MINISTERE DES ENSEIGNEMENTS SECONDAIRE,
SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE POLYTECHNIQUE
DE BOBO-DIOULASSO

ECOLE SUPERIEURE D'INFORMATIQUE
01 BP 1091, Tél. (226) 97 27 64
BOBO-DIOULASSO

MINISTERE DE L'ECONOMIE ET
DES FINANCES

SECRETARIAT GENERAL

DIRECTION DES SERVICES
INFORMATIQUES
BP 80, Tél. (226) 32 49 99
OUAGADOUGOU

Mise en place d'un Intranet au Ministère de l'Economie et des Finances

MEMOIRE DE FIN D'ETUDES

présenté et soutenu publiquement le 05 Janvier 2001

pour l'obtention du

Diplôme d'ingénieur de conception en informatique

par

Moussa DAVOU

Composition du jury :

Président :	Pr. Théodore TAPSOBA
Rapporteur :	M. Ali B. KABA
Examinateurs :	M. Mesmin T. DANDJINOU, directeur du mémoire
	M. Kisito TRAORE, maître de stage
	M. Mamadou PORGO, invité

Année Universitaire 1999/2000

SOMMAIRE

DEDICACE

Mes pensées vont droit à mon père et à ma mère, qui m'ont donné la vie et qui m'ont apporté les soutiens nécessaires à ma bonne éducation et à mes succès scolaires, au prix de nombreux sacrifices. Qu'ils trouvent ici l'expression de mon entière reconnaissance.

Je dédie le présent mémoire à mon petit frère, benjamin de ma famille, pour qui la carrière scolaire ne fait que commencer. Je lui souhaite beaucoup de courage et un parcours meilleur.

Moussa

INTRODUCTION

Les élèves-ingénieurs de conception en Informatique en fin de cycle à l'Ecole Supérieure d'Informatique de l'Université Polytechnique de Bobo-Dioulasso doivent réaliser un projet qui consiste en la résolution d'un problème scientifique et technique. Ce travail doit être l'occasion pour l'élève de mettre au service d'un organisme public ou privé une démarche synthétique, faisant intervenir tout ou partie des connaissances qui lui ont été enseignées au cours de sa formation. La période de mémoire est divisée en deux parties : une première partie qui se déroule à l'école parallèlement aux cours théoriques et pendant laquelle l'étudiant est supposé faire des recherches bibliographiques concernant son thème de mémoire et une deuxième partie qui se déroule au sein de l'organisme concerné par le thème de mémoire. C'est pendant cette seconde partie que l'étudiant procède à la réalisation concrète du travail qui lui est demandé.

Le thème du travail qui nous a été confié est « Mise en place d'un Intranet au Ministère de l'Economie et des Finances (MEF)».

Après l'ère de la productivité individuelle et l'explosion, dans les années 80, du marché du PC, nous entrons de plein pied dans l'ère du réseau et de la productivité de groupe. Mettant en œuvre les technologies et les infrastructures de l'Internet dans l'entreprise, les Intranets suscitent un réel intérêt depuis quelques temps. Les administrations publiques ou privées cherchent à se restructurer et à réorganiser leurs modes de communication et de travail que ce soit en interne ou avec leur environnement. Au regard de son importance, la réalisation d'un tel projet nécessite la définition de stratégies techniques et des niveaux techniques d'appréhension relativement élevés.

C'est certainement ce qui a motivé la Direction des Services Informatiques du MEF à nous confié ce travail que nous avons réalisé sous la supervision de Monsieur Kisito TRAORE, maître de stage et de Monsieur Mesmin DANDJINOU, directeur du mémoire.

Notons qu'une première appréhension du problème a été effectuée lors du stage industriel de deuxième année du cycle des ingénieurs de conception en informatique. Au regard de l'évolution du système informatique du MEF avec de nouvelles contraintes, une étude conceptuelle détaillée a été nécessaire avant la phase d'implémentation. Ce document, après avoir présenté le concept d'Intranet et les fonctionnalités attendues de l'Intranet du MEF, s'attarde sur la partie conceptuelle qui présente une étude comparative des solutions techniques envisageables, détaille la solution proposée (architecture, besoins matériels et logiciels, sécurité, évaluation financière) et propose une démarche de mise en œuvre. La deuxième partie du document, celle de l'implémentation, présente les réalisations pratiques effectuées et les directives d'exploitation.

I. DESCRIPTION DE L'ENVIRONNEMENT

1.1. Missions et organisation de la Direction des Services Informatiques

La Direction des Services Informatiques (DSI) est l'organe exécutif du Schéma Directeur Informatique (SDI) au sein du Ministère de l'Economie et des Finances (MEF). Elle est chargée de la résolution de toutes les questions informatiques au sein du MEF. Elle est rattachée au Secrétariat Général du MEF et a pour missions principales de

- veiller au bon déroulement du SDI conformément aux directives établies,
- rechercher les solutions de réalisations des projets,
- veiller à la cohérence du système d'information du MEF,
- assurer et/ou coordonner les actions de formation et de développement.

La DSI comprend trois services :

- Le Service Etudes et Applications qui a un rôle essentiellement conceptuel est responsable de l'analyse des besoins des utilisateurs et de la réalisation des applications informatiques ;
- Le Service Réseaux et Systèmes qui a un rôle actif sur le terrain assure le fonctionnement quotidien du réseau et du système d'information du MEF en vue d'une prestation de qualité aux utilisateurs ;
- Le Service Equipement et Support Technique qui est chargé de la gestion du matériel informatique et de la formation des utilisateurs.

Chacun de ces services a un responsable qui coordonne toutes les activités du service et qui dirige l'équipe de travail (*cf. Organigramme en Annexe 6*).

1.2. Système informatique existant

Le MEF dispose d'un parc informatique très important d'environ

- 850 PC,
- 528 imprimantes,
- 379 onduleurs,
- 71 terminaux,
- 14 serveurs.

Ce parc est réparti dans les différents bâtiments du MEF (sur plusieurs sites géographiques). Dans la plupart de ces bâtiments est installé un réseau local de type Ethernet, câblés selon la norme 802.3, avec pour support la paire torsadée non blindée (UTP) de catégorie 5, soit une quinzaine de réseaux locaux. Tous ces réseaux ont été interconnectés entre eux par la fibre optique du RESINA (cf. 1.3) et constituent donc un même et grand réseau pour le MEF. Les liaisons sont faites via un commutateur Ethernet fibre optique. Tous les bâtiments du MEF abritant un réseau local disposent d'une alimentation électrique sécurisée (onduleurs ou groupes électrogènes).

Pour l'exploitation de ce patrimoine informatique, la Direction des Services Informatiques utilise les systèmes d'exploitation suivants : MS-DOS et Windows (*Windows 3.11, Windows 95, Windows 98, Windows 2000, Windows NT*) pour les postes de travail, Netware de Novell (*versions 4.11, 4.2 et 5*) et Windows NT pour son réseau.

Notons par ailleurs que le MEF dispose d'un nombre relativement important d'applications utilisées, soit de façon privée et spécifique au MEF, soit en interne et en externe par des utilisateurs d'autres institutions. On distingue des applications comptables (par exemple l'application CIE - *Comptabilité Intégrée de l'Etat*), des applications soldes (par exemple l'application SIGASPE – *Système Intégré de Gestion Administrative et Salariale du Personnel de l'Etat*), des applications budgétaires comme le circuit informatisé de la dépense publique et bien d'autres. La plupart des applications ont été développées sous Foxpro et Oracle 7 (Developper 2000, Designer 2000). Néanmoins, quelques petites applications ont été développées sous Visual Basic et Dbase.

Remarque : Aucun des réseaux locaux du MEF ne dispose d'une connexion permanente à l'Internet. Dans certains bâtiments, la connexion se fait par RTC via le serveur de la DELGI et le nombre de postes y accédant est très limité. Les coûts (facturation téléphonique) sont alors élevés sans pouvoir fournir un accès large et permanent aux usagers.

1.3. Réseau Inter-Administratif (RESINA)

Le RESeau INter-Administratif (*RESINA, voir Schéma synthétique en Annexe 2*) de Ouagadougou est un grand réseau informatique reliant les bâtiments administratifs de Ouagadougou (dont les bâtiments du MEF). L'architecture de ce réseau métropolitain est constituée d'un double anneau sécurisé FDDI à 100 Mbps. L'anneau comprend une boucle FDDI primaire et deux boucles FDDI secondaires. Sur cet anneau sont raccordés les réseaux des administrations qui ont un serveur nécessitant un accès rapide et une haute disponibilité. Les bâtiments qui abritent ces serveurs sont classés sites de catégorie A (haut débit). Les autres bâtiments sont classés sites de catégorie B (moyen débit). Les bâtiments de catégorie B (bâtiments secondaires) sont liés en étoile aux bâtiments de catégorie A (bâtiments principaux) par des liaisons à 10 Mbps.

Le support physique de l'anneau FDDI ainsi que de toutes les autres liaisons inter- bâtiments est en fibre optique. Les interconnexions ont été effectuées en utilisant les conduits de l'ONATEL et creusant de nouveaux conduits. A l'intérieur de tous les bâtiments est installé un réseau de type Ethernet avec un câblage en paires torsadées non blindées de catégorie 5.

Le RESINA concerne toutes les Directions des Affaires Administratives et Financières (DAAF) des départements ministériels et institutions, toutes les Directions des Ressources Humaines (DRH) des différents Ministères et Institutions, les Directions des Etudes et de la Planification (DEP) situées dans le même bâtiment que la DAAF ou la DRH et tous les services du Ministère de l'Economie et des Finances.

1.4. Réseaux des Trésoreries Régionales et Principales

La Direction des Services Informatiques a commencé une opération de mise en réseau du patrimoine informatique disponible dans les Trésoreries Régionales (dans cinq provinces). Ainsi certaines Trésoreries Régionales (Bobo-Dioulasso, Fada) disposent déjà d'un réseau local type Ethernet avec un câblage en paires torsadées non blindées (UTP) catégorie 5. Toutes ces Trésoreries Régionales devront être reliées au grand réseau du MEF fonctionnant sur RESINA à travers des lignes spécialisées. Le point de jonction est le bâtiment de la DGTCP. Les équipements d'interconnexion (routeurs) sont déjà disponibles et la procédure de réalisation des interconnexions pour les réseaux de Trésoreries Régionales entièrement câblés est en cours. Le câblage réseau des autres Trésoreries Régionales (Kaya, Koudougou, Ouahigouya) est diligemment envisagé.

Par ailleurs, les réseaux des Trésoreries Principales, lorsque celles-ci seront entièrement câblées, devront être reliés aux réseaux de leurs différentes Trésoreries Régionales par des lignes spécialisées.

Ainsi, à la fin de cette opération le MEF disposera d'un réseau national à support hétérogène (*cf. Annexe 3*) qui devrait permettre aux agents de travailler en parfaite collaboration avec une certaine synergie et augmenter la productivité d'ensemble.

Dans le cas de la présente étude, nous prenons l'hypothèse que les différentes Trésoreries Régionales et Principales sont entièrement câblées et reliées au réseau global de Ouagadougou via le bâtiment de la DGTCP. La solution technique proposée tiendra compte de ces interconnexions.

II. PROBLEMATIQUE

Notre époque est dominée par des phénomènes tels le changement permanent, la formation continue, l'accélération et la globalisation des activités humaines telles que l'économie, les finances, la production des biens, les services, la recherche, le commerce, etc. Le développement de la science et de la technologie informatique a été associée très étroitement à ces phénomènes. Pour assurer des services de qualité, les administrations publiques et privées développent des politiques s'inscrivant dans l'évolution de ce courant technico-professionnel. Une réorganisation interne des modes de communication interne et externe s'impose alors.

Pour ce faire, le MEF a souhaité, dans le cadre de l'exécution de son SDI révisé pour la période 1999 à 2001, la mise en place d'un Intranet qui devra permettre d'améliorer la communication informatique entre les usagers de cet outil informatique. Les agents du MEF devront pouvoir alors utiliser les outils de productivité de groupe pour communiquer en interne et/ou avec l'extérieur, accéder à des banques de données spécifiques stockées à leur intention, maintenir des postes de travail et applications distants à partir de leur poste, accéder à l'Internet de façon plus large et plus rationnelle. Cet Intranet a pour objectifs, entre autres, de répondre aux besoins fréquents exprimés par les agents de ce ministère, à savoir des besoins de :

- communication entre agents par l'usage de la messagerie électronique ;
- consultation de documents administratifs nécessaires aux activités professionnelles quotidiennes (décisions, arrêtés, pages web du MEF, ...) ;
- échanges de documents de types variés ;
- traitements sur machines distantes ;
- télémaintenance d'applications et de postes de travail ;
- utilisation de l'Internet (à des fins professionnelles).

En tenant compte du très important patrimoine informatique existant (*cf. sections 1.1, 1.2 et 1.3 vues précedemment*), de nouveaux changements intervenus au sein de ce patrimoine, de l'évolution future prévue pour ce parc (l'interconnexion des réseaux de Trésoreries Régionales et Principales, *cf. section 1.4*) et au regard de l'importance et de l'intérêt qu'accordent les futurs utilisateurs à cet Intranet, il nous a été demandé de faire une étude conceptuelle détaillée qui fera ressortir les matériels et logiciels nécessaires, l'investissement financier pour les acquérir, de proposer une architecture technique et de suggérer une démarche de mise en œuvre de l'Intranet du MEF. A l'issue de cette phase conceptuelle, interviendra une phase de réalisation au cours de laquelle l'on réalisera certains modules.

III. PRESENTATION DU CONCEPT D'INTRANET

3.1. Approche définitionnelle

L'Intranet est une notion récente, pas réellement homologuée et dont la (ou les) définition(s) demeure(nt) floue(s). Néanmoins, il existe des particularités spécifiques à l'opinion publique auxquelles toutes les définitions font appel.

Un Intranet est un réseau configuré en TCP/IP utilisant la technologie Internet au niveau de l'entreprise [EVANS 96]. On y retrouve le courrier électronique, le web, les services FTP, Telnet, News (nouvelles),... auxquels il faut ajouter les services de productivité de groupe (groupware) tels le workflow, les forums de discussion, la vidéoconférence, la gestion de base de documents... Il correspond à la mise en œuvre d'applications au sein d'une organisation (applications qui échangent des flux de façon interne). Le fait que les technologies Internet et Intranet soient identiques peut aboutir à des confusions. Techniquement parlant, le support d'un Intranet est un réseau privé, il a donc une existence physique sans nécessaire lien avec le réseau Internet.

Du fait qu'il soit un outil de travail (outil organisationnel car utilisé pour organiser et synchroniser les actions au sein de l'entreprise) et de communication, l'Intranet induit les problèmes de sécurité vis-à-vis de l'éventuelle confidentialité des travaux d'une entreprise. L'accès réservé et réglementé au réseau peut alors apparaître comme une composante de la définition d'un Intranet.

3.2. Intranet et Internet

Internet est défini par :

- une infrastructure mondiale d'interconnexion de réseau,
- des outils et protocoles (SMTP, HTTP/HTML, Java, TCP/IP...),
- des utilisateurs (par dizaines de millions),
- des services (Usenet, Telnet...),
- des informations.

Un Intranet reprend ces 5 composantes mais en s'appliquant sur un champ plus restreint.

INTERNET	INTRANET
Des infrastructures publiques de transmission de données (payées par les opérateurs Internet)	Des infrastructures privées de transmission de données (les réseaux locaux des entreprises concernées), Eventuellement l'utilisation de l'Internet comme un réseau étendu privé
Des outils et protocoles (les protocoles, langages et technologies de l'Internet)	Des outils et protocoles (une partie des protocoles, langages et technologies de l'Internet)
Des utilisateurs (une communauté ouverte, celle des internautes)	Des utilisateurs (une communauté identifiée)
Des services (ceux fournis par les utilisateurs et entreprises connectés à Internet)	Des services (ceux fournis par les utilisateurs et entreprises connectés à l'Intranet)
Des informations (celles produites par les utilisateurs de l'Internet)	Des informations (celles produites par les utilisateurs de l'Intranet)

Les deux différences fondamentales qui ressortent de cette comparaison sont :

- la population des utilisateurs qui est connue et identifiable pour l'Intranet,
- une plus grande maîtrise des infrastructures réseaux et du débit disponible.

S'il est difficile, sur l'Internet de s'assurer une bande passante constante du fait de la multiplicité des intermédiaires, sur un Intranet le réseau est administré et contrôlé par une seule entité. Il est donc plus facile d'envisager, sur un Intranet des applications qui restent difficiles à exploiter sur l'Internet, par exemple la visioconférence.

3.3. Services et fonctionnalités d'un Intranet

Un Intranet est constitué de services destinés aux utilisateurs finaux, aux équipes informatique et réseau. Il couvre une large palette des besoins de ces populations et propose généralement des services parmi les sept (7) suivants :

3.3.1. Les services de transport

Les services de transport permettent de véhiculer l'information d'un point à un autre d'un Intranet. Un Intranet s'appuie sur les mêmes protocoles de transport que ceux de l'Internet. Ces services sont :

- le transport sur un réseau local,
- l'accès à distance au système d'information : soit par un accès direct au système d'information, soit en utilisant l'Internet comme canal de transport,
- l'ouverture sécurisée sur l'Internet : permet aux utilisateurs d'accéder aux gigantesques ressources de l'Internet à travers des passerelles sécurisées pour assurer la confidentialité des informations de l'organisme,
- l'interconnexion LAN/WAN.

3.3.2. Les services d'administration

Un Intranet peut également comprendre des services d'administration et de gestion du réseau, les mêmes utilisés sur l'Internet. En général, trois (3) services sont mis en place :

- une plate-forme de supervision : permet de surveiller les entités du réseau (routeurs, imprimantes, logiciels ...). Elle s'appuie sur le standard SNMP (*Simple Network Management Protocol*) de l'Internet.
- une plate-forme d'administration et de télémaintenance : pour une prise de contrôle à distance. Elle utilise les protocoles tels que TCP/IP, PPP...
- des serveurs cache : permettent d'alléger les infrastructures télécoms en exploitant le principe de la localité : une «copie» des informations recemment accédées sur un serveur distant est conservée sur le serveur cache de sorte que les machines proches du cache n'aient pas à faire des requêtes individuelles vers le serveur distant. Il s'agit généralement de serveurs proxies comprenant un mécanisme de réplication sélective.

3.3.3. Les services de sécurité

Les services de sécurité sur un Intranet sont assurés par un mécanisme venant souvent de l'Internet. Trois services de sécurité sont au cœur d'un Intranet :

- l'authentification : s'appuie sur des mécanismes simples comme les mots de passe, ou des mécanismes plus sophistiqués de chiffrement.
- le chiffrement : évite que les messages et trames IP soient lus ou modifiés par des personnes non habilitées. Il peut se faire au niveau applicatif mais aussi au niveau des couches réseau (dans le routeur, par exemple).
- le filtrage des services, des adresses et du contenu : permet d'interdire ou autoriser un service quelconque pour une adresse IP, de filtrer le passage de ces adresses et le transport de fichiers par rapport à leur contenu. Ce service remplit les mêmes fonctions qu'un firewall.

3.3.4. Les services de partage de l'information

Ces services sont destinés à archiver et restituer les informations. Il existe deux types de services de stockages dans un Intranet :

- les services de stockage et d'accès :

- les serveurs de fichiers : sont les serveurs de fichiers classiques des systèmes d'exploitation utilisés. Sur un Intranet, le transfert de fichiers s'appuie le plus souvent sur une couche supérieure à celle du système de fichiers. Le protocole FTP (*File Transfer Protocol*) permet à deux postes d'un Intranet d'échanger des fichiers, indépendamment de leur système d'exploitation.
- les "serveurs de données" : les bases de données s'interfacent avec les serveurs web pour être consultées à l'aide d'un navigateur. Cet interfaçage nécessite souvent l'utilisation d'un logiciel spécifique (middleware).

- les serveurs de documents : sont des serveurs web parfois couplés à des moteurs de recherche documentaire, et à travers lesquels les utilisateurs accèdent aux documents de l'entreprise.

    - les services de production et de publication d'information : permettent à l'utilisateur d'adapter ses documents au standard de l'Intranet avec un minimum d'effort.

3.3.5. Les services de communication et de travail coopératif

L'organisme cherche à être plus réactif. Dans ce but, un Intranet offre généralement cinq (5) services favorisant la communication et le travail coopératif au sein de la société. Ces services sont :

- la messagerie et les listes de diffusion : la messagerie d'un Intranet s'appuie sur les mécanismes de l'Internet SMTP, POP3 et IMAP (*Internet Message Access Protocol*). Les logiciels de messagerie intègrent filtres de messages, gestion des pièces jointes, gestion des adresses Internet...
- la circulation de documents (workflow) : c'est une extension naturelle de la messagerie, elle permet de faire circuler un document selon un schéma préétabli. Il existe plusieurs catégories de circulation de documents, selon le parcours ou le type d'interaction entre les différents acteurs du processus.
- la visioconférence et l'audioconférence : elles ont été conçues pour un Internet où la bande passante est précieuse mais elles trouvent toute leur puissance sur un Intranet où le réseau est mieux maîtrisé.
- le travail coopératif en temps partagé : permet à plusieurs acteurs de travailler ensemble et à distance sur un même document.
- les forums : suivent de très près la messagerie ou le serveur web dans la construction d'un Intranet. Il existe deux types de forums : les forums interactifs en temps réel et les forums interactifs en temps différés.

3.3.6. Les services de développement applicatif

Langages de développement : permettent de développer des applications de production qui pourront être télé-distribuées et utilisées à l'aide d'un navigateur. Le langage privilégié est le langage Java (langage multi plate-forme, orienté objet, orienté réseau : les fonctionnalités d'une application programmée en Java sont chargées au moment de l'utilisation. L'application complète réside sur le serveur. Cela facilite la mise à jour de l'application en supprimant les problèmes de distribution sur le poste client).

Atelier de génie logiciel (AGL) : permet de construire ses propres applications Intranet. Ils sont de trois types : les AGL du monde Intranet qui intègrent Java et/ou CGI, les AGL client-serveur classiques et les AGL simples de développement.

3.3.7. Les services d'accès aux informations et aux applicatifs

Ces services se concentrent dans le navigateur. Ce "Client Universel" (le navigateur) permet d'accéder aux serveurs web, aux serveurs de fichiers ainsi qu'aux bases de données et aux applications développées dans des langages tels que Java. Il est d'utilisation très simple et va jusqu'à intégrer la messagerie et les forums. Il permet l'accès aux systèmes d'information de gestion et de production.

3.4. Avantages

La mise en place d'un Intranet présente plusieurs avantages. Nous en présentons ici quelques-uns uns :

- **sa facilité d'emploi** : l'utilisation d'un Intranet est quasi similaire à celle d'Internet. Les usagers du réseau mondial auront donc une facilité à parcourir le réseau, répondre à des formulaires, envoyer ou consulter des messages, naviguer sur un serveur web interne ;

- **son efficacité** : toute information modifiée sur un serveur est automatiquement mise à jour pour tous les utilisateurs. Des outils de recherche interne peuvent être mis à disposition afin de trouver des documents classés par thème, par mots clés, ou l'adresse et le numéro de téléphone d'une personne que l'on veut contacter... L'Intranet peut aussi créer une dynamique nouvelle dans l'entreprise en garantissant une communication quasi instantanée d'un utilisateur à un autre, même en manipulant de grands documents, des informations complexes...

- **la sécurité** : sur un réseau informatique de type Intranet, l'information doit être protégée. L'accès aux pages des différents services peut être verrouillé. Chaque personne sur le réseau possède un nom d'utilisateur et un mot de passe. Pour chacune de ces personnes, ou pour un groupe d'entre elles, il est possible de restreindre les données consultables, ou même de demander un mot de passe supplémentaire pour effectuer certaines requêtes. L'accès de l'extérieur est garanti par la mise en place de différents mots de passe, ou d'un firewall (*pare-feu*), qui est une barrière infranchissable pour toute personne non admise dans le système.

- **réduction des coûts** : les économies réalisées grâce à un Intranet sont principalement de deux (2) types :
  - ***la réduction des charges*** : l'utilisation d'un Intranet fait disparaître un bon nombre de procédures à support papier,

- le courrier interne, les informations, les notes de services, circulaires, ... pouvant être publiés directement sur le réseau au sein de l'entreprise et ce, de façon rapide et efficace ;
- les piles de documents administratifs ou formulaires qu'il faut imprimer, stocker et remplir ou faire remplir à la demande.

La réduction des frais d'imprimés est drastique, entre autres aussi par la mise sur le réseau des brochures internes, directement consultables, immédiatement remises à jour dès que c'est nécessaire. Plusieurs traitements administratifs répétitifs peuvent être réalisés automatiquement sur la base des informations reçues par l'utilisateur. Par exemple, transmettre des fax, centraliser et comptabiliser les inscriptions pour une réunion, un séminaire...

- ***augmentation de la productivité*** : la facilité d'utilisation et une application bien pensée permettent de réaliser certaines opérations (telles la diffusion d'informations, les échanges de courriers ou autres documents administratifs...) beaucoup plus rapidement qu'auparavant.

Remarque : Il importe de distinguer la notion d'Intranet de celle d'Extranet. Un Extranet met en relation plusieurs Intranets d'une même organisation et utilise les infrastructures de l'Internet [ZANELLA & LIGIER 99]. Dans un Extranet, on peut retrouver une entreprise et ses partenaires. Les droits d'accès sont alors définis en tenant compte des profils d'utilisateurs.

PHASE D'ETUDE CONCEPTUELLE

IV.FONCTIONNALITES ATTENDUES DE L'INTRANET DU MEF

4.1. Messagerie électronique

La messagerie électronique ou e-mail est sans doute le service, utilisant la technologie Internet, qui est le plus largement exploité. En effet, un tel service permet de communiquer facilement et assez rapidement avec n'importe qui possède une adresse e-mail accessible. Ceci montre combien Internet et Intranet sont liés et c'est ici clairement le fait qu'un Intranet emprunte la technologie Internet qui crée cette similitude. Ainsi généralement, tous les messages sont stockés sur une machine disponible à toute personne reliée à l'Intranet.
Le courrier électronique désigne n'importe quel programme employé par un utilisateur de système informatique ou de réseau d'ordinateurs pour envoyer et recevoir des messages. Le programme reçoit l'adresse du destinataire et le message à faire parvenir. Si cet utilisateur se trouve sur un autre système dans un réseau, l'adresse doit comporter les éléments qui permettront d'identifier l'ordinateur cible. Le courrier électronique offre plusieurs avantages :

- la rapidité : l'information (rapports, données, documents...) parvient rapidement à destination ;
- la gestion de boîtes aux lettres (BAL) ;
- l'envoi de messages peut se faire n'importe quand ;
- la confidentialité des messages est assurée moyennant la sécurité.

L'avantage du courrier électronique sur le téléphone ou sur le fax est alors considérable. En effet, il permet de joindre un correspondant avec des informations écrites tout comme le fax, mais qui peuvent être recopiées dans un document en mode texte. Par rapport au téléphone, le courrier électronique permet d'aller droit à l'essentiel, évite les aléas des répondeurs et permet de laisser des traces écrites. En outre, on peut lire son courrier de n'importe où dans le monde lors des déplacements ; ce qui en fait un des meilleurs moyens de joindre son correspondant. Les logiciels de courrier électronique permettent d'envoyer des documents attachés à la note principale. Ainsi par le courrier les utilisateurs d'Internet/Intranet peuvent échanger des fichiers non-ASCII (documents Word, logiciels, etc.) qui peuvent aller jusqu'à des fichiers sonores.

4.2. Productivité de groupe

L'objectif de la productivité de groupe est de permettre aux agents d'un organisme de travailler ensemble, indépendamment des frontières hiérarchiques et des services. En effet, les procédures d'entreprise requièrent souvent des actions collectives nécessitant le traitement par plusieurs personnes d'un même document ou ensemble de documents selon un ordre établi. Ce processus étant souvent long et fastidieux (surtout quand il est fait manuellement) , la mise en œuvre d'outils de productivité de groupe tels que le workflow, la gestion de base de documents (administratifs, archives, etc.)... devrait offrir aux utilisateurs du MEF des moyens de collaborer afin d'être plus productifs et permettre une gestion beaucoup plus dynamique des procédures administratives.

Le workflow permet de définir des processus de circulation de l'information et d'automatiser cette circulation entre les différents utilisateurs. En cela, il permet l'exécution de tâches en série ou en parallèle par deux ou plusieurs personnes membres d'un groupe de travail et visant un but commun. Cet outil, destiné à la gestion des tâches et flux d'informations, remplace[1] la circulation des dossiers « papier » dans les administrations, bureaux et entreprises. Ces documents « papier » sont en effet convertis en fichiers électroniques (tâches), qui circulent de poste en poste, avec, à chaque étape, la possibilité de traiter le dossier en le modifiant, le complétant, le validant ou en refusant sa validation.

[1] Il ne s'agit pas ici d'un remplacement total du support papier par le système électronique car malgré l'automatisation l'on aura toujours besoin de faire suivre les flux de documents électroniques par des documents papier dûment visés par l'autorité compétente pour les besoins d'archivage administratif, les documents électroniques n'étant pas reconnus (pour le moment) comme documents juridiques.

4.3. Stockage de données spécifiques

Il s'agit de constituer une banque de données où seront stockées toutes les informations (de nature variée) susceptibles d'intéresser les agents dans l'exercice de leur fonction. Disponibles sur un serveur, ces informations pourront être consultées et/ou téléchargées par tous les agents et devront être mises à jour régulièrement. Par ailleurs, l'accès à la banque d'informations devra être réglementé et sécurisé et son utilisation devra être facile (consultation, recherche, stockage d'informations...).

4.4. Accès à l'Internet

L'Intranet du MEF devra fournir aux utilisateurs, à l'échelle nationale, un accès facile et beaucoup plus élargi à Internet avec un débit acceptable de support de communication. De plus, la mise en place d'un site web du MEF, visible de l'Internet et des utilisateurs internes, est souhaitée. Une politique de sécurité et de confidentialité conséquente devra alors être définie pour permettre cette ouverture vers le réseau mondial.

4.5. Télémaintenance d'applications et de postes de travail

Le parc informatique du MEF étant réparti sur des sites géographiquement distants, la maintenance d'applications et de postes de travail pose le problème de sollicitations et déplacements intempestifs des agents techniques de la Direction des Services Informatiques. On note une perte de temps massive et un recul notoire dans les activités journalières de ces agents.

La mise en place de l'Intranet devrait permettre de maintenir à distance des applications et des postes de travail par des procédures de déploiement de logiciels à partir un point fixe.

V. ETUDE COMPARATIVE DES SOLUTIONS POSSIBLES

Cette partie présente les performances techniques des solutions envisageables pour l'Intranet du MEF (architectures et aspects logiciels).

5.1. Comparaison d'architectures

Deux scénarii d'architectures sont ici étudiées. L'accent est mis beaucoup plus sur les aspects sécuritaires.

Le premier scénario isole l'ensemble des réseaux de Ouagadougou (sur le RESINA) vis-à-vis de l'Internet, des agents itinérants et des réseaux de Trésoreries Régionales et Principales en utilisant un firewall en haute disponibilité. Les réseaux de Tresoreries Régionales sont progégés de l'Internet par un routeur disposant de fonctions de firewall.

Le second scénario considère l'ensemble du réseau national comme un système fermé. La liaison avec l'extérieur est établie en un seul point d'entrée, celui de l'Internet.

Dans les deux cas, chaque réseau local du MEF sur le RESINA est protégée des autres par un firewall. De plus, la liaison avec l'Internet est préconisée via l'ONATEL. La liaison via la DELGI a été étudiée en remarque ; mais elle n'a pu être retenue car ne garantissant pas une optimisation de performances techniques (débits).

Le détail de chacun des scénarii est présenté dans les sections suivantes.

5.1.1. Scénario 1

L'Intranet du MEF doit fonctionner sur le RESINA avec certains de ses bâtiments pris comme bâtiments principaux de la boucle FDDI. Pour sa mise en œuvre, un de ces bâtiments peut être identifié comme étant l'entrée Internet du réseau (de préférence le bâtiment de la DGTCP car abritant la Direction des Services Informatiques du MEF qui est l'organe chargé de la résolution des questions techniques informatiques). Ce bâtiment abritera deux machines serveurs Intranet et web. Le serveur Intranet, dans les cas du workflow et de la banque de documents, fournira ses services en interne et de façon spécifique aux utilisateurs du MEF. Par contre, dans le cas de la messagerie, ses services pourront s'étendre à l'extérieur (échanges d'informations en interne (entre agents) et communications avec l'extérieur). De même le serveur web du MEF fonctionnera pour fournir des services aux agents utilisateurs et au monde extérieur. Pour l'accès à l'Internet, une ligne spécialisée reliera l'ONATEL au bâtiment de la DGTCP à travers un routeur R1. Ce routeur servira également à interconnecter les Trésoreries Régionales à la DGTCP (topologie étoile). Il doit être équipé d'une plate forme logicielle dotée de fonctions de firewall et d'IPSec (*Internet Protocol Security*, pour permettre le chiffrement de données entre les Trésoreries Régionales et la DGTCP). La sécurité du réseau (à l'entrée DGTCP) sera assurée par un firewall équipé d'un proxy et d'un logiciel de contrôle de virus. Le contrôle de virus permettra de « scanner » tous les paquets entrants pour détecter d'éventuels virus. Le proxy masquera les adresses IP des postes de travail vis-à-vis de l'Internet et filtrera les paquets par rapport à leur contenu, leur source ou destination... Le commutateur du bâtiment utilisé dans le cadre du RESINA et qui supporte le réseau local de ce bâtiment accédera au reste du monde en passant par le firewall. Les travailleurs itinérants du MEF devront pouvoir accéder à des serveurs internes en passant par un serveur d'accès distant et un serveur d'authentification. C'est le routeur R2 qui joue ici le rôle de serveur d'accès distant. Il devra alors être équipé d'un logiciel client d'authentification et disposer de cartes modem pour les liaisons téléphoniques. Tous les accès de l'extérieur au réseau de la DGTCP sont soumis au passage obligatoire par le firewall. Le firewall est constituée de deux machines physiques ayant la même adresse IP et qui sont configurées en fonctionnement maître/esclave. Si l'un tombe en panne, l'autre prend automatiquement la relève : on parle de haute disponibilité du firewall. L'ensemble de ces deux machines fonctionne comme un seul et même équipement.

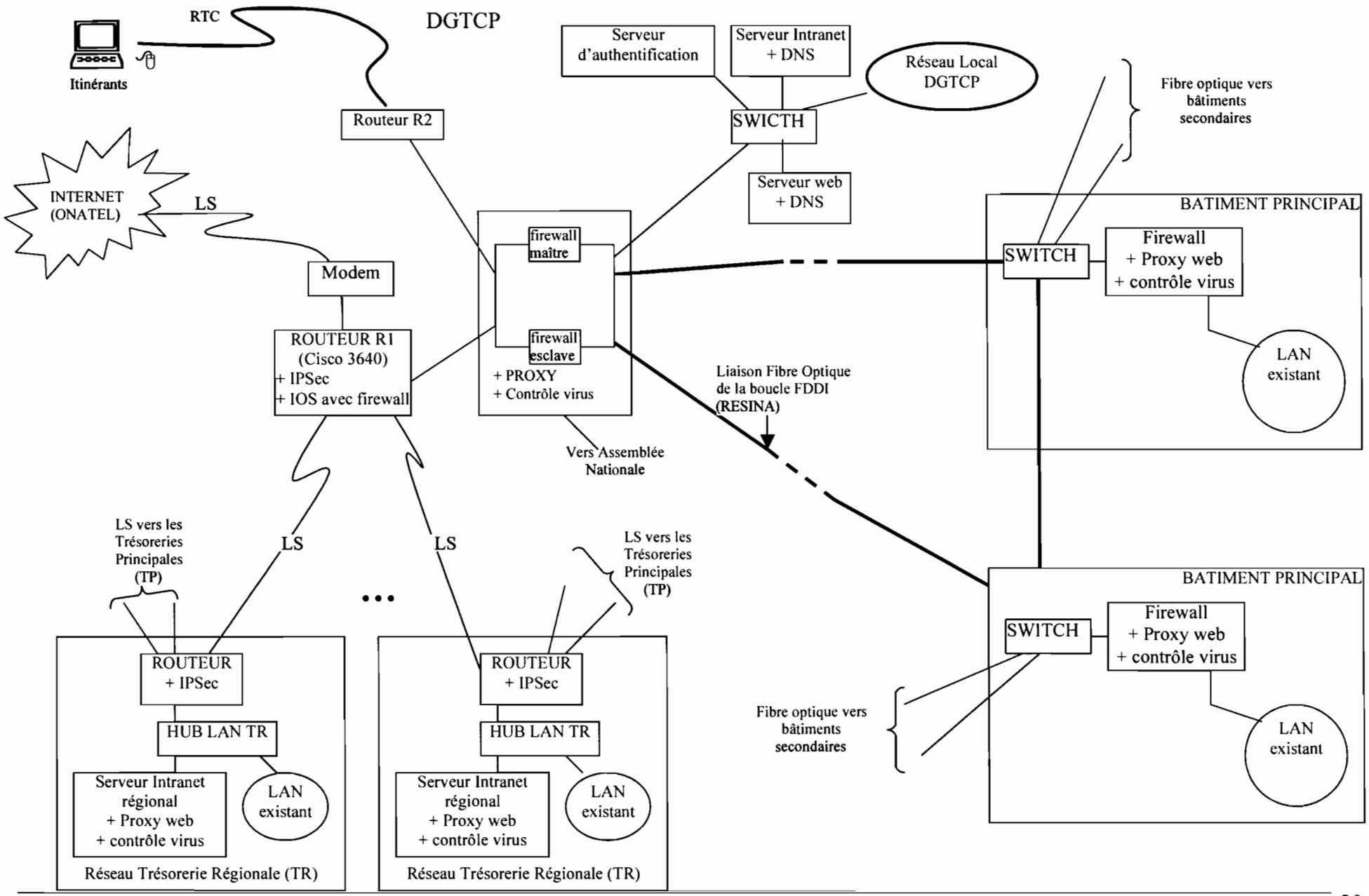
Tous ces équipements pourront être alimentés par le circuit électrique existant, la DGTCP disposant d'une alimentation électrique sécurisée et centralisée (deux onduleurs de 8 KVA, un de 10 KVA et un de 15 KVA) et d'un groupe électrogène.

Dans chaque bâtiment (du MEF) qui est un bâtiment principal dans le cadre du RESINA, un firewall équipé d'un proxy web et d'un logiciel de contrôle de virus devra être installé entre le commutateur connectant le réseau de ce bâtiment aux autres bâtiments et le réseau local. On rappelle que sur les réseaux de tous les bâtiments de catégorie A sont interconnectés des réseaux de bâtiments catégorie B qui ne sont pas tous du MEF. Les bâtiments de catégorie B constituent dans ce cas une menace pour l'Intranet du MEF car pouvant être sources d'intrusion (surtout ceux n'appartenant pas au MEF). L'installation des firewalls a pour objectif de ne laisser accéder au réseau local de chaque bâtiment que les paquets autorisés tout en empêchant les entrées de virus et d'augmenter les performances des requêtes http vers Internet ou vers le serveur web du MEF. L'installation du proxy web sur chaque serveur firewall de bâtiment principal a pour objectif d'optimiser le trafic entre bâtiments principaux. Les équipements dans chaque bâtiment pourront être protégés par l'alimentation électrique sécurisée du bâtiment.

Les bâtiments secondaires quant à eux restent reliés aux bâtiments principaux conformément à l'architecture du RESINA (*cf. Schéma synthétique du RESINA, Annexe 2*).

Dans chaque Trésorerie Régionale, on installera des serveurs Intranet régionaux pour desservir les agents de la Trésorerie Régionale et ceux des Trésoreries Principales associées. Ces serveurs pourront être mis à jour régulièrement par une technique de réplication transparente aux utilisateurs de sorte que les agents des structures décentralisées/déconcentrées puissent collaborer

avec les autres utilisateurs du réseau sur les mêmes données quasiment en temps réel. Pour faire de la messagerie électronique (SMTP/POP) avec un autre réseau local (d'une autre Trésorerie Régionale) ou avec le monde extérieur, chaque serveur régional devra s'adresser au serveur Intranet principal installé à la DGTCP qui lui se charge de gérer les communications vers le réseau cible. Cette technique permettra aux agents provinciaux de continuer à faire de la « messagerie régionale » et utiliser les autres outils Intranet de productivité de groupe en cas de problème sur la ligne les reliant au réseau de la DGTCP. Sur chacun de ces serveurs régionaux, on fera fonctionner un proxy web qui aura pour rôle de fournir aux agents des pages web de l'Internet ou du serveur web du MEF tout en fonctionnant comme un cache. Son avantage est que si une page web sollicitée par plusieurs agents est déjà disponible sur le serveur proxy (suite à la sollicitation d'un agent), tous ceux qui la sollicitent à cette période le reçoivent immédiatement sans avoir à effectuer chacun un accès sur le serveur web du MEF ou de l'Internet. De même, pour envoyer un message d'une Trésorerie Régionale à une Trésorerie Principale qui en dépend, il n'est pas nécessaire (et même pas idéal) de passer par un serveur central physiquement installé à Ouagadougou (ce qui induirait plusieurs utilisations de la LS entre Ouagadougou et la Trésorerie Régionale pour le même message). On augmente ainsi les performances du réseau tout en minimisant les accès longues distances, sources de saturation du trafic.


RTC
DGTCP
Itinérants
Serveur d'authentification
Serveur Intranet + DNS
Réseau Local DGTCP
Fibre optique vers bâtiments secondaires
Routeur R2
SWICTH
Serveur web + DNS
INTERNET (ONATEL)
LS
Modem
firewall maître
firewall esclave
+ PROXY
+ Contrôle virus
BATIMENT PRINCIPAL
SWITCH
Firewall + Proxy web + contrôle virus
LAN existant
ROUTEUR R1 (Cisco 3640)
+ IPSec
+ IOS avec firewall
Liaison Fibre Optique de la boucle FDDI (RESINA)
Vers Assemblée Nationale
LS vers les Trésoreries Principales (TP)
LS
LS
LS vers les Trésoreries Principales (TP)
BATIMENT PRINCIPAL
SWITCH
Firewall + Proxy web + contrôle virus
LAN existant
ROUTEUR + IPSec
HUB LAN TR
Serveur Intranet régional + Proxy web + contrôle virus
LAN existant
Réseau Trésorerie Régionale (TR)
ROUTEUR + IPSec
HUB LAN TR
Serveur Intranet régional + Proxy web + contrôle virus
LAN existant
Réseau Trésorerie Régionale (TR)
Fibre optique vers bâtiments secondaires

Avantages de cette architecture

- Toutes les communications entre postes du MEF et l'extérieur passent nécessairement par un proxy-firewall. Le réseau est alors protégé contre les attaques et tentatives d'intrusion venant de l'extérieur.
- Le proxy-firewall peut être configuré de sorte que toutes requêtes venant de l'Internet ne puissent accéder qu'au serveur web et ne rentrer dans le reste du réseau que s'il s'agit d'une information portant sur la messagerie électronique. Les informations sur la messagerie électronique pourront être filtrée par le proxy qui fera fonction de proxy mail. L'utilisateur à l'origine de toute autre requête (accès à des applicatifs, accès aux outils de productivité de groupe...) ne pourra accéder au reste du réseau qu'en fournissant des informations d'authentification correctes.
- Les informations provenant des Trésoreries Régionales et traversant le domaine public sont chiffrées et donc inexploitables par une personne qui les intercepterait.
- Les agents itinérants peuvent continuer à travailler et à communiquer avec le réseau du MEF au cours de leur déplacement.
- Le firewall de la DGTCP est composé de deux machines physiques ayant la même adresse IP et fonctionnant en mode maître/esclave comme une seule et même machine. Si une de ces machines tombe en panne, le second prend automatiquement la relève : ceci garantit la sécurité du réseau à un niveau assez élevé.
- Les serveurs Intranet régionaux équipés de proxy web et placés dans les Trésoreries Régionales permettent d'optimiser les performances du trafic réseau entre la DGCTP et ces Trésoreries Régionales.
- Tous les utilisateurs du WAN (*Wide Area Network, réseau longue distance*), qu'ils soient en province ou non, travaillent sur les mêmes données en temps réel comme s'ils travaillaient sur un même serveur d'un LAN (*Local Area Network, réseau local d'entreprise*).

Inconvénients

- Si malgré le principe de haute disponibilité, le proxy-firewall (à l'entrée Internet du réseau) tombe entièrement en panne, le réseau reste ouvert aux attaques (Il faudra alors déconnecter le réseau de l'Intranet pendant la période de dépannage du proxy-firewall, si l'on a pu être averti à temps).
- L'architecture proposée nécessite un équipement spécial pour l'accès distant : le routeur R2.
- Les réseaux de Trésoreries Régionales et Principales n'ont pas le même niveau de sécurité que ceux de Ouagadougou car n'étant protégés de l'Internet que par le seul routeur R1.
- Elle nécessite également deux machines physiques pour assurer la haute disponibilité de firewall.
- Toute personne qui arrive à passer outre les principes de sécurité mise en œuvre sur le firewall peut accéder au réseau local de la DGTCP (où il y a des serveurs d'applications sensibles).

Matériels existants

Matériel	Caractéristiques	Qté	Description
Routeur	Cisco 3640, Plate forme logicielle Cisco IOS avec fonctions de firewall	1	Accès Internet et interconnexion des Trésoreries Régionales avec bâtiment de la DGTCP
Routeur	Cisco série 2600, Cisco IOS avec fonctions de firewall	5	Pour les Trésoreries Régionales
Switch	CoreBuilder 2500 de 3Com	8	Interconnexion des bâtiments du RESINA
Ligne téléphonique	Ordinaire	4	Connexion par RTC des travailleurs itinérants
Liaison fibre optique RESINA	10 Mbps et 100 Mbps	-	Interconnexion des bâtiments du RESINA
LS	64 Kbps	5	Entre DGTCP et les TR
Serveurs	PC, Pentium, 128 Mo RAM, 16 Go disque dur	6	Serveurs Intranet pour les TR et TP Serveur d'authentification
Hub	Super Stack de 3Com 10/100 Mbps	1	Serveur web, Switch de la DGTCP
Onduleur	10 Kva, type Online	5	Pour les serveurs de chacune des TR

Matériels/Logiciels à acquérir

Matériels/Logiciels		Caractéristiques	Qté	PU HTHD	Total HTHD
Routeur		Fonctions de firewall, IPSec, logiciel d'authentification	1	3 000 000	3 000 000
Logiciel Firewall		Firewall 1de CheckPoint, avec fonctions de proxy intégrées	1	8 000 000	8 000 000
Serveur Firewall		PC, Pentium, 600Mhz, 128 Mo RAM, au moins 16 Go disque dur	9	1 150 000	10 350 000
Logiciel contrôle virus (*)		InterScan Viruswall	1	150 000	150 000
Serveurs web, Intranet		Pentium, 128 Mo RAM, 6 disques de 9 Go, Contrôleur RAID 5.	2	7 000 000	14 000 000
Modems (liaison RTC et LS vers Internet)		56 Kb minimum	5 (**)	98 000	490 000
LS vers l'ONATEL	Création	-	1	472 000	472 000
	Raccordement	-	1	144 000	144 000
				TOTAL	**37 906 000 F CFA**

(*) InterScan VirusWall 2000 pour Windows NT est téléchargeable sur Internet (www.trendmicro.fr)

(**) Pour commencer la mise en œuvre de l'Intranet, il est préférable que le nombre de modems pour l'accès distant (cf. batterie de modems) soit limité à quatre (compte tenu du nombre d'agents itinérants). Ce nombre pourra être revu à la hausse en cas de nécessité.

Remarque :

- L'installation de la LS vers l'ONATEL engendre des coûts récurrents mensuels de redevance de **300 000 FCFA** (spécifique aux institutions gouvernementales) et une location vente de modem de **94 400 F CFA** par mois sur une année.
- On aurait pu envisager d'installer la LS entre la DGTCP et la DELGI, cette dernière gérant les accès Internet pour l'ensemble de l'administration. Dans ce cas, les coûts d'installation de la LS seraient les suivants :

Création	472 000 F CFA
Raccordement	288 000 F CFA

Le coût total des matériels/logiciels serait de **38 050 000 FCFA** et l'installation de cette LS n'engendrerait que les coûts récurrents mensuels de redevance de **300 000 FCFA** (pas de location vente de modem).
Mais cette solution n'est techniquement pas performante car, du fait que la DELGI gère déjà les accès Internet pour toute l'administration, la connexion du MEF via le même serveur contribuera à diminuer les performantes du trafic (débit offert), dans la mesure où l'acquisition de la LS multipliera le nombre d'utilisateurs d'Internet au MEF.

5.1.2. Scénario 2

Ce deuxième scénario choisit également le bâtiment de la DGTCP comme bâtiment d'entrée Internet du réseau et d'installation des équipements Intranet/Internet. Il propose que le serveur web soit placé dans une DMZ (*zone démilitarisée*) et protégé par un serveur firewall (on l'appellera firewall A) équipé d'un logiciel de contrôle virus qu'on aura placé à l'entrée Internet du réseau. La ligne spécialisée qui offre la connexion permanente sur l'Internet arrivera sur un routeur (routeur R1) qu'on aura relié au serveur firewall. La plate forme logicielle de ce routeur devra avoir des fonctions de firewall. Un deuxième routeur (routeur R2) servira à relier les utilisateurs distants au réseau de la DGTCP par lignes spécialisées (utilisateurs des Trésoreries Régionales et Principales) ou RTC (utilisateurs itinérants). Ce routeur se comportera comme client d'authentification pour un serveur d'authentification qu'on placera dans le réseau local de la DGTCP pour identifier les utilisateurs itinérants qui ont des besoins d'accès aux services internes du réseau. De plus, l'utilisation du standard IPSec sur ce routeur (R2), ainsi que tous les autres routeurs des Trésoreries Régionales, permettra de faire du chiffrement et donc de garantir la confidentialité, la sécurité et l'intégrité des données. Sa plate forme logicielle devra également être équipé d'une fonctionnalité de firewall. Pour établir les liaisons RTC avec les utilisateurs itinérants, il suffira d'ajouter au routeur des cartes modem (analogique). Pour sécuriser le réseau local de la DGTCP vis-à-vis de l'Internet et des accès d'utilisateurs distants, un serveur firewall (on l'appellera firewall B) sera placé entre ce deuxième routeur et le commutateur utilisé dans le bâtiment dans le cadre du RESINA. Ce serveur firewall sera le point de jonction entre la DMZ et le réseau local de la DGTCP où se trouve le serveur Intranet et les autres serveurs d'application. Il sera équipé d'un serveur proxy et d'un logiciel de contrôle virus. Pour un besoin de sécurité renforcée, il serait intéressant de mettre en œuvre à ce niveau le principe de la redondance de firewall : deux serveurs ayant les mêmes fonctionnalités et la même adresse IP et fonctionnant en maître/esclave. Dès que le serveur « maître » tombe en panne, « l'esclave » prend la relève jusqu'à ce que le maître soit dépanné : c'est la technique de la haute disponibilité. Le serveur Intranet offrira ses services sur l'ensemble du RESINA et échangera des informations régulièrement avec les serveurs Intranet régionaux. Les deux firewalls seront configurés différemment. Le deuxième (firewall B) devra faire un filtrage beaucoup plus sélectif que le premier. Tout le monde peut accéder au serveur web et y faire des

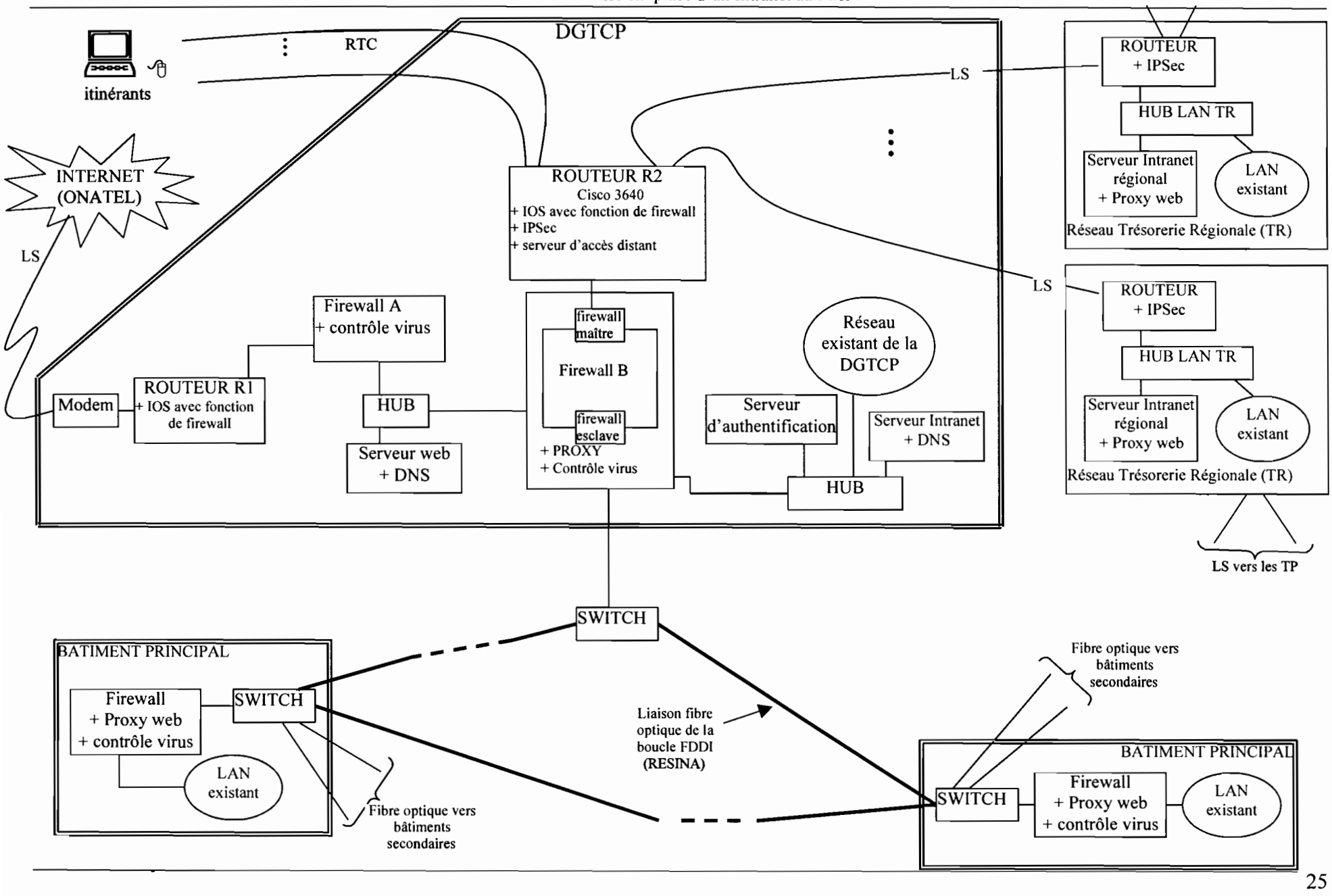
actions autorisées, mais en revanche, tout le monde ne peut pas accéder au réseau global du MEF à partir d'Internet.

Tous les équipements installés à la DGTCP pourront être alimentés par l'alimentation électrique sécurisée de ce bâtiment.

Dans chacun des autres bâtiments principaux du RESINA, un serveur firewall sera placé entre le commutateur utilisé dans le cadre du RESINA et le hub du réseau local. Un serveur proxy web tournera également sur cette machine serveur. Il permettra d'optimiser les performances des liaisons entre bâtiments principaux. Les bâtiments secondaires resteront reliés aux bâtiments principaux conformément à l'architecture du RESINA.

Chaque bâtiment utilisera l'alimentation électrique sécurisée existante pour protéger les équipements installés.

Dans les réseaux locaux de Trésoreries Régionales, l'on installera des serveurs Intranet régionaux qui fonctionneront en étroite collaboration pour former un même système logique, comme présenté dans le scénario 1. Chaque serveur régional desservira les agents de la Trésorerie Régionale mais aussi ceux des Trésoreries Principales qui en dépendent. Pour communiquer avec les autres réseaux de Trésoreries Régionales ou le réseau de Ouagadougou, ou même avec le monde extérieur, les agents d'une Trésorerie Régionale « s'adresseront » au serveur Intranet local qui, lui, se chargera de transmettre les informations au serveur Intranet principal de Ouagadougou. S'il s'agit d'une communication locale (entre agents d'une même province), le serveur principal n'est pas contacté. Comme présenté dans le premier scénario, on installera sur chaque machine serveur Intranet régional un proxy web. Tout ceci a pour but d'optimiser le trafic sur les liaisons entre Trésoreries Régionales et la DGTCP.


DGTCP
RTC
itinérants
INTERNET
(ONATEL)
LS
LS
LS
ROUTEUR R2
Cisco 3640
+ IOS avec fonction de firewall
+ IPSec
+ serveur d'accès distant
Firewall A
+ contrôle virus
ROUTEUR R1
+ IOS avec fonction de firewall
Modem
HUB
Serveur web
+ DNS
firewall maître
Firewall B
firewall esclave
+ PROXY
+ Contrôle virus
Réseau existant de la DGTCP
Serveur d'authentification
Serveur Intranet
+ DNS
HUB
ROUTEUR
+ IPSec
HUB LAN TR
Serveur Intranet régional
+ Proxy web
LAN existant
Réseau Trésorerie Régionale (TR)
ROUTEUR
+ IPSec
HUB LAN TR
Serveur Intranet régional
+ Proxy web
LAN existant
Réseau Trésorerie Régionale (TR)
LS vers les TP
SWITCH
BATIMENT PRINCIPAL
Firewall
+ Proxy web
+ contrôle virus
SWITCH
LAN existant
Fibre optique vers bâtiments secondaires
Liaison fibre optique de la boucle FDDI (RESINA)
Fibre optique vers bâtiments secondaires
BATIMENT PRINCIPAL
SWITCH
Firewall
+ Proxy web
+ contrôle virus
LAN existant

Avantages de cette architecture

- Si la première machine firewall (celle reliée directement au routeur R1 d'accès à l'Internet, firewall A) tombe en panne, seul le serveur web sera vulnérable aux attaques ; le reste du réseau reste relativement sécurisé.
- En cas de rupture d'une liaison entre une trésorerie régionale et la DGTCP, les agents de ladite Trésorerie Régionale peuvent continuer à bénéficier des services de messagerie électronique et des autres outils de productivité de groupe sur leur site et avec les trésoreries principales associées.
- Les serveurs Intranet équipés de proxies web et placé dans les Trésoreries Régionales permettent d'optimiser les performances du trafic réseau entre la DGCTP et ces Trésoreries Régionales. Ces serveurs se comportent comme des caches qui stockent les dernières informations auxquelles ils ont accédé, allégeant ainsi les charges des liaisons fibre optique ou lignes spécialisées entre réseaux locaux.
- Toute requête provenant d'Internet par le routeur R1 en direction d'un serveur d'application spécifique de la DGTCP passe obligatoirement par au moins deux niveaux de contrôle firewall (firewall A et B) et le serveur d'authentification.
- Tout message en direction d'un réseau du MEF quelle que soit sa provenance est soumis à un contrôle de virus. Cela permet de réduire les risques de propagation de virus à travers le réseau (cas où le contrôle permet de détecter les virus).
- Tout utilisateur du réseau du MEF désirant y accéder en dehors des limites physiques de ce réseau devra s'authentifier selon des critères bien définis avant d'y être autorisé.
- La mise en œuvre de la technique IPSec sur les routeurs reliant les Trésoreries Régionales à la DGTCP permet de crypter les données (très sensibles) qui transitent par les supports lignes spécialisées de ce réseau, la traversée du domaine public étant une menace importante pour la sécurité des données.
- Tous les utilisateurs du WAN (*Wide Area Network, réseau longue distance*), qu'ils soient en province (Trésoreries Régionales et Principales) ou non, travaillent sur les mêmes données en temps réel comme s'ils travaillaient sur un même serveur d'un LAN.

Inconvénients

Cette architecture nécessite également deux machines physiques pour assurer la haute disponibilité de firewall et demande beaucoup plus de travail d'administration pour les configurations des firewalls A et B. De plus, elle est plus coûteuse en nombre de routeurs (deux routeurs à la DGTCP).

Matériels existants

Matériel	Caractéristiques	Quantité	Description
Routeur (***)	Cisco 3640	1	Interconnexion des TR avec bâtiment de la DGTCP Gestion des accès distants par RTC
Routeur	Cisco série 2600, Cisco IOS avec fonctions de firewall	5	Dans les Trésoreries Régionales
Ligne téléphonique	Ordinaire	4	Connexion par RTC des travailleurs itinérants
Switch	CoreBuilder 2500 de 3Com	8	Interconnexion des bâtiments du RESINA
Hub	Super Stack de 3Com 6 ports, 10/100Mbps	2	Pour les serveurs web et mail et pour le LAN de la DGTCP
Ligne Spécialisée (LS)	64 Kbps	5	Entre DGTCP et les Trésoreries Régionales
Serveurs	PC, 128 Mo RAM,10 Go de disque dur	6	Serveurs Intranet dans les TR et serveur d'authentification à la DGTCP
Onduleur	10 KVA, type Online	5	Pour les serveurs de chacune des TR

(***) Il sera nécessaire d'acquérir des cartes modems et séries pour ce routeur (gestion de la batterie de modems).

Matériels/Logiciels à acquérir

Matériels/Logiciels		Caractéristiques	Qté	PU	Total par produit
Logiciel Firewall		Firewall 1de CheckPoint, avec fonctions de proxy intégrées	1	8 000 000	8 000 000
Serveur Firewall		PC, Pentium, 600Mhz, au 128 Mo RAM	10	1 150 000	11 500 000
Logiciel contrôle virus		VirusWall	1	150 000	150 000
Serveurs web, Intranet		Pentium, 128 Mo RAM, 600 Mhz, 6 disques de 9 Go, RAID 5	2	7 000 000	14 000 000
Routeur		Fonctions de filtrage et firewall, ACL, logiciel d'authentification, IPSec, extensibilité du nombre de cartes série, modem et voix	1	3 000 000	3 000 000
Modem		56 Kb	1	100 000	100 000
LS vers l'ONATEL	Création		1	472 000	472 000
	Raccordement		1	144 000	144 000
				TOTAL	**37 366 000 CFA**

Remarque :

- L'installation de la LS vers l'ONATEL engendre des coûts récurrents mensuels de redevance de **300 000 FCFA** (tarif spécifique aux institutions gouvernementales) et une location vente de modem de **94 400 F CFA** par mois sur une année.

- Ici également, on aurait pu envisager d'installer la LS entre la DGTCP et la DELGI. Dans ce cas, les coûts de la LS seraient les mêmes que ceux présentés en remarque dans le scénario 1.
Le coût total des matériels/logiciels serait de **37 510 000 FCFA** et l'installation de cette LS n'engendrerait que les coûts récurrents mensuels de redevance de **300 000 FCFA**.
Mais, comme dans le premier scénario, cette solution n'est techniquement pas performante car, du fait que la DELGI gère déjà les accès Internet pour toute l'administration, la connexion du MEF via le même serveur contribuera à diminuer les performantes du trafic (débit offert), surtout que l'acquisition de la LS multipliera le nombre d'utilisateurs d'Internet au MEF.

5.2. Logiciels pour la mise en œuvre des fonctionnalités

5.2.1. Workflow, banque de documents et messagerie électronique (serveur Intranet)

- **Le logiciel GroupWise**

Groupwise est un logiciel de Novell qui fonctionne sous la plate forme Netware et supporte d'autres plates-formes, notamment Windows NT, Macintosh et divers systèmes UNIX. Il constitue le complément de Netware 5. Il permet de

- faire de la messagerie électronique ;
- gérer les documents ;
- faire du workflow ;
- faire de l'accès distant ;
- etc.

Groupwise est un logiciel simple et rapide vers une solution Intranet. C'est une véritable application client/serveur qui fait appel au protocole TCP/IP pour la communication entre les postes clients et les serveurs. Dans ses versions 5.1 et 5.5, il intègre, en plus des fonctionnalités sus-citées, la gestion d'agenda et la planification, les possibilités de conférences électroniques, les formulaires, la télécopie... De plus, un utilisateur en déplacement peut accéder à toutes les ressources disponibles sur le réseau Netware via Internet en utilisant Groupwise WebAccess et n'importe quel browser web standard.

- Coût : la version 5.5 de Groupwise coûte 800 000 FCFA .
- Installation et configuration : Groupwise s'installe facilement sur une machine serveur Netware. Une grande partie du réseau du MEF fonctionnant sous Netware, Groupwise devrait pouvoir s'intégrer facilement à l'existant et aux habitudes des utilisateurs.

- **Le logiciel Lotus Notes/Domino**

Fonctionnant sur toutes les plates-formes et réseaux (*Windows 9x, Windows NT, OS/2, Unix, Netware, Macintosh,...*), Lotus Notes se révèle être le standard du Groupware.

Lotus Notes est une puissante plate-forme de développement de systèmes stratégiques, capables de coordonner les nombreuses activités nécessaires à l'accomplissement de plusieurs objectifs. Trois composantes technologiques sont rassemblées pour faire de Notes une plate forme de développement et de déploiement d'applications performante dans l'industrie du client/serveur :

- une base de documents composite puissante et souple : les utilisateurs peuvent accéder, suivre, stocker et organiser leurs informations ;
- un environnement de développement riche ;
- une messagerie intégrale.

La base de documents distribués , l'environnement de développement et le système de messagerie sont supportés par une infrastructure puissante : l'objet de stockage Notes. Le conteneur

d'objet Notes propose une architecture sur laquelle une variété d'applications mettant en œuvre communication, collaboration et coordination (workflow) peut être construite.

Lotus Notes/Domino présente l'avantage donc de faciliter les communications, de permettre le partage des informations en maintenant la sécurité et le contrôle des versions et de créer des groupes de travail dynamiques. De plus, beaucoup de produits orientés « messagerie » qui s'appuient sur le contenu du message lui-même (texte riche, pièces jointes...) ne sont pas comparables à la puissance et à la cohérence de la plate forme Notes. En effet, l'infrastructure de Lotus Notes/Domino, en plus de la gestion de messages s'étend à la circulation de formulaires, l'agenda-planning, le workflow, la gestion documentaire, les forums de discussion, les carnets d'adresses et d'autres applications.

La technologie de réplication utilisée par Lotus Notes/Domino permet de recopier les bases sur différents serveurs et de synchroniser tous les changements par propagations des deltas d'information. De ce fait, les utilisateurs travaillent sur la même information automatiquement mise à jour, et ceci même s'ils ne se connectent au réseau qu'occasionnellement. Les serveurs se connectent entre eux à intervalles réguliers, et répliquent les modifications de documents, de droits d'accès et conception (*design*) des applications tels que les masques et les vues. La réplication Lotus Notes/Domino peut également s'effectuer entre serveur et client. De cette manière, des utilisateurs nomades ont la possibilité de se connecter au serveur Domino en réseau commuté lorsqu'ils le souhaitent, le serveur prendra alors en charge la synchronisation des données entre les copies « serveur » et « clientes » des bases Notes. La réplication sous Lotus Notes/Domino est un système fondamentalement différent d'un SGBDR (Système de Gestion de Base de Données Relationnelles), qui réclame quant à lui des communications continues et rapides pour respecter son processus de fonctionnement. A l'opposé, le système de réplication de Lotus Notes/Domino a permis l'implémentation d'un nouveau modèle de synchronisation de bases de données plus léger, proposant le support natif d'utilisateurs distants ou mobiles.

- Coût : la version 5.0 de Lotus Notes/Domino coûte 3 500 000 FCFA.
- Installation et configuration : Lotus Notes s'installe facilement sur toutes les plates formes et réseaux : Netware, Windows NT, OS/2, Unix, Windows 95, Macintosh... Le réseau du MEF fonctionnant principalement sous Netware et Windows NT, l'acquisition d'une version de Lotus Notes compatible avec ces plates formes devrait permettre une intégration facile à l'existant et aux habitudes des utilisateurs.

Remarque : Il existe sur le marché d'autres produits fonctionnels avancés dans le groupware, tel qu'Interoffice d'Oracle dont la suite logicielle (construite sur la base de données Oracle) fournit des services de courrier électronique, de planification, de workflow, de gestion documentaire ainsi que des logiciels de présentation. Dans notre cas, l' intégration à l'existant pour la plupart de ces produits n'est pas évidente ou ne présente pas nécessairement un avantage.

5.2.2. Serveur web

5.2.2.1. La solution Linux : serveur Apache

La solution Linux consiste à utiliser le serveur Apache de ce système comme serveur web.

Linux désigne en fait un ensemble de logiciels gratuits, téléchargeables sur l'Internet (exécutables et sources), ou vendus sous forme de distributions peu onéreuses par des sociétés comme RedHat, Mandrake ou Caldera. Une distribution Linux comprend :

- le noyau (*kernel*) Linux (le cœur du système d'exploitation, environ 500 000 lignes de code écrit par Linus Torvalds ;)
- le compilateur et les outils de développement GNU ;
- un serveur X11 et un logiciel d'interface utilisateur comme KDE ou GNOME ;

- des serveurs de fichiers NFS ;
- le serveur web Apache ;
- le serveur de courrier électronique Sendmail ;
- les bibliothèques GLIBC de GNU.

Les différentes distributions comportent le même noyau conçu par une communauté d'experts en la matière. Elles diffèrent seulement par « l'habillage » effectué par les sociétés de distribution. Certaines sociétés comme Mandrake mettent l'accent sur l'interface de présentation (graphique, menus déroulants...) et la facilité d'utilisation. D'autres conservent l'interface en ligne de commande (exemple, Slackware).

Le système Linux est bien moins gourmand que les autres systèmes d'exploitation. Il peut fonctionner avec de faibles ressources matérielles (un ordinateur 386SX/16 équipé de 4 Mo RAM pour une configuration minimaliste, 8 Mo pour disposer de l'interface graphique X11). Linux offre une assistance technique gratuite en ligne sur l'Internet ou sur la distribution. Pour les aspects réseaux, Linux prend déjà en compte la nouvelle version d'Internet Protocol, Ipv6 ou Ipng (*IP nouvelle génération*).

Le serveur web Apache ne doit pas son nom à la communauté amérindienne mais initialement à la transposition phonétique de « *a patch* » qui correspond à un ajout logiciel fait au départ sur le serveur du NCSA. Aujourd'hui, Apache est le serveur http le plus utilisé dans le monde Internet (plus de 50% des serveurs web) et ce succès est dû d'une part à sa robustesse, et d'autre part à l'engouement actuel des logiciels gratuits sous l'impulsion d'Internet. Si au départ Apache était destiné uniquement au monde UNIX, la version 1.3 l'a rendu compatible avec Windows NT et Windows 9x. Sur Windows NT, Apache fonctionne comme un véritable service ou comme une application, et est compatible avec les ISAPI de Microsoft. De plus, Apache supporte les SSI (*Server Side Include*), les inclusions de code HTML, le protocole http/1.1, les mots de passe sur des pages, et enfin les SSL 2 et 3 (*Socket Secure Layer*). Le langage Perl inclus dans Linux permet d'écrire des scripts CGI (*Common Gateway Interface*) afin de construire des pages web interactives (formulaires, accès à une base de données...).

Remarque : Le serveur de courrier électronique Sendmail (littéralement, envoie le courrier), fourni gratuitement avec toutes les distributions est un outil performant pour la mise en œuvre d'un système de messagerie avec un grand nombre d'utilisateurs. Sendmail est le premier serveur à utiliser le protocole SMTP (*Simple Mail Transfert Protocol*). C'est une énorme machine capable d'expédier en permanence un grand nombre de messages électroniques et fonctionne sans l'aide de inetd. Le programme Sendmail se trouve dans /usr/sbin/sendmail. Ce serveur n'est pas proposé pour l'Intranet du MEF car le choix d'un des logiciels de productivité de groupe présentés ci-dessus (Lotus Notes et Groupwise) permet d'offrir la fonctionnalité de messagerie électronique ; mieux, on peut mettre en œuvre la gestion des agendas, de carnets d'adresses personnels, de tâches... D'autre part, du fait que Sendmail est constitué d'un ensemble de programmes (dont certains ne sont pas nécessaires pour la mise en œuvre d'un simple système de messagerie), sa mise en œuvre nécessite d'énormes précautions car pouvant être à l'origine de nombreux trous de sécurité.

- Coût : Linux est gratuit, téléchargeable sur Internet. Par ailleurs, les distributions fournies par certaines sociétés coûtent autour de 50 dollars US (moins de 35 000 F CFA).
- Installation et configuration : L'installation et la configuration relativement complexe du serveur Apache (et même de Sendmail) sont dues principalement à la spécificité des systèmes Unix (système de fichiers, interface souvent en ligne de commande, commandes Unix...) qui ne pas toujours maîtrisés des utilisateurs. Leur mise en œuvre nécessite l'adoption d'une culture préalable des systèmes Unix. Mais avec l'évolution actuelle des interfaces Unix (interface graphique des distributions Linux, par exemple) et au regard de la

robustesse des systèmes Unix, la complexité de manipulation ne devrait plus être un frein à la mise en œuvre d'une solution Unix.
Par ailleurs, remarquons qu'actuellement, le système Linux n'est pas largement utilisé dans le réseau du MEF. L'installation d'une solution Linux pour le serveur web créera un nouveau besoin de compétence en terme d'administration et augmentera les charges de l'administrateur du réseau.

5.2.2.2. La solution Microsoft : Internet Information Server

Microsoft propose un serveur web tout à fait rapide et robuste dans les environnements Windows NT appelé IIS. Internet Information Server (IIS), utilisé sur environ 22% des sites Internet, est plus utilisé dans les environnements Intranet. Les points forts du serveur web de Microsoft résident dans son ergonomie, puisque le serveur est administrable par un assistant graphique et également par le web. Dans les versions actuelles, la gestion des logs est tout à fait identique à celle des autres serveurs (HTTP 1.1, SSL2, SSL3). L'originalité du serveur IIS réside également dans son langage de scripting Active Server Page (que l'on reconnaît par l'extension des pages en ASP). Par contre, ce langage propriétaire interdit tout portage sur un serveur autre que celui de la marque. Ainsi la prudence sera de mise pour les utilisateurs de serveurs Microsoft Information Serveur en Intranet qui pourraient être amenés à mettre leurs pages sur Internet, via un hébergeur qui ne posséderait pas ce type de serveur. Il est à noter aussi que IIS supporte les agents SNMP permettant notamment l'administration par les outils d'administration. En outre, IIS est livré avec Microsoft Index Server qui est un moteur de recherche interne permettant d'indexer et de retrouver par mot clé les pages archivées sur le serveur. IIS est également étroitement couplé avec Front Page et Site Server Express les outils de développement de Microsoft.

Remarque : Pour la messagerie, le serveur Microsoft Exchange est une solution onéreuse (il faut l'acheter à part pour le faire fonctionner sous Windows NT qu'on aura également acheté) qui rencontre un succès mitigé dans un environnement d'entreprise. Il intègre une messagerie électronique, un agenda de groupe, des formulaires électroniques et des applications de partage d'information. Dans sa version 5.5, c'est un serveur de messagerie universel ouvert tant sur l'hétérogénéité du parc interne de l'entreprise que sur l'Internet et il met à disposition des utilisateurs de nombreuses fonctions de travail collaboratif prêtes à l'emploi, essentiellement via Outlook. Microsoft Server 5.5 Enterprise Edition contient Exchange 5.5 server, Exchange 5.5 Client, Outlook 97 client, connecteur MS Mail, service Internet Mail, connecteur cc :Mail, composants Active Server, service Internet News, Connecteur Exchange et Connecteur X.400.

Du fait que Groupwise et Lotus Notes intègrent des fonctionnalités de messagerie électronique, l'achat d'une solution onéreuse comme Microsoft Exchange pour assurer ces mêmes fonctionnalités ne présente plus d'intérêt.

- Coût : Windows NT Server coûte environ 3 549 Dollars US (plus 2 000 000 F CFA) pour une licence de 25 clients) et intègre le serveur IIS.
- Installation et configuration : les serveurs IIS de Windows NT et Exchange s'installent beaucoup plus facilement que les serveurs Linux. Windows NT étant une plate forme existant dans le réseau du MEF, l'intégration des serveurs IIS et Exchange devrait être facile et exigerait moins de problèmes d'administration.

5.2.2.3. La solution Novell : Netware web Server

Cette solution consiste à utiliser le serveur web intégré dans Netware 5 (Netware web Server) pour l'installation du site web du MEF. Le serveur web de Netware 5, permet de publier des informations statiques sous la forme de documents HTML. Ce serveur est également inclus dans

IntranetWare (système d'exploitation Netware 4.11). Les API (Application Programming Interfaces) L-CGI, R-CGI, les interpréteurs NetBasic et le langage Java inclus dans ce serveur web permettent de créer des applications web dynamiques.
Netware 5 fournit également le logiciel nécessaire à la mise en œuvre d'un serveur FTP (File Transfert Protocol) pour le transfert des fichiers TCP/IP à travers le réseau Intranet. Il est ouvert à plusieurs plates-formes clientes (Windows 95, Windows NT, UNIX, OS/2, Mac OS et DOS) et sécurise le réseau par un firewall de premier niveau.

- Coût : Netware 5 coûte environ 2 500 000 F CFA pour une licence de 25 postes et intègre Netware Web Server.
- Installation et configuration : l'installation du serveur web de Novell se fait sur une machine serveur où Netware est déjà installé et est relativement facile. Netware étant la plate forme principale du réseau du MEF, l'intégration de ce système devrait être facile et exigerait moins de problèmes supplémentaires d'administration.

5.2.2.4. La solution Netscape : Netscape Enterprise Server

Netscape Enterprise Server est le troisième des serveurs web utilisés sur Internet puisqu'il est passé en dessous de Internet Information Server en terme de nombre d'utilisateurs. Le fait que Netscape Enterprise Server puisse fonctionner sur les principaux systèmes UNIX et sur toutes les architectures Windows NT, ne parvient pas à en faire le produit le plus utilisé. Depuis qu'Apache fonctionne sous Windows 95 et NT, l'avantage d'un serveur multi plate forme n'est plus l'argument unique de Netscape. Le serveur Netscape possède ses API (Application Programming Interface), appelées NSAPI, qui sont bien sûr différentes de celles proposées par Microsoft sous le nom de ISAPI. Aujourd'hui les produits périphériques des serveurs http, comme les connexions base de données sont généralement ISAPI et NSAPI mais une étude statistique prouve que ISAPI est davantage suivi que NSAPI. Les dernières versions de Netscape comprennent une interface JAVA Applet API qui permet au serveur de lancer des programmes JAVA de façon plus rapide, en gardant en mémoire l'interpréteur JAVA. Les interfaces de maintenance par le web ou par des programmes spécifiques sont d'aussi bonne facture que celles proposées par Microsoft. Ainsi la version 3 de Netscape Enterprise Server équivaut à la version 4 d'Internet Information serveur. Il est à noter un compilateur JavaScript sur le serveur permettant de générer de façon dynamique les codes HTML. Netscape a rejoint quelques technologies intéressantes telles que LDAP (Lightweight Directory Access Protocol, voir Glossaire) et CORBA (Common Object Resquest Broker Architecture, voir Glossaire). Enfin Netscape Enterprise Server se décline en produits de bureautique avec une version personnelle de développement FastTrack fournie avec une version de Communicator accompagnée de son éditeur HTML.

Coût : Netscape Enterprise Server coûte environ 1 100 000 FCFA

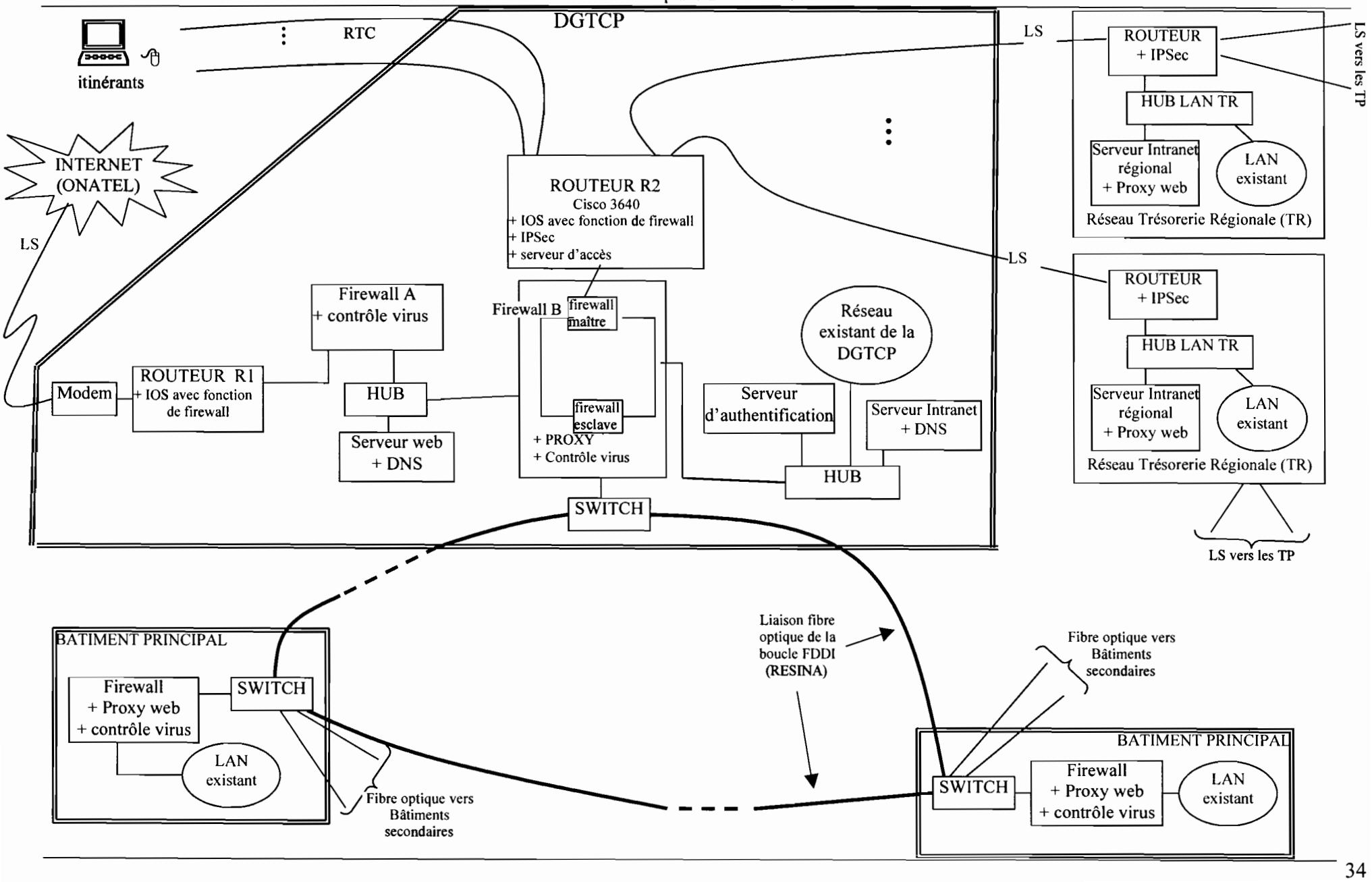
Installation et configuration : Ce logiciel serveur s'installe beaucoup plus facilement sous environnement Windows NT (Windows NT Server 4.0 est disponible à la DSI) et même dans les environnements Linux actuels.

VI. PRESENTATION DETAILLEE DE LA SOLUTION RETENUE

6.1. Architecture proposée

Pour la mise en œuvre de l'Intranet du MEF, il est préférable, au regard des avantages et inconvénients des scénarii présentés, que le scénario 2 (décrit dans l'étude comparative des solutions possibles) soit retenu avec une installation de la ligne spécialisée vers l'ONATEL. Malgré le fait qu'elle engendre des coûts mensuels de location modem sur une année (94 400 FCFA), cette solution est techniquement performante car garantissant un débit relativement élevé aux utilisateurs du MEF accédant à l'Internet. C'est une solution tendancielle qui intègre au maximum l'environnement existant (matériels et logiciels) en gardant à vue les aspects liés à la performance technique.

Remarquons qu'en dehors des problèmes de performances de la liaison, l'installation de la ligne spécialisée, qu'elle soit effectuée vers l'ONATEL ou la DELGI, ne change rien quant à l'architecture matérielle proposée.


DGTCP
RTC
itinérants
INTERNET
(ONATEL)
LS
ROUTEUR R2
Cisco 3640
+ IOS avec fonction de firewall
+ IPSec
+ serveur d'accès
Firewall A
+ contrôle virus
Firewall B
firewall maître
firewall esclave
+ PROXY
+ Contrôle virus
Modem
ROUTEUR R1
+ IOS avec fonction de firewall
HUB
Serveur web
+ DNS
Réseau existant de la DGTCP
Serveur d'authentification
Serveur Intranet
+ DNS
HUB
SWITCH
LS
ROUTEUR
+ IPSec
HUB LAN TR
Serveur Intranet régional
+ Proxy web
LAN existant
Réseau Trésorerie Régionale (TR)
LS vers les TP
LS
ROUTEUR
+ IPSec
HUB LAN TR
Serveur Intranet régional
+ Proxy web
LAN existant
Réseau Trésorerie Régionale (TR)
LS vers les TP
BATIMENT PRINCIPAL
Firewall
+ Proxy web
+ contrôle virus
SWITCH
LAN existant
Fibre optique vers Bâtiments secondaires
Liaison fibre optique de la boucle FDDI (RESINA)
Fibre optique vers Bâtiments secondaires
BATIMENT PRINCIPAL
SWITCH
Firewall
+ Proxy web
+ contrôle virus
LAN existant

6.2. Aspects logiciels

6.2.1. Banque de documents, workflow et messagerie

Au regard de la similarité de leurs fonctionnalités, les logiciels GroupWise et Lotus Notes (cf. Etude comparative) peuvent être les solutions à la mise en place d'une messagerie interne et d'un système de gestion efficace des documents d'usage général et spécifiques aux agents du MEF. Ces deux outils sont également reconnus pour leur capacité à gérer le workflow de façon efficace. Pour la mise en œuvre, l'un des deux logiciels pourrait être choisi pour obtenir des performances quasi similaires.

Remarquons que Lotus Notes coûte beaucoup plus cher que GroupWise. Mais, Groupwise est une solution propriétaire (quand bien même certaines version fonctionnent sous Windows NT) alors que Lotus Notes est le standard mondial du groupware (fonctionne sur toutes les plates formes). Dans le processus d'acquisition des logiciels pour la mise en œuvre de l'Intranet, il importe de tenir compte de ces facteurs.

La technologie de réplication utilisée par Lotus Notes/Domino et la possibilité de choix d'un système d'exploitation moins cher et robuste (tel que les systèmes ouverts, logiciels freeware) sont des atouts importants qui peuvent motiver le choix de ce produit. Par ailleurs, du fait qu'il existe déjà au sein de l'Administration burkinabè des Intranets réalisés par la DELGI (Premier Ministère, Présidence,...) avec principalement la messagerie Lotus Notes/Domino comme principale fonctionnalité, nous pensons que le choix de Lotus Notes/Domino pour l'Intranet du MEF permettra de garantir la compatibilité avec les autres Intranets de l'Administration et d'assurer les communications inter-ministérielles au sein d'un Intranet généralisé et homogène. A ce niveau également, la technologie de réplication de Lotus Notes/Domino sera d'un apport considérable pour « l'Intranet administratif » : les différents serveurs Domino de l'Administration pourront s'échanger automatiquement et régulièrement des informations (bases de données).

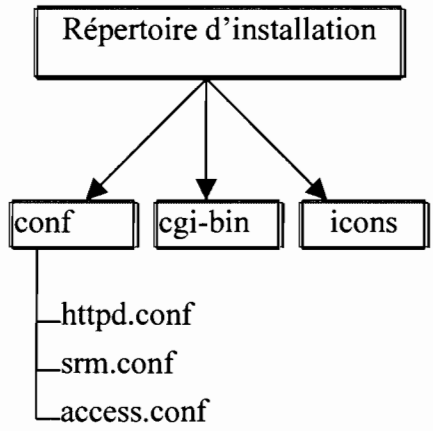
6.2.2. Serveur web et stockage de documents

Au regard de l'étude comparative, l'on retient que la mise en œuvre du système Intranet sous une plate Linux serait d'un avantage important à cause de sa robustesse technique et son coût moins onéreux. C'est pourquoi nous retenons le serveur web Apache pour le site web du MEF avec une plate forme Linux comme système d'exploitation.

Le logiciel Apache est actuellement le logiciel serveur http le plus utilisé dans l'Internet. Doté de nombreuses fonctionnalités, performant et gratuit, il constitue un choix très intéressant pour mettre en place un site web. Mais comme pour tout logiciel du genre, le fait d'offrir de nombreuses fonctionnalités implique également une complexité plus grande d'utilisation et en particulier de configuration. Cela entraîne également très souvent, dans le domaine de l'Internet, des problèmes potentiels supplémentaires concernant la sécurité.

6.2.2.1. Installation

L'installation du logiciel Apache se fait, par défaut, dans le répertoire **/usr/local/etc/httpd** . Ce répertoire contient en particulier un répertoire **conf** qui va contenir les fichiers de configuration d'Apache : **httpd.conf**, **srm.conf** et **access.conf**.



Ces fichiers sont organisés de la façon suivante :

- httpd.conf contient les directives de configuration générale
- srm.conf contient les directives concernant les ressources du serveur
- access.conf contient les directives concernant la politique d'accès au serveur.

Aujoud'hui (dans les versions de Linux les plus récentes), les deux derniers fichiers (srm.conf et access.conf) ont été transférés dans httpd.conf. On n'a dans ce cas qu'un seul fichier de configuration dans le répertoire *conf.*

A coté de ces trois (3) fichiers, on peut également utiliser des fichiers de configuration que l'on place dans les répertoires mêmes des documents du serveur. Ces fichiers ont un nom particulier (par défaut *.htaccess*) et peuvent contenir à peu près les mêmes directives que les 3 fichiers ci-dessus.

Les aspects sécurité du logiciel Apache ne concernent pas uniquement le fichier access.conf. Elles sont liées à l'utilisation d'un ensemble de directives qui se trouvent dans les 3 fichiers de configuration et à l'utilisation de certaines fonctionnalités du logiciel :

- politique d'accès aux documents : accès libre, filtrage par rapport aux domaines ou accès par utilisateur et mot de passe ;
- utilisation des programmes CGI ;
- utilisation des directives " Server Side Include " ;
- accès aux répertoires des utilisateurs de la machine où tourne le serveur Apache.

Remarque : Dans certains cas, les trois fichiers de configuration sont regroupés pour former un seul fichier : le fichier httpd.conf.

6.2.2.2. Configuration générale

La configuration du serveur Apache se fait par modification de fichiers textes : il s'agit principalement des fichiers htppd.conf, srm.conf et access.conf.

La configuration du fichier access.conf permet de définir les profils d'utilisateurs ayant accès à certains répertoires. Le fichier srm.conf permet d'indiquer les répertoires de stockages des fichiers du serveur web. Le fichier httpd est le fichier qui décrit le fonctionnement du serveur web. Il permet de

- définir le numéro de port TCP sur lequel le serveur scrute les requêtes (par défaut, le port 80) : choisir un numéro supérieur à 1024 (si on veut changer le port par défaut) ;
- définir la valeur de la directive ServerType : la valeur *standalone* permet au serveur, une fois lancé, de rester actif en attente des demandes des clients ;

- définir l'administrateur du serveur (ServerAdmin) ;
- le répertoire du fichier httpd.pid ; ce fichier contient le numéro du processus Unix du serveur.

6.2.2.3. Configuration des accès aux documents

Mettre en place un service web ne signifie pas pour autant rendre accessibles à tout le monde les documents du serveur. Certains services web ne sont d'ailleurs accessibles qu'à une certaine population. Cela signifie qu'il faut définir une politique d 'accès au service, décider qui a accès à quoi, et configurer le logiciel de manière à appliquer cette politique.
Le logiciel Apache comme la plupart des autres logiciels serveurs http permet deux (2) types de protection :

- une protection par domaine, qui permet de définir des droits d'accès en fonction des noms de machines ou de domaines
- une protection par utilisateur, qui permet de protéger tout ou partie du serveur par nom d'utilisateur et mot de passe.

La première méthode est simple à mettre en œuvre et ne nécessite pratiquement pas d'administration particulière. Par contre, la seconde implique la gestion de comptes utilisateur et donc plus de travail.
Les deux méthodes se définissent dans le fichier access.conf. Celui-ci contient au moins une directive <Directory> qui va définir la politique par défaut pour tous les documents du serveur. On peut ensuite ajouter des directives <Directory> pour modifier les caractéristiques de certaines sous-arborescences.
La directive <Directory> est un bloc pouvant contenir un certain nombre de sous-directives :

- Options : est suivi par une liste d'options possibles :
  - Indexes : indique que l'on peut avoir accès à la liste des fichiers des répertoires.
  - Includes : indique que l'on peut avoir des fichiers contenant des directives " Server Side Include " (SSI) dans cette arborescence.
  - includesNOEXEC : même chose que Includes mais on interdit la commande #exec ainsi que l'inclusion de script CGI.
  - FollowSymLinks : on autorise l'accès aux liens symboliques.
  - SymLinksIfOwnerMatch : on autorise l'accès aux liens symboliques si le propriétaire est le même aux deux (2) extrémités du lien.
  - ExecCGI : on autorise des programmes CGI dans cette arborescence.
- AllowOverride : indique si on peut ou non utiliser des fichiers de configuration à l'intérieur des répertoires. Ces fichiers, appelés par défaut .htaccess , peuvent contenir à peu près les mêmes directives que les fichiers httpd.conf, srm.conf et access.conf, et ne concernent que le répertoire dans lequel ils se trouvent. Les valeurs possibles sont :
  - All : les fichiers .htaccess sont autorisés.
  - None : les fichiers .htaccess sont interdits.
- On peut également utiliser l'une ou l'autre des valeurs suivantes :
  - AuthConfig : autorise les directives d'autorisation (AuthDBMGroupFile, AuthDBMUserFile, AuthGroupFile, AuthName, AuthType, AuthUserFile, require, etc.).
  - FileInfo : autorise les directives contrôlant le type des documents (AddEncoding, AddType, DefaultType, ErrorDocument, LanguagePriority, etc.).
  - Indexes : autorise les directives concernant la présentation des répertoires (AddDescription, AddIconByEncoding, AddIconByType, DefaultIcon, DirectoryIndex, FancyIndexing, HeaderName, IndexIgnore, IndexOptions, ReadmeName, etc.).

- Limit : autorise les sous-directives de la directive Limit (allow, deny et order).
- Options : autorise les directives Options et XBitHack
- <Limit> : est un bloc contenant des sous-directives permettant de définir les droits d'accès associés à une ou plusieurs méthodes d'accès (GET, PUT...) :

  order : indique l'ordre dans lequel on va définir les droits :

  order allow deny
  ou
  order deny allow

  allow : autorise un ou plusieurs domaines
  deny : interdit un ou plusieurs domaines
  require : dans le cas d'accès par utilisateur et mot de passe, indique le ou les groupes ou le ou les utilisateurs ayant accès.

Exemple :

```
<Directory /usr/local/etc/httpd/htdocs>
Options Indexes SymLinksIfOwnerMatch Includes
AllowOverride None
<Limit GET>
order allow,deny
allow from all
</Limit>
</Directory>

<Directory /usr/local/etc/httpd/htdocs/docs>
Options +ExecCGI
AllowOverride None
<Limit GET>
order allow,deny
allow from all
</Limit>
</Directory>
```

On suppose ici que /usr/local/etc/httpd/htdocs est le répertoire racine du serveur. Dans l'exemple ci-dessus, la première directive <Directory> permet de définir la politique général d'accès au serveur. La suivante spécifie les mêmes propriétés pour l'arborescence /usr/local/etc/httpd/htdocs/docs mais ajoute la possibilité d'y mettre des programmes CGI (+ExecCGI)

6.2.2.3.1. La protection par domaine

Elle consiste à donner, ou refuser, l'accès de certains documents en fonction du domaine auquel appartient la machine à partir de laquelle est faite la requête.

Exemple :

```
<Directory /usr/local/etc/httpd/htdocs/>
Options Indexes SymLinksIfOwnerMatch Includes
AllowOverride None <Limit GET>
order allow,deny
allow from all
</Limit>
</Directory>
<Directory /usr/local/etc/httpd/htdocs/local>
```

```
<Limit GET>
order deny,allow
deny from all
allow from .finances.gov.bf
</Limit>
</Directory>
```

Dans cette exemple, la première directive <Directory> indique que les documents du serveur sont accessibles à tout le monde. La deuxième directive <Directory> définit un filtre pour les documents dans /usr/local/etc/httpd/htdocs/local qui ne sont accessibles qu'aux machines appartenant au domaine finances.gov.bf.

6.2.2.3.2. La protection par utilisateurs

Pour mettre en place ce type de protection, il faut procéder de la manière suivante :

- récupérer ou compiler le programme *htpasswd* dont les sources sont fournies avec Apache
- créer avec cette commande un fichier (par exemple *htpasswd*) contenant les utilisateurs ainsi que leur mot de passe. Ce fichier a, à peu près, la même syntaxe que le fichier *passwd* sur les systèmes UNIX.
- créer à la main un fichier contenant les groupes d'utilisateurs, par exemple *htgroup*.
- Syntaxe : groupe : user1 user2 user3...
- mettre à jour le fichier *access.conf*

Exemple :

```
<Directory /usr/local/etc/httpd/htdocs/>
Options Indexes SymLinksIfOwnerMatch Includes
AllowOverride None
AuthType Basic
AuthUserFile /usr/local/etc/httpd/conf/htpasswd
AuthGroupFile /usr/local/etc/httpd/conf/htgroup
<Limit GET>
order allow,deny
allow from all
</Limit>
</Directory>

<Directory /usr/local/etc/httpd/htdocs/prive1>
AuthName Groupe dsi_users
<Limit GET POST>
require group dsi_users
</Limit>
</Directory>

<Directory /usr/local/etc/httpd/htdocs/prive2>
AuthName Prive2
<Limit GET POST>
require user traore
</Limit>
</Directory>
```

Dans cette exemple, on crée, pour tous les fichiers sous les arborescences /usr/local/etc/httpd/htdocs/prive1 et /usr/local/etc/httpd/htdocs/prive2, une protection par utilisateur. Dans le premier cas, l'accès est réservé aux utilisateurs appartenant au groupe dsi_users, dans le deuxième, seul l'utilisateur traore aura un droit d'accès.

- AuthType : indique le type d'authentification
- AuthUserFile : indique le nom du fichier utilisateurs
- AuthGroupFile : indique le nom du fichier groupe
- AuthName : indique une chaîne de caractère qui sera utilisé dans la fenêtre du navigateur qui demandera le nom d'utilisateur et le mot de passe.
  require : indique les utilisateurs ou les groupes d'utilisateurs qui ont le droit d'accès.

La principale difficulté dans ce type de configuration est de ne pas se tromper dans les noms de fichiers, de groupes ou d'utilisateurs.

6.2.2.4. Stockage et accès aux données bureautiques existantes

Le MEF dispose à ce jour d'un nombre important de fichiers créés à l'aide d'applications bureautiques (MS-Word, MS-Excel...) et stockés généralement sur les disques durs des machines des utilisateurs (secrétaires, chef de services...). Ces fichiers sont alors dispersés et l'exploitation par d'autres agents utilisateurs des informations qu'ils contiennent posent des problèmes. Par ailleurs, il serait fastidieux d'envisager la reprise intégrale de la conception de ces fichiers sous la forme de pages web. C'est pourquoi, il serait intéressant qu'on puisse stocker les fichiers de ces applications assistantes directement sans modification sur le serveur web et les rendre accessibles par les utilisateurs à travers leur navigateur. Pour ce faire, il faut définir le serveur pour qu'il reconnaisse les fichiers de ces applications.

Le serveur web utilise le mécanisme MIME (Multipurpose Internet Mail Extensions) pour identifier les documents en fonction de leur type/sous type de données MIME. Le mécanisme MIME partage les données en un nombre relativement restreint de types, chaque type regroupant un certain nombre de sous-types. Les documents de traitement de texte appartiennent au type de données *application*. Le serveur utilise l'extension du nom des fichiers pour associer ces fichiers avec un type de données MIME qu'il connaît. C'est le fichier de configuration *mime.types* du serveur qui réalise cette association. Pour définir le serveur de sorte qu'il reconnaisse le traitement de texte, il faut alors modifier ce fichier. Le fichier *mime.types*, quand il est édité contient, les deux lignes suivantes :

application /msword
application /wordperfect5.1

Ces deux entrées ne contiennent pas l'extension de fichier qui permet au serveur d'associer les fichiers de données avec l'application spécifique. Il faut alors compléter en associant à chaque type/sous-type MIME une ou plusieurs extensions. Word utilise normalement l'extension *.doc* mais on peut en ajouter d'autres.

Exemple :

application /msword doc rtf
application /wordperfect5.1 wp wpf wpd
application /msexcel xls xcl

Une fois que le serveur reconnaît les fichiers des applications assistantes, il faut configurer les navigateurs web des postes client pour qu'il puisse gérer les documents issus du traitement de texte. Netscape avec Windows possède une interface graphique pour définir des applications assistantes. La configuration de Netscape pour gérer les documents issus de traitement de texte se fait à partir du menu *Options* → *Préférences générales* (choisir l'onglet *Assistantes*).

Remarque : En environnement Linux, on pourra utiliser Netscape Composer pour développer les pages web.

6.2.3. Télémaintenance d'applications et de postes de travail

L'environnement informatique du MEF étant essentiellement dominé par le système d'exploitation réseau Netware, le produit ZEN Works (*Zero Effort Networks*) de Novell est le logiciel proposé par cet éditeur pour le déploiement d'applications et l'administration distante des postes de client. Il pourra servir, dans le cadre de l'Intranet du MEF à assurer la télémaintenance d'applications, et de postes de travail fonctionnant sur le réseau Netware. Pour ce qui concerne l'environnement Linux (proposé dans le cadre du site web, la messagerie externe et l'accès Internet), l'administration distante pourra se faire en utilisant les outils offerts par ce système (utilitaires, protocoles...). Pour l'administration globale du réseau du MEF, le logiciel ManageWise est proposé. ManageWise est un produit de Novell, basé sur le standard SNMP, qui permet de gérer et contrôler un réseau dans sa totalité. Avec ManageWise, on peut effectuer toutes les tâches de gestion de réseau à partir d'un seul point d'administration (le poste de l'administrateur) et gérer le réseau comme un système et non plus comme un ensemble de périphériques. Il permet de visualiser tous les équipements sur le réseau et des informations sur eux à partir d'une interface utilisateur convivial. Sa version 2.7 est compatible avec Netware 5 et tous les réseaux basés sur du TCP/IP pur.

Remarque : ZEN Works et ManageWise existent dans le patrimoine informatique du MEF, mais aucun d'eux n'est actuellement utilisé dans la gestion de ce patrimoine.

6.3. Connexion à l'Internet

6.3.1. Adressage

L'adressage est de toute première importance dans le réseau Internet. L'intérêt des utilisateurs est de pouvoir se connecter à n'importe quelle machine sur l'ensemble du réseau. Une adresse doit désigner de manière unique une machine et permettre au réseau de trouver facilement le chemin pour y accéder. En fait, une adresse IP ne représente pas une machine, mais une interface de cette machine. Comme la plupart des équipements ne possèdent qu'une interface, la confusion peut être faite. Par contre, si un équipement possède plusieurs interfaces réseau (routeur, serveur de fichiers connecté à plusieurs réseaux,...), il devra impérativement posséder plusieurs adresses IP. Pour qu'une machine puisse communiquer sur l'Internet, il lui faut donc nécessairement une adresse d'interface (IP) unique et facilement repérage de tous.

Au Burkina Faso, c'est l'ONATEL qui alloue les adresses de réseaux. Les classes d'adresses sont fournies au plan international par l'IANA (Internet Assigned Number Authority). Une adresse se divise en deux parties : le numéro de réseau et le numéro de la machine (de l'interface !) sur ce réseau.

Avant d'envisager son ouverture sur l'Internet, il est impératif que la DSI définisse un plan d'adressage de ses machines propre au MEF. Elle pourra alors créer des sous réseaux (par exemple, le sous réseau de la DGTCP, le sous réseau de la douane, le sous réseau du bâtiment principal du MEF...), faire une séparation logique des réseaux... Pour ce faire, il devra choisir une classe d'adresse conséquente. La classe d'adresse dépend du nombre de machines à connecter. Avec une adresse de classe A, le réseau peut contenir plus de 16 millions de machines (une politique actuelle consiste à ne plus attribuer ces adresses sauf cas exceptionnel, à cause de leur nombre très limité : 126 au plan mondial). Un réseau avec une adresse de classe B peut contenir jusqu'à 65 534 machines (stations de travail, micro-ordinateurs, imprimantes, routeurs, terminaux...). Environ 16 383 réseaux de classe B peuvent être définis sur le réseau Internet. Les réseaux de classe C, quant à eux, ne peuvent contenir que 254 machines. Pour l'ensemble du réseau du MEF, il serait

convenable d'utiliser une adresse de classe B compte tenu du nombre important des machines (*cf. 1.2. Système informatique existant*)

6.3.2. Utilisation des adresses réservées (pour les réseaux privés)

Pour chaque classe d'adresses, il est réservé des numéros IP qui ne seront jamais attribués :

Classe A : de `10.0.0.0` à `10.255.255.255`.

Classe B : de `172.16.0.0` à `172.31.255.255`.

Classe C : de `192.168.0.0` à `192.168.255.255`.

Ces adresses ne créent aucun conflit avec des sites sur l'Internet car n'étant attribuées à aucune institution. Avec l'utilisation du serveur proxy, il n'est pas nécessaire de demander administrativement l'adresse de classe B (proposée pour le plan d'adressage des machines du MEF) à l'ONATEL. La DSI peut choisir une adresse réservée de classe B pour définir son plan de numérotation IP en interne. Puisque ces adresses n'auront de signification qu' à l'intérieur du réseau privé du MEF, il conviendra alors de mettre en place un mécanisme permettant à ces machines de communiquer avec l'extérieur : c'est le proxy qui jouera ce rôle.

Le proxy devient alors un passage obligé pour toute communication avec l'extérieur. Seul son adresse est visible des machines de l'extérieur et se comporte comme un mandataire pour les machines du réseau interne qui désirent accéder à l'Internet : il reçoit les requêtes de ces machines, recherche l'information sur l'Internet en utilisant sa propre adresse et fourni au demandeur le résultat de la recherche. L'adresse du proxy doit être unique sur l'Internet et donc fournie par une institution habilitée.

VII. SECURITE VIS-A-VIS DE L'EXTERIEUR

La connexion des entreprises au réseau mondial est de plus en plus générale, aussi bien pour offrir un accès à l'Internet aux employés de l'entreprise que pour permettre l'échange de données avec le monde extérieur ainsi que la mise en place de services (site web, messagerie électronique, commerce électronique, banque à domicile (Home Banking...)). Le problème devient alors de différencier les services accessibles au grand public de ceux réservés aux seuls employés, voire à un certain type d'employés. Tout le monde doit pouvoir envoyer un mail à un employé quelconque, par contre l'accès à certaines ressources doit être réglementé. Les premiers essais en ce sens se composaient de mots de passe qui sont parfaitement efficaces tant que les utilisateurs ne tentent pas de dépasser leurs droits.

Malheureusement, les pratiques frauduleuses et malveillantes sont de plus en plus courantes sur l'Internet, avec une proportion relativement importante d'utilisateurs mal intentionnés. Les délits peuvent aller du simple détournement d'information à la dégradation pure et simple d'ordinateurs ou la mise hors service du réseau. Les motivations de malveillance vont de l'avantage individuel au vandalisme pur en passant par les défis (démontrer que l'attaque est possible sur tel système). Les enjeux financiers deviennent alors évidents.

Par ailleurs, des statistiques sur les dernières années écoulées montrent que les employés sont responsables de la plupart des failles de sécurité (70%). C'est pourquoi, une politique de sécurité qui ne tient pas compte des actions des utilisateurs internes est vouée à l'échec. Les employés doivent être des collaborateurs à la mise en œuvre d'un principe de protection vis-à-vis des attaques extérieures.

Il existe plusieurs types d'attaques extérieures :

- les attaques via le réseau : elles peuvent arriver si l'équipement d'interconnexion est mal configuré ou n'est pas adapté. Les risques sont l'intrusion (*des paquets non*

autorisés entrent sur le réseau), le déni de service (*des rafales de paquets paralysent une machine cible et lui empêchent de fournir un service normal*), le spoofing (*un paquet est émis avec une adresse IP falsifiée, de sorte à tromper les équipements du réseau cible*)...

- les attaques sur les serveurs : points critiques du système d'information, les serveurs constituent la cible privilégiée des pirates et doivent donc être protégés aussi bien vis-à-vis des utilisateurs externes que des utilisateurs internes. Les principaux risques sont le déni de service, des failles de sécurité des systèmes d'exploitation, serveur web..., les accès à des informations confidentielles...
- les attaques sur les mots de passe : elles peuvent consister en la récupération d'un fichier mot de passe ou la mise en œuvre par un pirate d'un mécanisme de détection de mots de passe triviaux.
- les attaques sur la messagerie : la messagerie constitue un des moyens les plus utilisés pour attaquer un système :
  - Le *email bombing* : envoi d'un message identique vers un email unique un grand nombre de fois ;
  - Le *email spamming* (variante de bombing) : envoi d'un message à un grand nombre de personnes ;
  - Le *email spoofing* : substitution d'adresse email source ; peut être combiné avec le bombing et le spamming.
- les attaques sur les services web : la mauvaise sécurisation du serveur entraîne des risques de déni de service, d'attaques par des applets java avec un comportement non maîtrisé, de mises à jour non autorisées du serveur...

7.1. Utilisation de firewalls

En plus de l'ouverture vers l'Internet, le fonctionnement de l'Intranet sur le RESINA est une menace pour la sécurité des informations au sein de cet Intranet. En effet, plusieurs bâtiments (réseaux locaux) du RESINA ne sont pas concernés par l'Intranet du MEF alors qu'ils devront utiliser un même support réseau : la boucle FDDI. Une politique de sécurité fiable et efficace est alors à mettre en œuvre. C'est pourquoi il est proposé l'utilisation d'un logiciel de filtrage des accès ou firewall. Un firewall, aussi appelé coupe-feu ou pare-feu, va consister en une machine ou un logiciel, voire un composé de ces deux éléments qui va servir d'interface entre le monde extérieur et l'Intranet. Son objectif va être de filtrer et de contrôler les informations entrantes et sortantes. Pour cela, il va falloir ne laisser aucun accès direct avec le monde extérieur, toute voie de sortie de l'Intranet étant protégée par un firewall. Tout accès non gardé deviendra une menace pour le réseau mais aussi pour le firewall lui- même, puisqu'il pourrait ainsi être désactivé de l'intérieur. Mais pour un Intranet relativement vaste comme celui du MEF, le contrôle de chaque utilisateur étant difficile, la solution sera de compartimenter les différents secteurs de l'Intranet, chaque secteur étant protégé par un firewall (*cf. Architecture proposée*).

Notons par ailleurs que l'utilisation de firewalls nécessite qu'un certain nombre de précautions soient prises. Il est impératif de protéger le firewall lui-même ; en particulier qu'il soit impossible de se connecter au firewall, y compris à partir de l'Intranet, à moins d'être l'administrateur. Le système d'exploitation du firewall doit être cloisonné afin d'éviter une intrusion par défection de ce dispositif de sécurité. L'une des protections les plus efficaces en matière de firewall est la mise en place d'un Intranet de nature différente de l'Internet : l'allocation de numéros aux machines de manière totalement différente de celle utilisée sur l'Internet, avec le firewall comme traducteur d'adresse permet d'empêcher la découverte d'une machine par une personne extérieure. Mais une autre faiblesse des firewalls se présente alors : il convient de limiter

le nombre de personnes s'occupant de la sécurité et donc ayant une facilité d'utilisation abusive de l'Intranet.

Il est préconisé qu'en plus de l'installation des serveurs firewalls, il soit mis en œuvre les fonctionnalités de firewall des routeurs Cisco. En effet, la plate forme logicielle Cisco IOS Firewall Software contient des fonctions essentielles qui permettent la mise en place d'un premier niveau de sécurité (détection des intrusions, authentification et habilitation dynamiques des utilisateurs, blocage d'applets Java, listes de contrôle d'accès standards et étendues...).

7.2. Protection contre les virus

Pour sécuriser les ordinateurs et préserver l'intégrité des données au sein du réseau, il convient d'installer des logiciels antivirus puissants sur tous les postes. Les logiciels antivirus (de par leur nom) détectent et détruisent les virus. Les virus étant de plus en plus sophistiqués, les antivirus ont dû, au fil du temps s'adapter et devenir de plus en plus performants sous peine de devenir obsolètes. En effet, avec l'accroissement constant du nombre de virus, les développeurs d'antivirus doivent sans cesse actualiser leurs produits. Il est souhaitable que l'utilisation actuelle de logiciels antivirus au niveau des postes de travail soit conservée dans l'ensemble du réseau. Ceci permettra d'éviter d'infecter et de propager des infections virales au sein du réseau à partir de postes de travail.

Remarquons que les principaux moyens de propagation des virus par le réseau sont les fichiers attachés aux messages SMTP et les flux FTP et http entre réseaux. C'est pourquoi, il est proposé qu'à chaque entrée du réseau du MEF soit installé sur la machine serveur firewall un logiciel de contrôle de virus (*cf. Architecture proposée*). Ce principe permettra de « scanner » tous les paquets passant par le firewall pour y détecter d'éventuels virus.

Aussi, faudra-t-il mettre à jour ces logiciels de façon périodique de sorte qu'ils ne soient obsolètes et donc inefficaces vis-à-vis des nouveaux virus. L'évolution des virus est aussi croissante qu'on ne peut prétendre être à même de détecter tous les virus avec l'utilisation d'antivirus. Un nouveau virus peut pendant un bon moment défier tous les antivirus existants malgré les mises à jour périodiques. La méthode des antivirus n'est alors pas suffisante pour se protéger des intrusions virales. Il faudra envisager :

- un filtrage sur certains fichiers tels que les fichiers exécutables au niveau des firewalls. Seul l'administrateur pourra manipuler ces types de fichiers à travers le réseau. Pour tous les autres utilisateurs, leurs fichiers exécutables devront subir un contrôle d'identité strict avant de les autoriser ;
- que certains postes de travail soient mis, pour des besoins spécifiques, sous environnement Linux : en effet, à la différence des systèmes Windows, Linux ne favorise pas la propagation de virus à l'heure actuelle.
- des sauvegardes périodiques des données du système de sorte qu'il soit possible de les restaurer en cas d'attaque virale irréversible.

7.3. Mots de passe

L'accès à certaines ressources du réseau doit être soumis à l'utilisation de mots de passe. Chaque utilisateur de l'Intranet disposera d'un mot de passe individuel qu'il aura l'autorisation de modifier. Par contre, l'administrateur seul aura le droit de supprimer ou de modifier certains fichiers stockés.

Une sécurité doit également être assurée pour le serveur web. Elle consiste à limiter l'accès du serveur à des clients suivant des critères tels que :

- des limitations sur les répertoires et sur les fichiers ;

• des protections sur certains fichiers spécifiques par un mot de passe ;

• les ACL (*Access Control List*) qui contiennent des informations sur les personnes, les groupes et les adresses IP qui ont le droit d'accès à des fichiers ou des répertoires ;

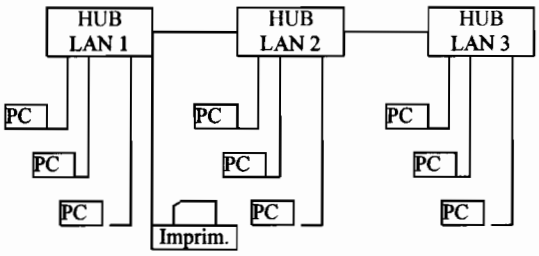
• les fichiers *password,* qui contiennent les mots de passe et les noms des utilisateurs qui ont accès au serveur ;

• les fichiers de groupe, qui contiennent des groupes d'utilisateurs qui ont le droit d'accès au serveur.

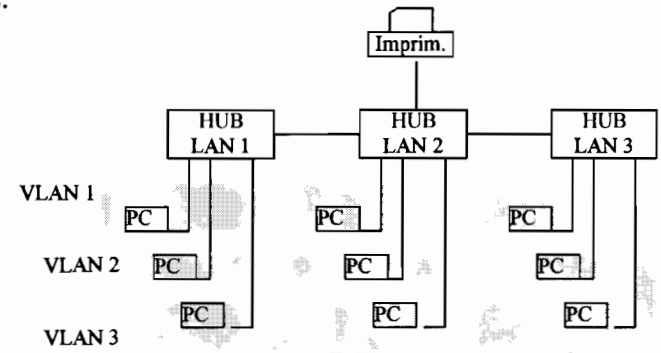
7.4. Création de VLAN

Les VLAN (*Virtual Local Area Network*) ou réseaux locaux virtuels sont des sous réseaux qui, une fois configurés, peuvent exister et fonctionner logiquement en tant que segments de réseau sécurisés et uniques. La technologie est idéale pour un réseau étendu comme le RESINA. Les VLAN offrent un moyen de définir des nouveaux chemins dynamiques sur le réseau et de créer des segments de réseaux virtuels novateurs qui s'étendent bien au-delà des limites traditionnelles des groupes de travail géographiquement isolés. En utilisant des commutateurs, on peut créer des VLAN sécurisés composés d'équipements sélectionnés répartis dans toute l'entreprise de sorte à ce que des personnes qui sont physiquement dans le même réseau local soient sur des VLAN différents. Cette technique permet de définir une catégorie de service ayant accès à une certaine partie du réseau global. On pourra par exemple créer le réseau virtuel des DAAF et/ou DRH de Ministères pour leur permettre de communiquer et travailler sur des applications spécifiques avec une sécurité et une confidentialité garanties des données manipulées.

Exemple :



RESEAU TRADITIONNEL A BASE DE HUBS



ETABLISSEMENT DE CONNEXIONS VIRTUELLES AVEC DES VLAN

Il existe plusieurs méthodes de construction de VLAN :

- définition par port : il s'agit de définir à quel VLAN appartient chaque port de l'appareil de connectique (hub, commutateur...). Son avantage, c'est qu'elle est facile d'emploi. L'inconvénient est qu'on ne définit qu'un seul VLAN par port.
- définition basée sur l'adressage MAC : il s'agit de dire quelles adresses MAC (adresses physiques) appartiennent à tel VLAN. L'avantage est que des stations sur un même port peuvent être sur des VLAN différents. L'inconvénient, c'est la difficulté de manipulation des adresses MAC.
- définition basée sur des informations de niveau 3 : il s'agit de définir, en utilisant les adresses IP (*Internet Protocol, niveau 3*), un VLAN par sous réseau. Cela permet une configuration plus aisée (par sous-réseau ou plages d'adresses IP). De plus, des stations sur un même port peuvent appartenir à des VLAN différents.

7.5. Exploitation de la fonction de filtrage du routeur

En utilisant la fonction de filtrage du routeur, on peut, avec des règles appropriées, autoriser ou interdire un certain nombre de services ainsi que bloquer l'accès aux équipements du réseau, tout en permettant à ses machines l'accès aux services de l'Internet. Le routeur route les paquets entre des hôtes internes et externes de façon sélective. Il examine chaque paquet puis il l'autorise ou le bloque selon les règles de filtrage. Pour ce faire, le routeur doit être configuré avec une liste d'accès (*access list*). Une liste d'accès définit les conditions pour qu'un paquet puisse franchir un routeur. Les informations contenues dans ces listes portent sur :

- le numéro du protocole de niveau 3, les adresses IP, les numéros de ports, etc. ;
- d'autres informations dans le paquet comme les drapeaux TCP ;
- le type de la règle, c'est-à-dire soit une autorisation, soit un refus de faire traverser le paquet.

Quand un paquet arrive sur le routeur, la liste est parcourue et le traitement du paquet est lié à la première condition rencontrée qui correspond au paquet. L'ordre d'entrée des conditions dans la liste d'accès est de ce fait très important. L'avantage de cette technique est son coût (les fonctions de filtrage étant disponibles sur le routeur) et la transparence pour les utilisateurs. Ses inconvénients sont que :

- elle nécessite une bonne connaissance des formats d'en-tête des paquets ;
- la configuration peut être longue et difficile, surtout si le nombre de postes est important ;
- le débit des paquets diminue lorsque le nombre de règles augmente ;
- elle ne prend pas de décisions basées sur les données.

Dans le cas du MEF où les machines doivent être inaccessibles de l'extérieur, sauf le serveur web et le service de messagerie qui peuvent être consultés par n'importe quel équipement connecté à l'Internet, la liste d'accès doit pouvoir interdire toutes les connexions venant de l'extérieur, sauf vers le port 80 (port par défaut du protocole http) de la machine mettant en œuvre le serveur web.
Exemple : liste d'accès pour le cas du service web

Règles	Action	Protocole	Source		Destination	
			Adresse	Port	Adresse	Port
1	Autorise	TCP	*	*	Serveur	80
2	Autorise	TCP	Serveur	80	*	*
3	Interdit	*	*	*	*	*

La règle 1 indique que le routeur laissera passer les paquets destinés à la machine « Serveur » pour le port 80. L'adresse source (notée *) que contient ce paquet est indéterminée puisque n'importe quelle machine connectée au réseau Internet est autorisée à accéder au service web. Le numéro de port source est aussi indéterminé car celui-ci est choisi dynamiquement par le client au moment de l'ouverture de connexion.

La règle 2 est symétrique de la première ; elle autorise le routeur à laisser passer les réponses du serveur au client distant.

La règle 3 empêche tout autre paquet de traverser le routeur. Elle permet d'appliquer la philosophie du « *tout ce qui n'est pas explicitement autorisé est interdit* ». Cette règle est la plus sûre, car il est nécessaire d'indiquer tous les services qui pourront être utilisés dans le réseau. Sur certains équipements, cette règle est implicite, et par conséquent, il n'est pas nécessaire de la donner.

7.6. Importance du serveur proxy

Le MEF disposant d'applications très sensibles dont l'accès par des personnes non autorisées entraînera inévitablement des conséquences désastreuses et catastrophiques (circuit informatisé de la dépense publique, SIGASPE...), il convient de contrôler efficacement les accès à l'Intranet à partir de l'extérieur, notamment de l'Internet. Le rôle du serveur proxy est alors très important dans ce processus de sécurisation. En effet, il permettra de masquer à l'Internet toutes les adresses IP du réseau interne. Concrètement, lorsqu'un employé se procure des informations Internet à partir d'un ordinateur de l'Intranet, le site Internet contacté ne détient jamais que l'adresse IP du serveur proxy, et en aucun cas l'adresse IP de l'ordinateur du réseau interne. Un pirate mal intentionné, à l'affût des échanges de données, ne lit par conséquent que l'adresse du proxy. Si ce n'était pas le cas, il pourrait découvrir l'adresse de l'ordinateur client puis s'identifier par IP-Spoofing en tant qu'utilisateur légitime (et même en tant qu'administrateur) auprès du réseau interne. Les conséquences sont incalculables. C'est pourquoi, nous proposons qu'en plus de la mise en œuvre des fonctions de filtrage du routeur et l'installation des serveurs firewalls, et au regard des faiblesses de ces dispositifs (cf. 7.1 et 7.5), soit installé sur la machine serveur firewall B un serveur proxy par lequel tous les postes en interne passeront pour accéder à l'Internet ou aux serveurs web et mail du MEF. Le proxy reçoit les demandes d'accès Internet des postes de travail et autorise les connexions. Pendant que l'utilisateur est connecté, les informations qu'il reçoit sont celles qui lui sont envoyées par le serveur proxy et les requêtes qu'il envoie vers l'extérieur le sont par le serveur proxy qui s'identifie sur l'Internet (ou le site web du MEF) comme étant le demandeur de l'information. Cette méthode empêche les postes de l'Intranet d'envoyer leur propre adresse sur l'Internet, ce qui constituerait une porte d'entrée pour les pirates. Le logiciel Firewall1 de CheckPoint peut servir à l'installation du serveur proxy. D'autres logiciels serveurs proxy existent sur le marché, mais certains ne sont pas très fiables et méritent une attention particulière. Dans certains cas, la prise en main par le pirate du système d'exploitation sur lequel fonctionne le proxy peut lui permettre de s'infiltrer dans le réseau. C'est pourquoi, il serait intéressant que le serveur proxy soit robuste et dispose de fonctions d'alarme pour informer des tentatives d'intrusion tout en fournissant des statistiques sur ces tentatives d'intrusion.

7.7. Technique du chiffrement

Il existe au MEF trois applications principales qui sont le circuit informatisé de la dépense publique, l'application de la Solde (SIGASPE) et l'application de gestion de la comptabilité intégrée de l'Etat et dont la sécurité des données est assez importante. Ces trois applications sont accessibles par des utilisateurs diversifiés et travaillant dans des bâtiments du RESINA géographiquement distants. La traversée du domaine public pour assurer les interconnexions et échanger les informations est alors une menace importante pour la sécurité, la confidentialité et la conformité des données. Une personne de mauvaise moralité peut se placer sur la fibre optique de la boucle FDDI du RESINA avec un logiciel approprié et intercepter toutes les communications entre serveurs et postes de travail. Les données de la Solde ainsi que celle de la Comptabilité Intégrée de l'Etat (CIE) n'ont plus alors leurs confidentialité et sécurité garanties car pouvant être interceptées sur la ligne spécialisée reliant la DGTCP aux trésoreries régionales. Certaines transactions peuvent subir des modifications et les transactions amorales peuvent se multiplier. Il devient alors nécessaire de crypter les informations échangées sur l'ensemble du réseau passant par le domaine public.

La fonctionnalité IPSec offert par les routeurs Cisco utilisés pour l'interconnexion des Trésoreries Régionales permet la mise en œuvre du cryptage. Toutes les communications entre routeurs de ce réseau « inter-provincial » sont chiffrées de sorte qu'elles ne puissent pas être décodées par n'importe qui sur le réseau. La technique utilisée est celle du chiffrement asymétrique

à clé double. Les systèmes asymétriques utilisent deux clés : une clé publique qui permet d'encrypter les messages et une clé sécrète utilisée pour le décryptage. Le clé publique peut être diffusée sans problème, alors que la clé privée n'est connue que du seul destinataire. Ces types d'algorithmes sont aussi utilisés pour générer des signatures digitales qui permettent d'authentifier l'auteur d'un message. Dans ce cas la clé sécrète est utilisée pour encoder la signature (un petit bloc de données) et la clé publique pour le valider (*cf. RSA, DSA et DSS dans le glossaire*).

Sur le RESINA, on pourra utiliser (en cas de nécessité) des boîtiers de chiffrement qui sont des équipements spécifiques dédiés au cryptage. Dans ce cas, il faut installer dans chaque bâtiment principal du RESINA un boîtier entre le serveur firewall et le commutateur d'interconnexion et dans chaque bâtiment secondaire du MEF un boîtier à l'entrée du réseau local. Remarquons que cette solution coûte relativement cher ; mais elle diminue encore davantage les risques de malversations sur les dépenses budgétaires, les ordonnancements, etc.

Par ailleurs, l'utilisation de PGP (*Pretty Good Privacy*) pourra être envisagée. PGP est un système de chiffrement de données très répandu basé sur l'utilisation des deux systèmes de clé. Les systèmes symétriques sont beaucoup plus rapides que les systèmes asymétriques, mais ils nécessitent de connaître la clé utilisée. Les systèmes asymétriques offrent une plus grande souplesse puisque l'encryptage est effectuée à l'aide de la clé publique du destinataire. PGP utilise les avantages des deux systèmes :

- le message à encrypter est encodé à l'aide d'une clé privée générée aléatoirement,
- la clé privée est encryptée à l'aide d'une clé publique,
- ce dernier code est inséré dans le message transmis.

Lors de la réception du message codé, PGP commence par décrypter la clé privée utilisée pour encoder le message (à l'aide de la clé sécrète du receveur). Il utilise ensuite cette clé privée pour décoder le message. PGP utilise l'algorithme RSA (voir glossaire) pour encoder la clé privée.

PGP est téléchargeable sur l'Internet.

VIII. TOLERANCE AUX PANNES – SECURITE INTERNE

Le matériel utilisé pour l'Intranet du MEF devra pouvoir résister aux différentes pannes susceptibles d'intervenir au cours de son exploitation. Une politique de tolérance aux pannes, mise en œuvre, permettra d'assurer la sécurité et la conservation fiable des données.

8.1. Utilisation des onduleurs

Tous les bâtiments principaux du RESINA où se trouve un réseau du MEF disposent d'une alimentation électrique sécurisée de grande capacité. Pour le serveur firewall, le commutateur et le boîtier de chiffrement, il convient de les protéger par une alimentation électrique ondulée pour éviter les reprises intempestives liées aux fréquentes ruptures de la fourniture de l'électricité courante.

8.2. Tolérance aux pannes disques

La gestion des disques durs peut se faire à l'aide des mécanismes de tolérance aux pannes dénommés RAID. RAID est un acronyme qui signifie "***Redundant Array of Inexpensive (or Independant) Disks***" soit un ***Réseau Redondant de Disques bons marchés***. Ceci est la définition historique, le terme "bon marché" étant utilisé en référence au système de sauvegarde de l'époque, de la taille d'une armoire et valant jusqu'à plusieurs centaines de milliers de francs. De nos jours, "inexpensive" est souvent remplacé par "independant".

La définition officielle de RAID est la suivante:

Une matrice de disques dans laquelle une partie de la capacité physique est utilisée pour y stocker de l'information redondante concernant les données d'utilisateurs. Cette information redondante permet la régénération des données d'utilisateurs perdues lorsqu'une unité ou un chemin de données à l'intérieur d'une matrice est défaillant.

Un système RAID **organise les données** parmi plusieurs disques durs et utilise un **processus de correction d'erreurs** afin d'assurer **la fiabilité** des archives. Le système d'exploitation voit la matrice de disques comme étant un seul disque. Il y a cinq types de RAID reconnus de RAID 1 à RAID 5. Ces classifications sont basées sur la division des données et sur les informations de corrections d'erreurs utilisées. De plus, le dépouillage des données sans redondance est communément dénommé RAID 0.

Augmenter la capacité : RAID permet de mettre "bout à bout" des disques durs, ce qui permet d'accroître la taille du volume.

Améliorer les performances : Les données sont écrites sur plusieurs disques à la fois. Ainsi, chacun des disques n'a qu'une partie des données à inscrire.

Apporter la tolérance de panne : Certaines configurations RAID permettent de se prémunir contre les défaillances d'un disque. Cette fonctionnalité est très importante, car sinon, la panne d'un seul des disques d'un ensemble RAID entraîne la perte des données de tous les disques. C'est d'ailleurs ce qui arrive au niveau de RAID 0.

Pour les serveurs Intranet et Internet (offrant les services mail, workflow, web...) du MEF, il convient de mettre en œuvre le RAID 5. Ce niveau de RAID fait appel à un contrôle d'erreur par calcul de parité pour créer un système de tolérance de pannes. Les fichiers sont découpés en paquets d'octets de la taille d'un cluster de disque dur, puis répartis sur n disques (et non plus n-1 comme en RAID 3 ou 4). Aucun disque dur n'est plus dédié au stockage des bits de parité, la tâche est partagée entre tous les disques. Ainsi le goulet d'étranglement de RAID 4 est éliminé. N'importe quel disque dur du volume peut tomber en panne sans causer la perte des données. Sa mise en œuvre nécessite au minimum trois disques. Le RAID 5 est un système à tolérance de panne qui, de plus, augmente considérablement les performances en lecture mais malheureusement se dégrade légèrement en écriture à cause du calcul de la parité. Il permet également de limiter le nombre d'unités logiques. La perte de place disque est moins grande que le cas du disque miroir (33% sur trois disques, 25% sur quatre, 20% sur cinq, etc.). Mais l'inconvénient est qu'il est plus cher (il faut commencer avec au moins trois disques, voire quatre).

RAID 5 (appelé le RAID le plus astucieux) est une solution très populaire et il existe de nombreuses implémentations sur le marché.

Les serveurs COMPAQ Proliant 3000 et IBM Net Finity utilisés à la DSI implémentent la technologie RAID. Il convient alors d'exploiter cette fonctionnalité pour assurer la protection des données. De plus, nous proposons que tous les serveurs à acquérir au MEF puisse mettre en œuvre cette technologie.

8.3. Sauvegardes

La technologie RAID n'est un système de sauvegarde ; ce n'est pas l'objectif des solutions RAID. Le RAID ne met pas à l'abri d'une erreur humaine telle que l'exécution malencontreuse d'une commande destructrice. C'est pourquoi même un système "protégé" par RAID doit être **sauvegardé régulièrement**.

Une sauvegarde des données implique une réelle **délocalisation** des données pour parer à tout accident grave (incendie, inondation, sabotage).

La sauvegarde peut consister en la mise en place d'un serveur secours pour la conservation des données stratégiques impliquées dans des processus de traitements dont la paralysie s'avère

coûteuse. Le serveur secours est une copie, ou presque, (sauvegardes périodiques sur le serveur) du serveur abritant les données à conserver. Ainsi, suite à l'intervention d'une panne sur le serveur habituel, le serveur secours peut être « monté » (en peu de temps) pour permettre aux utilisateurs de poursuivre leurs travaux. Le principe des sauvegardes doit également s'étendre à la conservation des données sensibles sur des supports tels que les cartouches de sauvegarde. Ces supports de données devront être gardés dans un bâtiment autre que celui abritant les serveurs de données. Cette précaution permet d'éviter qu'un accident grave (incendie, inondation, sabotage) intervenu dans le bâtiment des serveurs n'entraîne la disparition définitive de l'ensemble des données. Dans la même logique, les sauvegardes de différentes journées consécutives pourront être conservées dans des bâtiments différents.

8.4. Les pannes réseau

Le réseau de la boucle FDDI (RESINA) étant un réseau en anneau qui contient des hubs et des commutateurs « en cascade » aux différents nœuds d'interconnexion, une panne intervenue sur un hub principal ou sur un commutateur pourrait entraîner un blocage ou un isolement vis-à-vis de l'extérieur des postes ou réseaux locaux qui en dépendent. C'est pourquoi, il convient d'acquérir des hubs et/ou commutateurs secours en vue de remplacer immédiatement ceux qui s'avéreront défectueux. De plus, l'utilisation, par le MEF, d'appareils de connectique (hubs, commutateurs...) quasiment de même nature permet d'éviter d'acquérir, pour chacun de ces matériels, un double.

Par ailleurs, il est à noter que la mise en œuvre du RESINA avec la fibre optique (boucle FDDI) à double anneau est estimable et appréciée. Dans ce cas, les deux anneaux sont indépendants. En cas de rupture sur un anneau (entre deux bâtiments), le deuxième est utilisé pour l'acheminement des flux d'informations sans que cela ne transparaisse au niveau des postes utilisateurs.

Aussi, propose-t-on que les câbles fibres optiques qui permettent les interconnexions de bâtiments (à travers les conduits de l'ONATEL ou les nouveaux conduits) dans le cadre du RESINA soient blindés à l'extérieur. En effet, l'installation de câbles souterrains non blindés pose un problème de sécurité contre les intempéries et surtout les rongeurs.

8.5. Haute disponibilité des firewalls

Le principe consiste à utiliser deux machines physiques pour mettre en œuvre le serveur firewall. A ces deux machines on attribue une même adresse IP et on les configure de sorte qu'elles fonctionnent selon le principe maître/esclave. Les deux machines sont mises en activité en même temps et dès que « le maître » tombe en panne la machine esclave prend la relève immédiatement. Le principe présente une redondance de fonctionnalité, mais est assez efficace lorsqu'on veut garantir la sécurité des données sur un réseau sensible aux intrusions. La haute disponibilité des firewalls a été proposée dans l'architecture technique du réseau afin d'empêcher les utilisateurs non autorisés d'accéder au réseau du MEF suite à une panne intervenue sur le firewall. Elle minimise les risques d'intrusion et d'attaque.

8.6. Sécurité interne

La sécurité interne s'adresse aux agents utilisateurs du réseau du MEF. En effet, il peut arriver que certains agents, pour des intérêts personnels inavoués s'adonnent à des pratiques de reniflement (*sniffering*). En se connectant sur le réseau et avec un logiciel spécifique, ils peuvent capter toutes les communications qui y circulent. L'interception du mot de passe d'un DAAF de Ministère, par exemple, peut lui permettre d'effectuer des dépenses budgétaires fictives sur

l'application du circuit informatisé de la dépense publique, engageant ainsi la responsabilité juridique de ce DAAF. C'est pourquoi, il est nécessaire d'augmenter le niveau de sécurité interne pour dépasser l'usage du simple mot de passe, surtout pour la catégorie d'utilisateurs travaillant sur les données sensibles des applications du Trésor Public. On peut envisager un principe d'authentification forte à travers l'utilisation de cartes à puces électroniques qui contiendront pour chaque utilisateur un code spécifique qui est crypté avant d'être acheminé sur le réseau.

Par ailleurs, il important de sensibiliser les utilisateurs quant à la gestion de leurs mots de passe. En effet, beaucoup d'utilisateurs utilisent des mots de passe triviaux, faciles à trouver ou ne prennent aucune précaution quant au caractère secret du mot de passe. Il s'agit généralement d'un mot du dictionnaire, d'un nom ou un prénom, d'une date (de naissance, par exemple)... L'utilisation d'un algorithme peut permettre à un pirate de retrouver aisément un tel mot de passe. Il est conseillé d'utiliser des mots de passe relativement complexes et faciles à retenir (par exemple, les initiales des mots d'une phrase). Certains autres utilisateurs, sur la base de la confiance, fournissent volontairement leurs mots de passe à leurs collègues pour leur permettre de faire des travaux. Ces mots de passe ne sont généralement pas changés par leurs propriétaires. Les « nouveaux propriétaires » (les collègues) des mots de passe peuvent alors les utiliser, désormais sans l'avis des propriétaires originels. Les conséquences de tels actes sont inestimables et engagent les responsabilités individuelle et collective de tous les utilisateurs impliqués. C'est pourquoi, un mot de passe doit être choisi complexe et facile à retenir (avoir des indices permettant de le retrouver). Il est impératif qu'il soit individuelle, privé et secret.

8.7. Maintenance

Pour la maintenance du système, il est souhaitable que le MEF embauche un maintenancier pour s'occuper des questions techniques en matière de réseau, d'Internet et Intranet, ainsi que d'autres types de maintenance qui concerneront le matériel et les logiciels. Ceci permettra de fournir aux utilisateurs de services de qualité et d'éviter les problèmes inhérents au dépannage du système par des prestataires extérieures.

IX. SYNTHESE DES BESOINS

9.1. Besoins matériels

Matériel	Caractéristiques	Qté	Description	Existant
Commutateur (Switch)	Ethernet, double processeur, routage IP et IPX, double alimentation 220V/50Hz, alarme automatique, module d'administration	8	Interconnexion des bâtiments du MEF	Oui (cf. RESINA)
Routeur	Nombre extensible de cartes réseau, modem et voix, Fonctions de filtrage et de firewall, administrable SNMP, routage dynamique, IPSec, double alimentation 220/50Hz, processeur ASIC, accès distant, logiciel d'authentification	2	Nœud d'accès à l'Internet	1 existant 1 à acquérir
Hub	SynOptics et Super Stack de 3Com, 10/100 Mbps, 6 ports minimum	2	Pour les serveurs web et mail et le LAN de la DGTCP	Oui
Serveur Firewall	PC, Processeur Pentium Pro, fréquence 600Mhz, 128 Mo RAM, 2 cartes réseau, 16 Go disque dur	10	Serveur de sécurité, pour bâtiments principaux et l'entrée Internet du réseau	Non
Serveur (Intranet/web)	6 disques de 9 Go, nombre de disques extensible, lecteurs CD ROM et Disquette, Processeur Pentium II, au moins 128 Mo de mémoire RAM à 100 MHz en standard extensible à 4 Go, Contrôleur RAID 5	2	Serveurs web, FTP, workflow, mail, DNS…	Non
Serveur mail régionaux	PC, Processeur Pentium, fréquence 600Mhz, 128 Mo RAM, 2 cartes réseau, au moins 10 Go disque dur	5	Serveur de messagerie dans les TR	Oui
Serveur Authentification	PC, Processeur Pentium, fréquence 600Mhz, 128 Mo RAM, 2 cartes réseau, 16 Go disque dur	1	Serveur d'authentification des agents itinérants	Oui
Ligne Spécialisée	64 Kbits/s, vers l'ONATEL	1	Connexion à l'Internet	Non
Ligne téléphonique	Ordinaire	4	Connexion des travailleurs itinérants par RTC	Oui
Modem	56 Kb	1	LS vers Internet	Non
Scanner	Couleur, Format A4	1	Numérisation de documents à stocker (page web ou autres)	Oui
Micro-ordinateur PC	Pentium Pro, 64 Mo RAM, 300Mhz, multimédia, carte réseau et modem intégrés, lecteurs CD, disquette	1	Développements (pages web, applications workflow, …)	Oui

Remarque : Les routeurs dans toutes les Trésoreries Régionales et Principales sont des routeurs séries 2500 et 2600 et sont considérés ici comme existant.

9.2. Besoins logiciels

Logiciel	Caractéristiques	Qté	Description	existant
Lotus Notes/Domino	Version 5.0, Client Notes, Lotus Domino Server, Designer, Administrator. Logiciel de workflow et de gestion de documents.	1	Serveur workflow, Mail, gestion documentaire	Non
Linux	Distribution contenant le serveur web Apache, Telnet, FTP et l'ensemble du système d'exploitation	1	Serveurs web et Intranet	Oui[1]
ZEN Works	ZEN Works Version 2 ; Licence de 5 utilisateurs ; Version certifiée An 2000	1	Logiciel de déploiement d'applications et d'administration distante de postes clients	Oui
ManageWise	Version 2.7, basé sur le standard SNMP	1	Logiciel d'administration de réseau	Oui
Firewall1	De Check Point Software Technologies, logiciel de sécurité, fonctions de proxy intégrées, version certifiée An 2000	1	Pour serveurs de sécurité (Serveurs firewall)	Non
Cisco Secure	Logiciel de sécurité et d'authentification de Cisco	1	Pour serveur d'authentification	Non
VirusWall	Logiciel de contrôle de virus, Version la plus récente.	1	Pour serveurs firewall à l'entrée de chaque réseau	Non
Logiciel MS FrontPage Express	Développement de pages web (HTML), version certifiée An 2000	1	Pour le serveur web	Oui

[1] Linux est également téléchargeable sur plusieurs sites Internet (cf. Annexe 5)

9.3. Ressources humaines

La mise en œuvre ainsi que l'exploitation et l'administration de l'Intranet requiert des compétences en ressources humaines. Pour ce faire, nous proposons que l'on mette à la disposition du Service Réseaux et Systèmes (*cf. Annexe 6, Organigramme de la DSI*) un minimum de trois personnes ayant les profils suivants :

- un ingénieur de conception en Informatique ayant des connaissances :
  - dans la conception et l'administration des réseaux (LAN, MAN, FDDI) ;
  - dans la technologie Internet, ses protocoles et ses aspects sécuritaires ;
  - dans le domaine du groupware ;
  - des systèmes Unix, leurs langages et programmes ;
  - du système d'exploitation Netware ;
  - des concepts d'intégration des bases de données et le web ;
  - des techniques d'amélioration des performances des réseaux.

- deux ingénieurs de Travaux Informatiques ayant des connaissances
  - dans la conception des pages web ;
  - du système d'exploitation Netware ;
  - minimales des systèmes Unix ;
  - en analyse et conception de système d'information ;
  - en développement d'applications workflow ;
  - dans la topologie des réseaux, les protocoles de base, les différentes couches...
  - minimales de la technologie Internet.

X. EVALUATION FINANCIERE DES MATERIELS/LOGICIELS INEXISTANTS

L'évaluation financière des ressources informatiques à acquérir pour la réalisation de l'Intranet du MEF est estimée à un total de **40 866 000FCFA** reparti comme suit :

10.1. Matériels

Matériel		Quantité	PU HTHD	Total HTHD
PC (Serveurs firewall /proxy et haute disponibilité du firewall de la DGTCP)		10	1 150 000	11 500 000
Serveur (Intranet, web)		2	7 000 000	14 000 000
Modem 56 Kb		1	100 000	100 000
Routeur		1	3 000 000	3 000 000
Ligne Spécialisée (LS)	Création	1	472 000	472 000
	Raccordement	1	144 000	144 000
			Total général	**29 216 000 FCFA**

Remarque : L'installation de la LS engendre des coûts récurrents mensuels de redevance de **300 000 FCFA** (spécifique aux institutions gouvernementales) et une location vente de modem de **94 400 F CFA** par mois sur une année.

10.2. Logiciels

Logiciel	Quantité	Prix Unitaire HT	Total HT par produit
Firewall1 de CheckPoint	1	8 000 000	8 000 000
Lotus Notes/Domino 5.0	1	3 500 000	3 500 000
InterScan VirusWall	1	150 000	150 000
		Total général	**11 650 000 F CFA**

Remarque : Les coûts présentés dans ce document proviennent de la consultation de sociétés prestataires de services informatiques du Burkina Faso (Septembre-Octobre 2000). Il s'agit essentiellement de Liptinfor, Informatique Services et Soreco.

XI. DEMARCHE DE MISE EN ŒUVRE

Le plan d'action d'un Intranet doit être construit autour de quatre aspects principaux :

- ***L'aspect communication :***

- définir la « charte d'utilisation » de l'Intranet ;
- réaliser les premières applications dans les domaines présentant un niveau de stabilité suffisant et qui permettent de démontrer les avantages des technologies Intranet. Ces applications doivent donc intéresser un nombre important de personnes et être démonstratives pour les utilisateurs (pour disposer d'un retour d'expérience significatif et convaincre les utilisateurs de l'intérêt de ces technologies), mais également elles doivent permettre à la Direction des Services Informatiques d'évaluer les conditions de mise en œuvre et de fonctionnement de ces technologies.

- ***L'aspect infrastructure technique***

- regrouper les composants de base de l'architecture Intranet,
- mettre en place les premières briques de cette architecture (serveurs principaux, systèmes de sécurité, outils d'exploitation…
- déployer progressivement l'infrastructure.

L'accès aux applications du niveau précédent (communication) implique la mise en place d'un jeu de composants logiciels. Pour assurer un fonctionnement optimal de ces composants et pour simplifier l'accès à l'Intranet pour les utilisateurs, il convient de mettre en place plusieurs briques complémentaires qui s'avéreront indispensables pour envisager un usage plus large de l'Intranet par la suite.

- ***L'aspect organisation :***

- définir l'organisation d'exploitation ;
- définir l'organisation de publication et de mise à jour des données.

L'architecture Intranet doit s'intégrer dans l'architecture et l'organisation existante. Il est donc nécessaire d'introduire un minimum de cohérence dans la mise en œuvre de ces technologies, tant au niveau de l'architecture technique elle-même que de l'organisation et des règles de développement des applications.

- ***L'aspect applicatif :***

- définir les outils de développement communs ;
- définir les règles de développement communes ;
- accompagner les projets pilotes.

La Direction des Services informatiques est en mesure d'offrir à tous les acteurs du Ministère susceptibles d'utiliser les technologies Intranet un certain nombre de services qui doivent être définis et sur lesquels cette direction devra communiquer.

La mise en place pratique de l'Intranet du MEF impose une démarche modulaire qui consiste en un découpage en étapes du processus de réalisation. La démarche que nous proposons a été élaborée en tenant compte des priorités du MEF en matière d'Intranet, du degré de complexité des modules qui concourent à sa réalisation globale, mais aussi et surtout du degré de réalisabilité, à partir de l'existant, de chacun des modules identifiés. La durée de chacune de ces étapes dépend du volume de travail (nombre de pages à développer, nombre d'utilisateurs à former, types de

programmes à écrire ou d'applications à développer...) et de la complexité des processus de circulation des informations au sein des services.

11.1. Première étape

Elle consistera en une phase de préparation et d'analyse pour la mise en œuvre d'un système de gestion de base de documents et de workflow et une phase de mise en œuvre d'une messagerie interne restreinte. Au cours de cette étape, l'on s'attellera à

- rassembler tous les documents entrant dans le cadre de la gestion de bases de documents ;
- réaliser des interviews au sein des services afin d'identifier les différents processus de circulation de l'information, les dépendances et les relations existant entre eux ;
- identifier les groupes/équipes de travail possibles ;
- analyser et concevoir une solution d'automatisation basée sur le workflow ;
- installer et configurer la machine Intranet ;
- configurer la messagerie en interne sur une partie restreinte du réseau avec des utilisateurs avertis (par exemple, au sein de la DGTCP et de la DSI) ;
- configurer les postes de travail et créer les boîtes aux lettres ;
- Tester et évaluer les fonctionnalités mises en œuvre.

11.2. Deuxième étape

Cette étape est l'étape de réalisation technique de la banque de documents et de mise en place modulaire du workflow.

Les tâches à effectuer se présentent comme suit :

- mettre en œuvre le système de gestion documentaire ;
- identifier et créer les utilisateurs de la base de documents ;
- mettre en œuvre de façon modulaire, par processus et par service, le workflow ;
- faire les développements nécessaires ;
- tester la conformité globale des enchaînements entre les différents modules ;
- former les utilisateurs.

11.3. Troisième étape

C'est l'étape de mise en place des services web.
Pour sa mise en œuvre, deux équipes peuvent être mises en place :

➢ Une équipe de développement qui sera chargée de

- rassembler tous les documents entrant dans le cadre de la création de pages web ;
- numériser les documents (si nécessaire) à l'aide d'un scanner;
- distinguer clairement les documents dont les pages seront accessibles au grand public et ceux qui ne le seront pas ;
- identifier les documents qui feront l'objet de pages web interactives nécessitant la mise en œuvre d'autres technologies telles les bases de données, des programmes (scripts, CGI...) ;
- création de pages web statiques et dynamiques ;
- former les utilisateurs.

➢ Une équipe de conception et de configuration technique qui s'occupera de la mise en œuvre pratique du site web :

- installer et configurer le système Linux ;

- installer et configurer le serveur web (Apache) ;
- installer et configurer tous les systèmes de sécurité conséquemment ;
- stocker les pages web et définir les critères d'accès ;
- assurer la sécurité des pages (mots de passe, verrouillage...) pour les pages non destinées au public ;
- programmer au besoin des scripts ;
- étendre les services du serveur web à l'ensemble des réseaux du MEF interconnectés et fonctionnels ;

11.4. Quatrième étape

C'est l'étape d'ouverture vers l'Internet et de finalisation dans la mise en œuvre des principales fonctionnalités de l'Intranet. Il faudra alors

- installer la ligne spécialisée ;
- installer et configurer les serveurs firewall/proxy à l'entrée de chaque réseau du MEF ;
- installer et configurer le système d'accès distant (serveur d'authentification, client d'authentification...) ;
- configurer les accès à l'Internet ;
- installer et configurer les serveurs de messagerie des Trésoreries Régionales ;
- mettre en œuvre les mécanismes de communication de différents serveurs Intranet ;
- étendre la messagerie à l'ensemble du réseau et à l'extérieur ;
- mettre en œuvre complètement le workflow sur l'ensemble du réseau ministériel ;
- étendre les services web à l'extérieur (Internet).

XII. CRITIQUE DE LA SOLUTION PROPOSEE

12.1. Points forts

La solution proposée présente de nombreux avantages :

12.1.1. Au niveau de la sécurité

- Protection à deux niveaux : la mise en œuvre de deux systèmes de sécurité firewall est un atout très important pour la sécurité du réseau. Si la première machine firewall (firewall A) tombe en panne, seul le serveur web est exposé aux attaques ; le reste du réseau (et même tout le RESINA éventuellement) reste en sécurité.
- Gestion répartie de la messagerie : en cas de rupture d'une liaison entre une trésorerie régionale et la DGTCP, les agents de ladite Trésorerie Régionale peuvent continuer à bénéficier des services de messagerie électronique sur leur site et avec les trésoreries principales associées (en utilisant leur serveur mail régional).
- Cette gestion répartie de la messagerie ainsi que l'utilisation de proxy web sur chaque machine de messagerie régionale permettent d'optimiser le trafic des liaisons entre la DGTCP et les Trésoreries Régionales et donc d'améliorer les performances du réseau (le proxy se comporte comme un cache allégeant les charges des LS et ces LS ne seront utilisées pour la messagerie que quand il y a un besoin de communication inter-sites).
- Accès aux applications spécifiques du MEF : toute requête provenant d'Internet par le routeur R1 en direction d'un serveur d'application spécifique de la DGTCP passe

obligatoirement par deux niveaux de contrôle firewall (firewall A et B) et le serveur d'authentification.

- Gestion des attaques virales : tout message en direction d'un réseau du MEF quelle que soit sa provenance est soumis à un contrôle de virus. Cela permet d'éviter les propagations de virus à travers le réseau. De plus, d'autres mesures telles que le filtrage de certains types de fichiers et les sauvegardes périodiques permettent de réduire les risques de perte totale de données suite à des attaques virales.
- Accès par RTC ou de l'Internet : tout utilisateur du réseau du MEF désirant y accéder en dehors des limites physiques de ce réseau devra s'authentifier selon des critères bien définis avant d'y être autorisé.
- Chiffrement des données : la mise en œuvre de la technique IPSec sur les routeurs reliant les Trésoreries Régionales à la DGTCP permet de crypter les données (très sensibles) qui transitent par les supports lignes spécialisées de ce réseau, la traversée du domaine public étant une menace importante pour la sécurité des données.
- La solution proposée sépare clairement le réseau global en différents « sous-réseaux ». Un problème matériel ou logiciel intervenu dans un des sous-réseaux n'affecte pas forcément les autres.
- Sensibilisation des utilisateurs par rapport à l'usage strictement privé des mots de passe.
- Gestion des attaques virales : le filtrage (au niveau du firewall) de certains types de fichiers tels que les exécutables permet de réduire les risques d'entrée de virus. Par ailleurs, les sauvegardes périodiques permettent de restaurer les informations dans les cas où des virus arrivent à échapper aux logiciels antivirus installés.
- Prise en compte des données bureautiques existantes : la solution intègre

12.1.2. Au niveau des fonctionnalités

La solution globale proposée au terme de notre étude fait ressortir toutes les fonctionnalités attendues de l'Intranet du MEF : la messagerie électronique, le workflow, la gestion de documents, l'accès à l'Internet, les services web et l'administration distante.
Une des originalités de cette solution est la gestion des travailleurs itinérants qui ont un accès sécurisé au réseau au cours de leurs différents déplacements. Cette fonctionnalité permet de garantir la bonne marche du travail coopératif et des procédures informatisées de gestion administrative.

12.2. Services envisageables

La mise en œuvre complète de l'Intranet du MEF avec une ouverture sur l'Internet permettra à ce Ministère d'offrir de meilleurs services en interne, de s'ouvrir au monde extérieur et d'être une institution de proximité pour gérer aisément les nombreuses sollicitations et communications qu'elle effectue avec les citoyens et autres partenaires au développement. Par ailleurs, une fois les infrastructures de l'Intranet installées, il peut envisager, en plus des fonctionnalités attendues de la présente étude, d'offrir à ses agents d'autres types de services entrant dans la bonne marche des relations de travail et des prestations. Nous présentons ici quelques exemples de fonctionnalités que le MEF peut mettre en œuvre à partir de la solution Intranet proposée.

12.2.1. Assistance interne

L'assistance interne est une série de services destinés à l'utilisateur final :

- des informations sur la planification des stocks, leur évolution, ...

- des instructions pour effectuer par soi-même la maintenance de base des appareils sans recourir à chaque fois à un technicien spécialisé ;
- des pages FAQ (*Frequently Asked Questions*) qui contiennent les réponses aux questions les plus souvent posées ;
- des bons afin de commander du petit matériel (bureaux, consommables…) ;
- des annuaires avec les membres du personnel classés par services, par nom, … et avec les numéros de téléphone, les adresses de courrier Intranet ;
- des serveurs de logiciels afin d'installer automatiquement sur un ordinateur un programme dont on a besoin sans recourir au jeu de disquettes ou solliciter l'aide d'un informaticien ;
- etc.

12.2.2. Formation du personnel

Des pages peuvent être construites afin d'effectuer l'écolage de nouveaux employés. On leur explique les habitudes de l'institution, ce à quoi sert le réseau, les différents services et leurs rôles, et plus spécifiquement, on donne accès à des manuels, des instructions, des références nécessaires pour son travail. Un employé motivé peut ainsi découvrir rapidement et efficacement son institution et ce qu'on attend de lui.

12.2.3. Gestion des ressources humaines

- La gestion des demandes de congés, de permission, … à l'aide de formulaires (workflow) ;
- L'information des collaborateurs au quotidien ;
- La formation des employés à travers des applications multimédia, web,… pour permettre leur meilleure opérationnalité.

12.2.4. Gestion des appels d'offres

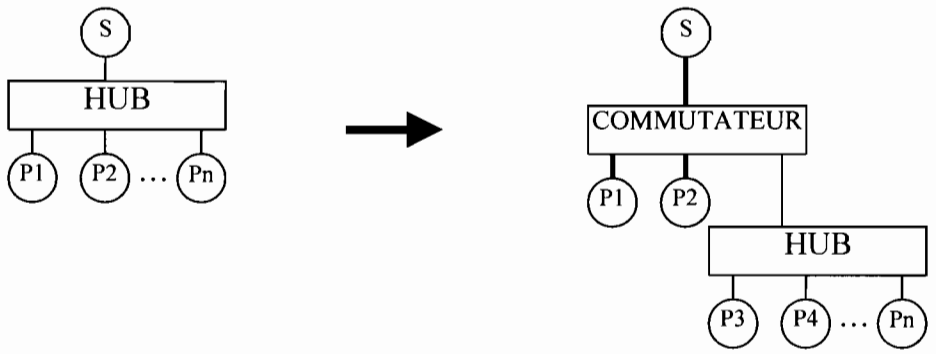
- La diffusion des informations à partir du site web ;
- La présentation de formulaires de candidature à remplir sur le web.

12.2.5. Forums de discussion et gestion des agendas

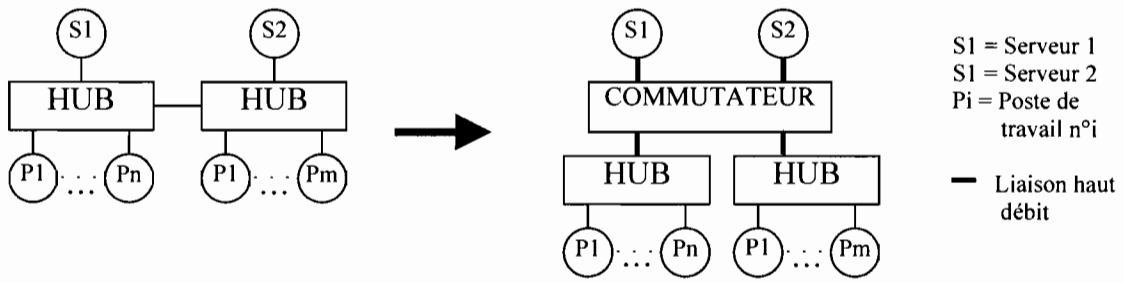
Les forums de discussion permettent d'entrer en contact avec des collègues pour parler de sujets d'intérêt commun sans que personne n'ait à se déplacer physiquement pour se rendre à une réunion. S'il en ressent le besoin, n'importe quel utilisateur peut créer un groupe de discussion et convier les personnes de son choix à y participer. Nul besoin de se demander où se trouve chacun et si son emploi du temps est chargé ou non. Les différents protagonistes suivent le fil du débat et apportent leur contribution pour des sujets d'intérêt pour le bon fonctionnement de l'administration. Il suffit d'ouvrir l'application pour afficher les sujets traités, participer à l'un d'eux ou lancer un nouveau sujet de discussion. Les forums peuvent également de dérouler en direct de façon interactive sous la forme d'une réunion ou d'une conférence où les questions sont traitées directement par les participants.

12.2.6. Restructuration du réseau

L'utilisation de commutateurs Ethernet dans les bâtiments principaux du RESINA permettra de réorganiser les réseaux locaux de ces bâtiments en déplaçant les stations fortement consommatrices de bandes passantes des hubs classiques vers des commutateurs. Les ports hauts débits pourront servir pour les interconnexions entre bâtiments et à relier les stations serveurs fréquemment sollicités. L'avantage d'une telle technique, c'est qu'elle améliore les performances du réseau.



De plus, dans le bâtiment de la DGCOOP-DGEP où deux réseaux locaux sont reliés à partir de leurs hubs, l'utilisation d'un commutateur permettra d'isoler les serveurs de ces réseaux. Ceci a l'avantage de supprimer les collisions générées par des communications vers des serveurs distincts.



Chacun de ces commutateurs doit disposer de ports hauts débits 100bFX (pour la fibre optique, 2 fibres multimodes) et 100bTX (paires torsadées catégorie 5) ou 100bT4 (paires torsadées catégories 3, 4 et 5).

PHASE DE REALISATION

XIII. CONFIGURATIONS MATERIELLE ET LOGICIELLE POUR L'IMPLEMENTATION

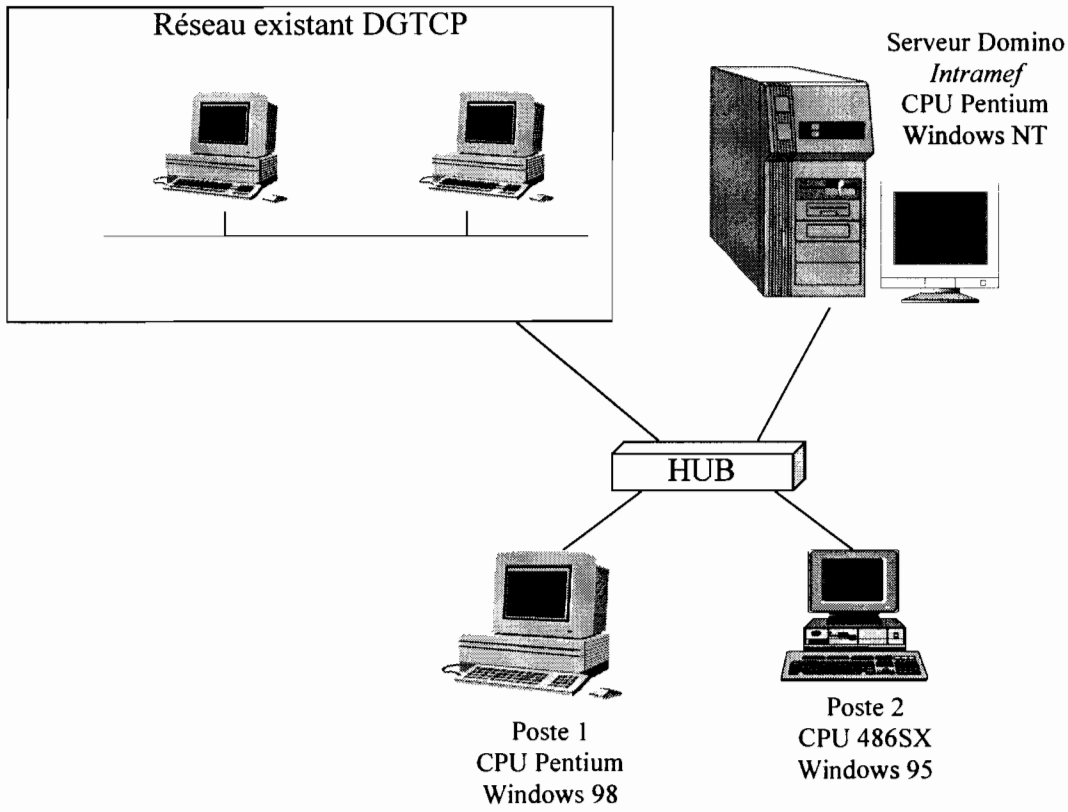
La phase de réalisation a consisté en la mise en œuvre pratique d'un prototype représentatif des fonctionnalités de l'Intranet en utilisant les ressources existantes.

13.1. Configuration matérielle

Le matériel utilisé pour la réalisation du prototype se compose essentiellement de trois (3) ordinateurs, d'un hub (SuperStack 10/100 Mbps de 3Com) et de câbles UTP (paires torsadées non blindées) catégorie 5. Les ordinateurs présentent les caractéristiques suivantes :

- un ordinateur serveur (*NetServer LH Plus*) avec CPU Pentium sur lequel nous avons installé le système d'exploitation Windows NT (*Windows NT Server 4.0*). Cet ordinateur de marque Hewlett Packard a une RAM de 97 Mo, six (6) disques durs de deux (2) Giga octets chacun, un lecteur de disquettes (3 pouces ½), un lecteur CD ROM, une carte réseau (*3Com 3C508 ISA Adapter*), un moniteur Super VGA (avec carte vidéo) ;
- un micro-ordinateur COMPAQ DeskPro de CPU Pentium équipé de Windows 98 avec une RAM de 64 Mo, un disque dur de 8 Go, un lecteur de disquettes (3 pouces ½), un lecteur CD ROM, une carte réseau (*3Com Fast Ether Link XL 10/100 Mb TX Ethernet NIC*), un moniteur couleur COMPAQ V55 ;
- un micro-ordinateur Hewlett Packard de CPU Intel 486 SX équipé de Windows 3.11 avec une RAM de 32 Mo, un disque dur de 200 Mo, un lecteur de disquette (3 pouces ½), une carte réseau, un moniteur couleur Super VGA avec carte vidéo. Compte tenu de contraintes liées à la réalisation du prototype (le client Lotus Notes disponible ne fonctionne que sous Windows 95 et supérieures ou Windows NT), le disque dur de cette machine a dû être formaté pour réinstaller la version 6.22 de MS-DOS et Windows 95 à partir de l'environnement DOS installé.

Ce matériel a permis la réalisation d'un réseau local type Ethernet d'une topologie physique en étoile en utilisant le hub de 6 ports. Le raccordement de ce hub au réseau global existant de la DGTCP permet aux utilisateurs du RESINA d'accéder au serveur Intranet. Pour le moment, seulement deux postes du réseau existant de la DGTCP sont configurés pour accéder au serveur Intranet : il s'agit de la machine du Chef du Service Etudes et Applications et de celle du Secrétariat de la Direction des Services Informatiques.



13.2. Configuration logicielle

Pour la réalisation du prototype seule une version promotionnelle de Lotus Notes/Domino d'une période d'essai de 90 jours est disponible.

13.2.1. Sur le serveur "intramef"

La version de Lotus Notes / Domino disponible est la Release 5 et fonctionne sous Windows NT en mode serveur (Lotus Domino Server) et sous Windows 95, Windows 98 et Windows NT en mode client (Lotus Notes). Pour l'installation du serveur Domino, un serveur Windows NT (Windows NT Server 4.0) a été préalablement installé. Le domaine du serveur est « GROUPWARE » et le serveur se nomme INTRAMEF. Une adresse IP de classe B choisie de façon aléatoire a été attribuée à ce serveur : `135.135.10.1`. Cette adresse ne pourra être utilisée qu'au sein de l'Intranet du MEF car n'ayant pas été fournie par une instance habilitée. Dans le cadre de la mise en œuvre du plan d'adressage globale des machines du MEF, cette adresse pourra être remplacée par une adresse choisie parmi celles de la classe utilisée.

Sur cette machine serveur équipé de Windows NT (comme système d'exploitation réseau), il a été installé le logiciel serveur Lotus Domino Server, les outils d'administration (Lotus Domino Administrator), les outils de développement (Lotus Domino Designor) et le logiciel client (Lotus Notes).

13.2.2. Sur les postes de travail

Les deux ordinateurs PC disponibles sont utilisés comme postes de travail des utilisateurs de réseau ainsi installé. Pour permettre à ces utilisateurs d'utiliser le serveur Intranet (intramef/finances/bf), le client Notes a été installé et configuré sur chacun des postes de travail.

Ainsi chaque utilisateur peut se connecter à la machine serveur du réseau Intranet, soit pour travailler sur son compte à partir du serveur NT (en tant que serveur de fichiers), soit pour des besoins de productivité de groupe (messagerie, workflow, ...) en utilisant le serveur Domino. Dans ce dernier cas, il devra lancé le client Notes à partir du poste de travail.

Remarques :

- Les programmes d'installation de Lotus Domino Server et Lotus Notes sont faciles à comprendre et simples à exécuter. Les programmes ont été installés directement depuis le disque compact (CD ROM Lotus Notes/Domino Release 5), sur la partition D du disque dur du serveur (coté serveur) et dans un répertoire (C:\Lotus) sur le disque dur du poste de travail (coté client).
- Pour installer le client Notes, il a été nécessaire de compresser le disque (200 Mo) du poste de travail de CPU 486 SX car ne fournissant pas assez d'espace disque pour l'installation du client Notes une fois Windows 95 installé.

La première fois qu'on met en fonction Domino sur un serveur ou Notes sur un poste de travail, un programme d'établissement des paramètres est invoqué (ce programme n'est pas le même pour le serveur et les postes de travail).

Le programme d'établissement des paramètres du serveur permet à l'administrateur de :

- définir un domaine ;
- activer le réseau et les ports série appropriés ;
- créer un carnet d'adresse public pour le domaine et y placer les documents nécessaires ;
- créer une identification de serveur (server.id) et une identification d'utilisateur (user.id) ; ces deux identifications devant être certifiées par le certifieur de l'organisation (cert.id) ;
- créer une méthode d'entrée en communication pour le serveur (connexion LAN ou connexion ligne téléphonique ou encore les deux) ;
- créer un répertoire de messagerie pour l'administrateur.

La plupart des tâches ci-dessus sont effectuées automatiquement, en fonction des informations communiquées par l'administrateur au moyen de boîtes de dialogue.

Le programme d'établissement des paramètres des postes de travail effectue des opérations limitées par rapport à celles du programme d'établissement des paramètres du serveur. Il raccorde le poste de travail au serveur et ajoute une icône de fichier de messagerie et le carnet d'adresse de l'utilisateur à son espace de travail.

Remarque : Le mot de passe de l'administrateur entré lors de l'établissement des paramètres du serveur est lisible quand il s'affiche à l'écran. Il vaudrait mieux prendre les précautions nécessaires de sorte qu'il ne puisse être lu par quelque personne que ce soit.

XIV. REALISATIONS EFFECTUEES

14.1. Organisation du serveur et des postes de travail

Tous les utilisateurs du réseau Windows NT installé disposent d'un compte (répertoire privé) créé sur le volume D du serveur et qui leur permet à chacun d'eux d'utiliser le serveur pour la gestion de leurs fichiers personnels à partir de leurs différents postes. Sur chacun des postes de travail du réseau de domaine GROUPWARE, est installé le client Notes et sur le serveur fonctionnent Lotus Domino Server, Lotus Domino Designer, Lotus Domino Administrator et le client Lotus Notes.

L'application fondamentale de Lotus Notes/Domino se rapporte aux bases de données, c'est-à-dire que ses fonctions d'exploitation s'appuient sur les bases de données (par exemple, le courrier électronique est constitué d'une base de données). Lorsqu'un utilisateur désire accéder à certaines informations contenues dans Notes, il doit accéder à la base de données appropriée. Les bases de données Notes se trouvent sur le serveur Domino où chaque utilisateur potentiel a accès, ou bien sur l'ordinateur d'un utilisateur qui peut en contrôler l'accès.

Lorsqu'un utilisateur invoque Lotus Notes, « un espace de travail » apparaît sur l'écran de son ordinateur (*cf. figure 14-1*). Cet espace de travail comprend des icônes symbolisant diverses bases de données (qui se trouvent sur le serveur Domino ou sur l'ordinateur de l'utilisateur) auxquelles l'utilisateur peut avoir accès. L'utilisateur peut organiser cet espace de travail en fonction de ses besoins particuliers.

Lorsqu'il clique deux fois sur l'icône d'une base de données, celle-ci s'ouvre et s'affiche dans une fenêtre pour lui permettre d'en examiner le contenu. Comme les bases de données sont en principe constituées d'un ensemble de documents, la fenêtre affiche une liste de tous les documents qui s'y trouvent. Cette fenêtre est divisée en deux volets (ce qui permet à l'utilisateur de trouver facilement les documents qu'il cherche) : un volet de navigation et un volet d'affichage. Le volet de navigation donne la liste des diverses vues et dossiers de la base de données. Ces vues et dossiers regroupent les documents de la base de données en fonction de formules (vues) ou de sélection effectuées par l'utilisateur (dossiers). Le volet d'affichage donne la liste des documents d'une vue ou d'un dossier sélectionné. En cliquant deux fois sur un document du volet d'affichage, l'utilisateur peut accéder à ce document.

Les documents dans Lotus Notes/Domino ne sont pas des fichiers de traitements de texte comme ceux de WordPerfect ou Word ; ce sont des documents basés sur des masques (ou formulaires). Bon nombre de divers masques sont définis pour créer divers types de documents dans Lotus Notes/Domino, mais l'utilisateur n'est pas tenu de s'en tenir seulement à ces masques. Tout utilisateur autorisé peut créer ses propres masques ou modifier ceux qui existent. Un masque est constitué de champs (il doit en comprendre au moins un). Un utilisateur crée un document en remplissant les champs et en sauvegardant les masques sur son ordinateur ou sur un serveur.

Il existe une base de données à laquelle tout utilisateur et tout serveur autorisés peuvent accéder : le livre d'accès public (Public Adress Book) ou carnet d'adresses public. Cette base de données est la plus importante d'un réseau Lotus Notes/Domino. Elle fournit un répertoire à tous les utilisateurs, groupes, certifieurs, serveurs et domaines étrangers situés dans les limites de Lotus Notes/Domino. Elle comprend également les documents qui permettent d'organiser les communications entre serveurs et d'administrer les programmes de serveurs. Cette base de données est automatiquement créée lorsque le premier serveur d'un domaine est invoqué.

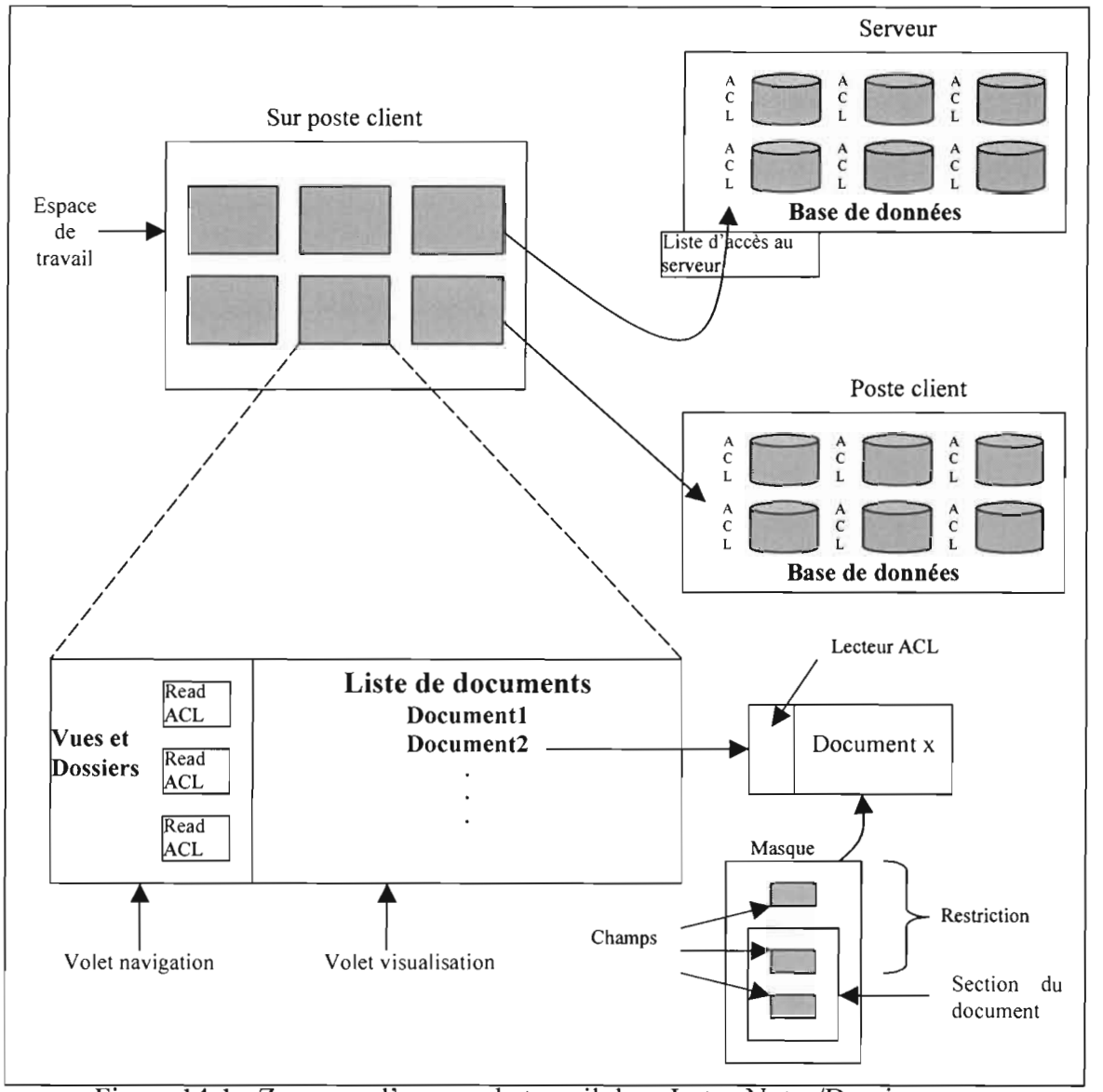


Figure 14-1 : Zoom sur l'espace de travail dans Lotus Notes/Domino

14.2. Fonctionnalités implémentées

Dans l'environnement Lotus Notes/Domino, il a été mis en œuvre les fonctionnalités de messagerie électronique et de workflow. Le processus de workflow réalisé concerne la gestion des autorisations d'absence et la publication de documents administratifs d'informations générales. Une demande d'autorisation d'absence contient des informations standards telles que le nom du demandeur, son matricule, sa qualité, son service, le motif de la demande, le nombre de jours demandés, la période de jouissance souhaitée, la date courante et le responsable à qui la demande est adressée. Une fois la demande formulée, le demandeur l'envoie au supérieur hiérarchique compétent qui va se charger de l'analyser et de répondre favorablement ou de refuser l'accord. Quant aux documents d'informations générales (notes de services, circulaires...), ils sont produits par les responsables de services ou les directeurs et publiés au sein des services. Tout le monde est tenu de les lire et de veiller à l'application des décisions qu'ils diffusent.

14.2.1. Connexion au serveur Domino

Le lancement du client Lotus Notes est suivi de la présentation d'un écran de demande d'authentification qui présente le nom d'utilisateur Notes du dernier utilisateur de la machine et exige un mot de passe. Si le nom d'utilisateur présenté ne correspond pas à celui de l'utilisateur désirant la session Notes, le bouton « Annuler » lui permet de choisir dans le répertoire approprié son fichier d'identification. La validation de cet écran d'authentification conduit l'utilisateur dans son espace de travail (cf. Figure 14-2).

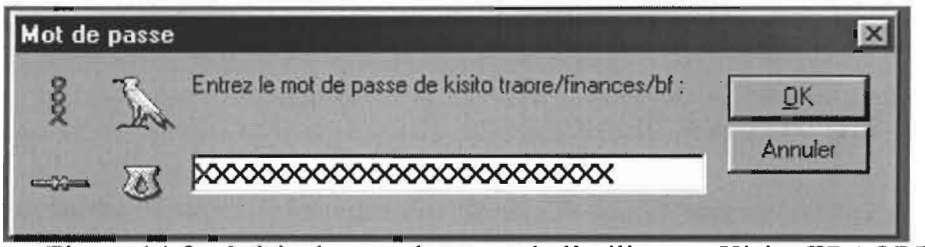


Figure 14-2 : Saisie du mot de passe de l'utilisateur Kisito TRAORE du certifieur « finances » dont le code est « bf »

Remarque :

- Lors de l'entrée du mot de passe, plusieurs caractères « X » s'affichent dans la zone de saisie chaque fois qu'une touche du clavier est actionnée ; cela permet de garantir la sécurité des mots de passe (un œil indiscret qui regarde l'écran en ce moment ne peut pas savoir la longueur du mot de passe entré)
- La première fois qu'on lance le client Lotus Notes l'espace de travail est vierge. Pour lire une base, il faut choisir la base à utiliser (cf. **Fichier → Base de Documents → Ouvrir**).

14.2.2. Messagerie électronique intégrale

Le système mis en œuvre comporte plusieurs fonctionnalités : la messagerie électronique simple, les agendas, la gestion des tâches, les forums... Le point commun principal de ces fonctionnalités est qu'elles utilisent toutes le carnet d'adresses du domaine (**GROUPWARE**) pour assurer les échanges d'informations et sont toutes contenues dans la même base de données. Pour accéder à cette base, il suffit de cliquer sur l'icône correspondant dans l'espace de travail (il s'agit de l'icône portant le nom de l'utilisateur) ou d'ouvrir le dossier Mail du serveur (**intramef/finances/bf**) et d'y choisir la base de documents qui porte le nom abrégé de l'utilisateur (par exemple, **mdavou** est le nom abrégé de Moussa DAVOU).

L'ouverture de la base permet à l'utilisateur de constater l'arrivée de messages, de les lire, de répondre immédiatement (**Répondre**), d'envoyer de nouveaux messages (**Créer mémo**) simplement ou en leur rattachant un fichier, d'acheminer un message vers un autre utilisateur (**faire suivre**)... L'ensemble des messages envoyés ou reçus sont automatiquement organisés dans des dossiers différents et apparaissant par ordre d'envoi (dossiers « Envoyés ») ou de réception (dossiers « Courriers en arrivé »). Il en est de même pour les informations échangées en utilisant les forums (cf. Figure 14-3). Certains dossiers sont crées automatiquement lors de la configuration du système (exemple, Courrier, Corbeille, Forums, Tous documents...). D'autres ont été créés lors de l'utilisation (Message départ, depart, Modèle).

L'utilisateur peut également gérer son agenda en programmant des activités, planifiant un réunion à laquelle il peut convier d'autres personnes,... et demander que le système rappelle chaque activité quelques temps avant (temps à préciser) son déroulement effectif.

Tous les messages en destination d'autres utilisateurs peuvent être signer et/ou chiffrer afin d'en assurer l'authenticité et la non-répudiation. Par ailleurs, l'utilisateur peut configurer son client Notes de sorte qu'il soit informer automatiquement, au moyen d'une boîte de dialogue, de l'arrivée d'un courrier le concernant. C'est une des originalités de l'environnement Lotus Notes/Domino qui fait qu'on peut utiliser la messagerie à des fins professionnelles avec l'usage de ce canal de communication en temps réel (cf. Figure 14-4).

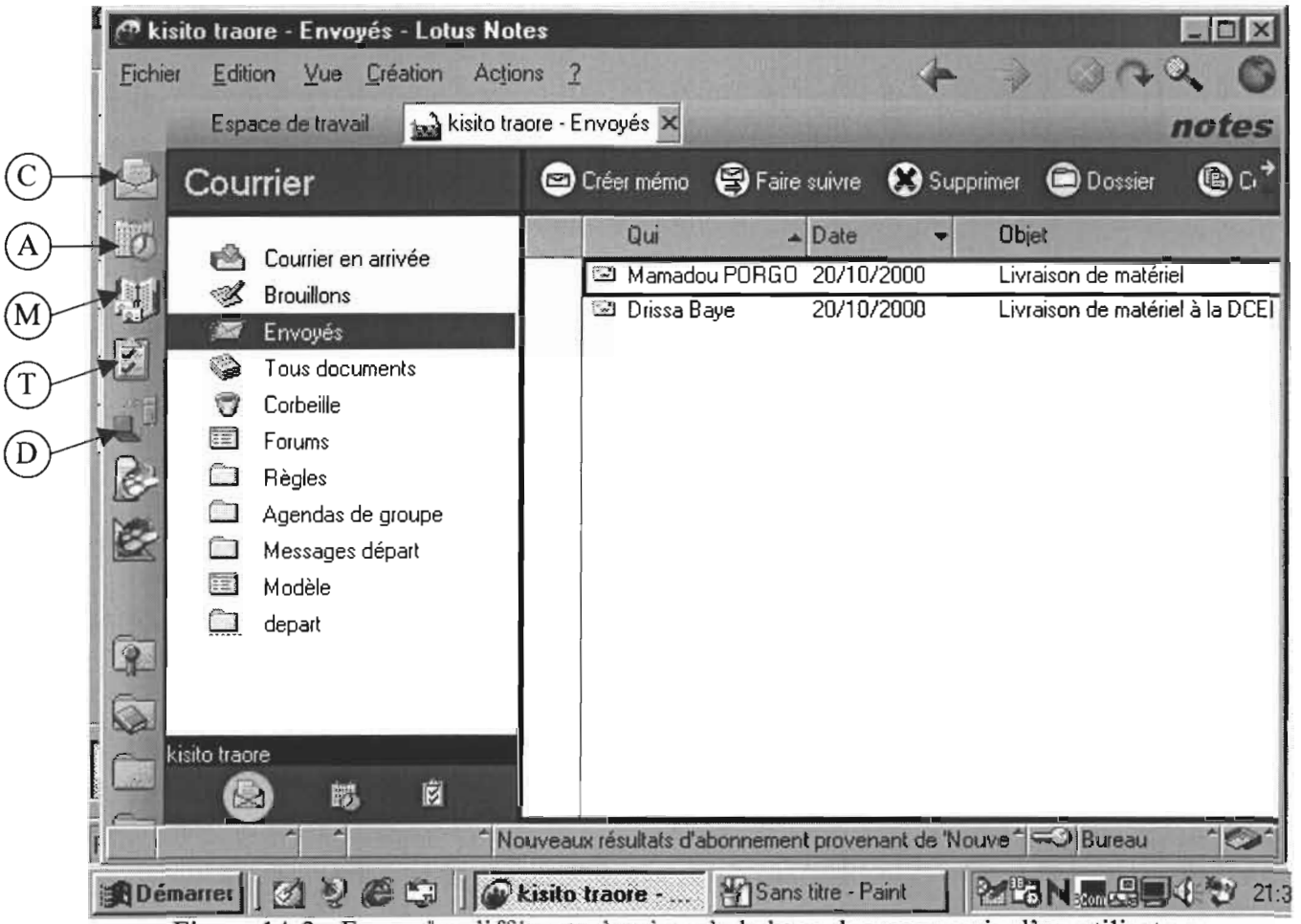


Figure 14-3 : Ecran des différents dossiers de la base de messagerie d'un utilisateur : volet navigation (dossier) et volet affichage (contenu du dossier)

(C) Courrier

(A) Bouton pour afficher un écran d'agenda

(M) Bouton pour afficher le carnet d'adresses utilisateur

(T) Bouton pour mettre et gérer les tâches en instances

(D) Accès distant pour utilisateurs mobiles

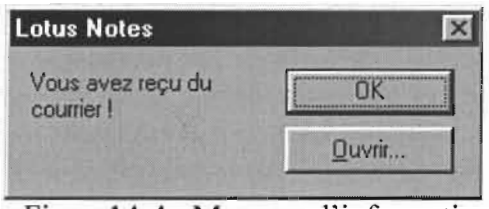


Figure14-4 : Message d'information de l'arrivée d'un courrier

14.2.3. Workflow

Pour le développement facile d'un système de workflow performant dans l'environnement Lotus Domino, un complément logiciel est nécessaire : il s'agit de Lotus Domino Workflow. L'indisponibilité de cet outil a amené à utiliser l'environnement de développement d'applications Lotus Domino Designer pour la réalisation de modules de workflow concernant la gestion des autorisations d'absence au sein des services du MEF et la production automatique suivi de la diffusion électronique de documents de type Note de services, circulaire... ou d'autres types de documents. Ces documents, de même que les boutons de manipulation (Envoyer, Répondre, Classer...), ont été réalisés en utilisant les masques, les formules, le langage LotusScript ainsi que des fonctions et commandes systèmes (Lotus Domino Designer).

14.2.2.1. La gestion des autorisations d'absence

Les demandes d'autorisations d'absence sont constituées de formulaires dûment remplis par l'agent demandeur et envoyer au supérieur hiérarchique. Le menu de création d'un document de type « **Demande d'autorisation d'absence** » se trouve dans le menu « **Création** » (cf. Figure 14-5) et est visible de tous les utilisateurs connectés au serveur Domino. Le choix de ce menu permet à l'utilisateur de disposer d'un formulaire qu'il devra remplir. Une barre de bouton lui permet de choisir l'adresse du destinataire dans le carnet d'adresses du domaine GROUPWARE, d'envoyer la demande,... Le destinataire peut classer le document dans un dossier (existant ou qu'il crée pendant le classement).

L'expéditeur d'une demande peut la signer et/ou la chiffrer. Un document chiffré ne peut être décodé que par les seuls expéditeur et destinataire(s). La signature (électronique) permet d'assurer la non-répudiation.

Tous les utilisateurs, habilités à donner une autorisation d'absence (Chef de service, Directeur Général,...) voient apparaître dans le menu « Création » de la fenêtre qui s'affiche lorsqu'ils ouvrent la base « **Documents Administratifs** » un élément permettant de créer un document de type « Autorisation d'absence » et donc de répondre favorablement à un utilisateur demandeur d'une autorisation d'absence. Si la demande n'est pas accordée, le supérieur peut envoyer, par courrier électronique, un message au demandeur, lui expliquant les motifs de la non–acceptation de la demande. Dans ce cas, il lui suffira de cliquer sur le bouton « **Répondre** » pour ouvrir son système de messagerie. La base « Documents Administratifs » a été créée pour permettre la création et le stockage de documents administratifs de types variés.

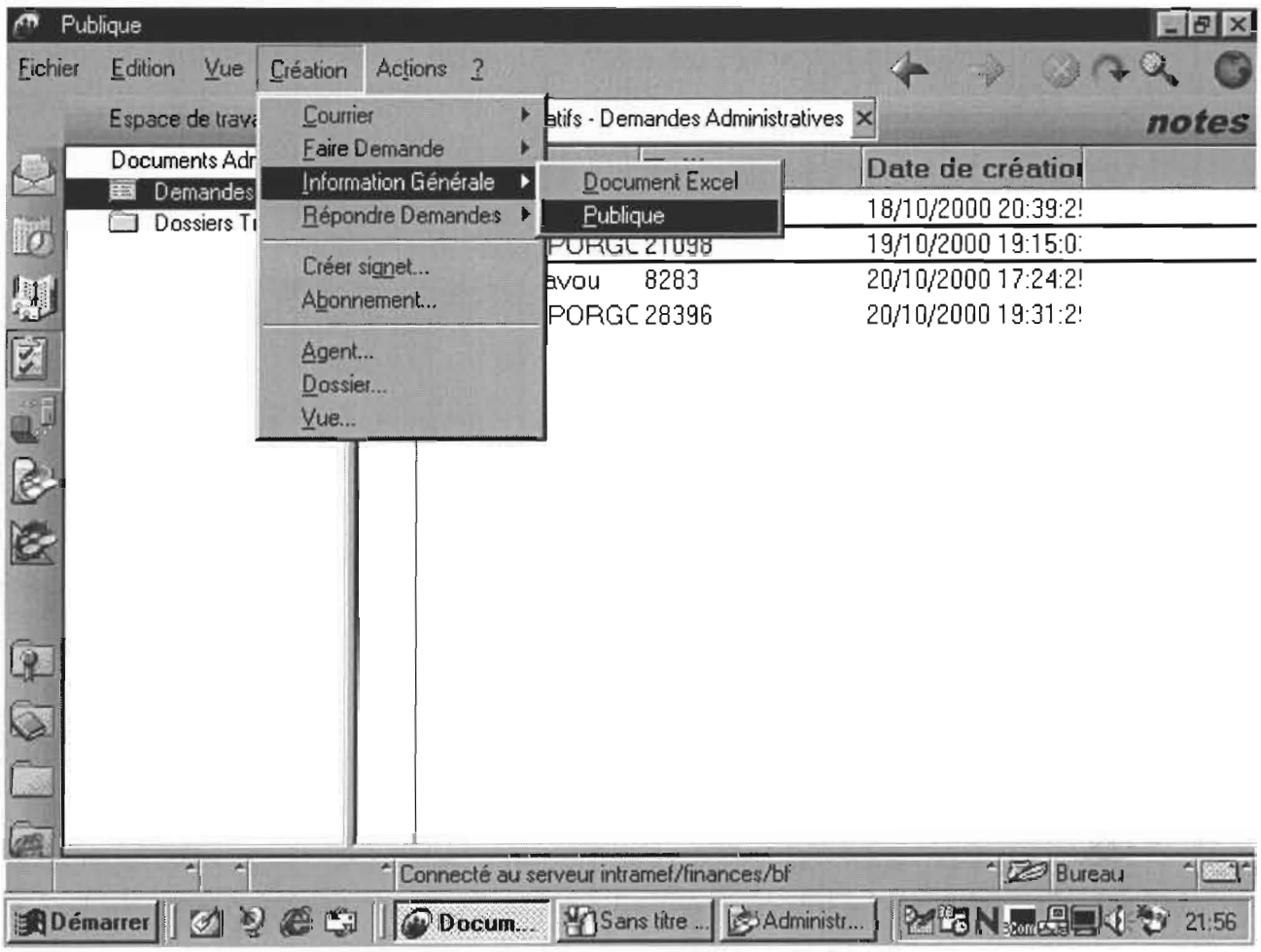


Figure 14-5 : Contenu du menu « Création »

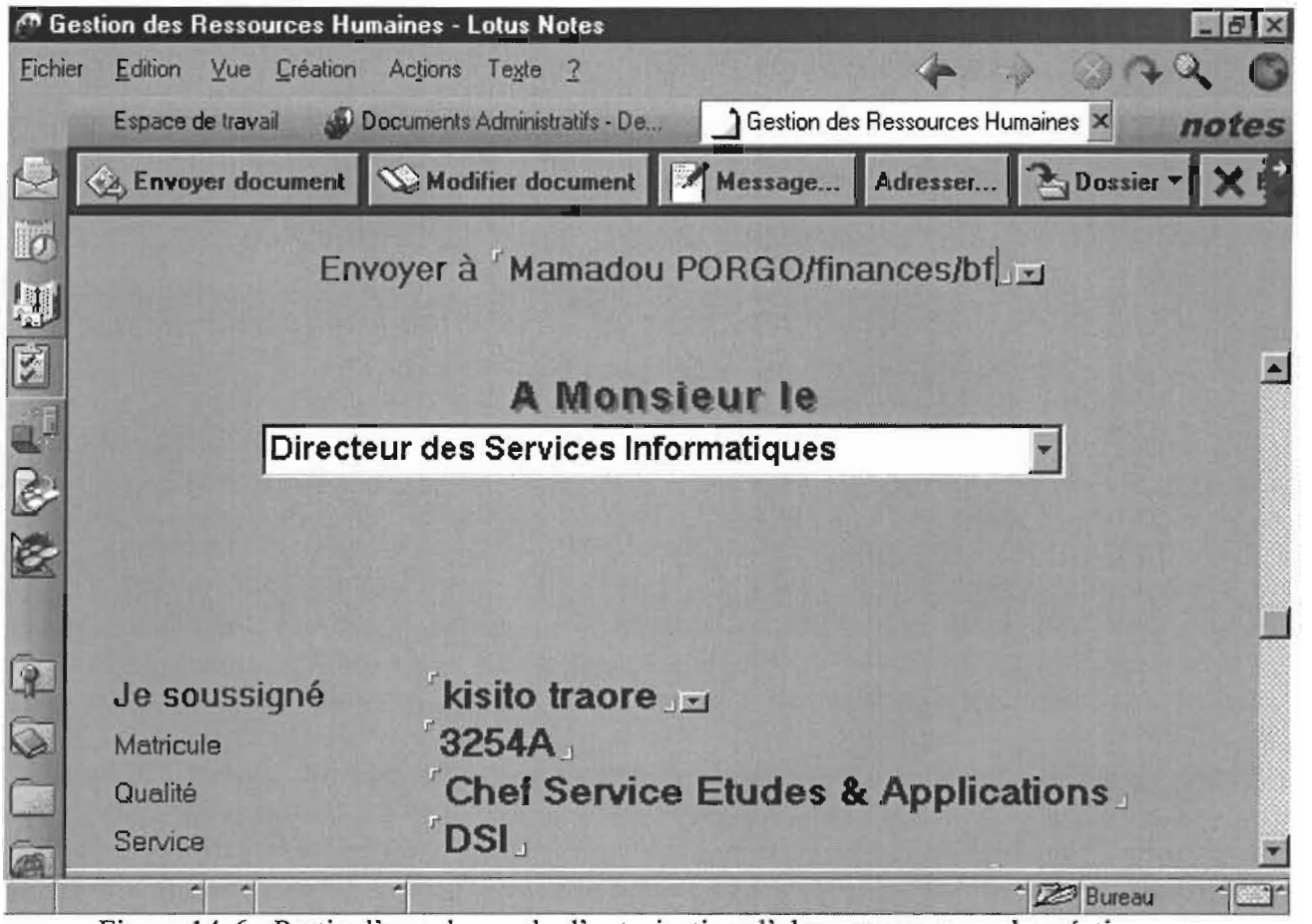


Figure 14-6 : Partie d'une demande d'autorisation d'absence en cours de création

L'utilisateur (responsable de service) qui reçoit cette demande peut l'imprimer pour des besoins d'archivage. A l'impression, le document apparaît avec un entête (l'entête utilisé pour les documents administratifs au MEF et qui précise le service, la devise du pays…) et le nom du demandeur en bas. La mention « **Envoyer à : …** » visible sur la figure n'apparaît pas dans le document lorsqu'il arrive chez le destinataire.

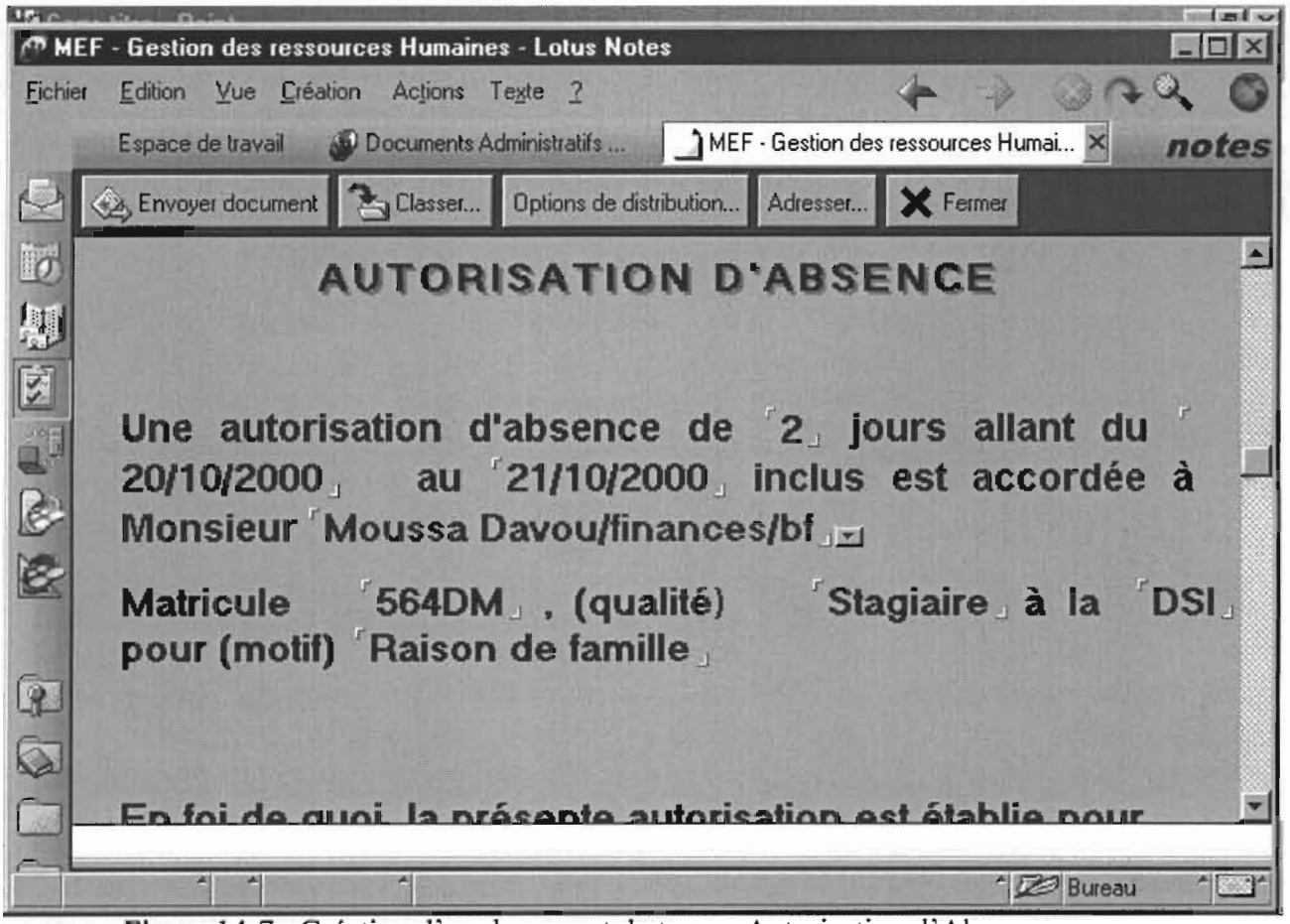


Figure 14-7 : Création d'un document de type « Autorisation d'Absence »

Le nom du signataire, de même que celui du destinataire sont pris automatiquement dans le carnet d'adresse du serveur (public). Le nom du destinataire est modifiable, mais par mesure de sécurité, celui de l'envoyeur ne l'est pas (le nom qui s'affiche est celui de l'utilisateur connecté) ; pour empêcher qu'un agent ne puisse donner une autorisation sous l'identité d'un autre.

14.2.2.2. Les documents d'informations générales

Il s'agit principalement de documents administratifs d'informations générales de type note de service, circulaire… Une note de service ou une circulaire est rédigée par un agent responsable de service(s) ou de Direction(s) ou encore un intérimaire. Le document, une fois signé, est publié au sein du service concerné avec des ampliations à d'autres services.

C'est ce deuxième processus administratif que nous avons automatisé à travers un prototype réalisé à l'aide de Lotus Domino Designer (tout comme le prototype de gestion des autorisations d'absences présenté précédemment). Les documents administratifs d'informations générales sont gérés par la base «Documents Administratifs » créé. Un utilisateur ayant un profil autorisé peut à partir du menu « Création de son logiciel client Notes créer un document administratif de type note de service ou circulaire (cf. figure 14-5). Selon le type de document choisi, un objet de type « Document word » ou « Document Excel » est inséré automatiquement dans la fenêtre qui s'affiche (cf. figure 14-8). L'utilisateur peut alors saisir le texte du message à publier, le traiter et l'envoyer aux destinataires spécifiés. Les destinataires sont choisis sur clic dans le carnet d'adresses public du serveur. Le nom qui apparaît dans la zone de signature (en bas du document) est celui de

l'utilisateur connecté qui est à l'origine de la création du document. Il n'est pas modifiable, pour éviter qu'un utilisateur ne puisse publier des informations sous l'identité d'un autre.

Toute personne qui publie une information peut la signer (de façon électronique) et/ou la chiffer (pour garantir sa confidentialité).

Tout recepteur de documents administratifs peut le classer ou l'imprimer pour des besoins d'archivage. Quand il est imprimé, le document contient un en-tête (le standard administratif au MEF), le type (note de service, circulaire…), le corps du message, et en bas, les nom et prénom(s) de l'envoyeur.

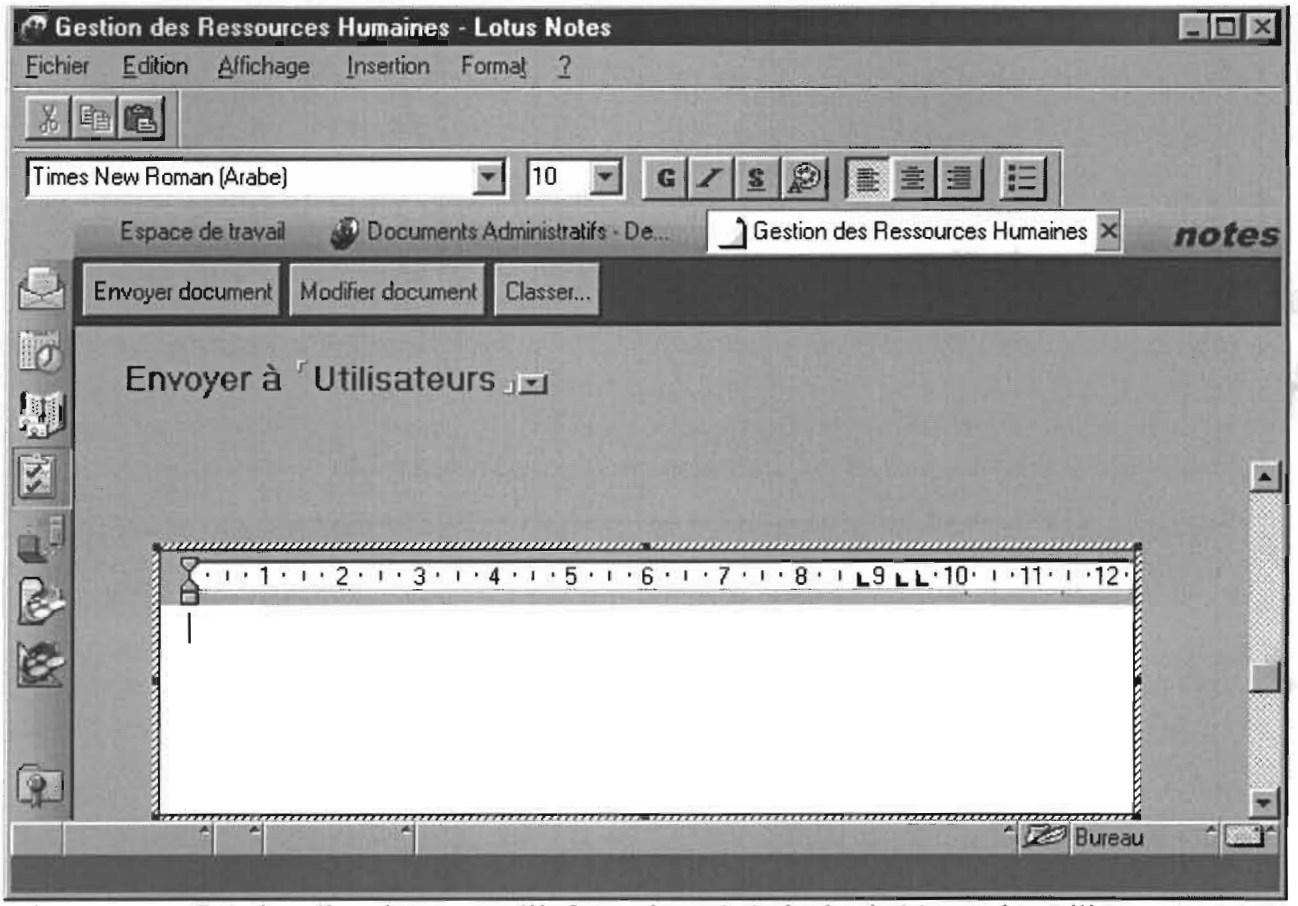


Figure 14-8 : Création d'un document d'information générale destiné à tous les utilisateurs.

Tout comme les autres documents, l'utilisateur qui reçoit un document de ce type peut l'imprimer et obtenir un document administratif respectant les normes prescrites (entêtes, nom de l'envoyeur en bas,…).

Remarque : Tous les utilisateurs qui reçoivent un document peuvent le classer dans un dossier (existant ou qu'il créent directement), envoyer une copie à d'autres utilisateurs (**Faire Suivre…**), répondre directement.

14.3. Fonctions de sécurité et Administration

La sécurité est une part importante de Lotus Notes/Domino. Pour assurer que les informations demeurent confidentielles (c'est-à-dire pour garantir que seuls les utilisateurs autorisés puissent y avoir accès), l'intégrité des informations (personne ne doit pouvoir trafiquer les données

enregistrées) et la disponibilité des informations enregistrées (l'accès par des utilisateurs autorisés doit être garanti), Lotus Notes/Domino dispose de plusieurs fonctions de sécurité. La plupart de ces fonctions peuvent être mises en œuvre au sein d'un environnement LAN (réseau local) ou au moyen d'un accès à distance.

14.3.1. Fichiers d'identification

Lors de l'enregistrement d'un utilisateur sur le serveur Domino, un fichier d'identification d'utilisateur protégé par un mot de passe est créé en fonction des informations fournies par l'administrateur pour cet utilisateur. C'est ce fichier que l'utilisateur utilise pour sa connexion vers le serveur Domino. L'administrateur peut communiquer physiquement à l'utilisateur son fichier d'identification (sur une disquette, par exemple ; ce qui est la méthode la plus sûre) ou placer le fichier sur le disque dur d'un poste de travail. Nous recommandons qu'une copie de sauvegarde de chaque fichier d'identification soit enregistrée sur un support (externe) et placé en lieu sûr de sorte qu'il soit possible de retrouver cette importante information si le fichier d'identification d'origine du disque dur du poste de travail est corrompu. Chaque fichier d'identification comprend :

- le nom du propriétaire ;
- le numéro de licences de Lotus Notes ;
- deux paires de clés publiques et privées ;
- au moins une identification de certificat ;
- un mot de passe ;
- un ou plusieurs clés de chiffrement (facultatives) ;

et est protégé par un mot de passe contre l'intervention de toute autre personne que son propre utilisateur.

Le mot de passe peut être changé une fois que l'utilisateur reçoit son fichier d'identification, mais sa longueur minimale (fixée par l'administrateur) ne peut être changée. Si l'utilisateur tape un mot de passe inférieure à la longueur minimale attendue, un message de non-validité du mot de passe est envoyé et il est invité à fournir un mot de passe valide.

Pour permettre l'exploitation du système mise en œuvre, il a été créé plusieurs utilisateurs correspondant principalement à des utilisateurs de la DSI :

Utilisateur	Nom d'utilisateur	Fichier d'identification
Abdou SANE	Abdou SANE/finances/bf	ASane.id
Alain OUATTARA	Alain OUATTARA/finances/bf	AOuattara.id
Armand YANOGO	Armand YANOGO/finances/bf	AYanogo.id
Issa BORO	Issa BORO/finances/bf	IBoro.id
Jean Drissa BAYE	Drissa BAYE/finances/bf	DBaye.id
Kisito TRAORE	kisito traore/finances/bf	Ktraore.id
Mamadou PORGO	Mamadou PORGO/finances	MPorgo.id
Mme Awa SANOU	Awa SANOU/finances/bf	ASanou.id

14.3.2. Console Serveur

La console serveur est une fenêtre à ligne de commande qui reste active tant que le serveur Domino est en activité. Elle affiche toutes les tâches exécutées par le serveur. L'administrateur utilise la console serveur pour contrôler les fonctions de Domino et assurer sa maintenance. Il entre

des commandes serveur à cette console pour lancer des tâches serveur, définir des variables d'environnement et afficher des informations systèmes. Pour empêcher les utilisateurs non autorisés d'effectuer des changements à la console d'un serveur, l'administrateur peut utiliser la commande **set secure** suivie d'un mot de passe. Tout utilisateur qui voudra utiliser la console serveur pour lancer des commandes devra connaître de mot de passe. Les commandes couramment utilisées à la console serveur sont :

- **load** qui permet de charger et de lancer une tâche ou un programme de serveur particulier ;
- **tell** qui permet de commander une tâche ou un programme de serveur ;
- **exit** qui permet d'arrêter le serveur (n'accepte pas les mots de passe contenant un espace ou un tilde) ;
- **quit** qui permet d'arrêter le serveur (n'accepte pas les mots de passe contenant un espace ou un tilde) ;
- **set configuration** qui permet d'effectuer des ajouts ou des changements à la configuration d'un fichier NOTES.INI du serveur ;
- **broadcast** pour transmettre des annonces importantes aux utilisateurs ;
- **show users** (ou **sh us**) pour contrôler l'activité utilisateur ;
- **show tasks** pour contrôler les tâches serveur en cours ;
- **show ports** pour diagnostiquer les problèmes de ports ;
- **set secure** pour protéger le processus serveur Domino des accès non autorisés. Le mot de passe entré lors de l'utilisation de cette commande est lisible en clair sur la console du serveur. Il faudra alors prendre les précautions nécessaires pour éviter son usurpation.

Un administrateur peut contrôler l'accès à un serveur en :

- permettant l'accès au serveur par les utilisateurs, par d'autres serveurs et par des groupes ;
- refusant l'accès au serveur par les utilisateurs, par d'autres serveurs et par des groupes ;
- permettant d'accéder de façon anonyme au serveur ;
- permettant la création de bases de données sur le serveur ;
- permettant la duplication des bases de données sur le serveur ;
- permettant au serveur d'être une destination directe ;
- permettant ou refusant l'accès au point d'accès du serveur ;
- exigeant la vérification des clés publiques avant de permettre l'accès au serveur.

14.3.3. Accès aux bases de données

Une ACL (*Access Control List*, liste de contrôle d'accès) est associé à chaque base de données. Elle est utilisée pour savoir quel type d'accès à la base de donnée est attribué à un utilisateur ou à un serveur. Seuls les utilisateurs ayant un accès de type **Gestionnaire** à la base de données peuvent modifier cette liste. Les divers niveaux d'accès accompagnés d'une brève description de la ou des tâches qui leur sont associées sont indiqués ci-dessous par ordre de niveau ascendant :

- **Accès refusé** : l'utilisateur n'a aucune possibilité d'accéder à la base de données en question.
- **Déposant** : l'utilisateur peut créer un document dans la base de données mais il ne peut ni lire, ni éditer ou supprimer de documents dans cette base de données (y compris ceux qu'il a créés).

- **Lecteur** : l'utilisateur peut lire des documents dans la base de données mais il ne peut pas en créer, en modifier ou en supprimer.
- **Auteur** : l'utilisateur peut lire et créer des documents dans la base de données mais il ne peut modifier que les documents qu'il a créés.
- **Editeur** : l'utilisateur peut lire, créer et modifier tous les documents de la base de données.
- **Concepteur** : l'utilisateur peut accéder en mode Editeur et peut également modifier la conception de la base de données (mais il ne peut pas changer les ACL de la base de données ou supprimer la base).
- **Gestionnaire** (Administrateur) : l'utilisateur peut effectuer toute intervention possible sur la base de données, y compris le changement des ACL et la suppression de la base.

Il est recommandé d'utiliser le mode groupes pour établir l'ACL d'une base de données. Ceci permet à l'administrateur de changer facilement les ACL lorsqu'un utilisateur a besoin d'accéder à plusieurs bases de données. Il est également recommandé de n'accorder l'accès à la base de données qu'à un seul administrateur (Gestionnaire). Ceci permet d'assurer qu'une seule personne puisse effectuer des changements à la base de données, éliminant ainsi les possibilités de conflit entre les changements d'ACL effectués par des personnes différentes.

14.3.4. Validation et Authentification

Lorsqu'un poste (client) tente de communiquer avec le serveur Domino pour un acheminement de courrier ou l'accès à une base de données, deux dispositifs de sécurité sont activés pour vérifier la légitimité du client : la validation et l'authentification.

La validation établit la sûreté d'une clé publique d'utilisateur par un serveur et d'une clé publique de serveur par l'utilisateur. La sûreté est basée sur la vérification des certificats d'utilisateurs et de serveurs, comme suit. Lorsqu'un utilisateur est enregistré, il doit être certifié par au moins un certifieur, qui place un certificat (signé au moyen de la clé privée du certifieur et comprenant la clé publique du certifieur) dans le fichier d'identification de l'utilisateur. Si un utilisateur et un serveur possèdent tous deux des certificats du même certifieur, ils peuvent valider mutuellement leur certificat.

L'authentification s'effectue au moyen d'une interaction de type réponse au défi, en utilisant une clé servant de ticket (une clé RC2). D'abord le serveur et l'utilisateur s'envoient mutuellement un nombre aléatoire. Puis, le receveur du nombre aléatoire effectue un chiffrement de ce nombre au moyen de la clé publique de l'envoyeur, à qui il renvoie le nombre ainsi chiffré. Si chaque envoyeur peut déchiffrer le nombre qu'il a envoyé à l'origine, l'authentification du serveur et de l'utilisateur est réussie.

Les trois phases de ce processus de validation et d'authentification (phase de défi, phase de création d'un ticket et phase de réponse) sont complètement transparentes pour l'utilisateur. Les phases sont décrites ci-dessous et sont représentées graphiquement par la figure qui suit.

- Phase de défi : un utilisateur et un serveur s'envoient mutuellement des messages comprenant le nom et la clé publique de l'envoyeur ainsi que huit octets correspondant à un nombre aléatoire (c'est-à-dire le défi).
- Phase de création de ticket : une clé servant de ticket (chiffré au moyen de la clé publique RSA du client et numériquement signée par le serveur) est créée par le serveur puis envoyée au client. Pour pouvoir se valider mutuellement, l'utilisateur et le serveur échangent une liste de certificats pour tenter de trouver un certifieur mutuellement reconnu. L'utilisateur et le serveur s'envoient ensuite mutuellement leurs certificats au

moyen de la clé publique du certifieur (enregistrée dans les fichiers d'identification de l'utilisateur et du serveur ainsi que dans le certificat).

Le serveur ne garde pas de copie des clés servant de ticket. Au lieu de cela, il effectue régulièrement une mise à jour des paramètres de création de ticket (environ une fois par semaine), rendant inutilisable tous les tickets déjà produits. Après quoi les utilisateurs doivent passer de nouveau par la phase de création d'un ticket.

Remarque : Cette phase n'entre en fonction que lorsqu'un utilisateur ne possède pas déjà la clé servant de ticket et venant du serveur en question, ou chaque fois que la phase de réponse ne réussit pas. Si le fichier d'identification de l'utilisateur comprend déjà la bonne clé servant de ticket, la phase de création de ticket est ignorée et on passe directement à la phase de réponse.

- Phase de réponse : en utilisant la clé servant de ticket venant du serveur, l'utilisateur effectue le chiffrement du défi du serveur (reçu au cours de la première phase) et le renvoie au serveur. Le serveur crée alors la clé servant de ticket (tel qu'indiqué plus haut, le serveur ne sauvegarde aucune copie de la clé mais « connaît » les paramètres utilisés pour créer la clé) et déchiffre la réponse.

Si la réponse déchiffrée correspond bien au défi du serveur, celui-ci crée une clé de séance, l'attribue au défi de l'utilisateur (en effectuant le chiffrement du résultat au moyen de la clé publique de l'utilisateur) et la renvoie à l'utilisateur. L'utilisateur déchiffre ensuite la réponse du serveur et, si les réponses correspondent bien, considère le processus d'authentification comme valable.

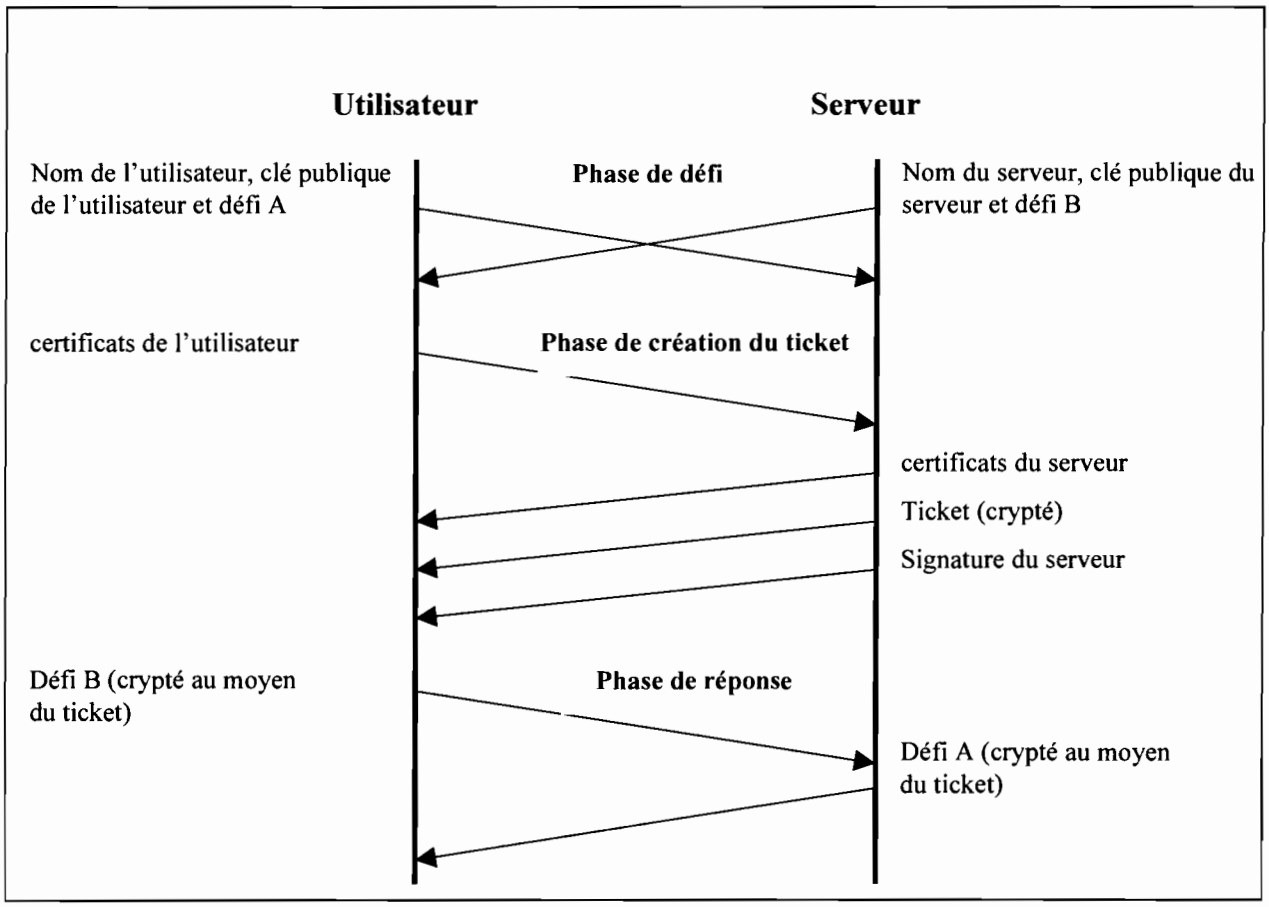


Figure 14-9 : Processus d'authentification et de validation entre client et serveur

CONCLUSION

Le mémoire de fin d'études s'est déroulé en deux phases principales. La première, celle de l'étude conceptuelle, nous a permis de proposer à la Direction des Services Informatiques du Ministère de l'Economie et des Finances une solution technique réalisable pour la mise en œuvre d'un Intranet couvrant l'ensemble de ses directions au plan national. La seconde phase a consisté en la réalisation de certains modules de cet Intranet, notamment un système de messagerie électronique intégrale et un système de workflow.

Notons que le thème de « Mise en place d'un Intranet au Ministère de l'Economie et des Finances » a été d'un apport considérable pour nous car nous ayant permis d'apprendre beaucoup (à travers les nombreuses recherches et les pratiques quotidiennes sur le réseau existant du MEF qui est un ensemble de réseaux interconnectés pour former un « WAN national ») en matière de réseau (LAN, WAN, FDDI), de sécurité, d'Intranet/Internet et de concilier pratique et théorie.

La réalisation de cet Intranet permettra au MEF sans aucun doute de

- faciliter la communication et le partage de l'information entre les structures centrales et les services déconcentrées/décentralisées,
- faciliter la mise en œuvre d'outils de productivité de groupe et d'applications multi-sites,
- rendre possible la transparence dans la gestion des affaires publiques et faciliter la communication et le partage de l'information avec les partenaires du MEF,
- permettre la vulgarisation de techniques de formation médiatisées en ligne à même de garantir une amélioration notable de la productivité,
- réaliser une véritable mutation de l'environnement de communication et d'accès à l'information, à la connaissance et au savoir-faire nécessaires au bon déroulement des activités du MEF,
- augmenter les productivités individuelles et collectives des agents,
- améliorer et rationaliser les moyens de communication extérieurs.

Nous espérons que le présent document sera d'un apport particulièrement notable dans ce processus et nous souhaitons au MEF un très bon usage.

ANNEXES

ANNEXE 1 : BIBLIOGRAPHIE

➢ Ouvrages

[DOREMUS 96], Marie-Claire et Robert DOREMUS, Fonctions pour l'utilisateur LOTUS NOTES 4.1, DUNOLD, 1996.

[EDELHART & ISRAEL 92], Mike EDELHART et Maurice ISRAEL, **Le Guide Novell Netware (du réseau Netware à l'architecture client-serveur)**, DUNOD TECH, 1992.

[EVANS 96], Tim EVANS. **INTRANET, Conception et Administration**, édition S&SM, 1996. ISBN : 2-7440-0180-5, 726 pages, CD ROM inclus.

[HORLAIT & PUJOLLE 92], Eric HORLAIT et Guy PUJOLLE, **Architecture des Réseaux Informatiques Tome 1 (Les outils de communication)**, Eyrolles, 1992, ISBN : 2-212-090062, 449 pages.

[KIRCH 99], Olaf KIRCH, **Administration Réseau sous Linux**, O'reilly (1ère édition), Mars 1995 révisée en Mars 1999, ISBN : 2-84177-00-9, 368 pages.

[ZANELLA & LIGIER 99], Paolo ZANELLA et Yves LIGIER, **Architecture et Technologie des Ordinateurs**, DUNOD (3ème édition), 1999, ISBN : 2-10-003801-X, 495 pages.

➢ Rapports, cours ou publications

[BULL-CI 00], Société Bull-Côte d'Ivoire, **Séminaire Sécurité Internet/Intranet,** 2000.

[DELGI 00], DELGI, **Rapport du Conseil Supérieur de l'Informatique du Faso pour l'année 1999**, 2000.

[GHAFFAR 99], Atif GHAFFAR, **Recycler des adresses IP**, 1999.

[GIACOMETTI 00], Arnaud GIACOMETTI, **Cours de conception des réseaux informatiques**, 2000.

[GRULOIS & JILIBERT 00], Loïc GRULOIS et Thierry JILIBERT, **NFS, un système de fichiers par réseau**, Février 2000.

[PLANCHAMP 00], Denis PLANCHAMP, **Cours « Protocoles réseaux et Internet »**, 2000.

[TARBOURIECH 99], Georges TARBOURIECH, **Virtual Network Computing ou VNC**, 1999.

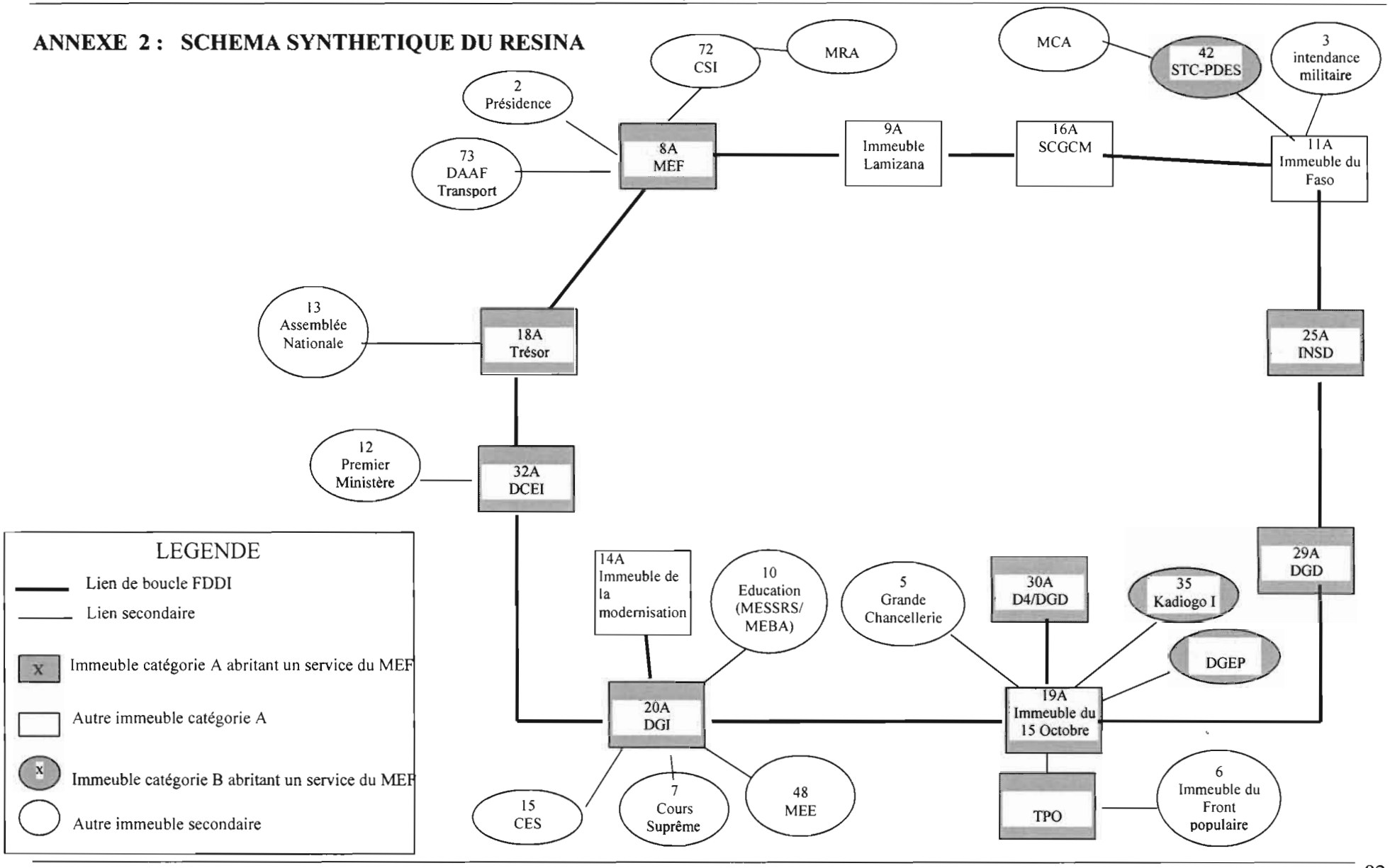
[VALANGENDONCK & ROULIVE 99], Alexandre VALANGENDONCK et Patrice ROULIVE, **La sécurité des réseaux informatiques**, 1999.

[VANBOCKSTAEL & ROLAND 99], Amélie VANBOCKSTAEL et Olivier ROLAND, **La technologie RAID**, 1999.

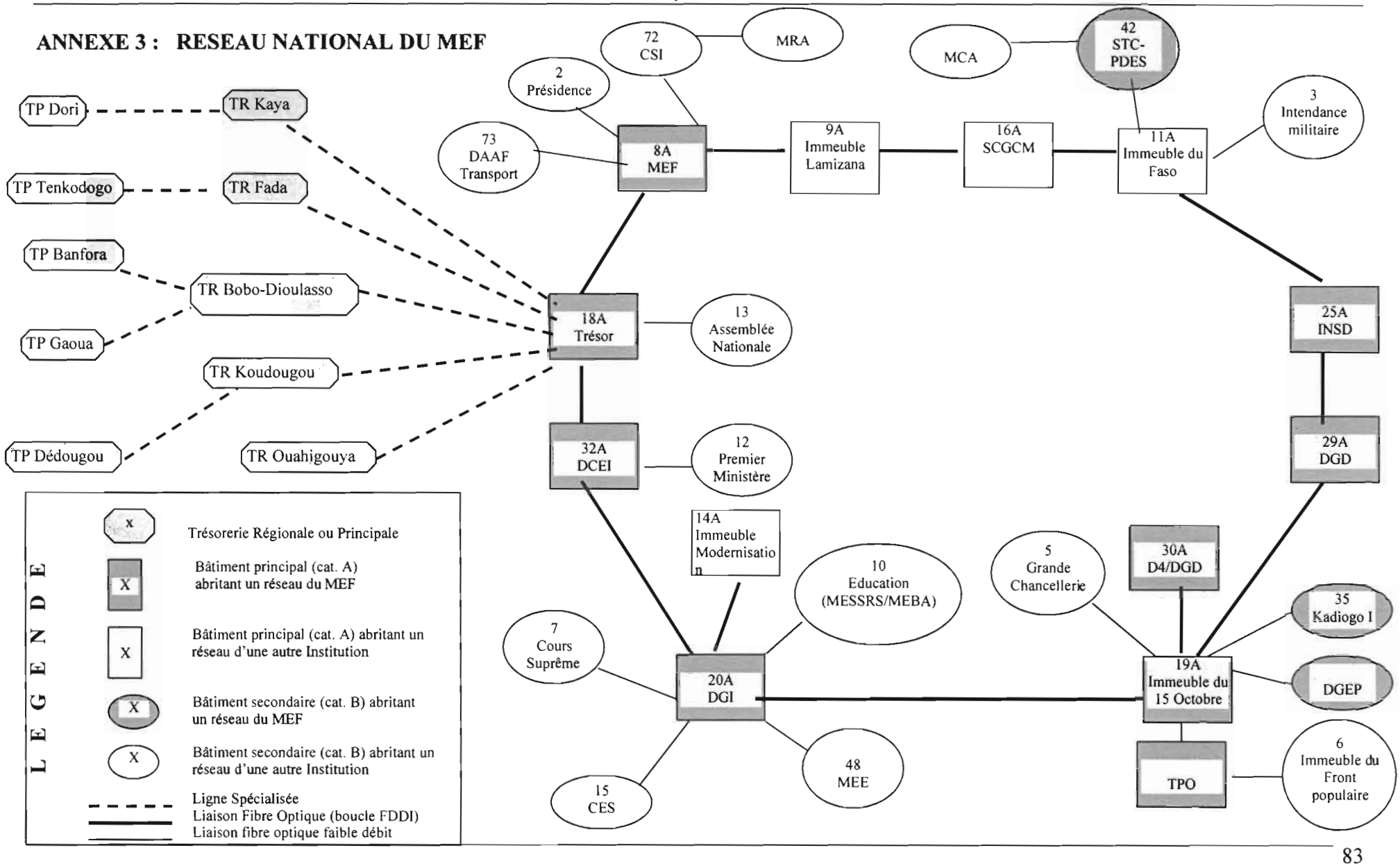
➢ URL des articles et publications sur le web

- http://cs-www.ncsl.nist.gov ;
- http://elektron.et.tudelft.nl/~vanessen/techover/chap5/5-2.htm ;
- http://infres.enst.fr/~paulet/
- http://linux.uhp-nancy.fr/INFOSHEET/;
- http://ncsa.com ;
- http://noe.unice.fr/labtrim/sysinfo.cours2/ ;
- http://pierre.bitner.free.fr ;
- http://ricercar.math-info.univ-paris5.fr/cft/;
- http://security.web-France.com ;
- http://www.3com.com/ ;
- http://www.api.ch/sftiii.htm ;
- http://www.cae.fr/caenet/neturl/;
- http://www.calisto.fr/securite/ ;
- http://www.compaq.com/ ;
- http://www.editions-oreilly/fr ;
- http://www.eisti.fr/doc/norm/;
- http://www.eleves.enst-bretagne.fr ;
- http://www.figer.com/Publications ;
- http://www.grd-publications.com/art/ls023/ls023086.htm ;
- http://www.ics.uci.edu/pub/ietf/http
- http://www.imaginet.fr/ime/ ;
- http://www.intranetjournal.com/ ;
- http://www.ipsilon.com/;
- http://www.lifl.fr ;
- http://www.loria.fr/services/linux/INFOSHEET/ ;
- http://www.lotus.fr ;
- http://www.lotus.net/ ;
- http://www.nokia.com/securitysolutions/;
- http://www.novell.com ;
- http://www.rennes.enst-bretagne.fr ;
- http://www.security.web-France.fr/ ;
- http://www.siatel.com/WorkflowFr.htm ;
- http://www.stud.enst.fr/~larminat/intranet ;
- http://www.unix-vs-nt.org ;
- http://www.yahoo.com/computers_and_Internet/programming_Languages ;

ANNEXE 2 : SCHEMA SYNTHETIQUE DU RESINA



ANNEXE 3 : RESEAU NATIONAL DU MEF



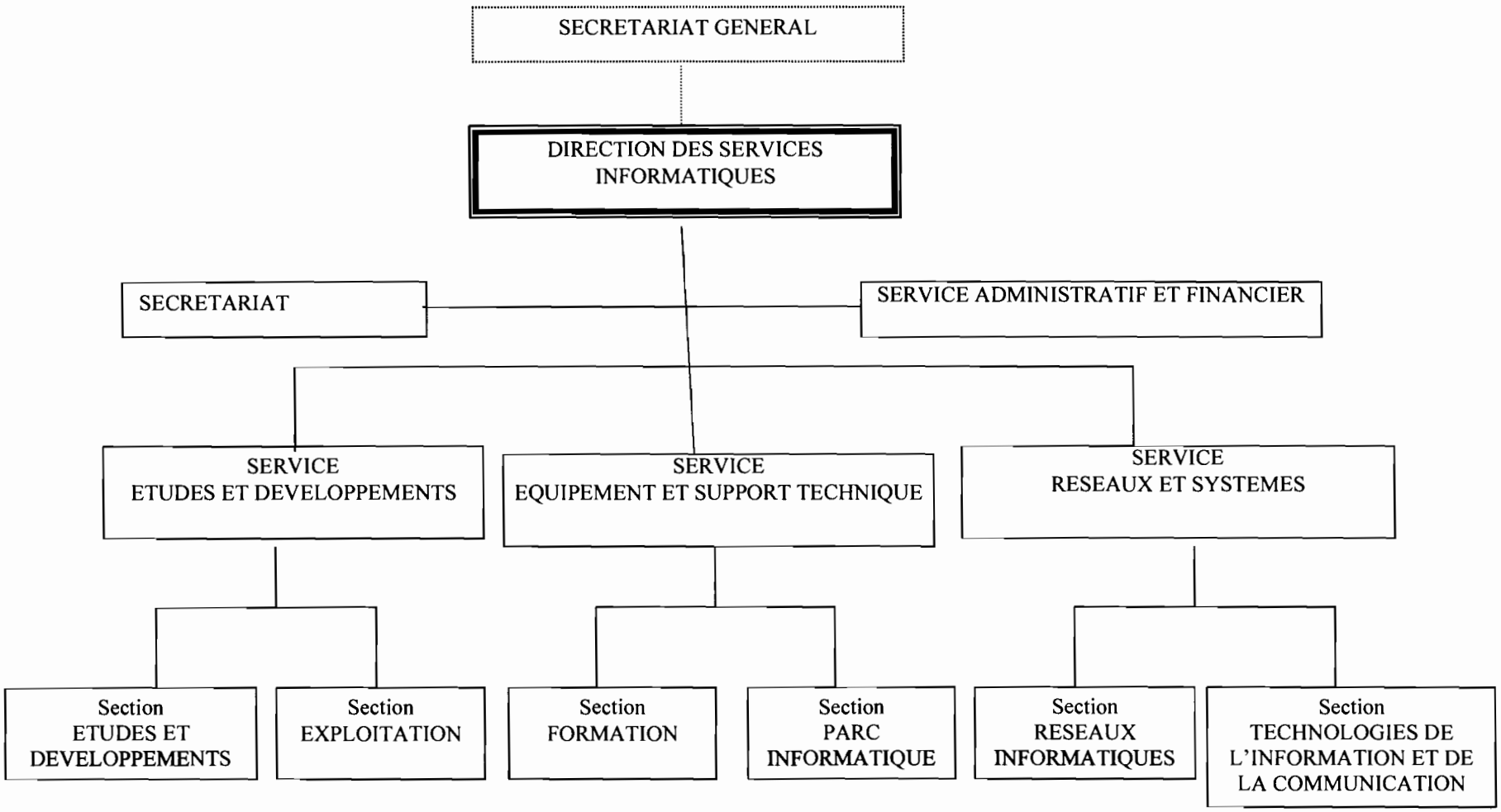
ANNEXE 4 : TABLEAU COMPARATIF DE LINUX, WINDOWS NT ET NETWARE

Composant	Linux	Windows NT Server 4.0	Novell Netware 5
Système d'exploitation	Gratuit, ou autour de 49,95 Dollars US pour une distribution CD ROM	809 dollars US pour 5 utilisateurs, 1129 dollars pour 10 utilisateurs, 3999 dollars US pour version d'entreprise à 25 utilisateurs.	2 500 000 F CFA (environ 3800 dollars US) pour une licence de 25 postes
Assistante technique gratuite en ligne	Oui, sur Internet ou sur la distribution	Non	Oui, documentation en ligne fournie
Code source du noyau	Oui	Non	Non
Serveur pour le web	Apache (gratuit)	MS-IIS (à acheter)	Novell Internet Access Server (fourni avec Netware gratuitement)
Serveur FTP	Oui	Oui	Oui
Serveur Telnet	Oui	Non	Non, mais un service similaire existe (RSPX)
Serveur SMTP/POP3	Oui	Non (acheter MS-Exchange pour la messagerie)	Non (acheter Groupwise pour la messagerie)
Serveur de noms (DNS)	Oui	Oui	Oui
Support pour le réseau	TCP/IP, Ipv6, NFS, SMB, IPX/SPX, Serveur NCP (Serveur Netware), AppleTalk…	TCP/IP, SMB, IPX/SPX, AppleTalk…	TCP/IP, NFS, SMB, IPX/SPX, Serveur NCP, SAP,NLSP, RIP, NetBIOS…
Serveur X Windows	Oui	Non	Oui
Outils d'administration à distance	Oui, tous les outils	Le logiciel web Administrator 2.0 propose un panel d'outils large, mais toujours incomplet	Oui (ZEN Works, ManageWise)
Serveur de nouvelles électroniques	Oui	Non	Non
Compilateurs C et C++	Oui	Non	Non
Perl 5.0	Oui	Non	Oui
Nombre de systèmes de fichiers compris	32	3	3
Possibilité de quota sur le disque	Oui	Non	Oui
Nombre de GUI (gestionnaires de fenêtres) parmi lesquelles choisir	4	1	1

ANNEXE 5 : QUELQUES SITES OU TROUVER LINUX

Nom du site	Adresse IP	Répertoire Linux
ftp.lip6.fr	195.83.118.1	/pub/linux
ftp.calvacom.fr	194.2.168.3	/pub/linux/slackware
ftp.change-espace.fr	195.6.132.1	/pub/Linux
ftp.ese-metz.fr	193.48.224.106	/pub/Linux
ftp.info.iut-tlse3.fr	192.134.157.5	/pub/debian
ftp.iut-bm.univ-fcomte.fr	193.52.61.33	/pub/linux
ftp.loria.fr	152.81.10.10	/pub/linux
ftp.univ-angers.fr	193.49.144.10	/pub/Linux
lirftp.insa-rouen.fr	193.49.9.163	/pub/linux
stef.u-picardie.fr	193.49.184.23	/pub/linux
tsx-11.mit.edu	18.172.1.2	/pub/linux
sunsite.unc.edu	152.2.22.81	/pub/Linux
ftp.funet.fi	128.214.248.6	/pub/Linux
net.tamu.edu	128.194.177.1	/pub/linux
ftp.mcc.ac.uk	130.88.203.12	/pub/linux
sunsite.doc.ic.ac.uk	146.169.2.1	/packages/linux
fgb1.fgb.mw.tu-muenchen.de	129.187.200.1	/pub/linux
ftp.informatik.tu-muenchen.de	131.159.0.110	/pub/comp/os/linux
ftp.dfv.rwth-aachen.de	137.226.4.111	/pub/linux
ftp.informatik.rwth-aachen.de	137.226.225.3	/pub/Linux
ftp.Germany.EU.net	192.76.144.75	/pub/os/Linux
ftp.uu.net	137.39.1.9	/systems/unix/linux
wuarchive.wustl.edu	128.252.135.4	/mirrors/linux
ftp.win.tue.nl	131.155.70.100	/pub/linux
ftp.stack.urc.tue.nl	131.155.2.71	/pub/linux
srawgw.sra.co.jp	133.137.4.3	/pub/os/linux
ftp.denet.dk	129.142.6.74	/pub/OS/linux
NCTUCCCA.edu.tw	140.111.1.10	/Operating-Systems/Linux
sunsite.cnlab-switch.ch	195.176.255.9	/mirror/linux
cnuce_arch.cnr.it	131.114.1.10	/pub/Linux
ftp.monash.edu.au	130.194.11.8	/pub/linux
ftp.dstc.edu.au	130.102.181.31	/pub/linux
ftp.sydutech.usyd.edu.au	129.78.192.2	/pub/linux

ANNEXE 6 : ORGANIGRAMME DE LA DSI



GLOSSAIRE

ACCT Agence Comptable Central du Trésor

Apache Logiciel (serveur) freeware d'un consortium international d'utilisateurs du web et d'Internet, le consortium W3C (cf. 6.2.2. de ce document)

API Application Programming Interface
Une API décrit le type d'interaction entre une application cliente et un serveur via un protocole de communication. Les échanges de données peuvent être synchrones ou asynchrones.

Architecture L'architecture d'un système informatique est la description des organes fonctionnels de ce système et de leurs interconnexions.

ASCII American Standard Code for Information Interchange.
Codage standard des caractères alphanumériques

ASIC Application Specific Integrated Circuits.
Circuits spécialisés utilisés dans la conception des processeurs. Leur avantage c'est qu'ils sont rapides et moins chers. Les processeurs ASIC peuvent effectuer des fonctions spécifiques très rapidement, mais n'ont pas les caractéristiques de programmabilité et de flexibilité des autres processeurs généraux.

ASP Active Server Page
Les pages ASP sont basées sur des canevas et permettent l'invocation de composants s'exécutant sur un serveur. Les scripts peuvent être écrits en Visual Basic, Java, Visual C++... et sont interprétés dans le contexte d'un serveur IIS (Internet Information Server de Microsoft).

Authentification Dans le cas d'un simple message, le service d'authentification assure que le message provient de l'endroit d'où il prétend venir. Dans le cas d'un échange bidirectionnel, deux aspects sont présents. Il faut assurer que les deux entités sont bien ce qu'elles affirment être. De plus, le service d'authentification doit montrer que la connexion ne peut être brouillée par une troisième entité essayant de se faire passer pour un des deux correspondants.

Bande passante Bande de fréquence qui est correctement transmise.

Cache Initialement, ce terme a été utilisé pour désigner un niveau de mémoire entre le processeur et la mémoire centrale.
Actuellement, il a un sens plus général : c'est tout espace de stockage qui est utilisé de manière à tirer partie de la localité (localité spatiale ou temporelle).

CDI Comité Directeur Informatique.
C'est l'organe de pilotage pour la mise en œuvre d'un Schéma Directeur Informatique

CES Conseil Economique et Social

CGI Common Gateway Interface (se traduit littéralement par « Interface de Passerelle Commune »).
C'est un programme exécuté sur un serveur web (http) pour permettre l'affichage de données traitées par le serveur (données provenant d'une autre application, comme par exemple un SGBD, d'où le nom de passerelle). Un des grands intérêts de l'utilisation de CGI est la possibilité de fournir des pages dynamiques, c'est-à-dire des pages pouvant être différentes selon un choix ou une saisie de l'utilisateur. L'utilisation la plus fréquente de cette technique repose sur l'utilisation de formulaires HTML permettant à l'utilisateur de choisir ou saisir des données, puis à cliquer sur un bouton de soumission du formulaire, envoyant alors les données du formulaire en paramètres du programme CGI.

Cisco Secure Utilitaire disponible sur les routeurs Cisco série 1600, 1700, 2500 et 3600 ; permet de gérer les authentifications d'utilisateurs. Cisco Secure est normalisé TACACS+ *(Terminal Access Controller Access System, protocole d'authentification).*

Client Le terme « client » s'applique à tout programme qui envoie une requête à un serveur et attend les résultats. **Voir Serveur**

Commutateur (Switch) Equipement de niveau 2 (couche liaison de données) du modèle OSI.
Evolution logique des ponts, les commutateurs sont généralement utilisés pour réorganiser un réseau, isoler des serveurs, segmenter des réseaux ou remplacer une épine dorsale.

Confidentialité Elle représente le fait que les données informatiques ne sont accessibles que par les personnes autorisées. Le type d'accès s'étalant de la simple connaissance de l'existence de l'objet à la surimpression de celui-ci. La confidentialité reste la notion de sécurité informatique la plus proche du monde réel et semble dès lors la plus claire.

Contrôle d'accès Elle représente la capacité de limiter et de contrôler les accès aux systèmes et applications via les liens de communication. Pour cela, chaque entité demandant un accès se voit identifiée ou authentifiée afin de lui adapter ses droits d'accès.

CORBA Common Object Request Broker Architecture.
Norme neutre du consortium OMG (Object Management Group) basée sur la technologie objet. Son objectif : permettre l'intégration d'applications distribuées hétérogènes.

CSI Conseil Supérieur de l'Information

DAAF Direction / Directeur des Affaires Administratives et Financières.

DAT Direction de l'Aménagement du Territoire.

DCEI Direction de la coordination et de l'Evaluation des Investissements.

DDP Direction de la Dette Publique.

DGB Direction Générale du Budget.

DGD Direction Générale des Douanes.

DGI Direction Générale des Impôts.

DGTCP Direction Générale du Trésor et de la Comptabilité Publique.

Disponibilité Elle se reflète dans l'information et dans les services. Ce domaine est aujourd'hui en pleine expansion. Il regroupe des sujets aussi variés que les temps de réponse, la tolérance aux fautes, le contrôle de concurrence, le partage équitable de ressources…

DMZ DeMilitarized Zone (zone démilitarisée).
Dans les principes de sécurisation, cette terminologie désigne une zone sécurisée par un firewall qui héberge, entre autres, les serveurs pouvant être accessibles via Internet ou le réseau externe.

DRH Direction / Directeur des Ressources Humaines

DSA Digital Signature Algorithm.
Algorithme développé sur la base de l'algorithme El Gamal. La signature est semblable à celles des clés de type Diffie-Hellman. La génération des signatures se fait plus rapidement qu'avec RSA. **Voir RSA**

DSI Direction des Services Informatiques

DSS DSA standard réservé aux signatures. **Voir DSA**

FDDI Fiber Distributed Data Interface.
Type d'architecture utilisé pour les réseaux longues distances à hauts débits. La structure physique ressemble à celle des réseaux en anneau (Token Ring) mais le support utilisé est la fibre optique avec un double anneau sécurisé : l'autre anneau prend le relais dès que l'un tombe en panne.

Firewall Un firewall ou pare-feu est un dispositif sécuritaire (logiciel et/ou matériel) qu'on met à l'entrée d'un réseau pour filtrer les accès, isoler des réseaux, protéger les ressources sensibles, obtenir des alertes et des statistiques sur les tentatives d'intrusion ou d'attaque. Un firewall effectue deux types de filtrage : le filtrage IP et le filtrage applicatif.
Un firewall IP (filtrage IP) filtre le trafic selon les adresses IP appelantes et appelées, les services, les protocoles (TCP, UDP, ICMP…), les plages horaires…
Un firewall applicatif (filtrage applicatif) s'occupe du filtrage des commandes, de l'isolation et du filtrage de services (FTP, TELNET…), de l'authentification des utilisateurs.

Frame Relay Les réseaux à relais de trames ou Frame Relay sont une évolution logique des réseaux X.25. **Voir X25.**

GBLIC GNU C Library.
GBLIC est utilise comme étant la bibliothèque C dans le système GNU et dans la

plupart des nouveaux systèmes fonctionnant avec le noyau Linux. Aujourd'hui, la bibliothèque C de GNU est assez complète : toutes les fonctions utiles et connues de toute autre bibliothèque C y sont disponibles.

Gbps Gigabit par seconde.
Le bps (bit par seconde) est l'unité de mesure du débit de transmission d'information sur un support informatique. Le bit (contraction de « Binary Digit ») est l'unité informatique élémentaire qui vaut soit 1, soit 0. Le 1 signifie que le courant passe et le 0 qu'il ne passe pas. Le débit mesure donc le nombre d'informations élémentaires pouvant circuler en une seconde. Compte tenu des techniques utilisées actuellement dans les réseaux informatiques, on utilise plus couramment le Mégabit (un million de bits) par seconde ou le Gigabit (un milliard de bits) par seconde.

GNOME Interface graphique dans les environnements Linux

GNU Le Projet GNU a été lancé en 1984 afin de développer un système d'exploitation complet et semblable à Unix qui soit un logiciel libre: le système GNU. Des variantes du système d'exploitation GNU, utilisant le noyau « Linux », sont utilisées largement à présent ; bien que ces systèmes soient communément nommés par le terme « Linux », ils sont plus exactement appelés « systèmes GNU/Linux ».

Go Giga octet(s).
Un octet est un ensemble de huit bits (**voir Gbps**). Un Go est un ensemble de 10^9 octets, soit huit milliards de bits

GUI Graphic User Interface.
Terme utilisé pour désigner les interfaces graphiques (généralement en environnement Unix).

HTML Hyper Text Markup Language.
Langage descriptif permettant de définir les différents composants d'un document du web. HTML n'est pas à proprement parler un langage de programmation ; c'est un langage descriptif qui se contente de décrire le document dans sa structure et sa logique.

HTTP Hyper Text Transfert Protocol.
Protocole permettant les échanges entre les différents systèmes d'information hypermédia du réseau. Ce protocole est le résultat des travaux du projet WWW du CERN

Hub Equipement réseau fonctionnant comme un régénérateur de trames : toute trame reçue sur un port est répétée sur tous les autres ports. Les hubs simulent une topologie logique en bus.

IANA Internet Assigned Number Authority

INSD Institut National de la Statistique et de la Démographie

Intégrité Elle signifie que l'information ne peut être modifiée que par les personnes autorisées ou seulement par les moyens autorisés. L'intégrité reste un domaine très large couvrant à la fois les modifications, les moyens de modification mais également l'après-modification et donc la consistance. L'intégrité est le troisième but de la sécurité informatique.

IP Internet Protocol (Protocole Internet, communément appelé Ipv4 pour IP version 4)
La fonction du protocole Internet est d'acheminer les datagrammes à travers un ensemble de réseaux interconnectés. Ceci est réalisé en transférant les datagrammes d'un module Internet à l'autre jusqu'à atteindre la destinataire. Les modules Internet sont des programmes exécutés dans des hôtes et des routeurs du réseau Internet. Les datagrammes sont transférés d'un module Internet à l'autre sur un segment particulier de réseau selon l'interprétation d'une adresse Internet. De ce fait, un des plus importants mécanismes du protocole Internet est la gestion de cette adresse. Lors de l'acheminement d'un datagramme d'un module Internet vers un autre, les datagrammes peuvent avoir éventuellement à traverser une section de réseau qui admet une taille maximale de paquet inférieure à celle du datagramme. Pour surmonter ce problème, un mécanisme de fragmentation est géré par le protocole Internet.

IPSec IP Security
Ensemble de standards ouverts développé par l'IETF (Internet Engineering Task Force) pour assurer la confidentialité des données, l'authentification des utilisateurs… Il permet de prendre en compte les aspects sécuritaires (absents dans Ipv4). IPSec est implémenté dans la nouvelle version d'IP (Ipv6) et dans certains routeurs.
C'est une forme d'extension du protocole IP avec deux champs principalement : AH (*Authentification Header*) et ESP (*Encapsulating Security Payload*).
Il peut être intégré à un équipement (routeur) par ajout logiciel.

IPX/SPX Internetwork Packet Exchange/ Sequenced Packet Exchange
Protocoles de communication utilisés dans les réseaux Netware

ISAPI API http propriétaire de Microsoft.
Les API http sont des mécanismes propriétaires permettant d'exécuter des programmes applicatifs, lancer dans le contexte d'un serveur http particulier, avec passage de paramètres à une interface propriétaire.
D'autres exemples d'API http : NSAPI (Netscape), API Apache (Linux)…

ISBN International Standard Book Number

JavaScript Si le langage Java impose le téléchargement de classe c'est-à-dire de programmes pré-compilés depuis le serveur, JavaScript propose l'exécution de programmes non compilés mais interprétés et contenus dans le corps de la page HTML

KDE KDE (*K Desktop Environment*) est une des interfaces graphiques de l'environnement Linux

LAN Local Area Network (Entendez : Réseau Local d'Entreprise)

	Un LAN peut être de type Ethernet ou Token Ring. Sa couverture géographique peut aller jusqu'à quelques centaines de mètres.
LAN	Local Area Network ou réseau local Un réseau local est un réseau dont les nœuds se trouvent dans un même bâtiment ou dans des bâtiments voisins (ou même à quelques kilomètres).
LDAP	Lightweight Directory Access Protocol. Protocole d'accès à un annuaire centralisé.
Logiciel	Ensemble de programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitements de données (*software*)
logs	Répertoire où sont stockés les fichiers mouchards dans les systèmes unix.
LS	Les lignes spécialisées ou LS sont des supports de transmission réseau qui donnent une connexion permanente entre les sites, un système de tarification indépendant du volume de données échangées et des durées de connexion et demandent un abonnement mensuel ou annuel en fonction de la distance inter-sites et du débit offert.
MAC	Medium Access Control
Matériel	Ensemble des éléments physiques employés pour le traitement de données (*hardware*)
Mbps	Mégabits par seconde. **Voir Gbps**
MCA	Ministère de la Culture et des Arts
MEF	Ministère de l'Economie et des Finances
Message	Ensemble d'informations transférées en un envoi dans une communication.
Mo	Méga octet(s). **Voir Go**
Modem	MODulateur DEModulateur : c'est un boîtier électronique que l'on branche d'un côté à un ordinateur sur un port série et de l'autre à une prise téléphonique. Il permet ainsi de connecter deux ordinateurs entre eux. Sa fonction est de convertir les informations numériques qu'utilisent l'ordinateur en une modulation analogique compatible avec le téléphonique. La conversion est symétrique.
MRA	Ministère des Ressources Animales
Multi -média	Selon un sens informatique restreint, le multimédia est relatif au traitement ou à la gestion intégrée de textes, d'images fixes ou animées, de sons, de vidéos, de

	programmes... numérisés en général à partir des mêmes supports micro-informatiques.
NCP	Netware Core Protocol
NCSA	National Center for Supercomputing Applications
NFS	Network File System. Système de fichiers dans un réseau informatique.
NLSP	Netware Link Services Protocol
Non-répudiation	Elle permet au récepteur ou à l'émetteur de ne pas refuser un message transmis. Donc, quand un message est envoyé, le récepteur peut prouver que le message a bien été envoyé par l'émetteur. De même, lorsqu'un message est reçu par le bon récepteur.
NSAPI	API http propriétaire de Netscape. **Voir ISAPI**
NTFS	NT File System. Système de fichiers dans un réseau informatique sous Windows NT.
NTIC	Nouvelles Technologies de l'Information et de la Communication.
ONATEL	Office NAtional des TELécommunications.
PC	Personal Computer. Terme utilisé pour désigner les micro-ordinateurs.
PERL	Pratical Extraction and Report Language
PNI	Plan National Informatique.
POP	Post Office Protocol. Protocole pour la récupération du courrier électronique. **Voir SMTP.**
Portabilité	Qualité d'un logiciel pouvant fonctionner sur différentes machines.
Protocole	Ensemble de règles qui doivent être respectées pour réaliser un échange d'informations entre ordinateurs, ou entre un terminal et un ordinateur, en général, entre unités communicant par un système commun de transmission de l'information.
RAM	Random Access Memory (Mémoire d'accès aléatoire) C'est une mémoire vive de contenu volatil. On distingue les SRAM (Static RAM) et les DRAM (Dynamic RAM)
RC2	Il s'agit d'un chiffrage de bloc de 64 bits. RC2 est utilisé pour effectuer la plupart des opérations de chiffrement dans Lotus Notes (par exemple, champs, courrier, etc.).

RC4 Il s'agit d'un chiffrage continu de 64 bits. RC4 est utilisé pour chiffrer les données transférées par l'intermédiaire d'un point d'accès au réseau.

Réseau Ensemble d'ordinateurs (et d'équipements terminaux), géographiquement dispersés, reliés entre eux par un ou plusieurs liens afin de permettre des échanges d'informations. Un réseau est dit homogène si les ordinateurs sont compatibles, il est dit hétérogènes si le matériel est disparate.

RESINA Réseau Inter – Administratif de Ouagadougou basé sur une topologie FDDI.
cf. 1.3 de ce document.

RIP Routing Information Protocol

RNIS Réseau Numérique à Intégration de Services (support de transmission réseau)
Le RNIS est caractérisé par ses temps de connexion beaucoup plus faibles (1 seconde pour le RNIS contre 30 secondes pour le RTC) qui peuvent enlever la notion d'accès intermittent grâce au Dial-on-Demand et son système de tarification est identique au **RTC**.

Routeur Equipement réseau de niveau 3 (couche réseau) du modèle OSI. Il utilise les systèmes d'adressage de niveau 3 (IP/IPX) pour acheminer les données. Ses principales fonctions sont de déterminer les chemins à suivre pour interconnecter les différents hôtes ou sous-réseaux et d'exploiter ces chemins pour acheminer les paquets reçus.

RSA Algorithme de cryptage conçu par Rivest, Shamir et Adelman en 1978. Il s'agit d'un algorithme à clé asymétrique (publique/.privée) très connu, supportant une longueur de clé variable et une longueur de message variable. Le bloc de messages doit toutefois être de taille inférieure à la longueur de la clé qui est de 512 bits (de façon typique). RSA est utilisé pour la gestion de clés (par exemple clés de chiffrement symétriques, transfert des clés utilisées pour l'authentification, etc.) et pour les signatures numériques. Lent, cet algorithme est peu utilisable pour du chiffrement de session performant.

RTC Réseau Téléphonique Commuté.
Le RTC se caractérise par son intermittence souvent régulière et automatique, sa facturation (coût) à la durée et en fonction de la distance inter-sites, ses taux d'erreurs importants et son débit limité (inférieur à 56 Kbps).

S&SM Simon & Schuster Macmillan

SAP Service Advertising Protocol

SDI Schéma Directeur Informatique

Serveur Le terme « serveur » s'applique à tout programme qui offre un service qui peut être atteint à travers le réseau comme par exemple un serveur de fichiers, un serveur d'impression ou un serveur de courrier électronique. Un serveur reçoit des requêtes à travers le réseau, il les traite et renvoie les résultats au demandeur (le client). **Voir**

	Client
SGBD	Système de gestion de bases de données
SGBDR	Système de gestion de bases de données relationnelles
SIGASPE	Système Intégré de Gestion Administrative et Salariale du Personnel de l'Etat
SMTP	Simple Message Transfert Protocol. Protocole pour l'envoi du courrier électronique. **Voir POP.**
SSI	Server Side Include Les SSI permettent d'exécuter de façon simple des primitives en temps réel sur le serveur, comme l'affichage de la date, le nombre de visiteurs ou de faire des tests conditionnels, pour envoyer un courrier électronique ou d'interroger une base de données pour y référencer la personne qui vient lire sur le serveur. Les SSI (Server Side Include) quand elles sont supportées par un serveur sont un bon compromis entre le langage Javascript et les CGI. En effet, elles sont supportées par le serveur http, elles restent compatibles avec tous les navigateurs puisque le code des SSI est transformé en HTML. Cependant, il se peut que le serveur qui abrite les pages HTML les accepte, mais que pour des raisons de sécurité l'administrateur système n'autorise pas l'accès à cette option. La technologie SSI qui n'était pas normalisée jusqu'à présent est aujourd'hui adoptée par Netscape et Microsoft, qui l'ont implanté sur leur serveur HTTP.
SSL	Secure Socket Layer. Protocole ouvert, non-propriétaire développé par Netscape pour transmettre des documents privés via Internet. SSL fonctionne en utilisant une clé privée pour crypter les données transférées à travers une connexion SSL. Netscape Navigator et Internet Explorer supportent tous deux SSL et beaucoup de sites web utilisant le protocole pour gérer les informations confidentielles sur les utilisateurs, comme les cartes de crédit. Par convention, les adresses de pages web qui requièrent une connexion SSL commence par **https :** au lieu de **http :**
STC-PDES	Secrétariat Technique Comptable – Programme de Développement Economique et Social
TCP	Transmission Control Protocol. Le protocole TCP est défini dans le but de fournir un service de transfert de données de haute fiabilité entre deux ordinateurs raccordés sur un réseau de type « paquets commutés », et sur tout système résultant de l'interconnexion de ce type de réseaux. TCP est un protocole sécurisé orienté connexion conçu pour s'implanter dans un ensemble de protocoles multicouches (juste au-dessus du protocole Internet), supportant le fonctionnement de réseaux hétérogènes. TCP fournit un moyen d'établir une communication fiable entre deux tâches exécutées sur deux ordinateurs autonomes raccordés à un réseau de données. Le protocole TCP s'affranchit le plus possible de la fiabilité intrinsèque des couches inférieures de communication sur lesquelles il s'appuie. Il suppose donc uniquement que les couches de communication qui lui sont inférieures lui procurent un service de transmission de

paquet simple, dont la qualité n'est pas garantie.

TCP/IP Transmission Control Protocol / Internet Protocol : familles de protocoles publics utilisées entre autre sur Internet.

Topologie (physique) Localisation des nœuds d'un réseau et agencement des liens entre ces nœuds (domaine des réseaux informatiques)

TP Trésorerie Principale

TPO Trésorerie Principale de Ouagadougou

TR Trésorerie régionale

URL Uniform Resource Locator.
Syntaxe unifiée de description (nom et adresse) des différents éléments d'un réseau.

UTP Unshielded Twisted Pair.
Paire torsadée non blindée. C'est un support de transmission dans les environnements réseau de type Ethernet.

Virus Le terme « virus » informatique est issu de la ressemblance avec les virus biologiques. Par exemple, un virus informatique se transmet d'ordinateur en ordinateur tout comme un virus biologique se transmet de personne en personne. On définit généralement un virus comme un programme qui exerce une action nuisible sur l'environnement, à l'insu de l'utilisateur. Cette action peut être continue, sporadique, périodique, ou n'avoir lieu qu'à une date précise (le virus Michelangelo, par exemple, ne se déclenche que le 6 mars). Il peut aussi se déclencher à partir d'un certain nombre de copies, d'une combinaison de touches, un certain nombre d'accès au disque dur ou encore la présence d'anti-virus (virus flibustier). On les caractérise par leur mode de propagation, plutôt que par leur capacité de malfaisance, trop générale.

WAN Wide Area Network
Réseau étendu ou (inter)national, un WAN est un réseau dont les nœuds sont géographiquement très éloignés les uns des autres (plusieurs centaines ou milliers de kilomètres).

X25 Les réseaux à commutation de paquets X.25 offrent une connexion à la demande entre sites (très rapides dans le cas de circuits virtuels permanents plutôt que commutés) et le système de tarification est indépendant des durées de connexion et de la distance inter-site, mais fonction des volumes de données échangées et des débits offerts.