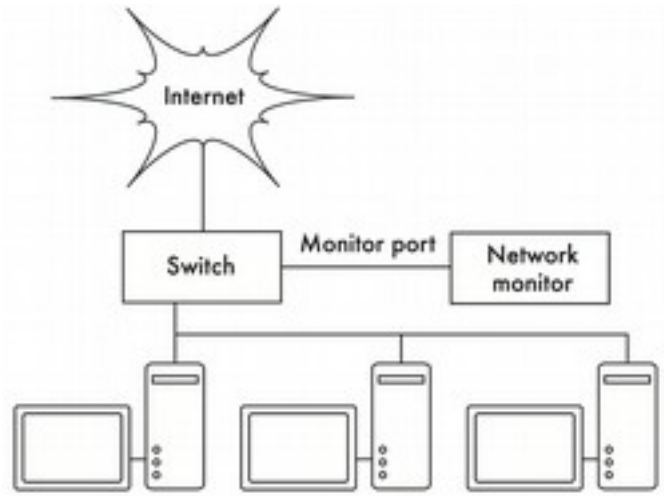


Figure NM 3: Utilisez le port moniteur de votre commutateur pour observer le trafic traversant tous les ports réseau.

Si la fonctionnalité du port de moniteur n'est pas disponible sur votre commutateur, le serveur de surveillance peut être installé entre votre réseau local interne et Internet. Bien que cela fonctionne, il y aura un point unique de défaillance pour le réseau, comme le réseau échouera si le serveur de surveillance développe un problème.
Il est également un goulot d'étranglement potentiel si le serveur ne se conforme pas aux exigences du réseau.

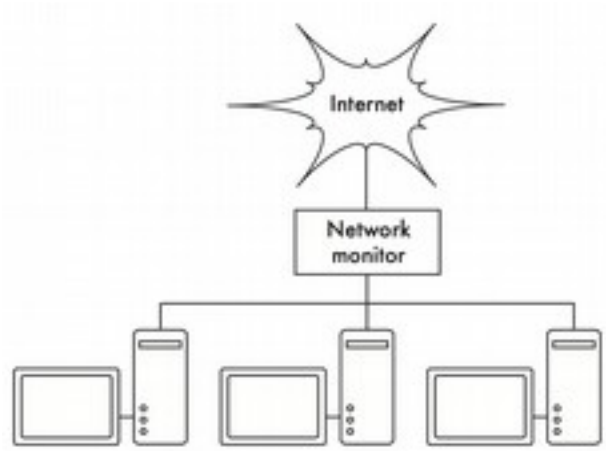


Figure 4 NM : En insérant un moniteur de réseau entre le réseau local et votre connexion Internet, vous pouvez observer tout le trafic réseau.

Une meilleure solution est d'utiliser un concentrateur de réseau simple (pas un commutateur) qui relie l'appareil de surveillance à un réseau local interne, un routeur externe et l'appareil de surveillance. Bien que cela crée toujours un point de défaillance supplémentaires sur le réseau (puisque l'ensemble du réseau sera inaccessible si le concentrateur ne fonctionne plus), les concentrateurs sont généralement considérés comme beaucoup plus fiable que les routeurs. Ils sont également très faciles à remplacer en cas d'échec.

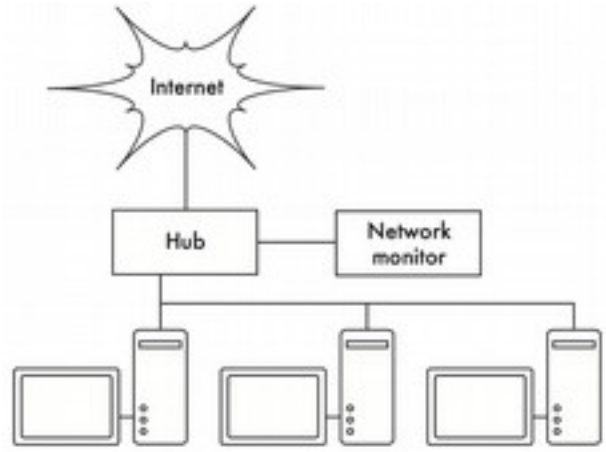


Figure NM 5: Si votre commutateur ne fournit pas de fonctionnalité port moniteur, vous pouvez insérer un concentrateur entre votre routeur et le réseau local et connecter le serveur de surveillance sur le concentrateur.

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 représenter graphiquement n'importe quel événement de réseau et d'observer sa valeur sur un graphique au fil du temps.
Étant donné que chaque réseau est légèrement différente, vous devrez décider sur l'importance de information pour évaluer la performance de votre réseau.
Voici quelques indicateurs importants que de nombreux administrateurs réseau typiquement contrôlent.

Statistiques sans fil

- Signal et le bruit reçu de tous les noeuds pivots
- Nombre de stations associées
- Les réseaux adjacents et les canaux détectés
- Retransmissions excessives
- Taux de données de radio, si vous utilisez des statistiques du commutateur à l'échelle automatique de fréquence
- L'utilisation de la bande passante par port de commutateur
- L'utilisation de la bande passante ventilées par protocole
- L'utilisation de la bande passante ventilées par adresse MAC
- Transmissions en term de pourcentage du nombre total de paquets
- La perte de paquets et le taux d'erreur

Statistiques Internet

- l'utilisation de la bande passante Internet par l'hôte et protocole
- accès au cache du serveur proxy
- 100 premier sites accessibles
- Les requêtes DNS
- Nombre des emails entrants / courriels de spam / email rebonds
- e-mail sortant taille de file d'attente
- Disponibilité des services essentiels (serveurs web, serveurs de messagerie, etc.)
- Le temps de Ping et les taux de perte de paquets de votre FSI
- Statut des copies de secours

Statistiques de la santé du système

- Utilisation de la mémoire
- l'utilisation du fichier d'échange
- Nombre de processus / processus zombies
- Charge du système
- Alimentation sans coupure (UPS) de tension et charge
- Température, la vitesse du ventilateur, et le système de tensions
- Statut de disque SMART
- Etat de la matrice RAID

Vous devez utiliser cette liste comme une suggestion de l'endroit par où commencer. Comme votre réseau évolue vous trouverez probablement de nouveaux indicateurs importants de la performance du réseau et vous devez bien sûr les contrôler aussi.
Il existe de nombreux outils librement disponibles qui vous montrera autant de détails que vous le souhaitez sur ce qui se passe sur votre réseau. Vous devriez envisager la surveillance de la disponibilité d'une ressource là où l'indisponibilité nuirait utilisateurs de votre réseau .
N'oubliez pas de veiller sur la machine de surveillance elle-même, par exemple, l'utilisation de son CPU et de son espace disque de manière à recevoir un avertissement préalable si elle devient surchargé ou défectueux. Une machine de surveillance qui est faible en ressources peut affecter votre capacité à contrôler efficacement le réseau.

Les types d'outils de surveillance

Nous allons maintenant examiner plusieurs classes différentes d' outils de surveillance.

1. Des outils de détection de réseau pour écouter les balises envoyés par les points d'accès sans fil et afficher des informations telles que le nom du réseau, intensité du signal reçu et le canal .
2. Outils de contrôle de point sont conçus pour le dépannage et fonctionnent normalement de manière interactive pour de périodes de courtes durée.
Un programme tel que ping peut être considéré comme un outil de contrôle de point active, car il génère du trafic en interrogeant une machine particulière .

3. Outils de contrôle de point passif comprennent des analyseurs de protocole, qui contrôlent tous les paquets sur le réseau et fournissent de détails complets sur n'importe quelle conversation à travers le réseau (y compris les adresses source et destination, les informations de protocole et les données même de l'application).
4 . Outils d'orientation effectuent la surveillance sans assistance pendant de longues périodes et représentent généralement les résultats sur un graphique .
5. Outils de test de débit vous donne des informations la bande passante réellement disponible entre deux points sur un réseau .
6. Outils de surveillance en temps réel effectuent une surveillance semblable mais informent les administrateurs immédiatement en cas de détection d'un problème.
7. Outils de détection d'intrusion surveillent le trafic réseau indésirable ou inattendu et prennent les mesures appropriées (généralement nier l'accès et / ou avertir un administrateur réseau).

Détection réseau

Les simples outils de surveillance sans fil fournissent simplement une liste des réseaux disponibles ainsi que des informations de base (telles que la puissance du signal et le canal).
Ils vous permettent de détecter rapidement les réseaux à proximité et de déterminer s'ils sont rangés ou causent de l'interférence.

Le client intégré.

Tous les systèmes d'exploitation modernes fournissent un soutien intégré pour les réseaux sans fil.

Cela comprend généralement la possibilité de scanner les réseaux disponibles, permettant à l'utilisateur de choisir un réseau à partir d'une liste.
Alors que pratiquement tous les périphériques sans fil sont garantis d'avoir un utilitaire de numérisation simple, la fonctionnalité peut varier considérablement entre les implémentations.
Ces outils ne sont généralement utiles pour configurer un ordinateur dans un cadre domestique ou de bureau. Ils ont tendance à fournir peu d'informations en dehors des noms de réseau et le signal disponible au point d'accès en cours d'utilisation.

Netstumbler

(http://www.wirelessdefence.org/Contents/NetstumblerMain.htm) .
C'est l'outil le plus populaire pour détecter les réseaux sans fil à l'aide de Microsoft Windows.
Il prend en charge une variété de cartes sans fil et il est très facile à utiliser. Il permet de détecter les réseaux ouverts et cryptés mais ne peut pas détecter les réseaux sans fil "fermés". Il dispose également d' un compteur de signal / bruit qui représentent les données du récepteur de radio sous forme graphique au fil du temps. Il intègre également une variété de dispositifs GPS pour enregister les informations précises sur l'emplacement et la force du signal. Ceci rend Netstumbler un outil pratique qu'il faut avoir pour une étude de site informel. MacStumbler (http://www.macstumbler.com/). Bien que n'étant pas directement liés à la Netstumbler, MacStumbler fournit une grande partie de la même fonctionnalité, mais pour la plate-forme Mac OS X. Il fonctionne avec toutes les cartes Airport d'Apple .

Outils de contrôle intermittent

Que faites-vous lors de la rupture du réseau? Si vous ne pouvez pas accéder à une page Web ou un serveur de messagerie et que cliquer sur le bouton de rechargement ne résout pas le problème, alors vous devez être en mesure d'isoler l'endroit exact du problème.
Ces outils vous aideront à déterminer exactement l'endroit où il ya un problème de connexion.
Cette section est tout simplement une introduction à des outils de dépannage couramment utilisé.
Pour une discussion plus approfondie des problèmes courants de réseau et la façon de les diagnostiquer, voir le chapitre intitulé **Entretien et dépannage**.

ping

Presque tous les systèmes d'exploitation (y compris Windows, Mac OS X, et bien sûr Linux et BSD) incluent une version de l'utilitaire ping.
Ceci utilise des paquets ICMP pour tenter de communiquer avec un hôte spécifié et vous indique combien de temps il faut pour obtenir une réponse. Savoir qu'est-ce qu'il faut ping est tout aussi important que de savoir comment faire un ping.
Si vous trouvez que vous ne pouvez pas vous connecter à un service particulier dans votre navigateur Web (par exemple, http://yahoo.com/), vous pouvez essayer le ping:

$ ping yahoo.com

PING yahoo.com (66.94.234.13) : 56 octets de données
64 octets de 66.94.234.13 : icmp_seq = 0 ttl = 57 time = 29,375 ms
64 octets de 66.94.234.13 : icmp_seq = 1 ttl = 56 time = 35,467 ms
64 octets de 66.94.234.13 : icmp_seq = 2 ttl = 56 time = 34,158 ms
^ C

--- Statistiques de ping yahoo.com ---

3 paquets transmis, 3 paquets reçus, 0 % de perte de paquets
round-trip min / avg / max / stdDev = 29.375/33.000/35.467/2.618 ms

Hit contrôle - C lorsque vous avez terminé la collecte de données .
Si les paquets prennent beaucoup de temps à revenir, il peut y avoir congestion du réseau. Si les paquets retour de ping ont une durée de vie [Time To Live (TTL)] exceptionnellement bas, vous pouvez avoir des problèmes de routage entre votre machine et la destination distante. Mais que faire si le ping ne retourne pas de données du tout? Si vous interrogez un nom au lieu d'une adresse IP, vous pouvez avoir les problèmes de DNS. Essayez d'interroger une adresse IP sur Internet.
Si vous ne pouvez pas l'atteindre, c'est une bonne idée pour voir si vous pouvez faire un ping de votre routeur par défaut :

$ ping 69.90.235.230

PING 69.90.235.230 (69.90.235.230) : 56 octets de données

64 octets de 69.90.235.230 : icmp_seq = 0 ttl = 126 time = 12,991 ms
64 octets de 69.90.235.230 : icmp_seq = 1 ttl = 126 time = 14.869 ms
64 octets de 69.90.235.230 : icmp_seq = 2 ttl = 126 time = 13,897 ms
^ C

--- 216.231.38.1 statistiques ping ---

3 paquets transmis, 3 paquets reçus, 0 % de perte de paquets
round-trip min / avg / max / stdDev = 12.991/13.919/14.869/0.767 ms

Si vous ne pouvez pas exécuter ping sur votre routeur par défaut alors les chances sont que vous ne serez pas en mesure de vous connecter à l'Internet. Si vous ne pouvez même pas exécuter un ping d'autres adresses IP sur votre réseau local, il est temps de vérifier votre connexion.
Si vous utilisez Ethernet, est-il branché? Si vous utilisez le sans fil, êtes-vous connecté au réseau sans fil approprié et est-il à portée?
Alors qu'il est généralement justifié de supposer qu'une machine qui ne répond pas à une commande ping est susceptible d'être bas ou coupé du réseau ce n'est pas toujours à 100 % de cas. En particulier sur un WAN ou Internet lui-même, il est également possible que certains routeur / pare-feu entre vous et l'hôte cible (même la cible elle-même) bloque les pings . Si vous trouvez une machine ne répond pas aux pings, essayez un autre service bien connu comme ssh ou http. Si vous pouvez atteindre la cible à travers l'un de ces services alors vous savez que la machine est opérationelle mais elle est entrain tout simplement de bloquer pings.
Il est également intéressant de noter que différents systèmes traitent ping différemment. L'utilitaire ping classique UNIX envoie un paquet ICMP ECHO protocole de l'hôte cible.
Certains périphériques de réseau répondront à la commande ping automatiquement indépendamment du fait que ICMP est bloquée en amont de la pile de protocole. Cela peut aussi être trompeur car il peut indiquer qu'un hôte est opérationel alors qu'en réalité, tout ce qui se passe réellement, c'est que le NIC (Network Interface Card) est sous tension et la machine elle-même n'est pas réellement en marche.
Comme nous l'avons dit ci-dessus, il est toujours bon de vérifier la connectivité avec de multiples méthodes. Le débogage de réseau avec ping est un peu un art mais il est utile d'apprendre
Comme vous allez probablement trouver ping sur presque toutes les machines sur lesquelles vous allez travailler, c'est une bonne idée d'apprendre à bien l'utiliser.

traceroute et mtr

http://www.bitwizard.nl/mtr/ . Comme ping, traceroute se trouve sur la plupart des systèmes d'exploitation (ça s'appelle tracert dans certaines versions de Microsoft Windows).

En exécutant traceroute, vous pouvez localiser les problèmes entre votre ordinateur et un point quelconque sur l'Internet:

$ traceroute - n google.com

traceroute à google.com (72.14.207.99), 64 hops max, 40 paquets d'octets

1 10.15.6.1 4.322 ms 1.763 ms 1.731 ms

2 216.231.38.1 36,187 14,648 ms ms 13,561 ms

3 69.17.83.233 14,197 13,256 ms ms 13,267 ms

4 69.17.83.150 32,478 29,545 ms ms 27,494 ms

5 198.32.176.31 40,788 28,160 ms ms 28,115 ms

6 66.249.94.14 28,601 29,913 ms ms 28,811 ms

7 172.16.236.8 2,328,809 2,528,944 ms ms ms 2428,719

*8 ****

L'option -n indique à traceroute de ne pas déranger la résolution des noms dans DNS, et rend l'exécution de la trace plus rapide.
Vous pouvez voir que, à l'étape sept, le temps de parcours tire à plus de deux secondes tandis que les paquets semblent être éliminés à l'étape huit.
Cela pourrait indiquer un problème à ce moment-là dans le réseau.
Si cette partie du réseau est sous votre contrôle, il pourrait être important de commencer votre effort de dépannage par-là. Mon TraceRoute (mtr) est un programme pratique qui combine ping et traceroute dans un seul outil.

En exécutant mtr, vous pouvez savoir la moyenne des temps de latence et la perte de paquet pour un seul hôte, au lieu de la capture instantanée que ping et traceroute fournissent.

My traceroute [v0.69]

tesla.rob.swn (0.0.0.0) (tos= fix0 psize = 64 bitpat Dimanche 8 janvier 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.net	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 continuellement mis à jour et en moyenne au cours du temps. Comme ping, vous devez taper control - C lorsque vous avez terminé l'examen des données.
Notez que vous devez avoir les privilèges d'être root pour exécuter mtr.
Bien que ces outils ne révèleront pas précisément ce qui ne va pas avec le réseau, ils peuvent vous donner assez d'informations pour savoir où continuer le dépannage.

Analyseurs de protocole

Analyseurs de protocole de réseau fournissent un grand nombre de détails sur les informations circulant dans un réseau en vous permettant d'inspecter les paquets particuliers. Pour les réseaux câblés, vous pouvez inspecter les paquets à la couche de liaison de données ou au-dessus. Pour les réseaux sans fil, vous pouvez inspecter toutes les informations en bas de tous les trames 802.11.
Voici quelques analyseurs de protocole de réseau bien connus (et gratuit) :

Kismet

http://www.kismetwireless.net/ .
Kismet est un puissant analyseur de protocole sans fil pour de nombreuses plates-formes, y compris Linux, Mac OS X, et même la distribution OpenWRT Linux intégré. Il fonctionne avec n'importe quelle carte sans fil qui prend en charge le mode de surveillance passive. En plus de la détection de base du réseau, Kismet identifiera passivement toutes les trames 802.11 sur le disque ou sur le réseau en format PCAP standard pour une analyse ultérieure avec des outils comme Wireshark.

Kismet dispose également d' informations associées au client, AP matériel 0ngerprinting, la détection Netstumbler et l'intégration du GPS.
Comme 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 machines au bureau, et avoir tous les rapport sur le réseau vers une interface de l'utilisateur central.
Cela permet la surveillance sans fil sur une grande surface, comme une université ou un campus d'entreprise. Comme Kismet utilise le mode de surveillance passive de la carte radio, il fait tout cela sans transmettre les données. Kismet est un outil précieux pour diagnostiquer les problèmes de réseau sans fil .

KisMAC

http://kismac-ng.org/
Exclusivement pour la plate-forme Mac OS X, KisMAC fait beaucoup de ce que Kismet peut faire, mais avec une interface graphique lisse de Mac OS X. Il s'agit d'un scanner passif qui identifiera les données sur le disque au format PCAP compatible avec Wireshark.
Il prend en charge l'analyse passive avec les cartes AirportExtreme ainsi qu'une variété d'adaptateurs sans fil USB.

tcpdump

http://www.tcpdump.org/ tcpdump
Est un outil de commande en ligne pour surveiller le trafic dans le réseau.
Il ne possède pas toutes les propriétés de wireshark mais il utilise moins de ressources .Tcpdump peut capturer et afficher toutes les informations de protocole de réseau jusqu'à la couche de liaison.
Il peut afficher tous les en-têtes de paquets et les données reçues, ou seulement les paquets qui correspondent à des critères particuliers. Les paquets capturés avec tcpdump peuvent être chargés dans wireshark pour visuel analyse et de diagnostic supplémentaires .
Ceci est très utile si vous souhaitez contrôler une interface sur un système distant et mettre le fichier à votre machine locale pour l'analyse.
L'outil tcpdump est disponible comme un outil standard dans les produits dérivés d'Unix (Linux, BSD et Mac OS X). Il ya aussi un port Windows appelé WinDump disponible à http://www.winpcap.org/windump/ .

Wireshark

http://www.wireshark.org/.

Anciennement connu sous le nom Ethereal, Wireshark est un analyseur de protocole de réseau gratuit pour Unix et Windows.

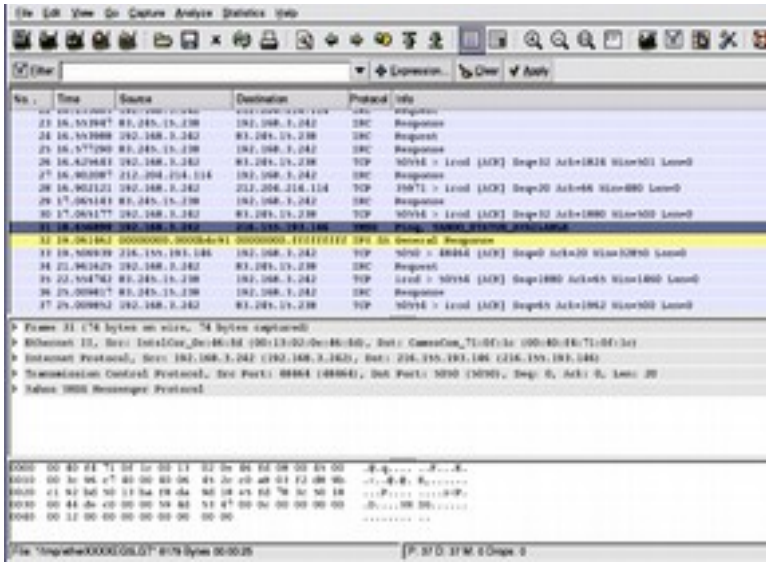


Figure NM 6: Wireshark (anciennement Ethereal) est un puissant analyseur de protocole réseau qui peut vous montrer autant de détails que vous le souhaitez sur tous les paquets.

Wireshark vous permet d'examiner les données d'un réseau en direct ou à partir d'un fichier de capture sur le disque, et de manière interactive parcourir et trier les données capturées.
Ensemble résumé et des informations détaillées sont disponibles pour chaque paquet, y compris l'en-tête complet et des parties de données.
Wireshark a plusieurs fonctionnalités puissantes y compris un riche langue d'affichage du filtre et la possibilité de visualiser le flux reconstruit d'une session TCP. Ceci peut être intimidant à utiliser pour les débutants ou ceux qui ne sont pas familiers avec les couches OSI.
C'est généralement utilisé pour isoler et analyser le trafic specique vers ou à partir d'une adresse IP mais il peut également être utilisé comme un outil d'usage général de recherche de panne.
Par exemple, une machine infectée par un ver de réseau ou d'un virus peut être identifiée par la recherche de la machine qui envoie le même genre de paquets TCP / IP à de grands groupes d'adresses IP.

Outils d'orientation

Les outils d'orientation sont utilisés pour voir comment votre réseau est utilisé sur une longue période. Ils travaillent en surveillant régulièrement l'activité de votre réseau et afficher un résumé sous une forme lisible par l'homme (comme un graphique). Outils d'orientation recueillissent des données et les analysent et produisent le rapport à ce sujet. Voici quelques exemples d'outils dorientation. Certains d'entre eux doivent être utilisés en conjonction avec l'autre comme ils ne sont pas des programmes autonomes.

MRTG

http://oss.oetiker.ch/mrtg/ . Le Multi Routeur Traffic Grapher (MRTG) surveille la charge de trafic sur les liaisons de réseau via SNMP. MRTG génère des graphiques qui fournissent une représentation visuelle de trafic entrant et sortant. Ceux-ci sont généralement affichés sur une page Web. MRTG peut être un peu compliqué à configurer surtout si vous n'êtes pas familier avec SNMP. Mais une fois installé, MRTG nécessite pratiquement aucun entretien sauf si vous modifiez quelque chose sur le système qui est surveillé (comme son adresse IP).

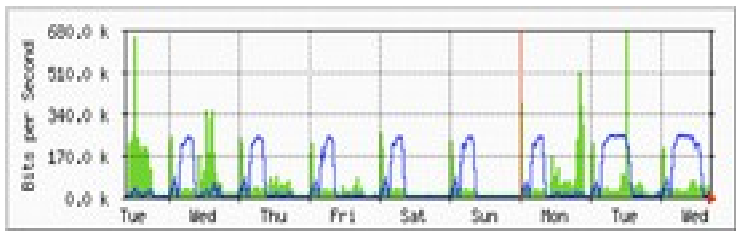


Figure NM 7: MRTG est probablement le grapheur de trafic réseau le plus largement installé.

RRDtool

RRD est l'abréviation de la base de données Round Robin. RRD est une base de données qui stocke des informations d'une manière très compacte qui ne s'etend pas au cours du temps. RRDtool se réfère à un ensemble d'outils qui vous permettent de créer et de modifier les bases de données RRD et de générer des graphiques utiles pour présenter les données. Il est utilisé pour garder une trace des données de séries chronologiques (tels que la bande passante du réseau, la température de la salle des machines ou la charge moyenne du serveur) et peut afficher les données en moyenne au cours du temps.

Notez que RRDtool lui-même n'entre pas en contact avec les dispositifs du réseau pour récupérer des données.
Il s'agit simplement d'un outil de manipulation de base de données.
Vous pouvez utiliser un script enveloppe (généralement en shell ou Perl) pour faire ce travail pour vous. RRDtool est également utilisé par de nombreux frontaux complet qui vous présentent avec une interface web conviviale pour la configuration et l'affichage. Graphes RRD vous donnent plus de contrôle sur les options d'affichage et le nombre d'articles disponibles sur un graphique par rapport à MRTG.

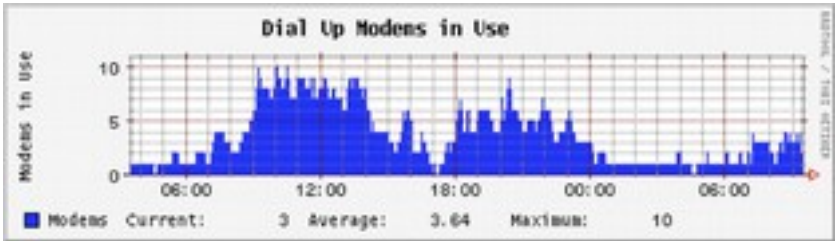


Figure NM 8: RRDtool vous donne beaucoup de flexibilité dans la façon dont les données collectées dans le réseau peuvent être affichées .

RRDtool est inclus dans pratiquement toutes les distributions Linux modernes et peut être téléchargé à partir http://oss.oetiker.ch/rrdtool/ .

ntop

Pour l'historique de l'analyse et de l'usage du trafic, vous aurez certainement envie de connaître ntop. Ce programme génère en temps réel un rapport détaillée du trafic observé sur le réseau, affiché dans votre navigateur. Il s'intègre avec rrdtool et produit des graphiques et des diagrammes illustrant visuellement comment le réseau est utilisé. Sur les réseaux très occupés, ntop peut utiliser beaucoup de CPU et d'espace disque mais il vous donne vaste aperçu de la façon dont votre réseau est utilisé.
Il fonctionne sur Linux, BSD, Mac OS X et Windows.
Certaines de ses caractéristiques les plus utiles incluent :

- Affichage du trafic peut être triée selon différents critères (source, destination, protocole, par adresse MAC, etc.)
- Statistiques de trafic regroupées par le protocole et le numéro de port.

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

ntop est disponible à partir de http://www.ntop.org/ pour la plupart des systèmes d'exploitation. Il est souvent inclus dans la plupart des distributions Linux populaires, y compris RedHat, Debian et Ubuntu.
Alors qu'il peut être laissé en marche pour recueillir des données historiques, ntop peut utiliser assez dd CPU en fonction de la quantité de trafic observé. Si vous l'exécutez pendant de longues périodes vous devriez veiller sur l'utilisation du processeur de la machine de surveillance.

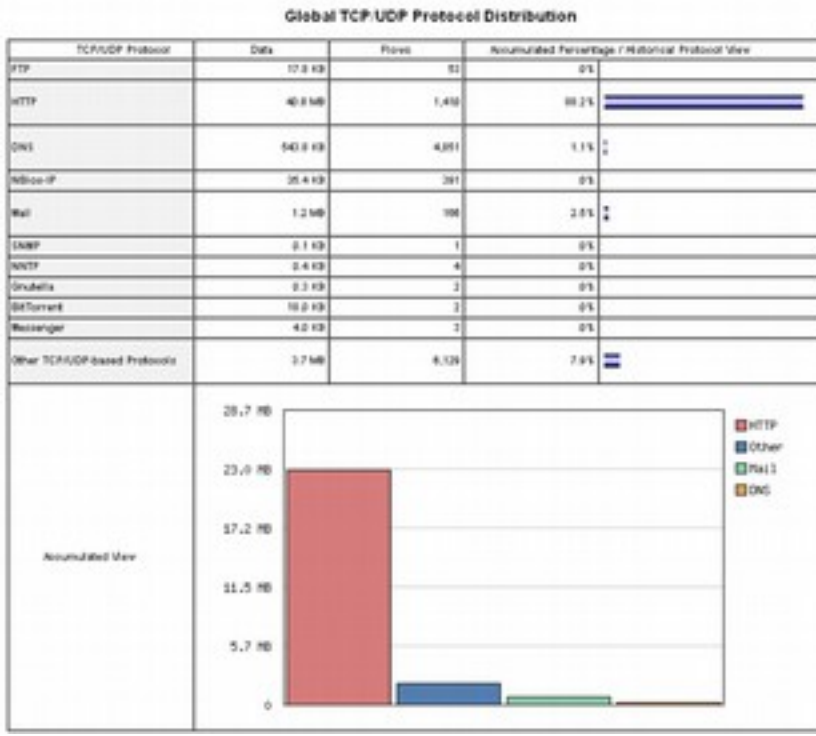


Figure NM 9: ntop affiche beaucoup d'informations sur la façon dont votre réseau est utilisé par de nombreux clients et serveurs.

Le principal inconvénient de ntop est qu'il ne fournit pas d'information instantanée mais seulement les totaux et les moyennes à long terme.
Cela peut rendre difficile à utiliser pour diagnostiquer un problème qui commence soudainement.

Cacti

http://www.cacti.net/. Cacti est une interface pour RRDtool. Il stocke toutes les informations nécessaires pour créer des graphiques dans une base de données MySQL . L'interface est écrite en PHP .
Cactus fait le travail de maintien des graphiques, des sources de données et gère la collecte de données réelle.
Il est le support des périphériques SNMP et des scripts personnalisés peuvent être facilement écrite pour interroger n'importe quel événement envisageable du réseau.

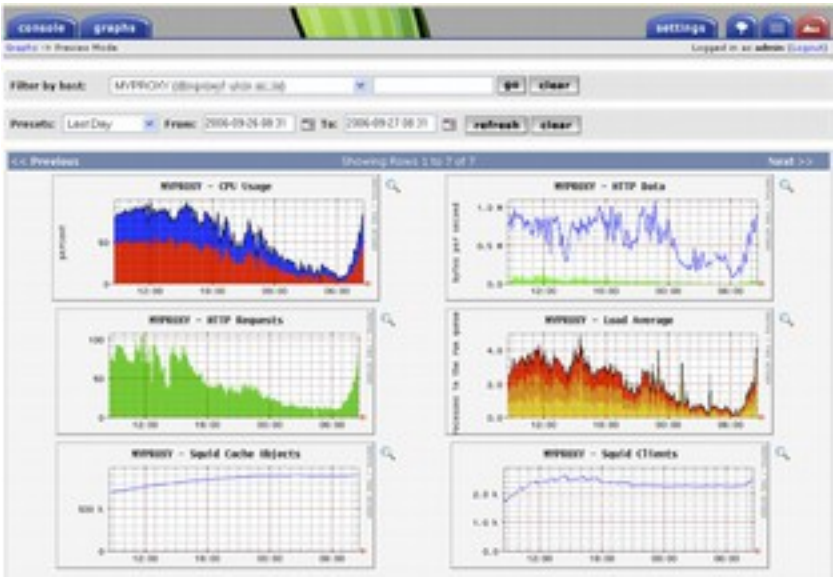


Figure NM 10: Cacti permet de gérer le choix de vos périphériques réseau et peut construire des visualisations très complexes et informatives de comportement du réseau.

Cacti peut être un peu compliqué à configurer mais une fois vous lisez la documentation et des exemples et ça peut produire des graphiques très impressionnants.

Il ya des centaines de modèles pour différents systèmes disponibles sur le site Web de cactus et le code est en cours de développement rapide.

NetFlow

NetFlow est un protocole de collecte d'informations de trafic IP inventé par Cisco. Depuis le site Web de Cisco:
Cisco IOS NetFlow fournit efficacement un ensemble clé de services pour les applications IP, y compris la comptabilité du trafic dans le réseau, facturation du réseau en fonction de l'utilisation, la planification du réseau, la sécurité, le déni de capacités de surveillance des services et la surveillance du réseau.
NetFlow fournit de précieuses informations sur les utilisateurs du réseau et des applications, les temps d'utilisation de pointe et le routage du trafic .
Routeurs Cisco peuvent générer des informations NetFlow qui sont disponible sur le routeur sous la forme de paquets UDP. NetFlow utilise également moins de CPU sur les routeurs Cisco que SNMP. Il fournit également des informations plus précises que SNMP, vous permettant d'obtenir une image plus détaillée de port et le protocole d'utilisation. Cette information est recueillie par un collecteur NetFlow qui stocke et présente les données comme un ensemble au fil du temps. En analysant les données de flux, on peut construire une image des flux de trafic et le volume de trafic dans un réseau ou une connexion. Il ya plusieurs collecteurs NetFlow commerciales et disponibles. Ntop est un outil gratuit qui peut agir comme un collecteur NetFlow et sonde. Un autre est Flowc (voir ci-dessous).
Il peut également être souhaitable d'utiliser NetFlow comme un outil de contrôle ponctuel, simplement en regardant un aperçu rapide des données au cours d'une crise de réseau. Pensez à NetFlow comme une alternative à SNMP pour les périphériques Cisco. Pour plus d'informations sur NetFlow, voir http://en.wikipedia.org/wiki/NetFlow .

Flowc

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

Figure NM 11: Un diagramme typique EOW généré par Flowc .

L'écart important dans les données indique probablement une panne de réseau.
Outils d'orientation généralement ne vous informera pas des pannes mais simplement enregister les événement.
Pour être averti quand des problèmes de réseau surviennent fréquemment, utilisez un outil de surveillance en temps réel tels que Nagios.

SmokePing

http://oss.oetiker.ch/smokeping/ . SmokePing est un outil de luxe de mesure de la latence écrit en Perl.
Il peut mesurer, stocker et afficher la latence, la distribution de latence et perte de paquets tout sur un seul graphique.
SmokePing utilise RRDtool pour le stockage de données et peut dessiner des graphiques très instructifs qui présentent des informations à la minute sur l'état de votre connexion réseau.
Il est très utile d'exécuter SmokePing sur un hôte avec une bonne connectivité sur l'ensemble de votre réseau. Au fil du temps, les tendances se dévoilent et indiquent toutes sortes de problèmes de réseau.
Combiné avec MRTG ou Cact, vous pouvez observer l'effet que la congestion du réseau a sur la perte de paquets et la latence.
SmokePing peut éventuellement envoyer des alertes lorsque certaines conditions sont remplies, par exemple lorsque la perte excessive de paquets est vu sur un lien pour une période de temps prolongée.

Un exemple de SmokePing en action est représentée sur la figure 12 NM.

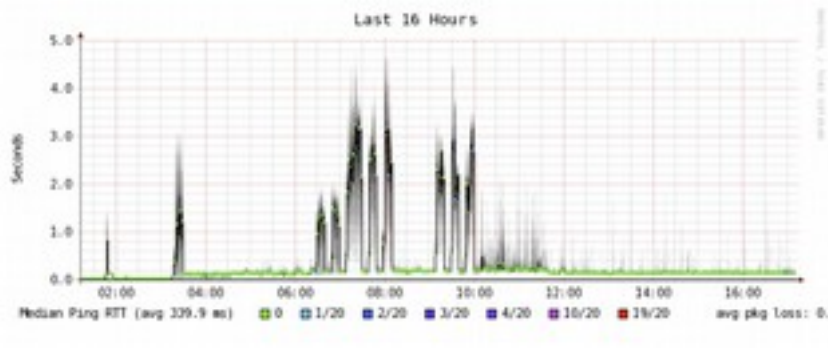


Figure NM 12: SmokePing peut afficher simultanément la perte de paquets et les écarts de latence dans un seul graphique .

EtherApe

http://etherape.sourceforge.net/ . EtherApe affiche une représentation graphique du trafic de réseau.
Les hôtes et les liens changent de taille en fonction de la quantité de trafic envoyé et reçu.
Les couleurs changent pour représenter le protocole le plus utilisé.
Comme avec wireshark et tcpdump, les données peuvent être capturées "hors-fil" à partir d'une connexion réseau ou lus à partir d'un fichier de capture tcpdump.
EtherApe ne montre pas tout à fait autant de détails que ntop mais ses besoins en ressources sont beaucoup plus légers.

iptraf

http://iptraf.seul.org/ . IPTraf est un moniteur sans fil léger mais puissant.
Il dispose d'une interface ncurses et fonctionne dans un shell de commande.
IPTraf prend un moment pour mesurer le trafic observé, puis affiche diverses statistiques de réseau, y compris les connexions TCP et UDP, ICMP et OSPF information, les flux de trafic, erreurs de total de contrôle IP et plus encore.
C'est un programme simple à utiliser et fonctionne avec un minimum de ressources.
Bien qu'il ne conserve pas de données historiques, il est très utile pour afficher un rapport d'utilisation instantanée .

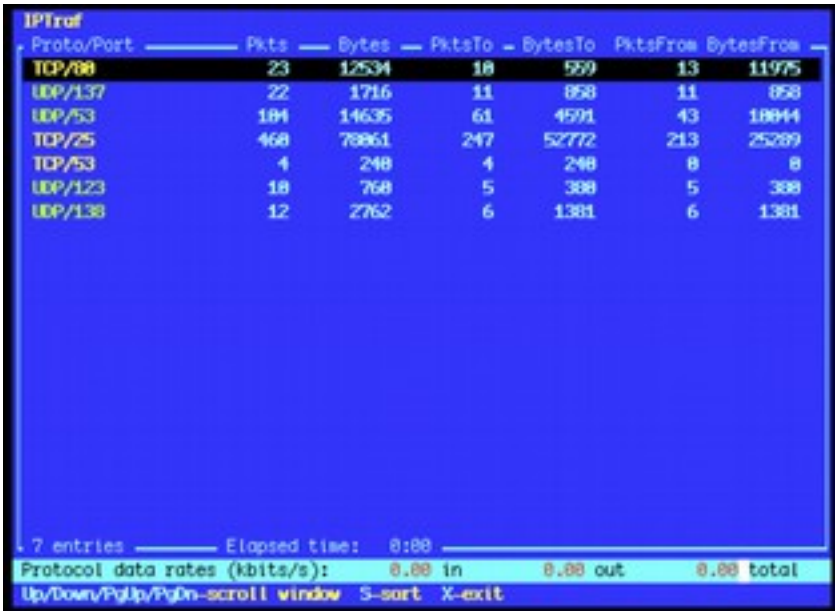


Figure NM 13: Répartition statistique par iptraf du trafic par port .

Argus

http://qosient.com/argus/

Argus est une abréviation de «Audit Record Generation and Utilisation System» qui signifie «génération de la fiche de vérification et d'utilisation du système». Argus est également le nom du dieu de la mythologie grecque qui avait des centaines d'yeux .

Depuis le site Web Argus :

Argus génère des statistiques de flux tels que la connectivité, la capacité, la demande, perte, retard, turbulence sur base de l'unité de transaction. Argus peut être utilisé pour analyser et faire rapport sur le contenu des fichiers de capture de paquets ou il peut fonctionner comme un contrôle continu, examinant des données à partir d'une interface connectée; générant un journal d'audit de toute l'activité du réseau observé dans le flux de paquets. Argus peut être déployée pour surveiller les systèmes individuels d'extrémité, ou toute une activité de réseau des entreprises. Pour un contrôle continu, Argus fournit des modèles de traitement des données combinant à la fois pousser et tirer, pour permettre des stratégies flexibles pour collecter des données d'audit du réseau. Clients de données Argus supportent un ensemble d'opérations tels que le tri, le rassemblage, l'archivage et le reportage.

Argus se compose de deux parties: un collecteur principal qui lit les paquets provenant d'un périphérique réseau et un client qui se connecte au collecteur principal et affiche les statistiques d'utilisation. Argus fonctionne sur BSD, Linux et la plupart des autres systèmes UNIX .

NeTraMet
http://www.caida.org/tools/measurement/netramet/. NeTraMet est un autre outil populaire d'analyse de flux. Comme Argus, NeTraMet se compose de deux parties: une collection qui rassemble des statistiques via SNMP et un gestionnaire qui spécifie le flux à contrôler. Les flux sont spécifiés en utilisant un langage de programmation simple qui définit les adresses utilisées à chaque extrémité et peuvent inclure Ethernet, IP, informations de protocole ou d'autres identificateurs. NeTraMet fonctionne sur DOS et la plupart des systèmes UNIX, y compris Linux et BSD .

Les tests de débit

Quelle est la durée du réseau?Quelle est la capacité réelle utilisable d'une liaison réseau particulière ? Vous pouvez obtenir une très bonne estimation de votre capacité de débit en chargeant le lien avec le trafic et mesurer le temps de transfert de données.

Figure NM 14: Des outils tels que celui-ci provenant de SpeedTest.net sont jolis, mais ils ne produisent pas toujours une image précise de la performance du réseau.

Bien qu'il existe de pages Web disponibles capable d'effectuer un «test de vitesse» dans votre navigateur (comme http://www.dslreports.com/stest ou http://speedtest.net/), ces tests sont de plus en plus inexacte quand vous vous eloignez de la source de test. Pire encore, ils ne vous permettent pas de tester la vitesse d'un lien donné mais seulement la vitesse de votre lien vers un site particulier sur Internet. Voici quelques outils qui vous permettront de réaliser des tests de débit sur vos propres réseaux.

ttcp

Maintenant une partie standard de la plupart des systèmes Unix, ttcp est un simple outil de test de performance de réseau. Un exemple est exécuté sur chaque côté du lien que vous souhaitez tester. Le premier nœud fonctionne en mode récepteur et l'autre en transmetteur:

nœud_a$ ttcp -r -s

node_b$ ttcp - t -s nœud_a

ttcp-t: buflen = 8192, nbuf = 2048, align = 16384 / 0, port = 5001 tcp - >

nœud_a

ttcp-t: socket

ttcp-t: connect

ttcp-t: 16777216 octets 249,14 secondes réelles = 65.76 Ko / s + + +

ttcp-t: 2048 appels d'E / S, ms / call = 124.57, les appels / sec = 8.22

ttcp- t: 0.0user 0.2sys 04:09 réel 0 % 0 0i d 0maxrss 0 +0 +0 pf 7533 csw

Après la collecte de données dans un sens, vous devez inverser la transmission et la réception des partenaires pour tester le lien dans l'autre sens. Ceci peut tester UDP ainsi que les flux TCP et peut modifier divers paramètres TCP et des longueurs de tampons pour donner au réseau une bonne séance d'entraînement. Il peut même utiliser un flux de données fournies par l'utilisateur au lieu d'envoyer des données aléatoires.
Rappelez-vous que l'indicateur 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 réel de ttcp est qu'il n'a pas été développé au cours des années .

Heureusement, le code a été publié dans le domaine public et est disponible gratuitement. Comme ping et traceroute, ttcp se trouve comme un outil standard sur de nombreux systèmes .

iperf

http://iperf.sourceforge.net/

Tout comme ttcp, iperf est un outil de ligne de commande pour estimer le débit d'une connexion réseau. Il prend en charge un grand nombre des mêmes fonctionnalités que ttcp mais utilise un «client» et «serveur» modèle à la place d'une paire «recevoir» et «transmettre».

Pour exécuter iperf, lancer un serveur sur un côté et un client sur l'autre:

nœud_a$ iperf -s

node_b$ iperf - c nœud_a

--- ----------------------

Client qui se connecte au nœud_a, le port TCP 5001

Taille de la fenêtre TCP: 16.0 Ko (valeur par défaut)

--- ----------------------

[5] local 10.15.6.1 port 1212 connecté à 10.15.6.23 port 5001

[ID] Interval de bande passante de Transfert

[5] 0,0-11,3 sec 768 Ko 558 Kbits/s

Le côté serveur continuera à écouter et à accepter les connexions du client sur le port 5001 jusqu'à ce que vous atteignez le contrôle - C pour l'arrêter. Cela peut être très pratique pour l'exécution de plusieurs séries de tests à partir de plusieurs endroits. La plus grande différence entre ttcp et iperf est que iperf est en cours de développement et a beaucoup de nouvelles fonctionnalités (y compris le support IPv6).

Cela en fait un bon choix comme un outil de performance lors de la construction de nouveaux réseaux .

bing

http://fgouget.free.fr/bing/index-en.shtml.

Plutôt que charger une connexion avec les données et observer la durée de transfert complet «test Wood», bing tente d'estimer le débit disponible

d'une connexion point-à-point en analysant les temps d'aller-retour pour paquets ICMP de différentes tailles. Alors qu'il n'est pas toujours aussi précis que le test Wood, il peut fournir une bonne estimation sans la transmission d'un grand nombre d'octets. Comme bing fonctionne en utilisant des requêtes d'écho ICMP, il peut estimer la bande passante disponible sans avoir à exécuter un client spécial sur l'autre extrêmité et peut même tenter d'estimer le débit de liens en dehors de votre réseau. Comme il utilise peu de bande passante, bing peut vous donner une idée approximative des performances du réseau sans courir les frais qu'un test Wood devrait certainement encourir.

Outils en temps réel et la détection d'intrusion

Il est souhaitable de savoir lorsque les gens essaient de s'introduire dans votre réseau ou quand une partie du réseau a échoué. Parce que aucun administrateur du système ne peut être surveiller un réseau tout le temps, il ya des programmes qui surveillent en permanence l'état du réseau et peut envoyer des alertes lorsque des événements notables se produisent.
Ce qui suit sont des outils libre qui peuvent aider à effectuer cette tâche.

Snort

Snort (http://www.snort.org/) est un paquets renifleur et enregistreur qui peut être utilisé comme un système de détection d'intrusion dans un réseau léger. Il dispose d'enregistrement fondé sur des règles et peut effectuer une analyse de protocole, recherche de contenu et paquet correspondant. Il peut être utilisé pour détecter une variété d'attaques et de sondes, tels que les scans de ports furtif, les attaques CGI, les sondes SMB, tentatives OS 0ngerprinting et de beaucoup d'autres types de modèles de trafic anormal. Snort a une capacité d'alerte en temps réel qui peut informer les administrateurs sur les problèmes à mesure qu'ils se produisent avec une variété de méthodes. Installation et exécution de Snort n'est pas banal, et en fonction de la quantité du trafic dans le réseau, il nécessitera probablement une machine dédiée à la surveillance avec des ressources considérables. Heureusement, Snort est très bien documenté et a une forte communauté d'utilisateurs. En mettant en place un ensemble de règles complètes de Snort, vous pouvez identifier un comportement inattendu qui, autrement, mystérieusement manger votre bande passante Internet. Voir http://snort.org/docs/ pour une longue liste de ressources d'installation et de configuration.

Apache : mod_security

ModSecurity (http://www.modsecurity.org/) est un système libre de détection d'intrusion et moteur de prévention pour les applications web.
Ce type d'outil de sécurité est également connu comme un pare-feu d'application web.
ModSecurity augmente la sécurité des applications Web en protégeant les applications web contre les 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 révisées de mod_security qui aident à protéger contre les dernières failles de sécurité.
Une excellente ressource est GotRoot, qui maintient un référentiel énorme et fréquemment révisées des règles:
http://www.atomicorp.com/wiki/index.php/Atomic_ModSecurity_Rules
La sécurité des applications Web est importante dans la défense contre les attaques sur votre serveur web qui pourrait entraîner le vol de données importantes ou personnelles, ou dans le serveur utilisé pour lancer des attaques ou envoyer du spam à d'autres utilisateurs d'Internet.
En plus d'être dommageable pour l' Internet dans son ensemble, de telles intrusions peuvent sérieusement réduire votre bande passante disponible.

Nagios

Nagios (http://nagios.org/) est un programme qui surveille les hôtes et services sur votre réseau, vous informant immédiatement en cas de problème.
Il peut envoyer des notifications par e-mail, SMS ou en exécutant un script et envoyer des notifications à la personne ou le groupe concerné en fonction de la nature du problème.
Nagios fonctionne sur Linux ou BSD et fournit une interface Web pour afficher l'état du système à la minute. Nagios est extensible et peut surveiller l'état de n'importe quel événement de réseau en pratique. Il effectue des contrôles en exécutant de petits scripts à intervalles réguliers et vérifie les résultats contre une réponse attendue. Cela peut conduire à des contrôles beaucoup plus sophistiqués qu'une simple sonde de réseau.
Par exemple, ping peut vous dire que la machine est allumée et nmap peut signaler que le port TCP répond aux demandes mais Nagios peut effectivement récupérer une page web ou faire une demande de base de données et vérifier que la réponse n'est pas une erreur.

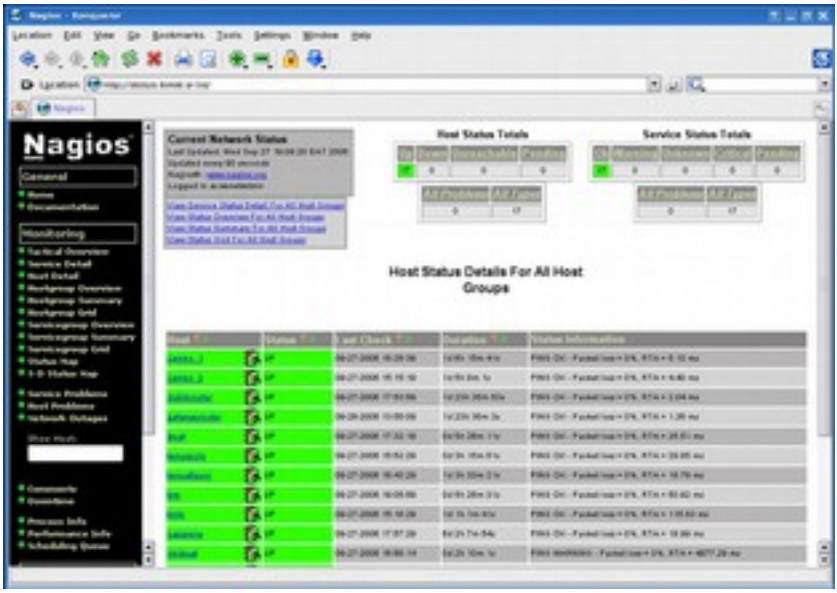


Figure NM 15: Nagios vous informe du moment où un défaut d'un réseau ou panne d'un service se produit.

Nagios peut même vous informer de l'utilisation de la bande passante, la perte de paquets, la température ambiante de la machine, ou qu'un autre indicateur de la santé du réseau franchit un seuil particulier.
Cela peut vous donner un avertissement préalable de problèmes de réseau, permettant souvent de répondre au problème avant que les utilisateurs ont une chance de se plaindre.

Zabbix

Zabbix (http://www.zabbix.org/) est un outil libre de surveillance en temps réel qui est quelque chose hybride entre cactus et Nagios.
Il utilise une base de données SQL pour le stockage de données, a son propre ensemble de rendu graphique et exécute toutes les fonctions que vous attendez d'une surveillace moderne en temps réel (comme l'interrogation SNMP et une notification instantanée de conditions d'erreur).
Zabbix est publié sous la licence GNU General Public License .

Autres outils utiles

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

ngrep

Ngrep fournit la plupart des functions correspondant au modèle de GNU grep mais les applique au trafic réseau. Il reconnaît actuellement IPv4 et IPv6, TCP, UDP, ICMP, IGMP, PP, SLIP, FDDI, Token Ring et bien plus encore. Comme il fait un usage intensif de correspondance d'expression régulière, c'est un outil adapté aux utilisateurs avancés ou ceux qui ont une bonne connaissance des expressions régulières. Vous n'avez pas nécessairement besoin d'être un expert regex pour être en mesure de faire usage de base de ngrep. Par exemple, pour afficher tous les paquets qui contiennent la chaîne GET (vraisemblablement des requêtes HTTP), essayez ceci:

 # ngrep - q GET

Motif correspond peut être contraint davantage à correspondre protocoles particuliers, les ports, ou d'autres critères en utilisant des filtres BPF. C'est le langage de filtrage utilisée par les outils ordinaire de reniflage de paquets, tels que tcpdump et snoop. Pour voir chaînes GET ou POST envoyées au port de destination 80, utilisez commande en ligne suivante:

 # ngrep - q 'GET | POST' port 80

En utilisant ngrep avec créativité, vous pouvez détecter quoi que ce soit de l'activité du virus de spam.
Vous pouvez télécharger ngrep à http://ngrep.sourceforge.net/

nmap / Zenmap

nmap est un outil de diagnostic réseau pour montrer l'état et la disponibilité des ports réseau sur une interface réseau.
Une utilisation courante est de scanner un hôte du réseau TCP / IP pour les ports ouverts, permettant ainsi de créer une «carte» des services de réseau que la machine fournit.

L'outil nmap fait cela en envoyant des paquets spécialement conçus pour un hôte de réseau cible et en alertant les réponses.
Par exemple, un serveur web avec un port ouvert 80 mais un serveur web ne fonctionnant pas réagira différemment à une sonde nmap que celui qui a non seulement le port ouvert mais exécutant httpd.
De même, vous obtiendrez une réponse différente à un port qui est tout simplement éteint contre celui qui est ouvert sur un hôte, mais couvert d'un pare-feu. Au fil du temps, nmap a évolué d'un simple port-scanner pour quelque chose qui peut détecter les versions du système d'exploitation, les pilotes de réseau, le type de matériel NIC utilisé par une interface, les versions des pilotes, etc. En plus de l' examen des machines individuelles, il peut aussi analyser des réseaux entiers d'hôtes .
Cela ne signifie pas que nmap est aussi potentiellement utile par les utilisateurs malveillants du réseau comme un moyen de "porter dehors" un système avant de l'attaquer.
Comme beaucoup d' outils de diagnostic, nmap peut être utilisée à bon ou mauvais et les administrateurs du réseau feraient bien d'être au courant des deux aspects.
L'outil nmap est publié sous la licence GPL et la dernière version peut être trouvé à http://www.nmap.org .

Zenmap

Zenmap est une interface graphique multi-plateforme pour nmap qui fonctionne sous Linux, Windows, Mac OS X, BSD, etc. et peut être téléchargé à partir du site www.map.org ainsi .

netcat

Quelque peu entre nmap et tcpdump, netcat est un autre outil de diagnostic pour piquer ou pousser aux les ports et connexions sur un réseau. Il tire son nom de l'utilitaire UNIX cat (1), qui extrait simplement le fichier que vous lui demandez. De même, netcat lit et écrit des données sur n'importe quel TCP ou UDP.
L'utilitaire netcat n'est pas un analyseur de paquets mais fonctionne sur les données (données utiles) contenues dans les paquets.
Par exemple, voici comment faire fonctionner un très simple 1-line, 1-time de serveur Web avec netcat:

{echo -ne " HTTP/1.0 200 OK \ r \ n \ r \ n"; cat some.file ; } | nc -l 8080

Le *some.file* de fichier sera envoyé au premier hôte qui se connecte au port 8080 sur le système exécutant netcat.
L'option -l indique au netcat d'«écouter» le port 8080 et d'attendre jusqu'à ce qu'il soit connecter. Une fois que c'est le cas, il arrête de bloquer, lit les données hors du tube et l'envoie au client connecté sur le port 8080. D'autres bons exemples de l'utilisation de netcat peuvent être trouvés sur le lien Wikipedia pour netcat:
https://secure.wikimedia.org/wikipedia/en/wiki/Netcat # Exemples
Vous pouvez télécharger la dernière version de netcat de
http://nc110.sourceforge.net/
Il est disponible sous une licence de logiciel libre permissive.

Qu'est-ce que c'est normal ?

Si vous cherchez une réponse définitive quant à ce que vos habitudes de circulation devraient ressembler, vous allez être déçu .
Il n'y a pas de réponse absolue droit à cette question, mais compte tenu des travaux que vous pouvez déterminer ce qui est normal pour votre réseau .
Bien que chaque environnement est différent, certains des facteurs qui peuvent influer sur l'apparence de vos modèles de trafic sont les suivantes:

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

Ce n'est pas une liste définitive, mais devrait vous donner une idée de la façon dont un large éventail de facteurs peut affecter vos habitudes de bande passante.

Dans cet esprit, nous allons regarder le sujet des lignes de base .

Établissement d'une référence

Étant donné que chaque environnement est différent, vous devez déterminer vous-même ce que vos habitudes de circulation ressemblent dans des situations normales . Ceci est utile car elle vous permet d'identifier les changements au fil du temps, soit soudaine ou progressive . Ces changements peuvent à leur tour indiquer un problème ou un problème potentiel, avec votre réseau . Par exemple, supposons que votre réseau est paralysé, et vous n'êtes pas sûr de la cause . Heureusement, vous avez décidé de garder un graphique des émissions en 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 seriez pas en mesure de voir que le nombre d'émissions a augmenté, mais seulement qu'il était relativement élevé, qui ne peut indiquer un problème . Des graphiques et des chiffres de base sont également utiles lors de l'analyse des effets des modifications apportées au réseau . Il est souvent très utile d'expérimenter ces changements en essayant différentes valeurs possibles . Savoir ce que la ligne de base ressemble à vous montrer si vos changements ont amélioré les choses, ou fait les aggraver.

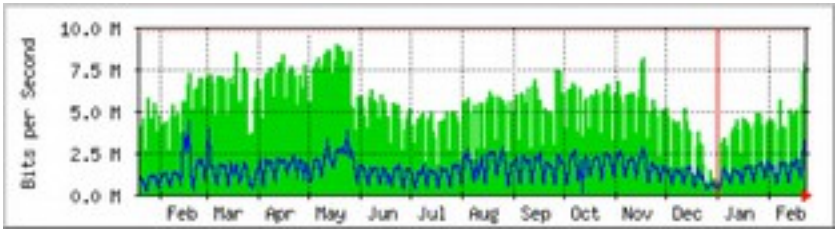


Figure NM 16: En recueillant des données sur une longue période de temps, vous pouvez prédire la croissance de votre réseau et faire des changements avant que les problèmes se développent.

Dans la figure NM 16, nous pouvons voir l'effet de la mise en œuvre des piscines de retard sur l'utilisation de l'Internet autour de la période du mois de mai . Si nous n'avons pas gardé un graphique de l'utilisation de la ligne, nous ne savons jamais ce qui était l'effet du changement sur le long terme . Lorsque vous regardez un graphique totale du trafic après l'avoir modifiée, ne présumez pas que simplement parce que le graphique ne changer radicalement que vos efforts ont été gaspillés .

Vous pouvez ensuite combiner cette base avec les autres, disent les 100.
Vous pourriez avoir enlevé utilisation frivole de votre ligne uniquement pour le faire remplacer par un véritable trafic légitime . sites accessibles ou l'utilisation moyenne par 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 garder une ligne de base .

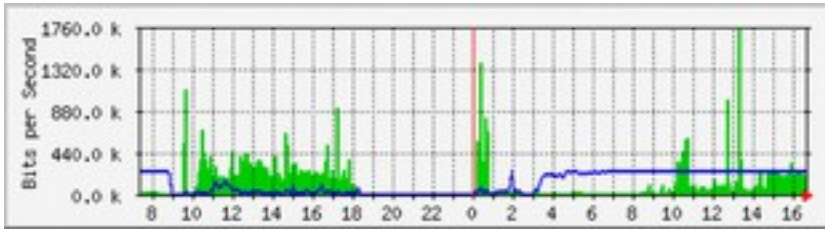


Figure NM 17: La tendance du trafic à Aidworld connecté sur une seule journée.

Figure NM 17 trafic des expositions sur un pare-feu Aidworld sur une période de 24 heures. Il est apparemment rien de mal à ce graphique, mais les utilisateurs se plaignaient de l'accès à Internet est lente . Figure NM 18 montre que l'utilisation de la bande passante de téléchargement (bleu) était plus élevé pendant les heures de travail le dernier jour que les jours précédents . Une période d'utilisation de téléversement lourde a commencé tous les matins à 3h00, et a été normalement fini par 09h00, mais le dernier jour il était encore en marche à 16h30 . L'enquête a révélé un problème avec le logiciel de sauvegarde, qui couru à 03h00 tous les jours .

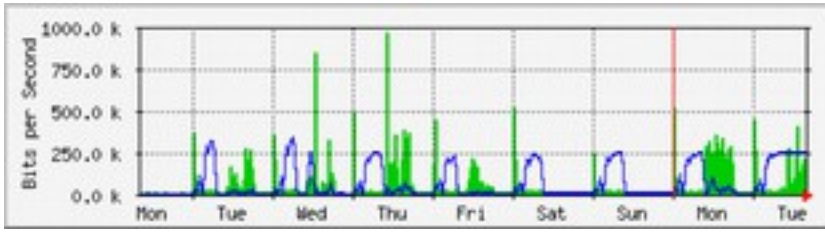


Figure NM 18: Le même réseau connecté sur une semaine entière révèle un problème avec les sauvegardes, qui a causé la congestion inattendu pour les utilisateurs du réseau .

La figure NM 19 montre les mesures de latence sur la même connexion, tel que mesuré par le programme appelé SmokePing . La position des points montre la latence moyenne, tandis que la fumée grise indique la répartition des temps de latence (gigue) . La couleur des points indique le nombre de paquets perdus . Ce graphique sur une période de quatre heures ne permet pas de déterminer s'il existe des problèmes sur le réseau .

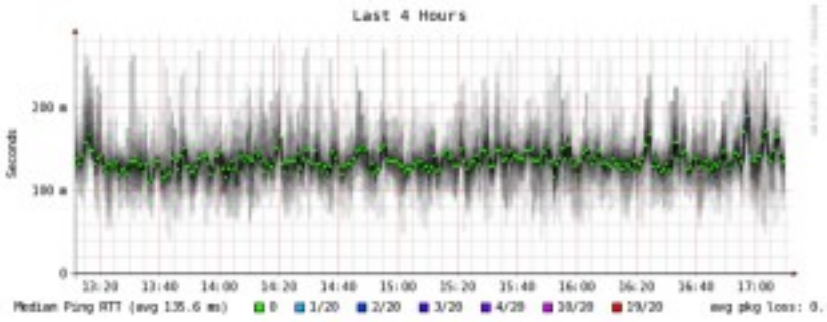


Figure NM 19: Quatre heures de gigue et la perte de paquets .

Le graphique suivant (Figure 20 NM) montre les mêmes données sur une période de 16 heures. Cela indique que les valeurs dans le graphique ci-dessus sont proches de la normale (de base), mais qu'il y avait des augmentations signi0cant la latence à plusieurs reprises au cours de la matinée, jusqu'à 30 fois la valeur de référence. Cela indique que la surveillance supplémentaire doit être effectué au cours de ces périodes pour établir la cause de la latence élevée pour éviter des problèmes tels que la sauvegarde ne pas terminer à l'avenir.

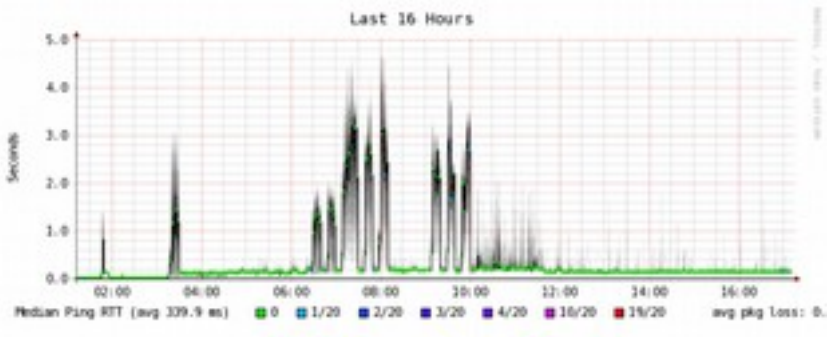


Figure NM 20 : Un écart supérieur de la gigue est révélé dans le journal de 16 heures.

La Figure NM 21 montre que mardi était significativement pire que dimanche ou lundi pour la latence, surtout pendant la période du matin. Cela pourrait indiquer que quelque chose a changé sur le réseau .

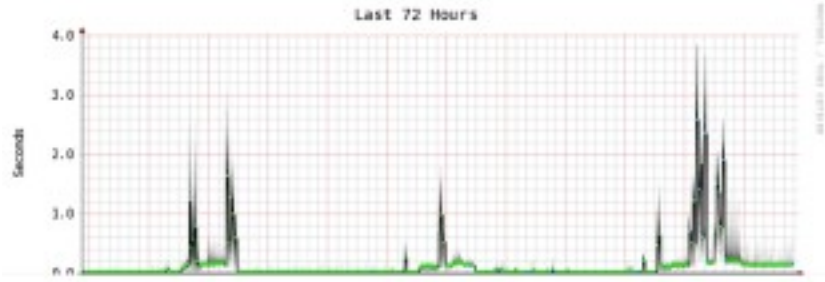


Figure NM 21: zoom arrière donnant une vue de la semaine révèle une répétition définitive de l'augmentation de la latence et perte de paquets dans les premières heures du matin.

Comment dois-je interpréter le graphique de la circulation ? Dans un graphe de flux réseau de base (tel que celui généré par l'outil de surveillance 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 s'adresse à un ordinateur de votre réseau. Trafic sortant est le trafic qui provient de votre réseau, et est adressée à un ordinateur quelque part sur Internet. Selon ce 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 grandes quantités de trafic sortant que les serveurs répondent aux demandes (comme l'envoi de courrier ou de servir des pages web), tout en surveillant les machines clientes pourraient révéler des quantités plus élevées de trafic entrant pour les machines qu'ils reçoivent des données de l' serveurs.

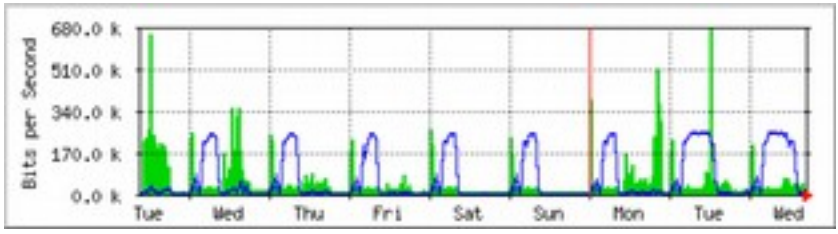


Figure NM 22: Le graphique de débit du réseau classique . La zone verte représente le trafic entrant, tandis que la ligne bleue représente le trafic sortant . Les arcs sortant répétitives montrent le trafic lors des sauvegardes nocturnes.

Modèles de circulation varieront avec ce que vous surveillez.
Un routeur affiche normalement le trafic entrant que le trafic sortant que les utilisateurs téléchargent des données à partir d'Internet . Un excès de trafic sortant qui n'est pas transmise par vos serveurs de réseau peut indiquer un client peer-to -peer, serveur non autorisé, ou même un virus sur un ou plusieurs de vos clients . Il n'y a pas de réglage des paramètres qui indiquent ce trafic sortant au trafic entrant devrait ressembler . C'est à vous d'établir une base pour comprendre ce que les modèles de trafic réseau normales ressemblent sur votre réseau .

Détection de surcharge du réseau

Figure NM 23 trafic 23 spectacles sur une connexion Internet surchargé

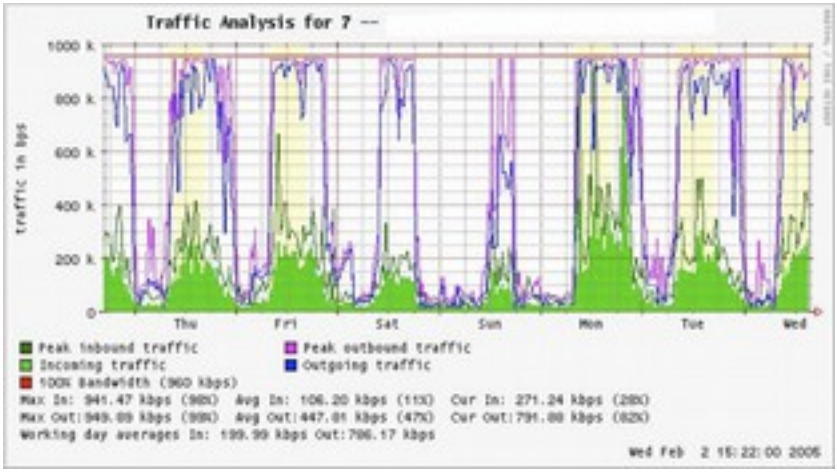


Figure NM 23: graphiques Plat garni indiquent une surcharge de la bande passante disponible.

Le signe le plus évident de surcharge est le sommet plat sur le trafic sortant au milieu de tous les jours . Sommets plats peuvent indiquer une surcharge, même si elles sont bien en deçà de la capacité théorique maximale de la liaison. Dans ce cas, il se peut que vous n'obtenez pas autant de bande passante de votre fournisseur de service que vous attendez .

Mesure 95e percentile

Le 95e percentile est un calcul mathématique largement utilisé pour évaluer l'utilisation régulière et prolongée d'un tuyau du réseau .

Sa valeur représente la plus forte consommation de trafic pour une période donnée . Calcul du 95e percentile signifie que 95 % du temps, l'utilisation est inférieur à un certain montant, et 5% du temps d'utilisation est supérieure à ce montant. Le 95e percentile est un bon guide pour montrer la bande passante qui est effectivement utilisé au moins 95 % du temps .

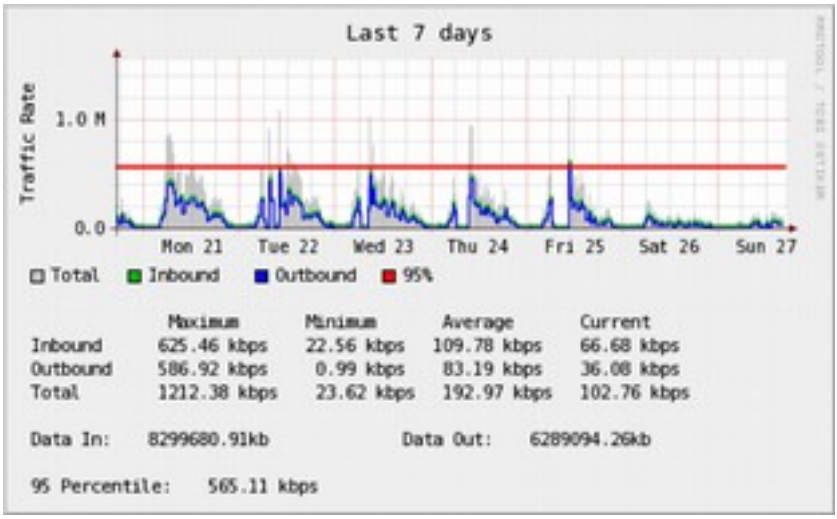


Figure NM 24: La ligne horizontale indique la quantité de 95e percentile.

MRTG et Cacti calculera le 95e percentile pour vous. Ceci est un exemple graphique d'une connexion 960 kbps . Le 95e percentile s'est établi à 945 kbps après avoir écarté le plus haut de 5% du trafic .

Surveillance RAM et CPU

Par définition, les serveurs fournissent des services essentiels qui devraient toujours être disponibles . Serveurs recevoir et de répondre aux demandes de la machine du client, offrant un accès à des services qui constituent le point d'avoir un réseau en premier lieu

Par conséquent, les serveurs doivent avoir des capacités matérielles suffisantes pour s'adapter à la charge de travail . Cela signifie qu'ils doivent avoir suffisamment de mémoire RAM, le stockage et la puissance de traitement pour accueillir le nombre de demandes des clients. Sinon, le serveur prendra plus de temps à répondre, ou dans le pire des cas, peut être incapable de répondre à tout .

Etant donné que les ressources matérielles sont limitées, il est important de garder une trace de la façon dont les ressources du système sont utilisés. Si un serveur de base (comme un serveur proxy ou un serveur e-mail) est submergé par les demandes, les temps d'accès deviennent lents .
Cela est souvent perçu par les utilisateurs comme un problème de réseau . Il existe plusieurs programmes qui peuvent être utilisés pour surveiller les ressources sur un serveur .
La méthode la plus simple sur une machine Windows est d'accéder au Gestionnaire des tâches en utilisant les touches Ctrl Alt + Suppr, puis cliquez sur l'onglet Performances . Sur une machine Linux ou BSD, vous pouvez taper dessus dans une fenêtre de terminal . Pour conserver les journaux historiques de cette performance, MRTG ou RRDtool peuvent également être utilisés .

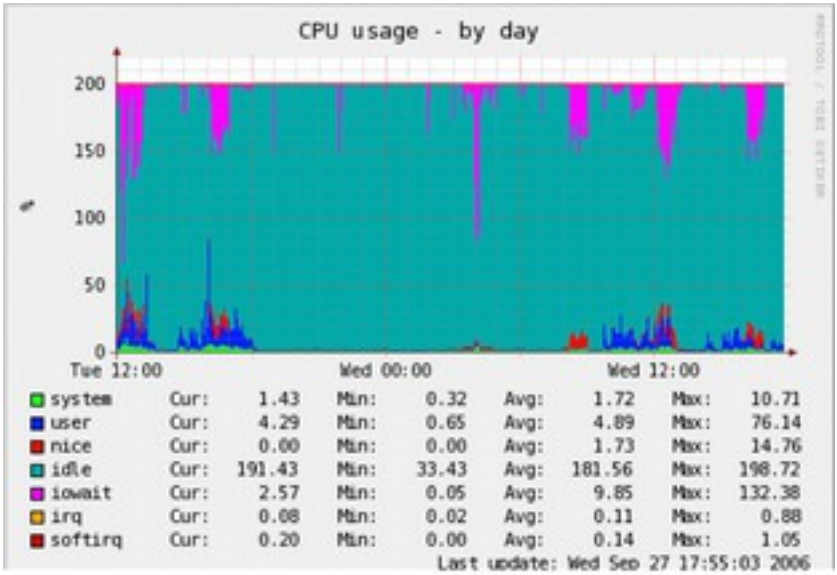


Figure NM 25: RRDtool peut afficher des données arbitraires, telles que l'usage mémoire et CPU, exprimées en moyenne au cours du temps.

Les serveurs de messagerie requièrent un espace adéquat, comme certaines personnes peuvent préférer laisser leurs e-mails sur le serveur pendant de longues périodes de temps .

Les messages peuvent s'accumuler et de remplir le disque dur, en particulier si les quotas ne sont pas en cours d'utilisation .
Si le disque ou la partition utilisée pour le stockage de courrier se remplit, le serveur de messagerie ne peut pas recevoir du courrier . Si ce disque est également utilisé par le système, toutes sortes de problèmes de système peuvent se produire comme le système d'exploitation à court d'espace de swap et stockage temporaire. Les serveurs de fichiers doivent être surveillés, même si elles ont de grands disques . Les utilisateurs trouveront un moyen de remplir un disque de taille plus rapidement que vous ne le pensez. L'utilisation du disque peut être assurée par l'utilisation de quotas, ou par la simple surveillance utilisation et dire aux gens quand ils utilisent trop .
Nagios peut vous informer de l'utilisation du disque, utilisation CPU, ou un autre ressource système qui traversent un seuil critique . Si une machine ne répond plus ou lent, et les mesures montrent que d'une ressource système est largement utilisé, ce peut être une indication qu'une mise à jour est nécessaire. Si l'utilisation du processeur dépasse constamment 60 % du total, il peut être temps de mettre à niveau le processeur . Les vitesses lentes peuvent aussi être le résultat de l'insuffisance RAM. Soyez sûr de vérifier l' utilisation globale de la CPU, la RAM et d'espace disque avant de décider de mettre à jour un composant particulier .
Une façon simple de vérifier si une machine n'a pas suffisamment de RAM est de regarder le voyant du disque dur. Lorsque le voyant est allumé en permanence, cela signifie généralement que la machine est constamment en train d'échanger des grandes quantités de données vers et depuis le disque . Ceci est connu sous le nom d'emballage, et est extrêmement mauvais pour la performance. Généralement il peut être fixé par l'enquête, procédé qui utilise le plus de RAM, et de tuer ou de reconfiguration de ce processus .
A défaut, le système a besoin de plus de RAM . Vous devez toujours déterminer s'il est plus rentable de mettre à niveau un composant individuel ou acheter une nouvelle machine.
Certains ordinateurs sont difficiles ou impossibles à mettre à jour, et il en coûte souvent plus à remplacer les composants individuels que de remplacer l'ensemble du système .
Depuis la disponibilité des pièces et des systèmes varie considérablement à travers le monde, assurez-vous de peser le coût des pièces par rapport à l'ensemble des systèmes, y compris l'expédition et taxes, pour déterminer le coût de mise à niveau.

Résumé

En résumé dans ce chapitre, nous avons essayé de vous donner un aperçu de la façon de contrôler les ressources de votre réseau et le cout de vos ressources de calcul de manière rentable et efficace. Nous avons introduit un grand nombre de nos outils préférés pour vous aider. Beaucoup d'entre eux sont essayés et testés par de nombreux opérateurs de réseaux. Avec espoir, vous avez compris l'importance du suivi pour vous permettre à la fois de justifier les mises à jour si nécessaire pour ceux qui financent ces mises à jour, ainsi que de minimiser l'impact des problèmes à mesure qu'ils surviennent. Le résultat final est de garder votre réseau et des ressources informatiques en bonne santé et garder tous vos utilisateurs heureux avec le service que vous leur fournissez.

17. VIABILITÉ ÉCONOMIQUE

Introduction

Assurer la viabilité à long terme est peut-être l'objectif le plus difficile lors de la conception et l'exploitation des réseaux sans fil. Le coût prohibitif de la connectivité Internet dans de nombreux pays, en particulier ceux qui sont fortement réglementés par le gouvernement, impose une charge d'exploitation importante qui rend ces réseaux sensibles aux fluctuations économiques et nécessite l'innovation pour garantir la viabilité. Des progrès substantiels dans l'utilisation des réseaux sans fil pour les communications rurales ont été accompli au cours de dernières années, en grande partie grâce à des percées technologiques. Les liens à longue distance ont été construits, des dessins à large bande passante sont possibles et moyens sécurisés d'accéder à des réseaux sont disponibles. En revanche, il ya eu moins de succès avec le développement de modèles commerciaux viables pour les réseaux sans fil, en particulier pour les régions éloignées. Basé sur les expériences et les observations des réseaux existants ainsi que la connaissance de meilleures pratiques du développement de l'entrepreneuriat, ce chapitre mettra l'accent sur des méthodes documentées de construction de réseaux sans fil viables.
Dans la dernière décennie, il ya eu une croissance phénoménale de l'accès à Internet à travers le monde.
La plupart des villes disposent maintenant de réseaux sans fil ou DSL et des connexions en fibre optique à l'Internet, ce qui est une amélioration substantielle .
Néanmoins, en dehors de zones urbaines, l'accès à Internet reste un défi redoutable. Il ya peu d'infrastructure câblée au-delà de principales villes dans de nombreux pays. Par conséquent, le sans fil reste l'un des rares choix pour fournir un accès Internet abordable. Il existe maintenant des modèles éprouvés pour l'accès rural à l'aide de sans fil. Ce livre a été écrit pour ceux qui souhaitent connecter leurs communautés. Les modèles décrits ici sont de plus petite échelle et utilise des modèles abordables. Notre objectif est de fournir des exemples de la façon dont les réseaux sans fil peuvent être conçues pour accroître l'accès viable là où les grands opérateurs de télécommunications n'ont pas encore installé leurs réseaux dans des zones qui autrement ne seraient pas économiquement réalisable par les modèles traditionnels. Deux idées fausses doivent être dissipés.

Tout d'abord, beaucoup de gens supposent qu'il existe un modèle d'affaires privilégié qui va travailler dans toutes les communautés, et la clé du succès est de trouver une solution "eureka".
En pratique, ce n'est pas le cas. Chaque communauté, ville ou village est différent. Il n'existe pas de modèle réglementaire qui répond aux besoins de tous les secteurs. Malgré le fait que certains endroits peuvent être similaires en termes économiques, les caractéristiques d'un modèle d'entreprise viable varient d' une communauté à l'autre.
Bien qu'un modèle peut fonctionner dans un village, un autre village voisin peut ne pas posséder les mêmes qualités nécessaires pour que ce modèle soit viable. Dans ce cas, d'autres modèles novateurs doivent être adaptés au contexte de cette communauté particulière.
Une autre idée fausse est que la viabilité a la même définition pour tout le monde. Bien que ce terme signifie généralement que le système est conçu pour durer indéfiniment, ce chapitre se concentre davantage sur la discussion des conditions économiques (financières et de gestion) que les autres aspects de la viabilité. Aussi, au lieu d'un horizon vague, il se concentre sur une période de temps de cinq ans - la période pendant laquelle ces technologies de sans fil et les infrastructures de TIC (Technologie de l'information et Communication) devraient être utiles. Ainsi, la viabilité à long terme sera utilisé pour encapsuler un système conçu pour durer environ cinq ans. Comme nous l'avons expliqué plus tôt dans le livre, les réseaux sans fil dans les communautés locales stimulent souvent la croissance de la connectivité et de l'utilisation et l'installation de la fibre commence à devenir une réalité . Ainsi, la création d'un modèle viable pour votre réseau sans fil peut conduire à la croissance d'autres réseaux et l'installation de plus grande bande passante des liens de fibre de longue durée. Sans fil devrait ensuite continuer à cohabiter aux côtés de fibres dans votre réseau à mesure qu'il grandit en taille et en portée. Lors de la détermination et de la mise en œuvre d'un meilleur modèle pour un réseau sans fil, plusieurs facteurs importants permettront d'assurer son succès.
Ce chapitre n'est pas destiné à être un guide pour la gestion des réseaux sans fil viables. Il s'agit plutôt d'un guide "comment-faire" cherchant à présenter une approche qui vous permettra de trouver le modèle qui correspond le mieux à votre situation.
Les outils et les informations contenues dans ce chapitre aideront les gens commençant des réseaux sans fil à poser les bonnes questions et de recueillir les données nécessaires pour concevoir les composantes les plus appropriées de 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 liés les uns aux autres et souvent vous allez revoir les étapes à plusieurs reprises en progressant.

Définir une déclaration de mission

Qu'est-ce que vous voulez accomplir en mettant en place votre réseau?
Ceci semble être une question simple.
Cependant, de nombreux réseaux sans fil sont installés sans une vision claire de ce qu'ils font et ce qu'ils espèrent accomplir à l'avenir.
La première étape consiste à documenter cette vision avec l'entrée de l'ensemble de votre équipe ou personnel.

- Quel est l'objectif du réseau sans fil?
- Qui est-ce que le réseau cherche à servir?
- Qu'est-ce que le réseau fait pour répondre aux besoins de la communauté et à créer de la valeur?
- Quels sont les principes qui guident le réseau?

Une bonne lettre de mission exprime le but de votre réseau d'une manière concise et significative tout en articulant vos valeurs et vos services. Surtout, votre mission fournit une vision des aspirations de votre réseau sans fil.
Il est important que chaque membre de l'équipe de travail de construction du réseau sans fil soit inclus dans le processus de développement de votre mission, ce qui contribue à créer davantage l'adhésion.
Il recueillera le soutien et l'engagement non seulement de votre personnel mais aussi des clients, des partenaires et des bailleurs de fonds, ce qui faira progresser vos objectifs globaux.
Dans le monde dynamique de la technologie, les besoins des clients et la meilleure façon de répondre à ces besoins changent rapidement et, par conséquent, le développement 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 est conforme aux réalités de votre environnement.
Basé sur une analyse de l'environnement externe et vos compétences internes, vous devez constamment modifier la mission tout au long du cycle de vie du réseau sans fil.

Évaluer la demande pour des offres potentielles

La prochaine étape pour dériver votre modèle d'affaires consiste à évaluer la demande de la communauté pour les produits et services du réseau.
Tout d'abord, identifier les individus, groupes et organismes de la communauté qui ont un besoin d'information et pourraient bénéficier de l'offre du réseau sans fil. Les utilisateurs potentiels pourraient consister d'une grande variété de personnes et d' organisations qui comprennent, mais ne sont pas limités aux:

- associations et coopératives d'agriculteurs
- groupes de femmes
- écoles et universités
- entreprises et entrepreneurs locaux
- cliniques et hôpitaux
- groupes religieux
- organisations non gouvernementales locales et internationales (ONG)
- Les agences gouvernementales locales et nationales
- Les stations de radio
- Les organisations de l'industrie touristique

Une fois que vous établissez une liste de tous les groupes d'utilisateurs potentiels du réseau, vous devez déterminer leurs besoins d'accès à l'information et à la communication. Souvent, les gens confondent les services aux besoins. Un agriculteur peut avoir besoin de recueillir l'information sur les prix du marché et les conditions climatiques pour améliorer son rendement agricole et les ventes. Peut-être qu'il obtient cette information à travers l'Internet, cependant l'agriculteur pourrait également recevoir ces informations par SMS sur un téléphone mobile ou par Voice over Internet Protocol (VoIP). Il est important de différencier entre les besoins et services, car il peut y avoir différentes façons de satisfaire les besoins de l'agriculteur. Votre réseau sans fil doit rechercher la meilleure façon de répondre aux besoins de l'agriculteur, créant ainsi de la valeur au moindre coût pour l'utilisateur. Lors de l'évaluation des besoins de la communauté, il est important de comprendre comment le réseau peut apporter le plus de valeur à ses utilisateurs. Par exemple, dans la petite ville de Douentza au Mali, un gestionnaire de télécentre a évalué les avantages potentiels de la création d'un réseau sans fil grâce à des discussions avec

plusieurs organisations locales. Il a interviewé une ONG locale qui a discuté de son besoin d'envoyer des rapports mensuels à son bureau du siège à Bamako. A cette époque, il n'y avait pas d'accès à Internet à Douentza. Pour envoyer une copie du rapport, l'ONG envoyait un de ses employés à Mopti une fois par mois, ce qui entraîne des coûts de transport et d'hébergement, ainsi que le coût d'opportunité d'avoir l'employé loin du bureau pendant plusieurs jours chaque mois. Lorsque le gérant du télécentre a calculé les coûts mensuels totaux engagés par l'ONG, il était en mesure de démontrer la valeur d'une connexion Internet grâce à des économies de coûts pour l'organisation. L'aide des partenaires importants peut aussi être nécessaire pour assurer la viabilité de votre réseau sans fil. Durant cette phase, vous devez vous connecter avec des partenaires potentiels et explorer des collaborations mutuellement bénéfiques. Vous pouvez évaluer la demande dans votre collectivité en communiquant avec vos clients potentiels et en demandant des questions directement ou à travers des enquêtes, des groupes de discussion, des entretiens ou de grandes réunions. Mener des recherches par un examen de la documentation statistique, les rapports de l'industrie, des recensements, des magazines, des journaux et d'autres sources de données secondaires aidera également à vous donner une meilleure image de votre environnement local. L'objectif de cette collecte de données est d'obtenir une compréhension approfondie de la demande d'information et de communication dans votre communauté afin que le réseau en cours de création répond à ces besoins. Souvent, les réseaux sans fil qui ne réussissent pas oublient cette étape importante. Ensemble de votre réseau doit être fondée sur la demande de la communauté. Si vous configurez un réseau sans fil dans lequel la communauté ne trouve pas de valeur ou ne peut pas payer ses services, il finira par échouer.

Établir des incitations appropriées

Souvent, il ya peu d'incitation économique pour les participants à base d'économie de subsistance pour accéder à Internet. En outre, le coût d'acquisition d'un ordinateur ou d'un téléphone mobile intelligent, d'apprendre à l'utiliser et d'obtenir une connexion Internet dépasse de loin les retombées économiques que cela peut offrir. Récemment i ya eu un développement d'applications qui traitent de ce manque de motivation, tels que les systèmes du marché de l'information, des normes de qualité imposées par les pays importateurs, et les échanges de matières premières.
L'accès à Internet devient un avantage évident dans les situations où la

connaissance des prix des produits au jour le jour peut faire une différence significative dans les revenus. L'instauration d'incitations économiques appropriées est primordiale pour la réussite du réseau. Le réseau doit offrir une valeur économique à ses utilisateurs d'une manière qui l'emporte sur les coûts, ou il doit être pas assez cher que ses coûts sont marginaux et abordable à ses utilisateurs. Il est crucial de concevoir un réseau avec les usages économiques viables et avec des coûts qui sont inférieurs à sa valeur économique. En outre, pour créer une structure d'incitation appropriée, vous devez impliquer la communauté dans la création du réseau depuis le début du projet, en s'assurant que cette initiative est organique et non imposée de l'extérieur.

Pour commencer, vous devriez essayer de répondre aux questions suivantes:

1.Quelle valeur économique que ce réseau peut générer pour l'économie locale et pour qui?

2. Que peut être la valeur économique perceptible générée?

3. Peut-on surmonter les presents obstacles 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 des produits de base de 2% », ou «l'accès à Internet vous permettra d'économiser X $ dans les frais de téléphone et les frais de transport par mois.» Vous devez comprendre comment votre réseau peut améliorer l'efficacité, réduire les coûts ou augmenter les revenus pour ces clients. Par exemple, si c'est la fourniture d'informations de marché pour l'industrie locale de maïs, le réseau doit être située près de l'endroit où les agriculteurs apportent leur récolte à vendre à des marchands .

Votre réseau aurait alors probablement besoin d'attacher - sur le marché les systèmes d' information, en fournissant des feuilles quotidiennes de prix (1 $ chacun), ou des terminaux pour les vendeurs et les commerçants (2 $ l'heure) . Votre réseau peut aussi fournir les moyens pour les agriculteurs de lire sur les nouvelles techniques et d'acheter de nouveaux produits. Vous pouvez également fournir des connexions sans fil aux marchands et leur donner en location les terminaux client léger pour l'accès à Internet.

Si le marché était petit, vous pourriez être en mesure de réduire les coûts en limitant l'accès aux images et d'autres services à grande demande de bande passante. Encore une fois, sachant la valeur que votre réseau va créer pour ces commerçants permettra de mesurer combien ils vont être en mesure de pouvoir acheter vos services.

Recherche de l'environnement réglementaire pour le sans fil

L'environnement réglementaire pour les réseaux sans fil affect aussi le type de modèle d'affaires qui peuvent être mis en œuvre. Premièrement, menez des recherches en vue de savoir si une organisation a le droit d'utiliser les fréquences 2,4 GHz sans licence. Dans la plupart des situations, 2.4 GHz est libre à utiliser dans le monde entier, mais certains pays limitent ceux qui peuvent exploiter un réseau ou nécessitent des licences coûteuses pour le faire. Ainsi, bien que les réseaux sans fil pourraient être légal dans un pays, l'opérateur d'un réseau doit avoir une licence d'utilisation de fréquences 2.4 GHz, ce qui rend cet usage prohibitif pour quelqu'un d'autre que les fournisseurs de services Internet établies qui ont suffisamment de liquidités pour payer les frais de la licence. Cette restriction rend la situation difficile pour les petites communautés à partager un réseau sans fil avec d'autres partis ou organisations potentiellement intéressés. D'autres pays sont plus permissifs sans ces restrictions sur les réseaux sans fil, de sorte que la possibilité de partager la connexion Internet dans les petites collectivités est une solution viable. La leçon est de mener des recherches au début en s'assurant que votre réseau sera conforme aux lois du pays et de la communauté locale. Certains gestionnaires de projet ont été contraints de fermer leurs réseaux sans fil, simplement parce qu'ils étaient inconsciemment en train d'enfreindre la loi. Vous devriez également vérifier la légalité des services de système vocal sur Internet (VoIP). Dans certains pays, il existe des règles compliquées sur VoIP. Les règles pour les services VoIP et passerelles VoIP varient beaucoup, alors s'il vous plaît vérifier dans votre propre pays ce qui est légalement autorisé . Vous pouvez commencer par vérifier wikipedia -http://en.wikipedia.org/wiki/Voice_over_IP.

Analyser la concurrence

La prochaine étape dans l'évaluation de votre communauté cocerne une analyse de la concurrence du réseau sans fil. Les concurrents sont notamment les organisations qui fournissent des produits et services similaires (par exemple, un autre fournisseur de services Internet sans fil ou WISP), des organisations considérées comme des substituts ou des alternatives aux produits et services que votre réseau offre (par exemple, un cybercafé), et des organisations considérées comme les nouveaux venus sur le marché du sans fil. Une fois que vous avez identifié vos concurrents, vous devriez mener les recherches approfondies. Vous pouvez obtenir des informations sur vos concurrents grâce à l'Internet, les appels téléphoniques, leurs publicités et

de matériel de marketing, enquêtes auprès de leurs clients et des visites de leur site. Créez un fichier pour chaque concurrent. L'information concurrentielle que vous recueillez peut inclure une liste de services (y compris les prix et les caractéristiques de la qualité), leurs clients cibles, les techniques de service client, la réputation, le marketing, etc. Soyez sûr 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, il vous aide à déterminer le niveau de saturation du marché. Sachant ce qui existe déjà vous permettra de déterminer comment votre réseau peut apporter une valeur à la communauté. En outre, l'analyse de la concurrence peut susciter des idées novatrices pour vos offres de services. Y a-t-il quelque chose que vous pouvez faire mieux que les concurrents pour permettre à ce que vos services s'adaptent plus efficacement aux besoins de la communauté?
Enfin, par l'analyse de vos concurrents du point de vue des clients et par la connaissance de leurs forces et leurs faiblesses, vous pouvez déterminer vos avantages concurrentiels dans la communauté. Les avantages concurrentiels sont ceux qui ne peuvent pas être facilement reproduit par la concurrence. Par exemple, un réseau sans fil qui peut uniquement offrir une connexion Internet plus rapide qu'un concurrent est un avantage concurrentiel.

Déterminer les coûts initiaux et récurrents et les prix

Lorsque vous envisagez de mettre en place et faire fonctionner votre réseau sans fil, vous devez déterminer les ressources nécessaires pour démarrer votre projet et les coûts d'exploitation récurrents. Les coûts de démarrage comprennent tout ce que vous devez acheter pour démarrer votre réseau sans fil. Ces frais peuvent aller de l'investissement initial que vous faites dans le matériel, l'accès aux tours et ainsi de suite, en plus, équipements pour les points d'accès, concentrateurs, commutateurs, câbles, équipements d'énergie solaire, UPS, etc aux coûts pour enregistrer votre organisation en tant qu'entité juridique. Les coûts récurrents sont ce que vous devez payer pour continuer à faire fonctionner votre réseau sans fil, y compris le coût de l'accès à Internet, des téléphones, des prêts, de l'électricité, les salaires, les frais de location de bureau, l'entretien du matériel et les réparations, et les investissements réguliers pour remplacer l'équipement défectueux ou obsolètes. Chaque pièce d'équipement finira par tomber en panne ou devenir obsolète à un moment donné, et vous devriez mettre de l'argent supplémentaire à cette fin.

Une méthode utile et très fréquent pour résourdre ce problème est de prendre le prix de l'appareil et de le diviser par la période de temps que vous estimez que cela durera. 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 Th1, 000 USD, et vous serez en mesure d'utiliser l'ordinateur pendant cinq ans, votre amortissement annuel sera TH200 USD. Autrement dit, vous perdrez Th16.67 USD chaque mois de sorte que vous pouvez éventuellement remplacer cet ordinateur. Pour rendre votre projet durable, il est d'une importance fondamentale que vous économisez de l'argent pour compenser la dépréciation de l'équipement de chaque mois. Gardez ces économies jusqu'à ce que vous devez finalement les liquider pour le remplacement de l'équipement. Certains pays ont des lois fiscales qui déterminent la période d'amortissement de différents types d'appareils. Dans tous les cas, vous devriez essayer d'être très réaliste sur le cycle de vie de tout le matériel et le plan mis en œuvre pour leur amortissement attentivement. Il est important de mener des recherches sur tous vos frais de démarrage à l'avance, et de faire des estimations réalistes de vos dépenses récurrentes. Il est toujours préférable de sur-budgétiser que de sous–budgétiser pour les dépenses. Avec chaque projet sans fil, il ya toujours des frais imprévus, surtout pendant la première année d'exploitation comme vous apprendrez à mieux gérer votre réseau. Après, c'est une liste non exhaustive des catégories de coûts que vous devriez inclure, à la fois en phase de démarrage et pour vos coûts récurrents, juste pour vous donner une idée de la façon de commencer sur le calcul de vos frais : -

Catégories de coûts

Les coûts du travail -

- Examens (analyses) et conseils
- Les coûts de développement pour la programmation, tests, intégration, etc
- Les coûts d'installation
- les coûts de recrutement
- Les coûts de formation (introduction et suivi)
- les coûts de manutention / salaires pour les employés ou pigistes, y compris vous-même
- les dépenses de personnel d'entretien de l'équipement
- les frais de personnel de support logiciel
- Le personnel de sécurité

Coûts non salariaux -

• Coûts d'acquisition et de production (pour le matériel comme les ordinateurs, VSAT, les appareils radio de liaison et de logiciels)
• L'équipement auxiliaire (par exemple, des commutateurs, câbles et câblage, générateur, UPS, etc)
• la protection et la sécurité des données
• inventaire de démarrage (chaises, tables, luminaires, rideaux, carrelage et moquette)
• Les frais de locaux (nouveau bâtiment, modification, climatisation, câblage électrique et boîtes, grilles de sécurité)
• les frais juridiques, tels que l'enregistrement des entreprises
• les coûts de licence initiaux (VSAT)
• les coûts initiaux de commercialisation (dépliants, autocollants, affiches, fête d'ouverture)
• Les coûts d'exploitation du matériel et des systèmes d'exploitation (accès Internet, téléphone, etc)
• taux de location ou crédit-bail (pour l'espace de la tour par exemple)
• L'amortissement du matériel et de l'équipement
• Les droits de licence
• consommables et fournitures de bureau (par exemple, des supports de données, papier, lie, clips)
• Les coûts de fonctionnement pour maintenir la protection des données et de la sécurité
• Les primes d'assurance
• Les coûts de l'énergie et pour assurer l'alimentation
• Le paiement du prêt, les coûts en capital pour rembourser le coût d'installation
• Les coûts de la publicité
• Des frais locaux
• les services juridiques et comptables

Pour améliorer vos chances de durabilité, il est généralement préférable de maintenir la structure la moins coûteuse pour votre réseau.
En d'autres termes, garder vos dépenses aussi bas que possible.
Prenez le temps de bien étudier tous vos fournisseurs, notamment les fournisseurs de services Internet, et à magasiner pour les meilleures offres sur un service de qualité.

Une fois de plus, être certain que ce que vous achetez auprès de fournisseurs correspond à la demande de la communauté. Avant d'installer un VSAT cher, s'assurer qu'il ya un nombre suffisant d'individus et d'organisations dans votre communauté désireux et capables de payer pour l'utiliser. Selon la demande d'accès de l'information et de la capacité de payer, une méthode alternative de la connectivité peut être plus approprié. Ne pas avoir peur de sortir des sentiers battus et faire preuve de créativité lorsqu'il s'agit de déterminer la meilleure solution. En limitant les coûts ne doit pas se faire au détriment de la qualité. Parce que l'équipement de mauvaise qualité est plus susceptible de dysfonctionnement, vous pourriez dépenser plus sur l'entretien à long terme.

Le montant d'argent que vous allez dépenser pour maintenir votre infrastructure TIC est difficile à deviner. Plus grand et plus complexe votre infrastructure devient, plus des ressources financières et humaines, vous devez allouer pour son entretien. Plusieurs fois, cette relation n'est pas linéaire mais exponentielle. Si vous avez un problème de qualité avec votre équipement une fois qu'il est déployé, il peut vous coûter une énorme quantité d'argent pour le réparer. Parallèlement, vos ventes vont diminuer parce que l'équipement n'est pas en marche.

Un exemple intéressant est celui d'un important fournisseur d'accès Internet sans fil (WISP) qui avait plus de 3000 points d'accès en fonctionnement pendant un certain temps. Toutefois, le WISP n'avait jamais réussi à atteindre l'équilibre, car il a dû dépenser beaucoup d'argent pour maintenir tous les points d'accès. En outre, la société a sous-estimé le cycle de vie court de ces dispositifs. Matériel TIC tend à devenir moins cher et mieux comme le temps passe. Dès que l'entreprise avait investi beaucoup de temps et d'argent pour installer la version de la première génération très chère de points d'accès 802.11b, la nouvelle norme "g" a été créée. De nouveaux concurrents ont conçus de meilleurs points d'accès et moins couteux et ont offert l'accès Internet plus rapide et moins cher. Enfin la première WISP a été contraint de fermer l'entreprise, même si elle a d'abord été le leader du marché. Gardez à l'esprit les progrès rapides et des changements dans la technologie et de réfléchir sur comment et quand viendra le temps pour vous de réinvestir dans de nouveaux appareils et moins cher (ou mieux) pour garder votre infrastructure compétitive et à jour. Comme mentionné précédemment, il est très important que vous économiser suffisamment pour être en mesure de le faire, le cas échéant. Une fois que vous avez identifié et cartographié vos coûts, vous devez également déterminer quoi et comment payer pour vos services.

Il s'agit d'un processus complexe et de longue haleine pour faire correctement.
Ces conseils aideront clés pour prendre des décisions de tarification :

- Calculer les prix que vous facturez de manière à couvrir tous les coûts pour fournir le service, y compris toutes les dépenses récurrentes.
- Examiner les prix de vos concurrents.
- Évaluer ce que vos clients sont prêts et capables de payer pour vos services, et assurez-vous que vos prix correspondent à ceux-ci.

Il est absolument essentiel de faire un plan financier avant de commencer à trouver si votre projet peut être viable .

Sécuriser le financement

Une fois que vous avez déterminé vos coûts initiaux et récurrents et créé votre plan financier, vous savez quel financement vous aurez besoin pour lancer un réseau sans fil avec succès.
La prochaine étape est d'étudier comment obtenir la somme appropriée d'argent pour démarrer et gérer votre réseau sans fil.
La méthode la plus traditionnelle est de recevoir un financement sur les réseaux sans fil à travers les subventions accordées par les bailleurs de fonds . Un donneur contribura généralement au financement et à d'autres types de dons à une organisation ou un consortium d' organisations pour les aider à gérer des projets ou de soutenir des causes. Parce que ce financement est fourni sous la forme de subventions ou d'autres dons, on ne s'attend pas à un remboursement de la part des organismes d'exécution des projets sans fil ou par les bénéficiaires du projet.
Ces bailleurs de fonds sont de grandes organisations internationales comme les Nations Unies (ONU) et diverses institutions spécialisées des Nations Unies comme le Programme des Nations Unies pour le développement (PNUD) et des Nations Unies pour l'éducation, la science et la culture (UNESCO). Les organismes gouvernementaux qui se spécialisent dans le développement international comme l'Agence américaine pour le développement international (USAID), le Département du Royaume-Uni pour le développement international (DFID) et l'Agence canadienne de développement international (ACDI), sont également considérés comme des donateurs.

Grandes fondations comme la Fondation Gates et la Fondation Soros et des sociétés commerciales privées sont d'autres types de bailleurs de fonds. En règle générale, recevoir un financement implique une compétition ou un processus non concurrentiel. Le processus non concurrentiel est plus rare donc nous allons nous concentrer sur le processus concurrentiel à un niveau très élevé. La plupart des donateurs ont compliqué les procédures entourant la répartition des fonds. Pendant le processus d'appel d'offres, le donateur crée une demande de proposition (DP) ou une demande d'application (RFA) sollicitant diverses organisations non gouvernementales, des entreprises privées et leurs partenaires à soumettre des propositions décrivant leurs plans pour les projets en respectant les contraintes des objectifs et des lignes directrices des bailleurs de fonds.
En réponse à ces demandes RFP ou RFA, les ONGs et d'autres organisations en concurrence à travers la soumission de leurs propositions, qui sont ensuite évaluées par les bailleurs de fonds sur la base de critères spécifiques établis. Enfin, l'organisme donateur choisit la proposition la plus appropriée et la plus cotée pour financer le projet.
Parfois, les donateurs fournissent également des fonds pour soutenir les activités d'une organisation, mais ce type de financement est plus inhabituel que le processus d'appel d'offres pour un projet spécifique. Un autre moyen est d'accéder à des fonds nécessaires pour démarrer et maintenir un réseau sans fil à travers la microfinance ou l'octroi de prêts, épargne et autres services financiers de base pour les personnes les plus pauvres du monde.
Mis au point dans les années 1970 par des organisations comme ACCION International et la Banque Grameen, le microcrédit, un type de la microfinance, permet aux entrepreneurs d' obtenir des prêts à de petites sommes d' argent pour démarrer de petites entreprises. Malgré le fait que souvent les individus n'ont pas beaucoup de qualifications traditionnelles nécessaires à l'obtention de prêts tels que le veritable crédit, garantie ou un emploi stable, les programmes de microcrédit ont eu beaucoup de succès dans de nombreux pays . Habituellement, le processus implique un individu ou un groupe remplissant et soumettant une demande de prêt dans l'espoir de recevoir un prêt, et le prêteur, l'individu ou l'organisation qui fournit le prêt, donnant l'argent à condition qu'il soit retourné avec intérêt. L'utilisation de micro-crédit pour financer les réseaux sans fil pose une contrainte. Habituellement, le microcrédit implique de très petites sommes d'argent. Malheureusement, parce qu'une grande quantité de capital est nécessaire pour acheter l'équipement initial pour réseau sans fil mis en place, parfois un microcrédit n'est pas suffisant.

Cependant, il ya eu de nombreuses applications réussies de microcrédit qui ont apporté la technologie aux communautés.
Un exemple inclut l'histoire des opérateurs de téléphonie de village.
Ces entrepreneurs utilisent leurs prêts de microcrédit pour acheter des téléphones mobiles et des crédits téléphoniques. Ils font louer ensuite l'utilisation de leurs téléphones mobiles aux membres de la communauté sur une base par appel et gagnent assez d'argent pour rembourser leur dette et faire un profit pour eux-mêmes et leurs familles.
Un autre mécanisme pour obtenir du financement pour lancer un réseau sans fil est le financement providentiel. Les investisseurs providentiels sont normalement des individus riches qui fournissent des capitaux pour le démarrage d'entreprises en échange d'un taux élevé de retour sur leur investissement. Parce que les entreprises dans lesquelles ils investissent sont des débutantes et, par conséquent, souvent à haut risque, les investisseurs providentiels ont tendance à attendre des choses différentes en plus de leur retour. Beaucoup s'attendent à une position du Comité et peut-être un rôle dans l'organisation. Certains supporteurs veulent avoir une participation dans la société, tandis que d'autres préfèrent des actions de la société qui peut être facilement rachetables à leur valeur nominale, ainsi fournissant une sortie claire pour l'investisseur. Pour protéger leurs investissements, les supporteurs demandent souvent les entreprises de ne pas prendre certaines décisions importantes sans leur approbation.
En raison du risque élevé impliqué dans les marchés en développement, il est souvent difficile de trouver des investisseurs providentiels pour aider à créer un réseau sans fil, mais pas impossible. La meilleure façon est de trouver des investisseurs potentiels à travers votre réseau social et par la recherche en ligne.

Évaluer les forces et les faiblesses de la situation interne

Un réseau est seulement aussi bon que les gens qui travaillent et l'exploitent. L'équipe que vous mettez en place peut faire la différence entre le succès et l'échec. C'est pourquoi il est important de réfléchir sur les qualifications et les compétences de votre équipe, y compris ceux du personnel et des bénévoles, en comparaison avec les compétences nécessaires pour un projet sans fil. Tout d'abord, faire une liste de toutes les compétences nécessaires pour lancer un projet sans succès. Domaines des capacités devraient inclure la technologie, les ressources humaines, la comptabilité, marketing, vente, négociation, juridique et des opérations, parmi tant d'autres.

Ensuite, identifier les ressources locales pour répondre à ces compétences.
Joignez l'ensemble de capacité de votre équipe aux compétences nécessaires, et identifier les principales lacunes. Un outil souvent utilisé pour aider à cette auto-évaluation est une analyse des forces, faiblesses, opportunités et menaces, appelé SWOT .
Pour réaliser cette analyse, spécifiez vos forces et faiblesses internes, et précisez les possibilités 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 manque.
Assurez-vous de faire la distinction entre l'endroit où votre organisation se trouve au début de cette entreprise et là où il pourrait être dans l'avenir. Vos forces et vos faiblesses vous permettent d'évaluer vos capacités à l'interne et à mieux comprendre ce que votre organisation peut faire, ainsi que ses limites. En comprenant vos forces et faiblesses et en les comparant à ceux de vos concurrents, vous pouvez déterminer vos avantages concurrentiels sur le marché. Vous pouvez également noter les domaines dans lesquels vous pouvez améliorer. Opportunités et menaces sont externes, qui vous permettent d'analyser les conditions du monde réel et comment ces conditions influent sur votre réseau.
Le schéma ci-dessous vous aidera à créer votre propre analyse SWOT pour votre organisation. Assurez-vous de répondre aux questions posées et la liste de vos forces, faiblesses, opportunités et menaces dans les espaces désignés.

Points forts	Points faibles
Que faites vous mieux? Sur quelle resource unique pouvez vous compter? Quelles sont les points forts que les autres trouvent en vous ?	Que pouvez vous ameliorer ? Où avez-vous moins de resources que les autres ? Q'est ce que les autres trouveront probablement comme faiblesses?
Opportunités	**Menaces**
Quelles sont les bonnes opportunités qui vous sont ouvertes ? Quelles sont les tendances dont vous pourriez tirer profit? Comment pouvez-vous transformer vos forces en opportunités?	Quelles sont les tendances qui peuvent vous nuire ? Qu'est ce que votre concurrence fait ? Quelles sont les menaces auxquelles vos faiblesses vous expose ?

Mettre le tout ensemble

Une fois que vous avez recueilli toutes les informations, vous êtes prêt à tout mettre ensemble et de décider sur le meilleur modèle pour le réseau sans fil dans votre communauté.

Basé sur les résultats de vos analyses internes et externes, vous devez raffiner votre mission et offres de services.
Tous les facteurs que vous avez étudiés dans les étapes précédentes entrent en jeu lorsqu'il s'agit de déterminer votre stratégie globale.
Il est essentiel d'utiliser un modèle qui capitalise sur les possibilités et fonctionne dans les limites de la environnement local.
Pour ce faire, vous devez souvent trouver des solutions innovantes pour atteindre la viabilité. En explorant plusieurs exemples et de discuter les composantes des modèles mis en œuvre dans ces cas, vous comprendrez mieux comment arriver à un modèle approprié.
Dans les jungles reculées de la République démocratique du Congo, il ya un hôpital rural dans un village appelé Vanga, dans la province de Bandundu. Il est si éloigné que les patients voyagent pendant des semaines pour y arriver souvent par une combinaison de Voyage à pied et en rivière.
Ce village, fondé par des missionnaires baptistes en 1904, a servi comme un hôpital pendant de nombreuses années.
Bien qu'il soit extrêmement faible, il est réputé pour être un excellent installation 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 établi un télécentre dans ce village pour aider à améliorer l'éducation dans cette communauté isolée; ce service Internet a également été utilisé largement par la classe instruite dans la communauté - le personnel de l' hôpital. Le centre a été une aubaine pour le communauté, offrant un accès à la connaissance du monde et même permettre la consultation avec des collègues éloignés en Suisse, en France et au Canada. Le centre requis près du total des subventions pour fonctionner et couvrir ses coûts et le financement devait prendre fin d'ici à 2006.
Bien que le centre a ajouté une grande valeur pour la communauté, il a encore certaines lacunes, principalement les questions techniques, économiques et politiques qui ont limité sa viabilité.
Une étude a été commandée pour examiner les options pour son avenir. Après avoir examiné la structure de coûts du centre, il a été déterminé qu'il était nécessaire de réduire ses coûts et trouver de nouvelles façons d'augmenter ses revenus.
Les dépenses les plus importantes ont été l'électricité et l'accès à Internet, par conséquent, des modèles créatifs devaient être construits pour réduire les coûts du télécentre et permettre l'accès d'une manière qui soit durable.

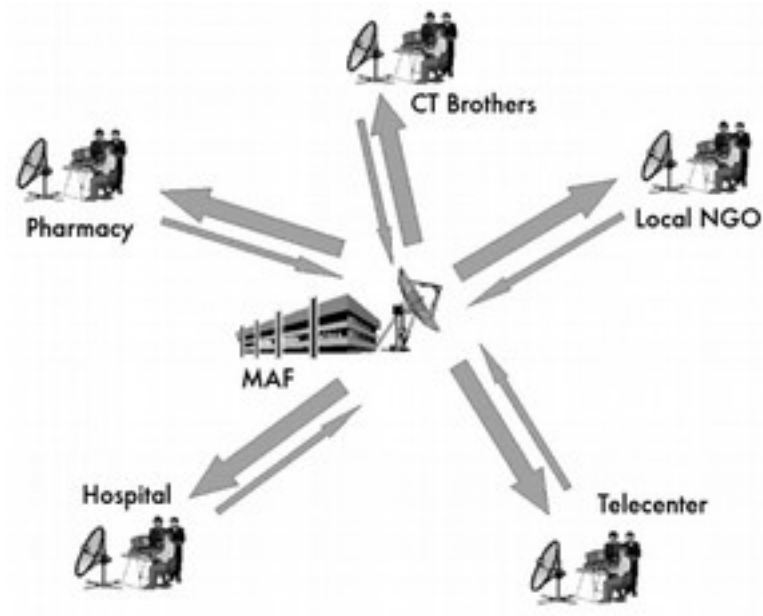


Figure ES 1: Partage Internet sur le sans fil

Dans ce cas, un VSAT traditionnelle a été utilisée pour la connectivité. Cependant, il y avait une façon unique d'adapter la capacité limitée des groupes communautaires locaux pour payer les services Internet. Diverses organisations de la communauté partagent cet accès à Internet via un réseau local sans fil; ce qui signifie qu'ils ont également partagé les coûts associés à la connexion VSAT et réseau local sans fil. Ce modèle a conduit à une plus grande viabilité pour tout le monde. A Vanga, plusieurs organisations, y compris un hôpital, une pharmacie, plusieurs groupes de missionnaires, un centre de ressources de la communauté, et certaines organisations à but non lucratif, ont besoin d'un accès à Internet et des moyens pour le payer.
Cette disposition a permis le réseau des organisations d'avoir une connexion de meilleure qualité à moindre coût. En outre, une organisation dans le village avait la capacité et la volonté de gérer plusieurs aspects des activités du réseau, y compris la collecte de la facturation et du paiement, la maintenance technique et les opérations générales de vente de l'ensemble du réseau. Par conséquent, ce modèle a bien fonctionné dans Vanga, car il avait été adapté pour répondre à la demande de la communauté et mobiliser des ressources économiques locales.

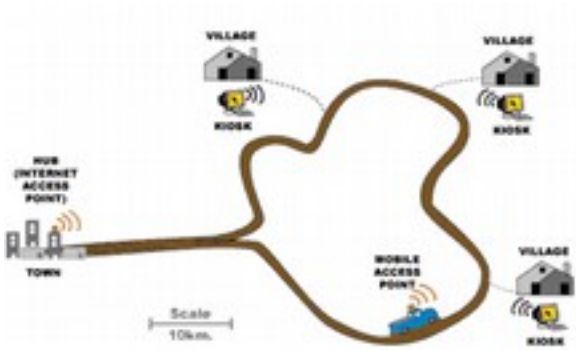


Figure ES 2 : itinérance point d'accès de DakNet

Un autre exemple d'un modèle conçu pour s'adapter au contexte local est celui de DakNet de First Mile Solutions. Ce modèle a été déployée dans les villages de l'Inde, le Cambodge, le Rwanda, et le Paraguay. En prenant en compte le pouvoir d'achat limité des villageois, ce modèle répond à leurs besoins de communication d'une manière innovante. Dans le modèle DakNet, il ya une franchise qui existe dans le pays, et les entrepreneurs locaux sont recrutés et formés pour faire fonctionner les kiosques équipés d'antennes Wifi. L'utilisation de cartes pré-payées, les villageois sont capables d'envoyer et recevoir des emails en mode asynchrone, les textes et messages vocaux, effectuer des recherches web, et de participer dans le commerce électronique. Par la suite, ces communications sont stockés dans le serveur du kiosque local. Quand un bus ou une moto avec un point d'accès mobile passe devant un kiosque, le véhicule reçoit automatiquement les données stockées du kiosque et fournit toutes les données entrantes.
Une fois le véhicule atteint une plaque tournante de la 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 les modèles de franchise pour apporter de la valeur aux personnes dans les villages reculés.
Pour un tel modèle soit viable, plusieurs conditions importantes doivent être présents. Tout d'abord, une organisation de franchise doit exister pour fournir un soutien financier et institutionnel, y compris un investissement initial, le fonds de roulement de certains coûts récurrents, des conseils sur les pratiques de démarrage, la formation en gestion, des processus normalisés, les mécanismes de rapport, et des outils de marketing.

En outre, ce modèle nécessite une personne très motivée et dynamique dans le village, avec les compétences nécessaires pour gérer une entreprise et la volonté d'accepter certaines exigences de l'organisation franchise.
Parce que ces entrepreneurs sont souvent invités à engager leurs propres ressources pour les coûts de démarrage, ils doivent avoir un accès suffisant aux ressources financières. Enfin, pour assurer que ce modèle va se maintenir, il devrait y avoir une demande suffisante pour l'information et la communication et moins de concurrents dans la communauté.

Conclusion

Aucun modèle d'affaires permettra les réseaux sans fil d'être viable dans tous les milieux; différents modèles doivent être utilisés et adaptés comme les circonstances l'exigent. Chaque communauté possède des caractéristiques uniques, et une analyse suffisante doit être effectuée au début d'un projet afin de déterminer le modèle le plus approprié. Cette analyse doit tenir compte de plusieurs facteurs importants de l'environnement local, y compris la demande de la communauté, la concurrence, les coûts, les ressources économiques, etc. Bien que la planification et l'exécution appropriée permettra de maximiser les chances de rendre votre réseau viable, il n'ya aucune garantie de succès. Cependant, en utilisant les méthodes décrites dans ce chapitre, vous aiderez à assurer que votre réseau apporte de la valeur à la communauté d'une manière qui correspond aux besoins des utilisateurs.

GLOSSAIRE

Glossaire

0–9

802.11. Alors que 802.11 est un protocole sans fil de plein droit, il est souvent utilisé pour désigner 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 b***atterie***.
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 oeuvre 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 oeuvre 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 Wattheure (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'an-

tenne 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 del'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 microonde 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'ali-

mentation 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 déter-

minée 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 parefeu 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.fssecurity.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 mêmetemps (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 pro-***

tocoles 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 (trafic shaping) et d'autres techniques avancées. Disponible à partir de *http://linuxnet.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/m2.

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 microonde 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 alterna-

tive 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 parefeu 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 danslaquelle 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 parefeux 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 allerretour 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-àmultipoints***.

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 (Pmax***)***. 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 microonde 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(DoDmax***)***. 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 ré-

seaux, 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 noeuds 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 microconnecteur 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 som-

mets. 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 luimême. 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 le trafic de tout autre noeud.

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 éli-

minant 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 100-baseT. 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'emplace-

ment 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.

APPENDICES

APPENDICE A: CONSTRUCTION D'ANTENNES

Directives pour la construction de certains types simples d'antennes

Omni colinéaire

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.

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
- 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

Figure AC 1: Plaque d'aluminium de 10 cm x 10 cm

Construction

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

Figure AC 2: Rendez le fil de fer aussi droit que possible.

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 AC 3: Frapper doucement sur le fil pour faire une courbe fermée.

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 AC 4: Plier le fil en forme de « Z ».

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.

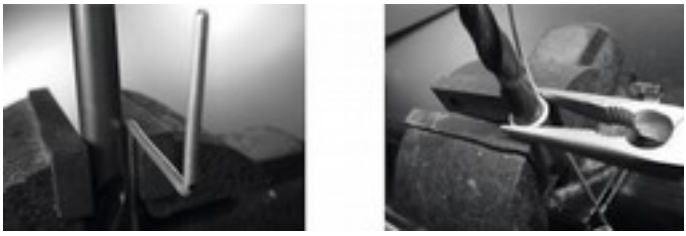


Figure AC 5: Courber le fil autour de la perceuse pour faire une boucle.

La boucle ressemblera à ceci:

Figure AC 6: La boucle complète.

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.

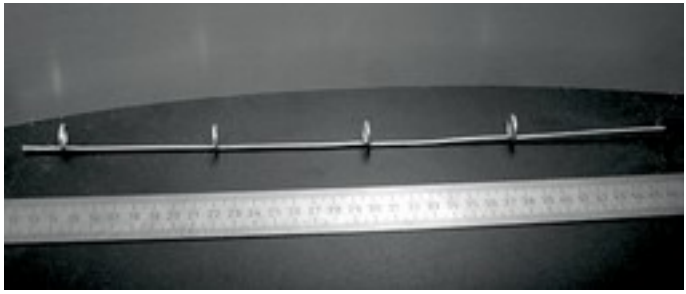


Figure AC 7: Essayer de le maintenir le plus droit que possible

Si les boucles ont été faites correctement, il devrait être possible de traverser toutes les boucles avec un tuyau tel qu'illustré ci-dessous.

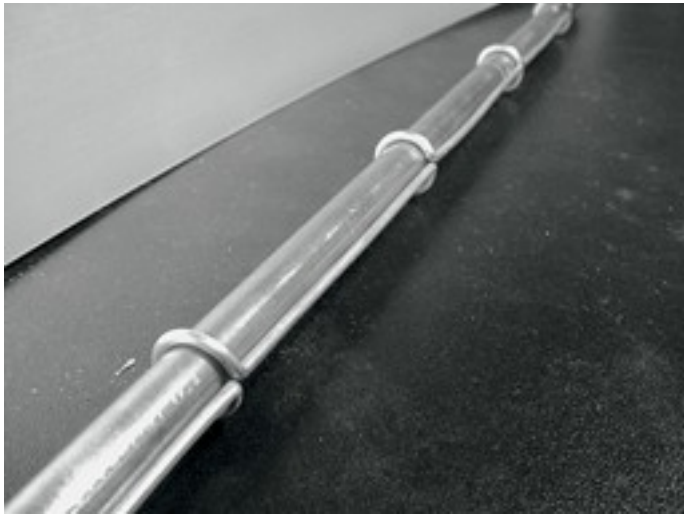


Figure AC 8: L'insertion d'un tuyau peut aider à redresser le fil.

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.

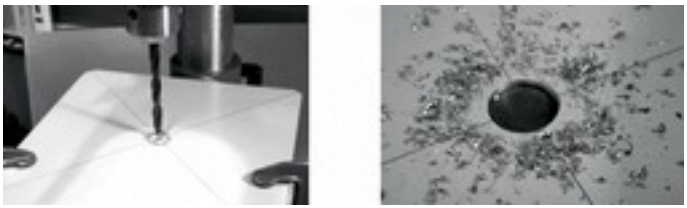


Figure AC 9: Percer un trou dans la plaque métallique.

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

Figure AC 10: Le connecteur N doit entrer parfaitement dans le trou.

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 AC 11: Ajouter un tuyau de cuivre comme entretoise aide à obtenir une impédance d'antenne de 50 Ohms.

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

Figure AC 12: Fixez étroitement le connecteur N à la plaque.

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.

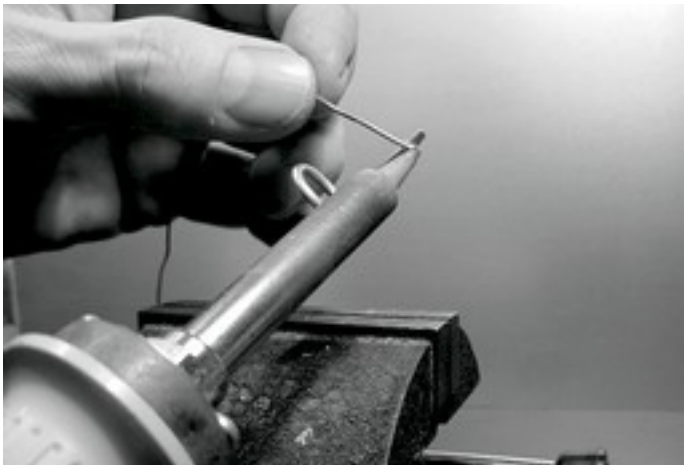


Figure AC 13: Ajouter un peu d'étain à l'extrémité du fil avant de le souder.

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.

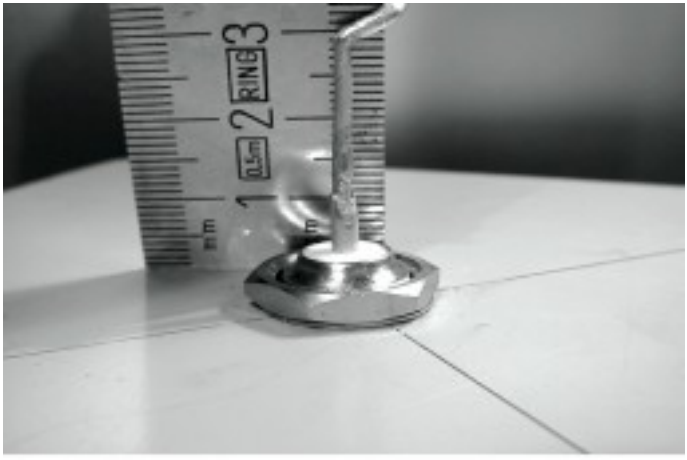


Figure AC 14: La première boucle devrait commencer à 3,0 centimètres de la surface de la plaque.

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 AC 15: Étirer les boucles. Procédez en douceur et essayer de ne pas érafler la surface du fil avec les pinces.

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

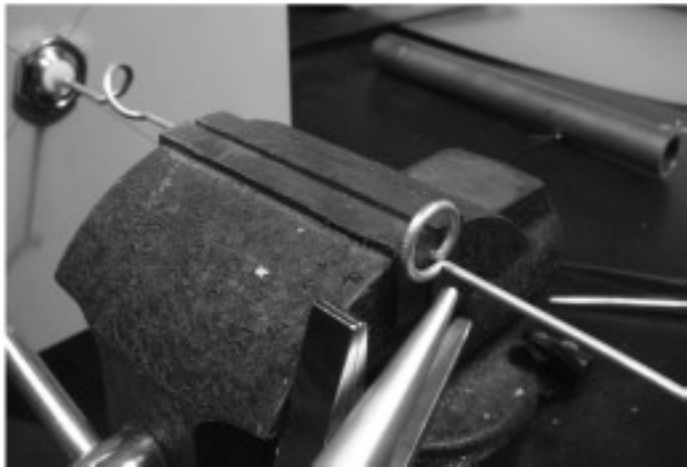


Figure AC 16: Répétez la même procédure «d'étirement» pour les boucles restantes.

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

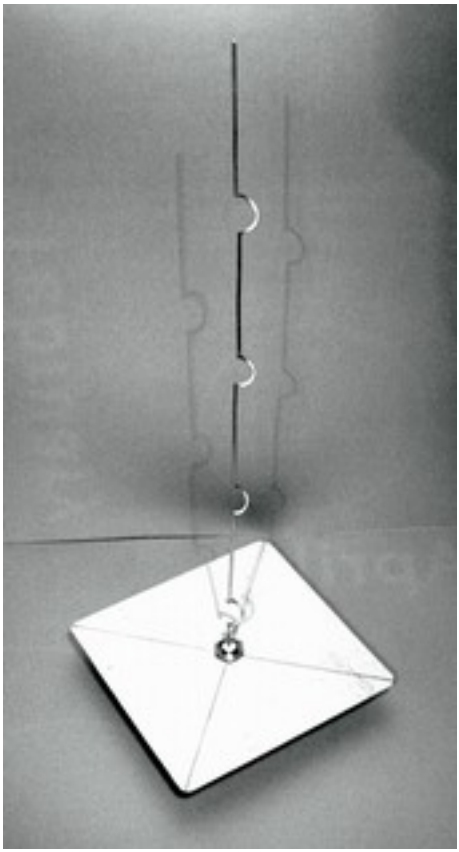


Figure AC 17: L'antenne finale devrait mesurer 42,5 cm de la plaque à l'extrémité du fil.

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.

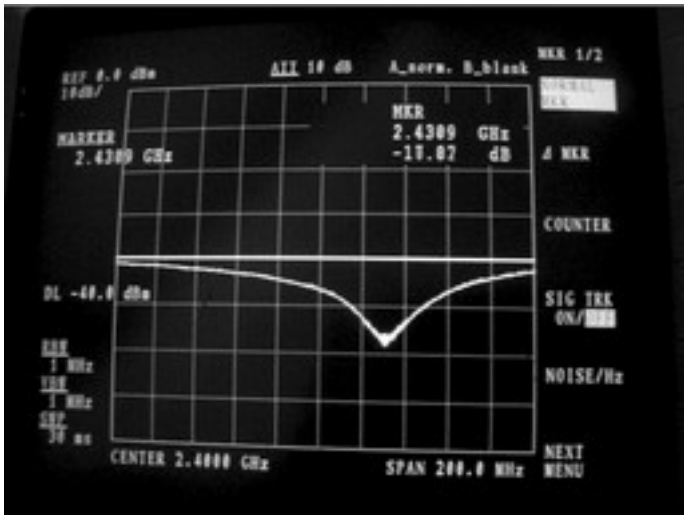


Figure AC 18: Un traçage du spectre de la puissance reflétée de l'antenne colinéaire omnidirectionnelle.

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 car certaines contraintes dimensionnelles sont applicables.
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 dia-

mètre de la boîte de conserve devrait être dans la gamme de 7,3 - 9,2 centimètres.

2. La longueur L de la boîte de conserve devrait préférablement être d'au moins 0,75 λG, où λG est la longueur d'onde du guide qui est définie par la formule suivante:

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

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.

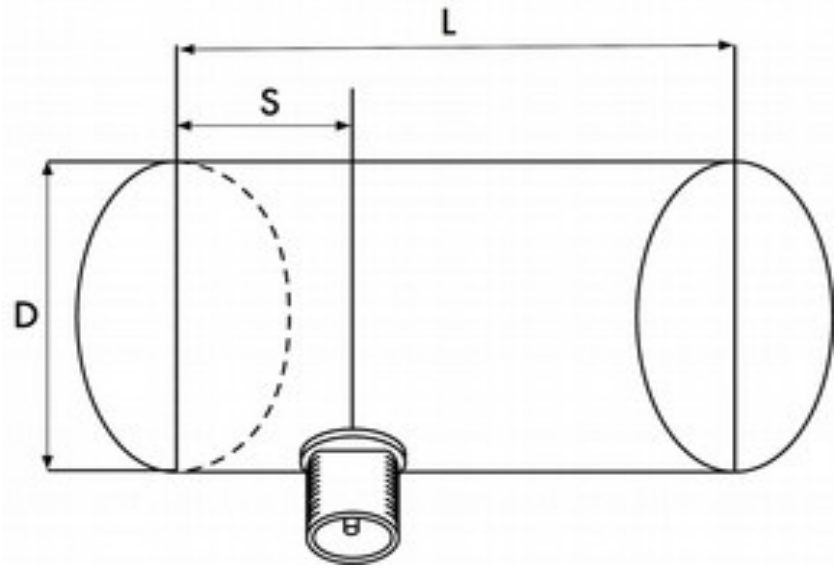


Figure AC 19: Contraintes dimensionnelles d'une Cantenna.

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

Figure AC 20 : Une cantenna finalisée.

Liste des composantes

- 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 AC 21: 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

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

Figure AC 22: Faites 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.

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 AC 23: Marquez le trou avant de percer.

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.

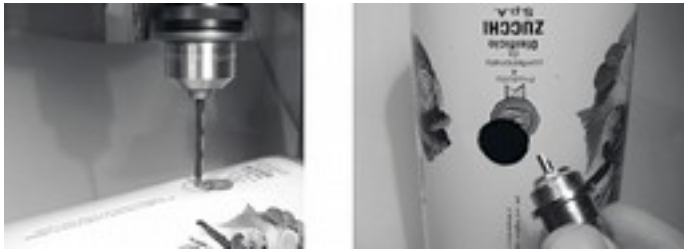


Figure AC 24: Percez soigneusement un trou pilote, puis utilisez une mèche plus grande pour terminer le travail.

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 AC 25: Ajouter de l'étain à l'extrémité du fil avant de souder.

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 AC 26: Soudez le fil à la pièce dorée du connecteur N.

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.

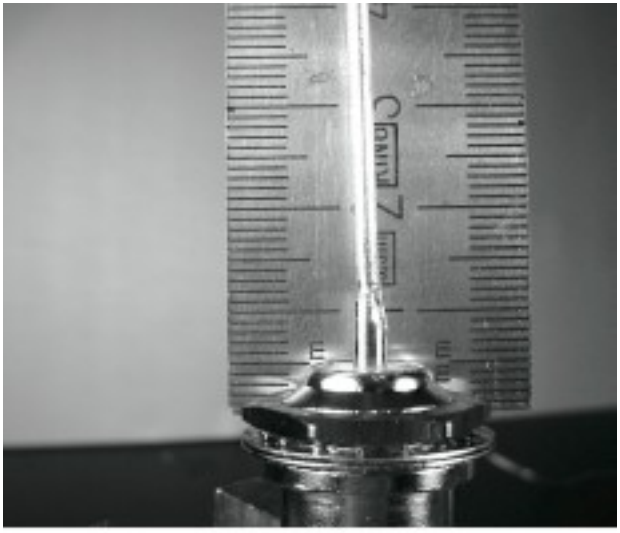


Figure AC 27: La longueur du fil est cruciale.

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 AC 28: Assemblez l'antenne.

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

Figure AC 29: 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.

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 visualiser 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 de recherche 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
http://www.nec2.org/

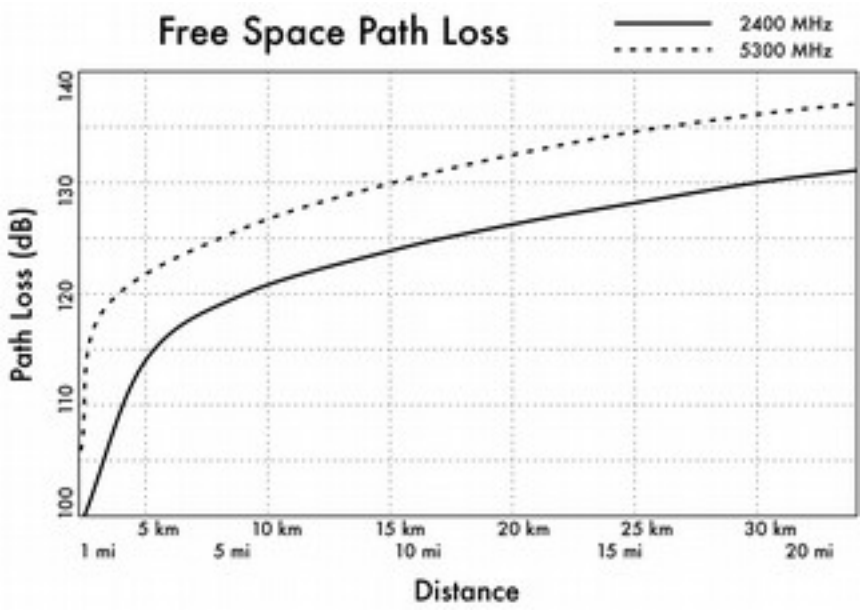
APPENDICE B: ALLOCATIONS DES CANAUX

The 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			
Canal #	Fréuence Centrale (GHz)	Canal #	Fréuence 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	
Canal	Fréuence 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	5805

APPENDICE C: PERTE DE TRAJET



APPENDIX D: TAILLES DES CÂBLES

Câble AWG, diamètre, capacité de courant, et résistance à 20 °C.
Ces valeurs peuvent varier d'un câble à câble.
En cas de doute, consulter les spécifications du fabricant.

AWG Gauge	Diamètre (mm)	Ohms / Mètre	Ampères Maximum
0000	11.68	0.000161	302
000	10.40.00	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

APPENDIX E: SOLAR DIMENSIONING

Utilisez ces tables pour collecter les données nécessaires pour estimer la taille requise pour votre système solaire.

General Data

Nom du site	
Latitude du site (°)	

Données d'irradiation

$G_{dm}(0)$, en kWh / m^2 par jour)

Jan	Feb	Mar	Avr	Mai	Jun	Juil	Août	Sep	Oct	Nov	Dec
Le mois de pire Irradiation											

Fiabilité et Tension opérationelle du système

Journées d'autonomie (N)	
Tension Nominale (V_{NEquip})	

Caractéristiques des composantes

Panneaux solaires	
Tension @ Puissance Maximale (V_{pmax})	
Courant @ Puissance Maximale (I_{pmax})	
Type de panneau/Modèle and 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})	
Regulator	
Tension Nominale (V_{NReg})	
Courant Maximum (I_{maxReg})	

Panneaux solaires	
Tension @ Puissance Maximale (V_{pmax})	
Courant @ Puissance Maximale (I_{pmax})	
Type de panneau/Modèle and Puissance (W_p)	
Convertisseur DC/AC (si nécessaire)	
Tension Nominale (V_{NConv})	
Puissance Instantanée (P_{IConv})	
Performance @ 70% Load	

Charges

Estimatation de l'énergie consommée par les charges (DC)				
Mois de plus grande consommation				
Description	# of Unités	x Puissance Nominale	x Usage Heures/ Jour	= Energie (Wh/jour)

Estimatation de l'énergie consommée par les charges (DC)				
Mois de plus grande consommation				
ETOTAL DC				
Estimatimation de l'énergie consommée par les charges (AC)				
Mois de plus grande consommation				
Description	# of Unités	x Puissance Nominale	x Usage Heures/ Jour	= Energie (Wh/jour)

Estimatation de l'énergie consommée par les charges (DC)				
Mois de plus grande consommation				
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												
(Month)	J	F	M	A	M	J	J	A	S	O	N	D
Inclinaison ß												

Nom du site												
Latitude du site (°)												
G_{dm} (ß) (kWh/m^2 × jour)												
E_{TOTAL} (DC) (Wh/jour)												
E_{TOTAL} (AC) (Wh/jour)												
E_{TOTAL} (AC + DC)=												
I_m (A) = E_{TOTAL} (Wh/jour) × $1kW/m^2$/ (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	

Nom du site	
Latitude du site (°)	
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 des panneaux	$N_{TOT} = N_{PS} \times N_{PP}$ =	
Batteries		
Capacité nécessaire (C_{NEC})	E_{TOTAL}(Pire des mois) / $V_N \times N$	
Capacité nominale (C_{NOM})	C_{NEC} / DoD_{MAX}	

Panneaux			
Panneaux en série (N_{PS})	$N_{PS} = V_N / V_{Pmax}$ =		
Panneaux en parallèle (N_{PP})	$N_{PP} = I_{mMAX} / I_{Pmax}$ =		
Nombre des batteries en série (N_{BS})	V_N / V_{NBAT}		
Câbles			
	Panneaux > Batteries	Batteries > Convertisseur	Ligne principale
Chtte de tension (V_a - V_b)			
Epaisseur (Section) r x L x I_{mMAX} / (V_a - V_b)			

Pour le calcul d'épaisseur du câble, r = 0.01286 $\Omega\ \mathrm{mm}^2/\mathrm{m}$ (pour le cuivre) and L is la longueur en mètres.

APPENDIX F: RESOURCES

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

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 NEC2 code archives, http://www.nec2.org/
USB WiFi dish designs, http://www.usbwifi.orcon.net.nz/

Outils de dépannage réseau

Bing throughput measurement tool,http://fgouget.free.fr/bing/index-en.-shtml
Cacti network monitoring package, http://www.cacti.net/
DSL Reports bandwidth speed tests, http://www.dslreports.com/stest
EtherApe network traffic monitor, http://etherape.sourceforge.net/
Flowc open source NetFlow collector, http://netacad.kiev.ua/flowc/
iptraf network diagnostic tool, http://iptraf.seul.org/
My TraceRoute network diagnostic tool, http://www.bitwizard.nl/mtr/
Nagios network monitoring and event notification tool, http://www.nagios.org/
NetFlow, the Cisco protocol for collecting IP traffic information, http://en.wikipedia.org/wiki/Netflow
ngrep network security utility for finding patterns in data flows, http://ngrep.sourceforge.net/
Network monitoring implementation guides and tutorials, http://wiki.debian.org/Network_Monitoring
Ntop network monitoring tool, http://www.ntop.org/
SoftPerfect network analysis tools, http://www.softperfect.com/
Squid transparent http proxy HOWTO, http://tldp.org/HOWTO/TransparentProxy.html
Wireshark network protocol analyzer, http://www.wireshark.org/
MRTG, http://oss.oetiker.ch/mrtg/

rrdtool, http://oss.oetiker.ch/rrdtool/
Smokeping, http://oss.oetiker.ch/smokeping/
Argus, http://qosient.com/argus/
Netramet, http://www.caida.org/tools/measurement/netramet/
Snort, http://www.snort.org/
Mod Security, http://www.modsecurity.org/
Apache, http://www.apache.org/
Zabbix, http://www.zabbix.org/
ngrep, http://ngrep.sourceforge.net/
nmap, http://www.nmap.org
netcat, http://nc110.sourceforge.net/

Securité

AntiProxy http proxy circumvention tools and information, http://www.antiproxy.com/
Anti-spyware tools, http://www.spychecker.com/
Driftnet network monitoring utility, http://www.exparrot.com/~chris/driftnet/
Introduction to OpenVPN, http://www.linuxjournal.com/article/7949
Linux security and admin software, http://www.linux.org/apps/all/Networking/Security_/_Admin.html
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
Stunnel Universal SSL Wrapper, http://www.stunnel.org/
TOR onion router, http://www.torproject.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/
Logging, http://wigle.net/, http://www.nodedb.com/, or http://www.stumbler.net/. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html http://www.cs.umd.edu/~waa/wireless.pdf

http://dl.aircrack-ng.org/breakingwepandwpa.pdf
http://download.aircrackng.org/wikifiles/doc/enhanced_tkip_michael.pdf
Captive Portals, CoovaChilli, CoovaAP (http://coova.org/CoovaChilli/)
WiFidog (http://www.wifidog.org/)
M0n0wall, pfSense (http://m0n0.ch/wall/)
Putty, http://www.putty.nl/
Win SCP, http://winscp.net/
Cygwin, http://www.cygwin.com/
OpenVPN Journal, http://www.linuxjournal.com/article/7949
Tor, http://www.torproject.org/
Spychecker, http://www.spychecker.com/

Optimisation de largeur de bande

Cache hierarchies with Squid,
http://squid-docs.sourceforge.net/latest/html/c2075.html
dnsmasq caching DNS and DHCP server,
http://www.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/
Linux Advanced Routing and Traffic Control HOWTO, http://lartc.org/
Microsoft Internet Security and Acceleration Server, http://www.microsoft.com/isaserver/
Microsoft ISA Server Firewall and Cache resource site, http://www.isaserver.org/
Optimising Internet Bandwidth in Developing Country Higher Education, http://www.inasp.info/pubs/bandwidth/index.html
Planet Malaysia blog on bandwidth management,
http://planetmy.com/blog/?p=148
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

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/

AirJaldi Mesh Router, http://drupal.airjaldi.com/node/9
Open WRT, http://wiki.openwrt.org/toh/start
Village Telco, www.villagetelco.org

Systèmes d'exploitation et pilotes pour périphériques sans fil

DD-WRT wireless router OS,http://www.dd-wrt.com/
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://code.google.com/p/pyramidlinux/
OpenWRT wireless router OS for Linksys access points, http://openwrt.org/
Tomato wireless router OS for Linksys access points, http://www.polarcloud.com/tomato

Outils sans fil

Chillispot captive portal, http://www.chillispot.info/
Interactive Wireless Network Design Analysis Utilities, http://www.qsl.net/n9zia/wireless/page09.html
KisMAC wireless monitor for Mac OS X, http://kismac-ng.org/
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, http://www.wirelessdefence.org/Contents/NetstumblerMain.htm
Netspot wireless network detection for Mac OS X, http://www.netspotapp.com/
PHPMyPrePaid prepaid ticketing system, http://sourceforge.net/projects/phpmyprepaid/
RadioMobile radio performance modeling tool, http://www.cplus.org/rmw/
Radio Mobile online, http://www.cplus.org/rmw/rmonline.html
Wellenreiter wireless network detection tool for Linux, http://sourceforge.net/projects/wellenreiter/
WiFiDog captive portal, http://www.wifidog.org/
Proxim, http://www.proxim.com/technology
WiSpy spectrum analysis tool, http://www.metageek.net/
Spectrum Analyser, http://www.seeedstudio.com/depot/rf-explorer-model-

wsub1g-p-922.html?cPath=174
"RF Explorer model 2.4G",
http://www.seeedstudio.com/depot/-p-924.htmlcPath=174
VideoSend. http://www.lightinthebox.com/Popular/Wifi_Video_Transmitter.html

Information générale sur le sans fil

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
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
White Spaces project, http://www.wirelesswhitespace.org/projects.aspx

Outils de calcul généraux

File sharing, http://sparkleshare.org, https://github.com/philcryer/lipsync, http://rsync.samba.org/
Open Relay testing, http://www.mailradar.com/openrelay, http://www.checkor.com/
Disk imaging, http://www.partimage.org, http://www.powerquest.com/

Services réseautages et formation

Wireless Toolkit,
http://wtkit.org/groups/wtkit/wiki/820cb/download_page.html
wire.less.dk consultancy and services, http://wire.less.dk/
Wireless Lab and training at ICTP, http://wireless.ictp.it/
WirelessU, http://wirelessu.org/
Network Startup Resource Center, Oregon, http://www.nsrc.org/
Inveneo, http://www.inveneo.org/
6Deploy (EC FP7 project), http://www.6deploy.org
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://mak.ac.ug/
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/
Collection of looking glasses, http://www.traceroute.org/

Regional Internet Registrars

IANA, http://www.iana.org/
AfriNIC, http://www.afrinic.net/
APNIC, http://www.apnic.net/
ARIN, http://www.arin.net/
LACNIC, http://www.lacnic.net/
RIPE NCC, http://www.ripe.net/

Transition vers l'IPv6

http://www.petri.co.il/ipv6-transition.htm
http://www.6diss.org/tutorials/transitioning.pdf
http://arstechnica.com/business/2013/01/ipv6-takes-one-step-forward-ipv4-two-steps-back-in-2012/
http://www.6deploy.eu/index.php?page=home
RIPE IPv6 transiton, http://www.ipv6actnow.org/
Test your IPv6, http://tet-ipv6.org
IPv6 Deployment status, http://6lab.cisco.com

Protocoles de routage dynamiques

http://www.ciscopress.com/store/routing-tcp-ip-volume-i-ccie-professional-development-9781578700417?w_ptgrevartcl=Dynamic%20Routing%20-Protocols_24090
http://www.ciscopress.com/articles/article.asp?p=24090&seqNum=5
http://ptgmedia.pearsoncmg.com/images/9781587132063/samplechapter/1587132060_03.pdf
http://www.inetdaemon.com/tutorials/internet/ip/routing/dyamic_vs_static.shtml https://learningnetwork.cisco.com/docs/DOC-7985
OSPF Design guide: http://www.cisco.com/warp/public/104/1.pdf

Conception de panneaux solaires

Low resolution PSH maps/calculation tools,

http://re.jrc.ec.europa.eu/pvgis/apps4/pvest.php?map=africa&lang=en
Highlands And Islands project,
http://www.wirelesswhitespace.org/projects/wind-fi-renewable-energy-basestation.aspx
PVSYST, http://www.pvsyst.com/
Solar Design, http://www.solardesign.co.uk/

Liens divers

Cygwin Linux-like environment for Windows, http://www.cygwin.com/
Graphviz network graph visualization tool, http://www.graphviz.org/
ICTP bandwidth simulator, http://wireless.ictp.trieste.it/simulator/ ImageMagick image manipulation tools and libraries, http://www.imagemagick.org/
NodeDB war driving map database, http://www.nodedb.com/
Partition Image disk utility for Linux, http://www.partimage.org/
RFC 1918: Address Allocation for Private Internets,
http://www.ietf.org/rfc/rfc1918
Rusty Russell's Linux Networking Concepts,
http://www.netfilter.org/documentation/HOWTO/networkig-concepts-HOWTO.html
Ubuntu Linux, http://www.ubuntu.com/
VoIP-4D Primer, http://www.it46.se/voip4d/voip4d.php
wget web utility for Windows, http://users.ugent.be/~bpuype/wget/
ISO Standard, http://standards.iso.org/ittf/PubliclyAvailableStandards

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 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

Wireless Hacks, 2nd Edition. Rob Flickenger and Roger Weeks, O'Reilly Media. ISBN #0-596-10144-9

IPv6 Security (Cisco Press Networking Technology). Scott Hogg, Eric Vyncke, Cisco Press. ISBN # 1587055945

LAN Switch Security: What Hackers Know About Your Switches. Eric Vyncke and Christopher Paggen. ISBN #1587052563

Building the Mobile Internet. Mark Grayson, Kevin Shatzkamer, Klaas Wierenga. ISBN # 1587142430

ÉTUDES DE CAS

ÉTUDES DE CAS-INTRODUCTION

Peu importe la planification requise afin d'établir un lien ou un nœud, 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 nœud, vous trouverez que les choses ne fonctionnent pas toujours comme vous pouviez l'avoir prévu. Cette section 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 et même les experts qui ont contribué à ce livre continuent à apprendre à travers les projets dans lesquels ils sont impliqués. Voici quelques conseils et idées de dernière minute avant de nous embarquer pour vous raconter nos dernières aventures sur le terrain.

Boitiers 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. E
n Afrique occidentale, le PVC le plus ordinaire se trouve dans la tuyauterie, avec une mesure de 90 mm à 220 mm. Parfois les points d'accès 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 s'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. Un treillis métallique fait à partir de matériel localement disponible fut utilisé pour protéger le trou d'échappement des infestations.

Mâts d'antenne

La récupération de matériaux usagés pour construire des mâts d'antenne est un bon plan. Les ouvriers locaux qui travaillent avec le métal seraient déjà familiers avec la façon de construire 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. Il est possible d'augmenter la taille de ce type de mât de plusieurs mètres par 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. Les détails sur la mise à terre du mât peuvent être trouvés dans le chapitre intitulé **Sélection et configuration du matériel**.

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 qu'il servira.
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.
De plus, prenez note des principaux acteurs dans un établissement ou dans la communauté. Identifiez les personnes qui sont susceptibles d'être des opposants et des partisans de votre projet. Aussitôt que possible, essayez de gagner le soutien des partisans éventuels et de diffuser les opposants. C'est une tâche difficile et qui nécessite une connaissance intime de l'institution ou de la collectivité. Si le projet n'a pas un allié local, le projet doit prendre le temps d'acquérir cette connaissance et la confiance de la communauté . N'essayez pas d'introduire une technologie à une communauté sans comprendre les applications qui serviront réellement cette communauté.

En recueillant l'information, vérifiez les faits qui vous sont présentés. Le plus souvent, les associés locaux qui vous font confiance seront très francs, honnêtes et utiles.
Lors du choix des méthodes de paiement pour votre nouveau service sans fil, les services prépayés sont idéales, car ils ne nécessitent pas un contrat légal. L'engagement est assuré par l'investissement des fonds avant que le service ne soit fourni. Le fait d'accepter un projet exige également que les personnes impliquées investissent eux-mêmes dans le projet. Un projet devrait exiger la participation réciproque de la communauté. Surtout, l'option " no-go " 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 car l'équipement, l'argent et la formation ne peuvent pas être des cadeaux. La communauté doit être impliquée et doit également contribuer.

Maintenant lisez la suite

Dans les chapitres suivants de cette section, vous trouverez décrits certains de nos projets à partir desquels nous espérons que vous trouverez utile d'apprendre. Nous n'avons pas inclus les études de cas des versions antérieures de ce livre à l'exception de l' un au Venezuela qui avait extrêmement contribué à établir la viabilité des liaisons point-a-point extérieures longue distance pour la connectivité rurale.

Une étude de cas n'est pas incluse dans cette section mais elle est conduite par Inveneo qui travaille en étroite collaboration avec l'équipe impliquée dans la rédaction de ce livre. Cette étude peut être trouvée à l'adresse suivante. http://www.inveneo.org/90km-wireless-link-for-mfangano-island/.
Le projet est dirigé par Andris Bjornson qui est CTO de Inveneo. Il y a quelques informations très utiles dans son rapport sur le projet.
Nous espérons maintenant que vous apprécierez la lecture de chacune des études de cas qui suivent cette introduction. Vous verrez qui a été impliqué et bien sûr leur profil est inclus dans la section remerciements de ce livre.
Tous les auteurs de ce livre ont participé à des déploiements sur le terrain.

Veuillez aussi surveiller notre page Facebook que vous pouvez trouver à l'URL suivant:
https://www.facebook.com/groups/wirelessu/

ÉTUDE DE CAS – 801.11 LONGUE DISTANCE AU VENEZUELA

Introduction

Bien que cette étude de cas soit vielle de plusieurs années, nous l'avons laissé dans cette version du livre car elle reste à ce jour le test de liaison 802.11 point à point de plein air le plus long jamais réussi.
Vous trouverez ici le travail de pionnier de ceux qui sont encore co-auteurs de ce livre. Et en fait, une partie du travail de préparation pour la mise en place de ce test est toujours d'actualité pour ceux qui envisagent des liaisons longue distance extérieures . Bonne lecture !

Background

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'url *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 *CsLD 1* en utilisant Google Earth:

Figure CsLD 1: 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 CsLD 2:

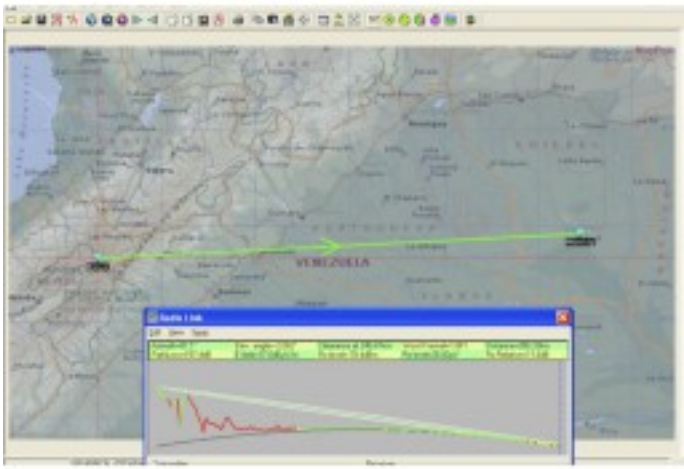


Figure CsLD 2: Plan et profil du projet de chemin entre Pico Aguila, et la colline Morrocoy, près de la ville de El Baul.

Les détails de la liaison sans fil sont affichés par la Figure CsLD 3:

Figure CsLD 3: 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 CsLD 4: 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 CsLD 5 montre le démontage du réflecteur maillé.

Figure CsLD 5: 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 CsLD 6:

Figure CsLD 6: 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 CsLD 7: 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 CsLD 8 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 CsLD 8: 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 5ms.

Figure CsLD 9: Installation d'antenne à 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 CsLD 10.

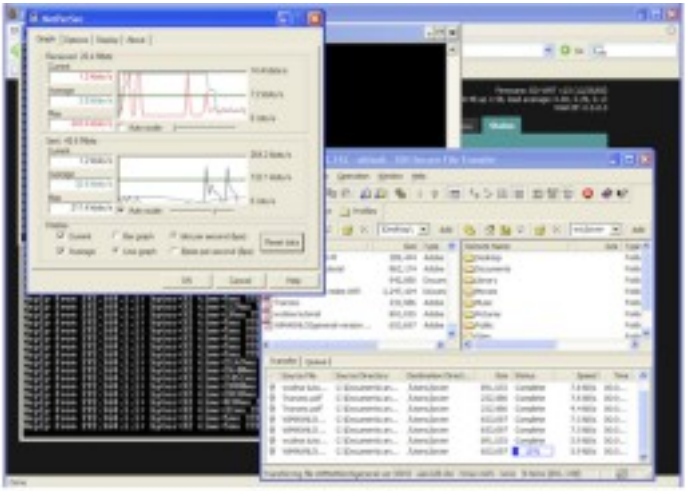


Figure CsLD 10: Capture d'écran de l'ordinateur portable de Javier montrant les détails de transfert de fichiers PDF à partir de l'ordinateur portable de Carlo a 280 km de distance, en utilisant deux routeurs sans fil WRT54G, et sans amplificateurs.

Notez le temps ping de quelques millisecondes.

Figure CsLD 11: Javier Triviño (à droite) et Ermanno Pietrosemoli rayonnant à cause de l'antenne d' El Baul.

Figure CsLD 12: 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.

Pouvions-nous 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 CsLD 13:

Figure CsLD 13: 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 CsLD 14: 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 GLD 15: 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

ÉTUDE DE CAS: PROJET PISCES

Liaisons Wifi Solaires en MicronésiePar Bruce Baikie et Laura Hosman, assistés sur le terrain par Marco Zennaro et Ermanno Pietrosemoli d'ICTP.

Deux liaisons sans fil longue distance alimentées par énergie solaire ont été implémentées mises dans la région de la Micronésie dans le Pacifique au début Août 2012 dans le cadre du projet Pacific Island Schools Connectivity, Education, and Solar (PISCES) (http://www .piscespacific.org/livesite/), une entreprise multipartenaire axée sur la formation et le renforcement des capacités locales vis-à-vis des technologies de l'information et communication (TICs) par énergie solaire dans la région du Pacifique.

Figure CSP 1: Formation pratique

La première partie du projet PISCES était un atelier de formation pratique sur la technologie WiFi longue distance par énergie solaire à l'Université de Guam. L'atelier avait porté sur la technologie Wi-Fi, les normes, l'énergie solaire, des études de site, la sécurité du projet, et des outils de planification de liaison. L'atelier avait fourni beaucoup de possibilités pour des expériences pratiques, avec chaque activité d'après-midi consistant d'un laboratoire d'une à trois heures où les élèves s'actualisent des informations pratiques sur la présentation du matin. Le dernier jour, les étudiants mirent en place une liaison point à point à haut débit alimentée par le solaire dans le centre de l'île pour la durabilité, remplaçant une liaison à l'Internet ancienne qui était plus lente.

Figure CSP 2 : Une nouvelle connexion Internet plus rapide pour le centre de l'île pour la durabilité.

Pour la deuxième partie du projet POISSONS, l'équipe s'est rendue à Chuuk, l'un des États fédérés de Micronésie et y a installé à la fois une liaison Internet Wifi longue distance et un laboratoire information de type lab-in-a-box alimenté par le solaire à une primaire école primaire appelée Udot sur une île qui auparavant n'était pas connectée à l'Internet dans le lagon de Chuuk.

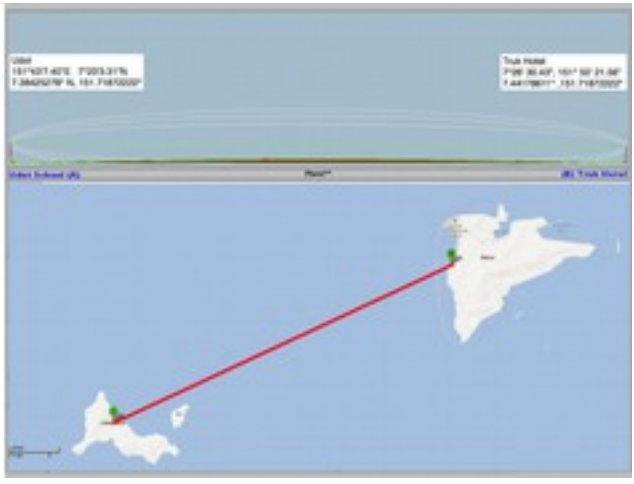


Figure CSP 3 : La connexion Internet pour l'école Udot venait de l'île principale de Chuuk, Weno, à 15 km.

Figure CSP 4 : Montage du poteau pour le mât dans Udot

L'équipement Wifi de marque Ubiquiti Networks installé dans Weno a été monté sur la toiture du 3e étage de l'hôtel de Truk, qui offrait la hauteur nécessaire pour obtenir une ligne de mire fournissant une connectivité à travers le lagon de Chuuk à l'île Udot.
L'école sans étage d' Udot nécessitait un poteau pour le mât de 40 pieds (12 m) sur lequel monter l'antenne/radio de type Ubiquiti Networks.
Les membres de la communauté se joignirent pour aider quand la stature du poteau de mât s'avéra trop lourd pour l'équipe POISSONS pour élever seule.
Avec les membres de l'équipe sur chaque île, les antennes furent alignées et connectées les unes aux autres.
Le réseau fut ensuite routé à travers une connexion Internet DSL locale pour fournir une connectivité Internet à l'école et la communauté locale environnante.

Chaque unité WiFi était alimentée par un système solaire photovoltaïque qui se compose d'un panneau solaire de 30 watts de Solarland USA, un régulateur de charge solaire avec Power over Ethernet, et 38 ampères-heures de batterie de secours.

CSP 5 : Udot

Le système unique laboratoire informatique de type Lab-in-a-Box déployé à l'école Udot avait été développé par des étudiants de l'Illinois Institute of Technology.
Ce laboratoire d'informatique clé en main avait été conçu pour être aussi près de plug-and-play que possible pour les environnements hors réseau. Il comprenait six ordinateurs portables Intel Classmate, des panneaux solaires et des engins de montage, un régulateur de charge, le câblage et l'équipement de sécurité pour ordinateur portable, le tout contenu dans un boîtier conçu de façon unique et prêt-à-expédier et qui se transforme de facilement en table de salle informatique .

Figure CSP 6

Le projet PISCES avait reçu le soutien financier de Google, la Pacific Telecommunications Council, et l'Internet Society.

En plus des partenaires mentionnés ci-dessus, les partenaires POISSONS projet comprennent:

- Université de Guam
- Illinois Institute of Technology
- Green WiFi, Inveneo
- iSolution
- Centre international de physique théorique (ICTP)
- Université de California, le groupe de recherche TIER de Berkeley.

ÉTUDE DE CAS - UNIVERSITÉ DU GHANA RÉSEAU CAMPUS SANS FIL

Introduction

L'Université du Ghana est l'un des six universités publiques et la première université au Ghana avec 41000 étudiants.
Avec le nombre croissant d'étudiants et de professeurs, il était évident que nous ne pouvions pas continuer à développer nos laboratoires informatiques pour faciliter l'apprentissage et de la recherche, car nous avions un espace limité et des fonds limités pour équiper ces laboratoires informatiques.
La solution était de passer au sans fil de sorte que tout élève avec son ordinateur portable pourrait accéder au réseau. Ceci cependant ne pouvait être atteint immédiatement en raison de l'état du réseau à ce moment. C'était un grand réseau plat non géré avec beaucoup de problèmes - les conflits IP, des DHCP non autorisés, et des grands domaines de diffusion pour n'en citer que quelques-uns.
Comme le service informatique ne fournissait pas un service sans fil à la communauté, les utilisateurs devinrent impatients et commencèrent à connecter leurs propres routeurs sans fil au réseau. Ceci rendit la gestion du réseau même plus difficile. Il devint évident que, si nous ne fournissons pas un service sans fil à la communauté des utilisateurs, ils trouveraient leur propre façon de faire.
Notre première étape remédier à ce problème fut de reconcevoir notre réseau allant d'un réseau à plat pour un réseau plus structurée avec des couches de base, de distribution et d'accès. Ceci apporta beaucoup de stabilité au réseau.
A cause des commutateurs gérés, des problèmes d'identification devinrent aussi beaucoup plus facile à gérer.
Le réseau câblé structuré nous a donné une bonne base pour construire un réseau sans fil qui complète le réseau câblé et répond aux besoins croissants de nos utilisateurs .

Configuration et installation Wifi

Un certain nombre de facteurs ont été pris en compte dans la détermination du type de point d'accès (AP) à déployer.
Certains d'entre eux étaient :

- Coût
- support
- Gestion
- Sécurité

A cause de la taille de notre réseau, if fut décidé d'aller pour une solution d'entreprise qui rendrait la gestion beaucoup plus facile . En raison du coût élevé de ces Solutions Entreprises (600 $ par point d'accès et plus + coût du contrôleur) nous nous sommes retrouvés dans un long débat sur le produit à utiliser pour l'implémentation WiFi. Nous consultâmes le NSRC (le Centre de ressources pour démarrage des réseaux à l'Université de l'Oregon) qui était également à la recherche des solutions sans fil abordables et évolutives et ils envoyèrent l'Ubiquiti UniFi qui coûte environ 80 $ par point d'accès et dispose d' un contrôleur de logiciel libre. Ensemble avec le personnel NSRC, nous conduisîmes une enquête ainsi qu'un projet pilote avec 10 points d'accès avec succès. En raison du coût, de fonctionnalité, maniabilité et facilité de déploiement, l'Université du Ghana décida d'étendre le réseau à l'aide des point d'accès Ubiquiti Unifi points et le réseau passa rapidement grandi de 10 points d'accès à 90. Pour plus de sécurité, les points d'accès Unifi supportent à la fois l'encryptage WPA Personal et WPA Enterprise qui permet aux utilisateurs de s'authentifier auprès d'un serveur radius. En plus de tous les avantages de déploiement d'Ubiquiti, nous trouvâmes qu'il y avait une grande communauté d'utilisateurs UniFi qui fournit une bonne aide technique en cas de problèmes.

Installation AP

L'installation et la configuration initiale impliquaient la connexion d'un point d'accès à un port de commutateur de réseau dans le même VLAN que le serveur du contrôleur. L'AP passe par l'adoption lors de la connexion ce qui permet à le nouveau AP de s'enregistrer avec le contrôleur pour la gestion. Après l'installation initiale, l'AP est alors relié au vlan sans fil du département désigné sur un switch. .

Adressage IP

L'adressage IP privé a été adopté pour le réseau sans fil sur le campus. Il y a en moyenne 25/24 sous-réseaux sans fil dans les départements, facultés, écoles et collèges.

Bande passante

L'allocation de bande passante sur le réseau sans fil est de 10% de la bande passante STM1 de l'Université. La croissance courante des utilisateurs sans fil couplée avec des applications émergentes en croissance demandera plus de bande passante pour donner une bonne expérience de navigation .

Sécurité / Authentification

Les utilisateurs et les points d'accès s'authentifient auprès d'un serveur radius utilisant 802.1x. A la fois les détails étudiant et personnel sont stockés dans une base de données Mysql. Le réseau campus sans fil existe dans des VLANs distincts du réseau câblé pour l'identification et la gestion facile.

Connexion au réseau sans fil du campus de UG

Le réseau campus sans fil de l'université du Ghana comporte trois grands réseaux/SSIDs - PERSONNEL, ÉTUDIANT, INVITÉ.

PERSONNEL

Ce SSID/réseau est disponible pour le personnel actif de l'Université. Les membres du personnel doivent s'authentifier avec leur numéro identité personnel et un PIN comme nom d'utilisateur et mot de passe respectives pour se connecter.

ÉTUDIANT

Ce SSID / réseau est disponible pour les étudiants de l'Université qui se sont inscrits pour une année scolaire donnée. Les étudiants s'authentifient avec leur numéro identité étudiant et un PIN comme nom d'utilisateur et mot de passe respectives pour se connecter.

VISITEUR

Ce SSID/réseau est disponible pour les visiteurs qui visitent l'Université dans un délai de temps donné. Les visiteurs sont priés de demander des détails d'un compte d'authentification du service informatique en soumettant leurs détails.

Photos de notre projet et l'installation

Figure CSG 1 : Notre campus

Figure CSG 2 : Notre campus

Figure CSG 3 : Une salle de classe

Figure CSG 4 : La bibliothèque

Figure CSG 5 : Un de nos points d'accès

Figure CSG 6 : Layout du campus de l'Université du Ghana avec des Aps.

Figure CSG 7 : Avec UniFi, nous sommes en mesure de simuler la couverture du signal sans fil comme indiqué ci-dessus.

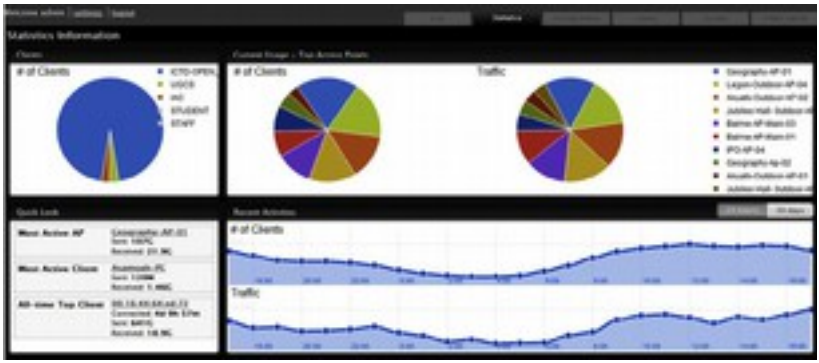


Figure CSG 8: Au-dessus se trouve le contrôleur UniFi montrant des statistiques de notre utilisation.

Figure CSG 9 : Voici les statistiques par point d'accès.

Figure CSG 10 : Nous sommes également en mesure d'obtenir des statistiques par utilisateur à partir du contrôleur.

Défis auxquels nous nous sommes confrontés.

L'un de nos principaux défis a été d'obtenir un bon câble CAT5 pour l'installation. En outre, il a été un peu difficile d'emmener le câble au bon endroit car les bâtiments n'ont pas été conçus avec cela à l'esprit. La bande passante est aussi un défi, mais nous essayons de limiter les activités peer-to -peer sur le réseau à l'aide de Cyberoam.

Prochaines étapes

Nous (le service informatique de l'Université du Ghana) exploitons le réseau sans fil nous-mêmes. Nous avons des plans immédiats pour étendre le réseau sans fil jusqu'à ce que nous couvrions nos bâtiments du campus autant que possible. Ce alors réduira la nécessité pour nos étudiants d'installer leurs propres APs, rendant ainsi notre travail de gestion de réseau beaucoup plus facile!

Auteur : Emmanuel Togo, Chef de l'Unité réseau des systèmes informatiques de l'Université du Ghana (UGCS).

ETUDE DE CAS- RÉSEAU AIRJALDI GARHWAL, INDE

Introduction

Dans la version 2 de ce livre, nous avons inclus une étude de cas sur le réseau maillé communautaire sans fil Dharamsala. À la suite de ce déploiement initial dans les années suivantes, une nouvelle série de réseaux et un fournisseur de services Internet sans fil commercial ont émergé dans la même région conduits par les mêmes personnes. Nous décrivons ici un de leurs grands projets.

Réseau Airjaldi Garhwal:

Oeuvrer pour la viabilité économique et technique dans la gamme de l'Himalaya

À propos de Rbb / Airjaldi

Rural Broadband Pvt . Ltd, est un innovateur et réalisateur de premier plan des solutions de connectivité techniquement et économiquement viables pour les zones rurales. Nous concevons, construisons et exploitons des réseaux à large bande dans les zones rurales en Inde. Constituée en société en Inde en 2009, RBB possède actuellement et exploite des réseaux dans les Etats indiens de l'Himachal Pradesh, Uttaranchal, Jharkhand, et le Karnataka. RBB utilise AirJaldi comme une marque déposée pour son réseau et d'autres initiatives liées à la connectivité. Les activités de l'entreprise sont réalisées à partir de notre bureau de gestion à Delhi, nos bureaux des opérations à Dharamsala, Himachal Pradesh et des bureaux dans chaque emplacement réseau . Notre équipe diversifiée comprend des villageois indiens, les réfugiés tibétains, des professionnels qualifiés des régions métropolitaines en Inde et les gens de l'extérieur de l'Inde. Nous pensons que les réseaux ruraux doivent être techniquement viables - ils ont besoin de fournir une qualité et des services cohérents qui sont à tout le moins similaires à ceux offerts nulle part ailleurs.

Ils doivent aussi être économiquement viables - ils ont besoin pour être en mesure de s'autofinancer dans un délai de temps relativement court (environ 18 mois) tout en offrant des services aux clients à des prix raisonnables.

En outre, nous sommes d'ardents défenseurs d'une approche «retail ecosystem» - quand nous atteignons une zone, nous cherchons à connecter tous les clients qui ont besoin de connectivité, quelle que soit la taille de leur exploitation ou de leur demande. Nous aspirons à faire payer tous nos clients pour leur connectivité, même si les subventions sont offertes aux clients sélectionnés, principalement ceux qui se consacrent à des causes sociales et de développement et montrant un besoin financier. RBB travaille en étroite collaboration avec a section recherche et innovation d' AirJaldi, une (section 25) entreprise à but non lucratif enregistrée en Inde. Créée en 2007, la section recherche et l'innovation d'AirJaldi identifie les solutions de réseaux appropriés et abordables pour les zones rurales, les teste dans des environnements réels et partage son apprentissage avec les organisations et les individus similaires. AirJaldi exploite également un centre de formation et de renforcement des capacités à Dharamsala, où les opérateurs et les activistes réseaux peuvent acquérir les compétences nécessaires pour construire et gérer des réseaux sans fil ruraux.
La plupart de nos membres de l'équipe de déploiement ont été formés par notre organisation sœur – la section recherche et d'innovation d'AirJaldi. Les membres de l'équipe suivent normalement un cours de base d'un mois "Wireless 108" et les cours plus avancés " Wireless 216 " offerts à la AirJaldi Network Academy. Après un stage de 3 mois supplémentaires où ils travaillent sous la supervision étroite de membres chevronnés de l'équipe dans une de nos réseaux, ils sont enrôlés comme membres de l'équipe permanente .

Le réseau Airjaldi Garhwal - Statistiques vitales

Date d'ouverture / création | Janvier 2010

Taille / diffusion | environ 100 km2, allant de la vallée de Dehradun aux hauteurs des montagnes Tehri Garwal (hauteur d'environ 2000 mètres) .

Principaux clients | l'entreprise Micro bancaire, les écoles, les organisations communautaires, les entreprises et utilisateurs privés

La plus longue liaison| 55 km .

La densité de population | 169/km2 (en comparaison: Delhi : 9294 / km2 ; ensemble Inde : 363/km2 ; USA : 33.7/km2)

Réalités, les besoins

Les districts Tehri et Pauri Garhwal d' Uttarakhand, qui s'étend des sommets de l'Himalaya incluant Thalaiya Sagar, Jonli et le groupe Gangotri à la vallée Dheradun et Rishikesh, sont l'une des régions les plus montagneuses de l'Inde. Connue pour ses nombreux temples, situés sur les rives du Gange et sur les collines menant à la chaîne de l'Himalaya, la région est connue pour sa beauté sauvage. Cette rugosité est cependant aussi une cause de la pauvreté relative de la région: ses habitants vivent pour la plupart dans de petits villages séparés les uns des autres par de hautes montagnes et des vallées profondes. Les principales sources locales de revenus proviennent de subsistance agricole et les industries artisanales. Beaucoup de gens travaillent en dehors de la région, dans les grandes villes, dans les plaines et dans les services militaires et gouvernementaux à travers l'Inde .
En 2009, KGFS rural Services[1], une institution de micro-finance affiliée à IFMR Trust[2], décida d'opérer dans cette région montagneuse. Leur objectif était d'atteindre les clients potentiels dans les villages de Tehri et Pauri qui jusque-là n'avaient que peu ou pas d'accès aux services bancaires courants et étaient aussi considérés comme «à peine bancables» par la plupart des banques. L'utilisation de la cartographie de la densité de population permit à KGFS de trouver des emplacements pour ses succursales de banques au centre des « versants» atteignant environ 10.000 personnes. Très vite, Il devint clair pour KGFS qu'après avoir résolu des prérequis de densité et d'accessibilité, ils étaient confrontés à des limitations graves de connectivité, comme la plupart de leurs emplacements sélectionnés n'avaient pas l'infrastructure Internet. Un déploiement initial de VSAT et l'utilisation des services ADSL locaux s'avéra coûteux, lent et sujet à des pannes. C'est alors qu'un appel de l' équipe informatique de IFMR nous arriva, demandant si nous étions intéressés à proposer une solution de connectivité pour leurs 15 premières branches.

Le déploiement initial : approche, conception, déploiement

Lorsque nous répondîmes à l'appel, comme nous le faisons avec des demandes similaires, AirJaldi répondît sur la base des informations sur les éléments de réseau essentiels suivants :
Quelle est la distance la plus proche entre l'emplacement disponible du backhaul (l'endroit d'où nous pouvons bénéficier de l'accès à un nuage In-

1 http://ruralchannels.ifmr.co.in/kgfs-model/what-is-a-kgfs/
2 http://www.ifmr.co.in/

ternet) et la zone de déploiement proposé ?
Nos enquêtes montrèrent qu'il y avait relativement peu de sites backhaul dans la région. La plupart étaient situés dans Dehradun et les villes voisines (voir la figure CSD 1). De cet emplacement, atteindre la zone de déploiement proposé s'avéra problématique. Après beaucoup d'efforts nous trouvâmes un point de chute backhaul sur un BTS dans la ville de Narrandar Nagar (voir la figure CSD 1). Bien que très proche de certaines branches, il n'y avait pas de ligne de mire à partir du point de chute à aucune des branches. Cela nous conduisit à proposer une solution un peu contre-intuitive: utiliser l'emplacement Narrandar Nagar comme backhaul pour connecter un Network Operation Center (NOC) qui sera placé dans la vallée, où une meilleure ligne de mire aux sommets des montagnes favorables pour les relais potentiels était disponible.

Figure CSD 1 : Le backhaul du réseau Garhwal, le NOC et certaines branches IFMR, 2009

Pouvons-nous proposer un plan de déploiement qui est techniquement solide, mais en même temps abordable au « client d'ancrage »[3] et futurs clients

3 Chacun de nos réseaux a un ou plusieurs clients qui sont désignés comme des «clients d'ancrage». Le terme désigne leur rôle de premiers clients dans un réseau ainsi que ceux qui contribuent principalement à sa faisabilité économique initiale

supplémentaires ? Notre enquête initiale de la zone avait consisté à recueillir des données de latitude et de longitude de succursales proposées, l'identification des emplacements de relais possibles, l'évaluation du potentiel de client globale dans la région et l'évaluation de l'infrastructure publique de la zone. Nous n'avons pas été surpris de découvrir que les branches ont été pour la plupart situés dans les vallées (accès plus facile pour les clients, à proximité des routes) et séparées les unes des autres par des chaînes de montagnes élevées empêchant une ligne de mire directe entre elles.
L'alimentation en courant des relais promettait d'être un défi - la plupart des emplacements de relais potentiels étaient soit loin de la grille ou situés à des points faibles où le courant était parti parfois pendant des jours et des fluctuations sauvages de courant provoquaient des routeurs de "stopper " ou brûler quand des piques de puissance les frappaient. Ayant décidé que nous allions poursuivre ce déploiement dans tous les cas, notre équipe de déploiement devrait donner un sens à tout cela. La solution à laquelle nous arrivâmes fut basée sur la mise en place des relais alimentés par le solaire sur le peu d'endroits stratégiques que possible.
Cela conduisit à des enquêtes supplémentaires sur le terrain, impliquant des heures de recherches préliminaires au bureau à l'aide de cartes topographiques, Google Earth et d'autres outils, suivis par des jours de trekking à des endroits identifiés afin de voir si un emplacement pourrait être garanti par un loyer et si la sécurité et l'intégrité du relais pourrait être garanties par les propriétaires de l'emplacement.
Quel est le potentiel client global dans la région et sera-t-il suffisant, à un niveau minimal, garantir l'autosuffisance économique du réseau dans environ 18 mois ?
Le potentiel client ne semblait pas non plus brillant.
Outre les agences bancaires proposées, nous trouvâmes quelques clients supplémentaires - surtout des écoles et d'autres organisations.
Nous étions sûrs que la clientèle va croître dans le temps, mais il a falloir trouver un moyen pour assurer la viabilité dans un délai relativement court.
Nous décidâmes d'étendre le réseau à des zones plus densément peuplées au pied de la ferme de Garhwal. Les travaux de déploiement proprement dit commencèrent en Octobre 2009. Après environ deux mois de travail de déploiement, le réseau de base était prêt. Sa taille était d'environ 50x70km.
Il fournissait la connectivité à 15 agences bancaires et autour de cinq écoles et institutions dans la vallée.
La plupart de ses relais autonomes étaient à l'énergie solaire et sa liaison d'un seul saut la plus longue était de 54 km.

Figure CSD 2 : réseau Garhwal, topologie de déploiement partielle, début 2010

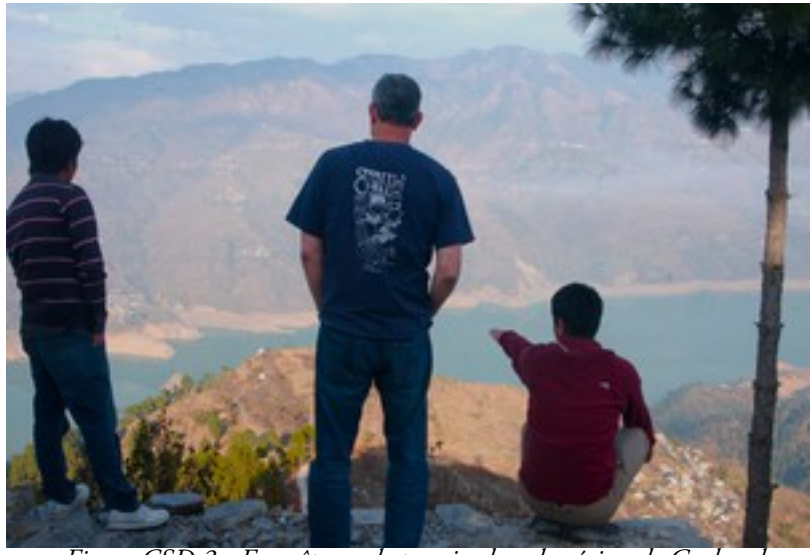


Figure CSD 3 : Enquête sur le terrain dans la région de Garhwal

Figure CSD 4 : Enquête sur le terrain dans la région de Kumaon

Figure CSD 5 : Préparation de l'installation de relais, réseau Kumaon

Figure CSD 6 : dépannage relais, réseau Kumaon

Figure CSD 7 : Dernières touches au relais solaire, réseau Kumaon

Figure CSD 8 : Relais backhaul, réseau Garhwal

Figure CSD 9 : Relais, réseau Garhwal

Figure CSD 10 : Relais client, réseau Kumaon

Trois ans après - exploitation, la viabilité économique, les défis et les réponses. Trois ans plus tard, le réseau actuel répond encore aux 15 premières branches et les clients originaux.
Il a également augmenté de manière significative. Sa taille actuelle est d'environ 120x100 km. Le temps de Voyage entre notre NOC/ Bureau a ses confins ultimes est de près de sept heures (!). Et le nombre des clients sur les montagnes et la vallée a considérablement augmenté. Dans ses efforts constants pour maintenir ce réseau difficile, notre équipe a dû faire face à des glissements de terrain, la neige, la pluie et des tempêtes de tonnerre, des éléphants sauvages, des léopards (eh oui!) et bien sûr des clients pour qui tout ceci importe peu lorsque leur liaison ne fonctionne pas.
Nous sommes très fiers du fait que notre disponibilité moyenne dans nos années d'exploitation dans la région dépasse 95 % et que le réseau a attiré beaucoup d'attention et des éloges de ses utilisateurs, d'autres acteurs de l'Internet et des médias. Cela dit, les défis ne manquent toujours et la lutte pour garder le tout en marche est encore un effort continuel. Les principaux défis auxquels nous sommes confrontés depuis la création du réseau sont:

Énergie – L'énergie est toujours un défi majeur. La grille pour la provision électrique est irrégulière et problématique. L'utilisation de la grille comme source d'énergie pour nos relais (même avec batterie de secours) a conduit à des routeurs brulés et des heures de Voyage pour dépanner les liaisons drainées de leur alimentation de secours après que la liaison soit coupée. L'énergie solaire, d'autre part, bien que presque sans-problème[4] est toutefois encore coûteuse.
Supporter les coûts en capital pour ces relais 'étend une proposition économique difficile encore plus loin, tout comme avoir des clients payant la totalité des coûts pour un relais limite le type de clients qui pourront profiter de nos connexions.

Relais - un bon relais est celui qui est placé dans un endroit couvrant autant d'espace que possible. Dans la région de Garhwal, ce sont des sommets de montagne. Ces lieux sont normalement et naturellement difficile d'accès et assez isolés. La construction, l'entretien et la sécurité dans ces sites est un défi permanent.

4 Chacun de nos réseaux a un ou plusieurs clients qui sont désignés comme des «clients d'ancrage». Le terme désigne leur rôle de premiers clients dans un réseau ainsi que ceux qui contribuent principalement à sa faisabilité économique initiale.

Au moment de la rédaction de cet article, nous étions en train de reconstruire un relais dont les panneaux solaires, la batterie, chargeur et autres équipements avaient été volés.
Certaines de nos nouvelles connexions se sont révélées être si difficiles qu'elles exigeaient un relais pour chaque nouveau emplacement, ce qui n'est clairement pas une proposition économique facile.

Taille - Aussi fiers que nous soyons de la taille du réseau, un voyage de plus de 10 heures entre ses points extrêmes est exhaustif pour les membres de note équipe, qui se déplacent la plupart du temps sur des vélos, à la limite avec des dépannages durant plus de deux jours à cause du voyage.

La viabilité économique - Le modèle dual montagne-vallée/faible densité grande densité de population, qui est implicitement une subvention croisée a fait ses preuves mais il n'a pas complètement résolu le problème de la viabilité économique des zones montagneuses marginales. Nos réponses à ces défis sont en évolution constante. Les observations présentes et les mesures mises en place sont:

Énergie - nous avons appris que les relais solaires sont la seule véritable option pour le réseau Garhwal (tout comme pour beaucoup d' autres endroits) . En essayant de rationaliser les coûts pour les clients, nous avons limité notre déploiement à clients de petites entreprises privées à des groupes où un minimum de 10 clients dont la demande d'au moins 1 Mbps par client peut être identifié dans un délai de 5-6 mois.
Une densité plus faible signifie des prix plus élevés et est généralement demandé par les clients pour qui la connectivité de leurs opérations est essentielle.
Nous avons également commencé à offrir des offres de type "paiement étendu pour engagement de temps ": les clients paient pour le coût de l'équipement et les relais (ou leur part de ceux-ci) sur une période de temps, si ils acceptent un contrat d'exclusivité sur une période de plus de deux ans .

Relais - le meilleur emplacement n'est pas nécessairement celui qui a la meilleure couverture seulement, mais celui qui présente une combinaison optimale de visibilité, sécurité, accessibilité et prix. Dans certains cas, cela signifie un plus grand nombre de relais, mais nous croyons que dans l'ensemble c'est une option moins onéreuse et plus rationnelle.

Taille - une solution simple au problème de la taille serait de morceler le réseau en petits sous réseaux ou des réseaux autonomes. Nous utilisons cette approche dans d'autres réseaux où la limite de taille est considérée par un voyage maximum de trois heures à un site.
Ceci cependant n'a pas de sens dans un réseau épars comme la partie supérieure de Garhwal. La solution de compromis à laquelle nous sommes arrivés était la mise en place de " points d'arrêt " dans les jonctions de réseau stratégiques. Essentiellement, ces " postes " sont des espaces de stockage où l'équipement est maintenu en quantité suffisante pour desservir un versant défini. Bien que ne résultant pas en gain de temps de voyage, ceci permet à notre équipe de se déplacer rapidement sans avoir à transporter le matériel lourd et encombrant.
L'évolution d'un poste relais à une base opérationnelle viendra quand l'assignation d'une équipe de deux personnes à un tel endroit pourra être justifiée par la densité de sa clientèle et des revenus.

La viabilité économique - l'objectif prioritaire d'AirJaldi est d'atteindre des zones non desservies et mal desservies avec une connectivité Internet de haute qualité. En tant que tel, le modèle de subventions croisées est justifiée comme une solution partielle aux problèmes rencontrés par de nombreux aspirant fournisseurs d'accès Internet en milieu rural qui n'ont pas les compétences ou le désir de construire des réseaux de l'échelle du réseau Garhwal. Ceci ne doit cependant pas être la seule voie économique pour le déploiement dans des environnements difficiles.
Nos tentatives pour accroître la viabilité de " fourniture d'accès en montagne " comprennent une tarification agressive de bande passante plus élevée - le coût marginal pour une bande passante supérieure est relativement faible, ce qui nous permet des revenus marginaux plus élevés tout en étant capable de proposer des offres très raisonnables pour ces packages.
Cela est en contradiction majeure avec les solutions non évolutives de dongle et VSAT qui sont souvent des alternatives à nos services dans ces domaines. À l'autre extrémité du spectre, nous avons commencé à offrir des packages de temps limité/bande passante.
Bien que plus chers sur une base unitaire, ces packages sont attrayants pour les clients qui souhaitent adapter leur consommation à leur volonté économique de payer. Les plans futurs comprennent l'introduction de « 4-C» : centres locaux où les utilisateurs peuvent utiliser la bande passante pour la configuration de la salle de classe (apprentissage en ligne individuel, enseigner à une classe en temps réel, etc) le cinéma (regarder des films ou

d'autres contenus en ligne dans un centre local), café (café Internet où les gens peuvent utiliser des ordinateurs individuels) et la connectivité (par hotspot local dans la région du centre ou par des offres de connectivité pour maisons et bureaux vendues au Café).

Résumé
Le réseau Garhwal a été créé en réponse à une demande d'un " client d'ancrage ", une entreprise de micro -finance pour qui la connectivité était une condition nécessaire pour une implémentation réussie de sa vision de la banque rurale. AirJaldi a relevé le défi de déploiement avec l'espoir d'assurer la connexion de haute qualité et de haute disponibilité Internet haut débit ainsi que la viabilité économique à long terme . Ces objectifs ont été atteints grâce à une combinaison de planification attentive de déploiement, l'utilisation des ressources topographiques naturelles, l'expansion du réseau des terrains de montagne peu peuplées à la vallée Dherdun plus densément peuplée, et des prix agressifs sur les demandes de bande passante plus élevée. Les plans futurs comprennent l'expansion du réseau, l'« épaississement » de la densité de la clientèle dans les zones existantes et l'enrichissement des tarifs offerts par AirJaldi.

ÉTUDE DE CAS - OPEN INSTITUTE

Technology Initiative Wifi Red Hook & Tidepools

L'initiative Red Hook WiFi est un réseau maillé conçu en collaboration.
Il offre l'accès à Internet à la section de Red Hook à Brooklyn, NY, et sert de plate-forme pour développer des applications et des services locaux. L'initiative de Red Hook a construit le réseau en partenariat avec l'Open Technology Institute, en mettant la conception centrée sur l'humain et l'engagement communautaire au cœur du projet .
La communauté a élargi le réseau de manière significative suite à une catastrophe naturelle en automne 2012.

Les principaux aspects

1. Les principaux du réseau consistent en des organismes communautaires de confiance.
2. Une relation solide avec le fournisseur d'appui technique venant de l'extérieur de la communauté.
3. Un processus de conception communautaire axé sur les besoins locaux et qui renforce l'engagement
4. Prototypage rapide des applications conçues pour le réseau local.

Historique du réseau

Àu début de l'automne 2011, l'Initiative de Red Hook (RHI), un association à but non lucratif de Brooklyn axée sur la création du changement social à travers l'engagement des jeunes a approché l'Open Institute Technology (OIT) pour une collaboration sur un réseau sans fil communautaire. RHI voulait un moyen de communiquer avec les résidents immédiatement autour de son centre communautaire.
Etant initialement incapable de soutenir l'initiative, OIT introduisit Anthony Schloss, coordonnateur des programmes médias RHI à Jonathan Baldwin, un étudiant diplômé du Parsons School of Design qui était en train d'expérimenter le réseau maillé sans fil comme une plate-forme numérique locale.

Figure 1 : CsOTI 1 : Red Hook West Houses - immeubles de logements sociaux

Red Hook est le coin nord-ouest de Brooklyn, qui s'avance dans la baie d'Hudson.
Il est coupé du reste de l'arrondissement par l'autoroute Gowanus, qui transporte le trafic venant des points du sud vers le bas de Manhattan.
Le quartier abrite environ 5000 habitants dans des logements sociaux et d'autres habitants des zones à faible revenu à proximité d'une autoroute, ainsi que d'une section de l'embourgeoisement avec des nombreuses petites entreprises plus près de la mer. Beaucoup de sites industriels, un magasin Ikea et un certain nombre de parcs publics font partie de la zone.

Figure CsOTI 2 : une marche des bureaux RHI à l'autoroute Gowanus

Figure CsOTI 3 : L'autoroute Gowanus qui divise le quartier de Red Hook du reste de Brooklyn .

Le plan initial Wifi de RHI était de fournir un accès sans fil à Internet dans et autour de l'immeuble de RHI, qui se situe près de l'autoroute et les logements sociaux Red Hook. Schloss et Baldwin installèrent un Ubiquiti Nanostation sur le toit et un routeur Linksys à l'intérieur du bâtiment, connecté par Ethernet. Ils relièrent le routeur Linksys au modem du centre. Cette installation donna une opportunité pour prototyper les premières versions d'applications locales Wifi RHI. Lorsque les résidents et les visiteurs de RHI se connectaient au point d'accès sans fil nommé " Red Hook Initiative WiFi ", ils étaient redirigés vers un site Web sur un serveur local.

Sur ce site se trouvait un " Shout Box ", un tableau d'affichage numérique de message local permettant à chacun de laisser un commentaire ou une note derrière et participer au projet.

Figure CsOTI 4 : Premier nœud Wifi de RHI (Ubiquiti Nanostation) installé sur le toit de l'immeuble qui abrite les bureaux RHI .

En Mars 2012, Baldwin et Schloss installerent un Ubiquiti Nanostation supplémentaire sur le toit d'un immeuble donnant sur Coffey Park et la plupart du reste du quartier.
Un résident de l'immeuble ayant des liens sociaux avec RHI fit un don de l'électricité et l'accès sur le toit.
Avec ce point donnant une vue sur le quartier, la possibilité d' un réseau sans fil reliant des espaces publics commença à prendre forme.
Au départ, le point d'accès sans fil Coffey parc n'était pas connecté à l'Internet, mais plutôt à un GuruPlug Server.
Le serveur de base de faible puissance, hébergeait une page web local sur le réseau et un " Shout Box " similaire à celui en cours d'exécution dans RHI.

Figure CsOTI 5 : Etalement du câble pour installer un noeud sur le toit d'un immeuble au nord de Coffey Park.

Figure CsOTI 6 : Noeud installé sur le toit d'un immeuble.

Le Wifi de RHI utilise le firmware sans fil Commotion d'l'OTI sur des routeurs Ubiquiti. Commotion est un outil de communication libre et à source ouverte conçu pour les téléphones mobiles, les ordinateurs et autres appareils sans fil pour créer des réseaux maillés décentralisées. Plus important à noter est que Commotion permet le développement du réseau de se produire de façon dynamique et organique - ainsi la communauté peut décider où et comment le réseau doit se développer. Les réseaux Commotion sont durables sans une connexion à l'Internet, ce qui les rend résistants aux coupures, ils peuvent distribuer l'accès aux applications hébergées sur des serveurs locaux ou sur les routeurs eux-mêmes.

Les logiciels sociaux et la croissance du réseau

Basé sur des recherches sur les réseaux sans fil communautaires à travers le monde, Baldwin avait identifié un besoin de logiciel social qui apporterait une valeur ajoutée et une identité distincte au réseau communautaire sans fil, en particulier pour :

- Susciter l'engagement civique et communautaire en adressant les besoins, les intérêts et la culture locale.
- Encourager la confiance, l'interdépendance et la réciprocité dans toute la communauté.
- Fusionner les espaces communautaires numériques et physiques.
- Veiller à ce que les participants connaissent le maillage réseau /ont le logiciel installé avant qu'une rupture de communication se produise.

Schloss et Baldwin commencèrent à travailler avec les participants dans les programmes médias RHI établis sur un processus de conception collaborative, centrée sur l'homme qui nécessitait la connaissance et les intérêts de la population locale.
Tout au long de la première année, Baldwin et Schloss menèrent des ateliers avec les membres de la communauté pour déterminer les besoins locaux et de recueillir des idées de conception pour Tidepools, développés par Baldwin pour le pilotage sur le réseau RHI. Tidepools est une plate-forme de cartographie locale de source ouverte personnalisable construite en utilisant Javascript, LeafletJS, PHP et MongoDB. Baldwin la conçut pour la communication locale, le placemaking, et l'organisation autour d'événements, les enjeux et les biens communautaires.

Figure CsOTI 7 : atelier pour identifier les besoins locaux pour réseau WiFi RHI. (Photo par Becky Kazan).

Figure CsOTI 8 : carte Tidepools de réseau WiFi RHI .

Les ateliers communautaires produisirent des idées pour des applications locales qui répondraient aux besoins spécifiques identifiés par la communauté. Les besoins identifiés dans les ateliers communautaires étaient:

- Accès à Internet (à la maison, par mobile, et dans les kiosques de quartier).
- Participation communautaire responsable (FAQ, bulletins de bord électroniques, fonctions SMS activées).
- Accès aux ressources (emploi et partage des compétences).
- Système d'information locale (archives historiques, monuments).
- Multi langage (espagnol, arabe et le tagalog).
- Interface amusant pour promouvoir l'exploration.

Pendant l'été 2012, Baldwin rejoint le personnel d'OTI, et OTI emmena une expertise technique supplémentaire à la collaboration avec une expérience pour couvrir la fracture numérique et le développement des infrastructures contrôlées par la communauté.

L'expérience de l'organisation à Detroit et Philadelphie fournit une orientation sur la façon de collaborer avec les communautés qui ont été socialement, géographiquement et technologiquement isolées au sein des cités.

Au cours des mois suivant les premiers tests du réseau local, OTI et RHI se focalisèrent sur la réalisation de trois applications initiales qui utiliseraient la plate-forme Tidepools et s'exécuteraient sur le réseau local sans fil:

- Où est le bus B61 ? - Une application pour accéder en temps réel à des emplacements de bus et les temps d'arrivée en utilisant les données du Metropolitan Transit Authority's BusTime API (*lancé le 9 Octobre 2012*).
- Enquête Stop & Frisk - Une application d'enquête que les résidents peuvent utiliser pour documenter les interactions avec la police à Red Hook pour améliorer la sécurité publique (lancées le 17 Octobre 2012).
- Radio RHI - Une station de radio en ligne, diffusant le contenu produit par le Groupe Radio Jeunesse de RHI (*en développement*) .

Figure CsOTI 9 : Magnet publicité " Où est le Bus B61". L'application Tidepools.

Figure CsOTI 10-11 : interface utilisateur mobile pour l'application " Où est le Bus B61 ? ".

Expansion après la super-tempête Sandy

Le 29 Octobre 2012, la super-tempête Sandy dévasta les bases de Red Hook avec une bonne partie de la région environnante. A la suite des pannes de courant et d'inondations, la nécessité d'accès aux systèmes de communication d'informations sur ce qui se passait et où l'aide était nécessaire était devenu cruciale. Le bâtiment RHI était l'un des rares endroits qui avaient réussi à se maintenir son courant électrique et, en conséquence, le Wifi RHI était resté fonctionnel en dépit de la tempête. Dans les jours qui suivirent la tempête, jusqu'à 300 personnes par jour purent accéder au réseau pour communiquer avec leurs proches, savoir ce qui se passait dans le reste de la ville et demander de l'aide de récupération . " Nous avons immédiatement vu les communications comme l'un des besoins essentiels de la communauté », explique Tony Schloss. " Nous voulions qu'il soit aussi facile que possible pour les personnes de contacter leurs réseaux pour trouver un logement avoir accès à l'information, et rendre compte de leur état de sécurité. " La messagerie texte était le plus largement, et dans certains cas, le seul moyen de communication pour les habitants du quartier après la tempête. Ainsi dans une affaire de quelques jours, OTI développa RHI Status – un plugin SMS to Map pour Tidepools en utilisant l'interface de programmation d'application Tropo (API) pour la gestion des messages SMS et l'API Google géocodage pour la manipulation des adresses en langage naturel. RHI Status fournit un moyen pour les résidents de texter leur emplacement et besoins a numéro de contact, qui associe automatiquement les informations dans Tidepools à une liste de discussion de sorte que les autres membres de la communauté puissent répondre.

Figure CsOTI 12 : Capture d'écran de l'application RHI Status, qui trace des messages SMS sur une carte Tidepools.

Alors la progression du rétablissement, Frank Sanborn, un chargé d'innovation du Federal Emergency Management Administration (FEMA), tendit la main à RHI pour l'extension du réseau à d'autres efforts de soutien au rétablissement dans Red Hook.

Sanborn recruta des volontaires de NYC Mesh and HacDC, un hackerspace de Washington, DC et en coordination avec l'International Technology Disaster Resource Center (ITDRC). OTI avait déjà maintenu un stockage de routeurs d'avant la tempête à RHI. Sous la direction technique d' OTI et fonctionnant selon les objectifs fixés par RHI, l'équipe mit en place une liaison par satellite FEMA sur le toit de RHI et installa un routeur Commotion sur le toit d'une boutique de carrosserie automobile en bas du bloc de RHI.

Auparavant, le propriétaire de la boutique avait été réticent à accueillir un routeur, comme il ne voyait aucun avantage à le faire. Cependant, quand la communauté se mobilisa en réponse à la crise, la boutique de carrosserie automobile devint un maillon essentiel servant de passerelle Internet entre RHI et le routeur donnant sur Coffey Park, qui par ce temps était devenu un point de distribution d'aide important pour Red Hook.

Bien que la liaison satellite avait été offerte pour seulement 30 jours et à condition modeste bande passante, le réseau maillé pouvait distribuer la connexion Internet à des endroits clés où les résidents, les premiers intervenants et les volontaires en avaient le plus besoin.

Quand la communauté se réunit pour répondre à la tempête, la nécessité de développer cette infrastructure de communication résiliente devint claire. Avec le courant et l'eau toujours coupés dans beaucoup d'endroits de Red Hook dans le mois suivant, de nombreuses organisations locales et les résidents vinrent aider. Brooklyn fiber, un fournisseur de services Internet (ISP) local, proposa une passerelle supplémentaire pour le Wifi RHI.

Pour ajouter la passerelle dans la maille, OTI, RHI et Brooklyn fibre installèrent un routeur Ubiquiti à 5 GHz Nanostation Loco utilisant AirOS (pour recevoir le signal de la fibre), et un routeur Ubiquiti Nanostation utilisant Commotion (comme un point d'accès sans fil) au 3ème étage de l' Église de la Visitation presbytérienne sur le côté ouest de Coffey Park. L'église était aussi sans courant à l'époque, mais l' équipe installa une alimentation électrique qui pourrait faire fonctionner les routeurs pendant 12 heures à la fois.

Figure CsOTI 13 : noeud sur le toit. Dans la foulée de Super-tempête Sandy, d'autres membres de la communauté supplémentaires offrirent d'accueillir les noeuds WiFi RHI et un fournisseur d'accès local fournit la connectivité Internet .

Figure CsOTI 14 : noeud sur le toit installé après la Super-tempête Sandy.

Depuis la tempête, le Wifi RHI a supporté environ 100 utilisateurs par semaine, même sans promotion de la ressource. Les données recueillies par Commotion sur les connections DHCP actuelles, ainsi que Google Analytics sur le site d'atterrissage, montrent que les résidents semblent être en train de se connecter en utilisant principalement les appareils Android et Apple iPod Touches. En outre, de nombreux habitants utilisent les postes de travail dans le laboratoire des médias RHI ainsi que le sans-fil disponibles dans RHI. RHI sert à la fois comme point d'ancrage physique et social pour le réseau sans fil, conduisant l'adoption numérique, l'éducation de la région, et coordonnant les efforts de secours .

Figure CsOTI 15 : La cartographie réseau RHI WiFi. Cartographie de base (c) Google Maps 2013 .

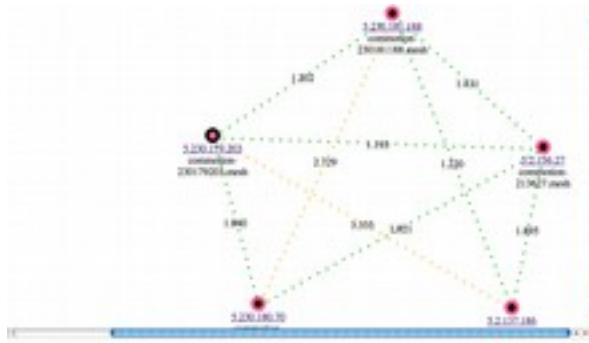


Figure CsOTI 16 : Topologie de maillage réseau vu dans OLSRViz .

Figure CsOTI 17 : Topologie de maillage réseau vu dans OLSRViz .

Durabilité et objectifs futurs

RHI continuera à développer le projet dans le but de soutenir la reprise à l'échelle communautaire de la Super-tempête Sandy. Avec le soutien du financement New York City Workforce Development, RHI et OTI sont en train de lancer un programme de formation en Janvier 2013 pour engager les habitants du quartier dans le maintien et l'extension du réseau sans fil. Suivant le modèle du programme « Digital Stewards" développé par les projets OTI et Allied Media Projects de Detroit, Michigan, le programme permettra de former les jeunes adultes à installer de nouveaux routeurs, de maintenir ceux qui existent déjà, et de promouvoir l'adoption du réseau WiFi RHI tout à travers Red Hook . Les régisseurs numériques RHI vont donner la priorité aux espaces publics supplémentaires pour l'expansion du réseau et travailler avec d'autres résidents dans la conception des nouvelles applications locales. OTI continuera à aider au développement des applications et soutenir l'ingénierie du réseau, en étroite collaboration avec la communauté.

Coût du réseau

Don de travail des résidents locaux et des technologistes.
Soutien institutionnel de RHI et OTI.
Hardware (~ 50 $ à ~ 85 $ pour chaque routeur).
Installation (3-5 heures de travail pour deux personnes par site).
Bande passante (don de RHI, Brooklyn fibre, et la FEMA) .
Programme de formation pour les résidents locaux pour maintenir et développer le réseau dans le cadre d'un programme d'emploi municipal.

Les leçons apprises

Avoir des relations et des nœuds sans fil d'ancrage en place avant une catastrophe facilite le déploiement rapide du réseau à travers:

- les relations déjà établies avec les principaux intervenants de la collectivité.
- Un niveau accru de connaissances technologiques dans la communauté.
- Pré-positionnement des équipements de réseau sans fil dans le quartier.

L'investissement le plus difficile est dans l'organisation initiale et la phase de conception avant qu'une valeur ne soit réalisée. Les applications conçues pour les communautés ajoutent de la valeur à un réseau local, même à petite échelle.

Articles et sites associés

PRESSE :

- New Community – Tech Tool to Help in Sandy's Aftermath
  http://oti.newamerica.net/pressroom/2012/release_new_community_tech_tool_to_help_in_sandys_aftermath

- What Sandy Has Taught Us About Technology, Relief and Resilience
  http://www.forbes.com/sites/deannazandt/2012/11/10/what-sandy-has-taught-us-about-technology-relief-and-resilience

- A Community Wireless Mesh Prototype in Detroit, MI
  http://www.newamerica.net/node/34925

Tidepools

http://tidepools.co
http://www.animalnewyork.com/2012/tidepools-a-social- networktool-in-the-service-of-the-community/
http://wlan-si.net/en/blog/2012/05/26/introducing - tidepools -social-wifi/
http://www.core77.com/blog/social_design/a_communityowned_map_accessed_via_mesh_networks_23319.asp
http://www.jrbaldwin.com/tidepoolswifi/

Stop & Frisk App

http://animalnewyork.com/2012/stop-and-frisk-app-from-red-hook-initiative/
http://www.dnainfo.com/new-york/20121017/red-hook/stop-and-frisk-app-launched-by-red-hook-initiative

Red Hook

http://www.nycgovparks.org/parks/redhookpark/history