# 8
# Dépannage

La façon dont vous établissez l'infrastructure de soutien pour votre réseau est aussi importante que le type d'équipement que vous employez. Contrairement aux connexions câblées, les problèmes avec un réseau sans fil sont souvent invisibles et peuvent demander plus de compétence et de temps afin de les diagnostiquer et de les résoudre. L'interférence, le vent et de nouvelles obstructions physiques peuvent rendre défectueux un réseau qui fonctionnait depuis longtemps. Ce chapitre détaille une série de stratégies pour vous aider à créer une équipe qui peut soutenir votre réseau efficacement.

## *Créer votre équipe*

Chaque village, compagnie ou famille a des individus qui sont intrigués par la technologie. Ce sont, entre autres, ceux que l'on retrouve à bricoler un câble, à réparer une télévision brisée ou à souder un nouveau morceau à une bicyclette. Ces personnes prendront de l'intérêt au sujet de votre réseau et voudront en apprendre autant que possible. Bien que ces personnes soient des ressources de valeur inestimable, vous devez éviter de former et donner toute la connaissance spécialisée du réseau sans fil à une seule personne. Si cette personne est votre unique spécialiste et perd l'intérêt ou trouve un travail mieux rémunéré ailleurs, elle partira en emportant toute la connaissance avec elle.

Il peut également y avoir beaucoup d'adolescents jeunes et ambitieux ou de jeunes adultes qui seront intéressés et auront le temps d'écouter, d'aider et de se renseigner sur le réseau. Encore une fois, ces personnes peuvent être très utiles et peuvent apprendre rapidement, mais l'équipe de projet doit concentrer son attention sur ceux qui sont le mieux placés pour soutenir le réseau dans les prochains mois et années. Les jeunes adultes et les adolescents iront à l'université ou trouveront un emploi, particulièrement les jeunes

ambitieux qui sont ceux qui tendent à vouloir être impliqués. Ces jeunes ont également peu d'influence dans la communauté où un individu plus âgé est susceptible d'être plus en mesure de prendre les décisions qui affectent directement le réseau dans l'ensemble. Quoique ces individus pourraient avoir moins de temps pour apprendre et pourraient sembler être moins intéressés, leur participation et une formation appropriée au sujet du système peuvent s'avérer essentiels.

Par conséquent, une stratégie principale lorsque nous créons une équipe de soutien est d'équilibrer et de distribuer la connaissance parmi ceux qui sont mieux placés pour soutenir le réseau à long terme. Vous devriez impliquer les jeunes, mais ne les laissez pas capitaliser à eux seuls l'utilisation ou la connaissance de ces systèmes. Trouvez et formez des personnes qui sont engagées au sein de la communauté, qui ont des racines dans la communauté et qui peuvent être motivées. Une stratégie complémentaire est de compartimenter les fonctions et les tâches, et de documenter toutes les méthodologies et procédures. De cette façon, les gens peuvent être formés facilement et être remplacés avec peu d'effort.

Par exemple dans un projet, l'équipe de formation a choisi un jeune diplômé d'université intelligent qui était revenu à son village. Il était très motivé et a appris rapidement. Comme il a appris si rapidement, on lui a enseigné plus que ce qui avait été prévu, en le rendant ainsi capable de traiter une variété de problèmes, de réparer un ordinateur à refaire le câblage Ethernet. Malheureusement, deux mois après le lancement du projet, il a reçu une offre d'emploi du gouvernement et a quitté la communauté. Même un meilleur salaire n'aurait pas pu le convaincre de rester puisque la perspective d'un travail stable au gouvernement était trop attirante. Toute la connaissance au sujet du réseau et comment le soutenir est partie avec lui. L'équipe de formation a dû revenir sur place pour recommencer une formation. La prochaine stratégie fut de diviser les fonctions et de former des personnes qui seraient enracinées dans la communauté de manière permanente: des personnes qui avaient une maison, des enfants et qui avaient déjà un emploi. La formation de trois personnes prend trois fois plus de temps que le temps dépensé dans la formation du jeune diplômé d'université, mais la communauté pourra retenir cette connaissance beaucoup plus longtemps.

Avec ceci nous voulons dire que le fait de choisir par vous-même la personne qui devrait être impliquée dans votre projet, n'est peut être pas la meilleure approche. Il est souvent mieux de trouver une organisation locale ou un administrateur local et de travailler avec eux afin de trouver l'équipe technique adéquate. Les valeurs, l'histoire, la politique locale et beaucoup d'autres facteurs seront importants pour eux, alors que complètement inaccessibles pour les personnes qui ne sont pas de cette communauté. La meilleure approche est de préparer votre partenaire local, lui fournir des critères cohérents, de vous assurer qu'il les comprend et d'établir des limites strictes.

Ces limites devraient tenir compte du népotisme et du patronage, tout en considérant la situation locale. Il peut être impossible de dire que vous ne pouvez pas employer un parent, mais il est mieux de fournir des moyens de contrôle et d'équilibre. Lorsqu'un candidat est un parent, il devrait y avoir des critères clairs et une deuxième autorité qui appuie cette candidature. Il est également important que ce soit le partenaire local qui ait cette autorité et non les organisateurs du projet, ce qui pourrait compromettre leur capacité de gestion. Ils seront mieux placés pour juger qui travaillera mieux avec eux. S'ils sont bien préparés dans ce processus, alors vos conditions devraient être satisfaites.

Le dépannage et le support de la technologie est un art abstrait. La première fois que vous regardez une peinture abstraite, celle-ci peut ne représenter pour vous qu'un ensemble d'éclaboussures aléatoires de peinture. Après avoir réfléchi sur la composition pendant un certain temps, vous pourriez commencer à apprécier le travail dans l'ensemble et la cohérence « invisible » peut devenir très réelle. Un débutant qui regarde un réseau sans fil peut voir les antennes, les câbles et les ordinateurs, mais il peut avoir besoin d'un certain temps pour apprécier le but du réseau « invisible ». Dans des secteurs ruraux, les personnes de la localité ont souvent besoin d'un grand travail de compréhension avant qu'ils n'apprécient un réseau invisible qui a été installé dans leur village. Par conséquent, une approche par étapes est nécessaire pour aider ces personnes à soutenir des systèmes technologiques. La meilleure méthode est la participation. Une fois que les participants sont choisis et sont engagés sur le projet, faites-les participer autant que possible. Laissez-les « conduire ». Donnez-leur le sertisseur ou le clavier et montrez-leur comment effectuer le travail. Même si vous n'avez pas le temps d'expliquer chaque détail et même si cela est plus long, ils doivent être impliqués physiquement et voir non seulement ce qui a été fait afin de bien apprécier le travail effectué.

On enseigne la méthode scientifique dans pratiquement toutes les écoles occidentales. Plusieurs personnes l'apprennent avant même d'entrer dans une classe de science de secondaire. Présentée simplement, elle consiste à prendre un ensemble de variables puis de les éliminer lentement à travers des tests binaires jusqu'à ce qu'il ne reste qu'une ou seulement quelques possibilités. Avec ces possibilités à l'esprit, vous pouvez compléter l'expérience. Vous devez alors examiner l'expérience pour voir si sa portée est semblable au résultat prévu. Si elle ne l'est pas, vous devez recalculez votre résultat prévu et réessayer. Le villageois rural typique a peut-être une première connaissance du concept, mais n'aura probablement pas eu l'occasion de résoudre des problèmes complexes. Même s'il est au courant de la méthode scientifique, il ne pensera peut-être pas à l'appliquer pour résoudre des problèmes réels.

Cette méthode est très efficace, bien que longue. On peut aller plus vite en faisant des suppositions logiques. Par exemple, si un point d'accès fonctionnant depuis longtemps arrête soudainement de fonctionner après un orage, alors vous pouvez supposer que le problème est relié à l'alimentation d'énergie et donc sauter la majeure partie du processus scientifique. On devrait enseigner les gens chargés du support technologique de dépanner en utilisant cette méthode, car il y aura des périodes où le problème ne sera ni connu ni évident. Des arbres de décision ou des organigrammes simples peuvent être faits pour tester ces variables et pour essayer de les éliminer afin d'isoler le problème. Naturellement, ces diagrammes ne devraient pas être suivis aveuglément.

Il est souvent plus facile d'enseigner cette méthode en utilisant un problème non technologique d'abord. Par exemple, faites développer à votre étudiant un procédé de résolution de problèmes sur quelque chose de simple et de familier, comme une télévision à batteries. Commencez par abîmer la télévision. Donnez-lui une batterie qui n'est pas chargée. Débranchez l'antenne. Insérez un fusible brisé. Testez l'étudiant en lui indiquant clairement que chaque problème montrera des symptômes spécifiques et indiquez le chemin quant à la façon de procéder. Une fois qu'il a réparé la télévision, faites lui appliquer ce procédé à un problème plus compliqué. Dans un réseau, vous pouvez changer une adresse IP, changer ou détruire des câbles, employer un faux SSID ou orienter l'antenne dans une fausse direction. Il est important que votre étudiant développe une méthodologie et un procédé pour résoudre ces problèmes.

# Technique de dépannage appropriée

Aucune méthodologie de dépannage ne peut complètement couvrir tous les problèmes que vous rencontrerez lorsque vous travaillerez avec des réseaux sans fil. Mais souvent, les problèmes découlent d'une ou de quelques erreurs communes. Voici quelques points simples à retenir qui peuvent faire que votre dépannage va dans la bonne direction.

- **Ne paniquez pas.** Si vous dépannez un système, cela signifie qu'il fonctionnait à un certain moment, probablement très récemment. Avant de commencer à faire des changements, examinez la scène et évaluez exactement ce qui est brisé. Si vous pouvez commencer à travailler à partir des journaux(*log*) d'historiques ou de statistiques, c'est encore mieux. Soyez sûr de rassembler l'information d'abord, ainsi vous pouvez prendre une décision avertie avant de faire des changements.
- **Est-ce branché?** Cette étape est souvent négligée jusqu'à ce que beaucoup d'autres avenues soient explorées. Des prises peuvent accidentellement (ou intentionnellement) être débranchées très facilement. Le câble est-il relié à une bonne source d'énergie? L'autre extrémité est-elle reliée à

votre dispositif? La lumière de puissance est-elle allumée? Ceci peut sembler idiot, mais vous vous sentirez encore plus idiot si vous perdez beaucoup de temps à vérifier une ligne d'alimentation d'antenne pour vous rendre compte qu'un AP a été débranché pendant tout ce temps. Faites-moi confiance, ce problème se produit beaucoup plus souvent que la plupart d'entre nous voudrait bien l'admettre.

- **Quelle a été la dernière chose à être modifiée?** Si vous êtes la seule personne avec l'accès au système, quel est le dernier changement que vous avez réalisé? Si d'autres ont accès à lui, quel est le dernier changement qu'ils ont fait et quand? Quand a été la dernière fois que le système a fonctionné? Souvent, les changements dans le système ont des conséquences fortuites qui ne sont pas notées immédiatement. Revenez en arrière et défaites ce changement pour voir quel effet ceci a sur le problème.
- **Faites une sauvegarde.** Ceci s'applique aussi bien avant que vous n'observiez qu'il y a un problème qu'après. Si vous faites un changement compliqué de logiciel à un système et que vous avez fait une sauvegarde, vous pouvez rapidement revenir à l'état précédent et recommencer si nécessaire. En dépannant des problèmes très complexes, avoir une configuration qui fonctionne partiellement peut être bien mieux qu'avoir un désordre qui ne fonctionne pas du tout (et que vous ne pouvez pas facilement reconstituer de mémoire).
- **Le connu comme étant bon.** Cette idée s'applique au matériel, aussi bien qu'au logiciel. Un « ***connu comme étant bon*** » (***known good*** en anglais) est n'importe quel composante que vous pouvez remplacer dans un système complexe pour vérifier que ses contreparties sont dans de bonnes conditions de travail. Par exemple, vous pouvez transporter un câble Ethernet fonctionnel et testé dans votre trousse à outils. Si vous suspectez des problèmes avec un câble sur le terrain, vous pouvez facilement échanger ce câble par « connu comme étant bon » et voir si les choses s'améliorent. Ceci est beaucoup plus rapide et est moins susceptible de causer des erreurs que de sertir un nouveau câble et vous indique immédiatement si le changement règle le problème. De même, vous pouvez également transporter une batterie de secours, un câble d'antenne ou un CD-ROM avec une dernière configuration effective pour le système. En réparant des problèmes compliqués, sauvegarder votre travail à un point donné vous permet de retourner à ce « connu comme étant bon » même si le problème n'est pas encore complètement résolu.
- **Changez une variable à la fois.** Lorsque vous sentez la pression de remettre un système en fonctionnement, il est tentant de vouloir changer beaucoup de variables immédiatement. Si vous le faites et que vos changements semblent régler le problème, alors vous ne comprendrez pas exactement ce qui a mené au problème en premier lieu. Pire encore, vos

changements peuvent régler le problème original, mais mener à des conséquences plus fortuites qui brisent d'autres parties du système. En changeant vos variables une par une, vous pouvez comprendre avec précision ce qui a mal tourné en premier lieu et voir les effets directs des changements que vous faites.

- **Ne l'abîmez pas.** Si vous ne comprenez pas entièrement comment fonctionne le système, n'ayez pas peur d'appeler un expert. Si vous n'êtes pas certain qu'un changement particulier n'endommagera pas une autre partie du système, alors trouvez quelqu'un avec plus d'expérience ou trouvez un moyen d'examiner votre changement sans causer plus de dommages. Mettre une pièce de monnaie au lieu d'un fusible peut résoudre le problème immédiat mais peut également causer un incendie dans le bâtiment.

Il est peu probable que les gens qui conçoivent votre réseau seront à l'appel vingt-quatre heures par jour pour régler les problèmes lorsqu'ils surgissent. Votre équipe de dépannage devra avoir de bonnes qualités de dépannage mais peut ne pas être assez compétente pour configurer un routeur à partir de zéro ou pour sertir une partie d'un LMR-400. Il est souvent beaucoup plus efficace d'avoir un certain nombre de composantes de secours et de former votre équipe pour pouvoir échanger la partie cassée en entier. Ceci peut signifier avoir un point d'accès ou un routeur préconfiguré dans un coffret verrouillé, simplement marqué et stocké avec les câbles et les alimentations d'énergie de secours. Votre équipe peut échanger la composante brisée et l'envoyer à un expert pour sa réparation ou commander une autre composante de secours. Si les pièces de secours sont maintenues sous clef et sont remplacées une fois utilisées, vous épargnerez du temps à tout le monde.

# Problèmes courants de réseau

Souvent, les problèmes de connectivité naissent de composantes brisées, de climat défavorable ou de simples problèmes de configurations. Une fois que votre réseau est connecté à Internet ou ouvert au grand public, des menaces considérables proviendront des utilisateurs du réseau eux-mêmes. Que les menaces soient bénignes ou pure malveillance, elles auront toutes un impact sur votre réseau si celui-ci n'est pas correctement configuré. Cette section se penche sur quelques problèmes communs identifiés dès que votre réseau est utilisé par des êtres humains réels.

## Sites Web hébergés localement

Si une université héberge son site Web localement, les visiteurs du site Web de l'extérieur du campus et du reste du monde concurrenceront le personnel de l'université pour la largeur de bande d'Internet. Ceci inclut l'accès automatisé des moteurs de recherche qui vont ***balayer*** périodiquement votre site au complet. Une solution à ce problème est d'employer un DNS divisé (*split*

*DNS*) et un site miroir. L'université reflète une copie de ses sites Web à un serveur, par exemple à une compagnie d'hébergement européenne et utilise un DNS divisé pour diriger tous les usagers de l'extérieur du réseau de l'université vers le site miroir alors que les usagers sur le réseau de l'université accèdent au même site localement. Des détails à propos de l'installation de cette solution sont présentés au chapitre trois.

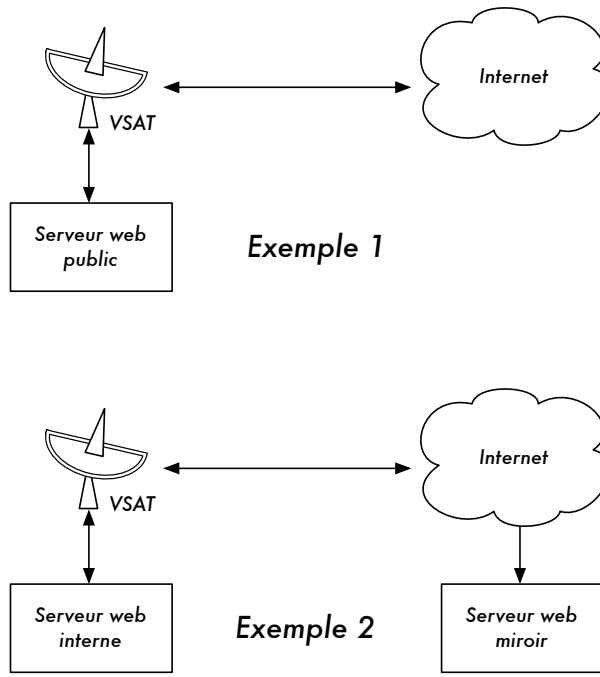


*Figure 8.1: Dans l'exemple 1, tout le trafic de site Web venant d'Internet doit traverser le VSAT. Dans l'exemple 2, le site Web public est hébergé dans un service européen rapide, alors qu'une copie est gardée sur un serveur internet pour un accès local très rapide. Ceci améliore la connexion VSAT et réduit le temps de chargement pour les usagers du site Web.*

## Serveur mandataire ouvert

Un serveur mandataire (*proxy*) devrait être configuré pour accepter seulement des connexions provenant du réseau de l'université, pas du reste de l'Internet. Ceci s'explique par le fait que les gens partout ailleurs voudront se connecter et employer des serveurs mandataires ouverts pour une variété de raisons, tel qu'éviter de payer la largeur de bande internationale. La manière de configurer ceci dépend du serveur mandataire que vous employez. Par exemple, vous pouvez indiquer la plage d'adresses IP du réseau du campus dans votre fichier **`squid.conf`** comme seul réseau qui peut employer Squid. Alternativement, si votre serveur mandataire se trouve derrière un

pare-feu, vous pouvez configurer celui-ci pour ne permettre la connexion au port du serveur mandataire qu'aux hôtes internes.

## Hôtes en mode relais ouvert

Un serveur de courriel mal configuré sera trouvé par des personnes sans scrupules sur Internet et employé comme hôte en mode relais ouvert pour envoyer des courriels non sollicités. Ceci est réalisé afin de cacher la vraie source de ce type de courrier électronique en évitant ainsi de se faire attraper. Pour tester un hôte en mode relais ouvert, l'essai suivant devrait être effectué sur votre serveur de courriel (ou sur le serveur SMTP qui agit en tant qu'hôte en mode relais ouvert sur le périmètre du réseau du campus). Utilisez ***telnet*** pour ouvrir une connexion au port 25 du serveur en question (avec quelques versions Windows de telnet, il peut être nécessaire de tapper « set local_echo » avant que le texte ne soit visible):

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

Puis, si une conversation de ligne de commande interactive peut avoir lieu (comme dans l'exemple suivant), le serveur est un hôte en mode relais ouvert:

```
MAIL FROM: spammer@waste.com
250 OK - mail from <spammer@waste.com>
RCPT TO: innocent@university.ac.zz
250 OK - rcpt to spammer@waste.com
```

Au lieu de cela, la réponse après le premier MAIL FROM devrait être quelque chose comme ce qui suit:

```
550 Relaying is prohibited.
```

Un test en ligne ainsi que de l'information sur le problème sont disponibles sur les sites tels que *http://www.ordb.org/*. Puisque ceux qui envoient des courriels non sollicités ont automatisé des méthodes pour trouver les serveurs en mode relais ouvert, un établissement qui ne protège pas ses systèmes de courriel sera très probablement trouvé et abusé. La configuration du serveur de courriel pour ne pas être serveur en mode relais ouvert consiste à indiquer les réseaux et hôtes qui ont la permission de transmettre du courriel à travers lui dans le MTA (par exemple, Sendmail, Postfix, Exim ou Exchange). Ceci sera probablement la plage d'adresses IP du réseau du campus.

## Réseautage pair à pair

L'abus de largeur de bande par des programmes de partage de fichier pair-à-pair (*peer-to-peer - P2P*) tels que Kazaa, Morpheus, WinMX et BearShare peut être empêché avec les manières suivantes:

- **Rendez impossible l'installation de nouveaux programmes sur les ordinateurs du campus.** Il est possible d'empêcher l'installation de programmes tels que Kazaa en ne donnant pas aux usagers réguliers l'accès administratif aux postes de travail PC. Beaucoup d'établissements normalisent également la structure du bureau, en installant le système d'exploitation requis sur un ordinateur, puis en y installant alors toutes les applications nécessaires d'une manière optimale. L'ordinateur est également configuré d'une manière qui empêche les usagers d'installer toute nouvelle application. Une image du disque de cet ordinateur est alors copiée à tous les autres ordinateurs en utilisant un logiciel tel que Partition Image (voir le site: *http://www.partimage.org/*) ou Drive Image Pro (voir le site: *http://www.powerquest.com/*).

  De temps en temps, les usagers peuvent réussir à installer un nouveau logiciel ou à endommager le logiciel sur l'ordinateur (par exemple, en le faisant figer souvent). Quand ceci se produit, un administrateur peut simplement remettre l'image du disque, remettant le système d'exploitation et tous les logiciels sur l'ordinateur exactement comme indiqué.

- **Le blocage de ces protocoles n'est pas une solution.** Kazaa et d'autres protocoles sont assez intelligents pour éviter les ports bloqués. Par défaut, Kazaa utilise le port 1214 pour la connexion initiale. Cependant, s'il n'est pas disponible, il essayera d'employer les ports 1000 à 4000. Si ceux-ci sont bloqués, il utilise le port 80, se faisant passer pour du trafic web. C'est pour cette raison que les ISPs ne le bloquent pas mais l' « étrangle », en utilisant un gestionnaire de largeur de bande (voir le chapitre trois).

- **Si la limitation du débit n'est pas une option, changez la disposition du réseau.** Si le serveur mandataire et celui de courriel sont configurés avec deux cartes de réseau (comme décrit dans le chapitre trois) et que ces serveurs ne sont pas configurés pour faire suivre (*ip forward*) les paquets, tout le trafic poste à poste (p2p) serait bloqué. Ceci bloquerait également tous les autres types de trafic, tels que Microsoft NetMeeting, SSH, VPN et tous les autres services qui n'ont pas été spécifiquement autorisés par le serveur mandataire. Dans les réseaux à faible largeur de bande, on peut décider que la simplicité de cette conception sera supérieure aux inconvénients. Une telle décision peut être nécessaire, mais ne devrait pas être prise à la légère. Les administrateurs réseau ne peuvent simplement pas prévoir de quelles façons innovatrices les usagers feront usage du réseau. Si vous bloquez tout accès de façon préventive, vous empêcherez les usagers de se servir de tous les services que votre ser-

veur mandataire ne soutient pas (même les services à faible largeur de bande). Même si ceci peut être souhaitable dans les circonstances à largeur de bande extrêmement faible, on ne devrait jamais le considérer comme une bonne politique d'accès en général.

## Programmes qui s'installent par eux-mêmes (à partir d'Internet)

Il y a des programmes qui s'installent automatiquement et continuent par après à utiliser la largeur de bande, par exemple: le dénommé Bonzi-Buddy, le Réseau Microsoft et quelques genres de vers. Certains programmes sont des logiciels espions qui envoient des informations sur les habitudes de navigation d'un usager à une compagnie quelque part sur Internet. Ces programmes sont évitables dans une certaine mesure par l'éducation des usagers et la restriction des ordinateurs afin d'empêcher l'accès administratif aux usagers réguliers. Dans d'autres cas, il y a des solutions logicielles pour trouver et enlever ces programmes problématiques, tels que Spychecker (*http://www.spychecker.com/*), Ad-Aware (*http://www.lavasoft.de/*) ou xp-antispy (*http://www.xp-antispy.de/*).

## Mises à jour Windows

Les derniers systèmes d'exploitation Microsoft Windows supposent qu'un ordinateur avec une connexion LAN a un bon lien à Internet et télécharge automatiquement des correctifs de sécurité, de bogues et des améliorations de fonctionnalités à partir du site Web de Microsoft. Ceci peut consommer massivement la largeur de bande sur un lien Internet dispendieux. Les deux approches possibles pour résoudre ce problème sont les suivantes:

- **Désactivez les mises à jour de Windows sur tous les ordinateurs.** Les mises à jour de sécurité sont très importantes pour les serveurs, mais il est discutable que les postes de travail dans un réseau privé protégé tel qu'un réseau de campus en aient réellement besoin.
- **Installez un serveur de mise à jour de logiciel.** C'est un programme gratuit de Microsoft qui vous permet de télécharger toutes les mises à jour de Microsoft durant la nuit sur un serveur local et de distribuer les mises à jour aux postes de travail clients à partir de ce serveur. De cette façon, les mises à jour de Windows n'emploient aucune largeur de bande sur le lien Internet pendant le jour. Malheureusement, tous les ordinateurs client doivent être configurés pour utiliser le serveur de mise à jour de logiciel pour que ceci puisse avoir un effet. Si vous avez un serveur flexible de DNS, vous pouvez également le configurer pour répondre aux demandes pour *windowsupdate.microsoft.com* et diriger l' « *updater* » vers votre serveur de mise à jour. C'est un bon choix seulement pour les grands ré-

seaux et peut sauver des quantités incalculables de largeur de bande Internet.

Le blocage du site de mises à jour de Windows sur le serveur mandataire n'est pas une bonne solution car le service de mise à jour de Windows (mises à jour automatiques) continue à réessayer plus agressivement et si tous les postes de travail font cela, le serveur mandataire aura à supporter une lourde charge. L'extrait ci-dessous provient du fichier de journal du serveur mandataire (fichier journal d'accès de Squid) où on a bloqué les fichiers Microsoft cabinet (.cab).

Une grande partie du fichier de journal Squid ressemble à ceci:

```
2003.4.2 13:24:17 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
  *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:18 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:18 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab HEAD 0
2003.4.2 13:24:19 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:19 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:20 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab HEAD 0
```

Même si ceci peut être tolérable si nous avons peu d'ordinateurs clients, le problème prend de l'ampleur de manière significative si des hôtes sont ajoutés au réseau. Plutôt que de forcer le serveur mandataire à répondre à des requêtes qui échoueront toujours, il est plus raisonnable de réorienter les clients de mise à jour de logiciel à un serveur local de mise à jour.

## Programmes qui supposent un lien de grande largeur de bande

En plus des mises à jour de Windows, beaucoup d'autres programmes et services supposent que la largeur de bande n'est pas un problème et la consomment donc pour des raisons que l'usager ne pourrait pas prévoir. Par exemple, les paquets d'anti-virus (comme le Norton AntiVirus) font des mises à jour périodiques automatiques et directement de l'Internet. Il est préférable que ces mises à jour soient distribuées à partir d'un serveur local.

D'autres programmes, tels que le RealNetworks video player, téléchargent automatiquement des mises à jour et des annonces puis envoie sur un serveur les habitudes d'utilisation. D'autres mini applications apparemment inof-

fensives (comme les gadgets de Konfabulator et Dashboard) sondent continuellement des hôtes d'Internet pour de l'information de mise à jour. Celles-ci peuvent êtres des requêtes qui demandent une faible largeur de bande (comme des mises à jour sur le climat ou des nouvelles) ou des requêtes qui exigent une très grande largeur de bande (telles que les webcams). Il peut être nécessaire de limiter ou bloquer totalement ce genre d'applications.

Les dernières versions de Windows et Mac OS X ont également un service de synchronisation de temps. Ceci maintient l'horloge de l'ordinateur précise en la connectant à des serveurs de temps sur Internet. Il est préférable d'installer un serveur de temps local et de distribuer le temps précis à partir de celui-ci, plutôt que d'occuper le lien Internet avec ces requêtes.

## Trafic de Windows sur le lien à Internet

Les ordinateurs Windows communiquent les uns avec les autres par l'intermédiaire de ***NetBIOS*** et de ***Server Message Block*** (***SMB***). Ces protocoles fonctionnent sur TCP/IP ou d'autres protocoles de transport. C'est un protocole qui fonctionne en tenant des élections pour déterminer quel ordinateur sera le ***navigateur principal***. Le navigateur principal est un ordinateur qui garde une liste de tous les ordinateurs, ressources partagées et imprimantes que vous pouvez voir dans le ***Voisinage réseau*** ou ***Favoris réseau***. L'information sur les ressources partagées disponibles est également transmise à intervalles réguliers.

Le protocole SMB est conçu pour des réseaux LAN et pose des problèmes quand l'ordinateur Windows est connecté à l'Internet. À moins que le trafic SMB soit filtré, il tendra également à se disperser sur le lien Internet, gaspillant ainsi la largeur de bande de l'organisation. Les mesures suivantes pourraient être prises afin d'empêcher ceci:

- **Bloquez le trafic sortant de SMB/NetBIOS sur le routeur périphérique ou pare-feu.** Ce trafic la largeur de bande Internet et pire encore, pourra poser un risque potentiel de sécurité. Beaucoup de vers sur Internet et d'outils de pénétration cherchent activement des SMB ouverts afin d'exploiter ces connexions pour gagner un plus grand accès à votre réseau.
- **Installez ZoneAlarm sur tous les postes de travail (pas le serveur).** Une version gratuite peut être trouvée à *http://www.zonelabs.com/*. Ce programme permet à l'usager de déterminer quelles applications peuvent établir des connexions à Internet et quelles ne peuvent pas. Par exemple, Internet Explorer doit se connecter à Internet mais pas Windows Explorer. ZoneAlarm peut empêcher que Windows Explorer se connecte.
- **Réduisez les ressources partagées du réseau.** Idéalement, seul le serveur de fichiers devrait avoir des ressources partagées. Vous pouvez utiliser un outil tel que le SoftPerfect Network Scanner

(*http://www.softperfect.com/*) pour identifier facilement toutes les ressources partagées de votre réseau.

## Vers et virus

Les vers et les virus peuvent produire d'énormes quantités de trafic. Le ver W32/Opaserv, par exemple, même s'il est vieux, est encore répandu. Il est distribué à partir des ressources partagées de Windows et est détecté par d'autres sur Internet parce qu'il essaye de s'étendre davantage. Il est donc essentiel que la protection anti-virus soit installée sur tous les ordinateurs. En outre, il est essentiel de former l'usager au sujet d'exécuter des pièces jointes et de répondre à du courriel non sollicité. En fait, ce devrait être une politique qu'aucun poste de travail ou serveur fournissent des services inutilisés. Un ordinateur ne devrait pas avoir de ressources partagées à moins que ce soit un serveur de fichiers; et un serveur ne devrait pas exécuter des services inutiles non plus. Par exemple, les serveurs de Windows et d'Unix exécutent généralement un service de serveur web par défaut. Ceci devrait être désactivé si ce serveur a une fonction différente; moins un ordinateur exécute de services, moins il y a de chances qu'il soit exploité.

## Boucle d'expédition de courriel

De temps en temps, un simple usager commettant une erreur peut poser un problème. Par exemple, un usager dont le compte d'université est configuré pour expédier tout le courrier à son compte de Yahoo. L'usager part en vacances. Tous les courriels que cet étudiant reçoit sont encore expédiés à son compte Yahoo qui a une capacité de jusqu'à 2 MB. Lorsque le compte Yahoo est complet, il commence à rebondir les courriels au compte de l'université, qui les expédient immédiatement à nouveau au compte Yahoo. On forme ainsi une boucle d'expédition de courriel qui pourrait envoyer des centaines de milliers de courriels dans les deux sens, produisant ainsi un trafic massif capable de détruire des serveurs de courriel.

Il existe des dispositifs dans les programmes de serveur de courriel qui peuvent identifier de telles boucles et qui devraient être activés par défaut. Les administrateurs doivent également faire attention de ne pas désactiver ces dispositifs par erreur ou de ne pas installer un expéditeur SMTP qui modifie les en-têtes de courriel de telle manière que le serveur de courriel ne puisse pas identifier la boucle de courriel.

## Grands téléchargements

Un usager peut commencer plusieurs téléchargements simultanés ou télécharger de grands fichiers comme des images ISO de 650MB. De cette

façon, un simple usager peut épuiser la majeure partie de la largeur de bande. Les solutions à ce genre de problème se situent dans la formation, le téléchargement sans connexion et la surveillance (y compris la surveillance en temps réel, tel que décrit au chapitre six). Le téléchargement sans connexion peut être réalisé par au moins deux manières:

- À l'université de Moratuwa, un système a été mis en application en utilisant la redirection URL. Les usagers entrant à **ftp://** URLs accèdent à une liste annuaire dans laquelle chaque fichier a deux liens: un pour le téléchargement normal et l'autre pour télécharger sans connexion. Si le lien sans connexion est choisi, le fichier indiqué est mis en attente pour le téléchargement postérieur et l'usager reçoit un courriel lorsque le téléchargement est complet. Le système garde une cache des fichiers téléchargés récemment et recherche ces fichiers immédiatement lorsqu'ils sont redemandés. La file d'attente de téléchargement est classée par la taille du fichier. Par conséquent, les petits fichiers sont téléchargés d'abord. Comme une certaine largeur de bande est assignée à ce système même pendant des heures de pointe, les usagers qui demandent de petits fichiers peuvent les recevoir en quelques minutes, parfois plus rapidement qu'avec un téléchargement en ligne.
- Une autre approche serait de créer une interface Web où les usagers entrent l'URL du fichier qu'ils désirent télécharger. Ceci est alors téléchargé durant la nuit en utilisant un ***cron job*** ou une tâche programmée. Ce système fonctionnerait uniquement pour les usagers qui ne sont pas impatients et qui savent quelles tailles de fichier seraient problématiques pour le téléchargement pendant les heures de travail.

## Envoie de fichiers de grande taille

Lorsque les usagers doivent transférer des fichiers de grande taille à des collaborateurs ailleurs sur Internet, ils devraient être entraînés pour planifier le téléchargement. Dans Windows, un téléchargement à un serveur FTP à distance peut être réalisé en utilisant un script de commandes FTP (sauvegardé comme **`c:\ftpscript.txt`**) ressemblant à ceci:

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

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

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

Sur des ordinateurs Windows NT, 2000 et XP, la commande peut être sauvegardée dans un fichier tel que **`transfer.cmd`** et programmé pour fonctionner durant la nuit en utilisant les Tâches Planifiées (Démarrer ➜ Paramètres ➜ Panneau de configuration ➜ Tâches Planifiées). Dans Unix, il est possible d'obtenir le même résultat en utilisant ***at*** ou ***cron***.

## Usagers s'envoyant des fichiers les uns aux autres

Les usagers doivent souvent s'envoyer des fichiers de grande taille. Si le destinataire est local, envoyer ces fichiers via Internet est un gaspillage de largeur de bande. Un point de partage de fichiers devrait être créé sur le serveur local de Windows/samba/web Novell afin que l'usager puisse y placer le fichier de grande taille et que d'autres puissent y avoir accès.

Alternativement, un front-end web peut être écrit pour un serveur web local pour accepter un fichier de grande taille et pour le placer dans un espace de téléchargement. Après l'avoir téléchargé au serveur web, l'usager reçoit un URL pour le fichier. Il peut alors donner ce URL à ses collaborateurs locaux ou internationaux. Ceux-ci pourront ainsi télécharger le fichier en accédant à cet URL. C'est ce que l'Université de Bristol a fait avec leur système FLUFF. L'université offre un service pour le téléchargement de fichiers de grande taille (FLUFF) disponible à: *http://www.bristol.ac.uk/fluff/*. Ces fichiers peuvent être consultés par n'importe qui ayant reçu son emplacement. L'avantage de cette approche est que les usagers peuvent offrir l'accès à leurs fichiers à des usagers externes, tandis que la méthode de partage de fichiers peut fonctionner seulement pour des usagers du réseau du campus. Un système comme ceci peut facilement être mis en application avec un script CGI utilisant Python et Apache.