LES OUTILS D'ADMINISTRATION D'UN RÉSEAU

Introduction

L'administration des réseaux est une fonction indispensable dont il faut tenir compte lorsqu'on décide de s'investir dans la conception d'un réseau. Cette fonction est tellement importante que l'*ISO* (*International Standard Organization*) a dû définir cinq directives pour spécifier l'étendue du travail d'administration. Ainsi, l'administrateur de réseau doit :

- surveiller et réparer les anomalies comme un câble défectueux ou autre…;
- s'occuper de toutes les configurations, que ce soit sur les postes ou sur les éléments du réseau;
- gérer toute la sécurité du réseau (mots de passe, coupe-feu, …);
- mesurer et analyser les performances du réseau;
- gérer les informations comptables du réseau (coût des liaisons longue distance, etc.).

Ces tâches peuvent s'apparenter à celles d'un technicien de maintenance. Mais avec l'évolution des technologies, on ne peut pas concevoir dans ce domaine un administrateur de réseau qui ne maîtrise pas le logiciel et le matériel! Pour une bonne partie de cette tâche, des logiciels d'administration de réseau aideront l'administrateur. Par ailleurs, il ne suffit pas à l'administrateur de posséder tous les outils d'administration de réseaux, il lui faut développer son inspiration, la perception de son réseau, son intuition. Pour donner un exemple : un petit champ magnétique peut perturber un réseau. Si l'administrateur de réseau n'a pas cette notion, il cherchera très longtemps la cause de la perturbation avec peu de chances de tomber sur la bonne! De plus, il ne s'agit pas tout simplement de déceler les anomalies, il faut savoir le faire très rapidement… au goût des exploitants! La maîtrise de « pouvoir penser réseau » est capitale pour un administrateur de réseau qui veut contrôler son réseau, l'optimiser et le faire évoluer. Il faut qu'il sache mesurer l'état de santé de son réseau.

Enfin, on peut définir l'administration réseau comme étant le contrôle des données d'un réseau complexe de manière à en optimiser le fonctionnement et les performances, les outils d'administration étant les instruments de l'administrateur réseau pour réussir cette mission. Cette étude concerne l'administration globale des réseaux. Il y sera question des protocoles, des bases de données d'administration, etc. Les systèmes d'exploitation de réseaux ne seront donc pas traités ici.

Les spécifications techniques contractuelles

Avant de se lancer dans la conception d'un réseau, il ne faut pas oublier les préalables : le cahier des charges. Il faut savoir dimensionner son réseau, déterminer le trafic qui y transitera, la taille de la bande passante, les différents supports, les ressources à mettre en jeu, l'objectif du réseau, les diverses topologies, la philosophie à adopter, etc. Il faut évaluer l'apport d'un réseau relativement aux investissements consentis.

Pour déterminer les spécifications techniques d'un réseau, il faut élaborer un catalogue non exhaustif des services d'assistance que le service informatique peut mettre en œuvre selon les besoins actuels de l'entreprise. Pour ce faire, une analyse des besoins s'impose. De plus, la suite des travaux doit se faire sur la base des documents complets et précis afin d'éviter tout malentendu, ce qui aura pour conséquence de minimiser les retards dans l'exécution des travaux.

Étant donné que l'informatique permet d'automatiser les tâches répétitives, d'améliorer la communication entre collaborateurs, de professionnaliser la communication clients/fournisseurs et d'aider à prendre les décisions importantes, il faudra arriver à intégrer ces possibilités dans une stratégie d'entreprise afin de faire face aux grands défis de la mise en réseau. Une coopération efficace est fondée sur l'utilisation rationnelle d'un réseau informatique. Ce réseau permettra de partager efficacement informations, télécopieurs et imprimantes. Il peut également aider à stimuler la communication interne et à sécuriser les documents (bases de données, comptabilité, etc.).

L'utilisation d'un logiciel de configuration et de construction du réseau nécessite des compétences spécifiques sans lesquelles il sera difficile d'assurer la qualité du projet. L'interconnexion à l'Internet ouvrira de nouveaux horizons à votre réseau. Cependant, parallèlement à ces avantages, se pose le problème de la sécurité du système d'information. Il faudra ainsi prévoir tous les outils nécessaires à l'administration quotidienne du réseau avant de subir les dégâts d'une intrusion, d'un virus ou d'une destruction accidentelle des données.

Installer un réseau informatique peut aider à stimuler la communication inter-utilisateurs. Le logiciel de groupe (*groupware*) en permettra l'optimisation. En effet, en rassemblant divers outils de communication (agenda partagé, courriel, etc.), le logiciel de groupe dynamisera la circulation de l'information et développera les collaborations au sein des utilisateurs.

Les solutions d'administration

Nous allons étudier l'évolution des protocoles afin de mieux comprendre la raison d'être des standards actuels en matière d'administration réseau. Depuis l'avènement de l'ARPANET, en 1969, les petits réseaux informatiques isolés ont évolué vers de grands réseaux interconnectés pour donner naissance à l'Internet. La gestion de ces petits réseaux devenant de plus en plus compliquée, le développement d'un protocole spécifique d'administration réseau s'avéra alors nécessaire.

En 1988, l'*Internet Activities Board* (*IAB*) approuva le développement de deux protocoles : le *SNMP* et le *CMOT* (*Common Management Information Protocol Over TCP/IP*) avec l'idée que le *SNMP* fut une solution à court terme, la préférence étant marquée pour le *CMIP* (*Common Management Information Protocol*).

CMOT est dérivé de *CMIP* qui a été prévu pour être exploité sur *OSI*. Afin de faciliter la transition future de *SNMP* vers *CMOT* (*CMIP over TCP/IP*), et en attendant que *OSI* émerge pour que l'on puisse reléguer le *TCP/IP* (!) aux oubliettes, il a été décidé de développer *CMOT* dans une phase purement transitoire. Afin de s'assurer que *CMIP* sera bel et bien le standard en matière d'administration réseau, l'*IAB* imposa le modèle informationnel défini par l'*OSI*. Ainsi, *CMOT* et *SNMP* doivent utiliser une même base de données d'objets gérables appelée *MIB* (*Management Information Base*). Donc, une *SMI* (*Structure of Managed Information*) et une *MIB* communes devaient être définies et utilisées. Il est malheureusement vite apparu que cette contrainte n'était pas réaliste, car en *SNMP*, on manipule essentiellement des variables et en *CMIP*, on manipule des objets au sens de la technologie orientée objet.

En 1989, l'*IAB* est revenu sur sa décision en acceptant que les deux protocoles suivent une évolution parallèle et indépendante. Une fois libérés de la contrainte de compatibilité avec *OSI*, les progrès ont été rapides. Le malheur des uns faisant le bonheur des autres, *SNMP* a été adopté par de nombreux constructeurs et est devenu à ce jour un standard très répandu de gestion de réseaux. Une des raisons supplémentaires qui a fait que les constructeurs ont opté pour un agent *SNMP* est qu'il occupe moins de 10 ko de mémoire au sein d'un équipement alors qu'un agent *CMIP* requiert près d'une centaine de ko.

La *MIB*, organisée selon une arborescence hiérarchique appelée *MIT* (*Management Information Tree*), détient toutes les informations des équipements à administrer se trouvant dans le réseau. Ces équipements sont repérés par une clé unique et gérés comme tel par un petit programme d'administration réseau appelé agent. C'est ce dernier qui est responsable de faire parvenir à la plate-forme d'administration toutes les informations sur l'équipement qu'il représente. Bien entendu, cet agent ne fait pas de zèle, il attend que les requêtes soient formulées par la plate-forme d'administration. Pour permettre à la *MIB* d'élargir le champ de travail de l'administrateur, notamment en ce qui concerne les routeurs et les ponts, un second standard fut défini pour ajouter des objets dans quelques-unes des catégories de la *MIB* initiale, alors redéfinie *MIB I*. Ce standard est appelé *MIB II* et, fort de près de 180 objets, a remplacé la *MIB I* dans l'arborescence du *MIT*. Ainsi, la *MIB RMON* (*Remote Monitoring*) fait partie de l'arborescence et offre des fonctions proches de celles des analyseurs de réseaux. Le schéma ci-dessous illustre l'organisation d'une *MBI*.

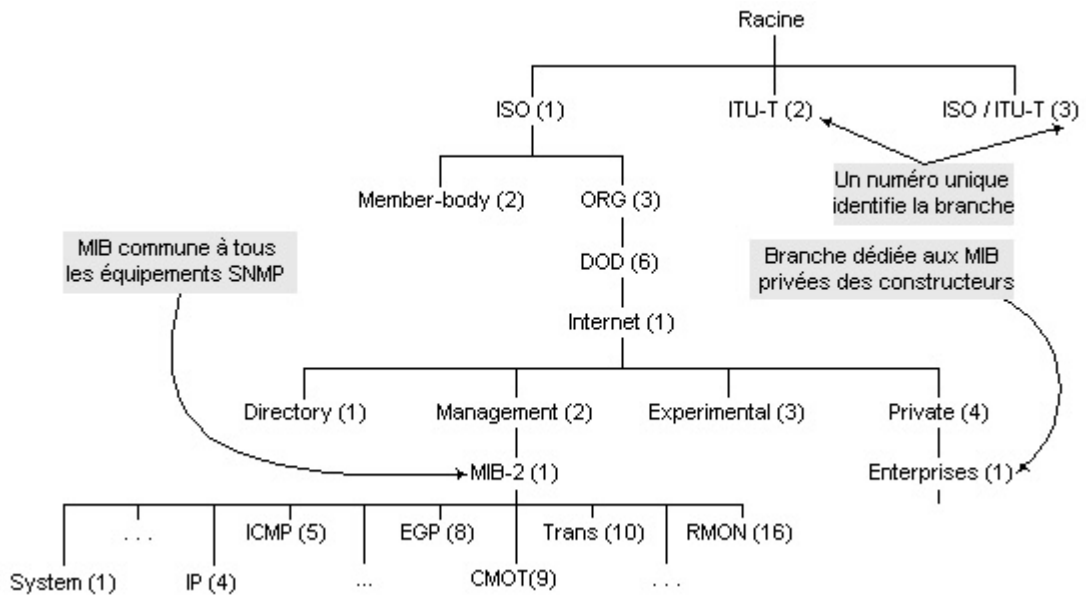

Figure 1 : Extrait d'arborescence de la *MIB*

Une *MIB* est donc simplement une collection d'informations sur tous les objets qui sont sous la responsabilité d'un agent donné. Ces informations sont codifiées dans le *MIT* selon le standard *ASN.1* (*Abstract Syntax Notation 1*). À partir de ce codage, il est alors assez simple de déterminer et de représenter l'identificateur d'un objet (*Object IDentifier – OID*) dans le *MIT*.

Afin d'avoir une idée plus claire du codage *ASN.1* au sein du *MIT*, nous pouvons voir que l'identificateur d'un objet d'administration commence par 1.3.6.1.2 (*iso.org.dod.internet. management*), tandis l'identificateur d'un objet appartenant à un constructeur commence par 1.3.6.1.4.1 (*iso.org.dod.internet.private.enterprises*).

Les protocoles liés à l'administration

Le protocole de gestion de réseau SNMP

SNMP est un protocole de gestion de réseau. C'est actuellement le protocole standard pour l'administration de réseau. Il part du principe qu'un système d'administration réseau se compose des éléments suivants :

- de nœuds administrés (*MN = Managed Node*) chacun contenant un agent. Les agents sont les serveurs;
- d'au moins une station d'administration (*NMS = Network Management Station*). Cette station d'administration est le client;
- d'un protocole réseau utilisé par la *NMS* et d'agents pour échanger des informations d'administration (ici *SNMP*). Voir la figure suivante.

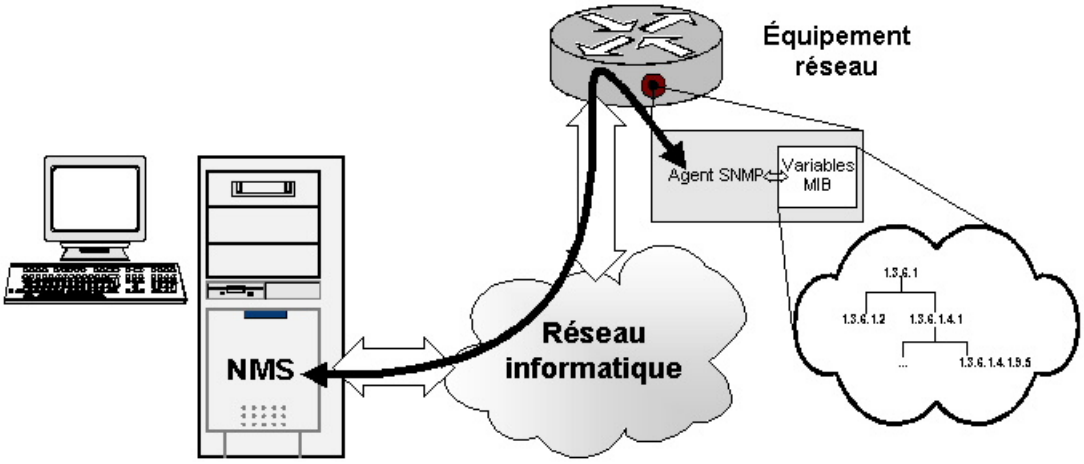

Figure 2 : Le modèle client/serveur

Nous constatons, sur ce schéma, que nous sommes en présence d'un modèle client/serveur, mis à part le fait que le schéma est inhabituel puisqu'il y a un client et beaucoup de serveurs. Comme nous l'avons expliqué plus haut, le client est en réalité la plate-forme d'administration tandis que les serveurs sont tous agents *SNMP* des équipements réseau. Il y aura autant de serveurs que d'équipements réseau dotés d'agents *SNMP*.

SNMP utilise les *SMI* pour donner l'ensemble des règles de définition des objets à gérer et les *MIB* pour représenter la base de données de l'ensemble des objets pour un agent donné. La station d'administration lit les informations de l'agent et, en agissant sur ce dernier, modifie la valeur de certains objets.

L'architecture des couches réseau selon le modèle *OSI* sur lesquelles s'appuie *SNMP* est la suivante :

Tableau 1 : Le protocole *SNMP* à l'intérieur du modèle *OSI*

Modèle *OSI*		Modèle *TCP/IP* (protocole)
7	Application	*SNMP*

<table>
<tr><td>6</td><td>Présentation</td><td rowspan="2"></td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td>4</td><td>Transport</td><td>UDP</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Réseau</td><td>IP</td></tr>
<tr><td rowspan="3">Interface réseau</td></tr>
<tr><td>2</td><td>Liaison</td></tr>
<tr><td>1</td><td>Physique</td></tr>
</table>

La structure d'informations de gestion de *SNMP* est conforme à celle de *SMI*. Ainsi, pour nommer les objets au sein d'une *MIB*, *SNMP* procède de deux façons :

- la première est un nom unique par objet (ex. : sysUpTime),
- la seconde utilise les notations d'*ASN.1*.

Comme la classification des objets est arborescente, dans le *MIT*, on identifie un objet en parcourant dans l'arborescence le plus court chemin qui conduit jusqu'à ce dernier, en partant de la racine du *MIT*, conformément au codage *ASN.1*.

SNMP est un protocole qui fonctionne de manière asynchrone en ce qui concerne les requêtes/réponses. Ceci a pour but de faire en sorte qu'une entité *SNMP* ne soit pas pénalisée par les délais que peuvent occasionner ses demandes après formulation d'une requête ou d'une réponse à une requête. Parmi les événements importants que peuvent envoyer les agents *SNMP*, il y a les alarmes (*trap*). Mais la réception de ce type de message aboutit au *NMS* par un canal différent. Voyons pourquoi.

Par sa position dans le modèle *OSI*, on peut constater que le *SNMP* est un service qui fonctionne au-dessus de la couche de transport *UDP*. Par conséquent, il a besoin qu'un port lui soit affecté pour qu'il puisse communiquer. Dans les faits, on constate que deux ports lui sont réservés : 161 et 162. Habituellement, la station d'administration formule ses requêtes en passant par le port 161 en direction de l'agent qui les reçoit aussi par le port 161. Cet agent renvoie ses réponses par le même port 161 à la station d'administration qui reçoit cette information toujours par le port 161. Mais lorsqu'il s'agit d'une alarme, l'agent l'émet toujours par le port 161, mais de par la nature du message, ce dernier est reçu à la station d'administration par le port 162. L'alarme est considérée comme un événement extraordinaire.

Pour récapituler, voici les différents cas de figure qui peuvent se présenter, en ce qui concerne les requêtes et les réponses.

Il existe quatre sortes de requêtes :

- GetRequest : obtenir une variable.
- GetNextRequest : obtenir la variable suivante (si elle existe, sinon retour d'erreur).
- GetBulk : rechercher un ensemble de variables regroupées.
- SetRequest : modifier la valeur d'une variable.

Puis, les réponses :

- GetResponse : permet à l'agent de retourner la réponse au *NMS*.
- NoSuchObject : informe le *NMS* que la variable n'est pas disponible.
- Les types d'erreurs sont les suivants : NoAccess, WrongLenght, WrongValue, WrongType, NoCreatio, WrongEncoding, NoWritable et AuthorisationError.

Les alarmes sont : ColdStart, WarmStart, LinkUP et AuthentificationFailure.

Il existe trois versions du protocole *SNMP* : *SNMPv1*, *SNMPv2* et *SNMPv3*.

La version 1, *SNMPv1*, demeure encore la plus largement utilisée. Elle utilise la *MIB I*. Son grand défaut est qu'elle utilise de manière non cryptée le nom de communauté pour accéder à un agent. Les pirates raffolent par conséquent de cette version tout à fait docile du *SNMP*. Ce qui n'est pas du goût d'un bon nombre d'administrateurs de réseaux!

La version 2, *SNMPv2*, est beaucoup plus complexe que la version 1. Elle contient un niveau hiérarchique d'administration plus élevé, ce qui permet d'avoir, dans le réseau, un administrateur central et des administrateurs secondaires. Elle incorpore aussi un niveau plus élevé de sécurité, contient une gamme de message d'erreurs plus vaste, utilise les *MIB I* et *MIB II*. Son champ d'action se trouve ainsi amélioré. La version 2 n'a cependant pas encore réussi à remplacer la version 1 du protocole. Ce qui est normal car il ne s'agit pas encore de la version « définitive » (*Full Standard*), mais d'une ébauche (*Draft Standard*), la version 1 donnant encore de très bons résultats.

La version 3, *SNMPv3*, n'est pas encore au point. Mais il a été prévu qu'elle vienne en remplacement de *SNMPv1*… pour peu que tout le monde se mette d'accord sur ce point. Le débat est encore ouvert. Cette version comprend un module de sécurité plus élevé, un module de traitements de messages, des modules d'application et de répartiteur de paquets. *SNMPv3* est compatible et peut cohabiter avec les versions précédentes.

Le RMON

La *MIB RMON* (*Remote MONitoring*) est une « extension » de la *MIB II*. Son identificateur au sein du sous-arbre est le numéro 16, ce qui lui donne pour *OID* (*Objet IDentifier*) le 1.3.6.1.2.1.16. La *MIB RMON* contient 9 branches pour assurer l'administration de tout un ensemble de supports réseau dont *ethernet*, *FDDI* et token ring. Les deux versions de la *MIB* sont chacune dotée d'un *RMON* qui se différencie par son appellation. Ainsi *RMON* est la version standard tandis que *RMON 2* va avec la *MIB II*. La figure 3 illustre l'arborescence de la *MIB RMON*.

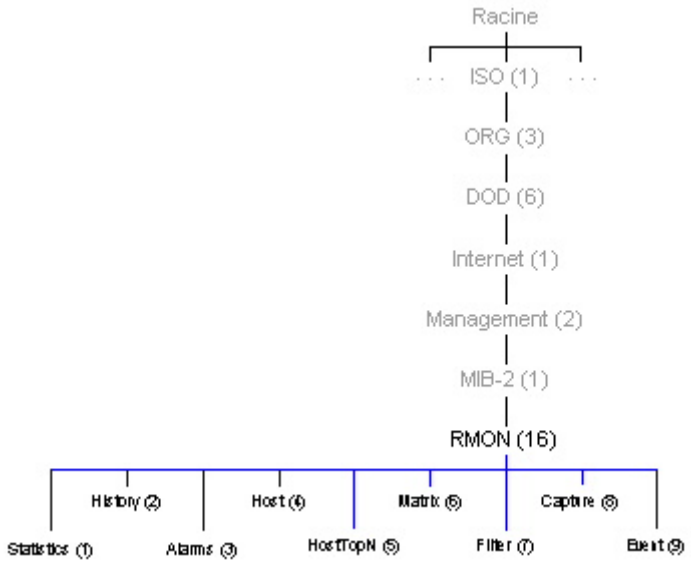

Figure 3 : Arborescence de la *MIB RMON*

Groupe *Statistics* – Contient toutes les informations associées au fonctionnement d'un réseau local *ethernet* :performances en temps réel, nombre d'octets sur le réseau, nombre de paquets, répartition par taille de paquets, *Multicasts*, *Broadcasts*, *CRC/Align*, *Jabbers*, *Fragments* (*Runts*), *OversizePackets*, *UndersizePackets*, *Collisions*.

Groupe *History* – Définition de campagnes de collectes permettant d'avoir des informations sur des indicateurs réseau : performances en temps différé, nombre d'octets, nombre de paquets, *Broadcasts*, *Multicasts*, *CRC/AlignErrors*, *Undersize Paquets*, *Oversize Paquets*, *Fragments* (*Runts*), *Jabbers*, *collisions*, estimation de l'utilisation en % du réseau pendant la collecte.

Groupe *Alarm* – Paramétrage des alarmes, objet concerné, variation ou valeur absolue, intervalle de mesure, mode de déclenchement (seuil en montée, descente), valeur du seuil en montée, valeur du seuil en descente, pointeur vers la table d'actions (groupe *Event*).

Groupe *Host* – Contient les informations de trafics associées à chaque nœud *ethernet* découvert : paquets émis, paquets reçus, octets émis, octets reçus, paquets d'erreurs émis, paquets *broadcasts* émis, paquets *multicasts* émis.

Groupe *HostTopN* – Définition d'études permettant d'avoir une liste d'équipements classée suivant un indicateur de trafic : paquets reçus, paquets émis, octets reçus, octets émis, paquets d'erreurs émis, paquets *broadcasts* émis, paquets *multicasts* émis, nombre d'équipements désirés, durée de la mesure.

Groupe *Matrix* – Contient les informations de trafic entre deux équipements *ethernet* : flux échangé en octets, flux échangé en paquets, flux d'erreurs.

Groupe *Filter* – Définition des filtres sur les captures de paquets : position du filtre dans le paquet, valeur du filtre, masque associé au filtre, masque complémentaire, masque associé à l'état du paquet, masque complémentaire, mode de capture (paquets correspondant au filtre ou paquets complémentaires), événement déclenchant l'ouverture du canal, événement déclenchant la fermeture du canal, nombre de paquets capturés, événement généré quand un paquet est capturé.

Groupe *Packet Capture* – Gestion de l'enregistrement des paquets capturés par le groupe *Filter* : no de canal utilisé, état de la mémoire (mémoire tampon disponible ou saturée), action quand la mémoire tampon est saturée, nombre d'octets enregistrés pour chaque paquet, nombre d'octets remontés par *SNMPGET*, déviation (*offset*) sur les paquets remontés, taille désirée pour la mémoire tampon, nombre de paquets capturés.

Groupe *Event* – Définition des actions associées aux alarmes générées : communauté des *Traps SNMP*, aucune action, émission d'une alarme *SNMP*, enregistrement dans la table des historiques, table des historiques et émission d'une alarme.

La particularité de ces différents groupes est qu'ils ne possèdent pas tous obligatoirement un agent *RMON*, c'est pourquoi un principe de dépendance a été défini. Ainsi, le groupe *Alarm* a besoin de celui des événements tandis que les groupes *HostTopN Group* et *Capture* s'appuient sur la présence du groupe *Hosts*.

Ainsi, pour réaliser des mesures, pratiquement impossibles à distance en environnement architecturé autour de routeurs ou de commutateurs, l'administration réseau bénéficie de

l'implantation locale de sondes. Ce procédé réduit ainsi la charge de trafic occasionnée par les fréquents échanges nécessaires à l'administration réseau pour la constitution de statistiques réalisées par un matériel ne supportant que *SNMP*. (Voir la figure 4.)

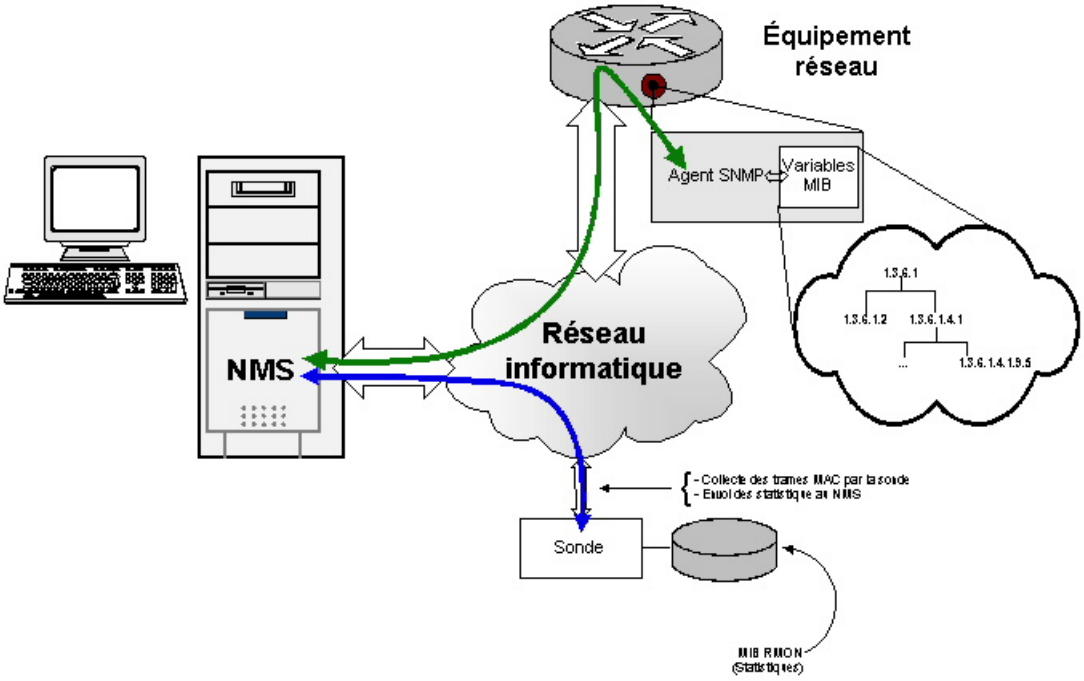

Figure 4 : Sonde *RMON* sur un réseau

RMON a été mis au point par l'*IETF* (*Internet Engineering Task Force*) afin d'étendre les possibilités de *SNMP*. Les sondes connectées sur différents segments du réseau en fournissent des mesures détaillées de l'activité, au niveau 2 (pour la première version), au niveau 3 du modèle *OSI* (pour *RMON 2*), en utilisant des variables *MIB* et les protocoles *SNMP*. Ainsi, là où le processus centralisé recueillerait des informations d'administration, ces sondes rapatrient des informations vers la plate-forme d'administration pour un traitement graphique et les enregistrent éventuellement dans une base des données afin de constituer un historique de l'état du réseau. Les sondes peuvent ainsi prendre l'initiative de collecter presque toutes les trames *MAC* qui transitent par le réseau, tel que spécifié dans les variables *MIB*. La *MIB* peut aussi être paramétrée de telle manière qu'à certains seuils les sondes déclenchent des alarmes *SNMP*.

Malgré l'utilité et l'intérêt évidents de *RMON*, il y a des limites à cette technologie. Celles-ci sont intrinsèques à *RMON* car il s'adresse aux deux premières couches du modèle *OSI* (physique et liaison). Par conséquent, une sonde *RMON* ne pourra analyser que le segment sur lequel elle se trouve, et cette analyse se fera au niveau *MAC* (couche 2, liaison). La reconnaissance des protocoles et de son adressage ne pourra se faire dans *RMON* que si on lui adjoint des groupes de *MIB* qui s'adressent aux couches supérieures du modèle *OSI*.

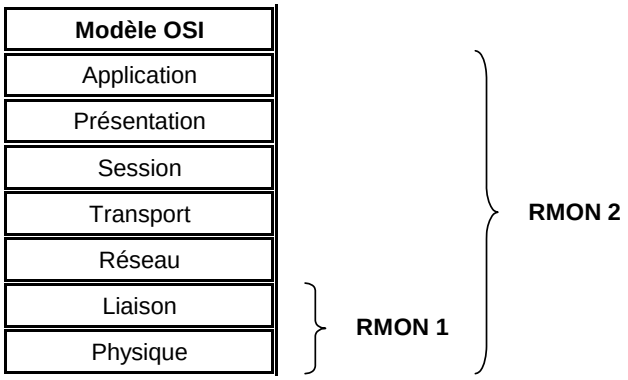

Figure 5 : Champs d'action de *RMON 1* et *RMON 2* par rapport au modèle *OSI*

Les performances de *RMON* – rebaptisé *RMON 1* pour les circonstances – devront donc être rehaussées par de nouvelles spécifications de manière à lui permettre de remonter jusqu'à la couche de niveau 7 (application) du modèle *OSI*. Ce nouveau procédé permettra au *RMON* de traiter les informations extraites et de les faire remonter sur la console de surveillance. La *MIB RMON 2*, s'appuyant sur les spécifications de la *MIB RMON 1*, devrait ainsi posséder les caractéristiques ci-dessous :

- *Protocol Directory* définit les protocoles que la sonde peut analyser.
- *Protocol Distribution* prend les statistiques suivant le protocole.
- *Address Mapping* fait la relation entre l'adresse *MAC* et l'adresse du protocole (ex. : *MAC -> IP*).
- *Network Layer Host* donne une mesure globale des trames suivant le protocole (plus cantonné au segment).
- *Network Layer Matrix* mesure entre deux hôtes (pas forcément dans le même segment).
- *Application lLayer Host* se déplace vers les couches hautes de l'*OSI* pour faire son analyse.
- *Application lLayer Matrix* mesure entre deux hôtes (suivant le protocole applicatif).
- *History* mémorise les statistiques de niveau 3 en local.
- *Probe Configuration* normalise la configuration d'une sonde à partir du gestionnaire.

Ainsi, grâce à l'analyse approfondie des trames, l'administrateur pourra avoir une vue complète du réseau géré. L'administrateur du réseau pourra ainsi déterminer avec précision quelle station de travail a un fonctionnement qui perturbe le réseau. La *MIB RMON 1* ne permettait pas cette fonction car les informations (adresses physiques des stations) contenues dans les couches superficielles de la trame étaient bloquées par les routeurs.

Le document final du groupe de travail *RMON 2* de l'*IETF* a été soumis à la standardisation en décembre 1995.

Les analyseurs de réseau

Il faut savoir qu'il existe sur le marché d'autres outils qui permettent une administration de réseau de manière optimale. Ces outils sont des appareils électroniques appelés analyseurs de réseau et sont uniquement dédiés aux « analyses de réseau ». Ces appareils ne savent rien faire d'autre, mais ce qu'ils font, ils le font bien. De nombreux constructeurs en proposent : des certificateurs de câblage de réseaux, des analyseurs de spectres, des renifleurs de paquets, des explorateurs, etc. Des constructeurs tels que *FLUKE*, *3Com*, *IBM*, *Hewlett-Packard*, *Cisco* et

bien d'autres en proposent toute une panoplie dont un administrateur de réseau ne saurait se passer.

Pour ce qui est de leur mode de fonctionnement, les analyseurs de réseaux se branchent comme un poste de travail, c'est-à-dire directement sur le réseau à administrer. Cette façon de procéder leur donne la possibilité d'observer et de récupérer tout ce qui se passe sur le nœud où ils sont branchés. Étant donné que les réseaux locaux fonctionnent par diffusion, les analyseurs de réseaux pourront observer, récupérer et afficher, sur leurs écrans, tout le trafic du sous-réseau. Les analyseurs ont aussi la possibilité d'afficher sur leurs écrans plusieurs autres types d'information dont :

- l'affichage des trames collectées,
- le filtrage des trames,
- l'instant exact du passage d'une trame,
- le compte des paquets et leur taille moyenne,
- le nombre de collisions, etc.

Il est aussi possible de paramétrer les analyseurs de réseaux, afin qu'ils se déclenchent soit à partir d'une heure donnée, soit à la suite de certains événements, soit une combinaison des deux. Il est aisé de se rendre compte qu'avec de tels outils, l'administration de réseaux peut être extrêmement simplifiée. De plus, l'analyseur peut déclencher l'analyse par rapport à une heure mais aussi par rapport à un événement ou une suite d'événements. L'un des inconvénients des analyseurs de réseaux est qu'ils se limitent au sous-réseau qu'ils observent…

Quelques analyseurs de réseau

Voici quelques analyseurs de réseau présentement sur le marché.

L'*OptiView*™ de *FLUKE*

Visualisation complète du réseau en quelques secondes.
Combine l'analyse de protocoles sur les sept couches *OSI*, la détection active, l'analyse des périphériques *SNMP*, l'analyse du trafic *RMON2* et le test des couches physiques en une seule solution mobile.
La conception et l'interface utilisateur offrent un même niveau d'efficacité, que l'unité soit portable ou placée en liaison réseau semi permanente.
L'analyse distante par l'entremise du Web permet à sept utilisateurs d'accéder en même temps à une seule unité.

CiscoWorks2000 Campus Manager*™ de *Cisco

Campus Manager dispose d'outils tels *Topology Services*, *User Tracking*, *Path Analysis*, de l'affectation de ports *VLAN/LANE* et d'une large gamme de fonctions qui permettent aux administrateurs de réseaux de mieux comprendre, surveiller, configurer, diagnostiquer leur réseau ou de réagir aux changements d'infrastructure.

Campus Manager 3,1 permet d'afficher des cartes de topologie réseau de différentes façons, d'une représentation à plat de la couche 2 jusqu'à des vues abstraites plus représentatives ou plus extensibles vers des réseaux de sites de grande dimension. Ces abstractions se répartissent en deux groupes : domaines gérés et vues réseau. Les domaines gérés sont des vues topologiques des groupes logiques de périphériques organisés en tissus commutés *ATM* et en domaines *VTP*. Les vues réseau sont des représentations physiques du réseau organisées en vues complètes ou abstraites, par exemple en vues des limites du réseau local, vues de couche 2, vues des périphériques non connectés ou vues *VTP*.

La démarche de conception d'un réseau

La conception d'un réseau exige beaucoup de prudence et de bon sens. C'est un grand défi que de mettre sur pied un réseau alors que la technologie évolue à grande vitesse et que le trafic qu'il doit gérer est important. Il ne suffit pas en effet de posséder tous les équipements nécessaires pour cette phase de conception (micro-ordinateurs, câbles, connecteurs, interfaces, imprimantes, systèmes d'exploitation, etc.), il faut de plus maîtriser sa mise en œuvre de manière que le réseau soit évolutif et facile à administrer. Mais, fort heureusement, ce défi n'est pas insurmontable malgré les difficultés que peut poser la conception d'un réseau contenant des milliers de nœuds.

Les administrateurs et les architectes de réseaux sont parfaitement conscients que tous les composants d'un réseau possèdent des exigences particulières. Force est de constater que la conception d'un réseau peut constituer un défi de taille vu que cette tâche dépasse largement le simple branchement d'ordinateurs entre eux. Une fois le réseau défini, il faut en documenter largement les caractéristiques.

Les caractéristiques d'un réseau

- Fonctionnalité – Le réseau doit répondre aux exigences des utilisateurs pour leur travail. Le réseau doit offrir la connectivité utilisateur-utilisateur et utilisateur-application avec une vitesse et une fiabilité adéquates.
- Évolutivité – La conception initiale du réseau doit pouvoir croître sans qu'il soit nécessaire d'apporter des modifications importantes à la conception globale.
- Adaptabilité – Le réseau doit être conçu en fonction des technologies futures et ne doit pas comporter d'éléments susceptibles d'entraver la mise en œuvre de nouvelles technologies, à mesure qu'elles deviennent disponibles.
- Facilité de gestion – La conception d'un réseau doit en favoriser la surveillance et la gestion afin d'assurer la stabilité de gestion de ce réseau.

Les étapes de conception d'un réseau

Pour bien concevoir un réseau, vous aurez besoin d'une bonne stratégie d'approche. Vous éviterez ainsi bien des déboires et vous n'aurez pas besoin de vous lancer dans une course effrénée au câblage. Nous allons vous guider ici à travers l'implantation de différentes architectures (logiques et physiques) afin de vous aider à mieux cerner la manière de procéder lorsque vous serez confrontés à ces situations.

Première étape

Cette première étape consiste à trouver des réponses à des questions telles que :

- À quelles fins servira le réseau?

- Faudra-t-il partager simplement de petits documents, et/ou des documents très volumineux tels que les fichiers graphiques de CAO?
- Aura-t-on besoin d'un réseau capable de soutenir la visioconférence?
- Le serveur de fichiers stockera-t-il des données partagées?

Il faudra bien prendre le temps de penser à tous les cas possibles.

Deuxième étape

Déterminer la durée de vie et le degré d'évolutivité du réseau à mettre en place, car il ne faut pas perdre de vue que la technologie évolue rapidement. Le réseau ne devrait pas devenir obsolète deux ans seulement après sa mise en service!

Troisième étape

Chaque utilisateur doit-il avoir ses logiciels directement installés sur son poste de travail (gros clients) ou chacun doit-il charger son application directement à partir du serveur (petits clients)? Voici les avantages et les inconvénients de chaque cas :

En ce qui concerne les « gros clients », tous les logiciels d'application sont installés sur leurs postes de travail :

Avantages : L'indisponibilité du réseau ne pénalisera pas les utilisateurs qui pourront poursuivre leurs travaux en local. Seules les ressources partagées ne seront pas disponibles.

Inconvénients : Étant donné le grand nombre d'utilisateurs, les mises à jour des applications peuvent demander un certain temps.

En ce qui concerne les « petits clients », tous les logiciels sont installés sur un serveur d'applications :

Avantages : La mise à jour des applications s'avère être beaucoup plus simple. Il n'y a qu'à la réaliser sur le serveur, et tout le monde la possède en même temps.

Inconvénients : Lorsque le réseau tombe… vous tombez avec lui!

La solution des « gros clients » paraît plus intéressante. Les logiciels ne sont pas très souvent mis à jour dans de grandes structures. Quant à la solution d'un réseau de « petits clients », il faut alors songer à doter les serveurs de la technologie RAID 5 pour les mémoires de masse et d'alimentation électrique redondante. Vous aurez besoin de plus d'un serveur de fichiers!

Quatrième étape

L'architecture globale du réseau comporte deux aspects : l'architecture physique et l'architecture logique.

L'architecture physique

L'architecture physique concerne le câblage, les commutateurs, les routeurs, etc. Il faudra retenir l'emplacement géographique des serveurs afin que l'administration soit relativement simplifiée. C'est aussi à ce niveau que sont déterminés les équipements de la couche physique du réseau. Voici trois types d'architecture physique.

L'architecture en bus. Il s'agit un réseau linéaire avec les serveurs connectés sur l'un des bouts et tous les clients connectés à différents points du réseau, que l'on peut

considérer comme étant fédérateur. Le réseau en bus ne donne pas beaucoup de marge de manœuvre et de flexibilité. Il est cependant excellent pour un petit réseau local où l'option d'évolutivité ne sera pas tellement prise en compte. Le grand inconvénient de cette architecture est que lorsqu'une section tombe en panne, une bonne partie du réseau pourra en être affectée.

L'architecture en étoile utilise à volonté des commutateurs ou des concentrateurs architecturés autour d'un commutateur ou d'un concentrateur central auquel tous les serveurs seront connectés. Une telle architecture est très flexible. Si plus de connexions s'avéraient nécessaires, il suffirait d'ajouter d'autres commutateurs ou concentrateurs près de l'endroit à desservir. Il faudra simplement s'assurer d'avoir en réserve quelques concentrateurs ou commutateurs supplémentaires pour le cas où le point de connexion des serveurs arriverait à faire défaut.

L'architecture hétérogène est une combinaison des deux architectures citées plus haut. Une architecture en bus pour relier tous les serveurs et une architecture en étoile pour tous les autres postes de travail clients. Ce modèle d'architecture est très apprécié dans les grands réseaux ou lorsqu'il n'est pas possible de garder tous les serveurs au même endroit.

L'architecture logique

Pour l'architecture logique, il s'agit de savoir si plus d'une adresse *IP* est nécessaire pour le réseau. Pour moins de deux cents postes de travail, un réseau de la classe « C » fera largement l'affaire. Ce type de réseau permet de gérer suffisamment d'adresses *IP* pour les nœuds actuels avec la possibilité d'ajouter quelques équipements dans l'avenir. Il ne faudra pas confondre la topologie logique du réseau avec les différents départements de l'établissement. Ainsi, chaque service n'a pas nécessairement besoin de son propre sous-réseau. Par exemple, si la comptabilité n'a pas besoin d'avoir accès aux données et aux serveurs du département de CAO, il suffit de relocaliser ce département sur un réseau physique et logique différent, voire dans un autre *VLAN*! De plus, il est possible de réduire considérablement les domaines de diffusion et d'accroître le débit du réseau.

L'idéal est de faire en sorte que le réseau soit le plus simple possible. Si on peut concevoir un réseau architecturé autour d'une seule adresse *IP*, alors c'est ainsi qu'il faut le faire. Il faut toujours garder à l'esprit que deux réseaux ayant des adresses *IP* différentes ne pourront pas communiquer directement ensemble. Il faudra munir chacun d'un routeur pour partager des ressources. Si les bonnes précautions ne sont pas prises, un réseau peut exiger plus de soixante heures de travail chaque semaine.

Cinquième étape

Passez en revue le réseau tel qu'il devrait être conçu tout en tenant compte des attentes des utilisateurs. Une fois le câblage réalisé, il sera difficile de procéder à de grandes modifications.

De plus, dans le passé, les administrateurs de réseaux devaient choisir entre les réseaux *Ethernet* partagés et les réseaux commutés en se basant sur le rapport qualité/prix. Mais au vu de la baisse considérable du prix des commutateurs, il n'est plus raisonnable de nos jours de concevoir des réseaux sur cette base. Rappelons brièvement la différence entre ces deux types de réseaux.

Dans les réseaux *Ethernet* partagés, toute la bande passante est partagée par chaque nœud. Lorsqu'un nœud est en transmission, tous les autres doivent attendre la fin de cette transmission avant d'entrer en compétition pour savoir lequel réussira à prendre le relais pour transmettre à son tour. S'il arrive que deux nœuds transmettent en même temps, il y a alors la fatale collision et les données doivent être retransmises. Pour de petit réseaux, ou encore lorsqu'il n'y a pas de gros volumes de données à gérer, ce type de réseau suffit largement. Et vu qu'un nœud récupère les données et les envoie à tous les autres périphériques connectés, on peut se contenter d'utiliser un concentrateur dans un réseau local *Ethernet* avec du câble *UTP*.

Par contre, un réseau commuté est doté d'une mémoire tampon qui lui permet de stocker temporairement les paquets qui doivent être acheminés vers les autres nœuds. Chaque poste de travail possède sa propre bande passante dédiée et n'a jamais à attendre qu'un nœud soit libéré pour commencer à transmettre. Les collisions sont ainsi minimisées, voire inexistantes. Les commutateurs sont conçus pour « connaître » automatiquement les adresses *MAC* des équipements qui leur seront connectés. Ainsi, ajouter de nouveaux postes de travail devient beaucoup plus simple : il n'y a qu'à les brancher et le commutateur « voit » les nouvelles connexions et commence à leur faire parvenir des données. Ainsi l'option du réseau *Ethernet* commuté semble préférable compte tenu des prix très abordables. Certains commutateurs ont même la capacité de « dialoguer » entre eux pour voir comment accroître la puissance de la bande passante. Enfin, il est possible d'interconnecter des commutateurs en passant par différents chemins, ce qui offre l'avantage de faire en sorte que même si un des câbles était coupé accidentellement, la liaison serait maintenue entre les commutateurs. Il suffirait ainsi de créer des lignes de réserve intercommutateurs. Ce qui nous amène à la sixième et dernière étape.

Sixième étape

En cas de panne de réseau, qu'exige le dépannage? Des câbles de rechange, des connecteurs, des cartes réseau (*NIC*), même des commutateurs supplémentaires et une bonne dose d'idées originales! Évitez de connecter directement les équipements aux commutateurs. Passer par des panneaux de brassage qui serviront de relais entre les commutateurs et les différents périphériques du réseau s'avère plus simple pour isoler les pannes. Surtout, utilisez des câbles de catégorie 5/5e au moins. Il faudra enfin pouvoir disposer d'analyseurs de réseaux. Muni de cet équipement, vous êtes fins prêts pour concevoir votre réseau.

La conception d'un réseau fédérateur

Définition

Un réseau fédérateur est un réseau qui, à haut débit, relie plusieurs autres réseaux à performances plus faibles, de manière à centraliser la transmission des informations. Plusieurs autres appellations désignent les réseaux fédérateurs, soit épine dorsale, arête principale, réseau à artère centrale, *backbone*, *backbone network*.

Les différents acteurs dans ce domaine, tant professionnels que grand public, bâtissent leur infrastructure d'accès à Internet autour de réseaux fédérateurs pour desservir des liaisons aux débits inférieurs.

Un réseau fédérateur bien conçu économisera bien des soucis en ce sens que l'administration s'en trouvera facilitée, et que les performances globales en réseau sont excellentes. Grâce aux réseaux fédérateurs, les administrateurs de réseaux peuvent enfin en centraliser l'architecture par l'adjonction d'un point de surveillance. Il est devenu possible, grâce aux *VLAN*, de regrouper sur un même réseau fédérateur des hôtes sur différents segments du fédérateur d'un réseau

local. Et comme les serveurs sont en général installés dans un même local central, ils deviennent beaucoup plus simples à configurer, à sécuriser et à administrer. En effet, les maintenances et les réparations sont plus simples à planifier et à exécuter. Il est possible de réaliser les sauvegardes et l'archivage à proximité des serveurs et même de centraliser le point de départ de toutes les connexions des télécommunications dans le même local.

Les réseaux fédérateurs, en agissant comme points de regroupement de grands volumes de trafic par des liens à large bande passante et à capacités élevées, transportent les données des utilisateurs entre les commutateurs, routeurs et les serveurs directement connectés. Les frontières physiques entre utilisateurs se trouvent ainsi éliminées et la configuration des *VLAN* s'en trouve simplifiée.

Il faut bâtir un réseau fédérateur avec l'idée que ce dernier sera en mesure de soutenir les différents segments des réseaux sachant qu'ils doivent être connectés au réseau fédérateur à l'aide des dispositifs capables de réaliser le routage des données transmises de manière transparente indépendamment de la configuration physique du fédérateur.

Il existe trois méthodes de conception d'un réseau fédérateur.

1. À l'aide de commutateurs

Concevoir un réseau fédérateur à l'aide de commutateurs constitue la manière la plus simple étant donné qu'un commutateur est un pont spécialisé qui crée une connexion virtuelle du type « *one-to-one* » entre un nœud émetteur et un nœud récepteur. Lorsque ce pont reçoit un paquet, il valide une connexion entre le nœud émetteur et le nœud récepteur tout juste pendant la durée de la transmission de ce paquet. À la fin de la transmission, le commutateur met fin à la connexion en attendant le prochain paquet.

Pour concevoir un fédérateur à l'aide de commutateurs, il suffit de relier les segments ou les nœuds individuels aux commutateurs, et de connecter par la suite les commutateurs à d'autres sur le câble fédérateur.

2. À l'aide de routeurs

Dans un réseau fédérateur architecturé autour de routeurs, ces derniers relient les segments au câble fédérateur. Le routeur fonctionne ainsi comme un trait d'union qui relie le fédérateur à chaque segment. Les routeurs possèdent une meilleure tolérance aux pannes que les ponts. Lorsque le réseau fédérateur est réalisé à l'aide de supports unidirectionnels tels que la fibre optique et lorsqu'il arrive que le signal réfléchisse sur lui-même, les routeurs paramètrent les chemins pour assurer une continuité du flux de données.

3. À l'aide de serveurs de fichiers

Dans une topologie de réseaux fédérateurs architecturée autour de serveurs de fichiers, chaque serveur constitue un fédérateur et est doté d'au moins deux interfaces réseau dont l'une connecte le serveur au réseau fédérateur rendant disponible l'accès au réseau fédérateur à tous les segments gérés par le serveur. Les autres interfaces réseau assurent la connexion entre le serveur et les segments qu'il gère.

L'inconvénient? Ce type de réseau fédérateur est d'office une zone de trafic intense des données, ce qui en général provoque des ralentissements considérables lors de la transmission. Ceci est dû au fait que le serveur (ou les serveurs) de fichiers connecte des segments de réseau au câble fédérateur. La plupart des systèmes d'exploitation réseau intègrent des fonctions de routage et de pont qui leur permettent de rallier des segments. Mais il faut s'attendre à ce que les capacités du serveur en soient beaucoup affectées vu que le serveur utilisera plus de ressources, grevant ainsi des traitements vitaux tels que l'administration, par exemple.

Les administrateurs de grands réseaux ou de réseaux trop gourmands en ressources devraient dédier des serveurs, les uns uniquement pour la gestion des fichiers et les autres uniquement pour faire du routage ou faire office de ponts, ou encore, concevoir un réseau fédérateur en se servant de routeurs ou de ponts.

Bien entendu, lorsqu'on a affaire à de petits réseaux ne gérant que de faibles volumes de données, la question peut être revue sans crainte d'amoindrir les performances du serveur de fichiers.

Quelques conseils

Il ne suffit pas de concevoir des réseaux fédérateurs. Il faut avoir assez de dextérité pour en assurer la maintenance, car une fois la conception de réseaux fédérateurs terminée, il faut songer à toutes les possibilités de pannes imaginables. Voici quelques exemples de problèmes susceptibles de se poser.

Congestion du trafic inter-réseaux. Il faut retenir que les réseaux fédérateurs sont le talon d'Achille du réseau car c'est à cet endroit que transite tout le trafic. Si un ralentissement des flux de données se produit sur le réseau, il y a de fortes chances que le réseau fédérateur connaisse quelques ennuis. Un bon indicateur de réseau fédérateur encombré (*clogged backbone*) est l'augmentation du temps de réponse lors de l'acheminement du trafic inter-réseaux, malgré le fait que tous les serveurs ne soient manifestement pas surchargés.

Mais avant d'affirmer que le réseau fédérateur est encombré, il serait plus sage de procéder à certains essais. Il faut s'assurer, dans un premier temps, que les mauvaises performances du réseau ne surviennent que lors des transmissions inter-réseaux. Si l'ensemble des réseaux est affecté par la baisse de qualité des communications (notamment, un ralentissement du flux des données), alors le problème pourrait ne pas provenir du fédérateur, ou du moins, un paramètre supplémentaire pourrait lui aussi être la cause du mauvais fonctionnement. Par ailleurs, un ralentissement global du réseau, entre autres au niveau du flux des données, peut être causé par un facteur supplémentaire, indépendant du réseau fédérateur à la base de la panne. Il faudra aussi être en mesure de déterminer l'emplacement géographique des logiciels utilisés susceptibles de faire baisser le débit du réseau. Si ces logiciels se trouvent sur un autre segment du réseau, il y a alors de bonnes raisons de croire qu'effectivement le réseau fédérateur souffre d'un ralentissement notable du débit des transmissions!

Avant de songer à doter le réseau d'une bande passante plus importante, peut-être faut-il, dans premier temps, voir à délocaliser ailleurs sur le segment les logiciels incriminés sans pour autant pénaliser les utilisateurs des autres segments. Il importe dans ce cas de s'assurer que les utilisateurs sont le plus près possible, physiquement et logiquement, des ressources réseaux qu'ils utilisent le plus souvent. Cela aura pour but de réduire les transmissions inter-réseaux inutiles. Par ailleurs, il est aisé de constater que relocaliser les logiciels est beaucoup plus économique qu'implanter un protocole haut débit dans un réseau fédéré.

La puissance des serveurs. Ce qui devra ensuite attirer l'attention, ce sont les serveurs et les postes de travail. Il faudra s'assurer que ces équipements sont dotés de mémoires suffisantes pour le traitement des fonctions pour lesquelles ils ont été prévus. Veillez à ce qu'ils ne créent pas de goulot d'étranglement. Lorsque les serveurs montrent des signes de ralentissement, c'est que le débit du réseau s'est écroulé. On peut y remédier en installant des serveurs plus puissants. Une autre cause d'effets néfastes sur le réseau est l'utilisation d'équipements incompatibles entre eux.

Les protocoles de communication utilisés par le système d'exploitation peuvent aussi congestionner le réseau fédérateur. En effet, parmi les services créés par les fonctions de communication, il y a ceux qui sont chargés de récupérer les adresses réseau de postes de travail, tandis que d'autres sont chargés de gérer les transferts de données à partir d'un poste de travail sur un segment de données vers un autre poste de travail se trouvant sur un segment différent.

Le protocole *IP*. D'autres protocoles de communication génèrent, quant à eux, énormément de trafic pour toute requête qu'ils émettent exigeant autant de réponses de la station garantissant ce service. Ce constant état de conversation entre le demandeur et le fournisseur a fait que ces protocoles ont été baptisés « protocoles bavards » (*chatty protocoles*). En général, les requêtes et les réponses de ces protocoles sont plus grandes qu'un paquet de données, et par la même occasion, ces protocoles augmentent le nombre de paquets véhiculés dans le réseau. Le protocole *IPX* de Novell fait partie du clan des protocoles dits « bavards ». Fort heureusement, les administrateurs de réseaux optent en général pour le protocole *IP* pour leur réseau puisque ce dernier n'a pas ce défaut. Plutôt que d'émettre une requête et d'en attendre la réponse, ce protocole formule l'ensemble de ses requêtes et les envoie en une seule fois. Il reçoit par la suite ses différentes réponses. Le protocole *IP* est ainsi un meilleur choix que *IPX* en tant que protocole de réseaux fédérateurs. Pour pallier cet inconvénient majeur de son protocole *IPX*, Novell a conçu un module dénommé le *PBURST*. Ce module permet au protocole *IPX* d'émettre ses requêtes en une seule fois aux différents services.

Pour ce qui est des réseaux fédérateurs, il est aussi fortement recommandé d'éviter l'émission de petits paquets. En effet, un gros paquet pénalise moins le réseau qu'un ensemble de petits paquets de données.

Les réseaux à hauts débits. Actuellement, on a tendance à connecter tous les groupes de travail à l'aide de commutateurs dans le but de créer un important réseau commuté. Il est vrai que cette idée va à l'encontre du principe traditionnel des câblages structurés qui veut que les applications soient le plus proche possible des utilisateurs. Cependant, grâce aux *VLAN*, il est devenu singulièrement plus aisé d'administrer les réseaux. On ne doit pas perdre de vue que pour bien concevoir un *VLAN*, il faut prévoir une bande passante suffisante afin que le réseau puisse supporter la charge de plusieurs groupes reliés au réseau commuté. C'est pour cette raison qu'il faut s'intéresser de près aux réseaux à hauts débits.

On se rend ainsi compte qu'une analyse approfondie du réseau s'avère indispensable lorsque survient une panne. Un analyseur de protocole est essentiel lors des diagnostics pour déterminer la destination réelle des différents paquets transitant par le réseau. De plus, cet

équipement aidera l'administrateur de réseaux à apprécier la charge supportée par le réseau qu'il gère et à en déterminer la bande passante en cours d'utilisation.

Il faut retenir deux qualités prépondérantes lors du choix d'un protocole à haut débit pour un réseau fédérateur : la gérabilité du réseau et sa tolérance aux pannes. Enfin, pour concevoir un bon réseau fédérateur, il faut éviter de lésiner sur les moyens! Il faut choisir d'excellents équipements et se munir de la technicité requise.

La sûreté de fonctionnement d'un réseau

La satisfaction d'avoir un réseau enfin opérationnel est acquise lorsque l'on a la conviction de l'avoir totalement sécurisé. La sûreté d'un réseau informatique recouvre aujourd'hui un très grand domaine, car il ne se limite pas au piratage des données qui ne lui sont pas destinées.

Il n'est pas rare d'observer dans la presse informatique des publicités pour telle ou telle « solution » réputée être en mesure de « sécuriser » de manière très fiable le courrier électronique, ou les accès à l'Internet, etc. Ces produits ne comportent pour ainsi dire jamais d'explications sur les risques qu'ils sont sensés nous empêcher de courir. Leurs interfaces d'utilisation sont relativement simples, alors que la sécurité informatique est un domaine complexe. Leurs systèmes de cryptage sont souvent couverts par le secret de la propriété industrielle, alors que d'excellents crypto-systèmes sont disponibles librement et ont fait l'objet d'une revue scientifique internationale sérieuse.

De tels produits doivent inciter l'acheteur à la méfiance. Dans l'état actuel de l'informatique, aucun logiciel ou matériel, quel que soit le soin avec lequel son concepteur affirme l'avoir mis au point, ne peut prétendre à la perfection : il en sera ainsi tant que ce sera des êtres humains qui programmeront les ordinateurs. Et plus le logiciel est complexe, plus il risque de contenir des erreurs. Malheureusement, certaines de ces dernières portent sur la sécurité! Quelqu'un d'assez futé pourrait se servir de ces bogues non seulement pour bloquer le fonctionnement d'un logiciel, mais aussi pour invalider la sécurité d'une portion ou de tout un système informatique.

Certaines histoires d'intrusions sont bien connues; elles ont été relayées par les médias, et font aujourd'hui partie de la légende du piratage informatique. Voici quelques faits.

- En 1986, de nombreux ordinateurs du gouvernement américain ont été infiltrés par des pirates ouest allemands enrôlés par le KGB. Chris Stoll, l'administrateur système qui découvrit les faits, en a tiré un livre devenu désormais un classique : *The Coockoo's Egg* (l'œuf du perroquet).
- En 1988, l'*Internet Worm*, un programme qui s'autoreproduisait, contamina le système informatique scolaire de tout le pays.
- En 1994, un ingénieur de MCI Communication a été inculpé pour avoir intercepté 60 000 numéros de cartes téléphoniques depuis un central téléphonique.
- En 1995, Kevin Mitnick, 31 ans, a été arrêté après une longue carrière de délinquant informatique, comprenant le vol de 20 000 numéros de cartes de crédit, en pénétrant des ordinateurs de Pacific Bell, Digital Equipment Corporation et en détournant pour environ un million de dollars d'informations.

Cependant, aussi inquiétantes que puissent être ces histoires, elles ne représentent qu'une infime partie du problème. Accompagnant la croissance du nombre de machines interconnectées à l'Internet et la conscience du grand public au sujet du développement des « autoroutes de l'information », le nombre d'intrusions explose littéralement. La nécessité d'une protection efficace s'est donc naturellement imposée.

Le domaine de la sécurité informatique est sujet à beaucoup de controverses. Pour la petite histoire, mentionnons une expérience réalisée en 1996. Il a été demandé à 10 000 utilisateurs de payer une modeste participation aux frais d'accès d'une inforoute expérimentale. Tous les moyens de paiement étaient présentés sur le serveur depuis la carte bancaire en ligne sécurisée, jusqu'à l'envoi du numéro de la carte en passant par le télécopieur ou le chèque. Contrairement aux idées reçues, environ 60 % des utilisateurs ont choisi le paiement en ligne sécurisée, 30 % le chèque et 10 % ont préféré l'envoi du numéro de carte bancaire par télécopieur dont un a même fourni le code confidentiel! La perception de la sécurité est donc un élément important à prendre en compte dans le développement de ces systèmes.

Nous examinerons ici une solution qui est retenue dans la plupart des réseaux aujourd'hui : celle du *firewall* ou coupe-feu. Il y sera expliqué dans quelle mesure il est nécessaire de protéger un réseau aujourd'hui et comment fonctionne le coupe-feu, tant du point de vue fonctionnel et que physique.

Un réseau présente de nombreux risques s'il n'est pas correctement protégé contre les intrusions. Ceux-ci sont variés, mais voici les plus courants et qui peuvent présenter un danger quelconque.

- L'espionnage industriel

Ce point concerne essentiellement les entreprises soucieuses de conserver des informations confidentielles. La concurrence pourrait être tentée d'utiliser Internet pour obtenir ces informations.

- La destruction de fichiers

De nombreux fichiers vitaux pour un système sont souvent les cibles privilégiées de pirates informatiques. En effet, à la suite d'une intrusion, les pirates préféreront détruire ces fichiers afin de ne pas laisser de traces de leur passage mais aussi et surtout pour laisser une « porte ouverte » à d'autres pirates!

- L'utilisation du système

De par le fait de l'existence des réseaux interconnectés, les pirates cherchent des « portes dérobées » lorsqu'il est difficile d'accéder directement à un système. Les pirates cherchent alors à s'introduire dans le système en passant par d'autres sous-systèmes qui « ont la confiance » du système ciblé pour arriver à leur fin. C'est une méthode assez courante mais elle nécessite de très bonnes notions de routage.

- Le vol d'informations

Dans tout système informatique, il existe certaines informations qui sont très importantes et qu'on aimerait garder confidentielles. C'est justement ce genre d'informations que recherchent les pirates avec beaucoup d'avidité afin de les utiliser pour toutes sortes de commerces.

Les motifs des pirates sont nombreux et évoluent avec le temps. Il n'est pas vraiment possible de dresser une liste exhaustive des motivations de ces criminels mais, en ce qui concerne des actes intentionnels, voici une partie de leurs motivations : l'espionnage, l'appât du gain, la fraude, le vol, le piratage, le défi intellectuel, la vengeance, le chantage, l'extorsion de fonds. Il y a aussi les actes non intentionnels mais qui constituent tout de même une menace pour les systèmes : la curiosité, l'ennui, la paresse, l'ignorance, l'incompétence, l'inattention...

Les catégories des problèmes de sécurité

On peut grosso modo classifier les problèmes de sécurité des systèmes d'exploitation en quatre catégories, en fonction de la provenance et de la difficulté à parer le danger.

- Protection contre les maladresses des utilisateurs : c'est le cas le plus simple à résoudre. Cette fonction fait en général parti intégrante du système d'exploitation. On trouve par exemple les copies de sauvegarde des éditeurs, les fichiers avec les attributs « lecture seule » ou « protégés » par mots de passe, etc. Une bonne politique de sauvegarde peut en général résoudre de nombreux problèmes de sécurité; cependant elle ne saurait suffire. Sur un système multi-utilisateurs, il serait inconcevable qu'une erreur de manipulation permette à un utilisateur d'effacer le fichier de quelqu'un d'autre! Le système des droits des utilisateurs les protège de façon extrêmement satisfaisante, sans aucune intervention de leur part ni de celle de l'administrateur.
- Protection contre les pannes : la sécurité, dans ce cas, consiste à se protéger contre les pertes de données consécutives à une panne matérielle ou logicielle. Une bonne politique de sauvegarde régulière, efficace et testée (avec des simulations de pannes) s'impose pour tout système, du plus simple au plus complexe.
  Il est à noter ici que haute disponibilité n'est pas synonyme de sauvegarde. On ne doit pas se contenter uniquement de la garantie apportée par un matériel redondant (ex. : des disques RAID) pour la sécurité des données : en effet, le logiciel lui-même n'est pas « redondant ». Lorsqu'un programme devient « fou » et efface tous les fichiers dont il a la charge, le matériel redondant reproduira l'opération sans broncher... Une véritable copie, si possible archivée sur un autre site, s'avère indispensable.
- Protection contre la malveillance externe : il s'agit ici de contrecarrer ceux qu'on appelle communément les pirates informatiques, qui tentent de prendre possession des ressources de votre ordinateur ou de l'empêcher de fonctionner normalement. Rentrent dans cette catégorie les attaques par réseau, les virus et chevaux de Troie, etc. Il faut s'assurer que le système d'exploitation réseau offre des services réseau non publics dûment protégés par mots de passe, et qu'il puisse assurer le cloisonnement des différents comptes système afin de limiter les dégâts en cas d'intrusion. De plus, le système doit offrir des fonctions plus que satisfaisantes de coupe-feu ou de réseau privé virtuel (*VPN*) afin de protéger les autres ordinateurs.
- Protection contre la malveillance de la part d'utilisateurs accrédités : c'est là malheureusement le talon d'Achille des systèmes d'exploitation. N'importe quel utilisateur ayant un accès administrateur sur une machine d'administration peut facilement mettre le système à genoux en consommant toutes ses ressources. Il ne faut pas perdre de vue que la délégation des privilèges est une source fréquente de trous dans la sécurité.

Il reste toutefois que l'administrateur réseau doit s'assurer que le système d'exploitation réseau qu'il gère est doté de fonctions complètes d'émission de traces d'audits (*logs*). Si elles sont correctement paramétrées, ces traces peuvent permettre d'évincer l'utilisateur fautif... et d'invalider son compte sans autre forme de procès, après s'être assuré qu'il n'a pas tenté de confirmer des privilèges indûment acquis en installant une « porte de derrière ».

Les pirates informatiques

Bien qu'il ne soit pas possible de réaliser un portrait robot des pirates, des enquêtes et études ont montré que les criminels en informatique étaient majoritairement des personnes ayant un travail peu gratifiant mais avec d'importantes responsabilités et un accès à des informations sensibles. L'avidité et l'appât du gain sont les motifs principaux de leurs actes. Mais il arrive

aussi que les problèmes personnels jouent un rôle primordial en influant sur le comportement social.

On distingue deux types de pirates informatiques : les hackers et les crackers.

Les hackers

Au départ, un *hacker* est considéré comme une personne qui réalise quelque chose de surprenant, d'inattendu, qui réussit ce qui semble impossible, qui innove et qui étonne. Au fil du temps, un *hacker* est devenu quelqu'un qui s'introduit dans un système pour y poser des actes qui ne lui sont pas autorisés afin d'exprimer son mécontentement au monde entier. Cette cause lui permet du même coup de consulter illégalement des fichiers (données et programmes), de les modifier ou de les détruire, de passer des coups de fils dans le réseau et de communiquer aux frais d'autres utilisateurs. Le *hacker* n'a pas de motivations réelles, on peut qualifier ses actions de « passe-temps ».

Les crackers

Ce sont des personnes dont l'activité favorite consiste à « pénétrer » frauduleusement dans des réseaux informatiques d'entreprises ou des administrations gouvernementales dans le but de percer les codes de sécurité. Selon la « déontologie » du milieu informatique, contrairement au *hacker*, le *cracker* a des motivations réellement criminelles. Il pille des informations et sème des virus par pur vandalisme ou par intérêt financier pour le compte d'un tiers. Son lieu de prédilection pour ces actions est d'agir via Internet.

Avec l'âge (maturité oblige), lorsque *hackers* et *crackers* ont décidé qu'ils sont enfin devenus adultes et qu'ils ont réussi à filer entre tous les pièges que leur ont tendus les forces de l'ordre (qui les traquent sans merci), ces deux catégories d'individus finissent par devenir des recrues de choix pour éprouver la sécurité d'un réseau.

Sécurisation des accès réseau

La sécurisation des accès réseau est l'étape la plus importante de l'activité de l'expert en sécurité. On peut noter les points ci-dessous :

– Auditer son réseau pour trouver les problèmes de sécurité : par exemple, les services privés qui ne doivent pas être accessibles de l'extérieur (exemple type : une imprimante en réseau). *TCP/IP* étant un protocole qui permet de faire abstraction de la différence entre le réseau local et le reste du monde, cette étape est importante et le vendeur du système d'exploitation ne peut pas la faire à la place de l'administrateur.

– Utiliser des protocoles intrinsèquement sûrs. Certains protocoles réseau véhiculent des mots de passe en clair (exemples typiques : *telnet* et *ftp*), d'autres utilisent l'adresse *IP* de l'appelant comme moyen d'authentification, ce qui est notoirement faible (*rlogin*, *rsh*, *NIS* et *NFS*). En fonction des besoins de sécurité du site, ces protocoles devront être réservés à certaines machines ou bien carrément supprimés.

– Éviter les vulnérabilités des logiciels réseau, c'est-à-dire les bogues qui sont exploitables par une personne mal intentionnée. Il convient de différencier celles qui sont accessibles depuis l'extérieur du réseau de celles qui ne le sont pas. Dans de nombreux cas, en effet, le scénario de sécurité est du type « nous contre eux » et un certain niveau de confiance peut être accordé aux ordinateurs du réseau interne.
– Remédier aux défauts constatés en installant des correctifs pour pallier les vulnérabilités découvertes (soit des mises à jour de logiciel, soit des modifications de configuration par défaut) et des procédures de filtrage adéquates pour les services privés.

– Mettre en place un système de surveillance qui allie récupération des alertes, détection précoce des intrusions et surveillance des machines et des réseaux ainsi sécurisées.

– Se munir d'outils de détection. À défaut de ne pas être en mesure de pouvoir lire toutes les documentations de tous les ordinateurs du réseau afin de déterminer les services qu'ils hébergent, l'administrateur de réseau doit se munir d'un outil automatique de détection. Un tel outil (appelé un *scanner* dans le jargon de la sécurité) est indispensable au-delà de quelques postes. On trouve dans cette catégorie les logiciels suivants, librement téléchargeables (voir les quelques liens proposés plus loin) :
    - Nmap est un outil d'analyse réseau simple mais très puissant et rapide. Il liste les ports *TCP* ou *UDP* ouverts sur une ou plusieurs machines, ce qui permet de repérer les services accessibles; il détecte également le type de système d'exploitation de l'hôte distant, en repérant la façon dont il réagit à certaines séquences de paquets inhabituelles.
    - Lorsqu'un port est ouvert, le client du protocole correspondant peut utilement être pointé vers lui pour savoir de quoi il retourne. On citera notamment smbclient pour l'analyse des partages exportés par des machines Windows, rpcinfo, showmount et ypcat pour explorer les protocoles *NIS* et *NFS* (tous deux peu dignes de confiance), et surtout netcat qui permet de réaliser des connexions à volonté en *TCP* ou en *UDP*, typiquement pour taper interactivement du texte vers les protocoles Internet usuels (*POP*, *IMAP*, *SMTP*, *HTTP*, *FTP*, etc.). Telnet peut remplir le même rôle que netcat, mais uniquement pour *TCP*.
    - Nessus est un logiciel complet de recherche de vulnérabilités en réseau. Il émet un rapport complet et facile à lire, dispose d'une interface graphique et de plus sa base de vulnérabilité est fréquemment mise à jour sur le site WWW qui l'héberge.

Pour supprimer un service *IP* ou le restreindre à certaines classes d'adresses, plusieurs méthodes sont disponibles :

- Pour supprimer un service, il suffit le plus souvent d'effacer son paquetage et de tuer le service correspondant.
- Les enveloppeurs *TCP* (*TCP wrappers*) permettent d'interdire certaines adresses *IP* pour certains services, et également de signaler toutes les connexions effectuées à certains ports.
- La voie royale en matière de filtrage *IP* est bien entendu l'installation d'un coupe-feu. À l'inverse des enveloppeurs *TCP*, après installation d'un tel dispositif, l'attaquant opérant depuis une adresse interdite ne pourra même pas savoir si le port correspondant est desservi ou pas! Cependant, la configuration d'un coupe-feu est une tâche ardue.

La sécurité informatique moderne est essentiellement une affaire de course à l'information : il faut en savoir suffisamment pour « boucher » les trous avant que les outils d'exploitation de ce trou ne soient conçus, testés et distribués (ce qui, heureusement, prend plus de temps que de mettre fin à un service). Et même lorsqu'on gagne cette course, il n'est pas question de s'endormir sur ses lauriers! Fort heureusement, il existe de nombreuses sources efficaces mises à la disposition de l'administrateur système consciencieux (ci-dessous et à la fin du chapitre) :

- consulter la liste de diffusion Bugtraq est l'élément incontournable d'information de l'administrateur système de sécurité. Non seulement c'est le canal d'alerte le plus rapide, mais de plus la lecture de cette liste de très haut niveau technique permet de se constituer une véritable culture de sécurité (même si les débuts sont parfois difficiles!).
- surveiller les sites WWW de sécurité : certains ont pour but d'avertir le consommateur (celui de RedHat et celui du CERT, notamment), d'autres... de faire peur aux vendeurs,

en publiant des scripts d'exploitation de trous de sécurité qui sont restés inchangés pendant plusieurs mois!

Si, en dépit de toutes ces précautions, vous repérez une intrusion réussie ou une ouverture de session suspecte sur un des serveurs, toute confiance doit immédiatement lui être retirée. Cette machine ne doit plus fournir de services critiques pour la sécurité du réseau, et elle doit être déconnectée du réseau dans les meilleurs délais. Ses disques doivent être montés sur d'autres machines afin de récupérer ce qui doit l'être (il ne faut surtout pas la faire redémarrer avec son propre disque!); elle ne devra pas être redémarrée tant que l'administrateur ne s'est pas assuré qu'elle ne contient pas de « porte de derrière » ou de « cheval de Troie ».

Et les virus? direz-vous. Cela peut paraître incroyable, mais il n'y a pas de virus sous Linux! Cela tient bien sûr à sa philosophie de conception : la sécurité fait partie du noyau du système et aussi de la mentalité des programmeurs. Pas question, sous Linux, de programmer un logiciel de traitement du courrier électronique qui interpréterait des macro-commandes dans les pièces jointes... Et pour ce qui est des virus plus classiques, qui s'attaquent au système d'exploitation et aux binaires des programmes, il n'est pas tout à fait inenvisageable d'en fabriquer; cependant l'avis de l'auteur est que la compétence nécessaire pour réaliser cela est hors de portée d'un programme automatique (et de surcroît minuscule) comme un virus. L'infodiversité dans le monde Linux est suffisamment importante pour qu'un virus ne puisse pas y trouver de « niche écologique » assez uniforme entre différentes distributions, différentes versions d'un même programme, etc. Et c'est sûrement la raison pour laquelle il n'y a pour l'instant qu'un seul virus Linux, qui exploite une vulnérabilité de confiance de rsh à présent presque totalement éradiquée.

En conclusion, pour utiliser Linux, il faut se creuser un peu les méninges, ce qui oblige l'utilisateur à avoir un minimum de connaissances du système. Plus particulièrement, pour installer Linux, il faut être curieux, car il n'est pas (encore) installé par défaut. Par contre, la plupart des utilisateurs sous Windows sont « passifs », et cliquent partout au lieu de réfléchir un minimum. Dès qu'un courriel un peu bizarre est reçu, la plupart des utilisateurs, sous Windows, cliqueront comme d'habitude, tandis que sous Linux, comme c'est plus compliqué que de cliquer pour lire la pièce jointe, la réflexion exigée pour parvenir à la lecture de cette dernière permettra d'éviter de lancer le virus.

Aspect juridique

Aujourd'hui, il est inscrit dans le code pénal de tous les pays industrialisés que le piratage d'un système informatique est un crime passible de nombreuses peines, souvent lourdes de conséquences sur le plan financier et sur celui des droits civiques.

Les peines varient suivant les délits commis, mais dans tous les cas, le problème n'est pas pris à la légère, et il est fait en sorte de dissuader un bon nombre de pirates informatiques (*hackers*, *crackers*).

Les peines encourues correspondent souvent à une importante somme d'argent, à une bonne peine d'emprisonnement allant de 1 à 3 ans, voire, dans certains cas, l'interdiction des droits civiques pouvant atteindre cinq ans.

La sécurité des informations lors des échanges

D'un point de vue technique, la sécurité recouvre à la fois l'accès aux informations sur les postes de travail, sur les serveurs ainsi que le réseau de transport des données. Nous allons ici nous concentrer sur les problèmes posés par la sécurité des informations lors des échanges au travers de réseaux publics ou privés. Internet, le réseau des réseaux, est un outil qui permet à tous les ordinateurs, quel que soit leur type, de communiquer entre eux. La technologie utilisée

(*TCP/IP*) a permis de simplifier la mise en place des réseaux, donc de réduire l'ardoise des communications. Par contre, ce protocole ne se préoccupe pas des fonctions de sécurité.

Sécuriser les données, c'est garantir :

- l'authentification réciproque des correspondants pour être sûr de son interlocuteur;
- l'intégrité des données transmises pour être sûr qu'elles n'ont pas été modifiées accidentellement ou intentionnellement;
- la confidentialité pour éviter que les données soient lues par des systèmes ou des personnes non autorisées;
- la non-répudiation pour éviter la contestation par l'émetteur de l'envoi de données.
- la confidentialité.

Une des manières d'assurer la sécurité des données serait de protéger physiquement l'accès au matériel. C'est possible dans une pièce ou un immeuble. C'est impossible dès que le réseau est physiquement étendu. Depuis très longtemps, les chercheurs ont travaillé sur ces sujets. Dans tous les pays, les militaires ont développé des techniques permettant de garantir la confidentialité des informations. Progressivement, ces techniques sont devenues nécessaires à de nombreuses activités économiques et leur emploi s'est répandu, favorisé par la diffusion de calculateurs de grandes puissances à bas prix. Aujourd'hui, un système s'est imposé sous de nombreuses variantes. C'est le système à double clé, une publique et l'autre privée, inventé en 1977 par trois chercheurs : Rivest, Shamir et Adleman. Ces trois chercheurs ont donné leurs initiales à leur code, le RSA. Même si nous allons voir cette technique de cryptage d'un peu plus près, il est intéressant de savoir qu'il en existe d'autres, notamment le célèbre PGP de Philip Zimmermann qui a fait beaucoup de vagues aux États-Unis. Mentionnons aussi le DES de IBM.

Dans le système de cryptage RSA, seule la clé privée associée à la clé publique permet de décrypter les informations. La possession d'une seule clé est donc sans aucun intérêt.

Le fait de connaître une clé n'aide pas à trouver l'autre. La théorie mathématique de ce codage asymétrique est maintenant inscrite au programme des classes de mathématiques supérieures. La sécurité du système est fondée sur le temps de calcul considérable nécessaire aux machines les plus puissantes pour trouver les facteurs premiers de nombres de plusieurs centaines de chiffres. Les clés habituellement utilisées comportaient 1 024 ou 2 048 bits ce qui était sensé garantir l'inviolabilité du système. Mais avec la montée en puissance des nouveaux processeurs, les clés utilisées sont codées sur plus de bits (au moins 4 096 bits)

La plupart des cartes de sécurité fonctionnent avec le principe du système à double clé. Chaque carte contient dans sa mémoire les deux clés, une publique en lecture libre par les applications informatiques, l'autre privée qui ne peut être utilisée qu'après la fourniture du code secret à 4 chiffres de l'utilisateur. Ce mode de fonctionnement est bien connu des utilisateurs des cartes bancaires. La confidentialité est obtenue en chiffrant le message entier avec la clé publique du destinataire. Lui seul pourra décoder le message avec sa clé privée après fourniture du code à 4 chiffres.

- L'authentification réciproque.

Elle consiste simplement à demander à la machine de l'utilisateur de coder un mot choisi au hasard avec sa clé privée. Si le décodage avec la clé publique restitue le mot attendu, on est « sûr » que c'est la bonne combinaison (bonne carte = clé privée, utilisateur légitime = code à 4 chiffres) qui a permis cette opération. D'où la nécessité de conserver en lieu sûr la carte et de garder le code à 4 chiffres confidentiel.

L'intégrité des données est obtenue par l'ajout automatique d'un petit message calculé à partir des données envoyées. Ce message est codé à partir de la clé privée de l'émetteur. Une fois

parvenu à destination, le message est décodé à l'aide de la clé publique disponible dans l'annuaire de l'émetteur. Toute modification intentionnelle ou accidentelle des données ou du message d'intégrité est détectée par le destinataire du message.

La confidentialité est obtenue en chiffrant le message entier avec la clé publique du destinataire. Lui seul pourra décoder le message avec sa clé privée après fourniture du code à 4 chiffres.

- La non-répudiation.

Le rejet ou le non-rejet est garanti en demandant à l'émetteur de signer avec sa clé privée. Il est le seul qui puisse réaliser cette opération et tous les destinataires pourront le vérifier avec sa clé publique. Ce système, très simple dans son principe, se complique rapidement.

  - Comment traiter les destinataires multiples? En fait, pour cette raison et pour des raisons de performances, on code avec les clés publiques ou privées une clé plus simple (40 ou 56 bits) qui sert à coder le message et qui n'est utilisée qu'une fois.
  - Comment être sûr que la clé publique n'a pas été modifiée par un intermédiaire? Il suffit de demander à l'autorité de certification dont la clé publique est connue de signer avec sa clé privée. Chacun pourra alors vérifier l'intégrité de la clé.
  - Que se passe-t-il lorsqu'il y a plusieurs autorités de certification?
  - Si une carte est volée ou perdue, comment révoquer la clé publique?
  - Comment limiter la durée de vie d'une certification pour des raisons de sécurité?

Pour répondre de manière satisfaisante à toutes ces questions, il faut mettre en place une organisation pour gérer la sécurité. Ce qui peut naturellement soulever de nouveaux problèmes de sécurité. Il faut que les dispositifs soient proportionnés aux enjeux pour éviter la tentation du coffre unique très sûr dont la porte reste ouverte en permanence.

Ce rapide tour d'horizon des problèmes liés à la sécurité des réseaux informatiques montre que des technologies connues et maîtrisées permettent aujourd'hui de garantir la sécurité de la transmission des informations sur des infrastructures publiques ou privées. Mais pour réussir, il faut aussi gagner la confiance des utilisateurs. Sur Internet comme dans la ville, les rumeurs se propagent relayées par des utilisateurs naïfs ou ignorants. L'exemple des fausses « alertes aux virus » est bien connu. L'utilisation de dispositifs de sécurité introduit des contraintes. Ces dernières ne seront acceptées que si elles sont comprises et proportionnées aux enjeux tout en restant simples à utiliser.

Quelques liens utiles

Tous les liens présentés ci-dessous pointent vers des sites anglophones... Certains documents ou livres traduits sont disponibles sur le sujet; cependant, en raison des délais de publication et de traduction, les informations qu'ils contiennent sont souvent un peu dépassées. Ils doivent donc être considérés plus comme des manuels d'initiation plutôt que comme du matériel d'expert.

Bugtraq est une liste de diffusion de courrier électronique qui parle de sécurité au jour le jour sur le mode de la divulgation complète. Elle est une source indispensable d'informations pour l'administrateur de réseau consciencieux, bien que son niveau technique soit assez élevé. Il s'agit d'une liste modérée, avec un volume d'une vingtaine de messages par jour (ou un seul gros message si on choisit le format *digest*).
http://www.securityfocus.com/archive

La page des errata de *RedHat* liste les mises à jour de sécurité disponibles pour cette distribution. Il est souhaitable de la consulter fréquemment.
https://access.redhat.com/security/updates/

Le *CERT* (*Computer Emergency Response Team*) est une entreprise mise en place au lendemain de la crise provoquée par l'*Internet Worm* de Morris en 1984. Sa tactique est de ne divulguer les trous de sécurité qu'après suffisamment de temps pour que les vendeurs de logiciels aient le temps de le corriger, ce qui fait qu'elle n'est pas toujours assez rapide (et est en butte aux critiques des membres de la liste *Bugtraq*).
http://www.cert.org

La *Secure UNIX programming FAQ* est un très bon document de référence pour programmer des composants sécurisés dans un système UNIX.
http://www.whitefang.com/sup/

Nmap est un excellent outil de *portscanning* qui offre entre autres extensions la fonction de détection du système d'exploitation distant par analyse de l'empreinte *TCP/IP*.
http://nmap.org/

Nessus, SATAN et COPS sont des logiciels de détection de failles de sécurité en réseau qu'il convient de faire tourner périodiquement. *Nessus* est le mieux maintenu et le plus à jour des trois; la documentation de *SATAN* contient des descriptions en détail de vieux trous de sécurité de *SunOS* qui sont une excellente introduction aux problèmes de sécurité du système *UNIX*.
http://www.nessus.org/nessus/
http://www.porcupine.org/satan

Le site ftp.zedz.net contient une archive complète des logiciels de cryptographie sous *Linux*.

StackGuard est une extension du compilateur C qui permet de rendre les programmes C beaucoup plus résistants à une classe d'attaques connue sous le nom de débordements de tampon. Le site propose en téléchargement une distribution de *Linux* entièrement recompilée de cette façon. Une version étendue et à jour est disponible à :
http://www.trl.ibm.com/projects/security/ssp/

Crypto-Gram est une lettre d'information généraliste sur la sécurité informatique et la cryptographie, d'une excellente tenue et accessible quel que soit le niveau du lecteur.
http://www.counterpane.com/crypto-gram.html

Applied Cryptography, Bruce Schneider, New York, John Wiley & Sons, 1986. Traduit en français sous le titre *Cryptographie appliquée – Algorithmes, protocoles et codes sources* (traduction de Marc Vauclair), France, International Thomson Publishing, 1995. Ce livre date un peu (notamment certains algorithmes cryptographiques sont moins dignes d'éloges aujourd'hui), mais il fournit un excellent aperçu du domaine de la cryptographie.

Conclusion

Dans cette section, nous avons pu voir que même si des outils sont censés simplifier la vie des administrateurs réseaux, ceux-ci doivent d'abord faire le choix des composants, avec un budget souvent limité. Entre concentrateurs, ponts, routeurs, commutateurs, administrables ou non, le choix est large et la gamme de prix aussi. Le choix des produits est tributaire des besoins du réseau (déterminés aussi par l'administrateur). Mais avec la forte croissance des réseaux,

l’administration est plus qu’une obligation : c’est un gage de sécurité et de bon fonctionnement pour une entreprise. Nous avons fourni une liste assez longue, mais non exhaustive, de liens utiles où l’on peut se procurer des outils pour l’analyse et l’administration des réseaux pour ceux et celles qui voudraient approfondir leur connaissance en la matière.