5
Matériel réseau

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

Sans fil, avec fil

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

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

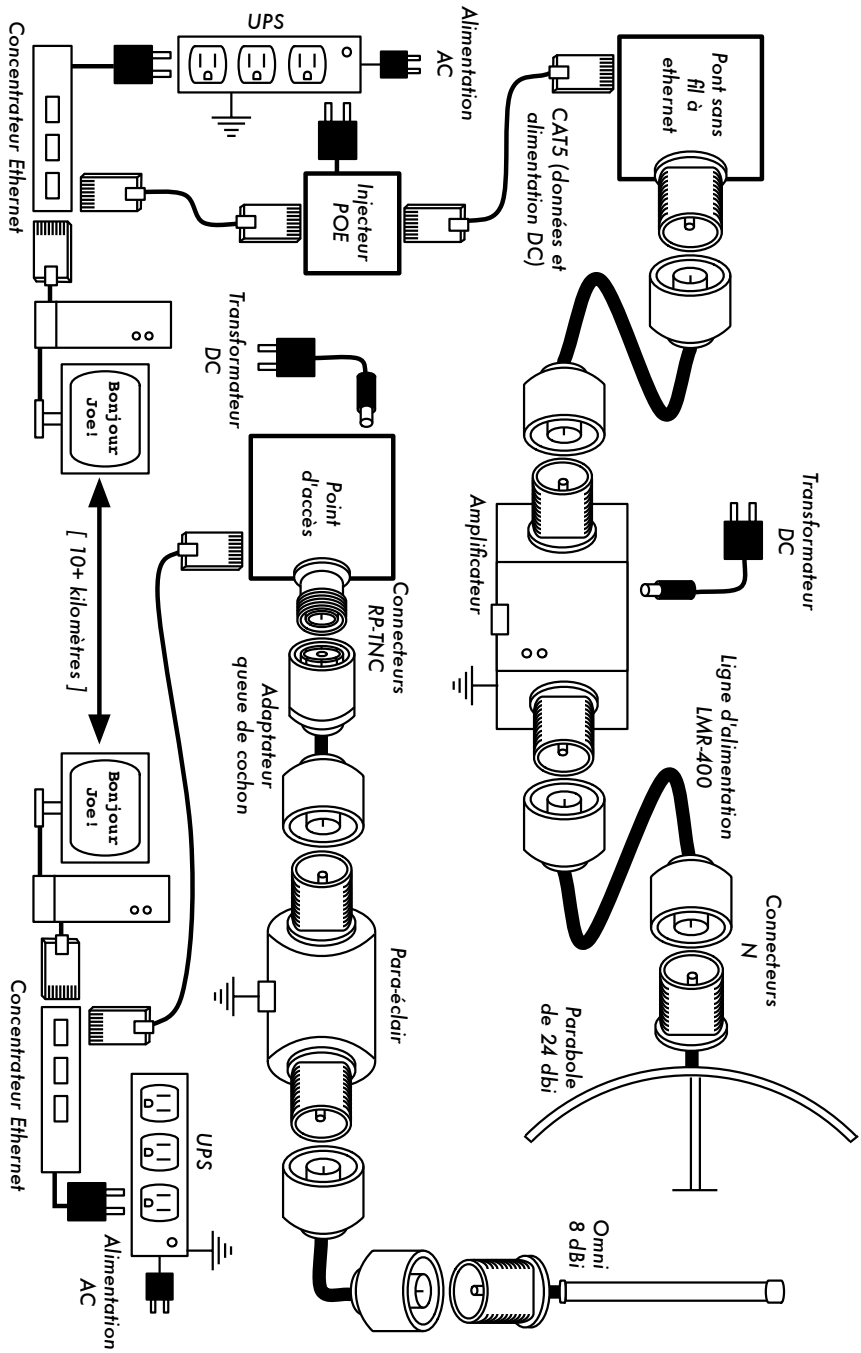

Figure 5.1: Composantes Interconnectées

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

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

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

Choisir des composantes sans fil

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Produits sans fil professionnels

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

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

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

Communications Redline

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

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

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

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

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

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

Alvarion

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

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

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

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

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

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

Communications de données Rad

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

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

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

Systèmes Cisco

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

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

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

En voulez-vous d'autres?

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

Protecteurs professionnels contre la foudre

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Prérequis

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

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

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

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

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

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

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

Scénario 1: Point d'accès avec mascarade

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

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

Configurer les interfaces

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

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

```
# dhclient eth0
```

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

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

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

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

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

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

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

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

Configurer la mascarade dans le noyau de Linux

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

```
# modprobe ipt_MASQUERADE
```

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

```
# iptables -F
```

Activez la fonction NAT entre les deux interfaces:

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

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

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

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

```
ip_forward=no
```

En

```
ip_forward=yes
```

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

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

Ou

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

Configurer la mascarade dans le noyau de Linux

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

```
# modprobe ipt_MASQUERADE
```

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

```
# iptables -F
```

Activez la fonction NAT entre les deux interfaces:

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

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

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

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

```
ip_forward=no
```

En

```
ip_forward=yes
```

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

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

Ou

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

Configurer le serveur DHCP

À présent, nous devrions avoir un point d'accès fonctionnel. Nous pouvons le tester en se connectant au réseau sans fil «*my network*» (mon réseau) à l'aide d'un autre ordinateur en lui donnant une adresse dans la même plage d'adresses que notre interface sans fil sur le serveur (10.0.0.0/24 si vous avez suivi les exemples). Si vous avez activé WEP, soyez sûr d'employer la même clef que celle que vous avez indiquée sur l'AP.

Afin de faciliter la connexion au serveur et de ne pas avoir à saisir manuellement les adresses IP sur les postes clients, nous allons configurer un serveur DHCP pour distribuer automatiquement des adresses aux clients sans fil.

Pour ce faire, nous emploierons le programme dnsmasq. Comme son nom l'indique, il fournit un serveur de cache DNS ainsi qu'un serveur DHCP. Ce programme a été spécialement développé pour être utilisé avec des pare-feu fonctionnant en NAT. Avoir un serveur de cache DNS est particulièrement utile si votre connexion Internet a une grande latence et/ou une faible bande passante, tel que les connexions VSAT ou d'accès par ligne commutée (*dial-up)*. Ceci signifie que plusieurs requêtes DNS peuvent être résolues localement, éliminant une grande partie du trafic sur Internet tout en permettant une connexion beaucoup plus rapide pour les utilisateurs.

Installez dnsmasq avec votre gestionnaire de paquetage. Si dnsmasq n'est pas disponible sous forme de paquet, téléchargez le code source et installez-le manuellement. Il est disponible à: *http://thekelleys.org.uk/dnsmasq/doc.html*.

Afin d'activer dnsmasq nous n'avons qu'à taper quelques lignes du fichier de configuration de dnsmasq, **`/etc/dnsmasq.conf`**.

Le fichier de configuration est bien documenté, et propose de nombreuses options pour différents types de configuration. Pour activer le serveur DHCP nous devons éliminer les commentaires et/ou taper deux lignes.

Trouvez les lignes qui commencent par:

```
interface=
```

...et assurez-vous qu'elles stipulent:

```
interface=wlan0
```

...changez wlan0 par le nom de votre interface sans fil. Puis, trouvez les lignes qui commencent par:

```
#dhcp-range=
```

Éliminez le commentaire de la ligne et éditez-la pour y mettre les adresses que vous utilisez, par exemple:

```
dhcp-range=10.0.0.10,10.0.0.110,255.255.255.0,6h
```

Puis, sauvegardez le fichier et lancez dnsmasq:

```
# /etc/init.d/dnsmasq start
```

Vous devriez à présent pouvoir vous connecter au serveur comme point d'accès et d'obtenir une adresse IP grâce à DHCP. Ceci doit vous permettre de vous connecter à Internet à travers le serveur.

Ajouter plus de sécurité: configurer un pare-feu

Une fois qu'il est installé et testé, vous pouvez ajouter des règles supplémentaires de pare-feu en utilisant n'importe quel outil pare-feu inclus dans votre distribution. Voici quelques applications qui vous permettront de configurer votre pare-feu:

- ***firestarter*** – un client graphique pour *Gnome* qui requiert que votre serveur fonctionne sur *Gnome*
- ***knetfilter*** – un client graphique pour *KDE* qui requiert que votre serveur fonctionne sur *KDE*
- ***Shorewall*** – un ensemble de programmes et de fichiers de configuration qui rendront plus facile la configuration du pare-feu iptables. Il y aussi d'autres interfaces pour *shorewall*, tel que *webmin-shorewall*
- ***fwbuilder*** - un puissant outil graphique, mais un peu complexe qui vous permettra de créer des règles iptables sur un autre ordinateur que votre serveur pour ensuite les transférer à celui-ci. Ceci n'exige pas un bureau graphique sur le serveur et il s'agit d'une bonne option pour la sécurité.

Une fois que tout est correctement configuré, assurez-vous que toutes les configurations sont reflétées dans le programme de démarrage du système. De cette façon, vous ne perdrez pas vos changements si l'ordinateur doit être redémarré.

Scénario 2: Faire du point d'accès un pont transparent

Ce scénario peut être employé pour un répéteur de deux radios et pour un point d'accès connecté à Ethernet. Nous utilisons un pont au lieu de routeur lorsque nous voulons que les deux interfaces sur ce point d'accès partagent le même sous réseau. Ceci peut être particulièrement utile pour les réseaux

à multiples points d'accès où nous préférons avoir un seul pare-feu central et peut-être un serveur d'authentification. Puisque tous les clients partagent le même sous-réseau, ils peuvent facilement travailler avec un seul serveur DHCP et un pare-feu sans avoir besoin de relai DHCP.

Par exemple, vous pourriez installer un serveur selon le premier scénario, mais utiliser deux interfaces câblées Ethernet au lieu d'une câblée et d'une sans fil. Une interface serait votre connexion Internet et l'autre se connecterait à un commutateur (*switch*). Connectez ensuite autant de points d'accès que vous le désirez au même commutateur, configurez-les en tant que ponts transparents et tout le monde aura à traverser le même pare-feu et utiliser le même serveur DHCP.

Cependant, la simplicité des ponts suppose un coût au niveau de l'efficacité. Comme tous les clients partagent le même sous-réseau, le trafic sera répété dans tout le réseau. Ceci ne cause habituellement aucun désavantage pour les petits réseaux, mais à mesure que le nombre de clients augmente, une plus grande quantité de bande passante sans fil sera gaspillée pour le trafic de transmission du réseau.

Configuration initiale

L'installation initiale d'un point d'accès configuré en tant que pont est semblable à celle d'un point d'accès avec mascarade mais sans la nécessité de dnsmasq. Suivez les instructions initiales d'installation de l'exemple précédent.

En outre, le paquet ***bridge-utils*** est exigé pour installer un pont. Ce paquet existe pour Ubuntu et d'autres distributions Debian, ainsi que pour Fedora Core. Assurez-vous qu'il soit installé et que la commande **`brctl`** soit disponible avant de procéder.

Configurer les interfaces

Sur Ubuntu ou Debian la configuration des interfaces se réalise en éditant le fichier: **`/etc/network/interfaces`**.

Ajoutez une section comme la suivante, mais changez le nom des interfaces et des adresses IP en conséquence. L'adresse IP et le masque réseau doivent être les mêmes que ceux de votre réseau existant. Cet exemple suppose que vous construisez un répéteur sans fil avec deux interfaces sans fil, wlan0 et wlan1. Dans cet exemple, l'interface wlan0 sera un client pour le réseau nommé "office" et wlan1 créera un réseau appelé «repeater».

Ajouter les commandes suivantes à: **`/etc/network/interfaces`**

```
auto br0
iface br0 inet static
  address 192.168.1.2
  network 192.168.1.0
  netmask 255.255.255.0
  broadcast 192.168.1.255
  gateway 192.168.1.1
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid “office” mode Managed
  pre-up iwconfig wlan1 essid “repeater” mode Master
  bridge_ports wlan0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
```

Commentez toute autre ligne qui fait référence à wlan0 ou à wlan1 pour vous assurer qu'elles n'interfèrent pas avec votre configuration.

La syntaxe pour configurer des ponts par l'intermédiaire du fichier **interfaces** est spécifique aux distributions Debian, et les détails pour installer le pont sont fournis par un couple de scripts: **/etc/network/if-pre-up.d/bridge** et **/etc/network/if-post-down.d/bridge**.

La documentation pour ces programmes est disponible dans: **/usr/share/doc/bridge-utils/**.

Si ces programmes n'existent pas sur votre distribution (telle que Fedora Core), voici une configuration alternative pour **/etc/network/interfaces** qui donnera le même résultat mais avec un peu plus de tracas:

```
iface br0 inet static
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid “office” mode Managed
  pre-up iwconfig wlan1 essid “repeater” mode Master
  pre-up brctl addbr br0
  pre-up brctl addif br0 wlan0
  pre-up brctl addif br0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
  post-down brctl delif br0 wlan0
  post-down brctl delif br0 wlan1
  post-down brctl delbr br0
```

Mise en marche du pont

Une fois que le pont est défini en tant qu'interface, il suffit de taper la commande suivante pour le mettre en marche:

```
# ifup -v br0
```

Le “-v” signifie *verbose output* et vous informera de ce qui se passe.

Sur Fedora Core (c.-à-d. les distributions non-Debian) vous aurez quand même à donner une adresse IP à votre pont et à ajouter une route par défaut au reste du réseau:

```
#ifconfig br0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
#route add default gw 192.168.1.1
```

Vous devriez maintenant être en mesure de connecter un ordinateur portable sans fil à ce nouveau point d’accès et de le connecter à Internet (ou au moins au reste de votre réseau) à travers cet ordinateur.

Si vous désirez avoir plus d’informations sur votre pont et ce qu’il fait, jetez un coup d’œil à la commande brctl. Essayez par exemple la commande suivante:

```
# brctl show br0
```

Ceci devrait vous donner de l’information sur ce que fait votre pont.

Scénario 1 & 2: la manière facile

Au lieu d'installer votre ordinateur comme point d'accès à partir de zéro, vous pouvez utiliser une distribution Linux créée à cette fin. Ces distributions peuvent rendre le travail aussi simple que de démarrer votre ordinateur équipé d’une interface sans fil à partir d’un CD. Pour plus d’information, voyez la section suivante, « les systèmes d'exploitation conviviaux avec la technologie sans fil ».

Comme vous pouvez le voir, il est facile de créer un point d'accès à partir d’un routeur standard Linux. Utiliser Linux vous donne sensiblement plus de contrôle sur la façon dont les paquets sont routés à travers votre réseau et propose des options qui ne sont pas disponibles sur un équipement pour consommateurs.

Par exemple, vous pourriez commencer par l'un ou l'autre des deux exemples ci-dessus et mettre en application un réseau sans fil privé où les utilisateurs sont authentifiés en utilisant un navigateur web standard. En utilisant un portail captif tel que *Chillispot*, les identifications des utilisateurs peuvent être vérifiées sur une base de données existante (par exemple, un serveur de domaine Windows accessible via RADIUS). Cette configuration peut permettre un accès préférentiel aux utilisateurs enregistrés dans la base de données, tout en fournissant un niveau très limité d'accès pour le grand public.

Une autre application populaire est la vente de temps de connexion. Dans ce modèle, les utilisateurs doivent acheter un ticket avant d'accéder au réseau. Ce ticket fournit un mot de passe qui est valide pour une quantité de temps limitée (en général un jour). Quand le ticket expire, l'utilisateur doit en acheter d'autres. Ce système de vente de tickets est disponible sur les équipements de réseau commercial relativement cher, mais peut être mis en place en utilisant des logiciels libres tel que Chillispot et phpMyPrePaid. Nous verrons plus en détail la technologie de portails captifs et du système de tickets dans la section **Authentification** du chapitre six.

Systèmes d'exploitation conviviaux avec la technologie sans fil

Il y a un certain nombre de systèmes d'exploitation libres qui fournissent des outils utiles pour travailler avec les réseaux sans fil. Ceux-ci ont été conçus pour être employés avec des ordinateurs recyclés ou tout autre matériel de gestion de réseau (plutôt que sur un ordinateur portable ou un serveur) et sont bien configurés et optimisés pour construire des réseaux sans fil. Certains de ces projets incluent:

- **Freifunk**. Basé sur le projet OpenWRT (*http://openwrt.org/*), le progiciel Freifunk offre un support OLSR facile pour les points d'accès de consommateurs basés sur MIPS, tel que les Linksys WRT54G / WRT54GS / WAP54G, Siemens SE505, et autres. En flashant simplement (c.-à-d. réécrire sa mémoire flash) un de ces APs avec le progiciel Freifunk, vous pouvez rapidement construire une maille OLSR autonome. Freifunk n'est actuellement pas disponible pour l'architecture x86. Il est maintenu par Sven Ola du groupe sans fil Freifunk à Berlin. Vous pouvez télécharger les *firmware* à l'adresse suivante: *http://www.freifunk.net/wiki/FreifunkFirmware*.
- **Metrix Pebble**. Le projet Pebble Linux a été lancé en 2002 par Terry Schmidt du groupe *NYCwireless*. C'était à l'origine une version dépouillée de la distribution Debian Linux qui inclut un pare-feu sans fil, des outils de gestion de réseau et de routage. Depuis 2004, *Metrix Communication* a prolongé le projet Pebble pour y inclure des pilotes mis à jour, de la surveillance de bande passante et un outil de configuration web. Le but du Pebble Metrix est de fournir une plateforme complète pour le développement sans fil. Il fonctionne sur les architectures x86 avec au moins 64MB de mémoire flash ou de disque dur. Vous pouvez le télécharger à l'adresse suivante: *http://metrix.net/metrix/howto/metrix-pebble.html*.
- **m0n0wall**. Basé sur FreeBSD, m0n0wall est un très petit paquet mais pare-feu complet qui fournit des services AP. Il se configure à partir d'une interface web et le système complet de configuration est stocké dans un simple fichier XML. Sa taille minuscule (moins de 6 MB) le rend attrayant pour une utilisation dans les systèmes embarqués très petits. Son but est

de fournir un pare-feu sécuritaire et, en tant que tel, il n'inclut pas d'outils utilisateurs (il n'est pas possible de se connecter à l'ordinateur en dehors du réseau). En dépit de cette limitation, c'est un choix populaire pour les équipements sans fil, en particulier ceux qui ont une certaine connaissance de FreeBSD. Vous pouvez le télécharger sur: *http://www.m0n0.ch/*.

Toutes ces distributions sont conçues pour s'adapter à des ordinateurs à stockage limité. Si vous employez un disque flash de grande capacité ou un disque dur, vous pouvez certainement installer un OS plus complet (tel qu'Ubuntu ou Debian) et utiliser l'ordinateur comme routeur ou point d'accès. De toute façon, vous devrez probablement investir une quantité non négligeable de temps pour vous assurer que tous les outils nécessaires sont inclus, afin de ne pas installer des paquets inutiles. En employant un de ces projets comme point de départ pour créer un noeud sans fil, vous économiserez considérablement de temps et d'efforts.

Le Linksys WRT54G

Un des points d'accès actuellement les plus populaires chez les consommateurs est le Linksys WRT54G. Ce point d'accès comporte deux connecteurs externes d'antenne RP-TNC, un commutateur Ethernet quatre ports et une radio 802.11b/g. Il se configure à partir d'une simple interface web. Même s'il n'est pas conçu comme solution extérieure, il peut être installé dans une boîte ou un tuyau en plastique pour un coût relativement peu élevé. Actuellement, le WRT54G se vend environ $60.

En 2003, des bidouilleurs se sont rendus compte que le micrologiciel (*firmware*) qui se vendait avec le WRT54G était en fait une version de Linux. Ceci a entraîné un vif intérêt pour la création de *firmwares alternatifs* qui peuvent augmenter de manière significative les possibilités du routeur. Certains de ces nouveaux *firmwares* incluent un support du mode radio client, des portails captifs et réseau maillé (*mesh*). Deux *firmwares* alternatifs populaires pour le WRT54G sont OpenWRT (*http://openwrt.org/*) et Freifunk (*http://www.freifunk.net/wiki/FreifunkFirmware*).

Malheureusement, en automne 2005, Linksys a lancé la version 5 du WRT54G. Cette nouvelle version est équipée de beaucoup moins de mémoire RAM et de stockage flash sur la carte mère, ce qui rend presque impossible le fonctionnement de Linux (de fait, il fonctionne avec VxWorks, un système d'exploitation beaucoup plus petit dont la personnalisation est plus compliquée). Puisque le WRT54G v5 ne peut pas faire fonctionner les *firmwares* Linux personnalisés, il devient une alternative moins attrayante pour les constructeurs de réseau. Linksys a également sorti le WRT54GL, qui est essentiellement le WRT54G v4 (qui fonctionne avec Linux) à un prix légèrement plus élevé.

D'autres points d'accès Linksys fonctionnent également sous Linux, y compris le WRT54GS et le WAP54G. Même si ceux-ci ont également des prix relativement bas, les caractéristiques de l'équipement peuvent changer à tout moment. Il est difficile de savoir de quelle version du matériel il s'agit sans ouvrir l'emballage, il est de fait risqué de les acheter dans un magasin et pratiquement impossible de passer une commande en ligne. Même si le WRT54GL fonctionne sous Linux, Linksys a clairement dit qu'il ne compte pas vendre ce modèle en grand volume et est resté imprécis sur la durée durant laquelle ce matériel sera proposé à la vente.

Si vous pouvez vous procurer une version précédente de WRT54Gs ou WRT54GLs, ceux-ci sont des routeurs maniables et peu coûteux. Avec des *firmwares* personnalisés, ils peuvent être configurés pour fonctionner en tant que nœud d'un réseau maillé ou en mode client et fonctionnent très bien comme solution bon marché côté client. Même si le nouveau modèle v5 fonctionnera en tant que point d'accès, il ne peut être configuré comme client et a des évaluations de performances partagées comparées au v4 et aux autres modèles précédents.

Pour plus d'information visitez un de ces sites Web:

- *http://linksysinfo.org/*
- *http://seattlewireless.net/index.cgi/LinksysWrt54g*