Réseaux locaux

Michel Quercia, avril 1997

Résumé : *Présentation des services que l'on peut attendre d'un réseau local, notamment le transfert de fichiers et l'impression à distance. Description sommaire des protocoles Ethernet, IP et TCP et racordement d'un réseau local au réseau Internet au moyen d'un pare-feu et de serveurs mandataires. Présentation du réseau local du lycée Carnot (Dijon) reliant une cinquantaine de PC mixtes Windows/Linux et des problèmes de fonctionnement constatés.*

1. Services disponibles dans un réseau

Un réseau est un dispositif reliant plusieurs ordinateurs et permettant le transfert de *données* d'une machine à une autre ou à plusieurs autres. La définition d'un réseau comprend :

– Le mode de transport physique : câblage électrique, fibre optique, ondes radio, ...
– Les méthodes d'identification des machines sur le réseau ;
– Le format des données échangées et les règles de communication entre les machines (protocoles).

On parle de réseau local (LAN = Local Area Network) lorsque les machines sont physiquement proches (dans une même salle, un même bâtiment, ...) et de réseau étendu (WAN = Wide Area Network) dans le cas contraire. Le réseau Internet n'est pas à proprement parler un WAN car les machines qui y sont reliées n'appartiennent pas à l' Internet Society, il s'agit en fait d'un ensemble de réseaux locaux ou étendus interconnectés à l'aide *routeurs* ou de *passerelles*.

La méthode de communication la plus fréquemment employée sur un réseau est la méthode *client/serveur* : une machine C contacte une machine S et lui demande l'exécution d'un *service*. S vérifie que C dispose des autorisations nécessaires, exécute le service demandé et éventuellement renvoie à C le résultat de sa *requête*. Le client, C, est la machine qui demande, le serveur, S, celle qui répond ; cette distinction entre les deux machines ne vaut que pour la communication considérée, il est tout à fait possible que pour une autre communication les rôles soient inversés. Il est même possible que C et S soient en fait la même machine, la véritable notion est celle de programme client et de programme serveur.

1.1. Transfert de fichiers

Le premier service que l'on trouve sur un réseau est celui de transfert de fichiers : le client demande au serveur de lui transmettre tout ou partie d'un fichier résidant sur S dont il indique le nom (accès en lecture) ou de copier dans un fichier précis les données qui suivent (accès en écriture). Le partage de disque est une variante : C demande à S un accès en lecture seule ou en lecture/écriture à un disque ou un répertoire détenu par S. Si l'accès est accordé, C fait croire à son utilisateur et à ses programmes qu'il disposent d'un nouveau disque ou répertoire. Les programmes tournant sur C peuvent accéder aux *fichiers distants* exactement de la même manière qu'aux *fichiers locaux*, le système d'exploitation de C se chargeant d'aiguiller les ordres de lecture/écriture vers son disque ou vers S.

Parmi les protocoles régissant le transfert de fichiers, on trouve :

– FTP : File Transert Protocol, utilisé pour des transferts «manuels» ;
– NetBIOS : Network Basic Input/Output System, utilisé pour les partages de disque entre machines Windows ou OS/2 ;
– NFS : Network File System, utilisé pour les partages de disque entre machines Unix.

Un transfert de fichiers ne peut avoir lieu que s'il existe un client sur C et un serveur sur S (il s'agit de programmes) parlant le même protocole. La différence entre FTP d'une part et NetBIOS,NFS d'autre part est qu'un transfert sous FTP relève d'une intervention de l'humain utilisateur de C tandis que les transferts sous NetBIOS/NFS sont effectués à l'initiative du système d'exploitation de C sans que son utilisateur humain en soit averti. Cette différence n'est toutefois pas absolue : un programme peut se substituer à un utilisateur pour lancer une requête FTP, répondre aux questions du serveur et transférer un document, tout cela automatiquement.

Un *serveur de fichiers* est une machine utilisée uniquement pour répondre aux requêtes de transfert de fichiers (uniquement signifie qu'il n'y a pas d'humain utilisant cette machine comme poste de travail). On utilise un serveur de fichiers pour stocker des répertoires volumineux ou non en un seul exemplaire, partagé entre les clients grâce au réseau. En général, le serveur exporte son disque en lecture seule, donc les fichiers détenus par le serveur de fichiers sont automatiquement protégés contre les attaques virales, les sabotages ou fausses manipulations de la part des clients sous réserve que le serveur de fichiers soit convenablement protégé. Outre cette protection, la maintenance et la mise à jour d'un logiciel distribué par serveur de fichiers sont facilitées par le fait qu'il ne faut intervenir que sur une seule machine, le serveur (ceci n'est pas toujours vrai, il peut être nécessaire de modifier les fichiers de configuration du logiciel sur les machines clientes). Dans la mesure où le serveur dispose de suffisamment de place, on peut même garder à disposition les anciennes versions pour les utilisateurs nostalgiques.

Par contre, l'accès à un fichier distant est plus lent que l'accès à un fichier local et, en cas de panne réseau, les logiciels du serveur sont indisponibles et les clients risquent d'être mis en chômage technique. La lenteur des accès distants peut être atténuée en utilisant un serveur rapide, la sensibilité aux pannes en prévoyant un serveur de secours. Enfin, certains logiciels ne peuvent fonctionner en réseau car ils tentent d'accéder en écriture à leur répertoire natif ce qui est refusé par le serveur. On notera par ailleurs que le fait d'installer un logiciel sur un serveur de fichiers impose d'avoir autant de licences qu'il y a de postes connectés au serveur, ce qui peut s'avérer problématique dans le cas d'un réseau de grande taille.

1.2. Impression à distance

Ici, le client envoie au serveur des données à imprimer. Le serveur est soit un ordinateur disposant d'une ou plusieurs imprimantes, soit directement une imprimante munie d'une interface réseau. La solution ordinateur + imprimante est plus souple à configurer notamment en ce qui concerne les autorisations d'accès, la solution imprimante réseau fournit un service plus rapide mais coûte plus cher. Dans les deux cas le serveur d'impression gère une *file d'impression* ce qui permet d'assurer que les documents envoyés par différents clients en même temps ne se mélangent pas sur le papier. Dans certains cas on peut examiner depuis un client cette file, modifier l'ordre des documents en attente et supprimer un document non encore imprimé.

La transformation du document à imprimer en codes compréhensibles par l'imprimante peut être réalisée par le client avant expédition sur le réseau ou par le serveur après réception. Dans le premier cas la charge de travail imposée au serveur d'impression est faible, mais les clients doivent connaître le modèle d'imprimante utilisé et disposer en local ou sur un serveur de fichiers des pilotes adaptés à cette imprimante. Dans le second cas le serveur d'impression travaille plus mais l'installation est plus souple car on peut changer de modèle d'imprimante sans avoir à reconfigurer chaque client. Dans les deux cas, lorsqu'on utilise un ordinateur comme serveur d'impression, la charge de travail résultant pour le serveur reste faible (si les impressions sont peu fréquentes) et l'ordinateur peut en même temps être utilisé comme poste de travail ou serveur de fichiers.

Les protocoles permettant l'impression à distance sont :

- NetBIOS pour les machines Windows ou OS/2 : la mise en forme des données est à la charge du client ;
- RPC (Remote Procedure Call) pour les machines Unix : la mise en forme des données est à la charge du serveur.

L'impression en réseau permet de n'utiliser que quelques imprimantes, une ou deux par salle suffit, et de rendre accessible depuis chaque poste relié au réseau toutes les imprimantes du réseau. En particulier on peut ainsi partager des imprimantes chères (haute résolution, couleur, ...) sans obliger les utilisateurs à lancer les impressions depuis un poste de travail spécifique. Il n'y a pas d'inconvénient particulier à utiliser l'impression en réseau, si ce n'est d'avoir à surveiller le serveur d'impression pour éviter que les travaux en attente ne s'accumulent lorsque l'imprimante manque de papier (et ressortent trois jours après lorsqu'on la recharge en papier). Par ailleurs, une panne du service d'impression n'a pas les conséquences dramatiques qu'a une passe d'un serveur de fichiers.

1.3. Autres services

Pour mémoire, on trouve aussi sur les réseaux les applications suivantes :

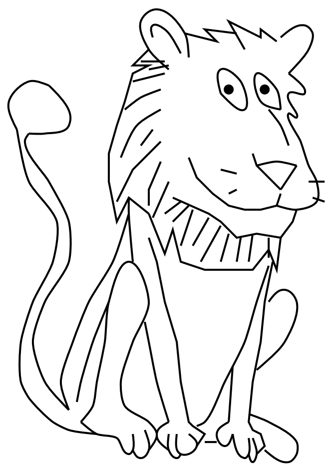
Terminal distant (protocole Telnet) : Le client demande l'accès à un compte utilisateur reconnu par le serveur. Si la connexion est acceptée, l'utilisateur peut lancer des commandes sur le serveur en utilisant le clavier du client et lire les résultats sur l'écran du client (ou dans une fenêtre en mode graphique). L'intérêt de ce service est de pouvoir utiliser «sa» machine sans être physiquement présent devant. Il est surtout utilisé sur les machines Unix reliées à l'Internet.

Terminal graphique (protocole X) : X désigne un gestionnaire de console graphique faisant office de serveur pour des programmes clients qui lui envoient des requêtes d'ouverture de fenêtre, de tracé de dessins, d'affichage de texte et d'interrogation sur le clavier et la souris. En général le serveur X et les clients tournent sur la même machine et communiquent par pipeline, mais un serveur X accepte (après autorisation) des requêtes arrivant par n'importe quel moyen, en particulier par un réseau local. En combinant les protocoles Telnet et X, on peut donc se connecter à une machine distante et y lancer des programmes graphiques qui seront affichés par le serveur X local. Dans cette situation, chaque machine fait office de serveur pour l'autre : la machine locale sert les requêtes X, la machine distante sert les requêtes Telnet. Bien qu'il existe des serveurs X tournant sous Windows, X est surtout utilisé sur des machines Unix.

Réplication d'écran : Il s'agit d'une variante du service X précédent, le client contacte n serveurs d'affichage graphique et leur transmet en temps réel l'image affichée sur son propre écran graphique. Les serveurs reproduisent l'image transmise sur les écrans qu'ils contrôlent, ce qui permet d'observer sur plusieurs écrans une démonstration effectuée sur le poste client. Dans le cas des machines Windows, on peut trouver sur Internet le programme `look@me` qui permet de répliquer sur une machine l'écran d'une deuxième. Si l'on veut observer sur n machines l'écran d'une $n+1$-ème, il suffit de «relier les machines en série».

Consultation de bases de données, documents hypertexte (protocoles SQL, HTTP) : Il s'agit d'une variante du transfert de fichiers où les données transmises du serveur vers le client résultent éventuellement d'un «calcul» effectué par le serveur. Dans le cas d'une base de données, le client envoie une clé ou une requête de recherche et le serveur lui retourne l'information associée à la clé ou les données correspondant au critère de recherche. Dans le cas de documents hypertexte, le client indique un URL (Uniform Resource Locator) qui ressemble à un nom de fichier Unix, et le serveur lui retourne le fichier correspondant si c'en est un, sinon fabrique un document HTML de circonstance à partir de l'URL et l'envoie au client.

Courrier électronique (protocoles SMTP et POP) : C'est encore un transfert de fichiers, le fichier en question contenant un message d'un utilisateur généralement humain à un autre lui aussi humain (mais comme pour le protocole FTP, il existe des programmes capables de rédiger et d'expédier du courrier et d'autres programmes capables d'y répondre). La différence avec les protocoles FTP, NetBIOS, NFS est que les machines émettrice et destinataire n'ont pas besoin d'être «visibles» l'une de l'autre, le message transite de passerelle SMTP en passerelle SMTP, en prenant le temps qu'il faut jusqu'à arriver à destination.



2. Protocoles physiques et logiques

Les protocoles précédents règlent les formats de communication entre un client et un serveur selon le service utilisé sans spécifier de quelle manière les données échangées entre le client et le serveur transitent sur le réseau. Il s'agit de protocoles de niveau *application* tandis que l'acheminement des données relève de protocoles *physiques* et *logiques*. Un protocole physique spécifie le type de liaison, le format des câbles, des connecteurs, etc. et un protocole logique spécifie la manière d'organiser les données à transmettre quel que soit le réseau physique sous-jacent.

Parmi les protocoles physiques, on trouve Ethernet décrit ci-dessous, Token-Ring (monde IBM), LocalTalk (monde Apple), PPP (Point to Point Protocol) et SLIP (Serial Line Internet Protocol). PPP et SLIP sont le plus souvent utilisés pour des connexions intermittentes via une ligne téléphonique, les autres protocoles décrivent des configurations matérielles fixes.

Les principaux protocoles logiques utilisés sur PC sont :

- NetBEUI : Network Bios Extended User Interface, utilisé en standard par les machines Windows ;
- IPX/SPX : Internet Packet eXchange/Sequenced Packet eXchange, utilisé en standard sur les réseaux Novell ;
- TCP/IP : Transmit Control Protocol/Internet Protocol, utilisé en standard sur les machines Unix et sur le réseau Internet ;
- AppleTalk : sur les machines Apple.

Un même réseau physique peut véhiculer simultanément des données pour n'importe quel protocole logique, et un protocole logique peut circuler sur n'importe quel réseau physique, et même traverser plusieurs réseaux physiques similaires ou différents avant d'arriver à destination. En particulier, les données TCP/IP voyagent souvent d'un bout à l'autre du monde en traversant des *passerelles* et des *routeurs* qui interconnectent les différents réseaux locaux constituant Internet. Une passerelle est une machine reliée à deux réseaux et qui sert d'intermédiaire entre les machines de ces réseaux : si une machine du premier réseau veut communiquer avec une machine du deuxième, elle envoie son message à la passerelle avec les instructions nécessaires et la passerelle le transmet au destinataire. Il est aussi possible que la passerelle transmette le message à une deuxième passerelle qui le fait suivre vers une troisième et ainsi de suite jusqu'à atteindre le réseau local du destinataire. Un routeur est (crois-je savoir) une passerelle qui choisit entre plusieurs routes pour acheminer un message.

Par exception, le protocole NetBEUI est limité à un réseau local sans passerelle ni routeur, et donc ne peut pas être employé sur un WAN.

2.1. Protocole physique : Ethernet

Les données sont transmises en série sur des fils électriques. Chaque ordinateur dispose d'une carte d'interface comportant l'électronique nécessaire pour émettre et recevoir des données et la logique implémentant le protocole Ethernet. Il y a 3 types de câbles normalisés :

- Ethernet fin : câble coaxial 75Ω, chaque carte d'interface est reliée au câble par un té muni de prises BNC et les deux extrémités du câble doivent être fermées par des «bouchons» pour éviter la réflexion des ondes électriques. La longueur totale du câble est limitée à 185m.

- Ethernet épais : câble coaxial 50Ω, les machines sont reliées au câble par des «prises vampires». La longueur totale du câble est limitée à 500m.

- Paires torsadées : câble souple à 4 conducteurs non blindés, les conducteurs sont torsadés 2 par 2 pour se protéger mutuellement des interférences. Chaque carte d'interface est reliée à un câble particulier et tous les câbles sont reliés à un répéteur (HUB) qui réémet sur chaque câble les données provenant de l'un d'entre eux. La longueur d'un câble est limitée à 100m, les hubs peuvent être reliés entre eux, mais le nombre de hubs à traverser est limité à 4. Les câbles sont reliés aux cartes et aux hubs par des connecteurs RJ45.

A priori, le câblage en Ethernet fin ou épais est plus économique que le câblage en paires torsadées (longueur de câble inférieure, pas de hub), mais la solution paires torsadées est plus souple, en particulier il est possible de câbler une salle en prévision d'un réseau futur : on pose des prises un peu partout, que l'on utilisera ou pas selon le nombre de machines installées. Par ailleurs, les hubs sont munis d'indicateurs lumineux de raccordement et d'activité pour chaque prise, ce qui permet de contrôler visuellement le bon fonctionnement du réseau.

La vitesse de transfert sur un réseau Ethernet est 10 Mb/s ou 100 Mb/s pour les réseaux les plus récents. Il s'agit d'une vitesse de pointe, sans tenir compte des problèmes dûs à l'encombrement du réseau et aux collisions. En pratique, sur le réseau de Carnot, j'ai mesuré des vitesses moyennes de transfert de fichier comprises entre 0.5 Mb/s et 2.5 Mb/s. A titre de comparaison, la vitesse de transfert de données depuis un disque dur est de l'ordre de 5 à 20 Mb/s selon les machines.

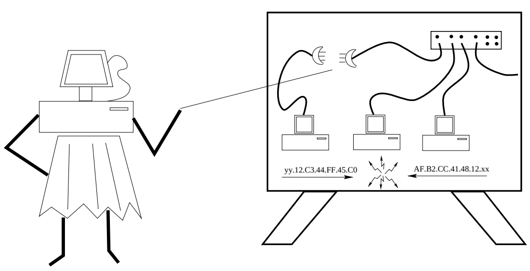
Coût approximatif : aux dires de l'agent de Carnot qui a procédé au câblage (paires torsadées), il faut compter 4000 F grand maximum et une journée de travail (grand minimum) pour une salle (20 prises). Un hub 24 voies coûte environ 4000 F et une carte réseau 300 F, soit un coût total de 10000 F à 15000 F pour une salle de 15 postes.

Format des trames : Chaque carte d'interface dispose d'un numéro sur 6 octets inscrit par le fabricant et en principe unique. Lorsqu'une carte doit envoyer des données sur le réseau, elle émet un train de bits appelé «trame Ethernet» contenant les informations suivantes :

– préambule : 8 octets, ne contient pas d'information, mais signale le début d'une trame ;
– adresse destinataire : 6 octets, seule la carte ayant ce numéro réceptionne le reste de la trame, les autres cartes doivent l'ignorer. Si l'adresse destinataire vaut FF:FF:FF:FF:FF:FF, le message est une annonce (broadcast) destinée à toutes les cartes ;
– adresse émetteur : 6 octets ;
– protocole logique ou taille des données : 2 octets ;
– données : de 46 à 1500 octets ;
– somme de contrôle : 2 octets.

Lorsqu'une carte émet une trame toutes les autres doivent écouter ou ignorer ; si deux cartes émettent en même temps il se produit une *collision*. Dans ce cas les deux cartes s'arrêtent d'émettre, chacune tire une durée aléatoire et attend ce temps là avant d'essayer de réémettre. Si les durées tirées sont différentes, la première des deux cartes peut réémettre. Sinon, il se produit une deuxième collision et les cartes retirent des durées d'attente aléatoires en doublant l'intervalle de tirage, et ainsi de suite jusqu'à 16 essais. Après 16 essais les trames sont abandonnées.

Conséquences : Du fait qu'une seule trame peut voyager sur le réseau à un instant donné, la vitesse de pointe (10 Mb/s ou 100 Mb/s) est en fait partagée entre toutes les machines ayant quelque chose à envoyer. Par ailleurs, il est possible de configurer une carte Ethernet pour qu'elle écoute toutes les trames, même celles qui ne lui sont pas destinées et donc pour espionner le réseau. Ceci est utilisé pour déboguer un réseau défectueux, mais peut aussi l'être pour capter des mots de passe ou des informations confidentielles. La seule manière de transférer des données sensibles sur un réseau est de les crypter.



2.2. Protocole logique : TCP/IP

IP reproduit au niveau logique la structuration des messages définie dans la protocole Ethernet, c'est à dire qu'une trame IP (la partie données d'une trame Ethernet) est constituée d'une en-tête de 20 octets et d'un champ données de longueur variable. L'en-tête contient entre autres les adresses *logiques* de l'émetteur et du destinataire, adresses attribuées aux interfaces des machines lors de la configuration de ces machines. Pour prendre une comparaison dans la vie courante, une automobile peut être désignée d'au moins 3 manières :

- les numéros de châssis et de moteur, inscrits à la fabrication de la voiture ;
- le numéro de police, inscrit lors de la déclaration d'achat de la voiture, et susceptible de changer en cas de déménagement ;
- une désignation symbolique, par exemple «La 4L de Dupont».

De la même manière, une machine sur Internet dispose d'un numéro d'interface (adresse Ethernet, numéro de téléphone pour un modem, ...) d'un numéro d'identification logique appelé «adresse IP» et d'un nom symbolique tel `ftp.inria.fr`. La correspondance entre une adresse IP et une adresse Ethernet est effectuée par broadcast, la correspondance entre un nom symbolique et une adresse IP est effectuée par consultation de tables internes ou par requête auprès d'un serveur de noms.

L'adresse IP est un nombre codé sur 4 octets, le début constituant «l'adresse réseau» et la fin l'adresse de la machine à l'intérieur de son réseau local. Il y a 3 types de réseaux définis :

- réseau de classe A : l'adresse réseau est constituée d'un octet compris entre 0 et 127, les adresses internes au réseau occupent les 3 octets restant. Un tel réseau peut comporter jusqu'à $2^{24} - 2 \approx 16$ millions de machines.

- réseau de classe B : l'adresse réseau est constituée de deux octets le premier étant compris entre 128 et 191, les adresses internes sont définies sur 2 octets ce qui fait environ 65000 machines.

- réseau de classe C : l'adresse réseau est constituée de trois octets le premier étant compris entre 192 et 223, l'adresse interne est constituée d'un octet ce qui permet de connecter jusqu'à 254 machines (les adresses internes 0 et 255 sont réservées pour la gestion du réseau).

Le *masque réseau* est un mot de 32 bits où chaque bit vaut 1 si et seulement si le bit correspondant des adresses IP utilisées fait partie de l'adresse réseau. Pour un réseau de classe A, le masque réseau vaut donc 255.0.0.0, pour un réseau de classe B : 255.255.0.0 et pour un réseau de classe C : 255.255.255.0. Ce masque est utilisé pour savoir si deux machines sont sur le même réseau ou non lorsque l'on connaît les adresses IP des deux machines : le et bit à bit d'une adresse IP avec le masque réseau doit rendre le même résultat pour les deux machines.

Compte tenu de son rôle d'interconnexion de réseaux locaux, Internet impose qu'une adresse IP soit unique au monde, et il existe une instance mondiale, l'ISOC (Internet SOCiety), qui attribue les adresses IP par blocs de classe A, B ou C aux demandeurs (l'ISOC est représentée par l'Inria en France). Cependant, on peut installer un réseau local suivant le protocole IP sans obtenir d'adresse officielle, il suffit d'utiliser des *adresses réseau privées* réservées à cet usage : $10.x.y.z$ (un réseau de classe A), $172.16.y.z$ à $172.31.y.z$ (16 réseaux de classe B) et $192.168.0.z$ à $192.168.255.z$ (256 réseaux de classe C). Il est «garanti» qu'aucune passerelle ni routeur de l'Internet ne laissera passer un message ayant l'une de ces adresses en émetteur ou destinataire, donc deux réseaux privés peuvent utiliser les mêmes adresses sans se gêner mutuellement, même s'ils sont tous les deux reliés à l'Internet. Bien entendu, à l'intérieur d'un réseau, toutes les adresses IP utilisées doivent être différentes. Par ailleurs, une passerelle ayant par définition plusieurs interfaces, dispose d'autant d'adresses IP que d'interfaces.

Au dessus d'IP, on trouve les protocoles TCP (Transmit Control Protocol), UDP (User Datagram Protocol) et ICMP (Internet Control Message Protocol) qui gèrent l'émission et la réception de données pour le compte des applications. TCP découpe les données à émettre en tronçons adaptés à la taille des datagrammes, les numérote et les expédie sur le réseau par l'intermédiaire de la couche IP. A la réception, la couche TCP assemble les tronçons reçus, les remet dans l'ordre s'ils ont voyagé sur routes différentes, contrôle les erreurs de transmission et les paquets perdus et demande leur réémission en cas de besoin, et enfin délivre le flot de données remis en forme au programme destinataire. L'ensemble de ces opérations consomme du temps et de la *bande passante*, mais assure une bonne fiabilité aux transmissions. A l'inverse, le protocole UDP ne procède à aucun tronçonnage ni rattrapage d'erreur, ce sont les programmes client et serveur qui doivent assurer la fiabilité ; en contrepartie les communications par UDP utilisent au mieux les capacités du réseau. Enfin, le protocole ICMP est utilisé pour la gestion du réseau et des messages échangés.

De même que IP et Ethernet définissent des adresses permettant d'identifier les machines, TCP et UDP définissent un mécanisme d'adressage des programmes qu'ils doivent mettre en communication. Une adresse TCP ou UDP est appelée *numéro de port* et est représentée par un entier codé sur deux octets. Ainsi, pour désigner un programme (client ou serveur) sur le réseau, on donne l'adresse IP de la machine, le protocole (TCP ou UDP) utilisé et le numéro de port du programme. Par exemple, le service HTTP correspond au port TCP 80, le service FTP aux ports TCP 20 et 21 (20 pour l'échange de données et 21 pour les messages de contrôle), le service NFS correspond au port UDP 2049, etc. Il s'agit là des numéros de port des serveurs, les clients peuvent utiliser un numéro de port quelconque pourvu qu'il ne soit pas déjà utilisé par un autre programme dans la même machine ni réservé par le système.

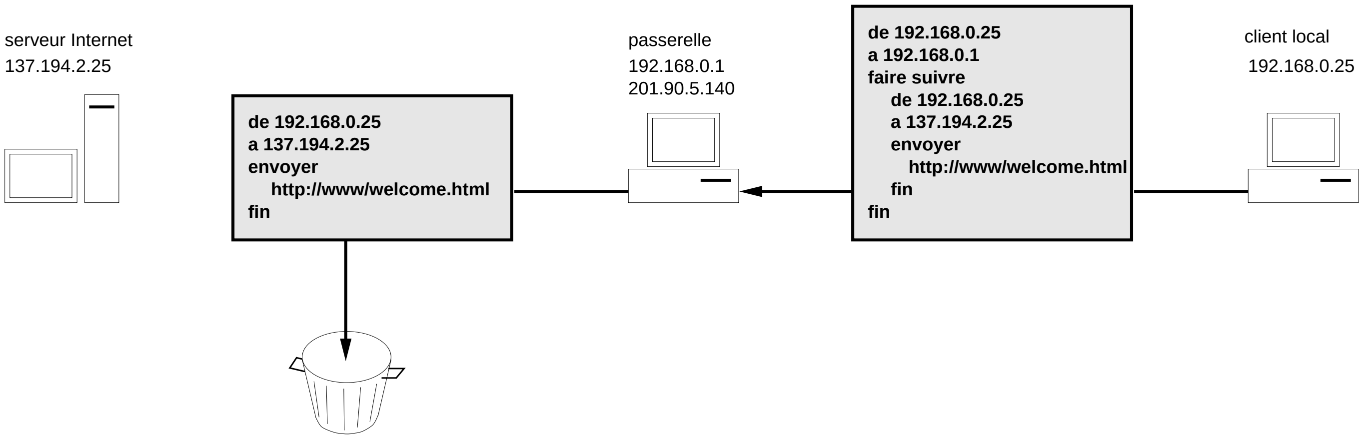
2.3. Masquerading et mandatement

Pour connecter un réseau local au réseau Internet on utilise une passerelle, c'est à dire une machine connectée au réseau local et au réseau Internet et capable de recopier des datagrammes d'un réseau vers l'autre. Les autres machines du réseau local sont configurées de façon à contacter la passerelle à chaque fois qu'elles doivent envoyer un datagramme à l'extérieur (l'extérieur est reconnu comme tel à partir du masque réseau et de l'adresse IP enregistrés dans la machine considérée). Dans l'autre sens, une machine extérieure peut faire parvenir un datagramme à une machine locale en s'adressant à la passerelle du réseau local. Lorsque les deux machines voulant communiquer ne sont ni sur le même réseau ni sur deux réseaux ayant une passerelle en commun, les datagrammes sont acheminés de passerelle en passerelle via le réseau Internet (c'est à dire le réseau d'interconnexion des réseaux locaux) pourvu qu'il existe une route entre ces deux machines et que cette route soit «connue» des passerelles.

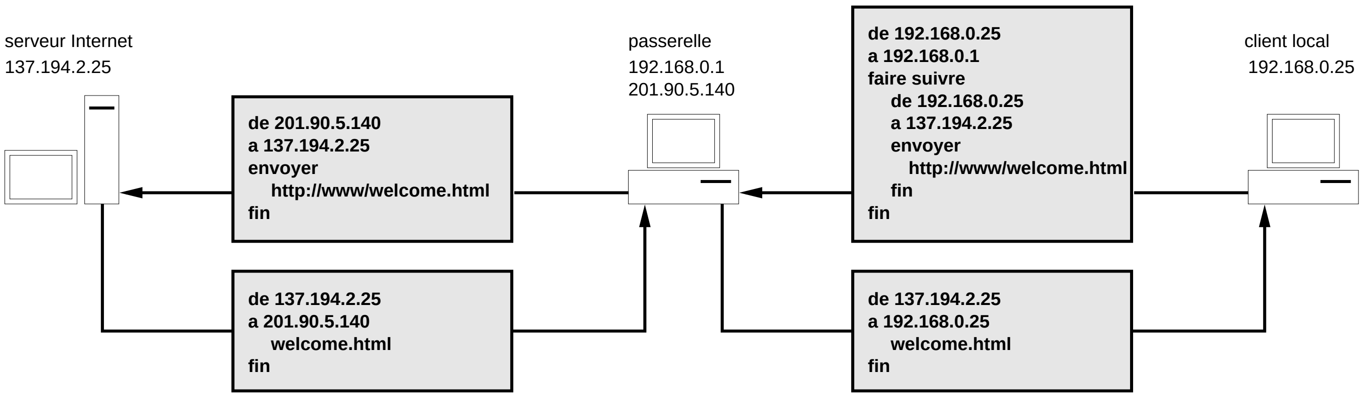
Malheureusement, sur un réseau local utilisant des adresses IP privées, une passerelle ordinaire ne suffit pas car les datagrammes émis par les machines du réseau local comportent des adresses privées dans leur en-tête, donc ne peuvent pas franchir les passerelles «officielles» de l'Internet. Et, même s'ils le pouvaient, les messages de retour émis par les serveurs contactés ne pourraient pas revenir vers la machine locale car, étant privé, le réseau local est inconnu du reste du monde. Il y a deux solutions à ce problème : la méthode de réécriture d'en-têtes et la méthode du mandataire.

Dans la méthode de réécriture d'en-têtes, la passerelle fait suivre les datagrammes du réseau local vers Internet en remplaçant l'adresse IP de l'émetteur par sa propre adresse IP «externe», celle correspondant à l'interface vers Internet. Le contenu du champ données du datagramme n'est pas modifié. Lorsque le serveur Internet destinataire reçoit le datagramme modifié, il croit recevoir une requête venant de la passerelle et il envoie donc la réponse à la passerelle. Celle-ci réceptionne la réponse, détermine à quelle requête il est répondu et réémet sur le réseau local la réponse à destination de la machine locale. Cette méthode est appelée *masquerading* car la passerelle cache son réseau local en trafiquant les adresses IP. La passerelle est appelée *pare-feu* (firewall en anglais) car elle protège les machines locales des agressions extérieures : aucun datagramme ne peut être transmis de l'Internet vers le réseau local s'il ne correspond pas à une requête émise dans l'autre sens, donc il est virtuellement impossible de contacter une machine locale depuis l'extérieur au moins tant que le pare-feu fonctionne et n'est pas tombé sous le contrôle d'un agresseur.

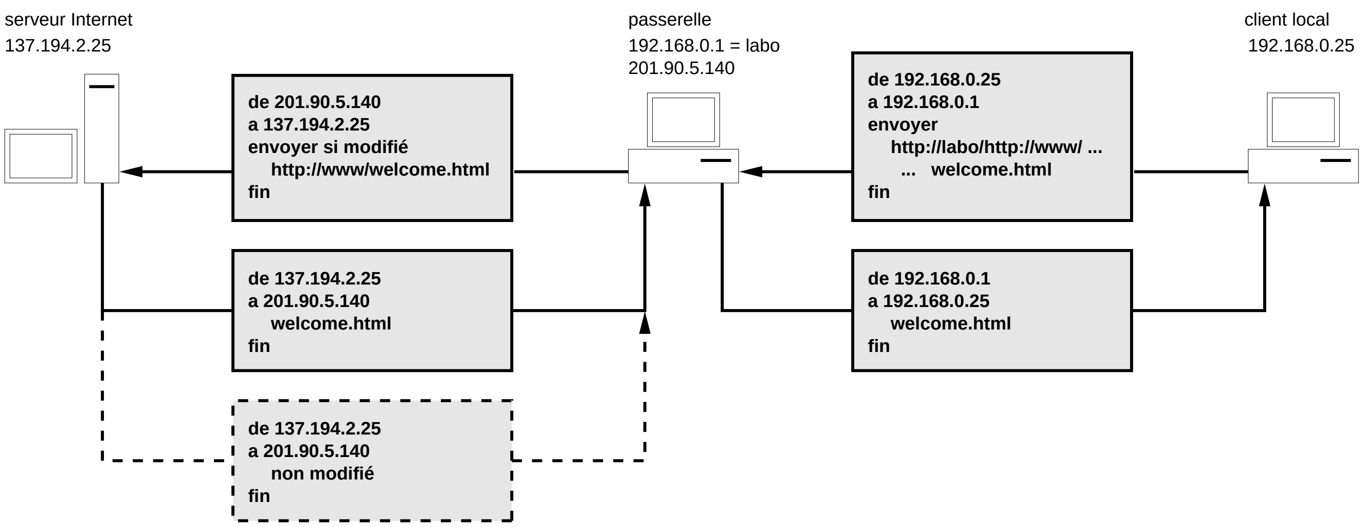
On notera que, fondamentalement, le masquerading constitue un faux en écriture, pour la bonne cause, mais un faux quand même et qu'il n'y a pas de problème avec une machine convenablement programmée pour fabriquer des datagrammes IP semblant provenir d'ailleurs. Le seul examen des en-têtes d'un message (en particulier d'un courrier électronique) ne permet donc pas d'identifier de façon probante l'émetteur du message. Enfin, le masquerading ne fonctionne pas avec tous les protocoles de communication, l'exception la plus notable étant le protocole FTP : dans ce protocole le client contacte le serveur pour lui envoyer des commandes, et le serveur contacte le client sur un port auxilliaire choisi par le client pour lui envoyer des données. Avec un pare-feu au milieu cela ne marche pas car la demande de connexion du serveur FTP aboutit sur le pare-feu et non sur le client réel et celui-là ne peut que refuser la connexion.



passerelle simple : la requête ne peut pas être routée



masquerading : transmission avec réécriture d'en-têtes



proxying : traitement local avec ou sans transfert

La méthode du mandataire (proxy server en anglais) ressemble à la précédente en ce sens que la passerelle réémet les requêtes vers Internet sous son propre numéro IP, elle en diffère en ce sens que la passerelle examine le corps du datagramme pour décider de la conduite à tenir. En pratique, pour chaque protocole mandaté il y a un serveur correspondant tournant sur la passerelle et les clients sur les machines locales s'adressent directement à ce serveur au lieu de formuler une requête vers le serveur Internet. Le serveur recevant une requête locale l'examine et émet une requête similaire sur le réseau Internet, puis transmet la réponse qu'il reçoit à son client (la machine locale). Dans le cas du protocole FTP, le mandatement est indispensable. Dans le cas du protocole HTTP, une simple réécriture d'adresses pourrait suffire mais les mandataires HTTP offrent en général un service appréciable : le stockage des documents reçus dans un cache et leur extraction du cache si le mandataire est sûr que le document caché est identique à celui disponible sur Internet (le protocole HTTP contient une forme de requête conditionnelle prévue pour cela).

Le mandatement exige une certaine coopération de la part du programme client sur la machine locale car il doit soumettre sa requête au mandataire au lieu du serveur visé tandis que la méthode de réécriture d'adresses peut être mise en œuvre sans que les machines locales ni extérieures ne s'en «rendent compte». Le serveur `apache` est un serveur HTTP qui fournit sur demande des documents HTML, mais est aussi un mandataire pour les protocoles HTTP, FTP, WAIS et Gopher. S'il reçoit une demande de transfert d'un document intitulé :

`http://`*`passerelle`*`/http://`*`url-ordinaire`*

alors il transmet le document spécifié par `http://`*`url-ordinaire`* après l'avoir obtenu soit du serveur Internet concerné, soit de son cache. Les explorateurs Internet courants (Microsoft-explorer, Mosaic et Netscape entre autres) sont prévus pour fonctionner avec ce type de mandataire, il suffit d'indiquer le nom de la passerelle ou son adresse IP privée ainsi que le port TCP utilisé dans les menus ou fichiers de configuration appropriés.

3. Exemple : le réseau de Carnot

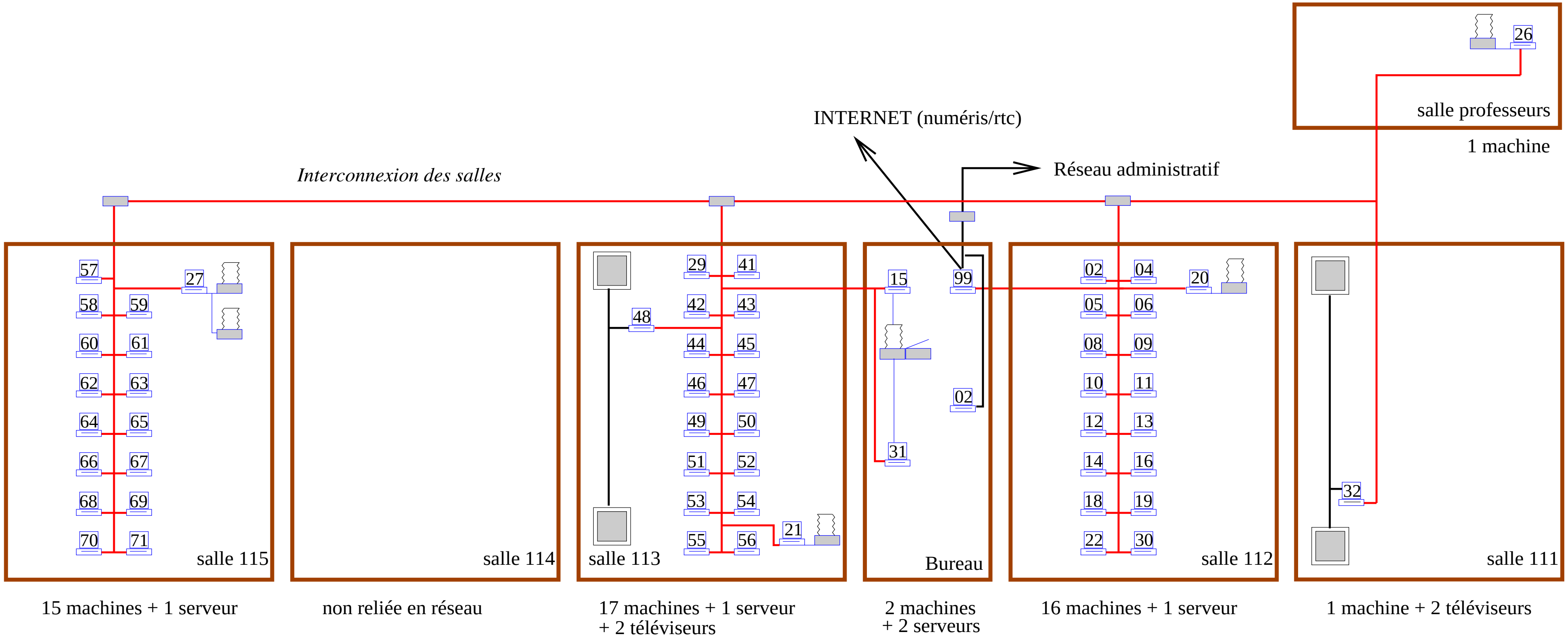
On dispose, à Carnot, depuis septembre 96 d'un réseau local assurant essentiellement les services de transferts de fichiers, impression à distance et accès à Internet.

3.1. Matériel

Le réseau est de type Ethernet avec câblage en paires torsadées, les câbles ont été posés en par les services techniques du lycée. Ils circulent dans des goulottes fixées aux murs et dans les faux plafonds, avec les câbles d'alimentation électrique. Il y a pour l'instant trois salles câblées, chaque salle contenant une vingtaine de prises réseau et un hub 24 voies. Les trois hubs sont reliés en chaîne par des câbles en paires torsadées, et constituent donc un unique réseau sur lequel on peut raccorder jusqu'à 68 machines (57 machines sont en service actuellement).

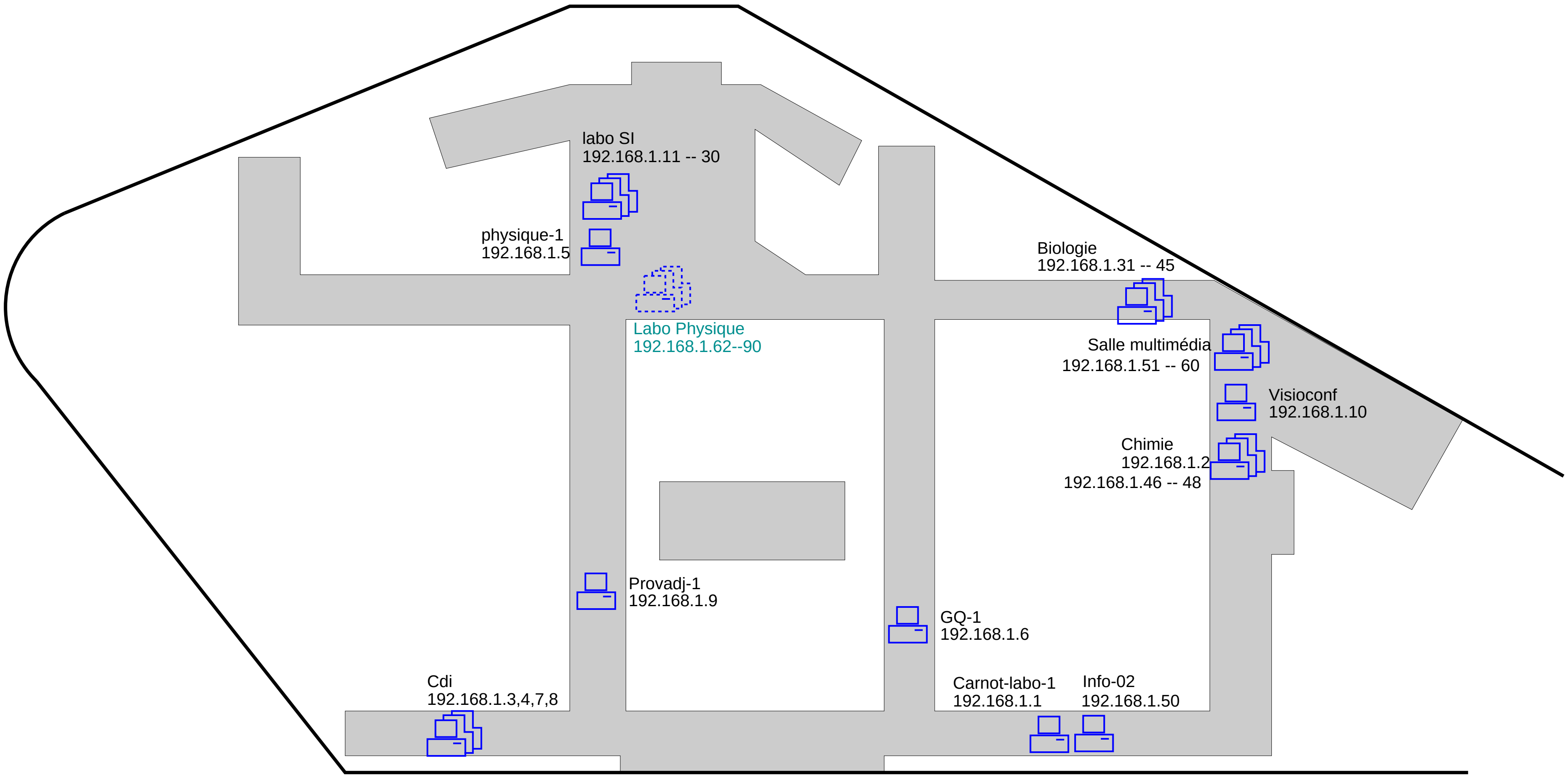
Les machines «élève» sont des 486DX2 et des Pentiums équipés de 16 Mo de mémoire et de cartes réseau 3Com-509, Svec (compatible NE-2000) ou Compaq (compatible NE-2100). Les serveurs de fichiers sont des 486DX-33 avec 8 Mo de mémoire, lecteur de CD et un disque de 2 Go, chacun est relié à une imprimante laser HP5L, celui de la salle 115 gère également une imprimante couleur HP deskjet 870. On a installé un serveur supplémentaire dans le bureau, inutilisé mais prêt à prendre le relais d'un serveur principal défaillant. Le laboratoire dispose d'un terminal numéris avec une ligne numéris et deux lignes analogiques pour l'accès Internet, la machine Internet est un Pentium-150 équipée d'un modem V34 et d'un adaptateur numéris Kortex-KXpro. Par ailleurs le lycée dispose d'un réseau «administratif» reliant les centres administratifs, le CDI et les différents laboratoires. La machine Internet est également reliée à ce réseau (ce qui lui fait donc 4 cartes d'interface) et joue le rôle de passerelle entre les deux réseaux et vers Internet (c'est peut-être plutôt un routeur ?) Enfin, un combiné scanner-imprimante couleur HP Officejet-Pro est relié à la fois à un poste «élève» et au serveur de secours dans le bureau.

La dernière salle du bâtiment est une salle de cours équipée d'un ordinateur relié au réseau et à un dispositif de projection sur deux écrans de télévision.



Réseau du laboratoire informatique

Michel Quercia, architecte



Lycée Carnot : réseau administratif (partie IP)

3.2. Serveurs

Chaque salle dispose d'un serveur de fichiers qui fait également office de serveur d'imprimante (tous les serveurs prétendent disposer d'une imprimante laser et d'une imprimante couleur, les travaux d'impression sur celle-ci étant retransmis vers le serveur de la salle 115). Les serveurs tournent sous Linux et disposent de *daemons* (Disk And Extension MONitor, programme résident en terminologie DOS) pour les protocoles NetBIOS, NFS, RPC, Telnet entre autres, ce qui leur permet de servir des fichiers et d'assurer l'impression de documents aussi bien pour des clients Windows que Linux. La passerelle entre les deux réseaux et Internet tourne aussi sous Linux et assure le mandatement des communications vers Internet avec `apache` pour les protocoles courramment utilisés sur le Web (HTTP, FTP, WAIS et ARCHIE).

Chaque machine élève tourne sous Windows-3.11 ou Linux et contacte au démarrage de Windows ou de Linux le serveur de sa salle pour obtenir l'accès aux répertoires exportés. Sous Windows, le répertoire partagé est installé comme disque `D:` et contient la quasi-totalité des logiciels utilisés (Maple, Mathematica, Lotus Smartsuite, Microsoft-Office, TeX, Turbo-Pascal, Borland C++, ...) ainsi que la base documentaire du CDI. Une machine élève ne contient en local que Dos/Windows, les fichiers de configurations `*.ini` des logiciels et les bibliothèques `*.dll` associées et les logiciels de CAO qui ne fonctionnent pas en réseau. Sous Linux, le répertoire partagé est monté sous `/usr` en NFS. Une machine Linux ne contient en local que le noyau Linux, Xwindow et Emacs (éditeur de texte). Sous Windows comme sous Linux, le protocole de communication utilisé est TCP/IP.

Au total, une machine élève contient environ 90Mo sur sa partition Dos et 45Mo sur sa partition Linux (15 Mo pour le système et 30 Mo pour le backup de la partition Dos), l'ensemble tient dans tout disque de capacité supérieure ou égale à 200Mo. Les serveurs de fichiers disposent d'un disque de 2 Go actuellement rempli à 50%. L'économie d'espace disque obtenue sur les machines élève se paye en termes de vitesse : il faut compter une à deux minutes pour que tous les postes d'une salle aient chargé un logiciel comme Maple, mais une fois chargé, le logiciel tourne en local et ne fait plus guère d'accès réseau. En cas de panne réseau, les machines peuvent démarrer et sont utilisables pour du traitement de textes uniquement ; en cas de panne serveur, on peut assez rapidement reconfigurer les machines pour qu'elles contactent le serveur d'une autre salle ou le serveur de secours, les quatre serveurs sont identiques sur ce point.

Les machines tournent 24h/24 : tous les soirs, on démarre les machines élève sous Linux en mode «nocturne». Dans ce mode, la machine reconstitue sa partition Dos à partir d'un backup stocké dans la partition Linux, puis lance un programme (`ecm`) de factorisation de grands nombres (120 chiffres) pour le compte de l'Inria jusqu'au lendemain matin. Les résultats sont collectés par la machine Internet et transmis par courrier électronique automatique à l'Inria.

Les autres laboratoires du lycée sont équipés de postes tournant sous Windows-95 et communiquent avec la passerelle par TCP/IP. En principe, ces postes sont autonomes, ils n'utilisent que le mandataire `apache` de la passerelle pour accéder à Internet, mais la passerelle autorise les connections entre les serveur de fichiers et les machines du réseau administratif pour le cas où on voudrait utiliser des logiciels ou imprimantes présents au laboratoire d'informatique.

3.3. Comptes personnels

Le serveur de la salle 115 gère également des répertoires personnels pour les professeurs ayant besoin de stocker des fichiers de façon permanente sur le réseau. Ces répertoires sont associés à des comptes Linux, accessibles depuis n'importe quel poste sous Linux (la validation des mots de passe est effectuée par NIS (Network Information Service)) mais aussi sous Windows en tant que répertoire partagé protégé par le même mot de passe.

Pour permettre l'accès en lecture seule aux fichiers qu'un professeur veut mettre à la disposition des élèves, chaque répertoire personnel contient un sous-répertoire `public` visible depuis chaque poste sans mot de passe (sous-répertoire `D:\profs` sous Windows et `/mnt/profs` sous Linux). Techniquement, si un serveur de fichiers reçoit une requête sur l'un de ces répertoires, il la redirige par NFS vers le serveur de la salle 115, ceci évite d'avoir à dupliquer ces répertoires publics.

3.4. Sécurité

En principe, les serveurs de fichiers sont protégés des utilisateurs par le simple fait qu'ils tournent sous Linux : le premier barrage est l'identification et le mot de passe à fournir, mais le fait d'avoir à lancer des commandes Unix et à mettre les barres obliques dans un sens inhabituel constitue un deuxième barrage probablement bien plus efficace. Par ailleurs, les serveurs n'ont pas d'écran donc il faut taper à l'aveugle ou passer par telnet. Aucun acte de sabotage sur les serveurs n'a été constaté à ce jour. Pour garantir la sécurité du réseau administratif contre les bidouilleurs éventuels, la passerelle a été programmée pour ne transférer d'un réseau à l'autre que les messages émis ou à destination des serveurs de fichiers, donc une machine élève ne peut pas «sortir» du laboratoire, si ce n'est par l'intermédiaire de mandataire `apache` pour la consultation des documents Internet.

Les machines élève sont faiblement protégées : il y a un détecteur de virus résident (en mode Dos/Windows) et la partition étant reconstituée tous les soirs, on est certain de trouver une machine bien réglée chaque matin, au moins à 8h. La partie Linux peut aussi être restaurée depuis le réseau à condition de bouter la machine sur une disquette Linux prévue à cet effet.

Enfin, l'ensemble de l'installation (disque serveur, comptes personnels, passerelle) est sauvegardé à la fois sur disquette Zip et sur bandes QIC (par le réseau) pour permettre une restauration complète en cas de catastrophe. Cette double précaution a prouvé son utilité (voir ci-dessous). Les machines reliées au réseau administratif sont maintenues par les responsables de laboratoire, le labo d'informatique n'assure ni sauvegarde ni restauration, son rôle se limite à leur attribuer des numéros IP et leur permettre l'accès à Internet.

3.5. Problèmes rencontrés

A la suite d'erreurs de configuration et de déplacement de machines, on a retrouvé des machines élève qui contactaient le serveur d'une autre salle. Pour le partage de disque ce n'est pas gênant, mais toutes les impressions commandées par ces machines arrivaient sur l'imprimante de la salle d'à côté. L'élève qui commandait une impression, ne voyant rien venir sur l'imprimante de sa salle, relançait plusieurs fois l'opération avant de se poser des questions et de signaler le problème. Dans l'autre salle, le professeur voyait sortir des tirages sans rapport avec le sujet de son TP et se demandait ce qui pouvait bien se passer ...

Certain Pentiums présentent un problème d'incompatibilité mineure entre le réseau et la souris : sous Windows, la souris cesse brutalement de fonctionner et ce de manière non reproductible. Après essais de diverses souris, de divers protocoles, et des deux ports série, on a trouvé par hasard que la souris reprenait vie si on lançait depuis Windows un interpréteur de commandes Dos et qu'alors elle ne faisait plus de caprices pour le reste de la session. Maintenant le problème est réglé de façon préventive : au démarrage de Windows, les Pentiums en question lancent un fichier de commandes `fixmouse.bat` contenant la seule et unique commande : `exit`.

L'accès aux répertoires partagés des serveurs impose de lancer Windows, donc les applications purement DOS telles que Turbo-Pascal doivent être lancées en mode compatibilité DOS depuis Windows. Pour Turbo-Pascal cela fonctionne, mais si on repasse temporairement à Windows (touches Alt-Tab ou Alt-Entrée) alors le retour en mode texte ne fonctionne pas et il faut continuer en mode fenêtré. Les logiciels de CAO, `dmt` et `mecaplan`, ne fonctionnent pas depuis Windows pour des raison de conflit d'accès à la carte graphique et la seule solution possible pour ces logiciels est de les installer sur les machines élève, ce qui complique les opérations de restauration des machines. On envisage de passer à `dmt-windows` pour régler ce problème.

L'interdiction d'écriture des clients sur le serveur de fichiers pose des problèmes avec certains programmes qui ne sont pas conçus pour fonctionner en réseau. Par exemple, le logiciel de recherche thématique des articles de «Pour la science» tient à jour des fichiers d'indexs modifiés à chaque requête ; de même le logiciel `pspice` de simulation de circuits électroniques et le logiciel d'interrogation de la base de données du CDI modifient leurs bases de données en cours d'utilisation. Pour les logiciels «Pour la science» et `pspice`, la solution retenue est de transférer les fichiers nécessaires sur les machines locales avant utilisation à l'aide d'un programme `.bat` de circonstance. En ce qui concerne le logiciel d'interrogation du CDI, cette solution n'est pas praticable, la base de données faisant près de 90 Mo. A titre temporaire, le répertoire contenant cette base de données a été mis en écriture publique, mais il est probable que cela occasionnera des plantages si plusieurs postes accèdent en même temps à cette base de données (l'acquisition d'une version avec interrogation par HTTP est à l'étude).

A la suite d'une erreur de manipulation, deux des trois serveurs de fichiers ont été ouverts en écriture publique pour l'installation d'un nouveau logiciel, ce qui a occasionné un plantage complet d'un autre logiciel, Maple, qui tournait à ce moment sur les postes élève reliés à ces serveurs. Dès le problème constaté, les machines élève ont été redirigées sur le troisième serveur et ont pu continuer à fonctionner normalement. Les deux premiers serveurs ont été reconstitués à partir du troisième pendant ce temps, mais les répertoires personnels des professeurs ont été perdus pendant la restauration (deuxième erreur de manipulation), il a fallu les restaurer à partir de la sauvegarde Zip. C'est à la suite de cet «incident» qu'on a monté un serveur de secours, et les essais de nouveaux logiciels se font maintenant sur celui-ci.

4. Bibliographie

- **Créer votre réseau :** Patrick T.Campbell, Sybex 1996
- **Administration réseau sous Linux :** Olaf Kirch, traduction de René Cougnenc, O'Reilly 1995
- **La communication sous Unix :** Jean-Marie Rifflet, Ediscience 1995
- **Firewalls :** D. B. Chapman, E. D. Zwicky, O'Reilly 1996