3
Conception d'un réseau

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

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

Conception du réseau physique

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

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

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

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

Point à point

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

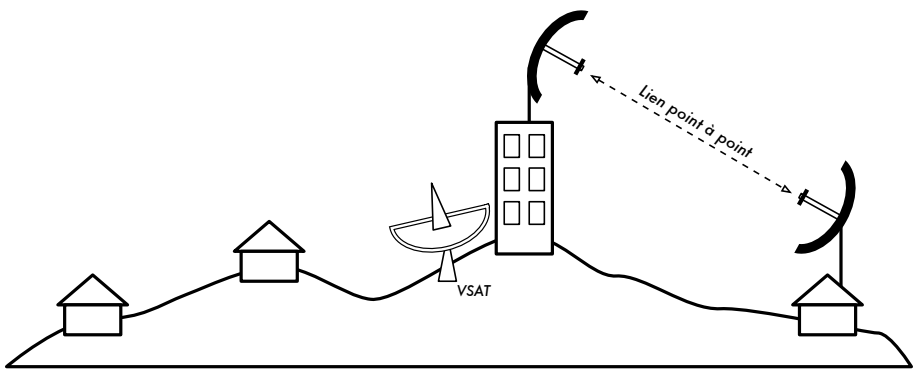

Figure 3.1: Une liaison point à point permet à un site distant de partager une connexion centrale à Internet.

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

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

Point à multipoint

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

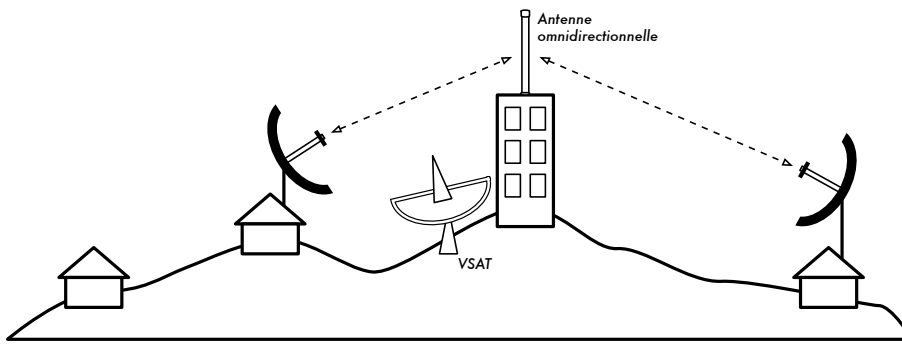

Figure 3.2: Le VSAT central est maintenant partagé par plusieurs sites distants grâce à une antenne omnidirectionnelle. Les trois sites peuvent aussi communiquer directement à des vitesses beaucoup plus rapides que le VSAT.

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

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

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

Multipoint à multipoint

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

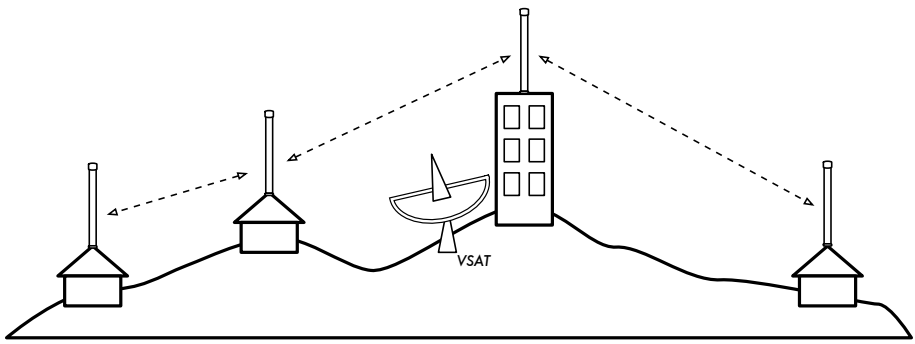

Figure 3.3: Un réseau multipoint à multipoint maillé. Chaque point peut accéder à un autre à de très grandes vitesses ou utiliser la connexion centrale VSAT pour avoir accès à Internet.

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

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

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

Utiliser la technologie appropriée

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

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

Le réseau logique

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

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

Le modèle TCP/IP

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

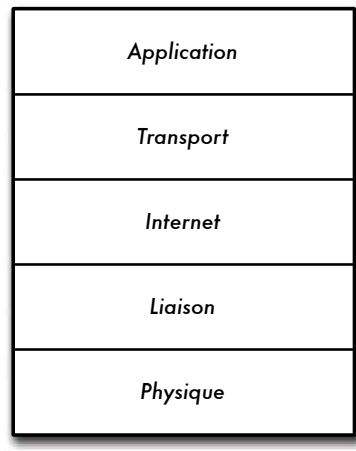

Figure 3.4: Le modèle de réseautage TCP/IP.

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

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

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

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

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

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

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

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

802.11 Réseaux sans fil

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

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

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

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

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

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

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

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

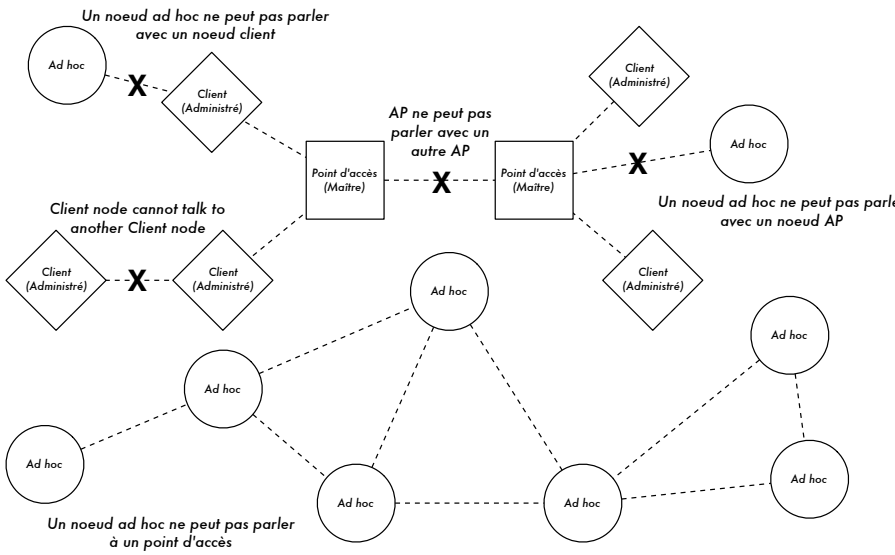

Figure 3.5: AP, Clients et nœuds Ad Hoc.

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

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

Réseautage Internet

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

Adresses IP

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

Adressage réseau

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

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

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

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

Routage

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

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

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

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

---

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

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

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

«Forwarding»

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

```
Destination     Passerelle      Masque          Drapeaux  Métrique  Interface

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

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

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

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

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

Tout rassembler

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

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

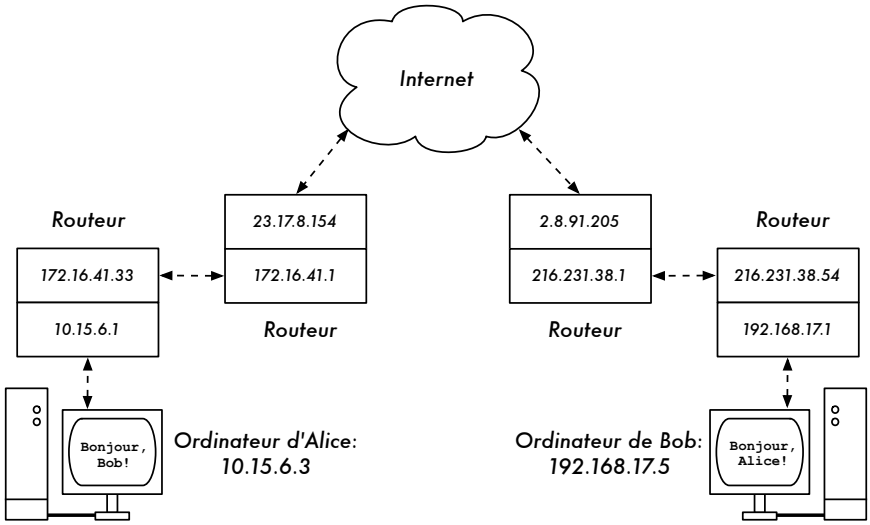

Figure 3.6: Réseautage Internet. Chaque segment de réseau a un routeur avec deux adresses IP, réalisant un «lien local» à deux réseaux différents. Les paquets sont expédiés entre les routeurs jusqu'à ce qu'ils atteignent leur destination finale.

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

Réseautage maillé avec OLSR

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

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

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

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

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

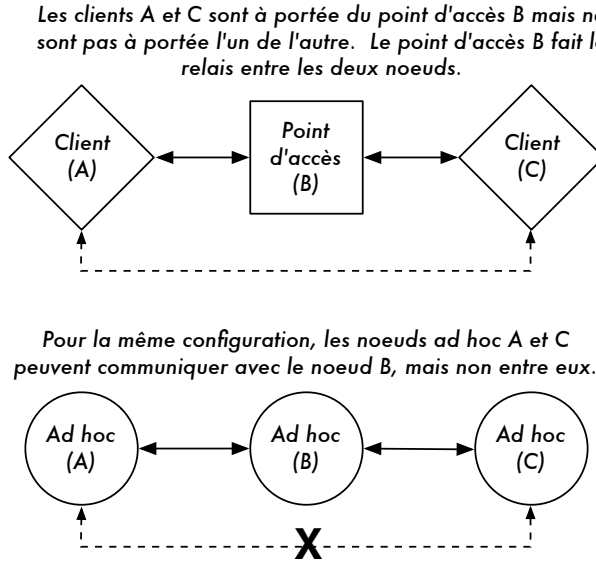

Figure 3.7: Le point d'accès B va transmettre le trafic entre les clients A et C. En mode Ad hoc, le nœud B ne transmettra pas le trafic entre A et C par défaut.

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

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

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

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

Routage maillé avec olsrd

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

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

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

Théorie

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

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

Mécanisme

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

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

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

Pratique

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Une configuration olsrd simple

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

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

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

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

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

```
olsrd -d 2
```

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

Le résultat devrait ressembler à ceci:

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

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

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

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

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

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

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

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

Utiliser OLSR sur Ethernet et sur des interfaces multiples

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

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

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

Plug-in

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

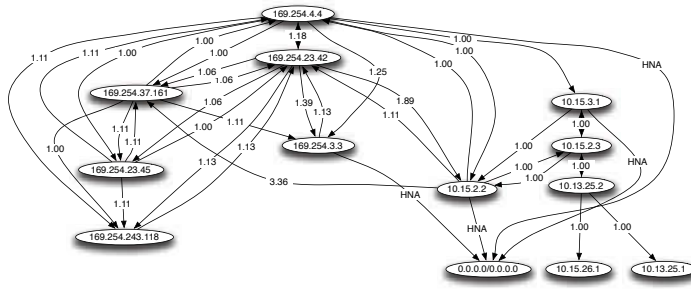

Figure 3.8: Une topologie réseau OLSR automatiquement générée.

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

Installer le plugin dot_draw

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

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

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

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

```
telnet localhost 2004
```

Après un moment un texte devrait apparaître.

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

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

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

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

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

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

Dépannage

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

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

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

Amusez-vous bien!

Évaluation de la capacité

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

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

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

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

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

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

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

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

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

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

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

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

Planification des liens

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

Calculer le potentiel de puissance

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

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

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

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

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

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

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

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

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

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

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

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

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

Où n est l'exposant mentionné.

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

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

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

Soustraire la perte de trajet du Gain Total:

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

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

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

Exemple de calcul du potentiel de puissance

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

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

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

  40 dB = Gain total
```

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

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

Soustraire la perte de trajet du gain total

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

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

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

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

  35 dB = Gain Total
```

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

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

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

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

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

Tables pour calculer le potentiel de puissance

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

Perte d'espace libre à 2,4GHz

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

Gain d'antenne:

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

Pertes:

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

potentiel de puissance pour la Radio 1 ➜ Radio 2:

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

potentiel de puissance pour la Radio 2 ➜ Radio 1:

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

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

Logiciel de planification de lien

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

Conception interactive CGI

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

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

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

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

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

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

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

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

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

RadioMobile

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

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

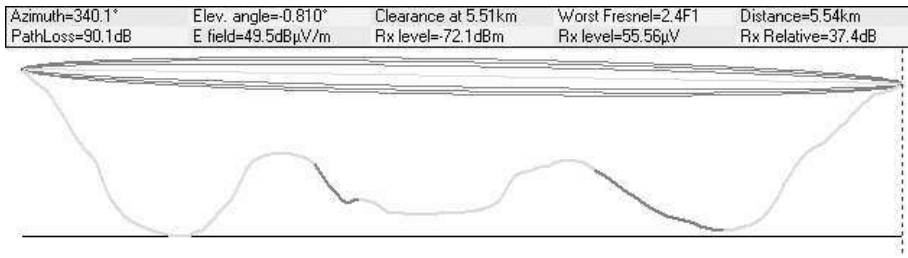

Figure 3.9: Viabilité du lien, incluant la zone Fresnel et une estimation de la ligne de vue, en utilisant RadioMobile.

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

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

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

RadioMobile sous Linux

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

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

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

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

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

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

```
# wine RMWDLX.exe
```

Vous devriez voir fonctionner RadioMobile sur votre session XWindows.

Éviter le bruit

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

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

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

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

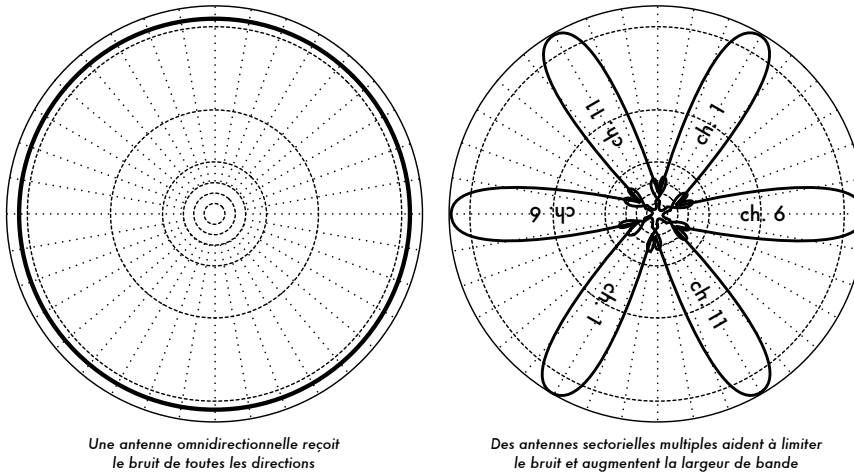

Figure 3.10: Une seule antenne omnidirectionnelle vs multiples antennes sectorielles.

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

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

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

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

Répéteurs

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

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

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

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

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

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

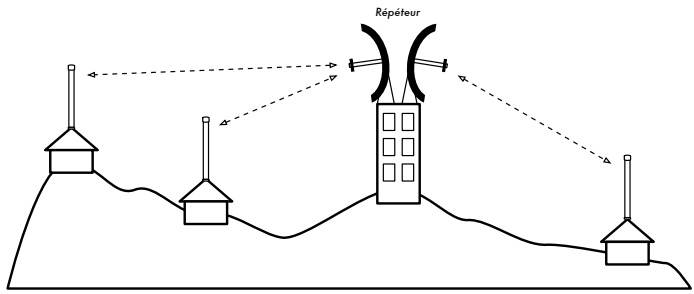

Figure 3.11: Le répéteur transmet des paquets dans l'air entre des nœuds qui n'ont pas de ligne de vue directe.

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

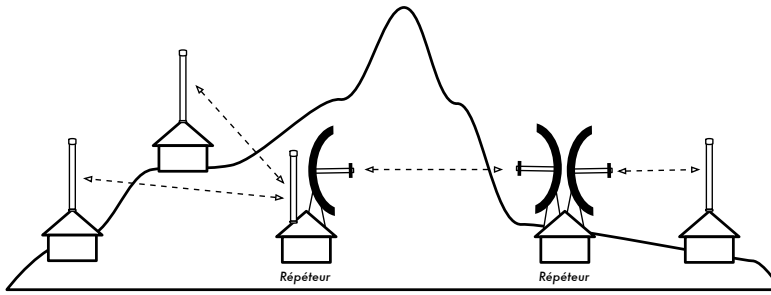

Figure 3.12: Il n'y avait pas d'énergie disponible au dessus de la colline, mais ceci a été résout en employant de multiples de répéteurs situés autour de la base.

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

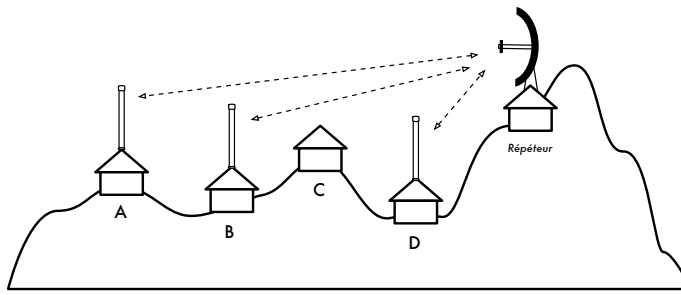

Figure 3.13: L'emplacement D ne peut pas voir les emplacements A ou B, car l'emplacement C est dans le chemin et n'est pas intéressé à héberger un nœud. En installant un répéteur plus haut, les nœuds A, B et D peuvent communiquer. Notez qu'en fait le trafic du nœud D voyage plus loin que celui du reste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

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

Optimisation du trafic

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

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

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

Cache Web

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

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

Produits de serveur Proxy

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

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

Empêcher les usagers de contourner le serveur Proxy

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

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

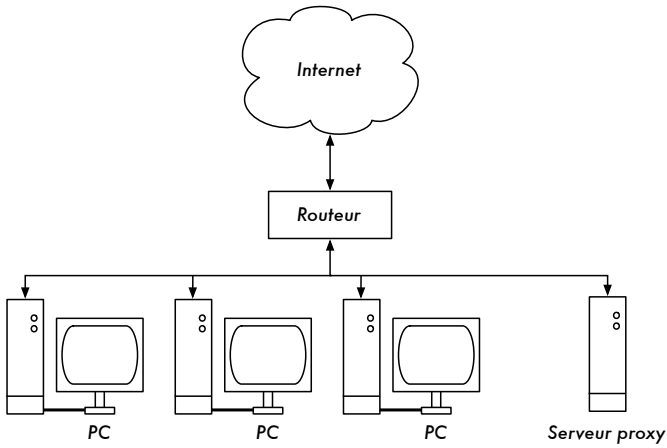

Figure 3.14: Ce réseau repose sur la confiance que ses usagers configureront correctement leurs ordinateurs pour utiliser le serveur mandataire.

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

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

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

Pare-feu

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

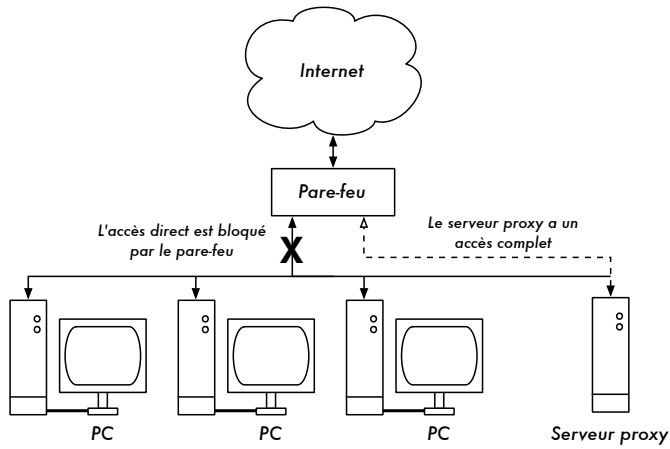

Figure 3.15: Le pare-feu empêche les ordinateurs d'accéder directement à Internet, mais permet l'accès via le serveur proxy.

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

Deux cartes réseau

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

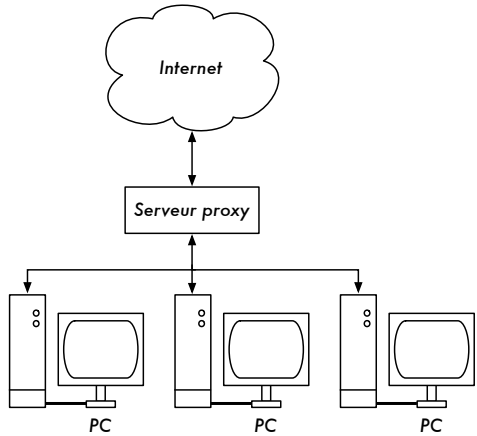

Figure 3.16: Le seul chemin vers Internet est à travers le serveur proxy .

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

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

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

Routage réglementé

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

Sites Web miroirs

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

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

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

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

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

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

Pré-actualiser le site dans la cache en utilisant wget

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

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

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

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

Explication:

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

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

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

Hiérarchies de cache

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

Spécifications proxy

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

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

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

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

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

Cache de DNS et optimisation

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

Serveur Bind (*named*)

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

```
apt-get install bind9
```

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

dnsmasq

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

Windows NT

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

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

Windows 2000

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

DNS divisé et serveur miroir

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

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

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

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

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

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

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

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

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

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

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

Optimisation des liens Internet

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

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

Facteurs TCP/IP qui affectent une connexion satellite

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

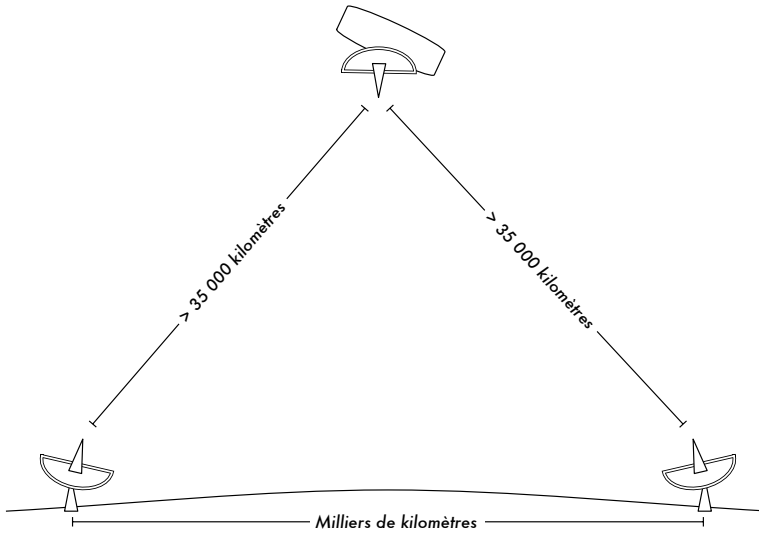

Figure 3.17: Étant donnée la vitesse de la lumière et les longues distances impliquées, la confirmation de réception d'un seul paquet «ping» peut prendre plus de 520 ms sur un lien VSAT.

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

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

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

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

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

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

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

Produit délai-bande passante élevé

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

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

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

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

Les erreurs de transmission

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

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

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

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

Considérations pour les universités

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

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

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

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

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