De l'intérêt d'utiliser la même plate-forme système sur un campus en général au radical déploiement de GNU/Linux sur l'ENS-Cachan en particulier

Emmanuel Quémener, Pascal Soullard, Pascal Varoqui
<quemener@cri.ens-cachan.fr>,<soullard@cri.ens-cachan.fr>, <varoqui@cri.ens-cachan.fr>

Introduction

L'ENS-Cachan s'est lancée, en l'espace d'une année, dans une vaste entreprise de modernisation de son réseau et ses services. Comme principal point de ces évolutions, la radicalisation de l'utilisation des logiciels libres dans son infrastructure, du réseau à l'utilisateur. Nous aborderons successivement, après quelques éléments introductifs, les chantiers que nous avons entrepris cette année là, à savoir les réseaux, les services, les postes de travail de même que la supervision, la sécurité et la gestion des classes de services. Nous terminerons sur le premier thème évoqué dans le titre : l'intérêt d'utiliser une même architecture, le couple GNU/Linux en l'occurrence, pour toutes les strates de notre édifice informatique.

Avertissement au lecteur

Avant toute chose et afin que tout demeure sans ambiguïté entre les auteurs et le lecteur, il convient de préciser certains points. Ce que nous vous présentons est une expérience vécue, une expérience de déploiement de solutions qui, longtemps, furent confinées dans les laboratoires de recherche ou sur les machines de quelques aficionados des logiciels libres. L'échelle de quelques dizaines d'utilisateurs à quelques milliers exigeaient certainement des précautions d'usage que nous n'avons pas, ne sachant pas lesquelles, appliquées scrupuleusement.
Témoignant donc de nos activités, nous chercherons à les justifier par rapport à notre histoire. Nous aborderons plus précisément les thèmes qui, malgré l'abondance de la littérature, à nous béotiens à l'origine, nous ont causé quelques difficultés.
En dernier lieu, nous nous adressons aux véritables professionnels du système et des réseaux. Malgré les « expériences » que nous avons menées en grandeur réelle à l'ENS-Cachan, la majorité des personnes du CRI n'ont pas suivi de formation particulièrement spécifique en réseau et en système. De plus, nous ne disposons que d'une expérience que dans son sens le plus étymologique, c'est-à-dire sur notre vécu au CRI de l'ENS-Cachan. Aussi les propos que nous tiendrons apparaîtront truismes, inexactitudes, mais ils décrivent notre expérience à l'échelle où nous l'avons menée, et uniquement la nôtre...

Les tâches du CRI de l'ENS-Cachan

La machine au service de l'humain... et l'inverse ?
Le Centre de Ressources Informatiques de l'ENS-Cachan dispose d'un nombre croissant de responsabilités sur les services généraux, allant du réseau informatique aux postes utilisateurs, des serveurs communs au développement d'applications spécifiques, ce pour une nature hétérogène de la destination des postes de travail : salles publiques, départements d'enseignement, laboratoires et administration.

Pour mener à bien cette tâche, le CRI dispose de ressources humaines et matérielles. Alors que l'informatique a pour dessein d'aider l'utilisateur dans ses tâches quotidiennes, le rôle des administrateurs du CRI reste de permettre une disponibilité maximale des équipements. Malheureusement, la disponibilité exigée dépasse généralement leurs heures de présence et donc de possibilité d'intervention en cas de problème.

Disposer d'équipements fiables, tant au niveau matériel que logiciel devient donc une nécessité lorsque la haute disponibilité devient une priorité. De plus, les administrateurs, malgré leurs prérogatives, doivent pouvoir intervenir le mieux possible sur des équipements dont ils n'ont pas la charge habituelle. L'uniformisation des équipements réseaux, services et postes de travail permettent de simplifier la tâche de l'administrateur lors d'une intervention.

Ce que nous avons peu voire pas touché :

- Le concours: École Normale Supérieure, l'ENS-Cachan dispose de longue date d'une gestion informatisée des concours. Elle accueille, depuis plus d'une année, le service commun de gestion des concours des ENS. L'intervention du logiciel libre s'est bornée, dans ce secteur, à permettre des

transactions chiffrées entre les postes clients des différentes ENS et le serveur disposant d'une base Oracle à l'ENS-Cachan. Les coûts exigés par Oracle semblaient si fantaisistes qu'une solution à base de tunnel SSH basé sur **OpenSSH**[1] est depuis utilisée, avec succès ;

- La compatibilité : comme tout établissement de l'enseignement supérieur, notre compatibilité dépend des produits fournis par l'AMU. Les produits, matériels ou logiciels, nous étant imposés, nous n'avons pu faire intervenir beaucoup de logiciels libres sinon compléter le système HP-UX d'outils bien confortables pour utiliser un UNIX dans des conditions plus optimales ;
- La scolarité : toute école dispose d'une scolarité informatisée. Des produits propriétaires originaires de Redmond ayant été choisi, nous ne sommes pas non plus intéressés à ce pan de responsabilité du CRI.

Bouleversement d'une matriochka

Cette poupée gigogne décrit de manière assez représentative la perception que les utilisateurs se font des services informatiques, réduisant souvent cette poupée à leur propre poste de travail et amalgamant sans difficulté leur poste aux réseaux ou services.

Dans notre évolution des réseaux et services généraux, nous distinguerons trois couches :

- les réseaux : les dispositifs permettant la communication d'entité à entité, autrement-dit les routeurs ;
- les services : les matériels offrant un service particulier à un utilisateur, autrement-dit les serveurs ;
- les postes de travail : l'interface directe de l'utilisateur vis-à-vis de l'édifice informatique.

Ces trois couches nécessitent, pour un fonctionnement optimal, trois structures transverses complémentaires : la supervision, la sécurité et la gestion des classes de services. Ces trois structures, développées dernièrement, offrent à l'utilisateur informations, sécurité et garantie sur l'utilisation des services informatiques courants.
Ainsi donc, nous nous attacherons, dans les sections suivantes, à décrire quelles ont été nos évolutions en matière de réseaux, de services et de postes utilisateurs, le tout dans un environnement supervisé, sécurisé.

I- Les réseaux

1) IP bas débit sur ATM haut débit

L'ENS-Cachan dispose d'un réseau informatique depuis plus de quinze ans, à l'époque où celui-ci assurait la communication entre des terminaux et un serveur, généralement dédié aux applications scientifiques. La circulation de données sur un réseau n'était plus une priorité lorsque les micro-ordinateurs apparurent au milieu des années 1980. L'essor d'Internet, au travers de la messagerie électronique et du partage de fichiers, a peu à peu permis au réseau de retrouver son importance dans l'édifice des systèmes informatiques.

Aussi les installations sont-elles passées successivement d'une dorsale en Ethernet épais et de terminaux en AUI à une dorsale en fibre optique multimode et des postes de travail en paires torsadées. A la dorsale, initialement en Ethernet s'est substituée une dorsale de technologie ATM, laquelle distribue toujours au poste de travail un flux Ethernet. Basée sur des équipements 3Com et Fore, cette dorsale permet, par la propagation des VLAN sur ATM via le LANE, la possibilité à une entité éclatée sur plusieurs bâtiments de gérer son réseau comme si elle demeurait sur un même bus. Cette technologie, cependant, imposait une contrainte de taille : seuls 16 ELANs (ou VLAN ATM pour simplifier) peuvent être gérés par chaque équipement ATM, aussi demeurait-t-il impossible d'associer à chaque entité, de part leur nombre, un VLAN particulier pour isoler ses propres flux de toute autre entité. Cette contrainte va imposer certains choix dans la disposition de notre future «zone de routeurs », sorte d'Internet interne à l'école. Nous y reviendrons par la suite.

2) Séparation des zones via IP

Le cadre physique de la transmission d'informations étant fixé, penchons-nous sur la séparation logique à appliquer entre les entités de nature différente telles que nous les rencontrons dans une école : serveurs communs, salles publiques, départements d'enseignement, laboratoires et administration.
Naturellement, l'ENS-Cachan s'est dotée, comme beaucoup d'autres centres universitaires ou scolaires, de trois réseaux séparés : le premier destiné à l'administration, le second aux départements et laboratoires, le troisième aux postes qualifiés de publics, généralement utilisés par les étudiants.
De plus, pour ne pas déroger à la règle en vigueur dans tout réseau, une zone démilitarisée, destinée à jouer le tampon entre mondes extérieur et intérieur, a été ajoutée.
A l'origine donc, quatre réseaux IP coexistaient, chacun composé d'un ensemble de classe C piochés dans la

[1] http://www.openssh.org

classe B attribuée au site ENS-Cachan. Ainsi, l'administration se partageait-elle 16 classes C, les départements et laboratoires 32 classes C, les salles « publiques » 32 classes C. D'autres entités, plus spécifiques, se sont vues ensuite attribuées d'autres classes C.
L'interconnexion entre ces quatre zones, de même que la communication avec l'extérieur, fut confiée à un routeur Cisco série 4700 équipé d'interfaces Ethernet 10BaseT. La sécurité s'établissait au niveau IP, par des filtrages de zone à zone. Chaque machine était identifiée comme associée à une zone et ses communications avec les autres zones se réduisaient au strict minimum. Cette structure ne fut jamais déployée dans sa totalité : le départ de l'ingénieur réseau en place vers d'autres horizons, l'incapacité physique du routeur à supporter une telle charge et le souhait d'un nombre croissant d'entités à prendre leur autonomie informatique stoppèrent net la migration vers cette belle structure policée.

3) Avant le JRES-1999 : délégation et centralisation

Si le CRI assurait la gestion de la dorsale globale de technologie ATM, certaines entités ont préféré, voici quelques années, assurer leur propre gestion de parc informatique, du niveau 1 (équipements actifs réseau : concentrateurs, commutateurs et routeur) au niveau 8 (assistance aux utilisateurs).
Ce choix imposait pour l'entité la récupération de toutes les classes d'adresses IP associées à ses utilisateurs, qu'ils soient enseignants, chercheurs ou étudiants. Ainsi, chacune des zones publiques, recherche & enseignement se voyait amputé d'une fraction de sa zone, l'entité prenant la propre responsabilité de son routage. Les techniques de *proxy arp* se devaient donc d'être utilisées pour permettre encore la communication d'entité à entité. En fait, la situation devenait de plus en plus inextricable lorsque, durant le JRES-1999, le routeur Cisco 4700 devint une brique (bref, rendit l'âme)... A cet instant, nous avons constaté quelle était notre fragilité face à une panne de la sorte. Les problèmes de bogue de l'an 2000 fixés, une réflexion complète sur le réseau et sa structure s'imposait.

4) Après le JRES-1999 : évoluer sans trop vexer

La panne d'un équipement stratégique permet souvent de se pencher sur la susceptibilité d'une panne sur d'autres équipements. Aussi avons-nous entrepris une généralisation de la diffusion de la dorsale ATM dans la majorité des locaux techniques, équipant chacun d'un commutateur Ethernet avec lien montant ATM de marque 3Com ou Fore.

Cette fonctionnalité a ainsi permis le regroupement de certaines entités dispersées sur un même VLAN, donc routable de n'importe quel endroit de l'école. Cependant, un soucis de généralisation nous aurait imposé d'associer à chaque entité un VLAN, mais, nous l'avons vu, nos équipements nous limitaient à 16 ELANs par commutateur ATM.

Comme principal enseignement de cette panne de routeur, nous avons retenu que le routeur de sortie ne doit s'occuper que de la sortie, si puissant soit-il. De plus, dans la mesure où chaque entité déléguée route elle-même les classes C de son domaine, pourquoi ne pas réaliser la même chose et router chaque entité indépendamment.
Pour ce faire, gardons cependant à l'esprit qu'un routage individuel compatible avec un niveau minimal de sécurité impose que son interface interne ne soit utilisée que par une entité ou plusieurs si elles partagent le même bus Ethernet. De plus, de manière à éviter d'inutiles charges de la dorsale, il s'avère intéressant de situer géographiquement le routeur au plus près de l'entité, c'est-à-dire dans le local technique desservant son réseau. C'est dans ce creuset de réflexions que l'idée d'une zone de routeurs a vu le jour.

5) Naissance d'une zone de routeurs

Comme nous l'avons vu, nous désirons placer les routeurs au plus près des entités si elles sont monolithiques. Nous voulons limiter le nombre de routeurs tout en cherchant à en isoler les flux le plus possible. Pour optimiser au mieux la circulation de l'information sur la dorsale ATM, chaque routeur doit être équipé d'une interface FastEthernet ou ATM.

De plus, sachant que l'installation se déroulera sur plusieurs mois, il faut pouvoir redéfinir rapidement les tables de routage de tous les routeurs, même ceux hors de la responsabilité du CRI. Le choix d'un routage dynamique s'impose donc. Avec cela, les paramètres réseau de tous les postes sont à modifier (masque et passerelle). Enfin, les routeurs propriétaires, comme tout produit manufacturé, ont un coût non négligeable et exigent des délais de livraison.

Convergence vers une solution générique
Le choix d'un matériel générique s'est imposé de lui-même : se doter d'une quarantaine de routeurs Cisco de série

2500 est économiquement irréaliste, tout comme l'achat d'une dizaine de Cisco 3600 permettant l'ajout de plus de deux interfaces FastEthernet. Exit également la solution visant à équiper le routeur 4700 d'une carte ATM, puisque sa mémoire est insuffisante et sa tâche réservée à la sortie du site.

La solution à base de PC générique s'avérait donc la plus économiquement réaliste. Restait à choisir un système d'exploitation stable, permettant de réaliser du routage dynamique, à terme du filtrage et du routage multipoints. Un OS à la norme POSIX s'imposait, **Solaris** trop lent et **xBSD** trop peu connu au CRI firent pencher la balance en faveur de **Linux**[2]. Linux fut donc choisi, associé aux outils sous licence **GPL**[3] de la distribution **Debian**[4], parce que, là encore, il s'agissait de la distribution choisie par les deux membres du CRI les plus favorables à l'utilisation de logiciels libres. De plus, **Linux** démontrait déjà son efficacité sur des tâches de routage AppleTalk depuis plusieurs années.

En ce qui concerne la base matérielle, nous avions remarqué qu'un PC équipé d'un 486DX était suffisant pour router 10 Mb/s. Ayant pris le parti d'équiper nos routeurs génériques d'interfaces FastEthernet et de placer plus de 2 interfaces dans un PC, le choix d'un Pentium de fréquence supérieure à 133 MHz semblait opportun. De plus, les cartes devaient être interchangeables à volonté sans configuration dans le BIOS de chacune d'elles : l'interface PCI offrait cette fonctionnalité. Nous avons ainsi fixé notre choix sur une carte 3Com 3c905. Les cartes Pentium ne disposant généralement que de quatre ports PCI, nous nous sommes décidés sur des routeurs Pentium à 4 ports PCI. La chasse aux cartes vidéo ISA fut lancée. De petits disques durs de capacité inférieure à 1 Go feraient largement l'affaire, même devant la nécessité de recompiler un noyau. Ceux-ci seraient situés dans un boîtier amovible permettant l'échange d'un routeur par un autre par le simple échange de disques durs.
Ainsi, le routeur générique était un PC de bureau déclassé, équipé généralement d'une carte mère ASUS T2P4 ou TXP4, d'un processeur Pentium cadencé autour de 200 MHz, de 32 à 64 Mo de mémoire vive, d'un disque dur dans un *rack* amovible d'autour de 1 Go, d'un boîtier *desktop* afin de pouvoir le glisser dans une baie 19", d'une carte vidéo ISA et enfin de 4 cartes réseaux 3Com 3c905. L'investissement se limitait donc, la machine étant déclassée pour une utilisation bureautique, à l'acquisition des quatre cartes réseaux. Les installations logicielles des machines se réalisèrent également progressivement, au gré des migrations. Elles se basaient sur une distribution Debian 2.2 et des versions de noyau 2.2.x avant que le noyau 2.4 ne se stabilise.

Un déploiement progressif
La zone de routeurs fut déployée progressivement. Les premiers routeurs à l'occuper furent ceux des entités ayant pris leur indépendance vis à vis du CRI pour la partie routage (et accessoirement filtrage). A l'origine, entre mars et juin, 6 routeurs « génériques » furent déployés, tous disposant d'un équipement identique, à la géométrie du disque dur près.

Puis, certaines entités disposant d'un routage propre à base de routeurs propriétaires ont nécessité l'installation de nouveaux routeurs. Parmi ces entités hébergées se trouvaient des entités devant assurer leur propre routage, mais leur nature (extérieure à l'école mais bénéficiant de notre connectivité de sortie) exigeait un filtrage particulier. Cette zone fut connectée à notre zone de routeurs directement par la dorsale ATM en utilisant le support du **LANE sous Linux**[5]. Les capacités de routage étant plus que satisfaisantes sur une configuration matérielle restreinte (un routage filtrant à plus de 60 Mb/s), nous avons donc décidé d'utiliser cette technologie pour notre future connectivité sur RENATER2 via InterLAN.

Un ensemble innombrable d'outils
Quels avantages avons-nous tiré de la réalisation de cette zone de routeurs dont les routeurs supplémentaires s'avéraient être des routeurs génériques ?

Le premier avantage qui vient naturellement à l'esprit est évidemment le prix. Pour le prix de 4 cartes réseaux PCI et d'un rack de disque dur amovible (soit autour de 250 euros), un routeur 4 ports FastEthernet dont la capacité de routage avoisinait les 90 Mb/s sans filtrage et 70 Mb/s avec (tests réalisés avec l'outil **TCPspray**). Le second était de permettre l'utilisation des mêmes outils de routage, de supervision et d'analyse que sur une station de travail POSIX. Le troisième de disposer d'une certaine autonomie vis-à-vis des constructeurs.

Le routage IP : GaTeD, Zebra et Mrouted
Le routage, nous l'avons dit, se devait dynamique, pour ne pas rendre la période de migration trop pénible aux administrateurs des routeurs de la zone. Notre choix s'est posé sur OSPF afin d'offrir un routage dynamique qui

[2] http://www.linuxhq.org
[3] http://www.gnu.org/philosophy/license-list.fr.html
[4] http://www.debian.org
[5] http://icawww1.epfl.ch/linux-atm/dist.html

soit implémenté sur les routeurs Cisco des entités autonomes. Le choix de BGP aurait certes pu être un choix plus judicieux, mais il obligeait les administrateurs de routeurs à modifier (moyennant des finances non-négligeables) leur IOS (pour ne pas le nommer). Pour l'outil POSIX nous permettant de réaliser ce routage dynamique sous OSPF, nous n'avons trouvé que **Zebra**[6] et **GaTeD**[7]. Le premier disposait d'un atout majeur : sa licence GPL, mais ne présentait pas la même stabilité que le second, gratuit pour certaines versions assez anciennes. GaTeD fut donc sélectionné pour les premiers routeurs génériques installés. **Zebra**, ces derniers mois, semble avoir très favorablement évolué. Aussi avons-nous décidé de l'utiliser pour les routeurs qui furent installés par la suite.

Cependant, si **GaTeD** puis **Zebra** nous donnent jusqu'à présent entièrement satisfaction, ils n'intègrent pas, en standard, le routage MultiCast complet. **GaTeD** propose bien une solution payante mais la seule que nous avons pu exploiter est Mrouted. Ne proposant qu'un routage DVMRP et pas PIM, **Mrouted**[8] nécessite, si nous voulons réaliser une diffusion MultiCast, un routeur intermédiaire supportant les deux protocoles, par exemple un Cisco hors d'âge (série 1605 par exemple).

Le routage AppleTalk

L'ENS-Cachan a toujours entretenu un parc non négligeable de machines Apple. En conséquence, très tôt, des trames AppleTalk se sont mélangées aux trames IP sur le réseau de l'école. A l'époque du réseau « à plat » (jusqu'en 1995), les répéteurs, ponts filtrants et autres concentrateurs laissaient passer tout cela dans tous les sens dans un joyeux désordre. Deux boîtiers Gatorbox étaient chargés de définir les noms de zone de cet unique brin EtherTalk.

Les inconvénients de cette configuration étaient nombreux, en particulier :

- difficulté de mettre à jour les noms des zones sans perturber l'ensemble du réseau de l'école ;
- beaucoup de machines et d'imprimantes étaient reliées au réseau sans préoccupation de nommage et de zone AppleTalk, ainsi la zone par défaut était encombrée d'une longue liste de matériels complètement impossible à localiser. La seule certitude était qu'ils étaient sur le campus...

En outre la nécessité de segmenter le réseau devenait de plus en plus évidente et c'est ainsi qu'en 1996 une première machine Linux équipée de 2 cartes réseau fût mise en service pour effectuer le routage IP et AppleTalk d'un brin Ethernet reliant une quinzaine de machines.

Pour le routage AppleTalk, deux solutions existaient dans le domaine du freeware : Netatalk[9] et UAR[10]. Quelques expérimentations mirent rapidement en évidence les insuffisances de la solution Netatalk, UAR fût donc installé et donna toute satisfaction.

Un des avantages d'UAR est de permettre facilement connecter en Appletalk des réseaux reliés par internet par des tunnels IP. Cette possibilité fût mise en pratique dès octobre 97 pour relier l'antenne de Bretagne de l'école à Cachan. Ainsi, il devenait possible d'imprimer depuis un Mac en Bretagne aussi facilement que dans le bureau voisin.

La mise en place du réseau de routeur a permis de faire disparaître le fourre-tout Appletalk du brin principal de l'école, les machines à la pomme se retrouvant automatiquement localisées dans une zone correspondant à leur réseau EtherTalk local.

De plus, la création ou la disparition d'une zone ne perturbe plus tout le réseau du campus, chaque routeur gèrant son bouquet de zone AppleTalk indépendamment de ses voisins. Il n'est relié à eux que par le réseau de routeur qui ne contient plus aucune machine cliente, gage de stabilité.
Aujourd'hui ce démon UAR donne toujours satisfaction, néanmoins, comme son développement semble arrêté, la cohabitation avec des noyaux actuels ne sera peut-être pas toujours assurée, et il ne reconnaît pas les interfaces ATM.

La supervision

Nous aborderons les outils de supervision dans la section présentant la machine dont c'est la fonction. Cependant, lors de la connexion pour intervention sur un routeur, il est toujours intéressant de disposer des outils

[6] http://www.zebra.org
[7] http://www.gated.org
[8] ftp://ftp.research.att.com/dist/fenner/mrouted
[9] http://netatalk.sourceforge.net
[10] http://www.cs.mu.oz.au/appletalk/atalk.html

standards comme ping, telnet sur un port, traceroute. D'autres, plus évolués, comme **IPTraf**[11], permettent, en temps réel, de regarder l'état des connexions et leur activité. **MTR**[12] est une alternative agréable à traceroute. D'un point de vue général, la distribution Debian inclut en standard un grand nombre de paquetage dédié à la supervision réseau. La difficulté reste de trouver dans le nombre celui qui nous satisfasse.

Dans le registre des outils indispensables pour que la machine de supervision recueille un maximum d'information, le démon **SNMP**[13] s'avère incontournable. Sa flexibilité (la possibilité de rajouter des MIBs pour, par exemple, recueillir la température du processeur ou la vitesse de rotation du ventilateur) permet une utilisation plus riche que les traditionnels champs SNMP associés aux interfaces réseaux.

De plus, afin de garder une trace de l'activité réseau d'un routeur, la « signature » des connexions est sauvegardée à l'aide de l'outil **NetAcct**[14]. Celui-ci, paramétrable, fournit information sur l'interface, la nature de la connexion (ICMP, UDP, TCP), les adresses source et destination, les ports source et destination, le nombre de paquets et la quantité totale d'information échangée lors de cette connexion.

6) Vers une nouvelle passerelle téléphonique

Bons et loyaux services d'une carte série multi-ports

Jusqu'en 1997, l'école disposait d'un accès distant par minitel grâce à un serveur IBM reconverti en frontal d'accès V23bis sur 4 lignes. La lenteur des communications, l'interface très « spartiate » et la nécessité de se limiter à des accès Telnet sur les machines de l'école en rendait l'utilisation difficile pour beaucoup d'utilisateurs potentiels. A l'heure du WWW et de la messagerie chargée de fichiers attachés, il était difficile de ne proposer que Lynx pour la navigation et au mieux Elm ou Pine pour le courriel. De plus, beaucoup de départements de l'école s'équipaient de serveurs d'accès par modem sur lesquels le CRI n'avait aucun contrôle, ce qui faisait courir le risque de laisser se développer des entrées directes sur le réseau sans forcément une véritable identification de l'appelant. Le CRI a donc décidé de s'équiper d'un accès PPP compatible avec les modems les plus rapides de l'époque : la norme V34.

Le choix du serveur n'a pas fait l'unanimité, certains membres du CRI soutenant une solution du type Portmaster, et un nouveau membre de l'équipe défendant une solution GNU/Linux. Ce dernier a pu obtenir de faire l'essai avec un budget réduit : le prix des modems et d'une carte multi-ports, la machine étant de récupération (un Intel 386 SX 16 MHz devenu inapte à la bureautique). Le serveur a donc été construit sur une base i386 sur laquelle a été installée une carte Cyclade 8 ports, chacun étant relié à un modem SupraFax V34.

Pour permettre un accès PPP simplifié (négociation PPP directe sans passer par un login/passwd) tout en conservant la possibilité de se connecter en mode console vt100, la scrutation des ports a été confiée à **mgetty**[15] (logiciel libre de Gert Doering), lequel passe ensuite la main au daemon **pppd** (version la plus avancée de l'époque : la 2.3.0 sur un noyau 2.0.29). Dans le cas d'un accès console, **mgetty** exécute un accès **telnet** vers une machine d'accueil chargée de l'authentification de l'utilisateur.

Ce système fut mis en service le 7 février 97 et a rapidement donné satisfaction, de part la rapidité de la connexion (le seul goulot d'étranglement étant le lien modem, merci Linux), le nombre d'accès simultanés, et la stabilité de la machine (elle a tourné jusqu'ici sans autres interruptions que quelques pannes de courant et quelques rares opérations de maintenance matérielle). La négociation des serveurs DNS lors de l'établissement du lien PPP pour les clients Windows est un « plus » très apprécié car il permet une configuration simplifiée (username, passwd, n° de téléphone). Très rapidement il y eût des clients des trois principaux systèmes d'exploitation : Windows, MacOS et bien sûr Linux.

Cette configuration n'a connu jusqu'à ce jour qu'une seule modification : un changement de carte mère, le 386SX a fini par lâcher brusquement au bout de 2 ans et a alors été remplacé par un ... 386DX. Début septembre 2001 ce serveur tourne toujours sans modification et a accumulé environ 150 000 connexions depuis sa mise en service.

Les seuls problèmes rencontrés sont totalement extérieurs au serveur lui-même :

[11] http://cebu.mozcom.com/riker/iptraf
[12] http://www.bitwizard.nl/mtr
[13] http://geekcorp.com/snmpd
[14] http://exorsus.net/projects/net-acct
[15] http://alpha.greenie.net/mgetty

- les modems Supra se bloquent aléatoirement, le problème empirant avec l'âge. Dans ce cas la ligne concernée devient inutilisable et les appels tombent dans le vide lorsqu'ils arrivent sur ce modem. La solution trouvée est un reset journalier de l'ensemble des modems par coupure d'alimentation d'une minute chaque nuit. Depuis ils sont tous fidèles au poste ;
- la stabilité de la connexion est très dépendante de la qualité de la ligne France Télécom. Dans certains endroits de Paris par exemple il s'est avéré très difficile d'obtenir un lien V34 durant plus d'une ou deux minutes, alors que d'autres utilisateurs ont obtenu des liens stables pendant plus de 5 heures d'affilé depuis le sud de la France. La résolution de ce problème est bien sûr hors de notre portée ;
- le coût de la connexion est fonction de la durée et du lieu d'appel, ce qui entraîne des factures téléphoniques importantes dans le cas des appels depuis la province.

L'avènement du numérique sur la téléphonie

La stabilité et l'efficacité de la «solution Linux» ayant été démontrées, il fût décidé d'assembler une nouvelle machine pour accepter des accès selon les normes actuelles : V90 et RNIS, tout en conservant les avantages de l'ancienne qui avait eu le temps de faire les preuves de son efficacité.
Les accès RNIS ne correspondaient pas à une demande de beaucoup d'utilisateurs, mais étaient rendus possibles sans supplément de coût du fait de la nécessité, pour un serveur V90, d'être relié au réseau téléphonique par RNIS.

Le nombre de ligne V90/RNIS fût encore fixé à 8, car les nouveaux fournisseurs d'accès de l'offre commerciale ont diminué l'intérêt de cette solution locale. Néanmoins cet accès conserve deux principaux avantages : la confidentialité des informations échangées et l'accès à l'intranet .

Une étude des produits disponibles sur le marché français nous a conduit à choisir une carte DIGI DataFire RAS B4ST. Celle-ci intègre sur une carte PCI les 8 modems, les UART et les interfaces pour 4 lignes RNIS S0 permettant de panacher 8 accès simultanés en analogique V90 et en numérique 64kb/s.

La machine est passée de l'expérimentation à la production en juillet 2001. Pour assurer une fiabilité maximale elle est équipée de deux disques de 1 Go en RAID 1, et son système d'exploitation a été étoffé par rapport à la précédente car la carte DIGI nécessite un environnement Xwindow pour faire tourner les utilitaires de configuration et de supervision. C'est un Pentium 200 Mhz en noyau 2.4.9 qui tourne depuis le début comme une horloge.

Caractéristiques de cette nouvelle configuration :

- suppression des modems externes et de leurs problèmes de «plantages» internes. Petit avantage accessoire : le câblage est beaucoup plus simple car il ne reste que 4 lignes S0 en remplacement des 8 modems et des 8 alimentations de la première machine ;
- stabilité de la connexion bien supérieure, car le lien entre client et serveur est maintenant de nature numérique sur une grande partie du câblage ;
- choix de la distribution Debian qui facilite beaucoup les évolutions futures, l'ancienne distribution Slackware associée à des compilations « sur mesure » de **mgetty** et **pppd** n'avaient pas facilité la mise à jour de l'ancienne machine ;
- d'un point de vue réseau, les affectations d'adresses IP peuvent à présent être allouées en fonction du client, et plus seulement en fonction de la ligne série utilisée. Elles sont prises dans une classe C réservée aux clients PPP, et routée en permanence par ce serveur. Les options *proxy arp* ne sont donc plus nécessaires.

Il est prévu d'intégrer rapidement à cette machine la carte Cyclade, les 16 accès se trouvant alors concentrés sur une machine unique pour en faciliter la gestion.

7) Vers un nouveau point de sortie sur RENATER2

Jusqu'en février 2001, un contrat liait l'ENS-Cachan à France Telecom pour une ligne spécialisée en ATM natif. France Telecom assurait, pour la connectivité IP, la conversion de l'Ethernet en ATM et le routage sur RENATER. Devant dans un futur proche disposer d'un accès direct à RENATER2, nous avons souscrit à un contrat InterLAN entre l'ENS-Cachan et le NRD RENATER2 situé à Jussieu. Passant de 12 Mb/s en IP (alors que nous ne pouvions en exploiter que 10 à cause des interfaces Ethernet du routeur de France Telecom), nous avons opté pour un débit de 20 Mb/s « open », nous permettant, selon la proposition commerciale, de disposer d'un minimum de 20 Mb/s. L'équipement France Telecom se compose donc d'un élément actif assurant la

conversion direct de l'Ethernet en ATM situé dans chaque local technique formant un liaison « point-à-point ». Enfin, nous raccordant directement à un routeur sur RENATER2, l'implémentation de BGP est indispensable.

D'un Cisco 4700 hors d'âge...
Le routeur Cisco série 4700, bien qu'il ait été libéré de la totalité du routage de l'ENS-Cachan, nécessitait un redémarrage toutes les 72 heures pour effacer sa mémoire vive. En effet, ce dernier se saturait et dégradait son routage en un routage poussif à 2 Mb/s. De plus, ne disposant que de cartes Ethernet 10BaseT, il ne nous était pas possible d'utiliser au mieux les 20 Mb/s souscrits auprès de France Telecom. La première approche fut de s'intéresser à l'achat d'un nouveau routeur Cisco série 7200, mais la difficulté de trouver un interlocuteur compétent, son prix prohibitif, le rachat ridicule de notre 4700 et l'âge avancé du châssis 7200 nous ont guidés vers un autre choix, plus générique.

… à un routeur « générique » à interface ATM
Fort de notre expérience sur la zone de routeurs, majoritairement à base de PC, nous avons choisi de franchir le pas en plaçant comme point d'entrée une machine de caractéristiques sensiblement identiques (Pentium MMX à 200 MHz), gonflée en mémoire vive, équipée de deux cartes FastEthernet et d'une carte ATM. Parmi les deux cartes FastEthernet, l'une servirait à l'extérieur, vers l'équipement France Telecom, l'autre en sécurité de la carte ATM, dirigée vers la DMZ.

Pour pallier tout risque de panne, une machine strictement identique fut construite. Clone de la première (aux adresses MAC près), elle permet un remplacement standard plus rapide que n'importe quel contrat de maintenance.

La migration sur RENATER2 ne s'est pas faite sans douleur. Les astuces réseaux de Communications & Systèmes" (basés sur des réseaux privés pour la communication directe d'interface à interface et l'association d'un alias correspondant aux adresses IP publiques) nous ont quelque peu désarçonnés, au point que nous avons, un temps, utilisé un Cisco 2600 déclassé pour établir une connectivité provisoire expérimentale avant de revenir sur notre choix, puis de le valider avant la migration finale. La partie la plus « simple » fut la configuration du routage BGP pour lequel nous avons utilisé Zebra. Le CLI intégré à Zebra étant très proche de Cisco, la configuration n'en fut que plus facile.

Actuellement donc, et ce depuis début juillet, notre routeur d'entrée est un routeur générique sous Linux, intégrant le routage BGP grâce à **Zebra**. Il remplit son office sans difficulté particulière, mais sa charge reste importante, surtout depuis les attaques massives lancées sur le port 80, à la recherche des serveurs Windows 2000. Les 20 Mb/s sont atteints lors des téléchargements FTP (synchronisation de miroirs, par exemple).

II- Les services

Exploitant au mieux la technologie ATM installée au cœur de l'ENS-Cachan par le placement des routeurs au plus près de la dorsale, disposant majorité d'entre eux sur une même matrice de commutation FastEthernet (7 routeurs sur 16 routeurs sont raccordés dans le même local technique), le réseau IP semble désormais exploiter au mieux l'existant. L'étape suivante consistait donc à se pencher sur les serveurs, qui, vieillissants remplissaient de moins en moins efficacement leurs offices à cause de l'augmentation croissante du nombre d'utilisateurs connectés au réseau.

1) Etat des services en septembre 2000

En septembre 2000, de nombreux serveurs tiennent plus de la pièce de musée que de la machine apte à remplir sa tâche en toute sérénité (autrement dit, sans monter à 10 de charge à la moindre requête). La majorité sont des stations de travail déclassées et réutilisées tel que. Nous y trouvons (les parenthèses présentent l'équivalent de puissance en processeur Intel) : 3 Sparc 1+ (i386), 3 Sparc 4 (Pentium 90 MHz), une Ultra 1 (Pentium 200 MHz), une Ultra 5 (PentiumPro 233 MHz). Toutes ces machines Sun sont équipées de disque dur de taille ridicule pour l'époque (quelques Go au mieux), toutes disposent (sauf l'Ultra5) d'interface réseau Ethernet 10BaseT et nécessitent un clavier par unité centrale pour ne pas chercher des difficultés supplémentaires. Le seul serveur sous Linux est un serveur de forums de discussion, basé sur un Pentium 200 MHz.

La situation devient critique lorsque les partitions de systèmes de fichiers, notamment utilisateurs, viennent à se saturer. Ces systèmes sont parfaitement sous-dimensionnés pour les tâches qui leur sont maintenant demandées. Il fallait donc les modifier.

2) Convergence vers une solution générique

A l'origine, nous pensions récupérer des stations de travail Sun Ultra5 destinées aux élèves pour les transformer en serveur. Cependant, cette solution fut rapidement écartée : la puissance brute était 5 fois inférieure à celle d'une machine PC d'entrée de gamme, la mémoire vive installée, sous dimensionnée, exigeait l'achat d'autres barrettes 5 fois plus chères que leurs homologues pour PC, les disques durs IDE étaient médiocres, les contrôleurs IDE de performances décevantes, le clavier ne permettait pas l'utilisation d'un partageur écran-clavier pour PC. Seul point positif, l'interface réseau intégrée est une FastEthernet...

Nous avons donc décidé de nous tourner vers le même type de solution générique que celles utilisées pour les routeurs génériques sous Linux. Comme base, nous avons opté sur une configuration à base de processeur Athlon d'AMD, sur une carte mère ASUS K7V, équipée d'un minimum de 256 Mo de mémoire vive. Pour les serveurs demandant de la sécurité matérielle, nous avons opté pour une carte RAID IDE 3ware disposant de 2 contrôleurs de disque dur et associée à 2 disques durs IBM de 45 Go en 7200 T/mn. Les cartes vidéo et réseau sont respectivement l'entrée de gamme chez ATI et la 3Com 3c905 déjà utilisée dans nos routeurs. Le boîtier est au format bureau, un ensemble de ventilateurs assure un refroidissement optimum de l'unité centrale, face à la dissipation thermique très significative de l'Athlon et des disques durs IBM.

3) Installation de base

L'installation de base consiste, pour les serveurs équipés de carte RAID, à configurer le RAID matériel. Pour redonder complètement le système, nous avons choisi le RAID 1. Le contrôleur 3ware se comporte alors comme un périphérique SCSI associé à un unique disque dur. La synchronisation RAID est assez lente, surtout lors de l'installation originelle ou lors d'un crash. Si e2fsck et synchronisation sont simultanées, l'opération peut durer plusieurs heures sur un disque de plusieurs dizaines de Go.

La migration des services a été relativement rapide, pour les services standards que sont le serveur DNS et MailHost principal, le serveur proxy, le serveur WWW, les serveurs dédiés à des entités telles que le CRI et les salles publiques d'élèves. En effet, les mêmes outils libres étaient installés sous Solaris (**Bind**[16] pour le DNS, **SendMail**[17] pour la messagerie, **Squid**[18] pour le proxy, **Apache**[19] pour le WWW). Seul le serveur de forums de discussion a posé des problèmes, par le changement de version de **INN**[20]. Dans la majorité des cas, la simple copie des fichiers de configuration a suffit à réactiver le service sur un nouveau serveur. Le plus pénible a donc été la fusion de plusieurs serveurs de messagerie en un seul, nécessitant une gestion diplomatique des homonymes.

4) L'accueil des élèves : interopérabilité entre systèmes

Proposer plusieurs outils de travail aux étudiants aussi hétérogènes que sont des postes sous Linux, Solaris ou Windows NT n'est pas sans poser de problèmes d'interopérabilité entre les machines. Aussi, les systèmes doivent-ils permettre d'authentifier de manière unique un utilisateur et d'accéder à ses documents de travail.

Évidemment, l'outil **Samba**[21] semblait la panacée pour une telle tâche : partage SMB sur Windows et partage NFS sous Solaris ou Linux. Toutefois, l'authentification n'était pas aussi simple à gérer : avec les NIS+ d'un côté et le **Samba** de l'autre, il s'avérait impossible de synchroniser simplement les mots de passe des deux univers UNIX et Windows. La principale difficulté venait de la difficulté à passer en entrée standard des caractères aux commandes NIS sous Solaris. De plus, la documentation du **NIS+**[22] sous Linux était très sommaire et exigeait un « bricolage » abondant des fichiers de configuration.

Plus tard, nous avons trouvé une méthode d'authentification globale utilisant les modules PAM, associé à Samba. Le fonctionnement sous Linux a été quasi-instantané, le temps de changer les lignes `auth required pam_unix.so nullok` par `auth required pam_smb_auth.so` dans les fichiers associés aux applications

[16] http://www.isc.org/products/BIND
[17] http://www.sendmail.org
[18] http://www.squid-cache.org
[19] http://www.apache.org
[20] http://www.isc.org/products/INN
[21] http://fr.samba.org/samba/samba.html
[22] http://www.suse.de/~kukuk/nisplus/index.html

demandant une authentification situées dans **/etc/pam.d** , par exemple **login**. Cette tâche suivait celle de la configuration du fichier **/etc/pam_smb.conf** définissant le serveur d'authentification ainsi que son domaine. La même opération sous les Solaris ne déroula sans trop de douleur si bien que nous avons choisi cette unique base Samba pour l'authentification, autant sous Linux et Solaris que sous Windows NT.

III- Les postes de travail

1) La gestion de l'hétérogène

Jusqu'en septembre 2000, les machines mises à disposition des professeurs pour leurs enseignements ou les étudiants étaient de différentes natures : Sparc IPX, Sparc 4, Ultra 5 pour les stations Sun et PC allant du Pentium 133 MHz au Pentium II 233 MHz équipés de 64 Mo de mémoire pour laisser tourner Windows NT dans des conditions tout juste acceptables. L'arrivée d'une douzaine de machines quasiment identiques à nos serveurs, juste équipées pour le multimédia (carte son et lecteur de cédéroms), marqua le début d'une évolution majeure de ces salles «publiques » : d'un parc de machines hétérogènes sur des systèmes hétérogènes, nous voulions converger rapidement vers un parc de machines homogènes disposant de deux systèmes installés : Windows NT et Linux.

L'authentification conjointe de ces deux systèmes sur une même base avait été ``réglée" conjointement lors de la mise en service du serveur des élèves : un serveur **Samba** assurait classiquement celle sous WindowsNT alors que l'utilisation des **modules PAM**[23] pour **Samba** assurait celle sous Linux. Aussi faut-il rajouter à cela un petit bémol : l'obligation que la totalité des utilisateurs apparaissent localement dans **/etc/passwd** et **/etc/shadow** (sans le mot de passe, bien évidemment). Ainsi, un Cron permet la mise à jour de ce fichier régulièrement, permettant le rajout des utilisateurs non encore dans ces derniers fichiers.

2) Le spectre des mises à jour

Le prototype installé dans sa version WindowsNT et Linux devait être déployé. La première étape fut une duplication sommaire, par le démarrage sur disquette et un **dd** brutal . Cette première étape permit de déployer les salles rapidement, mais une intervention était nécessaire (malgré l'utilisation de DHCP) pour utiliser correctement les machines, notamment surtout sous Windows NT.

Les mises à jour suivantes ne pouvaient utiliser la même méthode (ouvrir les machines, démonter le disque dur, faire les duplications, remonter le disque dur). Pour Windows NT et Linux, deux solutions fort différentes furent utilisées.

Sous Windows NT, l'utilisation du logiciel propriétaire Ghost, de Norton, remplit cette tâche sans trop de difficultés. Il est à noter que **Ghost** utilise une diffusion MultiCast pour le déploiement sur les autres postes. Cette méthode aurait l'avantage de n'avoir à diffuser qu'une fois la même information pour toutes les machines si elle ne saturait pas celles qui ne lui demandent rien ! Nos assistants ont fait les frais d'une installation de machine empêchant trois salles de travailler !

Sous Linux, les outils de réplication ne sont pas nombreux. Aussi avons-nous choisi celui qui nous paraissait à l'époque le mieux documenté : **Replicator**[24]. Réalisé par Sébastien Chaumat, à l'ENS-Lyon, cet outil permet la réplication par un **RSync**[25] d'un poste à l'autre, après une configuration initiale complète (partitionnement au besoin, formatage, etc). Lors de la prise en main de cet outil, nous avons constaté certaines anomalies d'installation. Aussi, nous avons placé un script s'exécutant lors du premier démarrage de la machine sous Linux. Sa tâche avait pour but l'installation de **GRUB**[26] en lieu et place de **LILO**[27], afin de fournir à l'utilisateur un choix entre les systèmes Linux et Windows NT moins spartiate que **LILO**. Le **GPM**, permettant l'utilisation de la souris en console, devenait également opérationnel par ce biais.

La réplication se déroulant via un **RSync**, la copie semble peu optimisée pour des installations multiples. Aussi, pour limiter les accès disques sur les mêmes fichiers, nous avons gonflé la mémoire de la machine matrice à son paroxysme. Le dernier point problématique fut l'arrivée d'une nouvelle série de PC ne disposant pas exactement

[23] http://www.us.kernel.org/pub/linux/libs/pam/
[24] http://replicator.sourceforge.net/
[25] http://rsync.samba.org/
[26] http://www.gnu.org/software/grub/
[27] ftp://brun.dyndns.org/pub/linux/lilo/

des même composants. La supervision des éléments matériels de la machine (température de la carte mère, vitesse du ventilateur) n'était plus la même, la géométrie du disque dur, plus étendu, non plus. L'exécutable réalisant la création du fichier de configuration de **LILO** (permettant le premier démarrage sous Linux) ne prenait pas en compte les géométries de disques étendues.

Parmi les services installés sur les machines, un démon **SNMP** permet la supervision, notamment matérielle, assurée par les outils **LM Sensors**[28], lesquels sont disponibles pour la majorité des cartes mères récentes. Leur installation commence par la compilation pour le noyau courant des modules associés au matériel embarqué, puis leur chargement dans le noyau. L'application **sensors** permet ensuite d'aller chercher les paramètres bruts pour leur appliquer des correctifs d'étalonnage. Cette supervision peut sembler superflue, mais elle permet d'anticiper les blocages de ventilateurs de moindre qualité et leur remplacement par d'autres équipés cette fois de roulements à bille.

IV- La supervision

1) Supervision : entre surveillance et information

En septembre 1999, quasiment aucun outil de métrologie n'était installé pour administrer le réseau et les services de l'informatique. Lors de la réalisation de la zone de routeurs au sein de l'ENS-Cachan, la supervision des interfaces réseaux de chaque routeur devint une priorité. Le but était de fournir des éléments sur l'occupation de la bande passante interne et externe.

L'objectif de la supervision telle que nous l'avons menée avait plusieurs objectifs, comme de :

- donner une vision globale en temps réel de l'état du réseau et de ses services ;
- fournir une approche quantitative de la charge des éléments actifs du réseau, du commutateur au poste de travail, en passant par les serveurs et leurs services associés ;
- récupérer les *logs* des routeurs, notamment ceux associés à leur filtrage ;
- présenter à l'utilisateur des informations simples et plus complexes afin de favoriser le dialogue *off line* avec l'administrateur (bref, responsabiliser l'utilisateur).

Penchons-nous sur les informations que nous récupérons et ce que nous pouvons en tirer.

2) Les outils de surveillance de l'administrateur

L'information tire son intérêt de son accumulation puis son analyse. Comme outil d'accumulation d'information, nous avons redirigé la totalité des *logs* de nos routeurs sur cette machine, par un déport du **syslog**. Les *logs* de filtrage apparaissant dans le **syslog**, nous segmentons ce fichier de plusieurs centaines de Mo en plusieurs fichiers, par classe de filtrage et par routeur.

De plus, le stockage, non des problèmes mais des connexions passées, reste intéressant pour procéder à une « ventilation » de la consommation de la connectivité externe. L'outil Acct, disponible pour un routeur Cisco à partir d'une machine sous POSIX, nous a ainsi permis de réaliser une première approche en ce sens. Cependant, l'apparition de plus en plus de routeurs sous GNU/Linux nous incita à utiliser aussi bien sinon mieux : **NetAcct**.

L'installation d'un démon **SNMP** sur les routeurs, serveurs et postes de travail nous a également permis la supervision de paramètres accessibles via les MIBs traditionnelles, mais aussi au travers d'autres MIBs programmées, basées sur l'appel de scripts ou programmes. Les informations tirées vont de la supervision matérielle au nombre de messages dans la queue d'un serveur de messagerie, l'activité d'un proxy, le nombre de connexions et celles établies sur un routeur, l'activité processeur, le trafic instantané sur une interface et bien d'autres informations utiles.

Toujours est-il que stocker ces données reste très lourd. Les compresser pour en limiter la place encore plus. Aussi, une machine dédiée, sûre, puissante, chargée en mémoire vive et en espace disque, demeure indispensable, surtout si nous lui associons également des tâches de calcul comme celles générées par les outils d'information de l'utilisateur.

[28] http://www2.lm-sensors.nu/~lm78/

3) Les outils d'information de l'utilisateur

Pour l'extraction de toutes les informations présentées ci-dessus, leur réduction sous forme de graphe ou de jalon, nous nous sommes, là encore, penché sur l'utilisation des outils libres **MRTG**[29], **AutoStatus**[30] et **CheckService**[31] :

- **MRTG**, réalise des graphes de données. La majorité des données récupérées est de nature numérique. La mise en graphe au cours du temps permet de regarder, à l'échelle d'une journée, d'une semaine, d'un mois et d'une année, l'évolution de telle ou telle variable ;
- **AutoStatus**, très sommaire mais très utile, teste périodiquement l'accès aux machines, l'accès à un service. Il réalise ensuite un tableau avec des feux, dont la couleur symbolise le problème. La double entrée « accès serveur » et « accès service » permet d'un coup d'œil de juger du problème d'un service sur un serveur particulier ;
- **CheckService**, scrute exclusivement les services, mais réalise en plus de statistiques sur l'accès au service.

Pour l'administrateur, **FWLogWatch**[32] permet le classement des *logs* de filtrage issus de différents routeurs, allant de Linux (IPchains, NetFilter) aux autres UNIX (IPfilter) ou les OS propriétaires Cisco. Le filtrage sur les *logs* est complètement paramétrable et le résultat se retrouve présenté sur une page HTML.

D'autres, enfin, oeuvres de Pascal Soullard, réalisent au travers de scripts Perl, une analyse des ports des commutateurs, citant le VLAN associé, les adresses MAC stockées et une équivalence IP des machines concernées.

4) Vers d'autres tâches de supervision

Les outils que nous utilisons ne nous permettent pas, pour l'instant, d'intervenir instantanément sur un problème, notamment, par exemple, une attaque externe de notre réseau. De plus, le filtrage, pour sa part, est également préventif et repose, comme des secours, sur une précaution prise suite à un accident.

Les dispositifs de détection d'intrusion et les outils d'attaques sont le bouclier et le glaive que nous prenons désormais en main pour développer une approche plus préventive que curative.

V- La sécurité

Nous aborderons essentiellement la sécurité au niveau des routeurs. Pour l'accès au serveur et leurs services, les TCP Wrappers comme inetd ont été déployés de la même manière que sur les anciens serveurs Solaris. Le même type de dispositif équipe également les postes de travail des salles publiques. Pour les services proprement dits, la majorité d'entre eux disposent de mécanismes de filtrage de type ACL. Une sécurisation plus approfondie des services fera, sans nul doute, partie de nos futurs chantiers.

1) Sécurité du réseau : filtrage des routeurs

Une politique de sécurité demeure touche le même dilemme : paranoïa et laxisme en sont les deux frontières. Naguères, la sécurité se limitait à quelques ACL sur le routeur d'entrée de site et la protection, sur d'autres domaines « sensibles », par d'autres routeurs. Ainsi, la politique destinée à séparer le réseau en trois réseaux distincts n'avait jamais connu son terme, si bien que la sécurité devenait chaque jour plus précaire. Dès lors, la réalisation de la zone de routeurs, par la segmentation naturelle qu'elle entraîna (séparation et isolation des flux) était propice à l'établissement d'une nouvelle politique de sécurité relativement simple : l'accès à un service dans une entité est interdit tant qu'il n'a pas été explicitement autorisé. Les requêtes de services de l'entité vers l'extérieur sont complètement ouvertes. Cette approche aurait exigé, sur un routeur muni d'ACL ou un routeur générique à base de Linux, une liste exhaustive de tous les services dont une entité a besoin pour travailler. Une solution allait bientôt permettre de simplifier cela à l'extrême, le **NetFilter**[33] des noyaux 2.4 de Linux.

---

[29] http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
[30] http://www.angio.net/consult/autostatus/
[31] http://www.linvision.com/checkservice/
[32] http://cert.uni-stuttgart.de/projects/fwlogwatch/
[33] http://netfilter.filewatcher.org/

2) Une petite révolution : NetFilter des noyaux 2.4

NetFilter marque une évolution majeure dans le filtrage des paquets sous Linux. Les connaisseurs des noyaux antérieurs connaissaient **IPfwadm** ou **IPchains**[34] des noyaux 2.0 ou 2.2, mais **NetFilter** apporte un ensemble de modules simplifiant la conception d'un routeur filtrant de qualité :

- limitation du nombre de paquets dans le temps pour un service donné ;
- définition de plusieurs ports (jusqu'à 15) sur une unique ligne de filtrage ;
- filtrage sur l'adresse MAC (très utile pour une association IP/MAC unique) ;
- marquage des paquets pour l'utilisation des classes de services ;
- modification à la volée des champs TOS des connexions TCP ;
- masquage en source ou en destination des paquets ;
- gestion des connexions.

C'est cette dernière option que nous allons abondamment utiliser. Grâce à elle, il suffit de déclarer que les connexions venant de l'extérieur ne sont acceptées que si elles ont été initiées de l'intérieur. Les drapeaux TCP permettent certes cette fonctionnalité, mais cette dernière se limite, d'une part au TCP et d'autre part à l'analyse de l'entête de la trame. Ici, une table de connexion se crée, comprenant l'état de chacune d'entre elles. Evidemment, une telle approche de filtrage demeure matériellement lourde à mettre en oeuvre. Ceci-dit, le nombre de connexions stockées dans la table peut dépasser les 8192 initiales et notre routeur central a dépassé sans difficulté les 12000 connexions simultanées. Cependant, certaines connexions en retour peuvent ne pas être établies, mais relatives, comme le FTP. **NetFilter** intègre ce dernier aspect par l'ajout d'un RELATED à ESTABLISHED pour définir ces nouvelles connexions correspondant aux réponses d'une requête.

Sur un plan plus pratique, nous commençons toujours par éviter tout *Spoofing* de l'extérieur ou de l'intérieur, par le rejet systématique des classes réservées du IANA[35] et par le rejet de toute adresse ne correspondant par à l'entité routée. Ensuite, l'autorisation de l'ICMP sur certains messages uniquement, et leur limitation à un nombre maximum sur un laps de temps donné, ainsi que les ports de traceroute (nous avons remarqué qu'il était très pénible de tester un service sur un poste sans pouvoir savoir si celui-ci était accessible via le ping). Ensuite vient la définition des services de cette entité qui doivent être accessibles de l'extérieur. Enfin l'autorisation totale d'aller de l'intérieur vers l'extérieur. Cette dernière option sera prochainement associée au filtrage par adresse MAC pour empêcher toute installation de poste informatique sur le réseau sans l'aval du CRI ou toute usurpation simple d'adresse IP. De plus, pour les entités hébergées, certains services sont complètement bloqués en sortie de l'entité (SNMP, RPC, NetBIOS, NFS,...).

Nous mentirions si nous disions que définir la sécurité sur une dizaine de routeurs a été simple. Rappelons que le choix de routeurs à quatre ports FastEthernet exigeait, pour une rationalisation du filtrage, certains aménagements. La puissance de **NetFilter** associée à la commande d'appel **IPtables**[36] nous ont permis de retrouver un fichier de configuration s'apparentant plus à un programme qu'à un fichier de configuration. De plus, les structures en sous-programmes proposés par **IPtables** offrent un balayage des filtres plus optimaux que dans une structure monolithique.

Associé aux modules **NetFilter**, nous ne devons pas non plus oublier d'autres drapeaux mis en place dans le noyau, qui, activés, offrent une protection efficace à des **NMAP**[37] brutaux : le **TCP SYN cookies**.

Pour terminer, l'association de **NetFilter** à la gestion des classes de services permet d'imaginer des prioritisations directement intégrées au routeur réalisant le filtrage.

VI- Classes de services

L'utilisation des classes de services s'est posé lors du rattachement des entités extérieur à l'école sur notre réseau local, initialement pour leur permettre un accès à Internet. Parmi ces entités, deux lycées et les étudiants d'un CROUS. L'installation d'une connectivité à haut débit sur le réseau de l'école eut pour première conséquence la saturation de notre accès à Internet. Une première méthode consista à dégrader leur connexion en plaçant un vieux routeur Cisco 3000 configuré avec des options de lissage de trafic. Cependant, cette solution n'était guère satisfaisante puisqu'elle pénalisait les élèves de l'ENS-Cachan présents au CROUS. De plus, il n'était pas

[34] http://netfilter.filewatcher.org/ipchains
[35] http://www.iana.org/assignments/ipv4-address-space
[36] http://netfilter.samba.org
[37] http://www.insecure.org/nmap

possible de changer simplement dynamiquement la configuration du Cisco pour modifier le lissage le soir, lorsque les personnels de l'ENS-Cachan, partis, n'en ont plus besoin et les étudiants du CROUS le plus besoin.

L'intégration des modules de *QoS and/or Fair Queueing*, associée à l'outil **tc** intégré dans les archives **IProute2**[38], permettent de réaliser pareille opération. Nul besoin de marquer les paquets avec les modules **NetFilter**, **tc** permet la création de classes, pour lesquelles nous définissons des méthodes de lissage, lesquelles sont associées à des filtres. Il est possible, dans ces filtres, de définir une priorité basée sur les adresses source et destination. Ainsi donc, nous réalisons deux filtres dont le premier, prioritaire, concerne ce qui va de l'entité au campus de l'école. Le second, lui, concerne ce qui va de l'entité vers ailleurs (c'est-à-dire toutes les adresses IP). Pour une connexion complète, il est nécessaire de créer deux classes, la première telle que nous l'avons créée et la seconde réciproque.

Pour réaliser la modulation en fonction du moment de la journée, deux fichiers de configuration existent : l'un pour le jour, l'autre pour la nuit. Un **Cron** assure le changement de configuration.

VII- GNU/Linux : une chance pour notre CRI ?

Revenons maintenant au titre de cet article ; nous évoquions l'intérêt de disposer d'une même plate-forme sur un campus, à savoir GNU/Linux, pour le routage, les services et les postes de travail. En fait, le mot directeur de notre témoignage a été « générique ». Nous avons cherché, pour tous nos chantiers, à poser un cadre matériel « générique » dont la principale force repose, non seulement dans son prix, mais dans la réactivité que nous avons pour remplacer le matériel si un problème intervenait. D'un point de vue logiciel, nous avons la même projection : possibilité d'intervenir avec ses capacités sur un service en se focalisant exclusivement sur la tâche à accomplir, sans être « pollué » par les changements incessants de clavier, de *shell*, de formatage de réponses, d'options d'outils d'investigation.

En ce sens, nous sommes parvenus à notre objectif : si, naguères, une personne et une seule pouvait intervenir sur nombre de services, nous sommes désormais trois, certes avec nos spécificités, à pouvoir agir. Sur le plan de la formation à ces systèmes, il n'est plus nécessaire d'assister à de très coûteuses formations trop spécifiques pour devenir, rapidement, opérationnel : la multiplication des documentations, des revues de vulgarisation, les formations dans des organismes moins mercantiles sont les éléments d'un rapide apprentissage.

Le bilan financier de telles évolutions se limitant à du matériel, parfaitement générique, suffit à estimer les économies réalisées par rapport à des solutions que d'autres qualifieront de professionnelles, parce que propriétaires. La dizaine de routeurs de la zone de routeurs construite auront eu un coût de revient de moins de 3000 euros ; le remplacement de la dizaine de serveurs environ 15 000 euros. Tout ceci intégrant les machines et les composants matériels de réserve (le *spare*). De plus, aucun frais de maintenance n'est venu s'ajouter à nos déploiements. Face aux récentes difficultés d'intégrateurs, voici un point qu'il est difficile de nous reprocher.

Désormais, nous pouvons conclure que le couple GNU/Linux remplit, pour nombre de tâches au CRI, parfaitement son rôle. Stable, puissant, gratuit, nous avons donc, en peu de temps, modifié dans de vastes proportions, ce qui existaient auparavant. Deux instantanés avant et après permettent d'en juger.

C'est justement au niveau des utilisateurs que le déploiement de logiciels libres est le plus faible. Des laboratoires ou départements d'enseignement utilisent des PC sous GNU/Linux, mais chacun a choisi sa propre distribution : RedHat, Mandrake, SuSE et Slackware sont utilisées quotidiennement. Le CRI aura certainement un rôle à jouer dans un futur « cadre de cohérence technique » définissant pour tous les outils recommandés. L'efficacité lors d'une intervention est à ce prix.

Conclusion : des solutions « dynamiques », tournées vers l'avenir

N'ayant à l'origine que peu d'expérience dans des déploiements à grande échelle, nous avons souvent tâtonné, perdu du temps notamment pour l'installation des machines, opérations très séquentielles que nous aurions pu confier à un dispositif automatique.

Notre futur chantier sera la mise en place de l'outil **FAI**[39], fraîchement développé par Thomas Lange. Ce dernier permet l'installation de machines après leur définition par des classes particulières. Il s'agit d'un outil qui se

[38] http://defiant.coinet.com/iproute2/
[39] http://www.informatik.uni-koeln.de/fai/

soustraira avantageusement à **Replicator** dans la mesure où il installe la machine comme si nous étions devant et pas par un **RSync**. Cette maîtrise nous permettra ainsi l'installation d'un nouveau routeur, serveur ou poste de travail par une personne n'ayant *a priori* aucune connaissance approfondie des fonctionnalités : en résumé, un matériel générique directement construit et adapté à sa tâche. Nous ne développerons pas davantage les solutions à base de logiciels libres que nous comptons mettre en place dans les prochains mois. Nous « sécuriserons » certainement les services de manière plus significative, par la commande d'arrêt ou de démarrage des serveurs à distance, par une généralisation des systèmes de fichiers journalisés, par un filtrage plus accru des services.

La principale difficulté que nous rencontrons vient de l'utilisation de projets, qui, lorsqu'ils sont trop « verts », risquent de ne pas drainer une communauté de développeurs suffisante pour en assurer la pérennité. Nous sommes contraints de continuellement assurer une veille technologique sur les nouveautés en matière de logiciels libres, comme dans tout autre domaine.

Pour conclure, nous estimons avoir, par ces évolutions, retrouver une certaine liberté vis-à-vis des solutions propriétaires. Evidemment, cette liberté est toute relative puisqu'elle se base sur la confiance faite aux développeurs de logiciels libres. Mais, dans des domaines aussi réactifs que sont l'informatique et le réseau, la communauté *Open Source* montre chaque jour plus de réactivité.

Remerciements

Nous tenons, pour clore ce témoignage, à remercier en premier lieu les développeurs de logiciels libres, qui, au travers du couple GNU/Linux, permettent désormais à tout utilisateur de disposer d'outils de qualité professionnelle pour leur travail. Ensuite, nous exprimons notre gratitude aux utilisateurs compréhensifs et reconnaissants, qui, par leur témoignage, ont reconnu les améliorations apportées aux services informatiques. Enfin, sans le soutien et la confiance de notre direction, nous n'aurions pu mener tous nos projets à leur terme. A ce titre, nous remercions Pierre Bazart, directeur des ressources informatiques de l'ENS-Cachan, pour la confiance et la patience dont il a fait preuve durant ces mois d'évolutions.