L'importance d'un réseau en bonne santé

Par Raymond Rivest, conseiller, spécialiste de test, CRIM

Raymond Rivest

Les utilisateurs d'une infrastructure réseau ne sont pas toujours conscients de ce qui se passe au-delà de leurs ordinateurs. Pourtant, ils sont souvent les premiers à subir les conséquences d'un réseau en mauvais état. Il faut reconnaître que certaines entreprises gèrent leurs réseaux internes en ne connaissant que très peu leur fonctionnement réel. Dans bien des cas, on peut comparer le réseau d'entreprise à celui d'un particulier qui effectue des branchements du type « manuel d'installation rapide » : la majorité des gens ignorent ce qui y circule. Pour des installations simples, il est généralement suffisant d'utiliser les configurations par défaut, mais que se passe-t-il quand des problèmes surviennent ?

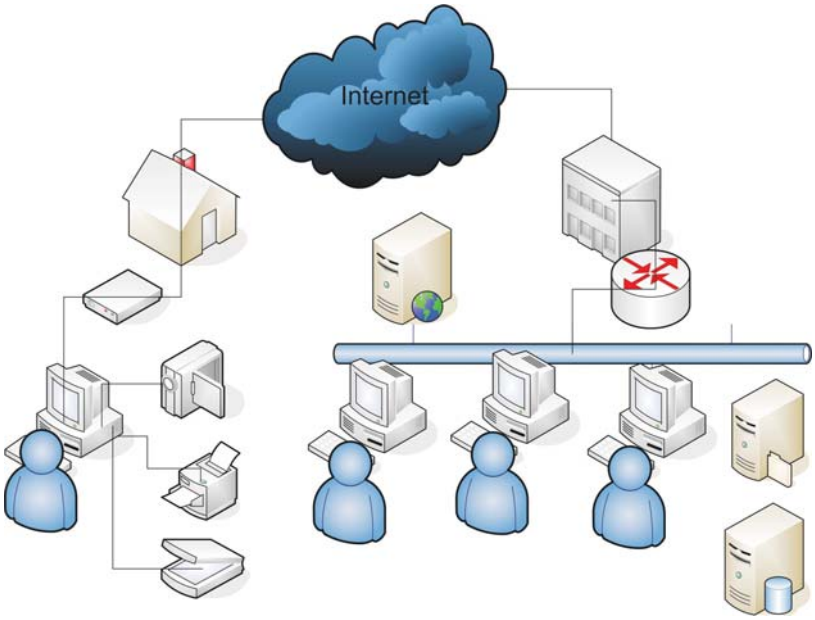

Figure 1 – Peu de gens savent ce qui circule sur leur réseau, qu'il s'agisse d'un réseau domestique ou d'entreprise.

Voir figure 1.

Les symptômes

Il existe plusieurs symptômes à des problèmes de réseau; encore faut-il savoir les distinguer les uns des autres. Voici les plus faciles à déceler parmi la multitude d'exemples possibles :

- Réseau lent : Les applications prennent plus de temps à fonctionner que normalement.
- Application lente : Un système en particulier semble plus lent que d'habitude.
- Saturation du branchement Internet : Il faut attendre plusieurs minutes avant de recevoir un fichier, alors que cette opération ne prend normalement que quelques secondes.
- Visibilité sur Internet : Votre ordinateur se comporte de façon inhabituelle. Vous êtes peut-être une proie facile pour les pirates informatiques, en étant peu ou pas protégé contre leurs attaques.
- Propagation rapide des virus : Votre ordinateur est continuellement infecté par des virus.

Les causes

On considère souvent à tort que les performances d'un ordinateur sont intimement liées à sa puissance ou à sa vitesse de connexion au réseau. Ce n'est pourtant pas toujours le cas.

- **Architecture désuète**
  Une architecture désuète peut constituer une cause de problèmes. Par exemple, de nouvelles technologies sont introduites et combinées à d'anciennes alors qu'elles ne sont pas nécessairement compatibles entre elles. Cela s'applique autant aux logiciels qu'aux plateformes (PC, Mac, etc.) ou au matériel réseau. Un exemple parmi d'autres : des postes de travail équipés d'une carte réseau à 100 Mbps sur des équipements réseaux plus lents (ex. : concentrateur 10 Mbps) ou non compatibles.

- **Protocoles et services superflus**
  Les installations par défaut activent fréquemment certains protocoles ou services qui ne sont pas nécessairement utilisés. En outre, ceux-ci diffusent des données sur le réseau, par exemple l'identification d'ordinateur, de disque partagé ou d'imprimante partagée.

- **Partage de disques et de ressources**
  Le partage de disques réseaux et de ressources telles que les imprimantes est courant sur la majorité des réseaux. En général, on y trouve quatre ou cinq répertoires et plusieurs imprimantes réseaux, mais s'en sert-on vraiment ? Sur un réseau Microsoft, le partage de disques et d'imprimantes transmet à intervalles réguliers un message à tous les souscripteurs de cette ressource. Selon le nombre d'utilisateurs et de ressources ainsi partagées, le volume de transmission (*broadcast*) de cette opération peut devenir très élevé.

- **Méconnaissance des protocoles**
  Les protocoles réseaux ne sont pas toujours bien connus et c'est pourquoi ils sont souvent mal utilisés, que ce soit dans l'installation ou encore dans la programmation sous-jacente. Or, les protocoles ont été conçus pour répondre à des besoins spécifiques, qui ne sont pas nécessairement liés à la performance ou au volume engendré.

- **Mauvaise utilisation des ressources**
  Les problèmes sont fréquemment dus au fait que les utilisateurs connaissent mal les systèmes dont ils se servent. Des applications telles que la radio sur Internet, le clavardage (ex. : Yahoo ou MSN Messenger) et autres sont des sources de trafic sur le réseau. Des logiciels comme Kazaa – dont le but est le partage et la distribution de fichiers par le biais d'Internet – diffusent des informations vers Internet et, dans certains cas, peuvent même causer des failles dans la sécurité des installations.

Voir figure 2.

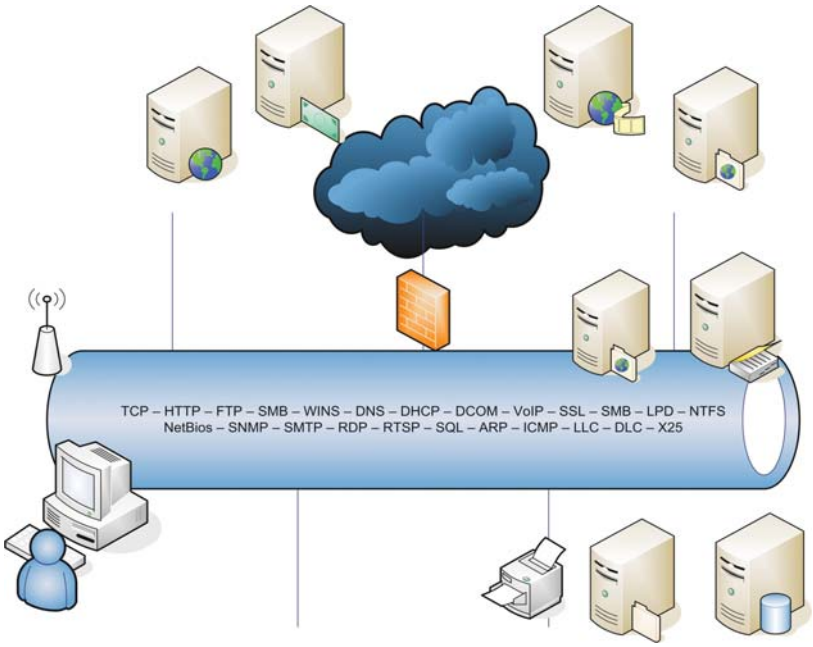

Figure 2 – Un réseau est une autoroute balisée d'une multitude de protocoles

Les technologies disponibles sur Internet changent constamment et il s'en ajoute continuellement de nouvelles, tout cela dans un désordre transparent pour la majorité des utilisateurs. Afin de mieux comprendre ce qui circule sur votre réseau, procurez-vous le gratuiciel Packetyzer produit par Network Chemistry à l'adresse suivante : http://www.networkchemistry.com/products/packetyzer/

À titre d'illustration, voici le résultat d'une capture d'activités de deux minutes à partir d'un ordinateur personnel :

Voir figures 3, 4 et 5.

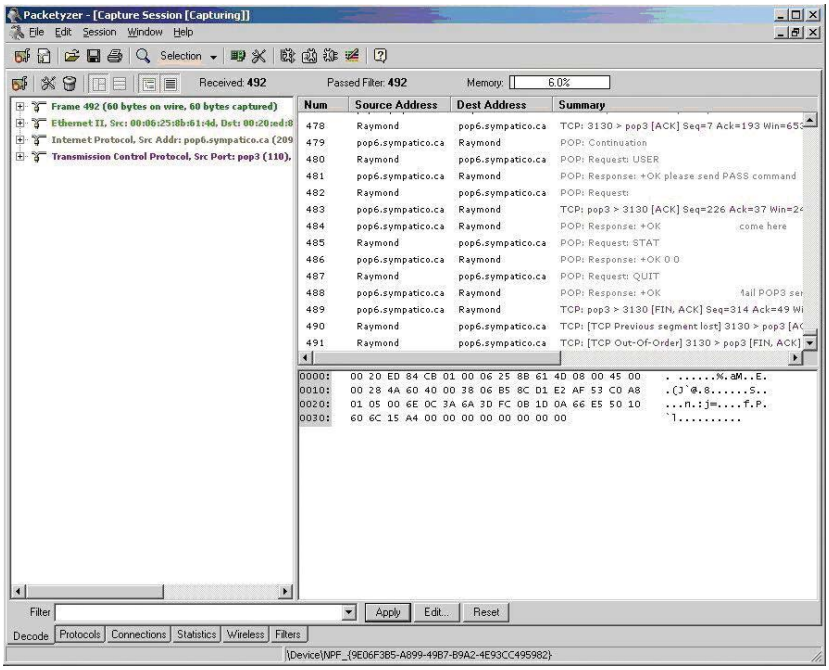

Figure 3 – Collecte de paquets avec Packetyzer

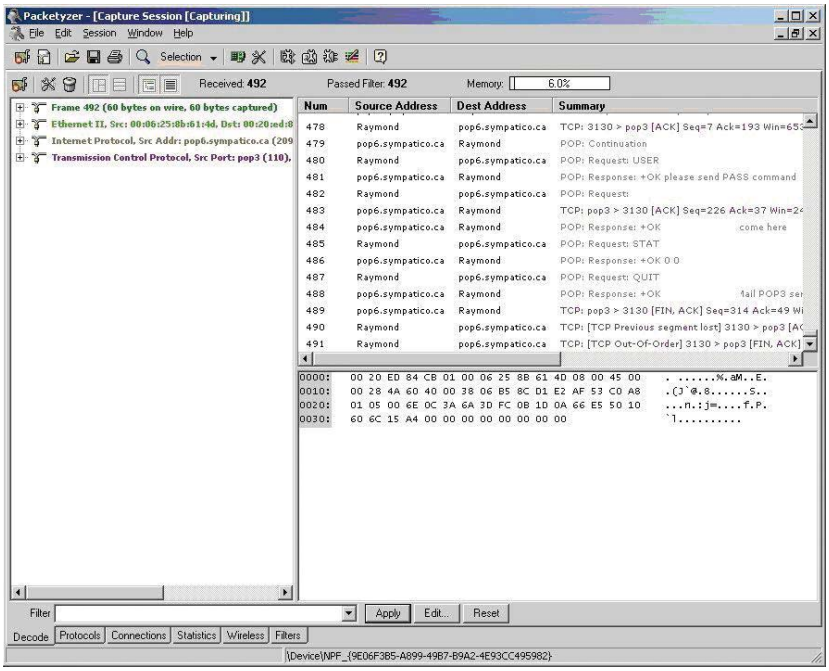

Figure 4 – Distribution de protocoles

Comme vous pouvez le constater, de très nombreux éléments circulent sur un simple réseau domestique commuté, et ce, en deux minutes seulement. Alors, imaginez un peu ce qui se passe dans un réseau de 300 utilisateurs, sans parler d'Internet!

Les coûts

Afin d'évaluer les coûts réels d'un réseau en mauvaise santé, il est impérieux de se poser les questions suivantes :

- **Coûts pour augmenter la capacité de votre réseau**
  Combien avez-vous investi pour augmenter votre bande passante ? L'augmentation des coûts d'immobilisation pour faire évoluer votre infrastructure matérielle est-elle vraiment justifiée ? Autrement dit, règlera-t-elle vraiment le problème ? La nouvelle capacité de votre réseau servira-t-elle bien les objectifs d'affaires de votre entreprise, ou est-elle plutôt gaspillée par une mauvaise utilisation, créant encore plus d'improductivité ?

- **Coûts de maintenance**
  Calculez le temps que votre personnel de soutien consacre chaque jour aux tâches suivantes : maintenance et réparation des services sur le réseau; maintenance des ordinateurs du parc informatique; nettoyage et récupération de données vitales à cause de virus informatiques ou de PC qui ne fonctionnent plus correctement…

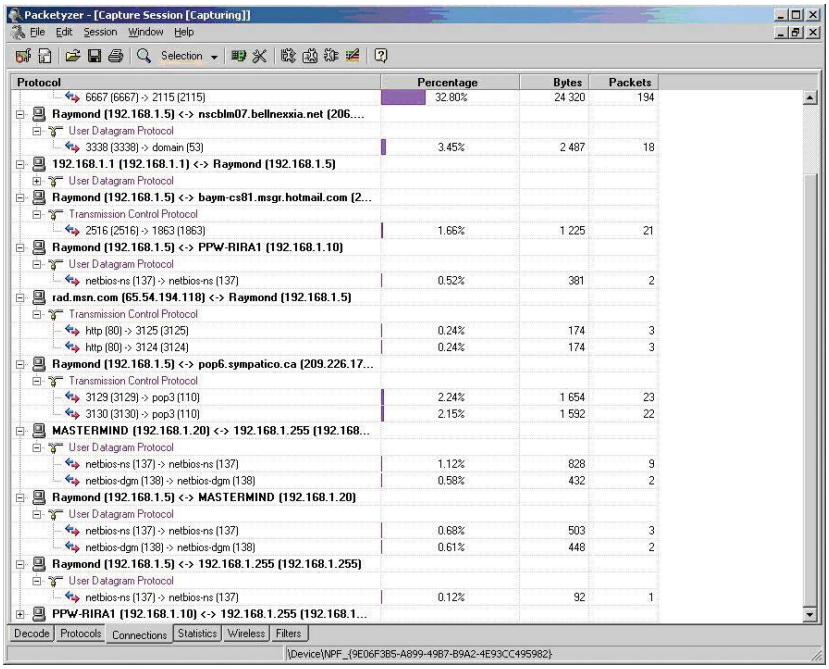

Figure 5 – Branchements, protocoles et ports utilisés

- **Perte de productivité**
  Tentez également d'estimer le nombre d'heures que l'ensemble des employés perd, chaque jour, à reprendre des opérations interrompues par une panne de système, à attendre un système qui ne répond pas adéquatement, à redémarrer des ordinateurs rendus instables à cause du nombre incalculable d'applications inconnues qu'ils contiennent… Analysez aussi le temps que passent vos collègues à clavarder avec des amis, à échanger des fichiers musicaux ou encore à chercher des postes de radio pour écouter leurs chansons préférées à partir de leur ordinateur.

- **Perte d'achalandage**
  Avez-vous une idée du nombre de vos clients qui n'ont pu accéder à votre serveur Web parce que votre lien Internet était saturé ? Et du nombre de ceux auxquels vous avez malencontreusement transféré un virus informatique parce que votre réseau était infecté ? Savez-vous combien de pirates informatiques tentent de pénétrer votre réseau, simplement parce que vous n'êtes pas conscients de votre vulnérabilité face à Internet ?

Les solutions

Il est difficile de résoudre un problème lorsqu'on n'en connaît ni l'origine ni la cause. Pour y parvenir, il importe de bien analyser la situation afin de choisir la meilleure solution.

- **Vue d'ensemble**
  Avant toute chose, précisons que la recherche de solutions implique des expertises multiples et que l'objectivité est primordiale. Si vous demandez à vos utilisateurs, à un spécialiste en réseautique, au spécialiste en sécurité, au développeur de logiciels ou à votre impartiteur de résoudre un problème de performance, vous risquez d'avoir des réponses bien différentes ! Qui peut donc vous aider ? L'équation idéale consiste à faire appel à un spécialiste neutre, capable de considérer les aspects tant applicatifs que réseaux tout en tenant compte des préoccupations d'affaires.

- **Analyse de la situation**
  Il faut commencer par prendre connaissance de l'état de santé de votre réseau et, pour cela, disposer de diagrammes réseaux à jour. Il s'agira ensuite de collecter ce qui circule sur votre réseau, afin d'établir des statistiques d'utilisation – par exemple, les heures auxquelles votre réseau est le plus utilisé et de quelle manière il l'est. Pour le découvrir, il existe des outils spécialement conçus à cet effet. Cependant, leur coût est parfois

100101
10110101
1011010110101
0101001110

élevé. De plus, il faut posséder de grandes connaissances techniques pour pouvoir tirer profit des informations très pointues qu'ils fournissent (matériel réseau, protocoles et ports de communication, technologies – java, corba, .Net, etc.).

Voir figures 6, 7 et 8.

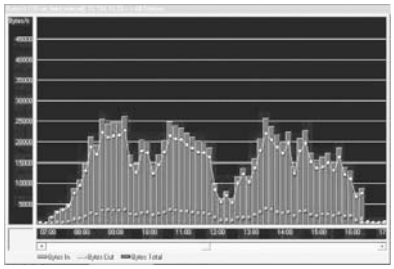

Figure 6 – Utilisation d'un réseau par tranche horaire

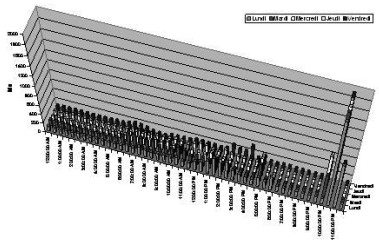

Figure 7 – Distribution de volume réseau

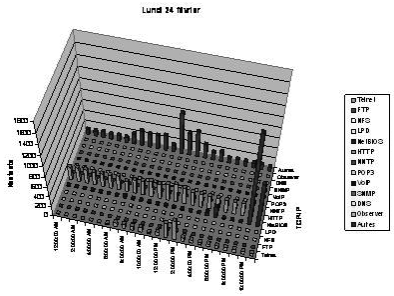

Figure 8 – Distribution de protocole réseau

- **Diagnostic**
  L'établissement d'un diagnostic valable est fréquemment une question de flair, de connaissances, mais aussi de patience. Le problème n'est pas nécessairement apparent au premier coup d'œil. Il peut être tout simplement causé par un mauvais branchement ou se révéler plus complexe et résulter de causes multiples.

- **Assainissement**
  Lorsqu'on dispose enfin d'une image claire de l'état du réseau, il faut l'assainir en retirant tout ce qui est inutile, en ajustant ce qui n'est pas optimal. Cette opération, qui peut s'avérer laborieuse, exige de la préparation. Il faut procéder par étapes et vérifier à chacune d'elles si les changements apportés portent fruit.

- **Réglementation**
  On doit instituer des règles d'utilisation des ressources si l'on ne veut pas que les problèmes se répètent. Grâce à des directives écrites et à une administration adéquate du réseau et de ses ressources, on peut souvent établir un fonctionnement plus restrictif mais beaucoup plus sécuritaire et performant.

- **Maintenance**
  Enfin, une fois le réseau redevenu en bonne santé, il faut prendre soin de le maintenir en forme ! Cela implique une surveillance régulière (monitoring) et un suivi des changements, qu'il s'agisse de logiciels, de matériel ou d'infrastructure. Les diagrammes devront être mis à jour et tout changement devra être effectué selon les règles établies, mais celles-ci devront par ailleurs être adaptées aux besoins.

En bref, un réseau en bonne santé est un gage de bon fonctionnement. Trop souvent, les réseaux sont montés à l'emporte-pièce, sans gestion ni planification. On fait des ajouts, on remplace des éléments au fur et à mesure de la demande, sans vraiment faire de suivi ni avoir une idée exacte de la situation. Quand les problèmes surviennent, l'argent a déjà commencé à sortir par les « tuyaux » du réseau.

Espérons que ces quelques conseils vous aideront à garder votre réseau en bonne santé et donc à assurer la satisfaction de vos usagers.

Saviez-vous que ...?

Le concept de virtualisation fut initialement introduit dans les années 1960 dans le but de permettre la partition des ressources des ordinateurs centraux. Son utilisation commença toutefois à diminuer à partir de 1980, les PC étant devenus plus performants et plus abordables.