

RAPPORT DE STAGE

Etude de l'intégration d'une plate-forme Linux
dans un réseau Microsoft



EBC Informatique

RAPPORT DE STAGE

Etude de l'intégration d'une plate-forme Linux
dans un réseau Microsoft

Enseignant tuteur : M. Dominique GRAD

Maître de stage : M. Luc CHRISTIANY



Département Informatique

IUT Robert Schuman
Département Informatique
72, Route du Rhin
67400 Illkirch-Graffenstaden



EBC Informatique
9, rue Paul Eluard
67087 Strasbourg Cedex 02

Remerciements :

Pour m'avoir accueilli au sein de son centre de compétences, pour m'avoir encadré et m'avoir fourni l'ensemble des éléments matériels dont j'avais besoin pour le bon déroulement du stage, je tiens à exprimer ma reconnaissance à M. Luc CHRISTIANY.

De plus, je remercie aussi chacun des employés d'EBC Informatique que j'ai rencontrés pour leur accueil chaleureux et sympathique, ainsi que pour les services qu'ils m'ont rendus.

Mes remerciements s'adressent aussi plus particulièrement à M. Dominique GRAD, sans qui je n'aurais jamais pu obtenir un tel stage, ainsi qu'à toute l'équipe pédagogique de l'I.U.T. pour la qualité de l'enseignement qu'ils m'ont apportés.

Sommaire

Introduction générale	3
I] Présentation de l'entreprise d'accueil	4
a) Localisation géographique	4
b) Effectif global de la société.....	4
c) Résultats de l'entreprise	5
d) Structure organisationnelle.....	5
e) Le centre de compétences UNIX.....	7
II] Objectifs du stage	7
a) Contexte général et présentation du sujet du stage.....	7
b) Objectifs.....	8
c) Contraintes.....	8
III] Comprendre	8
a) UNIX/Linux.....	8
b) TCP/IP	10
c) Le protocole DHCP	10
d) Le service DNS	11
e) L'IP Masquerade	14
f) Samba, NetBIOS et SMB	15
IV] Réalisations.....	16
a) DHCPd, implémentation du protocole DHCP	16
b) NAMED, le serveur DNS de référence.....	19
c) L'IP Masquerade	24
d) Samba	24
e) Journal de bord	26
V] Bilan.....	28
VI] Conclusion personnelle.....	29
VII] Sources d'informations	30
a) Bibliographie	30
b) Sites Internet consultés	30

Annexes : l'ensemble des études conçues au cours du stage.

Introduction générale

Vous tenez dans vos mains le bilan de mon stage de fin de premier cycle universitaire. Cette étape est l'avènement de ma formation à l'Institut Universitaire de Technologie Robert Schuman, le dernier palier avant l'obtention de mon D.U.T. Informatique et peut-être l'entrée dans la vie active. Afin de rendre cette expérience la plus constructive possible, j'ai soigneusement choisi son sujet et en voici les principales raisons.

Ce choix a surtout été guidé par mon envie d'approfondir mes connaissances dans les deux mondes de l'informatique qui me passionnent le plus : le système et le réseau. Certes, le développement logiciel est aussi très intéressant, mais la formation obtenue à l'I.U.T. m'a déjà faites entrevoir ses possibilités... et ses ennuis. Le monde des systèmes d'exploitations de la famille UNIX (concurrent du système Microsoft Windows) ne m'était pas totalement inconnu, mais je ne connaissais que la face visible de l'iceberg et je désirais fortement descendre dans ses profondeurs. Un concours de circonstances a fait que l'on m'a proposé un stage alliant système et administration de réseaux, à l'entreprise EBC Informatique. Ce fut une aubaine pour moi et j'ai immédiatement saisi l'occasion !

I] Présentation de l'entreprise d'accueil

Créée en 1988 à Strasbourg par son actuel PDG M. Pierre BURG et ses associés, EBC Informatique est une société offrant des solutions informatiques adaptées aux besoins des entreprises. Ces solutions sont axées autour de deux pôles principaux : le service et l'édition de logiciels.

a) Localisation géographique

Le siège social de la société EBC Informatique est situé à Strasbourg. Les coordonnées complètes sont les suivantes :

9, rue Paul Eluard
67087 Strasbourg Cedex 02
Tél. : 03.88.30.87.87
Fax : 03.88.30.87.77
Email : strasbourg@ebc-informatique.com

La société dispose de plusieurs implantations disséminées sur toute la France : Besançon, Bordeaux, Lille, Lyon, Marseille, Mulhouse, Nantes et Paris. Elle dispose également d'implantations, mais aussi de filiales à l'étranger : au Luxembourg, en Suisse (Genève, Sion, Tessin), en Belgique (Bruxelles) et en Allemagne.

Les perspectives d'implantations à venir sont principalement situées à l'étranger : Copenhague, Lausanne, Londres, Madrid, Milan, Oslo et Toulouse sont autant de lieux qu'EBC Informatique désire conquérir.

b) Effectif global de la société

A ce jour, la société compte un peu plus de 400 personnes. La progression de l'effectif est schématisée ci-dessous :

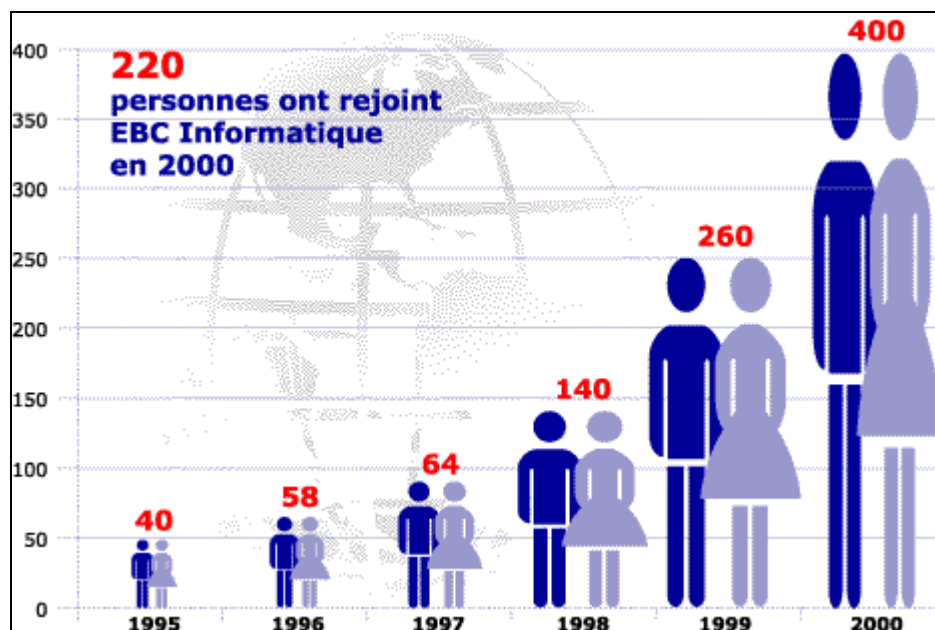


figure 1 : progression de l'effectif global d'EBC Informatique

c) Résultats de l'entreprise

EBC Informatique fait partie de ces entreprises au rythme de développement fulgurant. En effet, le chiffre d'affaires double pratiquement tout les deux ans comme en témoigne le graphique suivant :

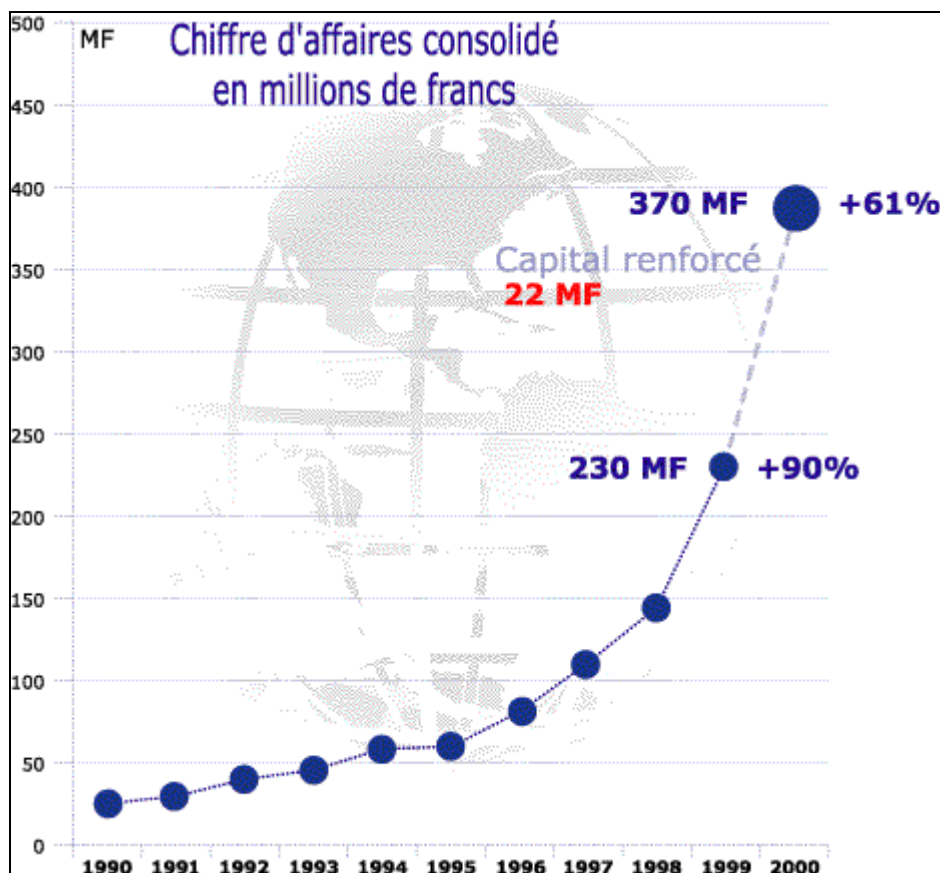


figure 2 : progression du chiffre d'affaires d'EBC Informatique

d) Structure organisationnelle

L'entreprise se décline en deux pôles d'activités principaux : le service et l'édition de logiciels. Elle se subdivise en plusieurs entités : les centres de compétences.

Qu'est ce qu'un centre de compétences ?

Un centre de compétence est un pôle d'activité technologique qui vise à promouvoir un domaine d'expertise appliqué au système d'information de l'entreprise.

Les centres de compétences sont nombreux et en voici l'énumération :

Centre de compétences	Description de l'activité
CAO	Offre complète CAO AutoDesk (Distribution, Intégration, Conseil) pour la mécanique, l'architecture, l'imagerie principalement.
AS/400	Adresser avec un haut niveau d'expertise tous les systèmes liés au monde AS/400.
Décisionnel et Management	Mise en place de systèmes d'informations performants.
Ordosoftware	Une gamme de Progiciels de Gestion Intégrés (ERP) pour les PME et grands groupes industriels travaillant à la commande, à l'affaire ou sur prévisions.
Distribution	Distribution de matériel informatique configurés prêt à l'emploi.
Télécom et Réseau	Mise en place de solutions de communication performantes.
e-pc	European Purchasing Concept (aide au commerce électronique).

Euro 400 Win	Offre complète Euro 400 Win (Distribution, Intégration, Conseil) qui est un progiciel de gestion et de marketing destiné aux directions des grosses et moyennes entreprises.
Smile	Méthodologie de déploiement de projets.
Solution	Intégration des progiciels EBC Informatique.
Formation	Dispense des formations aux utilisateurs et aux professionnels de l'informatique.
Stockage	Adresser avec un haut niveau d'expertise tous les thèmes liés au monde du stockage.
IT-C@re	Identification de tous les éléments de service liés à la production informatique, prise en charge de tout ou partie de la production, garantir les niveaux de services
TotalCompta	Outil de gestion dynamique et prévisionnel.
Logistique	Centre de configuration, logistique, maintenance et stocks.
TotalHorizon	Progiciel de gestion axé métier.
NTIC	Nouvelles technologies de l'information et de la communication (Internet mobile,...).
UNIX	Proposition de solutions UNIX (lieu du stage).

La structure fonctionnelle de l'entreprise est très intéressante de par la subdivision de cette dernière en centres de compétences. On pourrait penser que le client serait rebuté devant leurs nombre, ne sachant pas auxquels s'adresser. Mais il n'en est rien ! En effet, le client exprime ses besoins à un interlocuteur privilégié unique (commercial ou chef de projet) qui s'occupe de coordonner les différents centres de compétences entre eux afin d'élaborer une proposition pour le client qui pourra alors valider l'offre.

Le schéma suivant exprime bien le déroulement des opérations :

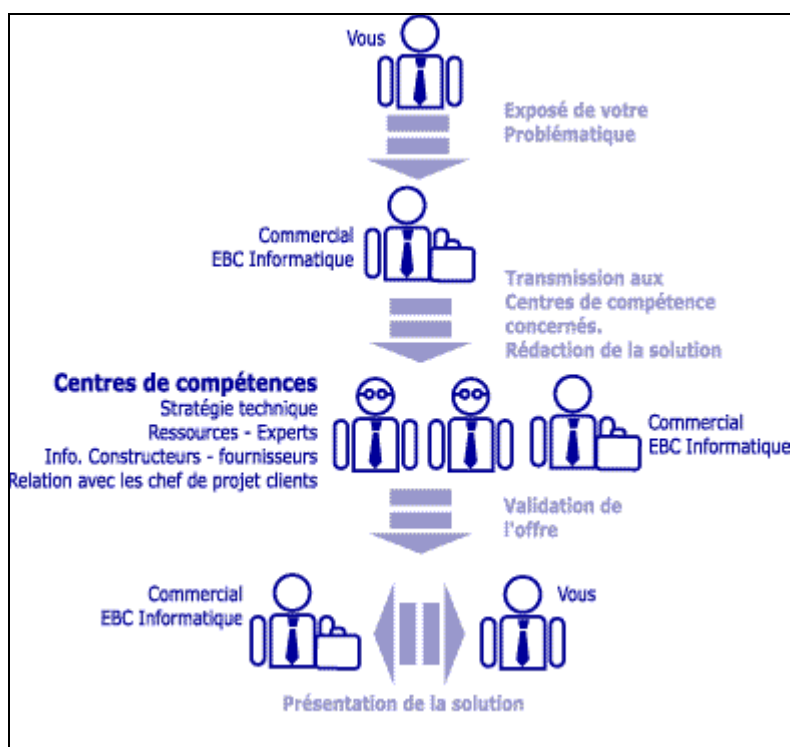


figure 3 : déroulement d'une transaction chez EBC Informatique

e) Le centre de compétences UNIX

Le centre de compétences UNIX a été créé récemment. Il a pour but de proposer des solutions basés sur les systèmes d'exploitations de la famille UNIX, principalement AIX, Solaris et Linux. Son responsable, également mon maître de stage, M. Luc CHRISTIANY est actuellement le seul employé du centre, ceci dû en particulier à la méconnaissance du monde UNIX des dirigeants de l'entreprise...

C'est dans ce centre que le stage s'est déroulé. Le matériel mis à ma disposition était amplement suffisant : un serveur LINUX performant sur lequel j'étais totalement libre de toutes manipulations, une imprimante, un petit portable sur lequel j'ai installé Windows 9x et NT 4, et de quoi relier tout cela en réseau local. Je disposais également d'une prise Internet me permettant d'accéder à la documentation en ligne. Les systèmes d'exploitations mis à ma disposition correspondait à la suite complète des Microsoft Windows (98, NT 4, 2000), ainsi que la version 7 de Red Hat Linux. Les autres grands logiciels telles que la suite Microsoft Office 2000, Macromedia Dreamweaver 2,... était également disponibles, mais seul Office m'était utile.

II] Objectifs du stage

a) Contexte général et présentation du sujet du stage

Dans le cadre du développement du centre de compétences UNIX, mon travail a été d'étudier l'intégration d'une plate-forme Linux au sein d'un réseau Microsoft.

En effet, Microsoft est présent en tout point sur le marché logiciel. Cette entreprise est la créatrice bien connue des systèmes d'exploitations Windows, qui sont installés sur la grande majorité des micro-ordinateurs actuels. Mais Microsoft est aussi un acteur important de la recherche et du développement dans le domaine des nouvelles technologies. La société est à la base de nombreuses découvertes et l'informatique actuelle doit son développement fulgurant en grande partie grâce à elle.

Cependant, Microsoft n'a plus la même réputation actuellement qu'il y a 6 à 8 ans. Certes l'entreprise est toujours leader, mais sa réputation est fortement entachée par les problèmes liés à la qualité de son système d'exploitation ainsi qu'à celle de quelques autres de ses logiciels, et surtout à sa philosophie expansionniste exubérante.

De plus, les prix des solutions logicielles Microsoft sont souvent trop élevés, pour une qualité de service qui n'est pas toujours à la hauteur des espérances. C'est ici que le bas blesse, et c'est là qu'interviennent les serveurs Linux.

En effet, Linux fait partie de ce que l'on appelle le monde du libre, c'est à dire totalement gratuit ! On peut cependant s'accorder les services de suivi des entreprises qui conçoivent les versions du système d'exploitation Linux, mais moyennant une somme bien moins conséquentes que celles stipulées dans les contrats Microsoft. De plus une myriade de logiciels développés sous et pour Linux sont aussi totalement gratuit et téléchargeable n'importe où sur Internet... C'est un avantage considérable !

Mais ce n'est pas tout, des développeurs Linux, aux quatre coins du globe, ont conçus des programmes, totalement gratuit, capables de substituer la quasi totalité des fonctionnalités des serveurs Windows NT...

Et c'est ainsi que s'est formé le sujet de mon stage : « étudier l'intégration d'une plate-forme Linux au sein d'un réseau Microsoft. ». En clair, il s'agit de concevoir des solutions générales permettant de substituer un serveur Linux à un serveur Microsoft Windows NT au sein d'un réseau composé de clients Microsoft Windows.

b) Objectifs

Globalement, On peut considérer un serveur Windows NT comme un ensemble de fonctionnalités et de services offerts aux clients d'un réseau. Mon travail a donc été dans un premier temps de lister grossièrement ces fonctionnalités et ces services.

Je devais ensuite, en me basant sur l'étude de trois applications Linux : un serveur DHCP, un serveur de noms et Samba (ces termes et concepts seront expliqués plus loin dans ce rapport), tenter de mettre en œuvre des solutions qui permettrait d'imiter les fonctionnalités du serveur Windows. Chacune de ces applications nécessite une configuration qui peut souvent devenir très complexe en raison de l'immense liste des paramètres de configuration disponibles. Je devais donc concevoir des configurations, « prêtes à l'emploi », pour chacune de ces applications qui permettrait de substituer Linux à Windows NT dans certains cas.

c) Contraintes

L'une des principales contraintes a été de prendre l'aspect sécurité en compte. Des abominations, telles que le passage des mots de passe en clair sur le réseau devaient être écartées. Un utilisateur mal intentionné et disposant d'un peu de connaissance sur la recherche d'informations sur Internet aurait pu sans problème se l'approprier.

Il fallait aussi que mon travail soit le plus professionnel possible, c'est à dire que je ne devais pas installer des programmes ou des fichiers de configurations n'importe où sur le système, mais que chaque chose devait être à sa place afin de garder une certaine « propreté » sur le système. En effet, un système « propre » est un système plus facile à administrer...

III] Comprendre

Je vais tenter dans cette partie de vous expliquer la plupart des concepts relatifs à mon stage. Il vous permettront de mieux comprendre le travail que j'ai effectué.

a) UNIX/Linux

Le système Unix a été mis au point par Ken Thompson dans les laboratoires Bell dans le New Jersey aux Etats-Unis. Le but de Ken Thompson était de mettre au point un système interactif simple pour faire tourner un jeu qu'il avait créé (space travel, une simulation du système solaire).

La première version de ce système a vu le jour en 1969, il s'inspirait des principaux systèmes d'exploitation de l'époque (Multics, Tenex), et était destiné à une utilisation mono-utilisateur, d'où son nom (Unix = Multix uni-utilisateur à priori).

Peu de temps après, D.Ritchie a rejoint l'équipe de K.Thompson afin de mettre au point, en 1971, une version d'UNIX permettant la multiprogrammation.

Parallèlement, D.Ritchie participe grandement à la définition du langage C (puisque'il est considéré comme un de ses créateurs avec B.W.Kernighan), ainsi l'ensemble du système a été entièrement réécrit en langage C en 1973.

En 1975, à partir de la version 6 du système, Unix va enfin être commercialisé.

1983 marque l'apparition de UNIX system V, un système Unix commercialisé par AT&T. De son côté l'Université de Californie met au point une variante du système destinée aux systèmes VAX nommée UNIX BSD. Les deux systèmes se sont longtemps fait la guerre et c'est le system V qui en est sorti vainqueur.

Actuellement, UNIX est utilisé dans les stations de travail à hautes performances, ainsi que dans les gros serveurs car il est considéré comme le système le plus stable (c'est à dire que le système tombe très rarement, presque jamais, en panne) et le plus adapté à l'utilisation en réseau. De plus, UNIX est devenu multi-utilisateur (plusieurs utilisateurs peuvent travailler en même temps sur une même machine), multi-tâches (plusieurs applications peuvent fonctionner en même temps sans qu'aucune n'affecte les autres), multi plate-forme (serveurs à base de processeurs Intel, Cyrix, AMD, Alpha, PowerPC,... peuvent disposer d'UNIX) et multiprocesseurs (certains serveurs, d'IBM entre autre, utilise UNIX pour gérer les quelques centaines de processeurs dont ils disposent).

Cependant, la qualité de ce système se paie. UNIX est un produit commercial, vous devez acheter des licences d'utilisation pour chaque plate-forme sur laquelle il s'exécute. Le coût de ces licences peut varier de quelques centaines de francs à plusieurs milliers.

Mais bien entendu, certains clones d'UNIX ont été conçu au cours des années, afin de le rendre accessible à tous, librement et gratuitement, tel que Minix, d'Andrew Tanenbaum, qui fournissait un système d'exploitation minimale pouvant être utilisé sur PC.

Mais Minix n'était pas très étendue dans ses fonctionnalités et en août 1991, un étudiant de l'université d'Helsinki envoie un message sur comp.os.minix (un forum des utilisateurs de Minix sur Internet), commençant par ces quelques mots :

Hello everybody out there using minix I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386 (486) AT clones.

Cet étudiant était Linus Torvalds, et le "hobby" dont il parle est devenu ce que nous connaissons aujourd'hui sous le nom de Linux, un clone d'UNIX (mais ne reprenant aucune ligne de code de ce système, en imitant simplement son fonctionnement et son principe). Ce message a été le début de cette grande aventure de la conception d'un système d'exploitation totalement gratuit et ouvert, qui parvient actuellement à concurrencer les grands UNIX commerciaux et le bastion Windows de Microsoft. Développé initialement par Linus, des centaines de programmeurs à travers le monde se sont associés à sa conception et ont permis d'améliorer Linux et d'en faire un système d'exploitation complet et performant. Il est intéressant de noter que cette gigantesque équipe de développement manquait complètement de coordination, mais malgré cela, chacun y est pourtant allé de sa participation soit en écrivant des petits programmes pour ses besoins personnels, soit en écrivant des pilotes de ses périphériques,...

L'avènement de Linux dans le monde de l'informatique est en grande partie due à l'équipe de développement Linux de Red Hat Software qui a conçu sa propre distribution (sa propre version) de Linux et qui y a apporté des concepts la rendant plus accessible au grand public tel que le principe des paquetages qui n'apparente plus une application à un ensemble de fichiers sources à compiler et à installer, mais à une sorte de boîte noire qu'il suffit d'ouvrir pour installer et utiliser immédiatement l'application contenu, et de supprimer pour désinstaller cette dernière.

Bien entendu, Red Hat a été le précurseur des distributions Linux accessibles à tous, et sa réputation est dors et déjà acquises : plus de 50% du parc Linux actuel est composé de sa distribution selon certains sondages américains. Mais Red Hat n'est plus seul, on ne compte plus les versions qui existent tellement leurs nombres est important. Pour ne citer que quelques uns des grands noms des distributions Linux, il y a SuZe Linux (un équivalent de la Red Hat mais mise en œuvre par une équipe allemande), Mandrake (idem, mais à la française), Corel Linux, Caldera, Debian. La Debian est un distribution un peu particulière car elle ne contient à sa base aucun logiciel propriétaire et se veut la distribution la plus pure et qui reflète le mieux la vraie philosophie de Linux (totale ouverture du système, de son code source et total gratuité). Elle est très appréciée sur des stations serveurs et est utilisée dans des routeurs telles que ceux de Cisco Systems.

b) TCP/IP

Si vous avez déjà « surfé » un peu sur Internet, vous avez certainement déjà entendu parler d'adresses IP et de TCP/IP.

IP (Internet Protocol) est un protocole de transport qui permet de transmettre des données au travers un réseau d'un ordinateur à un autre.

TCP est un protocole de communication, qui associé à IP, permet de transmettre des données d'une application vers une autre, sur des ordinateurs différents d'un réseau.

TCP/IP (prononcez TCP sur IP) représente l'encapsulation (l'association) de ces deux protocoles. C'est la méthode de communication préférée sur Internet car c'est la plus performante en terme de rapidité de transmission.

Pour caricaturer le fonctionnement, chaque ordinateur d'un réseau dispose d'une adresse IP qui le représente sur ce réseau. Actuellement, c'est une adresse composée de 4 nombres, de 0 à 255. Un ordinateur qui veut envoyer des données à un autre ordinateur sur le réseau doit connaître l'adresse IP de ce dernier, et va « déposer » ces données sur le réseau qui s'occupera de les acheminer à bon port. Bien entendu, la réalité est beaucoup plus compliquée, mais cette explication vous suffira à comprendre les principaux points de ce rapport.

c) Le protocole DHCP

L'utilisation des protocoles de communications TCP et IP par une machine d'un réseau nécessite la configuration de cette dernière. Il s'agit de lui assigner une adresse IP valide (pas encore utilisée par une autre machine du réseau), de lui indiquer les caractéristiques du réseau telles que son nom, l'adresse de diffusion, ... et de lui indiquer les adresses IP des machines remarquables : serveur de noms, passerelle ou routeur...

Bien entendu, dans un réseau où ces informations sont souvent modifiées, où les machines sont mobiles, souvent changées (assembleur informatique lors du test des ordinateurs), où certains utilisateurs ne maîtrisent pas forcément les notions informatiques relatives à TCP/IP, cette configuration peut se révéler fastidieuse et le protocole DHCP est là pour vous aider...

En effet, ce protocole permet à un client du réseau de s'autoconfigurer par le biais d'une « discussion » avec un serveur DHCP présent sur le réseau.

Dans la pratique, comment cela fonctionne-t-il ?

Le protocole DHCP utilise le principe des baux que l'on retrouve, par exemple, dans la location d'un appartement. Bien entendu, ce ne sont pas des mètres carrés qui sont loués, mais des « kits » de configuration TCP/IP qui comprennent l'adresse IP du client, ainsi que les informations relatives au réseau local.

Voici donc notre client connecté au réseau :

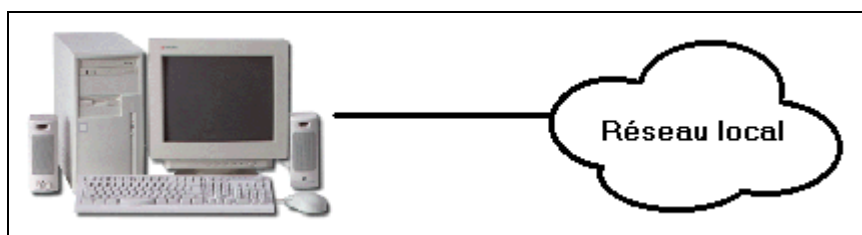


figure 4 : un client relié à un réseau local

Ce dernier démarre, il ne sait alors rien de son identité sur le réseau. Il envoie alors à toutes les machines du réseau une demande de bail IP.

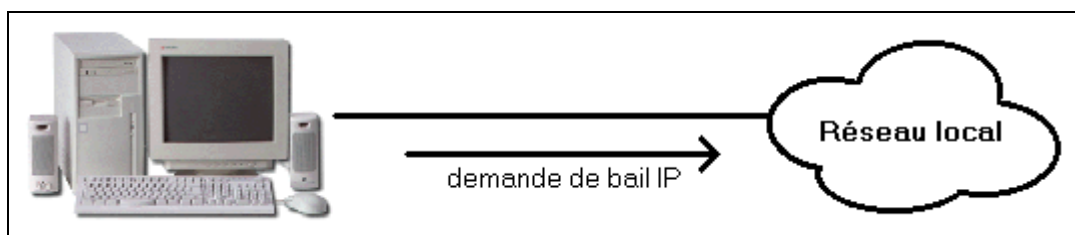


figure 5 : le client émet une demande de bail IP à tous les ordinateurs du réseau local

L'ensemble des machines réceptionnent donc cette demande, mais seul le ou les serveurs DHCP du réseau vont répondre à notre client en lui proposant chacun un bail :

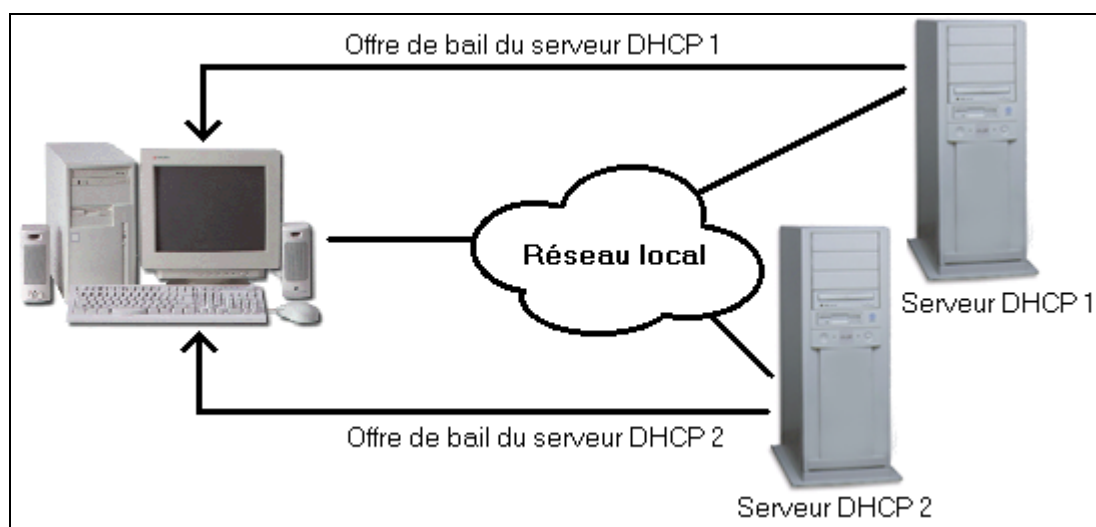


figure 6 : deux serveurs DHCP offrent des baux IP au client

Le client à réception de plusieurs offres de bail ne tient compte que de la première qui lui est parvenue. Il ne traite donc plus qu'avec le serveur émetteur de cette offre et lui demande l'affectation définitive du bail. Le serveur alors accepte normalement cet affectation et l'enregistre dans sa base de données des adresses IP affectées.

Le client dispose alors de l'ensemble des informations nécessaires pour son fonctionnement au sein du réseau.

Mais que se passe-t-il lorsque le bail du client arrive à expiration ? Le client demande au serveur DHCP un renouvellement de son bail. Ce dernier accepte alors ou non ce renouvellement. S'il ne l'accepte pas, le client doit recommencer le processus d'affectation de bail depuis le début.

d) Le service DNS

Pour des raisons de commodités, il est plus facile pour un humain de manipuler des noms significatifs, tels que « www.linux-france.org », pour accéder à une machine sur Internet, que des adresses IP codées sur plusieurs octets pour une machine (comme 216.167.114.128). Mais comment se fait la transcription du nom Internet d'une machine en son adresse IP ?

Au début des années 1970, lorsque Internet n'en était encore qu'à ses balbutiements, un système centralisé à Stamford avec un fichier « HOST.TXT » global a fonctionné. Ce fichier contenait l'ensemble des correspondances entre noms de machines enregistrés et leurs adresses IP. On pouvait récupérer la version la plus récente de ce fichier par FTP dont l'adresse IP était bien connue de tous, ce qui n'était pas très pratique. Avec l'explosion du nombre de machines connectées à l'Internet (on estime que plusieurs machines dans le monde apparaissent chaque

minute), ce système est devenu totalement ingérable. Un modèle centralisé sur un serveur est donc impossible à mettre en place, dû au nombre d'hôtes et au nombre de mises à jour nécessaires à apporter.

Le DNS ("Domain Name System" en anglais, « Système de noms de domaines » en français) a été conçu pour résoudre ce problème, en proposant un modèle hiérarchisé.

Chaque machine (terminal, serveur,...) reliée à un réseau se voit attribuer un nom. Ce nom est unique dans le domaine auquel elle appartient. Ainsi, pour les domaines domaine1.com et domaine2.com, on peut avoir deux machines portant des noms similaires ou différents. Par exemple, mail.domaine1.com et mail.domaine2.com désignent deux machines différentes, d'adresses IP différentes.

On peut comparer cette adresse à une adresse postale : pour trouver un domicile de façon certaine, on commence par chercher le pays, puis la ville, puis la rue et enfin le numéro. Ici le pays est un nom de domaine dit de « haut niveau ». Ils sont bien connus de tous les internautes : .com, .net, .fr,... Le nom de sous domaine (exemple : adobe.fr.) peut-être assimilé au nom de la ville dans ce pays. Il peut y avoir plusieurs villes dans le monde ayant le même nom, mais dans un même pays un nom de ville doit être unique, pour pouvoir l'identifier de façon certaine. Eventuellement, si la ville est petite, on peut se contenter de ne préciser que le nom d'une personne : le facteur saura à coup sûr où habite la personne (par exemple, pour la machine ftp.adobe.com). Mais si la ville est plus grande, on peut également la diviser en rue (pour la machine www.fr.adobe.com par exemple).

Comme un nom d'hôte complet est ordonné de façon logique, du plus précis au plus vague, le plus simple pour hiérarchiser la recherche est de le faire sur chaque partie du nom. Chaque serveur ne connaît que les noms de ses fils (le serveur pour .com sait comment atteindre www.linux-france.com mais pas www.linux-france.org), et renvoie à la racine ("Root") les requêtes qu'il ne sait résoudre. Celle-ci à son tour tente de résoudre un nom en une adresse IP en renvoyant l'adresse du serveur pouvant répondre à cette demande.

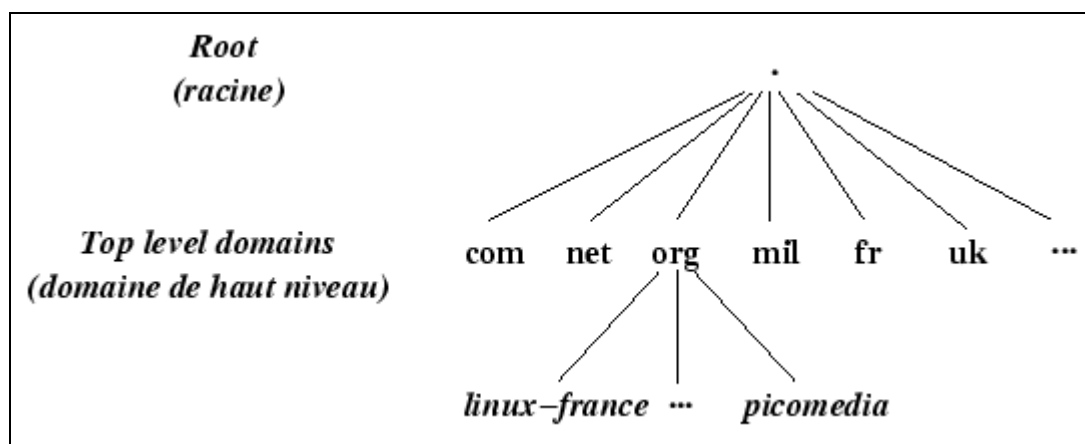


figure 7 : hiérarchie du DNS

La hiérarchie DNS est donc divisée en zones. Une zone représente un domaine (fr, org, linux-france.org). Une zone parente peut déléguer une zone fille à un ou plusieurs serveurs de noms (souvent appelés aussi serveurs DNS), et chaque zone est gérée par un serveur maître et éventuellement plusieurs serveurs secondaires dont le contenu est recopié à partir du serveur maître, afin de prévenir les éventuelles pannes).

Prenons un **cas pratique** : résoudre le nom d'hôte machine.division.domaine.fr.

La machine cherchant à atteindre cet hôte contacte l'un des serveurs de noms par défaut, c'est à dire qui sont enregistrés dans sa configuration (3 au maximum).

Si ce serveur de noms par défaut n'arrive pas à résoudre ce nom, il contacte les serveurs de noms à la racine. Il faut donc que tout serveur de noms ait au moins la liste de tous les serveurs de noms de la racine, ainsi que leur adresses IP associées. Parmi les serveurs de noms à la racine, le premier à répondre reconnaît l'adresse comme valide, et renvoie l'adresse IP du serveur de noms capable de mieux le renseigner : celui de la zone .fr (donc des noms de domaines du type xxx.fr).

Le DNS local interroge alors le DNS de la zone .fr. Si ce serveur de noms n'est pas capable de résoudre machine.division.domaine.fr, il renvoie la liste des serveurs de noms de la zone domaine.fr.

A son tour, un des serveur de noms de la zone domaine.fr reconnaît le suffixe division.domaine.fr, et renvoie l'adresse IP du serveur de noms de la zone division.domaine.fr, qui connaît l'adresse IP de machine.division.domaine.fr ;

Il y aura donc eu au maximum 1 interrogation pour chacun des 3 serveurs de noms par défaut, 1 pour celui de la zone racine (zone « . »), 1 pour celui de la zone .fr, 1 pour celui de la zone domaine.fr, et 1 pour celui de la zone division.domaine.fr. Chacun de ces serveurs de noms ne renvoient à chaque fois que l'adresse du serveur DNS le plus apte à répondre.

De plus, chaque serveur DNS garde en mémoire les dernières requêtes. Ainsi, si un nom est souvent demandé, il a toute les chances de figurer dans la mémoire du serveur qui n'aura pas besoin d'interroger les autres serveurs : la réponse sera directe.

On voit tout de suite l'avantage de cette méthode : au lieu d'avoir un serveur indexant toute les machines du Web, il y a des milliers de machines indexant un petit bout de l'Internet, en l'occurrence leur sous domaine. Cela répartit les informations et les charges sur ces milliers de machines plutôt que sur une seule...

Conversion d'adresse IP en nom

Il est parfois utile de pouvoir résoudre une adresse IP en nom de machine. Par exemple, en cas de demande de connexion de la part d'un hôte distant sur une machine, la machine distante n'envoie que son adresse IP. On peut donc résoudre cette adresse IP en nom (cela permet au passage de vérifier que l'adresse IP est valide, et non pas « détournée » par un pirate).

Pour pouvoir résoudre une adresse en nom, un pseudo-domaine a été mis en place : le domaine in-addr.arpa.

Le schéma suivant explique le principe de ce pseudo-domaine :

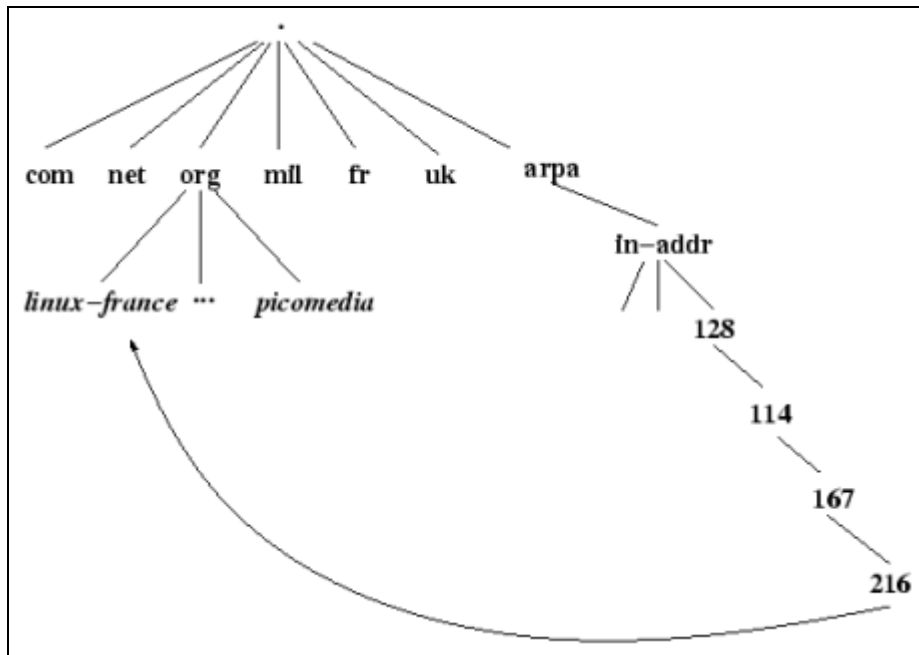


figure 8 : principe de la résolution inverse

En fait, pour l'hôte `www.linux-france.org`, l'adresse `128.114.167.216.in-addr.arpa.` est un pointeur vers les vrais enregistrements du nom de domaine `www.linux-france.org`.

e) L'IP Masquerade

L'IP Masquerade permet de sécuriser un réseau en jouant le rôle de passerelle Internet restrictive. C'est une fonctionnalité réseau de Linux, également disponible sous Windows NT Server.

Prenons l'exemple suivant :

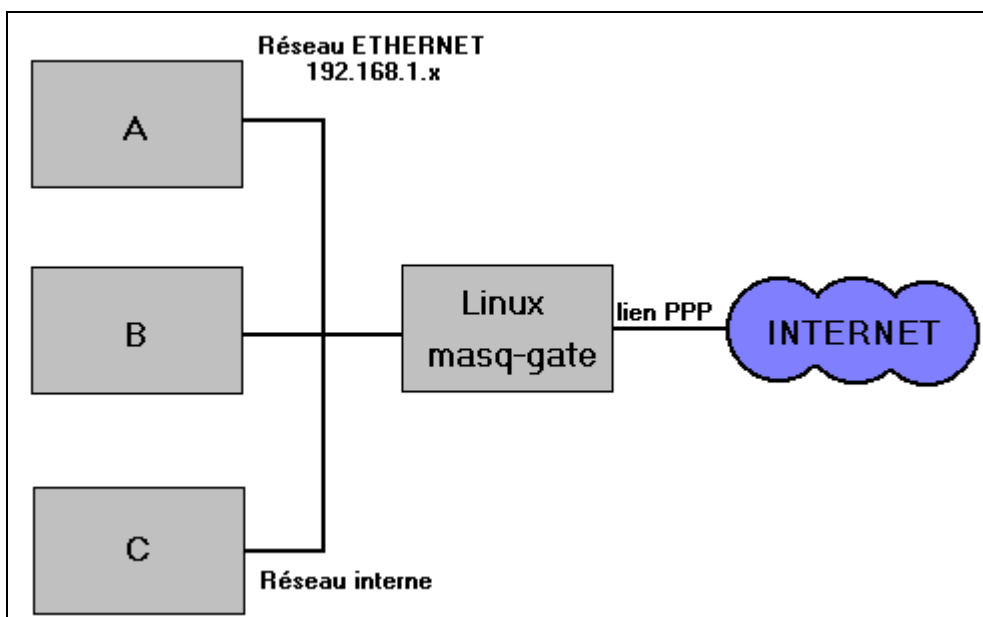


figure 9 : principe de fonctionnement de l'IP Masquerade

A, B et C sont des ordinateurs de notre réseau local. Ce sont des stations Windows, comme cela peut être des stations UNIX/Linux. La machine portant le label « masq-gate » est la machine

frontal du réseau (la seul « en contact » avec l'Internet). La machine « masq-gate » a accès à Internet, mais pas les ordinateurs A, B et C (enfin, pas encore !).

L'IP Masquerade permet à la machine « masq-gate » de transmettre vers Internet les données émises par A, B ou C vers le réseau des réseaux, et inversement, de renvoyer les réponses des serveurs contactés à la machine qui les a demandé. Les données en direction et provenant de l'Internet transitent donc par cette machine, et ainsi, l'ensemble des ordinateurs du réseau local peut avoir accès à Internet.

Mais j'ai parlé avant de l'aspect sécurité ! En effet, Linux dispose à sa base d'utilitaires permettant de filtrer les paquets de données qu'il reçoit et qu'il doit retransmettre. Un utilitaire que j'ai étudié particulièrement, nommé « IP Chains », permet d'interdire l'accès au réseau local pour toutes les machines de Internet ou seulement à quelques unes d'entre elles, permet de ne faire retransmettre que les données en direction d'un service spécifique (un serveur de pages Internet par exemple),... On choisit le type de données qui sont autorisées à pénétrer dans le réseau local, et on choisit aussi ce à quoi les ordinateurs du réseau local ont accès. Pour ne citer qu'un exemple, on peut interdire l'accès à un serveur de jeux afin que les employés ne passent pas tout leur temps dessus, ou on peut complètement interdire l'accès à Internet à certaines heures de la journée comme à l'I.U.T....

f) Samba, NetBIOS et SMB

Samba est une suite d'applications libres et gratuites qui est né du contexte qu'une machine fonctionnant sous Microsoft Windows est incapable de se connecter à un système de fichier Linux afin de, par exemple, lire les fichiers qui s'y trouvent ou en écrire.

Techniquement, Samba est implémentation du protocole SMB (« Server Message Block ») de Microsoft qui permet le partage de ressources telles que de l'espace disque, des imprimantes,... SMB fonctionne sur le principe d'échange client-serveur, c'est à dire que le client fait des demandes et le serveur envoie des réponses à ces demandes. Le rôle du client et du serveur n'étant pas mutuellement exclusifs, une machine peut être à la fois client et serveur.

SMB étant une extension de l'API NetBIOS, je vais dans un premier temps expliquer ce qu'est NetBIOS, puis que permet de faire exactement SMB.

Qu'est ce que NetBIOS ?

En 1984, IBM conçoit une API (Interface logicielle programmable) pour gérer les réseaux de ses micro-ordinateurs : l'API NetBIOS ou "Network Basic Input/Output System". Cette API fournit des outils rudimentaires pour permettre à une application de se connecter et de partager des données avec d'autres ordinateurs.

Comme NetBIOS n'est pas un protocole réseau, Les requêtes NetBIOS nécessite donc l'utilisation d'un autre protocole pour leurs transports d'un ordinateur à l'autre.

En 1985, IBM crée un protocole, en étroite relation avec l'API NetBIOS : NetBEUI ou "NetBIOS Extended User Interface ». Ce protocole a été conçu pour de petits réseaux locaux (LAN de moins de 256 machines) et permet à chaque machine d'avoir un nom unique sur le réseau.

Ce protocole a rencontré un vif succès dans les applications en réseaux, comme celle fonctionnant sous "Windows for Workgroups".

Plus tard, des implémentations de NetBIOS sur le protocole réseau IPX de Novell ont été créées, entrant en concurrence directe avec NetBEUI. De plus, le bourgeonnement de la communauté Internet a amené avec elle les protocoles TCP sur IP et UDP sur IP et implémenter NetBIOS sur ces protocoles est devenu une nécessité.

Mais, NetBIOS utilisant des noms d'ordinateurs et IP utilisant des adresses IP pour représenter ces mêmes ordinateurs, il a fallu trouver un moyen d'encapsuler ces deux protocoles. Des documents ont alors été publiés en 1987 indiquant comment faire fonctionner NetBIOS sur un réseau TCP-UDP.

Et c'est ainsi que NBT ou "NetBIOS over TCP/IP" est apparu. Le standard de ce protocole offre 3 services sur un réseau :

- un service de nom
- deux services de communications :
 - le service "datagram"
 - le service sessions

Le service de nom permet la résolution d'un nom d'ordinateur NetBIOS en son adresse IP. Mais attention, ce service n'a absolument rien à voir avec le service DNS précédemment expliqué. Les deux services de communications sont utilisés pour émettre et recevoir des données entre machines NetBIOS sur le réseau.

Et que vient faire le protocole SMB dans tout cela ?

SMB est un protocole, conçu par Microsoft, qui s'appuie sur les requêtes NetBIOS pour offrir des possibilités réseaux étendues pour son système d'exploitation Windows.

Ces services sont les suivants :

- partager un ou plusieurs systèmes de fichiers ou espace disque ;
- partager des imprimantes
- assister les clients lors de l'exploration du réseau (listage de ses machines)
- faciliter la résolution des noms NetBIOS en adresse IP grâce à WINS
- authentification des utilisateurs dans un domaine Windows

WINS ("Windows Internet Names Service") est un service permettant de résoudre plus rapidement un nom NetBIOS en une adresse IP. En effet, un serveur WINS gère une base de données contenant des enregistrements du style <nom de machine>=<adresse IP>. Les clients, pour se connecter à une machine envoie alors une requête de résolution au serveur WINS qui renvoie l'adresse IP correspondante. Certes WINS n'est pas indispensable, à la base NBT utilise le principe de diffusion (envoi d'une requête à toutes les machines du réseau) pour retrouver une machine sur le réseau. Mais si le réseau est imposant, WINS est nécessaire car il permet de supprimer tout ce trafic inutile qui encombre le réseau.

IV] Réalisations

L'objectif de mon stage a été de tenter de substituer une plate-forme Linux à un serveur Microsoft Windows NT. Ainsi, en premier lieu, je me suis mis à la lecture succincte du livre « Kit de ressources techniques Microsoft Windows 2000 Server : architecture TCP / IP » afin de lister les services proposés par Microsoft Windows 2000 Server.

Après la lecture de quelques explications sur Internet de l'utilité des serveurs DHCPd, NAMEd et Samba, je me suis vite aperçu que ces applications associées aux serveurs installés par défaut avec Linux offrait la majorité des services rendus par les serveurs Windows 2000.

a) DHCPd, implémentation du protocole DHCP

Le serveur DHCPd est une implémentation pour UNIX du protocole DHCP. Il permet à des ordinateurs fonctionnant sous Microsoft Windows de pouvoir configurer leurs informations IP automatiquement. Certes, le serveur ne se cantonne pas aux stations Windows, des stations UNIX, Linux, MacOS, Microsoft DOS,... peuvent aussi se configurer grâce à lui sous respect du protocole DHCP.

Quels informations IP peuvent bien être pertinentes pour une machine Windows ?

- bien évidemment, son adresse IP : par exemple 10.0.100.254
- le masque du réseau ou sous-réseau : par exemple 255.0.0.0
- l'adresse de diffusion préférée sur ce réseau : par exemple 10.255.255.255
- la durée du bail : par exemple 1 heure
- le nom du réseau auquel la machine appartient : par exemple « ebc-informatique.com »
- les adresses IP des serveurs DNS : par exemple 10.0.0.1
- les adresses IP des passerelles ou routeurs : par exemple 10.0.0.1
- les adresses IP des serveurs WINS : par exemple 10.0.0.1
- l'adresse du serveur DHCP pour le renouvellement du bail : par exemple 10.0.0.1

Dans la grande majorité des réseaux Microsoft, ces informations sont les seules à fournir. Il existe bien sûr une foule d'autres paramètres DHCP dont la liste est donnée, mais la plupart ne sont utiles qu'aux systèmes UNIX/Linux et les autres sont utilisés rarement.

Comment se configure le serveur DHCPd ?

La configuration du serveur DHCPd est effectuée dans un fichier « dhcpd.conf » situé dans le répertoire /etc dans la plupart des cas.

Le fichier de configuration est un fichier texte, totalement compréhensible par l'homme (je veux dire là que ce ne sont pas des mots totalement dénués de sens). Les seules connaissances nécessaires sont la syntaxe correcte des paramètres et de l'architecture du fichier, ainsi que des informations que l'on veut communiquer aux clients et de l'étendue des adresses IP distribuables.

En utilisant les informations du réseau cités dans les exemples quelques paragraphes plus haut, une configuration de base serait la suivante :

```
#
# Exemple de fichier de configuration du serveur DHCPd : /etc/dhcpd.conf
#

# Durée par défaut du bail IP en secondes (ici 1 heure = 3600 secondes)
default-lease-time 3600;

# Durée maximale de bail IP possible en secondes
# (Pour les clients Windows évolués : Windows 2000 par exemple)
max-lease-time 7200;

# Demande de non-prise en charge du DNS dynamique
ddns-update-style none;

# Déclaration correspondant au sous-réseau 10.0.0.0
subnet 10.0.0.0 netmask 255.0.0.0 {

    # Masque de sous-réseau du client
    option subnet-mask 255.0.0.0;

    # Adresse de broadcast préférentielle
    option broadcast-address 10.255.255.255;

    # Nom de domaine auquel appartiendront les clients
    option domain-name "ebc-informatique.com";

    # Adresses IP des serveurs de noms par ordre croissant de préférence
    option domain-name-servers 10.0.0.1;

    # Adresses IP des routeurs par ordre croissant de préférence
    option routers 10.0.0.1;
```

```
# Adresses IP des serveurs WINS par ordre croissant de préférence
option netbios-name-servers 10.0.0.1;

# Etendue des adresses IP distribuables
range 10.0.100.2 10.0.100.254;
range 10.0.101.2 10.0.101.254;
}
```

Ce fichier correspond à la base des configurations. Il existe cependant une variante que j'ai du mettre en place : la mise à jour automatique du serveur DNS lors de l'affectation d'un bail à un ordinateur.

En effet, Microsoft Windows 2000 Server prend en charge cette fonctionnalité. Elle consiste en les points suivants :

- lorsqu'un ordinateur rejoint le réseau et obtient un bail IP de la part du serveur DHCP, ce dernier informe le serveur DNS que cet ordinateur a rejoint le réseau et qu'il faut l'ajouter dans le domaine DNS.
- Lorsqu'un bail arrive à expiration ou se libère, le serveur DHCP doit informer le serveur DNS de ce départ et ce dernier doit mettre sa base de données à jour.

Une question se pose alors, que mettre dans la base de données du serveur DNS (appelé aussi tables DNS) ?

Pour Windows 2000 Server, le nom à insérer dans les tables DNS correspond au nom NetBIOS de l'ordinateur suffixé du nom de domaine indiqué dans la configuration du serveur DHCP.

Sous Linux, cette fonctionnalité est aussi facile à mettre en place : elle nécessite l'une des versions récentes de l'application DHCPd et elle nécessite un serveur DNS dynamique tel que NAMEd qui sera expliqué plus tard.

Le serveur DNS est dit dynamique si ce dernier autorise les mises à jour des correspondances <nom DNS de la machine>=<adresse IP>. Ce type de serveur existe déjà depuis quelques années.

Pour indiquer au serveur DHCPd de mettre à jour le DNS, le paramètre « ddns-update-style » de la configuration précédente doit avoir la valeur « ad-hoc ». Ainsi non seulement les tables DNS en mémoire seront mises à jour, mais ces mises à jour seront directement transcrites dans les fichiers de configuration du serveur DNS afin qu'en cas de panne de ce dernier, les mises à jour ne soit pas perdues.

Mais comment le serveur DHCP connaît-il le serveur DNS à mettre à jour ?

Il effectue des recherches en questionnant le DNS de la machine sur laquelle il est situé afin de connaître l'adresse IP du serveur DNS du domaine à mettre à jour.

Il lui envoie alors directement les requêtes de mises à jour.

Seulement voilà, ce ne devrait pas être aussi simple car des problèmes de sécurité se poserait. Ainsi, le serveur DNS doit être configuré de manière à ce que les demandes de mises à jour ne soient prises en compte que si elles proviennent d'un ordinateur autorisés. De plus, on peut mettre en place un système de mot de passe de sorte que les requêtes de mises à jour DNS du serveur DHCP soient cryptées.

Le serveur DHCP se configure alors en ajoutant les paramètres suivants :

```
# Demande de prise en charge du DNS dynamique
ddns-update-style ad-hoc;

# Déclaration d'une clé de protection pour les mises à jour du DNS
# (ATTENTION : il faudra configurer le serveur DNS en conséquence)
key DHCP_UPDATER {

    # Désignation de l'algorithme de cryptage
    algorithm HMAC-MD5.SIG-ALG.REG.INT;

    # Clé de cryptage
    secret pRP5FapFoJ95JEL06sv4PQ==;
}

# Déclaration d'informations DNS spécifiques à certaines zones
# (Comme par exemple la clé de MAJ à transmettre)

# Zone du domaine « ebc-informatique.com »
zone ebc-informatique.com. {

    # Adresse IP du serveur DNS (facultatif cependant)
    primary 10.0.0.1;

    # Clé à utiliser pour le cryptage
    key DHCP_UPDATER;
}

# Zone du domaine « 10.in-addr.arpa »
zone 10.in-addr.arpa. {
    primary 10.0.0.1;
    key DHCP_UPDATER;
}
```

C'est la méthode de sécurisation la plus élevée à l'heure où ces lignes ont été écrites.

b) NAMED, le serveur DNS de référence

NAMED est une application conçue par l'« Internet Software Consortium » ou ISC (Consortium du logiciel Internet) qui propose des logiciels libres utilisés dans le cadre de l'Internet. Le serveur DHCP cité ci-dessus (DHCPd) provient aussi de ce consortium.

Ce serveur DNS est basé principalement sur deux éléments :

- La configuration du fichier de configuration « named.conf »
- La base de données DNS initiale

Prenons un exemple simple pour expliquer comment se configure un serveur DNS. Voici un schéma expliquant la situation à gérer :

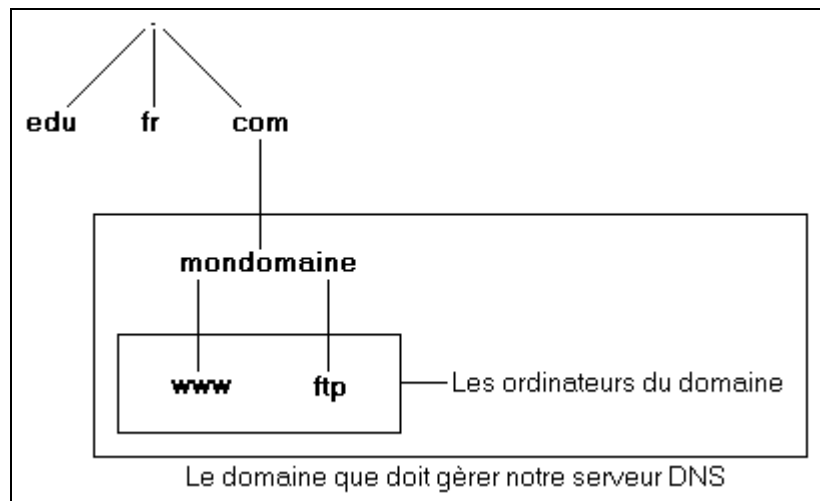


figure 9 : situation à gérer

Nous disposons donc du domaine « mondomaine.com ». Mais nous devons aussi disposer d'une classe d'adresses IP officielles. Prenons par exemple toutes les adresses IP de la forme 200.200.200.X où X est compris entre 0 et 255.

Notre serveur DNS aura donc la charge de la gestion des domaines « mondomaine.com » et « 200.200.200.in-addr.arpa ».

Choisissons des adresses IP pour les deux ordinateurs du domaine : 200.200.200.1 pour la machine **www**, et 200.200.200.2 pour la machine **ftp**. La machine **www** jouera aussi le rôle de serveur DNS.

En premier lieu, il s'agit de configurer le fichier « named.conf ». Le listing commenté suivant correspond au fichier de la situation ci-dessus.

```
/*
 * Fichier /etc/named.conf - Premier fichier lu par named.
 */

options {
    /* Répertoire des fichiers de la base de données */
    directory "/var/named";
};

/*
 * Enregistrement correspondant au serveurs de la racine « . »
 */

zone "." {
    type hint;
    file "named.ca";
};
```

```

/*
 * Fichier utilisé pour la résolution inverse des adresses IP commençant
 * par 127.0.0 (classe d'adresse non connectée à Internet utilisée uniquement
 * pour envoyer des données sur soi-même (enfin, sur sa machine))
 */

zone "0.0.127.in-addr.arpa" {
    type master;
    file "db.127.0.0";
};

/*
 * Fichier utilisé pour la résolution des noms se terminant par mondomaine.com
 */

zone "mondomaine.com" {
    type master;
    file "db.mondomaine.com";
};

/*
 * Fichier utilisé pour la résolution inverse. Les adresses IP commençant
 * par 200.200.200 peuvent être résolues en nom d'hôte dans le fichier
 * spécifié.
 */

zone "200.200.200.in-addr.arpa" {
    type master;
    file "db.200.200.200";
};

```

Dans cette configuration, le serveur ne gère que son domaine et enverra toutes les requêtes vers un autre domaine aux serveurs de la racine.

Le serveur est configuré en tant que serveur maître du domaine sur celui-ci. Etre serveur DNS maître d'un domaine indique que l'on est le seule apte à gérer ce domaine. Par opposition, les tables d'un serveur DNS esclave ne sont en fait que des copies conformes des tables du serveur DNS maître. Ceci permet de prévenir les éventuelles pannes et permet aussi de décharger le serveur DNS maître d'une partie des requêtes dans le cas de grand réseau.

Voyons maintenant les fichiers de la base de données DNS. Le premier, « named.ca. », est fourni d'office avec le serveur DNS. Il est aussi téléchargeable sur Internet sur le site de l'ISC par exemple. Ce fichier contient les adresses IP des serveurs de noms à la racine et ne doit pas être modifié.

Le second fichier, « db.127.0.0. » permet de résoudre particulièrement l'adresse 127.0.0.1 qui correspond au « loopback », c'est à dire à une boucle sur soi-même. Une machine envoyant un paquet sur 127.0.0.1 se l'envoie en fait à elle-même.

```

; db.127.0.0 : domaine « 0.0.127.in-adrr.arpa »
;
; Début d'autorité (SOA=Start Of Authority). Quel est le serveur de noms
; primaire pour ce domaine ? www.mondomaine.com. Quel est l'adresse mail de la
; personne à contacter en cas de problèmes ? root@www.mondomaine.com.
; @ représente le domaine courant, c'est à dire 0.0.127.in-addr.arpa.

@      IN      SOA      www.mondomaine.com.    root.www.mondomaine.com. (

```

```

; Les options qui suivent ne concernent que les serveurs de noms esclaves.
; Elles définissent les modalités des mises à jour.

    1997022700 28800 14400 3600000 86400
)

; "www.mondomaine.com." est le serveur de noms pour le domaine.

    IN      NS      www.mondomaine.com.

; l'adresse 127.0.0.1 sera associée au nom "localhost." (machine locale).

1      IN      PTR      localhost.

```

Le fichier « db.mondomaine.com » permet de résoudre les noms des machines du domaine « mondomaine.com » en leurs adresses IP. Voici son listing :

```

; db. www.mondomaine.com : domaine « mondomaine.com. »
;
; Début d'autorité

@      IN      SOA      www.mondomaine.com.      root.www.mondomaine.com. (
    2000070306 3600 900 1209600 43200
)

; Permet d'associer le domaine local (@) a l'adresse IP 200.200.200.1
    IN      A      200.200.200.1

; Commentaires sur le serveur DNS
    TXT      "Serveur DNS primaire de mondomaine.com"

; "www.mondomaine.com" est le seul serveur de noms du domaine.
@      IN      NS      www.mondomaine.com.

; Echange de mail : tout mail envoyé au domaine, doit être redirigé vers
; www.mondomaine.com., ainsi, l'adresse mail steve@mondomaine.com sera en
; réalité steve@www.mondomaine.com.
@      IN      MX      10      www.mondomaine.com.

; Liste des machines du domaine avec leurs adresses IP.
www      IN      A      200.200.200.1
ftp      IN      A      200.200.200.2

; localhost, pour l'interface de bouclage.
localhost IN      A      127.0.0.1

; Quelque alias (CNAME) : un nom d'hôte précisé par un enregistrement de
; type A peut avoir un ou plusieurs alias. Dans l'exemple ci-dessous,
; mail.mondomaine.com. => www.mondomaine.com.
mail     CNAME     www.mondomaine.com.

```

Et finalement, le fichier permettant la résolution inverse des adresses du type 200.200.200.X en noms de machines correspondant.

```

; db.200.200.200 : domaine « 200.200.200.in-addr.arpa »

@      IN      SOA      www.mondomaine.com.      root.www.mondomaine.com. (
    2000070305 3600 900 1209600 43200
)

; Serveur de noms pour le domaine.
    IN      NS      www.mondomaine.com.

```



```
; Associe des adresses IP a des noms.
1      IN      PTR      www.mondomaine.com.
2      IN      PTR      ftp.mondomaine.com.
```

Bien entendu, les possibilités de paramétrage du serveur DNS sont aussi vastes qu'il y a d'ordinateurs sur Internet, mais seule une configuration correspond à ses propres besoins.

En ce qui concerne le DNS dynamique dont j'ai parlé quelques pages auparavant, il faut configurer le serveur NAMED afin que ce dernier accepte les requêtes de mises à jour d'un serveur DHCP. J'ai expliqué que le serveur DHCP envoie des requêtes de mises à jour cryptées selon une clé de cryptage. Cette dernière doit être connue du serveur NAMED, ainsi que la méthode de cryptage utilisée. Pour ce faire, il faut modifier le fichier « named.conf » comme suit :

```
/*
 * Fichier /etc/named.conf - Premier fichier lu par named.
 */

options {
    /* Répertoire des fichiers de la base de données */
    directory "/var/named";
};

/*
 * Désignation de la clé ainsi que de son algorithme de cryptage
 */

key DHCP_UPDATER {
    algorithm HMAC-MD5.SIG-ALG.REG.INT;
    secret PRP5FapFoJ95JEL06sv4PQ==;
}

/*
 * Enregistrement correspondant aux serveurs de la racine « . »
 */

zone "." {
    type hint;
    file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "db.127.0.0";
};

zone "mondomaine.com" {
    type master;
    file "db.mondomaine.com";

    /* Autoriser les mises à jour des tables DNS au détenteur de la clé */
    allow-update { key DHCP_UPDATER; };
};

zone "200.200.200.in-addr.arpa" {
    type master;
    file "db.192.168.1";

    /* Autoriser les mises à jour des tables DNS */
    allow-update { key DHCP_UPDATER; };
};
```

c) L'IP Masquerade

L'étude de l'IP Masquerade n'était pas demandé dans le cadre du stage, mais en trouvant par hasard sur Internet un document anglophone relatant de ses possibilités, j'avais absolument envie de tester cet aspect. N'ayant plus beaucoup de temps à ma disposition, je ne me suis pas trop attardé sur cette option, mais j'en ai quand même observé les principaux attraits.

Tout d'abord, j'ai du rechercher comment mettre en place un tel procédé et je me suis rendu compte que c'était assez simple. J'ai utilisé plus de temps à configurer l'accès à Internet du serveur Linux que de mettre en place l'IP Masquerade. Il suffisait de mettre quelques variables mémoire (on modifie directement la valeurs des variables systèmes dans la mémoire de l'ordinateur) à une certaine valeur et le tour était joué...

Cependant, malgré que l'accès à Internet des clients du réseau local fonctionnait, ces derniers ne pouvaient se connecter à un serveur FTP parce le mode de fonctionnement de ce dernier est atypique. Des recherches sur Internet m'ont apportés la solution et des modifications sur le système Linux étaient nécessaires.

Les règles de filtrage des paquets de données m'ont le plus intéressées. La prise en main du logiciel « IP Chains » fourni par défaut avec Linux n'a pas été aisé, mais des sites web expliquaient comment l'utiliser. J'ai alors testé plusieurs cas de figures sur le réseau local, au grand dépend de mon camarade de l'I.U.T. Philippe Hahn, qui utilisait également ce réseau local dans le cadre de son stage...

Il m'est alors venu l'idée de reprendre un script, conçu par un anglais, qui permettait de mettre en place l'IP Masquerade, et d'y ajouter toutes les autres options que j'avais vu aux cours de ces quelques jours passés à étudier ce principe : possibilité d'utiliser une connexion FTP, mise en place des règles de filtrage,... Je l'ai commenté et j'ai écrit une succincte documentation sur l'IP Masquerade.

d) Samba

Samba est magnifique, mais pas simple à configurer ! Lorsque l'on voit les possibilités de ce logiciel, et les développements en cours, on se demande vraiment pourquoi des gens paient très cher des licences Windows NT Server alors que Samba est gratuit...

A sa version 2.2.0, voici ce que sait faire Samba :

- serveur de fichiers : permet de partager des espaces disques avec des clients ;
- serveur d'impression : les clients peuvent utiliser les imprimantes que Samba partage ;
- contrôleur de domaine Windows 95/98 : l'accès à un ordinateur fonctionnant sous Windows 95/98 est sujet à une authentification ;
- explorateur maître local : permet aux clients d'explorer les ordinateurs de leur groupe de travail plus rapidement, sans passer par la diffusion vers chaque machine du réseau ;
- explorateur maître du domaine ; permet aux clients de lister l'ensemble des ordinateurs de l'ensemble des groupe de travail du réseau ;
- serveur primaire WINS : permet de résoudre un nom NetBIOS en adresse IP ;
- proxy WINS : serveur primaire d'un groupe de travail.

Actuellement en cours de finalisation, les fonctionnalités de contrôleur primaire de domaine NT sont pourtant déjà très intéressantes. En effet, Samba peut jouer le rôle de serveur d'authentification pour Windows NT, permet de donner à un ou des individus des privilèges d'administrateurs, des privilèges d'invités ou d'utilisateurs (les 3 catégories d'utilisateurs sous Windows NT), permet le montage automatique de partage (des partages sont montés automatiquement sous des lettres de lecteurs) et gère parfaitement les profils itinérants (sur n'importe quel ordinateur de votre réseau, votre bureau, vos raccourcis, votre liste de programmes, vos favoris Internet sont les mêmes).

Que ne sait pas faire Samba ?

Pour poursuivre sur les fonctionnalités de PDC (contrôleur primaire de domaine) Windows NT, Samba ne gère pas encore bien la notion de groupes sous Windows NT et le téléchargement de stratégies systèmes à l'ouverture des sessions (par exemple, interdire l'accès au lecteur de disquette,...) est en phase de finalisation et de test.

De plus, Samba ne sait pas faire :

- contrôleur de domaine de sauvegarde ;
- explorateur local de sauvegarde ;
- serveur WINS secondaire.

Pour dire à Samba quoi faire et comment le faire, se dernier se configure à l'aide d'un seul fichier : le fichier « smb.conf », avec, éventuellement, des fichiers annexes tels que des bases de mots de passes,...

Voici l'architecture générale d'un fichier « smb.conf » :

```
;
; SAMBA : Architecture du fichier smb.conf
;

; Section global
[global]
```

Dans cette section sont regroupés les paramètres liés au comportement général du serveur Samba. On y retrouvera obligatoirement les informations liés à NetBIOS tel que le nom NetBIOS du serveur et le groupe de travail auquel il appartient. De plus, on indiquera les méthodes de résolutions des noms NetBIOS ainsi que les éventuelles fonctionnalités WINS prises en charge par Samba (si ce dernier doit être serveur ou proxy WINS). De plus, c'est ici qu'on indiquera à Samba qu'il doit tenter de devenir explorateur maître du groupe de travail ou du domaine.

C'est aussi dans cette section que l'on définira le mode de sécurité de Samba, c'est à dire les modes d'authentification des utilisateur pour accéder à leurs partages, ainsi que les ordinateurs autorisés à accéder au serveur Samba en indiquant des plages d'adresses IP ou des noms de domaines DNS.

On y verra aussi des paramètres liés au fonctionnement de Samba tel que les emplacements de fichiers journaux (permettant de garder une trace des actions effectués sur et par le serveur Samba), les modalités de créations des fichier journaux (par ordinateur connecté, par utilisateur, par système d'exploitation,...)

On y définira aussi le style d'impression du système hébergeant Samba : UNIX à des méthodes d'impression différente de Linux.

```
; Section homes
[homes]
```

Cette section est paramétrable en fonction de l'utilisateur qui se connecte. Elle est utilisé pour partager le répertoire personnel UNIX d'un utilisateur. On y indiquera des informations telles que les permissions UNIX des fichiers créés, les types de fichiers considéré comme caché sous Windows,...

```
; Section printers  
[printers]
```

Cette section permet d'indiquer les paramètres liés aux imprimantes : répertoire des fichiers temporaires, utilisateurs autorisés à les utiliser,...

En plus de ces sections, dont, seul la section global est obligatoire. On peut définir des partages.

```
; Exemple de partage  
[monpartage]
```

Dans chacun des partages, on devra définir son « comportement » : lecture seule ou autorisation d'écriture, permissions d'accès,...

Le travail que j'ai du effectuer a été de concevoir et de tester des fichiers de configurations standardisés pour chacune des fonctionnalités prises en charge par Samba. Vous trouverez en annexe de ce document l'ensemble de ces configurations.

e) Journal de bord

Les actions sont données dans l'ordre chronologique de leur exécution.

1ere semaine : du 17/04/2001 au 22/04/2001

Proposition de la part du maître de stage d'extension du sujet de stage : initialement cantonné à l'étude de Samba, il s'est étendue à l'étude complète de l'intégration d'une plate-forme Linux dans réseau Microsoft grâce à trois applications Samba, DHCPd et NAMED.

Dans un premier temps, j'ai découvert Windows 2000 coté serveur. Tout ce qui est administration Windows NT m'était presque totalement inconnu. Je ne disposais par d'un serveur Windows 2000, mais le livre « Kit de ressources techniques Microsoft Windows 2000 Server : architecture TCP/IP » était très bien fait et il expliquait en détail le déroulement des différentes opérations sous Windows 2000. J'ai feuilleté rapidement ce livre pour en voir les grandes lignes sans rentrer dans le détail.

Je me suis alors attelé à l'étude du protocole DHCP que ce même livre expliquait dans les moindres détails.

Après cette lecture instructive, j'ai recherché des informations sur Internet concernant le fonctionnement d'un serveur UNIX/Linux. J'ai alors compris le principe des démons, l'utilité et l'usage des plus intéressants d'entre eux.

2e semaine : du 23/04/2001 au 29/04/2001

C'est pendant cette semaine que je me suis vraiment intéressé de plus près au serveur DHCPd. Dans un premier temps, j'ai utilisé celui disponible à la base sur une distribution Red Hat Linux 7.

J'ai recherché des documents sur Internet relatant la configuration du serveur. Et n'ayant trouvé que des documents succincts, expliquant principalement l'architecture du fichier de configurations dans ses grandes lignes, j'ai entamé la traduction des pages man de la documentation Linux.

Ayant passés deux jour à lister les paramètres et à les décrire dans leurs grandes lignes, j'ai sélectionné les plus pertinents d'entre eux et j'ai rédigé une configuration de base.

J'ai ensuite testé cette dernière sur le réseau local mis à ma disposition qui comprenait un gros serveur et deux portables (le mien et celui d'un camarade de l'IUT également en stage au centre de compétences UNIX). J'ai également observé le comportement des machines Windows lors de l'expiration de bail, dans le cas où les informations fournies sont inexactes,...

3e semaine : du 30/04/2001 au 06/05/2001

A ce stade des opérations, j'ai délaissé DHCP pour me mettre à l'étude du DNS. J'avais déjà vu lors de la formation de l'IUT le principe du DNS, ainsi que les rudiments de l'administration. J'avoue à ce moment là n'avoir compris que les grandes lignes et non les détails.

La semaine a donc débuté par des recherches sur Internet de pages web, de documents expliquant le DNS, son principe, sa mise en place.

L'ouvrage « DNS and BIND » des éditions O'Reilly m'a été d'une grande utilité. En effet, ce dernier, malgré qu'il relatait l'administration de serveurs DNS assez ancien (à l'échelle de l'informatique), expliquait le DNS de tel façon que tout devenait plus simple...

J'ai alors configuré le serveur DNS installé par défaut sur le serveur Linux pour le réseau local. J'ai testé plusieurs cas de figure pour bien m'imprégner de la méthode et sauvegardé chaque configuration pour leurs consultations ultérieures.

4e semaine : du 07/05/2001 au 13/05/2001

Lors de la lecture du livre sur l'administration Windows 2000 Server, dans le chapitre concernant le service DHCP, un point m'avait paru particulièrement intéressant, celui concernant la mise à jour du serveur DNS par le serveur DHCP. Je me suis alors étonné de ne pas avoir vu dans la documentation du serveur DHCP un quelconque paramètre permettant ces mises à jour.

J'ai ainsi recherché des informations concernant le DNS dynamique sur Internet et mis à part des documents expliquant ce que c'est, je n'ai trouvé qu'un « patch » (mise à jour) expérimental d'un particulier pour le serveur DHCP que j'utilisais qui permettrait à ce dernier de prendre en charge les requêtes de mises à jour.

L'installation du patch a été aisée et j'ai immédiatement pu tester le DNS dynamique. Je me suis alors rendu compte d'une grossière erreur d'algorithme : si un ordinateur rejoignait le réseau, et que ce même ordinateur portait le même nom qu'une autre machine déjà enregistré dans les tables DNS, ce nouvel ordinateur remplaçait l'entrée de l'ordinateur déjà existant dans la base de données DNS, ce qui, m'a fois, n'était pas très logique. Lors de l'installation du patch, des incursions dans le code source devait être effectué pour le configurer. Ce code source était écrit en PERL et était très bien commenté, il a donc été aisé de retrouver la procédure construisant les requêtes de mises à jour et de la modifier. Le serveur était alors à peu près correcte. Quelques tests satisfaisant s'ensuivaient.

5e semaine : du 14/05/2001 au 20/05/2001

Cette semaine a été la semaine de découverte de Samba.

Dans un premier temps, j'ai lu les grandes lignes des ouvrages « Samba : L'intro » et « Using Samba » afin de voir ce que permettait de faire Samba.

J'ai alors listé les grandes lignes des fonctionnalités offertes par Samba et j'ai testé quelques configurations minimales trouvées de ça et là sur Internet, pour voir...

C'est pendant cette semaine que j'ai débuté la rédaction du rapport de stage, à la demande de mon tuteur de stage.

6e semaine : du 21/052001 au 27/052001

Mon tuteur de stage m'avait relaté un article paru dans la presse linuxienne (spécialisé dans le système d'exploitation Linux) de la sortie d'une nouvelle version du serveur DHCP qui implémentait pleinement les mises à jour des tables DNS.

Je me suis alors rendu sur le site de l'« Internet Software Consortium » lequel effectivement diffusait une nouvelle version de son serveur DHCPd et dont la description indiquait clairement qu'il prenait en charge le DNS dynamique.

J'ai immédiatement désinstallé le serveur DHCP que j'utilisais pour installer cette nouvelle version et effectivement, sans mise à jour, sans aucune configuration supplémentaire, sans incursions dans le code source, le serveur DNS était mis à jour à chaque fois qu'une machine joignait ou quittait le réseau à sa charge.

De nouveaux paramètres étaient alors apparus et je me suis chargé de modifier les configurations que j'avais écrites afin de les rendre conformes aux nouvelles options, en particulier celles concernant le cryptage des requêtes de mises à jour.

C'est aussi pendant cette semaine que j'ai trouvé, par hasard, un document concernant « l'IP Masquerade ». J'ai donc décidé de mettre en place cette option pour le réseau local et j'ai conçu, grâce à des recherches sur Internet, un script de lancement de cette fonctionnalité de Linux. Cela m'a occupé pendant 4 jours.

7e et 8e semaine : du 28/052001 au 10/06/2001

Je me suis remis à Samba pour ces deux semaines, mais en explorant plus profondément les paramètres du fichier smb.conf.

J'ai alors écrit des configurations pour la plupart des fonctionnalités offertes par Samba, sauf pour la plus intéressante : Samba en tant que contrôleur de domaine NT.

Pourquoi, simplement parce que la version de Samba dont je disposais (2.0.7) n'offrait que des services d'authentification et d'exécution de script au démarrage. La version 2.2.0 que j'avais installé par la suite offrait déjà des services plus évolués et j'ai alors pu mettre en place un vrai contrôleur de domaine Windows NT. Mis à part quelques fonctionnalités non prises encore en charges, Samba fait preuve de capacité étonnante dans ce domaine. Il aurait été intéressant, si plus de temps m'était imparti, d'étudier l'administration Windows NT afin de mieux rendre compte des capacités de Samba.

9e et 10e semaine : du 11/06/2001 au 24/06/2001

Pendant ces deux semaines, j'ai rédigé l'ensemble de la documentation sur mon travail. Je n'avais, hélas, pas vraiment encore commencé ce travail de rédaction et je me suis rendu compte bien vite que j'aurais dû commencer plus tôt...

V] Bilan

Les principaux objectifs du stage ont été atteints et le travail accompli semble satisfaire le maître du stage. Le degré de qualité ne pourra être évalué que lors de l'utilisation de ma documentation et de mes configurations dans le cadre d'une mise en place d'un système dans une entreprise.

Concernant le devenir de mon travail, il est fort probable que certaines études deviennent obsolètes. Par exemple, l'utilisation de Samba en tant que contrôleur primaire d'un domaine NT n'en est encore qu'au stade expérimental (certes bien avancé, mais la « Samba Team » insiste bien sur ce point) et les quelques paramètres relatifs à son fonctionnement peuvent être modifiés

dans les versions suivantes du serveur (comme ils l'ont été entre, par exemple, la version 2.2.0 et les versions précédentes). De plus, l'apparition de l'IPv6 (adresses IP des machines codés sur 16 octets au lieu de 4 pour palier au manque d'adresses IP officielles distribuables dû à l'explosion d'Internet) risque fort de modifier fondamentalement le serveur DNS et sa configuration et de rendre inutile l'utilisation d'un serveur DHCP... Mais cette nouvelle version du protocole IP n'est pas encore mise en place et ne le sera pas avant plusieurs années encore.

VI] Conclusion personnelle

Ce stage a été très bénéfique pour moi. Il m'a permis d'acquérir des notions nouvelles en relation avec la mise en place et l'administration de réseaux. Linux ne m'était pas totalement inconnu avant, mais ce stage m'a permis de l'explorer un peu plus profondément. Son fonctionnement et son administration me sont dorénavant beaucoup plus clairs. Le monde du libre, ma séduit par sa gratuité et sa philosophie. Il correspond à l'idée que je me fais de l'Internet : gratuité et liberté d'utilisation de tous programmes ou informations qui s'y trouvent. Mais Windows m'a également beaucoup étonné. Ce système d'exploitation offre malgré sa mauvaise réputation, une quantité de services dont je ne connaissais même pas l'existence.

Autre point important, j'ai pu me rendre compte du clivage entre monde étudiant et monde professionnel, ce dernier étant beaucoup plus contraignant que je ne le pensais. En effet, étant étudiants, nous sommes trop souvent tentés par le syndrome de la « bidouille » : on installe, on met des choses en place, on regarde si ça fonctionne, sinon on rajoute des options par ci et des options par là et ainsi de suite... (je caricature, mais c'est la réalité). Le monde professionnel ne permet pas cela, et mon maître de stage a bien réussi à me communiquer cette idée : un réseau performant et un réseau propre où chaque élément est à sa place. De même, un système propre est plus facile à administrer et à gérer...

Concernant l'aspect économique de Linux, on peut se demander comment un système gratuit peut-il intéresser une entreprise ? Je me posais cette question avant le stage et ce dernier a permis de m'inculquer la notion de service. En effet, Linux est gratuit... mais la mise en place du système demande des experts dans le domaine. Il n'est en effet pas donné à tout un chacun d'installer et de configurer Samba ou un serveur DNS, voir même tout simplement d'installer Linux... Windows est intuitif. La dernière version du système d'exploitation serveur de Microsoft, Windows 2000 Server, est facile d'installation, de prise en main, d'administration,... Mais Windows n'est pas stable et il est capricieux !

En analysant le déroulement du stage, je me rend compte que je n'ai rencontré que peu de difficultés. Le matériel mis à ma disposition était amplement suffisant, mais nécessaire. La suite logiciel disponible correspondait à mes besoins. La documentation fournie et l'accès à Internet me permettaient de résoudre l'ensemble des problèmes rencontrés dans des délais corrects.

Et si je devais tout refaire à l'identique, ma démarche serait différente. J'approcherais mon travail de façon plus méthodologique que je ne l'ai fait, en définissant un vrai planning de tâches à effectuer. De plus, je ne ferais pas la documentation seulement en fin de stage, mais j'y ajouterais des éléments chaque jour ou chaque semaine.

VII] Sources d'informations

a) Bibliographie

Voici la liste des ouvrages francophones consultés lors du stage :

Kit de ressources techniques Microsoft Windows 2000 Server : architecture TCP / IP

De la Microsoft Corporation
Edité par Microsoft Press
ISBN : 1-57231-805-8
Année : 2000

SAMBA : L'intro

De Gerald Carter et Richard Sharpe
Edité par CampusPress
ISBN : 2-7740-0745-5
Année : 1999

TCP/IP Administration de réseau

De Craig Hunt
Edité par O'Reilly & Associates, Inc.
ISBN : 2-87908-030-4
Année : 1995

Et voici la liste des ouvrages anglophones consultés :

DNS and BIND

De Paul Albitz et Cricket Liu
Edité par O'Reilly & Associates, Inc.
ISBN : 1-56592-236-0
Année : 1997


Using Samba (Electronic release)

De Robert Eckstein, David Collier-Brown et Peter Kelly
Edité par O'Reilly & Associates, Inc.
ISBN : 1-56592-449-5
Année : 1999

b) Sites Internet consultés

Voici les sites Internet que j'ai le plus consultés au cours du stage :

Adresse Internet	Description
http://www.toolinux.com/	Site sur Linux qui explique la majorité de ses aspects, de l'installation, de l'administration et de l'utilisation.
http://www.lea-linux.org/	Site de « Linux Electronique Aide », dont le sujet est le même que celui énoncé précédemment.
http://www.samba.org/	Site officiel de Samba et de la Samba Team.
http://www.isc.org/	Site de l'Internet Software Consortium.
http://www.linuxdoc.org/	Site du « Linux Documentation Project ».
http://www.linuxiso.org/	Site de téléchargement de la plupart des distributions Linux.
http://www.google.fr/ http://fr.altavista.com/ http://fr.yahoo.com/	Moteurs de recherche de sites Internet

Référence rapport :	0	1	0	2	3
Etudiant : FUCHS Steve					
 EBC Informatique					

Mots clés : UNIX Linux Réseau Administration Serveur Samba DHCP DNS IP Masquerade	Matériel/Système informatique utilisé : Serveur Intel Pentium III 800MHz Portable Toshiba Intel Pentium Hub Imprimante
	Logiciels utilisés : Linux Red Hat 7.0 DHCPd NAMEd Samba 2.2.0 Microsoft Windows 98 Microsoft Windows Workstation NT 4 (SP6) Microsoft Office 2000

Enoncé du sujet : Etude de l'intégration d'une plate forme Linux au sein d'un réseau Microsoft Windows.
Résumé : La finalité du stage était de pouvoir substituer un serveur Linux à un serveur Windows NT au sein d'un réseau composé de clients Microsoft Windows. On pourrait banaliser un serveur Windows NT en un ensemble de fonctionnalités dissociables : serveur DHCP, serveur DNS, serveur de fichiers, d'authentification,... Trois programmes du monde UNIX/Linux sont capables chacun de remplir certaines de ses fonctionnalités : - DHCPd est un démon serveur DHCP - NAMEd est un démon serveur DNS - SAMBA permet de partager des fichiers, des imprimantes, d'offrir les fonctionnalités WINS des serveurs Windows NT, de jouer le rôle d'explorateur de domaines Microsoft, de prendre en charge l'authentification des utilisateurs dans un domaine Windows NT ou 9x. Mon travail a été de concevoir des configurations « prêtes à l'emploi » pour ces trois applications qui remplaceraient les fonctionnalités des serveurs Windows NT.