

Administrer un service « IP à la demande »

S.Bortzmeyer Institut Pasteur
bortzmeyer@pasteur.fr

Le pourquoi

Sans tomber dans le délire récurrent sur le télétravail (en lisant certains articles ou rapports, on se sent ramené quinze ans en arrière à l'époque du début du Minitel; ni les espoirs, ni les craintes relatifs au télétravail n'ont évolué depuis), il est certain qu'il existe une demande pour l'accès aux ressources Internet dans d'autres endroits que le réseau local. En région parisienne, les difficultés de transport sont une puissante motivation en faveur d'un accès "de chez soi". Même si on ne se sent pas concerné par l'image du jeune cadre dynamique qui consulte l'état des stocks de son entreprise depuis une salle d'attente d'aéroport, il est certainement pratique de pouvoir de temps en temps travailler dans de bonnes conditions à partir de son domicile. Cela devient une nécessité pour le personnel "système": les serveurs d'aujourd'hui étant allumés 24 heures sur 24 et l'Internet ne dormant jamais, il faut pouvoir intervenir à distance.

Concernant plus spécifiquement les étudiants, l'accès à distance est surtout utile si l'université ferme trop tôt pour eux (cas fréquent) et/ou s'ils disposent à la maison d'un matériel informatique supérieur à celui de l'université (cas également fréquent) qu'ils souhaitent utiliser de préférence à celui des salles d'enseignements.

Les logiciels et matériels d'accès par le réseau téléphonique ont énormément progressé ces dernières années. En gros, on est passé de l'époque où "accès téléphonique" voulait dire "vi à 1200 b/s dans un émulateur VT100" à "les mêmes applications qu'au bureau, à 14400 b/s".

Les choix

Une fois prise la décision de créer un tel service dans son université, école ou centre de recherche, plusieurs choix se posent:

- simple serveur de terminaux traditionnel ou "IP à la demande" ("dialup IP").
- accès complet à l'Internet ou restrictions (pour des raisons de limitation de la bande passante ou de sécurité).
- et, naturellement, quel logiciel ou matériel choisir.

Concernant le premier choix, je pense qu'il est réglé aujourd'hui. Les mises en œuvre de TCP/IP sont devenues suffisamment perfectionnées et bon marché, le goût des utilisateurs pour les applications Internet est tel qu'il n'existe plus guère de raison pour se contenter du bon vieux serveur de terminaux qui permettait l'accès en émulation VT100 au "mainframe".

La question des limitations d'accès est plus délicate. Même en tenant compte de la rapidité des accès Renater (par rapport aux lignes dont disposent les fournisseurs "grand public" d'accès Internet), une batterie de modems rapides peut les saturer (neuf modems V32bis, le modèle de base, suffisent à saturer une ligne à 128 kb/s). Le nombre de modems étant de toute façon limité, on a peut-être intérêt à ne pas fournir un service trop vaste qui encouragerait les utilisateurs à rester connectés longtemps!

Mais surtout, le problème de sécurité nécessite une étude soignée. Le réseau téléphonique est totalement anonyme (sauf si on raccroche et qu'on rappelle l'appelant à un numéro prédéfini) et un accès par modem est un outil très utilisé par les pirates. Si cela n'est pas une excuse pour renoncer, il faut néanmoins prévoir une politique de sécurité rigoureuse.

Enfin, il faudra choisir matériel et logiciel. L'universitaire, par goût et par budget, choisira en général les solutions gratuites ou "shareware" pour le logiciel: il en existe un jeu très complet pour toutes les plates-formes. En revanche, le matériel (routeur entre le réseau local et le réseau

téléphonique) et les modems doivent être achetés pour des prix qui, en septembre 1995, oscillent de 8 000 à 25 000 F pour le routeur (en fonction du nombre de ports et de la qualité) et de 1 500 à 5 000 F pour chaque modem.

La théorie

Un accès Internet par le réseau téléphonique utilise une propriété fondamentale du protocole IP : il circule sur n'importe quel type de câble, du réseau téléphonique commuté (RTC, le réseau de tout le monde) à FDDI et ATM. Il "suffit" de définir une encapsulation, parfois un adressage et éventuellement certains protocoles auxiliaires pour chaque type de câble.

Pour le réseau téléphonique, ces définitions sont au nombre de deux, chacune avec ses avantages et ses inconvénients : SLIP (Serial Line Internet Protocol) et PPP (Point to Point Protocol).

SLIP est la mise en œuvre la plus ancienne du concept de "IP sur ligne série". Très simple et très répandu, SLIP garde de nombreux adeptes. PPP, plus récent et disposant de nombreuses fonctions utiles, s'impose de plus en plus. S'il faut en choisir un, il est nettement supérieur. Il permet d'ailleurs en théorie de transporter plusieurs protocoles réseau, pas seulement IP.

SLIP et PPP spécifient tous deux comment encapsuler des paquets IP pour qu'on puisse les transmettre sur la ligne téléphonique, vue, une fois que les modems ont "accroché" comme une simple ligne série (point à point). Mais SLIP s'arrête là alors que PPP spécifie en outre des protocoles de contrôle permettant de connaître et de surveiller l'état de la ligne et de négocier un certain nombre de ses caractéristiques, comme l'adresse IP.

Dans le mode d'exploitation le plus courant, on a à un bout un micro-ordinateur avec un modem et des mises en œuvre logicielles de TCP/IP et de PPP. A l'autre, se trouve un routeur (souvent appelé serveur de terminaux car les habitudes ont la vie dure) entre le réseau local (presque toujours Ethernet) et les lignes téléphoniques. Ce routeur parle également IP et PPP. Comme pour les routeurs entre lignes spécialisées et réseaux locaux, ce peut être une machine spécialisée ou un ordinateur (par exemple Unix ou Windows NT, ce dernier système étant loin d'avoir été autant testé). Il contrôle en général plusieurs modems, chacun relié à une ligne.

Une fois la liaison téléphonique établie (les modems se sont synchronisés) et l'initialisation de PPP faite, les paquets IP peuvent circuler. Le routeur se chargera de les transmettre sur le réseau local et, éventuellement, sur tout l'Internet. Les applications fonctionneront automatiquement : elles ont toujours parlé IP sans savoir sur quel câble tournait IP.

Dans la configuration typique d'une université, le routeur est placé dans les locaux de celle-ci, des micro-ordinateurs se trouvant chez les "clients". De ce côté-ci, n'importe quel micro-ordinateur convient, la grande majorité étant évidemment des PC ou des Macintosh. Le gestionnaire du routeur n'a typiquement pas de contrôle sur ces machines mais, si on lui demande conseil, il faut veiller à ce qu'elles disposent d'un port série rapide (les plus vieux PC sont très limités) et de suffisamment de mémoire pour faire tourner des applications Internet souvent gourmandes.

Le routeur peut être un ordinateur normal ou une machine spécialisée. Dans l'état actuel de la technique, il n'existe pas de logiciels permettant d'assurer un tel service de façon fiable sur une machine Unix, sans y passer beaucoup de temps. Sauf choix idéologique profond, il vaut donc mieux acheter une machine spécialisée. Dans ce domaine, il n'existe pas de constructeur qui domine le marché comme le fait Cisco pour les routeurs sur lignes spécialisées ou entre réseaux locaux. Les principaux produits sont, en septembre 1995 :

- Xylogics Annex
- Cisco CS500
- Livingston PortMaster
- Telebit Netblazer
- Xyplex

Ils se différencient par le support associé, la facilité de configuration, la richesse des fonctions, le prix, etc.

Les modems sont encore plus variés et sont classiquement un sujet de cauchemar pour l'administrateur réseau. Il est prudent, au moins du côté serveur, d'acheter des modems de qualité et de recommander à ses clients (en sachant que dans un environnement universitaire, ces conseils ne sont jamais suivis d'effet) d'acheter des modems de même marque, limitant ainsi les problèmes de compatibilité et surtout de support. Les vitesses disponibles sont de 14,4 kb/s (norme V32bis) ou, de préférence, 28,8 kb/s (norme V34).

Les logiciels

La plupart des logiciels nécessaires sont gratuits ou "shareware". Il faut évidemment disposer de TCP/IP (désormais en standard sur MacOS et Windows et naturellement sur tous les Unix sérieux). SLIP ou PPP sont disponibles en série sur les Unix gratuits (Linux, FreeBSD et NetBSD), SLIP l'est sur plusieurs Unix. Tous les deux existent en version gratuite sur le réseau mais sont souvent, à part sur Linux, très pénibles à installer et à configurer. Il existe un excellent PPP commercial, celui de MorningStar.

Sur MS-DOS pur, il existe plusieurs solutions mais que je connais mal. Sur Windows, Microsoft TCP/IP est disponible gratuitement (en téléchargement sur Internet) avec Windows for Workgroups ou Windows 95. Sinon, la référence est le produit "shareware" Trumpet Winsock qui parle SLIP et PPP, en plus de TCP/IP.

Sur MacOS, MacTCP est désormais livré avec les dernières versions du système et MacPPP est gratuit.

La sécurité

Quant aux applications, ce sont les mêmes que sur le réseau local: Netscape, Eudora, etc.

Le RTC ne permet aucune authentification. On ne peut même pas être sûr de l'origine d'un appel (sauf sur le RNIS). La seule façon d'être sûr de l'identité de l'appelant est de le rappeler à un numéro prédéfini. Cela implique de gérer une base de numéros et de payer la communication. Si l'accès est sur une machine Unix ou autre, celle-ci peut faire l'authentification. Mais en "IP à la demande", il n'y a pas de telle possibilité.

L'Internet est assez vulnérable comme ça pour ne pas autoriser n'importe qui à s'y connecter à partir du RTC. Il va donc falloir prévoir un certain nombre de mesures de sécurité.

Le problème n'est évidemment pas le même pour une université avec des milliers d'étudiants, un fournisseur de connectivité Internet avec une centaine de clients ou une entreprise qui ouvre un service d'accès distant pour ses cinq informaticiens.

Dans le cas d'un établissement d'enseignement, les secrets se gardent mal. La taille du public potentiel et le manque de personnel interdisent les solutions manuelles. Tout utilisateur d'un service "IP à la demande" devrait être identifié personnellement. Les "secrets partagés" (mots de passe d'un compte collectif ou numéro de téléphone sur liste rouge) ne restent pas secrets longtemps. Une fois ce principe mis en œuvre, les accès par le réseau téléphonique ne sont pas forcément moins sûrs que ceux par le réseau local: ils le sont moins car l'attaque peut venir de toute la planète mais d'un autre côté ils sont plus sécurisés car le réseau local ne demande typiquement aucune authentification à un micro-ordinateur.

Il faut évidemment tout enregistrer pour pouvoir enquêter en cas de problème (et prévenir les utilisateurs de cette atteinte à leur vie privée, ce qui est de toute façon obligatoire au titre de la loi Informatique et Libertés).

Du point de vue technique, la base d'utilisateurs autorisés peut être sur le routeur (mais elle est alors pénible à gérer pour l'administrateur) ou sur une machine Unix, interrogée par le routeur. On peut ainsi avoir une seule base d'utilisateur et un seul mot de passe par personne.

Il n'existe malheureusement pas de norme pour l'interrogation d'une base distante par le routeur d'accès. Les protocoles les plus employés sont Tacacs (Cisco), Radius (Livingston et Cisco), Kerberos, le DNS...

Quant à la surveillance, elle est typiquement effectuée par syslog ou un système équivalent, suivi d'un programme qui synthétise les données.

Le quotidien

La vie quotidienne de l'administrateur d'un tel service est surtout rythmé par des problèmes de mot de passe perdu et des difficultés de configuration du modem la première fois. L'hétérogénéité du jeu de commande Hayes est énorme. Même quand une commande est présente sur un grand nombre de modems, sa sémantique n'est pas forcément constante ("ATZ" n'est pas toujours équivalent à une coupure de courant, par exemple).

Si l'accès à ce service n'est que peu ou pas limité et qu'il n'y a pas de facturation, il faut aussi suivre la consommation et rappeler à l'ordre ceux qui abusent. Un modem est une ressource rare, d'autant plus que les accès sont très inégalement répartis dans le temps (au CNAM, la pointe est entre 23 h et minuit).

Les questions

Pour le futur, de nombreux problèmes restent à traiter. Les applications ne sont pas toujours bien adaptées à l'intermittence de la connexion. Prenons deux exemples:

- les lecteurs de News gratuits sur Macintosh ne permettent pas de récupérer les News d'un coup pour les lire ensuite à loisir, une fois déconnecté. Vu la technique de facturation de France-Télécom et le fait que l'administrateur souhaite que les modems soient libérés le plus tôt possible, c'est très rédhibitoire.

- si un administrateur d'un site Linux distant (cas courant parmi les étudiants en informatique) veut récupérer le courrier de tout son site à l'occasion des (rares) connexions, sendmail est très mal adapté. La nouvelle version 8.7 est censée corriger cela amis en attendant, UUCP au dessus de TCP reste la meilleure solution.

Les références

L'Internet professionnel <<http://www.urec.fr/internet.pro/>>

La réunion GERET sur le sujet <<http://www.urec.fr/Ftp/geret/94.06.petits.services/>>

Les RFC: 1661 (PPP), 1055 (SLIP), 1492 (Tacacs)

Les routeurs:

Livingston <<http://www.livingston.com/alt/altindex.htm>>

Cisco <http://www.cisco.com/public/guest_home.shtml>

Xyplex <<http://www.xyplex.com/>>

Telebit <<http://www.telebit.com/>>

Xylogics <<http://www.xylogics.com/>>

Les logiciels:

MorningStar <<http://www.morningstar.com/>>

Tout pour le Macintosh

<<http://www.uwtc.washington.edu/Computing/Internet/MacintoshResources.html>>

Pour Windows <<http://sage.cc.purdue.edu/~xniu/winsoc.htm>> (Trumpet Winsoc en <ftp://ftp.trumpet.com.au/>)