N° d'ordre : 12 / TRC Année Universitaire 2004 / 2005

UNIVERSITE D'ANTANANARIVO

ECOLE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT TELECOMMUNICATION

MEMOIRE DE FIN D'ETUDES

en vue de l'obtention

du DIPLOME d'INGENIEUR

en Télécommunications

Spécialité: Transmission – Réseau – Commutation

par : **RAMAMONJISOA Falihanta Domoina**

ETUDE ET INSTALLATION DU RESEAU CLIENT SERVEUR AU SEIN DU DEPARTEMENT TELECOMMUNICATION

Soutenu le Mercredi 01 Février 2006 devant la Commission d'Examen composée de :

Président : Monsieur RANDRIAMITANTSOA Paul Auguste

Examinateurs :

Monsieur RANDRIARIJAONA Lucien Elino

Monsieur RANDRIANTSIRESY Ernest

Monsieur BOTO ANDRIANANDRASANA Jean Espérant

Directeur de mémoire: Monsieur RATSIMBAZAFY Andriamanga

" Efa niady ny ady tsara aho, nahatanteraka ny fihazakazahako aho, nitahiry ny finoana aho "

II Timoty 4 : 7

REMERCIEMENTS

Ce mémoire n'ayant pu être achevé sans l'apport en conseil, le soutien matériel et moral de certaines personnes que je voudrais bien remercier :

- Monsieur RANDRIANOELINA Benjamin, Directeur de l'Ecole Supérieure Polytechnique d'Antananarivo.
- Monsieur RANDRIAMITANTSOA Paul Auguste, Chef de Département Télécommunication à l'Ecole Supérieure Polytechnique d'Antananarivo, qui a bien voulu présider cette soutenance.
- Monsieur RATSIMBAZAFY Andriamanga, Enseignant chercheur à l'Ecole Supérieure Polytechnique d'Antananarivo, qui a apporté aides et conseils inestimables durant la réalisation de ce mémoire.
- Messieurs RANDRIARIJAONA Lucien Elino, RANDRIANTSIRESY Ernest et BOTO ANDRIANANDRASANA Jean Espérant, qui ont voulu consacrer leur précieux temps pour juger ce travail.

Merci également à :

- Mes amis (es), pour les échanges d'idées enrichissantes et leurs aides matérielles.
- Dada et Neny, pour leurs appuis moral et financier durant toutes les années d'études que j'ai passés et pendant l'élaboration de ce mémoire.
- Ma famille pour leur soutien.

Enfin, je n'oublie pas de remercier Dieu pour la grâce et la force qu'Il m'a offerte.

AVANT PROPOS

Cet ouvrage est un travail de mémoire de fin d'études en vue de l'obtention du diplôme d'Ingénieur en Télécommunication.

Ce travail concerne l'étude et l'installation du réseau client - serveur au sein du Département Télécommunication de l'Ecole Supérieure Polytechnique d'Antananarivo.

Le but de cette étude est non seulement de mettre en œuvre un réseau, mais aussi de faire apparaître l'utilisation d'un récent système d'exploitation Fedora Core 4 de Linux.

Certes, ce livre n'était pas suffisant pour tout savoir sur le réseau et la distribution Fedora néanmoins il essayerait de nous expliciter les éléments de base fondamentaux.

TABLE DES MATIERES

ABREVIATIONS

ACR	Attenuation Crosstalk Ratio
ANSI	American National Standard Institute
API	Application Programing Interface
ARCNET	Attached Resource Computer Network
BNC	British Naval Connector
BSC	Binary Synchronous Communication
CPU	Central Processor Unit
CSMA / CA	Carrier Sense Multiple Access / Collision Avoidance
CSMA / CD	Carrier Sense Multiple Access / Collision Detection
DARPA	Defense Advanced Research Project Agency
DNA	Digital Network Architecture
DNS	Domain Name Service
DOD	Department Of Defense
DSA-DCM	Distributed System Architecture-Distributing Computing Model
DTS	Data Telecom Service
FAI	Fournisseur d'Accès Internet
FCS	Frame Check Sequence
FTP	File Transfer Protocol
FTP	Foiled Twisted Pair
GOF	Glass Optic Fiber
GPL	General Public Licence
HDLC	High-level Data Link Control
HSTR	High Speed Token Ring
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IANA	Internet Assigned Numbers Authority
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers

IGMP	Internet Group Managment Protocol
IP	Internet Protocol
ISO	International Standard Organisation
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitan Area Network
MAU ou MSAU	MultiStation Access Units
MIC	Media Interface Connector
NFS	Network File System
NIC	Network Interface Card
NRZ	No Return to Zero
NS	Name Server
OSI	Open System Interconnection
PC	Personal Computer
POF	Polymer Optic Fiber
PPP	Point to Point Protocol
QoS	Quality of Service
RAM	Random Access Memory
RL	Return Loss
RZ	Return to zero
SFD	Start Frame Delimiter
SGBD	Système de Gestion de Base de Données
SGBDR	Système de Gestion de Base de Données Relationnel
SLIP	Serial Line Internet Protocol
SMB	Service Message Block
SMTP	Simple Mail Transport Protocol
SNA	System Network Architecture
SOA	Start Of Authority
SQL	Structured Query Language
SSL	Secure Socket Layer
STP	Shielded Twisted Pair

TCP	Transmission Control Protocol
TelNet	Teletype Network
TLS	Transport Layer Securilty
TTL	Time To Live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
VDI	Voix Données Images
VSFTPD	Very Secure File Transfer Protocol Daemon
WAN	Wide Area Network
WiBro	Wireless Broadband
WiFi	Wireless Fidelity
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WWW	World Wide Web

INTRODUCTION

L'Ecole Supérieure Polytechnique d'Antananarivo, notamment le Département Télécommunication, a pour mission de former des Ingénieurs en télécommunication.

La formation se fait en mode tant théorique que pratique. En effet, le Département dispose d'équipements électronique analogique, d'équipements électronique numérique ainsi que de plusieurs équipements informatiques. L'existant informatique se résume à des ordinateurs et des commutateurs.

Dans cet ouvrage, nous allons étudier l'installation d'un réseau local informatique dans ce Département en partant du câblage jusqu'à la mise en service du réseau.

Les besoins sont à la fois simples et classiques : permettre aux utilisateurs (postes clients) d'accéder au système d'information du serveur, s'ouvrir sur l'Internet pour accéder aux informations extérieures.

Ce travail contient huit chapitres. Les trois premiers concernent les généralités, les technologies, les performances et sécurités dans le réseau local. Les deux chapitres qui suivent parlent de l'étude de l'installation d'un système client - serveur. Et les trois derniers chapitres traiteront les applications et l'exploitation du réseau.

CHAPITRE 1 GENERALITES SUR LE RESEAU LOCAL

1 . 1 . Terminologie [1]

Un « réseau local » est un ensemble d'éléments matériels et logiciels, qui met en relation physique et logique, des ordinateurs et leurs périphériques, à l'intérieur d'un site géographiquement limité. Son but est de permettre le partage de ressources communes entre plusieurs utilisateurs.

On emploie généralement les termes de :

☞ LAN pour un réseau géographiquement limité à l'entreprise ou à un bâtiment ;

☞ MAN ou réseau de campus pour un réseau s'étendant sur des distances ne dépassant pas les 10km ;

☞ WAN pour des LAN interconnectés ou des stations réparties sur de grandes distances.

Les différentes catégories de réseaux citées ci-dessus peuvent être représentées par le schéma suivant :

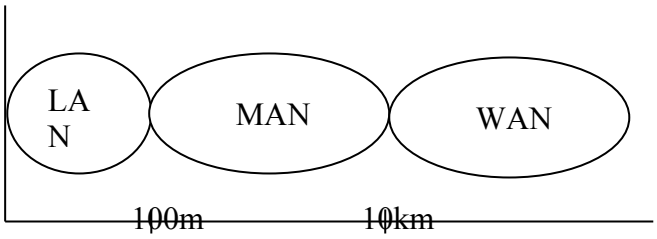


Figure 1 . 01 : Les catégories de réseaux locaux

1 . 2 . Topologies [1]

La topologie définie la manière d'interconnecter les différents équipements qui composent le réseau. On distingue trois types de topologies :

1 . 2 . 1 . Topologie en bus

Dans la liaison en bus, les stations de travail connectées se partagent une même voie de transmission. Le câble coaxial est le support de transmission fréquemment utilisé. Toutefois, du fait des faibles débits supportés par ces câbles coaxiaux (10Mbps), cette topologie est en régression dans les réseaux locaux.

Avantages : - Economie de câble.

- Mise en œuvre facile.

Inconvénients :

- Si le câble principal (épine dorsale ou backbone) est touché, toutes les stations se retrouvent en panne. De plus, sur un même câble encastré, par exemple dans le sol, il n'est pas facile de diagnostiquer l'endroit exact de la rupture. Il faut donc tout ouvrir.
- Faible sécurité sur tout le réseau due au média partagé.
- Ralentissement du trafic en cas de nombreuses stations.

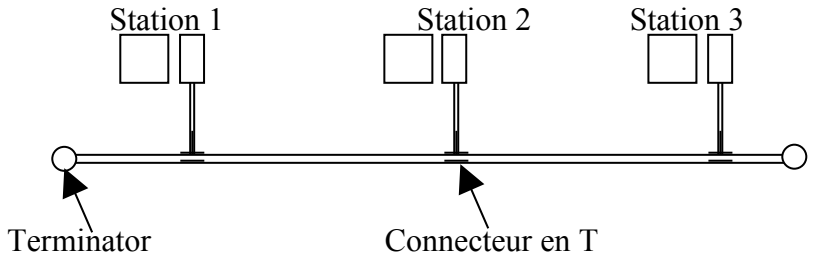


Figure 1 . 02 : Topologie en bus

1 . 2 . 2 . Topologie en étoile

La liaison la plus simple entre deux stations de travail est celle qui ne comporte que deux extrémités. Une telle liaison est dite point à point. Un ensemble de liaison point à point axées autour d'un nœud central (concentrateur ou commutateur) va former une configuration étoile.

La topologie en étoile est la plus utilisée en réseau local.

Avantages : - La simplicité : les stations de travail sont reliées directement au serveur.

- La gestion de ressources est centralisée.
- Si un ordinateur tombe en panne ou si un câble de liaison est coupé, un seul ordinateur est affecté et le reste du réseau continu à fonctionner.
- Facilité d'extension.

Inconvénients :

- Si le nœud central (concentrateur ou commutateur) tombe en panne, c'est tout le réseau qui est hors service.
- Elle nécessite autant de voies de liaisons que de stations de travail reliées au nœud central. Ce qui est générateur de coût.

Concentrateur ou

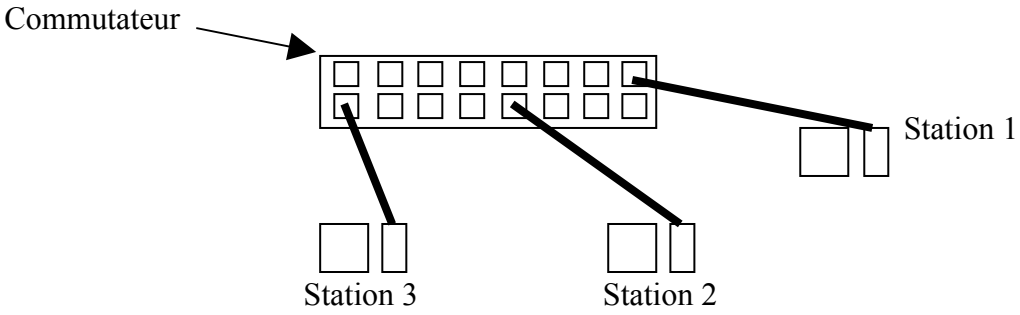


Figure 1 . 03 : Topologie en étoile

1 . 2 . 3 . Topologie en anneau

La topologie en anneau consiste en une série de liaisons points à points formant une boucle qui interconnecte un ensemble de stations de travail. Un poste plus puissant joue le rôle de serveur et distribue les jetons (token). Un boîtier central MAU joue généralement le rôle de l'anneau (ring).

L'accès des stations au réseau en anneau, appelé également réseau en boucle, est réglementé par le passage d'un « relais » appelé jeton. Dans cette configuration, la station n'est autorisée à émettre que si elle dispose du jeton.

Avantages : - Câblage moins important.

- Accès égalitaire de toutes les stations.

Inconvénients :

- Une interruption à un endroit quelconque de l'anneau empêche toute transmission sur le réseau.
- Le temps de réponse devient lent à l'ajout de nouvelles stations.
- Une panne d'ordinateur (qui est souvent le cas) peut affecter l'anneau.
- Problème difficile à isoler.
- La reconfiguration du réseau peut interrompre son fonctionnement.

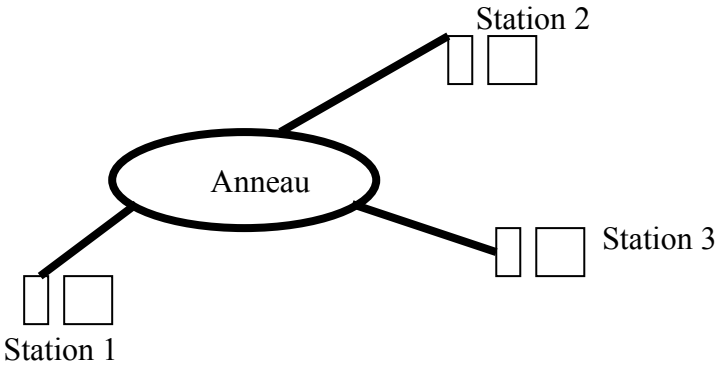


Figure 1 . 04 : Topologie en anneau

Remarques :

- Ces 3 types de topologies peuvent être combinées pour avoir des topologies hybrides (exemple : bus connecté en étoile).
- Plusieurs bus peuvent se connecter pour former des arbres.

1 . 3 . Eléments constitutifs du réseau local

1 . 3 . 1 . Les stations de travail [2]

Ce sont les machines (ordinateurs) interconnectées pour former le réseau. On peut distinguer :

1 . 3 . 1 . 1 . Le serveur

Un serveur peut être assimilé à une boîte contenant deux éléments :

- Le logiciel : ce terme désigne le système d'exploitation (Windows 2000 Server, Windows Server 2003, Linux, …) s'exécutant sur le matériel. Les services fournis par le serveur se dénombrent avec les logiciels qu'il faut lui ajouter (ou déjà disponible : cas de Linux). Chacun des logiciels est appelé logiciel serveur, ou tout simplement, serveur (exemple : Apache est un serveur Web).
- Le matériel : le matériel désigne l'ordinateur qui héberge et qui exécute le logiciel. Etant donné que le serveur fournit plusieurs services(transfert de fichiers, serveur de pages Web, …) sur les autres machines (clients), sa plate-forme devra être plus performante que celle des clients qui leurs sont connectés. En effet, la taille du disque dur désigne la capacité d'information qu'une machine (serveur) peut stocker, le RAM désigne la capacité d'information qu'elle peut transporter simultanément, la fréquence du processeur désigne la vitesse de transport d'information. Plus les valeurs de ces paramètres sont élevées plus meilleur est le serveur.

1 . 3 . 1 . 2 . Le client

Le poste client est souvent un PC (affichage et traitement).

Pour pouvoir communiquer avec le serveur, il devra disposer un logiciel client (exemple : Internet Explorer est un logiciel client Web). Au terme du matériel, la performance du plate-forme n'est pas exigée.

1 . 3 . 2 . La carte réseau [3]

C'est une plaquette de circuits imprimés logée dans l'emplacement d'extension d'un bus de la carte mère d'un ordinateur. On l'appelle aussi adaptateur réseau car il permet la connexion du PC au réseau. Chaque carte porte un nom de code unique appelé adresse MAC.
La carte réseau peut être intégrée sur la carte mère.

1 . 3 . 3 . Le concentrateur (hub) [1] [3]

Le concentrateur permet de connecter plusieurs ordinateurs où chacun d'eux est câblé à un port de l'hub. Actuellement, le plus utilisé est le hub Ethernet à port RJ45. Chaque port d'un hub ne peut qu'envoyer ou recevoir des trames (half/duplex). Il diffuse l'information qu'il reçoit à l'ensemble des stations du réseau. Ainsi, le débit du réseau est réparti entre les stations connectées au hub, limitant le débit de chacune.

Le hub peut disposer d'un port réservé (interhub ou uplink) à la connexion d'un autre hub ou d'un commutateur.

1 . 3 . 4 . Le commutateur (switch) [1] [3]

Le switch permet de connecter plusieurs ordinateurs ou pour relier des segments réseau. Chaque port d'un switch peut envoyer et recevoir des trames simultanément (full/duplex). En plus, il redirige l'information vers son destinataire grâce à l'adresse MAC de cette dernière. Ainsi chacune des stations connectées bénéficient toute la capacité de réseau en terme de débit
Dans le cas d'un switch «store and forward », le switch dispose d'une mémoire tampon (buffer) qui lui permet de stocker le message (information), d'en vérifier l'intégrité ou non, puis de l'envoyer vers son destinataire.

Dans le cas d'un switch « cut through », il ne dispose pas de mémoire tampon et commute le message à la volée, donc plus rapide mais moins sécurisant (sans vérification de l'intégrité de l'information).
Les « switch » peuvent être reliés en cascade pour augmenter le nombre de ports disponibles.

1 . 3 . 5 . Les segments de réseau [1] [3]

Le terme segment désigne le média de la couche 1 de l'architecture OSI (cf 1 . 4). C'est la voie commune de transmission des données dans un LAN. Comme pour chaque type de média (fil

de cuivre, fibre optique, média sans fil), il existe une longueur maximum de câblage avant que le signal à transmettre soit atténué, un nouveau segment réseau doit être crée en utilisant un dispositif électronique (pont, répéteur, switch, routeur).

Le « domaine de collision » est aussi à considérer pour l'étude du segment de réseau. En effet, le nombre d'ordinateurs connectés à un segment est limité selon la technologie utilisé (cf chapitre 2).

Exemple : Pour la technologie Ethernet 10 Base-2, 30 nœuds (ordinateur, switch, hub) par segment peuvent être connectés, 100 pour Ethernet 10 base-5.

Il faut respecter cette limite pour éviter la collision dans un réseau (s'il y a collision, on a un réseau saturé, certains paquets peuvent être perdus).

1 . 3 . 6 . Le pont [3]

Le pont est utilisé pour connecter deux segments LAN. En effet, lorsqu'un segment réseau ne peut plus recevoir une machine supplémentaire (cela dépend du type de la technologie employé, cf chapitre 2), il faut utiliser un pont pour relier ce segment à un nouveau segment.

1 . 3 . 7 . Le répéteur [3]

C'est un dispositif électronique, à un seul port d'entrée et un seul port de sortie, qui sert à étendre la longueur de transmission de données. Donc il régénère les signaux réseaux pour leur permettre de voyager sur une plus longue distance dans le média.

Le switch est aussi un répéteur mais avec plusieurs ports de sortie.

1 . 3 . 8 . Le routeur [3] [4]

Le routeur est souvent placé à l'entrée d'un réseau local. Il détermine le meilleur chemin pour les paquets dans un réseau. En effet, le routeur examine les paquets entrants et mènera ces paquets vers leur destination. Il empêche chaque paquet envoyé de le traverser si l'adresse de ce paquet n'est pas destiné aux réseaux connectés aux ports du routeur.

Cet routage est effectué en consultant la table de routage du routeur, donc le routeur doit être configurer. Ceci s'effectue par la connexion d'un ordinateur sur son port de configuration appelé port console. La configuration porte sur le paramétrage de la table de routage qui fait correspondre les entrées aux sorties.

1 . 3 . 9 . Les supports de transmission [1] [3] [5] [6]

Pour relier les équipements dans un réseau local on peut, soit utiliser des câbles soit effectuer une liaison sans fil.

Les différents types de supports de transmission dans un réseau local sont :

1 . 3 . 9 . 1 . Les câbles coaxiaux

Les câbles coaxiaux sont constitués de deux conducteurs cylindriques de même axe, séparés par un isolant. Le conducteur extérieur sert de blindage au conducteur intérieur, ils sont donc moins sensibles aux bruits et aux perturbations électromagnétiques. Ils permettent de faire passer des fréquences allant jusqu'à plus de 500MHz, et supportent un débit de 100Mbps.Le type de connecteur utilisé est le BNC.

En réseau, on peut disposer deux types de coaxial :

1 . 3 . 9 . 1 . 1 . Le câble coaxial fin (Thinnet)

Il est également connu sous la dénomination 10 Base-2 de la norme Ethernet où il est utilisé (cf 2 . 2 . 3). Son diamètre est de l'ordre de 6mm. Il est donc relativement souple. Il permet de transporter les données sur une distance de 2 fois 100m (Base-2), plus exactement 185m, avant que le signal ne soit soumis à un phénomène d'atténuation.

1 .3 . 9 . 1 . 2 . Le câble coaxial épais (Thicknet)

Il est également connu sous la dénomination 10 Base-5 de la norme Ethernet où il est utilisé (cf 2 . 2 . 3). Son diamètre est d'environ 12mm. Il est moins souple que le coaxial fin mais permet d'atteindre des débits et des distances plus importantes . La longueur du brin peut être de 5 fois 100m (Base-5) avant que ne se fasse sentir le phénomène d'atténuation.

Un schéma d'un câble coaxial avec son connecteur est donnée ci après :

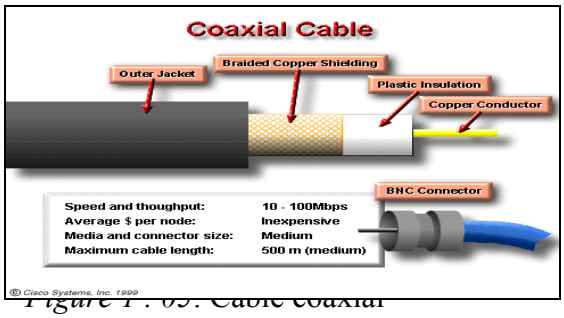


Figure 1 . 09. Câble coaxial

1 . 3 . 9 . 2 . Les paires torsadées

La paire torsadée est le média le plus employé actuellement en réseau local du fait de son faible coût. Elle est constituée de fils de Cuivre (2 ou 4 paires de fils par câble), d'impédance

100ohms. Les paires de fils sont tressées entre elles ce qui réduisent le phénomène de la diaphonie (cf 3 . 2 . 2). La longueur maximale acceptable est de 100m avant que le signal soit atténué. Le débit est de 10, 100, ou même 1000Mbps.

Il existe 2 types de câbles à paires torsadées :

1 . 3 . 9 . 2 . 1 . La paire torsadée non blindée (UTP)

Le câble contient 4 paires de fils de Cuivre. Chacun des 8 fils est protégé par un matériau d'isolation. Le diamètre extérieur du câble est d'environ 0,43cm.

Actuellement, le câble CAT5e (catégorie 5e) est employé. Le connecteur le plus utilisé est de type RJ45.

1 . 3 . 9 . 2 . 2 . La paire torsadée blindée (STP)

On rencontre également le terme FTP ou câble écranté.

Il utilise une qualité de Cuivre supérieure et possède une enveloppe de protection en Aluminium (feuillard ou écran) disposée autour des paires torsadées. Compte tenu du blindage et de la meilleure qualité du média, la paire torsadée blindée est moins sensible aux parasites extérieurs.

La figure d'un câble à paire torsadée avec son connecteur est donnée ci dessous :

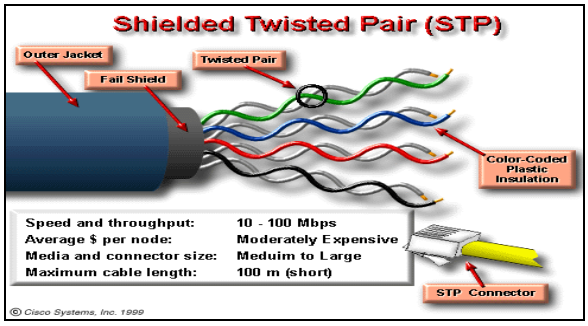


Figure 1 . 06 : Câble à paire torsadée

Actuellement, le câble CAT5 (catégorie 5) est le plus employé. Le connecteur le plus utilisé est de type RJ45.

1 . 3 . 9 . 3 . Les fibres optiques

La fibre optique est un conducteur de signaux lumineux. Les parties guidant la lumière sont appelées cœur et enveloppe. Le cœur est habituellement en verre GOF ou en plastique POF dont l'indice de réfraction est élevé. Il est enrobé d'une gaine d'indice de réfraction faible pour retenir la lumière au cœur de la fibre.

Comme la fibre optique ne transporte pas les impulsions électriques, contrairement aux médias réseaux qui utilisent le fil de Cuivre, les signaux représentant les bits sont donc convertis en faisceaux lumineux.

Le média à fibre optique est le plus onéreux mais il est insensible aux interférences électromagnétiques, à la foudre et prend en charge des débits de données très élevés avec une large bande passante.

Il existe 2 types de fibres optiques selon le diamètre du cœur de la fibre :

1 . 3 . 9 . 3 . 1 . La fibre optique monomode

Le diamètre du cœur est de l'ordre de 5 à 10µm. Cette fibre ne permet qu'un seul trajet optique, rectiligne d'où le signal transmis se présente sous la forme d'un faisceau de lumière. Les performances de transmission sont de haut niveau : faible atténuation (2dB/km à une longueur d'onde de 850nm), bande passante très importante (10GHz/km), longueur de transmission élevée.

Ce type de fibre est surtout utilisé pour une liaison de très longue distance et à haut débit.

1 . 3 . 9 . 3 . 2 . La fibre optique multimode

Le diamètre du cœur est de l'ordre de 100µm, la bande passante est de 10 à 50MHz/km, l'affaiblissement pour une longueur d'onde à 850nm est inférieur à 5dB/km. Elle est utilisée pour des liaisons inférieur à 2km et pour des débits inférieur à 50Mbps.

Cette fibre permet la propagation de plusieurs trajets optiques d'où le signal transmis se présente sous la forme des faisceaux de lumière.

Il existe 2 catégories de fibres multimodes selon la variation de l'indice du cœur vers l'indice de la gaine.

- La fibre à saut d'indice :

L'indice passe brutalement de la valeur du cœur à celle de la gaine.

- La fibre à gradient d'indice :

L'indice de réfraction est variable et suit une variation parabolique.

Remarques :

- Dans le domaine de réseaux locaux, la fibre à gradient d'indice 62,5/ 125µm est devenue la fibre optique la plus utilisée et est connue sous le nom de 10 Base F.
- Même si la lumière est une onde, la transmission par fibre optique n'est pas considérée comme une transmission sans fil, car les ondes sont guidées dans la fibre optique.

Voici un schéma d'un câble fibre optique :

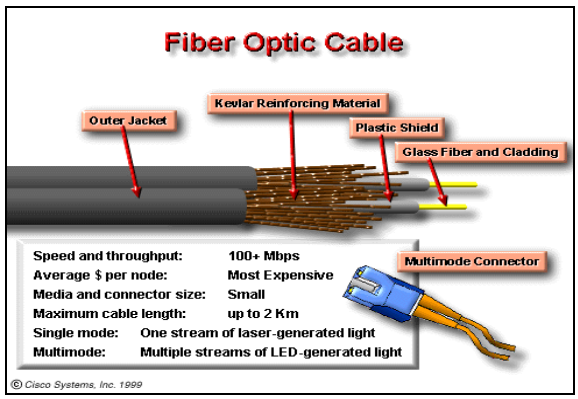


Figure 1 . 07 : Câble à fibre optique

1 . 3 . 9 . 4 . Les réseaux locaux sans fil

Ce sont les ondes électromagnétiques porteuses des informations à émettre qui circulent dans le vide de l'espace ou dans des médias tel que l'air. Une telle liaison sans fil est normalisée par la norme IEEE 802.11 .

Deux types de liaison sans fils sont possibles :

1 . 3 . 9 . 4 . 1 . Les liaisons infrarouges

L'émission infrarouge peut se présenter sous deux formes :

- Infrarouge diffus (Diffused Infrared) où les ondes infrarouges peuvent se refléter sur des surfaces passives telles que le mur, le sol ou le plafond et qui permettent ainsi à un émetteur d'être en relation avec plusieurs récepteurs.
- Infrarouge en émission directe (Direct Infrared) où le signal infrarouge est concentré, ce qui autorise des liaisons à plus longue distance et à débit plus élevé mais à condition que les points qui communiquent soient vis-à-vis.

Théoriquement, les liaisons infrarouges assurent des débits allant jusqu'à 10Mbps et la norme 802.11 comprend une spécification utilisant les infrarouges mais sur une distance limitée à 10m.

Les liaisons infrarouges trouvent leur intérêt essentiel dans des cas où l'utilisation d'un câble n'est pas facilement envisageable.

Exemple : Immeuble en vis-à-vis avec une route entre les deux.

1 . 3 . 9 . 4 . 2 . Les liaisons hertziennes

Les fréquences radio sont utilisées à cause de la très grande distance qu'elles peuvent parcourir. Actuellement, on rencontre :

- Le « Wi-Fi »

La norme IEEE 802.11b a pris le nom de Wi-Fi en 1999. Avec Wi-Fi, les appareils peuvent se communiquer et s'échanger des données par les ondes radio dans la bande de 2,4465 à 2,4835Ghz. Les débits peuvent atteindre les 54Mbits/s qui sont partagés entre le nombre de machines connectées simultanément sur le réseau. La portée varie (de 30 à 50m) selon la puissance du matériel utilisé, le bruit d'environnement, les différents obstacles.

- Le « Wi-Max »

La norme IEEE 802.16, validé en 2001, est la base de Wi-Max. Le Wi-Max est une solution de réseau hertzien permettant d'atteindre des débits et des portées très supérieurs aux technologies de réseau locaux WLAN. Théoriquement, le standard 802.16a , validé fin 2002, permet d'émettre et de recevoir des données dans les bandes de fréquences radio de 2 à 11GHz avec un débit maximal de 70Mbits/s sur une portée de 50Km. En pratique, cela permet d'atteindre 12Mbits/s sur une portée de 20Km.

- Le « Wi-Bro »

Cette technique de communication utilise les ondes radio (bande de fréquence 2,3GHz) et permet un débit théorique maximal de 30Mbits/s sur une portée de 1 à 5Km. En pratique, Wi-Bro se présente comme une technologie sans fil point à point, adapter pour desservir des zones peu peuplées pour lesquelles la fibre optique n'est pas envisageable. Le premier essai remonte en 2002.

Remarque: Dans un réseau sans fil, tout ordinateur possédant une carte référée par les normes 802.11 ou 802.16 (normalisation pour la liaison sans fil) peut accéder au réseau. On peut changer de place mais la continuité de connexion lors de déplacement d'un endroit à un autre n'est pas sûre. Aussi le débit décroît en fonction du nombre de postes connectés, de la taille d'information en circulation, des obstacles rencontrés et de la condition atmosphérique.

1 . 4 . Le modèle architectural OSI [1] [3] [4]

Le modèle OSI (ou ISO : Interconnexion des Systèmes Ouverts) a été mis au point par l'organisme de normalisation ISO en 1978.

On entend par système ouvert : n'importe quel équipement (ordinateur …) d' un réseau qui respecte la norme OSI donc apte à échanger des informations avec d'autres équipements hétérogènes et issus de différents constructeurs.

Le modèle OSI consiste en une décomposition des fonctions, sous forme de couches, que tout système des télécommunications (dans notre cas le réseau local) doit remplir. Chaque couche représente une fonction nécessaire à la transmission des données dans le réseau. Ainsi elle est censée de fournir des services au couche immédiatement supérieure et d'utiliser les données des couches inférieures pour accomplir sa fonction.

L'ISO a proposé la décomposition des fonctions nécessaires en système de télécommunications en 7 couches :

Couche application	(7)
Couche présentation	(6)
Couche session	(5)
Couche transport	(4)
Couche réseau	(3)
Couche liaison	(2)
Couche physique	(1)

Figure 1 . 08 : Le modèle architectural OSI

- Les couches 1 à 3 sont dites couches basses orientées transmission.
- La couche 4 est une couche charnière entre couches basses et couches hautes, on parle aussi de « middleware ».
- Les couches 5 à 7 sont les couches hautes orientées traitement.

Nous allons étudier chacune de ces couches en partant du plus bas niveau :

1 . 4 . 1 . La couche physique (niveau 1)

L'objectif de la couche 1 du modèle OSI est de déterminer les caractéristiques des matériels à utiliser pour relier physiquement les équipements d'un réseau donc tout ce qui concerne les câbles, les connecteurs, les cartes réseaux et le hub (cf 1 . 3).

Elle gère aussi le type de transmission. L'unité d'échange à ce niveau est le « bit » . La transmission de ces bits peut s'effectuer soit en mode série où les bits sont envoyés les uns derrière les autres de manière asynchrone ou synchrone, soit en mode parallèle où les bits d'un même caractère sont envoyés en même temps chacun sur un fil.

On procède également, dans cette couche, à la modulation / démodulation du signal, au mode de multiplexage qu'on veut adopter. Le multiplexage consiste à faire circuler sur une même ligne de liaison des communications appartenant à plusieurs pairs d'équipements émetteurs / récepteurs selon une méthode prédéterminée (multiplexage fréquentiel ou temporel).

C'est à cette couche donc qu'a lieu la transmission et la réception des informations.

La couche physique est normalisée par la norme ISO 10022.

1 . 4 . 2 . La couche liaison (niveau 2)

Cette couche contrôle l'établissement, le maintien et la libération de la liaison logique sur le réseau (transmission des données). Elle est responsable du bon acheminement des blocs d'informations. Les informations qui circulent sur le réseau sont les « trames » contenant les données proprement dites et des informations supplémentaires qui peuvent détecter et corriger les erreurs provenant du support physique. La couche 2 signale à la couche immédiatement supérieure (couche réseau) les erreurs irrécupérables.

Les équipements réseau de la couche 2 sont : hub, switch, pont, répéteur .

Les protocoles de liaison sont : BSC, HDLC.

La couche liaison est normalisée par la norme ISO 8886.

1 . 4 . 3 . La couche réseau (niveau 3)

Cette couche est chargée de l'acheminement des données sur l'ensemble du réseau. On y gère ainsi l'adressage, le routage et le contrôle de flux de données. L'unité de données est le « paquet ».

Il est nécessaire de contrôler le flux transité sur le réseau pour éviter le plus possible les problèmes de congestion qui surviennent lorsque trop de messages y circulent.

Le routage consiste à fixer par quelle ligne de sortie chaque commutateur du réseau réexpédie les paquets qu'il reçoit en tenant compte de la destination finale du paquet et selon une table de routage.

Ainsi, les ressources d'un réseau ne peuvent être atteintes que par l'intermédiaire d'un adressage spécifiant l'interface de sortie pour atteindre le destinataire des paquets.

L'équipement mis en œuvre par la couche 3 est le routeur.

Il existe plusieurs normes à ce niveau : ISO 8348, 8208, 8473, … et plusieurs protocoles d'adressage : Novell IPX, IPV4, IPV6 …

1 . 4 . 4 . La couche transport (niveau 4)

Elle fournit un service de transport de bout en bout transparent pour l'utilisateur. Elle doit assurer aussi les services qui n'auraient pas été assurés dans les couches basses (erreur, routage). C'est donc le dernier niveau chargé de l'acheminement de l'information. La couche transport de l'émetteur segmente les messages de données en paquets et celle du récepteur les reconstitue en les replaçant dans le bon ordre. A ce niveau, il faut aussi tenir compte des différents paramètres de la qualité de services (QoS) qui sont : le temps d'établissement, la probabilité d'échec d'établissement, le débit de la liaison, le temps de transit, le taux résiduel d'erreurs, le temps de connexion, la probabilité d'erreur de connexion, la protection des réseaux, l'ordre de priorité.

Il existe plusieurs normes à ce niveau : ISO 8072, 8073, 8602, …et les protocoles de transport sont TCP et UDP. UDP est moins fiable mais plus rapide que TCP et n'exige pas un accusé de réception (mode non connecté).

1 . 4 . 5 . La couche session (niveau 5)

C'est la première couche orientée traitement. Elle permet l'ouverture, la maintenance et la fermeture d'une session de travail entre deux systèmes distants et assure la synchronisation du dialogue (la couche session peut fournir une ou deux voies de communications). C'est à ce niveau que l'on décide du mode de transmission (simple, half-duplex, full-duplex : cf 1 . 3 . 3 et 1 . 3 . 4). C'est la couche la plus concernée par le modèle client / serveur.

Il existe plusieurs normes chargées de gérer ce niveau : ISO 08326, 8327, …

1 . 4 . 6 . La couche présentation (niveau 6)

Pour que deux systèmes ou équipements (ordinateurs issus des différents constructeurs) puissent se comprendre, ils doivent utiliser le même système de présentation de données et c'est la couche 6 qui le gère en se chargeant de transcrire les données dans une syntaxe compréhensible par les systèmes mise en relation. Elle assure également la conversion, la compression et le cryptage / décryptage des données (cf 3 . 3).

Il existe plusieurs normes chargées de gérer ce niveau : ISO 8824, 8326, 8327, …

1 . 4 . 7 . La couche application (niveau 7)

L'application de l'usager va utiliser cette couche car elle fournit des services utilisables sur le réseau. Les principaux services proposés sont : transfert de fichiers, messagerie ou courrier électronique (e-mail), soumission à des travaux à distance (client / serveur), Telnet (c'est une application de connexion à distance qui permet de connecter un terminal sur une machine à distance), accès aux fichiers distants, www (système de documentation). Plusieurs de ces services sont appelés API. Les API consistent en bibliothèque d'une programmation où le développeur peut l'utiliser.

Il existe plusieurs normes chargées de gérer ce niveau : ISO 9545, …et les protocoles mis en jeu sont : SMTP, FTP, TCP, NFS (service d'accès aux fichiers distants), HTTP (service www).

Remarques :

- D'autres modèles architecturaux existent également mais ils reprennent dans l'ensemble le modèle en couche OSI. D'où nous ne détaillerons pas ces architectures. Il s'agit du modèle architectural DSA-DCM proposé par Bull, le modèle architectural SNA proposé par IBM, le modèle architectural DNA proposé par DEC … ou ceux offerts par Hewlett Packard.
- On peut définir deux types de relations sur le modèle OSI de l'ISO : les relations verticales entre les couches d'un même système (interface) et les relations horizontales relatives au dialogue entre deux couches de même niveau.

1 . 5 . Les méthodes d'accès [1] [7]

La méthode d'accès dans un réseau définit la technique employée pour gérer le droit d'accès au média. Les méthodes les plus utilisés sont :

1 . 5 . 1 . Les méthodes aléatoires

Il s'agit de partager un même support de communication (topologie en bus) entre plusieurs utilisateurs. Chaque station connectée sur le bus transmet la trame en toute liberté sans se préoccuper des questions de droit d'émettre ou de disponibilité du canal.

Il se peut que deux ou plusieurs stations se décident à émettre au même instant, il y a contention ou collision des messages émis.

Pour résoudre le problème de collision, on peut arrêter momentanément la transmission des stations qui réemettront après un temps aléatoire : c'est la méthode CSMA / CD.

1 . 5 . 1 . 1 . CSMA / CD

Avant d'émettre, une station observe le média pour y détecter la présence de porteuse. Si une porteuse circule déjà (présence d'information sur le média), l'émission est reportée après un laps de temps aléatoire. Il est alors peu probable que les stations se décident à réemettre au même instant, si tel est le cas, le cycle d'attente reprendrait.

La méthode CSMA / CD, normalisée par l'ISO 802.3, est dite probabiliste car on ne sait pas à l'avance la station qui va émettre. C'est une méthode simple donc très utilisée mais elle présente des inconvénients : l'absence de système de priorité et l'accès aléatoire peuvent entraîner que certaines stations soient moins desservies que d'autres.

1 . 5 . 1 . 2 . CSMA / CA

Le but de cette méthode est d'éviter la contention plutôt que de la subir. La station qui veut émettre commence par écouter si la ligne est libre (Carrier Sense) de la même façon que dans la méthode CSMA / CD. Si la voie est libre, elle commence à envoyer un court signal (le préambule) prévenant ainsi les tentatives d'émission des autres stations qui vont alors bloquer temporairement leurs émissions. Enfin, la station émettrice va transmettre son message. Ce message devra faire l'objet d'un accusé de réception, sinon, on considérera qu'il s'agit d'une collision d'où la fiabilité

de l'échange d'informations. Mais dès que les charges seraient élevées, il y a ralentissement énorme du réseau.

La méthode CSMA est non déterministe car le temps d'accès à une ressource de réseau ne pouvant pas être garanti (temps aléatoire).

1 . 5 . 2 . Les méthodes déterministes

Pour remédier aux inconvénients des méthodes d'accès aléatoires (CSMA), on a développé des méthodes dites déterministes qui sont en mesure de garantir le temps de transfert des trames sur un support. La principale technique est basée sur la circulation d'un jeton.

Une station émet des informations sous formes de paquets de données normalisées, avec un en-tête, une zone centrale (le message) et une fin. Dans l'en-tête se trouve un bit particulier (le jeton) positionné à « 1 » si le réseau est occupé et à « 0 » dans le cas contraire. La station qui souhaite émettre ne peut le faire que si le jeton est libre. Chaque station reçoit donc le message à tour de rôle et en lit l'en-tête dans lequel figure l'adresse du destinataire. Si le message ne lui est pas destiné, la station régénère et le réexpédie sur le réseau. Le destinataire du message se reconnaît grâce à l'adresse, lit le message et le reémet acquitté, c'est à dire après en avoir modifié l'en-tête. La station émettrice peut alors, lorsque le jeton lui revient, valider la transmission et libérer le jeton ou émettre à nouveau ce message.

Avec cette méthode, la collision est impossible car une seule station peut émettre à un moment donné et on peut introduire les notions de priorité dans le choix de stations émettrices. Aussi, toutes les stations ont régulièrement accès au câble avec la même probabilité d'être servie et le débit ne se dégrade pas quand la charge augmente. Mais par contre, le temps mis par le jeton pour contourner la boucle est fonction du nombre de machines connectées. De plus, la panne d'une station peut immobiliser le réseau et si une station perd le jeton, elle doit attendre que celle-ci ait effectué un tour complet de la boucle.

Selon la topologie employé, on distingue :

1 . 5 . 2 . 1 . Le jeton sur anneau (Token Ring)

Cette méthode d'accès est utilisée dans la topologie en anneau. Avec l'anneau à jeton circulant, le jeton suit l'ordre physique des stations.

1 . 5 . 2 . 2 . Le jeton en bus

Le jeton circule de station en station en suivant le numéro logique qui se trouve sur la carte coupleur (numéro de la station précédente et celle de la station suivante) de chaque station.

Remarque : Avec la topologie en étoile, c'est le nœud central (hub ou switch) qui règle l'accès au réseau.

1 . 6 . Les types de transmission [8]

En général, deux approches sont possibles pour la transmission de l'information

1 . 6 . 1 . Transmission en bande de base

Un signal en bande de base est un signal qui n'a pas subi de transposition en fréquence. Il s'agit ici de transmettre le signal sous leur forme numérique. La suite binaire codée représentant l'information est transmise sur le support.

Le codage de l'information sert à convertir les « 1 » et « 0 » du signal numérique en éléments concrets tels qu'une impulsion électrique voyageant le long d'un fil ou une impulsion lumineux sur une fibre optique. Pour la transmission, différents types de codage peuvent être utilisés : code tout ou rien, code NRZ, code bipolaire, code RZ …

Les signaux bande de base sont sujets à une atténuation car susceptible au bruit et à l'interférence électromagnétique. Il ne peut transiter que sur une faible distance (<5Km), il est donc nécessaire de régénérer (utilisation de répéteur) le signal si l'on veut l'émettre sur une longue distance.

1 . 6 . 2 . Transmission à large bande

C'est une méthode utilisant le multiplexage en fréquence. Différents canaux sont crées en divisant la bande passante du support en plusieurs sous-bande de fréquences qui peuvent chacun supporter des informations. C'est une avantage pour ce type de transmission. Ainsi, son débit est élevé pouvant atteindre les 400Mbits/s sur un plus grand domaine géographique.

Dans le domaine de réseaux locaux, on utilise souvent la transmission en bande de base.

1 . 7 . Protocole de communication : TCP / IP [1] [3] [4]

Un protocole est un ensemble de règles et de conventions appliquées à l'échange de données. Pour que deux ou plusieurs équipements puissent se communiquer, ils doivent utiliser le même protocole.

TCP / IP est un des langages utilisés dans les réseaux, c'est donc un protocole de communication permettant à plusieurs ordinateurs de se dialoguer.

TCP / IP a été développé à partir de 1969 sur la base du projet DARPA de la défense américaine. Il n'est pas « un » unique protocole mais une « suite de protocoles » ou « pile TCP / IP », travaillant sur un modèle en couches particulier DOD, qui recouvre les différentes couches du modèle ISO (cf 1 . 4). En effet, TCP / IP recouvre un certain nombre de protocoles tels que :

→ niveau réseau - niveau 3 ISO

IP qui gère la circulation des paquets

ICMP, messages de contrôle et d'erreur

IGMP, adressage multipoint (classe D)

→ niveau transport - niveau 4 ISO

TCP en mode connecté

UDP en mode non connecté (n'exige pas un accusé de réception donc moins fiable)

→ niveau application - niveaux 5, 6, 7 de l'ISO

DNS qui établit la correspondance entre une adresse IP et un nom réseau

FTP destiné au transfert de fichiers

HTTP destiné aux pages web

NFS qui permet le partage de fichiers

SMTP qui gère le courrier électronique

Telnet qui permet l'ouverture de sessions à distance

SLIP et PPP adaptent TCP / IP à des liaisons série via le Réseau Téléphonique Commuté ou les Liaisons Spécialisés

La comparaison des 2 modèles ISO et DOD peut être schématisée par :

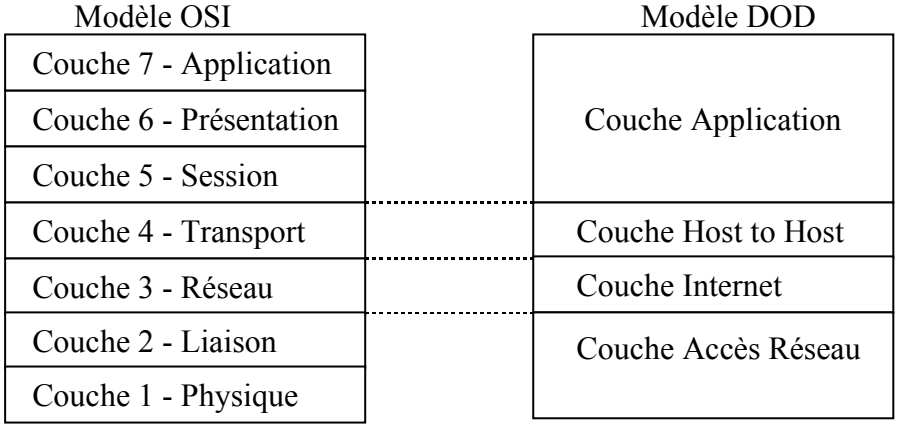


Figure 1 . 09 : Comparaison entre les modèles OSI et DOD

1 . 7 . 1 . Le protocole IP

C'est un protocole an niveau de la couche réseau du modèle OSI. Il traite de l'adressage et du routage des paquets entre les stations.

1 . 7 . 1 . 1 . L'adressage IP

La machine d'Internet a une adresse IP, unique dans le monde, représentée sur un entier de 32 bits (pour l'IPV4), partagée en 4 nombres de 8bits appelés Octets, séparés par un point. Ce format est appelé notation pointée.

L'adresse est constituée de deux parties : un identificateur réseau et un identificateur de la machine pour ce réseau. Les premiers octets servent à coder l'adresse réseau.

Le protocole IP divise les adresses en 4 classes :

→ Classe A :2^7 = 128 adresses réseaux et 2^{24} = 16777216 adresses de machines. Un réseau de classe A pourrait avoir une adresse comprise entre 0.0.0.0 et 127.255.255.255

→ Classe B : 2^{14} =16384 adresses réseaux et 2^{16} = 65536 adresses de machines. Un réseau de classe B pourrait avoir une adresse comprise entre 128.0.0.0 et 191.255.255.255

→ Classe C : 2^{21} = 2097152 adresses réseaux et 2^8 = 256 adresses de machines. Un réseau de classe C pourrait avoir une adresse comprise entre 192.0.0.0 et 223.255.255.255

→ Les classes étendues :

Classe D : les adresses 224 à 231 sont réservées à la classe D.

Classe E : les adresses 232 à 254 sont réservées à la classe E, destinées théoriquement à un usage futur.

Remarques :

- Adresse privée : Des adresses ont été réservées par un organisme (NIC-IANA) de gestion des adresses Internet. Ces adresses ne devront pas être utilisées pour l'Internet, elles sont utilisées dans des réseaux locaux privés susceptibles d'être connectés plus tard à Internet. Ces adresses sont :

Pour la classe A : 10.0.0.0 à 10.255.255.255

Pour la classe B : 172.16.0.0 à 172.31.0.0

Pour la classe C : 192.168.0.0 à 192.168.255.0

- L'utilisation de ces adresses ne cesse de s'augmenter par l'installation des réseaux un peu partout. D'où l'environnement TCP / IP va changer de IPV4 à IPV6: avec IPV6, les adresses sont représentées sur un entier de 128bits soit 16octets.

1 . 7 . 1 . 2 . Le routage IP

L'intérêt des classes IP se situe au niveau du routage des informations car les adresses IP ont été définies pour être traitées rapidement.

Comme la pile de protocoles TCP / IP a été conçue dès l'origine pour assurer l'interconnexion de réseaux physiques au moyen des routeurs, IP est donc un protocole « routable ». Deux techniques de routage peuvent être utilisées et mises en œuvre à partir de l'adresse IP :

- Le routage direct : quand il s'agit d'une communication des machines appartenant sur le même réseau, donc ayant la même adresse réseau.
- Le routage indirect : quand un nœud (machine) d'un réseau veut se communiquer avec un autre nœud (machine) d'un réseau différent. Il faut donc déterminer à quel routeur envoyer les datagrammes pour atteindre le destinataire.

La fonction de routage est basée sur les tables de routage qui associent, à l'adresse IP du réseau, l'adresse IP du routeur auquel est attaché ce réseau.

1 . 7 . 2 . Le protocole TCP

C'est un protocole au niveau de la couche transport du modèle OSI.

TCP est un protocole fonctionnant en mode connecté c'est à dire qu'il associe, à un moment donné, deux adresses de réseau. L'échange des données peut commencer quand une connexion est établie et comme plusieurs applications peuvent être mise en œuvre sur une connexion, TCP attribue un numéro de port à chacune. Théoriquement, TCP utilise 65000ports. L'usage courant des ports TCP est la suivante :

Service	Port	Description
FTP	21	Transfert de fichiers
Telnet	23	Connexion sur un hôte distant
SMTP	25	Transfert de courrier
HTTP	80	Pages Web
POP 3	110	Echange de courriers
NNTP	119	Services de newsgroups
XXX	>1024	Libres usage
IRC	6667	Services de « chat »

Tableau 1 . 01 : Usage des ports TCP

Le protocole TCP définit des acquittements (Ack : Acknowledgement) échangés entre les participants, il garantit la livraison dans le bon ordre des paquets, assure le contrôle par « checksum » des données.

Il utilise aussi le mécanisme de la fenêtre d'anticipation pour assurer le transfert de plusieurs paquets sans avoir à attendre d'acquittement. Ceci permet d'avoir un meilleur débit.
TCP est également capable de gérer les problèmes des congestions des nœuds de communication et de diminuer alors son débit.
Le protocole TCP définit donc les mécanismes permettant de rendre le transport fiable.

1 . 7 . 3 . L'architecture TCP / IP

La défense américaine (DOD) a décidé de définir sa propre architecture

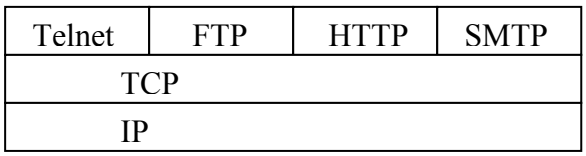


Figure 1 . 10 : Architecture TCP / IP

CHAPITRE 2 TECHNOLOGIE DES RESEAUX LOCAUX

2 . 1 . Définition [3]

Une technologie est un ensemble de processus et de méthodes mise en œuvre pour accomplir une tâche bien déterminée.

Pour un réseau, cette tâche est la transmission de données entre deux ou plusieurs équipements interconnectés.

Ethernet et Token Ring sont actuellement les deux grands standards utilisés sur les réseaux locaux. Une part nettement moins significative du marché est cependant couverte par des réseaux de type Starlan, Arcnet , …

2 . 2 . Technologie Ethernet [1] [3]

La technologie Ethernet est la plus utilisée dans le monde.

2 . 2 . 1 . L'origine d'Ethernet

En 1972, le centre de recherche de Rank Xérox à Palo Alto met au point un système de câblage qui utilise la diffusion CSMA / CD (cf 1. 5) qui donne naissance au réseau Ethernet.

2 . 2 . 2 . Les caractéristiques du réseau Ethernet

→ Topologie : à l'origine en bus linéaire, puis en étoile sur hub ou sur switch

→ Mode de transmission : en général, bande de base mais on peut aussi utiliser la large bande.

→ Mode d'accès : CSMA / CD

→ Vitesse de transmission : 10Mbps, 100Mbps, 1Gbps et évolution vers le 10Gbps.

→ Câblage : coaxial fin, coaxial épais, paire torsadée

→ Normalisation: IEEE 802 et ses adaptations (802.1,802.2, …), ISO 8802 et ses adaptations (8802.2, 8802.3, …)

Nous avons déjà étudié les caractéristiques citées ci-dessus, alors nous allons voir la place de l'architecture Ethernet par rapport au modèle ISO niveau 2 ainsi que la structure des trames Ethernet.

Place d'Ethernet dans les normes ISO et IEEE

La norme IEEE 802 introduit une division de la couche liaison du modèle ISO en deux sous couches. Or la référence en matière de réseau Ethernet est la norme IEEE 802. Il est donc préférable d'étudier ces deux sous couches :

→ La sous couche MAC: elle est située entre la couche physique et au dessous de la sous couche LLC. Elle est chargée de faire le lien de la carte réseau avec l'adresse matérielle ou adresse MAC. L'adresse MAC est une adresse unique composée d'une suite de 6octets dont les 3 premiers identifient le constructeur et les 3 autres identifient l'adaptateur (carte réseau).

→ La sous couche LLC: elle est située au dessous de la couche réseau et au dessus de la sous couche MAC. Elle est chargée de gérer les communications en assurant le contrôle du flux de données et des erreurs.

Structure de la trame Ethernet

Ethernet transporte les données sur des trames. La trame Ethernet est généralement composée de 7 champs :

→ Le préambule : comporte 7octets de valeur AAh, il assure la fonction de synchronisation du récepteur sur la trame émise.

→ Le délimiteur de début de trame SFD de valeur ABh pour trouver le début du champ des adresses.

→ Les adresses de destination et source sur 6octets chacun.

→ La longueur de données sur 2octets.

→ Le champ de données sur une taille variable de 46 à 1500octets par trame.

→ Le FCS: sur 4octets, c'est le résultat d'un contrôle destiné à savoir si la trame est arrivée en bon état. C'est un contrôle de redondance cyclique (CRC).

Préambule 7octets	SFD 1octet	AD 6octets	AS 6octets	Long 2octets	Données 46 à 1500octets	FCS 4octets

Figure 2 . 01 : Structure de la trame Ethernet

2 . 2 . 3 . Les principales architectures Ethernet

→ Ethernet 10 Base-2 : la norme IEEE 802.3 10 Base-2 correspond à Ethernet à 10Mbps en bande de base sur coaxial fin (Thin Ethernet).

→ Ethernet 10 Base-5 : la norme IEEE 802.3 10 Base-5 correspond à Ethernet à 10Mbps en bande de base sur coaxial épais (Thick Ethernet). Thick Ehernet est une amélioration de Thin Ethernet pour avoir de fiabilité et de rapidité.

→ Ethernet 10 Base-T : la norme IEEE 802.3 10 Base-T, définie en 1990, correspond à Ethernet 10Mbps (10) en bande de base(Base) sur paire torsadée (T). Le câble utilisé est un câble UTP ou FTP.

→ Ethernet 100 Base-T ou Fast Ethernet : pour passer de 10Mbps à 100Mbps (10 Base-T à 100 Base-T), il faut tout simplement changer les équipements de transmission comme les cartes réseau, les répéteurs. Les spécifications du 100 Base-T incluent également un mode « Auto Negociation Scheme » ou « Nway » qui permet à l'adaptateur réseau, au hub, au switch, … de définir automatiquement son mode de fonctionnement (10 ou 100Mbps).

→ Ethernet 10 Base-VG ou 100 VG Anylan : le 100 Base VG (Voice Grade) assure un débit théorique de 100Mbps sur la paire torsadée ou sur la fibre optique. La méthode d'accès employée met en œuvre la technique dite de priorité à la demande (demand priority), de type déterministe (cf 1 . 5 . 2). Ce qui améliore l'efficacité du réseau évitant au maximum les collisions.

→ Ethernet 1000 Base-T ou Gigabit Ethernet : Ethernet gigabits doit fonctionner sur du câble de catégorie 5 en utilisant 4 paires en full /duplex (cf 1 . 3 . 4) avec chaque paire travaille sur un débit de 250Mbps. Il est actuellement plutôt employé backbone (épine dorsale) sur de la fibre optique.

→ Ethernet 10Gbps : Ethernet 10Gbps est destiné pour la fibre optique mais le support paire torsadée est également employé.

→ Ethernet commuté : en utilisant les techniques de commutation à l'aide de commutateurs Ethernet (switch Ethernet), on peut augmenter le nombre de machines connectées au réseau local sans intensifier les collisions donc les performances ne se dégradent pas.

2 . 3 . Technologie Token-Ring [1] [3]

Le réseau Token-Ring occupe la deuxième place des réseaux locaux dans le monde.

2 . 3 . 1 . L'origine de Token-Ring

Token-Ring est introduit en 1984 et normalisé par l'ANSI / IEEE 802.5 en 1985. Token-Ring ou anneau à jeton a été pendant longtemps le fer de lance d'IBM en réseaux locaux.. En 1999, il ne couvre plus que 7% du parc en nombre de ports.

2 . 3 . 2 . Caractéristiques du réseau Token-Ring

Token-Ring est caractérisé par une méthode d'accès déterministe par jeton (token, cf 1 . 5 . 2) et par une topologie en anneau (ring, cf 1 . 2 . 3).

A l'origine, le débit est de 4Mbps et permet d'interconnecter 72 stations, puis 260 stations sur 16Mbps. En 1998, la version HSTR à 100Mbps est apparue.

Token Ring utilise la paire torsadée STP avec connecteur IBM type A dits connecteurs MIC ou UTP de catégorie 3 ou 5 avec des connecteurs RJ11 ou RJ 45. La fibre optique peut aussi être employée.

La structure de la trame Token-Ring est :

Si jeton occupé :

Marqueur de début 1octet	Contrôle d'octets 1octet	Contrôle de trame 1octet	Adresse destination 6octets	Adresse source 6octets	Informations optionnelles de routage 2 à 18octets

Accès service de destination 1octet	Champ de contrôle 1 ou 2octets	Champ de données variable	Marqueur de fin 1octet	FCS 4octets	Statut de trame 1octet

Figure 2 . 02 : Trame Token Ring IBM 802.5

Si jeton libre :

Marqueur de début 1octet	Contrôle d'accès 1octet	Marqueur de fin 1octet

Figure 2 . 03 : Trame Token Ring avec jeton libre

Note : La taille maximale de trame est de : 4096, 4472, 4500octets selon la vitesse du réseau.

2 . 3 . 3 . Architecture de Token-Ring

Les principaux éléments du réseau sont:

→ MSAU ou MAU: c'est le point central de la configuration physique de Token-Ring sur lequel les stations sont branchées. Pour agrandir l'anneau, les MAU peuvent être interconnectés au moyen d'un port d'entrée RI (Ring In) et d'un port de sortie RO (Ring Out) et il faut que le dernier RO soit connecté au premier RI pour avoir l'anneau logique.

→ Les câbles : les deux types de câbles à utiliser pour le réseau Token-Ring sont le câble adaptateur pour relier les stations au MAU et le câble de liaison pour interconnecter les MAU.

→ Le répéteur : il est utilisé pour étendre l'anneau jusqu'à 750m sur câble paire torsadée et 4km sur fibre optique.

Note : Physiquement, Token Ring est un réseau en étoile mais logiquement il est caractérisé bien évidemment par une topologie en anneau (utilisation de jeton).

2 . 4 . Les autres types de technologies [1]

2 . 4 . 1 . Technologie Starlan

Starlan constitue une alternative à Ethernet et Token Ring. Il ne couvre que 4% du marché. Il utilise une architecture en bus, étoile et de la paire torsadée comme support. Le circuit d'émission de données est différent du circuit de réception d'où la nécessité d'une double paire. Il fonctionne à 10Mbps avec un protocole de type CSMA / CD sur des tronçons allant jusqu'à 300m.

Starlan a été normalisé par IEEE 802.3.

2 . 4 . 2 . Technologie Arcnet

Arcnet est un réseau de type étoile qui couvre environ 3% du marché. C'est un réseau de type déterministe (cf 1 . 5 . 2) à jeton comme Token Ring. Il utilise le coaxial ou la fibre optique comme support. Il se caractérise par un débit de 2,5Mbps pour Arcnet à 20Mbps pour Arcnetplus. Il est un système ouvert car il accepte un environnement hétérogène en système d'exploitation et en type de machine utilisée.

Arcnet n'est pas encore normalisé.

Nous allons étudier maintenant la performance et la sécurité dans le réseau local.

CHAPITRE 3 PERFORMANCE ET SECURITE DANS LE RESEAU LOCAL

3 . 1 . Introduction

Lors de la conception et de l'étude de réseau local, il ne faut surtout pas oublier la performance et la sécurisation de celui ci.

Tout d'abord, nous allons voir en ce qui concerne la performance.

3 . 2 . La performance d'un réseau local [1] [9]

3 . 2 . 1 . Caractéristiques des équipements à mettre en œuvre

Pour rendre une performance acceptable ou même meilleure pour le réseau local, il faut prendre en considération les caractéristiques des équipements à mettre en œuvre.

→ Caractéristiques de câblage :

- L'atténuation, en dB, traduit l'énergie perdue par le signal au cours de sa propagation sur le câble.
- Le débit, en bits/s, traduit le nombre de bits que peut supporter le câble, lors d'une transmission, pendant 1seconde.
- La bande passante, en Hz, traduit la bande de fréquence que peut supporter le câble avec une atténuation donnée.
- L'impédance, en ohms, traduit le comportement du câble en présence d'un courant alternatif. Actuellement, on utilise des câbles 100 ou 120ohms.

Exemples : Les caractéristiques de câblage en transmission Voix Données Images (VDI) d'un câble à fibre optique multimode à gradient d'indice 62,5 / 125µm sont données par :

- pour une longueur d'onde de 850nm, l'atténuation maximale est de 3,2dB / km dans une bande passante de 200MHz . km
- pour une longueur d'onde de 1300nm, l'atténuation maximale est de 1,5dB / km dans une bande passante de 500MHz . km

La caractéristique de câblage pour une liaison de 90m avec la paire torsadée à 100Mhz : l'atténuation maximale est de 20,4dB.

Les valeurs du débit et de la bande passante dépendent de l'application voulue.

→ Caractéristiques des machines connectées au réseau (cf 1 . 3 . 1)

- Stations de travail : la performance d'une machine est caractérisée par la fréquence d'horloge du microprocesseur, la mémoire vive RAM et la capacité du disque dur.
- Serveur : comme le serveur est destiné à satisfaire les requêtes venant des autres stations de travail (clients), sa plate - forme devra être la plus performante des machines connectées au réseau.

→ Les autres éléments à mettre en œuvre :

- Les connecteurs de types : BNC, RJ11, RJ45, ….Il faut respecter, considérer l'atténuation de ces connecteurs (l'atténuation maximale sur la plupart des connecteurs est de 0.5dB).
- La goulotte et la gaine sont utilisées pour la bonne esthétique de câblage et la protection contre les bruits et perturbations externes.

3 . 2 . 2 . La performance de transmission [9]

Pour une performance de transmission, il faut prendre en compte de :

→ L'atténuation :

Déjà évoquée dans le paragraphe ci-dessus. Elle doit être de faible valeur lors de la transmission.

→ L'impédance caractéristique :

Déjà vue précédemment. Le bon fonctionnement du réseau dépend de la constance de l'impédance caractéristique dans l'ensemble des câbles et des connecteurs du système.

→ La diaphonie :

C'est la transmission indésirable d'un signal d'une paire d'un câble vers une autre paire rapprochée. Par conséquent, les dépairages provoquent une diaphonie grave car les signaux des paires torsadées proviennent de circuits différents.

Les problèmes de diaphonie peuvent être réduits en torsadant ensemble les deux fils de chaque paire de câble, ce qui supprime les champs électromagnétiques autour des fils, éliminant virtuellement le champ de transmission des signaux aux câbles proches et faites en sorte que les sections non torsadées soient les plus courtes possibles lors de branchement aux blocs perforateurs ou lors de l'installation des connecteurs.

→ ACR

C'est la valeur du signal / bruit. Plus l'ACR est important, meilleur est la qualité de transmission.

Pour qu'un système de transmission fonctionne, il lui suffit de disposer généralement d'un ACR compris entre 10 et 20dB.

→ RL

C'est la perte par réflexion. Sa valeur est donnée par la formule :

RL = puissance du signal transmis – puissance du signal réfléchi dû aux variations de l'impédance du câble.

Dans la transmission des signaux d'un réseau local, les câbles à perte par réflexion élevée sont très efficaces car la perte du signal est faible.

→ Les sommes de puissance :

Elles montrent les effets d'interférence sur une paire de fils combinée avec les autres paires dans un câble.

Une bonne performance en terme de somme de puissance est importante pour les réseaux opérant à grande vitesse, comme 1000 Base-T, qui transmettent des données en parallèle sur plusieurs paires de fils. Même si ce n'est pas le cas, il faut vérifier la performance des sommes de puissance en prévision des mises à niveau ultérieures du système.

→ Le délai de propagation :

C'est le temps nécessaire à un signal pour parcourir un support d'un point à un autre. Ce temps dépend donc de la nature du support, de la distance et aussi de la fréquence du signal. Il faut que ce délai doit être faible pour avoir une performance du système.

Exemple :

Câble	Fréquence du signal	Distance	Temps de propagation
10 Base 5	5 à 10MHz	1km	4µs
10 Base 2	5 à 10MHz	1km	5µs
10 Base T	5 à 10MHz	1km	5µs

Tableau 3 . 01 : Exemple des paramètres de transmission des câbles

Tous ces paramètres de performance de transmission peuvent être acquis facilement en utilisant un appareil d'analyseur de réseau (Fluke par exemple).

→ La performance du réseau local peut aussi être définie par les paramètres de QoS (cf 1 . 4 . 4). Les plus concernées sont :

- Le débit efficace maximum : dans la pratique, ce débit n'atteint jamais la capacité du support de transmission - du hub et de la carte réseau - de transmettre et de recevoir les informations.
- Le temps de réponse : c'est le temps écoulé entre l'émission d'une trame par un utilisateur du système et la réception de la réponse après la traversée du support de transmission et du hub ou switch. Ce temps est donc fonction de la performance des différentes machines connectées au réseau, du temps de propagation du signal dans le support de transmission, de temps de transmission d'une trame sur le support.

Pour terminer l'étude théorique du réseau local, nous allons voir sa protection et sécurisation.

3 . 3 . La sécurisation du réseau local [3]

Voici quelques méthodes utilisables pour la sécurité dans un réseau :

→ Authentification des utilisateurs par login et mot de passe.

→ Suppression des informations confidentielles des machines reliées au réseau si elles n'ont pas besoin d'y être.

→ Protection physique des machines contenant des informations sensibles (locaux fermés à clé)

→ Contrôle pour l'accès aux informations sensibles, avec login délivré uniquement pour ceux qui en ont besoin.

→ Installation d'un logiciel anti-virus à jour sur chaque poste.

→ Recours à la cryptographie des données :

- Le chiffrement : pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par un clé unique correspondant au cryptage (cf 1 . 4 . 6).

→ Les firewalls : face aux nombreuses menaces, il est préférable d'isoler les réseaux locaux du réseau international. Une solution efficace est la machine « Firewall ». C'est une machine qui est placée à la place d'un routeur IP qui sépare deux réseaux (firewalls internes) ou qui sépare le réseau local d'Internet (firewalls externes). Les firewalls sont configurés pour protéger contre les accès non authentifiés du réseau externe. Ils autorisent les utilisateurs à communiquer librement avec l'extérieur.

→ Le serveur proxy : le but d'un serveur proxy est d'isoler une ou plusieurs machines pour les protéger. Il permet de faire le relais au niveau des applications pour rendre les machines internes invisibles de l'extérieur.

« Si personne à l'extérieur ne peut voir les machines internes, l'attaque est beaucoup plus difficile, car l'attaquant est aveugle ».

Cette étude théorique, précédemment faite, est une étape nécessaire pour faire la conception d'un réseau local. Dans le chapitre suivant, nous allons étudier l'installation du réseau local au sein du Département Télécommunication.

CHAPITRE 4 ETUDE DE L'INSTALLATION D'UN RESEAU DANS LE DEPARTEMENT TELECOMMUNICATION

Dans ce chapitre, nous allons étudier la mise en place d'un réseau informatique au sein du Département Télécommunication.

4 . 1 . Introduction

Au moment de notre étude, une dizaine d'ordinateurs, possédant chacun une ou plus de cartes réseaux, sont disponibles dans le Département Télécommunication. La plupart de ces cartes sont de types Fast Ethernet Realtek RTL8139. Et les ordinateurs fonctionnent sous différents systèmes d'exploitation en ne citant que Windows95, Windows98, Windows XP, Windows 2000 Server, …

4 . 2 . Choix de la topologie

En tenant compte de l'étude des différents types de topologies (cf 1 . 2), nous allons adopter la topologie en étoile pour notre réseau.

4 . 3 . Eléments nécessaires pour l'installation

4 . 3 . 1 . Poste de travail

On a déjà mentionné auparavant (cf 4 . 1) qu'une dizaine de postes équipé chacun d'au moins une carte réseau sont disponibles. Notre étude se base sur 14 ordinateurs d'adresse réseau 172.16.0.0 (cf 1 . 7 . 1 . 1, remarques), fonctionnant sous Windows ou Linux .

4 . 3 . 2 . Switch

Pour connecter les machines dans le Département, un switch de 16 ports est nécessaire.

4 . 3 . 3 . Support de transmission

L'utilisation d'un câble à paire torsadée blindée nous convienne par considération des équipements (switch) à notre disposition et des études faites dans 1 . 3 . 8.

La longueur de câble nécessaire est de 194m (voir Annexe 1 pour les détails) .

4 . 3 . 4 . Accessoires

- Connecteurs RJ45 : 3 x 14 = 42
- Prises murale RJ45 : 13
- Goulotte (pour encastrer les câbles) : 58m (voir Annexe 1)

4 . 4 . Câblage

Chaque machine est connectée au switch grâce au câble paire torsadée blindée CAT5 :

- Un câble de longueur variable, selon la distance de la machine au switch, encastré dans le goulotte. L'un des deux bouts du câble équipé d'un connecteur RJ45 entre sur le port RJ45 du switch. L'autre bout est connecté au prise murale RJ45 (noyau RJ45) à côté de l'emplacement de la machine.

- Un autre câble de longueur 1,50m appelé couramment « cordon de brassage » est utilisé pour la liaison entre le port réseau de l'ordinateur et la prise murale RJ45. Donc chaque bout de ce câble est équipé d'un connecteur RJ45.

Le plan de câblage du Département Télécommunication est fourni en Annexe 1.

4 . 5 . Evaluation des coûts de matériels

Dans un tel projet, une évaluation de coût est indispensable.

Désignation	Prix unitaire (Ariary)	Quantité	Montant (Ariary)
Carte réseau 10/100Mbps Compex	12 000	5	60 000
Switch 16ports RJ45 D-Link 10/100Mbps	190 000	1	190 000
Connecteur RJ45	500	42	21 000
Prise murale RJ45	27 690	13	359 970
Câble FTP CAT5	700	194mètres	135 800
Goulotte 1 compartiment	10 868	58mètres	630 344
TOTAL			**1 397 114**

Tableau 4 . 01 : Evaluation des coûts de matériels 1

Le montant total s'élève à **1 397 114Ariary** ou **6 985 570Fmg**

CHAPITRE 5 L'ARCHITECTURE CLIENT – SERVEUR

5 . 1 . Introduction

Dans un réseau local , deux types d'architectures sont possibles :

- Le réseau « poste à poste » : tous les ordinateurs sont égaux et peuvent se communiquer, tout en mettant certaines ressources à la disposition des autres.
- Le réseau « client – serveur » : il existe une hiérarchie à deux niveaux, le serveur et les clients. (cf 1 . 3 . 1).

Nous allons adopter ce dernier pour l'architecture réseau du Département Télécommunication.

5 . 2 . Le concept client – serveur [10]

Dans notre étude, les applications réseaux reposent sur le concept client – serveur .

Des processus « clients » utilisent, sur le réseau, des services assurés par des processus « serveur ». En d'autres termes, client et serveur sont les deux moitiés d'une application réseau et sont conçus pour travailler ensemble via le réseau.

Le client prend l'initiative de communication lancée par un utilisateur. Le serveur, programme démarré automatiquement à la mise en route de la machine, répond aux requêtes du client.

Dans la terminologie Unix / Linux, on parle de 'daemon' (démon en français) pour désigner ces processus qui tournent constamment en attendant une requête provenant d'un client. La terminologie Microsoft Windows utilise le mot : 'service'.

L'architecture client – serveur peut donc être résumé comme ceci :

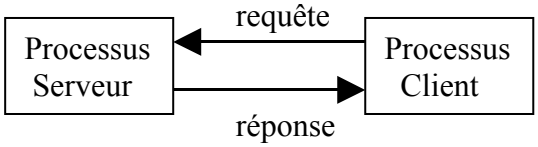


Figure 5 . 01 : Architecture client – serveur

5 . 3 . Choix du système d'exploitation

5 . 3 . 1 . Les versions des systèmes d'exploitation [2]

Les versions grand public comme : Windows 95 / 98 / XP Familial … sont en général dépourvues de logiciels serveurs. Elles sont donc destinées aux postes clients.

Par contre, les versions évoluées comme : Windows NT / 2000 / XP Professionnel / Server 2003, Linux …incluent déjà les outils et services ou même les logiciels serveurs (cas de Linux) nécessaires pour le réseau. Elles sont donc bien adaptées aux postes destinés à servir les clients (le serveur).

5 . 3 . 2 . Le système d'exploitation Linux [10] [11] [12]

5 . 3 . 2 . 1 . Présentation

Linus Thorvalds, étudiant finlandais, avait crée le système d'exploitation Linux. C'est en 05 Octobre 1991 que la première version de Linux 0.01 a été annoncé par Linus. Tous les codes sont sous licence GPL, créant ainsi un noyau Unix totalement libre.

Linux est diffusé sous forme de distribution, un ensemble de programmes (noyau, sources des utilitaires, commandes, applications) formant après installation un système complet. Parmi les distributions les plus utilisées, on trouve Debian, Mandrake, Red Hat, Fedora.

5 . 3 . 2 . 2 . Caractéristiques et avantages

→ Logiciel libre : l'utilisateur a la liberté de modifier (les sources sont fournies avec le logiciel) Linux pour l'adapter à ses besoins. Il peut copier et redistribuer gratuitement ou moyennant finance. Il peut modifier et redistribuer sous sa forme altérée de manière à en faire profiter la communauté.

→ Multi-utilisateurs et multi-tâches : il accepte de nombreux utilisateurs de travailler sur la même machine ou de l'utiliser d'une façon distante (cf 5 . 7). Il met en œuvre des mécanismes d'identification des utilisateurs, de protection et de confidentialité des informations.

→ Stabilité : Linux ne plante pratiquement jamais. Mais si on est planté et si la touche <CTRL-C> ne permet pas d'interrompre l'exécution d'une commande, on peut recourir au lancement d'un écran virtuel <ALT-CTRL-F2> et lancer les commandes de destruction de processus et on pourra ainsi récupérer la main. <ALT- CTRL-F7> pour revenir en environnement graphique.

→ Il fonctionne sur différents plates-formes (processeurs : INTEL, Power PC, AMD,IBM S/390, Sun SPARC, Alpha …).

→ Plusieurs utilitaires sont inclus dans une distribution comme : les langages de programmation (C++, Perl …), les outils bureautique (traitement de texte, messagerie …), un environnement graphique (X11, KDE, GNOME) …

→ Linux peut s'effectuer soit en mode graphique (X11, KDE, GNOME) soit en mode texte (utilisation des lignes de commande depuis un environnement shell, cf 5 . 3 . 2 . 3 . 4).
→ Linux peut devenir l'ensemble des solutions suivantes : un serveur web (Apache), un serveur de transfert de fichier FTP, un serveur de messagerie, un serveur de fichier et d'impression en environnement Microsoft (Samba), un serveur de nom DNS, un serveur de base de données PostgreSQL,, un serveur de base de données MySQL, un serveur de news, un serveur de réseau, un serveur de réseau hérité.

5 . 3 . 2 . 3 . Les concepts de base

5 . 3 . 2 . 3 . 1 . Création d'un compte utilisateur

L'utilisateur doit avoir un compte propre à lui pour qu'il puisse utiliser le système soit sur la même machine, soit en réseau (cf 5 . 7).
La création d'un compte utilisateur est exécutée par l'administrateur (root) par les commandes :
useradd *nom_utilisateur*
passwd *mot_de_passe_utilisateur*

5 . 3 . 2 . 3 . 2 . Se « loguer » sur le système

Au moment de se « loguer », il faut taper le nom d'utilisateur et le mot de passe. En appuyant sur la touche entrée, l'utilisateur est connecté au système.

5 . 3 . 2 . 3 . 3 . Les commandes Linux :

Une commande est composée de code mnémonique en minuscules (son nom proprement dit), suivi parfois d'options et / ou de paramètres.
La syntaxe générale a la forme :

commande [options] [paramètres]

Quelques commandes de base seront fournies dans l'Annexe 2.

5 . 3 . 2 . 3 . 4 . Le shell

L'interpréteur de commande ou shell est la liaison la plus élémentaire entre l'utilisateur et le système d'exploitation. Les commandes saisies sont interprétées par le shell et transmises au système d'exploitation.

Il existe plusieurs interpréteurs de commandes : Z-shell, TC-shell (Tenex C-shell), Bash (Bourne Again Shell). Le shell standard de Linux est le Bash.

5 . 3 . 2 . 3 . 5 . Les principaux répertoires

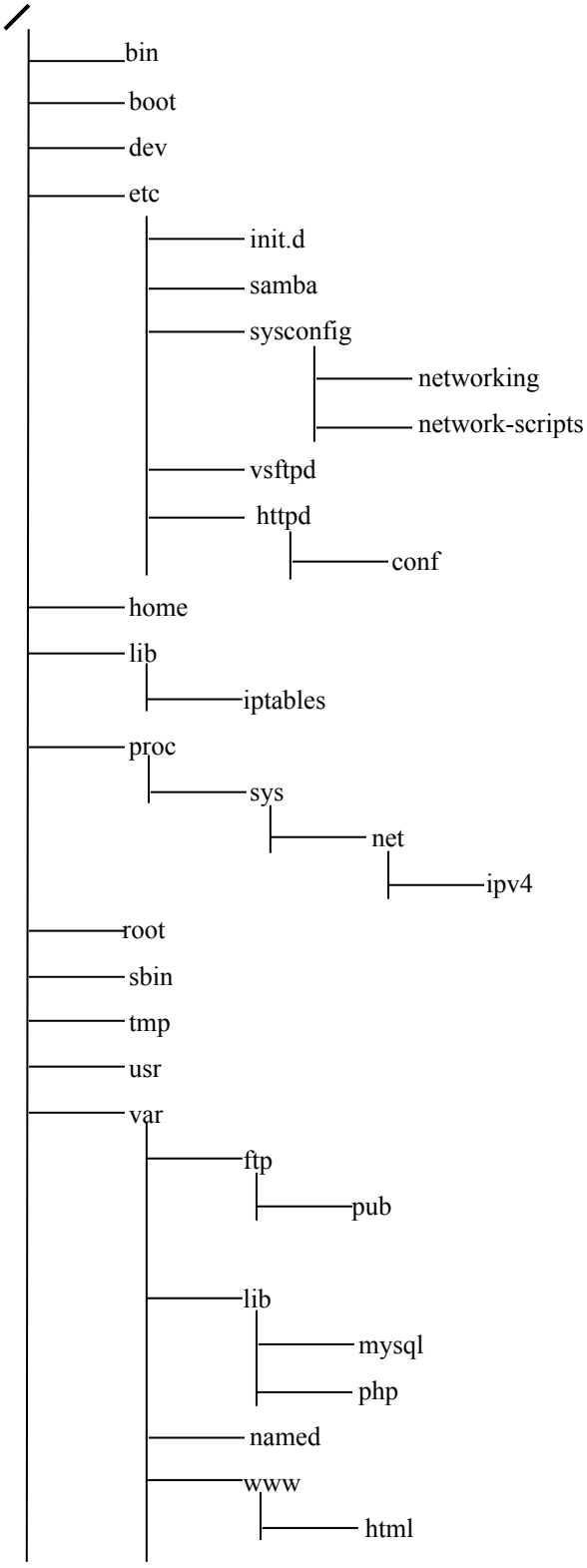


Figure 5 . 02 : Arborescence des répertoires sous Linux

Note : L'explication de ces répertoires est fournie en Annexe 3.

5 . 3 . 3 . Choix de Linux pour système d'exploitation destiné au serveur

Les caractéristiques et avantages de Linux citées ci-dessus nous amènent à choisir Linux comme système d'exploitation destiné au serveur. En effet, Linux incluse déjà les logiciels serveurs qui nous conviennent (serveur de nom DNS, serveur web Apache , serveur de fichiers Windows Samba, serveur de transfert de fichiers FTP, serveur de base de données MySQL). Il nous reste à configurer tous ces serveurs.

5 . 4 . Installation de la distribution Fedora Core 4 [13] [14] [15]

5 . 4 . 1 . Historique de Fedora

Red Hat Linux a décidé de créer le Red Hat Enterprise Linux en 2002 qui est le standard Linux en entreprise. Ce dernier met en œuvre le projet Fedora en 2003. Le 30 Avril 2004, Red Hat a pris sa limite de vie dans sa dernière version Red Hat 9.

Le 16 Mai 2005, Fedora atteint sa quatrième version appelée couramment Fedora Core 4.

5 . 4 . 2 . Configuration requise pour l'installation

Pour installer Fedora Core 4, il faut :

- CPU: unité centrale exécutant les instructions d'un programme

→ Minimum : Pentium, optimal pour Pentium 4

→ Mode texte : 200Mhz Pentium ou plus

→ Mode graphique : 400Mhz Pentium II ou plus

→ Processeur AMD64

→ Intel®EM64T : Intel processors with Intel®Extended Memory 64 Technology

- Disque dur

→ Installation minimum : 90Mo (mode texte)

→ Installation complète : 175Mo (mode texte et mode graphique)

	Système X86 32-bits	Système X86_64 64-bits
Bureau personnel	2,3Go	2,7Go
Poste de travail	3 Go	3,4Go
Serveur	1,1Go	1,5Go
Installation personnalisée (minimal)	620Mo	900Mo
Installation personnalisée (maximal)	6,9Go	7,5Go

- Mémoire

	Système X86 32-bits	Système X86_64 64-bits

Mode texte (minimum)	64Mo	128Mo
Mode graphique (minimum)	192Mo(256Mo recommandé)	256Mo(512Mo recommandé)

Tableau 5 . 01 : Configuration requise pour l'installation de Fedora Core 4

5 . 4 . 3 . Installation

L'installation de la distribution Fedora Core 4 de Linux se fait à l'aide des 4CD. Le cinquième CD appelé « rescue » n'est pas nécessaire pour l'installation.

Nous allons décrire les étapes effectuées lors de l'installation:

→ Tout d'abord, l'ordinateur destiné à être « serveur » fonctionne sous Windows XP. Il est doté de disque 40Go, de mémoire 128Mo. Nous allons partitionner en deux ce disque dont l'une des parties reste pour fonctionner sous Windows XP tel que l'autre partie sous Fedora Core 4 de Linux. La partition magic 8.0 non destructive (données non formatées) est utilisée pour accomplir cette tâche.

→ Après le partitionnement et au redémarrage de la machine, insertion du premier CD d'installation.

→ Sur l'écran de bienvenue '**Welcome to Fedora Core**', Anaconda, l'installateur graphique, propose de choisir la langue d'installation : Français (Français).

→ Configuration du clavier : Français (Latin1).

→ Analyse de la mise à niveau : ● Installer Fedora Core

○ Mettre à niveau une installation existante

→ Type d'installation : ○ Bureau personnel

○ Poste de travail

○ Serveur

● Personnaliser

→ Choix du type de partitionnement : ○ Partitionnement automatique

● Partitionnement manuel avec Disk Druid

→ Configuration du disque :

Disque Point de montage Système de fichier Formatage Taille en Mo

Δ /dev/hda

/dev/hda1		ntfs		20191
/dev/hda2	/boot	ext3	√	102
/dev/hda3	/	ext3	√	18654
Δ /dev/hda4		Etendu		259
/dev/hda5		swap	√	259

→ Configuration du chargeur de démarrage : ● Windows XP /dev/hda1

○ Linux FC_4 /dev/hda3

→ Configuration réseau : nous allons effectuer la configuration ultérieurement.

→ Configuration du pare-feu : ● Pas de pare-feu

○ Activer le pare-feu

On peut configurer aussi SELinux (Security Enhanced Linux). : ○ Désactiver

● Avertir

○ Activer

Durant l'installation, nous avons choisi de désactiver le pare-feu car nous allons le configurer ultérieurement (cf chapitre 8).

L'implémentation de SELinux dans Fedora Core est conçue afin d'améliorer la sécurité de plusieurs démons serveur (smbd, vsftpd, httpd, mysqld, …) tout en minimisant l'impact sur les opérations du système.

→ Sélection du fuseau horaire : Inde / Antananarivo

→ Définition du mot de passe root (super-utilisateur)

→ Paramètres par défaut de l'installation de paquetage :

○ Installation des paquetages de logiciels par défaut

● Personnalisation des paquetages de logiciels à installer

→ Sélection des groupes de paquetages :

Il faut cocher les cases correspondants aux paquetages choisis à installer :

Dans la figure 5 . 03 ci dessous, le case situé à gauche de Serveur Web est coché donc le paquetage de base est installé. En cliquant sur « Détails » à droite, une liste des paquetages supplémentaires parue à l'écran (cf figure 5 . 04) :

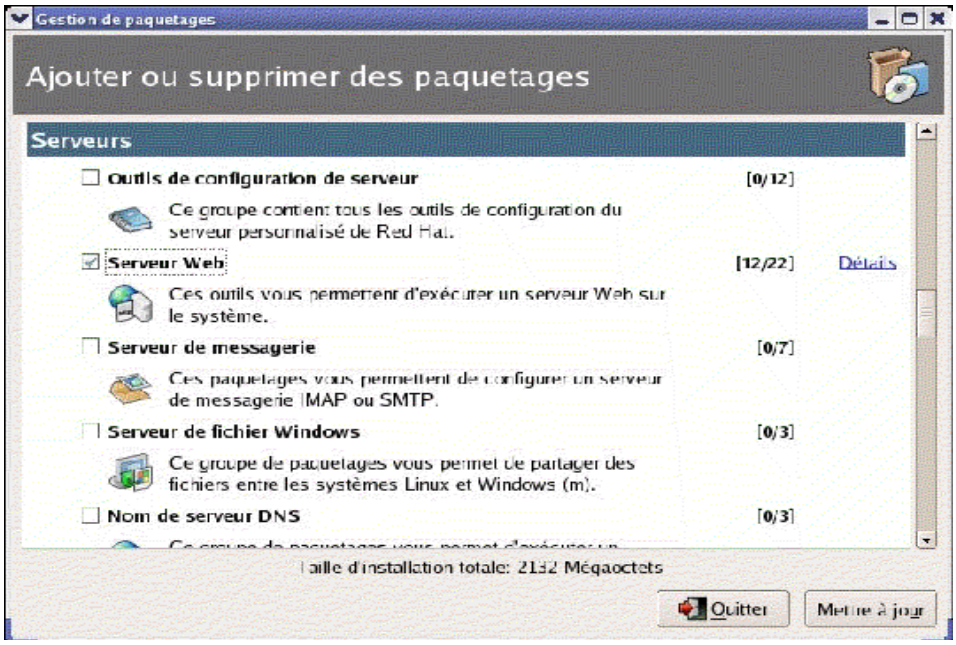


Figure 5 . 03 : Choix de paquetages sous Fedora Core 4

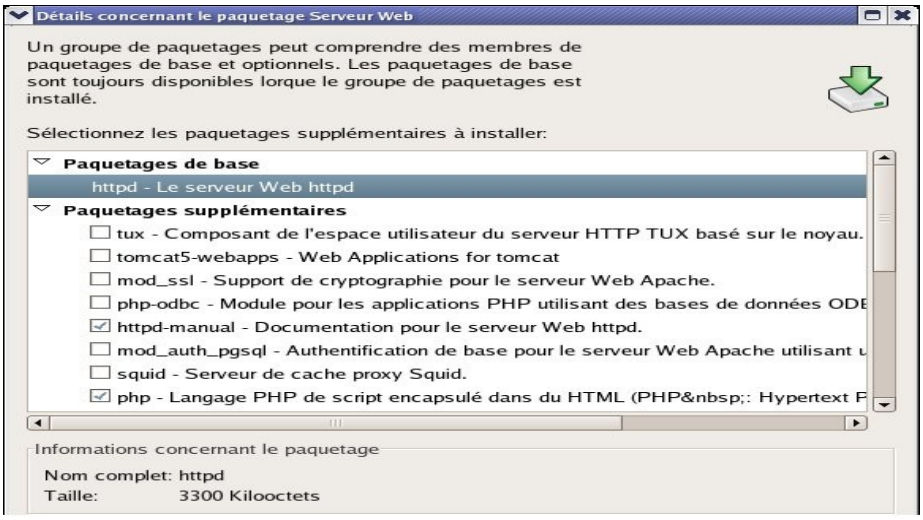


Figure 5 . 04 : Choix de paquetages supplémentaires sous Fedora Core 4

Voici la liste des paquetages supplémentaires nécessaires pour notre étude :

- Internet graphique :

- Firefox – Mozilla Firefox Navigateur Web
- Gftp – Client FTP à unité d'exécution multiple pour le système Xwindows

- Outils de configuration de serveur :

- System-config-samba – Utile pour la configuration du serveur Samba

- System-config-bind – Utile pour la configuration du serveur DNS
- System-config-httpd – Utile pour la configuration du serveur Apache

  ➢ Serveur Web :

- Httpd-manual – Documentation pour le serveur Web
- Mod_auth_mysql – Authentification de base pour le serveur Web Apache utilisant une base de données MySQL
- Php-mysql – Module pour les applications PHP utilisant des bases de données MySQL

  ➢ Serveur de fichier Windows :

- System-config-samba – Utile pour la configuration du serveur Samba

  ➢ Nom de serveur DNS :

- Bind – Utile pour la configuration du serveur DNS

  ➢ Serveur FTP : pas de paquetage supplémentaire

  ➢ Base de données MySQL :

- Php-mysql – Module pour les applications PHP utilisant des bases de données MySQL
- Mod_auth_mysql – Authentification de base pour le serveur Web Apache utilisant une base de données MySQL
- Mysql-server – Serveur MySQL et fichiers connexes

→ Début d'installation

→ Anaconda copie les fichiers sur le disque et demandera au fur et à mesure l'introduction des CD suivants. L'installation dure aux environs d'une heure trente minutes selon les paquetages à installer.

→ A l'issue de l'installation, une fenêtre apparaît en indiquant :

« Félicitation, l'installation est désormais terminée »

et une redémarrage de la machine est recommandée.

→ Après redémarrage, une réglage de quelques paramètres est à faire, guidé là aussi par l'installateur Anaconda et on peut aussi, soit juste après l'installation, soit ultérieurement, faire la configuration de sécurité du système, en particulier la cryptographie (cf 3 . 3).

Avec Fedora Core, la configuration de la cryptographie se fait dans : menu Démarrer / Centre de configuration de KDE (si on utilise l'environnement KDE) / Sécurité et confidentialité / Cryptographie. Le mode chiffrement utilisé est SSL.

SSL est un protocole mis en œuvre par la société Netscape et repris par l'IETF sous le nom de TLS. Le protocole repose sur le protocole TCP avec des numéros de port spécifiques comme HTTPS (443), FTPS (989), …

Les services de sécurité fournis sont : confidentialité des données transmises (chiffrage de données, cf 3 . 3), authentification et intégrité des données.

5 . 5 . Le serveur de nom DNS [16] [17]

5 . 5 . 1 . Présentation

Parmi les services supportés par Linux figure le DNS.

Le serveur de nom DNS est déjà inclus dans la distribution Fedora Core 4 mais il faut le sélectionner lors de l'installation (cocher la case Nom de serveur DNS).

Le DNS fait correspondre l'adresse IP au nom de la machine et vice versa. Ce service est utile dans un réseau contenant plusieurs machines. En effet, il n'est pas facile de se souvenir des adresses IP (adresse connue par le processeur) des machines, par contre l'appellation de ces dernières par son nom sera beaucoup mieux pour l'humanité.

5 . 5 . 2 . Mise en œuvre du serveur de nom

Avant la configuration des systèmes de fichiers nécessaires à la mise en marche du serveur de nom, les commandes suivantes sont à exécuter dans un terminal :

# /etc/init.d/named start	// il est recommandé de démarrer le service de nom //après l'installation
Démarrage de named :	*[OK]*
# chkconfig - -level 345 named on	// réglage des niveaux de démarrage aux niveaux //345 standard pour le réseau. Ceci renseigne le fichier //de démarrage automatique /etc/init.d/named de //démarrer le serveur à chaque boot aux niveaux 345
# /etc/init.d/named status	// pour voir l'état de fonctionnement du serveur

5 . 5 . 3 . Configuration du DNS

La plupart des configurations des serveurs sous Linux sont basées sur la manipulation des fichiers fournis avec les services auxquels ils correspondent. Le contenu de ces fichiers sont à modifier selon le besoin. Les lignes débutées par '//' sont des lignes de commentaires.

5 . 5 . 3 . 1 . Le fichier /etc/named.conf

```
options {
        directory "/var/named";

// on va mettre ici les adresses IP des serveurs de nom de notre
// Fournisseur d'Accès Internet (DTS : Data Telecom Service)
// notre serveur relaiera les requêtes à ceux-ci s'il n'est pas capable de les résoudre.

forward first;
forwarders {
193.251.141.253;
80.15.245.3;
};
};

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

zone "telecom.mg" IN {
        type master;
        file "localdomain.zone";
};

zone "17.16.172.in-addr.arpa" IN {
        type master;
        file "named.local";
} ;
```

Explication de ce fichier :

- la ligne « directory » indique à named où il doit trouver tous ses fichiers de zone.

- déclaration de la zone « **.** », la zone racine (**.**org, **.**fr, **.**mg, …).
- déclaration de la zone « telecom.mg », pour les requêtes directes c'est-à-dire trouver l'adresse IP à partir du nom de la machine.
- déclaration de la zone « 17.16.172.in-addr.arpa », pour les requêtes inverses c'est-à-dire trouver le nom d'une machine à partir de son adresse IP (cf 4 . 3 . 1)

5 . 5 . 3 . 2 . Les fichiers /var/named

5 . 5 . 3 . 2 . 1 . Le fichier /var/named/localdomain.zone

```
$TTL    86400
@               IN SOA      serveur root (
                                    42              ; serial
                                    3H              ; refresh
                                    15M             ; retry
                                    1W              ; expiry
                                    1D )            ; minimum
                IN NS           serveur
serveur         IN A            172.16.17.1
```

Explication de ce fichier :

- '$TTL' indique la durée de vie de la zone exprimée en secondes.
- Le nom de la machine serveur est : serveur.
- Le '@' est une notation spéciale qui désigne l'origine.
- Le champ 'SOA' décrit la zone, son origine (serveur.telecom.mg).
- Les champs 'serial, refresh, retry, expiry, minimum' définissent les paramètres techniques et administratifs de la zone. Il est conseillé de laisser telles quelles les valeurs qui leurs sont affectées initialement.
- Le champ 'NS' indique le nom du serveur DNS : il s'agit de serveur.telecom .mg .
- Le champ 'A' (Address) indique l'adresse IP de la machine.

5 . 5 . 3 . 2 . 2 . Le fichier /var/named/named.local

```
$TTL    86400
@       IN      SOA     serveur.root.serveur.  (
                              1997022700      ; Serial
                                   28800      ; Refresh
                                   14400      ; Retry
                                 3600000      ; Expire
                                   86400 )    ; Minimum
            IN          NS   serveur.
1           IN          PTR serveur.
```

Note : Le champ ‘PTR’ indique que ‘1’, c’est-à-dire ‘1.17.16.172’.in-addr.arpa, est l’adresse de serveur.telecom .mg

5 . 5 . 3 . 3 . Le fichier /etc/host.conf

```
order hosts,bind
```

Note : Cette ligne oblige le resolveur à regarder d’abord dans le fichier /etc/hosts puis de faire appel aux serveurs de nom qui sont spécifiés dans le fichier /etc/resolv.conf.

5 . 5 . 3 . 4 . Le fichier /etc/resolv.conf

```
search telecom.mg
nameserver 172.16.17.1
nameserver 193.251.141.253
nameserver 80.15.245.3
```

Explication de ce fichier :

- La ligne ‘search’ spécifie dans quel domaine il faudra chercher lorsqu’une application va lancer une requête DNS.
- Les lignes ‘nameserver’ indiquent les adresses aux quelles on peut contacter un serveur de nom. Les deux dernières sont les adresses IP des serveurs DNS de notre FAI (DTS).

Remarque : Après la configuration, il faut redémarrer le serveur de nom en exécutant la commande suivante dans un terminal :

```
# /etc/init.d/named restart
```

5 . 5 . 4 . Configuration d'un client

5 . 5 . 4 . 1 . Client sous Linux

Le fichier /etc/resolv.conf doit contenir les lignes :

```
domain telecom.mg
nameserver 172.16.17.1
```

L'adresse IP de la machine peut être reconfigurée dans le fichier /etc/sysconfig/network-scripts/ifcfg-eth0 où les adresses IP de ces clients ont la forme :

172 .16.17.X (X varie de 2 à 255).

5 . 5 . 4 . 2 . Client sous Windows

Pour un client sous Windows, la configuration se fait dans :

Menu Démarrer / Panneau de configuration / Réseau et régler les valeurs correspondantes dans les onglets IP et DNS.

5 . 5 . 5 . Test de fonctionnement

La commande 'nslookup' permet de tester si le serveur de nom est bien configuré :

```
nslookup serveur                    // serveur est le nom de la machine du serveur DNS
```

On obtient à l'écran l'affichage :

```
Serveur : serveur
Address : 172.16.17.1 # 53
Nom : serveur.telecom.mg
Address : 172.16.17.1
```

5 . 6 . Le serveur Samba [18] [19]

5 . 6 . 1 . Présentation

Parmi les services supportés par Linux figure Samba.

Le serveur de fichiers, pour les clients Windows, Samba est déjà inclus dans la distribution Fedora Core 4 mais il faut le choisir lors de l'installation (cocher la case Serveur de fichier Windows).

Samba est composé de plusieurs programmes qui permettent de partager et d'utiliser des ressources partagées via le protocole SMB.

Le protocole SMB, appelé aussi LanManager, est utilisé par les stations Microsoft pour le partage des disques. Donc, avec Samba, on peut partager un disque Unix pour des machines Windows.

5 . 6 . 2 . Mise en œuvre du serveur Samba

Avant toute configuration, les commandes suivantes sont à exécuter dans un terminal :

```
# /etc/init.d/smb start                    // il est recommandé de démarrer les services Samba
Démarrage des services SMB :                [OK]
Démarrage des services NMB :                [OK]
```

Deux démons, nécessaires au fonctionnement du serveur Samba, sont lancés.

- smbd qui fournit les services nécessaires au partage de fichiers,
- nmbd qui permet de montrer les services offerts par Samba.

```
# chkconfig - -level 345 smb on            // réglage des niveaux de démarrage aux niveaux
                                           //345 standard pour le réseau. Ceci renseigne le fichier
                                           //de démarrage automatique /etc/init.d/smb de
                                           //démarrer le serveur à chaque boot aux niveaux 345
# /etc/init.d/smb status                   // pour voir l'état de fonctionnement du serveur
```

5 . 6 . 3 . Configuration de Samba

Le fichier de configuration principal de Samba est /etc/samba/smb.conf. Les lignes débutées par '#' ou '//' sont considérées comme des commentaires, donc pour activer une commande il faut enlever le '#'.

Exemple : # security = user (ligne non active)

security = user (ligne active)

La configuration de Samba se divise en deux sections :

```
#============ Configuration générale ============
[global]

# workgroup : Nom du groupe de travail Windows
        workgroup = MSHOME
```

```
# server string : Description affichée lors du parcours réseau
        server string = Samba Server

# hosts allow : Adresse réseau des machines autorisées à se connecter au
# serveur samba
        hosts allow = 172.16.17.

# security : L'utilisateur doit s'authentifier (login et mot de passe)
# avant d'accéder au serveur
        security = user
# encrypt passwords : Le mot de passe est crypté
        encrypt passwords = yes

# smb passwd file : Fichier de configuration des utilisateurs
        smb passwd file = /etc/samba/smbpasswd

# unix password sync : Le changement de mot de passe de l'utilisateur
# depuis les postes Windows n'est pas autorisé
        unix password sync = No

#============ Configuration de partage ============

[homes]                                 // nom du partage.
Comment = Home                          // les répertoires /home sont
                                        // partageables.
        Browseable = yes                // le partage sera visible lors
                                        // du parcours du réseau.
        Writable = yes                  // on autorise l'utilisateur à
                                        // partager ses fichiers
                                        // dans le répertoire /home.

[public]
        comment = Public                // on définit ici que le répertoire
        path = /home/public             // /home/public ne peut pas être
        public = yes                    // modifier par l'utilisateur
        read only = yes
```

Remarques:

- L'ajout d'utilisateur est exécuté par le 'root' (superutilisateur), dans un terminal, par la commande :

 # smbpasswd –a domoina

L'écran affiche :

New SMB password :

Retype new SMB password:

Added user domoina.

L'utilisateur "domoina" est ajouté dans le fichier /etc/samba/smbpasswd.

- Un redémarrage du serveur Samba est recommandé après la configuration :

 # /etc/init.d/smb restart

5 . 6 . 4 . Test de fonctionnement

Après la configuration, la commande 'testparm' exécuté sur le serveur, dans un terminal, permet de tester les options utilisées dans le fichier smb.conf (fichier de configuration du serveur Samba) ainsi que la syntaxe. Elle spécifie aussi les partages effectifs sur le serveur. « Testparm » est donc un vérificateur de syntaxe pour le fichier de configuration du serveur Samba smb.conf.

Test depuis le client Windows : Dans le Menu Démarrer / Panneau de configuration / Connexions réseaux / Favoris réseau / Voir les ordinateurs du groupe de travail, double- cliquez sur le nom du domaine correspondant au nom du serveur Samba, une fenêtre apparaît pour se loger via Samba Server

Figure 5 . 05 : Test de fonctionnement Samba Server

En cliquant sur le bouton OK, on visualise l'ensemble des partages configurés, à condition que ces ressources soient « browseable ».

Remarques :

- Seuls les utilisateurs enregistrer dans /etc/samba/smbpasswd peuvent accéder à Samba Server.
- Le programme 'smbclient' permet d'envoyer des messages.

Editez un petit fichier texte dans un terminal :

 # cat > essai

 # cat « fichier_texte »| smbclient –M poste8

Sur l'écran de la station poste8 doit s'afficher le contenu du fichier texte, mais il faut que le service de messagerie soit actif sur la station poste8.

5 . 7 . Le serveur FTP [20] [21]

5 . 7 . 1 . Présentation

FTP est un protocole de transfert de fichier. Il permet aux clients de transférer des fichiers au serveur appelé chargement (uploading en anglais). Aussi les clients peuvent demander le déchargement (downloading en anglais) des fichiers présents sur le serveur vers son poste.

Le serveur FTP est disponible sous Linux mais il faut le choisir lors de l'installation (cocher la case serveur FTP).

Sous Linux, il existe de très nombreux démons (daemon en anglais) comme Wuftpd, Proftpd, vsftpd … pour faire tourner FTP.

Nous allons configurer vsftpd qui est un « démon » déjà inclus dans la distribution Fedora Core 4.

5 . 7 . 2 . Mise en œuvre de vsftpd

Avant la configuration du serveur FTP, les commandes suivantes sont à exécuter dans un terminal :

# /etc/init.d/vsftpd start	// il est recommandé de démarrer le serveur
Démarrage de vsftpd pour vsftpd :	*[OK]*
# chkconfig - -level 345 vsftpd on	// réglage des niveaux de démarrage aux niveaux //345 standard pour le réseau. Ceci renseigne le fichier //de démarrage automatique /etc/init.d/vsftpd de //démarrer le serveur à chaque boot aux niveaux 345
# /etc/init.d/vsftpd status	// pour voir l'état de fonctionnement du serveur

5 . 7 . 3 . Configuration de vsftpd

La configuration de vsftpd est traitée par son fichier de configuration : /etc/vsftpd/vsftpd.conf. Dans ce fichier, chaque directive a la forme :

<directive> = <value>

Lors de la configuration, il faut affecter la valeur souhaitée pour la directive et activé la ligne correspondante.

Les lignes débutées par le dièse '#' sont considérées comme des commentaires, donc pour activer une commande il faut enlever le '#'.

Exemple : # anon_upload_enable = YES (ligne non active)

anon_upload_enable = YES (ligne active)

La configuration du fichier vsftpd.conf ci-dessous offre la possibilité de se logger en anonyme, autorise les utilisateurs FTP (ayant un compte sur la machine serveur, dans le fichier /etc/password) de faire le chargement (upload) et le déchargement (download) des fichiers.

```
# Le serveur FTP fonctionne en mode autonome
#
listen=YES
tcp_wrappers=YES
pam_service_name=vsftpd

# Les utilisateurs anonymes 'ftp' ou 'anonymous' sont autorisés à se
# connecter au serveur
#
anonymous_enable=YES

# L'utilisateur anonyme n'a pas besoin de saisir de mot de passe
#
no_anon_password=YES

# Répertoire utilisé par vsftpd après la connexion d'un utilisateur
# anonyme
#
anon_root=/var/ftp/pub

# Le téléchargement des fichiers vers le serveur par l'utilisateur
# anonyme n'est pas autorisé (problème de sécurité)
```

```
#
anon_mkdir_write_enable=NO
anon_upload_enable=NO

# Les utilisateurs locaux ayant un compte dans le serveur (/etc/password)
# sont autorisés à se connecter au système
#
local_enable=YES

# Ces utilisateurs sont autorisés à télécharger (download) des fichiers
# dans l'arborescence du répertoire du serveur, mais le
# téléchargement vers le serveur (upload) est restreint dans son
# répertoire  (problème de sécurité)
#
write_enable=YES
pasv_enable=YES

# Quelques réglages  nécessaire sur la configuration du serveur
#
xferlog_enable=YES
connect_from_port_20=YES
xferlog_file=/var/log/vsftpd.log
idle_session_timeout=600
ftpd_banner=Bienvenue dans mon petit serveur !
```

Remarques :

- L'ajout d'utilisateur est exécuté par le 'root' (superutilisateur), dans un terminal, par la commande :

```
# useradd domoina
# passwd domoina
```

L'écran affiche :

```
New UNIX password :
Retype new UNIX password:
passwd: all authentication tokens successfully
```

L'utilisateur "domoina" est ajouté dans le fichier /etc/passwd.

- Un redémarrage du serveur FTP est recommandé après la configuration :

```
# /etc/init.d/vsftpd restart
```

5 . 7 . 4 . Test de fonctionnement

5 . 7 . 4 . 1 . Pour l'utilisateur anonyme (ftp ou anonymous)

Dans la figure 5 . 06 suivant, l'utilisateur anonyme fait le déchargement (get) d'un fichier du serveur vers son poste. Le téléchargement a été fait avec succès (File send OK).

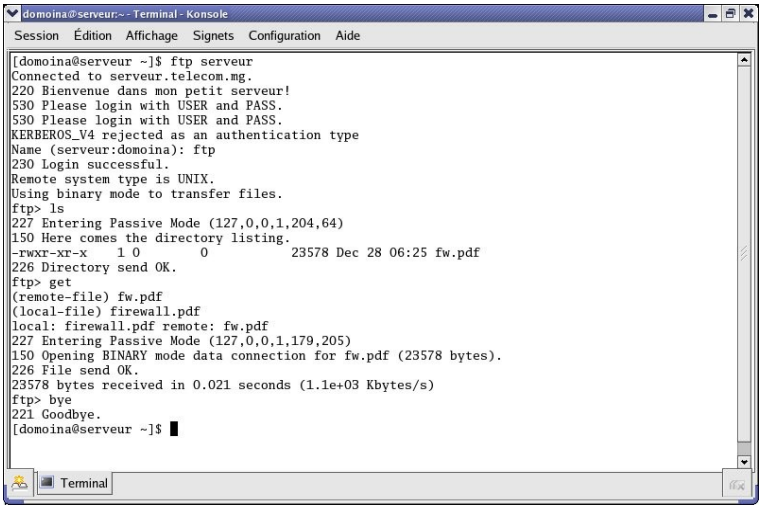


Figure 5 . 06 : Test 1 de fonctionnement ftp anonyme

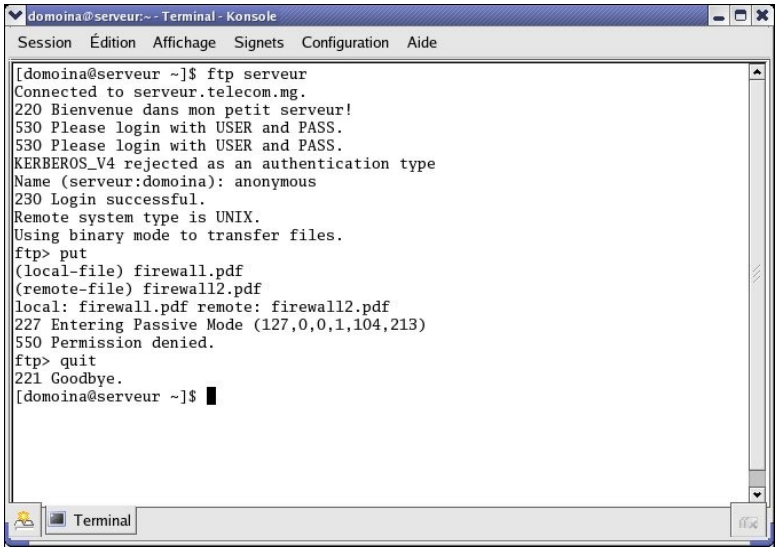


Figure 5 . 07 : Test 2 de fonctionnement ftp anonyme

Ici l'utilisateur anonyme fait le chargement (put) d'un fichier de son poste vers le serveur. Le téléchargement n'a pas été fait car il n'a pas l'autorisation (Permission denied).

5 . 7 . 4 . 2 . Pour FTP utilisateur

Dans la figure 5 . 08 suivant, l'utilisateur FTP (domoina) fait le déchargement (get) d'un fichier de l'arborescence de répertoire du serveur vers son poste. Le téléchargement a été fait avec succès (File send OK).

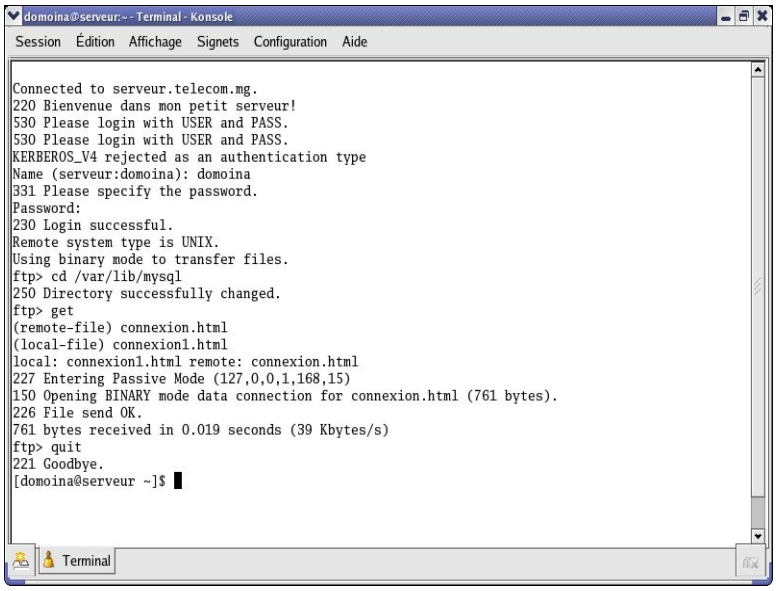


Figure 5 . 08 : Test 1 de fonctionnement ftp utilisateur

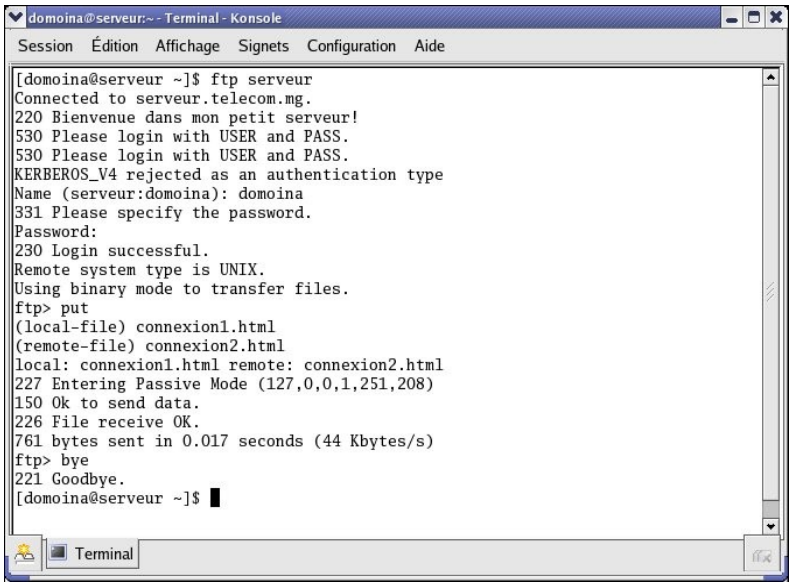


Figure 5 . 09 : Test 2 de fonctionnement ftp utilisateur

Ici, l'utilisateur FTP fait le chargement (put) d'un fichier de son poste vers le serveur. Le téléchargement a été fait avec succès (File receive OK). Ce fichier est placé sur le serveur dans

son répertoire personnel (/home/domoina), crée lors de l'ajout d'utilisateur 'domoina' dans /etc/passwd par le root, pour une raison de sécurité.

5 . 8 . Le serveur Web Apache [11] [22]

5 . 8 . 1 . Présentation

Un serveur Web est un logiciel permettant de rendre accessible, à des ordinateurs connectés au réseau, des pages Web stockés sur le disque. Un page Web contient des liens pour passer d'un endroit à un autre (sur le même page ou à un autre page). Le langage utilisé est HTML (cf chapitre 6) appelé aussi langage à balise et le protocole de dialogue entre client-serveur est HTTP. HTTP est un protocole utilisé par le WWW pour échanger des informations. L'exécutable Apache sous Linux est le httpd pour http daemon.

Le serveur Web Apache est déjà inclus dans la distribution Fedora Core 4 mais il faut le choisir lors de l'installation (cocher la case Serveur web). Il peut être utilisé comme simple serveur Web, ou bien comme serveur d'application et interface de base de données.

5 . 8 . 2 . Mise en œuvre du serveur web

Avant la configuration du serveur Web Apache, les commandes suivantes sont à exécuter dans un terminal :

# /etc/init.d/httpd start	// il est recommandé de démarrer le serveur
Démarrage de httpd:	*[OK]*

# chkconfig --level 345 httpd on	// réglage des niveaux de démarrage aux niveaux 	
	//345 standard pour le réseau. Ceci renseigne le fichier
	//de démarrage automatique /etc/init.d/httpd de
	//démarrer le serveur à chaque boot aux niveaux 345

# /etc/init.d/httpd status	// pour voir l'état de fonctionnement du serveur

5 . 8 . 3 . Configuration d'Apache

Apache se configure par modification de son fichier /etc/httpd/conf/httpd.conf.

La présence de dièse '#' devant chaque ligne de cet fichier indique que c'est un commentaire. Il faut donc l'enlever pour activer une ligne de commande.

Exemple : # LanguagePriority fr en it (ligne non active)

LanguagePriority fr en it (ligne active)

Le contenu de fichier httpd.conf convenable à notre serveur est :

```
### Section 1: Configuration générale
#
# ServerTokens: Indique la version suivie du système d'exploitation
# (Apache/2.054 Fedora)lorsque la frappe du site à consulter
# n'est pas correcte.
# Exemple: http://serveur.telecom.mg/Site_tco a été frappé au lieu de
#               http://serveur.telecom.mg/site_tco
#
ServerTokens OS

#
# ServerRoot: Indique le répertoire principal qui contient les sous
# repértoires de configuration, de modules et de journal d'Apache.
#
ServerRoot "/etc/httpd"

#
# PidFile: Indique le numéro de processus d'Apache s'il tourne
# Exécuter la commande /etc/init.d/httpd status dans un terminal pour le savoir
#
PidFile run/httpd.pid

#
# Listen: Indique le port d'écoute d'Apache
#
Listen 80

#
# User/Group: Utilisateur et groupe avec lesquels va s'exécuter Apache
#
User  nobody
Group nobody

### Section 2: Configuration des paramètres du serveur
#
```

```
# ServerName: Nom du serveur suivi de son port d'écoute
#
ServerName serveur.telecom.mg:80

#
# UseCanonicalName: Apache utilisera le port et le nom d'hôte demandés
# par l'utilisateur
#
UseCanonicalName Off

#
# DocumentRoot: Indique les répertoires de base dont Apache servira les
# fichiers
#
DocumentRoot "/var/www/html"
#
# Option FollowSymLinks: Les liens symboliques sont autorisés
# AllowOverride None: Aucun utilisateur ne pourra défini des droits
# spécifiques ( écriture, lecture, exécution)
#  sur les répertoires qu'il gère (seul le root peut le faire)
# Allow from all: Tout le monde peut accéder au serveur dans le
# répertoire /var/www/html
#
<Directory "/var/www/html">
   Option FollowSymLinks
   AllowOverride None
   Order allow,deny
   Allow from all
</Directory>

#
# UserDir: Les utilisateurs n'ont pas le droit de proposer des fichiers à
# partir de leurs répertoires personnels (problème de sécurité)
#
<IfModule mod_userdir.c>
   UserDir disable
</IfModule>

#
```

```
# DirectoryIndex: Indique l'extension de fichier qu'Apache peut utiliser
#
DirectoryIndex index.html index.html.var index.php index.php3 index.php4 index.php5

#
# LanguagePriority: Les langages utilisés par ordre de priorité
# (fr:french, en:english, it:italian)
#
LanguagePriority fr en it

#
# AddType application: Les types d'applications acceptable par le serveur
#
AddType application/x-compress .Z
AddType application/x-gzip .gz .tgz
Addtype application/x-httpd-php .php .php3 .php4 php5 .phtml
Addtype application/x-httpd-php-source .phps
```

Remarque : Après la configuration du serveur par modification de son fichier de configuration, il faut redémarrer le serveur par la commande :

```
# /etc/init.d/httpd restart
```

5 . 8 . 4 . Test de fonctionnement

Pour tester le serveur Web Apache, lancer dans le champ d'adresse URL d'un navigateur : http://serveur.telecom.mg.

L'écran affiche la page de test du serveur (cf figure 5 . 10 de la page qui suit):

Si cette page apparaît sur l'écran, c'est que la configuration est correcte et le serveur marche bien. Sinon, il faut revoir la configuration.

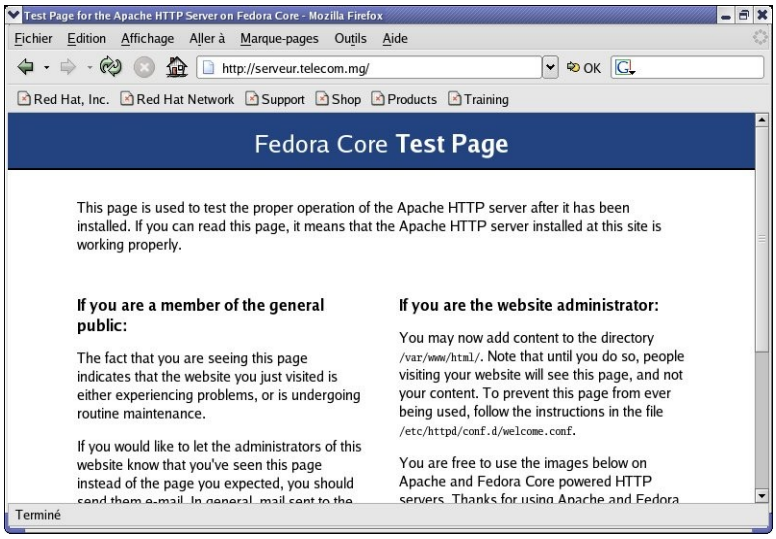


Figure 5 .10 : Test de fonctionnement d'Apache

5 . 9 . Le serveur MySQL

5 . 9 . 1 . Présentation [23]

Le serveur MySQL est un serveur de base de données déjà inclus dans la quatrième mouture de Fedora mais il faut le choisir lors de l'installation (cocher Base de données MySQL).

Mysqld pour Mysql daemon est le serveur de MySQL.

MySQL est un SGBDR (comme Oracle, SQL Server …).

5 . 9 . 2 . Quelques définitions utiles [23]

5 . 9 . 2 . 1 . Base de données

Une base de données est un ensemble de fichiers stockant des informations. Elle permet d'organiser un ensemble de données à partir duquel on peut retrouver ou extraire des informations.

5 . 9 . 2 . 2 . SGBD et SGBDR

Un SGBD est une interface (écran) entre les utilisateurs et le serveur de base de données. C'est un outil permanent pour insérer , modifier et rechercher des données spécifiques dans une grande masse d'information (base de données). Et le SGBDR repose sur le modèle relationnel : les données sont mise en relation dans un table. Un table est un ensemble de lignes et de colonnes.

5 . 9 . 2 . 3 . MySQL

MySQL consiste en un ensemble de programmes qui sont chargés de gérer une ou plusieurs bases de données et qui fonctionnent selon une architecture client / serveur. Le serveur est le seul qui peut lire ou écrire dans ces fichiers, en fonction de la demande effectuée par les clients MySQL. Les clients communiquent avec le serveur pour effectuer des recherches ou de mise à jour dans la base. Le langage SQL est la base du programme MySQL (cf chapitre 7).

5 . 9 . 3 . Mise en œuvre du serveur MySQL

Pour la mise en œuvre du serveur, les commandes suivantes sont à exécuter dans un terminal :

# /etc/init.d/mysqld start	// il est recommandé de démarrer le serveur
Démarrage de mysqld pour mysqld :	*[OK]*
# chkconfig - -level 345 mysqld on	// réglage des niveaux de démarrage aux niveaux //345 standard pour le réseau. Ceci renseigne le fichier //de démarrage automatique /etc/init.d/mysqld de //démarrer le serveur à chaque boot aux niveaux 345
# /etc/init.d/mysqld status	// pour voir l'état de fonctionnement du serveur

5 . 9 . 4 . Configuration du serveur MySQL

Le fichier de configuration du serveur MySQL est /etc/my.cnf. Il n'y a pas grande chose à modifier dans ce fichier, la configuration par défaut marche bien.

CHAPITRE 6 CONSTRUCTION D'UN SITE WEB DU DEPARTEMENT

6 . 1 . Introduction [24]

Après la configuration du serveur Apache, on peut mettre à la disposition des clients des pages Web. Le logiciel permettant d'accéder au Web s'appelle un navigateur (ou browser). La lecture de ces pages ne se fait pas de façon linéaire mais repose sur des modes de navigation hypertexte. L'hypertexte est un système de lien symbolisé par des mots soulignés qui indique où doit cliquer sur tel mot pour accéder à l'information . C'est le langage HTML qui génère ces liens.

6 . 2 . Définition [24]

Le HTML est un langage utilisé par le concepteur de site-web pour mettre des éléments (texte, liens, images …) dans une page web.

Une page Web est un fichier texte ayant comme extension « **.**htm » ou « **.**html ».Ce fichier est composé des balises universellement reconnues. D'où le langage HTML est parfois appelé « langage à balise ». Chacune de ces balises a une fonction précise.

6 . 3 . Structure [24]

Dans le langage HTML, la gestion des balises est à la charge du programmeur. Les balises sont délimités par les signes « < » (inférieur à) et « > » (supérieur à).

On peut diviser en deux parties la structure du langage HTML :

→ L'en-tête de la page (HEAD)

Elle contient les éléments d'identification de la page : langue utilisée, auteur, durée de vie de la page. Elle contient aussi d'autres informations définissant les contenues de la page pour qu'elles puissent être facilement indexées dans le moteur de recherche.

→ Le corps de la page (BODY)

Elle contient la mise en page, la typographie utilisée, la taille, la couleur… des caractères, l'emplacement des textes et des images …

6 . 4 . Outils à utiliser [24]

Pour créer une page HTML, il suffit de n'importe quel bloc-notes ou éditeur de texte.

Exemple : en Linux, Kwrite ou Kedit ou quanta permet de créer une page écrite en HTML.

6 . 5 . Document HTML minimum [24]

Tous les documents HTML commencent toujours par <html> et se termine par </html>. Voici un exemple d'un document HTML minimum :

```
<html>
  <head><title>  </title></head>
    <body>
      HTML
   </body>
</html>
```

Ceci affiche « HTML » à l'écran.

6 . 6 . Application

Nous allons maintenant utilisés quelques balises html pour créer le site du Département Télécommunication.

```
<html>
 <head>
  <title>index</title>
 </head>

        <frameset rows="135,*" cols="*" frameborder="NO" border="0" framespacing="0" noresize>
        <frame src="haut.html" name="topFrame" scrolling="NO">
        <frameset cols="148,*" frameborder="NO" border="0" framespacing="0" noresize>
        <frame src="menus.html" name="leftFrame" scrolling="NO">
        <frame src="accueil.html" name="rightFrame">
        </frameset>
        </frameset>
        <noframes><body>     </body></noframes>
</html>
```

Ce programme divise la fenêtre de navigateur en trois.

Et nous avons construit le site Web du Département Télécommunication à l'aide de quelques programmes écrits en langage html.

Ce site est accessible en tapant sur le champ d'URL d'un navigateur l'adresse :
http://serveur.telecom.mg/site_tco

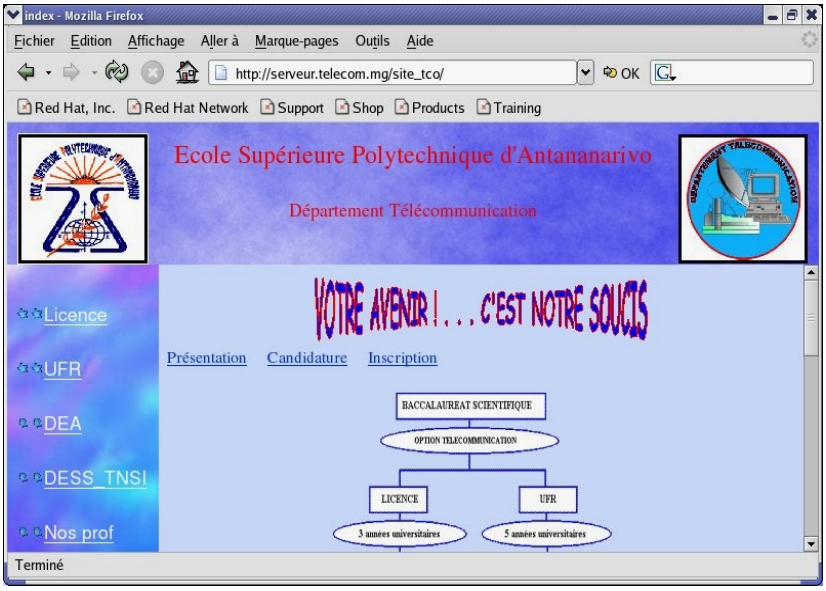


Figure 6 . 01 : Page d'accueil du site Web Département Télécommunication

Remarque:

On peut aussi, avec HTML, créer des formulaires ou des tableaux. Nous allons voir ces applications dans le chapitre suivant.

CHAPITRE 7 MISE EN PLACE DE LA BASE DE DONNEES BIBLIOTHEQUE DES ENSEIGNANTS AU SEIN DU DEPARTEMENT TELECOMMUNICATION

7 . 1 . Introduction

Autre l'hébergement des sites Web, le serveur Web Apache peut aussi être utilisé comme une interface pour afficher les données demandées par les clients au serveur de base de données.

7 . 2 . Le langage PHP [23]

7 . 2 . 1 . Définition

PHP est un langage de programmation très proche de C (basée sur l'utilisation des fonctions et des conditions). Il est destiné à être intégré dans des pages HTML, c'est à dire, la programmation en PHP est inclus dans le langage HTML mais il est aussi possible d'introduire des balises HTML à l'intérieur de PHP (cf 7 . 3 . 2).

Le délimiteur (marqueur de début et fin) du programme PHP est les balises **< ?php** et **?>**. Donc, tout ce qui se trouve entre ces balises est envoyé à l'interpréteur du langage PHP intégré à Apache (cf 5 . 8 . 3), seul le résultat est visible au niveau client.

7 . 2 . 2 . Utilisation

PHP est dédié à la production de page HTML générée dynamiquement.

Exemple : Production des pages HTML pour afficher les données (souvent modifiées) récupérées dans un serveur de base de données.

7 . 3 . Application

7 . 3 . 1 . Création de la base de données et des tables

Pour notre application, utilisation de Apache / PHP / MySQL, nous allons mettre en place une base de données bibliothèque des enseignants du Département Télécommunication.

Voici la structure des commandes à utiliser pour créer cette base et les tables nécessaires, dans un terminal et en positionnant en tant que root, exécutant la commande :

 # mysql –u root

Au prompt de mysql :

mysql>CREATE DATABASE nombase ;

```
mysql>USE nombase;
mysql>CREATE TABLE nomtable (champ1 type, champ2 type, ..., champn type);
mysql>INSERT INTO nomtable (champ1,champ2, ..., champn)
        VALUES ('valeur1','valeur2', …, 'valeurn') ;
mysql>SELECT*FROM nomtable ;
mysql>quit;
```

Explication:

- « nombase » est le nom de la base de données, pour notre cas « biblio_prof »
- « nomtable » est le nom de la table. Deux tables nommés « enseignant » et « livre » sont nécessaires pour notre base.
- « champ1 type, …, champn type » sont respectivement le nom de la colonne et leur type dans le table « nomtable ». Le type de chaque colonne peuvent être : INTEGER, CHAR, VARCHAR, DATE, …
- « valeur1, , valeurn » sont les données à insérer à chaque colonne du table
- « CREATE » pour créer une base de données ou un table
- « USE » pour utiliser ou pour ouvrir la base de données
- « INSERT INTO … VALUES » pour insérer les données dans un table
- « SELECT … FROM » pour voir le contenu de la table avec (WHERE) ou sans condition

7 . 3 . 2 . Récupération et affichage des données dans des pages HTML

Tout d'abord, le but de cette application est l'affichage, sur une page HTML, des informations concernant les livres qui sont empruntés par les enseignants du Département.

Voici les programmes nécessaires pour avoir le résultat d'une requête :

- Programme 1 :

```
<html>
 <head><title>acceuil</title></head>
  <body background="couleur0.jpg">
   <center><h2><font color=brown face=arial>ECOLE SUPERIEURE POLYTECHNIQUE
   D'ANTANANARIVO</font></h2>
   <h3><font color=brown face=arial>D&eacute;partement
  T&eacute;l&eacute;communication</font></h3></center>
  <h1><center>Requ&ecirc;te sur la biblioth&egrave;que des enseignants</center></h1><br><br>
  <center>
  <form method="post" action="connect_1.php">
  Utilisateur:      <input type=text name="utilisateur">
```

```
    <p>
    Mot de passe:&amp;nbsp;&amp;nbsp;<input type=password name="mot_de_passe">
    <p>
    Cote du livre:&amp;nbsp;&amp;nbsp;<input type=text name="cote">
    <p>
   <br><br><input type="submit" value="Valider">
   </form>
   </center>
  </body>
</html>
```

Ceci est un langage HTML qui permet de créer un formulaire nécessaire pour l'authentification des utilisateurs voulant accéder à notre base biblio_prof.

Lançons dans un navigateur l'adresse http://serveur.telecom.mg/bibliotheque:

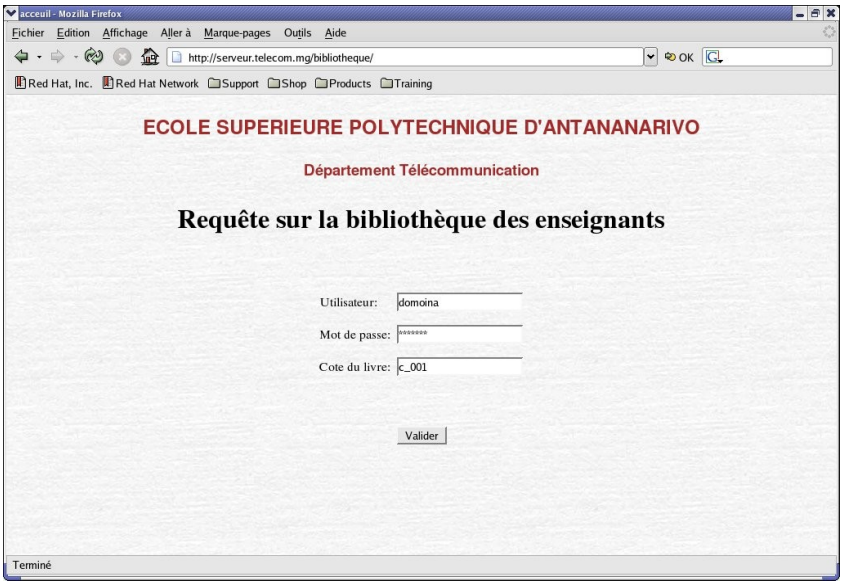


Figure 7 . 01: Authentification de l'utilisateur

Note: Le formulaire contient 4 champs à remplir :

→ le champ « Utilisateur »

→ le champ « Mot de passe »

→ le champ « Cote du livre »

→ le champ de validation des informations entrées: bouton « Valider »

- Programme 2 :

```
<html>
   <head><title>connect_1</title></head>
    <body background="couleur0.jpg">
     <?php
     echo "<font size=4 color=brown>";
     echo "Votre login est:\n\n";
     echo $_POST['utilisateur'];
     echo "<br>";
     echo "Votre mot de passe est:\n\n";
     echo $_POST['mot_de_passe'];
     echo "</font>";
     echo "<br>";
     if ($_POST['utilisateur']=='domoina')
     if ($_POST['mot_de_passe']=='domoina')
     {
      $bd=mysql_pconnect('172.16.17.1','root','') or die (mysql_error());
      mysql_select_db('biblio_prof',$bd);
       $result=mysql_query("SELECT
       livre.*,enseignant.num_prof,enseignant.nom_prof,enseignant.prenom_prof,enseignant.contact_prof,
       enseignant.date_emprunt,enseignant.date_retour FROM livre INNER JOIN enseignant ON
       livre.cote=enseignant.emprunt",$bd);
      $myrow=mysql_fetch_row($result);
         if ($_POST['cote']<'c_005')
         {
         echo "<center><font size=5 color=brown>";
         echo "Voici le r&eacute;sultat de votre requ&ecirc;te:<br><br>";
         echo "<table border=2>\n";
         echo
         "<tr><td>cote</td><td>titre</td><td>auteur</td><td>edition</td><td>num_prof</td><td>nom_prof
         </td><td>prenom_prof</td><td>contact_prof</td><td>date_emprunt</td><td>date_retour</td></tr
         >\n";
         echo
         "<tr><td>$myrow[0]</td><td>$myrow[1]</td><td>$myrow[2]</td><td>$myrow[3]</td><td>$myrow[
         4]</td><td>$myrow[5]</td><td>$myrow[6]</td><td>$myrow[7]</td><td>$myrow[8]</td><td>$myro
         w[9]</td></tr>\n";
         echo "</table>\n";
          }
        if ($_POST['cote']>'c_004')
```

```
        {
        echo "<center><font size=5 color=brown>";
        echo "Ce livre n'existe pas encore dans notre biblioth&egrave;que.<br><br>Merci de votre visite";
        echo "</font></center>";
        }
 }
else
 {
  echo "<center><font size=5 color=brown>";
  echo "D&eacute;sol&eacute;,vous n'avez pas le droit!";
  echo "</font></center>";
 }
?>
</body>
</html>
```

Notes : - Ce fichier est d'extension **.**php.

- PHP fournit des fonctions permettant de manipuler les bases de données :

→ mysql_pconnect : fonction de connexion au serveur

→ mysql_select_db : fonction de choix de la base de données

→ mysql_query : fonction de requête

→ mysql_fetch_row : fonction qui retourne une ligne de résultat MySQL sous la forme d'un tableau.

En cliquant sur le bouton « Valider » de la figure 7 . 01, on a les résultats suivants :

→ Si l'utilisateur est authentifié, c'est à dire peut accéder au serveur de base de données :

Figure 7 . 02 : Résultat de la requête sur la base biblio_prof

→ Sinon :

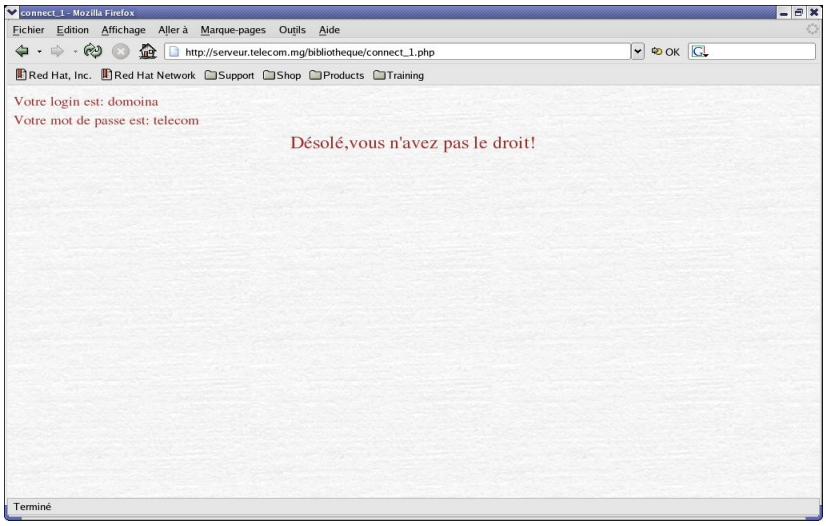


Figure 7 . 03: Utilisateur non authentifié

→ Si utilisateur authentifié mais le livre demandé n'existe pas encore dans la base de données :

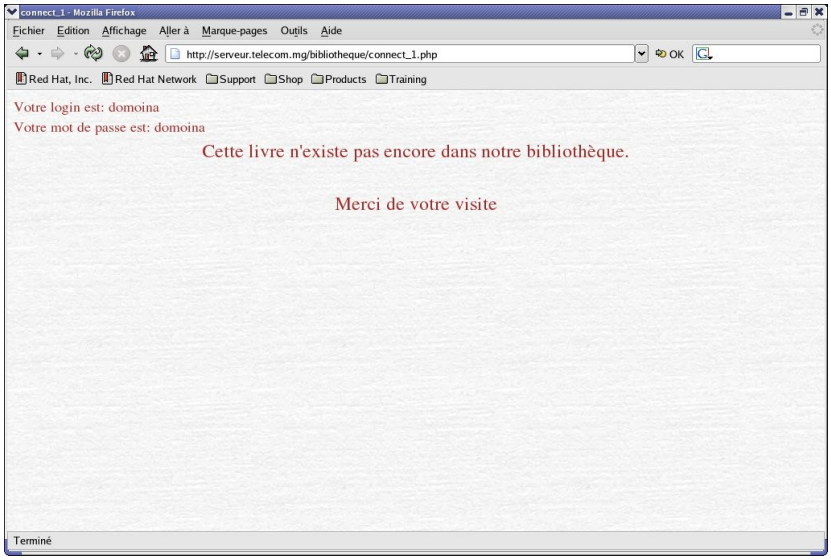


Figure 7 . 04: Requête non admise

Du point de vue logiciel, le réseau client – serveur au sein du Département Télécommunication est installé. Il ne reste qu'à faire le câblage.

Dans le chapitre suivant, nous allons étudier l'ouverture de ce réseau à l'Internet.

CHAPITRE 8 OUVERTURE DU RESEAU A L'INTERNET

Le réseau au sein du Département Télécommunication, étudié précédemment, étant basé sur l'architecture client – serveur. Son ouverture au réseau Internet est l'extension que l'on peut y ajouter.

8 . 1 . Etude du support de transmission

Lors de notre étude, l'Ecole a déjà eu une connexion via Internet fournie par le fournisseur d'accès DTS. Donc il ne nous reste qu'à étudier la liaison entre le point d'accès Internet et le Département Télécommunication.

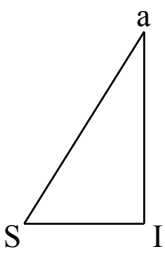
8 . 1 . 1 . Choix du support

Deux types de supports (cf 1. 3 . 9) sont envisageables :

- utilisation de câble
- liaison sans fil

Le choix de support porte sur la distance à parcourir. La distance entre le point d'accès Internet 'S' et le Département Télécommunication 'a' est de 117m en vol d'oiseau. Nous avons mesuré cette distance en utilisant le théorème de Pythagore :

$[Sa]_d^2 = [IS]^2 + [Ia]^2$



$[IS] = 110m$

$[Ia] = 40m$

$[Sa]_d^2 = 13\ 700m$

$[Sa]_d = 117m$

Figure 8 . 01: Distance entre le point d'accès Internet et le Département Télécommunication

Les liaisons WiFi, WiMax et WiBro peuvent être mise en place (utilisation d'un répéteur de signal appelé aussi point d'accès avec le WiFi). Mais en tenant compte de ce qu'on a vu dans 1. 3 . 9 . 4 (remarques), nous allons choisir le câble pour notre étude. En effet, la condition climatique (venteux) où se trouve notre département (Vontovorona) est un des facteur qui nous pousse à prendre cette décision. Le signal est perturbé par le vent ou même une discontinuité de transmission peut être rencontrée.

8 . 1 . 2 . Choix du type de câble

Différents types de câbles peuvent être utilisés (cf 1. 3 . 9).

Le choix du type de câble dépend des applications à mettre en œuvre (vidéo-conférence, recherche sur le Web, …).

Pour nous, l'utilisation de fibre optique n'est pas vraiment nécessaire. En effet, ce type de câble fourni un débit très élevé et une bande passante très large (cf 1. 3 . 9 . 3) surtout utilisé avec les applications comme la vidéo-conférence, le forum, ….(qui n'est pas notre cas). Donc c'est logique de choisir un câble qui nous convienne (Il n'est pas nécessaire de construire un autoroute pour faire passer un petit nombre de voitures).

En ce qui concerne les câbles coaxiaux (cf 1. 3 . 9 . 1), le Thinnet nous convienne mais actuellement son utilisation est rare. Le transceiver BNC / RJ 45 est peu nombreux.

Toutes ces raisons nous amène à choisir la paire torsadée (cf 1. 3 . 9 . 2), en particulier le FTP CAT5 qui est le câble le plus utilisé actuellement en réseau. Aussi, ce type de câble nous convienne en terme de débit et des équipements à notre disposition.

Remarque :

La longueur maximale du câble FTP CAT5 est de 100m (théoriquement) avant que le signal soit atténué (cf 1. 3 . 9 . 2), or la liaison entre le point d'accès Internet et le Département Télécommunication dépasse cette limite (plus de 117m). Il est donc nécessaire de mettre en œuvre au moins un répéteur de signal (switch ou hub).

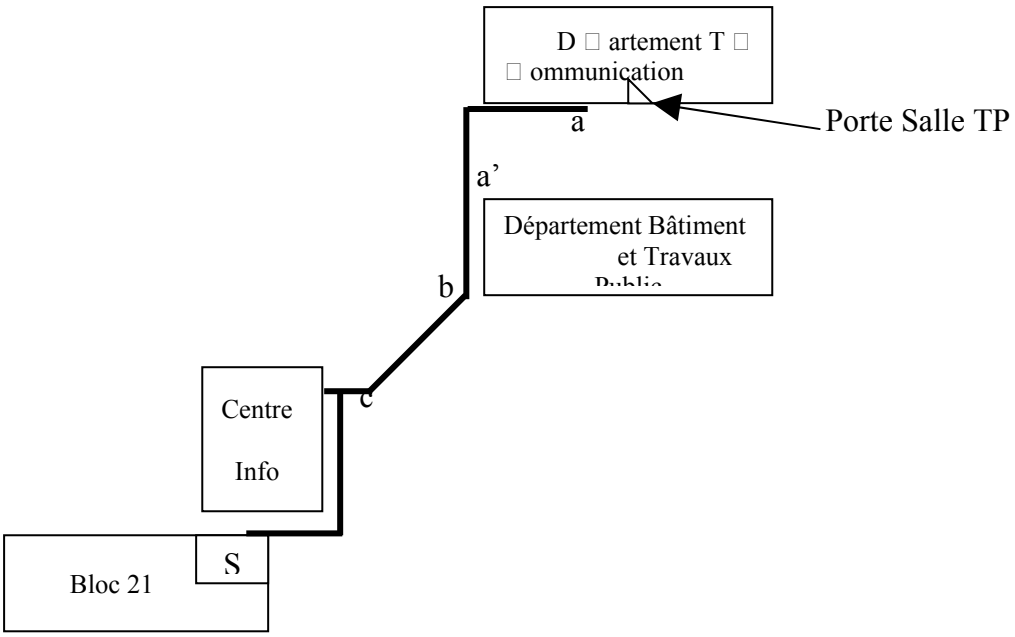
8 . 1 . 3 . Etude de réalisation de câblage [3]

Notre étude se rapporte sur la liaison entre le switch1 placé dans le bloc 21, en bas de la salle informatique du Département Mines (S), jusqu'à notre serveur / passerelle Linux.
Un schéma simplifié du chemin de câble est décrit par la figure 8 . 02 dans la page suivante :

La distance [aS] est égal à 150m.

Pratiquement, avec le câble FTP, le signal est atténué si la distance dépasse les 90m. Il est donc nécessaire de mettre en place deux switch (switch2, switch3 cf figure 8 . 03).

L'un des deux switch sera placé dans le centre info (switch2) tel que l'autre dans le Département Batîment et Travaux Public (BTP)(switch3).



distance [ab] = 55m

distance [bc] = 50m

distance [cS] = 45m

Figure 8 . 02 : Plan de liaison entre le Département Télécommunication et la salle S

Lors de l'étude, le Département Télécommunication possède déjà deux switch que nous allons les utiliser:

- Switch D-Link DES-1008D, Ethernet / Fast Ethernet, 10 / 100Mbps, 8 ports
- Switch Cnet CNSH-800, Ethernet / Fast Ethernet, 10 / 100Mbps, 8 ports

Le switch4 est le switch vu dans 4 . 5, le switch1 appartient à l'Ecole mais un port est à notre disponibilité.

Du point d'accès Internet (routeur) vers le réseau local, quatre switch sont donc mis en œuvre. Pas de soucis, la règle de 5-4-3 est encore respectée : « sur le réseau Ethernet, lorsqu'on prolonge des segments (cf 1. 3 . 5) LAN, on peut connecter 5 segments de réseau de bout en bout à l'aide de 4 répéteurs (switch), mais seuls 3 des segments peuvent comporter des hôtes ». Pour notre cas, les switch1 et switch4 comportent des hôtes.

En ce qui concerne la mise en place du câble FTP CAT5, le chemin aérien n'est pas une bonne idée. En effet, les problèmes de vent et de pluie (mobilité et usure rapide du câble) diminue la durée de vie d'un câble, perturbe la transmission du signal. La sécurité n'est pas garantie (vol). Nous allons donc faire un câblage sous terrain (à 50cm) en utilisation des gaines de protection de

câble contre l'humidité. De plus, le chemin direct entre [aa'] (cf figure 8 . 02) n'est pas conseillé. Lors de l'étude, cette partie est libre mais une réhabilitation du milieu (plantation d'arbres, construction du jardin …) peut être envisagée d'ici quelques années. Cela nécessite le changement de notre plan de câblage (à éviter).

En arrivant sur le point 'a', le câble entre sur le coin de la salle TP (Travaux Pratiques), traverse le mur de cette dernière équipé de goulotte jusqu'à la prise murale RJ45 située à côté de la machine Linux dans la salle des professeurs (cf Annexe 1).

8 . 1 . 4 . Schéma bloc de la liaison entre DTS et le réseau du Département Télécommunication

Le schéma bloc de liaison entre notre Fournisseur d'Accès Internet et la machine serveur Linux est décrit ci-dessous :

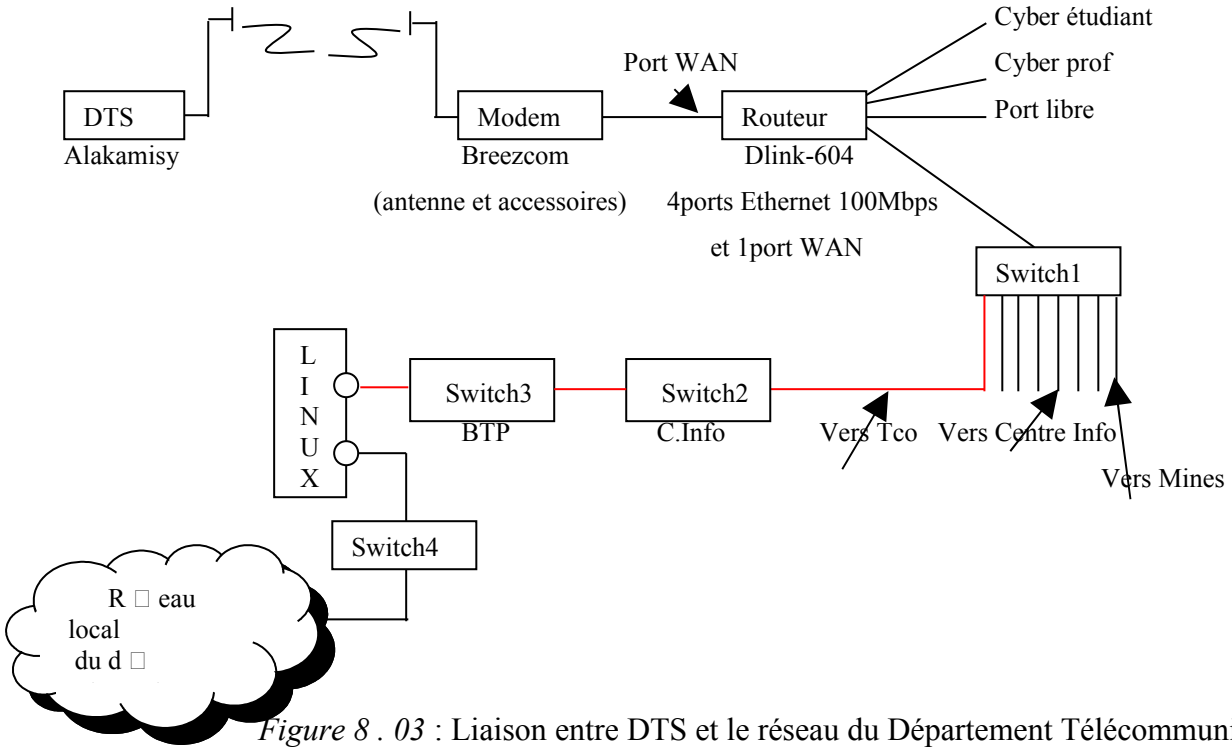


Figure 8 . 03 : Liaison entre DTS et le réseau du Département Télécommunication

8 . 1 . 5 . Les équipements à mettre en œuvre

- câble FTP CAT5 et gaine pour la protection du câble de longueur 150m pour la liaison [aS] (cf figure 8 . 02)
- 4 switch, déjà à notre disposition

- câble FTP CAT5 et goulotte de longueur 30m pour la liaison du point ‘a’ au prise RJ45F ([ad], cf Annexe 1).
- connecteurs RJ45 : 7
- prise murale RJ45 : 1

8 . 1 . 6 . Evaluation des coûts des matériels

Dans un tel projet, une évaluation de coûts est nécessaire :

Désignation	Prix unitaire (Ariary)	Quantité	Montant (Ariary)
Câble FTP CAT5	700	180m	126 000
Goulotte	10 868	30m	326 040
Gaine (tube orange)	2 000	150m	300 000
Connecteurs RJ45	500	7	3 500
Prise murale RJ45	27 690	1	27 690
TOTAL			**783 230**

Tableau 8 . 01 : Evaluation des coûts de matériels 2

Le montant des équipements s’élève à **783 230Ariary** ou **3 916 150Fmg**

Remarque :

Dans cette évaluation, les prix des deux switch (switch2 et switch3) ne sont pas inclus car ils sont déjà à notre disposition (cf 8 . 1 . 3).

Mais si on les évalue, le montant total augmente de 90 000 x 2 = 180 000Ariary, donc :

TOTAL = 783 230 + 180 000

TOTAL = 963 230Ariary ou **4 816 150Fmg**

L’accès Internet est maintenant sur la machine serveur Linux. Mais comment elle distribue cette connexion aux autres machines du réseau local ?

8 . 2 . Configuration de passerelle sous Linux [17]

8 . 2 . 1 . Mise en place de la passerelle

La machine serveur Linux, fonctionnant sous la distribution Fedora Core 4, est connectée au réseau local du Département Télécommunication via la carte réseau eth1 (Fast Ethernet PCI Realtek RTL 8139 Family, intégrée). L’adresse de cette interface est de 172.16.17.1 (cf 5 . 5 . 3 .

2). Les adresses des machines connectées au serveur par l'intermédiaire de switch4 sont de types 172.16.17.X (X varie de 2 à 14).

L'autre interface eth0 (Fast Ethernet PCI Realtek RTL 8139 Family) est connectée à l'Internet, son adresse est de 192.168.1.40.

La machine Linux est donc à la fois serveur et passerelle (cf figure 8 . 03) : les ordinateurs du réseau local du Département accèdent à Internet grâce au serveur / passerelle Linux.

8 . 2 . 2 . Partage de la connexion Internet

Nous allons utiliser « iptables », service déjà inclus dans le noyau 2.6.11 de la distribution Fedora Core 4, pour le partage de connexion.

Les étapes citées ci-dessous sont nécessaires pour que les ordinateurs du réseau local peuvent accéder à Internet via la machine Linux :

→ il faut que la redirection des paquets d'information est possible (liaison entre les deux interfaces eth1 et eth0). Pour cela, le fichier /proc/sys/net/ipv4/ip_forward contient le chiffre '1' et non '0' qui le désactive. Dans un terminal, exécutons la commande suivante (en tant que root):

 # echo 1> /proc/sys/net/ipv4/ip_forward

→ pour que cette modification soit activée à chaque redémarrage de la machine, nous allons renseigner le fichier /etc/sysctl.conf :

éditer le fichier /etc/sysctl.conf, il faut que *net.ipv4.ip_forward = 1*

→ il faut que la passerelle dirige aussi les paquets de l'extérieur vers le réseau local. Pour cela, exécutons la commande suivante dans un terminal (en tant que root):

 # iptables –A POSTROUTING –t nat –o eth0 –j MASQUERADE

Explication :

-A	ajout de la règle 'iptables' à la fin d'une chaîne donnée
POSTROUTING	cette chaîne modifie les paquets avant qu'ils ne soient envoyés (paquet du réseau local → paquet destiné à l'extérieur)
-t	spécifie un nom de table
nat	Network Address Translation, table utilisée pour la traduction d'adresse réseau
-o	spécifie l'interface de sortie des paquets
eth0	interface connectée à Internet

-j passe directement au cible spécifiée lorsqu'un paquetage correspond à une règle particulière

MASQUERADE ce cible permet aux ordinateurs internes connectés à la machine Linux d'accéder à Internet

→ il faut maintenant sauvegarder la configuration obtenue :

 # service iptables save

Ceci renseigne le fichier /etc/sysconfig/iptables des règles d'iptables configurées ci-dessus.

→ pour que, à chaque démarrage de la machine, les ordinateurs internes peuvent accéder à Internet, il faut revoir le fichier de configuration des scripts de contrôle d'iptables /etc/sysconfig/iptables-config et affecter les valeurs :

IPTABLES_SAVE_ON_STOP = YES

IPTABLES_SAVE_ON_RESTART = YES

Note: Il faut enlever le « # » devant chaque directive si on veut l'activer.

8 . 2 . 3 . Test de fonctionnement

Pour tester le bon fonctionnement du partage, il suffit - depuis un client (Windows ou Linux) - de lancer une URL à partir d'un navigateur (Internet Explorer, Mozilla, …) ou exécuter la commande : 'ping www.google.fr' dans une fenêtre d'invite de commande (client Windows) ou dans un terminal (client Linux).

Le test réalisé lors de notre étude est fourni en Annexe 4.

8 . 3 . Configuration de pare-feu (firewall) sous Linux [20] [21]

Le protocole TCP / IP (cf 1 . 7) est le protocole de base d'Internet assurant la transmission de données mais ne garantit pas la sécurité dans le réseau. La mise en place d'un pare-feu est donc nécessaire pour empêcher les intrusions dans le réseau.

Le noyau 2.6.11 de Fedora Core 4 met à disposition l'outil permettant le filtrage des paquets réseau : le 'netfilter'.

8 . 3 . 1 . Principes de base

Le processus consiste à contrôler les paquets réseaux lorsqu'ils entrent, traversent et sortent de la pile réseau (cf 1 . 7) au sein du noyau.

Le 'netfilter' du noyau contient trois tables de règles intégrées :

- la table « filter » : cette table contient les règles qui permettront de filtrer les paquets. Elle va contenir trois chaînes (ensembles de règles permettant d'identifier les paquets correspondant à certains critères) : la chaîne INPUT qui s'applique aux paquets ciblés pour l'hôte, la chaîne OUTPUT qui s'applique aux paquets réseaux générés localement, la chaîne FORWARD qui s'applique aux paquets routés à travers l'hôte.
- la table « nat » (Network Address Translation) : cette table est utilisée pour modifier les paquets qui créent une nouvelle connexion et pour la traduction d'adresses réseaux. La chaîne PREROUTING modifie les paquets lorsqu'il arrive. La chaîne OUTPUT modifie les paquets réseaux générés localement. La chaîne POSTROUTING modifie les paquets avant qu'ils ne soient envoyés.
- la table « mangle » : cette table est utilisée pour la modification de type spécifique de paquets comme le marquage de paquets associés aux fonctions de Q_OS (cf 1. 4 . 4). Les chaînes intégrées pour cette table sont : INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING.

Chaque paquet réseau reçu ou envoyé par un système Linux est soumis à au moins une de ces règles. La règle à spécifier dans un système est exécuté en mode console (dans un terminal) par le root (superutilisateur). C'est la commande « iptables » qui permet d'accéder au Netfilter donc de définir la ou les règles à appliquer.

8 . 3 . 2 . Création des règles de filtrage

La structure générale de la commande 'iptables' a la forme : iptables [options]. Les options sont à remplacer par les expressions convenables.

Nous décrivons ici les étapes à suivre pour la configuration de notre pare-feu.

On va demander à iptables de :

→ interdire l'accès depuis l'extérieur :

```
# iptables –A INPUT –i eth0 –j DROP
```

→ autoriser accès FTP (avec précaution prises cf 5 . 7 . 3):

```
# iptables –I INPUT –p tcp --dport 20 –j ACCEPT
```

→ autoriser accès Web (lecture car upload interdit, cf 5. 7 . 3):

```
# iptables –I INPUT –p tcp --dport 80 –j ACCEPT
```

→ interdire l'accès Internet des postes locaux sauf pour un (ou des) client(s) spécifié(s):

```
# iptables –A POSTROUTING –t nat –s 172.16.17.3 –o eth0 –j MASQUERADE
```

→ enregistrement de ces règles :

 # /sbin/service iptables save

→ redémarrage du service iptables

 # /sbin/service iptables restart

Explication des options utilisées :

→ Options de commande :

-A	ajout de la règle 'iptables' à la fin d'une chaîne donnée
-I	insère une règle à l'intérieur d'une chaîne à un point précis

→ Options de paramètre d'iptables :

-i	règle l'interface réseau entrante (si aucune interface n'est spécifiée, toutes les interfaces sont affectées par la règle)
-p	paramètre le protocole IP pour la règle
-j	passe directement à la cible spécifiée lorsqu'un paquetage correspond à une règle particulière
-t	spécifie un nom de table
nat	Network Address Translation, table utilisée pour la traduction d'adresse réseau
-o	spécifie l'interface de sortie des paquets
eth0	interface connectée à Internet
-s	définit l'origine d'un paquet
- -dport	paramètre le port de destination pour le paquet

→ Les cibles :

DROP	le paquet est abandonné et se voit refuser l'accès au système
ACCEPT	le paquet est autorisé à passer
MASQUERADE	cette cible permet aux ordinateurs internes connectés à la machine Linux d'accéder à Internet

Le partage et la sécurisation via Internet sont ainsi faits par la commande « iptables » exécutant sur un terminal en positionnant en tant que root.

CONCLUSION

Nous avons pu fournir dans ce travail de mémoire des informations se rapportant sur: le réseau local, l'installation du réseau client – serveur dans le Département Télécommunication et l'ouverture de ce dernier à Internet.

Ainsi, l'étude est faite tant du côté 'matériel' (disponibilité, achat et coût) que 'logiciel'.

La disponibilité 'matériel', l'achat à effectuer et son coût, ainsi que l'étude de faisabilité sont des critères à ne pas oublier dans un tel projet. Un bon Ingénieur est un bon Manager.

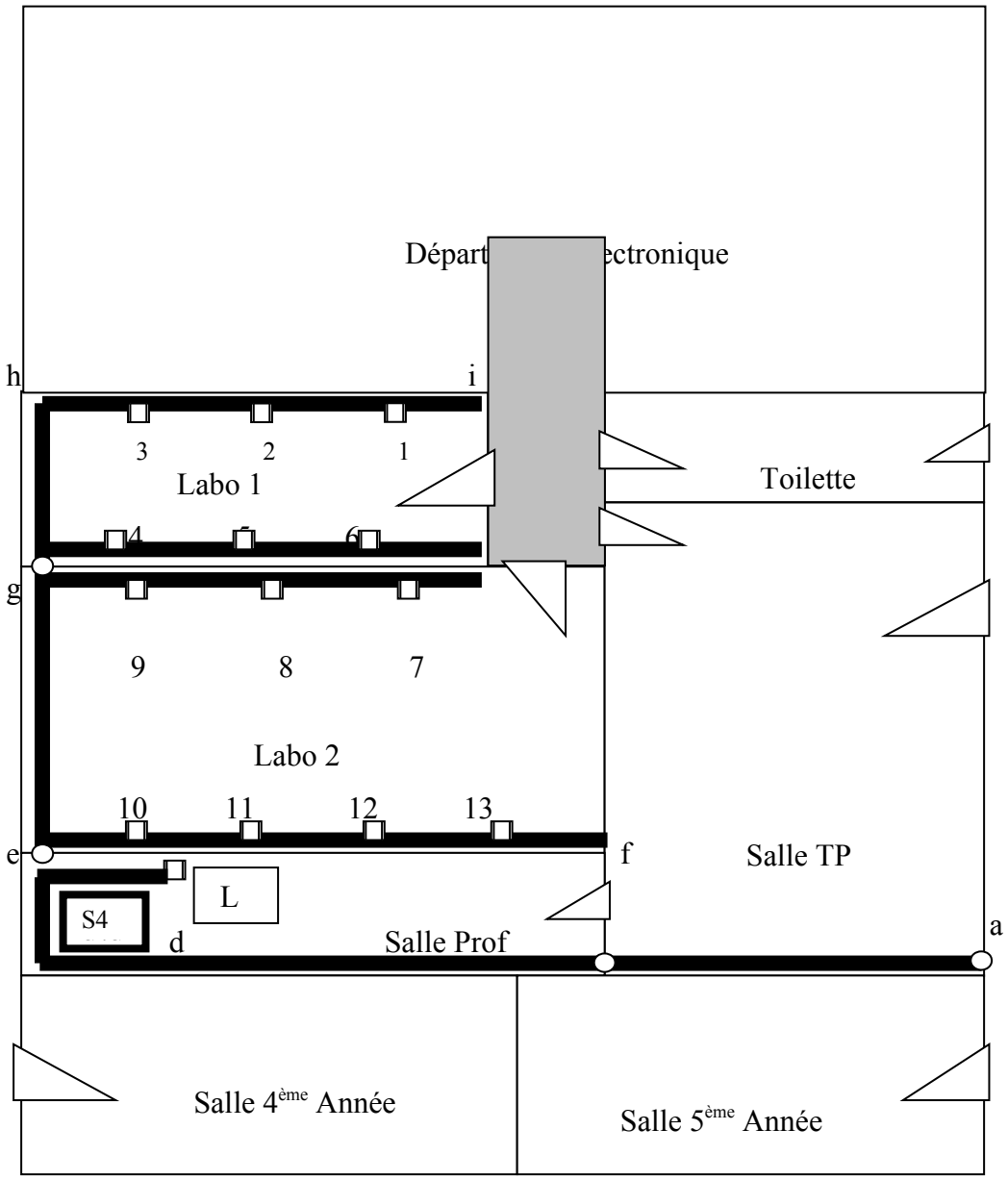
En outre, le système d'exploitation Linux incluant les logiciels serveurs utiles dans le réseau a été choisi pour le serveur.

Par conséquent, la mise en place des serveurs DNS, Samba, FTP et Web a été étudiée pour que le partage de disque, le transfert de fichiers et la consultation des sites peuvent avoir lieu sans obliger de taper l'adresse IP difficile à tenir.

En plus, les étudiants ne seront plus obligés de chercher d'autres endroits pour consulter des documents sur le net, le Département leur donne l'opportunité.

Bref, l'installation d'un réseau client – serveur au sein du Département Télécommunication et son ouverture à Internet s'avère utile.

ANNEXE 1 : PLAN DE CABLAGE



Légende :

Câble équipé de goulotte	Mur à percer
Prise murale RJ45	Porte
S4 — Switch4 (cf chapitre 8 : figure 8 . 03)	
L — Machine serveur / passerelle Linux	

Calculs et mesures :

[ad] = 30m

[ef] = 13m

[eg] = 7m

[gh] = 5m

[hi] = 10m

goulotte nécessaire:

[ad] = 30m

[fi] = (2*[fe]) + [eg] + [hg] + (2*[hi]) = 26 + 7 + 5 + 20 = 58m

câble nécessaire:

→ 1: 7 + 5 + 10 = 22

2: 7 + 5 + 7 = 19

3: 7 + 5 + 4 = 16

4: 7 + 4 = 11

5: 7 + 7 = 14

6: 7 + 10 = 17

7: 7 + 10 = 17

8: 7 + 7 = 14

9: 7 + 4 = 11

10: 4

11: 7

12 9

13: 12

Total1 = 173m

→ Cordon de brassage (liaison entre RJ45F et ordinateur, RJ45F et switch4 pour le serveur)

Total2 = 1,50 * 14 = 21m

→ Total = total1 + total2 = 194m

ANNEXE 2 : QUELQUES COMMANDES DE BASE SOUS LINUX

Manipulations des répertoires

cd — change directory
permet de changer de répertoire de travail

find — recherche un fichier à partir d'un répertoire donné

mkdir — make directory
créer un nouveau répertoire

pwd — print working directory
affiche le chemin d'accès du répertoire courant

rmdir — remove directory
supprime un répertoire s'il est vide

Manipulations des fichiers

cat — concatenate
permet d'afficher, de créer, de copier et de concaténer des fichiers

cp — copy
permet la copie de fichiers

echo
affiche à l'écran le texte qui suit la commande echo

grep
recherche, dans un ou plusieurs fichiers, de toutes les lignes contenant une chaîne donnée de caractères

ls list files

permet d'obtenir la liste et les caractéristiques des fichiers contenus dans un répertoire

man ou info

permet de rechercher des informations sur les commandes

mv move

change le nom d'un fichier ou d'un répertoire

rm remove

supprime un ou plusieurs fichiers d'un répertoires

touch

permet de créer un fichier vide

ANNEXE 3 : LES PRINCIPAUX REPERTOIRES SOUS LINUX

Sous Linux, on peut classer les répertoires en deux catégories :

- Les répertoires standards :

/ répertoire contenant tous les répertoires

/ home répertoire contenant les répertoires personnels de tous les utilisateurs autres que root

/ root répertoire personnel de l'administrateur système (root ou superutilisateur)

- Les répertoires systèmes :

/ bin répertoire contenant les commandes et utilitaires employés par tous les utilisateurs

/ boot répertoire contenant des informations permettant le chargement de Linux

/ dev répertoire contenant tous les fichiers périphériques permettant d'accéder aux composants matériels

/ etc répertoire contenant les commandes et fichiers de paramétrages nécessaires à l'administration système

/ lib répertoire contenant les bibliothèques communes à tous les utilisateurs

/ proc répertoire spécial utilisé par le système et contenant la liste des processus en cours d'exécution

/ sbin répertoire contenant les commandes et utilitaires utilisées seulement par l'administrateur système

/ tmp répertoire contenant les fichiers temporaires

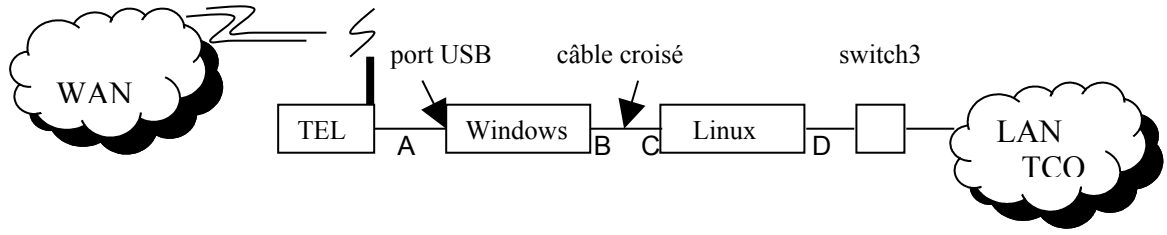
/ usr répertoire composé d'un certain nombre de sous répertoires utilisés par l'ensemble des utilisateurs

/ var répertoire spécial utilisé par le système pour stocker des données souvent modifiées

ANNEXE 4 : TEST DE PARTAGE INTERNET

Nous allons décrire ici le test de fonctionnement du partage Internet dans le réseau du Département Télécommunication.

Schéma de la réalisation de test:



TEL : téléphone utilisé pour accéder à Internet

A : adresse public du téléphone 196.192.45.X1 où X1 varie à chaque connexion

B : adresse privée du téléphone (connecté vers le réseau local) donc adresse de la machine Windows : 192.168.0.1.

C : adresse de l'interface de la machine Linux connectée à Internet eth0. Nous avons modifier cette adresse pendant notre test pour être compatible à l'adresse de la machine Windows. En effet, les 2 machines Windows et Linux appartient ici à un même sous-réseau. C = 192.168.0.2.

D : adresse de l'interface de la machine Linux connectée au réseau local eth1.

D = 172.16.17.1.

Note : Nous utilisons une machine fonctionnant sous Windows car le pilote du téléphone (pack TELMA) utilisé ne connaît pas Linux.

Test : Le test de fonctionnement est effectué sur les postes clients appartenant au réseau local du Département (LAN TCO) :

- client Windows : sur la fenêtre d'invite de commande exécutons la commande 'ping' pour chaque adresse (D, C, B, A) et pour www.wanadoo.mg ou www.google.fr . La réponse est positive (paquets perdus=0). Puis sur le champ d'adresse URL du navigateur lancer www.google.fr , sur la fenêtre apparaît la page d'accueil de google.

- client Linux : même démarche que précédemment mais la commande est à exécuter dans un terminal.

BIBLIOGRAPHIE

[1] P. A. GOUPILLE, *Technologie des ordinateurs et des réseaux,* Dunod : 6ème édition, 2000.

[2] S. COULIBALY, P. FONTAINE, F. HOUSTE et P. E. MULLER, *Montez votre serveur de A à Z,* 1ère édition, Novembre 2003.

[3] L. E. RANDRIARIJAONA, *Réseaux,* Cours et Travaux Pratiques 4ème année, Dép. Tél. – E.S.P.A., A.U. : 2003 – 2004.

[4] A. RATSIMBAZAFY, *Téléinformatique et Télématique*, Cours 4ème année, Dép. Tél. – E.S.P.A., A.U. : 2003 – 2004.

[5] C. RATSIHOARANA, *Composants photoniques et Fibres optiques*, Cours 5ème année, Dép. Tél. – E.S.P.A., A.U. : 2004 – 2005.

[6] http://wimax.free.fr

[7] B. BRULLER, *Les réseaux locaux informatiques,* Puf : 1ère édition, Octobre 1998.

[8] G. PUJOLLE, *Les réseaux,* Edition 2003.

[9] *Guide de précâblage Voix – Données –Images,* Infra +, Edition 2001.

[10] J. P. ARMSPACH, P. COLIN et F. O. WAERZEGGERS, *Linux – Initiation et utilisation,* Dunod : 2ème édition, 2004.

[11] http://www.africacomputing.org

[12] P. LOGEROT, *Linux ou Windows – Guide d'aide à la décision,* Dunod : Paris, 2003.

[13] http://www.fr.redhat.com

[14] http://www.zdnet.fr/actualites/informatiques

[15] http://www.commentcamarche.net

[16] http://www.funix.org/fr/linux/dns.htm

[17] http://lea-linux.org/cached/index

[18] http://www.africacomputing.com

[19] http://www.ca/mille

[20] http://www.polytechnique.fr

[21] http://web.mit.edu/rhel-doc

[22] http://www.mat-info.univ-paris5.fr/cdc/sr-httpd.html

[23] L. RABEHERIMANANA, *Base de données et systèmes d'information,* Cours 5ème année, Dép. Tél. – E.S.P.A., A.U. :2004 – 2005.

[24] H. RANDRIANARIVONY, *Technologie de l'Information et de la communication,* Cours 4ème année, Dép. Tél. – E.S.P.A., A.U. :2004 – 2005.

FICHE DE RENSEIGNEMENTS

Nom : **RAMAMONJISOA**
Prénoms : **Falihanta Domoina**
Adresse de l'auteur : IMMEUBLE M.A.MA Ambalavao Isotry

Titre : « **ETUDE ET INSTALLATION DU RESEAU CLIENT SERVEUR AU SEIN DU DEPARTEMENT TELECOMMUNICATION** »

Pagination : **99**
Tableaux : **5**
Figures : **31**

Mots clés : **Réseau, client, serveur, DNS, Linux, Internet**

Directeur de mémoire : **Monsieur RATSIMBAZAFY Andriamanga**

RESUME

Le Département Télécommunication de l'Ecole Supérieure Polytechnique d'Antananarivo possède maintenant son réseau informatique de type client - serveur.

En plus, le serveur fonctionne sous un système d'exploitation Fedora Core 4 de Linux, qui contient déjà presque tous les logiciels serveurs nécessaires pour son architecture.

En outre, l'ouverture du réseau à Internet met à la disposition des enseignants et des étudiants les documents nécessaires pour enrichir leurs connaissances sans chercher ailleurs.

SUMMARY

Nowadays, the Department of Telecommunication in the Polytechnic High School of Antananarivo has his own informatic Network, kind of customer - waiter.

And, the waiter is working under the operating system Fedora Core 4 of Linux, with the software of waiter that are really important for her architecture.

Morcover, opening this Network to Internet helps teachers and students in order to keep information to enrich and to develop their knowledge in stead of to look for everywhere else.