Création du réseau informatique d'un laboratoire de recherche avec les composantes supervision et sécurité

Thierry Dautcourt

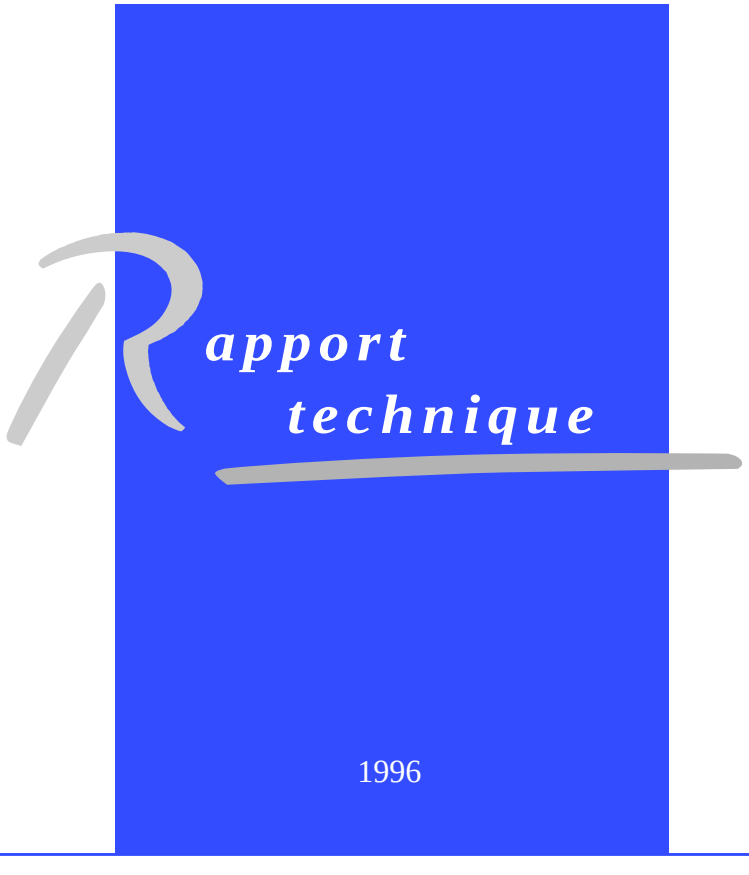
INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Création du réseau informatique d'un laboratoire de recherche avec les composantes supervision et sécurité

Thierry Dautcourt

N° 189

PROGRAMME 7



Création du réseau informatique d'un laboratoire de recherche avec les composantes supervision et sécurité

Thierry Dautcourt
Thierry.Dautcourt@loria.fr

Programme 7

Rapport Technique n°189 - Février 1996 - 128 pages

Résumé : L'objectif de ce rapport est de présenter l'approche originale et efficace mise en oeuvre lors de la création d'un réseau informatique reliant plus de deux cent cinquante stations de travail UNIX. Ce réseau devait offrir aux cinq cents chercheurs, enseignants-chercheurs et thésards d'un centre de recherche en informatique, un cadre de travail performant et adapté à leurs besoins particuliers. Parmi ces besoins, nous pouvons citer un temps de réponse rapide et homogène aux services, une disponibilité maximale tant au niveau matériel que logiciel, une demande d'outils scientifiques très diversifiés.

Le rapprochement physique en 1992 dans un même bâtiment des deux centres de recherche : le CRIN (Centre de Recherche en Informatique de Nancy) et l'unité Lorraine de l'INRIA, a nécessité la fusion des deux réseaux informatiques initiaux.

Tous les éléments nécessaires à la réalisation d'un réseau informatique sont analysés. Ainsi, successivement, nous décrivons l'étude et l'implantation du câblage, l'infrastructure et l'interconnexion réseau et les services offerts aux utilisateurs et aux administrateurs systèmes.

Nous présentons également les aspects concernant la sécurité informatique et la supervision du réseau qui doivent être complètement intégrés au niveau de la conception du réseau au moment de la conception et non a posteriori.

UNITE DE RECHERCHE INRIA-LORRAINE

Technopole de NANCY-BRABOIS Campus Scientifique - 615 rue du Jardin Botanique - BP 101
54602 VILLERS LES NANCY - Tél : 83 59 30 00- Télécopie : 83 27 83 19 - Télex: 850 238 F

Title : Network construction of a computer science research center with supervision and security aspects.

Abstract : The aim of this technical report is to present the original approach taken in the creation of a computer network. This network is composed of more than two hundred and thousand Unix workstation and has to provide a specific frame for researchers and teachers.

Among their needs, we could mention a fast and homogenous answering time to network services and a maximal availability of the software level.All elements of a computer network , following the layers of the OSI model, are analysed in this report : cabling system , network infrastructure and services. During the creation, the two features security and supervision have been strongly included.

Ce rapport a été rédigé pour l'obtention du Titre d'Ingénieur Diplômé par l'Etat en Informatique. Ce travail a été soutenu le 9 novembre 1995 à l'Ecole Supérieure d'Ingénieurs en Electrotechnique et Electronique de Noisy-Le-Grand.

Le jury composé de Madame M.C. WEBER et de Messieurs A. CABESSA, O. MOULIN et D. PERROT était présidé par P. ABEILLE. Que ces personnes soient ici remerciées d'avoir accepter d'évaluer mon travail.

Introduction

L'objectif de ce rapport est de présenter l'approche originale et efficace que nous avons mise en oeuvre lors de la création d'un réseau informatique reliant plus de deux cent cinquante stations de travail UNIX. Ce réseau devait offrir aux cinq cents chercheurs, enseignants-chercheurs et thésards d'un centre de recherche en informatique, un cadre de travail performant et adapté à leurs besoins particuliers.

Le rapprochement physique en 1992 des deux centres de recherche : le CRIN, Centre de Recherche en Informatique de Nancy, et l'unité Lorraine de l'INRIA, Institut National de Recherche en Informatique et Automatique, a nécessité la fusion, et donc la restructuration complète, des deux réseaux informatiques initiaux. En même temps que la construction et l'aménagement du bâtiment devant abriter les deux centres, il fallait élaborer l'architecture du nouveau réseau informatique commun.

La création et l'implantation d'un réseau informatique, tant au niveau de l'architecture, de la topologie que de l'implantation des services aux utilisateurs, est une opération complexe surtout lorsque ce réseau met en oeuvre plusieurs centaines de stations de travail et micro-ordinateurs hétérogènes, comme des stations *Sun*, *Hewlett Packard*, *Silicon Graphics*, *Dec* et des micro-ordinateurs *Macinstosh* ou *PC*. De plus, chaque réseau est particulier en ce qui concerne le nombre et le type des stations de travail, la structuration du réseau, les services à fournir aux utilisateurs ; aussi il n'est guère possible de transposer un réseau déjà existant d'un site à un autre et l'on peut seulement étudier ou fortement adapter d'autres réseaux déjà mis en place. Pour des raisons que nous détaillons dans ce rapport, il n'était également pas souhaitable de reprendre l'une des deux architectures des réseaux initiaux.

Ce rapport explique la démarche que nous avons suivie pour créer un réseau informatique commun aux deux centres de recherche avec pour objectif, une fiabilité de fonctionnement maximale et l'intégration des composantes supervision et sécurité.

Le **premier chapitre** est consacré à la présentation des deux centres informatiques et de leur réseau informatique respectif. Nous y étudions les points faibles et les points forts de l'architecture et du fonctionnement de ces réseaux, car cette étude a initialisé la conception du nouveau réseau.

Nous décrivons ensuite, au **chapitre 2**, la première opération qui a été réalisée pour la création du nouveau réseau. Cette opération a consisté en la fusion des espaces d'adressage des deux réseaux initiaux et a nécessité la renumérotation de l'ensem-

ble des adresses des stations du site.

Les deux chapitres suivants sont consacrés à la définition de l'architecture du nouveau réseau. Nous présentons, au **chapitre 3**, le câblage et les interconnexions des sous-réseaux, et, au **chapitre 4**, les services logiciels pour les utilisateurs et les administrateurs système.

Nous décrivons au **chapitre 5**, l'implantation d'outils permettant une bonne administration du réseau.

Enfin, tout implantation de réseaux implique l'installation de mécanismes qui permettent de détecter, de contrer toutes actions malveillantes, qu'elles soient internes ou externes au réseau, et de garantir la restitution des données dans leur état initial s'il s'est produit une quelconque modification. Nous étudions au **chapitre 6** cet aspect de la sécurité des réseaux.

Le **dernier chapitre** aborde le réseau actuel avec le recul nécessaire ; nous y étudions la préservation de l'investissement ainsi que les extensions réalisées de 1992 à 1995. Nous concluons sur l'étude de l'avenir de ce réseau face aux nouvelles technologies qui arrivent sur le marché.

L'ensemble des opérations concernant la mise en oeuvre et le fonctionnement d'un réseau informatique fait partie des tâches à assurer et/ou à diriger par un ingénieur réseau. Une telle personne doit, d'une part effectuer un travail quotidien comprenant la maintenance du réseau, l'analyse des problèmes du réseau afin de garantir un fonctionnement continu de ce dernier, la surveillance au niveau de la sécurité et la formation aux utilisateurs. D'autre part, la veille technologique occupe une part importante du travail d'un ingénieur réseau afin que celui-ci soit à même de conduire les évolutions matérielles et logicielles du réseau avec une vision à long terme.

La phase de création du nouveau réseau Loria a duré une dizaine de mois et a mobilisé trois ingénieurs systèmes à plein temps, issus à la fois du CRIN et de l'INRIA, lesquels ont été aidés par d'autres personnes de l'équipe système. Mon rôle dans ce travail, outre des réalisations techniques comme l'implantation du logiciel de montage automatique de partitions, la mise en oeuvre de la supervision ou bien encore les filtrages au niveau de la sécurité, a été de prendre en charge la coordination entre les différents travaux effectués, de conserver une vue globale du projet et de ses objectifs permettant ainsi de donner au réseau une structure homogène. J'avais déjà dans mon précédent emploi effectué un travail organisationnel du même type mais dans un cadre plus logiciel lorsque j'ai piloté l'opération de transferts d'applications de l'INIST[1] d'un réseau à un autre.

1 Institut National de l'Information Scientifique et Technique.

La création du nouveau réseau s'est passée en douceur et sans heurts. En réalité, les utilisateurs n'ont subi que très peu de modifications dans leur environnement de travail alors que la structure du réseau et les environnements système ont été complètement modifiés. Cependant, j'ai jugé utile, six mois après la mise en service du nouveau réseau, d'effectuer une formation aux utilisateurs. Il ne s'agissait pas de donner un cours sur les réseaux informatiques, mais de fournir des éléments techniques aux utilisateurs leur permettant ainsi d'utiliser le réseau de manière optimale.

Notons que toute modification touchant au fonctionnement d'un réseau, qu'elle soit logicielle ou matérielle, doit obligatoirement être préalablement testée sur un échantillon réduit avant d'être effectuée en grandeur réelle. Nous devons toujours être soucieux de la fiabilité et du confort de l'environnement de travail offert aux utilisateurs et respecter leurs besoins. Aussi, dans la mesure du possible, chaque modification du réseau (renumérotation des adresses des machines, montage automatique des partitions, etc) a été préalablement testée sur quelques machines connectées en mini-réseau, comme nous le détaillons à nouveau dans la suite du rapport.

Enfin, précisons que ce rapport n'est pas exhaustif dans la description des différentes tâches qui ont conduit à la création du nouveau réseau, mais que seuls les éléments dans lesquels je me suis impliqué sont détaillés.

CHAPITRE 1

Les deux centres informatiques et leurs réseaux

Mon arrivée à l'Inria a précédé d'une année le regroupement des deux centres de recherche, le CRIN et l'Inria Lorraine, et la fusion de leurs réseaux. Venant de l'extérieur, j'avais l'avantage de percevoir et d'analyser les points forts et les points faibles des réseaux. L'étude que j'ai menée sur le fonctionnement des réseaux est décrite dans ce chapitre, après la présentation deux centres informatiques et de l'évolution de leurs réseaux respectifs.

1. Présentation du CRIN et de l'Inria Lorraine

Le CRIN est l'un des premiers centres de recherche en informatique français et il a maintenant plus de 20 ans d'existence. Ce laboratoire est une unité de recherche associée au CNRS (URA 262) et aux Universités de Nancy : Université de Nancy 1 Henri Poincaré, Université de Nancy 2 et INPL[1].

L'objet des recherches menées au laboratoire est centré sur la définition, le développement et l'exploitation de modèles informatiques.

Le CRIN compte 13 équipes de recherche, dont 6 communes avec l'Inria Lorraine, qui sont regroupées suivant deux thèmes principaux :

- les théories et techniques de la production du logiciel,
- la communication homme-machine et l'intelligence artificielle.

L'Inria Lorraine est l'une des cinq unités de l'INRIA réparties sur le territoire français (Grenoble, Nancy-Metz, Rennes, Rocquencourt et Sophia). Les missions de l'INRIA sont les suivantes :

1 Institut National Polytechnique de Lorraine.

- la recherche fondamentale et appliquée,
- la réalisation de systèmes expérimentaux,
- la valorisation des résultats,
- la diffusion des connaissances,
- les échanges scientifiques internationaux,
- la contribution à des programmes de coopération,
- les expertises scientifiques,
- la contribution à des actions de normalisation.

L'INRIA est un EPST[1] placé sous la tutelle du Ministre chargé de l'Education Nationale, de l'Enseignement Supérieur, de la Recherche et de l'Insertion Professionnelle, conjointement avec le Ministre chargé des Technologies de l'Information et de la Poste.

Cette unité a été créée en 1987 en association étroite avec des laboratoires universitaires régionaux associés au CNRS : six projets en Informatique avec le CRIN, un projet en Mathématiques Appliquées avec l'Institut Elie Cartan de l'Université Henri Poincaré et un projet avec le Laboratoire de Méthodes Mathématiques pour l'Analyse des Systèmes (MMAS) de l'Université de Metz.

Cette collaboration est coordonnée par un comité de concertation : le Loria[2], et s'inscrit dans le pôle technologique régional IAE+M[3].

Son activité de recherche est répartie en quatre programmes :

- Calcul symbolique, Programmation et Génie logiciel ;
- Intelligence artificielle, Systèmes cognitifs et Interaction homme-machine ;
- Automatique et Productique ;
- Calcul scientifique, Modélisation et Logiciel numérique.

En outre, des responsabilités particulières au niveau de l'unité de recherche, sont assurées par des chargés de mission : relations industrielles, relations internationa-

1 Etablissement Public à caractère Scientifique et Technologique.
2 La désignation Loria est multiple : elle définit la collaboration entre le CRIN et l'Inria Lorraine et elle représente également le nom du réseau ainsi que le nom du bâtiment.
3 Informatique, Automatique, Electronique et Mathématiques.

les, communication, formation.

Pour l'année 1994, les deux centres regroupaient environ 260 personnes (80 Enseignants-Chercheurs, 10 Chercheurs CNRS, 10 Chercheurs INRIA, 109 Doctorants, 18 Ingénieurs, Techniciens et Administratifs) auxquels il faut ajouter une cinquantaine d'étudiants préparant un DEA. La production scientifique commune aux deux centres donne lieu annuellement à une moyenne de 25 thèses et de 250 publications dans des revues spécialisées, ouvrages de synthèse et colloques.

2. Le réseau physique initial du CRIN

Le CRIN n'avait à sa création, en 1973, aucun moyen informatique local et travaillait sur le centre de calcul de Nancy, l'Institut Universitaire de Calcul Automatique (IUCA), créé en 1959, et devenu aujourd'hui le Centre Inter-universitaire de Ressources en Informatique de la Région Lorraine (CIRIL).

Par la suite, un, puis plusieurs ordinateurs centraux (MITRA 15, Vax, Convex C201,...), localisés sur le site du laboratoire ont été installés. Successivement, l'outil de travail du chercheur est passé du terminal non graphique connecté à un ordinateur central par une liaison série, à une station de travail graphique gérée par un système multi-fenêtrage, ayant une puissance de calcul propre, fonctionnant sous le système d'exploitation UNIX et livrée avec une interface réseau, en l'occurrence ethernet. Ethernet est une technologie de réseau local, développée au début des années 1980, permettant, le dialogue entre des ordinateurs relativement proches. Ethernet a été standardisé en 1985 par le comité IEEE sous la référence IEEE802.3. Ce standard définit à la fois le support physique, la méthode d'accès au support, la topologie et les contraintes d'implantation [FERRERO 95].

Intéressons-nous à présent à l'architecture de l'ancien réseau du CRIN. Il n'y avait initialement qu'un seul type de média pour implanter ethernet. Ce média est appelé «Thick ethernet cable» ou câble épais ou encore câble jaune de par la couleur de l'enveloppe isolante extérieure. Aujourd'hui, les supports physiques d'ethernet se sont largement diversifiés et ce type de câblage a été nommé 10 base 5 (10 correspond à la vitesse de transmission soit 10Mb/s et 5 fait référence à la longueur maximale du segment autorisée, soit 500 mètres).

Le laboratoire de recherche du CRIN occupait en 1992, trois étages consécutifs d'un bâtiment représentant une superficie de 1800 m^2. La structure initiale du câblage était du câble coaxial épais qui parcourait les trois étages de manière linéaire, passant dans chaque bureau comme représenté figure 1. Les stations de travail étaient reliées au câble par l'intermédiaire de prise vampire. La figure 2 illustre une coupe

du câble coaxial et une prise vampire.

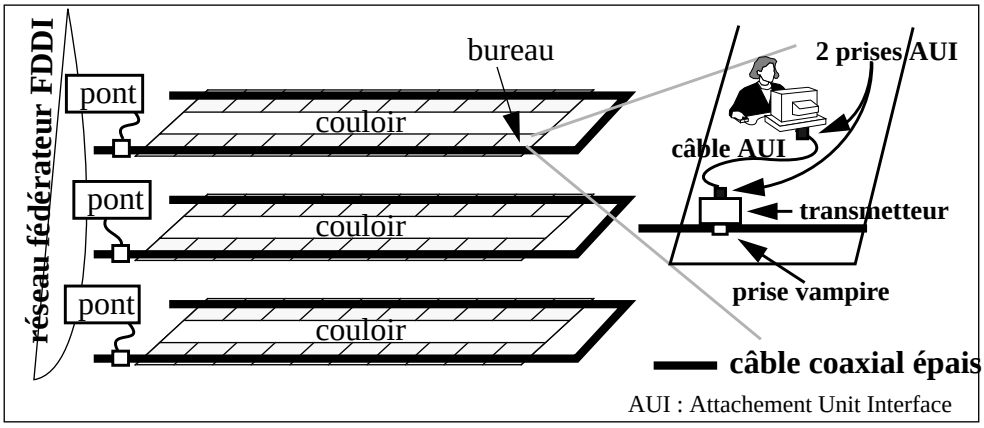


FIGURE 1. La structure de l'ancien réseau du CRIN.

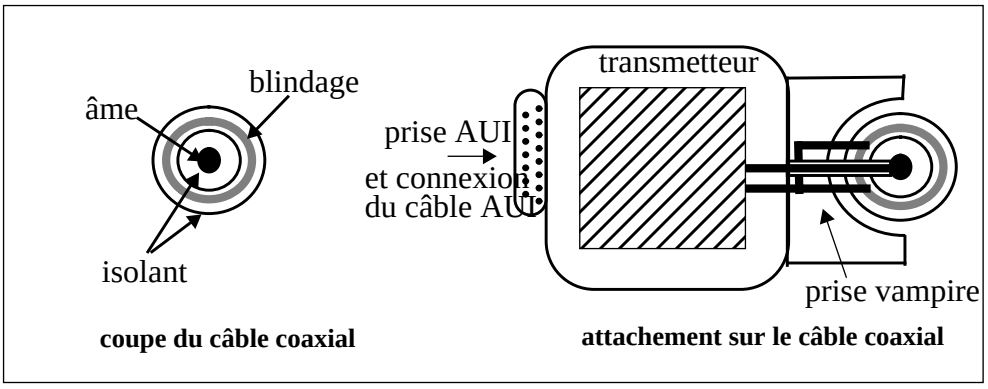


FIGURE 2. Le câble ethernet épais et l'attachement d'une station sur le câble.

Chaque étage du bâtiment avait son propre segment ethernet, chacun de ces segments était connecté à un pont. Un pont a plusieurs interfaces (au minimum deux) et établi l'interconnexion de segments en filtrant le passage des trames entre ses interfaces. Le filtrage est réalisé par la création de tables d'adresses physiques par interface. Le pont apprend la localisation des stations de part et d'autre de ses interfaces et ne laisse transiter que les trames dont les adresses source et destination sont sur deux segments dif-

férents. Ce mécanisme simple permet de diminuer le trafic sur chaque segment.

Les trois segments ethernet de chaque étage étaient fédérés et filtrés par des ponts qui dialoguaient entre eux par le protocole FDDI[1]. Cela signifie qu'au lieu d'utiliser ethernet pour les couches 1 et 2, on utilise un autre moyen de transport qui a un débit de transmission plus élevé (100 Mb/s). Le mécanisme du pont travaille au niveau 2 des couches définies par l'OSI, il est détaillé par la suite dans la section 4. à la page 52. Ces ponts étaient physiquement connectés entre eux par de la fibre optique multimode[2].

Il est intéressant ici de présenter dans le détail quelques problèmes de fonctionnement liés à l'architecture de ce réseau local ethernet dans l'objectif de les supprimer du nouveau réseau à construire.

Différents types de problèmes de fiabilité se sont posés, ils étaient liés soit à la structure en bus, soit à la structure même du câble, et provenaient également des règles d'accès au support.

Les problèmes liés à l'architecture en bus

La topologie du câblage était «en bus», c'est-à-dire que tous les attachements étaient réalisés sur un même câble physique[3].

Dans une topologie de câblage en bus, lorsqu'une source émettrice ou l'interface ethernet d'une station se met à dysfonctionner, il y a propagation de la perturbation sur l'ensemble du câble et donc dysfonctionnement général. La cause peut être aussi bien un problème de liaison électrique au niveau de l'attachement vampire, que le non respect de la norme par les fournisseurs d'équipement ethernet.

Cette anomalie est très difficile à détecter car il n'existe pas de mécanisme permettant de fournir des informations sur la localisation de la panne. Ainsi pour identifier la source de la panne, il est nécessaire de déconnecter une par une toutes les stations se trouvant sur le bus jusqu'à la disparition du problème.

1 «Fiber Distributed Data Interface».

2 Ce type de fibre supporte la propagation de plusieurs fréquences de lumière par opposition à la fibre monomode qui ne propage qu'un seul faisceau. La fibre multimode est la plus utilisée pour les liaisons inférieures à deux kilomètres et en raison du coût plus bas des sources lumineuses (LED au lieu de laser).

3 Les autres topologies des réseaux sont en étoile, en anneau, etc.

Les problèmes liés à la connectique et au câble

La connexion d'une station au câble du réseau se fait par l'intermédiaire d'une prise vampire. Comme son nom le suggère, cette prise perce le câble pour effectuer le contact avec l'âme du câble. Des connexions successives sur le câble endommagent celui-ci et peuvent ainsi provoquer des problèmes électriques. Une difficulté supplémentaire provient de la nécessité de respecter des distances fixes entre les prises vampires.

Le câble est dénommé «thick cable» en raison de son épaisseur, il fait 1 cm de diamètre environ. Cette épaisseur provoque une grande rigidité du câble et la nécessité de respecter un rayon de courbure important (50 cm) dans les courbes sous peine de fragiliser le câble [ROLLIN 88].

Les problèmes liés aux règles et aux limites d'ethernet

Les équipements raccordés sur le câble augmentent au fur et à mesure des acquisitions de matériels. Cependant, la structure même d'ethernet fait que le nombre de stations directement connectées sur un même segment doit être limité si l'on veut conserver de bonnes performances. Le seuil d'écroulement du réseau dépend du nombre du stations mais également de l'activité des machines connectées.

Voyons comment se présentent les règles de communication que doivent respecter les interfaces par l'intermédiaire de la couche d'accès au media (couche MAC[1]) :

- avant d'émettre un paquet ou une trame, l'interface doit attendre un temps minimum de silence (9,6 µs) sur la ligne ; après ce temps réglementé, l'émission peut commencer ;
- si deux interfaces émettent simultanément, il se produit une collision. Cette collision est détectée et toutes les interfaces concernées stoppent leurs émissions respectives. Elles ne réemettent chacune qu'au bout d'un temps aléatoire pour éviter de reproduire une collision.

Il devient alors évident que lorsque le nombre de stations sur un même segment augmente, il se produit un phénomène d'écroulement du réseau car trop de stations veulent dialoguer simultanément et provoque ainsi de multiples collisions.

D'autres problèmes difficilement identifiables peuvent survenir. En 1993, une étude réalisée par Xerox [METCALFE 93] a démontré que certaines machines ou stations perdaient des paquets. La cause en serait une zone d'ombre dans la définition[2] du standard IEEE802.3. Plus particulièrement, il est indiqué que le délai entre deux tra-

1 «Medium Access Control» ou contrôle d'accès au media.

mes[1] doit être de 9,6 µs. L'interprétation de détection de la collision faite par l'interface est différente suivant les technologies employées et ceci peut provoquer un délai inférieur au seuil de 9,6 µs entre la fin de la collision et la trame suivante. Dans ce cas, l'interface est généralement incapable de prendre en compte le paquet et, ce qui est plus grave, ce paquet est perdu sans qu'il soit comptabilisé dans les paquets perdus puisqu'il n'a pas été capté par l'interface. Ces problèmes peuvent avoir des effets désastreux puisque la gestion des erreurs s'effectue dans les couches supérieures du protocole. Par exemple, s'il manque un seul paquet, il est redemandé de transmettre à nouveau l'ensemble de la séquence ce qui provoque alors un trafic réseau supplémentaire. Ces pertes de paquets ne sont pas détectables sans matériel sophistiqué et ne se produisent que sur un réseau ayant un fort taux de charge, engendrant alors un nombre important de collisions.

3. Le réseau physique initial de l'Inria Lorraine

Le bâtiment de l'Inria Lorraine a été construit au début de l'année 1990. Il constitue en fait la première tranche du futur bâtiment Loria. Ce bâtiment a été édifié sur le Campus de la Faculté des Sciences, à quelques centaines de mètres du bâtiment abritant le CRIN. Pour la réalisation de cette première tranche, il n'y a eu aucune opération de précâblage. Seule la partie de passage de câble a été intégrée sous la forme de caniveaux centraux inclus dans la dalle de chaque bureau, eux-mêmes reliés aux caniveaux des couloirs permettant ainsi le passage des câbles des bureaux vers les salles serveurs.

Les stations étaient reliées entre elles par des répéteurs multi-ports via des câbles du même type que ceux reliant la station à la prise vampire. Ces câbles sont appelés «drop cable» ou également câble AUI. La structure de liaison entre les stations est en étoile sur un répéteur multi-port. Les répéteurs multi-port sont des dispositifs électroniques passifs, ils comportent au maximum 16 ports et peuvent être chaînés entre eux. La taille maximale des câbles de raccordement est de 50 mètres. La figure 3 représente le raccordement des stations aux répéteurs sur le réseau de l'Inria Lor-

2 Ce point reste un sujet de polémique, car au-delà des détails techniques, il concerne des enjeux économiques considérables : les fondeurs de circuits et les constructeurs d'interfaces ne souhaitent pas assumer la responsabilité des problèmes de fonctionnement engendrés par leurs réalisations.

1 «Inter Frame Gap» ou espace entre les trames.

raine.

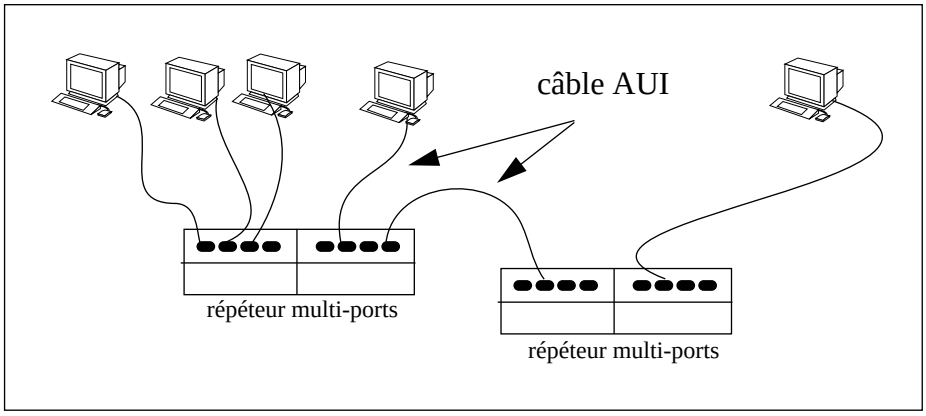


FIGURE 3. La structure physique du réseau de l'Inria Lorraine.

4. L'interconnexion des deux réseaux

Les ponts des réseaux du CRIN et de l'Inria Lorraine étaient reliés entre eux par de la fibre optique et dialoguaient en utilisant le protocole FFDI. Les deux bâtiments étaient placés sur le même Campus Universitaire ; ce campus étant un domaine privé, il a permis l'installation de lignes privées en fibre optique sans passer par un opérateur et donc sans avoir à supporter un coût de fonctionnement.

Les deux réseaux étaient reliés d'un coté au réseau de la Faculté des Sciences comprenant les ordinateurs et les stations de travail des autres laboratoires et de l'autre au monde Internet par l'intermédiaire d'une liaison spécialisée à 64 kb/s vers le site INRIA de Rocquencourt. La figure 4 présente l'interconnexion des deux réseaux.

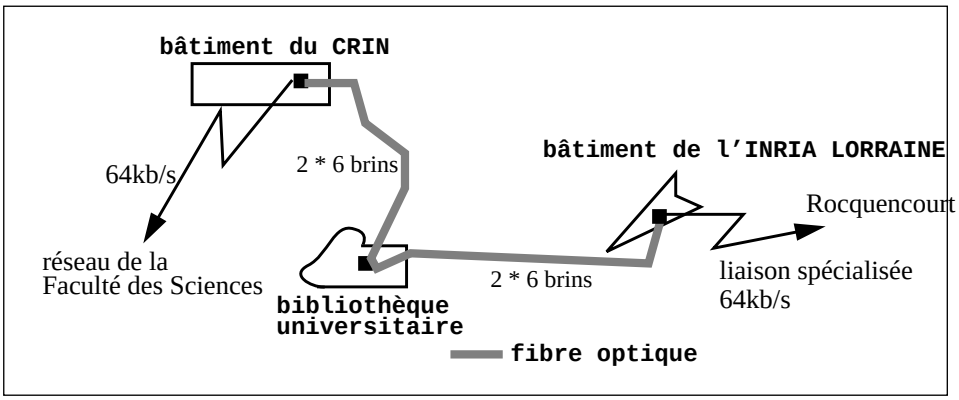


FIGURE 4. L'interconnexion des réseaux CRIN et Inria Lorraine.

Pour pouvoir communiquer, une machine doit disposer de trois identificateurs : une adresse ethernet, un nom et une adresse IP[1] :

- l'adresse ethernet est unique et verrouillée en mémoire morte par le constructeur sur sa carte de communication. Cette adresse est codée sur 6 octets et des tranches d'adresse sont affectées à chaque constructeur. Bien évidemment cette adresse n'est pas modifiable par l'utilisateur ;
- le nom d'une machine, choisi par les utilisateurs, est une facilité d'identification. Tous les sites ayant un parc d'ordinateurs sous Unix procèdent ainsi. Ce nom est appelé nom court par opposition au nom qualifié qui est unique et composé du nom court suivi du nom de domaine du réseau. Par exemple **clovis** est le nom court d'une machine, son nom qualifié est **clovis.loria.fr** sur le réseau Loria;
- l'adresse IP est codée sur 4 octets que l'administrateur paramètre dans le système.

L'adresse IP et le nom de la machine sont stockés dans un fichier modifiable par l'administrateur système.

L'adresse IP est utilisée lors de la connexion au réseau international Internet, permettant ainsi l'accès à ses nombreux services. Pour disposer de la «connectivité internationale», chaque adresse IP doit être unique et connue de l'ensemble des routeurs composant le réseau Internet. La visibilité de ces adresses et des noms associés est assurée par un mécanisme d'annuaire. Ce gigantesque annuaire[2] est géré mondialement de manière arborescente et nécessite lui aussi une identification préalable pour être connu de l'extérieur. Les informations stockées dans cet annuaire concernent les adresses IP des machines ainsi que leurs noms, mais également des informations spécifiques comme l'adresse de la machine distribuant son annuaire local ou l'adresse de la station habilitée à traiter en réception tout le courrier électronique d'un site.

Les deux réseaux (CRIN et Inria Lorraine), bien qu'ayant une infrastructure physique différente, disposaient d'un mode de fonctionnement collectif. L'administration réseau et système était centralisée et globale. Par exemple, l'ouverture d'un compte était unique et permettait l'accès à l'ensemble des ressources des deux réseaux. En fait, l'existence de deux réseaux distincts mais interconnectés était transparente pour les utilisateurs, lesquels ne percevaient qu'un seul réseau.

1 «Internet Protocol».

2 Cet annuaire est géré par des serveurs de noms ou DNS (Domain Name Server) répartis géographiquement sur tout l'Internet. Ils sont logiquement attachés entre eux de façon hiérarchique, la racine se trouvant aux Etats-Unis.

Dans l'ensemble des services de gestion du réseau utilisé, certains apportaient effectivement un avantage en ce qui concerne la facilité d'utilisation et la cohérence du réseau ; ce sont les services NIS et NFS [STERN 91]. Ces services ont été analysés en détail et tous les points positifs ont été incorporés dans le nouveau réseau. En revanche, l'utilisation de ces services provoquait certains problèmes de fonctionnement et ceux-ci ont été étudiés avec attention. La section suivante est consacrée à ces deux services.

5. Les services d'administration réseau utilisés dans l'ancien réseau

La gestion centralisée des informations administratives devient rapidement indispensable lorsqu'un réseau atteint une taille importante, surtout si l'on veut conserver une cohérence sur un parc de machines hétérogènes.

Prenons l'exemple de l'ouverture d'un compte utilisateur. L'ouverture d'un compte sur une machine correspond à la création d'une part d'un enregistrement dans le fichier **/etc/passwd** et, d'autre part, d'un espace de travail sur disque.

Si nous prenons le cas de deux utilisateurs ayant chacun un compte sur une machine différente, nous nous apercevons que ceux-ci ne peuvent pas travailler ensemble. En effet, dans la situation illustrée figure 5, l'utilisateur A possède un environnement A sur la machine 1, c'est-à-dire un compte et une partition de travail ; de même l'utilisateur B a un environnement B sur la machine 2. L'utilisateur B ne peut pas se connecter sur la machine 1 car il n'a pas de compte sur cette machine, il ne peut pas non plus accéder à la partition de l'utilisateur A puisque celle-ci n'est disponible que sur la machine 1.

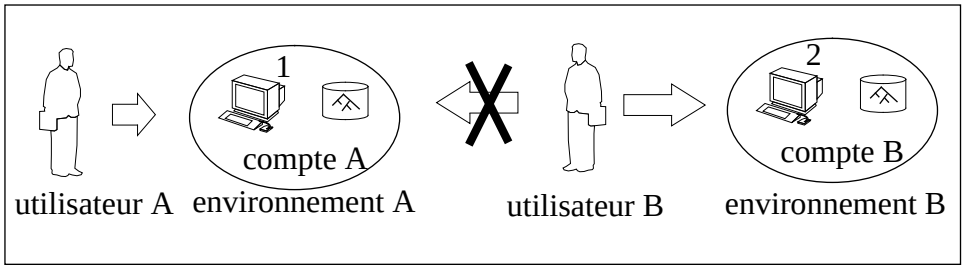


FIGURE 5. L'environnement utilisateur sur une machine.

Afin qu'un utilisateur puisse travailler avec l'ensemble de sa communauté de recherche au sein d'un même laboratoire, il faut lui ouvrir un compte sur chaque station du réseau. Pour une seule machine, l'ouverture d'un compte est une opération très simple à réaliser, mais il n'est pas raisonnable d'envisager de créer un

fichier de comptes par station quand le réseau regroupe quelques centaines de machines avec plus de 500 utilisateurs. La gestion de compte doit être centralisée et unique. De même l'accès aux stations et aux partitions sur disque doit être banalisé.

Un constructeur, *Sun*, a conçu un mécanisme d'administration centralisée sous la forme d'une relation client-serveur entre les stations d'un même réseau. Le nom de ce service est NIS[1] ; ce service permet de centraliser les informations administratives nécessaires à chaque utilisateur : ceci permet à ce dernier de se connecter sur n'importe quelle machine du réseau. Les stations sont alors banalisées.

Pour que cet utilisateur puisse travailler, il lui faut accéder à son répertoire : c'est l'utilisation du service NFS[2] qui permet l'accès à la partition disque quel que soit le lieu physique où celle-ci se trouve. La figure 6 schématise l'utilisation de comptes, de stations et de partitions utilisateurs banalisées grâce aux deux services NIS et NFS.

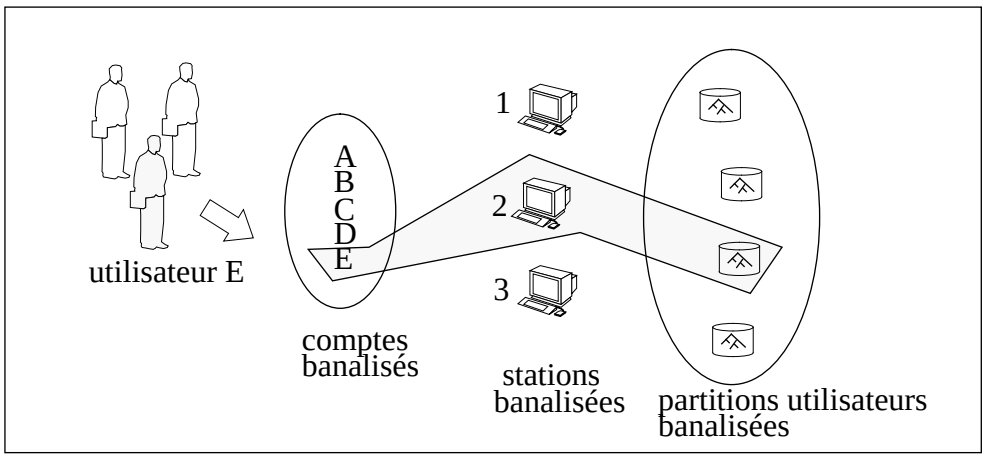


FIGURE 6. L'environnement utilisateur sur un ensemble de machines.

Le service NFS permet d'accéder à une partition distante comme si elle était locale à la machine. L'attachement de la partition distante à la partition locale est réalisé par une opération appelée montage. Ces opérations de montage sont décrites dans un fichier qui est lu au démarrage du système de la machine, les montages sont alors effectués automatiquement pour toute la durée de vie de la session. La figure 7 montre un exemple de montage NFS d'un client sur un serveur. La partition **/equipe/durand** se trouve physiquement sur un disque attaché à la station serveur **hugo**, ce serveur annonce qu'il exporte cette partition. Le client va demander le montage de

1 «Network Information Service». Ce service s'appelait initialement «pages jaunes» («yellow pages»), mais il a été décidé que cette dénomination était réservée aux Télécommunications.

2 «Network File System», également développé par Sun.

hugo:/equipe/durand sur le répertoire **/nfs/equipe/durand**. Ainsi, le fichier **toto** appartenant à la partition **/equipe/durand** est accessible de la station cliente sous la référence **/nfs/equipe/durand/toto.**

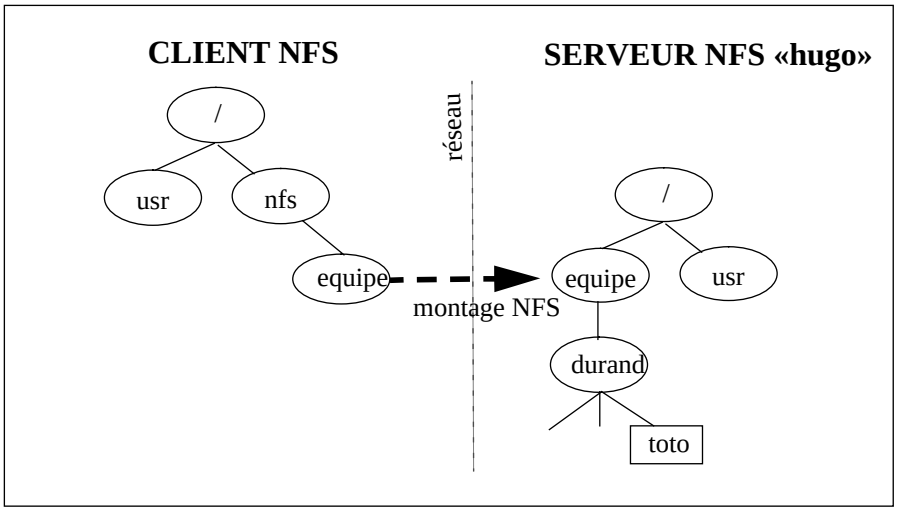


FIGURE 7. Un exemple de montage NFS.

Les deux services NIS et plus particulièrement NFS sont des protocoles qui produisent une forte activité sur le réseau. Il est donc intéressant de les étudier dans le détail afin de construire un réseau dont l'architecture permette à ces services de fonctionner au mieux.

5.1. NIS et les problèmes provoqués par son implantation

Ce mécanisme, développé par *Sun* et repris par la majorité des autres constructeurs, permet de gérer une copie unique des informations sur un serveur appelé maître ; d'autres serveurs, dits esclaves, vont conserver des copies de ces informations. Les créations ou modifications d'enregistrement sont exclusivement effectuées sur le serveur maître qui les distribue ensuite à tous les serveurs esclaves.

Lorsqu'une station cliente démarre et si elle a été configurée pour utiliser ce mode, elle envoie une requête sous la forme d'un message de diffusion globale[1] : cette requête est lue par toutes les autres stations car elle n'a pas de destinataire particulier. Tous les serveurs NIS, maître ou esclave indistinctement, qui reçoivent cette requête vont y répondre. Le premier serveur qui répond devient alors le serveur NIS

1 Traduction du terme anglais : *broadcast*. Pour des commodités d'écriture dans la suite du document, nous conservons le terme *broadcast* pour «message de diffusion globale».

associé à la station demandeur. Cette station reste ensuite liée à son serveur NIS durant toute la durée de vie de la session du système d'exploitation de la station ou du serveur.

Une fois le lien effectué, les demandes d'information se font ponctuellement et de façon dynamique par la station cliente à son serveur. Par exemple, l'utilisateur **dupont** désire se connecter sur la station A, le système d'exploitation via le programme *login* vérifie que **dupont** a été préalablement enregistré, pour cela il le recherche dans le fichier local. S'il ne trouve pas l'information en local, il envoie une requête au serveur esclave sur l'entrée **dupont**, le serveur lui retourne alors l'enregistrement complet avec les champs mot de passe, répertoire, etc. Ce mécanisme est illustré figure 8.

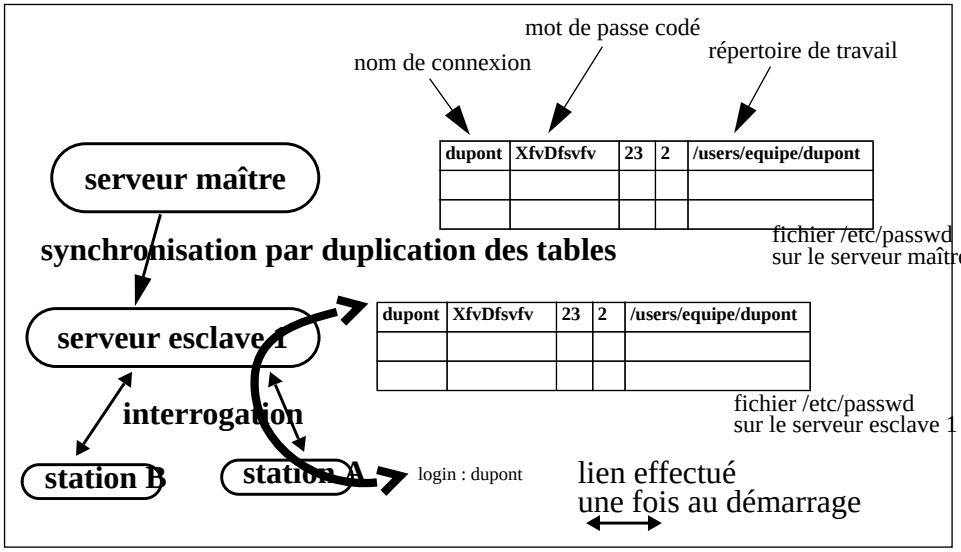


FIGURE 8. Schéma de fonctionnement de NIS.

L'administration centralisée par NIS était utilisée pour la gestion unique des deux anciens réseaux du CRIN et de l'Inria Lorraine. Chaque utilisateur ne disposait que d'un seul compte, et donc d'un seul mot de passe, pour travailler indifféremment sur n'importe quelle machine des deux réseaux. Cette gestion centralisée renforçait la sensation qu'il n'existait déjà qu'un seul réseau.

La particularité du service NIS, comme d'ailleurs d'autres services comme *rusers* ou *bootp*, est qu'une station à la recherche d'un serveur utilise le mode *broadcast*. Le *broadcast* est un paquet de données qui est destiné à l'ensemble des stations du réseau d'un même segment[1] ethernet. Chaque machine lit le paquet reçu et vérifie si elle sert ou non le service demandé ; dans l'affirmative, elle envoie son offre de ser-

vice à la station cliente demandeur. La première machine temporellement qui répond devient le serveur de cette station.

Ceci signifie que les critères de sélection sont fondés sur la rapidité d'un serveur à établir une réponse. Ces facteurs comprennent la charge de la machine à l'instant de la requête et la date de construction de la machine. En effet, chaque fois qu'une nouvelle machine est connectée sur le réseau, elle est généralement plus puissante que les autres au niveau CPU, elle a également un meilleur débit au niveau de son interface réseau. Une telle machine devient donc un très bon candidat pour faire office de serveur.

Le danger est alors que toutes les stations du réseau se lient au dernier modèle de serveur, ce qui est totalement à l'encontre d'une répartition maîtrisée du trafic réseau.

De même, un serveur qui réinitialise son système est un bon candidat à un instant donné car de très faible activité, mais ce n'est pas obligatoirement un candidat de proximité géographique dans la topologie physique du réseau.

Quand ce phénomène se généralise, on perd beaucoup de l'efficacité de la segmentation du réseau par l'intermédiaire de ponts, car les ponts filtrent les messages entre deux segments du réseau en fonction de l'adresse destination de ces messages ; les ponts laissent donc passer les *broadcasts*.

Dans un réseau complexe, les dialogues entre les différentes stations deviennent alors difficilement maîtrisables et il n'y a pas de possibilité d'administration du flux réseau.

5.2. NFS et les problèmes liés à son utilisation

Le principal inconvénient du montage de partition est la forte dépendance entre la station cliente et son serveur NFS. Nous expliquons ci-après les conséquences de cette dépendance.

Le service NFS a un fonctionnement «sans mémoire des événements»[1]. Lorsqu'une station cliente a établi un montage avec un serveur, elle lui envoie une requête *RPC*[2]. Deux cas se présentent alors :

1 La notion de segment indique que les machines sont connectés sur une même portion de câble physique et que les boitiers électroniques d'interconnexion éventuellement nécessaires sont entièrement passifs au niveau du protocole ethernet.

1 Le serveur ne gère pas l'état des requêtes déjà effectuées.

2 RPC est l'abréviation de «Remote Procedure Call» ou «appel de procédure à distance».

- soit le serveur est actif et il répond donc à la requête de la station cliente,
- soit le serveur ne répond pas. Malheureusement, la station cliente ne peut pas faire la distinction entre un serveur écroulé en raison d'une très forte charge mais encore actif, et un serveur arrêté sur une erreur. Tant que le serveur ne répond pas, la station cliente lui retransmet régulièrement la requête qui n'a pas abouti.

  L'utilisateur est prévenu du problème par l'affichage dans sa fenêtre d'un message du type «NFS server *nom_du_serveur* not responding».

  Cet état perturbe l'environnement de travail de l'utilisateur et le bloque généralement jusqu'à la réinitialisation de la station cliente, afin que celle-ci se trouve un autre serveur NFS.

Initialement, les partitions NFS étaient montées de façon statique.

Les montages statiques

Le montage statique de toutes les partitions sur chacune des machines entraîne une occupation des tables du système. Quand on sait que l'utilisateur ne travaille qu'avec une moyenne de cinq partitions alors que plus d'une centaine de partitions sont montées, on se rend compte de l'occupation inutile de la mémoire de la station par les tables de montage.

Pour limiter les encombrements mémoire liés aux montages statiques d'une part et ne pas risquer de bloquer sa station en demandant inutilement le montage d'une partition d'autre part, un mécanisme de montage de partition dynamique est utilisé depuis quelques années.

Les montages dynamique.

L'outil de montage dynamique, initialement développé par Sun, est fourni en standard avec le système d'exploitation *SunOs4.x* et également avec la plupart des systèmes UNIX. Le principe est le suivant : plutôt que d'effectuer le montage de toutes les partitions au démarrage de la station, le démon *automount* effectue les montages NFS à la demande, c'est-à-dire en fonction du travail de l'utilisateur.

Quand l'utilisateur se positionne sur un répertoire n'appartenant pas au système de fichier de la station, deux cas se présentent :

- la partition NFS est déjà montée sur le système, l'utilisateur travaille alors de manière transparente sur cette partition;

- la partition NFS n'est pas montée ; le système provoque alors une erreur de montage, cette erreur est déroutée et récupérée par le démon *automount* qui vérifie dans ses tables si la partition existe ou non :
  - si la partition n'existe pas, un simple message d'erreur est affiché ;
  - si la partition existe effectivement, alors une requête NFS est transmise par démon au serveur. Lorsque le montage de la partition a abouti, le démon crée un lien et l'utilisateur peut travailler sur cette partition.

  Lorsque la partition n'est plus accédée au bout d'un temps fini paramétré dans le système, généralement de 5 minutes, une opération de démontage est alors exécutée par le démon *automount*.

Cette procédure fonctionne correctement lorsque tous les serveurs sont dans un état sain. Une station cliente dépend très fortement de ces serveurs de partitions, aussi lorsque l'un d'entre eux s'écroule ou s'arrête sur une erreur, la station se bloque également. Seul le rechargement du système de la station permet de rétablir un bon fonctionnement.

L'outil *automount* de montage dynamique apporte une facilité de gestion pour un site possédant un grand nombre de partitions NFS et ce nombre, dans notre cas, ne cesse de croître. Il apporte un irremplaçable confort d'utilisation pour les utilisateurs, car le montage statique de toutes les partitions NFS sur chaque machine provoquerait des blocages quasiment permanents des stations dûs au grand nombre de serveur. De plus, La modification dynamique et centralisée des tables de montage permet une très bonne cohérence des montages NFS sur toutes les stations. En effet la table de montage des partitions est commune à toutes les stations et diffusée par NIS. Ainsi l'ajout ou le retrait d'une partition se résume à une opération d'écriture dans la table centralisée des montages.

Il faut cependant noter que cet outil provoque quelques problèmes quand on en fait une utilisation intensive, plus particulièrement lors du blocage d'une station serveur. Or le nombre important de partitions NFS disponibles sur le site fait qu'une station est dépendante d'un grand nombre de serveurs et est donc plus apte à se retrouver bloquée.

Conclusion

Dans ce chapitre, nous avons étudié les problèmes qui existaient dans les deux anciens réseaux. Nous avons montré que ces réseaux, bien qu'utilisant une technologie vieillissante et une faible structure au niveau de la topologie, avaient un mode de gestion collective bien structuré et utilisaient déjà des services permettant une

gestion efficace des comptes utilisateurs. En particulier, l'utilisation des deux services NFS et de NIS n'a nullement été remise en cause et leur suppression aurait été considérée comme un retour en arrière.

Toutefois, ces services ont entraîné de nouvelles causes de pannes ou de blocages. C'est pourquoi lors de la définition de l'architecture du nouveau réseau, nous avons essayé de supprimer les problèmes engendrés. Ces services ont eu une influence sur le nouveau réseau tant au niveau de l'architecture, pour régler le problème des *broadcasts*, qu'au niveau des services, par le remplacement de la fonction *automount*.

CHAPITRE 2

Le changement de numérotation IP

Le réseau Loria résulte de la fusion logique et physique de deux réseaux distincts, chacun associé à un centre de recherche. Dans ce chapitre, nous présentons la première action qui a été réalisée en vue de la fusion en un seul réseau : le changement d'adressage IP[1].

Avant de décrire les opérations effectuées, nous présentons brièvement la structure des adresses IP des stations et la façon dont elles sont gérées.

1. Les classes de réseau

Lors de la présentation des réseaux CRIN et Inria Lorraine, nous avons précisé que la connexion au réseau international Internet implique l'utilisation, pour chaque machine, d'une adresse IP unique. L'unicité des l'adresses IP ne peut être garantie que par un organisme mondial central. C'est le NIC[2] qui s'occupe de cette opération, il existe un NIC central aux Etats-Unis et une ou plusieurs délégations dans chaque pays ou continent.

En pratique, le NIC attribue à un site une plage de numéros consécutifs appelée classe. Une classe détermine un nombre de machines qui vont pouvoir être reliées sur un même réseau. Il existe trois classes de réseaux[3] : la classe A permet de définir 254 x 254 x 254 adresses différentes, soit plus 16 millions, la classe B autorise 254 x 254 adresses, soit environ 64 000 machines, et la classe C seulement 254.

L'adresse IP d'une machine est toujours codée sur 4 octets, elle est composée d'un numéro de réseau suivi d'un numéro de machine sur le réseau. Le numéro de réseau attribué est codé sur 1, 2 ou 3 octets en fonction de la classe, et les octets suivants définissent l'adresse de la machine au sein du réseau ; celle-ci est laissée au libre choix de l'administrateur. Par exemple, dans le cas d'un réseau de classe C, le numéro de réseau attribué par le NIC est codé sur 3 octets et l'adresse de la machine

1 IP signifie protocole de l'Internet («Internet Protocol»).

2 «Network Information Center» ou centre d'information réseau, qui est un département de la DoD (département de la défense américaine).

3 Pour être totalement exact, mentionnons qu'il existe en réalité 5 classes de réseau. Nous ne parlerons pas des classes D et E qui ont une utilisation très spécifique.

sur le quatrième octet. La classe du réseau est donc fonction de la valeur du premier octet de l'adresse IP. Le tableau présenté ci-après résume cette codification.

Classe d'adresse	**premier octet**	**réseau attribué**	**nombre d'adresses possibles**
A	1 à 126	X	254*254*254
B	128 à 191	X.Y	254*254
C	192 à 223	X.Y.Z	254

Tableau 1 : Les classes de réseaux IP.

On comprendra que cette répartition sous-entend qu'il existe beaucoup de réseaux de moins de 254 machines et très peu de réseaux de plusieurs millions de machines.

Le réseau du CRIN avait l'adresse 192.33.167 et le réseau de l'Inria Lorraine le numéro 192.33.168. Ils appartenaient tous deux à la classe C, laquelle ne permet la connexion que d'au plus 254 machines. Le regroupement de ces deux réseaux et l'évolution du nouveau réseau ont incité l'organisme commun, le Loria, à faire une demande de classe B[1].

Le changement d'adressage du réseau est intervenu avant que la fusion des deux réseaux du CRIN et de l'Inria Lorraine ne soit réalisée et même avant que son architecture ne soit complètement définie. Il n'était pas techniquement possible, ni même souhaitable, que le changement d'adressage et la fusion des réseaux interviennent simultanément.

Ce changement de classe du réseau a été réalisé en plusieurs étapes et a soulevé principalement deux questions :

- comment structurer les adresses des machines sur les deux réseaux, devait-il y avoir un lien avec le futur réseau ?
- comment procéder effectivement au changement des adresses sans perturber le travail des utilisateurs ?

Les réponses apportées à ces deux questions sont discutées dans les deux sections suivantes.

1 Remarquons qu'actuellement, le NIC est beaucoup plus restrictif sur l'attribution de classe B en raison du très faible nombre de numéros de classe B restants et préfère attribuer plusieurs classes C consécutives. La pénurie de classes B étant cependant inéluctable en raison du succès de l'Internet, un autre type d'adressage est actuellement à l'étude : IP Version 6 (la version actuelle est la version 4).

2. La structuration de l'adressage

Auparavant, lors de l'arrivée d'une nouvelle station, l'affection de son numéro IP était faite en prenant tout simplement le premier numéro libre dans la classe de réseau auquel elle appartenait. Il n'y avait aucune logique de regroupement et les serveurs n'avaient aucune affectation particulière. La structuration existait bien au niveau des personnes mais l'ensemble des machines était vu comme un conglomérat structuré suivant la géographie des locaux. Le réseau avait atteint une taille trop importante pour continuer à être gérer sans structuration.

L'utilisation d'un adressage de classe B nous a donné la possibilité de gérer le réseau comme un ensemble de sous-réseaux ; chaque sous-réseau correspondant à un groupe de machines, lui-même associé à une entité logique de travail, c'est-à-dire un ensemble de machines sur lequel travaille un groupe de personnes d'une même équipe ou dans le cadre d'un même projet.

La première opération a été d'identifier le rattachement d'une machine à une équipe et l'identification des moyens communs[1]. Le groupe de machines associé à une équipe constitue ainsi une grappe à laquelle on affecte un nom.

Suivant les équipes, le nombre de stations varie de cinq stations pour les plus petites à une trentaine pour les plus importantes. Deux possibilités se sont alors offertes : soit affecter un numéro de sous-réseau différent pour chaque équipe, soit regrouper les plus petites équipes pour en faire des groupes de taille homogène et leur affecter un numéro de sous-réseau. C'est cette deuxième option qui a été retenue, l'objectif était de gérer des réseaux de taille similaire dans un souci d'efficacité.

Bien que totalement indépendant de l'adressage IP, le nombre de stations dans un sous-réseau leur permettait d'être connectées sur un même segment ethernet. De plus, comme chaque station de travail était livrée en standard en 1992 avec une interface ethernet et qu'aucune autre technologie de réseau local pour TCP/IP n'émergeait ni n'avait un coût aussi bas que ethernet[2], le choix d'ethernet pour effectuer la connexion immédiate des stations sur un même sous-réseau s'imposait.

Les autres types d'attachement comme FDDI étant coûteux mais plus rapides, ils ont été réservés à l'arête centrale du réseau.

La figure 9 représente l'évolution des adresses IP du réseau : deux réseaux de classe

1 Le service des Moyens Informatiques a un budget propre pour l'acquisition des moyens communs, c'est-à-dire les serveurs et l'infrastructure du réseau ; les stations de travail restent habituellement à la charge de chaque équipe.

2 Cela est encore vrai aujourd'hui, une station est toujours livrée avec une interface ethernet. Toute autre extension nécessite l'acquisition d'une carte de communication et occasionne donc un surcoût.

C ont été fusionnés en un réseau de classe B, lequel a été découpé en plusieurs sous-réseaux.

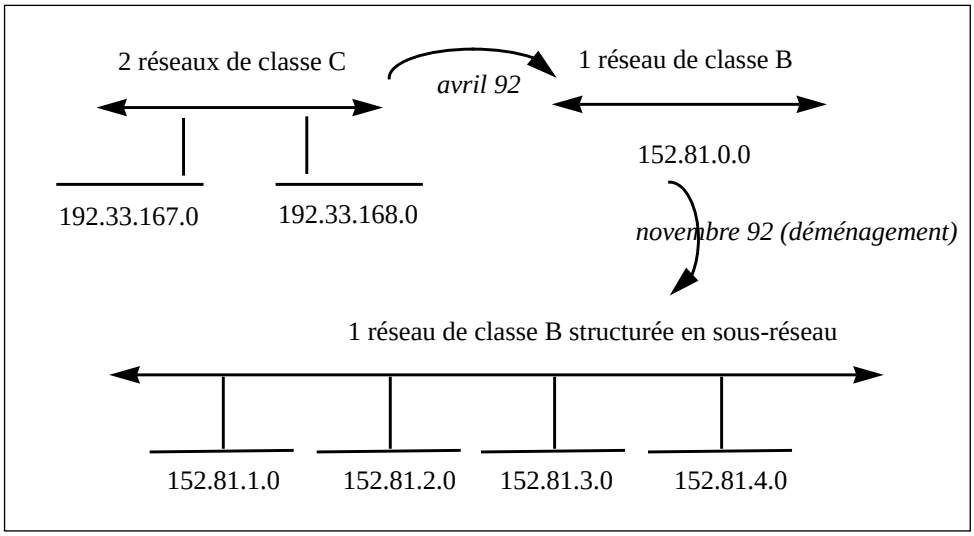


FIGURE 9. L'évolution de l'adressage.

Une machine a une adresse IP qui se décompose de la manière suivante :

- 2 octets codant le réseau de classe B : 152.81
- 1 octet représentant le numéro des sous-réseaux que nous avons définis
- 1 octet stockant le numéro de la machine.

Cette machine a également besoin de deux autres paramètres : une adresse de diffusion globale appelé *broadcast* et un masque.

Le masque permet d'indiquer à la machine combien de bits sont affectés à l'adresse du sous-réseau et donc combien de bits sont réservés au numéro de la machine. Il faut noter que la frontière entre le réseau et la machine peut se faire sur n'importe quel bit mais il est préférable, pour une question de lisibilité, d'utiliser une frontière d'octet. C'est le masque qui permet le découpage d'une classe B en sous-réseau.

Le *broadcast* est un message dont l'adresse représente l'ensemble des adresses IP d'un réseau. Ceci permet à une station d'envoyer un paquet à toutes les stations de son réseau. Ce mécanisme peut être utilisé lorsque la station émettrice ne connaît pas l'adresse destination ou lorsqu'il y a plusieurs destinataires concernés par un

même message. La figure 10 résume cette représentation.

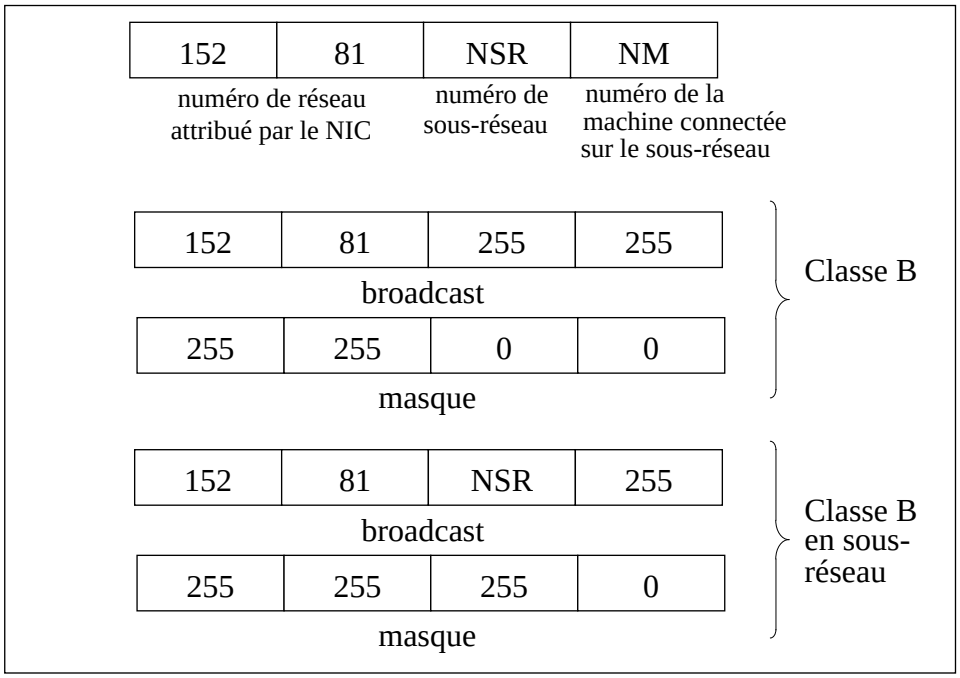


FIGURE 10. La représentation d'une adresse IP d'une machine du nouveau réseau.

Le principe d'accès au media de communication ethernet est non déterministe et lorsque le nombre de stations augmente, il se produit un phénomène d'écroulement provoqué par les collisions de paquets de données (voir page 14). Ce nombre de stations dépend bien sûr de leur activité de communication. Nous avons fixé une moyenne de 30 stations avec un maximum de 50 stations par sous-réseau afin de limiter les risques d'écroulement. Ce sont des chiffres courants dans des réseaux de type ethernet.

Une fois les numéros de sous-réseaux affectés, il restait à affecter l'attribution du numéro de la machine dans le sous-réseau. Plutôt que d'attribuer un numéro séquentiellement, nous avons défini des affectations de plage de numéro en corrélation avec la fonction des appareils électroniques. La structuration fixe une règle d'attribution des adresses IP et facilite les modifications collectives faites par les ingénieurs systèmes. Le tableau suivant

indique cette répartition :

152.81.x.1-9	routeurs, passerelles
152.81.x.10-49	serveurs
152.81.x.50-99	concentrateurs
152.81.x.100-199	stations unix
152.81.x.200-249	autres (TX-PC-MAC...)
152.81.x.250-254	imprimantes réseaux

Tableau 2 : Répartition de l'adressage dans un sous-réseau.

Ces choix sont libres, la seule numérotation recommandée est l'utilisation du numéro 1 comme port de sortie du réseau (le numéro 0 n'étant pas autorisé).

L'étape suivante a été de préparer la renumérotation de toutes les machines des deux sites CRIN et Inria Lorraine afin que le changement effectif puisse se réaliser en douceur pour les utilisateurs. Nous avons construit une table de correspondance comportant l'ancienne et la nouvelle adresse IP de chaque machine. Le nom «court» de chaque machine est resté identique, en revanche le nom qualifié tel qu'il est défini dans le DNS, c'est-à-dire le nom court suivi du nom de domaine, était quant à lui modifié.

3. L'opération de renumérotation des adresses IP du réseau.

Le déroulement de la numérotation des adresses IP a dû être soigneusement préparé afin de perturber le moins possible le travail des utilisateurs. Cette opération devait être complètement planifiée et ne pas dépasser 24 heures.

Il s'est avéré indispensable d'automatiser au maximum cette opération car toute modification manuelle sur l'ensemble du parc aurait immédiatement entraîné un temps cumulé d'indisponibilité très important et incompressible. Il était donc hors de question de se connecter sur chaque machine pour en changer son adresse IP manuellement.

La renumérotation demandait de changer, pour chaque machine, son adresse IP, son nom de domaine ainsi que l'adresse IP de la passerelle de sortie. Cette modification consistait à remplacer des chaînes de caractères dans les fichiers systèmes de la station. La station concernée devait bien évidemment être active pendant ce changement, elle était donc toujours intégrée au réseau et il importait de savoir quelle influence cette modification allait entraîner sur le fonctionnement global du sys-

tème.

L'utilisation des services d'administration du réseau comme NIS ou NFS rendait l'opération délicate : dans une telle architecture, chaque station-cliente établit un dialogue avec une station-serveur. Chaque station-cliente est donc dépendante dans son fonctionnement d'un serveur NIS, d'un ou plusieurs serveurs NFS et d'un serveur DNS local pour la résolution des noms extérieurs au réseau. Dans la majorité des cas, l'arrêt intempestif d'un serveur provoque le blocage de ses stations clientes et donc l'impossibilité d'une connexion à distance, mais locale au réseau, pour renuméroter à son tour ce serveur.

Une station bloquée, parce que son serveur vient de se réinitialiser suite à son changement d'adresse IP, signifie que cette station va, au bout d'un temps fini de l'ordre d'une dizaine de minutes, chercher un autre serveur sur le réseau auquel elle appartient toujours. Si tous les serveurs d'un même réseau changent d'adresse IP, et donc de réseau, les stations de ce réseau ne vont plus trouver de serveur et rester définitivement bloquées. Or, il n'est plus possible de travailler à distance sur une station bloquée pour lui changer à son tour son adresse IP.

En aucun cas, il ne fallait donc bloquer une station. De plus chaque station renumérotée devait pouvoir être réinitialisée à distance et elle devait disposer de tous les éléments lui permettant de trouver un nouveau serveur dans son nouvel environnement.

Toutes les dépendances impliquaient un blocage et une perte de contrôle à distance des stations. La liste de ces dépendances a été établie afin de les supprimer au maximum et ainsi de conserver le contrôle sur chaque station jusqu'au changement final ; le changement final étant l'activation d'un serveur NIS du nouveau réseau et le rechargement à distance de tous les systèmes d'exploitation.

La figure 11 montre un exemple de dépendances liant des stations-clientes à des sta-

tions-serveurs.

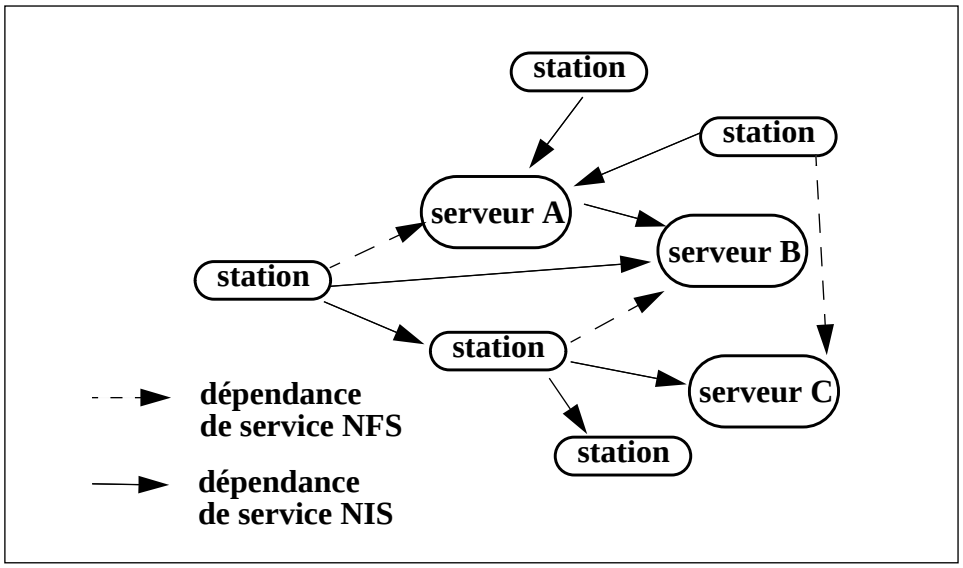


FIGURE 11. Les dépendances entre les stations-clients et les stations-serveurs.

Les opérations ont donc été soigneusement séquencées, chaque modification devait être non bloquante pour la suivante jusqu'au rechargement du système de chaque station.

Pour le service NIS, la seule solution était de conserver des serveurs NIS en fonctionnement mais de réduire leur nombre au minimum, en fait il fallait conserver un serveur actif pour chacun des deux réseaux : crin.fr et inria-lorraine.fr. La veille de l'opération, les autres serveurs NIS ont été arrêtés. Les stations liées aux serveurs dont les services ont été arrêtés, se sont alors bloquées, puis au bout d'une dizaine de minutes ont émis une requête de liaison sur un autre serveur actif. A terme, toutes les stations du réseau crin.fr étaient reliées à un seul serveur et toutes les stations du deuxième réseau inria-lorraine.fr étaient reliées à un autre serveur.

En ce qui concerne les services NFS, les utilisateurs ont été avertis de terminer toute session en cours. La seule session en cours autorisée était sur la station servant de pilote à l'opération, les programmes étaient sur un disque local à cette station.

Pour chaque type de système d'exploitation, il a été nécessaire de dresser la liste de tous les fichiers devant subir une modification ; en effet les noms des fichiers systèmes comportant des informations concernant le nom ou l'adresse IP de la station ne sont pas standardisés. De plus, chaque constructeur utilise de plus en plus des outils spécifiques (par exemple *sam* pour les systèmes *HP/UX*) pour configurer le sys-

tème et lorsque les modifications sont faites de manière directe dans les fichiers, il existe un risque d'oublier des fichiers de dépendances prévus par le constructeur. Le résultat donne alors un système non cohérent.

Une fois tous ces fichiers identifiés, nous avons préparé puis réalisé des scripts permettant la modification de l'adresse IP et des noms de chaque machine, chaque script était dépendant du système d'exploitation de la machine destination. Un exemple de ces scripts se trouve dans l'annexe A.

Le nouveau réseau loria.fr devait être connu et identifié dans le monde entier pour que les connexions avec l'extérieur et l'acheminement du courrier électronique puissent fonctionner. Ceci a impliqué une annonce préalable du réseau à un centre gérant le DNS, ainsi qu'une annonce aux organismes gérant le routage pour que les routeurs puissent trouver le chemin permettant d'atteindre le nouveau réseau.

La modification des adresses IP des stations a eu lieu simultanément avec le changement du nom de domaine. Il était cependant nécessaire de conserver un recouvrement avec les anciens noms de domaine crin.fr et inria-lorraine.fr et de modifier les routages[1].

Ceci nous a conduit à établir une planification des modifications à effectuer afin de gérer le changement des adresses IP des stations et le changement du nom de domaine.

Conclusion

Le changement de numérotation IP s'est déroulé selon le schéma prévu. Il y a eu seulement 24 heures d'interruption de fonctionnement pour les utilisateurs. Aucun courrier électronique n'a été perdu.

Les seuls incidents ont concerné quelques machines éteintes par des utilisateurs absents pour lesquelles le changement d'adresse n'a donc pas pu se faire de manière automatique.

Lors de mon arrivée dans l'équipe des Moyens Informatiques en 1991, le numéro de classe B du nouveau réseau avait déjà été attribué par le NIC, mais l'opération de renumérotation n'avait pas été planifiée. J'ai pris la responsabilité de diriger la réalisation de cette opération car elle représentait la première étape de la restructuration du réseau.

1 Les serveurs DNS possèdent un mécanisme de cache. La durée de validité de ce cache peut atteindre 3 jours. Avant de mettre en service la nouvelle adresse, il est nécessaire de modifier la durée de validité des informations du cache pour réduire une très petite valeur (1 heure).

Tous les ingénieurs et techniciens ont été mis à contribution pour effectuer les changements d'adresse des matériels dont les modifications ne pouvaient pas être faites à distance. C'est, par exemple, le cas de quelques imprimantes, des Macinstoshs, des PCs et des terminaux X.

CHAPITRE 3

L'architecture du nouveau réseau

Pour être efficace, la création d'un réseau doit respecter une méthodologie et doit être structurée comme le sont les protocoles de communication de données. Il est usuel de s'appuyer sur un modèle de référence, en l'occurrence le modèle abstrait OSI[1]. Le modèle OSI est un modèle architectural structuré, il se compose de sept couches numérotées de 1 à 7, dont chacune spécifie des fonctions réseaux particulières. La couche la plus basse, numérotée 1, définit l'aspect technique du réseau, c'est-à-dire le support de communication, la couche la plus haute concerne directement l'utilisateur, c'est la couche application.

L'approche que nous avons suivie pour structurer le nouveau réseau est similaire au modèle OSI : chaque couche réseau correspond à une action dans la création du réseau. Dans ce chapitre, nous présentons le modèle OSI, puis nous étudions successivement l'infrastructure du câblage et la structuration du réseau qui représentent les trois couches les plus basses du modèle.

Nous avons créé un groupe de travail de 5 personnes pour traiter plus particulièrement de l'appel d'offre du câblage et de l'étude de la structuration du réseau. Ce groupe, au sein duquel j'ai travaillé, avait pour rôle d'étudier les problèmes liés au câblage et à l'architecture du réseau et de décider du choix final.

Le chapitre suivant est consacré aux services offerts aux utilisateurs et les services systèmes qui représentent les couches les plus hautes du modèle OSI.

1. Le modèle OSI

Depuis que la station de travail existe, celle-ci est livrée avec une interface ethernet en standard et avec le support du protocole IP. L'interface ethernet permet la connexion à un réseau physique et le support du protocole IP qui est généralement intégré dans le système d'exploitation UNIX et autorise la connexion à un réseau

1 «Open System Interconnect».

logique[1]. Ethernet définit à la fois le support de communication et l'ensemble des fonctions permettant l'accès au réseau physique ; il correspond aux couches 1 et 2 du modèle OSI.

En réalité le protocole TCP/IP utilisé dans notre nouveau réseau a été défini bien antérieurement au modèle OSI, il s'inscrit cependant dans ce modèle comme d'ailleurs tous les autres protocoles de communication, le nombre de couches de communication est simplement réduit à quatre ainsi que l'illustre la figure 12.

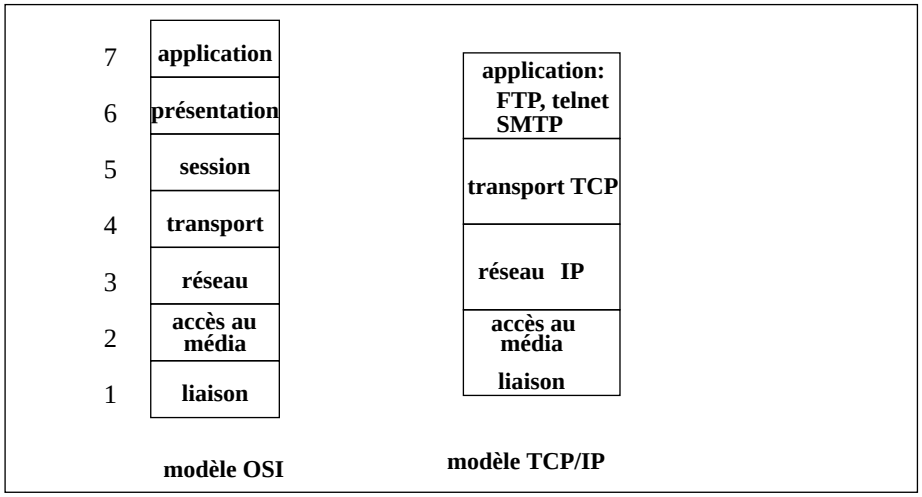


FIGURE 12. Le modèle OSI et le modèle TCP/IP.

La création d'un réseau nécessite que toutes les couches de communication telles qu'elles sont définies dans le modèle OSI soient implantées[2]. Nous les détaillons ci-après.

La couche liaison et accès au média

La couche liaison et accès au media[3] est généralement totalement ignorée des utilisateurs. Elle comprend la définition du support physique de transmission, par exemple : le câble, les interfaces (connecteurs, transmetteurs), les signaux, ainsi que l'ensemble des fonctions permettant l'accès au réseau physique.

Les protocoles de niveau 2 sont totalement dépendants de la technologie utilisée et

1 Le terme réseau logique désigne le niveau IP. Il est indépendant du réseau physique, lequel est lié à la structure physique : câble, prise, topologie physique, méthode d'accès au support.

2 Le modèle OSI est utilisé comme modèle théorique. La pile IP ne possède que quatre couches. Certaines couches sont liées entre elles comme le montre la figure 12.

3 Le terme media indique le support physique véhiculant les signaux de transmissions : paires torsadées, fibre optique, etc.

toute nouvelle technologie nécessite l'implantation d'un nouveau protocole. Ethernet est le protocole le plus utilisé actuellement dans la famille des protocoles TCP/IP, il permet la communication entre les stations de travail à la vitesse de 10 Mb/s. Il existe cependant d'autres techniques qui autorisent des vitesses de transfert plus élevées comme token-ring (4 ou 16 Mb/s), FDDI (100Mb/s) ou bien encore plus récemment ATM[1] (52 Mb/s, 155 Mb/s, 622 Mb/s,...).

La couche liaison est généralement transparente pour l'administrateur car elle ne nécessite aucun paramètrage, mais il est néanmoins nécessaire d'avoir une très bonne connaissance de son fonctionnement pour réaliser un réseau fonctionnel. Cette couche conditionne le choix du câblage qui est la première brique du réseau. La question qui se pose lors de la conception du réseau est la suivante : quel type de support doit-on implanter pour qu'il soit capable de véhiculer le protocole utilisé aujourd'hui en l'occurrence ethernet, et de supporter demain les nouveaux protocoles disponibles sur le marché. De plus, le câblage représente un coût important dans l'installation du réseau et il doit être capable de supporter les technologies naissantes, c'est un investissement pour le long terme.

La deuxième couche, accès au média, conditionne la topologie physique du réseau ainsi que le choix des modules électroniques qui permettent l'interconnexion physique des câbles. Nous verrons en effet que l'utilisation d'ethernet qui représente les couches 1 et 2 du modèle OSI impose certaines contraintes comme la limitation du nombre de stations sur un même câble physique. Ces contraintes obligent à segmenter l'ensemble du réseau en plusieurs sous-réseaux de plus petite taille [RUTGERS

1 «Asynchronous Transfer Mode» ou mode de transfert asynchrone. C'est un relais de transfert de cellules (de taille fixe) qui permet la transmission de différents types de services (voix, données, vidéo).

88].

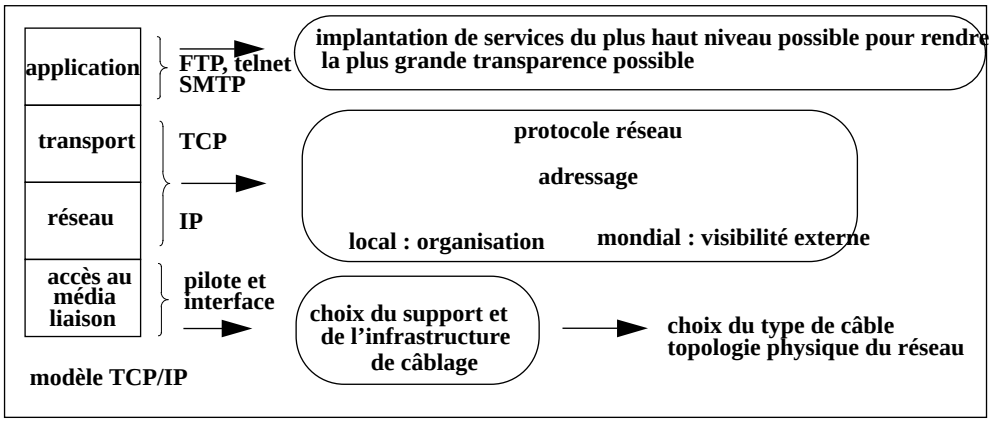


FIGURE 13. Résumé des actions à effectuer lors de l'implantation d'un réseau TCP/

La couche réseau

La couche réseau est totalement indépendante du support de transmission et de l'accès à ce support, cette couche permet l'interconnexion de réseaux informatiques qui peuvent être reliés entre eux par des supports très diversifiés. Le protocole standard de communication des machines sous UNIX est le protocole IP. Il permet l'interopérabilité, c'est-à-dire le dialogue entre divers matériels de différents constructeurs respectant les mêmes standards[1], cette couche permet également l'interconnexion avec les réseaux mondiaux.

Le protocole IP permet l'acheminement de données sous la forme de paquets et ceci à travers différents réseaux intermédiaires. La façon de structurer l'ensemble des adresses IP du réseau détermine la structure logique de celui-ci. Dans la famille des protocoles TCP/IP, chaque noeud possède une adresse IP unique[2] et cette adresse est utilisée pour acheminer les informations à leur destinataire.

L'ensemble des réseaux IP dans le monde, en dehors cependant des réseaux IP privés, forme un et un seul réseau qui relie plus d'un million de noeuds ; ce gigantesque réseau virtuel s'appelle Internet. L'interconnexion des réseaux est rendue

1 Ceci demande généralement d'être vérifié, spécialement pour les nouveaux matériels qui implantent de nouveaux standards. Un salon mondial, Interop, leur est dédié plusieurs fois par an.

2 En réalité, une machine peut posséder plusieurs interfaces et donc une adresse IP pour chaque interface.

possible par la présence de routeurs. Les routeurs sont des machines qui contiennent des tables de routage permettant à un paquet de données de prendre le meilleur chemin pour arriver à son destinataire. Les routeurs s'échangent les informations grâce à des protocoles de routage permettant l'échange dynamique de tables. Ces protocoles sont des fonctionnalités supplémentaires de la couche 3 du modèle OSI.

Le choix de la structuration du réseau local, c'est-à-dire du découpage en segments, peut se réaliser à deux niveaux suivant les besoins, soit au niveau 2 : ethernet, donc à un niveau physique par l'utilisation d'un pont, soit au niveau 3 : IP, et donc à un niveau logique par l'utilisation d'un routeur.

La couche transport

La couche transport (TCP[1]) assure que les données échangées sont délivrées de manière fiable. Elle est également responsable de l'aiguillage des paquets reçus vers la bonne application.

Nous ne présentons pas cette couche transport car un administrateur réseau n'a pas à y intervenir. La modification de paramètres de ce protocole se fait seulement dans quelques cas précis comme pour les réseaux haut débit [PARTRIDGE 94].

La couche application

La dernière couche du modèle OSI correspond aux applications. C'est la plus diversifiée car à chaque application correspond un dialogue de communication qui lui est propre. C'est cette couche qui offre les services à l'utilisateur et nous lui consacrons le chapitre suivant.

Revenons à présent sur la couche la plus basse du modèle OSI, la couche média, et présentons le résultat de notre étude.

2. Etude de l'infrastructure du câblage

Rappelons que les types de câblage existants sur les deux sites n'avaient pas une architecture identique :

- le bâtiment du CRIN était câblé en câble coaxial ethernet avec le standard Ethernet d'origine en 10 base 5 («thick cable») ; ce câble passait géographiquement de chaque coté des bureaux (voir figure 1 à la page 12) ;

1 «Transmission Control Protocol» ou protocole de contrôle de communication.

- les stations de travail du bâtiment de l'Inria Lorraine étaient connectées par l'intermédiaire de répéteurs multi-ports : un «drop cable» relie en étoile chaque station à un répéteur multi-ports (voir figure 3 à la page 16). Chaque répéteur multi-ports est capable d'accepter en entrée 16 stations.

Pour le nouveau bâtiment, il n'était pas question de reprendre un câblage du type de celui précédemment utilisé pour le bâtiment du CRIN, principalement pour les raisons suivantes[1] :

- la connexion des stations en bus : une machine peut alors polluer l'ensemble des stations se trouvant sur le même câble physique ;
- les contraintes techniques directement liées à la technologie : par exemple, il faut respecter une distance minimale entre deux transmetteurs, les prises vampires grâce auxquelles les stations sont connectées au réseau peuvent parfois engendrer des problèmes électriques, ...

Le principal avantage du câblage du bâtiment de l'Inria Lorraine était la suppression du câble central et donc des problèmes induits par celui-ci. Cependant, les problèmes comme la limitation de la longueur du «drop cable» subsistaient ainsi que la difficulté de manipulation de ce câble en raison de son diamètre relativement important. Il n'était alors pas possible d'étendre cette méthode de câblage au nouveau bâtiment en raison des difficultés de chaînage, de la limitation de la longueur des câbles et du coût très élevé des câbles AUI pour des distances supérieures à 2 mètres. En fait, ce type de réseau convient bien, seulement, pour câbler une pièce ou de très petits locaux.

Ni le réseau du CRIN, ni le réseau de l'Inria Lorraine n'ont été précâblés, c'est-à-dire que les câbles ont été tirés après la construction des bâtiments et au fur et à mesure des besoins. Cette façon de procéder est coûteuse en temps et engendre des erreurs lors de la manipulation des câbles.

Pour la tranche B du nouveau bâtiment, il a été décidé d'effectuer un précâblage. Une opération de précâblage doit respecter quelques principes et en particulier doit pouvoir prendre en compte les futures évolutions des technologies réseaux. Le câblage doit :

- être surdimensionné pour ne pas faire d'ajout de nouvelles lignes ou prises ;
- permettre, dans la mesure du possible, de supporter les nouveaux protocoles en cours de définition ou de standardisation.

1 Les problèmes liés au câblage des bâtiments ont été présentés section 2. à la page 11.

3. Le précâblage

Le nouveau bâtiment (tranche B) a été construit dans le prolongement du premier bâtiment (tranche A) accueillant l'Inria Lorraine. Il comporte trois niveaux représentant 4700 m^2, découpés en 160 bureaux ou salles de travail. Tous les bureaux, les salles, ainsi que les couloirs ont été équipés, au moment de la construction, de caniveaux de sol centraux intégrés dans l'épaisseur des chapes. L'ensemble de ces caniveaux forment un chemin de câble et relient les bureaux aux salles serveurs.

Ces caniveaux sont réservés au courant faible (téléphone et informatique) et leur localisation au sol évite la proximité d'appareil générateur de parasites comme les néons. Les caniveaux sont métalliques, ceux des bureaux font 200 mm de large par 60 mm de hauteur et ceux des couloirs 380 mm par 60 mm. Le bâtiment comporte 3 étages avec à chaque étage 4 salles serveurs ou local de sous-répartition (LSR), sauf en ce qui concerne le rez-de-chaussée qui ne comporte que deux salles serveurs. Les salles serveurs sont toutes équipées de plancher technique et sont reliées verticalement par des fourreaux.

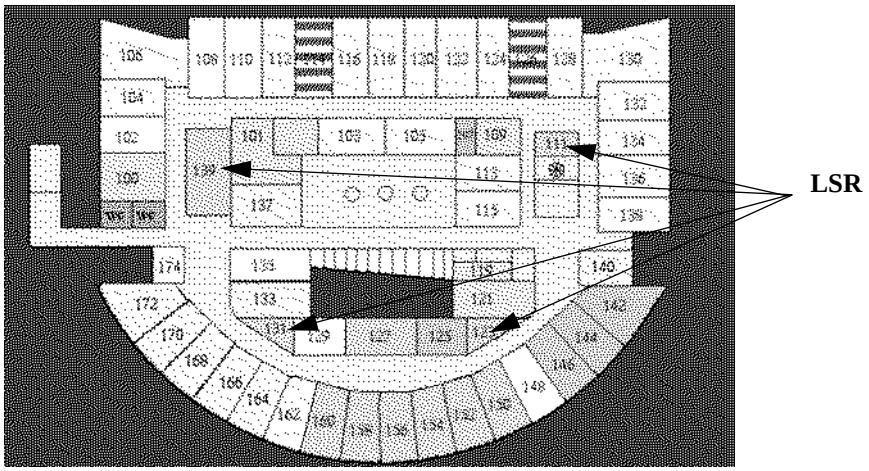


FIGURE 14. Le premier étage de la tranche B du bâtiment Loria.

Les chemins de câble ont été intégrés dans le cahier des charges du bâtiment ; en revanche, le précâblage a fait l'objet d'un appel d'offre séparé.

Dans le cahier des charges du précâblage, il était demandé :

- le raccordement des salles serveurs entre elles par fibre optique,
- l'installation de 3 prises par bureaux, salles de réunion et de conférence,
- l'installation de 15 prises dans chaque salle serveur.

Les prises terminales devaient permettre le raccordement d'un poste informatique sur un réseau ethernet ou sur un réseau turbonet pour les Macintosh, et autoriser également le passage de la vidéo.

Initialement, dans les spécifications d'ethernet telles qu'elles ont été publiées en 1980 par un consortium multi-vendeurs créé par Dec, Intel et Xerox, le seul support physique était le câble jaune («thick cable»). En 1985, le comité IEEE a adopté la technologie ethernet. Ce standard IEEE802.3 a évolué en fonction des possibilités technologiques et définit aujourd'hui plusieurs supports physiques. Les caractéristiques physiques des câbles définis par cette norme sont présentées dans le tableau ci-après.

Tableau 3 : Caractéristiques physiques de IEEE 802.3

dénomination	10 base 5	10 base 2	1 base 5	10 base T	10 broad 36	10 base FL
vitesse Mb/s	10	10	1	10	10	10
méthode de signal utilisée	bande de base	bande de base	bande de base	bande de base	large bande	
taille maximale du segment	500	185 m	250 m	100 m		2000 m
média	coaxial épais 50 ohms	coaxial fin 50 ohms	paire torsadée non blindée de catégorie 3	paire torsadée non blindée	coaxial 75 ohms	fibre optique
topologie	bus	bus	étoile	étoile	bus	point à point

Nous ne souhaitions pas utiliser une structure de réseau en bus, pour les raisons déjà évoquées page 11. Nous avons donc choisi la technologie «10 base T» qui est adaptée à nos besoins et qui a une topologie physique en étoile.

L'électronique et le câble respectant les spécifications de la technologie «10 base T» permettent de transmettre sur 100 mètres des trames ethernet à 10 Mb/s sur de la paire torsadée standard de catégorie 3. Initialement la technologie «10 base T» a été développée pour utiliser le câblage téléphonique existant dans les bâtiments.

La topologie physique du réseau étant en étoile, il était nécessaire de relier les stations des bureaux à un ou plusieurs panneaux de brassage. Deux solutions se sont présentées : soit relier toutes les stations directement à une salle serveur centrale, soit relier ces stations par l'intermédiaire de plusieurs sous-réseaux de répartition.

La figure 15 illustre ces deux options.

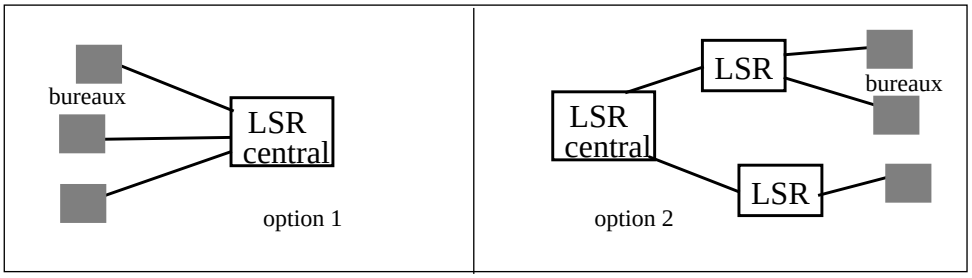


FIGURE 15. La structure du câblage.

Très rapidement, le choix d'un seul et unique panneau de répartition centralisé est apparu comme la solution la plus simple et la plus efficace à gérer. En effet, dans ce cas, il n'y a qu'une seule source pour chaque arrivée de station ; les prises peuvent alors être facilement identifiées par la concaténation du numéro de bureau et d'un numéro de rang de la prise dans le bureau. Ceci évite une gestion complexe des connexions. De plus, les problèmes liés à la longueur des raccordements sont de fait résolus. En effet, il n'y a pas besoin de vérification additionnelle des longueurs puisque la longueur maximale de la station la plus éloignée au local central est inférieure aux 100 mètres requis dans l'utilisation du câblage en fil de cuivre.

L'appel d'offre portait donc sur la réalisation de la «partie fixe» du câblage, c'est-à-

dire :

- le câble,
- les prises de raccordement de ce câble à chaque station,
- les prises de raccordement de ce câble dans le local de répartition, intégré dans un châssis de répartition,

comme l'illustre la figure 17.

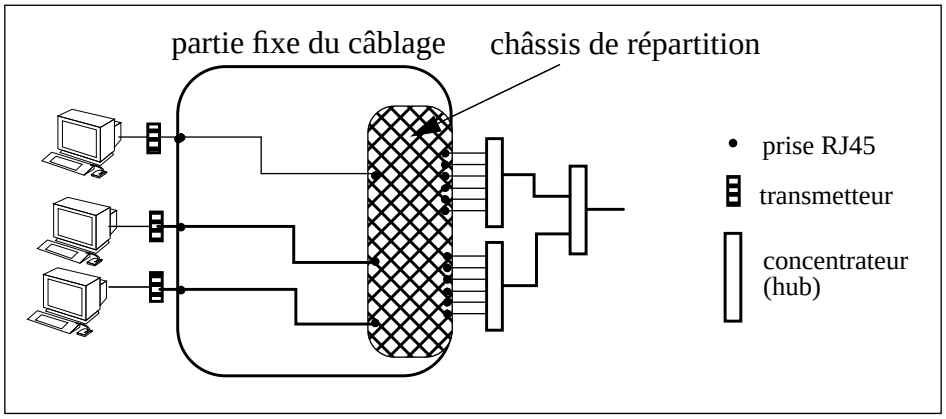


FIGURE 16. L'appel d'offre du précâblage.

Nous allons expliquer les choix qui se sont proposés pour chacun de ces trois éléments. Les critères de choix du câblage du nouveau bâtiment ont été à la fois techniques et financiers.

Les points techniques ont porté sur :

- le type de câble utilisé et sa capacité à supporter les hauts débits,
- le type de prise utilisé dans les panneaux de brassage.

Les différences économiques ont concerné :

- le coût moyen par prise,
- la durée de garantie du câblage.

La procédure de recette implique la vérification de la continuité électrique de tous les fils et la fourniture d'un cahier technique de recette comportant pour chaque câble posé dans les caniveaux, sa longueur de prise à prise.

3.1. Le câble

Différents types de câbles en paire torsadée acceptent la technologie «10 base T» de la norme IEEE 802.3. Les offres portaient sur les trois types de câble suivants : 1061 de ATT, CTD 20 de ACOME, L120 de COREL. Ces vocables représentent des câbles ayant des caractéristiques physiques différentes comme la structuration des fils de cuivre (par exemple le pas de torsade), le diamètre des fils de cuivre, l'impédance du câble ou bien encore sur l'existence ou non d'un blindage. Le tableau ci-après permet la comparaison des caractéristiques techniques des câbles.

TABLEAU 4. Comparaison des caractéristiques des câbles.

type	blindage	impédance	diamètre de l'âme	nombre de paires
1061	non	100 ohms	0,5 mm	4
L120	écranté	120 ohms	0,6 mm	4/8/12/32/64/128
CTD20	écranté	120 ohms	0,64 mm	2 * 4

Au-delà de toutes ces caractéristiques techniques, il convient de regarder l'utilisation du câble, ses capacités futures et son positionnement dans la normalisation ou l'émergence de normalisation.

Un des aspects sur lequel il était nécessaire de trancher portait sur l'impédance. Sur ce point, il y a eu une véritable guerre commerciale. En 1992, le câble recommandé par les organismes européens est un câble ayant une impédance de 120 ohms, celui préconisé par les organismes américains a une impédance de 100 ohms. En décembre 1990, une norme américaine sur le câblage des immeubles est publiée par l'EIA[1] et la TIA[2]. Cette norme, référencée EIA/TIA-568-B, définit différents types de supports pour les câblages d'immeuble :

- la paire torsadée non blindée (UTP untwisted pair) à 100 ohms,
- la paire torsadée blindée (STP shielded twisted pair) à 150 ohms,
- les coaxiaux à 50 ohms,
- la fibre optique multimode (62,5/125 microns).

Les câbles paires torsadées non blindées, dont nous présentons une coupe figure 17,

1 «Electronic Industries Association», association américaine qui spécifie les normes de transmission électroniques.

2 «Telecommunications Industry Association».

ont été classés par l'EIA en trois catégories en fonction des débits qu'ils supportent :

- la catégorie 3 pour les débits allant jusqu'à 16Mb/s, est destinée principalement au token-ring (vitesse de 4 ou 16Mb/s),
- la catégorie 4 pour les débits allant jusqu'à 20 Mb/s,
- la catégorie 5 pour des débits allant jusqu'à 100Mb/s.

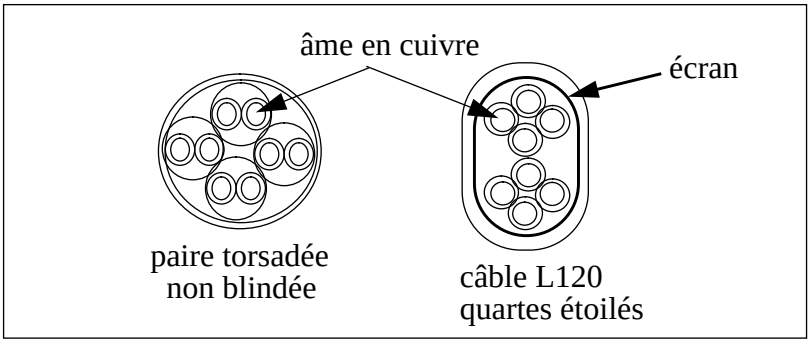


FIGURE 17. Coupe de câble en paire torsadée non blindée.

Un des problèmes est qu'il n'y avait aucune norme européenne. Les Européens sont représentés dans le comité au nom enchanteur de ISO-CEI/JTC1/SC25WG3[1] qui étudie la généralisation au plan international des normes américaines et des normes européennes. Entre les impédances 100 et 120 ohms, il y a eu une véritable guerre de chiffres en particulier sur la performance des câbles avec les hautes fréquences. Plus précisément, les tests effectués sur l'atténuation du signal révélaient une supériorité du câble L120 sur les câbles paires torsadées de catégorie 5.

Au-delà de ces chiffres, notre choix technique s'est porté sur le système de câblage *Systimax PDS*[2] qui nous garantissait la vitesse de 100Mb/s. La majorité supportait des débits maximum de 20Mb/s. Outre la garantie du débit et donc la pérennisation du câblage, ce choix était appuyé par deux facteurs non négligeables : le coût par prise le plus bas et la garantie du système de câblage pour une période de 5 ans.

Aujourd'hui ce choix est totalement validé. Depuis octobre 94, j'ai installé un serveur avec un attachement FFDI sur paire torsadée. La normalisation ANSI de FDDI sur paire torsadée, appelée FDDI TP/PMD[3], date seulement de décembre 93. Depuis juin 95, nous utilisons ce même câblage pour véhiculer de l'ATM à la vitesse de 155Mb/s. Ces deux types de technologie nécessitent un câblage paire tor-

1 Working Group 3 (câblage des locaux) du sous-comité 25 (interconnexion des appareils de traitement de l'information) du Joint Technical Committee 1 (technologie de l'information), qui fait partie de ISO et de la CEI (Commission Electrotechnique Internationale).

2 «Premise Distribution System».

3 «Twisted Pair / Physical Medium Dependant» ou paire torsadée / dépendance physique avec le media.

sadée de catégorie 5. La vitesse limite sur ce type de câble ne semble pas encore atteinte car il existe un prototype en laboratoire qui permet des débits de 622Mb/s sur des câbles de catégorie 5. Cette technologie ne sera peut-être jamais commercialisé en raison de son coût excessif actuel car elle nécessite des interfaces complexes qui mettent en oeuvre le traitement du signal et le codage à multiples niveaux, mais elle montre que les limites de vitesse de transfert ont été encore repoussées.

3.2. Les prises de raccordement des stations au câble

Toutes les sociétés qui ont répondu à notre appel d'offre, ont proposé comme raccord des équipements terminaux dans les bureaux la prise femelle RJ45. Cette prise, normalisée sous la référence ISO 8877, comporte 8 fils ; elle est représentée sur la figure 18.

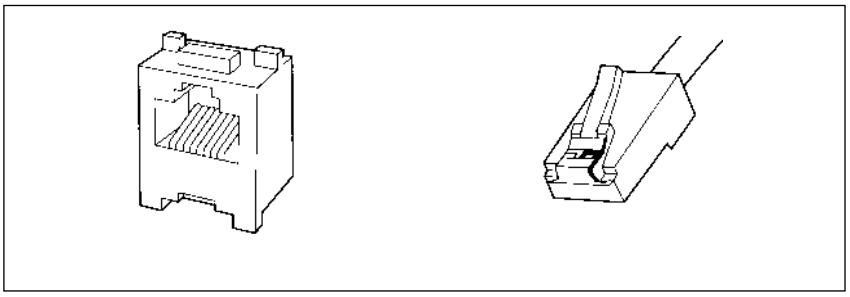


FIGURE 18. La prise RJ45 (femelle et mâle) [RES. & TEL. 94].

Une station sera donc reliée au câble via un cordon ayant une prise RJ45 mâle à son extrémité, cette prise est également représentée figure 18.

3.3. Les prises du panneau de répartition

Les panneaux de répartition sont connectés d'une part au câble reliant chaque station et d'autre part au concentrateur par autant de cordons que de stations, comme

l'illustre la figure 19.

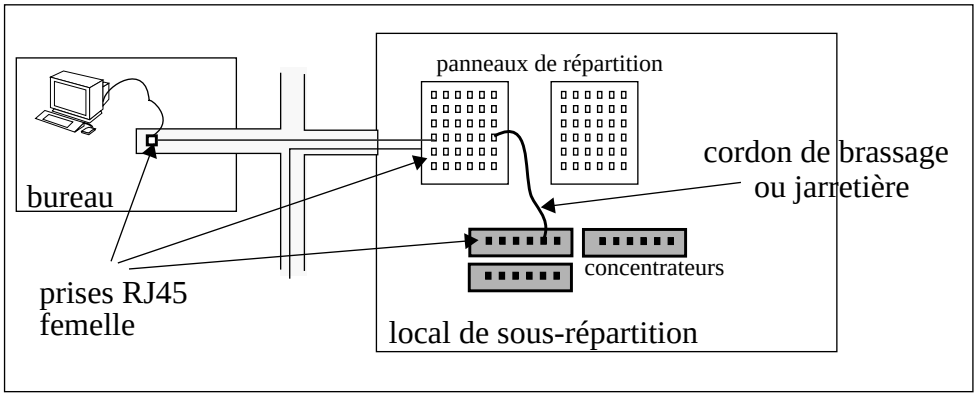


FIGURE 19. La structure du câblage

Les panneaux peuvent être équipés de différents types de prises ; elles peuvent être soit standards, dans ce cas c'est généralement la prise RJ45 qui est utilisée, soit propriétaire, la prise est alors produite par un constructeur particulier.

Le type de prise propriétaire induit plusieurs problèmes. Premièrement, le surcoût des cordons de brassages, ou jarretières, reliant une prise du panneau de brassage au concentrateur, est à prendre en compte. Par exemple, un câble de liaison Infra+ RJ45 coûte 240 F HT alors qu'un câble de même longueur équipé d'une prise RJ45 à chaque extrémité est seulement facturé 85 F HT. Cette différence devient importante lorsqu'on a plusieurs centaines de câbles à implanter. Deuxièmement, une prise propriétaire nous lie à un constructeur particulier qui fixe ses prix quasiment sans concurrence et décide seul de l'évolution de ses produits.

Le seul avantage du câblage propriétaire est de pouvoir gérer séparément les 8 fils d'un câble et de pouvoir disposer de connecteurs supportant 2, 4 ou 8 fils. Dans le cas d'ethernet 10Mb/s sur paire torsadée, il y a seulement 2 paires qui sont utilisées, soit seulement la moitié des fils disponibles. Cependant, avec le passage des hauts débits sur ce type de câble, il est spécifié par les constructeurs de ne pas passer d'autres signaux sur les fils non utilisés car cela peut entraîner des ruptures de communication [FORE 94].

Il paraissait donc assez évident de choisir des prises RJ45 pour équiper les panneaux de répartition.

Une fois l'opération de câblage réalisée, il était nécessaire d'ajouter tous les éléments permettant la jonction entre la prise AUI de la station et la prise RJ45 du câble arrivant dans le bureau[1] ainsi que les jarretières et les concentrateurs comme le montre la figure 20. Tous ces éléments représentent une partie non négligeable du coût total.

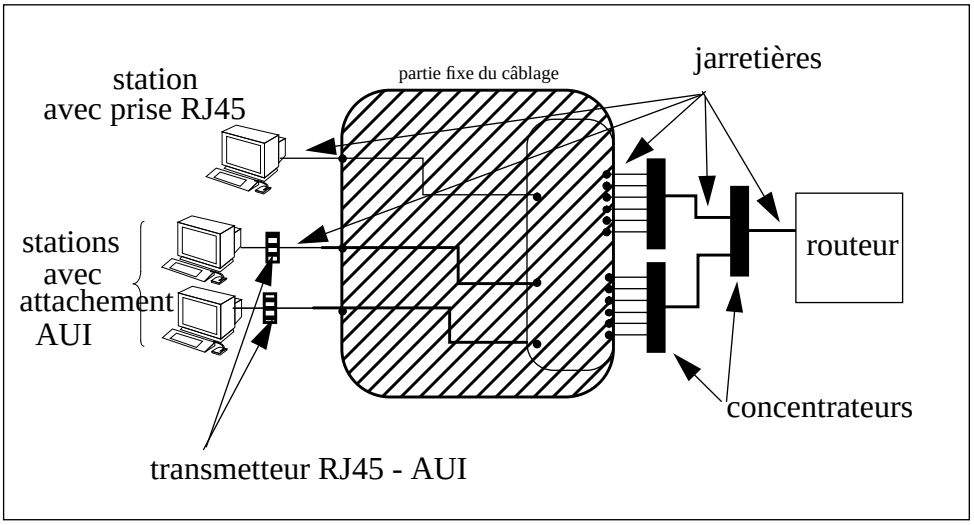


FIGURE 20. Les connexions restant à assurer.

3.4. L'attachement d'une station au réseau

Chaque station doit être reliée au câble terminé par la prise femelle RJ45. Pour ce faire, il suffit d'utiliser un cordon de quelques mètres de longueur comprenant deux prises RJ45 mâles dont l'une des extrémités est connectée à la prise du sol, et l'autre extrémité est connectée :

- soit directement à une prise RJ45 pour les stations livrées après 1992 : aujourd'hui la majorité des équipements se connectant sur ethernet sont livrés avec un attachement «10 base T», en standard ou en option ;
- soit un transmetteur AUI/RJ45 permettant d'adapter les signaux entre les deux technologies pour les stations plus anciennes.

3.5. La liaison panneau de brassage - concentrateur

Les jarretières relient chaque prise du panneau de répartition à un équipement

1 Trois câbles arrivent dans chaque bureau et permettent ainsi la connexion directe d'au plus trois stations.

réseau : concentrateur, routeur, etc. Il est important de noter que le câble utilisé pour les cordons doit être du même type que celui utilisé pour le câblage, surtout en ce qui concerne le pas de torsade [SPURGEON 94].

3.6. Concentrateur

Le câblage ethernet «10 base T» étant en étoile, il est nécessaire de concentrer tous les câbles d'un même segment en un point unique ; c'est le rôle des concentrateurs. Les concentrateurs sont des boites électroniques qui ont un nombre fixe de portes. Quand toutes les portes sont utilisées, on connecte un deuxième concentrateur en cascade. Le coût d'attachement d'une station au réseau en 1992 était alors de :

Tableau 5 : Coût de l'attachement par station en 1992

désignation	quan-tité	tarif unitaire HT	TOTAL HT
coût d'une prise :coût câblage / nbre de prises	1 prise	700 F	700 F
jarretière	2	80 F	160 F
transmetteur	1	900 F	900 F
porte concentrateur[a]	1/12	8 500 F	708 F
TOTAL			2 468 F

a. Initialement les concentrateurs comportaient 12 ports. Actuellement on trouve sur le marché des concentrateurs ayant 24, 36 ou 48 ports.

4. L'interconnexion locale : pont ou routeur

Nous avons déjà évoqué le fait qu'un réseau ethernet ne peut supporter qu'un nombre limité de stations sur un même segment. Dans le cas du réseau Loria, nous avons défini un découpage en 12 segments, représentant ainsi 12 sous-réseaux. Le nombre 12 correspond approximativement au nombre d'équipes et projets. Ces 12 segments doivent être reliés par un dispositif permettant d'isoler le trafic local d'un segment. Ce dispositif doit autoriser les transmissions de données entre stations de segments différents, en même temps il doit avoir une action pour limiter le passage des paquets.

Un tel dispositif peut être soit un pont, soit un routeur ; le premier travaille au niveau 2 du modèle OSI (ethernet) et le deuxième se situe au niveau 3 (IP). Ils gèrent tous les deux des domaines séparés de collision, c'est-à-dire qu'ils ne propagent pas les collisions. Il existe en fait un troisième dispositif, de plus en plus

répandu, qui remplit également ces fonctions. Il s'agit du commutateur ethernet[1]. Nous ne le présentons pas dans ce chapitre car ces dispositifs sont apparus sur le marché après l'implantation du réseau.

Le tableau ci-après compare les principales caractéristiques des ponts et des routeurs.

Tableau 6 : Tableau comparatif des fonctionnalités des ponts et routeurs

PONT	ROUTEUR
connexion brin ethernet (adresse ethernet)	connexion de réseau IP (adresse IP)
passage des *broadcasts*	filtrage des *broadcasts*
passif (pas de programmation possible)	actif (programmable)
coût peu élevé	coût élevé
gestion par table d'adresses ethernet	gestion par masque
débit rapide	débit proche des ponts
dépendant du protocole	indépendant du protocole

Afin d'expliquer notre choix, présentons dans le détail les particularités des ponts et des routeurs.

4.1. Les fonctions

Un pont interconnecte un ou plusieurs segments ethernet, un routeur interconnecte entre eux des réseaux IP mais également des réseaux IPX, Appletalk et cela sur des supports physiques qui peuvent être ethernet, FDDI, etc. Les routeurs remplissent des fonctions plus complexes que les ponts car ils possèdent des fonctions de routage et permettent la cohabitation de multiples protocoles.

Un protocole de routage possède un algorithme propre lui permettant de calculer le chemin optimal entre un émetteur et un récepteur. Les protocoles de routages les plus répandus sont RIP (Router Information Protocol), IGRP (Internet Gateway Router Protocol), OSPF (Open Shortest Path First) et EGB (External Gateway Protocol) [DUPONT 91][HUITEMA 95]. Les routeurs ont généralement la capacité de gérer tous ces protocoles sauf en ce qui concerne IGRP qui est un protocole propriétaire et qui est seulement disponible sur les routeurs *Cisco*.

1 Les commutateurs ethernet sont évoqués au dernier chapitre.

4.2. Les débits

La comparaison des débits entre les portes n'a actuellement plus de sens pour effectuer un choix entre ponts ou routeurs. En effet, la majorité des boitiers ponts ou routeurs utilise des processeurs de plus en plus puissants et dont le coût baisse régulièrement. En revanche, le routeur reste un dispositif beaucoup plus complexe qu'un pont car il nécessite le décodage des trames jusqu'au niveau IP alors que le pont ne décode que les trames ethernet. Quel que soit le choix retenu, il est nécessaire de retenir une ossature capable de supporter un débit égal à la somme des débits de chaque segment connecté.

Signalons que l'analyse des performances s'est appuyée sur des analyses existantes[1] [BRADNER 92] car les mesures demandent un équipement spécifique et ne peuvent être effectuées que par des laboratoires spécialisés ou des organismes comme ARISTOTE. Les équipements nécessaires sont des générateurs de trafic de trames de taille variable puisqu'il faut être en mesure de saturer la bande passante d'ethernet, et des analyseurs de trafic précis.

4.3. Les broadcasts

Les différences de fonctionnement entre les ponts et les routeurs concernant les messages de type *broadcast* sont suffisamment significatives pour en faire un critère de premier ordre. Cela justifie de détailler le comportement d'un *broadcast*. Soit une station sur le réseau dont l'adresse IP est 192.33.167.226. Lors de la configuration de l'interface réseau, l'administrateur affecte non seulement une adresse IP mais également deux autres informations qui sont l'adresse de *broadcast* et le masque (précédemment décrits dans la section 2. à la page 29).

Pour le réseau 192.33.167, l'adresse de *broadcast* est 192.33.167.255. Un paquet dont l'adresse de destination est 192.33.167.255 va donc être lu par toutes les stations du réseau local dont les adresses IP commencent par 192.33.167. Ceci sous-entend bien sûr que cette adresse particulière est réservée aux *broadcasts* et ne peut en aucun cas être attribuée à une station.

Pour qu'un message puisse transiter sur le réseau ethernet, un protocole spécifique fait correspondre l'adresse IP de la station destination avec son adresse physique sur le réseau ethernet. Dans le cas particulier d'un message *broadcast*, l'adresse ethernet associée est une adresse spécifique qui doit être connue de toutes les interfaces ethernet ; cette adresse est ff.ff.ff.ff.ff.ff (en hexadécimal). Ainsi toutes les machines

1 Nous avons notamment étudié les tests effectués Scott O. Bradner consultant à l'Université de HARVARD, publié dans Data Communications (février 1992). Ces tests révèlent que 20 équipements étudiés supportent 99% du débit maximum théorique d'ethernet sur les plus gros paquets et 50% sur les plus petits paquets. Ceci montre la bonne qualité des équipement d'interconnexion.

d'un même segment physique lisent ce message.

Le comportement des ponts et des routeurs est différent face à un paquet de type *broadcast* :

- le pont, qui travaille au niveau des adresses ethernet, laisse passer le *broadcast.*

  Dans un réseau entièrement segmenté par des ponts, tous les *broadcasts* sont diffusés sur l'ensemble du réseau. Le message est alors lu par toutes les stations, même si seulement un petit nombre d'entre elles est concerné ;
- le routeur, au contraire, ne se soucie pas du niveau ethernet, un *broadcast* ethernet s'arrête à la porte du routeur, il reste donc local aux segments.

Deux problèmes liés aux *broadcasts* apparaissent lors de l'utilisation de ponts. Ce sont les «flux croisés» et les «tempêtes de broadcasts». Nous les présentons ci-après.

4.3.1 Les flux croisés

Lorsqu'une station du sous-réseau A va chercher un service sur le serveur du sous-réseau B et que, réciproquement, une station du sous-réseau B va chercher un service sur le serveur du sous-réseau A, les flux réseaux se croisent. Dans le cas d'un réseau segmenté par ponts, on constate que le pont n'a plus aucun effet et n'assure donc pas son rôle d'isolation du trafic.

L'utilisation des ponts sur un réseau nécessite de forcer chaque station à choisir un serveur connecté sur son propre sous-réseau. Ceci n'est pas réalisable pour les services où l'attribution se fait par demande collective. Dans ce cas, le choix des serveurs est totalement déstructuré et entraîne ainsi de nombreux flux croisés, lesquels occupent le réseau et ralentissent le travail de tous les utilisateurs.

4.3.2 Les tempêtes de broadcast

Un service utilise les *broadcasts* lorsqu'il ne connaît pas l'adresse d'un serveur répondant à un type de service donné ou lorsqu'il a besoin de connaître sa propre adresse[1] IP ; c'est, par exemple, le cas pour un terminal X ou pour une station Unix sans disque). Si nous prenons l'exemple d'une machine désirant obtenir sa propre adresse IP, nous constatons que la station émet une requête par *broadcast* et reste ainsi en attente jusqu'à ce qu'elle obtienne satisfaction. Le *broadcast* encombre le

1 Service RARP, ou service de résolution d'adresse réverse.

réseau alors que le message concerne que la station émettrice et son serveur.

Une mauvaise configuration d'une adresse de *broadcast* peut également provoquer l'envoi sur le réseau d'une multitude de *broadcasts.* L'adresse standard d'un *broadcast* correspond actuellement au positionnement à 1 de tous les bits, c'est-à-dire 192.52.167.255 pour un réseau de classe C. Avant qu'elle ne soit standardisée, la notation de tous les bits à 0 était utilisée, notamment par *Sun* dans *Sunos4.x*, ce qui dans notre exemple correspond à l'adresse 192.52.167.0. Si cette adresse n'est pas modifiée par l'administrateur, il en résulte une incompréhension mutuelle entre client et serveur et une surcharge inutile de paquets. Ce dernier phénomène, appelé *tempête de broadcast*, a été constaté sur les anciens réseaux.

Le choix retenu

Les paragraphes précédents expliquent tous l'encombrement du trafic d'un réseau dû aux *broadcasts*, quand celui-ci est segmenté par des ponts. L'utilisation de routeurs pour notre réseau s'est donc quasiment imposée.

La phase suivante a été de choisir un type de routeur parmi ceux proposés sur le marché. Deux critères ont été évalués : la vitesse de débit entre deux portes ethernet et la manière dont les routeurs allaient s'insérer dans notre réseau. Il fallait prendre également en compte le fait que le réseau du CRIN était connecté au réseau du Campus Universitaire, équipé lui-même de routeurs *Cisco*, et que le réseau de l'Inria Lorraine était relié par une ligne spécialisée à Rocquencourt vers le réseau Internet via un routeur *Cisco* également.

Globalement, le marché des routeurs est principalement partagé par deux acteurs : *WellFleet* (devenu *Bay Systems* depuis la fusion en 1994 entre *WellFleet Communications* et *Synoptics Communications*) et *Cisco. Cisco* a été retenu comme fournisseur pour les motifs suivants :

- très bonne performance en terme de débit,
- utilisation du protocole IGRP pour la gestion du routage au niveau du réseau de Campus,
- langage de programmation déjà maîtrisé par deux personnes de l'équipe,
- fonctionnalités étendues, et en particulier des fonctions de sécurité,
- reprise de notre ancien matériel.

Conclusion

L'opération d'achat de l'ossature du réseau constitue le poste principal des dépenses d'acquisition. Elle représente un total de 1,4 MF réparti de la façon suivante : 470KF pour le système de câblage qui comprend 674 prises, 600KF pour les équipements des routeurs et 300KF pour les éléments électroniques nécessaires à l'interconnexion (concentrateurs, transmetteurs,...).

Avec le recul, nous pouvons être satisfaits des choix qui ont été faits aussi bien pour le câblage que pour la structure en sous-réseau. Le choix effectué sur l'infrastructure du câblage est totalement validé par rapport au support des nouvelles technologies. L'utilisation de protocole à des vitesses de 100MB/s pour FDDI et 155Mb/s pour ATM n'a posé aucun problème de fonctionnement sur notre câblage en paire torsadée. La segmentation en sous-réseau a permis, quant à elle, une bonne absorption de la croissance du trafic réseau.

CHAPITRE 4

Les services sur le nouveau réseau

Après la structuration du réseau physique et logique, nous abordons l'étude de l'implantation et de la disponibilité des services aux utilisateurs. Cette phase est importante car elle représente le niveau le plus visible pour l'utilisateur et doit lui apporter le maximum de confort dans son travail.

La conception du nouveau réseau commun aux deux laboratoires a nécessité une succession de réunions techniques, d'échanges d'opinion, de recherche de documents, de collecte d'information sur d'autres plates-formes réseau du même type. J'ai pris une part déterminante dans l'organisation des réunions et dans la synthèse de tous les éléments collectés, notamment en apportant une vue globale de la structuration du réseau, afin que celui-ci ne se construise pas seulement par la concaténation d'éléments techniques hétérogènes.

Lors de mon précédent emploi à l'INIST, en tant que responsable du Service Assistance et Exploitation du Département Informatique, j'ai eu très fréquemment un contact direct avec les utilisateurs. Aussi, il me paraissait opportun de rappeler que la structuration et l'installation d'un réseau informatique n'a de sens que dans la mise à disposition d'un outil de travail aux utilisateurs, en l'occurrence les membres des deux laboratoires de recherche en informatique. Il faut garder à l'esprit que sans eux notre travail n'a pas lieu d'être.

Je me suis plus particulièrement impliqué dans l'implantation du service de montage automatique des partitions, à savoir, l'étude d'un outil plus performant que celui fourni en standard et son implantation sur les multiples systèmes d'exploitation.

Dans ce chapitre, après le détail de la couche application du modèle OSI, nous présentons l'analyse que j'ai effectuée des différents services vitaux au bon fonctionnement de l'environnement utilisateur.

1. La couche application du modèle OSI

La plupart des applications sont construites sur le modèle client serveur [HUNT 92]. Les plus connues et les plus anciennes fonctionnant sur TCP/IP sont : Telnet, permettant la connexion d'un terminal distant, et FTP[1], utilisé pour le transfert de

fichiers à distance. De nombreuses applications utilisent également le protocole SMTP[1] pour gérer le courrier électronique, comme *mail*, *xmh* ou encore *elm*. Parmi d'autres produits plus récents, nous pouvons citer le protocole SNMP[2] destiné principalement aux administrateurs réseaux et plus amplement décrit dans le chapitre 5 consacré à la supervision de réseau, et X qui est un service de multi-fenêtrage.

Si nous prenons le cas de l'application Telnet, nous constatons que le programme (*telnetd*) qui attend une requête d'un client, tourne en permanence sur un serveur. Sur Unix, ce programme en exécution s'appelle un démon. Lorsqu'une personne veut se connecter à distance, elle lance l'exécution d'un programme client *telnet* sur sa station en fournissant en paramètre à ce programme l'adresse ou le nom de la station où elle veut se connecter. Le programme client envoie une requête de connexion au serveur sur lequel se trouve le démon. Le serveur répond au client et reste actif jusqu'à la fin de la session, c'est-à-dire jusqu'à la terminaison du client.

Dans un réseau TCP/IP, ces programmes serveurs sont fournis en standard avec le système d'exploitation. Notre objectif est d'ajouter certains services pour faciliter le travail de l'utilisateur, c'est-à-dire d'une part rendre son environnement de travail le plus transparent et homogène possible, et d'autre part automatiser et centraliser les informations de gestion pour obtenir le maximum de cohérence.

Tout cet environnement de services systèmes et utilisateurs que nous avons ajouté, est détaillé dans ce chapitre.

2. Les services offerts aux utilisateurs

Le réseau doit rester pour l'utilisateur une structure transparente dont il n'a pas à se soucier. Ceci implique que cette structure ne doit pas induire de problèmes. C'est la raison pour laquelle l'un des soucis majeurs de l'étude a porté sur les services offerts aux utilisateurs, afin que ceux-ci trouvent un environnement de travail leur garantissant fiabilité, redondance et sécurité.

Nous nous sommes fixés une liste d'objectifs généraux que doit respecter tout nouveau service mis à la disposition des utilisateurs, via le réseau. Ces objectifs sont les

1 «File Tranfer Protocol» ou protocole de transfert de fichier.
1 «Simple Mail Transfer Protocol» ou protocole simple de transfert de courrier.
2 «Simple Network Management Protocol» ou protocole simple de gestion de réseau.

suivants :

- **la transparence des services aux utilisateurs**

  Par ce terme, nous entendons la banalisation des accès aux services : nous voulons que ces accès soient homogènes et respectent une méta-structure de fichier. Quelles que soient les architectures des ordinateurs, l'utilisateur doit se retrouver avec le même environnement (compte, partition, etc) ;

- **la fiabilité**

  Afin de ne pas subir de rupture de fonctionnement, il est nécessaire d'introduire une redondance maximale pour protéger les services «vitaux», comme l'accès aux exécutables.

  La redondance sous-entend la duplication de logiciels et de données afin que plusieurs serveurs soient capables de répondre aux requêtes des stations. Ceci implique donc une occupation mémoire importante et une mise-à-jour plus complexe, car en plusieurs exemplaires, lors des évolutions des logiciels.

  Il est alors évident que les services moins demandés font l'objet d'une redondance moins importante, voire nulle ;

- **la gestion cohérente de l'ensemble du parc de stations hétérogènes**

  La gestion cohérente d'un parc de stations hétérogènes implique qu'elle soit fortement centralisée que ce soit au niveau des comptes utilisateurs, des espaces disques, des logiciels, des sauvegardes, ...

- **la supervision du réseau**

  Il doit être possible de détecter les problèmes réseau, d'analyser les performances du réseau et d'anticiper ;

- **la sécurité**

  L'installation de nouveaux services doit permettre l'implantation de mécanismes de sécurité. De plus, l'ensemble des services doit être structuré ;

- **l'utilisation de standards et normes**

  L'utilisation maximale des standards et des normes permet d'obtenir, en règle générale, un bon amortissement du matériel et la pérennisation de l'ensemble de la structure du réseau.

Nous avons établi une classification de l'ensemble des services du réseau et nous les avons réparti dans un modèle en trois couches, comme illustré figure 21 ; la couche

la plus externe correspondant à l'Internet :

- les services locaux à la station,
- les services locaux à une équipe,
- les services globaux à l'ensemble du réseau.

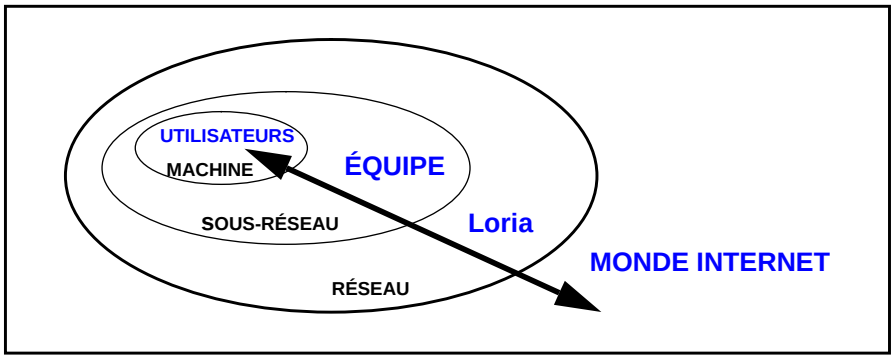


FIGURE 21. Les strates d'accès aux services.

Afin de mieux contrôler et donc de réduire le trafic réseau, nous avons installé, dans la mesure du possible, les services consommateurs en transmission de messages localement dans chaque équipe. Cette répartition permet ainsi à de nombreux messages de ne pas transiter dans tout le réseau et ainsi de ne pas l'encombrer.

Nous présentons ci-après les trois types de services offerts aux utilisateurs.

2.1. Les services globaux au réseau Loria

Un service est installé de façon globale au réseau, soit parce qu'il est coûteux en matériel, il nécessite par exemple un serveur ou un espace disque particulier, soit parce que sa duplication sur chaque sous-réseau ne se justifie pas car les requêtes à celui-ci sont peu nombreuses et/ou de faible volume. Un service destiné à l'extérieur, par exemple le DNS et le courrier électronique, est également installé de façon globale.

Nous avons établi quatre types de services globaux fournis par les serveurs suivants :

- **le serveur de nom** : le DNS (voir la note à la page 17) a un mécanisme intrinsèque de redondance. Il existe pour un site donné un serveur primaire et un ou plusieurs serveurs secondaires ;

- **le serveur de mail** : toutes les stations du site peuvent envoyer du courrier électronique, mais il n'y a qu'un seul noeud qui concentre les envois et réceptions de courrier. La redondance a été étudiée mais aucune solution satisfaisante n'a été trouvée ;
- **le serveur d'information** : les services d'information, comme la diffusion des manuels et les logiciels *ftp, gopher, wais, news, www* étaient initialement considérés comme ne nécessitant pas de redondance. En effet, le coût de la duplication d'un serveur, c'est-à-dire du service et de son espace disque, étaient prohibitifs par rapport à la nécessité d'offrir un service opérationnel 24 heures sur 24.

  Aujourd'hui, cette position peut être modifiée en raison de la baisse du coût de l'espace disque et de l'augmentation de l'utilisation de tels services ;
- **le serveur de partition et imprimantes** pour les MacInstosh. Le produit AUFS[1], de l'Université de Columbia permet d'une part l'accès transparent d'une partition UNIX à partir d'un Macintosh, et d'autre part l'accès aux systèmes d'impression UNIX.

2.2. Les services locaux liés aux sous-réseaux

Un service est installé localement si son indisponibilité bloque le travail des utilisateurs ou si le trafic réseau engendré par ce service est très important. Parmi ces services, nous trouvons :

- **le serveur de carte centralisé**

  Le service NIS, décrit page 20, est totalement indispensable car si ce service est interrompu, il n'est plus possible de se connecter sur une station en mode standard. Il n'y a qu'un seul serveur maître pour le domaine NIS et nous avons pris soin d'installer au minimum un serveur esclave sur chaque segment. De ce fait, lorsqu'une station cliente envoie une requête de service sous la forme d'un *broadcast*, c'est le serveur propre au segment qui répond à la requête. Le mécanisme de *broadcast* est filtré au niveau des routeurs et le trafic engendré par les services NIS reste alors local au segment, il ne «pollue» pas les autres brins ;
- **le serveur de terminaux X**

  Les terminaux X ont besoin de deux types de services. Le premier concerne la configuration du terminal X, c'est un service qui génère peu de trafic mais qui demande une haute disponibilité (les protocoles utilisés

1 «Apple Unix File System», fait partie de l'outil CAP (Columbia Appletalk Package) du domaine public disponible sous rutgers.EDU:/src/cap60.tar.Z.

sont *bootparam*, *tftp*). De plus, le terminal X a besoin d'un serveur sur lequel vont s'exécuter les programmes clients, c'est le deuxième type de services. Celui-ci est consommateur en bande passante car il concerne tout le trafic qu'il peut y avoir entre un client X et son serveur ;

- **le serveur d'impression**

  La fonction des serveurs d'impression est de permettre l'accès pour de multiples utilisateurs à une ressource unique : l'imprimante. Le serveur gère une file d'attente de fichier à imprimer ainsi que la communication avec l'imprimante. Nous avons choisi de multiplier les petites imprimantes réparties à proximité des bureaux par rapport à une grosse imprimante centralisée. Nous avions initialement une imprimante laser *AGFA P400* que nous avons remplacée par une dizaine de petites imprimantes laser, dont 3 sont couleurs.

  La banalisation toujours croissante, l'augmentation de la qualité et la baisse régulière des prix des petites imprimantes laser (10KF HT) ont confirmé notre choix.

  De plus, cette installation présente deux avantages : elle permet aux utilisateurs de disposer d'une imprimante de proximité et la forte redondance du matériel garantit de trouver une imprimante de service quels que soient le jour et l'heure ;

- **le serveur de partition disque**

  Nous détaillons ces services ci-après.

On distingue quatre catégories de partitions qui sont les partitions utilisateurs, les partitions d'exécutables, les partitions locales à une équipe et les partitions système :

- **les partitions utilisateurs**

  Les partitions utilisateurs possèdent le plus grand nombre d'accès car elles correspondent au répertoire principal des utilisateurs, elles sont sollicitées en permanence par des opérations de lecture ou d'écriture. Elles sont vitales pour le travail de l'utilisateur qui a besoin en permanence de ses propres données ; la perte de son répertoire entraînant l'impossibilité de connexion. Elles sont régulièrement sauvegardées et il n'en existe qu'un seul exemplaire en accès direct sur disque.

  En cas de problèmes physiques sur un disque, les données sont restaurées manuellement sur un autre disque. Ceci peut entraîner une indisponibilité temporaire pour toute une équipe. La seule solution à ces problèmes serait l'installation de disque miroir, c'est-à-dire que chaque écriture sur un disque est dupliquée sur un deuxième disque. C'est un mécanisme

éprouvé qui avait été testé sur notre site, mais il est très coûteux car il nécessite le doublage de l'espace disque ainsi que l'ajout d'une carte contrôleur disque ;

- **les partitions d'exécutables**

  Les partitions d'exécutables supportent un très grand nombre de logiciels du domaine public ; ceux-ci sont compilés pour toutes les architecture de machines disponibles sur le site. Actuellement, environ 800 programmes sont compilés pour chaque architecture. Ceci apporte une grande souplesse dans l'utilisation car une même version d'un logiciel est disponible quelle que soit l'architecture utilisée.

  Les logiciels implantés sont très diversifiés et répondent aux besoins des utilisateurs, nous trouvons, entre autres :

  - les interfaces utilisateur système X11 et les gestionnaires de fenêtre comme *motif, twm, fwm,*
  - les outils nécessaires au développement de logiciels : les compilateurs c et c++, le debugger du gnu : *gdb* et *xxgdb,*
  - les éditeurs de texte et outils de composition : *emacs, LaTeX,*
  - des outils de manipulation graphique comme *tgif* ou *xfig*.

  Ainsi l'environnement de l'utilisateur est essentiellement composé de logiciels du domaine public. Ceci permet de disposer d'un même environnement sur différentes plate-formes matérielles et de ne pas utiliser les environnement graphiques propriétaires proposés par les constructeurs comme *HP-VUE* par *HP* ou bien encore *Openwindow* pour *Solaris ;*

- **les partitions locales à une équipe**

  Dans cet espace sont généralement stockés des outils, publics ou commerciaux, qui sont propres à une équipe. Physiquement, ils sont aussi accessibles aux autres équipes.

  Cet espace sert également de zone de stockage de données qualifiées de données de proximité ;

- **les partitions systèmes**

  Les partitions systèmes sont réservées au stockage de différents types de programmes ou de données nécessaires au fonctionnement du système. Ce peut être des données qui occupent un grand volume d'espace disque et dont l'accès n'est pas intensif, c'est le cas des manuels, ou des données qui par nature ont besoin d'un point de centralisation ou de partage global pour toute la communauté, par exemple la comptabilité imprimante, la partition utilisée pour le courrier électronique, etc.

Ces services sont offerts localement à chaque brin et un serveur spécifique leur est attribué. Parmi ces services, il y a NIS pour les raisons évoquées page 63.

2.3. Les services locaux aux machines

Les services installés localement sur chaque machine comprennent tous les services classiques disponibles sur une station UNIX, comme par exemple la partition d'exécutables locale. Nous ne les évoquons pas ici car ils ne conditionnent pas directement l'infrastructure du réseau.

3. Les services système

Nous avons montré, section 5.2. à la page 22, que l'utilisation de NFS provoque des problèmes de fonctionnement. Il existe dans le domaine public un outil, *amd*, initialement développé pour le système *UNIX BSD4.4*, qui offre des similitudes de fonctionnement avec l'outil *automount* de *Sun* tout en supprimant les principales faiblesses de ce dernier.

Les apports de ce produit sont la faible dépendance par rapport au serveur NFS et la disponibilité de nombreux sélecteurs pour effectuer les montages conditionnels dépendant de l'architecture de la station, de la version de système d'exploitation, etc. Ces nouvelles fonctionnalités ainsi que la restructuration de l'ensemble des partitions telles qu'elles sont décrites à la page précédente imposaient de modifier la conception des partitions exportées.

L'implantation d'un tel produit demande de prendre des précautions particulières dans la mesure où il influe sur le fonctionnement général du réseau. Un montage erroné ou ne s'effectuant pas correctement bloque tout un sous-réseau et aucun utilisateur de celui-ci ne peut alors travailler. Un comportement instable, c'est-à-dire des montages NFS non cohérents, serait catastrophique.

Les opérations pour implanter le service *amd* ont été les suivantes :

- écriture des tables de montage, la syntaxe de ces tables est incompatible avec celle de l'outil *automount*,
- compilation des programmes *amd* sur toutes les architectures puisque cet outil se doit d'être fonctionnel sur les architectures disponibles. Ce produit continue à évoluer, et aujourd'hui nous l'utilisons sur *HPUX* de *Hewlett Packard, IRIX de SGI, OSF1* de *DEC* et *Solaris 2.x* de *Sun*,
- écriture du script de démarrage du démon *amd* lors de l'initialisation de la station.

Enfin, la phase la plus importante est la planification et l'installation de cet outil sur l'ensemble des machines du site. Dans un premier temps, nous effectuons la vérification du fonctionnement sur les différentes architectures ainsi que les tests des fonctionnalités annoncés du produit. Ensuite l'outil est implanté sur les stations des ingénieurs systèmes durant une période d'un mois. Comme aucun problème majeur n'a été découvert, nous avons implanté l'outil *amd* sur le segment d'une équipe pilote, puis nous l'avons rapidement généralisé à l'ensemble du réseau.

Les descriptions des montages sont différents selon le type de partitions montées. Examinons les méthodes de montage pour chaque type de partitions :

- **les partitions d'équipe et les partitions utilisateurs**

  Le montage de ces partitions est différent selon que l'on se trouve sur un serveur ou sur un client. La partition existe en un seul exemplaire pour l'ensemble du réseau. Les points de montage pour l'utilisateur sont **/users** pour les partitions utilisateurs ou **/local** pour les partitions locales.

- **les partitions d'exécutables**

  L'objectif est de normaliser les chemins de montage. Ceci signifie qu'un même point de montage NFS correspond à plusieurs chemins physiques sur le serveur en fonction de l'architecture demandée par le client. Par exemple, la partition **/usr/local/bin** ne correspond pas à la même partition physique quand on y accède depuis une station *sun4* ou depuis une station *hp*. Le montage est conditionnel selon le type d'architecture de la machine.

Des exemples des montages des partitions exécutables, ainsi l'utilisation du sélecteur «cluster» sont décrits dans l'annexe B.

Conclusion

Dans l'opération de création du réseau, on peut, en terme de coût, distinguer deux catégories : l'acquisition de matériels que nous avons détaillé dans le chapitre précédent et l'acquisition de logiciels concernant les services. Le coût des services correspond au temps passé à leur implantation, car les logiciels utilisés étant soit du domaine public, soit fournis avec le système d'exploitation, ils n'ont alors aucun coût d'acquisition.

L'aboutissement de cette fusion des deux réseaux a été le déménagement. Il peut sembler curieux que la phase de déménagement proprement dite ne fasse pas l'objet d'une présentation. Ceci s'explique par le fait que le travail concernant l'homogénéité, les tests et les configurations a été entièrement réalisé avant le déménagement.

Celui-ci a consisté principalement au déplacement des stations et des serveurs et à leur connexion à la nouvelle infrastructure. Les serveurs ont été déménagés par nos soins. Le déménagement et la connexion au nouveau réseau des stations ont été réalisés par l'ensemble des utilisateurs. Ceux-ci avaient à leur disposition les équipements de raccordement : transmetteurs et jarretières. Cette phase a été réalisée sur trois jours et équipe par équipe. Enfin, signalons que les utilisateurs ont été agréablement surpris de la rapidité avec laquelle la mise en place opérationnelle de la nouvelle structure s'est effectuée.

CHAPITRE 5

Supervision

En 1991, les réseaux des deux laboratoires CRIN et Inria Lorraine comportaient plus de 200 noeuds IP installés pour la majorité dans deux bâtiments sur le Campus de la Faculté des Sciences de Nancy et, pour une vingtaine de stations, à Metz. Un des aspects qui m'a surpris lors de mon arrivée dans l'équipe système est que pour un réseau d'une telle importance, il n'y ait aucun outil d'administration réseau. Un tel outil permet, entre autres, la représentation graphique du réseau, indispensable quand le réseau est en constante évolution, la gestion des équipements ou la remontée d'incidents. Tant que l'administrateur réseau est privé d'une vue globale du réseau, il ne peut que subir les pannes sans pouvoir réellement maîtriser son réseau, ni réaliser d'actions préventives.

Un choix et une implantation d'un outil de gestion de réseau s'imposaient alors. Plutôt que d'étudier de tels outils après la mise en oeuvre du nouveau réseau, il nous a paru opportun, à partir du moment où l'ensemble de l'équipement réseau était renouvelé, d'étudier simultanément la possibilité de gérer à terme tous les équipements réseaux et donc d'intégrer cette composante dans la construction du réseau.

Ce chapitre est donc consacré à la présentation de la gestion de réseau et aux contraintes à prendre en compte lors de la conception de l'architecture du nouveau réseau. Nous présentons tout d'abord les outils disponibles pour effectuer une gestion de réseau, puis le protocole SNMP[1] ainsi que les choix effectués et les implantations qui sont propres à notre site.

1. Administrer un réseau

L'architecture d'un réseau est conçue à un instant donné, cependant elle doit être capable de s'adapter aux inévitables modifications futures. Pour illustration, indiquons que le nombre de noeuds[2] sur le réseau Loria est passé de 227 en avril 92 à 557 en janvier 95. Ceci implique que la structure même du nouveau réseau doit être évolutive.

Cet accroissement induit plusieurs problèmes qui sont l'augmentation de la complexité, la dégradation des performances et l'augmentation de l'hétérogénéité. Nous pouvons résoudre le problème de l'hétérogénéité par l'utilisation de standards infor-

1 «Simple Network Management Protocol» littéralement protocole simple de gestion de réseau.

2 Le terme de noeud regroupe tous les appareils électroniques qui sont connectés sur le réseau et qui possèdent une adresse IP.

matiques. La gestion des performances et de la complexité doivent être prises en compte par l'administration réseau.

C'est précisément pour aider à résoudre les problèmes liés à l'accroissement de la taille des réseaux que les organismes ISO et UIT[1] (anciennement CCITT) ont défini la norme ISO 7498-4, laquelle est aujourd'hui acceptée par la grande majorité des constructeurs matériels et logiciels. Cette norme couvre cinq grands domaines qui sont :

- la gestion des erreurs et incidents ; ceci recouvre l'observation de l'erreur et son identification, le recouvrement et les tests,
- la gestion de la sécurité,
- la gestion des configurations : manipulation des états des médias du réseau,
- la gestion des performances : analyse des taux d'erreurs, analyse des débits, des paramètres du réseau,
- la gestion de la comptabilité.

2. Choisir un logiciel d'administration de réseau

Historiquement, les mécanismes disponibles pour administrer un réseau étaient très réduits. Les outils les plus connus et les plus utilisés comme les commandes *ping* ou *traceroute* sont fondées sur le protocole ICMP[2]. Ce protocole fait partie de la famille TCP/IP et est principalement destiné à véhiculer des informations de contrôle ou d'erreur entre les équipements.

- La commande *ping*, lancée sur un équipement distant, transmet une trame ICMP de type «echo request». Si l'équipement distant répond, cela signifie que la connectivité existe entre la source produisant la trame et l'équipement distant. Si on ne reçoit aucune réponse au bout de 20 secondes, on en déduit que l'équipement distant n'est pas accessible pour quelque motif que ce soit : ligne coupée, station chargée ou arrêtée, ...

  On peut aussi envoyer plusieurs trames successives et calculer le pourcentage de succès qui donnera une indication sur la qualité de la ligne.

1 «Union Internationale de Télécommunications» : organisme international chargé dans le cadre de l'ONU des questions concernant les télécommunications.

2 «Internet Control Message Protocol» ou protocole de message de contrôle.

- Le programme *traceroute* est plus sophistiqué : il permet d'établir la liste des différents équipements réseaux traversés et de donner des indications sur le temps cumulé de passage à travers les noeuds d'interconnexion.

  Ces informations n'étant pas implantées dans le protocole ICMP, *traceroute* utilise le champ TTL[1] qui existe dans toutes les trames IP. Ce champ était initialement prévu pour éviter le bouclage permanent d'un paquet suite à un mauvais routage. La valeur initiale de ce champ, généralement 32, est décrémentée de 1 à chaque passage dans un routeur. Lorsque ce champ prend la valeur zéro, le routeur suivant le jette et envoie un message d'erreur à la source pour l'informer de la destruction du paquet.

  Le programme *traceroute* envoie successivement trois trames avec le champ TTL initialisé à 1. Il passe le premier routeur et revient en erreur, le programme renvoie le même paquet mais avec le champ TTL incrémenté de 1 et ainsi de suite jusqu'à l'arrivée de la trame à destination. Il fournit les informations concernant les équipements traversés ainsi que les temps de passages par l'étude des messages d'erreurs successifs. L'envoi de trois trames permet de calculer des valeurs moyennes [STEVENS 95].

  Cet outil a donc constitué un grand progrès pour l'administration système et montre comment on peut utiliser le protocole ICMP bien au-delà de ce pourquoi il avait été conçu.

C'est seulement à partir de la fin des années 1980, en raison de la croissance exponentielle du nombre de noeuds IP dans les réseaux, que l'intérêt s'est porté sur l'utilité des outils d'administration de réseau. Il devenait nécessaire de standardiser un mécanisme qui puisse délivrer beaucoup plus d'informations que ne le pouvait le protocole ICMP.

En 1987, SNMP[2] définit un moyen de gérer les réseaux utilisant le protocole TCP/IP [ROSE 91]. L'objectif de SNMP est de permettre à un administrateur d'envoyer des requêtes à des noeuds du réseau pour observer, analyser leur fonctionnement mais aussi détecter les erreurs. En 1988, l'IAB[3] a approuvé les développements réalisés autour de SNMP. Cet organisme a cependant précisé qu'ils ne devaient avoir qu'une durée de vie assez courte puisque des travaux demandés par l'OSI étaient en cours pour développer une solution de gestion de réseau plus générique CMIP[4]. L'IAB a également imposé que les deux développements se fassent autour d'une

1 «Time To Live», ou durée de vie.
2 SNMP existe aujourd'hui sur d'autres protocoles.
3 «Internet Activity Board» : groupe de chercheurs qui se réunissent régulièrement pour discuter des questions concernant Internet dont ils fixent la plupart des règles de fonctionnement.
4 «Common Management Information Protocol».

description unique de la structure de gestion d'information et d'une base d'information.

Nous ne présentons cependant pas la solution CMIP, celle-ci est très peu implantée à l'heure actuelle et elle dépasse le cadre du protocole TCP/IP. SNMP a pris de l'ampleur en raison de sa simplicité. Ainsi, un agent SNMP peut être facilement implanté dans une mémoire morte[1], contrairement à CMIP.

En 1990 et 1991, l'IAB a validé trois RFC[2] définissant un cadre standard pour la gestion de réseau autour de SNMP. Ces trois RFC décrivent la structure du protocole SNMP ainsi que l'organisation et le codage des données. Ces RFCs sont les suivants :

- RFC1155 : structure et identifications des informations de gestion pour un réseau TCP/IP,
- RFC1157 : un protocole simple de gestion de réseau (SNMP),
- RFC1213 : la base de gestion des informations pour une réseau TCP/IP : la MIB-II.

Les trois RFCs précédents décrivent les quatre composants qui forment un système de gestion de réseau :

- une station au minimum qui exécute le programme «maître» de gestion de réseau,
- des noeuds gérés ; chaque noeud possède un agent capable de communiquer avec le programme «maître» de gestion de réseau,
- un protocole communication utilisé entre la station «maître» et les agents,
- une base d'information.

Notons que les noeuds gérés peuvent appartenir indifféremment au réseau local du noeud «maître» ou à un réseau distant.

La figure 22 représente la structure de gestion de réseau où les communications

1 C'est le cas des concentrateurs ethernet, des imprimantes, etc.

2 «Request For Comments» ou appel à commentaires, qui est le mécanisme de standardisation ouvert de toute la famille TCP/IP.

entre les agents et le noeud «maître» respectent le protocole SNMP.

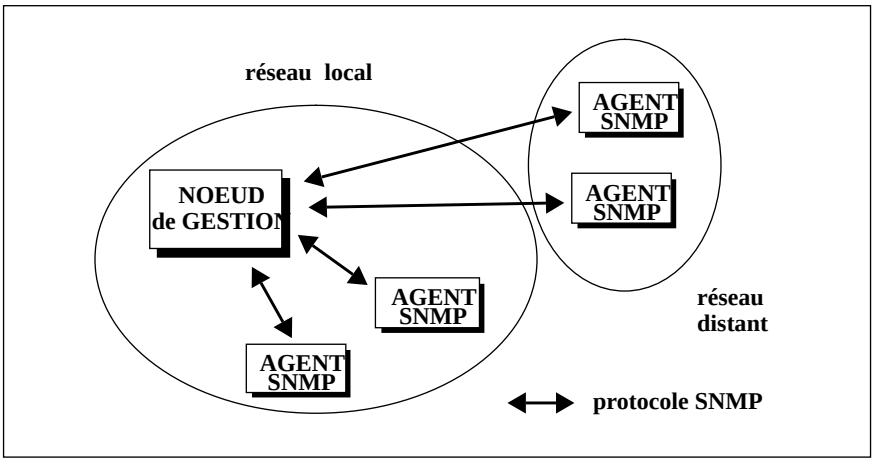


FIGURE 22. La structure de communication établie entre les agents et le noeud de

Le programme de gestion de réseau, exécuté sur le noeud «maître», envoie des requêtes vers tous «ses» agents en respectant le protocole SNMP. Le gestionnaire et les agents se partagent une base de données commune. Cette base de données, appelée MIB[1], est une collection structurée en arbre d'objets gérés. Chaque objet représente une abstraction des ressources d'un équipement que chaque agent maintient à jour. Certains objets ont une seule instance, comme la localisation de l'équipement géré, ou plusieurs instances, comme les connexions réseaux d'un système.

Les objets sont identifiés de manière unique par l'affectation d'un identificateur d'objet appelé OID[2]. Un OID est une séquence d'entiers positifs organisée hiérarchiquement. Un nom textuel est associé à chaque élément d'un OID facilitant leur désignation. Par exemple, l'objet *sysDescr* a pour OID : 1.3.6.1.2.1.1.1 (voir figure

1 «Management Information Base» ou base d'information de gestion.
2 «Object Identifier».

23).

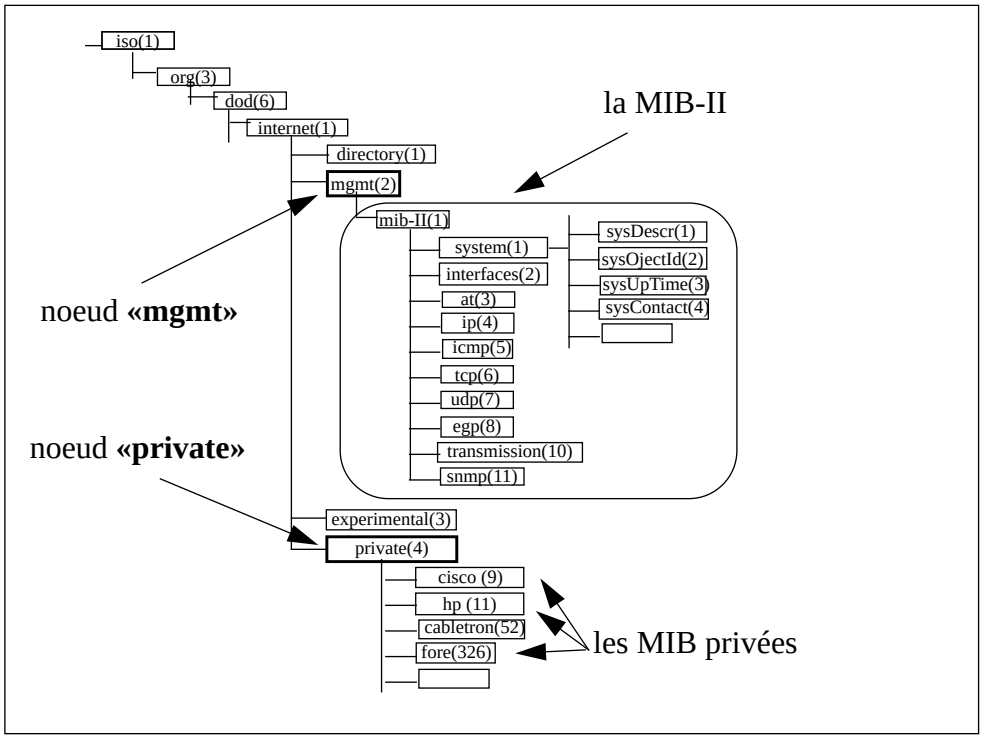


FIGURE 23. La structure arborescente de la MIB.

La structure de la MIB est commune à TCP/IP et OSI. Il existe plusieurs MIBs, celles-ci sont des sous-arbres connectés sous une racine commune. La MIB-II décrit les variables relatives au protocole TCP/IP. Il existe des MIB spécifiques à un constructeur, celles-ci sont attachées sous le noeud «private» (voir figure 23) ou des MIBs spécifiques à un équipement (définies par un RFC) qui se trouvent sous le noeud «mgmt» comme la MIB-II.

Le protocole SNMP est utilisé pour effectuer les interrogations et les mises à jour des variables de la MIB [STALLINGS 93]. Ce protocole, volontairement simple, n'a que quatre commandes de base. Deux pour l'interrogation par le noeud de gestion, une pour l'écriture de la valeur d'un objet par le noeud de gestion et une pour la remontée d'alarme à l'initiative de l'agent :

- get : lecture d'un objet de la MIB,
- getnext : lecture de l'objet suivant dans l'ordre lexicographique,
- set : écriture d'une variable de la MIB,
- trap : remontée d'alarme.

Les niveaux d'accès sur les variables d'une MIB sont les suivants :

- lecture seulement,
- lecture-écriture,
- rien

Le protocole SNMP possède un mécanisme d'identification simple pour vérifier que l'expéditeur de la requête est habilité à recevoir ou à modifier une information dans la base de données. Chaque requête inclut un nom de communauté qui valide les accès en lecture ou en écriture. Les agents ignorent les requêtes sans nom de communauté.

Ce mécanisme de sécurité est faible car le stockage du nom de communauté n'est pas crypté. De plus, en standard, les agents autorisent la lecture sous le nom de communauté «public». Ce qui permet, si aucune modification n'est faite, d'accéder aux informations des MIBs de n'importe quelle station du réseau Internet.

Pour que les éléments d'un réseau puissent être gérés par SNMP, il est nécessaire d'implanter des agents SNMP et un noeud de gestion permettant la centralisation des informations. Voyons à présent ces éléments dans le détail afin de comprendre comment nous les avons intégrés dans nos réflexions lors de la construction du réseau.

3. Les agents SNMP

Un agent est un logiciel opérant à l'intérieur d'un équipement à gérer, qu'il s'agisse d'un équipement terminal de type station de travail, Macintosh, PC, imprimante ou serveur de terminaux, ou d'un équipement de type réseau : passerelle, routeur, pont, concentrateur ou commutateur.

Pour une gestion optimale d'un réseau, il est préférable que tous les noeuds gérés constituant ce réseau possèdent chacun leur propre agent SNMP. On peut classer les agents SNMP en trois catégories :

- **les agents simples** : ils implantent seulement les variables de la MIB-II ;
- **les agents étendus** : ils répondent aux variables de la MIB-II mais également à celles d'une MIB privée constructeur et/ou à une ou plusieurs MIBs définies dans les RFC. Par exemple, la MIB décrite dans le RFC1493 défini les objets pour caractériser les ponts ;
- **les agents extensibles** : Par rapport aux autres types d'agents, ils sont ouverts dans le sens où on peut leur ajouter des fonctionnalités. Ils sont programmables et permettent l'implantation de MIB «expérimentale»,

c’est-à-dire locale à un site. Le fonctionnement est le suivant : on crée un sous-arbre correspondant à une MIB «expérimentale». A chaque instance de cette MIB, on associe un programme ou un script qui retourne l’instance de la variable.

Le coût de l’implantation d’un agent sur un noeud du réseau dépend du type d’appareil géré. Ce coût doit être pris en compte et mérite que l’on s’intéresse aux implantations sur les différents appareils.

Les ordinateurs multi-tâches

L’agent SNMP permettant de gérer un ordinateur multi-tâches se présente sous la forme d’un démon lancé au démarrage de la station.

Il peut être fourni avec le système d’exploitation ; c’est le cas de *IRIX* pour *Silicon Graphics*, de *HPUX* pour *Hewlett Packard*, de *OSF1* pour *DEC* et de *AIX* pour *IBM*. On peut en trouver des versions commerciales ou dans le domaine public.

Les agents SNMP du domaine public intègrent la MIB-II mais vont rarement au-delà. Quelques tentatives d’extension ont cependant vu le jour, par exemple *smux* [ROSE 91], mais elles ne sont pas généralisées car trop complexes à mettre en oeuvre. Toutefois, de tels agents présentent l’intérêt de proposer directement le code source du démon, lequel peut être généralement compilé sur différentes architectures. Les agents peuvent donc être modifiés et adaptés à une utilisation plus spécifique.

Les agents fournis avec le système d’exploitation sont généralement des agents étendus, ils intègrent la MIB-II et une MIB propriétaire.

Les micro-ordinateurs

Les systèmes d’exploitation de ces micro-ordinateurs, *Mac/Os* pour *Macintosh* et *MS/DOS* pour *PC*, ne sont pas multi-tâches et ne permettent donc pas d’exécuter un démon simultanément au travail de l’utilisateur.

Certains fabricants intègrent un agent SNMP directement sur la carte réseau. Sur les Macintoshs, la couche logicielle *mac/tcp* du système *MacOs 7.5* permet l’intégration d’un agent SNMP**.**

Les équipements réseaux

> Pour répondre aux requêtes SNMP, il est obligatoire que chaque constructeur intègre un agent SNMP dans ses équipements réseaux. Soit l'agent est fourni en standard comme dans le cas des routeurs *Cisco*, soit il est en option et provoque alors un surcoût d'équipement, c'est le cas des concentrateurs *Cabletron* pour lesquels il faut ajouter environ 20% du prix de base pour les équiper d'un agent SNMP.

Ce descriptif de l'implantation d'agent SNMP sur différents noeuds d'un réseau montre qu'il existe des contraintes pour gérer un réseau avec SNMP et que celles-ci doivent être intégrées aux critères de choix des matériels et logiciels du nouveau réseau.

Etudions à présent le noeud de gestion, qui va être le point central des requêtes SNMP.

4. Le noeud de gestion du réseau

Il n'existait que très peu d'outils du domaine public cumulant les différentes opérations nécessaires à la centralisation de la gestion d'un réseau. Les outils se résumaient à un «programme d'application» comprenant une bibliothèque de programmes et des commandes implantant les opérations basiques : *get, getnext* et *set*, permettant ainsi d'interroger les agents SNMP. Ces outils étaient écrits en C ou en langage interprété comme PERL. Il était alors plutôt fastidieux de créer un produit intégrant de manière conviviale les différentes fonctionnalités d'un noeud de gestion comme la collecte de données, la gestion de performances, la gestion d'événements, la gestion d'historique ou la compilation d'une MIB provenant de tiers. Les bibliothèques de programmes permettaient de répondre essentiellement à la collecte de données mais il n'existait aucun outil intégrant un maximum de fonctionnalités.

Trois ans après ces remarques, nous constatons que les outils du domaine public n'ont pas été notablement améliorés et sont plutôt des plates-formes de développement.

Nous nous sommes tournés vers les gestionnaires de réseau commerciaux. Les trois principaux produits disponibles sur le marché et fonctionnant sous UNIX ont été étudiés ; il s'agissait de *Openview* de *Hewlett Packard*, *Spectrum* de la société *Cabletron* et *Sunnet Manager* de *Sun*. Les autres produits existants étaient des dérivés de ces trois premiers produits, comme *Netview 6000* (qui est initialement un produit construit sur la base d'*Openview*).

Sur ces trois produits, deux seulement ont fait l'objet de tests approfondis. Nous

n'avons pas retenu le produit *Spectrum* qui ne correspondait pas tout à fait ni à nos besoins, ni à notre budget. Il faut cependant noter que ce produit offre un certain nombre de fonctionnalités intéressantes et plus avancées que celles des autres produits notamment en ce qui concerne la gestion du câblage et la connectivité. Il dispose d'un moteur d'inférence lui permettant de déterminer la dépendance entre les événements. Ceci est particulièrement important lorsque l'on gère un grand nombre de réseaux à distance car le mécanisme mis en oeuvre permet de détecter finement le point de coupure et de ne plus interroger les équipements qui se trouvent au-delà de celui-ci. Les interrogations régulières sont alors évitées, ce qui minimise ainsi la réception d'événements. Toutefois, cette fonctionnalité n'avait pas d'intérêt direct pour notre site qui gère seulement trois sites distants. De plus, le coût de *Spectrum*, dix fois plus élevé (300 KF en 1992) que celui des autres produits, l'a rapidement éliminé de la liste des outils étudiés.

Les domaines dans lesquels nous avons testés les deux produits restants ont concerné la représentation automatique de la topologie réseau par graphique, les outils d'analyse de performances, la gestion des alarmes, les outils de gestion d'historique et la capacité d'intégration des MIBs de tiers. Voici les conclusions des tests que nous avons effectués dans chacun de ces cinq domaines.

La représentation de la topologie du réseau - Les deux produits, *Openview* et *Sunnet Manager*, découvrent de manière automatique les noeuds de chaque réseau dès l'instant où ces noeuds possèdent une adresse IP. Pour initialiser l'opération, ils utilisent soit le fichier **hosts**, soit le numéro de réseau.

La différence majeure est que *Openview* construit automatiquement les liaisons topologiques IP alors qu'il est nécessaire d'établir ces liens manuellement sous l'éditeur graphique pour *Sunnet Manager.*

La surveillance des débits et des performances - Ils centralisent les informations que les agents SNMP collectent sur le réseau. Les deux produits ont des fonctionnalités équivalentes. En réalité, la surveillance d'événements anormaux sur le réseau demande que les agents puissent fournir des informations très précises sur l'état de la ligne, particulièrement en ce qui concerne les erreurs. Or les interfaces des stations ne sont en général pas assez sophistiquées pour délivrer une information sur les différents types d'erreurs physiques liées à ethernet (collision simple, collision multiple, jabber, etc). Il est alors souvent nécessaire d'installer des appareils électroniques dédiés pour ce travail. Ces appareils, ou sondes, sont des dispositifs ayant une interface ethernet plus sophistiquée que celle d'une station.

Les gestion des alarmes - Ils gèrent tous deux correctement la réception et le stockage dans un fichier centralisé des événements produisant des alarmes. Ils permettent également l'association d'une action à la réception d'une alarme.

Les outils de gestion d'historique - Ils permettent d'effectuer des interrogations régulières de variables de la MIB et le stockage de ces valeurs dans un fichier. Cependant, il n'existait aucune structure de base de données permettant la gestion réelle d'historique. Les outils disponibles proposaient seulement une utilisation sur des périodes courtes, c'est-à-dire inférieures à 8 jours.

La capacité d'intégration des MIBs de tiers - Ce test d'intégration n'était pas considéré comme très important au début des tests. Cependant, cette fonction est vite apparue comme vitale pour permettre de suivre l'évolution du réseau.

En effet, tout logiciel de gestion de réseaux est fourni avec les MIBs constructeurs les plus répandues à la date de commercialisation. Il doit ensuite être capable de charger une nouvelle MIB. En effet, à chaque ajout d'un nouvel équipement est associé une nouvelle MIB et celle-ci doit être intégrée si l'on veut gérer l'équipement par SNMP.

Toutes les MIBs respectent le format ASN.1[1] et sont fournies par le constructeur dans ce format, soit par leur serveur FTP, soit avec le logiciel, sur un support magnétique ou optique. Tous les gestionnaires de réseaux permettent l'intégration de nouvelles MIBs et disposent pour ce faire d'un compilateur de MIB.

Les deux produits testés diffèrent sur la facilité d'intégration :

- *Sunnet Manager* nécessite d'une part un outil de traduction pour intégrer une nouvelle MIB et d'autre part l'arrêt du logiciel lors de cette modification.
- Avec *Openview*, le chargement et le déchargement d'une MIB se font de manière dynamique et directement par l'intermédiaire de menus, sans interrompre d'aucune manière le fonctionnement du logiciel.

Une autre différence entre les deux produits concerne le compilateur de MIB : celui d'*Openview* est de très bonne qualité ; en revanche, celui de *Sunnet Manager* n'est vraiment pas satisfaisant puisque lors des tests, aucune MIB n'a pu être compilée par le traducteur de *Sun* : *mib2shema*.

1 «Abstract Syntax Notation One», langage normalisé par l'ISO permettant de décrire les types des données de façon indépendante des techniques de représentations informatiques utilisées

Il existe une autre différence entre les deux produits qui n'est pas apparue immédiatement. Elle est intrinsèquement liée à la structure de communication mais elle est cependant essentielle. Le logiciel de *Sun* n'utilise pas seulement le protocole SNMP, il interroge les machines distantes avec le protocole RPC (Remote Procedure Call). Ceci est certes, plus efficace, mais rompt d'une part avec la standardisation et d'autre part avec la gestion centralisée de toutes les stations du réseau, quelle que soit leur architecture. Cette façon de procéder apparaît comme une solution privilégiant trop le constructeur ; en effet, le démon RPC qui fournit d'ailleurs des informations complémentaires notamment sur les disques, n'est disponible que sur les stations *Sun*. Or notre réseau comporte des équipements multi-constructeur, et nécessite donc de s'appuyer au maximum sur les standards.

La figure 24 schématise le mode de fonctionnement de *Sunnet Manager* et l'utilisation des protocoles SNMP et RPC.

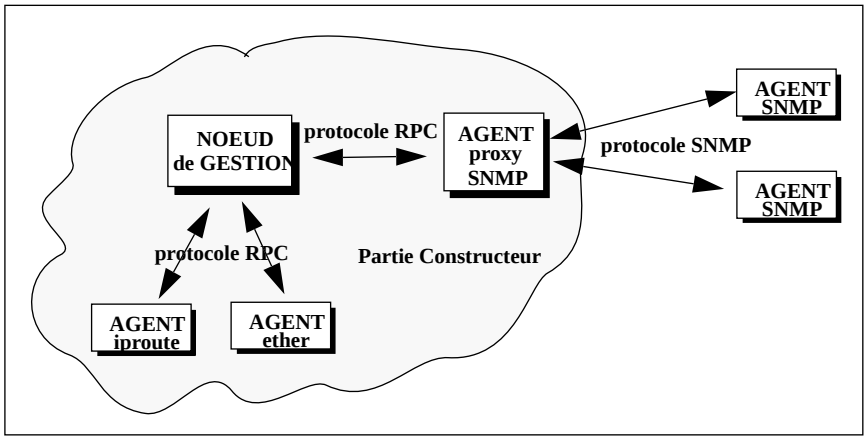


FIGURE 24. L'utilisation des protocoles SNMP et RPC dans le logiciel.

Nous avons donc choisi de travailler avec l'outil *Openview* qui, d'une part, respecte le standard SNMP sur l'ensemble du réseau, et d'autre part, propose un compilateur de MIB fiable. De plus, *Openview* effectue de manière automatique la reconnaissance et la représentation graphique de la topologie des noeuds IP gérés. Il présente également des qualités ergonomiques.

Une fois, le logiciel choisi et implanté, il est intéressant d'exploiter les possibilités de l'outil et d'en faire une version adaptée à notre site. Examinons à présent les extensions réalisées.

5. L'implantation de Openview sur notre site

Les extensions réalisées concernent la création d'icones graphiques, et pour chaque équipement du réseau, nous avons identifié les variables des MIBs dont les valeurs

sont pertinentes pour l'amélioration du fonctionnement du réseau.

Nous présentons ci-après les investissements à réaliser afin que le gestionnaire de réseau fonctionne correctement et aide ainsi l'administrateur à maîtriser le réseau.

5.1. Les extensions visuelles

Le logiciel *Openview* détecte de manière automatique toute présence d'un nouvel objet sur le site. Cet objet est symbolisé sur le schéma représentant la topologie du réseau, par une icone. A chaque type d'objet est associée une icone, au moment de la commercialisation du logiciel. Lorsque le logiciel ne possède pas l'icone associée aux nouveaux matériels connectés sur le réseau, il utilise alors l'icone **Generic** représentée figure 25.

Pour éviter que la représentation graphique de la topologie du réseau évolue vers une collection d'icones **Generic**, il convient de déclarer chaque nouvel équipement et de lui associer ou de lui créer une nouvelle icone. La figure 25 présente les icones fournies en standard dans *Openview* et celles que nous avons créées pour les associer aux stations afin de différencier les différentes architectures disponibles. Les stations représentent 80% des équipements d'un site.

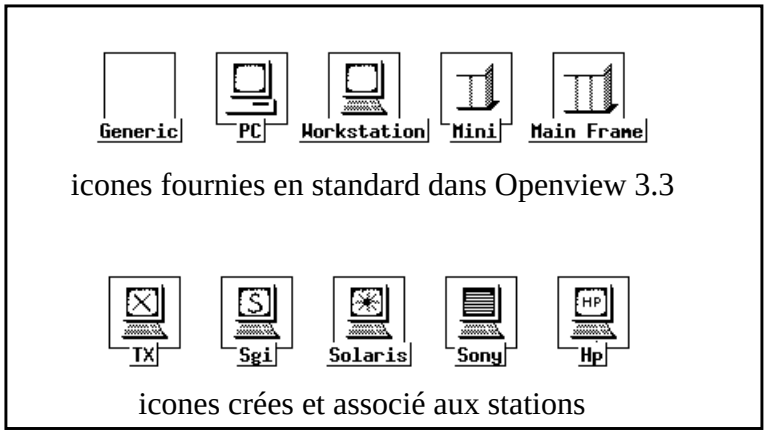


FIGURE 25. Les icones permettant la différenciation des stations.

La représentation graphique de la vue d'une partie de notre réseau, telle que *Openview* la dessine se trouve figure 26. Un exemple plus complet des niveaux successifs

gérés par *Openview* se trouve dans l'annexe C.

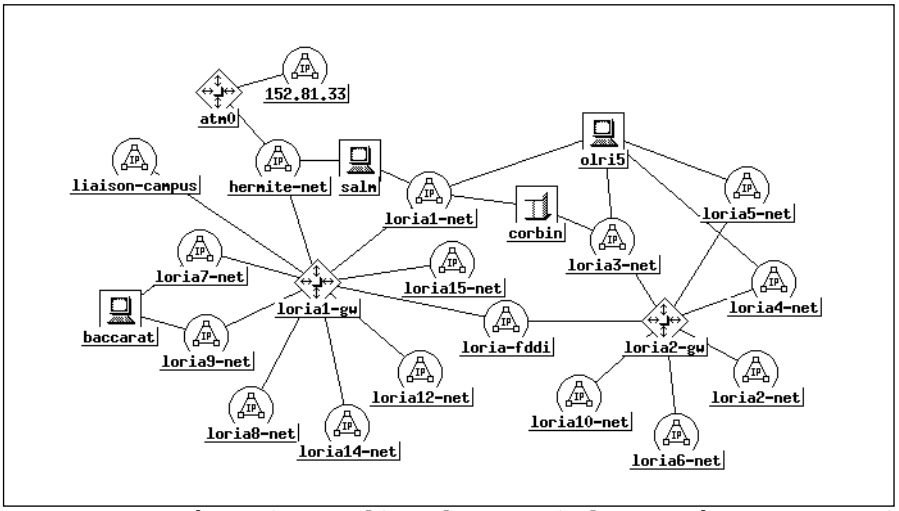


FIGURE 26. La représentation graphique d'une partie de notre réseau par Openview.

5.2. Les extensions de gestion des équipements locaux.

Outre la construction automatique de la topologie du réseau, un gestionnaire permet l'interrogation et la collecte des instances de variables de la MIB. La difficulté réside dans le fait que chaque constructeur implémente dans ses MIBs des fonctions particulières. Au-delà des opérations standards effectuées par le gestionnaire de réseau, il est intéressant d'adapter l'outil au site pour exploiter les possibilités offertes par le constructeur sur son équipement.

Toute nouvelle acquisition de matériel augmente donc le nombre total de variables de MIB à gérer. Dans ces MIBs privées, il convient d'analyser les variables qui ont un réel intérêt[1] pour le site ainsi que les extensions de remontée d'alarme. Ce travail n'est pas aisé car les objets de MIBs ne sont pas toujours correctement documentés. L'information est souvent limitée au champ description du format ASN.1 comme le montre l'exemple suivant :

```
whyReload OBJECT-TYPE
          SYNTAX  DisplayString
          ACCESS  read-only
          STATUS  mandatory
          DESCRIPTION
              "This variable contains a printable octet
```

1 Certaines variables sont internes et uniquement destinées à effectuer des tests de fonctionnement matériel, comme par exemple la lecture des tensions d'alimentation électrique des cartes électroniques composant l'appareil ; elles sont alors difficilement intégrables sans une parfaite connaissance électronique du matériel.

```
                    string which contains the reason why the
                    system was last restarted."
                ::= { lsystem 2 }
```

Malgré ces inconvénients de documentation, les MIBs constructeurs présentent l'avantage d'être généralement en libre accès, elles sont accessibles soit par réseau via *ftp* ou *w3*, soit par support magnétique avec l'équipement.

Pour chaque équipement connecté sur le réseau, notre travail a consisté à identifier les objets pertinents pour l'amélioration de la gestion et du fonctionnement du réseau. Ces objets se répartissent entre deux classes : les objets interrogeables par scrutation et les objets «remontée d'alarme» qui sont gérés à l'initiative de chaque agent.

Nous présentons ci-après les fonctionnalités intéressantes à intégrer dans le gestionnaire de réseau pour les trois catégories d'équipements intervenant sur notre site.

Les Terminaux X - Les terminaux X connectés sur notre réseau sont exclusivement de marque *NCD*, ils possèdent tous un agent SNMP implanté en standard par le constructeur. Cet agent gère la MIB de base et une MIB privée, laquelle contient un objet permettant de réinitialiser un Tx à distance.

Cette fonctionnalité est particulièrement intéressante puisqu'elle permet à l'administrateur d'intervenir sur un terminal X alors que celui-ci est de par sa définition non gérable de l'extérieur.

Les imprimantes - Pour la majorité d'entre elles, les imprimantes sont d'origine HP ; ce constructeur a été le premier à implanter un agent SNMP sur la carte de communication des imprimantes. Cet agent utilise une MIB imprimante privée qui permet, entre autres, d'obtenir à distance l'état d'une imprimante, et plus particulièrement la cause de son dysfonctionnement : bac papier vide, bourrage papier, capot ouvert, ...

Les concentrateurs - Un concentrateur ethernet possède une fonctionnalité très intéressante concernant la détection de problème : chaque port du concentrateur est autonome et est déconnecté du reste du réseau quand le concentrateur y détecte une erreur. Cette erreur peut être, par exemple, une collision qui dure un temps anormal ou une succession de 30 collisions. Le port est activé à nouveau quand un «bon» paquet est transmis (un bon paquet est un paquet généré par une interface et qui est à la norme IEEE802.3, une interférence électrique peut être vue comme un paquet ou une collision). Cette fonctionnalité permet d'isoler une station qui dysfonctionne. Mais cela n'est pas suffisant car il faut que l'administrateur en soit averti et puisse juger ainsi de la gravité de la

panne. En effet, le problème peut être simplement temporaire ou il peut provenir d'une interface en mauvais état ou bien se situer au niveau des câbles de liaison.

Les concentrateurs peuvent être configurés pour envoyer une alarme en présence d'un problème. Cette information est récupérée par *Openview* qui exécute alors l'action associée à cette alarme. Sur notre site, *Openview* transmet à l'administrateur un courrier électronique lui indiquant le problème en précisant le nom du concentrateur et le numéro du port concerné.

Les nouveaux concentrateurs possèdent des fonctions étendues, l'une d'entre elles est particulièrement intéressante puisqu'elle permet de remonter, toujours par le mécanisme d'alarme, l'adresse ethernet des équipements connectés derrière chaque port. Ceci permet d'identifier précisément le nom de la station ou de l'équipement connecté. Cette fonctionnalité est utilisée sur notre site distant, à Metz, qui possède ce type de concentrateur. Malheureusement nous ne pouvons pas généraliser cette procédure car la majorité des concentrateurs sur le réseau Loria n'a pas cette fonctionnalité.

J'ai réalisé cette étude des fonctionnalités pour chaque catégorie d'équipement connecté sur le réseau. Sur ma demande, un stagiaire de fin d'année de DESS en a effectué la réalisation technique. L'intégration effectuée permet, aujourd'hui, à des personnes ne possédant pas une connaissance intrinsèque de SNMP d'utiliser *Openview* et d'interroger facilement les MIBs.

Conclusion

La gestion par le protocole SNMP des équipements d'un réseau représente indéniablement une avancée dans la maîtrise du réseau. La gestion dynamique de l'ensemble des équipements et la mise en place d'alarme facilitent l'administration du réseau. Outre l'implantation d'un agent SNMP sur chaque équipement, l'acquisition d'un outil central de gestion est indispensable car il effectue le lien entre les données brutes fournis par les agents et il permet ainsi leur exploitation.

Il convient de noter que la notion de MIB propriétaire, initialement séduisante devient lourde à gérer en raison du nombre de MIBs en constante augmentation, la sélection de l'information pertinente étant difficile à effectuer.

De plus, chaque acquisition d'un nouvel équipement demande un important temps de travail pour son intégration dans le gestion réseau, cet investissement est normal lorsque cet équipement existe ou va exister à court terme en grand nombre sur le réseau. En revanche, on peut s'interroger sur la nécessité d'intégration de ses fonc-

tionnalités lorsque celui-ci est en un seul exemplaire.

Ce problème est cependant en instance d'être résolu : les MIBs privées étaient nécessaires dans la mesure où les constructeurs voulaient rapidement implanter des fonctionnalités qui n'étaient pas décrites dans la MIB-II. Actuellement, la tendance s'inverse : les constructeurs s'orientent vers la standardisation. Leur démarche est de proposer des MIBs par catégorie d'équipement. Ainsi, il existe maintenant des RFC décrivant les répéteurs, les ponts (RFC1493), les imprimantes, les stations (MIB host) et aussi d'autres protocoles que ethernet (réseau numérique à intégration de services, FDDI RFC1285 et RFC1512), ATM. La plupart sont seulement à l'état de **«**drafts[1]**»** mais leur état d'avancement permet d'espérer une proche standardisation. Cette orientation vers des MIBs standards réduit ainsi la dépendance vis-à-vis des constructeurs et facilite le travail d'intégration.

J'ai réalisé les parties décrites concernant la supervision de réseau, c'est-à-dire l'étude de l'intégration de SNMP sur le réseau, l'implantation des agents sur les stations ainsi que les adaptations locales. La partie technique sur la gestion des traps a été réalisée par un stagiaire de DESS réseaux que j'ai encadré.

1 Littéralement «brouillon», c'est un des états de transition des RFC, l'état suivant est «adopted» et signifie la standardisation du RFC.

CHAPITRE 6

La sécurité sur le réseau

Sur un réseau informatique, les accidents sont généralement bien maîtrisés et les erreurs mieux contrôlées. Mais il existe une menace de plus en plus grave qui affecte les réseaux, à savoir la fraude et la malveillance informatique. La sécurité a pour objectif de protéger un réseau informatique du piratage et également de détecter toute intrusion et de restaurer les informations en cas d'endommagement de celles-ci.

Je suis le responsable INRIA de la sécurité du site Loria. Ce site, regroupant deux centres de recherche, est placé sous la tutelle administrative de deux autorités : le CNRS et l'INRIA. Aussi, une autre personne dépendant du CNRS avec laquelle je travaille en étroite collaboration, assure également la responsabilité de la sécurité.

C'est l'architecture même d'un réseau qui fragilise la sécurité d'un site et nous devons être extrêmement vigilants pour garantir aux utilisateurs un réseau fiable et sécurisé. L'objectif de ce chapitre n'est pas d'énumérer toutes les réalisations techniques de sécurité mises en oeuvre sur notre réseau, mais d'expliquer l'approche utilisée pour parer à d'éventuelles attaques. Nous présentons tout d'abord les principaux mécanismes d'intrusion sur tous les niveaux d'un réseau. Nous détaillons ensuite les protections que nous avons mises en place, puis les tests de sécurité que nous avons effectués. Dans les actions menées, outre le contrôle a priori des mots de passe, je me suis occupé de la programmation des routeurs concernant les mécanismes d'accès.

1. La sécurité

La sécurité fait partie des éléments fondamentaux qui ont été pris en compte lors de la création et de l'installation du réseau dans le bâtiment du CRIN, puis dans celui de l'Inria Lorraine. Toutefois, la sécurité était relativement facile à gérer et n'avait pas encore pris l'ampleur spectaculaire qu'elle atteint aujourd'hui. Ce phénomène

provient essentiellement de trois facteurs :

- **La taille du réseau Internet**

  L'accroissement exponentiel du nombre de stations connectées à l'Internet a provoqué une augmentation de la population ayant accès à ce réseau et donc, a fortiori, une augmentation des risques d'intrusion.

- **La banalisation des micro-ordinateurs**

  Dans un système d'exploitation multi-utilisateurs, il existe une notion d'utilisateur privilégié, par exemple l'utilisateur **root** sous Unix, qui détient l'accès exclusif aux fonctions de supervision de la machine. Ces fonctions de «super-utilisateur» et le compte **root** associé sont généralement réservés aux administrateurs système du site.

  Or cette notion de super-utilisateur n'existe pas sur les machines fonctionnant en mode système mono-utilisateur, comme les micro-ordinateurs sous *Windows* ou sous *MacOs*. Dans ce cas, tout utilisateur peut devenir un super-utilisateur et à ce titre, peut se proroger des droits spéciaux en supprimant toutes authentification ;

  La banalisation des micro-ordinateurs sur un réseau introduit une équivalence dangereuse entre utilisateur et administrateur.

- **Le raccordement à l'Internet par abonnement téléphonique**

  La banalisation de ce type d'accès au réseau mondial a facilité la circulation d'informations. Certaines personnes utilisent cette facilité pour distribuer des logiciels complets tout prêts pour craquer un système.

  Ainsi, il est relativement simple de se procurer le *guide du parfait craqueur*[1] ou des programmes permettant d'usurper les droits d'administrateur ou de super-utilisateur. L'«avantage» de ces programmes est que leur mise en oeuvre et leur utilisation ne nécessitent pas de connaissances techniques approfondies.

Face à ces dangers potentiels, nos objectifs sont, dans l'ordre, la prévention, la surveillance et la reconstruction. La prévention consiste à minimiser les risques d'intrusions sur le réseau, la surveillance doit aider à détecter les intrusions éventuelles et la reconstruction permet à l'ensemble du réseau de fonctionner à nouveau sur une base saine lorsque des dégâts ont été constatés.

Si on reprend les différentes couches de la pile TCP/IP, on constate que la sécurité concerne l'ensemble des couches. Nous avons regroupé les attaques et les risques

1 Traduction du terme anglais «cracker» signifiant «qui casse un système pour s'y introduire de façon illégale».

d’intrusion en trois niveaux, lesquels sont représentés figure 27.

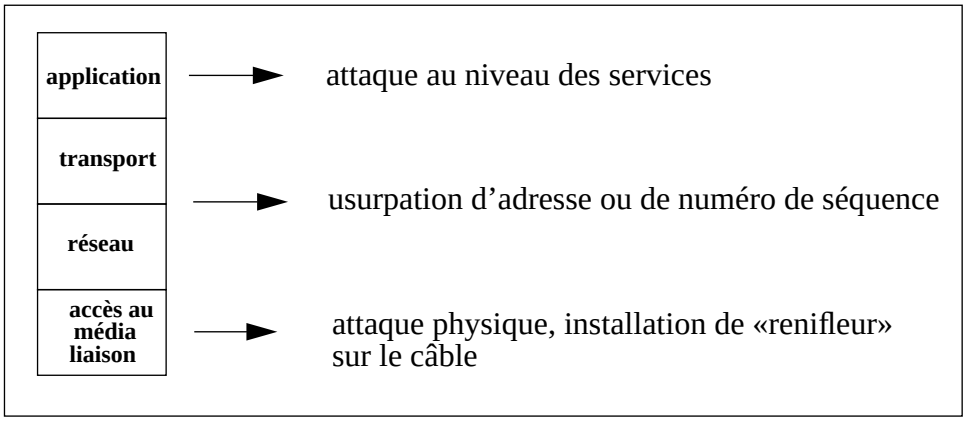


FIGURE 27. Les différents niveaux d’attaque d’un réseau.

Niveau physique - Le danger d’intrusion provient de l’installation d’un «renifleur», c’est-à-dire de la connexion d’une machine permettant de capter toutes les trames qui transitent sur le réseau. Il suffit alors d’étudier les paquets ethernet pour obtenir les mots de passe qui circulent de manière non codée dans les trames.

Niveau réseau - Pour s’introduire illégalement sur un réseau, le principe est de falsifier l’adresse source IP d’un paquet en la remplaçant par une adresse source interne au réseau dans lequel on veut s’infiltrer. Les «nouveaux» paquets sont alors interprétés comme faisant partie du réseau et sont autorisés à en utiliser tous les services [BELLOVIN 89].

Il est également possible d’intervenir au niveau TCP/IP mais le mécanisme à mettre en oeuvre est plus complexe. Le protocole TCP utilise un numéro de séquence pour gérer l’ordre des paquets. Ce numéro de séquence est généré aléatoirement. Si le pirate arrive à prédire ce numéro de séquence, il peut créer une séquence de paquets «autorisée» sans recevoir de réponse. Cette possibilité d’intrusion est décrite dans [MORRIS 85] mais n’avait jamais été mise en oeuvre jusqu’en décembre 94.

Niveau application - Chaque application possède un protocole de communication et une implantation spécifique, ainsi elle a ses propres trous de sécurité et les méthodes d’intrusion peuvent être très diversifiées.

Les applications réseaux fonctionnent sur le mode client-serveur. Le programme client, lancé sur la machine de l’utilisateur envoie des requêtes au serveur. Le serveur est un programme qui reçoit et interprète

les requêtes et fonctionne généralement en mode super-utilisateur. Le piratage consiste à détourner l'utilisation du programme serveur pour lui faire exécuter des programmes ou des commandes du *shell* autres que ceux prévus, dans le but de créer des autorisations d'accès.

Les mécanismes d'usurpation utilisés sont souvent de même nature, à savoir :

- le passage de paramètres à un programme interprété par un *shell*. Le principe est de passer à ce programme le paramètre demandé suivi du caractère «;» et d'une commande *unix* que l'on veut faire exécuter par le programme. Le *shell* appelé va alors interpréter la première commande, puis la deuxième non prévue par le serveur, le point virgule agissant comme séparateur de commande ;
- la provocation du débordement d'une pile ou d'un tampon. Dans ce cas, il s'agit d'exploiter l'oubli d'un test de débordement d'un tableau utilisé pour stocker un paramètre du programme exécuté.

  Le principe est de lancer ce programme avec en argument une chaîne de caractères de longueur supérieure à la dimension du tableau prévu pour la contenir [CIAC 95:02]. Ce tableau et la zone supplémentaire sont stockés dans la pile d'exécution ; cette zone supplémentaire reste au sommet de la pile et elle va être considérée comme l'adresse de retour de la dernière fonction appelée, généralement la fonction *strcpy*. L'exécution du programme se poursuit donc à cette pseudo-adresse de retour, à laquelle le pirate a implanté son propre programme.

Un exemple typique d'une application fréquemment attaquée est le démon *sendmail* qui assure l'acheminement du courrier électronique. Ce démon existe en de multiples implantations et est réputé pour ses trous de sécurité, même si ceux-ci sont cependant rapidement corrigés.

De nouvelles applications, comme les serveurs et les clients utilisant *WWW*, permettent le lancement de programmes interprétés ou compilés, ils introduisent de nouveaux types de trous de sécurité très difficiles à maîtriser car ils sont liés au type de l'application.

Pour contrer les attaques du réseau et se protéger au maximum des intrusions, il est primordial d'une part de posséder une bonne connaissance des systèmes et d'autre part de pouvoir obtenir très rapidement des informations, par exemple, par abonnement à des listes de diffusion[1], ou dans des forums de discussion électronique[2], ou encore par des organismes[3] centralisant les problèmes de sécurité [MICRO-BUL.

1 Traduction du terme anglais «mailing list». On peut citer, entre autres, les listes : Bugtraq (discussion sur la découverte de nouveaux trous de sécurité), Academic-Firewalls (discussion sur les pare-feux).

95].

Ceci permet de combler les trous de sécurité dans les plus brefs délais. C'est une opération inévitable mais elle est réalisée a posteriori. Il est donc indispensable de faire le maximum de protection de manière préventive. La sécurisation d'un site impose d'effectuer l'identification des risques et leur classification.

2. L'identification des risques et la protection mise en oeuvre

Toutes les attaques potentielles viennent du réseau de manière soit interne, soit externe.

Sécurité interne - Les personnes possédant un compte sur le réseau ont déjà une équivalence d'accès sur toutes les machines de notre site. La sécurité interne repose essentiellement sur une bonne information et sur une sensibilisation des utilisateurs aux problèmes de sécurité.

Sécurité externe - Les accès externes ont la particularité de passer par un point d'accès unique, ce qui facilite le filtrage des informations.

Le filtrage peut alors être effectué par un routeur ou/et par une station possédant deux interfaces. La figure 28 représente une telle configuration.

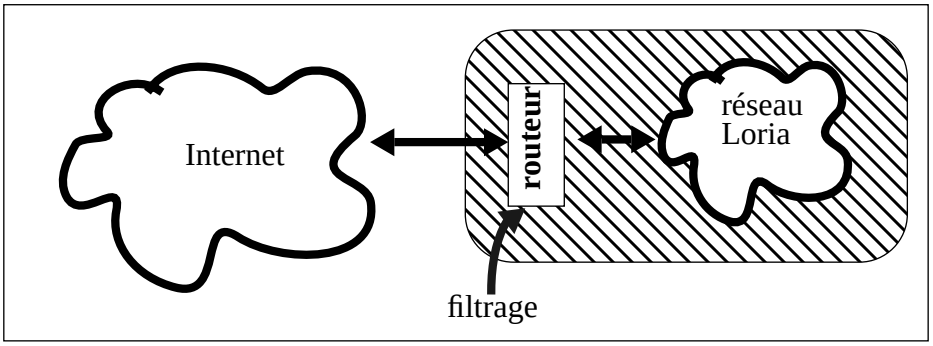


FIGURE 28. Le filtrage des services.

Parmi tous les services «ouverts» sur une station, certains s'avèrent nécessaires pour

2 Traduction du terme anglais «news». On trouve par exemple, les groupes «comp.security.unix», (général à la sécurité sous unix), «comp.security.misc» (question sur la sécurité en général), «alt.2600» (groupe de hackers).

3 CERT (Computer Emergency Response Team) Renater, CERT US, NIST.

le fonctionnement interne mais totalement inutiles pour les stations extérieures au réseau. C'est le cas, par exemple des services NIS ou NFS, dont l'accès doit être interdit à l'extérieur car ils comportent des trous de sécurité. NIS permet, par exemple, de diffuser le fichier des mots de passe codés, il offre ainsi la possibilité de casser ultérieurement un compte.

Une attaque extérieure peut donc se faire de deux manières différentes : soit en utilisant un compte et son mot de passe, soit en passant par un service et en détournant son utilisation. Examinons ces deux possibilités afin de présenter les protections que nous avons mises en place.

2.1. La connexion classique par un compte utilisateur

L'obtention d'un compte permet à son utilisateur de disposer d'un *shell* et donc d'effectuer la plupart des opérations de connexion comme tout utilisateur licite. La détection d'une telle usurpation d'identité n'est pas aisée et est souvent effectuée par la personne propriétaire du compte.

Voyons les différents moyens qu'un intrus peut utiliser pour usurper une identité et quels sont les moyens dont nous disposons pour le contrer.

Utiliser un compte sans mot de passe - Certains comptes, comme **sync** sous *SunOs4.x,* sont positionnés en standard sans mot de passe dans le fichier **passwd**. Leur fonction est généralement réduite, par exemple la connexion sous le compte **sync** provoque la synchronisation entre la mémoire et le disque d'une station *Unix,* mais elle peut être néanmoins exploitée pour s'introduire sur un réseau.

Il nous faut alors soit affecter un mot de passe à de tels comptes, soit les supprimer de notre site.

Obtenir un nom de compte utilisateur - Il est facile d'obtenir un nom de compte utilisateur dans la mesure où certains services comme *finger* fournissent la liste des noms de **login** des personnes connectées sur une station.

La solution pour se protéger est généralement de verrouiller de tels services. La suppression d'un service doit cependant s'accompagner d'une information à l'attention des utilisateurs, lesquels n'apprécient généralement pas une restriction de leurs outils de travail.

Une fois le nom de compte identifié, il est nécessaire d'obtenir le mot de passe associé à celui-ci, ce qui est tout à fait réalisable.

- **Obtenir un mot de passe en clair -** Il est possible d'obtenir un mot de passe non codé par divers moyens très simples comme le téléphone[1] ou plus complexe comme la connexion directe sur le réseau d'un dispositif électronique, généralement un micro-ordinateur, permettant de capter les trames[2] d'entête de session *telnet* ou de *rlogin*, ces trames contiennent le mot de passe de l'utilisateur.

  Il n'existe aucune parade directe à ce type de piratage, le premier cas nécessite de faire de la sensibilisation à la sécurité.

- **Obtenir un mot de passe crypté -** Il est facile d'obtenir le fichier des mots de passe cryptés par l'intermédiaire d'un service comme NIS, FTP ou TFTP. Il suffit ensuite d'utiliser un programme de type *crack* pour décoder les mots de passe. Un tel programme essaie de multiples combinaisons de cryptage à partir de plusieurs dictionnaires de mots usuels et opère par comparaison. Ainsi les mots de passe faibles, c'est-à-dire faisant référence à un prénom ou à un mot usuel de n'importe quelle langue dans le monde constituent une ouverture [CHESWICK 94].

  La prévention consiste à ne pas utiliser de mots de passe triviaux, c'est-à-dire composés de mots usuels. Plutôt que d'essayer de craquer les mots de passe de nos utilisateurs a posteriori afin de leur demander d'en changer, nous avons choisi d'effectuer cette vérification en amont. Lors du changement d'un mot de passe, un programme vérifie instantanément la non-trivialité du mot de passe directement sur la chaîne de caractères en clair qui vient d'être saisie au clavier.

  L'installation de cette fonctionnalité nécessite plusieurs éléments :

  - les sources d'un programme *passwd*[3],
  - une fonction qui effectue des vérifications : syntaxiques à partir de règles et combinatoires à partir de listes de mots,[4]
  - un maximum de listes de mots de tous les pays[5].

1 Ceci fait référence à des moyens pratiqués pour le piratage de carte bancaire : on téléphone au propriétaire de la carte en se faisant passer pour une autorité et on lui demande son code pour, par exemple, une opération de vérification.

2 Seuls les 128 premiers octets de ces trames sont conservés, réduisant ainsi le volume nécessaire au stockage.

3 *passwd+* ou *npasswd* : ces programmes proviennent des sites suivants : *dartmouth.edu* :*pub/passwd+.tar.Z* ou *ftp.lirmm.fr:/pub/LIRMM/comp/security.*

4 Cette fonction *facist_check* existe dans le logiciel «cracklib» disponible sur b*lack.ox.ac.uk:src/security/cracklib25.tar.Z.*

5 On trouve de nombreuses listes sur les sites suivants : *ftp.denet.dk:/pub/wordlists* ou *black.ox.ac.uk:/wordlists*.

Ce mécanisme permet d'obtenir des mots de passe assez robustes et a été généralisé sur l'ensemble du réseau. La commande *passwd* d'origine est systématiquement supprimée lors de l'installation d'une nouvelle station et est remplacée par la commande *passwd* sécurisée.

2.2. L'intrusion par un service

Les intrusions sur le réseau peuvent bien sûr se produire via un service externe, mais aussi par l'intermédiaire d'un service interne dans la mesure où les services internes sont par défaut ouverts à l'extérieur.

Sécuriser le site consiste donc à étudier les mécanismes permettant de verrouiller les services internes et à protéger les services externes, comme nous le montrons plus en détails dans ce qui suit.

Les services internes

L'objectif de l'intrus est d'obtenir des droits d'accès ou de se créer un compte sur un système en faisant exécuter des commandes par l'intermédiaire d'un service donné.

Les services du réseau [CHESWICK 94] peuvent être classés en trois catégories :

- les services qui n'ont pas d'utilité directe pour le site de manière interne ou externe. Généralement, le système d'exploitation d'une station est livré avec une vingtaine de services actifs de base. Il est important de fermer ces services car ils représentent des trous potentiels ;
- les services utilisant un numéro de port fixe défini dans le RFC1700, ces numéros de port sont appelés «well known port». Ces services peuvent être verrouillés ou filtrés par un routeur, lequel possède en général des fonctions de filtrage. Le filtrage se fait par autorisation ou interdiction sur les champs adresse, protocole et numéro de port.

  Ce mécanisme de protection est le plus radical et le moins coûteux, même si les routeurs sont complexes à programmer et s'ils présentent des limitations. Le routeur peut être considéré comme effectuant un service de filtrage fiable, si sa programmation est bien vérifiée et testée [CHAPMAN 92].

  De cette façon, nous avons protégé tout accès aux services comme SNMP, SYSLOG, TFTP et NFS et nous avons restreint l'accès à certains services comme le courrier électronique qui n'est autorisé que sur le serveur du courrier électronique du site.

Un exemple de configuration utilisé sur nos routeurs est détaillé à l'annexe D ;

- les services utilisant les procédures d'appel distante. L'accès se fait par l'intermédiaire d'un programme en attente sur le port fixe 111, généralement nommé *portmap*, qui donne des renseignements sur les services RPC offerts par la station.

  Ces services utilisent des numéros de port aléatoire, dans une tranche définie, c'est le cas par exemple de NIS avec le démon *ypserv*. Il n'est donc pas possible d'effectuer un filtrage par programmation des routeurs puisque le numéro de port utilisé n'est pas connu. La protection doit s'effectuer de manière logicielle sur la station, ce qui implique qu'elle soit prévue par le constructeur ou ajoutée par un mécanisme de correction provisoire.

Les services ouverts vers l'extérieur

Lorsqu'un service est ouvert aux utilisateurs extérieurs au réseau, il est primordial d'en utiliser les versions de démons les plus récentes, correspondant généralement aux versions les mieux protégées.

Les deux services les plus sensibles et les plus réputés pour leurs trous de sécurité sont :

- *sendmail* : programme de réception et de routage du courrier électronique,
- *ftp* : programme permettant le transfert de fichiers entre machines.

La sécurisation de ces deux programmes est identique et consiste à remplacer les versions constructeurs par les versions du domaine public, lesquelles possèdent les avantages suivants :

- la disponibilité très rapide des programmes sources mises à jour suite à la découverte et à la correction d'un trou de sécurité,
- l'utilisation d'une version unifiée pour la majorité des systèmes d'exploitation.

Plus généralement, je pense que la lutte contre les intrusions consiste à implanter uniquement les programmes sensibles dont on possède les sources et qui ont été écrits avec un réel souci de sécurité.

3. Les moyens utilisés pour tester ou valider les configurations

Nous venons de présenter les principaux trous de sécurité existants dans un réseau et les protections que nous avons mises en place pour contrer les intrusions. Pour valider et/ou conforter ces protections, nous devons les tester et donc essayer de s'introduire illégalement sur notre propre réseau.

Les tests concernant la validité de connexion sur un port donné sont généralement effectués à partir de machines connectées sur un réseau tiers. Il existe dans le domaine public des programmes qui permettent de tester l'efficacité des protections mises en place. Il y a ceux qui testent un service spécifique et ses failles et ceux, plus généraux, qui permettent le test de l'ensemble des services. Analysons ces deux types de programmes que nous utilisons sur notre site.

3.1. Les programmes faisant appel à un service distant spécifique

Ces programmes permettent de tester les accès et les failles de sécurité d'un service donné. Sur notre site, nous utilisons deux programmes qui testent respectivement les services NFS et NIS.

Les services NFS

Le programme *nfsbug* permet d'une part en interne, de tester les mauvaises configurations ou les oublis, et d'autre part en externe, de valider les restrictions d'accès vis-à-vis de l'extérieur. Ce programme est lancé avec en paramètre le nom de la machine serveur NFS que l'on veut tester, il tente d'établir une connexion avec les démons qui effectuent les montages (*mountd*) et il dialogue avec *nfsd*.

Dans l'exemple suivant, nous avons effectué un test depuis le réseau Loria de l'antenne Inria de Metz sur le réseau Loria de Nancy. Nous pouvons constater que les accès aux démons sont autorisés et que les accès aux partitions sont bien restreints. Un accès à partir d'un autre site ne donne aucune réponse car les accès à ce service sont verrouillés au niveau du routeur.

Voici un exemple d'information fourni par *nfsbug* :

```
./nfsbug -v ilm
Connected to NFS mount daemon at ilm.loria.fr using TCP/IP
Connected to NFS server at ilm.loria.fr using UDP/IP
Failed: /global/bin: Permission denied
Failed: /global/doc: Permission denied
Failed: /var/spool/mail: Permission denied
Failed: /u/sagep: Permission denied
```

Les services NIS

Le programme *ypx* permet de se connecter au démon *ypserv* gérant les requêtes NIS d'une machine serveur. Ses fonctionnalités permettent d'obtenir le nom de domaine NIS qui est indispensable pour ensuite récupérer les cartes contenant des informations locales au réseau [CERT 92:13]. La carte la plus intéressante pour effectuer une intrusion est la carte **passwd.byname** qui contient les noms de compte et leurs mots de passe codés associés. Le résultat de ce programme permet de tester que les mécanismes mis en place sont valides.

3.2. Les programmes plus généraux

Ces programmes permettant de tester l'ensemble du réseau sont appelés «scanner». De tels programmes vont, pour chaque adresse IP d'une plage préalablement définie, scruter tous les ports, de type UDP ou TCP, du numéro 0 au numéro 32000. Le programme le plus connu est *iss*[1], mais il existe d'autres programmes fonctionnant sur le même modèle dont le plus récent et le plus médiatique est SATAN[2]. Ces programmes permettent de vérifier avec exactitude que les actions de limitation des services sont effectives.

La commande lancée dans l'exemple suivant est la scrutation de la machine d'adresse IP 152.81.1.17. Elle effectue la scrutation de tous les ports TCP et UDP de la machine citée. Le résultat indique l'ensemble des services réseaux qui sont ouverts ou accessibles sur cette machine. Dans l'exemple suivant, nous constatons que les services *echo* et *discard* sont ouverts sur ce serveur ; ce sont des services ayant des ports fixes. Il existe également d'autres services accessibles, comme celui sur le port 653, mais ceux-ci ne peuvent pas être identifiés par l'outil *iss*.

1 «Internet Security Scanner», disponible par : ftp ftp.iss.net:/pub/iss

2 «Security Administrator Tool for Analyzing Networks», SATAN est un programme destiné aux administrateurs pour l'amélioration de la sécurité d'un site.

```
iss -p 152.81.1.17 152.81.1.17
   -->  Inet Sec Scanner Log By Christopher Klaus (C) 1995    <-
              Email: cklaus@iss.net Web: http://iss.net/iss
============================================================
Host 152.81.1.17, Port 7  ("echo" service) opened.
Host 152.81.1.17, Port 9  ("discard" service) opened.
Host 152.81.1.17, Port 13  ("daytime" service) opened.
Host 152.81.1.17, Port 19  ("chargen" service) opened.
Host 152.81.1.17, Port 21  ("ftp" service) opened.
Host 152.81.1.17, Port 23  ("telnet" service) opened.
Host 152.81.1.17, Port 25  ("smtp" service) opened.
Host 152.81.1.17, Port 37  ("time" service) opened.
Host 152.81.1.17, Port 53  ("domain" service) opened.
Host 152.81.1.17, Port 110  ("pop" service) opened.
Host 152.81.1.17, Port 111  ("sunrpc" service) opened.
Host 152.81.1.17, Port 513  ("login" service) opened.
Host 152.81.1.17, Port 514  ("shell" service) opened.
Host 152.81.1.17, Port 515  ("printer" service) opened.
Host 152.81.1.17, Port 602  ("dsvd" service) opened.
Host 152.81.1.17, Port 653 opened.
Host 152.81.1.17, Port 848 opened.
```

Une des caractéristiques de la sécurité d'un site est que celle-ci se dégrade avec le temps. En effet, l'arrivée de nouvelles machines et surtout de nouveaux logiciels ou de leurs mises à jour remet systématiquement en cause les protections que nous avons implantées sur notre site. Aussi, nous devons être particulièrement vigilants et exécuter périodiquement les tests que nous venons de décrire.

Conclusion

Nous venons de présenter les différentes protections que nous avons implantées pour contrer les attaques de notre site. Parmi celles-ci, j'ai personnellement réalisé l'étude et l'implantation des filtres sur les routeurs et la mise en place du contrôle a priori des mots de passe. J'ai actuellement la fonction de responsable sécurité informatique de l'Inria Lorraine du site et je travaille à ce titre directement avec le responsable sécurité du CRIN/CNRS en ce qui concerne l'approche globale de la sécurité du site.

L'aspect sécurité est intimement lié au réseau et le fait que celui-ci ait été bien structuré a fortement aidé à la mise en oeuvre de la sécurité. Par exemple, l'isolation d'un segment par un routeur a autorisé l'installation de listes d'accès, ces listes d'accès ont également permis l'isolation des applications confidentielles pour les services administratifs. Le découpage en segments a facilité la séparation des machines très sollicitées par l'extérieur comme celles supportant les serveurs FTP et WWW. Elles ont été installées sur un brin qui leur est dédié.

Les pare-feux n'ont volontairement pas été évoqués dans ce chapitre. L'installation d'un pare-feu nécessite une restriction drastique du nombre des services offerts sur les stations, en particulier, seuls sont conservés les services TCP qui fonctionnent en mode connexion et qui sont ainsi plus sécurisés [CHAPMAN 95]. Cette solution,

même si elle apporte un renforcement de la sécurité, peut difficilement être mise en oeuvre dans un laboratoire de recherche au regard des nombreux besoins des utilisateurs. En revanche, elle peut servir de modèle et nous devons être prêts à la mettre en oeuvre si cela devenait nécessaire.

Conclusion et perspectives

Cette dernière partie se propose de dresser un bilan de la conception et de l'implantation d'un réseau informatique et de présenter les adaptations que nous avons réalisées afin de prendre en compte les évolutions matérielles et logicielles qui sont intervenues. Nous avons créé d'autres sous-réseaux et réglés des problèmes de charge réseau pour répondre à l'arrivée de machines à architecture parallèle et à la demande de bande passante des applications multimedia.

Le travail actuel consiste en une veille technologique importante tant dans les domaine de la sécurité que dans celui des nouvelles technologies.

1. Les adaptations réalisées

Le nouveau réseau Loria, fusion des deux réseaux crin.fr et inria-lorraine.fr, a été mis en service en 1992. Depuis cette date, le site a considérablement évolué, notamment lors de ces deux dernières années. Les modifications ont portées d'une part sur le matériel et d'autre part sur les logiciels :

le matériel : le nombre de noeuds connectés sur le réseau, stations de travail, terminaux X, Macintoshs, PCs, routeurs, concentrateurs et imprimantes, a plus que doublé ; il est passé de 227 en avril 92 à 618 en septembre 95;

les logiciels : de nombreux services, consommateurs en bande passante, sont arrivés. On peut citer spécialement la généralisation du mode de transmission en mode de diffusion restreinte ou *multicast*[1] qui permet la diffusion à un groupe d'adresses, d'images animées et de son. Les visioconférences utilisent ce mécanisme. La difficulté provient des équipements qui ne gèrent pas bien encore ce mode de transmission et qui diffusent l'information sur l'ensemble du réseau. Ainsi, même les sous-réseaux non concernés par les messages, supportent ces trames à diffusion restreinte.

Ces deux facteurs ont provoqué une importante augmentation du trafic sur le réseau

1 Le terme *multicast* caractérise un seul envoi de message vers un groupe de destinataires identifiés et multiples.

mais celui-ci reste cependant de manière générale en-dessous des seuils acceptables, c'est-à-dire avec un taux de collision inférieur à 10%.

Nous pouvons surtout mettre l'accent sur le fait que depuis son implantation et sa structuration en 1992, l'architecture du réseau Loria est restée identique à son état initial, soit un réseau en étoile, segmenté en plusieurs sous-réseaux reliés entre eux par l'intermédiaire de deux routeurs, chaque brin desservant un groupe de stations d'un ou plusieurs projets/équipes.

Cette architecture a donc bien accepté et également facilité les modifications matérielles et logicielles du réseau nécessaires à l'évolution du site alors que celle-ci n'est pas forcément parfaitement connue**.**

Certaines modifications ont cependant été réalisées pour s'adapter à l'augmentation constante du trafic, aux évolutions technologiques et aux nouvelles contraintes du site.

Nous présentons ci-après ces modifications qui concernent l'extension des sous-réseaux, la maîtrise du trafic réseau et le regroupement des exécutables.

1.1. Les nouveaux sous-réseaux

Rappelons que le réseau comportait 12 sous-réseaux lors de sa création. Cependant, certaines modifications intervenues sur le site nous ont conduit à créer quatre nouveaux sous-réseaux :

- les Macintoshs des services administratifs du CRIN ont été connectés à ethernet, ce qui permet d'offrir un meilleur service grâce à une vitesse réseau plus élevée que celle de l'ancien réseau utilisé, Appletalk. Ce sous-réseau, tout comme celui regroupant les stations des services administratifs de l'Inria Lorraine, est équipé de concentrateurs filtrant les adresses, assurant ainsi une meilleure sécurité ;
- les Macintoshs et des PCs des équipes de recherche du site Loria ont été regroupés sur un même brin spécifique dans un souci d'isolement du trafic des autres brins. L'objectif est de ne pas permettre à ces micro-ordinateurs de pouvoir observer et décoder les trames transitant sur les autres sous-réseaux ;
- l'arrivée prochaine d'une machine parallèle et l'implantation d'une grappe de stations de travail rapides dans le cadre de la création du Centre Charles Hermite[1] ont conduit à la création d'un sous-réseau spécifique ;

- un brin est réservé aux participants des colloques organisés dans nos locaux ; il sert à la connexion rapide et temporaire de stations destinées généralement à des personnes externes au laboratoire.

Ces nouveaux accès ont été ouverts en janvier 95 et ont consisté en l'ajout d'une carte de quatre ports ethernet dans l'un des deux routeurs. Cette installation représente en réalité une extension et n'a rien changé à la structure du réseau.

Le réseau Loria comporte donc à ce jour 16 sous-réseaux et peut tout naturellement être étendu à nouveau très facilement pour s'adapter aux nouveaux besoins du centre de recherche.

1.2. La charge réseau sur les segments

L'augmentation globale du trafic sur le réseau Loria n'a actuellement pas provoqué de congestion réseau sauf en ce qui concerne le brin d'une équipe. Ce segment est celui qui comprend le plus grand nombre de stations du réseau Loria, actuellement 91 adresses. De plus, cette équipe travaille dans le domaine de la parole et manipule de volumineux fichiers de données, provoquant un trafic NFS beaucoup plus important que d'autres équipes.

Pour éviter une segmentation logique sur les adresses IP, c'est-à-dire pour ne pas créer plusieurs sous-réseaux, nous avons décidé d'utiliser une technique «physique». Cette façon de procéder évite l'identification de sous-groupes, la renumérotation des machines et la fragmentation des ressources communes. Le principe retenu a été celui de la commutation des trames ethernet qui permet de garder la visibilité d'un groupe de machines utilisant les mêmes ressources et de décongestionner un réseau sans modifier sa structure. C'est un commutateur ethernet *Catalyst* de la société *Cisco* qui a été mis en place. Ce commutateur a la particularité de pouvoir offrir une interface FDDI permettant ainsi un accès haut débit, de l'ordre de 100Mb/s, à un ou plusieurs serveurs.

Le principe de fonctionnement du commutateur est le suivant :

> Tous les paquets émis par la station connectée à un port du commutateur, sont examinés. Le commutateur analyse les adresses source et destination des paquets et ouvre un circuit dédié par un mécanisme de commutation du port source vers le port destination.

1 Le Centre Charles Hermite regroupe les compétences en informatique et mathématiques pour la simulation et le calcul intensif en Lorraine et possède comme plate-forme matérielle une grappe de stations HP interconnectées par un réseau haut débit ATM.

Le traitement du paquet est effectué soit dès réception du début du paquet, c'est la technique dite au vol, soit lorsque le paquet est entièrement reçu.

La figure 29 illustre le fonctionnement du commutateur.

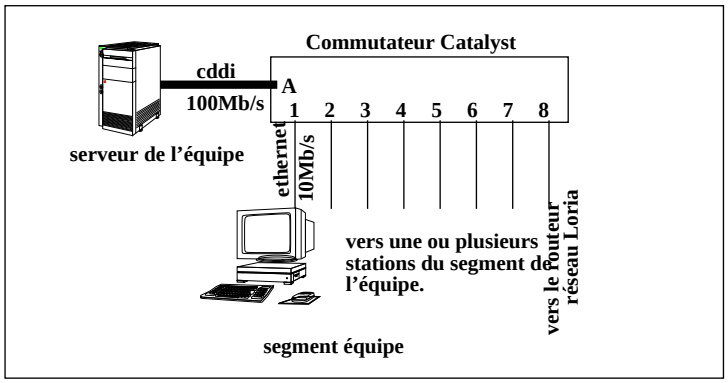


FIGURE 29. Eclatement d'un segment du réseau par un commutateur.

Ainsi le trafic entre le port A et le port 1 sera commuté et ne sera pas distribué sur les autres ports. Dans le cas du *Catalyst*, chaque port est affecté à un réseau local. Le commutateur possède en standard pour son administration un agent SNMP supportant la MIB-II.

1.3. Les exécutables

Enfin la dernière évolution concerne le regroupement des exécutables sur une seule machine pour desservir l'ensemble des sous-réseaux.

Dans la situation initiale, chaque serveur d'équipe avait son propre serveur d' exécutables. Cependant, cette solution était devenue lourde et coûteuse du fait de l'augmentation de la taille et du nombre des exécutables ainsi que de l'ajout de nouvelles architectures systèmes comme *Irix* ou *Solaris*. En deux ans, la taille de l'ensemble des exécutables est passée de 800 Méga-octets à 2 Giga-octets. De plus, ce volume est multiplié par le nombre de serveurs, soit une dizaine.

Nous avons mis en place un serveur NFS unique d'exécutables pour tout le site Loria. Ce serveur est une station sparc20/61 sous *Solaris 2.4* avec actuellement dix sorties ethernet connectées directement sur les sous-réseaux. L'accès à ce serveur est strictement restreint au service NFS.

Une configuration identique à celle du serveur d'exécutables a été mise en place pour des

raisons de continuité de fonctionnement en cas de panne.

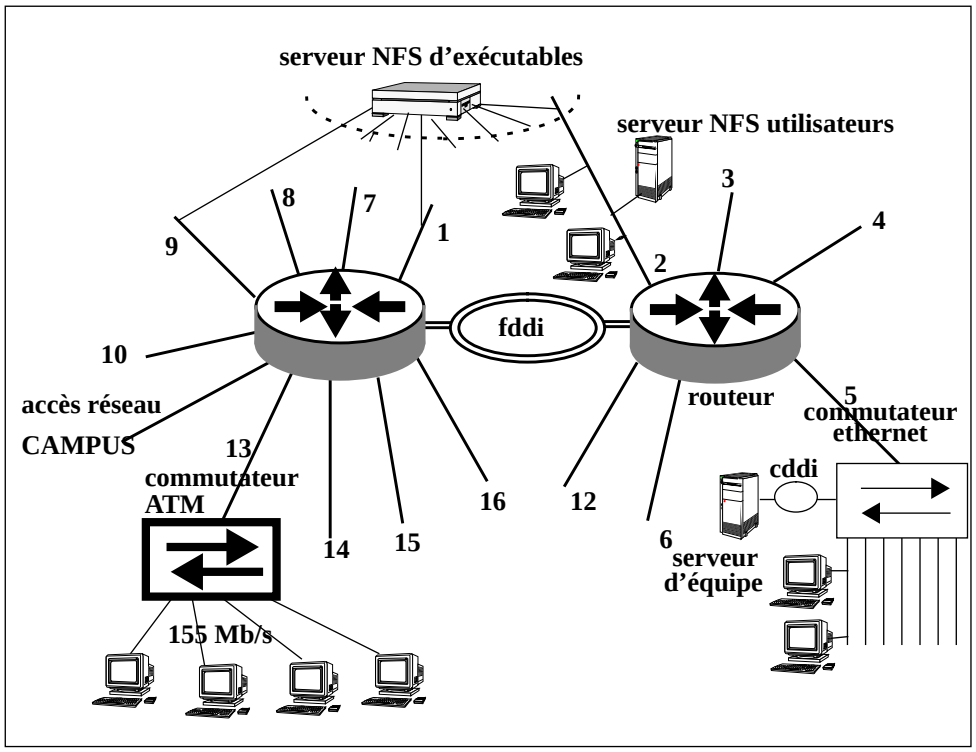


FIGURE 30. L'architecture du réseau Loria en 1995.

2. Les évolutions futures

La création du réseau Loria est une opération qui a pris plus d'une dizaine de mois. Dans cette opération, on peut dissocier d'un part la partie câblage et d'autre part la structure électronique du réseau. Le câblage est une opération qui doit avoir une durée de vie assez longue, de l'ordre d'une dizaine d'années. Les options que nous avons prises dans les choix permettent d'intégrer les évolutions futures. En revanche, les éléments qui forment la structure électronique, c'est-à-dire les routeurs, les concentrateurs, etc sont des matériels qui deviennent rapidement obsolètes. Leur durée de vie est de l'ordre de 5 ans.

Aujourd'hui, la bande passante du réseau n'est pas saturée, mais la généralisation de service consommateur comme le multimedia demande une infrastructure autorisant des débits plus élevés. La solution consistant à implanter des commutateurs ethernet permet de donner du souffle à un réseau et de fonctionner avec des débits soutenus. Des mesures effectuées sur le site avec des outils comme *netperf*[1] ont montré des débits supérieurs à 9Mb/s, ceux-ci sont très proches de la bande passante théorique.

L'étape suivante est l'utilisation de moyens de transport ayant un débit supérieur à 10 Mb/s. Ceux-ci existent, cependant ils ont soit d'importants inconvénients, comme une standardisation non finalisée des protocoles, soit des coûts trop élevés. Parmi ceux-ci on peut citer FDDI, les deux évolutions d'ethernet et ATM. Le protocole le plus ancien et sûrement le plus stable est FDDI. Les deux évolutions d'ethernet à 100 Mb/s sont le «100 base T» qui est l'évolution naturelle d'ethernet et qui conserve un fonctionnement indéterministe et le 100VG Anylan d'origine *Hewlett Packard* qui utilise quant à lui un mécanisme à jeton [FERRERO 95]. ATM permet actuellement des transferts à des vitesses de 100 ou 155 Mb/s mais il n'est pas, contrairement aux autres protocoles, lié à une vitesse fixe de transfert ; d'autres vitesses telles que le 622 Mb/s sont en cours de normalisation. Quelles que soient soit les technologies qui s'imposeront sur le marché, le réseau Loria est un réseau suffisamment structuré pour être prêt à recevoir une infrastructure réseau haut débit.

Avec les hauts débits apparaît la notion de groupe de travail virtuel. C'est une notion très intéressante car elle gomme le découpage ou la segmentation physique nécessaire pour des raisons de performance. La notion de sous-réseaux routés peut alors disparaître. Elle restera toutefois nécessaire pour la liaison avec les réseaux extérieurs et sûrement aussi pour les services administratifs dans le cadre de la sécurité.

En réalité, la technologie marque encore trop son empreinte dans la structuration du réseau telle qu'elle a été conçue en 1992. Les évolutions vers un réseau virtuel permettront une adéquation plus forte avec la structure administrative. Dans ce nouveau schéma, l'architecture du réseau actuel devient obsolète car trop figée. Une station possède une adresse donnée fixe et associée de façon statique à un réseau, lequel possède lui-même une bande passante fixe et non garantie. Dans le futur, chaque station devra être capable de se connecter, éventuellement temporairement, sur n'importe quel réseau dans le monde et de fonctionner immédiatement, sans avoir à gérer manuellement des problèmes d'adressage. L'augmentation massive de machines portables qui doivent être immédiatement opérationnelles lorsqu'elles sont connectées sur un réseau, nécessitent que leur intégration soit prise en compte.

La conception et l'implantation du réseau informatique du site Loria sont des opérations qui ont été pleinement réussies. De plus, le réseau est suffisamment évolutif pour accepter les nouvelles technologies.

Le travail actuel consiste à assurer la maintenance journalière de ce réseau, tant au niveau des petits problèmes de fonctionnement qu'au niveau de la sécurité. Il est également indispensable d'effectuer une veille technologique afin que le réseau continue a évolué et garantissent aux utilisateurs un cadre travail performant et adapté à leurs besoins.

1 Programme de mesure de performance de transfert de données sous UDP ou TCP entre deux équipements.

Annexe A : Changement d'adresse IP

Cette annexe décrit les scripts qui ont été utilisés pour effectuer les modifications des adresses IP durant deux phases : la préparation avant le jour J des modifications et le changement des adresses le jour J des modifications.

1. Déroulement des opérations effectuées avant le jour J

- Création de la table de correspondance entre les anciennes et les nouvelles adresses IP. A partir de cette table nous avons créé un fichier d'ordres destiné à être interprété par la commande de filtrage Unix *sed*. *Sed* est utilisé pour effectuer les remplacements de chaîne de caractères.
- Sur chaque station du réseau, on lance l'exécution d'un script «modif.sh» qui va créer des nouveaux fichiers systèmes avec l'extension B.

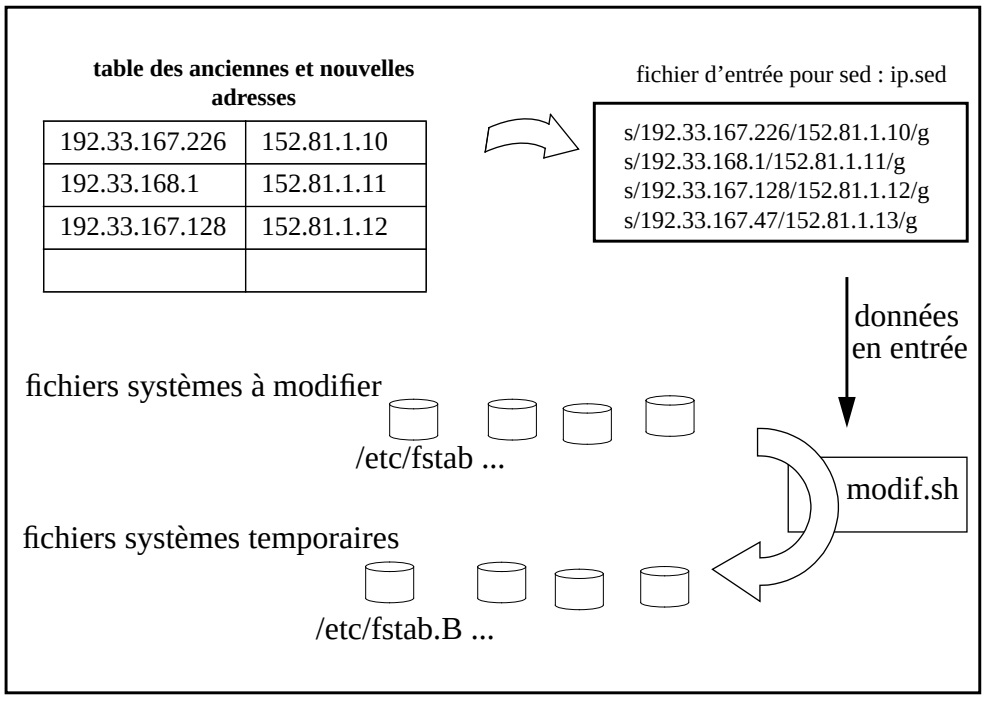


FIGURE 31. Création des nouveaux fichiers sur une station.

Contenu du script *modif.sh* :

```
/bin/rm /etc/*\.B
/bin/rm /\.rhosts\.B
# modification du .rhosts
sed -f /local/sys/B/ip.sed < /.rhosts > /.rhosts.B
# modification des fichiers systèmes de /etc
for fichier in hosts defaultrouteur fstab exports rc.custom syslog.conf alia-
ses
sed -f /local/sys/B/ip.sed < /etc/$fichier  > /etc/$fichier.B
# pour les sony
if test -f /etc/rc.custom
then
sed -f /local/sys/B/ip.sed < /etc/rc.custom  /etc/rc.custom.B
fi
echo hostname
# modification du nom qualifié : crin.fr -> loria.fr
IFS="$IFS."
set `echo /etc/hostname\.*`
sed 's/.crin.fr/.loria.fr/g' < /etc/hostname.$2 > /etc/hostname.${2}.B
#  modification  du  broadcast  pour  les  Sun  :  broadcast  de  classe  B
152.81.255.255
sed  -e "/^broadcast=/c\\
broadcast=\`fgrep \$a /etc/hosts | cut -f1-2 -d.\`.255.255 " < /etc/rc.local
> /etc/rc.local.B
```

L’exécution de ce script sur l’ensemble des machines a été lancé par un outil développé en local par l’équipe système, cet outil s’assure que les modifications ont bien été faites.

2. Opérations de modifications le jour J

Le principe est de copier les fichiers systèmes des anciens réseaux dans des nouveaux fichiers avec l’extension C et de renommer les fichiers ayant l’extension B en supprimant leur extension. Ces derniers deviennent alors les nouveaux fichiers de configuration du système.

contenu du script *move.sh* qui effectue le déplacement de fichiers :

```
# copie des fichiers originaux en .C
# remplacement par les fichier.B
#
cd /etc
for i in *.B
         do
         fichier=`expr match $i '\(.*\).B'`
         cp $fichier ${fichier}.C
         cp ${fichier}.B $fichier
         echo $fichier
done
cd /
for i in .*.B
do
```

```
        fichier=`expr match $i '\(.*\).B'`
        cp $fichier ${fichier}.C
        cp ${fichier}.B $fichier
        echo $fichier
done
```

Une fois les modifications réalisées, le nouveau serveur NIS a été mis en place et toutes les stations ont été réinitialisées avec le programme local.

Annexe B : Exemples de tables de montage AMD

Voyons tout d'abord un exemple de montage des répertoires **/usr/local/bin :**

```
/defaults   opts:=rw,intr,grpid,soft;type:=nfs;
                  rfs:=/global/bin${arch}${key};
                  fs:=/global/bin/${arch}/${key}

         bin     -type:=link \
                  host==salm || \
                  -type:=nfs;fs:=${autodir}/${rhost}${path};
                  rfs:=/global/bin/${key} \
                  rhost:=salm \
```

Ce mécanisme de montage est utilisé pour tous les types d'exécutables et permet ainsi de donner une vision homogène des partitions depuis n'importe quelle station du réseau. Sur la figure 32 est représentée la succession d'opérations lancée par *amd* lors d'un accès au répertoire **/usr/local/bin**. Lors de l'accès à une partition, *amd* vérifie si celle-ci est déjà montée, dans ce cas l'utilisateur peut accéder directement à sa partition. Dans le cas contraire, *amd* crée le répertoire sur la machine cliente (1), lance l'opération de montage (2) sur un répertoire

intermédiaire (géré seulement par *amd*) et enfin crée un lien symbolique (3) qui rend disponible l'accès de la partition à l'utilisateur.

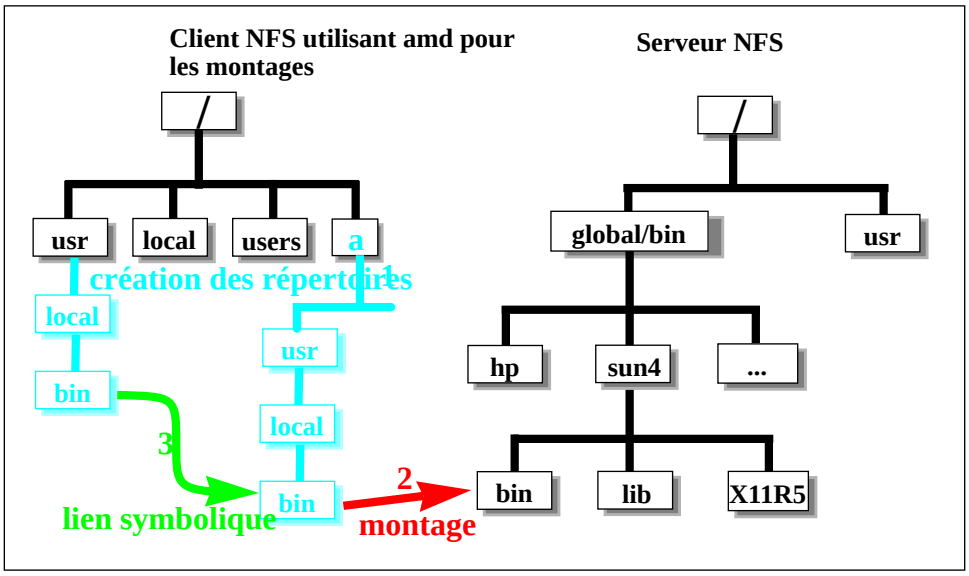


FIGURE 32. Séquence des opérations lors du montage d'une partition NFS par

L'outil *amd* dispose d'un sélecteur nommé *cluster*. Ce sélecteur est un paramètre transmis au démon *amd* lors de son démarrage, il permet d'effectuer des montages conditionnels sur des grappes de stations préalablement définies.

Ce mécanisme de *cluster* est largement utilisé, en particulier pour les montages d'exécutables. Le principe est le suivant : le sélecteur *cluster* est positionné au nom de l'équipe à laquelle la station est attachée. Le montage du serveur local au brin, ou le plus proche, va s'effectuer par cette sélection.

La figure 33 représente deux segments du réseau Loria ainsi que les grappes qui leurs sont associées.

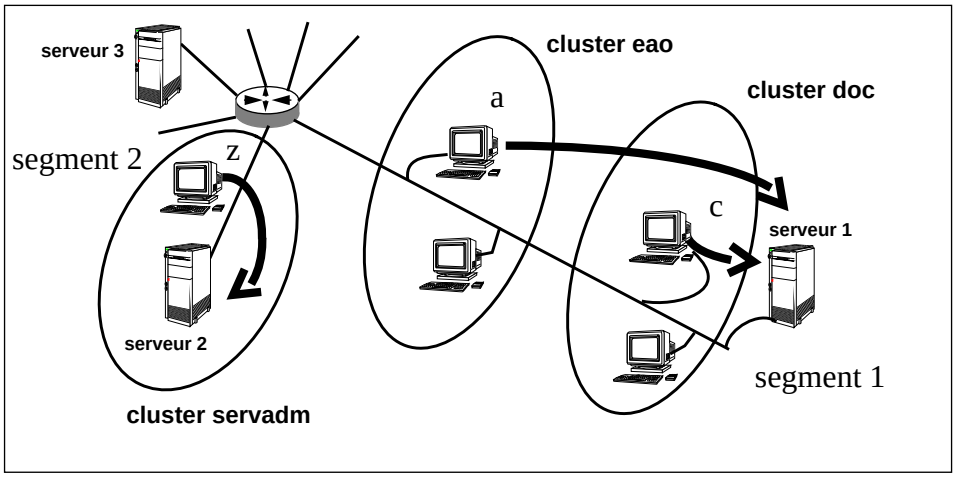


FIGURE 33. Les montages à la demande par le sélecteur cluster de l'outil amd.

La machine «a» appartient à l'équipe *eao*, la machine «z» appartient aux services administratifs. Pour ces deux machines le répertoire des exécutables est **/usr/local/bin** mais leur serveur NFS respectif est différencié par le *cluster*. De plus, deux *clusters* appartenant au même segment peuvent utiliser le même serveur NFS.

Lorsqu'un utilisateur souhaite accéder au répertoire **/usr/local/bin**, le démon *amd* exécute l'algorithme suivant :

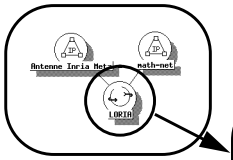
```
si hote = serveur1 ou serveur 2
alors création d'un lien de /usr/local/bin sur /global/bin/$ARCH/bin
    si cluster = doc ou cluster = eao
    alors   si serveur1 est actif alors montage NFS de la partition
              /global/bin/$ARCH/bin de la machine serveur1 sur le répertoire
              /usr/local/bin
    si cluster=servadm
    alors   si serveur2 est actif alors montage NFS de la partition
              /global/bin/$ARCH/bin de la machine serveur1 sur le répertoire
              /usr/local/bin
    sinon si le serveur3 est actif alors montage de la partition NFS de server3.
```

La carte *amd* est la suivante :

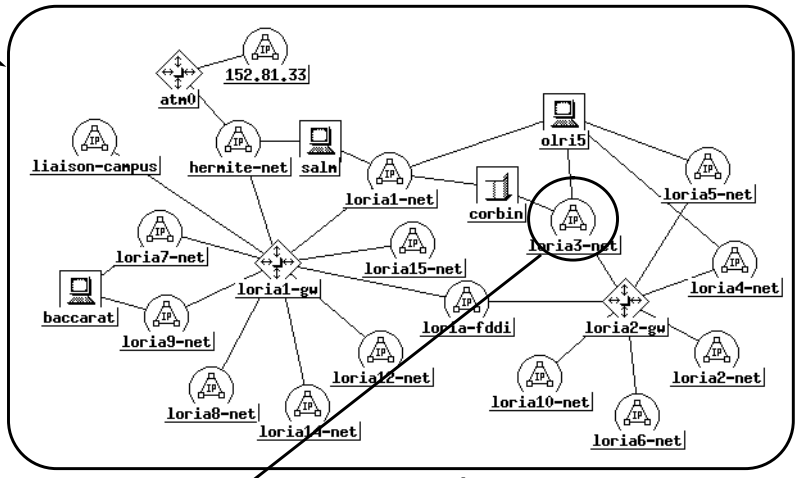
```
bin     -type:=link \
         host==serveur1 || host==serveur2 || host ==serveur3\
         -type:=nfs;fs:=${autodir}/${rhost}${path};
         rfs:=/global/bin/${key} \
         cluster==doc; rhost=serveur1 \
         cluster==eao; rhost=serveur1 \
         cluter==servadm; rhost=serveur2 \
```

Annexe C : Openview

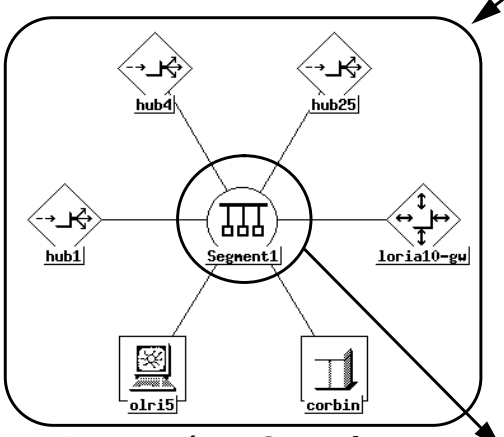
1- Visualisation graphique du réseau Loria par Openview.



Les trois réseaux Loria Nancy, Loria Metz et le Département de Mathématiques

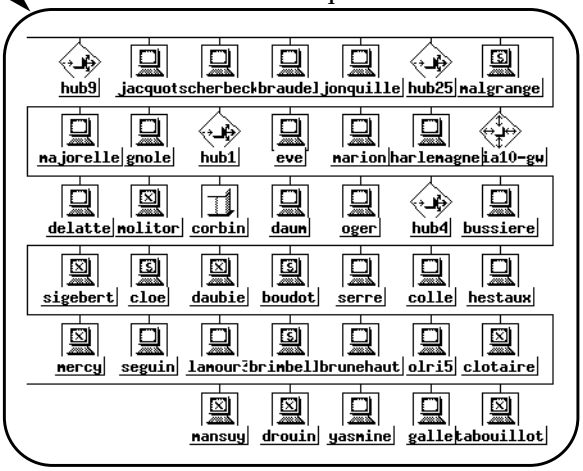


Le réseau IP Loria



Le sous-réseau 3 avec les équipements d'interconnexion

Le sous-réseau 3 avec tous les médias électroniques connectés



Les figures suivantes représentent les différents niveaux visualisés par Openview. Ces schémas sont organisés de façon arborescente, il suffit de sélectionner un noeud avec la souris pour visualiser son contenu. Cet exemple permet de montrer les différents types d'icones disponibles.

2- Exemples de mesures réalisées à l'aide d'Openview.

Les deux graphiques utilisent des données collectées par des requêtes SNMP sur les équipements. La représentation graphique des données est effectuée également par *Openview.*

Le premier graphique (figure 34) représente le trafic de la liaison entre le réseau Loria et l'Internet sur une période de deux semaines. Les trois courbes représentent respectivement les protocoles TCP, UDP et le dernier regroupe les protocoles IGRP et «IP encapsulé». L'objectif de ces courbes est de visualiser l'importance du trafic concernant les visioconférences qui utilisent les protocoles IGRP et l'«IP encapsulé». Nous constatons également que le trafic est principalement de type connecté (TCP) et que le trafic utilisant le protocole UDP est très faible.

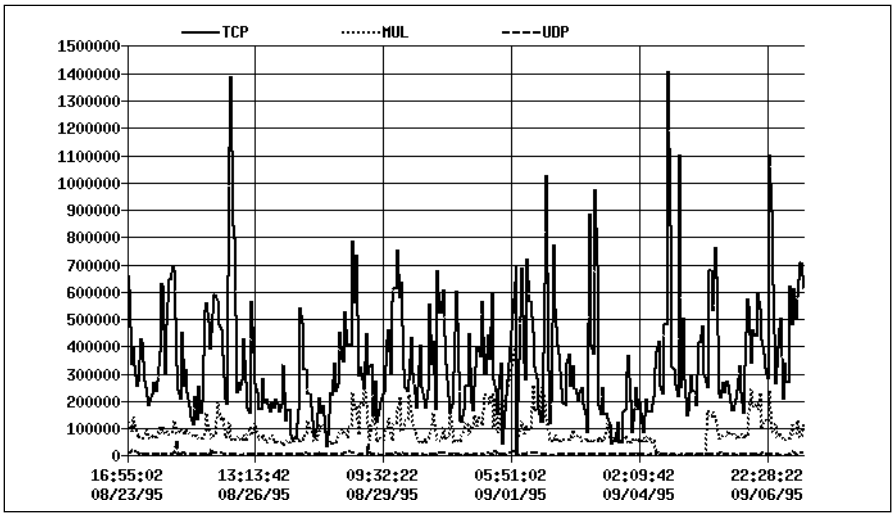


FIGURE 34. Le trafic en nombre d'octets sur le segment de liaison à Internet.

Le deuxième schéma (figure 35) représente le trafic d'un sous-réseau sur une période de 24 heures avec pour objectif de vérifier que la charge réseau n'est pas trop élevée et ainsi que le nombre de collisions reste faible. On constate que le taux de collision est normal et donc que le fonctionnement global de ce sous-réseau est satisfaisant. La courbe illustre bien le fait que la charge d'un réseau n'est jamais constante et que le réseau doit absorber des pointes importantes en terme de trafic.

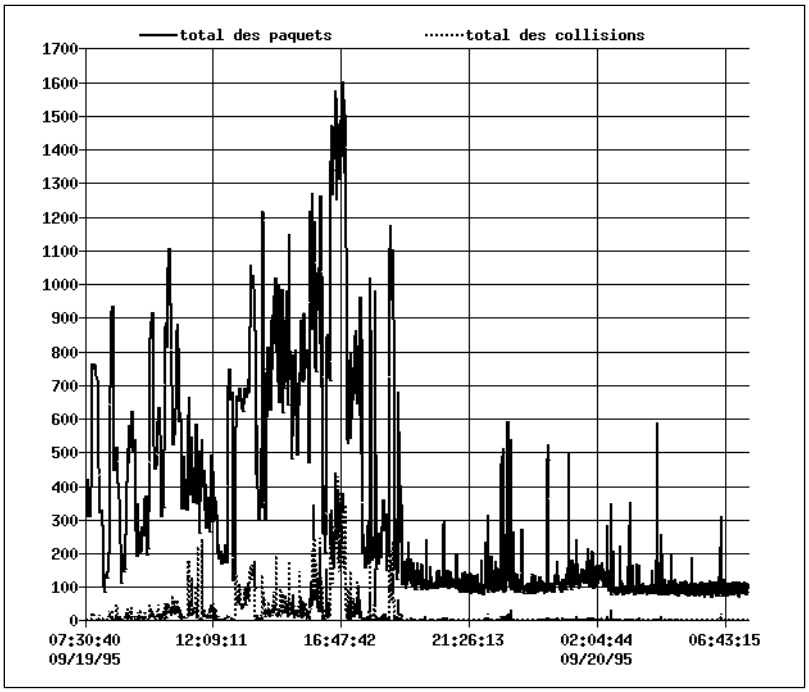


FIGURE 35. Trafic en nombre de paquets d'un sous-réseau

Annexe D : Programmation des listes d'accès

Le filtrage des informations par un routeur permet d'accepter ou de refuser l'accès à une machine ou à un réseau par une autre machine ou un autre réseau. Les paquets entrants et sortants sont analysés par le routeur auquel on a précisé les droits par des règles d'accès. Ces règles sont décrites dans un langage de programmation propre au constructeur et elles sont usuellement appelées listes d'accès ou «access-list».

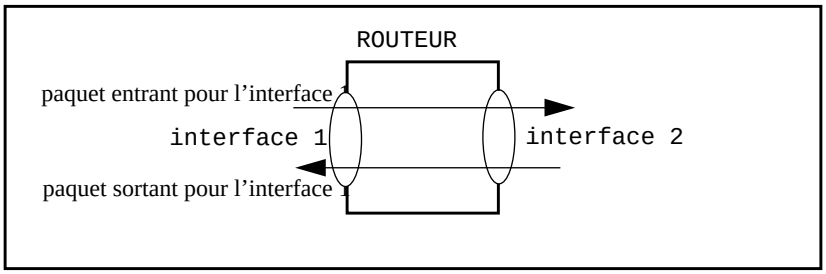


FIGURE 36. Schématisation du passage des paquets dans un routeur.

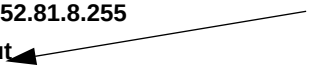
Le principe général est de tester et de filtrer les services qui ne doivent pas être accessibles de l'extérieur pour raison de sécurité et d'autoriser le tranfert . L'accès se fait en précisant les adresses IP source et destination et leur masque, ainsi que le protocole (UDP ou TCP) et le numéro du port que l'on veut inhiber.

```
access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 established
access-list 101 deny   udp 0.0.0.0 255.255.255.255 152.81.0.0 0.0.255.255 eq 69
access-list 101 deny   tcp 0.0.0.0 255.255.255.255 152.81.0.0 0.0.255.255 eq 87
access-list 101 deny   udp 0.0.0.0 255.255.255.255 152.81.0.0 0.0.255.255 eq 2049
access-list 101 deny   tcp 0.0.0.0 255.255.255.255 152.81.0.0 0.0.255.255 eq 111
access-list 101 deny   udp 0.0.0.0 255.255.255.255 152.81.0.0 0.0.255.255 eq 111
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

FIGURE 37. Déclaration d'une liste d'accès référencée 101 sur un routeur *Cisco*.

Une fois déclarée, la liste d'accès est affectée à une interface en précisant si le filtrage doit être fait en entrée ou en sortie :

```
interface Ethernet1
ip address 152.81.8.1 255.255.255.0
ip broadcast-address 152.81.8.255
ip access-group 101 out
no ip redirects
ip accounting output-packets
...
```



on affecte la liste d'accès 101 définis ci-dessus au paquet sortant de l'interface

Bibliographie

[BELLOVIN 89] Steven M. Bellovin, Security Problems in the TCP/IP Suite, Computer Communication Review, Vol. 19, N. 2, pp. 32-48, Avril 1989.

[BRADNER 92] Scott O. Bradner, Ethernet Bridges and Routers: Faster Than Fast Enough, DATA COMMUNICATIONS, September 1992.

[CERT 92:13] Computer Emergency Response Team, SunOS NIS Vulnerability, CERT ADVISORY92:13, June 1992.

[CIAC 95:02] Computer Incident Advisory Capability, F-11 Unix NCSA httpd Vulnerability, note électronique, ciac.llnl.gov:/pub/ciac/ciacdocs, 1995.

[CHAPMAN 95] Brent Chapman, INTERNET SECURITY FIREWALLS, Séminaire FNET, Paris, Février 95.

[CHAPMAN 92] Brent Chapman, Network (In)Security Through IP Packet Filtering, USENIX Proceedings, Unix Security Symposium III, September 1992

[CHESWICK 94] William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addison-Wesley Professional Computing Series, 1994.

[COMER 88] D. Comer, Internetworking with TCP/IP : Principles, Protocols, and Architecture, Prentice Hall, 1988.

[DUPONT 91] Francis Dupont, Routage dans les réseaux TCP/IP, Document Inria, ftp.inria.fr:/doc/networks/Dupont-routage.ps, Janvier 1991.

[FERRERO 95] Alexis Ferréro, Ethernet et ses évolutions, Addisson-Wesley, 1995.

[FORE 94] Fore Systems, Copper Media and the ATM Network, Technical document version 1.0, September 1994.

[HUITEMA 95] Christian Huitema, [Le]Routage dans l'internet, Eyrolles, 1995.

[HUNT 92] Craig Hunt, TCP/IP Network Administration, O'Reilly & Associates, Inc, 1992.

[MEHTA 91] Varun Mehta, Rajiv Khemani, Tuning SPARCserver 690 for Optimal NFS Performance, Service Performance Engineering, Sun Microsystems, Inc, February 1991.

[METCALFE 93] Bob Metcalfe, From the Ether, InfoWorld, Vol. 15, N. 46, 1993.

[MICRO-BULL. 95] Ouvrage collectif - Le Micro Bulletin, L'Internet professionnel, CNRS EDITIONS, 1995.

[PARTRIDGE 94] Craig Partridge, Les réseaux gigabit, Addison-Wesley, Collection Brian W. Kernighan, 1995.

[ROLIN 88] Pierre Rolin, Réseaux locaux normes et protocoles, HERMES, 1988.

[ROSE 91] Marshall T. Rose, The Simple Book An Introduction to Management of TCP/IP-based Internets, Prentice Hall 1991.

[RES. & TEL. 93] RESEAUX & TELECOMS, PASSEPORT pour LES RESEAUX, 1993.

[RUTGERS 87] Charles L. Hedrick, Introduction to Internet Protocols, document électronique, cs.rutgers.edu:/runet/tcp-ip-intro.ps, 1987.

[RUTGERS 88] Charles L. Hedrick, Introduction to Administration of an Internet-based Local Network, document électronique, cs.rutgers.edu:runet/tcp-ip-admin.ps, 1988.

[SPURGEON 94] Charles Spurgeon, Guide to 10-Mbps Ethernet, document electronique, ftp.utexas.edu/pub/netinfo/ethernet/ethernet-guide-A4.ps, 1994.

[STERN 91] Hal Stern, Managing NFS and NIS, O'Reilly & Associates, Inc, 1991.

[STALLINGS 93] William Stallings, SNMP, SNMP v2 and CMIP. The practical Guide to Network-Mangement Standards, Addison Wesley, 1993.

[STEVENS 95] W. Richard Stevens, TCP/IP Illustrated, Vol.1 The Protocols, Addison-Wesley Professional Computing.

[TANENBAUM 92] Andrew Tanenbaum, RESEAUX, Architecture, protocoles, applications, InterEditions, 1992.

Glossaire

ASN.1 «Abstract Syntax Notation One», langage normalisé par l'ISO permettant de décrire les types des données de façon indépendante des techniques de représentations informatiques utilisée

AUI «Attachement Unit Interface», interface de raccordement de station. Le terme AUI peut également faire référence au connecteur sur lequel un câble AUI peut être branché.

broadcast message de diffusion globale, un même message est lu par plusieurs récepteurs sans être dupliqué.

CERT «Computer Emergency Response Team», terme générique désignant une équipe d'alerte sur la sécurité informatique, par exemple : le CERT RENATER.

CIAC «Computer Incident Advisory Capability», c'est un des CERTs américains.

démon programme chargé en mémoire et en exécution qui est en attente d'un événement.

DNS «Domain Name Server», serveur de noms qui gère un annuaire contenant les adresses IP et les noms de toutes les stations de l'Internet qui ont été préalablement enregistrées.

FDDI «Fiber Distributed Data Interface», norme ANSI spécifiant un réseau à jeton à 100 Mb/s utilisant initialement un câble en fibre optique.

IFG «Inter Frame Gap» ou espace entre les trames.

IAB «Internet Activity Board» : groupe de chercheurs qui se réunissent régulièrement pour discuter des questions concernant Internet dont ils fixent la plupart des règles de fonctionnement.

IP	«Internet Protocol», protocole réseau utilisé dans Internet.
ISO	«International Standard Organisation», organisme qui dépend de l'ONU et chargé de la normalisation.
MAC	«Media Access Control» couche définissant le contrôle d'accès au media.
NFS	«Network File System», protocole permettant l'accès partagé des fichiers sur un réseau.
NIC	«Network Information Center», centre d'information réseaux gérant entre autres les attributions de classe réseau IP
NIS	«Network Information Service». Ce service s'appelait initialement «pages jaunes» («yellow pages»), mais il a été décidé que cette dénomination était réservée aux Télécommunications.
OSI	«Open system Interconnect», modèle architectural de réseau développé par l'ISO et le CCITT. Ce modèle est composé de 7 couches.
RENATER	REseau NAtional de TElécommunications de la Recherche, projet commun au MRT et au MEN.
RFC	«Request For Comments», mécanisme de standardisation ouvert de toute la famille TCP/IP.
RPC	«Remote Procedure Call», ou «appel de procédure à distance».
SNMP	«Simple Network Management Protocol», protocole de gestion des réseaux Internet qui permet de contrôler ou spécifier la configuration réseau.
TCP	«Transmission Control Protocol» ou protocole de contrôle de communication, TCP correspond à la couche 4 du modèle OSI et assure la fiabilité des transmissions.

Table des matières

Table des matières