Description de l'intranet du lycée Jean Bart

Georges KHAZNADAR

17 janvier 2002

Table des matières

1 Intranet, Internet

1.1 Le réseau mondial

Plusieurs types de réseaux d'ordinateurs ont été inventés ces dernières années. L'un de ces types de réseau, le réseau TCP-IP, s'est imposé pour la raison simple qu'il s'est étendu à toute la planète. Une des raisons de son extension est que les protocoles de communication sont librement disponibles et que les logiciels permettant l'accès à ce réseau sont gratuits. Les données voyagent sur un réseau TCP-IP regroupées en paquets identifiés par l'adresse de la machine expéditrice et celle de la machine destinataire. Les protocoles assurent un acheminement sûr même si les moyens de transmission sont brouillés, tout paquet de données corrompu ou perdu peut être redemandé par la machine destinataire. La machine destinataire cesse de demander des paquets de donnée quand elle réussit à reconstituer la donnée complète en bon état.

1.2 Réseau d'établissement

Quand l'extension des ordinateurs connectés entre eux est limitée à un établissement ou à une entreprise, même multinationale, on parle d'intranet. Il existe un seul internet, c'est le réseau mondial. Des machines appartenant à un intranet peuvent aussi faire partie de l'internet. Une machine de l'internet est identifiée par son adresse IP, qui doit être unique dans le monde. Une adresse IP est une séquence de quatre octets (nombres binaires à huit bits). Certaines séquences sont interdites dans l'internet et ne peuvent exister que dans un intranet.

1.3 Le routage des paquets de données vers l'internet

Dans le cas du lycée Jean Bart, la structure est celle d'un intranet. Pour le bâtiment B, la seule machine à faire partie de l'internet par intermittence est un petit boîtier, dénommé ¡¡ le routeur ¿¿. Au moment où le *routeur* se connecte au réseau mondial, par une ligne numéris, commence une connection payante. Le *routeur* reçoit dynamiquement une adresse IP (pas la même à chaque connection). Le *routeur* est construit de manière à empêcher toute connection directe entre une machine de l'intranet et une machine de l'internet. La distinction se fait selon les catégories d'adresses IP, les adresses particulières qui sont définies dans l'intranet n'ayant pas vocation à circuler sur l'internet.

1.4 Les relations entre une machine du lycée et l'internet

Quand le *routeur* est actif, il réalise une opération qui permet cependant aux machines de l'intranet de communiquer avec des machines de l'internet. Tous les paquets de données sortant du lycée Jean Bart portent l'adresse IP du *routeur*, et uniquement celle-là, mais le *routeur* ajoute dans le paquet un code défini par lui-même qui permet à réception d'un paquet de données venant de l'internet, de le distribuer à la bonne machine de l'intranet.

1.5 Protection des ordinateurs du lycée vis à vis de l'internet

Une intrusion dans l'intranet d'une personne mal intentionnée est possible, mais demande des moyens assez sophistiqués et une grande rapidité d'exécution du fait que l'adresse du routeur varie fréquemment et que l'identification d'une machine particulière de l'intranet du lycée n'est pas directement accessible. L'intranet du lycée Jean Bart n'est en ce moment pas protégé par d'autres mécanismes.

2 Structure du réseau

La structure du réseau pédagogique du bâtiment B du lycée Jean Bart a été dictée en partie par la localisation des machines installées à la date de septembre 2000. Une partie d'entre elles communiquent à l'aide de cartes capables d'échanger 100 millions de bits par seconde (environ 10 millions d'octets effectifs par seconde), et une autre partie à l'aide de cartes dix fois moins rapides.

2.1 Emplacement des ordinateurs

Le machines à la communication la moins rapide sont situées dans les salles B301 (huit postes), B304 (un poste), B200 (un poste), B100 (huit postes) et B02 (neuf postes). Les machines capables d'échanger 100 mégabits par seconde sont en salle B202 (huit postes), B102(un poste) et au CDI (douze postes).

2.2 Incompatibilités partielles

Quand une machine capable de communiquer rapidement est connectée à une machine plus lente directement, la vitesse effective de communication est automatiquement ajustée aux capacités de la machine la plus lente. Il a donc été décidé d'interposer entre les deux catégories de machines des mécanismes tampons qui permettent l'échange de données à la cadence maximale acceptable à l'intérieur de chaque sous-ensemble du réseau intranet.

2.3 Le serveur du lycée

Ainsi, un serveur, dotation du CDI, est installé en salle B302. On lui a ajouté du matériel supplémentaire (carte réseau, onduleur, système de sauvegarde) afin de le rendre apte à isoler les segments du réseau intranet communiquant à des cadences différentes.

2.4 Les boîtiers de raccord

La mise en réseau des diverses salles équipées d'ordinateurs est assurée par deux types de boîtiers de raccordement des câbles : des *hubs* et des *switches*. Un hub raccorde les machines de façon passive, il agit seulement en répéteur des signaux. Un switch est plus actif : il repère l'adresse IP des machines qui lui sont connectées en analysant les signaux que celles-ci émettent. Quand un paquet de données lui parvient, il ne le répète pas à toutes les machines qui lui sont branchées, il l'achemine uniquement vers la machine qui en est destination. De plus, le switch permet de transcoder les paquets pour les passer d'une cadence de 100 mégabits par seconde à 10 mégabits par seconde et vice versa. Les salles B02, B100 et B301 sont équipées d'un hub, la salle B202 et le CDI sont équipées d'un switch. Il est impératif que ces boîtiers de raccord ne soient manipulés que par des personnes conscientes de ce qu'elle font.

2.5 Goulet d'étranglement vers l'internet, et tarification

Le *routeur*, situé en salle B02, se connecte à l'internet par un canal numéris, dont la cadence maximale est 64 kilobits par seconde. Cette ¡¡ largeur de bande ¿¿ est partagée entre toutes les machines du bâtiment B qui font des accès à l'internet à moment donné. Ainsi la largeur de bande effective pour une machine est très variable, selon le nombre d'utilisateurs simultanés dans le lycée, et éventuellement l'encombrement d'autres concentrateurs de trafic situés ailleurs sur l'internet. En ce moment, cette bande passante ne peut pas dépasser environ 7 kilooctets par seconde. Pendant une communication, le tarif pratiqué est celui d'une communication urbaine ordinaire (environ 20 F par heure). Si on considère 100 heures de mise en communication pour un mois, cela coûte 2000 francs par mois, et ceci pour un trafic de 2,5 gigaoctets au maximum (en réalité cette valeur limite n'est jamais atteinte.)

2.6 Élargissement de la bande passante vers l'internet

La ville de Dunkerque est maintenant dotée de la solution technique de l'ADSL, qui consiste à faire transiter des données à grande vitesse par le support des cales de téléphonie ordinaire, sans interférer avec les communications téléphoniques ordinaires. L'usage de cette solution nécessite de placer un modem (modulateur-démodulateur) à l'extrémité même d'une ligne téléphonique directe (les signaux de l'ADSL ne sont pas de nature à franchir un standard téléphonique). Cela signifie que le modem doit être place avant le standard, ou

qu'une ligne téléphonique directe nouvelle soit tirée. Dans tous les cas, un câble doit être tiré pour raccorder le modem au restant du réseau intranet. Il était urgent d'attendre la fin du monopole des télécommunications, qui permet que les tarifs soient fixés de façon concurrentielle.

On trouve actuellement des tarifs de 300 francs par mois pour une connection non limitée dans le temps, et une cadence de communication qui peut atteindre 100 fois celle de la ligne numéris. Un calcul naïf fait apparaître une division des coûts par un facteur 700 si on les rapporte à la quantité de données échangeables. Dans ces conditions, un intranet dans le lycée Jean Bart complété par un accès à l'internet devient financièrement plus facile à assumer. L'augmentation très grande de la largeur de bande au sortir du lycée ne signifie pas pour autant que les données circuleront à toute vitesse. D'autres goulets d'étranglement existent, et les embouteillages peuvent se situer ailleurs.

2.7 Optimisation du trafic des données grâce à un proxy

Il est possible d'améliorer l'efficacité de l'accès à l'internet grâce au serveur situé en salle B302, qui est configuré pour offrir un service de proxy : il est capable de stocker localement les données que d'autres machines font transiter par son service, et quand ces données sont qualifiées de permanentes, il les ressert à l'identique lors de toute nouvelle requête, en évitant leur transit sur le canal numéris qui est 150 fois plus lent.

3 Rôle des machines, hiérarchies

3.1 Les machines ordinaires

Le parc d'ordinateurs du lycée Jean Bart est constitué d'ordinateurs compatibles PC, il est hétérogène pour ce qui est de la composition matérielle des machines, et plus hétérogène encore si on tient compte de la diversité des versions de systèmes d'exploitation et des configurations adoptées sur chaque machine. Les aides-éducateurs qui assurent l'entretien de la salle B02 peuvent témoigner combien cela est coûteux en travail de maintenir l'intégrité d'un tel parc de machines quand il est utilisé par de nombreuses mains.

3.2 Bridage des actions accessibles aux utilisateurs

La seule solution fiable à moyen terme, celle qu'utilisent déjà de nombreux lycées, consiste à supprimer toute possibilité de reconfiguration ou d'effacement accidentel pour les utilisateurs ordinaires de ces machines, de même que la possibilité d'introduire arbitrairement un disquette dans la machine. Il faut aussi être en mesure de tenir un journal des utilisations des ordinateurs pour arriver à tracer les actes de malveillance s'il s'en produit.

3.3 Sécurisation par le système d'exploitation

La logithèque la plus étendue pour les ordinateurs à usage pédagogique est publiée pour le système d'exploitation Microsoft Windows (R), cependant que ce système d'exploitation n'est pas conçu pour une utilisation d'une machine par une communauté d'utilisateurs. La solution que propose la firme Microsoft est l'installation de Windows NT(R), tarifé à 5 kF la licence individuelle. Une solution retenue par les services du rectorat de Lille a été la diffusion de serveurs préconfigurés sous système d'exploitation Linux, qui assurent entre autre le service de domaine NT.

3.4 Le serveur du lycée

Le serveur préconfiguré par les services rectoraux est arrivé en dotation pour le CDI, au printemps 2000. Il est actuellement placé en salle B302, et sa configuration matérielle a été augmentée pour faciliter sa cohabitation avec un réseau de machines matériellement hétérogènes, ainsi que pour en sécuriser le fonctionnement à l'aide d'un onduleur et de systèmes pour la sauvegarde périodique des données.

Les quelques 1800 élèves au lycée pour l'année scolaire 2000-2001 se sont vu créer un compte personnel sur le serveur, de façon semi-automatique d'après un extrait de la base de données GEP de l'établissement. Ce compte leur réserve un espace personnel sécurisé sur le disque dur du serveur et une adresse électronique pour les échanges de méls localement à l'intranet.

4 Gestion matérielle et logicielle

L'utilisation des machines ordinaires du lycée nécessite l'acquisition de quelques techniques de base relatives à l'usage du claver et de la souris, et quelques aptitudes relatives à l'usage de traitements de texte, de tableurs, de navigateurs web et de logiciels de courrier électronique. Cette formation peut être dispensée au sein de modules de formations spécialisés, ou diluée dans les usages que les professeurs font avec leur classe des ordinateurs dans le cadre des enseignements disciplinaires. La deuxième option a l'intérêt de ne pas apparaître comme artificielle, mais il faut alors réfléchir aux possibilités d'hétérogénéité qui apparaîtront entre élèves qui ont eu des parcours différents.

La configuration matérielle et logicielle des machines ordinaires sera hors de portée des utilisateurs sans pouvoir d'administration dès que celles-ci auront été inféodées au serveur. Les seules personnes à même de modifier la configuration logicielle d'une machine sans forcer l'accès à la salle où celle-ci se situe disposeront d'un mot de passe particulier, ainsi que d'une disquette d'amorçage diminuant la protection de la machine qu'ils doivent maintenir. Il est clair que cette responsabilité d'administration doit être partagée par un nombre de personnes suffisant pour éviter une situation de forte dépendance, ou de désuétude en cas de mutation de quelques personnes.

Dans la situation actuelle, les connaissances glanées lors de l'administration d'une machine sous Windows (R) à domicile sont généralement suffisantes pour faire des modifications efficaces à *une machine dans une configuration initialement correcte*, par exemple l'installation d'un nouveau logiciel spécifique à une discipline. Quand les machines seront dépendantes d'un domaine NT, il faudra quelques connaissances supplémentaires, mais le prix à payer (acquérir de nouvelles connaissances) est largement remboursé par la sécurisation des postes. La gestion d'un parc de machines déconfigurables par tout un chacun est un travail de Sysiphe, que l'on échange très volontiers contre la gestion de machines un peu plus compliquées mais plus sûres.

Le lycée comporte fin 2000 plus de quatre personnes capables de réaliser ce type de maintenance. Il faut porter ce nombre à plus de dix pour que l'intranet soit utilisable sans interruption et sans perte de confiance.

La formation à ce type d'administration peut durer deux jours pour une personne utilisant déjà le clavier et la souris d'un ordinateur de façon régulière.

5 Services accessibles

Le serveur du lycée fournit actuellement les possibilités suivantes :

5.1 Le domaine NT

Le serveur a été équipé du kit logiciel Samba-Édu, inventé par Olivier Lécluse, au CRDP de Caen. Ce kit permet de définir un domaine NT géré par le serveur, auquel les machines ordinaires peuvent être configurées pour se connecter après identification de l'utilisateur. Plusieurs actions d'administration de ce serveur peuvent être réalisées par des personnes disposant d'une formation légère.

5.2 Un bureau itinérant pour chaque utilisateur

À chaque machine configurée pour établir une session NT, les utilisateurs sont conviés à s'identifier par un nom de *login* (nom d'utilisateur simplifié), et par un mot de passe qui n'apparaît pas en clair lorsqu'ils le dactylographient. Une fois l'utilisateur identifié, un bureau lui apparaît, qui contient des liens vers les applications qu'il peut utiliser, ainsi qu'un lien vers un dossier où il peut conserver des données personnelles à l'abri de toute indiscrétion et de tout effacement accidentel. La nature du bureau, et l'étendue des prérogatives qui lui sont associées varie selon que l'utilisateur identifié est un professeur ou un élève. Il est possible de créer des catégories différentes de professeur et d'élève avec des prérogatives autres. Le même bureau et le même dossier personnel réapparaissent devant l'utilisateur identifié quelle que soit la machine qu'il choisit pour travailler. Le quota de chaque utilisateur est fixé à 1 mégaoctet, ce qui représente quelques mille pages de texte dactylographié, mais seulement

quelques secondes d'image vidéo. À chacun de bien gérer son quota. Il est possible d'obtenir une extension du quota individuel.

5.3 Sécurisation des machines ordinaires

Les machines qui se connectent au domaine NT peuvent être sécurisées en diminuant de façon drastique le nombre d'actions potentiellement nuisibles accessibles par des manoeuvres à la souris, au clavier, ou par l'introduction d'une disquette. Les machines ainsi bridées ne réalisent plus qu'un sous ensemble des opérations initialement permises dans un environnement Windows (R), suffisant pour travailler efficacement à l'aide des applications fournies par le lycée. Un administrateur peut, à l'aide d'une disquette d'amorce adéquate, rétablir la configuration d'une machine pour que celle-ci fonctionne indépendamment du réseau. Ça peut être nécessaire pour des opérations de configuration de la machine, ou alors pour lui permettre d'être transportée et de fonctionner en dehors du contrôle par le serveur.

5.4 Service local de pages WEB

Le serveur est doté du logiciel Apache, qui est un standard (il équipe actuellement plus de 60 % des serveurs web de l'internet). Les professeurs (et les élèves) peuvent demander aux personnes qui en ont la responsabilité de publier des pages de leur composition, qui seront alors accessibles dans l'intranet du lycée.

5.5 Capture de sites WEB

Les professeurs, après une formation légère, peuvent programmer la capture d'un site web intéressant, pour une consultation plus facile et plus sûre par les élèves. Cela permet d'avoir une assurance importante sur la disponibilité des pages à consulter au moment où elles sont nécessaires pour une classe, et cela permet aussi de restreindre l'accès des élèves à des domaines limités.

5.6 Service de proxy

Les machines de l'intranet peuvent être configurées pour utiliser le service de proxy, c'est à dire que chacun de leurs requêtes vers l'internet passe par le serveur du lycée, qui leur renvoie les pages internet demandées, en stockant au passage toutes les données qui sont marquées comme non temporaires. Le proxy permet de gagner un temps précieux lorsque l'on accède à des sites où le contenu est riche en images ou en gadgets graphiques, qui n'ont plus à être récupérés sur l'internet après leur premier passage par le proxy. Un bon exemple est celui de la page d'accueil des moteurs de recherche, où des dizaines de gadgets graphiques (fonds dégradés, coins de tableaux, boulettes destinées à fixer l'attention, logos du site) sont conservés sur le proxy.

5.7 Service de fichiers

Le protocole ftp (file transfer protocol) est supporté par le serveur, ce qui permet un transfert efficace de fichiers possédant des formats divers. D'autre part, il existe un dossier dénommé ¡¡ Public ¿¿ qui est géré à la façon d'un partage Windows (R), et qui est accessible en lecture seule par tout utilisateur identifié.

5.8 Courrier interne

Tout utilisateur possède une adresse électronique pour le mél à l'intérieur du lycée. Par exemple l'utilisateur dont le *login* est `rtop` est joignable à l'adresse `rtop@serveur.lycee` ou encore `rtop@serveur`. Par défaut, les courriers sont conservés sur le disque du serveur, le quota est de 100 kilooctets par utilisateur (quota extensible). Chaque utilisateur peut envoyer un courrier à tout autre utilisateur du domaine `lycee`. Tout courrier porte l'adresse de son émetteur si bien qu'il n'y a pas de courrier anonyme.

Les professeurs, au terme d'une formation d'un jour, qui a déjà été proposée par la MAFPEN, peuvent apprendre à composer des pages WEB accessibles sur le site interne au lycée, comportant des documents, des illustrations, des questions et des champs de réponses associés, que les élèves peuvent utiliser lors d'un travail scolaire. La conception de la page est telle que l'élève provoque l'émission de toutes ses réponses vers l'adresse mél du professeur en cliquant sur un bouton de la page WEB.

La conversion d'un document de traitement de texte en un document interactif de cette sorte est l'affaire d'une demi-heure si le document initial s'y prête.

5.9 Service de noms de domaines (DNS)

Le service de noms est l'opération qui consiste à associer un nom écrit en caractères faciles à mémoriser (par exemple `www.voila.fr`) en une adresse IP, plus difficile à mémoriser qu'un numéro de téléphone. La machine dédiée assure le service de noms (DNS) pour tout le réseau interne du lycée, ainsi qu'un service de noms de type ¡¡ conseil ¿¿ pour l'internet, c'est à dire que si l'on déclare le serveur du lycée comme serveur de nom principal, celui-ci donne l'adresse IP des machines externes avec l'étiquette *adresse conseillée*. En cas d'échec de l'adressage, l'ordinateur demandeur renvoie la demande à un serveur de noms officiel de l'internet. Le service de noms de type *conseil* permet de gagner du temps lors de plusieurs accès consécutifs au même ordinateur distant.

5.10 Service IMAP

Le protocole IMAP est utile pour organiser les courriers électroniques reçus, tout en les laissant résider sur le serveur. Ce service permet de définir des dossiers diversement nommés afin de classer le courrier par catégories après une première lecture.

5.11 Échange de courrier avec l'extérieur du lycée

Il est possible d'habiliter certains utilisateurs à échanger du courrier avec l'extérieur du lycée tout en recevant les réponses au lycée, sans avoir à se connecter explicitement à d'autres sites proposant des services de messagerie.

Plusieurs solutions techniques existent, qui diffèrent par leur mise en oeuvre, ainsi que par la tarification associée, car nous dépendons toujours de machines externes au lycée qui ne disposera pas d'un ordinateur présent en permanence sur l'internet avec une adresse IP fixe.

Une des solutions possibles est de programmer pour les utilisateurs qui en feront la demande la récupération à leur adresse mél locale (`utilisateu@serveur.lycee`) de tout courrier qui leur arrive sur un autre serveur doté d'un accès POP ou IMAP. Ce peut être le cas pour les professeurs disposant d'une adresse sur le domaine `mail.ac-lille.fr`, et bientôt pour chaque élève ou membre du personnel disposant d'une adresse fournie gratuitement sur le domaine `laposte.fr`.

5.12 Une interface WEB pour la gestion légère du serveur

Les utilisateurs habilités, après une formation légère, peuvent accéder à un service web distinct de celui des pages web ordinaires accessibles à tous. Depuis n'importe quel poste du réseau, sous réserve de disposer d'un mot de passe, on peut accéder à l'administration légère du serveur. Les possibilités offertes sont les suivantes :

- La configuration du domaine NT, la création de partages de fichiers ou d'imprimantes, une gestion fine des droits d'accès, de visite, d'écriture aux dossiers et aux fichiers.
- La création de nouveaux utilisateurs, avec un profil professeur ou un profil élève.
- Le changement d'un mot de passe pour un utilisateur.
- L'aspiration des données d'un site web pour en faire un miroir local.

6 Documentation supplémentaire

Olivier Lécluse, créateur et mainteneur du kit Samba-Édu au CRDP de Caen, a publié de nombreuses informations (`http ://www.linux-france.org/prj/edu/sambaclg/`) sur ce système dans plusieurs pages web, et propose des compléments de formation sous forme d'exercices (`http ://www.linux-france.org/prj/edu/sambaclg/util.html`). Il est possible d'accéder à un forum (`http ://193.49.64.10/forumse/news.php3`) destiné aux utilisateurs du kit Samba-Édu réalisant un contact entre de nombreux utilisateurs de ce système, si bien qu'on peut immédiatement partager difficultés, problèmes et trouvailles avec plusieurs personnes en France.