SÉCURITÉ DANS LES RÉSEAUX

Patrick Cegielski
cegielski@univ-paris12.fr

Novembre 2005

Pour Irène et Marie

Contents

List of Figures

Chapter 1

Généralités

1.1 Introduction aux réseaux

1.1.1 Origine des réseaux informatique

La notion de calcul est l'une des grandes conquêtes de l'humanité, certainement apparue au néolithique pour les besoins de comptabilité des ressources indispensables pour les premières cités, concernant le cheptel et les réserves de nourriture. Les grandes quantités manipulées pour cette comptabilité a conduit à rechercher rapidement des outils d'aides au calcul (petits cailloux, puis abaque, puis machine arithmétique de Pascal...). La notion d'ordinateur, outil universel d'aide aux calculs dans la mesure où, par définition, un ordinateur est capable de calculer ce qui est calculable par n'importe quel outil, date de 1936 avec la définition par Alan Turing de sa célèbre machine (en fait un modèle, car il s'agit d'une machine imaginaire). La réalisation effective d'ordinateurs attendra encore quelques années, puisque le premier date de 1949[1].

Quelques années après, il fut envisagé de partager l'unité centrale d'un ordinateur entre plusieurs sites, soit pour des raisons de bonne économie, soit pour des raisons intrinsèquement liées à l'application envisagée (projet SAGE [pour *Semi-Automatic Ground Environment*, environnement au sol semi-automatique] de surveillance radar des États-Unis). L'alliance des télécommunications et de l'informatique était née.

Au milieu des années 1960 vint l'idée de relier les unités centrales elles-mêmes.

[1]Ce que l'on vend sous le nom d'ordinateur n'est pas réellement une machine universelle. Mathématiquement ce sont des automates finis à un très grand nombre d'état et non des machines de Turing.

1.1.2 Notion de réseau informatique

Un **réseau informatique**[2] (*computer network* en anglais) est un ensemble d'ordinateurs et de périphériques (imprimantes, traceurs, scanners, etc.) connectés ensemble par le biais d'un support physique (en anglais *medium*). La connexion peut être directe (par câble coaxial, par exemple) ou indirecte (par modem).

1.1.3 Matériel et logiciel pour réseau

Comme pour les systèmes informatiques[3], la distinction entre *matériel* et *logiciel* est importante dans le cas des réseaux.

L'objet de ce livre concerne la sécurité des réseaux du point de vue des logiciels et non du matériel.

1.1.4 Protocoles

1.1.4.1 Notion de protocole

Dans un réseau informatique, lorsqu'un ordinateur envoie des informations à un autre, les matériels et les logiciels sont en général différents. On a donc besoin d'un ensemble de règles pour coordonner l'échange de ces informations. Celles-ci forment un **protocole**, nom donné par Tom Marill en 1966 ([HL–96], p.83).

Le mot provient évidemment du langage diplomatique. Les diplomates suivent des règles lors des discussions entre nations, appelées un protocole. Le protocole diplomatique indique qu'il ne faut pas insulter ses hôtes et qu'il faut tâcher de respecter les coutumes locales. La plupart des ambassades et des consulats abritent des spécialistes du protocole, dont le rôle est de s'assurer que tout se passe harmonieusement lors des rencontres. Le protocole est un ensemble de règles qui doivent être suivies pour "jouer le jeu", pour reprendre une expression diplomatique.

1.1.4.2 Suite de protocoles

Les protocoles ont évolué. De processus très simples ("je t'envoie un caractère, tu me le renvoies, et je m'assure que les deux correspondent") au départ, ils sont devenus des mécanismes complexes qui prennent en compte tous les problèmes et conditions de transfert possibles. Un protocole unique qui couvrirait tous les aspects du transfert serait de taille trop importante, difficile d'emploi et trop spécialisé. Plusieurs protocoles ont donc été développés, chacun s'acquittant d'une tâche spécifique.

On appelle **suite de protocoles** un ensemble de protocoles cohérents qui couvre pratiquement tous les besoins de communication.

1.1.5 Systèmes propriétaires et systèmes ouverts

Au début, il n'y avait qu'un réseau (ARPANET) avec ses protocoles associés. Devant le succès de celui-ci, des produits commerciaux furent développés, plus particulièrement pour les réseaux locaux et étendus. Chaque constructeur avait sa ligne de produits, matériels comme logiciels.

[2] Désormais nous ne parlerons que de *réseau* au lieu de *réseau informatique*. L'histoire des premiers réseaux de télécommunication (premiers essais, télégraphe optique, télégraphe électrique, télégraphie d'images, téléphone, transmission radio et systèmes de commutation) est contée dans [HUU–03].

[3] On appelle **système informatique** un poste de travail informatique complet : ordinateur, bien sûr, mais aussi périphériques (tels que imprimante ou scanner) et logiciels. De nos jours, les outils réseau font partie intégrante du système informatique, dans un sens plus large.

On parle de **système propriétaire**. Les sources, et même les spécifications complètes, des systèmes propriétaires sont rarement diffusées. Ceci présente une difficulté pour la conception des inter-réseaux.

Par opposition, un **système ouvert** est un système dont au moins les spécifications complètes sont diffusées, éventuellement les sources des logiciels.

Le mouvement des systèmes ouverts n'est pas né à propos des réseaux, même si c'est là qu'il a connu son plus grand succès puisqu'il n'existe plus de système propriétaire, mais à propos des systèmes d'exploitation. Jusqu'aux années 1980, chaque constructeur de matériel avait sa ligne de produits, et on était dans une très large mesure dépendant de ce constructeur pour tout ce qui concernait le logiciel et le matériel. Certains constructeurs profitaient de cette situation pour pratiquer des tarifs prohibitifs ou pour imposer certaines configurations à leurs clients. Le ressentiment des clients prit une telle ampleur que ces derniers finirent par imposer leurs souhaits. IBM commença par diffuser le code du BIOS de ses micro-ordinateurs. DEC (*Digital Equipment Corporation*) passa d'un système d'exploitation propriétaire, VMS, sur ses mini-ordinateurs à un système d'exploitation ouvert de type Unix. Ses clients lui en furent gré et l'entreprise vendit plus de machines. Microsoft essaie de faire passer sa technologie .NET comme un standard ECMA (*European Computer Manufacturer Association*), sans totalement y réussir pour l'instant (seule la spécification du langage C# est définie par un standard ECMA pour l'instant, début 2005).

1.2 Modèles en couches

La partie logicielle des réseaux comprend un grand nombre de fonctions, chacune relevant d'un protocole. Un ensemble de protocoles cohérent couvrant l'ensemble des besoins pour un réseau s'appelle une **suite** de protocoles. L'ensemble d'une telle suite s'appelle un **modèle réseau** ou **architecture réseau**.

1.2.1 Étude générale

1.2.1.1 Notion

Imaginez que vous deviez écrire un programme qui fournisse des fonctions de réseau à toutes les machines de votre réseau local. L'écriture d'un logiciel unique se chargeant de toutes les tâches nécessaires à la communication entre plusieurs ordinateurs serait un vrai cauchemar. De plus, dans l'hypothèse où vous arriveriez à gérer tous les matériels présents sur le réseau, le programme résultant serait bien trop grand pour être maintenu ou même exécuté.

Il est plus raisonnable de diviser chaque domaine d'opérations en groupes de natures proches. Les groupes sont assez évidents à discerner. Un groupe traite du transport des données, un autre de l'empaquetage des messages, un autre des applications utilisateur, etc. Chaque groupe de tâches proches est appelé une **couche**. On obtient ainsi un **modèle en couches**.

Les couches d'une architecture réseau sont censées être des entités autonomes et indépendantes. Une couche ne peut évidemment pas effectuer une tâche observable sans interagir avec d'autres couches mais, du point de vue de la programmation, elles sont indépendantes. Elles ne doivent interagir les unes avec les autres que grâce à leur **interface** proprement définie.

1.2.1.2 Pile réseau

Dans un modèle en couches, les couches sont numérotées de 1 à N, allant du niveau le plus proche du matériel (concernant le port série, puis la carte réseau) au niveau le plus proche de

l'application de l'utilisateur (courrier électronique, transfert de fichier...). Plus on est proche du matériel, plus le numéro de couche est bas.

Chaque protocole encapsule les données dans un ensemble plus grand comprenant en général un **en-tête** et quelquefois un **suffixe**. Supposons qu'il n'y ait pas de suffixe. Les données de l'utilisateur sont encapsulées avec l'en-tête du niveau N :

en-tête N	données

Cela devient des données de niveau N qui sont encapsulées avec l'en-tête de niveau N-1 pour obtenir des données de niveau N-1 :

en-tête N-1	en-tête N	données

et ainsi de suite jusqu'aux données encapsulées de niveau 1 :

en-tête 1	. . .	en-tête N-1	en-tête N	données

L'intérêt des modèles en couche est, qu'à chaque niveau, il n'est pas besoin de passer en revue l'ensemble des en-têtes mais uniquement celui du niveau correspondant.

On parle aussi de **pile réseau**, *stack* en anglais, car on peut considérer que les en-têtes des niveaux N à 1 sont empilés au-dessus des données de base lors de l'expédition et qu'elles sont dépilées lors de la réception, comme le montre la figure 1.3 ([K-R–01], p.52).

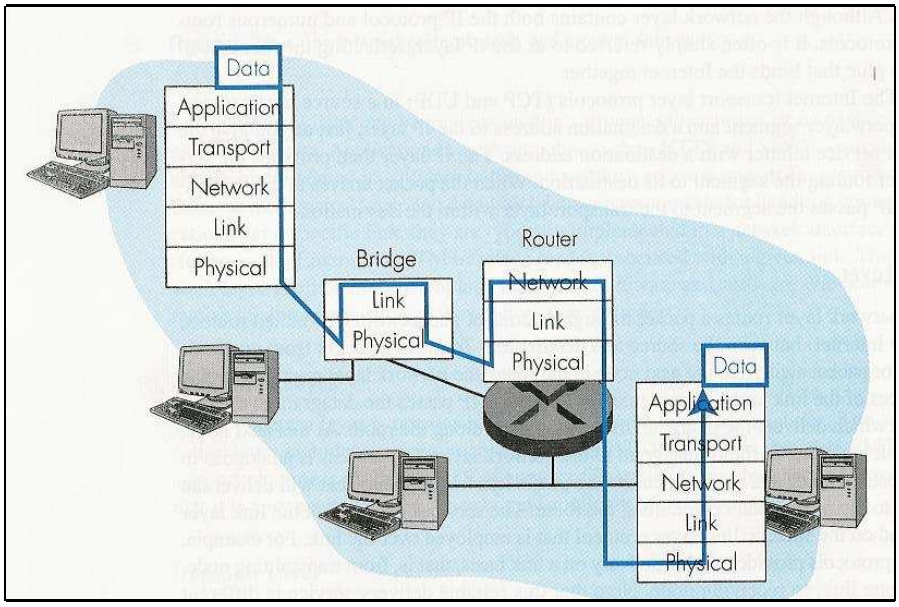

Figure 1.1: Pile réseau

1.2.1.3 Intérêts et réalisations

Les modèles en couches présentent beaucoup d'intérêt. La suite de protocoles est beaucoup plus simple à concevoir : le protocole d'un niveau donné peut être conçu par une équipe différente du protocole d'un autre niveau. Il en est de même de la suite de logiciels mettant en place ce modèle. De plus, les matériels actifs du réseau n'ont à considérer que les niveaux les plus bas, par exemple :

- un répéteur ne considérera que les données brutes, sans même entrer dans le détail, autrement dit ne concernera que la couche physqiue ;
- un routeur ne considèrera que les en-têtes des couches les plus basses pour obtenir l'adresse de destination.

Deux modèles furent développés pratiquement en parallèle : le **modèle OSI** (par l'organisme de standardisation international ISO) et la **suite TCP/IP** (d'après le nom de deux des protocoles de la suite). Rétrospectivement on s'aperçoit qu'un modèle est largement dominant, pour ne pas dire exclusif : la suite TCP/IP. Il est quand même intéressant de dire quelques mots du modèle OSI, même s'il est désormais pratiquement abandonné, car les deux couches les plus basses ne sont pas prises en considération par TCP/IP, ce qui a conduit à un modèle mixte.

1.2.2 Modèle OSI

L'ISO (*International Standardisation Organisation*), l'organisation de standardisation la plus prioritaire dans le monde entier, fondée en 1947, a proposé un modèle en sept couches en 1984 [ISO 7498-1], appelé **modèle OSI**, en fait **OSI–RM** pour *Open Systems Interconnection Reference Model* (modèle de référence d'interconnection des systèmes ouverts) :

7	Application	Couches supérieures
6	Signification	
5	Session	
4	Transport	Couches inférieures
3	Réseau	
2	Liaison des données	
1	Physique	

Le modèle OSI ne décrit aucune implémentation réelle d'un système particulier, mais se contente de définir les tâches des différentes couches.

Les couches d'application, de présentation et de session sont toutes les trois orientées application, c'est-à-dire qu'elles présentent l'interface de l'application à l'utilisateur. Ces trois couches sont totalement indépendantes des couches situées sous elles, elles ne connaissent rien de la façon dont les données parviennent à l'application. Elles sont appelées **couches supérieures**.

Les quatre **couches inférieures** se chargent de la transmission des données, en gérant l'empaquetage, le routage, la vérification et la transmission de chaque ensemble de données. Elles ne font aucune différence entre les diverses applications.

Détaillons maintenant le rôle de chacune des sept couches :

- La **couche physique** (*physical layer* en anglais) contrôle la transmission des différents bits *via* un support physique (*media* en anglais). C'est dans cette couche qu'on s'occupe de la façon dont les suites de bits sont converties (sans structuration) en signaux physiques et transmises *via* un support physique (câble de cuivre, fibre de verre, radio, etc.). La couche

physique définit les procédures de codage physique (telle ou telle différence de potentiel par exemple), la géométrie des connecteurs enfichables et les types des supports spéciaux. Les protocoles de cette couche dépendent du support physique.

- La **couche de liaison des données** (*data link layer* en anglais) est chargée de la transmission correcte des données d'un point du réseau à un autre relié directement à lui *via* un support physique. Elle s'occupe de la correction des erreurs survenant lors de cette transmission (différentes des erreurs dans les données elles-mêmes, traitées dans la couche de transport). Elle doit tenir compte des interférences de signal (fréquentes, pouvant provenir de plusieurs sources, parmi lesquelles les rayons cosmiques et les interférences magnétiques provenant d'autres équipements).

- La **couche réseau** (*network layer* en anglais) est chargée de la transmission des données d'un point du réseau à un autre, que celui-ci soit relié directement à lui ou non. Il s'agit d'abord de déterminer un chemin (ou **route**, comme on préfère l'appeler dans le vocabulaire des réseaux) de l'expéditeur vers le destinataire en utilisant des machines intermédiaires : on parle du **routage** physique des données. Elle est chargée également de l'adaptation des unités de données à la taille admissible de la couche liaison existante : on parle de **fragmentation**.

- La **couche transport** (*transport layer* en anglais) se charge du multiplexage (lors de l'envoi) et du démultiplexage (lors de la réception), c'est-à-dire de distribuer aux différentes applications les paquets arrivés sans encombre.

  Il y a **multiplexage** lorsque plusieurs communications transitent par un support physique unique. Le **démultiplexage** est l'inverse du multiplexage. Le multiplexage est indispensable pour prendre en charge de nombreuses connexions simultanément, tout en ne disposant que de ressources limitées. Un exemple classique est un bureau distant comprenant vingt terminaux. Chaque terminal pourrait être connecté au bureau principal par le biais d'une ligne téléphonique dédiée. Au lieu d'utiliser vingt lignes, on peut aussi s'arranger pour multiplexer les connexions afin de n'utiliser que trois ou quatre lignes téléphoniques.

  Elle peut, de plus, assurer d'autres tâches. Elle peut établir, maintenir et terminer les communications entre deux machines (dans le cas des **communications** dites **connectées**). Elle peut se charge d'assurer que les données envoyées correspondent aux données reçues, tout au moins modulo certains points de comparaison et, si elles ne correspondent pas, demander à ce que les données soient envoyées à nouveau. Elle peut gèrer l'envoi des données, en déterminant l'ordre et la priorité de l'envoi.

- La **couche de session** (*session layer* en anglais) contrôle l'échange structuré de dialogues *via* les liaisons de communication. Il est, par exemple, possible de contrôler au cours d'une session si le transfert des données peut avoir lieu simultanément dans les deux sens ou si un seul partenaire à la fois dispose du droit d'émission. Dans ce dernier cas, la couche session gère le droit d'émission. Elle opère avec la couche d'application pour fournir des ensembles de données simples, appelés **points de synchronisation**, qui permettent à l'application de connaître l'état de progression de la transmission et de la réception des données. Il s'agit donc d'une couche de temporisation et de contrôle des flux.

- La **couche de présentation** (*presentation layer* en anglais) contrôle la présentation des données à transmettre sous une forme ne dépendant pas des systèmes. Elle convertit les données de l'application en un format commun, souvent appelé la **représentation**

canonique, par exemple pour éviter le problème du code (Unicode, ASCII ou EBDIC) de représentation des caractères, le problème du format (petit-boutien ou grand-boutien) des entiers ou la façon d'indiquer le passage à la ligne.

Le seul problème qui relève de cette couche que nous aborderons sera celui concernant le format (petit-boutien ou grand-boutien).

- La **couche d'application** (*application layer* en anglais) est l'interface utilisateur vers le système OSI. C'est là que résident les applications telles que le courrier électronique. La tâche de la couche d'application est d'afficher les informations reçues et d'envoyer aux couches inférieures les données fournies par l'utilisateur.

1.2.3 Suite TCP/IP

L'architecture TCP/IP est similaire au modèle OSI mais ne met en jeu que trois couches, car elle combine les couches supérieures OSI en une seule et ne s'occupe pas des couches en-dessous de la couche réseau, les protocoles des ces couches étant propres au réseau sous-jacent. Elle date de 1974 mais elle est définie, après coup en 1989, dans la section 1.1.3 de [RFC 1122] :

Application
Transport
Internet

- La **couche application** (*application layer* en anglais) regroupe toutes les tâches orientées application, c'est-à-dire celles des couches 5 à 7 du modèle OSI.
- La **couche transport** (*transport layer* en anglais), comme dans le modèle OSI, permet le multiplexage et le démultiplexage entre les applications de systèmes d'extrémité.
- La **couche Internet** (*Internet layer* en anglais) est principalement chargée de de router les paquets IP de l'expéditeur au destinataire à travers le réseau. Elle correspond à la couche réseau du modèle OSI.

1.2.4 Le modèle des sockets

Les modèles ci-dessus datent de 1984 et 1989. Tout se complique encore par le fait que les sockets, mises en place en 1983, comme nous le verrons plus loin, donnent lieu à un modèle du sous-système réseau des systèmes d'exploitation en trois couches avec un vocabulaire différent, mais que l'on peut relier aux modèles précédents :

- La couche physique n'interfère pas du tout avec le sous-système réseau des systèmes d'exploitation, donc on n'en parle pas.
- Les protocoles de la couche liaison sont traités dans la partie électronique (le contrôleur) des cartes réseau. Il n'y a donc pas besoin non plus d'en parler au niveau du sous-système réseau.
- La couche réseau s'appelle **famille d'adresses**, la mise en place des sockets retenant essentiellement la structure des adresses.
- La couche transport s'appelle **type de communication**.

- Une troisième couche, appelée **protocole**, avait été prévue si les deux couches précédentes n'étaient pas suffisantes. On la retrouve comme paramètre (presque toujours égal à zéro) mais ne sert pas à grand chose.

- Les couches supérieures concernent les applications et non le sous-système réseau, donc on ne s'en occupe pas.

1.2.5 Modèle hybride

L'Internet et la plupart des réseaux intranets d'entreprise ont recours à une **architecture hybride** TCP/IP–OSI qui s'appuie sur les couches basses de l'architecture OSI pour spécifier les infrastructures de réseau de type LAN ou autres :

Application
Transport
Réseau
Liaison
Physique

Nous verrons de plus que la couche liaison de données est divisée en deux sous-couches dans le standard IEEE.

1.2.6 Cas de Linux

Linux se réfère au modèle hybride mais la mise en place conduit à deux commentaires :

- Linux ne s'occupe pas du tout de la couche physique puisque aucun élément de programmation n'intervient à ce niveau. La mise en œuvre des protocoles de la couche liaison est presque entièrement traitée dans les cartes réseau de nos jours ; Linux n'a donc pas à s'en préoccuper si ce n'est sous la forme d'une interface avec celle-ci (il faut bien commencer par quelque chose).

- Linux ne respecte pas entièrement la philosophie des couches avec une interface bien définie. Nous verrons, par exemple, que l'on passe directemnt de la couche application à la couche réseau dans certains cas (plus exactement lors de l'envoi de données UDP).

1.2.7 Les en-têtes de protocole

Une unité d'information est composée de données et d'informations de contrôle de cette unité d'information. Ces informations de contrôle sont généralement assemblées dans un bloc venant avant les données, ce qui est le cas pour tous les protocoles de TCP/IP. On appelle ces informations un **en-tête de protocole**.

Lorsque l'unité d'information est passée à la couche inférieure, celle-ci ajoute son en-tête à l'unité d'information passée, considérée comme les données de cette couche inférieure. De cette manière, lorsqu'une unité d'information est partie de la couche d'application, au moment où il atteint la couche physique, elle contient quatre en-têtes de protocole (sept avec le modèle OSI).

Pour mieux visualiser ce processus, on peut se représenter les différentes couches d'un oignon. L'intérieur est constitué par les données à envoyer. À chaque fois que l'unité d'information passe à travers une des couches, une couche d'oignon est ajoutée. Lorsqu'elle a parcouru toutes les couches, plusieurs en-têtes de protocole entourent les données initiales. Lorsque l'unité

d'information est envoyée à travers toutes les couches en partant du bas (sur une autre machine en général), chaque couche pèle l'en-tête de protocole lui correspondant. Lorsque la couche d'application de destination est atteinte, il ne reste plus que les données initiales.

OSI dispose d'une description formelle pour tout ce processus. La couche en cours porte le numéro N. Les données N-utilisateur à transférer doivent être précédées d'informations de contrôle de N-protocole (**N-PCI** pour *Protocol Control Information*) pour former une unité de données de N-protocole (**N-PDU** pour *Protocol Data Unit*). Les N-PDU sont passéss par l'intermédiaire d'un point d'accès de N-service (**N-SAP** pour *Service Access Point*) sous la forme d'un ensemble de paramètres de service comprenant une unité de données de N-service (**N-SDU** pour *Service Data Unit*). Les paramètres de service comprenant les N-SDU sont appelés les données d'utilisateur de N-service (**N-SUD** pour *Service User Data*), mis devant le (N-1)-PCI pour former un autre (N-1)-PDU.

1.3 Historique

Une bonne introduction à l'histoire des réseaux est [HL–96]. Elle a été écrite par des journalistes qui ont pu, d'une part, consulter les documents de littérature grise très difficilement accessibles et, d'autre part, interviewer les premiers acteurs de cette histoire. Elle contient une très grande documentation dont le seul reproche que l'on puisse faire est la non visibilité de la structuration par le manque de titres et sous-titres suffisamment explicites.

1.3.1 Naissance des ordinateurs

Il n'existe pas, à ma connaissance, d'étude abordable sur l'origine de la comptabilité au Néolithique, ni sur l'origine du calcul.

La notion de machine de calcul universel et l'apparition des premiers ordinateurs sont contés, à un niveau de haute vulgarisation avec des pointeurs sur la littérature primaire, dans [DAV–00], malheureusement non traduit en français.

1.3.2 Terminaux distants

Nous avons vu qu'une première alliance entre informatique et télécommunication est l'utilisation de terminaux distants de l'unité centrale, parfois situés à plusieurs milliers de kilomètres.

Le premier problème à résoudre pour cela est celui des utilisateurs multiples (*time-sharing* en anglais). Ceci est un problème du système d'exploitation. En 1961 est développé le **CTSS** (*Compatible Time Sharing System*) au MIT (*Massachussets Institute of Technology*), première réalisation importante mais encore expérimentale dans ce domaine.

Ceci conduira, en 1964, un groupe de chercheurs du MIT, des Bell Laboratories et de General Electric à s'associer pour initier le développement d'un système d'exploitation multi-utilisateur. Ils baptisèrent leur ambitieux projet **MULTICS** (*Multiplexed Information and Computing System*). Ce projet n'a pas vraiment abouti et sera abandonné en 1968. Il est cependant à l'origine de Unix, qui date de 1971.

Du point de vue matériel, dans les premiers essais d'utilisation des terminaux distants, on utilisait des lignes télex.

En 1974, IBM lance le **SNA** (*Systems Network Architecture*) qui normalise la communication entre un ordinateur et les terminaux distants. **VTAM** (*Virtual Telecommunication Access Method*) tourne sur l'ordinateur (un IBM 370) alors que **NCP** (*Network Control Program*) tourne sur le contrôleur de communication pour établir et surveiller en permanence le trafic.

1.3.3 Première mise en réseau : 1965

La première mise en réseau, entre deux ordinateurs (et non une unité centrale et un terminal), eut lieu en 1965. Le psychologue Tom Marill lança cette année-là une petite société de systèmes en temps partagé. Mais son principal investisseur ayant fait défaut à la dernière minute, il dut chercher un contrat de recherche et développement. Il proposa donc à l'ARPA de mener une expérience de mise en réseau, en joignant l'ordinateur TX-2 du Lincoln Laboratory et le SDC Q-32 situé à Santa Monica. La société de Marill était si petite que l'ARPA lui recommanda de procéder à son expérience sous l'égide du Lincoln Laboratory. L'idée plut aux responsables du Lincoln et ils chargèrent Larry Roberts de surveiller le projet.

La liaison entre les deux ordinateurs était réalisée grâce à un service spécial de la Western Union : quatre fils en duplex intégral. Marill branchait sur cette liaison un type de modem rudimentaire, opérant à 2 000 bits par seconde, qu'il appelait un composeur automatique (*automatic dialer*). Marill établit une procédure pour grouper les caractères en messages, les envoyer et vérifier qu'ils arrivent. Si aucun accusé de réception ne suivait, le message était transmis à nouveau. Il appela " protocole" de message l'ensemble des procédures pour faire circuler l'information dans les deux sens. En dépit de leurs efforts, lorsque Marill et Roberts connectèrent effectivement les deux machines, le résultat fut mitigé : le temps de réponse était médiocre (voir [HL–96], pp. 82–83).

Même si le résultat n'est pas vraiment celui escompté, il s'agit bien de la première mise en réseau : les ordinateurs ont des systèmes d'exploitation différents et on utilise des protocoles.

1.3.4 Réseaux de communication

De nos jours, "réseau" sans adjectif désigne toujours un réseau informatique. Le réseau est un concept général très utilisé depuis le réseau de nos connaissances personnelles jusqu'aux réseaux de communication et de télécommunication.

Les réseaux de communication cohérents commencent avec les Romains pour les routes, revus aux dix-neuvième siècle avec le réseau de routes nationales (départementales et vicinales) et celui des autoroutes au vingtième siècle sans oublier les chemins de fer.

Les réseaux de télécommunication commencent avec les feux dans l'Antiquité, les signaux de fumée des indiens d'Amérique, les relais de poste au début des Temps modernes. Il prit vraiment son essor avec le télégraphe optique de Chappe sous le Révolution puis avec le télégraphe électrique qui le détronera dans la seconde moitié du dix-neuvième siècle. C'est aussi le début des premiers câbles transatlantiques. Le réseau téléphonique suivra avec la naissance des grandes sociétés telles que AT&T aux États-Unis et les PTT dépendant directement du gouvernement dans de nombreux pays dont la France.

1.3.5 Le premier réseau : ARPANET en 1971

Le vendredi 4 octobre 1957, l'Union Soviétique lance le premier satellite artificiel, appelé Spoutnik. Les Américains considèrent cela comme une menace. Le président Einsenhower demande le 7 janvier 1958 au Congrès les fonds nécessaires pour créer l'ARPA (*Advanced Research Projects Agency*). Directement lié au président at au secrétaire à la défense, cet organisme de recherche avait pour but de garantir, par la promptitude de sa réaction, que les américains ne soient désormais plus jamais en retard dans aucun domaine technologique ([HL–96], pp. 19–31).

En 1961, le directeur de l'ARPA cherchait quelqu'un pour gérer le contrat d'un nouvel ordinateur commandé par l'ARPA, le Q-32, ainsi que quelqu'un qui pût diriger un nouveau programme, demandé par le département de la Défense et axé sur les sciences du comportement. À l'automne 1962, il trouve enfin un candidat susceptible d'occuper les deux postes, un éminent psychologue

nommé Joseph Carl Robnett Licklider. D'après son contrat, sa tâche principale était de trouver pour l'ordinateur des utilisations qui en fassent autre chose qu'un outil destiné aux calculs numériques des scientifiques. En un rien de temps, il prit contact avec les meilleurs informaticiens du moment, à Stanford, au MIT, à Berkeley, à UCLA (*University of California, Los Angeles*), ainsi qu'avec une poignée de sociétés. Six mois après son arrivée à l'ARPA, Licklider envoya une longue note aux membres de cet entourage à propos de la dispersion excessive des thèmes de recherche ([HL–96], pp.32–49). Comment parvenir à y remédier ? Il discuta de l'hypothèse d'un réseau (*network*) d'ordinateurs :

> "Considérez la situation où plusieurs centres sont réunis dans un même filet [*netted*], chaque centre étant tout à fait singulier, avec son propre langage et sa propre façon de façon de faire les choses. N'est-il pas désirable ou même nécessaire que tous les centres s'accordent sur un quelconque langage ou, du moins, sur quelques conventions pour poser des questions telles que : "Quel langage parlez-vous ?" À ce point, le problème est avant tout celui dont débattent les auteurs de science-fiction : comment amorcer des communications entre des êtres doués de raison, mais privés de toute forme de correspondance ?"

L'une des personnes récrutées par Licklider, Robert Taylor, devint le directeur du service de celui-ci, le LIPTO, en 1966. Il décida de mettre en pratique les idées de Licklider et demanda un financement pour faire l'expérience d'un réseau d'ordinateurs. Il suggéra que l'ARPA finance un petit réseau à titre d'essai : on commencerait, par exemple, avec quatre nœuds, et on poursuivrait jusqu'à une douzaine environ ([HL–96], pp.49–53). Il obtînt un million de dollars pour mettre en place son système.

L'architecte d'un tel réseau devrait être également un expert en télécommunication. Taylor recruta Larry Roberts en décembre 1966 ([HL–96], pp.55–63). Celui-ci commença par écrire une note dans laquelle il appelait les ordinateurs intermédiaires qui contrôleraient le réseau des "serveurs de messages", des **IMP** pour *Interface Message Processor*. Ils devaient remplir les fonctions suivantes : interconnecter le réseau, envoyer et recevoir des données, effectuer des tests d'erreur, retransmettre en cas d'erreur, acheminer les données et vérifier que les messages arrivent aux destinations voulues ([HL–96], pp.81–91). Un protocole serait établi pour définir avec exactitude comment les IMP devraient communiquer avec les ordinateurs hôtes (il ne le sera jamais).

Fin 1967, Roberts présenta son premier exposé sur ce qu'il appela l'"ARPA net", le réseau de l'ARPA, à un colloque d'informatique de l'ACM à Gatlinburg, dans le Tennessee.

Roberts estimait que le réseau devait démarrer avec quatre sites : UCLA, le SRI (*Stanford Research Institute*), l'université d'Utah et l'UCSB (*University of California, Santa Barbara*). Dans un second temps, il se développerait jusqu'à en réunir dix-neuf environ. Il décida de passer un appel d'offres, qu'il termina fin juillet 1968. Les premières réactions, négatives, à l'appel d'offres vinrent des deux plus grands constructeurs d'ordinateurs, IBM et Control Data Corporation (CDC). Les deux sociétés refusèrent de soumissionner car elles estimaient que le réseau ne pourrait jamais être construit parce qu'il n'existait pas d'ordinateur assez petit pour rendre l'affaire rentable. Plus d'une douzaine d'offres furent soumises. Juste avant noël 1968, l'ARPA annonça que le contrat pour la construction des serveurs de messages était attribué à Bolt, Beranek & Newman (BBN), une petite société de conseils de Cambridge, Massachussetts ([HL–96], pp.92–97).

Les cinq années suivantes furent consacrées à des tests et à des mises au point. En 1971, ARPANET entra en service régulier. Les machines utilisaient ARPANET en se connectant à un IMP. La façon de connecter un IMP au réseau se faisait à l'aide du **protocole "1822"**, dont le nom provient du nombre de pages techniques décrivant le système. Nous verrons que la

façon dont un hôte devait se relier à l'IMP ne fut jamais décrit dans un protocole de la part des concepteurs de l'ARPANET.

Notons qu'en 1980 l'agence change de nom, passant de ARPA à DARPA (*Defense Advanced Research Projects Agency*).

Références

[TAN–81], à travers ses éditions successives, est devenu le classique pour une vue d'ensemble sur les réseaux. Il contient beaucoup d'informations mais pas d'exemple étudié en détail. [K-R–01] peut devenir un concurrent sérieux et au minimum un très bon complément. [PUJ–04] est le classique français.

La norme ISO 7498, *Open System Interconnection Model standard* est décrite dans quatre documents, disponibles en anglais et en français : [ISO 7498-1], [ISO 7498-2], [ISO 7498-3] et [ISO 7498-4].

L'architecture TCP/IP a été décrite, après coup, dans [RFC 1122].