

Institut Supérieur des Etudes Technologiques en Communications de Tunis

Projet de fin d'études

**CONCEPTION ET REALISATION D'UN SYSTEME DE
GESTION DES DONNEES DE
TAXATION A BASE DE PROTOCOLE FTAM**

Réalisé par :

Sana ELMESTIRI
&
Zakia ESSID
TS5-Télécommunications

Encadré par :

M.Mondher ELLOUZE
&
M.Mohamed HMAOUI

2001-2002

Dédicace

À mes très chère parents.

À mes frères et mes sœurs.

À toute ma famille.

À ma binôme.

À mes amis(es).

À tous ceux que j'aime.

Je dédie ce travail

Sana... 

REMERCIEMENTS

Avant d'entamer ce rapport de fin d'étude, nous tenons à exprimer notre sincère gratitude envers tous ceux qui nous ont aidés ou ont participé au bon déroulement de ce projet.

Nous sommes particulièrement reconnaissantes à nos encadreurs Messieurs Mondher ELLOUZE et Mohamed HMAOUI pour leur générosité, leur compréhension et leurs aides inestimables.

Nos vifs remerciements s'adressent aussi à tous nos enseignants de l'ISSET-COM pour la formation qu'ils ont eu le soin de nous apporter le long de notre cursus universitaire et surtout à Mr Kamel BOULEIMEN pour ses aides et ses précieux conseils.

Sana & Zakia

TABLE DES MATIERES

INTRODUCTION GENERALE.....	1
ETUDE ET EVALUATION DU SYSTEME EXISTANT.....	3
1.1 Introduction.....	3
1.2 Généralités sur le réseau de commutation en Tunisie.....	3
1.3 La taxation.....	4
1.4 La facturation.....	4
1.4.1 Présentation de la facturation téléphonique.....	4
1.4.2 Organisation du centre de la facturation la Kasbah.....	4
1.5 Etude de la situation actuelle.....	5
1.5.1 Cas des centraux E10 et DMS.....	5
1.5.2 Cas des centraux EWSD et AXE.....	8
1.5.3 Insuffisances du système actuel de collecte de données de taxation.....	9
1.6 Définition des besoins du centre de facturation.....	9
1.7 Conclusion.....	10
SYSTEME DE COLLECTE A BASE DU PROTOCOLE FTAM.....	11
2.1 Introduction.....	11
2.2 Présentation générale.....	11
2.3 Les services et les primitives FTAM.....	13
2.4 Exemple d'utilisation de FTAM.....	17
2.5 Avantage du protocole FTAM par rapport au protocole FTP.....	19
2.6 Conception du système FTAM.....	20
2.6.1 Solution moyen terme.....	20
2.6.2 Solution long terme.....	21
SOLUTION DE COLLECTE A BASE DE PROTOCOLE FTP.....	22
3.1 Introduction.....	22
3.2 Composants fonctionnels du système de collecte automatique.....	23
3.3 Présentation du protocole TCP/IP.....	23
3.4 Présentation du protocole FTP.....	26
3.5 Administration et maintenance du système.....	28

3.5.1 Architecture d'administration des réseaux.....	28
3.5.2 Un exemple de modèle d'architecture de réseaux.....	29
3.5.3 Protocole SNMP.....	29
3.5.3.1 Définition.....	29
3.5.3.2 Environnement de gestion SNMP.....	30
3.5.3.3 Fonctionnement du protocole SNMP.....	31
3.5.4 Télémaintenance.....	32
3.6 Etude de sécurisation du système de collecte automatique.....	33
3.6.1 Introduction.....	33
3.6.2 Sécurisation de FTP par la couche SSL.....	34
3.7 Sécurisation du réseau.....	35
IMPLEMENTATION DE LA PLATEFORME TCP/IP.....	36
4.1 Introduction.....	36
4.2 Architecture du système de collecte automatique.....	37
4.3 Conception et réalisation d'une application du transfert automatique.....	39
4.3.1 Environnement de développement.....	39
4.3.2 Objectifs.....	40
4.3.3 Architecture générale de l'application.....	40
4.3.4 Algorithme Client FTP.....	41
4.3.5 Interface graphique de l'application.....	42
4.3.6 Installation et paramétrage du serveur FTP(WS_FTP Server).....	42
4.3.7 Installation et paramétrage du PC-ANYWHERE.....	46
4.3.8 Installation et paramétrage de Tiny Personal Firewall.....	48
4.4 Conclusion.....	51
CONCLUSION ET PERSPECTIVES.....	52
BIBLIOGRAPHIE.....	54
GLOSSAIRE.....	55

CAHIER DES CHARGES

Actuellement, au niveau du centre de la facturation de TUNISIE TELECOM: les données de taxation: comptes de taxe et CDR (Call Detail Record) sont collectés mensuellement à partir des différents systèmes de commutation qui composent le parc du réseau téléphonique de TUNISIE TELECOM par le biais d'une plate-forme utilisant le transfert de fichier sur le RTCP (solution FTP).

Afin d'améliorer ce système, on désire concevoir et réaliser un système de gestion des données de taxation qui assure essentiellement la collecte et le transfert des dites données au centre de la facturation via le réseau transmission de données X25 et ce, en utilisant un protocole de transfert plus fiable et performant à l'instar du protocole FTAM (FILE TRANSFERT ACCESS AND MANAGEMENT).

Etant donné l'importance de la qualité de service rendue à la clientèle de TUNISIE TELECOM en matière de la facturation, le système de gestion proposé doit prévoir une étude sur les outils nécessaires pour l'Administration et la Sécurité de tout le système d'information et ce, en se référant aux standards et normes existants.

INTRODUCTION GENERALE

L'innovation, l'environnement concurrentiel et une clientèle de plus en plus exigeante poussent les opérateurs des télécommunications, fondement de la société d'information, à fournir à ses clients de nouveaux services et prestations dont les performances et la convivialité ne cessent d'évoluer.

Un grand nombre, pour ne pas dire la quasi-totalité des opérateurs Télécoms, soucieux de faire bénéficier leurs clientèles des avantages de nouvelles technologies, ont décidé de prendre les dispositions nécessaires pour promouvoir leurs services et surtout garantir un certain niveau de qualité des dites services dans tous les azimuts à savoir particulièrement sur les plans techniques et commerciaux.

Au fait, la question incontournable à la quelle les opérateurs des télécommunications doivent répondre pour justifier les investissements de masse dans le monde des télécommunications est claire : *Ces investissements créent-elles des valeurs ajoutées, sous formes de services et prestations exigés pour leurs clients ?*

L'Office National des Télécommunications : TUNISIE TELECOM ne cesse de connaître ces dernières années des changements radicaux qui visent les mêmes orientations sus indiqué à savoir offrir une panoplie de services avec une meilleure qualité et ce, à l'instar de tous les opérateurs mondiaux et selon les normes en vigueur.

Parmi les prestations qui reflètent l'image de marque de TUNISIE TELECOM et qu'on peut la citer comme la première notion pour juger les prestations d'un opérateur et servir comme référence pour évaluer la satisfaction est la facturation téléphonique.

De ce fait, et étant donnée l'importance de la facturation téléphonique, pour TUNISIE TELECOM, et ayant comme objectif de promouvoir cette prestation, notre travail au titre du présent projet sera consacré à étudier le système de facturation utilisé actuellement par TUNISIE

TELECOM dans un but de trouver les solutions optimales qui s'adaptent aux spécificités de cet opérateur et répond à ses besoins de court et long termes.

Plan du mémoire

Notre travail, effectué au sein de TUNISIE TELECOM dans le cadre du projet de fin d'études, présenté dans ce présent mémoire, est décrit dans quatre chapitres dont nous donnons une succincte présentation du contenu de chaque chapitre..

Le premier chapitre, intitulé « Etude et évaluation du système existant », présente notre évaluation du système de la facturation actuellement en exploitation par TUNISIE TELECOM.

L'étude du protocole FTAM ainsi qu'une présentation de notre approche pour le déploiement à moyen et long terme de systèmes de collecte qui solutionnent les problématiques de la facturation est l'objet du chapitre 2.

Une solution à court terme est également explicitée au cours du troisième chapitre. Cette solution s'articule autour d'un protocole de transfert très répandu connu par sa simplicité : le protocole FTP sécurisé.

A travers le dernier chapitre, intitulé « Implémentation de la plate-forme TCP/IP », nous décrivons la partie programmation, interface graphique et outils de gestion utilisés dans l'application informatique qui concrétise notre solution à court terme.

Des perspectives et propositions de développements futures qui sembleraient être prometteuses sont données dans la conclusion de ce mémoire.

CHAPITRE 1

ETUDE ET EVALUATION DU SYSTEME EXISTANT

1.1 Introduction

Une étape essentielle de tout projet informatique ou autre consiste à effectuer une étude préalable. Cette étude consiste à examiner le système auquel on veut apporter des solutions afin de déceler les défaillances et les insuffisances auxquelles on doit remédier.

Ainsi, durant ce chapitre nous commençons par une étude et évaluation du système existant adopté par TUNISIE TELECOM pour traiter les données de taxation.

1.2 Généralités sur le réseau de commutation en Tunisie

Le commutateur est un élément essentiel du réseau de commutation. C'est lui qui réalise les fonctions de base de l'application téléphonique à savoir : le traitement des appels, l'acheminement du trafic et surtout la taxation des communications téléphoniques, etc....

Les types de commutateurs existants en Tunisie sont les suivants :

- ERICSSON : AXE, APZ212.20 et APZ 212.25.
- SIEMENS : EWSD, CP113 version 11.
- ALCATEL : OCB 181 palier 11, OCB 283 Palier R21E.
- NORTEL : DMS 100, BCS 43i, DMS 10, Generic 453. 50.

1.3 La taxation

La taxation des communications téléphoniques est effectuée au niveau des commutateurs. A chaque abonné correspond un nombre d'index (4 ou 5 selon le modèle du commutateur) stockés sur le commutateur. Par exemple, un index pour les communications locales, un autre pour les communications interurbaines, etc....

Lorsqu'une communication est établie (dès que l'appelé décroche), les index relatifs au type de cette communication sont incrémentés.

Le comptage se fait par impulsions, l'établissement de l'appel correspond à un nombre déterminé d'impulsions et, à chaque période de temps (durée selon le type de communication), le compteur est incrémenté. Le coût de l'impulsion ainsi que sa durée sont fixés par l'opérateur des télécommunications.

1.4 La facturation

1.4.1 Présentation de la facturation téléphonique

La facturation est la dernière étape par laquelle passent les index pour aboutir à une facture exhaustive prête à être livrée à l'abonné. En effet, la phase de facturation repose essentiellement sur la base de données alimentée par le processus de traitement des données de taxation.

En accédant à cette base de données, le processus de facturation récupère les index locaux, nationaux, internationaux et totaux pour calculer les montants respectifs. Ainsi, le total à payer est calculé en fonction de la consommation cumulée et des services alloués pour élaborer la facture.

1.4.2 Organisation du centre de la facturation la KASBAH

La direction des systèmes de facturation a pour mission :

- L'élaboration des règles d'exploitation et de gestion de facturation.

- La supervision de la qualité de facturation.
- L'élaboration des statistiques, du trafic, des produits et des recettes de télécommunications.
- La collecte, le traitement et le contrôle de toutes les données nécessaires à la facturation.
- L'exploitation et la maintenance des applications informatiques.
- L'administration des systèmes d'exploitation et du réseau de facturation.

1.5 Etude de la situation actuelle

Le processus de collecte de données de taxation est basé sur la création d'un fichier de type ASCII à partir des données de taxation sauvegardées dans les bandes ou disques de taxes. Ce fichier est stocké au niveau d'un micro-ordinateur installé dans chaque centre de communication (Nœud de collecte).

Le transfert de fichier de taxation à partir des différents nœuds de collecte vers le centre de facturation la kasbah (serveur) est considéré comme une transmission de données d'une source (centre de commutation) vers une destination (serveur) en utilisant soit le protocole FTP, soit le protocole FTAM.

1.5.1 Cas des centraux E 10 et DMS

Le réseau téléphonique commuté public est le support de transfert de fichiers de taxation.

La figure 1.1 donne une idée générale sur les éléments de base qui consistent la plateforme du système de collecte pour les centraux de type E10 et DMS.

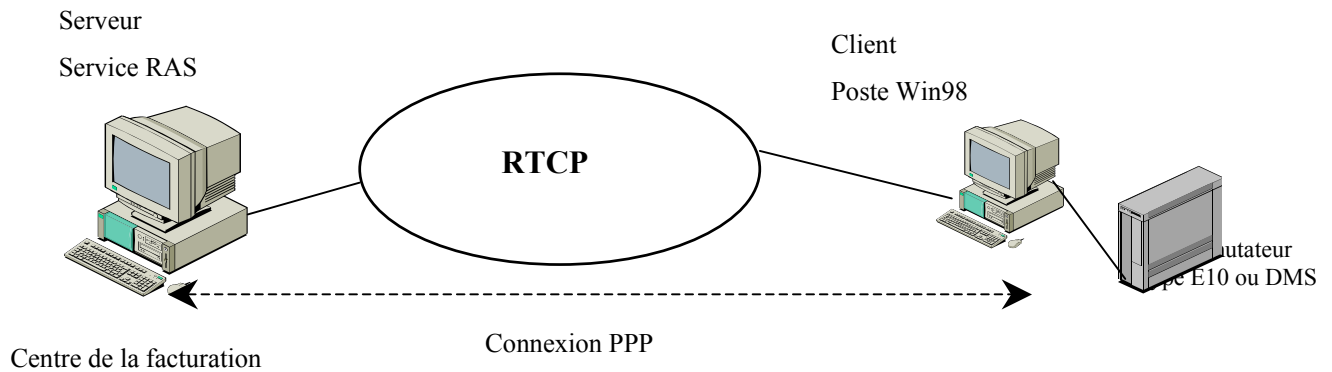


Fig 1.1 : Système de collecte : cas des centraux E10 et DMS

Chaque poste de travail est considéré comme un client distant qui doit établir une connexion avec un serveur (centre de la facturation).

- **Fonctionnalités de système:**

- ❖ Connexion au central de commutation.
- ❖ Extraction des fichiers de taxation (détail, compteur).
- ❖ Formatage des fichiers sources (détails, compteur).
- ❖ Chargement des fichiers (détail, compteur) dans la base des données de taxation.
- ❖ Exportation du fichier compteur détail de base de données en fichier ASCII.
- ❖ Transfert du fichier détail compteur au serveur de facturation via le RTCP.

- **Module de calcul du détail compteur:**

Ce module assure le calcul et la mise à jour des différents compteurs de chaque numéro d'appel (local, national, international,...) à partir des détails des communications de chaque numéro d'appel.

La table compteur contient uniquement la consommation globale de chaque numéro (compteur global), les autres compteurs : national (CN), international (CI) et local (CL) sont initialisés à 0 et seront calculés à partir des détails des communications de table détail en procédant aux étapes suivantes :

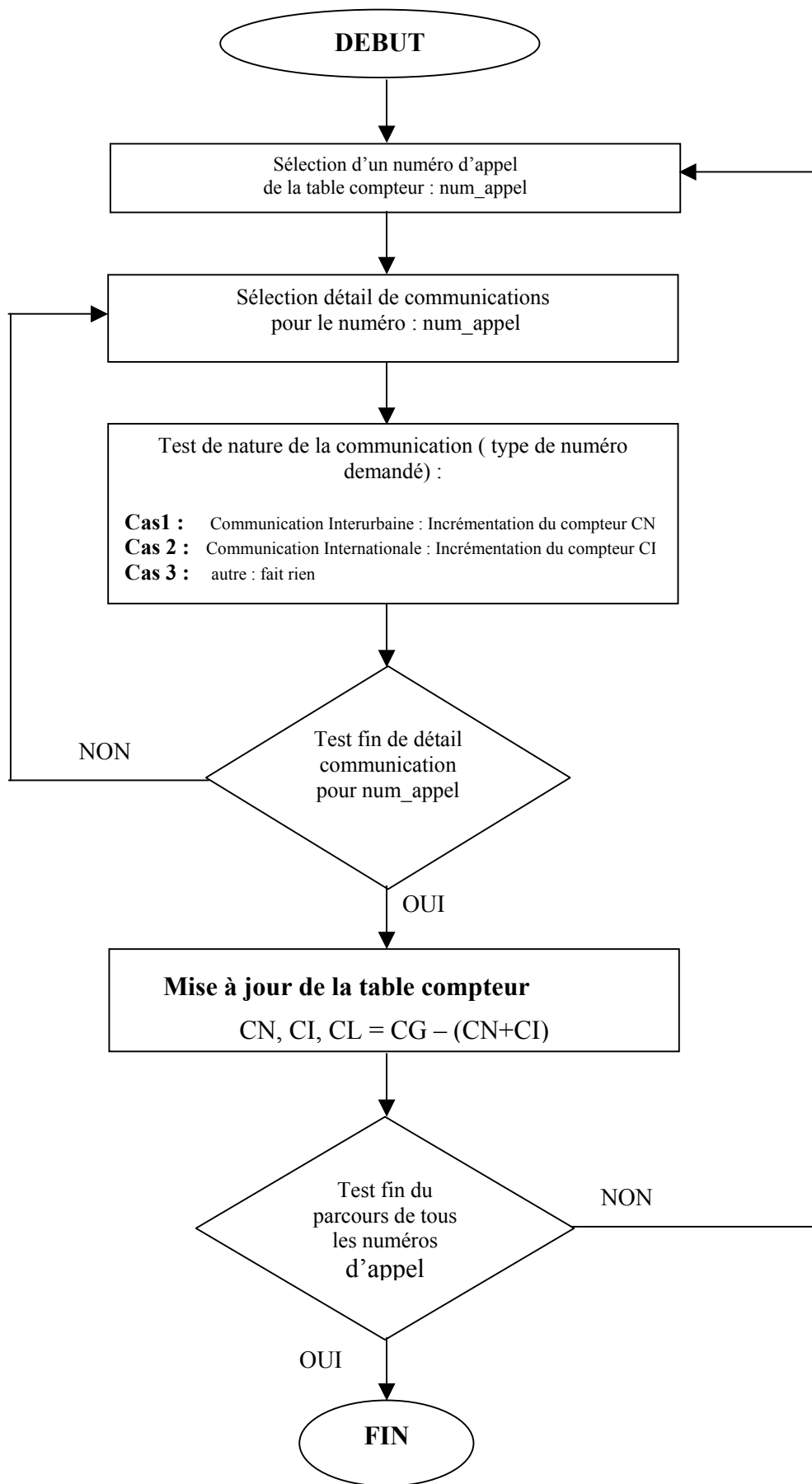


Fig 1.2 : Module calcul des compteurs (centraux E10)

1.5.2 Cas des centraux EWSD et AXE

Le réseau X25 est le support de transfert de fichier de taxation à partir des différents centres de commutation (EWSD ou AXE) vers le centre de facturation la kasbah (serveur).

La figure 1.3 illustre l'idée générale du processus de transfert des fichiers de taxation basé sur le protocole FTAM.

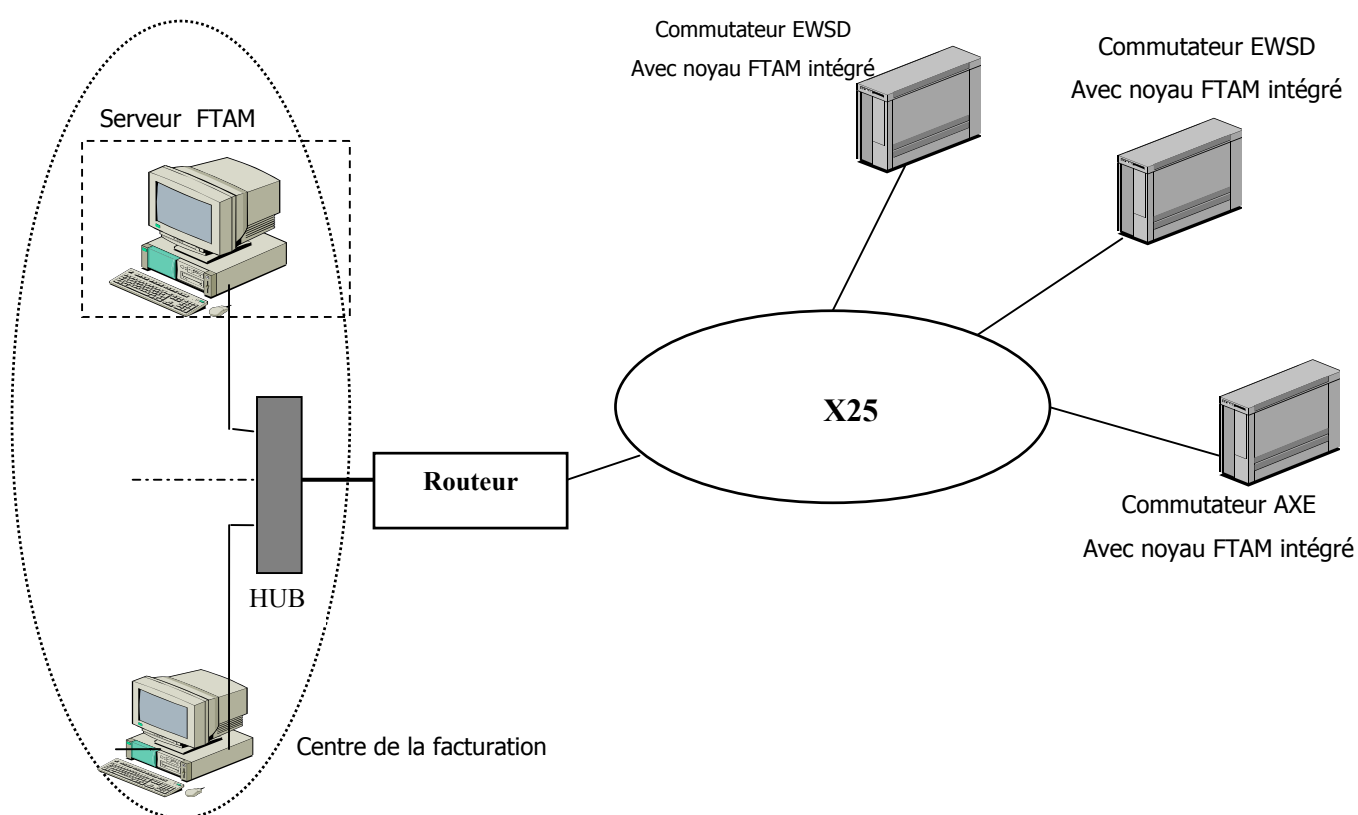


Fig 1.3 Système de collecte: cas EWSD et AXE

1.5.3 Insuffisances du système actuel de collecte des données de taxation

En évaluant les systèmes de collecte actuellement utilisés pour les centres de commutation E10 et DMS et le système d'informations de la facturation utilisé par TUNISIE TELECOM, on a remarqué que ce système présente plusieurs points de faiblesse parmi ces points on cite :

- Temps de transfert de fichiers très important à cause de transfert manuel des données de taxation.
- Absence de mécanisme de sécurité d'outil d'administration des applications.
- Accès facile et modification illégale de données car il suffit qu'on ait le mot de passe pour modifier et changer des informations importantes et confidentielles.
- Limitation de débit de système de transfert utilisé : d'une part la bande passante du RTC et d'autre part son rapport signal/Bruit (de l'ordre de 40 dB en moyenne) limitent la qualité du signal analogique transmis.
- etc.

1.6 Définitions des besoins du centre de la facturation

Cette étape est d'une importance primordiale. Elle consiste à réécrire de manière spécifique le cahier des charges.

Elle doit définir clairement les finalités du notre projet, et les contraintes restrictives aux quelles il est soumis.

Nous donnons un récapitulatif des besoins du centre de facturation :

- **Besoins relatifs aux orientations de collecte des données de taxation**

Les comptes de taxe ainsi que la facturation détaillée (CDR) doivent être collectés automatiquement c'est à dire sans intervention d'un agent.

- **Besoins relatifs aux gestions et administration du système d'information**

Pour maintenir notre système dans leur état fonctionnel et opérationnel, nous devons disposer d'informations de gestion qui décrivent leur comportement vis à vis des phénomènes agissent sur leur environnement.

- **Besoins relatifs à la sécurité des données**

Les données de taxation sont d'une importance capitale dans le bon déroulement du processus de facturation téléphonique.

Toute erreur, accidentelle ou intentionnée, peut provoquer des dégâts très importants.

En effet, une politique de sécurité s'avère nécessaire pour protéger le système contre les risques et les interventions externes.

1.7 Conclusion

Ayant décelé les différentes faiblesses et insuffisances dans ce système, notre travail consiste à apporter les améliorations suivantes :

- Accélérer le processus du transfert et de la collecte des indexes de taxation ;
- Automatiser les tâches de collecte ;
- Assurer une sécurité maximale lors du transfert des informations de taxation, l'intégrité et l'authenticité des fichiers transférés doivent être vérifiés;
- Mettre en place des outils d'administration et de gestion du système d'information;

CHAPITRE 2

SYSTEME DE COLLECTE A BASE DU PROTOCOLE FTAM

2.1 Introduction

Les services et protocoles FTAM sont définis respectivement par les normes ISO8571-3 et 8571-4.

Ces normes spécifient un élément de service de transport, accès et de gestion de fichiers qui peut être utilisé dans des environnements d'application très variés. L'application la plus simple consiste à créer une entité d'application entièrement dédiée au transfert, à l'accès et à la gestion de fichiers. La norme FTAM définit les services, sous la forme habituelle, par des primitives.

On détaillera dans la suite les services et le protocole FTAM (File Transfer, Access and Management).

2.2 Présentation générale

Le protocole FTAM se subdivise en un protocole de base (Basic FTAM Protocol) qui fournit le service interne et un protocole de reprise sur erreur qui fournit le service externe. Le protocole de base fait correspondre aux primitives de service des unités de données FTAM.

Le protocole de reprise sur erreur assure les fonctions suivantes :

- ❖ Gestion des informations de reprise sur erreur pendant le fonctionnement normal,
- ❖ Redémarrage du transfert de données après son interruption,
- ❖ Reprise après une terminaison anormale du régime d'ouverture ou de régime de sélection,
- ❖ Reprise après une terminaison qui provoque une destruction du régime de service interne.

Le protocole de reprise sur erreur est exécuté par l'automate FTAM de reprise sur erreur, FERPM qui est défini dans la norme par des tables d'état.

Le protocole de base est également spécifié par des tables d'état qui définissent le fonctionnement de l'automate FTAM de base, FPM. Le modèle est ici un peu plus complexe, car l'automate de base se subdivise en trois automates interconnectés, qui sont les suivants :

- ❖ Automate de gestion du régime FTAM,
- ❖ Automate de gestion du régime de fichiers,
- ❖ Automate de gestion du régime de transfert de données.

Les unités fonctionnelles du protocole sont définies de la même façon que pour le service, et chaque unité fonctionnelle du protocole doit être capable de fournir le jeu complet des services qui sont spécifiés pour cette unité fonctionnelle.

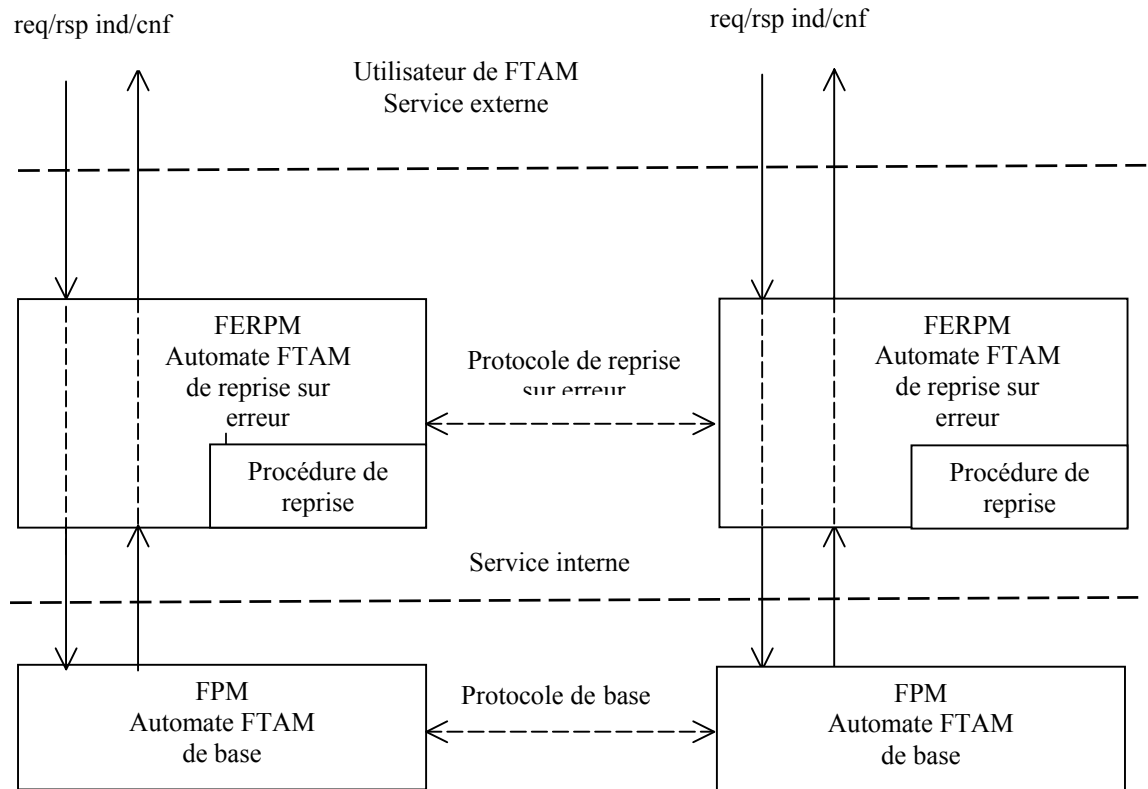


Fig 2.1 : Services et protocole FTAM

2.3. Les services et les primitives FTAM

Le protocole FTAM offre des services qui peuvent être utilisés lorsqu'un environnement de travail approprié, appelé régime, a été établi. Quatre régimes sont définis: la connexion, la sélection de fichier, l'accès aux fichiers et le transfert de données.

Le régime de connexion présente un environnement où la session de travail a débuté, le régime de sélection de fichiers a identifié ou crée un fichier unique sur lequel des opérations seront éventuellement faites. Dans le régime d'accès, le fichier a été ouvert et il est possible d'effectuer des opérations sur ses composantes. Finalement, le régime de transfert de données permet d'envoyer des données de l'initiateur au répondeur ou inversement.

Les services offerts par le protocole, et qui sont appelés à l'aide de primitives définies dans le FTAM, sont les suivants :

❖ Les services de connexion

Trois services de connexion sont offerts :

- Un service d'établissement d'association est utilisé par l'initiateur pour initier une session avec une entité répondeuse.
- Un service de terminaison d'association sert à l'initiateur pour mettre un terme à la session.
- Un service d'abandon est utilisé par l'une ou l'autre des entités pour interrompre brusquement et inconditionnellement à la session.

Ces services sont invoqués respectivement par les primitives F-Initilize, F-Terminate et F-Abort.

❖ Les services de sélection de fichier

Quatre services de sélection de fichier sont offerts à l'initiateur :

- Un service de sélection de fichier lui permet de désigner au répondeur le fichier sur lequel il veut travailler.
- Un service de désélection de fichier est utilisé pour libérer le dit fichier.
- Un autre service permet de créer un fichier et de le sélectionner.
- Un dernier service est utilisé pour supprimer le fichier sélectionné.

Ces services sont obtenus à l'aide des primitives F-Select, F-Deselect, F-Create et F-Delete.

❖ Les services de gestion de fichier

Deux services de gestion sont offerts à l'initiateur :

- Le premier permet de consulter les attributs du fichier sélectionné.
- Le second est utilisé pour modifier les attributs de ce même fichier.

Ces services sont obtenus à l'aide des primitives F-Read-Attrib

et F-Change-Attrib.

❖ **Les services de contrôle d'accès au fichier**

Deux services de contrôle d'accès au fichier sont offerts à l'initiateur.

- Le premier lui permet d'ouvrir le fichier en indiquant les contextes de présentation et de concurrence qui seront en vigueur.
- Le second libère le contexte établi par le précédent en fermant le fichier.

Ces services sont obtenus à l'aide des primitives F-Open et F-Close.

❖ **Les services de contrôle de concaténation**

Deux services sont offerts à l'initiateur :

- Le premier est utilisé pour indiquer le début de la concaténation des primitives qui doivent être traités comme un seul bloc.
- Le second sert à préciser la fin de cette concaténation.

Ces services sont obtenus à l'aide des primitives F-Begin-Group et F-End-Group.

❖ **Le service de recouvrement**

Ce service de recouvrement est utilisé par l'initiateur pour recréer le régime d'accès au fichier après une panne quelconque. Ce service est obtenu à l'aide de la primitive F-Recover.

❖ Les services d'accès au contenu du fichier

Deux services d'accès au contenu du fichier sont mis à la disposition de l'initiateur :

- Le premier permet d'identifier une unité de données, appelée FADU (File Accès Data Unit), qui sera localisée par le répondeur et deviendra l'unité courante
- Le second permet d'éliminer une unité de données du fichier.

Ces services sont obtenus à l'aide des primitives F-Locate et F-Erase.

❖ Les services de transfert de fichier

Il existe **six** services de transfert de données :

- Un service de lecture est utilisé par l'initiateur pour indiquer le début d'un transfert du répondeur à l'initiateur,
- Un service d'écriture sert à commencer le transfert dans le sens inverse,
- Un service de transfert d'unités de données,
- .Un service de transfert d'unité de données permet à l'émetteur d'indiquer que tous les blocs ont été transmis,
- Le service de fin de transfert est utilisé par l'initiateur pour confirmer la terminaison du transfert,
- Finalement, un service d'annulation de transfert permet à l'une ou l'autre des parties d'annuler le transfert en cours.

Ces services sont obtenus à l'aide des primitives F-Read, F-Write, F-Data, F-Data-End , F-Transfer-End et F-Cancel.

❖ Le service de point de reprise et le service de reprise

Le service de point de reprise permet à ce lui qui envoie des données d'insérer des points de reprise entre les blocs de données transmis, afin de mieux contrôler les progrès du transfert et de faciliter une reprise. Le service de reprise peut être utilisé par l'émetteur où le récepteur pour interrompre un transfert et négocier un point où celui-ci sera repris. Ces services sont obtenus à l'aide des primitives F-Check et F-Restart.

2.4 Exemple d'utilisation du FTAM

A fin d'illustrer l'utilisation des services FTAM, nous présenterons l'exemple de transfert d'un fichier en écriture. Cet exemple concerne la création d'un nouveau fichier, et il faut donc initialiser successivement le régime FTAM, le régime de sélection et le régime d'ouverture avant de pouvoir commencer l'écriture. La sélection est en fait ici une création et les primitives de création et d'ouverture sont regroupées grâce aux primitives de services F-Begin-Group et F-End-Group de façon à accélérer l'ouverture.

Le transfert proprement dit prend place après l'ouverture, avec spécification du transfert en écriture par le service F-Write puis transfert des différents segments du contenu par des services successifs F-Data. La fin des transferts et le retour dans le régime d'ouverture sont marqués par les services F-Data-End et F-Transfer-End. La fermeture et la désélection sont ici encore regroupées, l'association est libérée par le service F-Terminate.

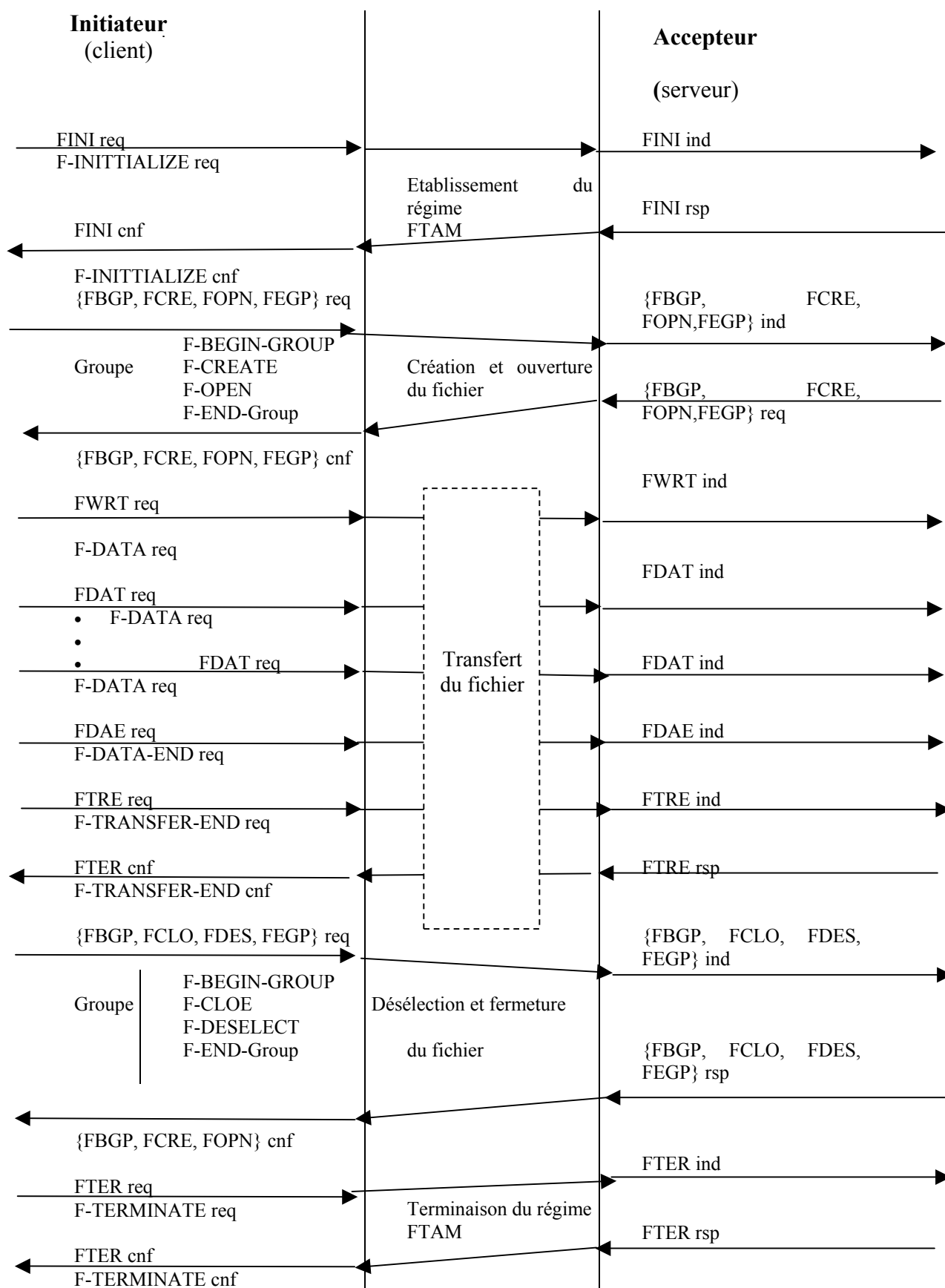


Fig 2.2 : Transfert d'un fichier vers un système distant

2.5 Avantages du protocole FTAM par rapport au protocole FTP

Le protocole FTAM est plus robuste que le protocole FTP , en effet il présente un nombre d'avantages par rapport à ce dernier :

1- Le protocole FTAM, comme son l'indique, assure le transfert, l'accès et la gestion du fichier. L'accès au fichier permet, par exemple, de lire ou écrire un enregistrement, alors que la gestion permet de créer ou détruire un fichier. Ces deux applications, donc, nous offre la possibilité de manipuler des fichiers distants de même façon que si ces fichiers étaient situés dans notre propre système.

On dit, alors, que le groupe des fonctions du protocole FTAM est plus large que celle du protocole FTP qui ne permet que le transfert de fichier.

2- Le protocole FTAM offre la possibilité de transférer le continu, la structure et les attributs d'un fichier. En effet, on peut avoir une idée sur les caractéristiques d'un fichier tels que : le nom, la taille, les opérations réalisables sur celui-ci, l'organisation de l'information dans le fichier et les modes d'accès à cette information.

3- Le protocole FTAM capable d'accéder à une base de données distante: c'est à dire que cette norme nous permet de lire où modifier une base de données existante sur une machine distante.

4- Le protocole FTAM prévoit des mécanismes de reprise sur erreur qui sont assurés par le protocole FERPM (FTAM File Error Protocol Machine)

5- La norme FTAM permet de grouper plusieurs primitives, de façon à ce que qu'un seul échange de message soit nécessaire pour assurer une suite de services. Ensuite rendre plus rapide l'opération du transfert.

6- La connexion distante est établie par l'initiateur (le client) mais comme cette dernière demande des services, le répondeur (serveur) aussi, alors que pour le protocole FTP, seul le client demande des services.

7- Le protocole FTAM permet l'établissement de plusieurs régimes simultanément avec le même système de fichiers virtuels, ce qui permet l'accès simultané aux fichiers par des associations distincts entre le serveur et le même client ou entre le serveur et différents clients.

2.6. Conception du système FTAM

2.6.1 Solution Moyen Terme

La solution de collecte à moyen terme est illustrée par la figure 2.3. Il s'agit de collecter les données de taxation à partir des centraux E10 par un système propriétaire vers un serveur de fichiers. Ce serveur doit être équipé d'une interface logicielle pour être connecté au serveur FTAM existant dans le centre de la facturation et qui est exploité actuellement pour collecter les données de taxation à partir des centraux de type EWSD et AXE.

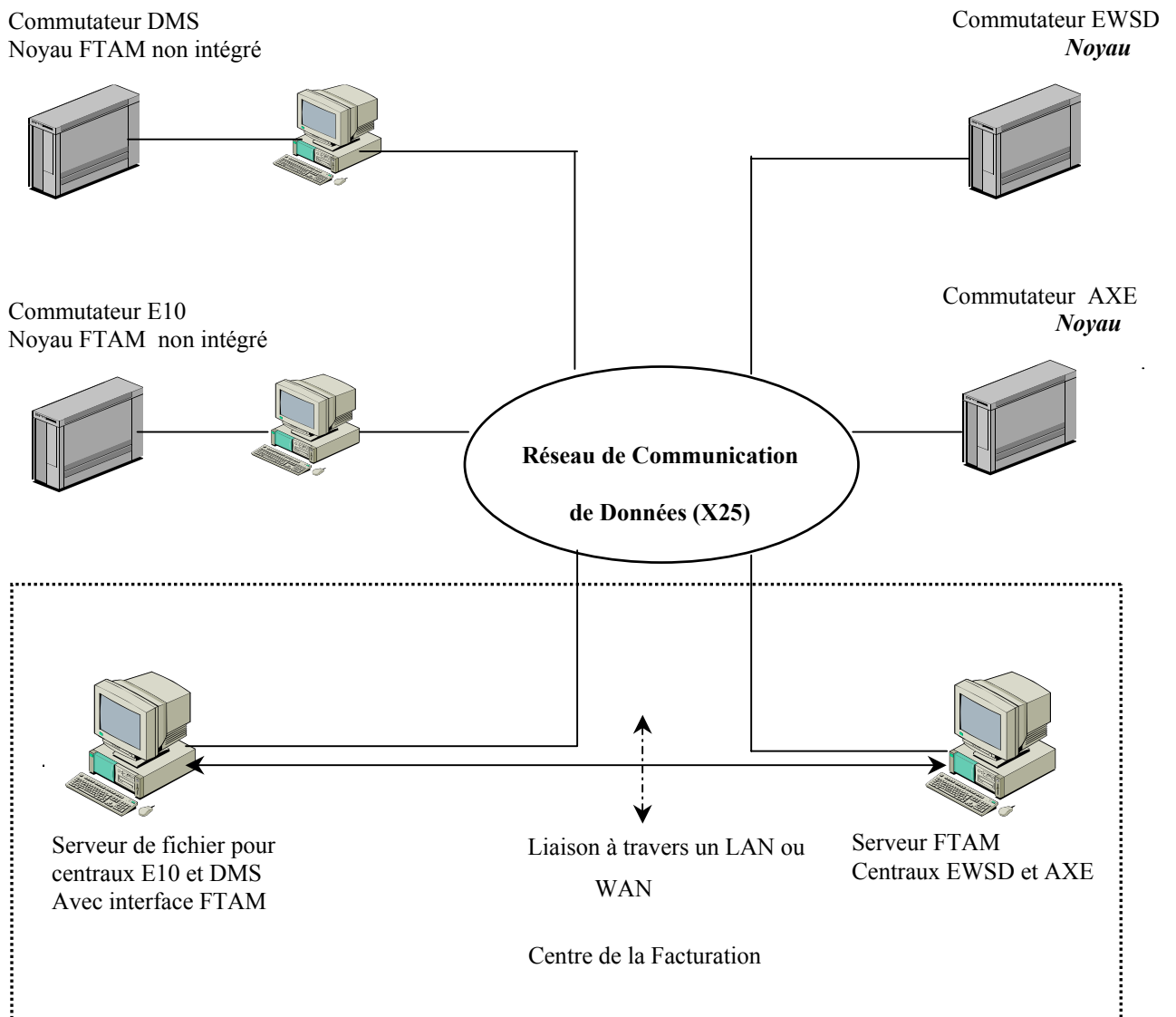


Fig 2.3 : Solution FTAM à moyen Terme

3.6.2. Solution long terme

C'est la solution qui nécessite l'implémentation d'un noyau FTAM au niveau de tous les centres de commutation de type E10 et DMS et ce, à l'instar des centraux de type EWSD et AXE.

Ce noyau FTAM est une couche logicielle qui doit être introduite dans le système d'exploitation de chaque commutateur et seules les fournisseurs des systèmes de commutation peuvent réaliser le développement et l'implémentation de ce noyau FTAM vu que les systèmes d'exploitation des systèmes de commutation sont des systèmes propriétaires.

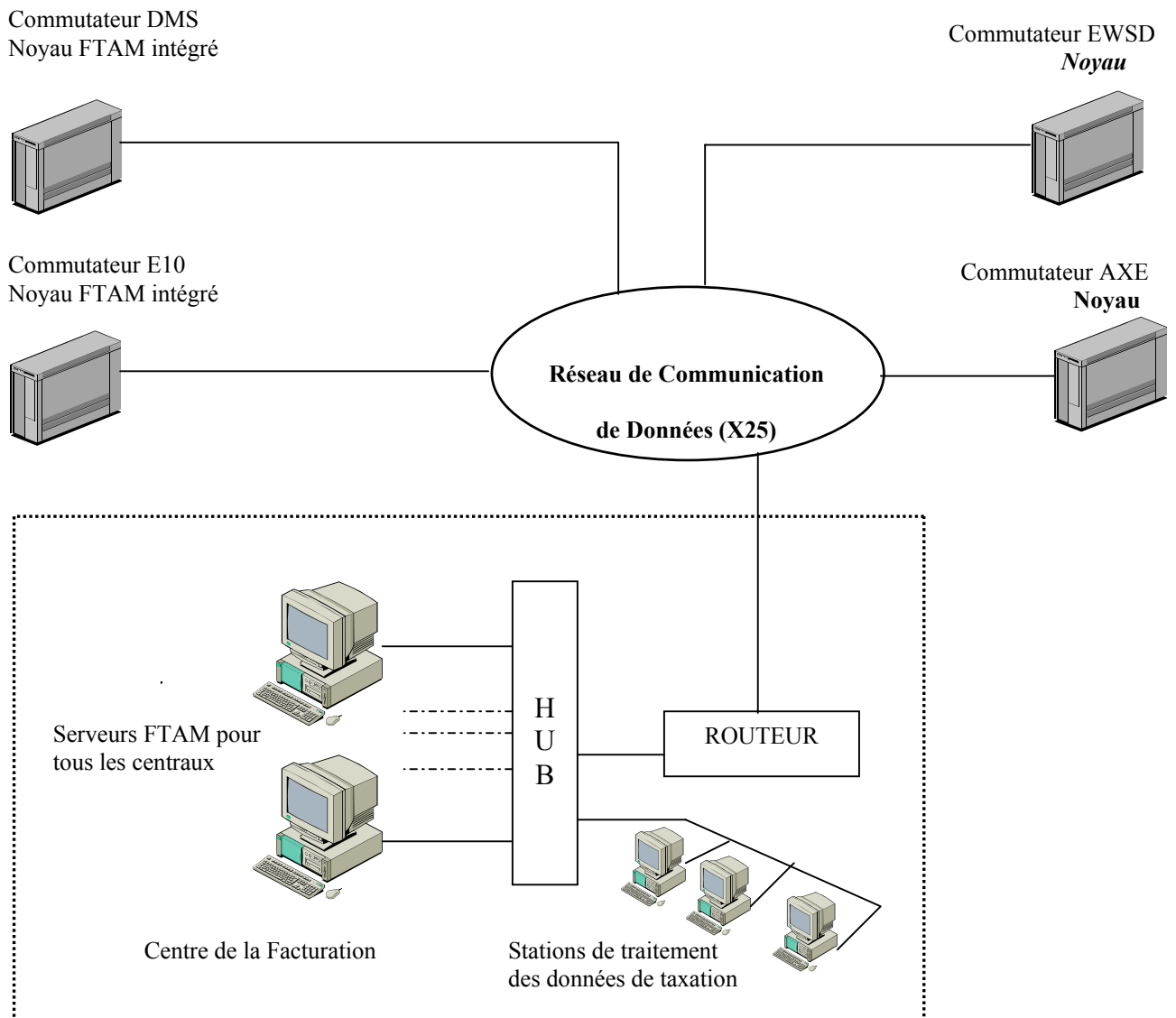


Fig 2.4. : Solution FTAM à long terme

CHAPITRE 3

SOLUTION DE COLLECTE A BASE DU PROTOCOLE FTP

3.1 Introduction

L'implémentation d'un système de collecte de données de taxation à base de protocole FTAM présente un ensemble de contraintes au stade de la réalisation complète de ce projet. D'une part, les centraux de type E10 et DMS avec la version logiciel actuelle ne permettent pas d'intégrer le noyau FTAM, aussi l'implémentation du protocole FTAM est encore réduite à des plate-formes propriétaires.

D'autre part, la mise en place d'une plate-forme de gestion et d'administration pour gérer l'ensemble des entités de cette solution demande la mise en place la conception et l'implémentation d'un système de gestion et de maintenance qui se base sur la normalisation ISO qui dépasse le cadre de ce projet.

A cet effet, nous avons choisi d'étudier et réaliser ce projet en utilisant la famille de protocole TCP/IP vue la disponibilité des entités logiciels nécessaires pour réaliser une solution intégrant les fonctionnalités de transfert, d'administration, de télémaintenance et de sécurité. D'autre part, les réseaux de données et de télécommunications convergent vers l'utilisation et le développement des services en utilisant la pile de protocole TCP/IP qui est devenue un standard de fait.

Dans ce chapitre on va présenter la famille de protocole de TCP/IP comme un protocole de communication, le protocole FTP présente le moyen de transfert de données de taxation à partir de centraux vers le centre de collecte de facturation et enfin étudier les outils et les moyens nécessaires pour l'administration, la maintenance et la sécurisation du système de collecte automatique de données de taxation.

3.2 Composants Fonctionnels du Système

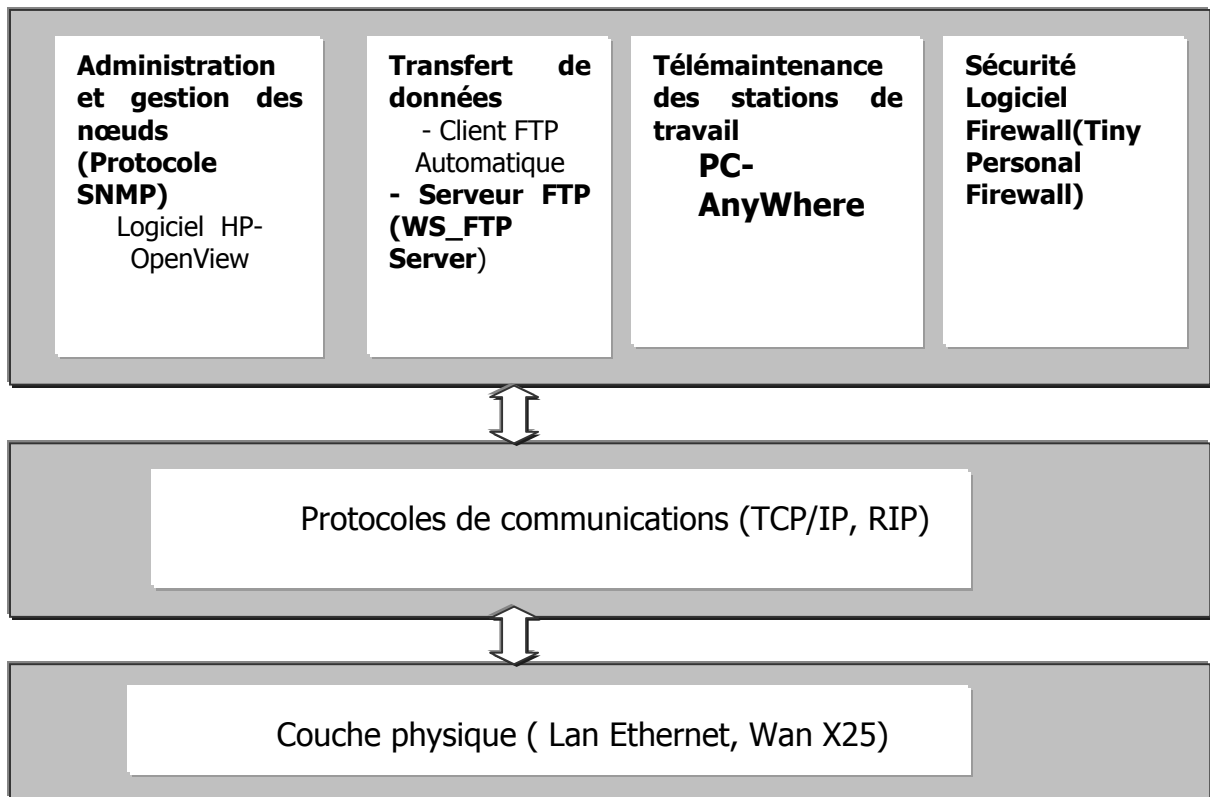


Fig 3.1 : Composants Fonctionnels du Système de collecte Automatique des données de taxation

3.3 Présentation du protocole TCP/IP

Le protocole Internet a été conçu pour réaliser l'interconnexion de réseaux informatiques et permettre ainsi les communications entre systèmes. Ce protocole assure la transmission des paquets de données, appelés data grammes entre un ordinateur source et un ordinateur destination.

Ces ordinateurs source et destination peuvent être interconnectés par un ou plusieurs réseaux. Pour assurer une communication Internet, chaque ordinateur et chaque équipement d'interconnexion, impliqué dans la communication, doivent posséder un module logiciel, appelé "PILE TCP/IP".

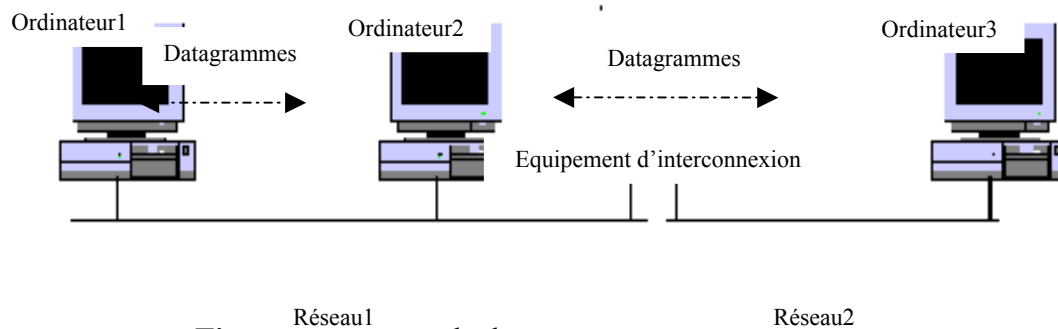


Fig 3.2 . Echanges de data grammes entre deux ordinateurs

Chaque data gramme Internet, considéré comme une entité indépendante, possède un en-tête propre qui contient l'ensemble des informations nécessaires à son acheminement vers sa destination.

Les communications Internet entre les ordinateurs source et destination nécessitent l'utilisation d'adresses pour identifier les équipements. Ces adresses sont aussi transportées dans l'en-tête de chaque data gramme et exploitées par les équipements d'interconnexion pour réaliser le routage.

Pour adapter la longueur des data grammes à la longueur maximale des trames physiques véhiculées sur les différents réseaux, le protocole Internet implémente un mécanisme de fragmentation et d'assemblage.

Architecture du protocole TCP/IP

Dans la figure 3.3, on a regroupé et classifié les différents protocoles en fonction de chaque hiérarchie dans l'architecture ARPA (Advanced Research Projects Agency).

A chaque groupe ainsi formé correspond une couche dont le patronyme désigne la ou les fonctionnalités du groupe.

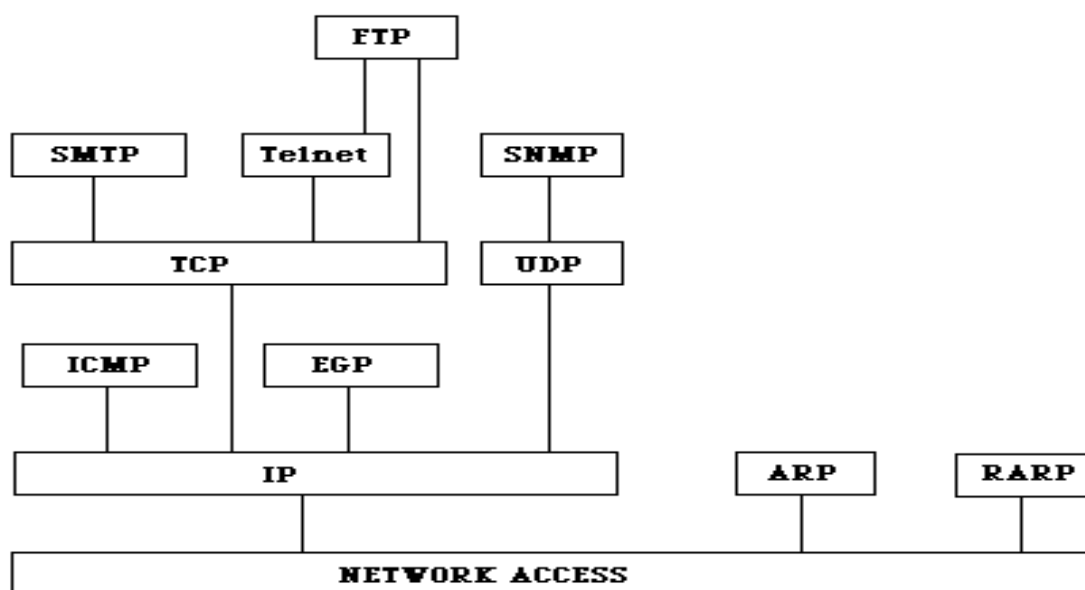


Fig3.3: L'architecture ARPA

Le tableau 1 fait apparaître le modèle ainsi obtenu :

Couche des processus	SNMP, TELNET, FTP et autres applications
Couche Host to Host	UDP, TCP
Couche Internet	IP (+ICMP), ARP, RARP
Couche d'accès au réseau	Protocoles des LAN, WAN et MAN.

Tableau 1 : Modèle TCP/IP

▪ Couche Physique :

Comporte les routines permettant d'accéder aux réseaux physiques.

▪ Couche Internet :

Définit le data gramme et prend en charge le routage des données.

▪ **Couche Transport :**

Assure les services de transmission de données de bout en bout.

TCP fournit un service de communication de processus à processus, dans un environnement réseau, il est défini comme un protocole de communication "host to host".

TCP s'interface avec un processus utilisateur ou applicatif et un protocole de niveau inférieur du type Internet Protocol.

▪ **Couche Application :**

Comporte les applications et processus utilisant le réseau (FTP, http..).

3.4 Présentation du protocole FTP

Le protocole FTP a pour objectifs de :

- Permettre un partage de fichiers entre machine distante,
- Permettre une indépendance aux systèmes de fichiers des machines clientes et serveur,
- Permettre de transférer des données de manière efficace.

Le transfert de fichiers entre deux machines est sans doute une des applications de TCP/IP les plus souvent utilisées. On fait appel à cette technique lorsqu'on télécharge un fichier sur Internet, par exemple.

FTP est une application de type Client /Serveur: une machine (le serveur) met des fichiers à la disposition d'autres machines (les clients). FTP fonctionne dans les deux sens : un client peut aussi envoyer un fichier au serveur. Le transfert de fichiers FTP est orienté connexion et basé sur le protocole TCP: il s'agit donc d'un transfert fiable.

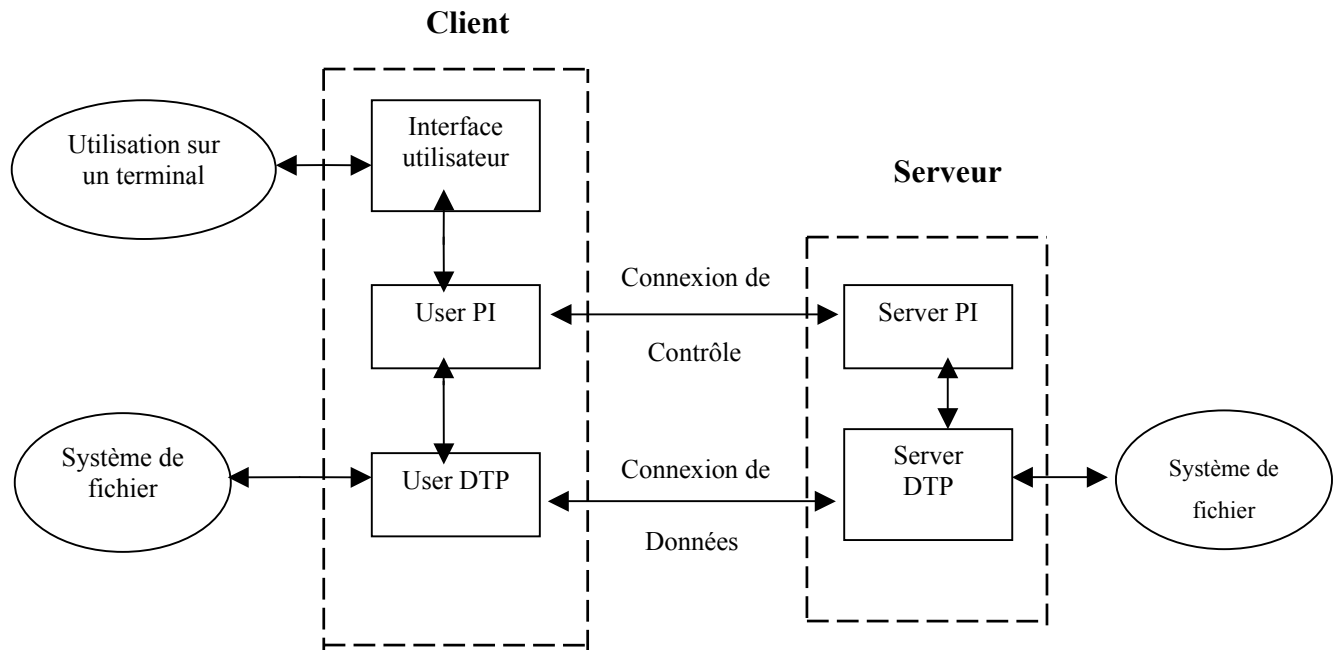


Fig3.4 : Le modèle FTP

Ainsi, le client comme le serveur possède deux processus permettant de gérer les informations entre eux :

- Le **DTP** (*Data Transfer Process*) est le processus chargé d'établir la connexion et de gérer le canal de données. Le DTP côté serveur est appelé *SERVER-DTP*, le DTP côté client est appelé *USER-DTP*.
- Le **PI** (*Protocol Interpreter*) est l'interpréteur de protocole permettant de commander le DTP à l'aide des commandes reçues sur le canal de contrôle. Il est différent sur le client et sur le serveur:

✓ Le **SERVER-PI** est chargé d'écouter les commandes provenant d'un **USER-PI** sur le canal de contrôle sur un port donné, d'établir la connexion pour le canal de contrôle, de recevoir sur celui-ci les commandes FTP de l'**USER-PI**, d'y répondre et de piloter le **SERVER-DTP**.

✓ Le **USER-PI** est chargé d'établir la connexion avec le serveur FTP, d'envoyer les commandes FTP, de recevoir les réponses du **SERVER-PI** et de contrôler le **USER-DTP** si besoin.

Principe de protocole FTP

FTP fonctionne avec deux connexions : l'une (port 20) sert au *transfert des données* du fichier proprement dites, tandis que l'autre (port 21) sert à *envoyer les commandes et recevoir des réponses* (c'est le canal de contrôle, qui utilise le protocole Telnet).

Tout utilisateur de FTP doit être identifié, c'est-à-dire posséder un nom d'utilisateur (*login*) et un mot de passe (*password*). Dans certains cas, tout le monde peut accéder aux fichiers du serveur FTP : C'est le FTP anonyme (*anonymous FTP*).

Lorsque l'identification a eu lieu, le client peut envoyer une série de **commandes** au serveur pour demander ou proposer un fichier. Une commande FTP est simplement constituée d'un mot-clé, éventuellement suivi de paramètre(s), le tout en texte clair. Avant d'envoyer la commande suivante, le client doit attendre une réponse du serveur.

3.5 Administration et Maintenance du Système

Le présent projet porte également sur la mise en place d'un système de gestion, d'administration et de télémaintenance du système de collecte automatique des données de taxation, dans le but d'assurer une flexibilité totale au niveau du contrôle du bon fonctionnement des entités impliquées dans ce projet.

3.5.1 Architecture d'administration de réseaux

Une architecture d'administration de réseaux présente trois objectifs :

- définir la structure globale d'un système d'administration de réseaux,
- définir chaque composante dans ce système,
- définir les relations entre ces composantes.

3.5.2 Un exemple de modèle d'architecture de réseaux

La figure 3.5 symbolise un modèle d'architecture de réseaux :

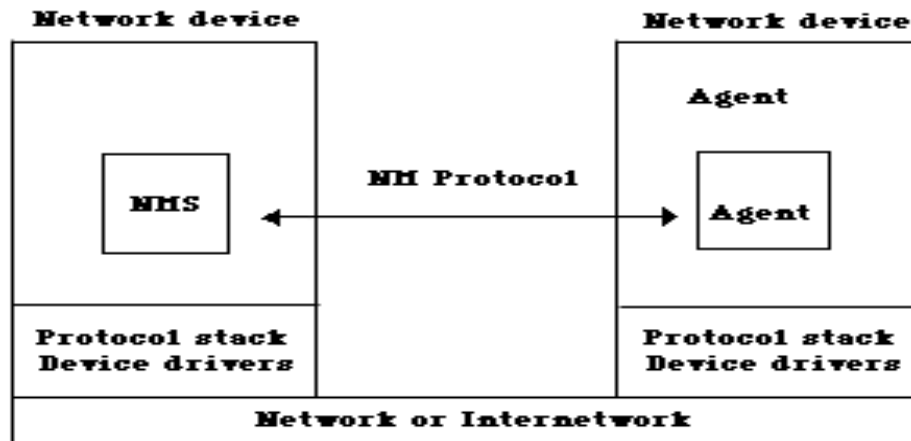


Fig3.5 : Modèle d'architecture de gestion de réseau

Ce modèle décrit deux équipements réseaux : un système de gestion de réseaux NMS (Network Management System) et un agent de gestion. Le NMS et l'agent communiquent via un protocole de gestion de réseaux. Le modèle décrit une communication 'point à point' sur le réseau Internet entre deux entités à travers un ensemble de "protocoles stacks" (pour désigner la pile TCP/IP) et d'équipements.

Ce modèle d'architecture est le dénominateur commun de toute administration de réseaux et s'applique, en particulier, à SNMP qui utilise également le concept NMS/Agent (on dit aussi Client/Serveur).

3.5.3 Protocole SNMP

3.5.3.1 Définition

Le protocole SNMP (Simple Network Management protocole) est un protocole de gestion de réseaux qui a été proposé par l'IETF (RFC 1155 et RFC 1156). Il est actuellement le plus utilisé pour la gestion des équipements de réseaux. Le protocole SNMP est un protocole relativement simple. Toutefois, l'ensemble de

ses fonctionnalités est suffisamment puissant pour permettre la gestion de réseaux hétérogènes complexes. Son utilisation dépasse largement le cadre de la gestion des équipements de réseau. Il est aussi utilisé pour la gestion à distance des applications: les bases de données, les serveurs, les logiciels, etc.

3.5.3.2 Environnement de gestion SNMP

L'environnement SNMP a été initialement développé pour être supporté par le système d'exploitation Unix sous protocole TCP/IP et fonctionner en mode Data gramme sous le protocole UDP (User Data gram Protocol).

Le protocole SNMP fournit à l'administrateur du réseau la facilité d'interroger les éléments de son réseau sans se déplacer. Il fonctionne sur un modèle client-serveur, où il n'y a qu'un seul client, la station d'administration (NMS Network Management Station) et beaucoup de serveur (chaque agent SNMP), le client interrogeant les serveurs pour récupérer les informations.

Chaque agent est placé sur un nœud du réseau qui est dit administrateur (MN: Managed Node). Ces nœuds peuvent être soit des hôtes (stations de travail ou serveurs), soit des éléments d'interconnexion (Switchs, hubs, routeurs), soit des supports physiques (câbles).

Les différents composants du SNMP sont les suivants :

- Les éléments de réseaux sont les équipements ou les logiciels que l'on cherche à gérer.
- Les agents sont des modules qui résident dans les éléments de réseau. Ils vont chercher l'information de gestion tel le nombre de paquets erronés reçus par un élément de réseau.
- La plate-forme de gestion de réseau (NMS) exécute les applications de gestion qui contrôlent les éléments de réseau.

- Une MIB (Management Information Base) est une collection d'objets résidant dans une base d'information.
- Un protocole permet à la plate-forme NMS d'aller chercher les informations sur les éléments de réseaux. De plus, il permet à la NMS de recevoir des alertes de la part des éléments de réseaux.

3.5.3.3 Fonctionnement du protocole SNMP

Le SNMP fournit quelques commandes de base pour la recherche et la mise à jour des variables du MIB.

❖ Les requêtes et les réponses SNMP

Le fonctionnement du protocole SNMP est asymétrique. Il est constitué d'un ensemble de requêtes, de réponses et d'un nombre limité d'alertes. La station de gestion envoie des requêtes à l'agent SNMP, lequel retourne des réponses. Lorsqu'un événement anormal se produit sur l'élément de réseau, l'agent envoie une alerte (trap) à la station de gestion de réseau. Le SNMP utilise le protocole UDP. Le port 161 est utilisé par l'agent pour recevoir les requêtes de la station NMS et le port 162 est réservé pour la station NMS à fin de recevoir les alertes provenant des agents.

❖ Les requêtes :

Il existe quatre types de requêtes : Get Request, Get Next Request, Get Bulk et Set Request :

- La requête Get Request permet la recherche d'une variable d'un agent
- La requête Get Next Request permet la recherche de la variable suivante.
- La requête Get Bulk permet la recherche d'un ensemble de variable regroupée
- La requête Set Request permet de changer la valeur de la variable d'un agent.

❖ Les réponses :

A ces requêtes l'agent répond par l'une des deux réponses suivantes: Get Response ou No Such Object.

- La réponse Get Response permet à l'agent de retourner la réponse à la requête demandée.

- La réponse No Such Object informe la station de gestion de réseau que la variable demandée n'est pas disponible.

Les réponses négatives sont les suivantes :

- No Acces: Accès non permis.
- Wrong Lengh: Erreur de longueur.
- Wrong value: Valeur erronée.
- No creation: Objet non crée.
- Authorisation Error: Erreur d'autorisation.

❖ Les alertes :

Les alertes sont envoyées de l'agent à la station de gestion de réseau.

On cite: Cold start, Warm Start, Link Down, Link Up et Authentification Failure.

- Cold Start: agent relancé : modification de la configuration possible.
- Warm Start: agent réinitialisé sans modification de la configuration.
- Entreprise specific: événement dépendant du constructeur.
- Link Down: l'agent a détecté une rupture de réseau.
- Link Up : l'agent a détecté que le réseau est de nouveau actif.

Les alertes sont des interruptions signalées par un événement prédéfini.

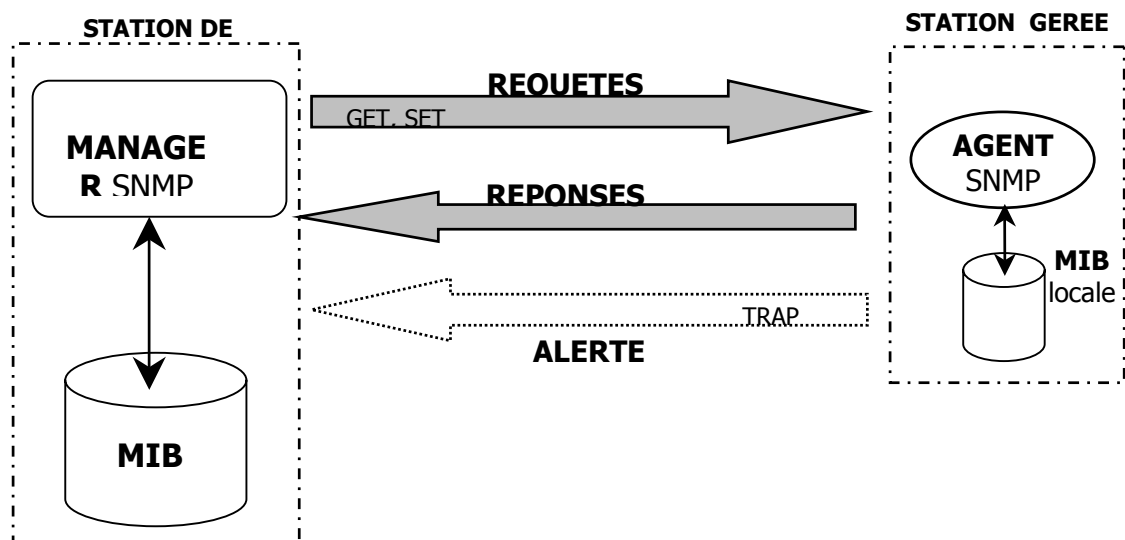


Fig 3.6 : Concept du protocole SNMP

3.5.4 Télémaintenance

Le bon fonctionnement d'un système informatique n'est pas déterminé seulement par la qualité du matériel mis en service, mais aussi par l'efficacité des services offerts par

la maintenance. Il s'est avéré intéressant, de maintenir les postes de travail à distance sans perturber le bon fonctionnement du réseau. Et selon cette approche, la télémaintenance est définie comme étant un ensemble d'actions à entreprendre pour surveiller, contrôler et réparer à distance un dispositif défaillant d'un système. Elle consiste à obtenir d'un point de contrôle plus ou moins éloigné des informations sur le fonctionnement d'une installation.

3.6 Etude de sécurisation du système de collecte automatique

3.6.1 Introduction

Pour définir un système d'information sécurisé, on peut mettre en avant les 5 points que l'International Standard Organization (ISO) a fait ressortir dans ses études sur les sécurités des réseaux :

- **La confidentialité:** l'information échangée entre deux correspondants ne peut pas être consultée par un tiers.
- **L'authentification:** les personnes utilisant une ressource correspondent aux noms d'utilisateurs.
- **La disponibilité ou non-répudiation:** les données ainsi que les ressources du système d'information sont accessibles par ceux qui en ont besoin à chaque fois qu'ils en ont l'utilité.
- **L'intégrité:** l'information n'est modifiée que par les personnes en ayant le droit, et de façon volontaire.
- **Le contrôle d'accès:** une ressource n'est accessible que par les personnes autorisées.

Mettre au point une politique de sécurité pour un réseau va donc consister à connecter entre eux les composants du système d'information tout en faisant respecter ces cinq règles.

3.6.2 Sécurisation de FTP par la couche SSL

Il est indispensable de sécuriser les données de taxation qui circulent à travers un réseau. Toutes les opérations de transfert de données doivent offrir des qualités de confidentialité, d'authentification et d'intégrité.

L'utilisation de FTP présente un ensemble de failles de sécurité ce qui rend nécessaire de mettre en place une solution qui rend ce protocole FTP sécurisé. L'utilisation

de SSL est la solution adéquate pour surpasser les défaillances de sécurité de protocole FTP.

La SSL (Secure Sockets Layers), que l'on pourrait traduire par *couche de sockets sécurisée*) est un procédé de sécurisation des transactions effectuées via Internet mis au point par *Netscape*, en collaboration avec *Mastercard*, *Bank of America*, *MCI* et *Silicon Graphics*. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur le réseau.

Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des liaisons via le **protocole FTP** ou Telnet. En effet, SSL agit telle une couche, permettant d'assurer la sécurité des données, et située entre les sockets (l'implémentation logicielle, c'est-à-dire les lignes d'un programme orienté Internet, permettant à l'ordinateur d'envoyer des informations via une ligne de transmission) et un protocole de la suite TCP/IP.

La sécurisation des transactions par SSL est basée sur un échange de clés entre client et serveur. La figure3.7 est une illustration étape par étape de la façon dont le SSL fonctionne.

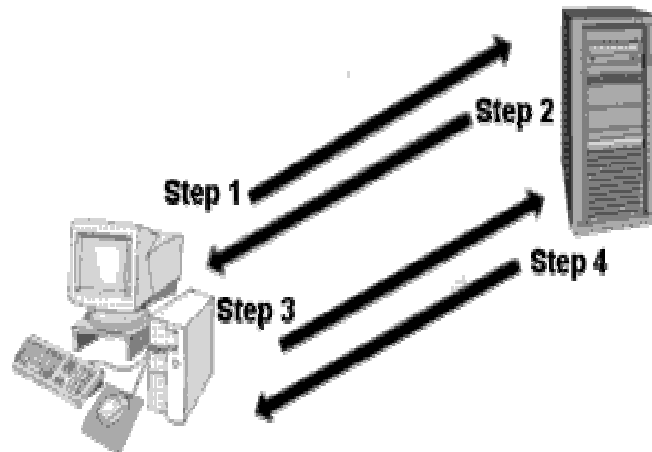


Fig3.7 : Les étapes de fonctionnement de SSL

- **Etape1** : Le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier. Le client envoie également la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant de la longueur des clés.

- **Etape2** : Le serveur a réception de la requête envoie un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA), ainsi que le nom du cryptosystème le plus haut dans la liste avec lequel il est compatible (la longueur de la clé de chiffrement - 40 bits ou 128 bits - sera celle du cryptosystème commun ayant la plus grande taille de clé).
- **Etape3** : Le client vérifie la validité du certificat (donc l'authenticité du marchand), puis crée une clé secrète aléatoire (plus exactement un bloc prétendument aléatoire), chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session).
- **Etape4** : Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée. Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peut se faire à l'aide de la clé de session, garantissant l'intégrité et la confidentialité des données échangées.

3.7 Sécurisation du réseau

Il est indispensable de protéger chaque élément du réseau contre toute malveillance, il est aussi primordial que l'ensemble du système de collecte soit cohérent. La topologie du réseau doit intégrer la sécurité. Il faut mettre des

Protections entre le réseau interne et le réseau externe. Un firewall permet de filtrer ce qui entre et ce qui sort.

Firewall

Un Firewall est un système ou un groupe de système qui gère les contrôles d'accès entre deux réseaux. Deux mécanismes sont utilisés le premier consiste à interdire le trafic et le deuxième à l'autoriser.

CHAPITRE 4

IMPLEMENTATION DE LA PLATEFORME TCP/IP

4.1 Introduction

Dans le chapitre précédent, nous avons exposé l'architecture fonctionnelle des composants constituant le système de collecte automatique de données de taxation. Nous devons maintenant tourner vers l'implémentation et la recherche des composants logiciels nécessaires pour aboutir à un système répondant aux besoins spécifiés au cahier des charges qui touche à la fonction de transfert, à la gestion, à la maintenance et en fin à la sécurité du dit système.

D'abord, la réalisation de ce projet passe par la spécification de connexion des entités matérielles impliquées dans le transfert des données.

En second lieu, la conception et la réalisation d'une application qui permet d'assurer le transfert automatique de données de taxation à partir des sites des centres de commutation vers le serveur de la facturation.

Enfin, l'intégration et l'installation des logiciels nécessaires à l'administration du serveur FTP(WS_FTP Server), à la maintenance (PcAnywhere) et à la sécurité (Tiny Personal Firewall).

4.2 Architecture du système de collecte automatique

- **Site Centre de commutation :**

Type de réseaux LAN : Ethernet 10 Mbps.

Type de réseaux WAN : X25.

Equipements réseaux :

- ✓ Concentrateur.
- ✓ Routeur.
- ✓ Modem X25.

Serveur de données de taxation :

- ✓ Système d'exploitation : Windows NT Server.
- ✓ Serveur FTP: WS_FTP Server.
- ✓ Firewall: Tiny Personnel Firewall.
- ✓ Logiciel de télémaintenance : PCAnyWhere (Side exclave).

Protocole de communication : TCP/IP.

Protocole de routage : RIP.

Protocole de transfert de données : FTP.

Protocole d'administration : SNMP.

- **Site Centre de facturation :**

Type de réseaux LAN : Ethernet 10 Mbps

Type de réseaux WAN : X25

Equipements réseaux :

- ✓ Concentrateur.
- ✓ Routeur.
- ✓ Modem X25.

Serveur de collecte des fichiers de taxation :

- ✓ Système d'exploitation : Windows NT Server.
- ✓ Application de transfert automatique.
- ✓ Base de données contenant les informations nécessaires pour le transfert.
- ✓ Système de télémaintenance : PCANYWHERE (Maître Side).

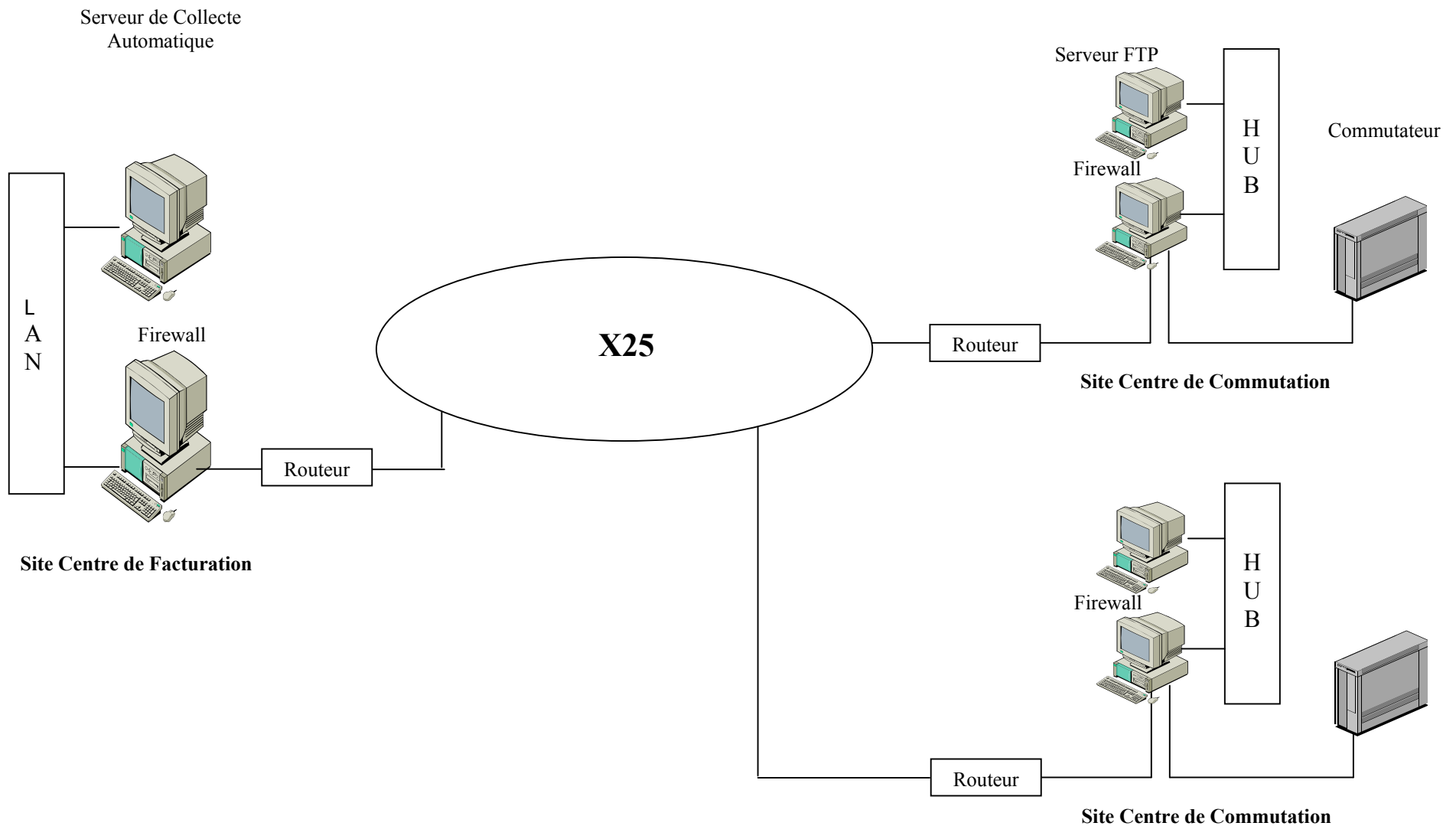


Fig.4.1 : Architecture Réseaux du Système de Collecte sous TCP/IP

4.3 Conception et réalisation d'une application de transfert automatique

4.3.1 Environnement de développement

- **Microsoft Visual Basic**

Le Visual Basic 6.0 est l'un des outils les plus efficaces pour la réalisation d'applications WINDOWS performantes. Les fonctionnalités telles la compilation du code natif optimisé, l'affichage accéléré des formulaires et l'accès amélioré aux bases de données permettent aux développeurs de créer des applications et des composants alliant richesses fonctionnelles et performances élevées.

- **Base de données Microsoft Access**

Microsoft Access est un système de gestion de base de données. A l'aide de ce logiciel nous pouvons gérer nos informations.

Dans le cadre de notre projet, nous avons choisi Microsoft Access pour stocker et gérer des données contenues dans une table nommée 'SERVEUR'provenant de la base de données. Dans cette table, on dispose de toutes les informations nécessaires pour l'exécution de l'application.

4.3.2 Objectifs

- Transfert automatique de données de taxation à chaque fin de mois.
- Journalisation des anomalies de transfert.
- Transfert manuel en cas de problème.

4.3.3 Architecture générale de l'application

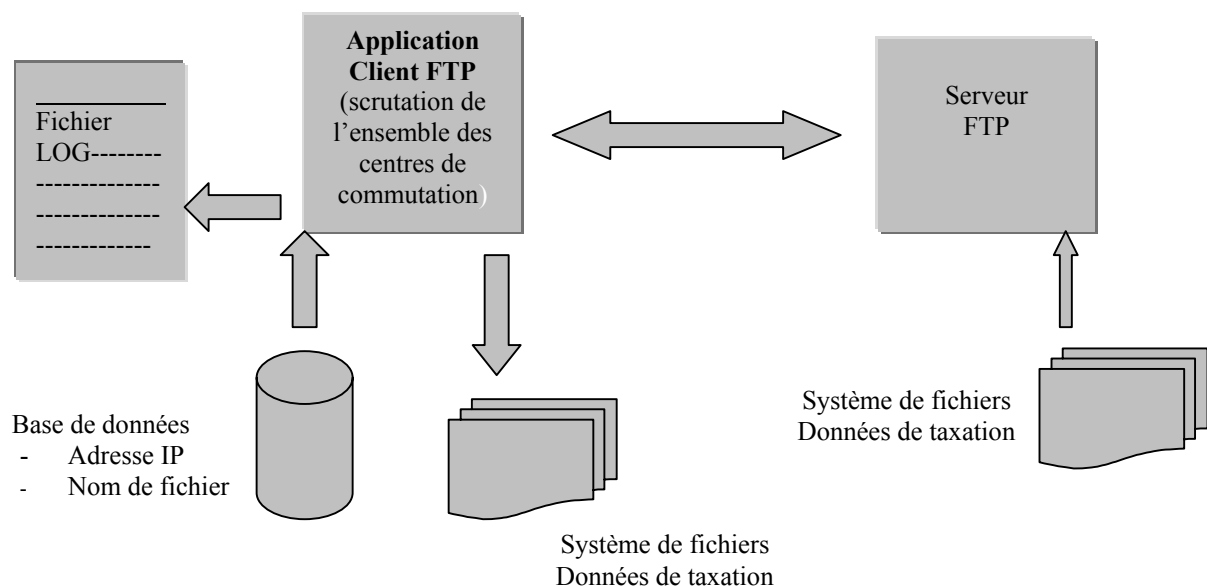
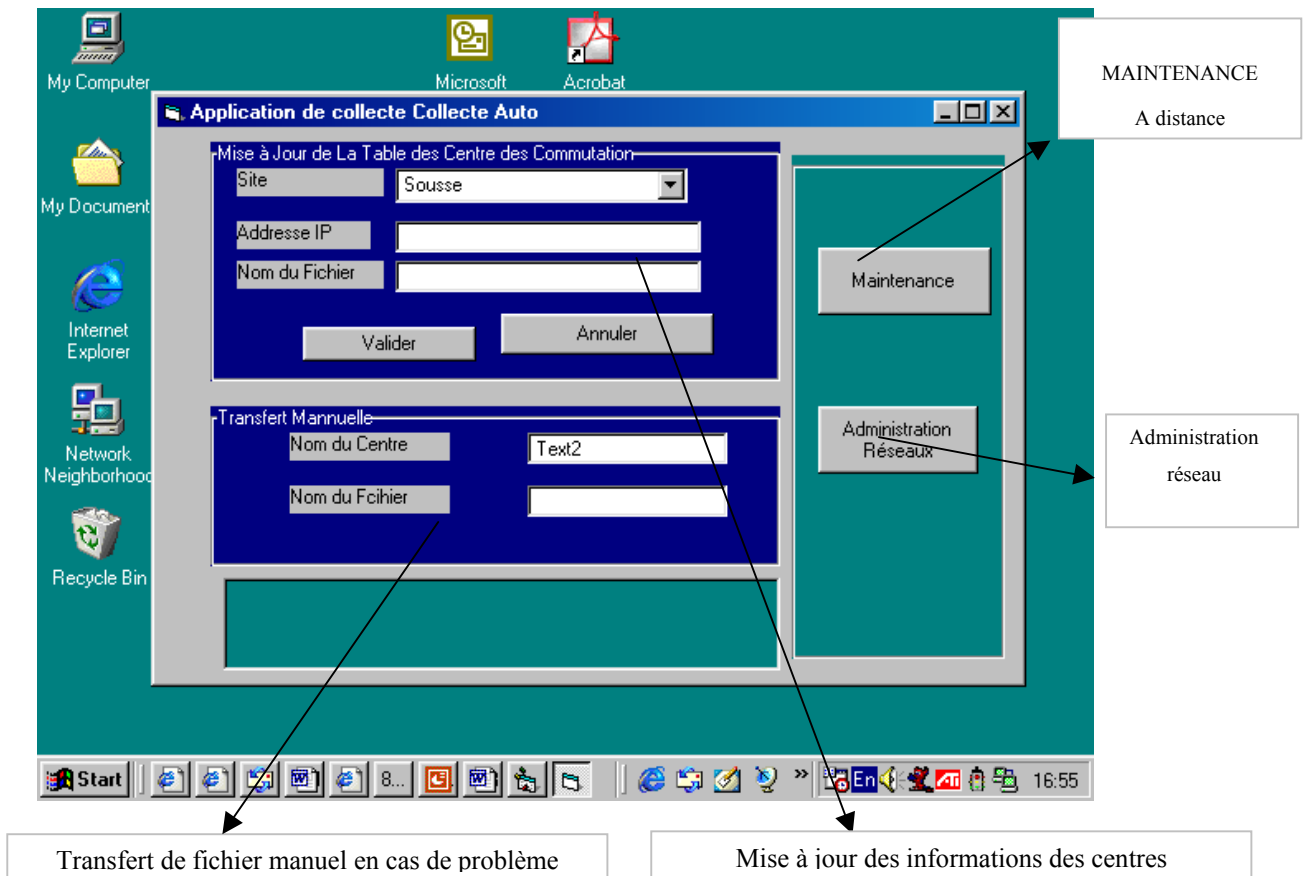


Fig 4.2 : Architecture générale de l'application

4.3.4 Algorithme Client FTP

4.3.5 Interface Graphique de l'application



4.3.6 Installation et paramétrage du serveur FTP (WS_FTP SERVER)

- **Description du logiciel**

WS_FTP Server est un serveur FTP sécurisé pour Windows NT Server permet la création des sites FTP en mettant à la disponibilité des utilisateurs distants des fichiers et des répertoires en gérant les droits d'accès des utilisateurs à ces ressources.

Le FTP SERVER fonctionne sans interruption dans le fond et écoute sur le port 21 une demande de raccordement d'un client de FTP. Quand un client ftp demande un raccordement, le FTP SERVER vérifie l'identification de l'utilisateur d'ouverture et le mot de passe et, si valide, lui ouvre un raccordement de commande.

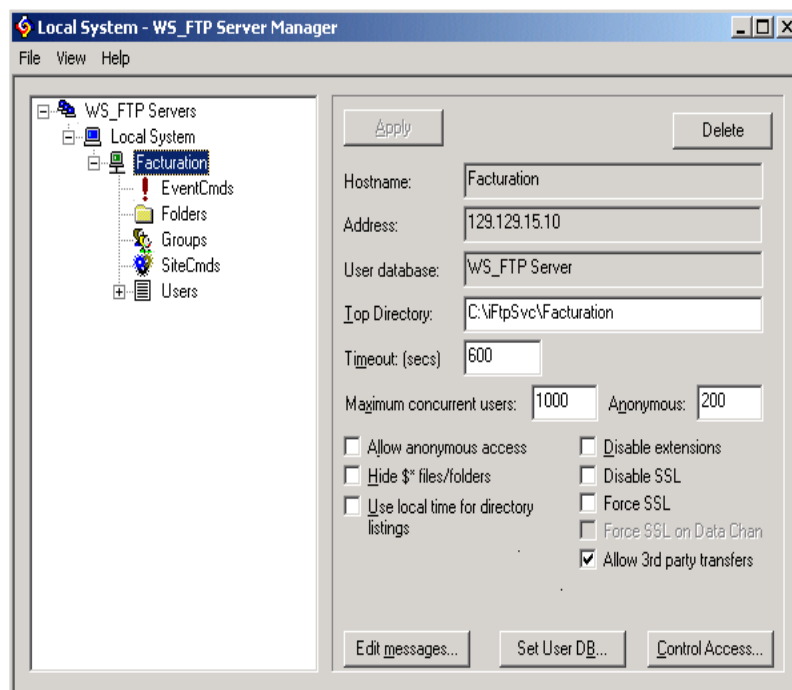
Après qu'un utilisateur entre, leur accès au système de fichiers des centres serveurs de ftp est déterminé par des permissions assignées.

- **Dispositifs principaux :**

Le serveur de WS_ftp fournit les dispositifs principaux suivants:

- Soutient tous les clients de ftp d'enchaînement qui se conforment aux normes dans RFC 959 et 1123.
- Soutient les centres serveurs multiples de ftp (sites) sur un PC simple.
- Soutient les raccordements (SSL) bloqués de sorte que toutes les données transférées à et du serveur puissent être chiffrées.
- Emploie une base de données existante d'utilisateur pour l'autorisation d'utilisateur.
- Capacité de contrôler à distance de serveur.

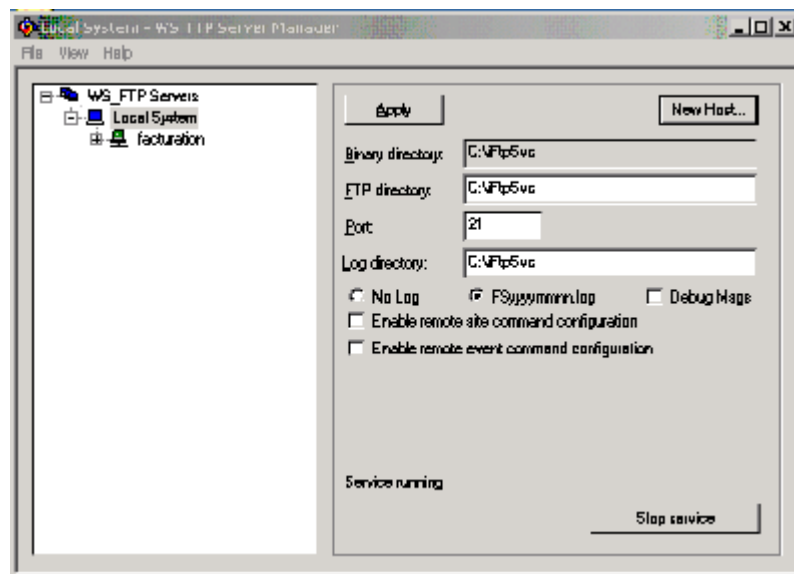
- **Interface d'administration de serveur FTP :**



- **Configuration**

Pour placer les options de la configuration de serveur WS_FTP :

- Dans le panneau gauche, il faut choisir « Local System ». Les propriétés locales de système apparaissent dans le panneau droit.



Les propriétés locales de système montrent les annuaires principaux pour le serveur WS_ftp.

Annuaire binaire(Binary directory) : Dans lequel le service FTP est installé.

Annuaire de FTP(FTP directory) : Sous lequel les annuaires pour chaque centre serveur FTP apparaîtront.

Annuaire de notation : Si la notation est permise, des dossiers de notation sont placés dans cet annuaire.

Aucune notation : Des événements de serveur ne seront pas notés.

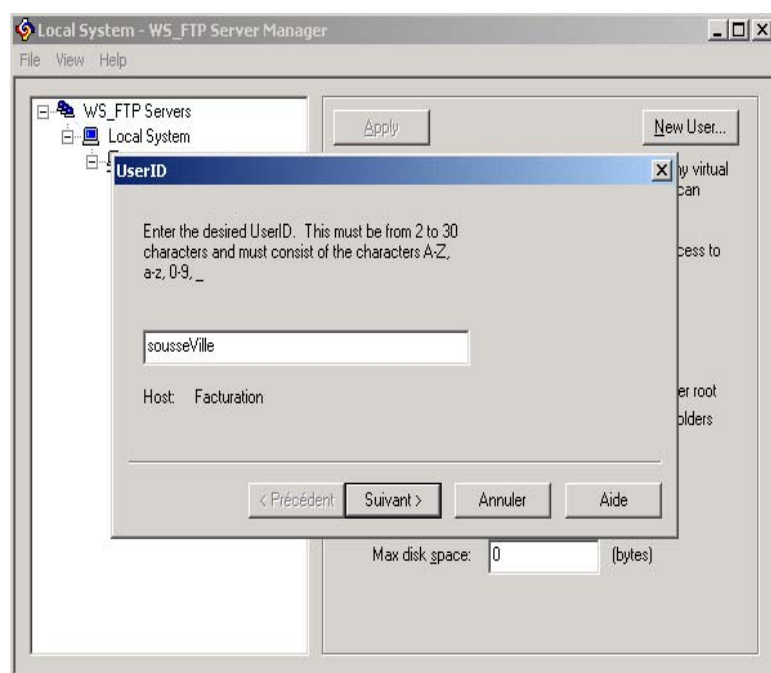
Fsyyymmmn.log : Des événements de serveur pour tous les centres serveurs sont notés à ce dossier.

L'option de **Msgs de correction** permet d'ajouter des informations plus détaillées à la notation.

- **Fonctions :**

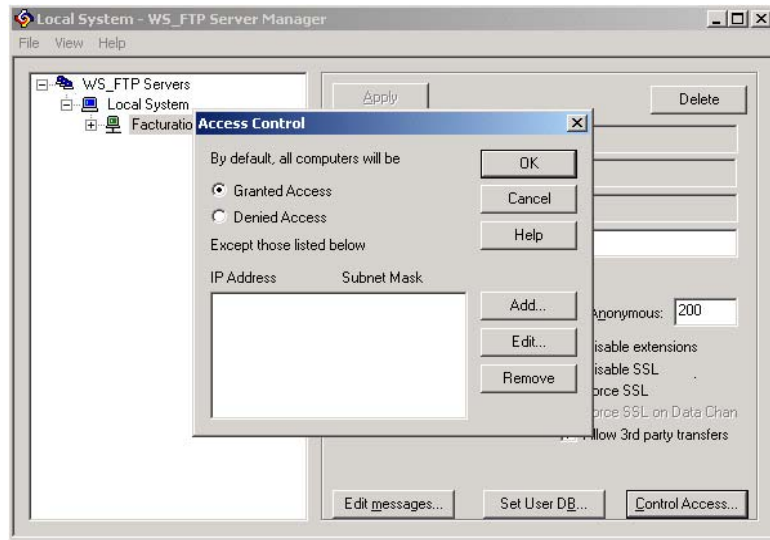
- Gestion des utilisateurs

Pour identifier les utilisateurs de WS_FTP Server, on clique sur « WS_FTP Server », « Users » puis « New User ». Le premier écran du magicien d'utilisateur apparaît :



- Gestion de la sécurité

L'accès à un centre serveur ftp est assuré en plaçant un IP ADDRESS ou une gamme des adresses pour lesquelles le centre serveur ftp accorde ou nie l'accès.



4.3.7 Installation et paramétrage de PCANYWHERE

- **Description générale**

PC Anywhere est un logiciel de télémaintenance qui va permettre aux administrateurs de prendre le contrôle de serveurs et des PCs pour résoudre plus rapidement les problèmes de maintenance. C'est la solution de télé intervention et de transfert de fichiers la plus sécurisée du marché. Il nous permettra aussi de transférer rapidement les fichiers quel que soit le système d'exploitation utilisé.

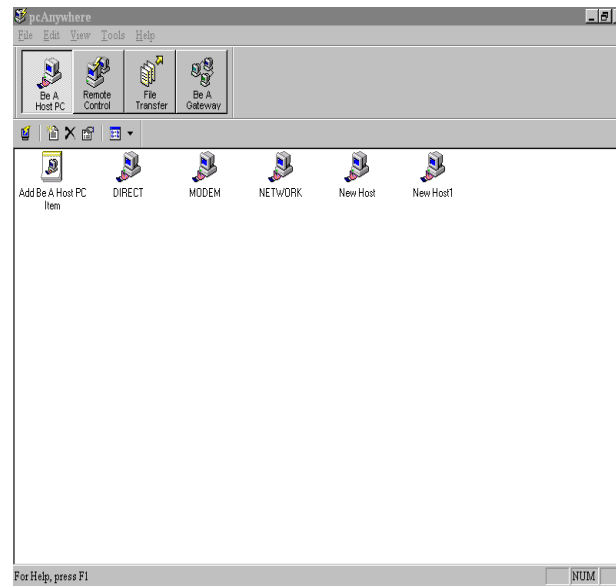
Le logiciel PC anywhere renforce la sécurité, accroît le débit de transfert de fichiers et optimise les fonctions de personnalisation.

- **Installation de PC anywhere**

L'installation de PC anywhere est utilisée sur deux ordinateurs : un Elève et un Maître.

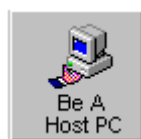
● Configuration de logiciel

Lors de premier démarrage après installation, le logiciel PC anywhere nous présente l'écran comme suit :



❖ Configuration PC anywhere Elève

Pour créer un élément de connexion Etre un Elève (Be A Host PC), on clique sur le bouton d'action «Be A Host PC» et poursuit la procédure correspondante.



❖ Configuration PC anywhere Maître

La technique de télé intervention permet à un PC Maître de se connecter à un PC Elève et d'utiliser ce dernier comme si l'utilisateur se trouvait sur le site de l'Elève.

Pour créer un élément de connexion, on clique sur le bouton «Remote Control » et on poursuit la procédure de la configuration.

4.3.8 Installation et paramétrage de Firewall Tiny Personnel Firewall

- **Description du logiciel**

Tiny Personal Firewall est un pare-feu personnel (donc un logiciel dont l'utilisation est prévue pour des particuliers) permettant de protéger une machine en réseau.

Ce pare-feu propose trois modes de sécurité :

- Cut me off (traduisez "me déconnecter"): Permettant de déconnecter temporairement l'ordinateur du réseau.
- Ask me first (traduisez "me demander d'abord"): le logiciel demande l'avis de l'utilisateur (accepter ou refuser la connexion) à chaque fois qu'un trafic inconnu est détecté.
- Don't bother me (traduisez "ne pas m'ennuyer"): le logiciel laisse passer le trafic inconnu

Le firewall Tiny personal firewall permet en outre:

- De protéger l'accès à la configuration et au logs (fichiers journal) à l'aide d'un mot de passe.
- D'administrer la machine à distance (de façon optionnelle).
- De créer une somme de contrôle (MD5) pour chaque application. Ainsi lorsqu'une application sera modifiée, le logiciel en avertira l'utilisateur et redemandera confirmation.
- De définir les adresses IP des machines autorisées à se connecter.
- De contrôler les accès selon des règles horaires.
- Des alertes en cas de tentatives de connexion extérieures.

- **Installation de Tiny Personal Firewall**

L'installation du logiciel est très simple : il faut dans un premier temps se procurer la version de Tiny personal firewall la plus récente et ce, par téléchargement du réseau internet. Il suffit ensuite d'exécuter l'application et de suivre les étapes d'installation. Après installation, le logiciel demande de redémarrer la machine.

- **Configuration de Tiny personal firewall**

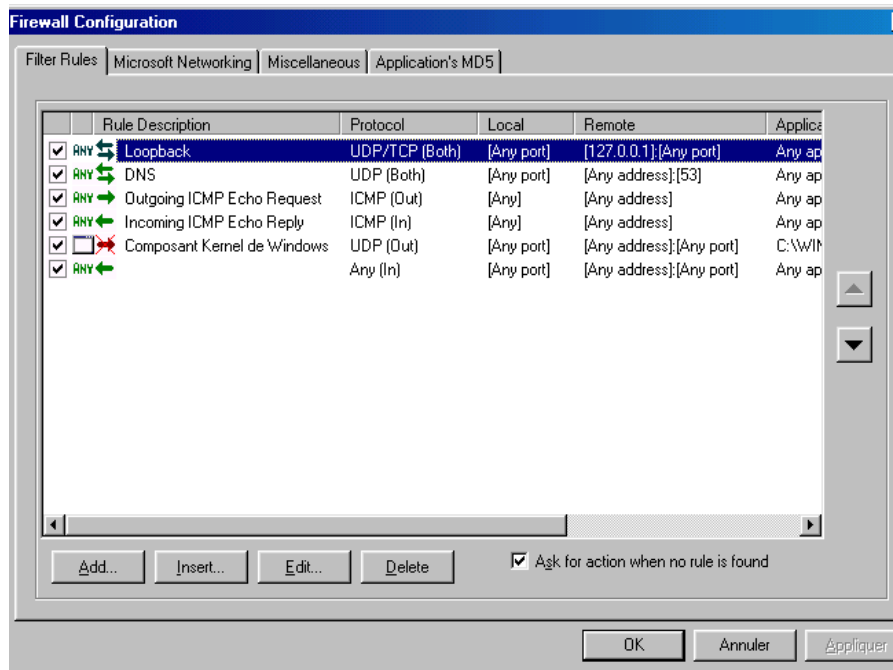
Lors du premier démarrage après installation, le logiciel Tiny personal firewall nous présente cet écran



On a ainsi assuré qu'aucune information ne peut sortir du système sans autorisation. La case à cocher en bas de page (**create appropriate filter rule and don't ask me again**) permet de créer une règle de filtrage appropriée sans répétition de la demande d'une même application.

Les règles de filtrage

Tiny Personal Firewall permet de définir précisément les règles de filtrage à l'aide de l'interface de configuration avancée du firewall:



L'interface présente l'ensemble des règles ayant été définies par l'utilisateur. Chaque ligne représente une règle de filtrage définie par :

- Une description, accompagnée d'un symbole :
 - ➡ Ce symbole représente une communication sortante autorisée.
 - ← Ce symbole représente une communication entrante autorisée.
 - ↔ Ce symbole représente une communication bidirectionnelle autorisée.
 - ✖ Ce symbole représente une communication sortante interdite.
 - ✖ Ce symbole représente une communication entrante interdite.
 - ✖ Ce symbole représente une communication bidirectionnelle interdite.
- Le ou les protocoles concernés (UDP, TCP, ICMP, ...)
- L'adresse IP et le port local concernés
- L'adresse IP et le port distant concernés
- L'application concernée

Le bouton **Add** permet d'ajouter une règle à la suite des règles déjà définies.

Le bouton **Insert** permet d'insérer une règle après la règle sélectionnée.

Le bouton **Edit** permet d'éditer la règle sélectionnée.

Le bouton **Delete** permet de supprimer la règle sélectionnée.

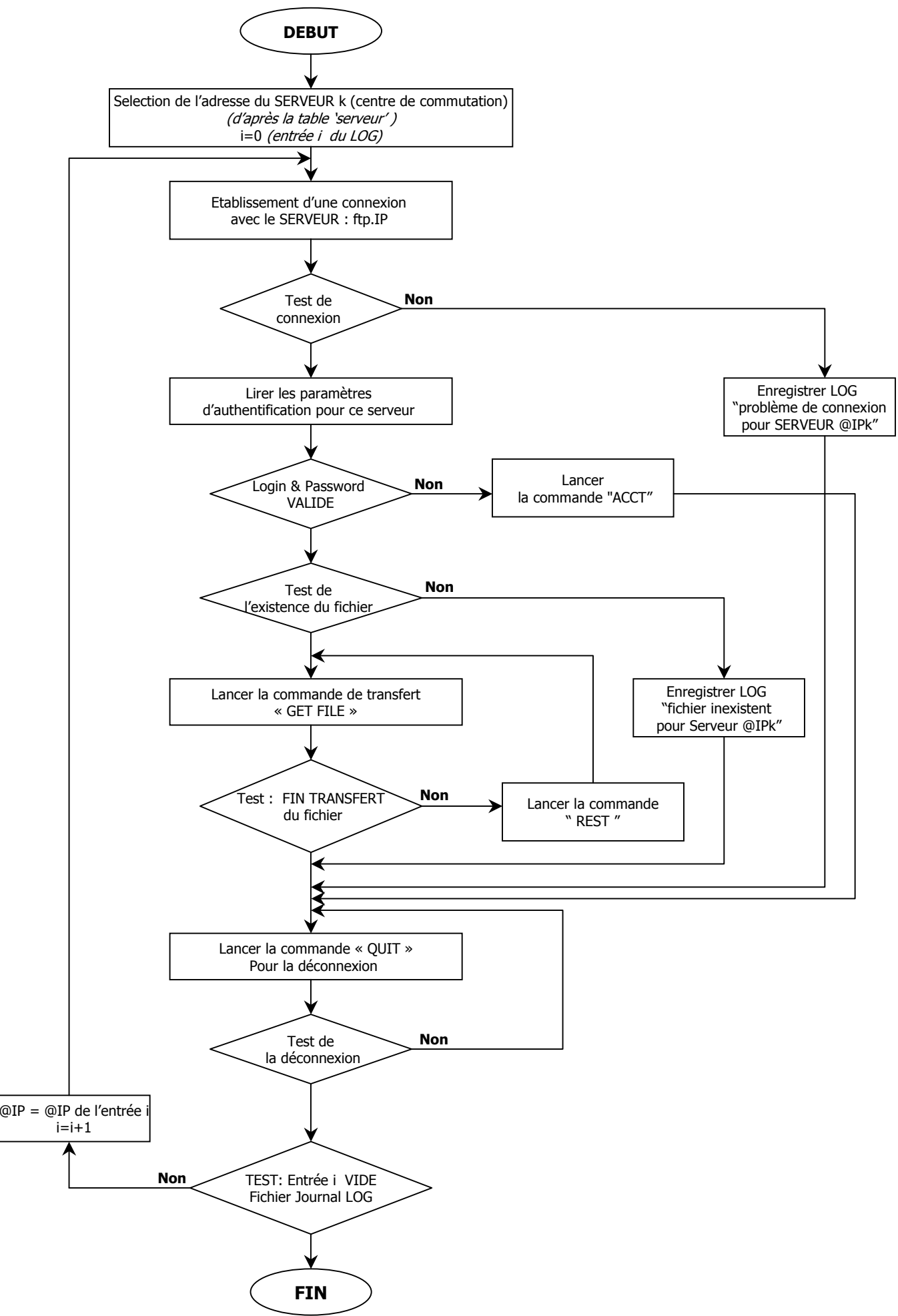
4.4 Conclusion

L'idée d'implémenter des logiciels d'administration, de maintenance et de sécurité du réseau vient de fait que le transfert de données de taxation entre le client et le serveur nécessite une grande performance.

Néanmoins des améliorations pourront avoir lieu au niveau du logiciel plus développé notamment l'implémentation de logiciel de gestion du réseau informatique HP-OpenView.

HP-OpenView est une solution complète de gestion de systèmes distribués qui offre un environnement de base sur lequel tournent toutes les applications de gestion. Un ensemble de services permet à l'administrateur de planifier, de gérer l'adressage, de surveiller et de contrôler son environnement.

Le coût élevé de ce logiciel présente le principal obstacle qui nous empêche de l'implémenter dans notre solution.



CONCLUSION ET PERSPECTIVES

Notre idée était essentiellement de concevoir des solutions pragmatiques, exploitables, de nouvelles technologies et surtout qui respectent les normes en vigueur..

D'une manière générale, la mise en œuvre d'une solution pour les réseaux de télécommunication, qui se caractérisent par l'hétérogénéité de leurs équipements de commutation, systèmes d'exploitation, protocoles de communication, doit passer par plusieurs étapes afin de bien répondre à l'ensemble des spécifications exigées par l'opérateur et garantir la pérennité de la dite solution.

Nous donnons, ici, notre approche qui a été appliquée durant le présent travail :

- ***Etape 1 :*** Etudes du préalable : elle concerne toutes les activités d'identification du besoin, l'étude ainsi que l'évaluation de l'existant ;
- ***Etape 2 :*** : Choix et décision : elle a pour principal but de concevoir les solutions moyen et long termes qui répondent le mieux aux préoccupations de l'opérateur ;
- ***Etape 3 :*** : Implémentation de la solution : elle correspond à la mise en place d'une solution transitoire dite aussi à court terme ;
- ***Etape 4 :*** phase finale : c'est l'étape qui se caractérise par une cohabitation entre la solution transitoire et les solutions projetées. La fin de cette étape est marquée par l'arrêt de la solution transitoire et le passage aux solutions de moyen/long terme.

Ce travail, objet de notre projet de fin d'études, a porté sur la conception et la réalisation d'un système de gestion des données de taxation à base de protocole FTAM comme solutions à moyen et long terme et la mise en place d'un système de collecte des données de taxation le transfert automatique de ces données par le biais d'un protocole simple : Le protocole FTP et ce, dans un environnement répondu qui est le TCP/IP.

Suite à notre travail, nous pouvons conclure que ce projet était la bonne occasion pour acquérir des nouvelles connaissances théoriques et pratiques de grandes valeurs essentiellement dans le domaine de la gestion des réseaux informatiques.

Par ailleurs, ce projet nous a permis d'apprendre et manipuler des notions avancées sur :

- les logiciels et protocoles de gestion et télémaintenance :PC-ANYWHERE, SNMP, ...
- les protocoles de communication, de transfert de fichiers, de routage comme : FTP, FTAM...

Le développement de notre application avec un langage de programmation orienté objet à savoir « Visual Basic 6.0 », nous a permis de consolider nos connaissances en matière d'algorithmique et développement informatique.

En ce qui concerne les perspectives de notre travail, sa continuation devrait aboutir à un protocole de gestion plus riche et plus fiable que le protocole SNMP, il s'agit du protocole CMIP.C'est un protocole normalisé ISO, de communication entre gestionnaire et agents et qui est utilisé essentiellement pour l'administration des réseaux de grand taille comme les réseaux de télécommunication.

BIBLIOGRAPHIE

Livres :

- [1] H.Nussbaumer, TELEINFORMATIQUE IV, Presses polytechniques romandes, Lausanne, 1991.
- [2] J.Pierre et M.Claude, GESTION DES RESEAUX INFORMATIQUES, édition EYROLLES 1993.
- [3] D.Comer, TCP/IP, ARCHITECTURE, PROTOCOLES, APPLICATIONS, Inter Editions 1998.
- [4] O.Cherkaoui, TELEINFORMATIQUE, édition 1998.
- [5] J.Sehan, VISUAL BASIC 6, édition DUNOD 1999.
- [6] P.Wright, VISUAL BASIC 6, édition EYROLLES 1998.
- [7] Daylas E.Comer, RESEAUX ET INTERNET, Compus Press 2000, Paris.
- [8] David J.Stang, SECURITE RESEAUX , Dunod 1994, Paris.

Mémoires de fin d'études :

- [9] Abdelkhalek MANSOUR, conception et modélisation d'une MIB-RGT, ESPTT 1996.
- [10] Batti LARBI, téléchargement de fichiers, ESPTT 1994.

Sites Internet :

- [11] <http://www.guill.net/>
- [12] <http://www.ipswitch.com/support/WS-ftpserver/guide/v3/index.html>
- [13] <http://www.normos.org/ietf/rfc/rfc1415.txt>
- [14] <http://www.commentcamarche.net>

GLOSSAIRE

-A-

ARP : Adresse Resolution Protocol : méthode de résolution d'adresses physiques qui assure la correspondance adresse IP/adresse physique.

ARPA: Advanced Research Projects Agency.

ASCII : (Américain Standard Code for Information Inter change), c'est un ensemble de codes allant de 0 à 255 attribués à des lettres dans un but de normalisation.

ASN.1 : Abstract Syntax Notation : Un langage qui peut servir de définir la structure des données.

Authentification : Dans un environnement réseau ou Multi-Utilisateur, processus selon lequel le système valide les informations d'ouverture de session d'un utilisateur. Le système vérifie le nom et le mot de passe utilisateur par rapport à une liste d'autorisation et s'il détecte une correspondance, autorise l'accès.

-C-

Clef de Session : est la clef de session ce qui le client et le serveur emploient pour chiffrer des données. Elle est crée par le client.

Clef Publique : La clef publique est le dispositif avec lequel le client chiffre une clef de session. Elle n'existe pas comme dossier, mais est un sous-produit de la création d'un certificat et d'une clef privée. Des données chiffrées avec une clef publique peuvent seulement être déchiffrées par la clef privée qui l'a faite.

Clef Privée : La clef privée déchiffre la clef de la session du client qui est chiffrée par une clef publique. Le dossier principal privé a la fin de key. Des clefs privées devraient ne jamais être distribuées à n'importe qui.

Client : Micro-ordinateur capable d'utiliser les ressources partagées sur le réseau par d'autres ordinateurs appelés serveurs.

Communication à distance : Dialogue entre un ordinateur Maître et un Elève par l'intermédiaire d'une connexion téléphonique ou autre ligne de communications.

-D-

DTP : Data Transfer Processus, chargé d'établir la connexion et de gérer le canal de données.

Elément de connexion : Fichiers représentés par une icône et un nom. Ces fichiers contiennent des informations sur la connexion, telles que le périphérique utilisées et les commandes ou options utilisées au cours d'une session.

-F-

FADU: File Access Data Unit.

FERPM: FTAM File Error Protol Machine.

FTAM: File Transfer Acces and Management, élément de service d'application de transfert, accès et gestion de fichiers. Il est normalisé par l'ISO.

FTP: File Transfer Protocol, programme utilisé sous TCP/IP pour permettre le transfert de fichiers entre deux ordinateurs. Utilisé sous Internet pour naviguer et télécharger des fichiers.

-H-

Hétérogène : Système constitué de composants qui ont des caractéristiques techniques différentes et/ou provenant de divers fournisseurs.

HUB : C'est un boîtier électronique qui collecte et concentre les informations de plusieurs micros et permet une organisation physique plus efficace.

-I-

ICMP : Internet Control Message Protocol.

IP : Protocole Internet : Couche réseau pour l'ensemble de protocole TCP/IP, fréquent utilisée sur les réseaux Ethernet. Cette couche est un protocole de commutation par paquet optimisé sans connexion.

ISO : Organisme International dépendant de l'ONU chargée de la normalisation. Il regroupe les instituts nationaux de 89 pays qui sont répartis en 72 comités membres. Les résultats de travaux techniques de l'ISO sont publiés sous la forme de normes internationales.

-L-

LAN : Local Area Network, technologie définissant un réseau local.

Modem : Modulation/Démodulation, boîtier ou carte interne permettant le transfert des informations entre deux ordinateurs par le réseau téléphonique. Le rôle principal étant d'adapter et transformer les signaux numériques en signaux analogiques.

-M-

MAN : Metropolitan Area Network, ce type de réseaux est récent et garde les avantages des LAN sur de plus longues distances de l'ordre de la ville.

MIB : Management Information Base.

-N-

NMP: Network Management Protol.

Nœud : Ordinateur connecté au réseau(serveur ou station de travail). Egalement appelé « poste de travail ».

-O-

Open View : est la stratégie adoptée par Hewlett Packard pour gérer des réseaux informatiques constitués de matériels hétérogènes.

OSI : Open System Interconnexion, ensemble des normes d'interconnexion des systèmes ouverts définis par l'ISO pour faciliter la constitution de réseaux et d'applications multiconstructeurs. Le modèle OSI est structuré en 7 couches principales.

-P-

PI : Protocol Interpreter, est l'interpréteur de protocole permettant de commander le DTP à l'aide des commandes reçues sur le canal de contrôle.

PPP : Point to Point Protocol, protocole de connexion sur le réseau téléphonique via TCP/IP.

Protocole : Ensemble de règles définissant la façon que les informations peuvent être reçues ou transmises par un système.

-Q-

QUIT : Commande FTP permettant de terminer la session en cours. Le serveur attend de définir le transfert en cours le cas échéant, puis de fournir une réponse avant de fermer la connexion.

-R-

RARP: Reverse Adresse Resolution Protocol, assure la connexion adresse physique/adresseIP.

RAS : Remote Access Service(service d'accès distant), connexion au cours de laquelle un PC appelle un serveur et se comporte comme une station de travail locale sur ce réseau.

REST : Restart, c'est l'une des commandes de paramètres de transfert qui permet de reprendre un transfert là où il s'était arrêté. Pour cela cette commande envoie en paramètre le marqueur représentant la position dans le fichier à laquelle le transfert avait été interrompu.

RFC: Request For Comments.

RTC: Réseau Téléphonique Commuté, lignes téléphoniques classiques qui forment le réseau public des télécommunications.

-S-

Serveur : micro-ordinateur exécutant le logiciel réseau et mettant ses ressources à la disposition des postes clients. On parle de serveur d'impression, de serveur de fichiers ou de serveur d'applications.

SNMP : Simple Network Management Protocol.

Socket : C'est une interface de programmes d'application pour les réseaux TCP/IP, elle définit un ensemble de fonctions logicielles ou routines qui permettent au programmeur de développer des applications pour TCP/IP.

SSL : Secure Sockets Layer, norme extensible développée par Netscape communications pour l'établissement d'un canal de communication sécurisé sous TCP/IP. Cette technologie, qui utilise un encodage à clé publique, est incorporée dans plusieurs navigateurs et serveurs Web.

-T-

TCP/IP : Transmission Control Protocol/Internet Protocol, protocole utilisé sur les réseaux grande distance comme Internet.

Telnet : c'est un service de connexion à distance émulant un terminal virtuel.

Télémaintenance : Contrôle d'un PC Elève à partir d'un PC Maître.

-U-

UDP : User Datagram Protocol, fonctionne en mode non connecté et ne fournit pas des liaisons successives.

-W-

WAN : Wide Area Network, réseau généralement composé de lignes série et s'étendant sur des distances supérieures à un Kilomètre.

WS: Work Station.

Conception et Réalisation d'un Système de Gestion des Données de Taxation à Base du protocole FTAM

**Réalisé par
Zakia ESSID & Sana ELMESTIRI
TS-5 Commutation**

Résumé :

Le présent mémoire a porté sur l'étude et la réalisation d'un système de gestion des données de taxation à base du protocole FTAM. Ces données sont localisées au niveau de plusieurs sites de commutation, qui sont réparties au niveau du réseau des télécommunications de l'office national des télécommunications « TUNISIE TELECOM ».

Ce projet vise à moderniser le processus de taxation et de la facturation des abonnés. En effet, et à fin d'améliorer ce processus, on a conçu et réalisé un système de gestion des données de taxation qui assure le transfert automatique basé sur le réseau de commutation par paquets X25 comme support de transfert, le modèle client/serveur sous TCP/IP et le protocole SNMP pour la gestion et l'administration d'information.

En ce qui concerne les perspectives de notre travail, sa continuation devrait aboutir à un système d'administration à base de protocole normalisée ISO : CMIP.

Mots clés : données de taxation, transfert automatique, FTAM, FTP sécurisé, Client/Serveur, administration, SNMP.