Ministère des Enseignements Secondaire,
Supérieur et de la Recherche Scientifique
(MESSRS)

Université Polytechnique de Bobo-Dioulasso
(UPB)

Ecole Supérieure d'Informatique
(ESI)
01 BP 1091 Bobo-Dioulasso 01
Tel: (00226) 20-97-27-64

Cycle des Ingénieurs deTravaux Informatiques
(CITI)
Option : Réseaux et Maintenance Informatique
(Re.M.I)

Ministère des Enseignements Secondaire,
Supérieur et de la Recherche Scientifique
(MESSRS)

Université de Ouagadougou
(UO)
03 BP 7021 Ouagadougou 03
Tel : (00226) 50-30-70-64/65
Site : www.univ-ouaga.bf

Présidence de l'Université de Ouagadougou

Direction de la Promotion des NTIC

PROJET DE FIN DE CYCLE

THEME

MISE EN ŒUVRE DE RESEAUX LOCAUX VIRTUELS AU SEIN DU RESEAU DE L'UNIVERSITE DE OUAGADOUGOU

Stage effectué au sein de la DPNTIC du 26 juillet au 26 octobre 2004

Réalisé et soutenu par :
M. Moussa DAO
M. Kader Youssouf TRAORE

Maîtres de stage :
M. Zacharie KOALAGA
M. Romuald SAWADOGO

Superviseur :
M. Ludovic TRAORE

Année Académique 2003-2004

SOMMAIRE

DEDICACES

A la mémoire de :

- *notre très cher père le* ***Professeur agrégé Oumar TRAORE*** *qui nous a quitté voilà un an ; que son âme repose en paix et que son esprit nous guide.*

- *notre ami,* ***Habib TRAORE*** *qui nous à précocement quitté le 15 Août dernier ; que le seigneur tout puissant lui accorde le repos éternel.*

Remerciements

Nos sincères remerciements s'adressent à :

- *Dieu tout puissant ;*
- *Nos familles respectives DAO et TRAORE, qui ont su nous encourager et nous accompagner durant tout notre cursus scolaire ;*
- *Tous nos encadreurs, pour les efforts qu'ils ont consenti dans le but de nous donner une formation de qualité ;*
- *Tout le personnel de la DPNTIC et en particulier à Messieurs KOALAGA, KIKETA, Romuald SAWADOGO, MIHIN ,KONE, pour leur accueil, leur disposition à l'écoute et leurs conseils dans le sens de la réussite du présent rapport ;*
- *Tous nos camarades de classe, pour leur franche collaboration ;*
- *Tous nos parents, amis et connaissances qui de près ou de loin nous ont apporté un soutien de quelque nature que ce soit.*

Puissent-ils trouver là, l'expression de notre profonde gratitude.

SIGLES ET ABREVIATIONS

BGP	:	Border Gateway Protocol
CNRST	:	Centre National de la Recherche Scientifique et Technique
DHCP	:	Dynamic Host Configuration Protocol
DMZ	:	Demilitarized Zone
DNS	:	Domain Name System
EIGRP	:	Enhanced Interior Gateway Routing Protocol
FTP	:	File Transfer Protocol
HTTP	:	Hyper Text Transfer Protocol
IEEE	:	Institute of Electrics and Electronics Engeneers
IGRP	:	Interior Gateway Routing Protocol
IMAP	:	Internet Mail Protocol
IOS	:	Input Output System
LDAP	:	Lightweight Directory Access Protocol
MAC	:	Medium Access Control
Msis	:	Microsoft Installation Server
Msus	:	Microsoft Update Server
OSPF	:	Open Shortest Path First Protocol
POP	:	Post Office Protocol
QoS	:	Quality of Services
RAS	:	Remote Access Service
RNIS	:	Réseau Numérique à Intégration de Services
SMTP	:	Simple Mail Transfer Protocol
SNMP	:	Simple Network Management Protocol
SSH	:	Secure Shell
STP	:	Spanning Tree Protocol
TACACS		Terminal Access Controller Access Control System
TPID	:	Tag Protocol Identifier
UTP	:	Unshielded Twisted Pair
VLAN	:	Virtual Local Area Network
VLAN_form:		VLAN formation
VLAN_mon :		VLAN Monitoring
VLAN_Staff:		VLAN Administration
VLAN_Maint:		VLAN Maintenance
VPN	:	Virtual Private Network
VSAT	:	Vip Satellite
VTP	:	Virtual Trunk Protocol

INTRODUCTION

L'information a toujours été un élément essentiel dans la vie des hommes. En effet, sa quête, son traitement, sa maîtrise sont déterminants dans la gestion de toute activité (économique, socio-politique, militaire, ...). Ainsi, l'informatique qui est la science de la gestion automatique de l'information, connaît une véritable expansion dont le Burkina-Faso ne reste pas en marge ; pour former des Hommes compétents et aptes à se servir des moyens informatiques dans le sens de contribuer au développement du pays, l'Ecole Supérieure d'Informatique a été créée en 1990. La formation d'analyste-programmeurs qui a constitué son premier objet ne s'avère pas suffisant pour répondre à la demande d'un marché de plus en plus exigeant. Au fait, les entreprises ont aussi besoin de personnel pouvant se consacrer aux tâches de maintenance et de réseau. La filière Réseau et Maintenance Informatique connut ainsi le jour à la rentrée 2000. Repartie sur trois (03) ans, la formation se termine par un stage de trois (03) mois sanctionné par un rapport qui sera support d'une soutenance en vue de l'obtention de l'attestation de fin d'études. C'est dans ce cadre que nous avons eu durant douze (12) semaines à effectuer des travaux au sein de la Direction de la Promotion des Nouvelles Technologies de l'Information et de la Communication (DPNTIC) et dont le présent rapport en constitue un bilan détaillé. Ainsi, après avoir présenté la DPNTIC, nous évoquerons les différentes tâches notamment de maintenance que nous avons eu à effectuer puis nous terminerons par l'étude du thème portant sur la mise en œuvre de réseaux locaux virtuels au sein du réseau de l'Université de Ouagadougou.

PREMIERE PARTIE

PRESENTATION DE L'ENTREPRISE ET DU JOURNAL D'ACTIVITES

APERCU SUR L'UNIVERSITE DE OUAGADOUGOU

Suite au décret n°2000-469/PRES/PM/MESSRS/MEF portant nomination du chancelier de l'Université de Ouagadougou, celle-ci a connu une restructuration de ses différentes facultés en Unités de Formation et de Recherche (UFR). Ainsi elle regroupe désormais sept (07) UFR et un institut dirigés respectivement par des directeurs d'UFR et d'institut à leur tour organisés sous la coupole d'une chancellerie. Nous avons :

- UFR/SJP :Unité de Formation et de Recherche en Sciences Juridiques et Politiques .
- UFR/SEG : Unité de Formation et de Recherche en Sciences Economiques et de Gestion.
- UFR/LAC : Unité de Formation et de Recherche en Lettres, Arts et Communication.
- UFR/SH : Unité de Formation et de Recherche des Sciences Humaines.
- UFR/SEA : Unité de Formation et de Recherche des Sciences Exactes et Appliquées.
- UFR/SVT : Unité de Formation et de Recherche des Sciences de la Vie et de la Terre.
- UFR/SDS : Unité de Formation et de Recherche en Science de la Santé.
- IBAM : Institut Burkinabè des Arts et Métiers

La chancellerie est la structure administrative chargée de l'organisation et de la mise en œuvre des objectifs des UFR. Pour cela, elle veille à l'exécution des plans de gestion et assure le bon fonctionnement de la politique générale de l'Université. Son organisation hiérarchique est peinte conformément à l'organigramme en annexe1.

Elle comprend :

- **la présidence** où se trouve le chef de cabinet, le secrétariat du Président, l'attaché de presse et communication, l'assistant de sécurité, le conseiller technique et le conseiller juridique.
- **la Vice-Présidence chargée des Enseignements et des Innovations Pédagogiques** (VPEIP) qui supervise la Direction des Affaires Académiques, de l'Orientation et de l'Information (DAAOI) ; la Direction du développement Institutionnel et des innovations Pédagogiques (DIP), la Direction de la Promotion des Nouvelles Technologies de l'Information et de la Communication (DPNTIC) et la Direction de la Formation à Distance (DFD).
- **La vice-présidence chargée de la professionnalisation et des relations université-entreprises** qui est chargée de suivre le fonctionnement de la Direction de la Formation Professionnelle Continue (DFPC) et la Direction des Etudes et Consultations (DEC)
- **La vice présidence chargée de la recherche et de la coopération internationale** qui assure le fonctionnement de la Direction de la Coopération Universitaire (DCU) et la Direction de la Promotion des Enseignants et des relations avec le CAMES (DPE-CAMES)
- **Le secrétariat général** qui veille au bon fonctionnement des services centraux :Direction des Etudes et de la Planification (DEP), la Direction des Ressources Humaines (DRH) et des services rattachés tel que : le centre Système Francophone d'Edification et de Diffusion (centre SyFED) la Bibliothèque Universitaire Centrale (BUC) l'Office du Baccalauréat (OB) la Direction des Presses Universitaires (DPU) la Librairie Universitaire (LU) et l'Atelier Central de Maintenance (ACM)

- **Le service de sécurité du campus (SSC)**
- **La direction des affaires sociales (DAS)**
- **Le contrôle financier (CF)**
- **L'agence comptable (AC)**

C'est au sein donc de la **DPNTIC** évoquée plus tôt que nous avons passé trois (03) mois de stage dans le but de nous imprégner des réalités du monde de l'entreprise, de renforcer nos connaissances acquises à l'école, mais aussi d'apporter notre contribution à la promotion des nouvelles technologies de l'information et de la communication au Burkina-Faso. Mais comment la DPNTIC est-elle organisée ? Quels sont ses objectifs, ses missions, ses activités ? Comment sont structurés ses différents services et comment fonctionnent-ils ?

CHAPITRE I
PRESENTATION DE LA DPNTIC

Créée en septembre 1998, la Direction de la Promotion des Nouvelles Technologies de l'Information et la Communication (ex centre informatique) est une direction centrale de l'Université de Ouagadougou. Son but est de procéder à la rationalisation de l'utilisation de l'outil informatique de l'Université. Dirigé par un Directeur, assisté d'un adjoint (qui le remplace en cas d'absence) sa mise en place a été rendue possible grâce à l'apport du Gouvernement Néerlandais à travers le projet d'appui institutionnel ''Management Universitaire''.

I- Le cadre physique

La DPNTIC dispose d'un bâtiment entièrement câblé comprenant plusieurs salles dont :

- une salle pour la formation et le recyclage du personnel de l'Université, la formation continue et celle des étudiants
- un premier local technique (salle serveur) abritant certains serveurs
- une salle de consultation mise à la disposition des enseignants afin de leur permettre de consulter leur courrier électronique
- un deuxième local technique servant de cadre aux techniciens pour la maintenance des logiciels des différents services.

II- Les objectifs

La DPNTIC est chargée du suivi de l'étude, et de la réalisation du schéma directeur informatique de l'Université ainsi que de la formation des enseignants-chercheurs et du personnel administratif. Elle sert d'appui aux facultés en contribuant à la mise en œuvre des projets dans le domaine informatique.

III- Les missions

La DPNTIC a pour mission, la gestion du système informatique de l'Université ; la mise en œuvre et le suivi de la formation à distance et la formation des enseignants et agents administratifs ; elle s'occupe aussi de l'appui et du suivi des projets informatiques de l'Université, de la mise en place et de l'hébergement des sites Web des établissements et instituts.

IV- Les activités

La DPNTIC mène diverses activités articulées autour de :

- ✓ L'administration du réseau informatique de l'Université
- ✓ La gestion du système de messagerie de l'Université
- ✓ La gestion de la base de données de la DAAOI
- ✓ La gestion et la maintenance du parc informatique
- ✓ La formation à distance

V -Fonctionnement de la DPNTIC

1) La Direction

La Direction de la Promotion des Nouvelles technologies de l'information et de la Communication, depuis 2001 est devenue une direction centrale de l'Université de

Ouagadougou. Elle offre ses services au public et de ce fait, contribue à la réalisation de recettes au profit de l'Université. Le Directeur assisté de son adjoint est chargé de la mise en oeuvre de la politique générale de la Direction.

2) La formation à distance

Le département de la formation à distance est dirigé par un chef de département. Il s'occupe de :

- la mise en place des moyens techniques pour le suivi des cours à distance à travers les procédures pédagogiques, la mise en place de matériel didactique et médias.
- La formation classique, programmée sur les modules de bureautique ou de maintenance de premier niveau, ouverte au personnel administratif et au public.
- La formation des formateurs et des étudiants sur Cisco networking

3) L'Université Virtuelle Africaine

L'Université Virtuelle Africaine est une initiative de la banque mondiale visant à exploiter le potentiel des nouvelles technologies de l 'information et de la communication afin d'apporter à la communauté universitaire des institutions partenaires des ressources éducatives de qualité élevée au coût le moins élevé possible. Sa gestion est l'une des attributions du Directeur Adjoint.

4) Le service administratif financier et comptable

Le service administratif financier et comptable doit veiller au bon fonctionnement administratif et financier de la Direction. Cela passe par la gestion du personnel et des carrières des agents, la rédaction des projets de lettre sous instruction du Directeur, la gestion de la comptabilité, et l'exécution du budget de la DPNTIC.

5) La section administration système réseau

Cette section est dirigée par un administrateur réseau système, chargé de la gestion des structures informatiques à travers la mise en place d'un système de réseau répondant aux besoins des différents points d'accès. A cet effet, ses attributions sont :

- l'étude des besoins nécessaires au fonctionnement des différentes structures informatiques
- l'analyse et la conception
- la mise en place du réseau
- la gestion de la sécurité du réseau
- la maintenance des services réseau (messagerie, service d'accès distant, transfert de fichier)

6) La section intervention sur le parc informatique

Les techniciens informaticiens jouent un rôle d'assistance auprès des utilisateurs des services informatiques des différentes structures de l'Université. Ils se chargent de

l'aspect maintenance logicielle.

Certaines de ces tâches ont fait l'objet de notre travail pendant notre stage.

CHAPITRE II :

ACTIVITES JOURNALIERES

Au cours des trois mois que nous avons effectué au sein de la DPNTIC, nous avons souvent eu à intervenir sur des équipements en panne ou à apporter des installations nouvelles à des postes en bon état de fonctionnement. Avec l'arrêt de certains services pour congés du personnel, ce ne sont que quelques dépannages isolés, que nous avons eu à effetuer.

- Dépannage d'un ordinateur Acer Pentium II

Manifestation de la panne

Doté d'un disque dur de 4GO organisé en deux partitions de 2GO chacune et d'une mémoire vive de 32MO, cet ordinateur se plante à chaque démarrage.

Diagnostic

Nous avons diagnostiqué après plusieurs essais l'absence de certains fichiers systèmes dont l'impossibilité de chargement empêchait la poursuite du démarrage de la machine.

Résolution du problème

La résolution du problème a nécessité deux étapes. En effet, nous avons dans un premier temps commencé par la sauvegarde des données sur la partition D : du disque dur ; et dans un second temps, nous avons procéder au formatage de la partition C : puis nous y avons installé successivement Windows 98 et Microsoft Office 97.

- Mise à jour d'un ordinateur Hewlett Packard

Nous avons installé de nouveaux utilitaires sur cet ordinateur puis nous avons procéder à des mises à jour. Nous avons d'abord mis à jour Internet Explorer 5.0 en 5.1 avant de passer à l'installation de Adobe Acrobat Reader 6.0. Ensuite nous avons effectuer l'installation de Norton Antivirus 2004 ; enfin, nous avons mis cet antivirus à jour.

- Dépannage d'un ordinateur de marque IBM

Manifestation de la panne

Des messages d'erreurs intempestifs s'affichent périodiquement à l'écran réclamant l'arrêt de l'ordinateur

Diagnostic

Un virus est à l'origine de ce désagrément. Il s'agit du cheval de Troie « Sobig » qui avait déjà contaminé beaucoup de fichiers.

Résolution du problème

Pour éliminer le virus, nous avons créé un compte utilisateur sur la machine afin d'obtenir une connexion au serveur d'antivirus. Cela fait, nous avons procédé à l'examen des fichiers à travers le réseau local et ce grâce à l'antivirus réseau Vexira.

Ces interventions loin d'avoir constitué l'essentiel de notre travail, ont parfois fait l'objet de notre occupation et ont contribué à la consolidation de nos connaissances notamment en matière de maintenance.

DEUXIEME PARTIE

ETUDE DU THHEME :

Mise en œuvre de Réseaux locaux virtuels au sein du Réseau de l'université de Ouagadougou

CHAPITRE I :

PRINCIPES DES RESEAUX LOCAUX VIRTUELS

I- Généralités sur les réseaux

1) La notion de réseau

Le mot réseau est un terme très souvent employé dans un sens qui le lie à la communication. Ainsi l'on parlera de réseau téléphonique, de réseau routier, ou de réseau d'administration.

En informatique, deux (02) ordinateurs reliés entre eux par câble par exemple forment un réseau. On peut donc définir un réseau comme un ensemble d'au moins deux ordinateurs interconnectés au moyen d'éléments d'interconnexion (câble, satellite, ponts, concentrateurs...) . On notera que deux réseaux reliés entre eux par un moyen quelconque permettant aux informations de circuler forment un nouveau réseau. Un utilisateur doit être capable depuis son poste de travail d'accéder quand il le désire à toutes les informations de l'entreprise auxquelles il est censé avoir accès, où qu'elles se trouvent. En effet, il doit pouvoir formuler ses requêtes en ne sachant qu'une chose de l'information : elle existe, il a le droit d'y accéder, et elle porte un nom connu de lui. L'utilisateur accédera à une information ou à une ressource en utilisant une interface graphique ou pas, mais sans pour autant avoir conscience de l'enchaînement complexe des procédures mettant en œuvre les réseaux déclenchés par sa demande. Il y a alors nécessité d'interconnecter les différentes sources d'information afin de répondre à cette exigence. Ainsi les réseaux constituent la base indispensable préalable, l'infrastructure routière nécessaire à la circulation des informations.

2) Les réseaux locaux

a) Définition

Un LAN (Local Area Network) est un groupe d'ordinateurs connectés entre eux et situés dans un domaine géographique limité. Un réseau local permet de :

- ✓ Gérer des fichiers (partage, transfert, ...)
- ✓ Partager des applications
- ✓ Partager des périphériques (imprimante, lecteur CDROM, scanner, fax, ...)
- ✓ Interagir avec des utilisateurs connectés (agenda de groupe, courrier électronique, Internet)

Un réseau local permet généralement l'interconnexion des ordinateurs et périphériques d'une entreprise ou d'une même organisation, d'où l'appellation de réseau local d'entreprise (RLE). Dans ce concept datant de 1970, les employés d'une entreprise ont à leur disposition un système permettant l'échange d'information, la communication, et l'accès à divers services.

b) Topologie physique

Toutes les architectures dérivent de quatre (04) topologies fondamentales :le bus, l'anneau, l'étoile et la maille.

La connexion dans un LAN se fait au moyen de différents types de support de transmission filaires(paire torsadée, câbles coaxiaux, ...) ou non filaire (Wireless).

Topologies	Avantages	Inconvénients	Caractéristiques
Bus	▪ Economise la longueur de câble ▪ Support peu coûteux ▪ Simple, fiable et facile à étendre	▪ Ralentissement possible du réseau lorsque le trafic est important ▪ Problèmes difficiles à isoler ▪ Coupure pouvant affecter de nombreuses stations	▪ Connu sous le nom de bus linéaire, il s'agit de la méthode la plus simple et la plus fréquente ▪ Consiste à connecter tous les ordinateurs les uns à la suite des autres à l'aide d'un câble unique ou épine dorsale, par segment
Anneau	▪ Accès égal pour tous les ordinateurs ▪ Performance accrue	▪ La panne d'un seul ordinateur peut affecter le réseau ▪ Problèmes difficiles à isoler	Ordinateurs connectés sur une seule boucle de câble
Etoile	▪ Facilité d'ajout de postes et de modification ▪ Contrôle et administration centralisées	▪ La reconfiguration du réseau interrompt le fonctionnement de celui-ci ▪ Si le point centrale tombe en panne, tout le réseau est paralysé	Ordinateurs reliés par des segments de câble à un composant central appelé concentrateur, par lequel transitent tous les signaux
Maille	▪ Tolérance de panne ▪ Il n'y a pas d'arrêt des communications en cas de rupture de câble	▪ Coût élevé du fait de la quantité de câble à utilisée ▪ Difficultés d'installation	Ordinateurs connectés par plusieurs chemins aux autres ordinateurs.

c) Techniques d'accès au média

Dans les réseaux locaux, diverses méthodes sont utilisés par les adaptateurs réseau pour l'accès au média afin de transmettre des informations. Ces techniques sont normalisées par l'IEEE et définies à travers ses spécifications, notamment 802. Ainsi nous avons par exemple:

- ✓ L'accès multiple avec écoute de la porteuse et détection de collision (Carrier-Sense Multiple Access with Collision Detection :CSMA/CD) : cas des réseaux locaux Ethernet ;

- ✓ L'accès à jeton : cas du Token Bus LAN et du Token Ring LAN
- ✓ L'accès fondé sur la priorité de la demande (Demand Priority Access LAN) : cas des réseaux locaux 100BaseVG-AnyLAN

Le mode de communication a donc longtemps consisté en l'écoute du média par les différents postes connectés ou en une organisation autour d'un jeton qui oblige chacun d'eux à attendre son tour. Mais avec l'expansion des réseaux, l'augmentation du nombre de postes à câbler, l'exigence des utilisateurs en demande de bande passante, l'utilisation des équipements traditionnels (répéteurs, concentrateurs faisant de la recopie bit à bit des informations de tronçon à tronçon) est peu à peu abandonné au profit d'autres éléments plus efficaces.

3) L'Ethernet classique et ses améliorations

Les réseaux Ethernet ont été révolutionnés dans le but de pallier les différentes difficultés que rencontraient les réseaux Ethernet traditionnels. En effet, ces derniers fonctionnaient à 10Mbit/s et diffusaient toutes les données sur le même lien physique, utilisant dans la plupart du temps, soit la paire torsadée, soit le câble coaxial et partagé par tous les équipements actifs. La norme Ethernet ne permet qu'à un seul équipement de transmettre à la fois, les autres devant attendre que le media soit libre.

Les ponts sont des équipements d'interconnexion de deux segments de réseaux locaux. Ils permettent déjà de ne plus propager les erreurs ou les collisions (limitation des domaines de collision à chaque réseau local), mais ne constituent pas toujours pas une solution idoine de commutation .

D'autres type de ponts (ponts filtrant) ont permis de ne laisser passer que le trafic devant transiter d'un tronçon à l'autre (forwarding). Mais bien que ce soit un pas vers la commutation souhaitée, les diffusions s'étendent encore à tous les tronçons.

C'est alors que l'utilisation de commutateurs associée à la mise en œuvre de VLANs permet d'atteindre de meilleurs résultats.

4) La commutation

a) Définition

Un commutateur permet simultanément plusieurs connexions indépendantes entre les ports. Chaque port du commutateur relie un segment différent. Cela permet de supprimer les goulots d'étranglement et de mettre en œuvre des architectures Clients-Serveurs performantes. De plus cette technique permet de conserver l'infrastructure de câblage existant.

b) Fonctionnement

Les commutateurs peuvent être configurés dans le réseau tout comme il peuvent s'auto configurer par apprentissage.

- l'apprentissage

Les commutateurs peuvent ne pas être configurés au préalable. A l'initialisation, les tables de commutation sont alors vides et elles devraient être remplies progressivement grâce au processus d'apprentissage. Ainsi toutes les trames circulant sur les tronçons reliés à un commutateur sont écoutés; à chaque arrivée de

trame sur un port, les commutateurs notent dans la table de commutation l'adresse d'émission avec son port. Si la destination d'une trame à relayer n'est pas connue, la trame est diffusée sur tous les ports pour atteindre son destinataire. Par contre, si la destination est connue, la trame est recopiée sur le seul port de l'adresse destination, sauf si c'est le même port que celui de la source.

Exemple d'apprentissage :

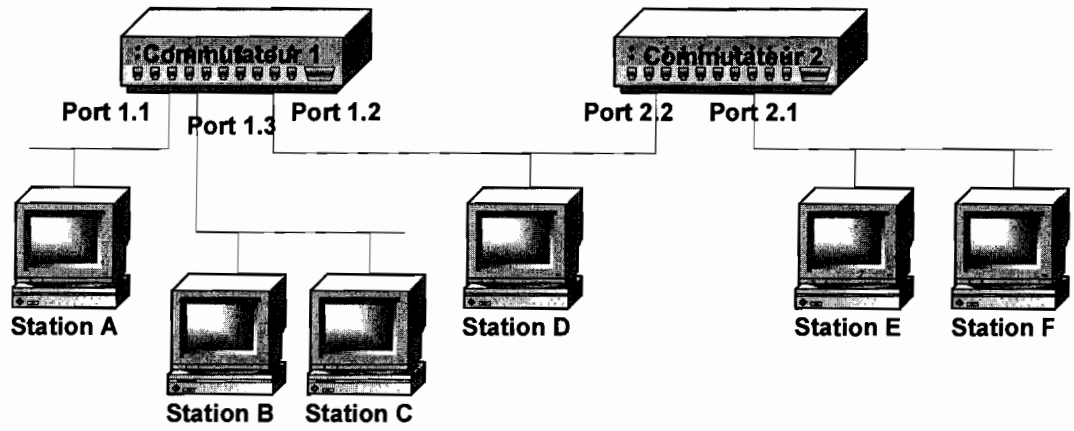


Schéma d'organisation de postes sur deux switchs

- trame de la station C vers la station D

Le commutateur1 diffuse la trame sur port1.1 et port1.2 et apprend que la station C est du côté de port1.3 ; la trame est délivrée à la station D.

- trame de la station B vers la Station C:

Le commutateur1 apprend que B est du côté de port1.3 tout comme la station C. Il ne retransmet pas la trame ; la trame est délivrée à la station C.

- trame de station F vers station A

Le commutateur1 reçoit et diffuse ; il apprend que station F est du côté de port1.2. Quant au commutateur2, il diffuse également la trame et apprend que la station F est du côté de port2.1.

- la technique de stockage et retransmission (shared memory ou store and forward)

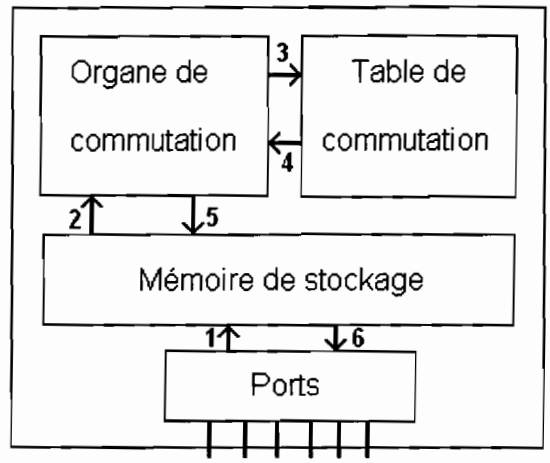


Schéma de fonctionnement

1- la trame entrante est entièrement reçue et stockée dans la mémoire ;
2- le module de commutation extrait l'adresse de destination ;
3- l'adresse destination est envoyée à la table de commutation ;
4- le résultat de la recherche est retourné ;
5- l'adresse du port de sortie est propagée ;
6- la trame est renvoyée à partir de la mémoire sur le port de sortie approprié.

Cette technique a longtemps été délaissée à cause du temps de stockage, mais aujourd'hui elle prend de l'intérêt grâce aux meilleures performances des microprocesseurs. Un contrôle d'erreurs est effectué, les trames correctes sont relayées vers le bon port tandis que les trames erronées sont supprimées.

- la commutation à la volée (On the fly ou cut through)

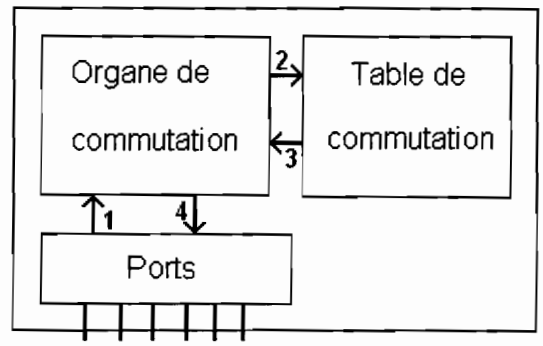


Schéma de fonctionnement

1- l'organe de commutation lit le début de la trame et extrait l'adresse de destination ; la trame continue à arriver
2- l'adresse est envoyée à la table
3- le résultat est retourné
4- le module de commutation renvoie la trame sur le port de sortie dès que possible (de préférence avant qu'elle ne soit totalement entée).

Cette méthode a pour principal avantage, la réduction du temps de transit à

quelques microsecondes. En revanche, le contrôle d'erreurs n'est pas effectué ; ces commutateurs ont peu de mémoire et certaines trames peuvent être supprimées si la mémoire tampon de sortie est insuffisante. De plus ils relayent toutes les trames erronées et les fragments de collision.

Les réseaux commutés offrent donc :

- Une économie et une efficacité : ils sont bon marché, utilisent le câblage, les cartes réseau et les applications existantes ;
- Une bande passante totale plus élevée : chaque port du commutateur dispose de toute la bande passante ;
- La capacité de fournir un réseau hétérogène
- Une réduction du nombre d'adresses de chaque sous-réseau disponible grâce aux groupes logiques ;
- La possibilité d'adapter les vitesses entre nœuds de communication en fonction du trafic ;
- Les commutateurs sont faciles à déployer progressivement dans un réseau existant ; ils sont extensibles par rajout de port

En comparaison à l'Ethernet classique, l'Ethernet commuté n'utilise pas le principe de média partagé ; il permet à chaque utilisateur de disposer d'une bande passante dédiée. Chaque port du commutateur étant couplé avec un autre, le commutateur autorisera autant de dialogue qu'il y a de ports sur deux (02) .

De plus, l'écoute du réseau est quasi impossible contrairement à l'Ethernet classique. Les réseaux commutés divisent un réseau local en segments indépendants, ils interconnectent les segments en fonction des besoins. Le débit d'interconnexion interne est généralement très élevé.

II- Les réseaux locaux virtuels.

1) Les limites des commutateurs

Les commutateurs présentent par ailleurs de nombreuses contraintes : Les sous réseaux sont physiquement liés au matériel ce qui engendre des difficultés de câblages. Les utilisateurs sont alors nécessairement regroupés géographiquement. L'apparition d'applications exigeant une excellente qualité de service (QoS), le volume du trafic en forte croissance et la nécessité de sécurité ont amené à un travail d'optimisation dans la gestion de la bande passante. Les réseaux locaux virtuels corrigent ces défauts et permettent de mettre en œuvre des réseaux informatiques locaux ou métropolitains axés sur l'organisation de l'entreprise s'affranchissant de la localisation géographique.

2) Notions de réseaux locaux virtuels

On pourrait définir un réseau local virtuel (Virtual Local Area Network VLAN en Anglais) comme étant un réseau local « évolué » dans un sens où la segmentation en sous réseau, en groupe de machines ou d'utilisateurs, n'est pas dictée par les regroupements physiques de machines et la répartition physique des ponts entre les segments, mais par d'autres facteurs sur lesquels on peut agir logiquement. Ces stratégies logiques sont mises en œuvre par la commutation.

On peut ainsi définir logiquement des domaines de diffusion et des groupes de travail indépendamment de l'endroit où se situent les systèmes. Toute station se trouvant en dehors du réseau local virtuel considéré ne recevra pas les trames destinées à ce dernier. Cette segmentation virtuelle permet également de constituer des sous

réseaux logiques en fonction des critères prédéfinis comme les adresses MAC ou les protocoles et de sécuriser et contrôler les échanges à l'intérieur d'un domaine et entre les domaines de réseaux virtuels locaux.

Ils facilitent la configuration et l'administration physique des réseaux locaux d'entreprises. Il n'existe quasiment plus un reconfiguration physique au niveau de l'armoire de brassage, mais une action logique directe à partir d'une console d'administration. Le changement de groupe de travail devient plus aisé. Ils permettent également une meilleure gestion du flux, mais nécessitent pour cela des protocoles d'administration réseau tels que SNMP (Simple Network Management Protocol), associé à des MIB (Management Information Base) adéquates.

Le concept initial des réseaux locaux virtuels consistait donc en la définition de sous réseaux traités comme domaines de diffusion. Le succès actuel des réseaux locaux virtuels repose sur les nouvelles organisations hiérarchiques et fonctionnelles des entreprises en groupe de travail.

Mais de plus en plus, on constate que la notion de réseaux locaux virtuels s'élargit pour aboutir à un concept définissant des groupes d'utilisateurs, sans nécessairement associer la notion précise de broadcast.

3) Importance des réseaux locaux virtuels

Les réseaux locaux virtuels sont d'une grande importance dans l'implantation des réseaux d'entreprise dans la mesure où ils permettent :

- La mobilité des utilisateurs du réseau : la définition des groupes étant logique, à travers le réseau, les utilisateurs pourront accéder à leur groupe indépendamment de la localisation physique, mais grâce à des machines définies dans ce groupe;
- L'assouplissement des conditions de diffusions de données : les sous groupes auxquels un même message est destiné peuvent être aisément reconfigurer selon les besoins ;
- L'interdiction de communiquer entre des utilisateurs de groupes de travail différents ou le contrôle les communications inter réseaux virtuels selon les besoins ;
- Une meilleure gestion des flux donc de meilleures performances (la facilité d'affectation à un réseau local virtuel ou à un autre va permettre de gérer de façon simple les flux d'informations)

En résumé, les réseaux locaux virtuels ont révolutionné le concept de segmentation des réseaux locaux. Ils permettent de constituer autant de réseaux logiques que l'on désire sur une seule infrastructure physique, réseaux logiques qui auront les mêmes caractéristiques que des réseaux physiques.

4) Normalisation relatives aux réseaux locaux virtuels

Plusieurs normes sont plus ou moins directement liées au réseaux locaux virtuels :

- La norme 802.10 qui a été détournée au départ pour faire du tagging ;
- La norme 802.1q que l'IEEE a défini en 1998 pour l'échange des tables MAC entre commutateurs ;
- La norme 802.1d, qui traite de la reconfiguration automatique des réseaux locaux avec le protocole STP
- La norme 802.3ac qui est cours de consultation et qui traite également du tagging.

L'IEEE a parfois tardé à développer ces normes et les solutions propriétaires se sont multipliées notamment pour les liaisons inter commutateurs, interswicthlink (ISL) chez CISCO, alors que la norme 802.1q est appliquée ailleurs), ce qui peut causer des problèmes d'interopérabilité. Cependant, il est constaté que la norme 802.1q est maintenant suivi par tous les industriels, qui définissent en plus d'autres normes propriétaires, notamment pour le management des commutateurs.

Les réseaux locaux virtuels sont couramment utilisés pour les réseaux locaux importants des universités, des centres de recherches ou des grandes entreprises au sein desquels il est facile de définir différents départements ou secteurs.

III) Constitution et classification des réseaux locaux virtuels

La mise en oeuvre des réseaux virtuels s'axent de manière succincte autour de deux (02) aspects:

- Les méthodes de constitution des réseaux locaux virtuels ;
- Les méthodes de communication intra et inter réseaux locaux virtuels.

La constitution des réseaux locaux virtuels est dépendante du type de support utilisé. On distinguera en fait 02 types de support au comportements différents :

- ✓ Ethernet pour représenter les supports fonctionnant en mode diffusion
- ✓ ATM (Asynchronious Transfert Mode) pour représenter les supports en mode circuits virtuels.

Pour un réseau à base d'une technologie de type diffusion tel que Ethernet, la constitution du réseau virtuel va consister à filtrer ou bloquer les trames normalement diffusées sur l'ensemble du réseau. Ainsi la constitution des réseaux locaux virtuels, s'appuiera sur un réseau constitué de commutateurs (fonctionnellement identiques à des ponts filtrants multi ports) et une technologie propriétaire permet alors au différent commutateurs de se tenir informer des constitutions de ces réseaux locaux virtuels.

Les technologies offertes actuellement permettent la constitution des réseaux locaux virtuels basés sur Ethernet. Les switches Cisco permettent (généralement) de le faire sur Token Ring et FDDI. Mais dans tous les cas, les méthodes de réalisation des réseaux locaux virtuels sont :

- Par ports
- Par adresse IEEE ou adresse MAC
- Par protocole
- Par sous réseaux
- par règles

1) Constitution des réseaux locaux virtuels

a) les réseaux locaux virtuels par ports

Un réseau local virtuel par port, aussi appelé réseau local virtuel de couche physique, est obtenu en associant chaque port du commutateur à un réseau virtuel particulier. C'est une solution pratique qui a été rapidement mise en œuvre par les constructeurs. La gestion des réseaux locaux virtuels devient alors simple dans la mesure où l'association du numéro du réseau virtuel au numéro de port s'effectue par l'administrateur réseau d'où la notion en anglais de « VLAN port based ». Les réseaux virtuels locaux par port manquent de souplesse. tout déplacement d'une station nécessite une reconfiguration des ports. Toutefois la sécurité y est excellente du fait que toutes les stations peuvent communiquer entre elles sur un même tronçon parce

qu'appartenant au même réseau local virtuel. Elles communiqueront avec d'autres réseaux virtuels selon les configurations et les besoins.

b) les réseaux locaux virtuels par adresse MAC

Un réseau local virtuel par adresse MAC ou encore réseau local virtuel de niveau 2 est constitué en associant les adresses MAC des stations à chaque réseau virtuel. L'intérêt de ce type de réseau est surtout l'indépendance vis-à-vis de la localisation : la station peut être déplacée sur le réseau physique, son adresse physique ne changeant pas, il est inutile de reconfigurer le réseau. Toutefois la configuration peut s'avérer rapidement fastidieuse puisqu'elle nécessite de renseigner une table de correspondance avec toutes les adresses du réseau. Cette table doit aussi être partagée par tous les commutateurs ce qui peut engendrer un trafic supplémentaire sur le réseau.

c) les réseaux locaux virtuels par protocole

Ils sont obtenus en associant un réseau virtuel à chaque type de protocoles rencontré sur le réseau. Ainsi on peut constituer un réseau virtuel pour les stations communiquant avec le protocole TCP/IP, un autre communiquant avec le protocole IPX. Dans ce type de réseau, l'avantage est que les commutateurs apprennent dynamiquement leur configuration. Par contre elle est légèrement moins performante puisque les commutateurs sont obligés d'analyser les informations de niveau 2. les réseaux virtuels par protocoles sont surtout intéressant dans des environnements hétérogènes multi protocoles quoique la généralisation de TCP/IP leur a fait perdre de l'intérêt.

d) Les réseaux locaux virtuels par sous réseaux

Ils utilisent les adresses IP sources des data grammes émis. Un réseau virtuel est associé à chaque sous réseau IP. Dans ce cas les commutateurs apprennent aussi dynamiquement la configuration de ces réseaux virtuels et il est possible de changer une station de place sans reconfiguration. Cette solution est l'une des plus intéressante, malgré une légère dégradation des performances de la commutation due à l'analyse des informations du niveau réseau (couche 3).

e) Les réseaux locaux virtuels par règles

Ils constituent une nouvelle méthode de définition des réseaux virtuels basées sur la possibilité pour les commutateurs d'analyser le contenu des trames. Les possibilités sont multiples, allant des réseaux virtuels par type de service(ports TCP) aux réseaux virtuel par adresses multicast IP.
Quelque soit le mode de construction d'un réseau local virtuel, les trames véhiculées peuvent avoir deux formats ; c'est-à-dire marquée ou non.

f) Classification des réseaux locaux virtuels

De nombreuses solutions de constitution des VLAN ont été mises en œuvre, chacune avec ses avantages et ses faiblesses. Mais, leur classification est toujours relatives à la conception et la compréhension des uns et des autres.

➢ **Classification basée sur les couches (niveau)**

La classification tient compte du niveau de couche dont l'information ou le matériel est l'élément caractéristique autour duquel le VLAN a été réalisé. Ainsi on parlera de :

- **Vlan de niveau 1** : ceux constitués par ports physiques (couche1)
- **Vlan de niveau 2** : ceux associés aux adresses MAC ou aux en-têtes de protocole (couche 2)
- **Vlan de niveau 3** : ceux construits autour des règles, ou des sous-réseau (couche 3)

➢ **Classification basée sur le mode de reconfiguration**

En effet, quand on réalise un Vlan par port, à chaque modification du système (déplacement de machine par exemple) il faut reconfigurer manuellement le réseau. Par contre quand il s'agit des Vlan par adresse MAC, par protocole, par sous-réseau ou par règles, la reconfiguration se fait dynamiquement. Ainsi, dans le premier cas, on parlera de Vlan statique et dans le second, de Vlan dynamique.

➢ **Choix d'une classification**

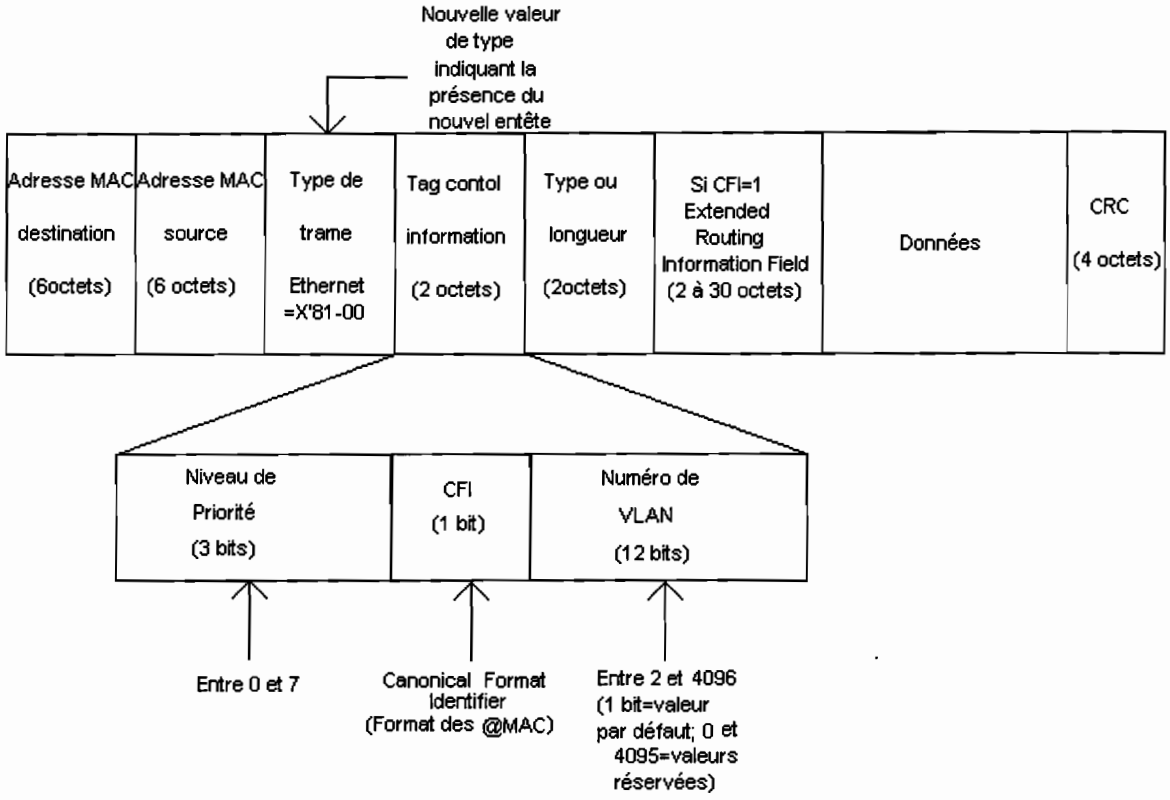
La classification basée sur les couches (par niveau) est davantage détaillée que la deuxième. Elle permet de distinguer les Vlan par adresse MAC de ceux par protocoles et autres services. Ainsi, c'est sur cette classification que nous nous baserons tout au long de notre travail qui consistera en la mise en œuvre de Vlan au sein du réseau de l'Université de Ouagadougou .

2) le marquage des trames

Vu comme un concept d'encapsulation des trames dans les réseaux locaux virtuels, le marquage (ou l'étiquetage) des trames consiste à insérer des informations relatives à la description du réseau virtuel d'origine dans les trames transmises à travers les commutateurs. Il permet donc de reconnaître le réseau virtuel d'origine d'une trame et à l'acheminer vers la destination. Il existe trois (03) type de trames véhiculées à travers les commutateurs des réseaux virtuels :

➢ **Les trames non taggées** : on observe l'absence d'en tête (Tag Protocol Identifier + tag control information) après l'adresse source MAC ;

- **Les trames taggées de priorités** : si le bit du VID (Virtual LAN Identification) est positionné à zéro (0), cela signifie que cette trame n'est pas signifiante. Elle ne transporte que des informations de priorité. Du point de vue du processus de transmission, elle est générée comme une trame non taggée.
- **Les trames taggées de réseaux virtuels** : les différents bits sont tels que



Format d'une trame Ethernet avec nouvel en-tête normalisé

TPID :0x8100 ; CFI(Canonical format identifier)=0 ; et le VID= 1 et 4094.

a) le marquage implicite des trames

Ce marquage consiste à déduire des informations contenues dans la trames (adresses MAC, protocoles, sous réseaux IP...). Dans le cas d'un réseau local virtuel par port, le transfert d'une trame vers un autre commutateur ne conserve pas d'information sur son appartenance à un réseau virtuel. Le marquage implicite est alors quasi inexistant. Dans le cas d'un réseau virtuel par adresses MAC, il est possible d'envisager que la table de correspondance entre adresses MAC et numéro de réseau virtuel soit distribuée sur tous les commutateurs. Mais c'est une solution lourde à laquelle on peut préférer l'autre type de marquage. Par contre les réseaux locaux virtuels réalisés par rapport à des protocoles, des adresses IP ou des règles utilisent un marquage

implicite. Il n'est pas obligatoire de marquer les trames sur les liaisons inter commutateurs.

b) le marquage explicite des trames.

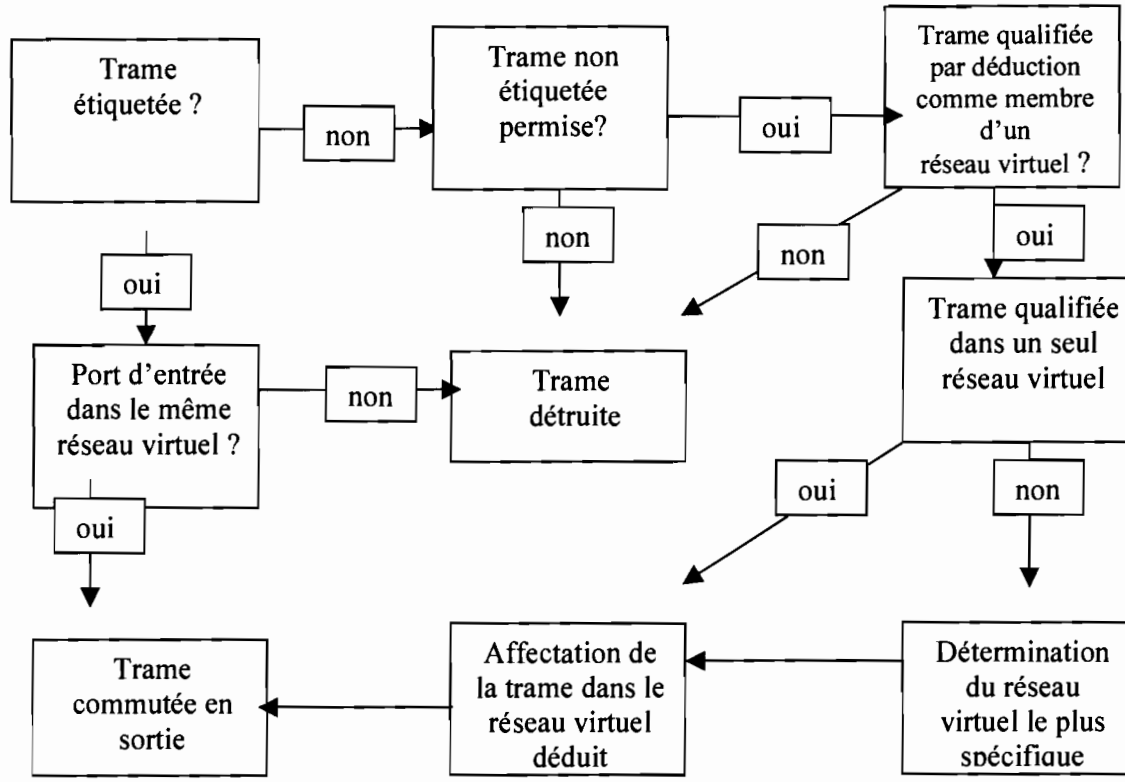
Ce marquage consiste à insérer des informations supplémentaires (souvent un numéro de réseau virtuel) dans la trame afin d'en déduire à quel réseau virtuel elle appartient. La définition de réseau virtuel à travers plusieurs commutateurs se complique. Dans le cas d'un réseau virtuel par port, le marquage implicite étant quasi inexistant, il est nécessaire de mettre en œuvre un marquage explicite des trames. Dans le cas d'un réseau virtuel par adresses MAC, comme mentionné précédemment, le problème de distribution des tables de correspondances entres les commutateurs peut se solutionner par un marquage explicite des trames. Aussi, dans le cas d'un réseau virtuel réalisés par rapport à des adresses IP ou des règles , il est parfois préférable de marquer explicitement les trames du fait que leur analyse au niveau de la couche 3 dégrade les performances du commutateurs.

Plusieurs solutions constructeurs ont été proposées telles que le Virtual Tag Trunking de 3COM ou encore InterSwitchLink (ISL) de CISCO, toutes incompatibles entre elles.

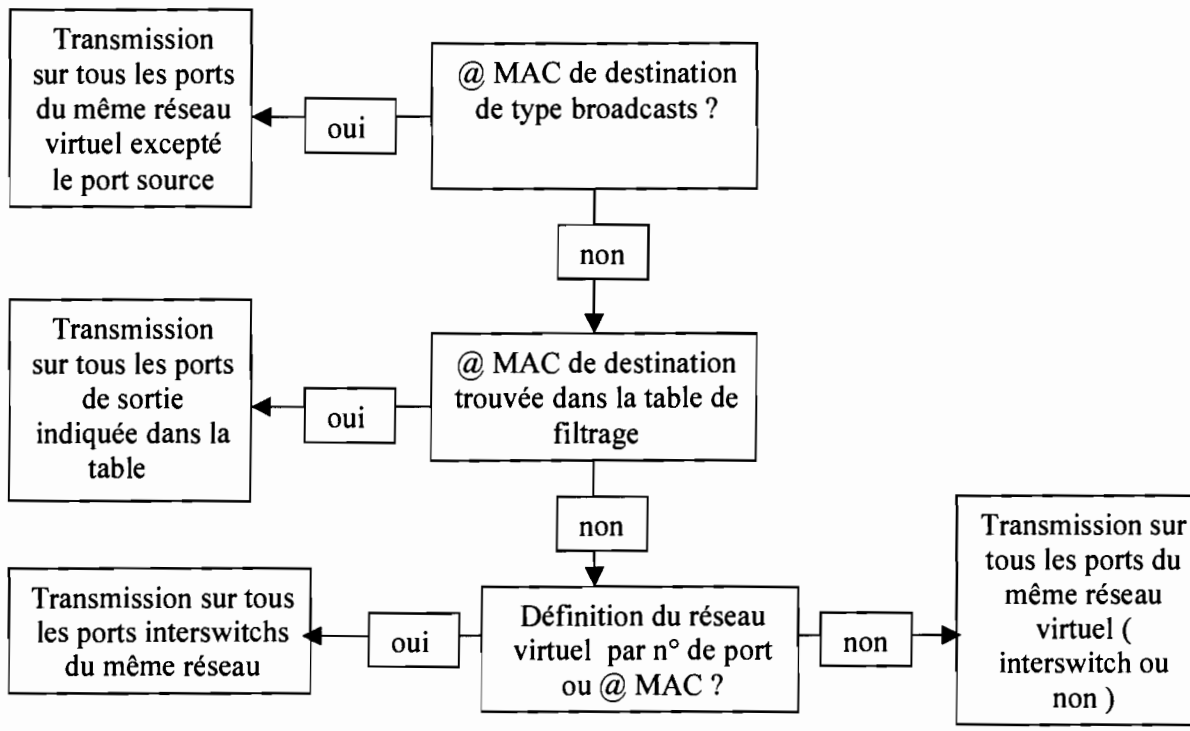
c) le traitement des trames

Trois étapes résument le traitement des trames dans les réseaux locaux virtuels :

- d'abord, il s'effectue une détermination du réseau virtuel d'origine de la trame reçue en entrée ; elle est immédiate si la trame est étiquettée, et par déduction sinon.
- ensuite se déroule un examen de la table de filtrage afin de déterminer le port de sortie
- enfin, pour chaque port de sortie, il s'effectue un test de son appartenance au réseau virtuel de la trame ou si la trame doit être étiquettée avant d'être transmise.



Traitement des trames en entrée



3) Types de liens dans les VLAN et communication inter VLAN

a) Types de liens dans les VLAN

Deux types de liens peuvent être rencontrés dans les Vlan :

Acces link (lien d'accès) : ce sont des liaisons entre équipements ne supportant pas les Vlan. Des trames non-étiquetées transitent sur ces liens (untagged frame)

Trunk link : ce sont les liaisons entre deux équipements (switchs, serveurs...) supportant les Vlan. Des trames étiquetées transitent sur ces liens.

b) Communication inter Vlan

Il existe différentes solutions pour la communication entre Vlan :

- **utilisation d'un routeur** : ce routeur peut être connecté sur plusieurs ports appartenant à plusieurs Vlan ou sur un seul port de type Trunk link
- **utilisation d'un switch/routeur** : c'est un switch de niveau 2 et 3 c'est-à-dire un switch incluant des fonctionnalités de routage.

CHAPITRE II : MISE EN ŒUVRE DE VLANs AU SEIN DU RESEAU DE L'UNIVERSITE DE OUAGADOUGOU

Un réseau d'établissement ou d'université bien structuré, et connecté vers l'extérieur, est un atout majeur pour l'évolution des méthodes de travail et des pratiques pédagogiques. Il favorise un nouveau type de travail, fondé sur l'échange et le partage d'informations. En général les besoins des utilisateurs de ces réseaux sont tels que:

- L'étudiant ou l'élève est amené à travailler plus souvent sur les mêmes documents depuis des lieux variés (salles de cours, salles de travail en autonomie, domicile...) et à les partager avec d'autres utilisateurs du milieu scolaire ou universitaire, professeurs, personnels d'encadrement, voire avec des personnalités d'extérieures.
- L'enseignant est amené à partager et à produire des ressources communes depuis différentes salles de l'établissement ou de l'université, depuis son bureau ou son domicile : il conduit des projets en collaboration avec des équipes au Burkina ou à l'étranger.
- Les équipes administratives et de gestion partagent des informations, tant au niveau local qu'au niveau central.

Cette évolution des méthodes, des pratiques pédagogiques, mais aussi celle des technologies font que le réseau d'université ou d'établissement scolaire est devenu un outil indispensable dans la collectivité éducative.

I- Présentation du sujet

Le réseau informatique de l'Université Ouagadougou est un réseau qui s'étale sur un domaine géographique assez vaste et pour lequel il est prévu des perspectives d'expansion. Regroupant différents types d'utilisateurs, dont des services administratifs, des enseignants chercheurs, des étudiants recourant à de multiples services allant de la messagerie à la formation, notre prérogative première est de bien organiser la cohabitation de tous ces acteurs tout en satisfaisant leurs nombreux besoins de communication. Ainsi, c'est dans le souci de parvenir à la réalisation d'un réseau dont la répartition des services et ressources serait la plus profitable aux utilisateurs, que nous avons choisi de réfléchir et de mettre en œuvre des réseaux locaux virtuels au sein de ce réseau.

1) Objectifs

Cette organisation devra d'abord permettre aux utilisateurs de bénéficier de façon plus qualitative mais aussi quantitative des potentialités réseau offertes par les équipements (bande passante, rapidité de traitement) ou de pouvoir appartenir à des groupes de travail indépendamment de l'endroit où se situent les systèmes.

Ensuite elle devra permettre de contrôler et de sécuriser les échanges à l'intérieur d'un domaine et entre les domaines de réseaux virtuels locaux, ce qui est une solution au problème de la confidentialité des données.

Enfin la réalisation de VLANs devra permettre une certaine centralisation, d'où un meilleur contrôle du réseau et des procédures de reconfiguration plus facile pour les administrateurs.

2) Démarche utilisée

Afin de parvenir à la réalisation effective de ce projet nous devons passer par

plusieurs étapes :

- premièrement nous procéderons à une étude suivie d'une analyse de l'existant afin de prendre connaissance des plans déjà réalisés, des équipements disponibles et de leurs potentialités
- deuxièmement, nous examinerons des propositions de solutions, puis nous en retiendrons une.
- troisièmement nous passerons à la simulation de configuration des équipements.

II- Etude de l'existant

1) Présentation géographique du réseau de l'université de Ouagadougou

Le site de l'université de Ouagadougou est traversé par le canal d'évacuation des eaux de pluies du quartier Zogona qui le subdivise en deux (02) zones. Ainsi d'un coté, on a la rive droite ou la zone UFR/SJP, et de l'autre coté, la rive gauche ou la zone DPNTIC. Chaque zone est ensuite subdivisée en secteurs. La zone DPNTIC comporte les secteurs suivant :

- la DPNTIC
- la BUC
- l'UFR/SEA
- l'UFR/SEG

La zone UFR/SJP comporte quant à elle les secteurs :

- l'UFR/SJP
- l'UFR/SDS
- l'UFR/SVT (CRSBAN)

Le CENOU est le seul secteur à avoir un réseau informatique indépendant de celui de l'université jusqu'à ce jour.

Dans la zone DPNTIC, le secteur DPNTIC compte les réseaux locaux de la DPNTIC, du SAOI, de la vice-présidence, de la présidence et de l'UFR/SEG et assure le service d'un ensemble de serveurs de l'université. Le secteur de la BUC compte les réseaux locaux des UFR LAC/SH (salle des professeurs) et de la BUC. Le secteur de l'UFR/SEA regroupe les réseaux locaux du laboratoire de physique (scolarité SEA), celui du bâtiment de chimie et celui du bâtiment belge SH (salle de cours).

Dans la zone SJP, on retrouve le secteur de l'UFR/SJP regroupant la scolarité de l'UFR/SJP (Bâtiment SJP sur le schéma), la bibliothèque SJP et le bâtiment belge SJP/SEG. Le secteur de l'UFR/SDS regroupe quant à lui les réseaux locaux de l'ACM et celui de la bibliothèque SDS. Enfin le secteur de l'UFR/SVT regroupe les réseaux locaux de la scolarité, de la bibliothèque SVT et l'ex-IBAM. (Voir le plan géographique)

2) Présentation du réseau actuel de l'université de Ouagadougou

L'artère fédératrice (backbone) s'articule autour d'une topologie physique en étoile étendue et une topologie logique utilisant la méthode CSMA/CD (la topologie logique étant la représentation de la manière dont l'information circule sur le réseau, la topologie physique étant la représentation physique du réseau).

Le backbone comporte deux nœuds principaux : le répartiteur principal de la DPNTIC et le répartiteur principal de l'UFR/SJP. A côté de ces nœuds principaux, on trouve les nœuds secondaires dont les répartiteurs secondaires de la BUC, de la SEA, du

CRSBAN. En outre au sein de chaque nœud principal on trouve un nœud secondaire dont un à la DPNTIC et l'autre à la SJP. Le schéma de la figure illustre cette organisation du Backbone en topologie étoile étendue.

3) Plan d'adressage actuel

Le système d'adressage du réseau actuel de l'Université de Ouagadougou s'organise comme indiqué dans le tableau suivant :

Tableau des adresses IP

ZONE	ADRESSE RESEAU	MASQUE RESEAU	SERVEURS/PC UTILISATEURS
DMZ	212.52.131.0	255.255.255.0	Ancien MAIL, DNS, Nouveau MAIL, CNRST, WEB, Fichiers FTP, FAD
INTERNE Dynamique	172.18.0.0	255.255.240.0	PC utilisateurs
INTERNE Statique	172.18.0.1 - .16	255.255.240.0	BUCIS, AASIS,SINDOU, ANTIVIRUS
EXTERNE	192.168.1.1 - 5.2	255.255.255.0	Console management, TACACS (Authentification accès distant) DNS VSAT, Interface de routeur VSAT.
UONET CORE	192.168.3.0	255.255.255.0	Ensemble des switchs du réseau pour le monitoring.

4) Inventaire du matériel et des logiciels réseau existants

Le réseau de l'université se compose d'environ :

- 13 serveurs ;
- 01 firewall ;
- 03 routeurs ;
- une vingtaine de commutateurs ;
- environ 05 concentrateurs dans chaque UFR ;
- plus de 250 PC utilisateurs à travers toute l'Université

Ces équipements seront utilisés dans la mise en œuvre de notre projet. De façon plus détaillée, les caractéristiques de quelques-uns des éléments actifs du réseau sont regroupées dans des tableaux plus loin.

a) Les serveurs

Les serveurs présents dans le réseau de l'Université offrent les services applicatifs suivants :

- le service de messagerie ;
- le service WEB de l'université et du CNRST ;
- les services de stockage de base de données relatifs aux étudiants et au personnel…
- les services d'antivirus ;
- le service d'accès distant par réseau téléphonique public commuté.
- le service de résolution de noms DNS
- le service de transfert de fichiers FTP

Mais il existe d'autres services qui ne sont pas directement visibles par les utilisateurs et dont l'implémentation au sein du réseau de l'université se révèle très important pour le bon fonctionnement du réseau. Ce sont entre autre le service de translation d'adresse (NAT), et le service d'attribution dynamique d'adresses IP (DHCP)… De manière plus exhaustive les principaux services applicatifs fonctionnels au sein du réseau sont :

Le Web : c'est ce dernier qui héberge le site de l'Université de Ouagadougou.

La base de données BUCIS: c'est l'application destinée à la gestion de la Bibliothèque Universitaire Centrale.

La base de données AASIS : cette base de données est conçue pour gérer les inscriptions académiques des étudiants de l'université de Ouagadougou. Le nombre d'utilisateurs dépend fortement de la période d'activité du service de la Scolarité. Ainsi, en début de rentrée académique on a une vingtaine d'utilisateurs concurrents de la base de données.

Le DNS : Domain Name Service : Le DNS est un service permettant à un ordinateur du réseau d'inscrire et de résoudre des noms de domaine plus accessibles aux utilisateurs (correspondance nom<=>IP) et ainsi de permettre une meilleure accessibilité des ressources.

Le Mail (Messagerie): Postfix : Le service de la messagerie a été implémenté à partir du logiciel Postfix, disponible dans la distribution Linux (Red Hat 8.0.)

Le service de la messagerie électronique regroupe plus de 797 comptes électroniques dont les utilisateurs sont principalement le personnel administratif et technique, le personnel enseignant de toute l'Université de Ouagadougou et certain enseignant de l'Université Polytechnique de Bobo.

Le NAT (Network Address Translation)

NAT est l'abréviation de Network Address Translation, une norme Internet qui permet à un réseau local d'utiliser un ensemble d'adresses IP pour le trafic interne et un deuxième ensemble d'adresses pour le trafic externe. Autrement dit, NAT permet à une interface (routeur ou serveur) de "cacher" des machines internes, permettant à ces multiples machines internes de partager une unique adresse IP publique.

Le NAT permet la cohabitation des machines avec des adresses IP sur un réseau relié à Internet sans devoir obtenir et assigner des "vraies" adresses IP pour chaque machine. Cela fonctionne grâce à une modification de l'en-tête des adresses IP et de certains champs des en-têtes des protocoles de plus haut niveau. Ainsi les adresses IP internes "cachées" sont remplacées par une "vraie " IP adresse qui peut traverser sans risque Internet. Avec une seule "vraie" adresse IP assignée au routeur, jusqu'à 64000 machines clientes IP peuvent partager cette adresse simultanément pour accéder à Internet.

Le DHCP (Dynamique Host Control Protocol) : c'est le service chargé de l'attribution automatique d'adresses IP aux clients DHCP.

Le FTP : File Transfer Protocol (ou Protocole de Transfert des Fichiers)

Ce service était implémenté au départ sous le système d'exploitation Novell avant d'être redirigé vers le système Linux.

A travers donc un tableau plus exhaustif nous avons relevé les différentes caractéristiques de chaque serveur existant sur le réseau.

Type de serveur	Ancien serveur Mail	Serveur Mail	Serveur Web	Serveur SINDOU	Serveur BUCIS	Serveur AASIS	Serveur DNS	Serveur d'accès distant (RAS)	Serveur du projet FAD	Serveur WEB du CNRST
Marque	IBM	COMPAQ Proliant ML 370	IBM netfinity	DELL power Edge	ZERNIKE	ZERNIKE	DELL Optiplex GX 110	DELL Optiplex GX 110	DELL Optiplex GX 110	IBM
Processeur	PII 800MHz/XEON	Processeurs Intel XEON DP 3,4 GHz	PII 800MHz	PII 200 MHz	Pentium XEON 2GHz	Pentium XEON 2GHz	PIII 500 MHz	X86 family	PIII 500 MHz	PII 800MHz/XEON
Taille RAM	128 Mo	1Go	128 Mo	128 Mo	2096Mo	2096Mo	128Mo	64Mo	64Mo	128 Mo
Taille disque	3*8Go	8*36,4Go	3*8Go	3*8Go	72Go	72Go	13Go	8Go		3*8Go
Carte réseau	10/100	10/100	10/100	10/100	10/100	10/100	10/100	10/100	10/100	10/100
Type de sauvegarde	Réseau Sync		Réseau Sync	Bande	Bande HP	Bande HP	Réseau Sync			Réseau Sync
Système D'exploitation	LINUX Red hat 7.0	LINUX Redhat 8.0	LINUX Mandrake 9.2	NOVELL Netware 4.10	W2K advanced Server	W2K advanced Server	LINUX Redhat 8.0	Win NT4 Service Pack 6	LINUX Mandrake 9.2	LINUX Red hat .8.0
Services offerts	Postfix	Postfix Webmail	HTTP index OPAC/DNS ext. Sec	Lp /SMB	Web OPAC	SQL Server	DNS ext. Pri.	Tacacs ++	Ganesha	HTTP, IMAP SMTP, POP
Logiciels utilisés	Roxen	Apache Squiredmail	Apache/Bind9	SAMBA3	IIS/ADLIB	ARIS	Bind 9	Tacacs ++	Ganesha	Apache/Postfix
Lecteur de cd-rom	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Lecteur de disquette	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Type de licence	GPL	GPL	GPL		microsoft	microsoft	GPL	Microsoft	GPL	GPL

Type de serveur	Serveur d'antivirus 1	Serveur d'antivirus 2
Marque	COMPAQ Proliant ML 370	DELL Optiplex
Processeur	Processeurs Intel XEON DP 3,4 GHz	PIII 500MHz
Taille RAM	1Go	128Mo
Taille disque	36,4Go	13Go
Carte réseau	10/100	10/100
Système d'exploitation	W2K server	W2K server
Services offerts	Antivirus Workgroup	Antivirus Workgroup
Logiciels utilisés	Vexira antivirus	Vexira antivirus
Lecteur de cd-rom	Oui	Oui

b) les routeurs et les commutateurs(switch)

➢ **les commutateurs (switchs)**

Ce sont les pièces maîtresses du réseau local de l'université. Du fait de leurs importantes fonctionnalités, elles sont la garantie du bon fonctionnement du réseau. On dénombre actuellement au sein de ce réseau une trentaine de commutateurs repartis dans les différentes Unités de Formation et de Recherche. Les principaux types de commutateurs fonctionnels à cette date sont :

- le switch catalyst 3550 series qui constitue avec le 3508 les commutateurs principaux du BACKBONE;
- les switchs catalyst 3524 qui constituent dans chaque UFR des commutateurs principaux;
- les switchs catalyst 2950 qui secondent les 3524 en cas de nécessité (nombre important d'utilisateurs ou de groupes de travail) dans les UFR et raccordent les serveurs au sein de la DPNTIC;
- les switchs catalyst 1900 qui assurent les connexions internes dans les UFR tout en secondant les 3524 en cas de besoins;

✓ **Caractéristiques du commutateur 3550 series de la gamme catalyst 3550**

En matière de performance, les commutateurs 3550 sont des Commutateurs Ethernet intelligents à configuration fixe en configuration 10/100 empilable avec une alimentation en ligne ou Ethernet Gigabit. Le contrôle du réseau et l'optimisation de la bande passante se font par qualité de service (QoS), limitation fine du débit, liste de contrôle d'accès (ACL) et services multicast. La sécurité du réseau est assurée par l'intermédiaire d'un grand nombre de méthodes d'authentification, de technologies de cryptage de données et de fonction de contrôle d'accès en fonction des utilisateurs, des ports et des adresses MAC. Aussi, l'évolutivité des réseaux est assurée par des protocoles de routages évolués tels que EIGRP, OSPF, BGP et exige l'image logicielle EMI (Enhanced Multiplayer Software Image). Enfin l'adaptabilité intelligente grâce aux services IBNS (Cisco Identity Based Networking Services) qui garantissent une plus grande souplesse et une meilleure mobilité aux utilisateurs en fonction de leurs groupes.

En matière de configuration, le commutateur 3550 series supporte le routage de niveau 3. Il a la capacité à négocier la vitesse et le mode de transmission full duplex sur les ports 10/100/1000 Ethernet ; il permet également de rechercher des erreurs dans la trame reçue en utilisant la commutation « store and forward ». Il supporte plus de 12000 @MAC.

Il possède comme matériel :

- 10 slots GBIC Gigabit Ethernet ;
- 02 ports 10 BaseT/100 baseTX/1000BaseT ;
- il supporte les modules GBIC 1000 Base SX ; 1000 Base SX ; 1000 base LX/LH ; 1000 Base ZX.

✓ **Caractéristiques des commutateurs 3508 et 3524 de la gamme catalyst 3500 XL**

Les commutateurs 3524 et 3508 autonégocient la vitesse et le mode de transmission full duplex sur leurs ports 10/100 Ethernet et leurs slots GBIC. Le commutateur 3524 supporte plus de 250 réseaux virtuels par port, et près de 8192 @MAC par CGMP (Cisco Group Management Protocol). Il utilise également l'ISL, la norme 802.1q et le VVID (Voice VLAN ID). On peut aussi avoir des connexions entre switchs et serveurs en haute vitesse, en Etherchannel (création de liaison haut débit virtuelle à partir d'au moins deux liaisons physiques).

Le commutateur 3524 a comme capacité matérielle 24 ports Ethernet 10/100 et 02 slots GBIC avec alimentation en ligne et le commutateur 3508 possède 08 slots GBIC et 02 ports 10/100 Ethernet. Le commutateur 3508 supporte les modules GBIC Cisco suivant : le Gigastack GBIC, les

modules GBIC 1000 Base SX, 1000 base LX/LH, 1000 Base ZX. L'administration du commutateur peut se faire avec CISCO IOS CLI (Command Line Interface) à travers le port console ou par Telnet. On peut aussi procéder à l'installation des logiciels d'applications CISCO VIEW et Cluster Management Suite permettent le suivi d'un ensemble de commutateurs indiqués à travers l'adresse IP. Enfin les commutateurs 3508 et 3524 peuvent supporter jusqu'à 09 commutateurs empilables avec le convertisseur GBIC Gigastack.

✓ **Caractéristiques du commutateur Catalyst 2950**

Il s'agit d'un commutateur à 24/12 ports Ethernet 10/100 avec des options variées de liaisons ascendantes 100 base Fx, 100 base T fixes, 1000 Base SX fixes et GBIC. Les modèles avec image logicielle évoluée (EI) offrent des services intelligents de niveau 2 à 4 comme la qualité de service (QoS) évoluée, la limitation du débit, le filtrage de sécurité et des possibilités d'administration multicast. D'autres avec image logicielle standard (SI) offrent une fonctionnalité Cisco IOS de niveau 2 pour des services de données, voix et vidéo de base à la périphérie du réseau. On peut avoir également jusqu'à 9 commutateurs empilables avec le convertisseur GBIC Gigastack.

L'administration réseau est simplifiée grâce à Cisco CMS (Cluster Management Suite) pour 16 commutateurs Catalyst à configuration fixe.

✓ **Caractéristiques techniques des commutateurs de la gamme 1900 series (voir en annexe)**

➢ **Les routeurs**

Ils permettent l'accès ou la connexion au WAN ou à Internet, et l'accès par RTC au réseau de l'université. Les routeurs sont au nombre de quatre (04) : 02 pour le réseau local de l'université et deux (02) pour le réseau du VSAT (en essai). Nous noterons ici que le réseau VSAT est un réseau indépendant de celui de l'université, qui est en essai pour une implémentation future dans le réseau. Les deux (02) routeurs fonctionnels au sein du réseau sont :

- le routeur CISCO 1721 ;
- le routeur CISCO 2509 series (serveur d'accès) ;

✓ **Caractéristique du routeur 1700**

Il comporte un port de réseau LAN Fast Ethernet 10/100 à détection automatique et aussi des emplacements modulaires supportant un large éventail de cartes réseau WAN. Ils supportent aussi l'accès sécurisé Internet et Intranet ainsi que de nouvelles applications WAN, notamment les VPN, l'intégration de voix, les données (VoIP) et les services haut débit. Il intègre en son sein une fonctionnalité VLAN.

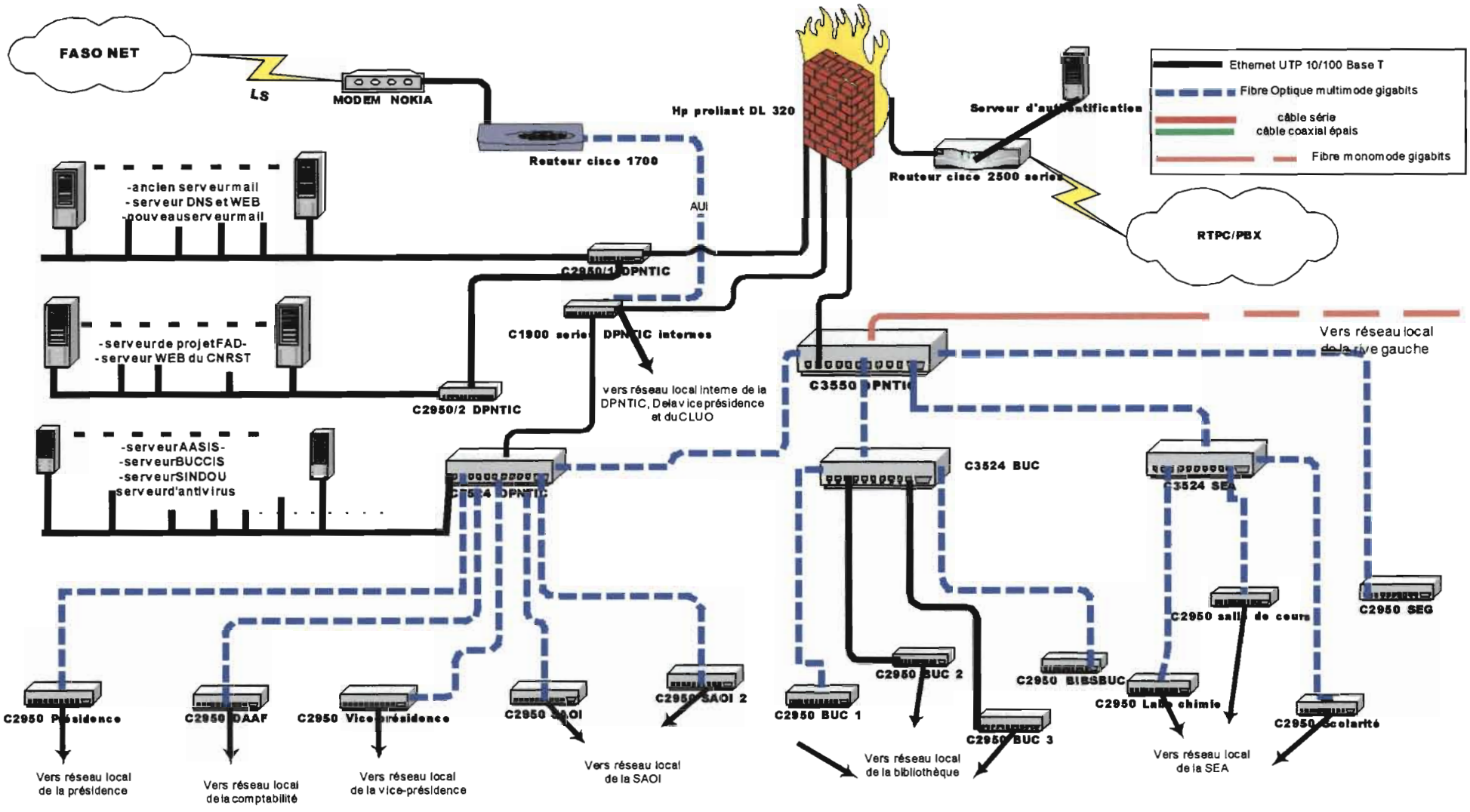
✓ **Caractéristiques des routeurs de la gamme cisco 2500 series (voir en annexe)**

✓ **Caractéristique des routeurs de la gamme Cisco 2600 series**

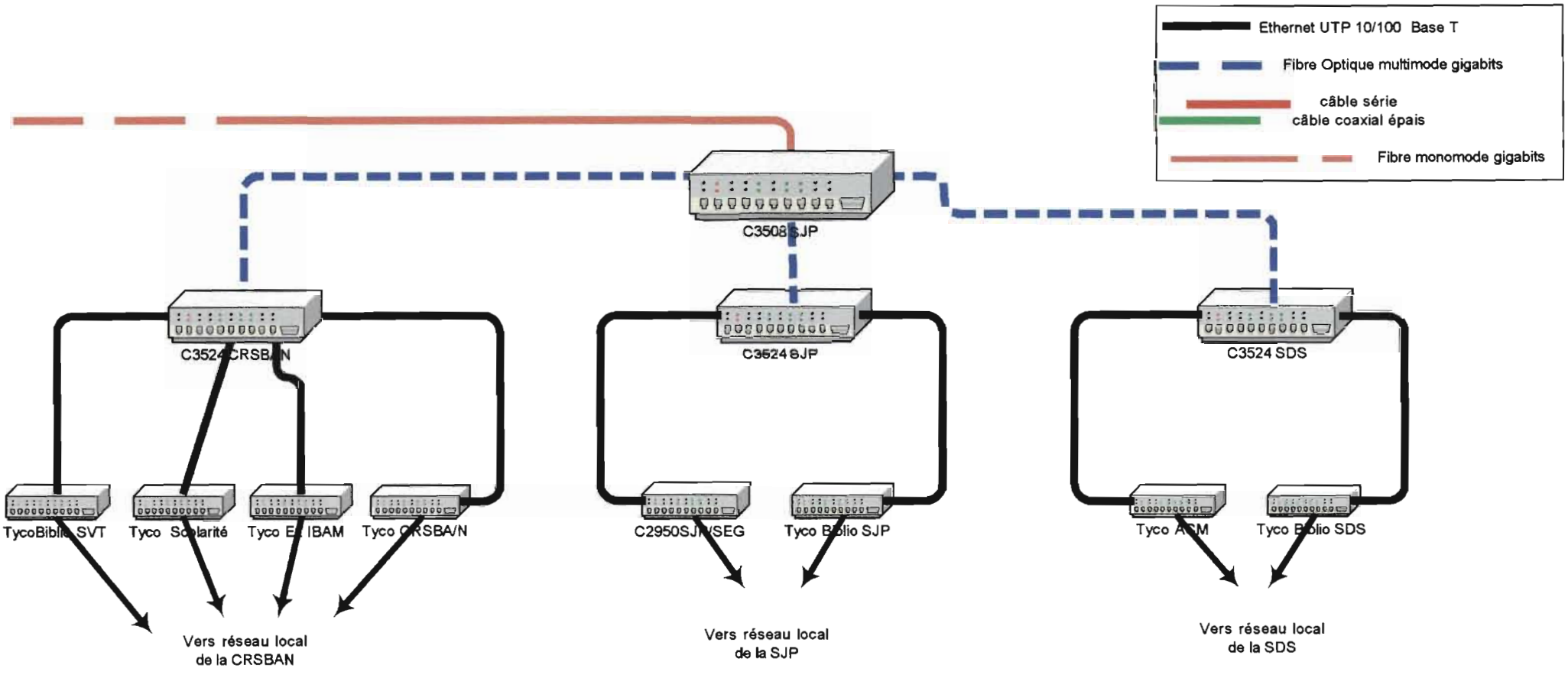
Elles peuvent supporter un LAN simple ou double (options Ethernet 10/100 Mbits/s et Token Ring/Ethernet). Ils supportent un large éventail d'interfaces, notamment la commutation 16 ports intégrés hautes densités analogique et numérique, voix pare-feu Cisco IOS et VPN, série synchrone et Asynchrone, RNIS, T1/E1 fractionnée et « chanellisée », Ethernet, modems analogiques, ADSL, G.SHDSL, intégration de commutation et ATM. Ils partagent également les mêmes cartes d'interfaces WIC et les mêmes modules de réseau que les gammes Cisco 1700,3600 et 3700 ; ils existent en versions AC et DC et redondantes en options.

c) Le firewall HP Proliant DL 320

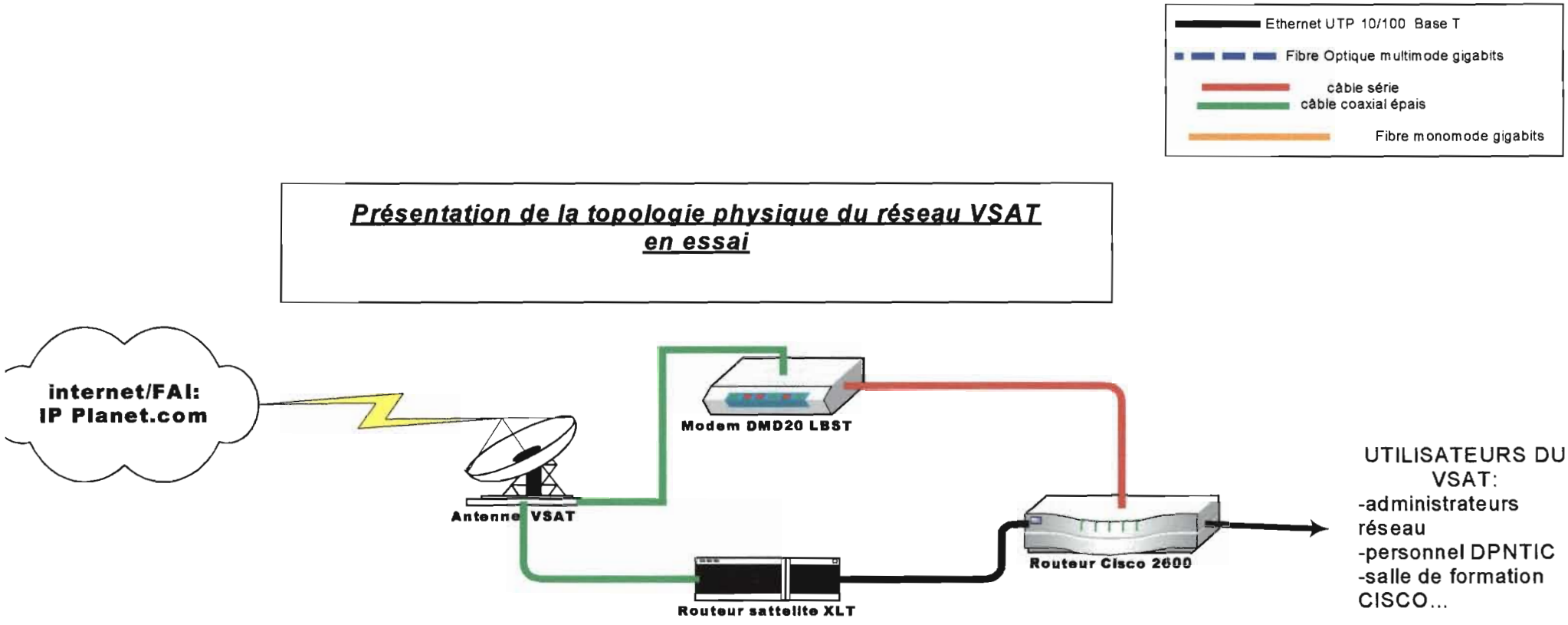
Il constitue l'essentiel de la sécurité du réseau de l'université contre les attaques extérieures. Le firewall ou pare feu, placé à l'entrée du réseau, constitue ainsi un unique point d'accès par où



Présentation de la topologie physique du réseau local actuelle de l'université/ coté rive GAUCHE/ zone DPNTIC



Présentation de la topologie physique du réseau local actuel de l'université/ coté rive DROITE/ zone SJP


Ethernet UTP 10/100 Base T
Fibre Optique multimode gigabits
câble série
câble coaxial épais
Fibre monomode gigabits
Présentation de la topologie physique du réseau VSAT en essai
internet/FAI:
IP Planet.com
Modem DMD20 LBST
Antenne VSAT
Routeur satellite XLT
Routeur Cisco 2600
UTILISATEURS DU VSAT:
-administrateurs réseau
-personnel DPNTIC
-salle de formation CISCO...

toutes les requêtes venant de l'extérieur doivent passer. Sans omettre que 80% des attaques proviennent de l'intérieur du réseau, il constituera par la suite dans notre futur réseau un point unique par lequel toute requête circulant à l'intérieur du réseau local devra transiter.

Caractéristiques du pare feu (firewall) HP proliant DL 320

Le pare-feu HP Proliant DL320 est un serveur monoprocesseur économique. C'est une nouvelle génération des serveurs Proliant DL320 qui supporte désormais le processeur Intel Pentium 4 et 512Ko de mémoire cache et peut accueillir au maximum 4 Go de mémoire DDR à 266 MHz. Le DL 320 G2 dispose également de plusieurs fonctionnalités perfectionnées visant à l'amélioration de la souplesse d'emploi : un connecteur d'extension PCI, une mémoire ROM redondante et les fonctionnalités de surveillance améliorées tels que RILOE II, Smart Start et Insight Hewlett Packard. Sa capacité à centraliser les échanges de données nous est offerte pour notre mise en œuvre (voir documentation en annexe). D'un point de vue logiciel, le HP 320 nous procure un logiciel puissant : check point Secure Platform utilisant un système d'exploitation Windows 2000 et configurable graphiquement ou en ligne de commande.

5) Présentation de la topologie physique du réseau actuel de l'université de Ouagadougou

La topologie physique actuelle de l'université de Ouagadougou se présente comme le schéma l'indique à la page suivante :

6) Critique de l'existant

Une analyse de l'infrastructure réseau de l'Université de Ouagadougou, des différents équipements rencontrés, et de la politique d'organisation et de gestion, nous a permis de relever des points positifs, mais aussi des imperfections.

a) Points positifs

✓ **l'architecture réseau**

On remarque une bonne élaboration de l'architecture du réseau, à travers l'organisation autour d'une épine dorsale. Chaque bâtiment principal constitue un nœud auquel sont raccordé les bâtiments secondaires et les salles s'y rattachant. Ces nœuds principaux sont à leur tour reliés au backbone.

✓ **les équipements d'interconnexion**

Les équipements d'interconnexion (switchs, hubs, routeurs...) sont de bonne qualité et permettent la réalisation de l'organisation logique à laquelle nous aspirons à savoir la mise en œuvre de réseaux locaux virtuels. En majorité de provenance Cisco (Routeur Cisco 1700, routeur Cisco 2621, switch Cisco 3500, switch 2900) ces équipements sont fournis avec leurs IOS et sont couverts par une garantie. De plus ces équipements connaissent une sécurité tant au niveau physique qu'électrique. Ils sont installés dans des armoires sécurisées et protégés par des onduleurs.

✓ **le câblage**

Deux types de câble permettent de réaliser les différentes liaisons. La fibre optique (multimode et monomode) permet de connecter les secteurs et les zones avec tous les avantages qu'elle offre en matière de bande passante ou de sécurité. Quant à la paire torsadée, elle correspond aux meilleures spécifications (catégorie 5, EIA/TIA 568-A-5) et est utilisée pour les LANs des bâtiments au sein des zones ou des secteurs.

✓ **la surveillance réseau**

Le logiciel de surveillance réseau, what's up permet d'observer à partir d'une console centrale les différents équipements, et d'avoir une vue globale sur l'état du réseau. Les incidents sont signalés avec suffisamment de précision, ce qui permet d'intervenir rapidement et efficacement.

b) Les imperfections

✓ **le manque de documentation complète**

Au titre des imperfections, nous avons constaté un manque de documentation complète relative au réseau. En effet les différentes interventions et modifications effectuées sur le réseau ne font pas toujours l'objet de nouvelles schématisations. En outre, les schémas existants sont pour la plupart de brefs aperçus montrant seulement l'interconnexion de quelques éléments majeurs.

✓ **l'instabilité du réseau**

Le réseau connaît une situation d'instabilité qui fait qu'aucun schéma n'est assez complet à un instant donné pour le décrire. A vrai dire, certaines procédures d'installation de nouveaux équipements sont faites à l'insu de la DPNTIC.

Cette instabilité s'accroît avec les coupures d'électricité qui surviennent souvent et entraînent le dysfonctionnement de certains équipements.

✓ **l'absence de tâches de maintenance préventive**

De la poussière s'encrasse sur les équipements, faute d'un plan de maintenance préventive (nettoyage) bien établi. Ces dépôts de poussière peuvent être à la base de pannes qui affecteraient le réseau et entraîneraient des coûts de dépannage plus élevés.

7) Les plans déjà conçus

Dans l'optique de résoudre les problèmes de manque d'adresses IP publique, de sécurisation

du réseau Uonet et d'utilisation de la bande passante, un plan a déjà été formulé mais pas intégralement mis en œuvre. Ce plan projetaient l'organisation de Uonet en trois (03) LAN Virtuels qui pourront communiquer à travers des règles judicieusement élaborées dont la communication inter VLAN qui est implémentée au travers du firewall (voir figure).
Ces trois VLANs sont :

- La **formation** qui regroupe :
  - Les salles de formation, de consultation et de libre accès ;
  - Les serveurs destinés à la formation (fichiers, messagerie, autoformation…) ;
  - Les serveurs spécifiques (DNS interne, DHCP, serveur d'installation/update) ;
  - Les périphériques destinés à la formation (Imprimantes, Chargeur de CD-ROM, …) ;
  - Les bâtiments connectés à Uonet avec des équipements ne supportant pas les VLANs
- Le **staff** qui regroupe :
  - Les serveurs destinés à l'administration de l'université (BUCIS, AASIS, SINDOU, SERVEUR D'IMPRESSION, et d'autres systèmes comme la comptabilité, les ressources humaines, les services Web internes, etc)
  - La messagerie du staff ;
  - Les postes de travail du staff
- Le **monitoring** regroupe les équipements destinés :
  - A la connectivité (switchs) ;
  - A la gestion, à la surveillance et à la maintenance d'Uonet (consoles et station d'administration).

Pour parvenir à la mise en œuvre de ces VLANs des plans pour les adresses IP et pour le Firewall ont été élaborés. Ces différents plans sont résumés à travers les tableaux ci-après :

Tableau des adresses IP :

Zone		Plage d'adresses	Masque	Equipements concernés
DMZ		212.52.131.0	255.255.255.0	Relais Mail, DNS externe, UO Web, Web CNRST
VLAN STAFF	Statique	172.16.0.1 – 172.16.15.255	255.255.240.0	BUCIS, AASIS, Backup, DHCP1, Mail Staff
	Dynamique	172.16.16.0 – 172.16.31.254	255.255.240.0	Postes utilisateur
VLAN FORMATION	Statique	172.16.32.1 – 172.16.32.255	255.255.240.0	DNS interne, DHCP2,
	Dynamique	172.16.33.0 – 172.16.47.254	255.255.240.0	Postes utilisateur
VLAN MONITORING		192.168.3.0	255.255.255.0	Switch Cisco
Firewall-1700		192.168.4.4	255.255.255.252	Serveur COMPAQ proliant
RAS		192.168.5.0	255.255.255.240	Cisco 2509 TACACS
1700-2514		192.168.4.8	255.255.255.252	Routeur IOS sécurisé

Tableau des serveurs par segment

Segment	Serveurs (hostname)	Services	Logiciels	OS
DMZ	Serveur Web UO (www) (Web_DMZ)	http, index sur OPAC	Apache	Linux
		DNS externe secondaire	Bind 9	
	Serveur mail relay (Mail_dns_dmz)	SMTP relay	Postfix 2002	Linux
		DNS externe primaire	Bind 9	
		Anti-Virus passerelle pour SMTP	Trend Micro InterScan VirusWall	Linux
	Serveur Web CNRST	http, IMAP, SMTP, POP	Apache, Postfix	Linux
	Anti-Virus Passerelle Serveur Cache	VirusScan http, FTP	Trend Micro InterScan VirusWall	W2K
		Proxy transparent	Squid	
VLAN FORMATION	Serveur mail étudiant	DNS Interne Dynamique	Bind 9, Smb 3	W2K/Linux
		DHCP1	DHCPd	
		SMTP, POP,IMAP	Postfix	
		http	Apache, SquirelMail	
		FTP	ProFTPd	
		Smb	Samba 3	
	Serveur d'installation	Anti-Virus Workgroup	Vexira	W2K
		Msis, Msus	Microsoft Installation Server, Microsoft Update Server	
	DNS Secondaire	DNS Interne secondaire	Bind 9	Linux
	NAS (Option)	Stockage de masse en réseau	Network Area Storage	
VLAN STAFF	Serveur Mail	DHCP2	DHCPd	Linux
		SMTP, POP, IMAP	Postfix	
		http	Apache, SquirelMail	
		FTP	ProFTPd	

		Smb	Samba 3	
	Serveur BUCIS	http, SQLServeur	IIS, ADLIB	W2K
	Serveur AASIS	SQLServeur	Aris	W2K
	Serveur de Backup	http, SQLServeur	ADLIB, Aris	W2K
	Serveur de Spool d'impression et de fichiers (Sindou)	Lp, Smb	Samba 3	Linux
VLAN MONOTORING	Console de gestion	SNMP, ICMP	What'sUp, FW smartconsole	WXP
	Concentrateur VPN	Cisco VPN Software	VPN Soft	IOS
RAS	Serveur RAS	Tacacs++	Tacacs++	NT

Suite du tableau des serveurs par segment

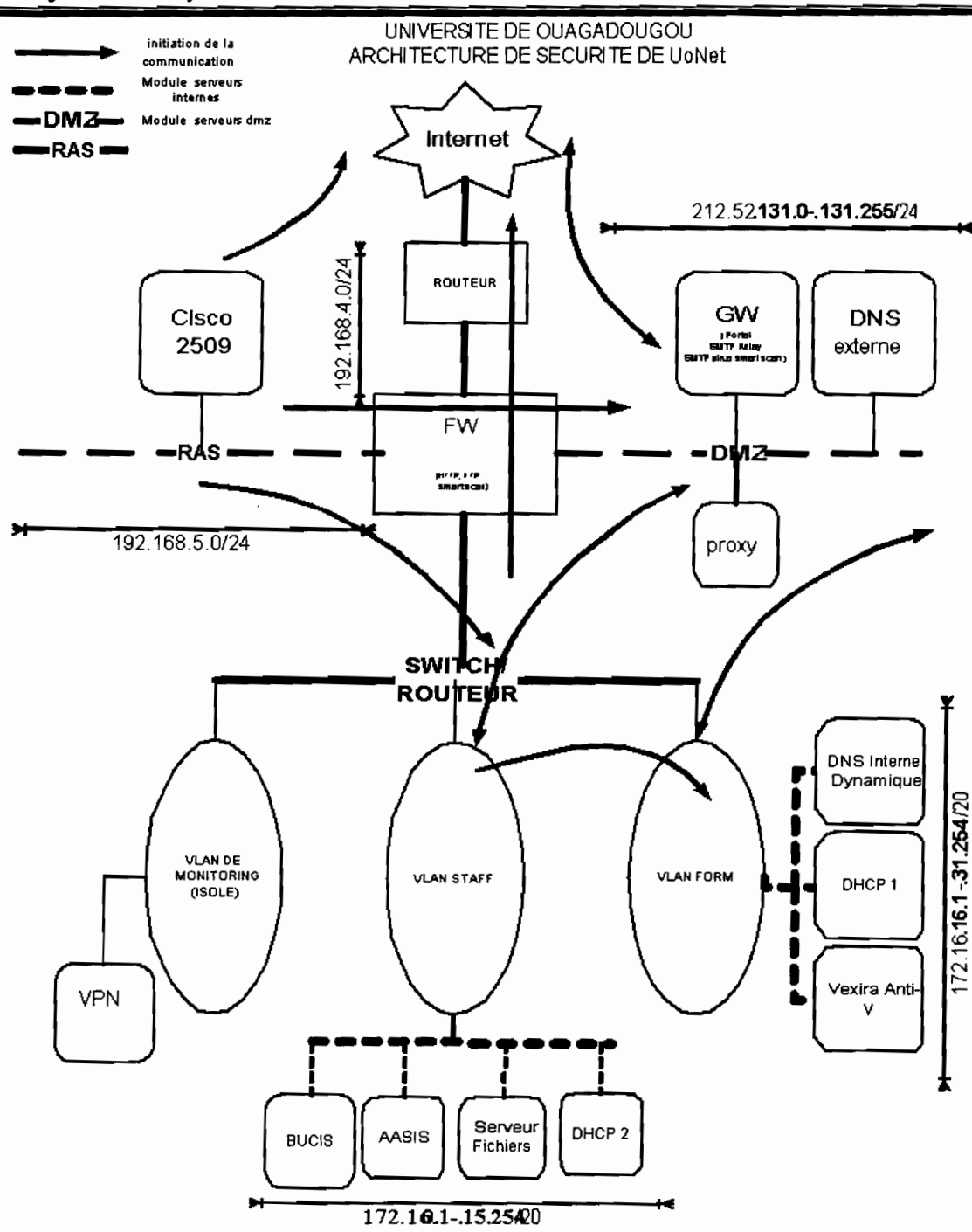
La politique de filtrage conçue est ainsi qu'il suit :

- Tout le trafic inter segment doit passer par le Firewall. Ainsi le routage inter VLANs et le routage avec l'extérieur doivent se faire à son niveau.
- Le Firewall n'autorisera que les services offerts dans chaque segment selon leur impact sur la bande passante et la sécurité des applications critiques de l'Université de Ouagadougou.

Sans être exhaustif, cette politique devrait permettre :

1. l'accès aux serveurs de la DMZ à partir d'Internet ;
2. l'accès des serveurs de la DMZ à Internet ;
3. l'accès au Web interne à travers un portal situé dans la DMZ ;
4. l'accès au réseau interne Uonet à partir d'Internet est interdit, sauf les réponses attendues par les requêtes initiées depuis l'intérieur ;
5. toutes les stations de travail dans les VLANs FORM et ADMIN doivent pouvoir initier des requêtes vers Internet ;
6. Le VLAN MONITORING est isolé ;
7. l'accès à la messagerie à travers un relais situé dans la DMZ.

Cette politique est décrite à travers la figure suivante et les tableaux de flux et d'autorisations du pare-feu sur les pages suivantes :


UNIVERSITE DE OUAGADOUGOU
ARCHITECTURE DE SECURITE DE UoNet
initiation de la communication
Module serveurs internes
DMZ
Module serveurs dmz
RAS
Internet
212.52131.0-.131.255/24
ROUTEUR
192.168.4.0/24
Cisco 2509
GW
DNS externe
FW
RAS
DMZ
192.168.5.0/24
proxy
SWITCH ROUTEUR
VLAN DE MONITORING (ISOLE)
VLAN STAFF
VLAN FORM
DNS Interne Dynamique
DHCP 1
Vexira Anti-V
172.16.16.1-.31.254/20
VPN
BUCIS
AASIS
Serveur Fichiers
DHCP 2
172.16.0.1-.15.254/20

Le tableau des flux

NB : Les cases vides ne comportent aucune règle

→	EXT	RAS	DMZ	MON	FORM	STAFF
EXT			http, Dns, Smtp		http, Dns	http, Dns
RAS	http, Dns, Ldap, Pop, Imap, Https, Ssh,		Dns, Http		Http, Dns, Webmail	Http, Dns, Webmail
DMZ	Smtp, Dns				Smtp	Smtp
MON						
FORM	Http, Dns, Ldap, Pop, Imap, Msn, Https, Ssh		Http, Dns, Smtp, Ssh			
STAFF	Http, Dns, Ldap, Pop, Imap, Https, Ssh				Http (Msi, Msus), Dns	

Tableaux des autorisations et restrictions du pare feu

N°	*Réseau/adresse Source*	*Port/ Service*	*Réseau/adresse Destination*	*Port/ Service*	*Type*	*Action*
1	Mail_DNS_DMZ		Excepter(VLAN_form VLAN_staff, RAS, VLAN mon	DNS		Accepter
2	Mail_DNS_DMZ		Excepter (RAS, VLAN_mon)	SMTP		Accepter
3	Excepter (VLAN_mon)		Web_DMZ Web_Cnrst	HTTP		Accepter
4	Excepter (RAS, VLAN_mon)		Mail_DNS_DMZ	SMTP, DNS		Accepter
5	VLAN_form VLAN_staff		DMZ	SSH		Accepter
6	Mail_DNS_form Mail_DNS_staff		Mail_DNS_DMZ	SMTP		Accepter
7	VLAN_form VLAN_staff		Excepter(DMZ, VLAN_staff, VLAN_mon, RAS)	POP, IMAP, HTTP HTTPs, FTP, DNS, SSH, vexira.		Accepter
8	Excepter (DMZ, VLAN_mon)		Mail_DNS_form Mail_DNS_Staff	HTTP, DNS.		Accepter
9	RAS		Excepter (DMZ, VLAN_staff, RAS, VLAN_mon)	POP, IMAP, HTTPs, HTTP, FTP, DNS, SSH, Vexira.		Accepter

10	Tout	Tout	Tout	Tout	Tout	Rejeter

Les perspectives envisagées sont :

- ✓ La nécessité d'avoir accès au Vlan monitoring à partir d'Internet ou des VLANs ouverts (cet accès se fera de manière sécurisée à travers le réseau VPN-Uonet réservé à la console de gestion du réseau sécurisé et bien patché.
- ✓ La possibilité d'extension des VLANs staff et formation grâce à la solution VPN (office connecte) à d'autres réseaux liés à Uonet par l'accès distant ou par Internet.

La représentation organisationnelle du plan déjà conçu est donnée à la page suivante :

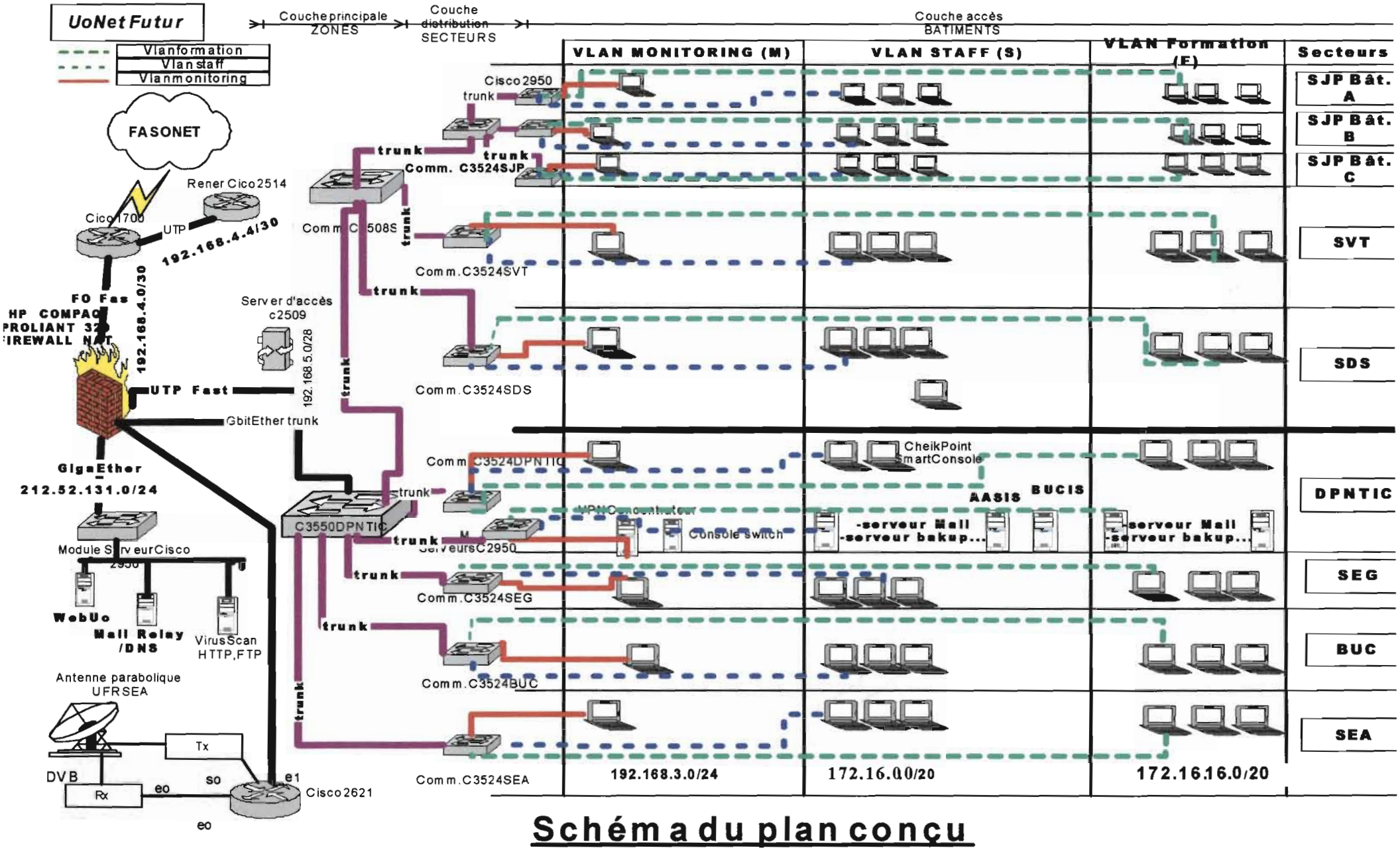


Schéma du plan conçu

A ce stade nous noterons que seul la mise en mode VTP (Virtual Trunk Protocol) de tous les commutateurs a été effectuée. Cependant bien que ce plan déjà conçu soit bien élaboré nous pensons qu'au vue de certains aspects liés à la disponibilité des ressources et des services, certaines modifications doivent être apportées. Il conviendra donc pour nous d'examiner des solutions et d'en adopter une qui répondra au mieux à ces besoins.

III) Proposition de plan de réalisation

Le plan d'organisation en trois VLANs prévu dans le plan de sécurisation déjà conçu tient compte des différents besoins des utilisateurs en terme de regroupement logique d'exploitation des ressources et d'utilisation des services. Cependant, afin de réduire les délais d'intervention et de fournir ainsi une grande disponibilité des données aux utilisateurs, nous pensons que l'ajout d'un service de maintenance logicielle est nécessaire. Ce service assurera la maintenance logicielle et préventive à distance du réseau local de l'université Ouagadougou. En effet, le réseau de l'université de Ouagadougou s'étalant sur un vaste domaine géographique, les délais d'intervention en cas de pannes sont souvent très longs. La mise en place d'un Vlan MAINTENANCE ou la disponibilité d'un serveur et d'un ensemble de poste de maintenance logicielle dans le VLAN_STAFF sont deux solutions pouvant pallier à ces problèmes. Il sera de plus offert la possibilité d'effectuer le contrôle de flux et de la bande passante du réseau de manière optionnelle. Cet apport servira en premier lieu à assurer :

- ✓ **La sécurité et la disponibilité permanente des outils et des données**. Des solutions de protection contre les pannes de courant, les défaillances matérielles, les intrusions, les attaques virales doivent être mis en service pour répondre à ces objectifs de disponibilité.
- ✓ **La pérennité des données** : cette pérennité sera assurée par la mise en service des solutions de sauvegarde et par la définition de procédures de restauration en cas de problèmes.

Ce service de maintenance regroupera des serveurs d'antivirus et fournira les outils tels les logiciels de prises de contrôle à distance des équipements, des logiciels de maintenance adéquats. De plus le rapport prix/qualité de ces logiciels reste très convaincant pour une utilisation dans un vaste réseau.

L'ajout de ce nouveau service logiciel de maintenance nous conduira, selon les différentes solutions à :

- ➢ une nouvelle organisation du plan d'adressage;
- ➢ un réaménagement du plan d'organisation des serveurs par segments ;
- ➢ la définition de flux supplémentaires ;
- ➢ l'ajout de nouvelles règles de filtrage.

A) Première solution : Création d'un VLAN de maintenance

La création d'un VLAN supplémentaire est une solution que nous pouvons envisager dans l'optique de l'accomplissement de nos objectifs.

1) détermination des VLANs

L'une des clés de la sécurité informatique réside dans le regroupement des utilisateurs sur des réseaux logiquement ou physiquement distincts selon les autorisations et les droits qu'ils ont dans le réseau. Afin de mettre en place une politique de sécurité répondant le mieux possible en terme d'usage et aux impératifs de sécurité dont a besoin l'université de Ouagadougou, il est nécessaire de distinguer différents domaines correspondant aux types d'utilisateurs et aux types d'usages du réseau. Dans les établissements d'enseignement et dans les universités, on distingue généralement :

- **les types d'utilisateurs suivants :**
  - ✓ les étudiants ou les élèves ;
  - ✓ la communauté pédagogique (les enseignants) ;
  - ✓ la communauté administrative (le personnel d'encadrement, les gestionnaires…) ;
  - ✓ le plus souvent la communauté externe (les parents d'élèves, d'étudiants..) ;
- **et les usages suivants :**
  - ✓ pour les activités d'enseignement ;
  - ✓ pour la vie scolaire ;
  - ✓ pour les usages de gestion administrative.

Dans le cas de notre étude, nous pourrons ainsi distinguer 02 éléments fondamentaux qui régissent le caractère structurel et fonctionnel de l'université de Ouagadougou :

- **la pédagogie** qui regroupe les étudiants ;
- **l'administration et l'enseignement** qui regroupe les enseignants-chercheurs et le personnel administratif de l'université.

Les communications entre ces réseaux seront régies par des règles implémentées sur le firewall et sur les switchs. Ainsi la politique de filtrage sera principalement défini de telle sorte que les étudiants ne puissent pas accéder au réseau de l'administration. Aussi, pour la communication vers l'extérieur, implémentera-t-on également la translation d'adresse par port sur le Firewall (NAPT Network Address Port Translation).

Comme le plan que nous proposons le montre, le réseau de l'université va regrouper en son sein quatre (04) réseaux locaux virtuels qui pourront communiquer ou pas selon des règles judicieusement élaborées. Ce sont :

- **le réseau virtuel formation** : qui regroupera en son sein
  - ✓ les salles de formations, de consultation ou de libre accès ;
  - ✓ les serveurs destinés à la formation (fichier, messagerie et autoformation) ;
  - ✓ les serveurs spécifiques (DNS interne, DHCP, serveur d'installation/update) ;
  - ✓ les périphériques destinés à la formation (imprimante, chargeur de CDROM, etc.…)
  - ✓ les bâtiments connectés au réseau avec des équipements ne supportant pas les réseaux virtuels.
- **Le réseau virtuel administration (staff)** : qui regroupera :

Des serveurs destinés à l'administration de l'université :

- BUCIS ;
- AASIS ;
- Serveur SINDOU ;
- Serveur d'impression ;
- Et d'autres applications comme la comptabilité, les services de ressources humaines, les services Web internes, la messagerie de l'administration et les postes de travail.

- **Le réseau virtuel du monitoring** : qui regroupera les équipements destinés :
  - ✓ A la connectivité (des commutateurs, des routeurs et des concentrateurs) ;
  - ✓ A la gestion, à la surveillance du réseau (consoles et station d'administration) ;
- **Le réseau virtuel maintenance** qui regroupera les équipements destinés à :
  - ✓ L'intervention de manière logicielle et préventive sur tous les postes utilisateurs du réseau local de l'université de Ouagadougou.
  - ✓ Au redémarrage d'un service arrêté sur un des serveurs de la DMZ, du VLAN STAFF ou du VLAN formation à distance;
  - ✓ Au contrôle effectif des échanges du réseau et du bon fonctionnement des machines du réseau.

En plus de ces réseaux locaux virtuels, nous aurons donc une zone démilitarisée (DMZ : Demilitared Zone) déjà existante qui la partie visible du réseau depuis l'extérieur. On y trouve les

sites de l'université et du CNRST, les cours dispensé sur Internet, la messagerie de l'université et le réseau d'accès distant pour les utilisateurs qui de l'extérieur désireraient accéder au réseau local.

2) Choix de la méthode de configuration des VLANs

Associer de façon statique chaque port d'un commutateur à un VLAN est une solution pratique. En effet, la gestion devient facile du moment où l'association du numéro de VLAN au numéro de port est faite par l'administrateur réseau et mieux à partir d'une console centrale. De plus, dans le réseau actuel de l'Université de Ouagadougou, on ne rencontre pas une diversité de protocoles, du moins, du point de vue hétérogénéité ; par ailleurs, il n'est point souhaitable de dégrader les performances actuelles, pouvant faire suite à l'analyse d'information de niveaux supplémentaire dans les trames (cas de VLAN de niveau 2 et niveau 3). Ce même phénomène peut résulter des échanges de tables entre les commutateurs. Mais dans tous les cas, mettre en œuvre ce type de VLANs nécessite des moyens supplémentaires.

Ces raisons nous conduisent ainsi malgré son manque de souplesse à préférer la méthode de configuration des VLANs par ports.

3) Plan d'adressage proposé

Aucun réseau ne peut bien fonctionner sans une attribution et une configuration correcte des différentes adresses réseau. En effet, l'élaboration des règles de communication inter et intra réseau, imposent le respect d'un certain nombre d'éléments (classe d'adresse, définition de sous-réseaux, attribution statique ou dynamique des adresses). C'est ainsi que nous avons mis en œuvre un plan d'adressage répondant à ces différents besoins. Ce plan d'adressage est d'ailleurs basé sur le plan qui existe déjà car il ne faut pas perdre de vue que l'un des avantages de la mise en œuvre de VLANs est qu'ils s'organisent autour de l'infrastructure déjà en place. Les différentes modifications que nous avons introduites sont les suivantes :

- ✓ Assimilation du VLAN Monitoring à la partie UONET CORE déjà existante avec l'adresse réseau 192.168.3.0
- ✓ L'adoption de l'adresse réseau 172.16.0.0 en lieu et place de l'adresse 172.18.0.0 de masque 255.255.240 .0 pour les VLANs Staff et Formation. L'adresse 172.18.0.0 n'étant utilisée pour le moment que pour des raisons de perte de configuration de certains équipements avec l'adresse 172.16.0.0.
- ✓ L'affectation d'un sous réseau à chacun de ces deux VLANs : 172.16.0.0 pour le VLAN Staff et 172.16.16.0 pour le VLAN Formation. A l'intérieur de chaque VLAN se fait l'organisation des adresses en statique ou en dynamique.

Zone		Plage d'adresses	Masque	Equipements concernés
DMZ		212.52.131.0	255.255.255.0	Relais Mail, DNS externe, UO Web, Web CNRST
VLAN STAFF	Statique	172.16.**0.1** – 172.16.**0.254**	255.255.240.0	BUCIS, AASIS, Backup, DHCP1, Mail Staff
	Dynamique	172.16.**1.1** – 172.16.**15.254**	255.255.240.0	Postes utilisateur
VLAN FORMATION	Statique	172.16.**16.1** – 172.16.**16.254**	255.255.240.0	DNS interne, DHCP2,
	Dynamique	172.16.**17.0** – 172.16.**31.254**	255.255.240.0	Postes utilisateur
VLAN MONITORING		192.168.3.0	255.255.255.0	Switch Cisco

VLAN MAINTENANCE	192.168.2.0	255.255.255.0	Postes des techniciens de la DPNTIC.
Firewall	192.168.4.4	255.255.255.252	Serveur compact proliant
RAS	192.168.5.0	255.255.255.240	Cisco 2509 TACACS
1700-2514	192.168.4.8	255.255.255.252	Routeur IOS sécurisé

Commentaires sur le plan d'adressage

La DMZ

La DMZ, zone démilitarisée, est une partie du réseau ouverte et visible de l'extérieur. A cet effet, les équipements de cette zone possèdent une plage d'adresse publique qui est ici l'adresse réseau 212.52.131.0 de classe C, pouvant adresser jusqu'à 254 équipements. Ces équipements sont entre autres, le serveur Web de l'Université, le relais Mail, le DNS externe…

- **Les VLANs**

Un adressage basé sur l'attribution d'adresses de classe C et B est effectué dans le LAN ; pour des requêtes vers Internet, ces adresses sont soumises au mécanisme de translation (NAT) au niveau du firewall. Ainsi, en vertu de la RFC1918 les adresses de classe B sont du type 172.16.0.0 avec le masque 255.255.240 .0 et pour celles de classe C, elles sont du type, 192.168.0.0 avec pour masque, 255.255.255.0.

- **Le VLAN monitoring**

Il concerne les équipements destinés à la connectivité, à la gestion, à la surveillance et la maintenance de Uonet. Une classe d'adresses C de 254 adresses permet de les adresser.

-**Le VLAN Maintenance**

D'un adressage alloué de manière statique, il constituera l'ensemble des postes de la salle des techniciens de la DPNTIC et des administrateurs réseau et aura pour adresse réseau 192.168.2.0. Cet adressage de la classe C et permettra d'adresser 254 adresses IP.

- **Le VLAN staff**

Les 254 adresses de classe B (172.16.0.1 à 172.16.0.254) permettent d'adresser les différents serveurs destinés à l'administration de l'Université. Ces adresses sont allouées de façon statique. Quant à la plage d'adresses de 172.16.1.0 à 172.16.15.254, allouée de façon dynamique, elle servira à adresser les postes utilisateurs de ce groupe.

- **Le VLAN formation**

La plage d'adresse 172.16.16.1 à 172.16.16.254 sert à adresser les serveurs destinés à la formation et d'autres serveurs spécifiques. Les bâtiments connectés au réseau de l'Université ne supportant pas les VLANs, les périphériques et les postes utilisateurs de ce groupe utilisent la plage de 172.16.17.1 à 172.16.31.254 qui leurs sera allouée de façon dynamique.

- **L'accès distant**

Avec l'adresse 192.168.5.0, l'accès distant peut relier jusqu'à 16 sous réseaux de 16 postes chacun.

4) Politique de filtrage et de communication inter segment et inter VLAN

D'un point de vue logiciel, la politique de communication et de filtrage consistera à élaborer des règles judicieuses pour la communication à l'intérieur et à l'extérieur du futur réseau de l'université de Ouagadougou. Aussi plusieurs possibilités nous sont-elles offertes : à titre d'exemple l'introduction d'un routeur peut permettre un meilleur filtrage dans les communications inter-VLAN. Le switch catalyst 3550 offre également une possibilité de filtrage et de routage des données mais son efficacité restera un problème à certaines violations extérieures (fonction absente du pare-feu). Ainsi pour un meilleur rendement de sécurité et de gestion du réseau, il s'avère fort utile de centraliser les échanges des données. En effet, de par sa fonctionnalité, le firewall COMPAQ Proliant

DL 320 nous offre cette possibilité de centraliser ce trafic. En d'autres termes tout le trafic inter segment et inter VLAN, de l'intérieur vers l'extérieur et vice versa doit passer par le firewall. Il n'autorisera que les services offerts dans chaque segment selon leur impact sur la bande passante et la sécurité des applications critiques de l'université de Ouagadougou.

La première des choses serait donc de choisir la politique de filtrage. Nous avons donc le choix entre :

- Tout est interdit sauf ce qui est autorisé ;
- Tout est autorisé sauf ce qui est interdit ;

Il est souvent conseillé aux sites ou aux réseaux locaux ayant un nombre considérable d'utilisateurs qui ont acquis une longue pratique des réseaux ouverts de choisir la deuxième solution et de faire ensuite évoluer petit à petit évoluer les filtres pour tendre vers la première solution. Cette méthodologie n'est pas satisfaisante du fait que les filtres n'évoluent pas suffisamment vite, de la nécessité de mise à niveau constante des filtres pour la protection des nouveaux services émergeants....

La première solution ayant la capacité d'être élaborée et installée directement même lorsque les utilisateurs ont acquis une longue pratique des réseaux ouverts sera la solution à notre présent problème. Elle doit cependant être installée avec une certaine méthodologie en impliquant et en informant les utilisateurs. Nous avons par ailleurs le choix entre un filtrage dynamique et un filtrage statique. Le filtrage dynamique sera notre seconde option pour la politique de filtrage qui offre plus d'avantages du simple fait par exemple qu'elle reprend le principe du filtrage statique. Il s'agira ensuite de définir des contrôles d'accès, de routage des données inter VLAN...

Pour la communication inter VLAN, nous définirons des règles de filtrage de sorte à ce que certaines règles qui régissent le fonctionnement interne de l'université ne soient pas violées. Pour cela une redéfinition des chartes d'usage de l'utilisation des informations est nécessaire. Les utilisateurs du VLAN ADMINISTRATION pourraient par exemple accéder au réseau virtuel FORMATION pour certains besoins tels que la dispense des cours et non le contraire. Ou encore permettre aux utilisateurs de tous les réseaux virtuels d'accéder au service Web interne ou à Internet et empêcher les utilisateurs du VLAN FORMATION d'accéder aux serveurs réservés à l'administration. Et enfin permettre aux techniciens du Vlan MAINTENANCE d'accéder aux autres réseaux virtuels (sauf le VLAN MONITORING) si besoin y est. A travers donc une autre configuration du firewall et des switchs du réseau, nous implémenterons cela.

La segmentation du réseau de l'université, l'interconnexion des réseaux administratifs et pédagogiques au sein de l'université de Ouagadougou et son ouverture vers l'extérieur doivent respecter un niveau de sécurité dont le rôle est de définir de manière générale :

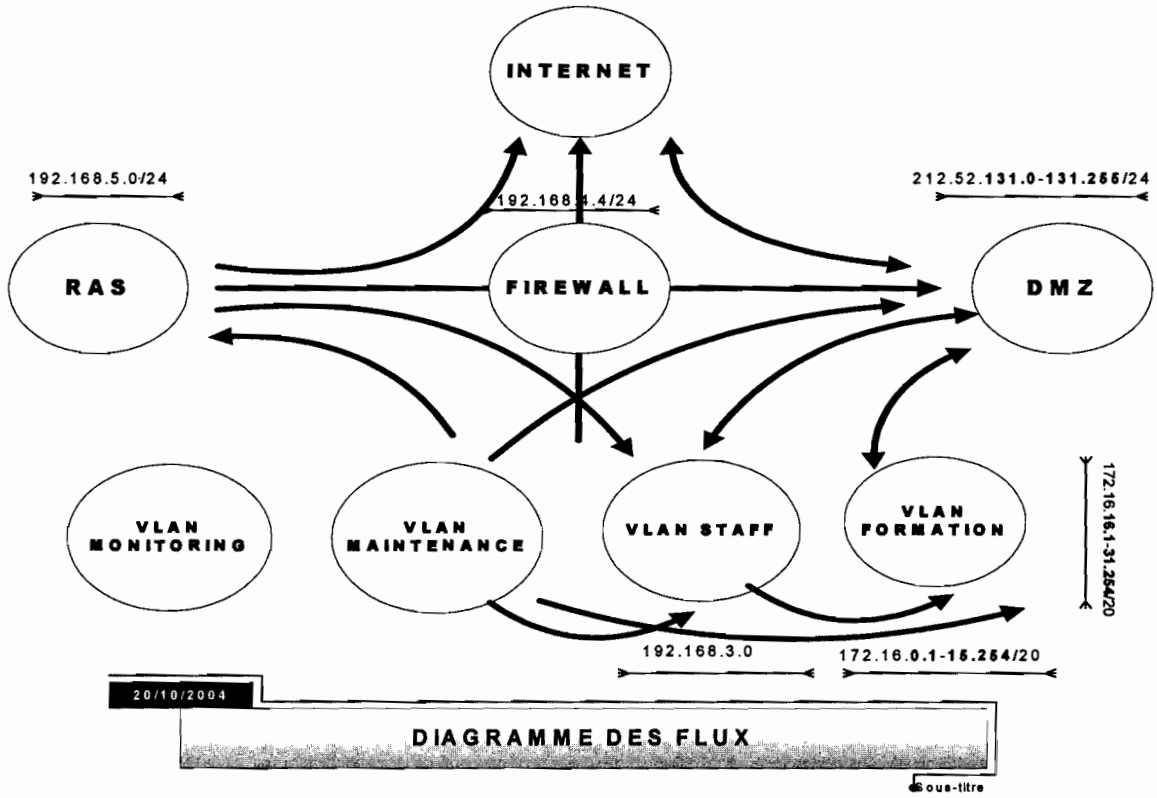
- Les règles d'accès entre les réseaux internes à l'université ;
- Le filtrage d'accès aux ressources ;
- Le contrôle par authentification ;
- La « journalisation » des accès...

De manière concrète elle devrait permettre entre autre :

- L'accès aux serveurs de la DMZ à partir d'Internet ;
- L'accès des serveurs DMZ à Internet ;
- L'accès au Web interne à travers un portail situé dans la DMZ ;
- L'accès au réseau interne Uonet est interdit sauf les réponses attendues par les requêtes initiées depuis l'intérieur ;
- Toutes les stations de travail dans les réseaux virtuels FORMATION et ADMINISTRATION doivent pouvoir initier des requêtes vers Internet ;
- La surveillance et le contrôle du flux du réseau à travers le réseau virtuel MONITORING ;
- L'intervention sur des postes distants du réseau local de l'université de manière logicielle avec la possibilité d'un deuxième contrôle du flux du réseau;
- L'accès à la messagerie à travers un relais situé dans la DMZ.

Pour initier de telles requêtes vers différents réseaux virtuels ou segments un ensemble de

service sera défini. Ces services vont permettre aux différents utilisateurs de communiquer de manière restrictive. Comme exemple un utilisateur du réseau voulant effectuer des recherches sur le net devra alors utiliser comme service le HTTP (Hyper Text Transfert Protocol) qui va lui permettre de naviguer sur différents sites. Ou encore pour consulter sa boîte sur Yahoo ! il devra utiliser comme services du SMTP, IMAP, POP... Ainsi un certain nombre de service devront permettre quelques requêtes de certains utilisateurs des deux réseaux virtuels. A travers un schéma illustratif, nous avons donc représenté les différents flux ou initiation de connexion qui peuvent s'effectuer.



Les différents services de connexion s'établiront comme suit :

→	*Internet*	*DMZ*	*RAS*	*Monitoring*	*Administration*	*maintenance*	*Formation*
Internet		HTTP, DNS, SMTP ,FTP, SSH					
DMZ	http, DNS, SMTP FTP, SSH				SMTP	SMTP	SMTP
RAS	SSH, FTP, IMAP,HTTPs, HTTP, LDAP, POP, DNS	SMTP,IMAP, POP,DNS, http, FTP			HTTP, DNS, POP, IMAP, HTTPs, SMTP		HTTP, DNS, HTTPs, SMTP
Monitoring							
Administration	http,HTTPs, DNS,POP, IMAP,LDAP, SMTP	HTTP, HTTPs, DNS,LDAP, SMTP					FTP,HTTP MsusMsis,FTP

Maintenance	HTTP,HTTPs SMTP,POP, IMAP,DNS ,Msus Msis.FTP	TELNET,SSH, SMTP,POP, IMAP,DNS , MsusMsis,FTP	TELNET, SSH		TELNET,SSH		TELNET,SSH
Formation	HTTP,HTTPs, DNS,POP, IMAP,LDAP, SMTP	HTTP, HTTPs, DNS, SMTP					

TABLEAUX DES FLUX ET DES SERVICES D'INITIATION DE CONNEXION

NB : les cellules vides ne comportent aucune règle de connexion.

Le tableau ci-après défini les autorisations et les restrictions au niveau du pare-feu.

N°	*Réseau/adresse Source*	*Port/ Service*	*Réseau/adresse Destination*	*Port/ Service*	*Type*	*Action*
1	Mail_DNS_DMZ		Excepter(VLAN_form VLAN_staff, RAS, VLAN mon	DNS		Accepter
2	Mail_DNS_DMZ		Excepter (RAS, VLAN_mon)	SMTP		Accepter
3	Excepter (RAS, VLAN_mon)		Mail_DNS_DMZ	SMTP, DNS		Accepter
4	VLAN_maint		Excepter (VLAN mon, Internet)	SSH, telnet		Accepter
5	Excepter (VLAN_mon)		Web_DMZ Web_Cnrst	HTTP		Accepter
6	VLAN_form VLAN_staff		DMZ	SSH		Accepter
7	Mail_DNS_form Mail_DNS_staff		Mail_DNS_DMZ	SMTP		Accepter
8	VLAN_form VLAN_staff		Excepter(DMZ, VLAN_staff, VLAN_mon, RAS)	POP, IMAP, HTTP HTTPs, FTP, DNS, SSH, vexira.		Accepter
9	Excepter (DMZ, VLAN_mon)		Mail_DNS_form Mail_DNS_Staff	http, DNS.		Accepter
10	RAS		Excepter (DMZ, VLAN_staff, RAS, VLAN_mon)	POP, IMAP, HTTPs, HTTP, FTP, DNS, SSH, Vexira.		Accepter
11	Tout	Tout	Tout	Tout	Tout	Rejeter

Pour des besoins d'économie et afin de décharger le réseau virtuel STAFF de certains serveurs d'installation et de mise à jour, nous les aménagerons dans le réseau virtuel FORMATION. Ceci devrait rendre le réseau virtuel STAFF plus extensible en matière d'installation de serveurs (de fichiers, d'impression, de noms...). Il devra ensuite permettre à tous PC utilisateurs de se connecter

depuis n'importe quel réseau local virtuel pour des éventuels mises à jours ou installations. Quant au VLAN_MAINTENANCE il regroupera des logiciels de prises à distances, de réparations ou d'optimisation des PC utilisateurs et d'un serveur de contrôle de machines.
La répartition des serveurs se fera comme dans le tableau ci-après :

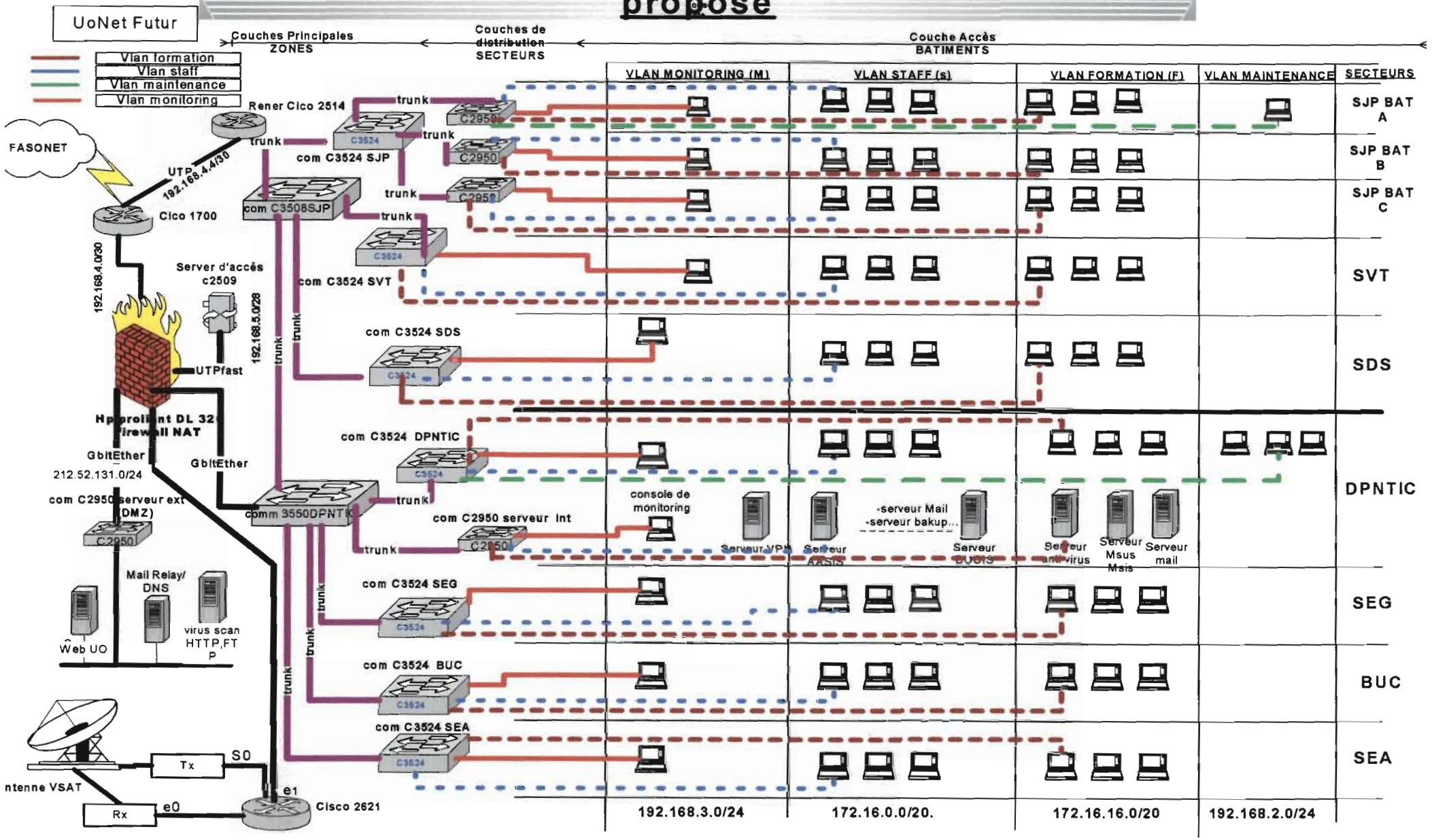
Segment	Serveurs (hostname)	Services	Logiciels	OS
DMZ	Serveur Web UO (www) (Web_DMZ)	http, index sur OPAC	Apache	Linux
		DNS externe secondaire	Bind 9	
	Serveur mail relay (Mail_dns_dmz)	SMTP relay	Postfix 2002	Linux
		DNS externe primaire	Bind 9	
		Anti-Virus passerelle pour SMTP	Trend Micro InterScan VirusWall	
	Serveur Web CNRST	http, IMAP, SMTP, POP	Apache, Postfix	Linux
	Anti-Virus Passerelle Serveur Cache	VirusScan http, FTP	Trend Micro InterScan VirusWall	W2K
		Proxy transparent	Squid	
VLAN FORMATION	Serveur mail étudiant	DNS Interne Dynamique	Bind 9, Smb 3	W2K/Linux
		DHCP1	DHCPd	
		SMTP, POP,IMAP	Postfix	
		http	Apache, SquirelMail	
		FTP	ProFTPd	
		Smb	Samba 3	
	DNS Secondaire	DNS Interne secondaire	Bind 9	Linux
	Serveur d'installation et de mise à jour	Anti-Virus Workgroup	Vexira	W2K
		Msis, Msus	Microsoft Installation Server, Microsoft Update Server	
	Serveur Mail	DHCP2	DHCPd	Linux
		SMTP, POP, IMAP	Postfix	
		http	Apache, SquirelMail	

		FTP	ProFTPd	
		Smb	Samba 3	
	Serveur BUCIS	http, SQL Serveur	IIS, ADLIB	W2K
	Serveur AASIS	SQL Serveur	Aris	W2K
	Serveur de Backup	http, SQL Serveur	ADLIB, Aris	W2K
	Serveur de Spool d'impression et de fichiers (Sindou)	Lp, Smb	Samba 3	Linux
VLAN MAINTENANCE	Logiciel de prise de contrôle à distance	PC anywhere	PC anywhere	WXP
	NAS (Option)	Stockage de masse en réseau	Network Area Storage	LINUX
	Logiciel de maintenance	Disk Manager, Disk Recover all…	Disk Manager, Disk Recover all…	WXP
VLAN MONOTORING	Console de gestion	SNMP, ICMP	What's Up, FW smart console	WXP
	Concentrateur VPN	Cisco VPN Software	VPN Soft	IOS
RAS	Serveur RAS	Tacacs++	Tacacs++	NT

Suite du tableau des serveurs par segment

Cette solution aboutit à la réalisation du schéma de la page suivante :

schéma explicite de l'architecture réseau proposé



5) Les différentes étapes de mise en œuvre

La réalisation de ce travail suit un ensemble d'étapes :

- Mettre tous les commutateurs dans le mode VTP transparent (déjà fait).
- Définir tous les trunk dans le réseau (liaisons inter commutateurs)
- Définir les trois (03) autres réseaux virtuels : VLAN STAFF,VLAN FORM, VLAN MAINT (le réseau VLAN MON sera le VLAN par défaut).
- Transférer tous les utilisateurs du VLAN par défaut vers le VLAN STAFF exceptées les stations de management réseau et des techniciens ;
- Transfert des serveurs selon leur appartenance aux VLANs ;
- Installation du pare-feu ;
- Création des utilisateurs des VLAN FORMATION et VLAN MAINTENANCE ;
- Mutation et création de certains serveurs (serveur de mise à jour...) ;
- Installation des différents logiciels sur les postes des utilisateurs du VLAN MAINTENANCE ;

6) Coût du matériel à acquérir

L'introduction d'un nouveau service de maintenance entraînera des dépenses supplémentaires pour le bon fonctionnement du réseau local. Le matériel à acquérir se compose de serveurs, de logiciels et d'utilitaires de maintenance. Le coût du matériel à acquérir s'établit comme suit :

DESIGNATION	CARACTERISTIQUES	QUANTITE	PRIX UNITAIRE(TTC)	PRIX TOTAL(TTC)
SERVEURS	INTEL XEON 2,8GHZ 04 DD SCSI 512 MO DE RAM (EXT À 8GO) CARTE RESEAU 10/100/1000 + MODEM	1	4.130 .000FCFA	4.130 .000FCFA
LOGICIEL DE PRISE DE CONTROLE A DISTANCE	SYMANTEC PC ANYWHERE HOST & REMOTE V11.0 ENSEMBLE COMPLET S.E REQUIS: 98/NT4.0/2OOO/XP	1	475.127 FCFA*	475.127 FCFA
LOGICIEL DE MAINTENANCE	NORTON SYSTEM WORKS 2004 / NORTON INTERNET SECURITY 2004 S.E REQUIS: 98/ME/2000/XP	1	60.180 FCFA	60.180 FCFA
COUT TOTAL PARTIEL	4.665.307 FCFA (TTC)			

* Prix en France

7) Evaluation de la solution

Cette solution présente aussi bien des avantages que des inconvénients.

Avantages :

En créant un VLAN Maintenance, nous mettons l'accent sur le principe du regroupement fonctionnel ; en effet, nous différencions la partie administration au sens pédagogique de la partie administration du réseau.

De plus nous pouvons définir plus facilement les permissions et restrictions en nous basant sur l'appartenance ou non au VLAN. Mais au-delà de ces atouts, différents inconvénients se présentent vis-à-vis de cette solution.

Inconvénients :

La création de ce VLAN va porter entrave à la consommation rationnelle de bande passante. En effet, dans ses communications avec les autres VLANs auxquels il a accès, il y aura génération d'un flux supplémentaire qui aura un impact considérable sur la bande passante. Et ce n'est pas tout.

Quiconque ayant accès au VLAN Maintenance aura quasiment une main mise sur le réseau, car il pourra avoir le contrôle sur les autres VLANs.

B) Deuxième solution : installation d'un serveur de contrôle et de maintenance dans le VLAN STAFF

Faire cohabiter les deux formes d'administration (pédagogique et technique) au sein du même VLAN est aussi réalisable.

1) détermination des VLANs

Pour cette deuxième solution, nous préconisons l'organisation du réseau en trois (03) réseaux locaux virtuels qui pourront également communiquer ou pas selon des règles judicieusement élaborées. Cependant le réseau virtuel STAFF regroupera à la fois la partie administration de l'Université et la partie maintenance. Ces trois (03) VLANs se définissent comme suit :

- **le réseau virtuel formation** qui regroupera en son sein
  - ✓ les salles de formations, de consultation ou de libre accès ;
  - ✓ les serveurs destinés à la formation (fichier, messagerie et autoformation) ;
  - ✓ les serveurs spécifiques (DNS interne, DHCP, serveur d'installation/update) ;
  - ✓ les périphériques destinés à la formation (imprimante, chargeur de CDROM, etc....)
  - ✓ les bâtiments connectés au réseau avec des équipements ne supportant pas les réseau virtuels.
  - ✓ Un serveur de contrôle de machines si le nombre de machines non fonctionnelles atteint un taux élevé.
- **Le réseau virtuel administration (staff)** qui regroupera :
  - ✓ Des serveurs destinés à l'administration de l'université :
    - BUCIS ;
    - AASIS ;
    - Serveur SINDOU ;
    - Serveur d'impression ;
    - Et d'autres applications comme la comptabilité, les services de ressources humaines, les services Web internes, la messagerie de l'administration et les postes de travail.

✓ Des serveurs destinés à la maintenance à distance des postes dans tous les autres réseaux virtuels (hormis le VLAN monitoring) c'est-à-dire :

- Des serveurs pour le contrôle des postes utilisateurs ;
- Des postes de maintenance servant à maintenir à distance les autres postes utilisateurs du réseau.
- Des postes servant au redémarrage d'un service sur les différents serveurs à l'aide de logiciels spécifiques.

➢ **Le réseau virtuel monitoring** qui regroupera les équipements destinées :

✓ A la connectivité (des commutateurs et des routeurs) ;

✓ A la gestion, à la surveillance et à la maintenance du réseau (consoles et station d'administration).

Bien entendu le choix de configuration des différents reste la configuration par port.

2) Plan d'adressage proposé

Nous suggérons pour cette solution, la réservation d'une plage d'adresse pour les postes et les serveurs de maintenance et de contrôle. Cette plage d'adresse nous permettra de différencier l'administration pédagogique de l'administration réseau. En intégrant donc un service de maintenance logicielle dans le VLAN_STAFF, notre tableau d'adressage se dresse comme ceci :

Zone		Plage d'adresses	Masque	Equipements concernés
DMZ		212.52.131.0	255.255.255.0	Relais Mail, DNS externe, UO Web, Web CNRST
VLAN STAFF	Statique	172.16.**0.1** – 172.16.**0.254**	255.255.240.0	BUCIS, AASIS, Backup, DHCP1, Mail Staff
		172.16.**1.1** – 172.16.**1.254**	255.255.240.0	Postes et serveurs de maintenance logicielle
	Dynamique	172.16.**2.1** – 172.16.**15.254**	255.255.240.0	Postes utilisateur
VLAN FORMATION	Statique	172.16.**16.1** – 172.16.**16.254**	255.255.240.0	DNS interne, DHCP2,
	Dynamique	172.16.**17.0** – 172.16.**31.254**	255.255.240.0	Postes utilisateur
VLAN MONITORING		192.168.3.0	255.255.255.0	Switchs Cisco
Firewall		192.168.4.4	255.255.255.252	Serveur COMPAQ proliant
RAS		192.168.5.0	255.255.255.240	Cisco 2509 TACACS
1700-2514		192.168.4.8	255.255.255.252	Routeur IOS sécurisé

Tableau des adresses IP

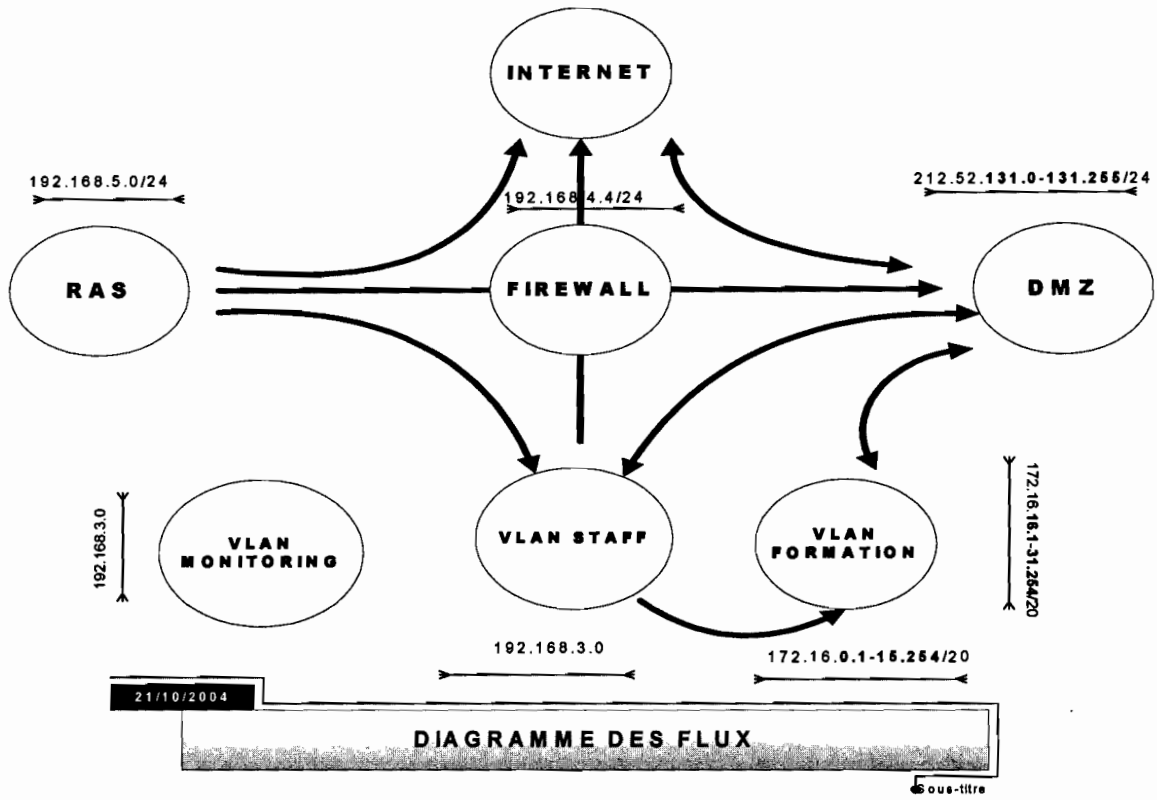
3) Politique de filtrage et de communication inter segment et inter vlan

La politique de filtrage pour cette solution tient compte des mêmes éléments sauf pour ce qui concerne le VLAN_MAINTENANCE qui n'existe alors plus. De plus, des règles spécifique au service de maintenance intégré dans le VLAN Staff sont à définir. Ces règles sont :

➢ L'accès des postes des techniciens aux autres postes utilisateurs du réseau sauf du VLAN_MONITORING ;

- La surveillance et le contrôle des postes utilisateurs par les postes de maintenance logicielle à travers le VLAN_STAFF ;
- L'intervention sur des postes utilisateurs des VLAN_FORM et VLAN_STAFF à distance.

Les différents flux ou initiations de connexion s'établissent comme suit :



Compte tenu de la création d'un sous groupe dans le VLAN Staff, et qui doit faire le travail du VLAN Maintenance de la première solution, l'utilisation des services subira une légère modification. En effet, ce sont les postes de la maintenance qui peuvent initier les services SSH et TELNET initiés depuis l'administration, dans le sens d'effectuer les tâches de contrôle du réseau et de maintenance des postes. Ces services seront implémentés indépendamment des autres services attribués sur le Firewall aux postes utilisateurs du VLAN Staff. Le tableau d'utilisation des services se présente ainsi qu'il suit :

→	*Internet*	*DMZ*	*RAS*	*Monitoring*	*Administration*	*Formation*
Internet		HTTP, DNS, SMTP ,FTP, SSH				
DMZ	HTTP, DNS, SMTP FTP, SSH				SMTP	SMTP
RAS	SSH, FTP, IMAP,HTTPs, HTTP, LDAP, POP, DNS	SMTP,IMAP, POP,DNS, http, FTP			HTTP, DNS, POP, IMAP, HTTPs, SMTP	HTTP, DNS, HTTPs, SMTP
Monitoring						

Administration	HTTP,HTTPs, DNS,POP, IMAP,LDAP, SMTP	HTTP, HTTPs, DNS,LDAP, SMTP,**TELNET, SSH**				FTP,HTTP MsusMsis,FTP, **TELNET,SSH**
Formation	HTTP,HTTPs, DNS,POP, IMAP,LDAP, SMTP	HTTP, HTTPs, DNS, SMTP				

TABLEAUX DES FLUX ET DES SERVICES D'INITIATION DE CONNEXION

Les services marqués en gras sont les nouveaux services ajoutés et qui ne seront définis que pour les postes de maintenance intégrés dans le VLAN_STAFF. Ils seront donc implémentés indépendamment des autres services que doivent effectuer les utilisateurs du VLAN_STAFF. Pour ce faire, à travers les autorisations élaborées sur le Firewall, nous ajouterons donc ce privilège que doivent utiliser les postes et les serveurs de maintenance. Le nouveau tableau des autorisations qui doit être défini sur le Firewall est le suivant :

N°	***Réseau/adresse Source***	***Port/ Service***	***Réseau/adresse Destination***	***Port/ Service***	***Type***	***Action***
1	Mail_DNS_DMZ		Excepter(VLAN_form VLAN_staff, RAS, VLAN mon	DNS		Accepter
2	Mail_DNS_DMZ		Excepter (RAS, VLAN_mon)	SMTP		Accepter
3	Excepter (RAS, VLAN_mon)		Mail_DNS_DMZ	SMTP, DNS		Accepter
4	**Postes_Serveurs_maint_ VLAN_STAFF**		**Excepter(RAS, VLAN_MON,Ext)**	**TELNET,SSH**		**Accepter**
5	Excepter (VLAN_mon)		Web_DMZ Web_Cnrst	HTTP		Accepter
6	VLAN_form VLAN_staff		DMZ	SSH		Accepter
7	Mail_DNS_form Mail_DNS_staff		Mail_DNS_DMZ	SMTP		Accepter
8	VLAN_form VLAN_staff		Excepter(DMZ, VLAN_staff, VLAN_mon, RAS)	POP, IMAP, HTTP HTTPs, FTP, DNS, SSH, vexira.		Accepter
9	Excepter (DMZ, VLAN_mon)		Mail_DNS_form Mail_DNS_Staff	http, DNS.		Accepter
10	RAS		Excepter (DMZ, VLAN_staff, RAS, VLAN_mon)	POP, IMAP, HTTPs, HTTP, FTP, DNS, SSH, Vexira.		Accepter
11	Tout	Tout	Tout	Tout	Tout	Rejeter

Tableau des autorisations et restrictions du pare feu

Notre deuxième solution entraîne une redistribution des serveurs par segment. Le VLAN_STAFF regroupera les serveurs de contrôle et de maintenance en plus des autres serveurs qu'il contient déjà. Pour une solution de secours, le VLAN_FORM devra contenir également ces mêmes serveurs si le nombre de pannes des postes au niveau du VLAN_FORM est très élevé. Le nouveau tableau des serveurs par segment se dresse ainsi :

Segment	Serveurs (hostname)	Services	Logiciels	OS
DMZ	Serveur Web UO (www) (Web_DMZ)	http, index sur OPAC	Apache	Linux
		DNS externe secondaire	Bind 9	
	Serveur mail relay (Mail_dns_dmz)	SMTP relay	Postfix 2002	Linux
		DNS externe primaire	Bind 9	
		Anti-Virus passerelle pour SMTP	Trend Micro InterScan VirusWall	
	Serveur Web CNRST	http, IMAP, SMTP, POP	Apache, Postfix	Linux
	Anti-Virus Passerelle Serveur Cache	VirusScan http, FTP	Trend Micro InterScan VirusWall	W2K
		Proxy transparent	Squid	
VLAN FORMATION	Serveur mail étudiant	DNS Interne Dynamique	Bind 9, Smb 3	W2K/Linux
		DHCP1	DHCPd	
		SMTP, POP,IMAP	Postfix	
		http	Apache, SquirelMail	
		FTP	ProFTPd	
		Smb	Samba 3	
	DNS Secondaire	DNS Interne secondaire	Bind 9	Linux
	Serveur d'installation et de mise à jour	Anti-Virus Workgroup	Vexira	W2K
		Msis, Msus	Microsoft Installation Server, Microsoft Update Server	

	NAS (Option)	**Stockage de masse en réseau**	**Network Area Storage**	**LINUX**
	Serveur de contrôle et de maintenance	**PC anywhere**	**PC anywhere**	**WXP**
		Disk Manager, Disk Recover all...	**Disk Manager, Disk Recover all...**	
VLAN STAFF	Serveur Mail	DHCP2	DHCPd	Linux
		SMTP, POP, IMAP	Postfix	
		http	Apache, SquirelMail	
		FTP	ProFTPd	
		Smb	Samba 3	
	Serveur BUCIS	http, SQL Serveur	IIS, ADLIB	W2K
	Serveur AASIS	SQL Serveur	Aris	
	Serveur de Backup	http, SQL Serveur	ADLIB, Aris	
	Serveur de Spool d'impression et de fichiers (Sindou)	Lp, Smb	Samba 3	Linux
	Serveur de contrôle et de maintenance	**PC anywhere**	**PC anywhere**	**WXP**
		Disk Manager, Disk Recover all...	**Disk Manager, Disk Recover all...**	
VLAN MONOTORING	Console de gestion	SNMP, ICMP	What's Up, FW smart console	WXP
	Concentrateur VPN	Cisco VPN Software	VPN Soft	IOS
RAS	Serveur RAS	Tacacs++	Tacacs++	NT

Tableau des serveurs par segment

4)Les différentes étapes de mise en oeuvre

La mise en œuvre de cette solution nécessite le respect des étapes suivantes :

- Mettre tous les commutateurs dans le mode VTP transparent (déjà fait).
- Définir tous les trunk dans le réseau (liaisons inter commutateurs)
- Définir les trois (02) autres réseaux virtuels : VLAN STAFF,VLAN FORM (le réseau VLAN MON sera le VLAN par défaut).
- Transférer tous les utilisateurs du VLAN par défaut vers le VLAN STAFF;
- Créer les postes de maintenance dans le VLAN Staff ;
- Transferer les serveurs selon leur appartenance aux VLANs ;
- Installation du pare-feu ;
- Etablir les règles et attribution des privilèges aux postes de maintenance ;
- Créer les utilisateurs des VLAN FORMATION;

- Muter et installer certains serveurs (serveur de mise à jour...) ;
- Installer les différents logiciels sur les postes des techniciens du service de MAINTENANCE ;

L'organisation nouvelle entraînée par cette solution est représentée par le schéma ci-après :

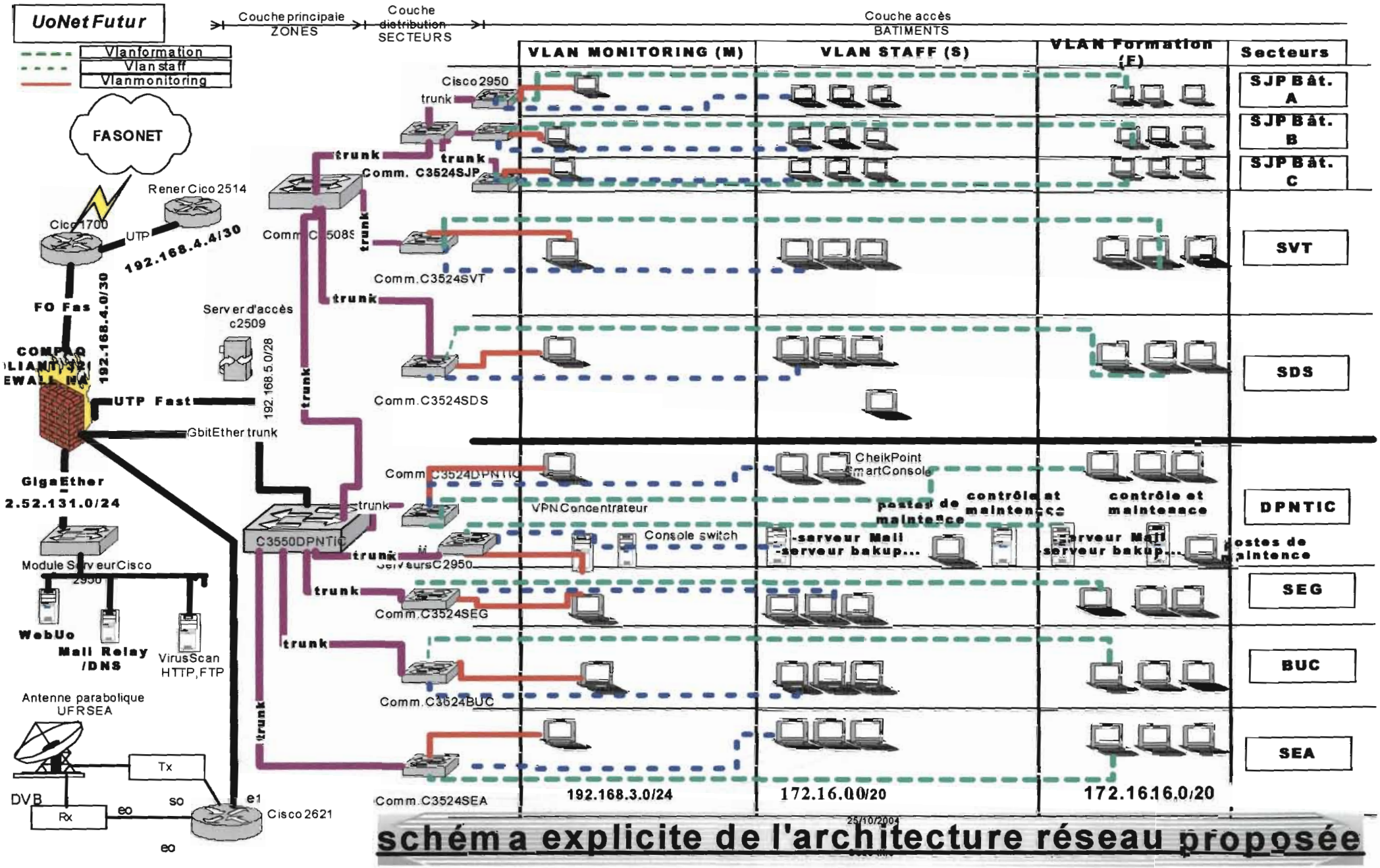


schéma explicite de l'architecture réseau proposée

5)Coût du matériel à acquérir

Dans cette deuxième solution, il sera nécessaire de déployer deux serveurs de maintenance et de contrôle : l'un pour le VLAN_STAFF et l'autre dans le VLAN_FORM pour servir de relais si le nombre de panne des postes utilisateurs de ce VLAN est élevé. Ce qui donc rendra le coût de notre matériel à acquérir plus onéreux. Cependant, l'acquisition de ce deuxième serveur pourrait être optionnelle selon les moyens financiers de l'université. Ce coût est détaillé dans le tableau ci-après :

SERVEURS	INTEL XEON 2,8GHZ 04 DD SCSI 512 MO DE RAM (EXT A 8GO) CARTE RESEAU 10/100/1000 + MODEM	2	4.130 .000FCFA	8.260.000 FCFA
LOGICIEL DE PRISE DE CONTROLE A DISTANCE	SYMANTEC PC ANYWHERE HOST & REMOTE V11.0 ENSEMBLE COMPLET S.E REQUIS: 98/NT4.0/2OOO/XP	1	475.127 FCFA*	475.127 FCFA
LOGICIEL DE MAINTENANCE	NORTON SYSTEM WORKS 2004 / NORTON INTERNET SECURITY 2004 S.E REQUIS: 98/ME/2000/XP	1	60.180 FCFA	60.180 FCFA

*** Prix en France**

6) Evaluation de la solution

- Avantages :

Se limiter au VLAN Staff pour réussir le travail de surveillance et d'administration du réseau à travers un serveur destiné à cela constitue une grande économie en matière de bande passante. En effet, les trames appartiennent au même VLAN et ne génèrent pas alors de flux supplémentaire.

Un autre aspect est que vu le nombre réduit d'éléments servant à effectuer ce travail, les possibilités d'y avoir accès et d'intervenir dans le sens de nuire au bon fonctionnement du réseau sont assez réduites. Cependant, des inconvénients apparaissent à certains niveaux.

- Inconvénients :

L'inconvénient majeur de cette solution apparaît lorsque l'on assiste à un taux important de panne au sein du VLAN Formation. En effet, à ce moment l'intervention du VLAN Staff à travers le serveur de contrôle pour remédier au problème est susceptible de générer le même flux que dans la première solution. De ce fait, la consommation de bande passante s'accroîtrait et nuirait ainsi au fonctionnement adéquat du réseau souhaité. Il faudrait alors mettre dans ce cas un autre serveur destiné à la même tâche

dans le VLAN Formation.

C) Choix de la solution

La différence entre les coûts de réalisation des deux solutions examinées n'est pas aussi considérable que si l'on utilisait qu'un seul serveur de maintenance c'est-à-dire dans le VLAN_STAFF. En effet, le réseau de l'université est un vaste réseau très sécurisé, utilisant de nombreux serveurs et une technologie bien adaptée à la conception réseau. Nous utiliserons donc les mêmes équipements actifs répertoriés dans l'existant à savoir les commutateurs, les routeurs et les serveurs mais aussi, les câbles UTP catégorie 5 et de la fibre optique monomode et multimode déjà existant dans le réseau. Mais dans tous les cas, l'acquisition d'un serveur et des logiciels destinés au travail de contrôle et de maintenance est nécessaire. Et comme déjà évoquée, ce n'est qu'en cas de taux de pannes élevé que la nécessité d'installer un serveur supplémentaire s'impose dans la deuxième solution. Dans le cas contraire, les coûts s'équivaudraient pour les deux solutions.

De plus, créer un VLAN qui a accès à tous les VLANs n'est pas recommandable car la mise en place d'un VPN est mieux indiquée et adaptée à cette situation. Mais l'on notera surtout que la gestion optimale de la bande passante est très déterminante. On ne saurait d'ailleurs surcharger le trafic pour remettre seulement quelques postes en état de fonctionnement alors que tout le reste du réseau en pâti.

De ces différents constats, et au regard des objectifs poursuivis, la deuxième solution s'avère la plus profitable pour une solution palliative du problème de maintenance. Et ainsi, c'est cette solution dont la réussite restera fort tributaire des moyens humains qu'il implique (charte d'utilisation du réseau, gestion du réseau…) que nous mettrons en œuvre.

Quelques apports à la mise en oeuvre

Comme souligné dans le plan déjà conçu nous réserverons deux switchs 10/100/1000 Mbps pour minimiser les problèmes de montée en charge, et faciliter la maintenance des serveurs, l'un pour la connexion des serveurs internes en respectant leurs appartenances aux VLAN FORM ou ADMIN, et l'autre pour les serveurs de la DMZ. Ces switchs seront placés dans la salle serveur. Cela permettra:

- d' avoir moins de câbles entremêlés dans l'armoire de brassage ;
- de libérer des ports sur le switchs fédérateur 3550 ;
- d'optimiser la vitesse d'accès aux serveurs d'applications.

Il faudrait cependant noter que cette sécurité au niveau logique n'est pas le seul moyen qu'il faudra mettre en œuvre pour une sécurité accrue du futur réseau de l'université. D'autres aspects de la sécurité doivent être pris en compte pour une non-altération de la confidentialité, de la disponibilité et de l'intégrité des ressources critiques de l'université. Ce sont :

- La sécurité applicative ;
- La sécurité de l'exploitation ;
- La sécurité physique.

Cette étude menée sur l'existant et la définition d'un plan de réalisation constitueront les éléments sur lesquels nous nous appuierons pour la configuration des différents équipements et la mise en œuvre proprement dite de réseaux locaux virtuels au sein du réseau de l'université de Ouagadougou.

CHAPITRE III
SIMULATION DE CONFIGURATION DE LA MISE EN ŒUVRE DES RESEAUX LOCAUX VIRTUELS .

La mise en œuvre effective des VLANs suit un plan par étape que nous avons évoqué plus tôt. La réussite véritable du projet va du bon acheminement et du respect de ce plan. Cependant au sens pratique, nous proposons une simulation basée sur la configuration de VLANs à travers deux (02) commutateurs (Switchdessai et Switchdessai2) et trois (03) postes de travail (Pc essai formation1, Pc essai formation 2 et Pc essai staff) . Dans cette simulation nous ferons ressortir des aspects tels que les définitions de VLANs sur les commutateurs, la configuration de ces VLANs, le paramétrage des ports ainsi que les aperçus des organisations en groupes logiques ainsi formées.

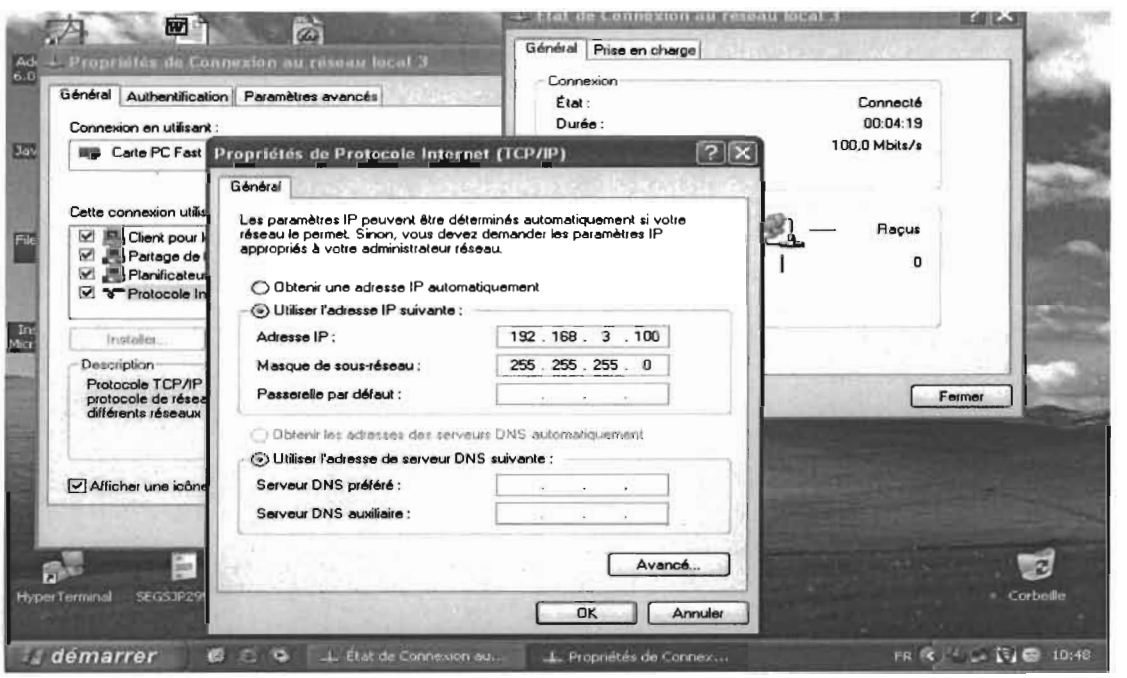
I- Démarrage

Pour ce qui est de l'attribution d'une adresse IP au commutateur, nous l'effectuerons en mode ligne de commande.

1) Connexion au commutateur Switchdessai

Ce commutateur est un Catalyst 2950 Séries 24 ports Ethernet 10/100 et deux ports GBIC.

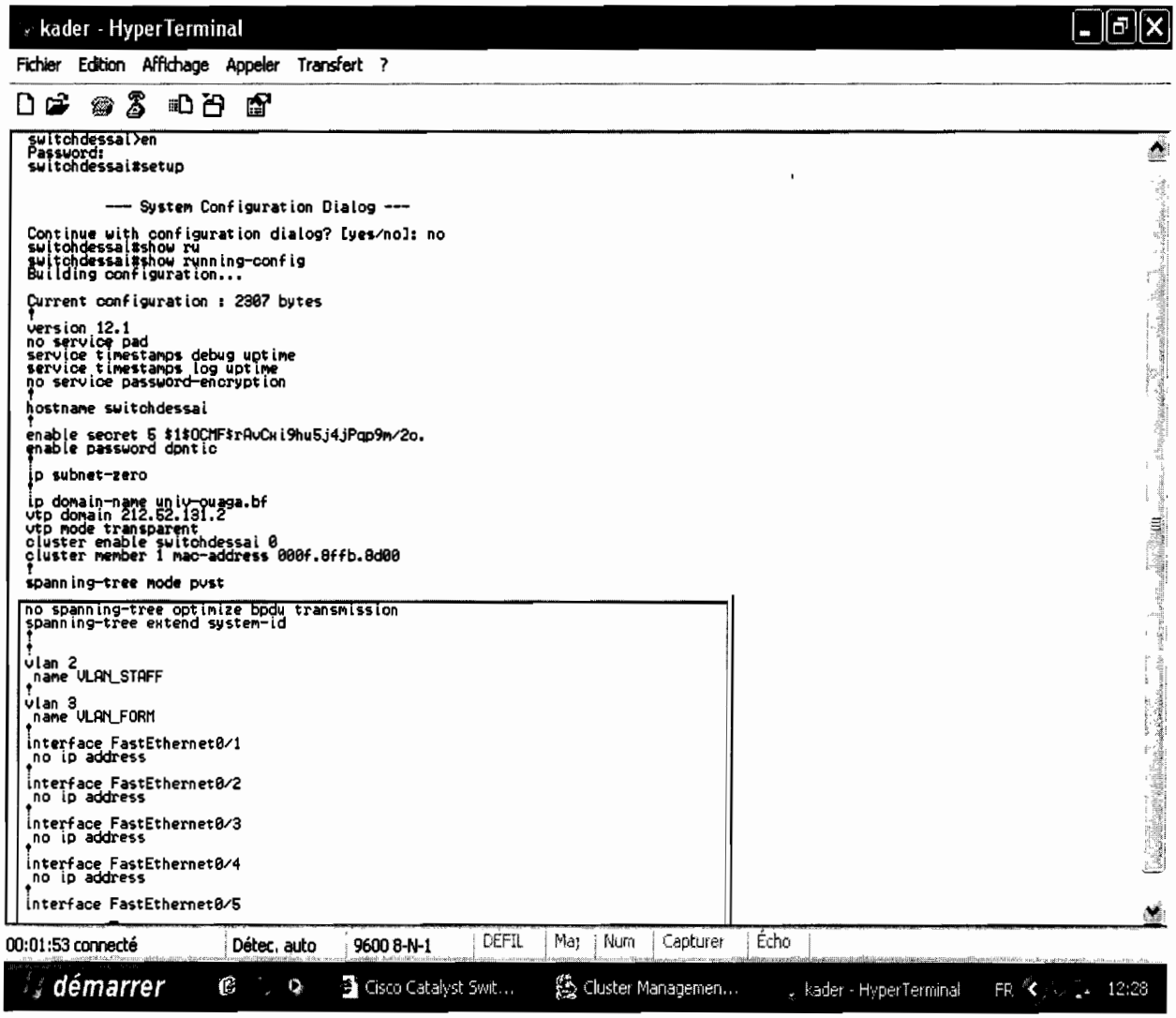
A la mise sous tension, le commutateur effectue une série de tests afin de vérifier le bon fonctionnement de ses composants. Nous connectons alors la console de configuration au commutateur à l'aide d'un câble console RJ45-DB9, après lui avoir attribué une adresse IP et défini le masque de sous-réseau correspondant.



Paramétrage de la console de configuration des commutateurs

Après la configuration de l'hyper terminal, une session de dialogue s'établit pour permettre d'entrer les paramètres minimaux du commutateur tel le nom d'hôte, le mot de passe, l'adresse IP. Nous entrons dans ce cas pour Switchdessai :

Adresse IP : 192.168.3.3
Masque de sous-réseau :255.255.255.0
Nom de l'hôte : Switchdessai
Mot de passe : xxxxxxxxxxx



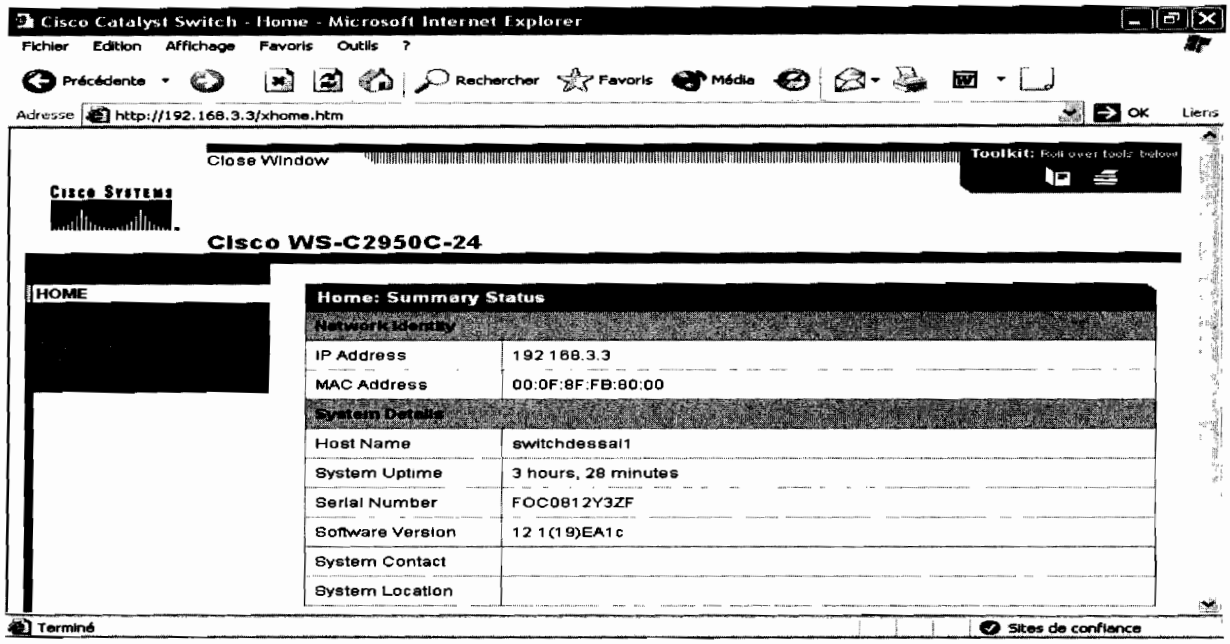
Configuration en mode CLI des commutateurs

Bien que cela soit possible en mode ligne de commande, nous poursuivrons à travers le CMS (Cluster Management Suite).

2) Le Cluster Management Suite

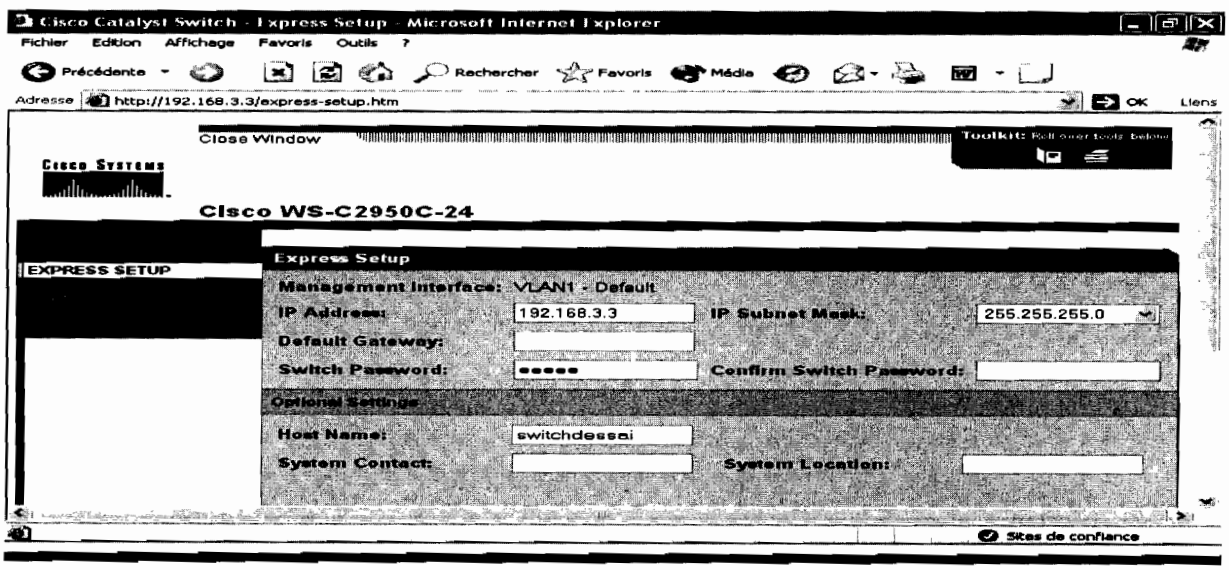
Cette rubrique que nous utilisons pour la poursuite de la configuration du commutateur offre des

sous-rubriques permettant la configuration des ports, des interfaces, des VLANs, la visualisation de l'organisation des commutateurs ou encore des vues sur leur aspect physique.



Ecran graphique du Cluster Management

La rubrique EXPRESS SETUP affiche les informations sommaires (adresse IP, masque de sous-réseau, mot de passe…) relatives au switch.



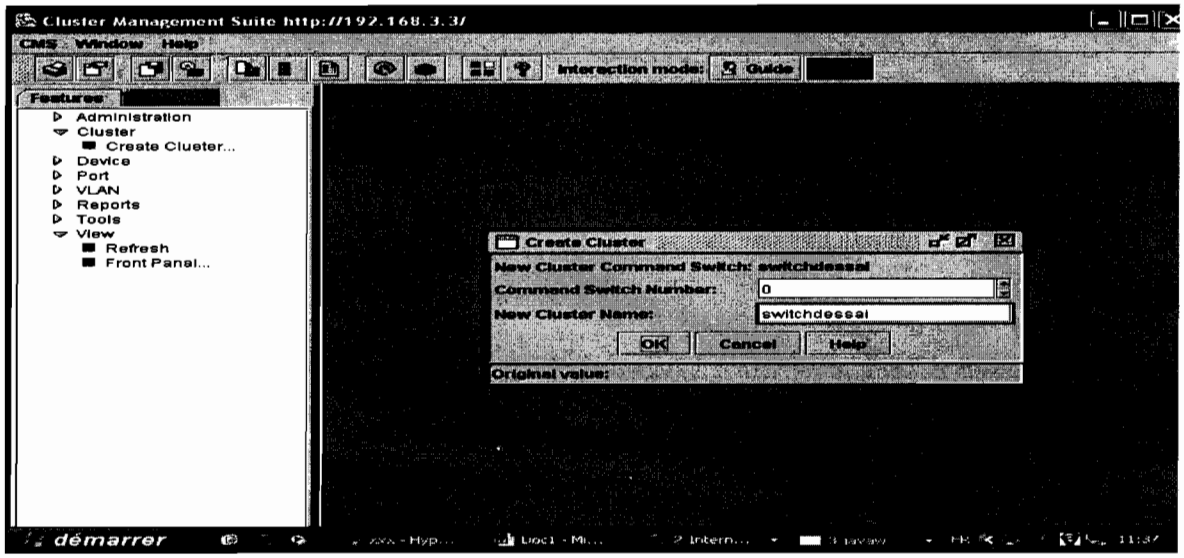
paramétrage graphique des commutateurs

3) Ajout du commutateur Switchdessai2 au cluster

L'ajout d'un switch à un cluster permet de le considérer directement dans des configurations

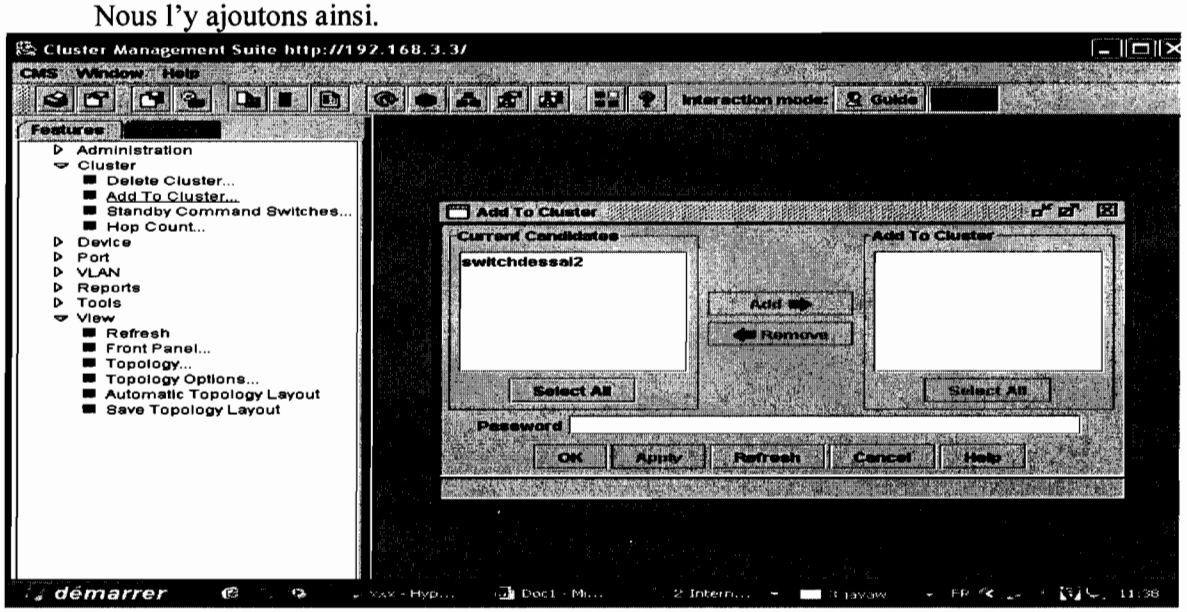
applicables à d'autres switches. En effet, on pourra par exemple attribuer en même temps des paramètres identiques à des ports sélectionnés sur les différents switches. Pour obtenir ce genre de configuration nous ajoutons Switchdessai2 au cluster managé par Switchdessai.

Au préalable nous mettons Switchdessai2 sous tension puis nous le relions à Switchdessai à l'aide d'un câble réseau. Nous configurons Switchdessai en CMD (Cluster Management Device), ce qui lui permet de reconnaître Switchdessai2 comme commutateur candidat, potentiel élément du cluster.



Création d'un commutateur de gestion du cluster

Nous l'y ajoutons ainsi.



Ajout de Switchdessai2 au cluster

II- Paramétrage du commutateurs Switchdessai

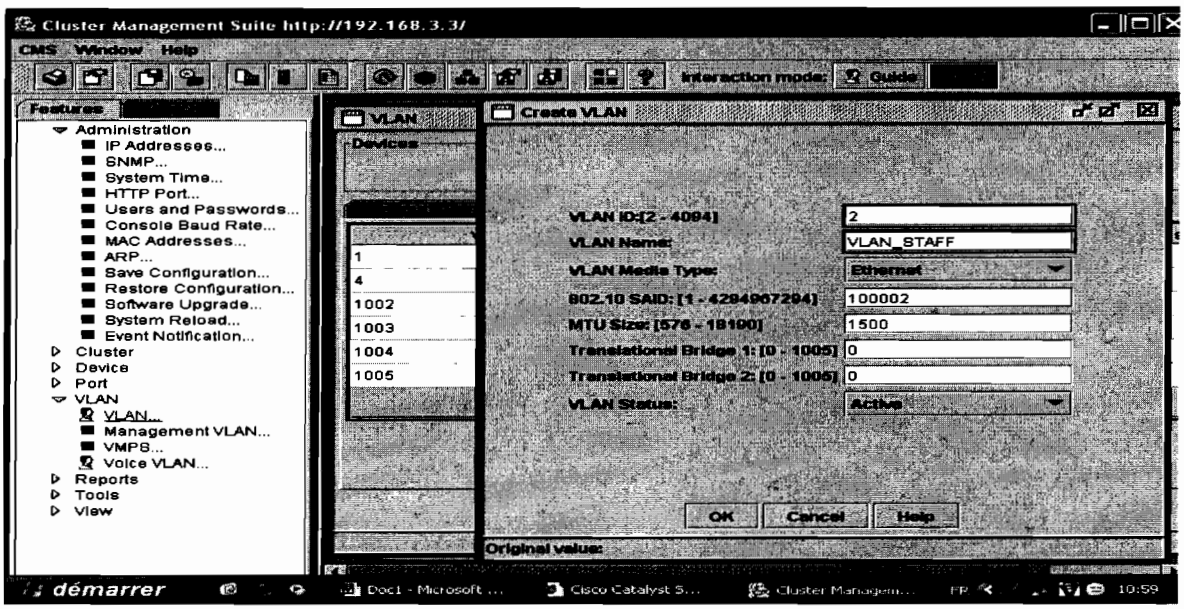
1) Création des VLANs

Trois VLANs sont à créer sur les deux commutateurs. Ce sont le VLAN_STAFF, le

VLAN_MONITORING et le VLAN_FORMATION. Pour chacun d'eux, les éléments suivants sont entrés : numéro de VLAN, Nom de VLAN, type de média du VLAN et statut du VLAN.

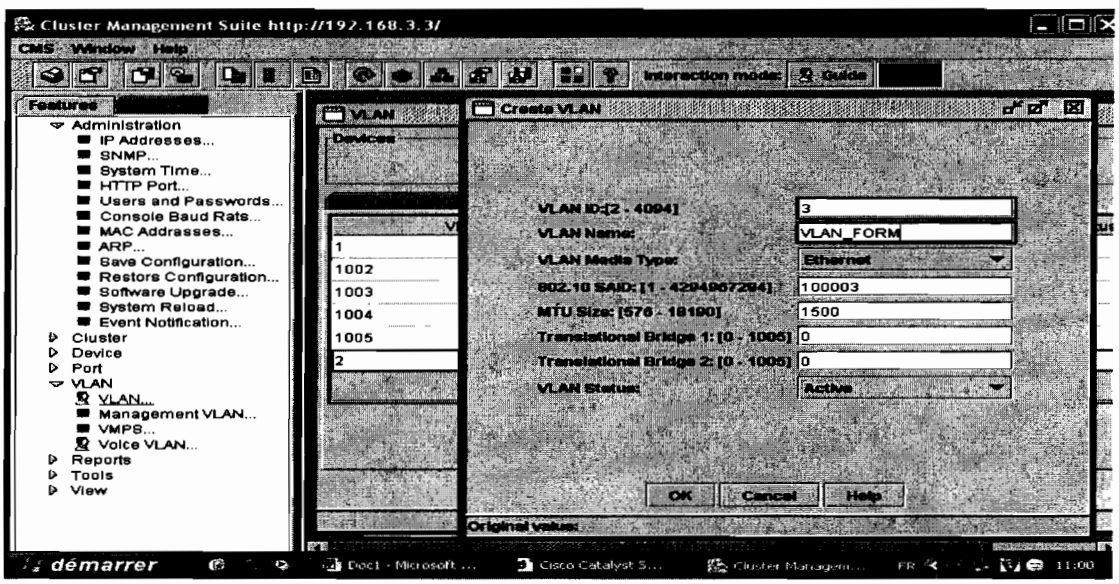
Ainsi en ce qui concerne le VLAN_STAFF, nous entrons les valeurs :

Numéro de VLAN : 2
Nom de VLAN: VLAN_STAFF
Type de media: Ethernet
Statut du VLAN: activé



Création d'un VLAN

Le même procédé est appliqué pour la création du troisième VLAN : le VLAN_FORM

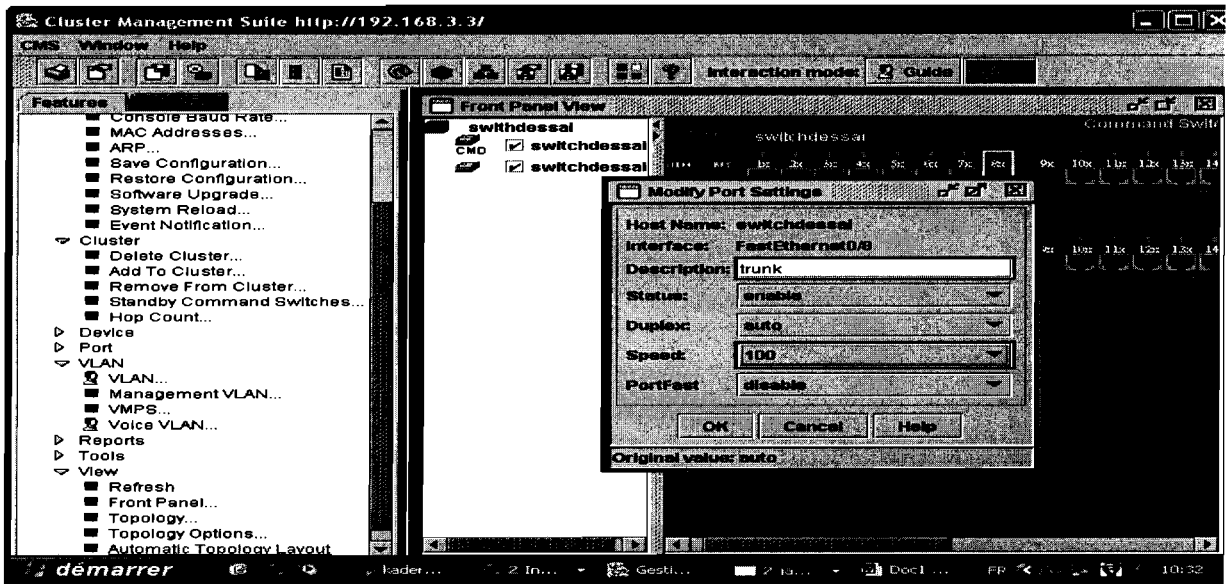


2) Paramétrage des ports

Un port peut appartenir à un ou plusieurs VLANs.

a) Port trunk

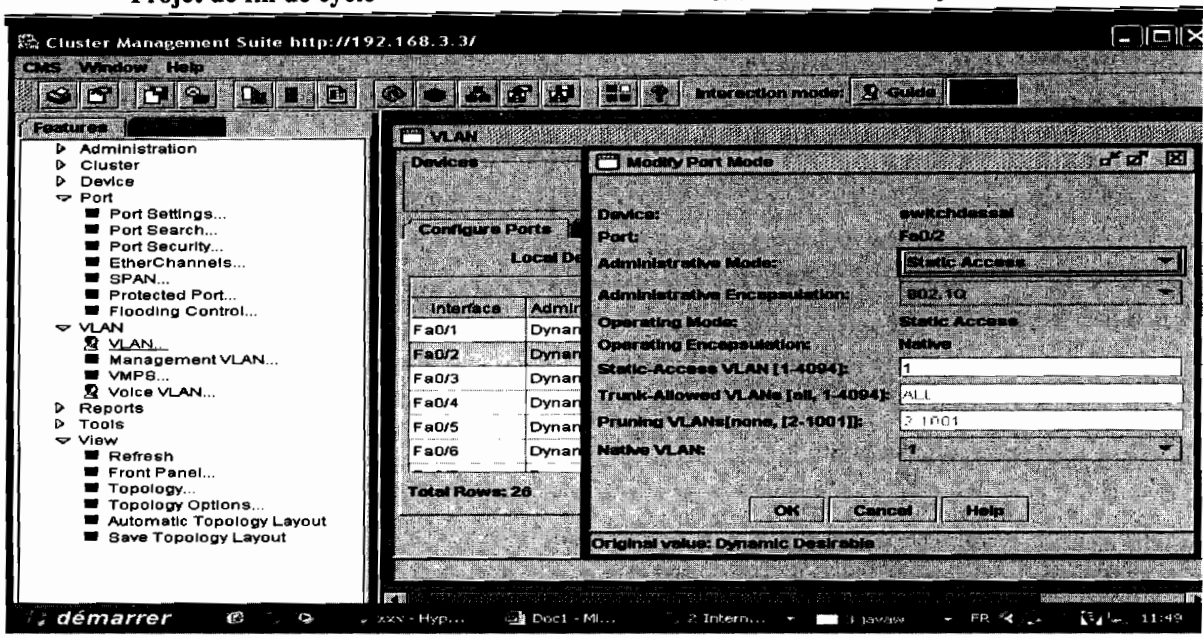
Nous définissons le port FastEthernet0/8 et le port FastEthernet0/9 comme ports trunk. Ils appartiennent à tous les trois VLANs définis sur le commutateur. Ils sont activés, fonctionnent à 100Mps en mode duplex.



Description et paramétrage d'un Trunk

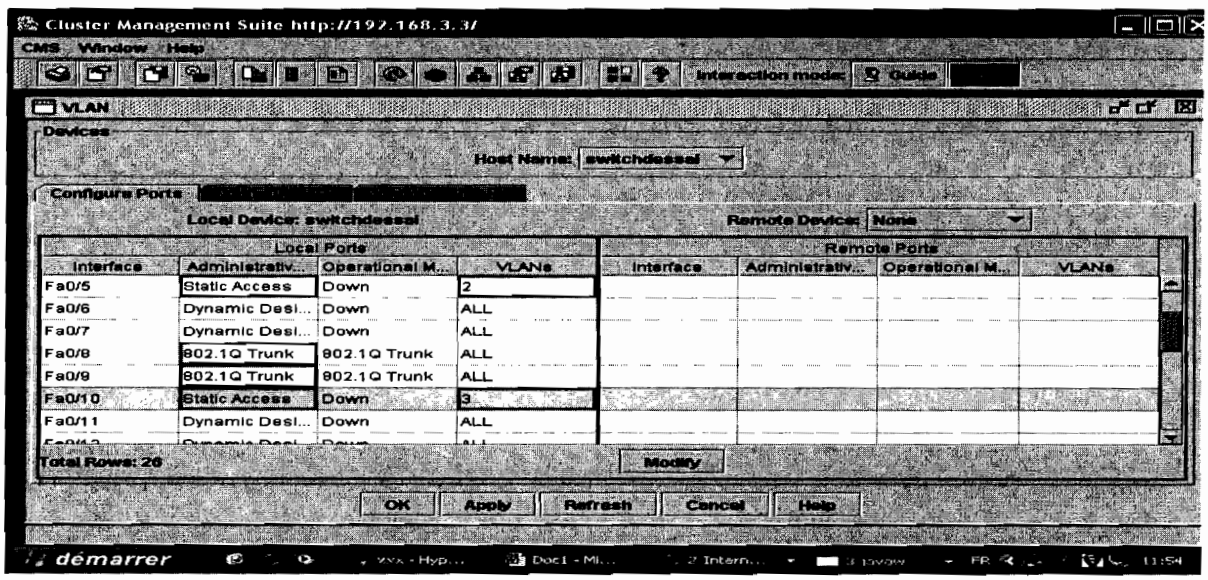
b) Port Monitoring

Nous définissons le port FastEthernet0/2 comme appartenant au VLAN_MONITORING. Il est activé et fonctionne en mode duplex à 100Mps. C'est celui par lequel nous administrons les deux commutateurs de notre simulation à travers la page de configuration.



Attribution d'un port à un VLAN

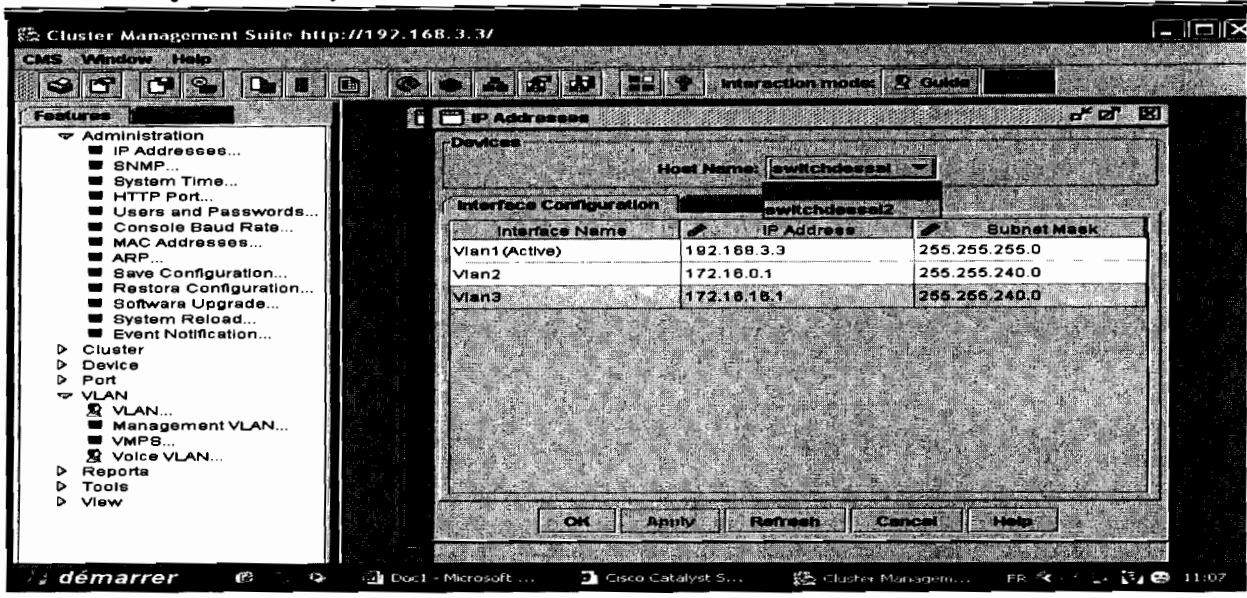
De même nous définissons le port FastEthernet0/5 comme appartenant au VLAN Staff et le port FastEthernet0/10 comme appartenant VLAN Formation.



Vue des appartenances des ports au différents VLANs

3) Configuration des adresses des interfaces.

Un interface est affecté à chaque VLAN sur les deux commutateurs. Il s'agit donc d'entrer les adresses IP et les masques de sous-réseau associés, correspondant à chaque interface. Nous avons ainsi :
VLAN1 : 192.168.3.3 255.255.255.0
VLAN2 : 172.16.0.1 255.255.240.0
VLAN3 : 172.16.16.1 255.255.240.0

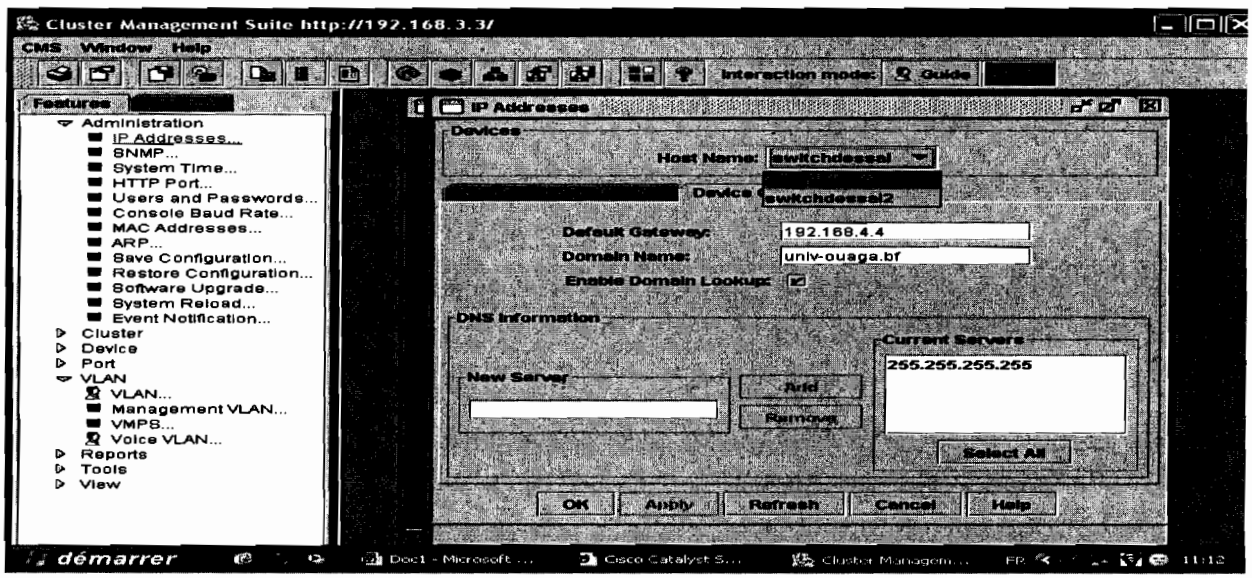


Paramétrage des différents VLANs

4) Autres paramètres

a) La passerelle par défaut et le DNS

La passerelle par défaut et le nom du DNS sont des informations à fournir. Pour Switchdessai, il s'agit de 192.168.4.4 pour la passerelle par défaut qui est l'adresse du Firewall et **univ-ouaga.bf** pour le DNS.

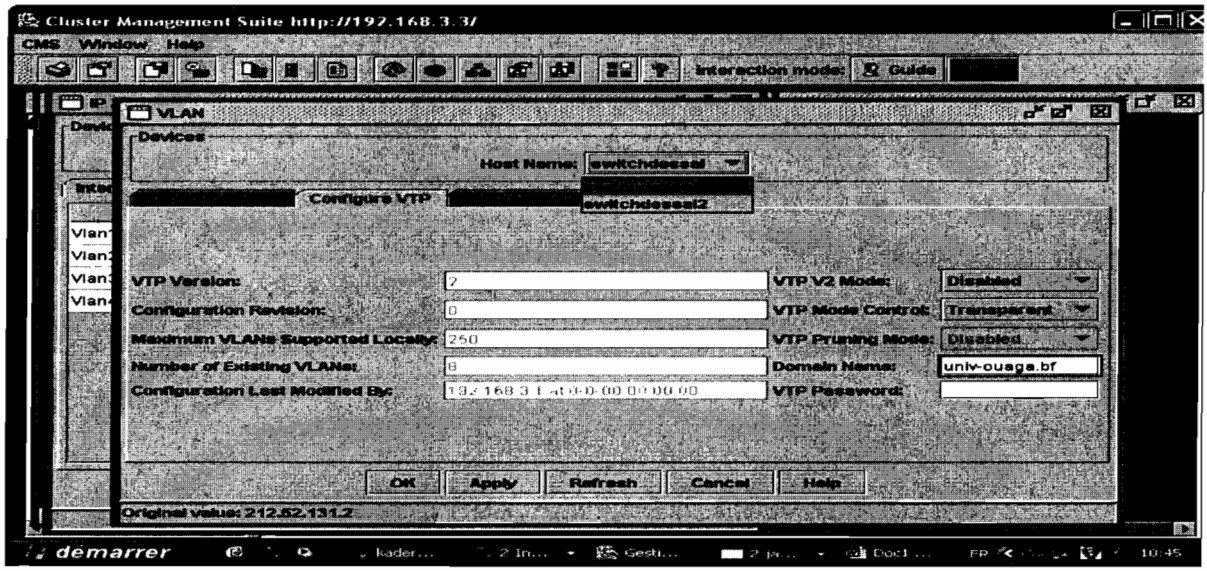


configuration de la passerelle par défaut et du DNS

b) Le mode VTP

Le VTP est mis en mode transparent ; cela empêche les switchs de se synchroniser aux autres en ce qui concerne les différents messages de reconfiguration qui sont souvent source de nombreux

problèmes. A cela l'on peut ajouter le nom du domaine dans lequel l'on se trouve.

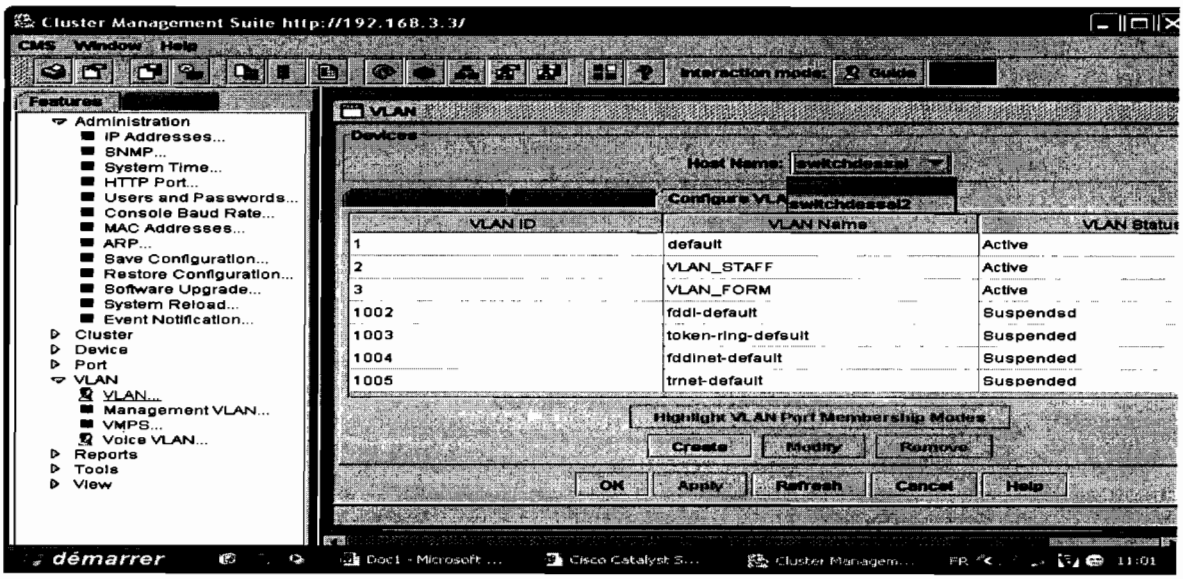


configuration en mode VTP

III- Paramétrage de Switchdessai2

1) Création des VLANs

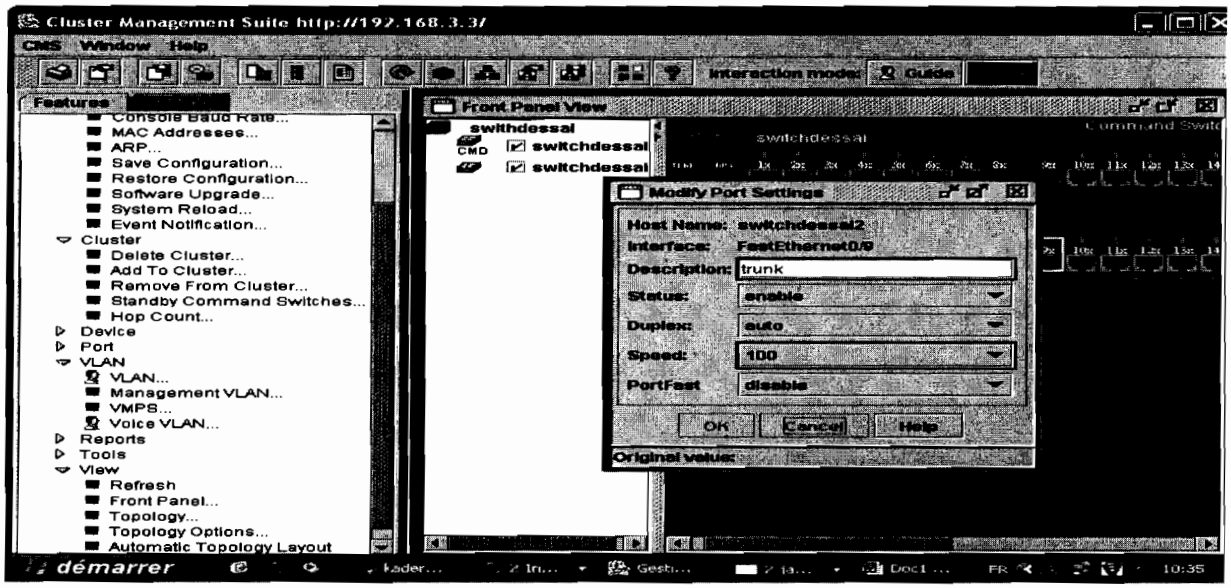
La création des trois VLANs définis plus haut s'effectue également sur le commutateur Switchdessai2 conformément à la même procédure. De plus ce commutateur est aussi mis en mode VTP transparent avec les mêmes valeurs pour la passerelle par défaut et le DNS.



création des VLANs pour le second commutateur

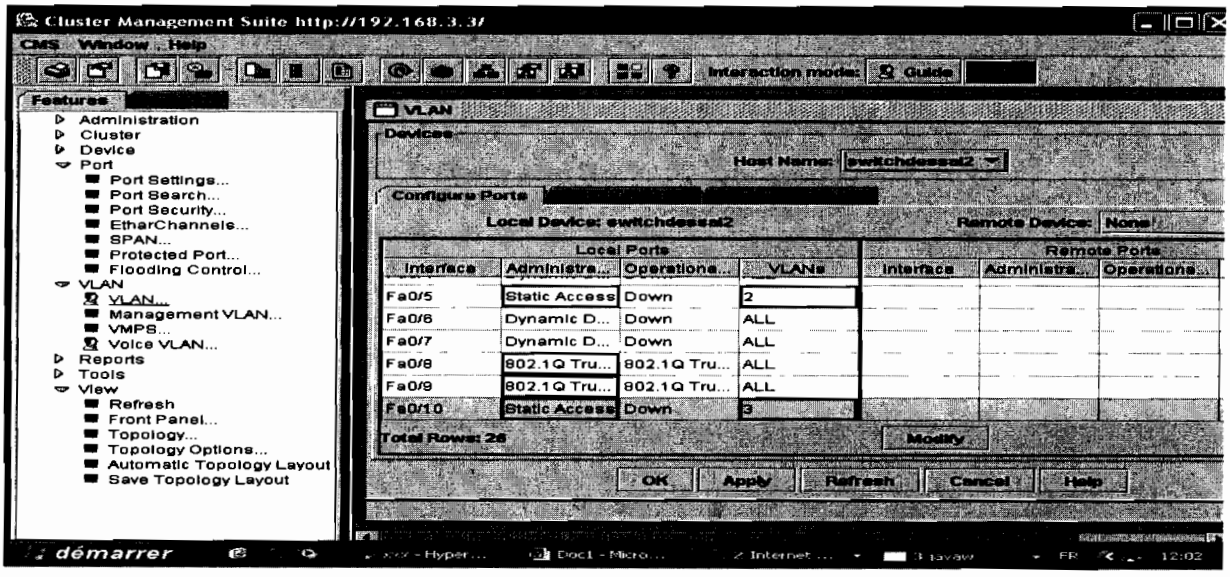
2) Paramétrage des ports

Nous configurons les ports FastEthernet0/8 et FastEthernet0/9 comme ports trunk, servant à établir la liaison entre le commutateur Switchdessai et le commutateur Switchdessai2.



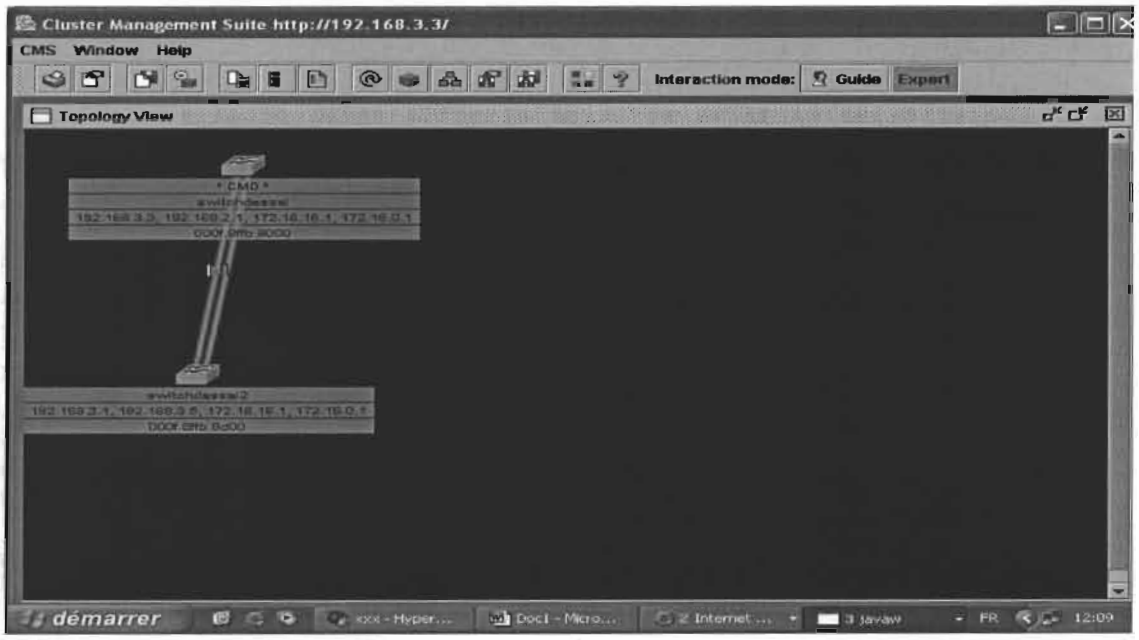
description des ports trunk

Quant aux ports FastEthernet0/5 et FastEthernet0/10, ils appartiennent respectivement au VLAN_STAFF et au VLAN_FORM



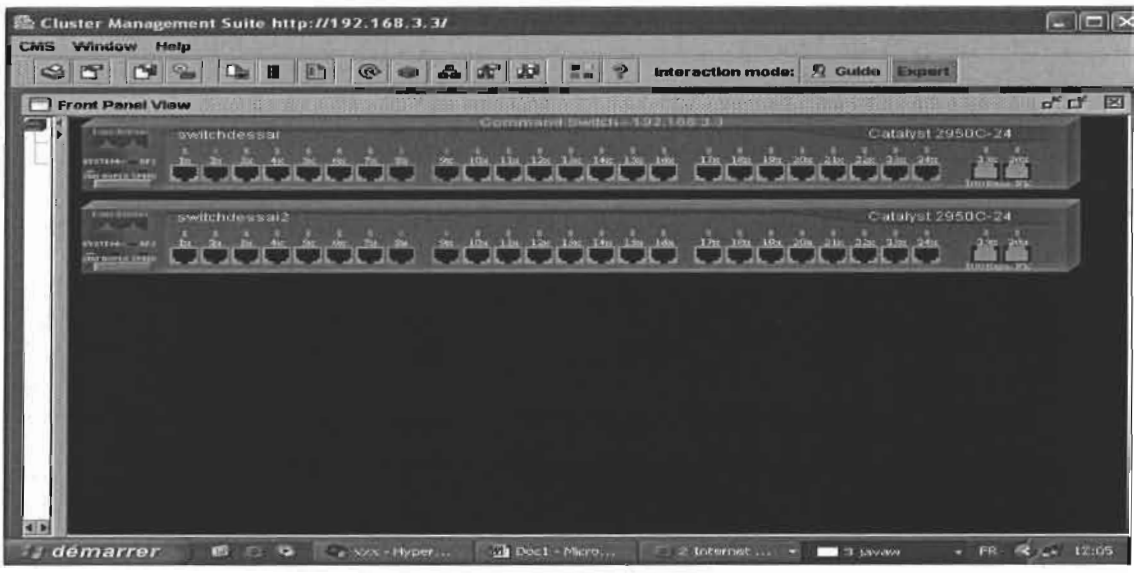
Attribution des ports au différents VLANs

Deux vues des deux commutateurs ainsi configurés se présentent comme ci-après :



Vue topologique

L'aperçu des ports est tel que nous montre la capture ci-dessous :



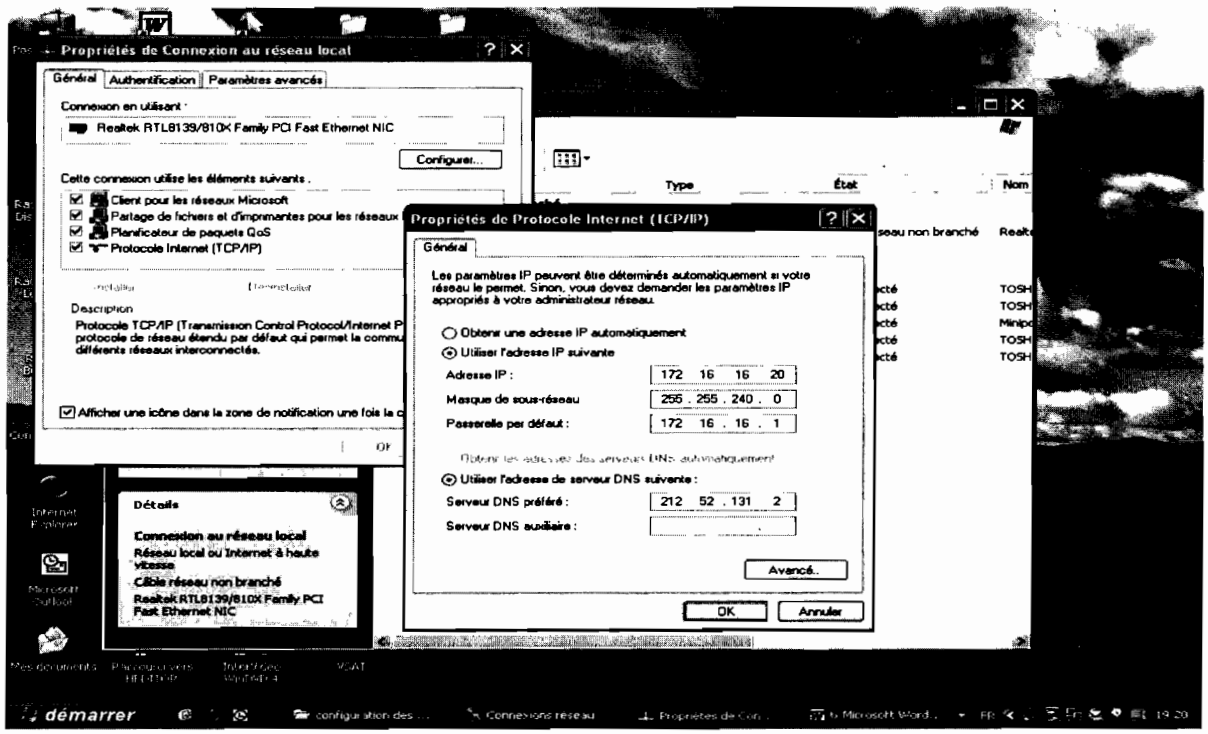
Aperçu des ports

IV- Configuration de postes de travail

1) Postes de travail dans le même VLAN

Nous connectons deux postes de travail respectivement **pc d'essai formation1** et **pc d'essai formation2**, l'un sur le port FastEthernet 0/10 (VLAN Formation) de Switchdessai et l'autre sur le port FastEthernet 0/10 (VLAN Formation) de Switchdessai2. De plus nous configurons les adresses IP tel que correspondant à l'adressage des interfaces des VLANs définie sur les deux commutateurs. Ainsi pour le premier poste (PC essai formation1) nous entrons :

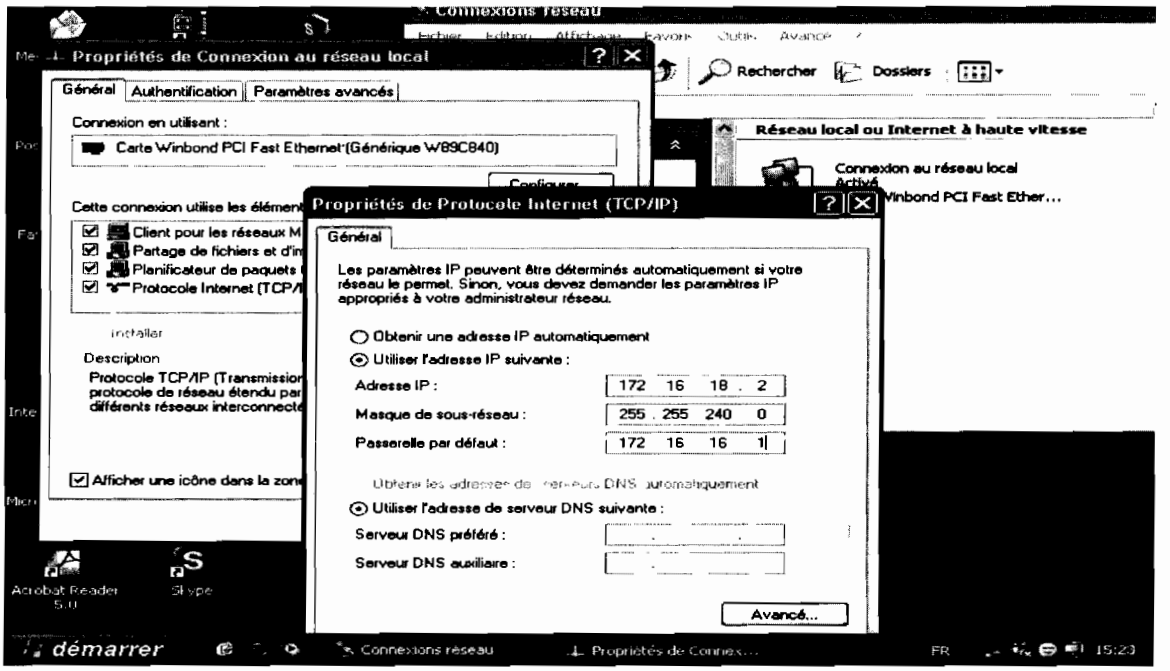
Adresse IP : 172.16.16.20
Masque de sous-réseau : 255.255.240.0
Passerelle par défaut : 172.16.16.1



configuration du premier poste appartenant au VLAN_FORM

De même nous entrons les valeurs pour le deuxième poste de travail (Pc essai formation2) ainsi qu'il suit :

Adresse IP : 172.16.18.2
Masque de sous-réseau : 255.255.240.0
Passerelle par défaut : 172.16.16.1



configuration du deuxième poste appartenant au VLAN FORM

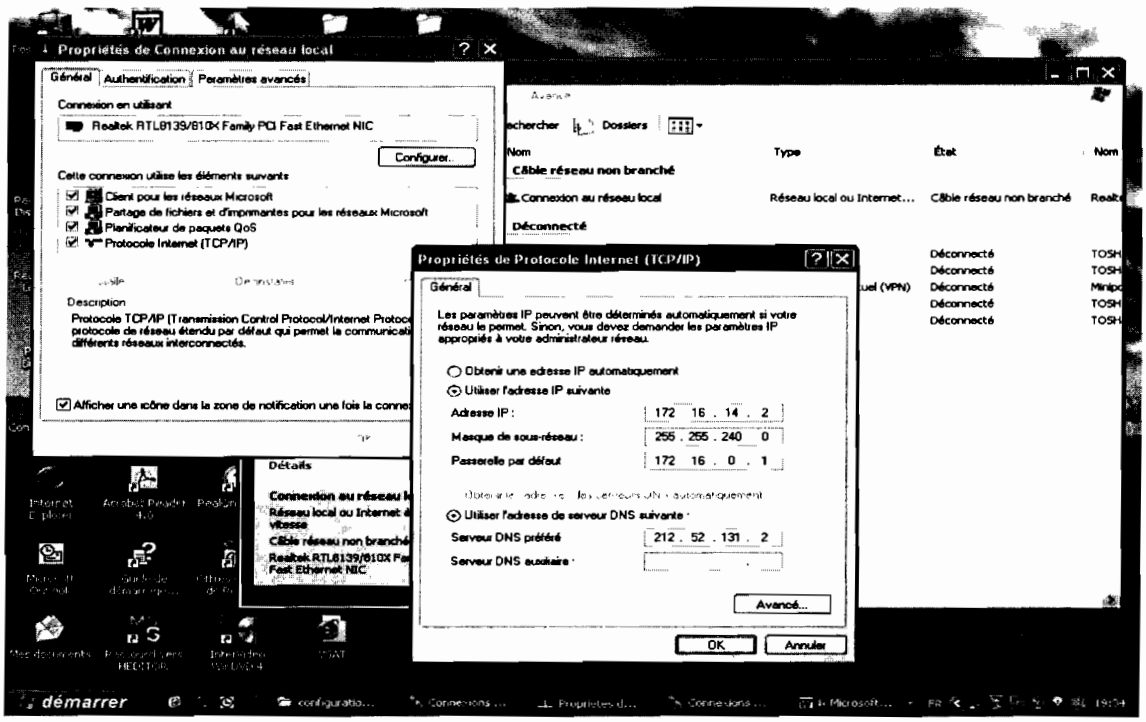
Nous constatons alors que les deux postes de travail se voient dans un groupe de travail, car appartenant au même VLAN (VLAN Formation).

Vue du réseau VLAN FORM

2) Postes de travail ne faisant pas partir du même VLAN

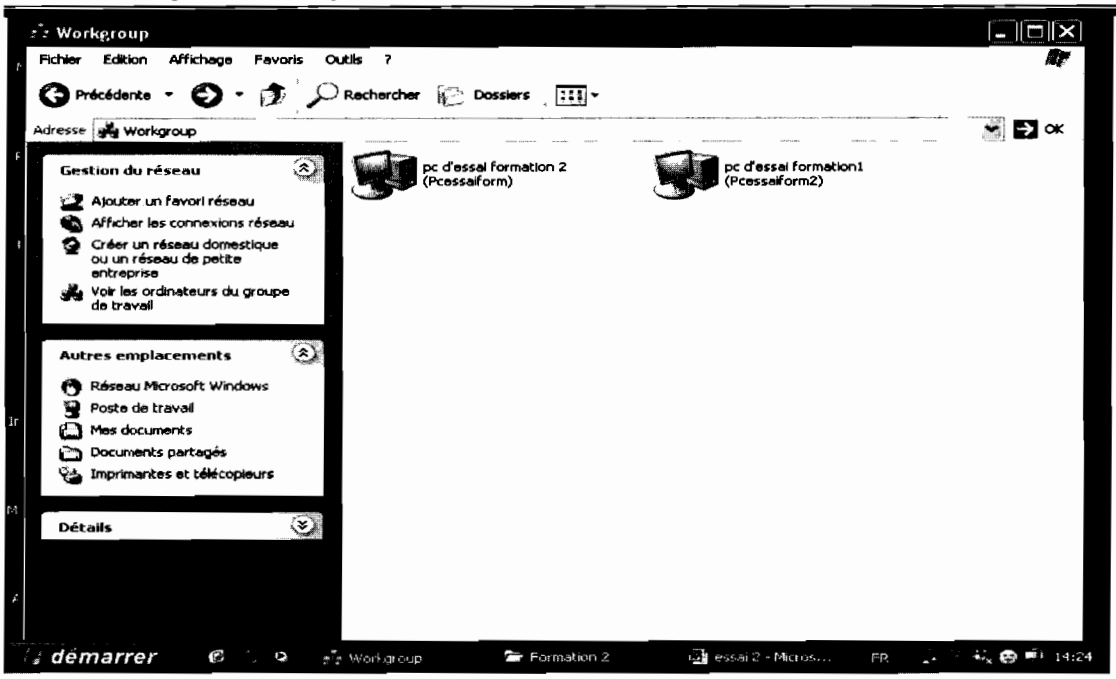
Nous connectons un poste de travail sur le port FastEthernet 0/5 (VLAN Staff) de Switchdessai. De plus nous configurons les adresses IP tel que correspondant à l'adressage des interfaces des VLANs définie sur les deux commutateurs. Ainsi nous entrons :

Adresse IP : 172.16.14.2
Masque de sous-réseau : 255.255.240.0
Passerelle par défaut : 172.16.0.1



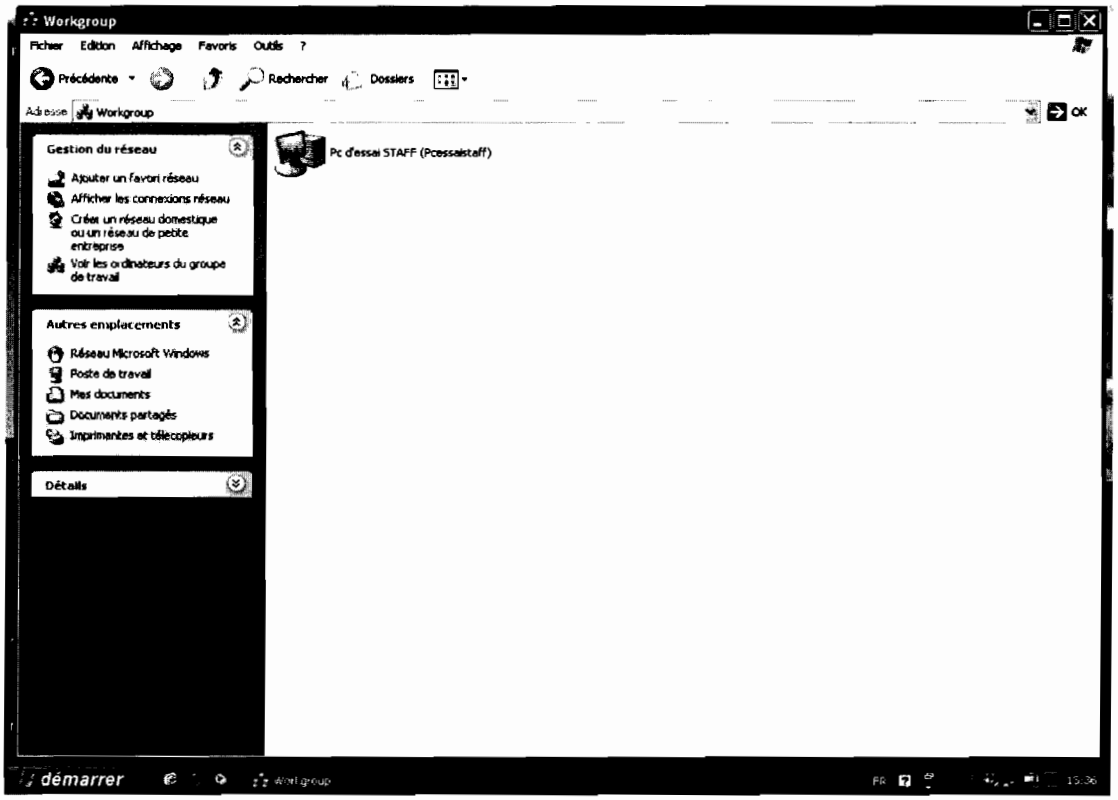
configuration d'un poste appartenant au VLAN STAFF

Nous constatons que d'une part Pc essai formation1 et Pc essai formation 2 du VLAN Formation se voient mais ne voient pas Pc essai staff du VLAN Staff.



vue du réseau VLAN_FORM

D'autre part, ce dernier se voit mais ne voit pas les deux autres.



vue du VLAN_STAFF

Ainsi configurés, les commutateurs permettent d'organiser les postes de travail en groupe logiques. La configuration statique par port des VLANs que nous avons effectué ne donne pas directement lieu à une appartenance au VLAN dès que le poste est branché sur un port donné. En effet le poste doit être préalablement configuré (adresse IP, Masque de sous-réseau, Passerelle par défaut) afin de répondre aux exigences provenant de l'association à chaque VLAN d'un interface adressé. Les services tel le DHCP, le DNS ... permettront d'effectuer ces différentes tâches et de rendre ainsi la configuration et le fonctionnement VLAN transparents à l'utilisateur. Mais dans tous les cas, ce n'est qu'à partir de partages effectués sur les fichiers ou dossier que l'utilisateur se rendra compte du profit qu'il peut tirer de cette forme d'organisation.

AVANTAGES ET INCONVENIENTS DE LA NOUVELLE ORGANISATION DU RESEAU

L'organisation en réseaux locaux virtuels du réseau de l'Université de Ouagadougou va nous permettre d'apporter un certain nombre d'éléments pouvant améliorer les besoins des utilisateurs. En effet, le futur réseau de l'université nous permettra:

- De réduire la diffusion de trafic au sein du réseau ;
- De créer des groupes de travail indépendamment de l'infrastructure physique de l'université ;
- De contrôler les échanges inter VLAN.

Les messages de diffusion seront limités à l'intérieur de chaque VLAN. Ainsi les broadcasts des serveurs du VLAN STAFF seront limités aux membres de l'administration. De plus les communications inter VLAN se réaliseront tout comme des échanges inter réseaux, c'est-à-dire à travers une mise en œuvre de filtrage des données.

Cependant, des insuffisances demeurent. En effet, l'un des principaux handicaps que pourrait connaître notre futur réseau serait une panne survenant sur le pare-feu (firewall).Toute la communication inter-VLAN se trouvera alors bloquée. Différentes insuffisances pourraient aussi menacer le bon fonctionnement du réseau :

- Une reconfiguration statique des commutateurs du réseau est nécessaire en cas de perte de configuration.
- Les échanges administratifs sur le réseau ne seront pas négligeables et ce, au détriment du débit utile : il faut en effet que les informations de VLAN soient échangées entre les commutateurs et vers le firewall pour la diffusion régulière des adresses MAC.
- Une impossibilité d'implémenter la solution du Spanning Tree car, il peut y avoir des problèmes dans la configuration de l'arbre lorsqu'une station sera déplacée d'un commutateur vers un autre du fait de la vaste étendue du réseau et du nombre de plus en plus croissant de commutateurs. On peut assister à des effets de bords dans ce cas.
- Un important effort de formation est requis pour une bonne connaissance des normes et du matériel utilisé en vue d'une utilisation et d'une bonne gestion du réseau.

Il faut cependant retenir qu'aucune solution n'a que des avantages. Seulement, on tentera toujours de réduire ces insuffisances tout en ne perdant pas de vue les objectifs à atteindre.

Perspectives

Avec les moyens dont nous disposons et grâce aux possibilités offertes par les techniques d'organisation aujourd'hui, nous pouvons suggérer un certain nombre d'éléments dans l'optique d'un développement du réseau de l'Université de Ouagadougou.

Utilisation de la liaison VSAT

L'exploitation à une échelle plus bénéfique de la liaison VSAT pourrait faire l'objet d'une étude. En effet, cette liaison pourrait être utilisée pour réaliser une certaine forme de redondance dans le réseau. Vue alors comme solution alternative, cela va consister à balancer la connexion vers cette liaison dans certaines circonstances telle que la survenance d'éventuelles perturbations pouvant affecter la liaison spécialisée (LS). Ce serait améliorer un élément dans l'élaboration de la sécurité, c'est-à-dire la disponibilité. Mais cela ne sous-entend pas que la liaison VSAT ne doit être utilisée qu'à cette fin.

Il est en effet envisageable d'effectuer une répartition de charge entre les deux liaisons quand tout fonctionne normalement. Pendant que certaines stations sont connectées sur la liaison spécialisée, d'autres vont plutôt utiliser la liaison VSAT. Mais dans tous les cas, ce n'est qu'au bout d'une réflexion bien menée sur les possibilités et sur la nécessité réelle de ces alternatives que l'on pourra dégager des choix.

Possibilités d'interconnexion

La notion de réseau local virtuel va de plus en plus au-delà du simple principe de domaine de diffusion. Dans un contexte de développement des réseaux, il permet une augmentation de taille des réseaux locaux (même sans utilisation de routeurs). Dans cette perspective d'élargissement du réseau local, nous pouvons suggérer la réalisation de l'interconnexion des différents réseaux des deux universités du BURKINA FASO (l'Université de Ouagadougou et l'Université polytechnique de Bobo).

Analyse et suggestions

1) De l'enseignement donné à l'Ecole Supérieure d'Informatique

L'enseignement donné à l'Ecole Supérieure d'Informatique est d'une bonne qualité mais connaît quelques insuffisances.

b) Le manque de matériel

Le matériel de travaux pratiques doit être en quantité suffisante et composé d'une gamme d'éléments assez diversifiée. Pour exemple, il est assez délicat de réussir des travaux pratiques de routage en réseau avec un seul routeur de disponible. De plus, ces matériels doivent être assez fréquemment renouvelés pour permettre aux étudiants d'être à niveau avec les exigences dues à l'évolution rapide de l'informatique. Si tel n'est pas le cas on aura beau mis l'accent sur la pratique, on formera des techniciens en déphasage avec les réalités du monde professionnel.

a) L'insuffisance de travaux pratiques

Une chose est de comprendre la théorie, une autre est de pouvoir la mettre en pratique. En effet, la formation d'un technicien ne saurait être complète si elle n'est suffisamment accompagnée de pratique. Les travaux pratiques doivent donc tenir une place prépondérante pas seulement dans le programme d'enseignement, mais aussi dans l'exécution proprement dite des cours, afin d'assurer l'opérationnalité du technicien à la fin du cursus.

2) Du stage

La réussite du stage dépend fortement de l'organisation qui le précède et de celle qui l'accompagne. Pour cela une amélioration doit être apportée à certains éléments.

a) La période de stage

Le stagiaire a non seulement besoin d'information mais de matériel de travail aussi. Ainsi, programmer les stages autour du mois d'Août (période du 15 Juillet au 15 Octobre généralement) fait naître des difficultés liées à la disponibilité des acteurs de l'entreprise, principale source d'information, qui sont alors en congés. Le stagiaire perd ainsi un temps précieux souvent compromettant pour la réussite du travail. Il serait donc nécessaire d'aménager les programmes afin que les stages puissent débuter plus tôt au grand bénéfice de tout un chacun.

b) Les conditions du stage

L'organisation n'est pas la seule clé de la réussite du stage. En effet, Ecole et entreprise pourraient trouver le moyen de mettre à la disposition du stagiaire des ressources pouvant favoriser la fourniture d'un bon rendement. Ces ressources peuvent se présenter sous deux formes. Primo, l'étudiant stagiaire pourrait bénéficier de ressources en nature (bons de navigation, blocs-notes, supports de stockage ...). Secundo, une contribution financière, aussi minimale soit-elle peut permettre au stagiaire de subvenir à ses besoins en matière de déplacement, hébergement, restauration ...Cet aspect est d'une grande importance, car il faut le souligner, le stage ne se limite pas au côté pédagogique mais s'étend aussi au social.

c) Le suivi du stage

Un suivi poussé du stage participe à sa réussite. La disposition des maîtres et superviseurs de stage, à l'écoute et aux conseils est si importante que leur choix doit être souvent guidé par leur niveau de disponibilité. De plus, leur désignation doit s'effectuer dans les meilleurs délais, si possible en même temps que le stagiaire rejoint sont lieu de stage, afin d'éviter quelque amalgame que ce soit.

En résumé, que ce soit au niveau de l'Ecole ou des structures d'accueil, des efforts doivent être menés. Des concertations régulières et une franche collaboration des deux parties sont souhaitables dans l'intérêt de tous, car centre de formation et entreprise ne sauraient se passer l'une de l'autre.

Conclusion

La Direction de la Promotion des Nouvelles Technologies de l'Information et de la Communication est la structure chargée de l'élaboration et de la gestion du réseau de l'Université de Ouagadougou. Trois mois durant, nous y avons effectué un séjour dans le cadre du renforcement des connaissances acquises depuis l'école et de la constitution d'un mémoire devant sanctionner le cycle. Pour cela, nous avons effectué des activités journalières entrant dans les assignations de la structure. Parallèlement, une étude suivie d'une analyse de l'existant nous a conduit à la formulation d'un plan d'organisation devant contribuer à mieux satisfaire les besoins des utilisateurs du réseau. La mise en œuvre de réseaux locaux virtuels au sein du réseau de l'Université de Ouagadougou, objet de cet apport a donc constitué le thème de notre étude que nous avons menée à travers la proposition de plan de réalisation et de la présentation d'une simulation. Ce stage à travers les diverses notions de maintenance et de réseau que nous avons eu à aborder durant tout ce travail, nous rend aujourd'hui plus compétents et plus aptes à affronter le monde professionnel. Les différentes suggestions que nous avons évoquées, une fois prises en compte, participeront à la consolidation de cette excellence dans la formation, prônée par l'ESI. Car former des Hommes pour un marché de l'informatique en pleine croissance est bien, mais fournir des techniciens très compétents serait l'idéal pour ce marché de plus en plus exigeant.

BIBLIOGRAPHIE

Titres	Auteur(s)	Date d'édition
La Secrétaire face à l'évolution de la bureautique et des NTIC	Mlle Touissida Ulda Jeannette TAPSOBA	Mars 2002
Formulation du plan par étape pour la sécurisation du réseau UONET	Romuald SAWADOGO Zacharie KOALAGA Adil BIKARBASS Andries RUITER Rik STIGTER Marc PETIT	21 Février 2004
Cisco IOS Desktop Switching Software Configuration Guide	Cisco System	
www.cisco.com	Cisco System	

ANNEXES

Annexe 1 ⟶ Organigramme de l'université de Ouagadougou

Annexe 1 ⟶ Organigramme de la DPNTIC

Annexe 3 ⟶ caractéristiques des routeurs de la gamme 2500 series

Annexe 4 ⟶ caractéristiques techniques des commutateurs 1900 series

Annexe 5 ⟶ caractéristiques techniques du pare-feu HP PROLIANT

ANNEXE 1

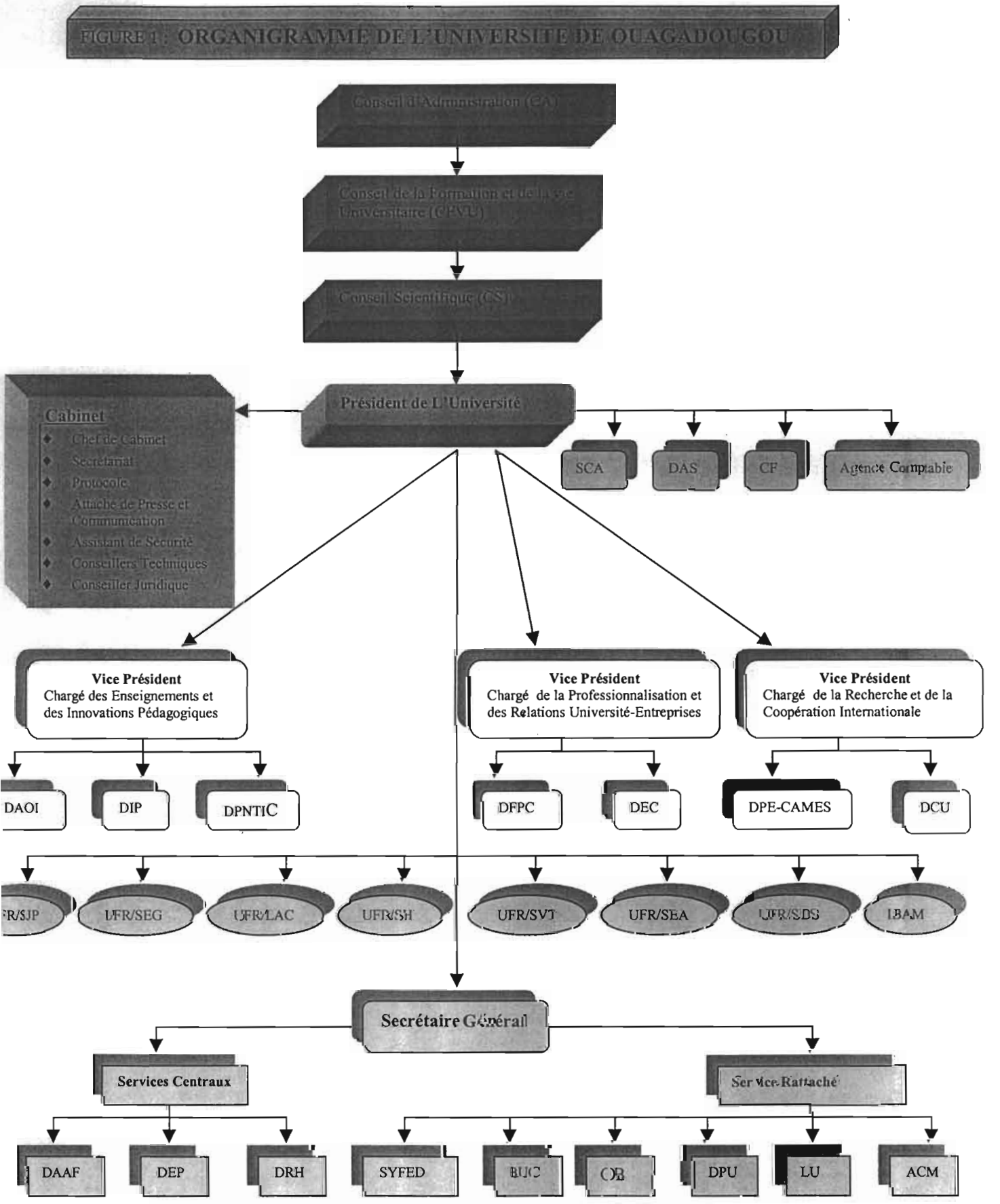
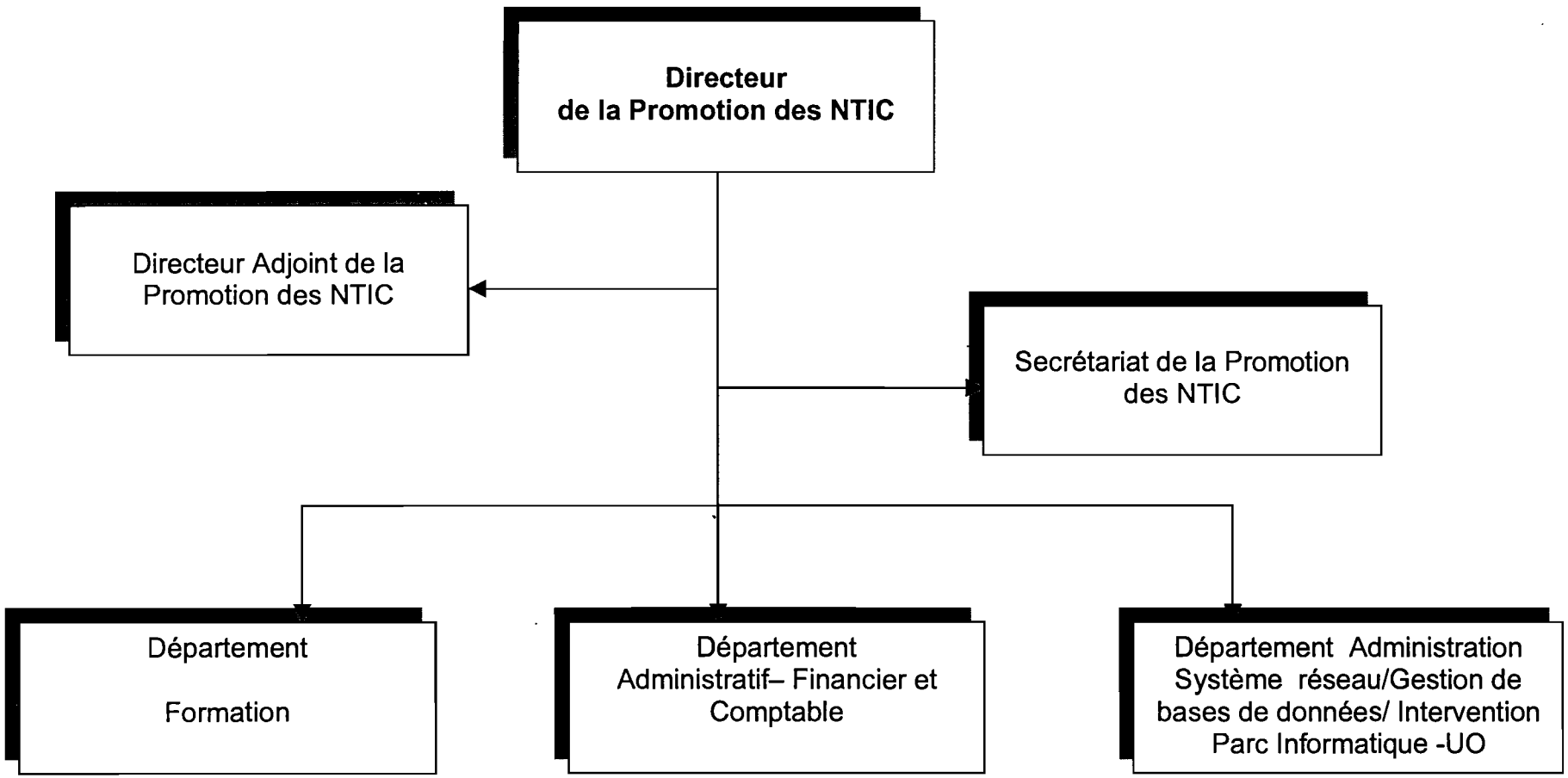


FIGURE 1 : ORGANIGRAMME DE L'UNIVERSITE DE OUAGADOUGOU
Conseil d'Administration (CA)
Conseil de la Formation et de la vie Universitaire (CFVU)
Conseil Scientifique (CS)
Président de L'Université
Cabinet
Chef de Cabinet
Secrétariat
Protocole
Attaché de Presse et Communication
Assistant de Sécurité
Conseillers Techniques
Conseiller Juridique
SCA
DAS
CF
Agence Comptable
Vice Président
Chargé des Enseignements et des Innovations Pédagogiques
Vice Président
Chargé de la Professionnalisation et des Relations Université-Entreprises
Vice Président
Chargé de la Recherche et de la Coopération Internationale
DAOI
DIP
DPNTIC
DFPC
DEC
DPE-CAMES
DCU
UFR/SJP
UFR/SEG
UFR/LAC
UFR/SH
UFR/SVT
UFR/SEA
UFR/SDS
IBAM
Secrétaire Général
Services Centraux
Service Rattaché
DAAF
DEP
DRH
SYFED
BUC
OB
DPU
LU
ACM

ANNEXE 2


Directeur
de la Promotion des NTIC
Directeur Adjoint de la Promotion des NTIC
Secrétariat de la Promotion des NTIC
Département
Formation
Département Administratif– Financier et Comptable
Département Administration Système réseau/Gestion de bases de données/ Intervention Parc Informatique -UO

ANNEXE 3

Overview of the Cisco 2500 Series Access Server

The Cisco 2500 series access server is a full-featured communication server with multiprotocol routing capability between synchronous serial, LAN, and asynchronous serial ports.The Cisco 2500 series access server is available in four models, as follows:

Access Server Hardware Features

The access server has the following hardware features:

- 8 or 16 ports for connection to modems, terminals, or other asynchronous (EIA/TIA-232) equipment
- 2 MB to 16 MB (depending on the selected feature set) of primary memory, using dynamic random-access memory (DRAM) single in-line memory modules (SIMMs)
- 32-KB nonvolatile random-access memory (NVRAM) to store configurations
- 4-MB to 8-MB Flash memory for running the Cisco Internetwork Operating System (Cisco IOS) image
- 2-MB shared packet memory
- Two synchronous serial ports for connection to a WAN
- EIA/TIA-232 console port for connection of a console terminal
- EIA/TIA-232 auxiliary port for connection of a terminal or modem

Note EIA/TIA-232 and EIA/TIA-449 were known as recommended standards RS-232 and RS-449 before their acceptance as standards by the Electronic Industries Association (EIA) and Telecommunications Industry Association (TIA).

The serial WAN connections use a proprietary, 60-pin connector. The Ethernet and Token Ring connections use standard LAN cabling with an attachment unit interface (AUI) or DB-9 connector.

The console terminal is used to provide basic and emergency local system access. The auxiliary port is used to provide basic and emergency remote system access.

Table of Contents
Technical Specifications

Technical Specifications

This appendix provides the technical specifications and regulatory agency approvals (see Table A-1) for the switch.

Table A-1: Technical Specifications

Environmental Operating Ranges	
Operating temperature	23 to 113°F (-5 to 45°C)
Storage temperature	-13 to 158°F (-25 to 70°C)
Operating humidity	10 to 85% (noncondensing)
Operating altitude	Up to 9842 ft (3000 m)
Power Requirements	
AC input voltage	100 to 127/200 to 240 VAC (autoranging) 50 to 60 Hz
DC input voltage	+5V_ @6A, ±12V _@1A
Power consumption	50W
Physical Dimensions	
Weight	7 lb (3.2 kg)
Dimensions (H x W x D)	1.73 x 17.5 x 8.25 in. (4.4 x 44.5 x 21 cm)
Agency Approvals	
Safety	**EMI**
AS/NZS 3260, TS001	FCC Part 15 Class A
UL 1950/CSA 22.2 No. 950	EN 55022A Class A (CISPR 22 Class A)
IEC 950/EN 60950	VCCI Class A
NOM 019	AS/NRZ 3548 Class A

ANNEXE 5

ProLiant DL320 G2
Overview & Features

Overview

The DL320 G2 is designed with all the performance a fast paced, fast growing front-end and single-function applications demands in a 1U server. The 1U size and the 1-way processor capability provide the customers with a low cost, rack-optimized solution for single function and front-end applications.

The performance features include the Intel Pentium 4 processor, with a 533MHz Front Side Bus (FSB) and 512K cache, standard 128MB PC2100, 266MHz ECC DDR SDRAM DIMMs expandable for 4GB for future investment protection, 64-bit PCI slot offers twice the bandwidth of 32-bit PCI for enhanced data transfer rates, two integrated Fast Ethernet 10/100/1000 controllers for flexible network connectivity, two ATA or SCSI hard drive bays for internal data storage, ATA RAID 0 or 1 for data protection and availability of servers.

What's new

Announcing the ProLiant DL320 Firewall/VPN/Cache Server with Microsoft ISA Server 2004

latest performance technologies

- 3.06GHz Intel Pentium 4 with 512K cache with Hyper-Threading technology
- ServerWorks GC-SL chipset, with a 533MHz FSB
- Up to 4GB 266MHz DDR
- 2 BroadCom Gbit NICs

flexibility features

- One 64-bit/33MHz PCI expansion slot
- ATA/100 supporting RAID 1 or 0
- SCSI available with optional slot-less daughter card
- Redundant ROMs
- Removable CD-ROM/Diskette drive assembly
- Optional DVD-ROM/Diskette drive assembly

server-class uptime and manageability

- Optional RILOE II functionality
- SmartStart & HP Insight Manager
- 3 year next business day, on-site limited warranty

Specs at a glance