BURKINA FASO
UNITE – PROGRES – JUSTICE

MINISTERE DES ENSEIGNEMENTS SECONDAIRE ET SUPERIEUR
(MESS)

UNIVERSITE POLYTECHNIQUE DE BOBO – DIOULASSO
(UPB)

ECOLE SUPERIEURE D'INFORMATIQUE
(ESI)

Sadouanouan MALO

MEMOIRE DE FIN DE CYCLE

en vue de l'obtention du

DIPLOME D'INGENIEUR DE CONCEPTION EN INFORMATIQUE

Thème :

AMELIORATION DE L'ARCHITECTURE DU RESEAU INFORMATIQUE DU SIEGE DE LA SOFITEX

Présenté par :

Abdoul Karim TRAORE & Ousmane SOUABO

Maitre de stage
M. Marc NAKANNABO
Chef du SIRT à la SOFITEX

Directeur de mémoire
Dr Sadouanouan MALO
Enseignant à l'E.S.I

A nos parents,

dont nous sommes le résultat de tant de sacrifices

!!!

REMERCIEMENTS

Nous tenons à remercier toute l'équipe pédagogique de l'Ecole Supérieure d'Informatique ainsi que les intervenants professionnels pour l'accompagnement et la formation reçus tout au long de notre cursus.

Nous remercions la Société Burkinabè des Fibres Textiles (SOFITEX) pour nous avoir donné l'opportunité de consolider nos connaissances théoriques acquises à l'Ecole. Nous remercions également tout le personnel de ladite société pour leur disponibilité et l'accueil chaleureux qu'il nous a témoigné à notre arrivée dans la structure.

Nous remercions particulièrement M. Marc NAKANNABO notre maître de stage pour son soutien, son accompagnement durant notre séjour à la SOFITEX.

Nous remercions particulièrement M. Yacouba OUATTARA le chef de la section infrastructure réseaux pour son soutien, ses conseils, sa disponibilité et son accompagnement pour l'élaboration de ce document.

Nous remercions Dr Sadouanouan MALO, notre superviseur pour son entière disponibilité à répondre à nos préoccupations, ainsi que pour ses conseils pour nous aider à mener à bien notre étude.

Nous tenons également à remercier nos parents, tuteurs et aussi les personnes qui d'une manière ou d'une autre ont contribué à notre formation et à la réussite de ce stage.

Que chacun trouve ici un motif de satisfaction et puisse DIEU tout puissant rendre à chacun au centuple ses bienfaits.

SOMMAIRE

REMERCIEMENTS ..... **II**

SIGLES ET ABREVIATIONS ..... **IV**

LISTE DES TABLEAUX ..... **VII**

LISTE DES FIGURES ..... **VIII**

AVANT-PROPOS ..... **IX**

INTRODUCTION **1**

PREMIERE PARTIE : CONTEXTE ET ENVIRONNEMENT D'ETUDE **2**

CHAPITRE 1 : PRESENTATION DE LA STRUCTURE D'ACCUEIL **3**

CHAPITRE 2 : PROBLEMATIQUE ET CAHIER DE CHARGES **7**

CHAPITRE 3 : ETUDE DU RESEAU LOCAL DE BOBO-DIOULASSO **10**

DEUXIEME PARTIE : ETUDE TECHNIQUE **22**

CHAPITRE 1 : ETUDE PREALABLE ET CHOIX TECHNIQUES **23**

CHAPITRE 2 : ETUDE DETAILLEE DE LA SOLUTION RETENUE **35**

CHAPITRE 3 : IMPLEMENTATION DE LA SOLUTION **53**

CONCLUSION **80**

REFERENCES BIBLIOGRAPHIQUES **81**

ANNEXES **83**

SIGLES ET ABREVIATIONS

SIGLES	DEFINITIONS
ADSL	Asymmetric Digital Subscriber Line
AIC	Application Intégrée Coton
API	Application Programming Interface
BID	Bridge ID
BLR	Boucle Locale Radio
BPDU	Bridge Path Data Unit
CGI	Common Gateway Interface
CICI	Cycle des Ingénieurs de Conception en Informatique
CITI	Cycle des Ingénieurs de Travaux en Informatique
CMGS	Compta Matière et Gestion des Stocks
CSMA/CD	Carrier Sense Multiple Acces with Collision Detection
DEEP	Direction des Etudes Economiques et de la Prospective
DHCP	Dynamic Host Configuration Protocol
DI	Direction Industrielle
DICA	Direction des Intrants et du Crédit Agricole
DMZ	DeMilitarized Zone
DNS	Domain Name System
DTL	Direction du Transport et de la Logistique
ESI	Ecole Supérieure d'Informatique
FDDI	Fiber Distributed Data Interface
FO	Fibre Optique
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GHz	Giga Hertz
GL	Garage Lourd
GVRP	Generic VLAN Registration Protocol

LISTE DES TABLEAUX

Tableau 1 : Tableau récapitulatif des équipements actifs du réseau 14
Tableau 2 : Présentation des différents serveurs physiques et virtuels 18
Tableau 3 : Les applications métiers utilisées à la SOFITEX 19
Tableau 4 : Comparaison des topologies physiques 24
Tableau 5 : Comparaison des supports de transmission utilisés pour l'interconnexion 25
Tableau 6 : Avantages et inconvénients entre sous réseautage et VLAN 30
Tableau 7 : comparaison des outils de supervision 34
Tableau 8 : Caractéristiques du WiMax 38
Tableau 9 : Valeur par défaut du cout des ports 44
Tableau 10 : Coût financier de la mise en œuvre 77
Tableau 11 : coût d'amortissement annuel des équipements actifs de la mise en œuvre 79

LISTE DES FIGURES

Figure 1 : Organigramme fonctionnel du SIRT 3
Figure 2 : Chronogramme prévisionnel du projet 9
Figure 3 : Architecture d'interconnexion 10
Figure 4 : Présentation des locaux du site de Bobo-Dioulasso 12
Figure 5 : Architecture simplifiée du réseau de Bobo-Dioulasso 15
Figure 6 : Architecture du réseau existant de Bobo-Dioulasso 16
Figure 7 : Architecture hiérarchisée en trois couches [13] 35
Figure 8 : Exemple de rôles des ports dans une topologie [13] 42
Figure 9 : L'architecture de Nagios [18] 50
Figure 10 : Supervision active [18] 51
Figure 11 : Supervision passive [18] 51
Figure 12 : Chronogramme de déploiement prévisionnel. 54
Figure 13 : Architecture hiérarchisée en trois couches 56
Figure 14 : Architecture physique du réseau 57
Figure 15 : réseau de simulation 68
Figure 16 : configuration du serveur mail 75
Figure 17 : Configuration du mail sur un PC client 76
Figure 18 : Envoi d'un mail 76
Figure 19 : Réception d'un mail 77
Figure 20 : Monitoring Engine information 85
Figure 21 : Admin information 86
Figure 22 : Informations de la base de données 86
Figure 23 : Création des bases de données 87
Figure 24 : Suite de la création de la base de données 87
Figure 25 : Fin de l'installation 88

AVANT-PROPOS

L'Ecole Supérieure d'Informatique (ESI), créée en Septembre 1990 au sein de l'Université de Ouagadougou et implantée par la suite sur le site de l'Université Polytechnique de Bobo-Dioulasso, offre des formations pour le premier et le second cycle en informatique.

Le premier cycle a pour objectif de former des cadres moyens opérationnels et évolutifs aptes à participer efficacement à la conception, à la réalisation et à la maintenance d'applications informatiques. La fin de ce cycle de formation est sanctionnée par le grade de licence en informatique correspondant à l'ancien diplôme de fin de cycle des ingénieurs de travaux en informatique (CITI). Deux options y sont offertes : l'option « Ingénierie des réseaux et systèmes », et l'option « Ingénierie des systèmes d'information ».

Le second cycle correspond au cycle des ingénieurs de conception en informatique (CICI) qui n'est encore pas organisé selon le système LMD. Il permet à des étudiants recrutés avec un diplôme d'informatique de niveau BAC+3 d'atteindre le niveau BAC+5 en informatique avec un large éventail de compétences leur permettant de conduire des projets de conception et de réalisation de systèmes d'informations informatisés complexes.

Pour imprégner ses futurs ingénieurs à la réalité du terrain et à la vie professionnelle, l'E.S.I intègre dans leur formation des stages obligatoires à effectuer au sein d'une entreprise. C'est dans ce contexte que nous avons été reçus du 1er Octobre 2013 au 31 mars 2014 au sein de la Société Burkinabè des Fibres Textiles (SOFITEX).

PREMIERE PARTIE : CONTEXTE ET ENVIRONNEMENT D'ETUDE

Chapitre 1 : Présentation de la structure d'accueil

La Société Burkinabè des Fibres Textiles SOFITEX [4] est une société anonyme créée le 20 juin 1979 avec un capital de 19.528.000.000 F CFA. Ses principales activités sont la commercialisation de la fibre et de la graine de coton, l'appui conseil aux producteurs, l'achat, le transport et l'égrenage du coton. Basée à Bobo-Dioulasso, elle comporte plusieurs départements dont le Service Informatique Réseaux et Télécommunications (SIRT) où nous avons effectué notre stage sur le thème : « **Optimisation de l'architecture du réseau informatique du siège de la SOFITEX** » que nous allons décrire dans les lignes qui suivent.

I. Organisation et fonctionnement du SIRT

Le projet réseaux informatiques a été créé en 2004 avec la mise en place de l'intranet dans tous les sites de la SOFITEX. C'est dans ce cadre que le service SIRT a été mis en place à côté du Service Informatique et Exploitation (SIE) en 2010 afin de gérer l'importance des réseaux, le besoin croissant en communication, le partage des informations (interne et externe) et s'approprier des TIC dans les tâches quotidiennes. Pour mener à bien ses activités, le SIRT se compose d'un Service Réseaux et Télécommunications, d'une Section Intranet et Promotion des T.I.C, d'une Section Télécommunication et Support utilisateur, d'une Section Infrastructure Réseaux et d'une Section Maintenance préventive (cf. Figure 1).

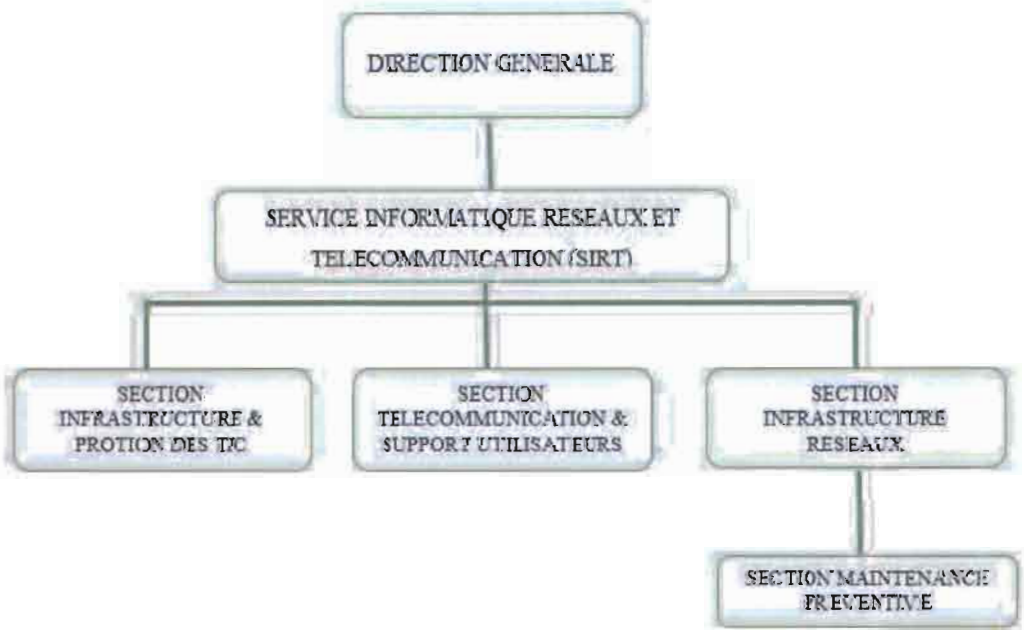

Figure 1 : Organigramme fonctionnel du SIRT

Le SIRT dans sa quête d'offrir le meilleur service réseau que l'on puisse avoir, supervise et veille à la bonne marche du réseau en place. A cet effet, il a à sa charge la gestion des incidents sur les différents sites, la gestion de l'infrastructure réseau et met à la disposition du SIE les ressources nécessaires pour son bon fonctionnement. Sur les sites distants, le SIRT est appuyé par les correspondants informatiques dont les activités principales sont la surveillance des réseaux et des serveurs du site, la gestion des consommables informatiques du site, la gestion administrative, la gestion des incidents, le support aux utilisateurs, l'appui du service dans la gestion du parc informatique et enfin servir d'interface entre le SIRT et les utilisateurs dans les sites décentralisés.

II. Missions et activités

1. Les missions du SIRT

L'objectif stratégique assigné lors de la création du SIRT est la mise en place, la surveillance et l'expansion d'un réseau Intranet et Internet performant. De cet objectif ont été définies les missions portant sur les réseaux informatiques et télécommunication, la gestion du parc informatique et enfin la protection des TIC.

Au titre des réseaux informatiques et télécommunication, il s'agit **:**

- de maintenir opérationnels les réseaux intranet, extranet et internet de la SOFITEX et de veiller à ce qu'ils soient accessibles à partir de tous les postes de travail de l'entreprise ;
- de fournir des services réseaux efficients et alignés sur les objectifs stratégiques de la Direction ;
- d'intégrer progressivement les télécommunications au réseau informatique pour aboutir à terme à la communication unifiée.

Au titre de la gestion du parc informatique, il faut :

- s'assurer que les postes de travail où l'outil informatique indispensable pour leur activité soient dotés de ressources matérielles nécessaires ;
- gérer le parc informatique en respectant le cycle de vie des équipements informatiques et télécommunications ;
- veiller à une meilleure productivité des utilisateurs de l'outil informatique dans leurs activités quotidiennes par des renforcements de capacité.

Au titre de la promotion des TIC il s'agit :

- de conseiller et d'assister les décideurs dans les usages et l'intégration des TIC dans les processus métiers de l'entreprise ;
- d'accompagner les utilisateurs dans l'appropriation des TIC dans l'exécution de leurs tâches quotidiennes ;

2. Les activités du SIRT

Le SIRT assiste les utilisateurs au niveau des applications, des systèmes d'exploitation, du matériel informatique et des réseaux courant fort et courant faible.

Les activités du service informatique réseaux et télécommunications sont reparties dans chacune des trois sections qui les composent.

Dans la **section Intranet et Promotion des TIC,** il s'agit :

- d'assurer l'administration, la maintenance et l'audit de l'intranet, l'extranet et l'internet de la SOFITEX ;
- de planifier, de mettre en œuvre et de maintenir le niveau de la sécurité des réseaux informatiques en conformité avec la politique sécuritaire de l'entreprise, de gérer les accès des utilisateurs aux différentes ressources intranet, extranet et internet ;
- de gérer tous les incidents et problèmes liés aux prestations intranet, extranet et internet, de tenir à jour une base des incidents et des problèmes et de capitaliser sur les solutions de contournement en vue de la mise en place d'une base de connaissances ;
- de participer aux études d'avant-projet pour l'introduction de nouveaux services TIC à la SOFITEX, d'organiser et de réaliser des études sur l'impact des TIC sur les activités de l'entreprise.

Dans la **section Télécommunication et Support utilisateur**, il faut **:**

- gérer tous les incidents et problèmes liés à l'exploitation des réseaux distants, tenir à jour une base des incidents et des problèmes et capitaliser sur les solutions de contournement en vue de la mise en place d'une base de connaissance ;
- assurer le suivi de toutes les liaisons de communication (réseaux distants) installées, assurer en collaboration avec l'ONATEL-SA la maintenance préventive et curative des liaisons spécialisées louées ;
- planifier et mettre en œuvre une politique de sauvegarde efficiente des serveurs de la SOFITEX ;

- gérer la capacité des réseaux distants en s'assurant que les réseaux d'interconnexion sont à même de supporter les besoins de communication et d'échange actuels et futurs des Directions et des applications métiers de la SOFITEX.

Dans la **Section Infrastructure Réseaux,** il s'agit **:**

- d'assurer ou de coordonner la maintenance préventive et curative du matériel informatique installé et exploité à la SOFITEX (ordinateurs, imprimantes, onduleurs, …) ;
- d'assister les utilisateurs en cas de panne et d'assurer le déplacement, le remplacement ou l'installation de tout matériel informatique ;
- d'assurer une première assistance aux utilisateurs et remonter au chef de section les incidents non résolus et les besoins exprimés par les utilisateurs.
- de veiller au bon fonctionnement des réseaux locaux installés dans tous les sites SOFITEX, en assurant une maintenance préventive et curative efficiente ;
- d'assurer en collaboration avec l'ONATEL le suivi et la maintenance de la liaison fibre optique louée pour l'interconnexion du Siège à la Zone Industrielle et à Bobo3. Tenir à jour un registre des pannes et incidents sur cette liaison ;
- de gérer la capacité des réseaux locaux en s'assurant que les réseaux sont à même de supporter les contraintes actuelles et futures des logiciels réseaux et applications métiers de la SOFITEX ;
- d'assurer ou de participer à la configuration et au déploiement physique de tout nouveau matériel informatique acquis par la SOFITEX, de faire des propositions pour l'acquisition de nouveaux matériels pour les postes de travail dont l'outil informatique est requis pour mener à bien leur activité ;
- d'assurer la gestion du parc informatique, de maintenir à jour un inventaire physique du matériel informatique (en exploitation, en panne, hors service) par site, direction et service, et s'assurer de la couverture par l'assurance de tout matériel informatique en exploitation à la SOFITEX ;
- de gérer tous les incidents et problèmes liés à l'exploitation des réseaux locaux en tenant à jour une base des incidents et des problèmes et en capitalisant sur les solutions de contournement en vue de la mise en place d'une base de connaissances.

Chapitre 2 : Problématique et cahier de charges

I. Problématique

En place depuis 2004, le réseau informatique est devenu incontournable à la SOFITEX. Cet état se traduit par l'appropriation des TIC par les utilisateurs dans l'accomplissement de leurs tâches quotidiennes. Ainsi l'utilisation de la messagerie, les recherches d'informations sur internet et la mise en œuvre future de l'Application Intégrée Coton prenant en charge toute la chaîne métier du coton ne fait que renforcer le caractère stratégique des réseaux dans l'activité de ladite société.

Cependant la non maitrise de l'étendue du réseau actuel engendre un domaine de collision très vaste et provoque une certaine lenteur du réseau. En effet, le SIRT est quelquefois alerté par des utilisateurs sur notamment des temps de réponse de plus en plus longs des applications réseaux en fonctionnement ou encore des difficultés d'accès aux serveurs. Outre ces différents incidents remontés par les utilisateurs, le SIRT est confronté au manque de documentation à jour du réseau, à l'absence d'outil de supervision du réseau et à la non maitrise de la couche basse. Dans un tel contexte, comment assurer la fluidité du trafic du réseau actuel ? Comment combiner les ambitions futures de la SOFITEX avec ce réseau actuel? Ou encore comment maitriser la couche basse du réseau ? Ce sont autant de questions auxquelles il nous est demandé d'apporter des éléments de réponse.

II. Cahier de charges

L'optimisation de l'architecture du réseau informatique du siège de la SOFITEX devra à terme permettre :

- de faire une étude du réseau en faisant ressortir son impact sur l'activité de la SOFITEX.
- d'étudier le réseau actuel et d'identifier les mises à jour nécessaires ;
- d'identifier les points faibles de l'architecture actuelle et faire ressortir les conséquences sur le réseau ;
- de proposer une nouvelle architecture réseau pour le siège à même de répondre aux besoins actuels et futurs ;

- de proposer à la SOFITEX des outils efficaces d'administration du réseau informatique.
- de proposer une mise à jour de la documentation du réseau ;
- de proposer un planning et un budget estimatif de la mise en œuvre de la solution retenue.

III. Démarche à suivre

Pour mener à bien cette mission d'optimisation qui nous a été confiée nous allons, vu la taille du réseau, réfléchir sur la solution au siège tout en ayant une vision globale du réseau de la SOFITEX. En matière de solutions nous allons procéder par une approche en couche. Ainsi, au niveau physique, il s'agira de trouver des solutions pour assurer aussi bien la disponibilité, la fiabilité que la fluidité du réseau. Au niveau logique, il s'agira d'assurer une meilleure circulation des paquets sur le réseau tout en sécurisant ces différentes transactions.

S'échelonnant sur une période de 25 semaines à compter du 16 octobre 2013, les différentes étapes de la réalisation du projet soumis à notre étude sont représentées sur un diagramme du nom de Gantt (cf. Figure 2) permettant ainsi de visualiser simplement toutes les tâches à mener suivant un chronogramme bien établi.

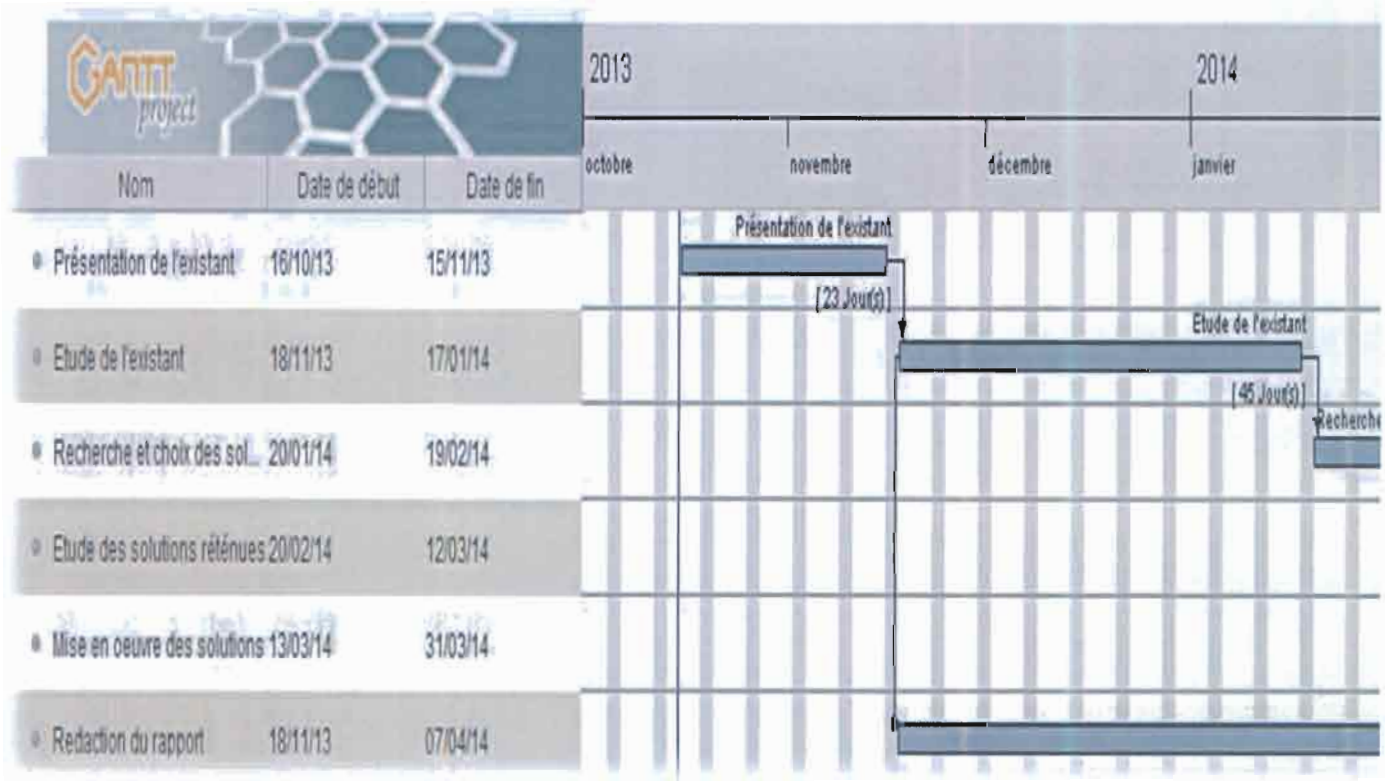

Figure 2 : Chronogramme prévisionnel du projet

Du 16 octobre 2013 au 15 novembre 2013, nous allons effectuer la visite des locaux de la SOFITEX, des interviews des utilisateurs du réseau afin d'établir le squelette du réseau existant, ensuite nous étudions ce réseau pour déceler les différents problèmes sur ce réseau. Ce travail sera effectué du 16 novembre 2013 au 15 janvier 2014. Après avoir mis la main sur les problèmes, nous allons faire sur une recherche sur les solutions possibles de résolution de ces problèmes qui sera fait du 20 janvier 2014 au 19 février 2014. Ainsi du 20 février au 12 mars 2014, après avoir étudié ces solutions, nous allons faire le choix des solutions appropriées et du 13 au 31 mars nous ferions la mise en œuvre de ces solutions. Notons que la rédaction du rapport sera faite en parallèle du 18 novembre 2013 au 07 avril 2014.

Chapitre 3 : Etude du réseau local de Bobo-Dioulasso

La SOFITEX dispose d'un vaste réseau informatique qui s'étend sur toutes les localités où la société mène une activité. Les 11 sites distants issus du découpage de la SOFITEX en régions cotonnières sont interconnectés par VPN à la salle technique principale située à Bobo-Dioulasso. La figure 3 nous montre comment est effectuée l'interconnexion des sites distants.

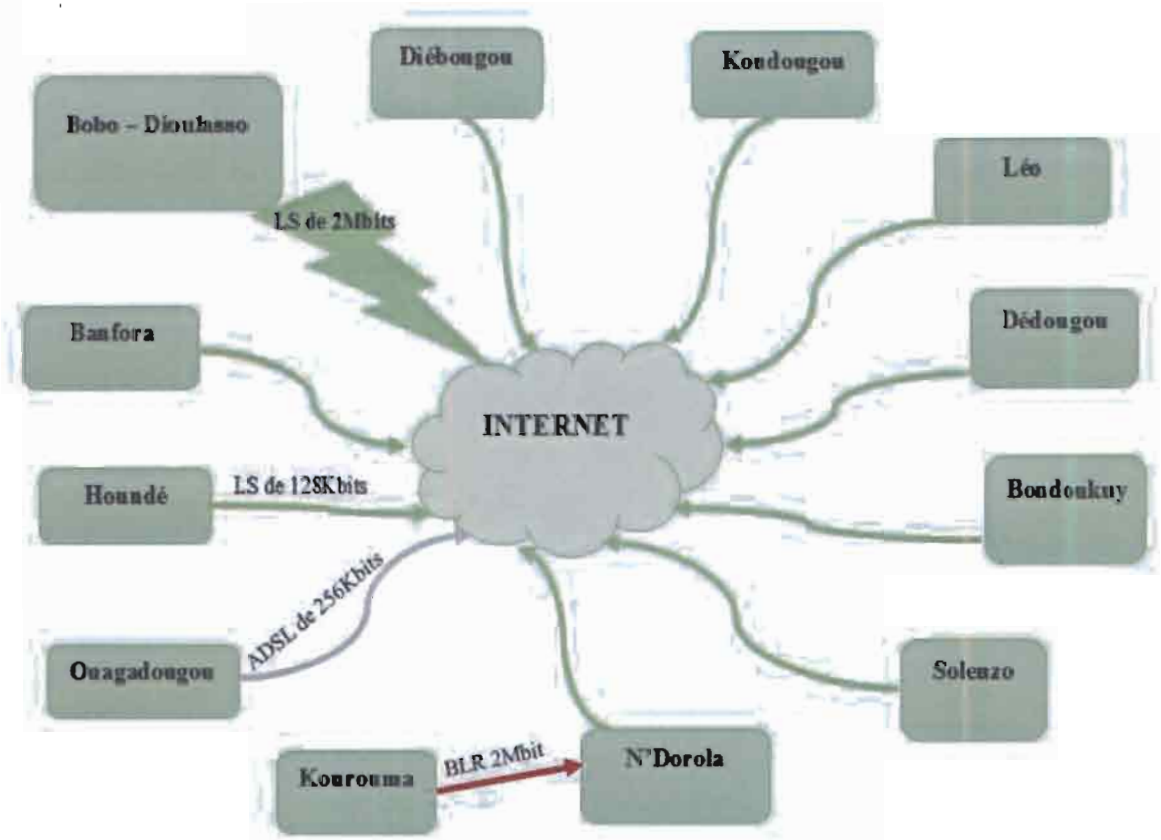

Figure 3 : Architecture d'interconnexion

Dans le cadre de notre étude, nous nous limiterons uniquement au réseau local de Bobo-Dioulasso.

Cette étude de l'existant aura pour objet de présenter le réseau existant et de mettre en exergue les problèmes de ce réseau.

I. Présentation de l'existant

1. Topologie physique

Le réseau de Bobo-Dioulasso est reparti en deux zones : le centre-ville et la zone industrielle.

Au niveau du centre-ville, ce réseau existe dans les locaux de la Direction Générale, de l'immeuble KAMBOU et la DEP distant respectivement d'environ 100 m et 1500 m. Au niveau de la zone industrielle, il est présent à la DICA, CMGS, Bobo I, DI, DTL, Bobo II, Garage Lourd, SOPAGRI et Bobo III qui est le point le plus éloigné de la Direction Générale avec une distance d'environ 4,1 Km à vol d'oiseau.

Tous ses locaux de Bobo-Dioulasso sont interconnectés et forment un réseau local unique. L'infrastructure système de ce réseau se trouve à la Direction Générale, ce qui en fait un noeud très important pour le réseau de Bobo-Dioulasso. Une liaison spécialisée de 2 Mbit est utilisée pour connecter le réseau de Bobo-Dioulasso à internet.

La figure 4 ci-dessous nous montre la disposition des différents locaux constituant le réseau de bobo.

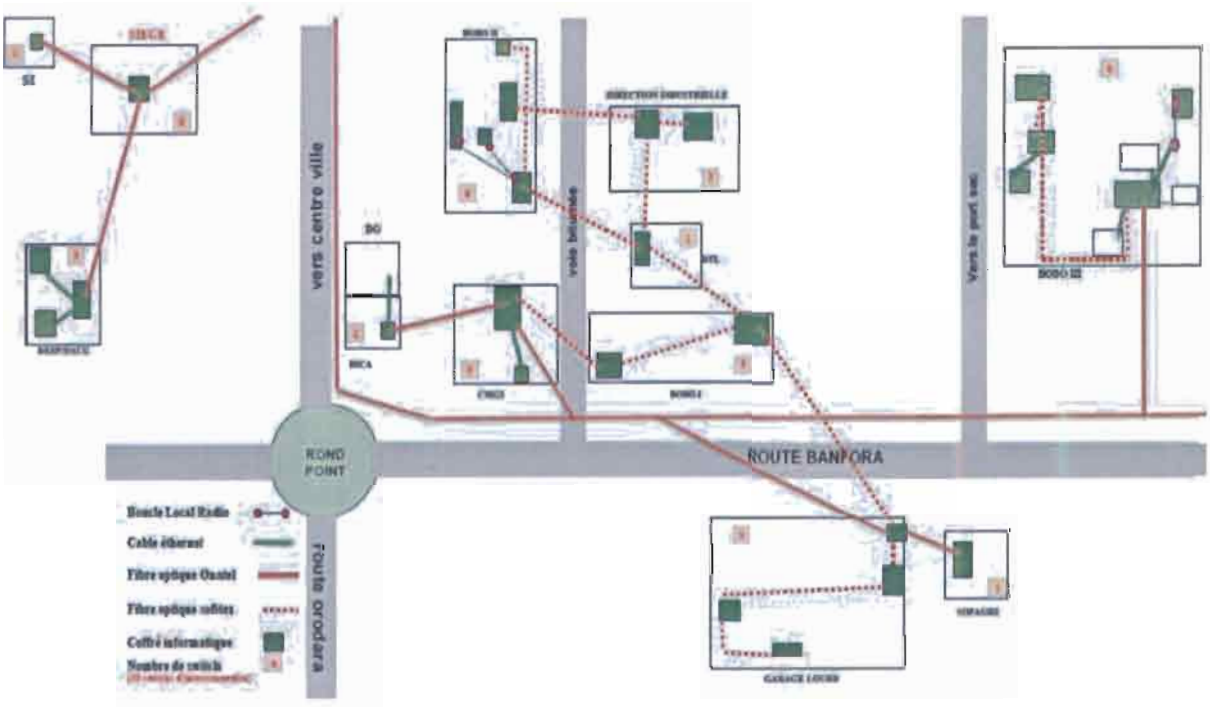

Figure 4 : Présentation des locaux du site de Bobo-Dioulasso

1.1. Le câblage réseau de la Direction Générale

Située en plein centre-ville, la Direction Générale de la SOFITEX est un bâtiment R+3 avec 171 prises Ethernet. À l'instar de tous les locaux, le câble utilisé est de Catégorie 6 UTP et les équipements d'interconnexion sont de la gamme CISCO. Ces équipements sont branchés en cascade sur ce vaste.

Pour chaque poste de travail sont prévues deux (02) prises dont une pour les données et la seconde pour la voix. A ce jour, seul les prises pour les données sont employées.

A chaque niveau du bâtiment de la Direction Générale, il y'a un coffret informatique relié au local technique principal qui se trouve au R+1 et qui héberge l'ensemble des serveurs, deux (02) switch 2950 pour le brassage des prises Ethernet du niveau R+1, un (01) switch concentrateur 3500 et un (01) routeur 2900 utilisé pour la connexion internet.

Sur le switch 3500, nous avons au total huit (08) départs. Un (01) départ vers le rack des serveurs, quatre (04) départs en fibre optique multi mode pour desservir chaque niveau du bâtiment de la Direction Générale et le reste des liens permet d'interconnecter la DEP, l'immeuble KAMBOU et l'ensemble de la zone industrielle.

Une solution point à point via notamment la BLR a été envisagée pour l'interconnexion des équipements actifs dans les locaux de Bobo II et Bobo III. Ce choix a été effectué parce qu'il n'y a au maximum que deux (02) postes de travail dans les usines.

1.2. Le réseau d'interconnexion au siège

Ses locaux de Bobo-Dioulasso sont interconnectés pour former un réseau local. Afin de donner une meilleure description de cette interconnexion, nous allons la subdiviser en trois parties qui sont : l'interconnexion des locaux du centre-ville, ensuite celle de la zone industrielle et enfin l'interconnexion entre les deux zones.

- L'interconnexion des locaux du centre-ville est réalisée au niveau du switch 3500 de la Direction Générale où nous avons deux (2) départs de fibre optique monomode en direction de l'immeuble KAMBOU et de la DEP. La liaison entre l'immeuble KAMBOU et la Direction Générale est en fibre optique appartenant à la SOFITEX et celle entre la Direction générale et la DEP est une fibre optique de l'ONATEL-SA.

- L'interconnexion des locaux de la zone industrielle est effectuée du CMGS d'où nous avons quatre (04) départs vers Bobo I, la DICA, le Garage lourd et Bobo III. Les liaisons en fibre optique CMGS Bobo I et CMGS DICA appartiennent à la SOFITEX tandis que les autres appartiennent à l'ONATEL-SA. A Bobo I, toujours avec la fibre optique SOFITEX, nous avons un départ vers le site Garage Lourd et un autre vers la DTL. Du point DTL, nous avons deux départs de fibre optique multimode : le premier vers le site DI et le second vers Bobo II. Une fois à la DI, la fibre optique de la SOFITEX permet de relier Bobo II. Nous pouvons noter donc la présence de deux itinéraires pour rejoindre les sites Bobo I et Bobo II.

  Au niveau du site Garage Lourd, nous avons un départ de fibre optique de l'ONATEL-SA en direction du site SOPAGRI. Il existe également un départ de SOPAGRI vers Bobo III. Nous avons deux itinéraires pour connecter Bobo III au reste du réseau et ces liaisons passent par la fibre optique gérée par l'ONATEL-SA. Précisons que l'on ne considère ces deux itinéraires que d'un point de vu logique vu que les brins utilisés sont dans le même câble et une fois celui-ci sectionné, Bobo III est coupé du réseau.
- Pour l'interconnexion entre les locaux du centre-ville et ceux de la zone la SOFITEX, pour des raisons propres à la structure, elle a établi une relation contractuelle avec

l'ONATEL-SA. Dans cet accord, l'opérateur à travers des chambres de raccordement, emprunte des brins de la boucle nationale qui traverse Bobo en direction de la COTE D'IVOIRE pour réaliser l'interconnexion entre la Direction Générale et le CMGS. Le backbone du réseau de la SOFITEX est constitué d'une part de la fibre optique monomode appartenant à l'opérateur ONATEL-SA et d'autre part de la fibre optique multi-mode appartenant à la SOFITEX. Dans ce scenario d'interconnexion l'ONATEL-SA est transparent.

Les différentes fibres optiques permettent de connecter localement les switchs à travers des convertisseurs FO/Ethernet de type 100 base-TX. Au total, nous avons en matière d'équipement quarante-six (46) switchs et cinq (05) BLR tous de la gamme Cisco sur l'ensemble du réseau local de Bobo Dioulasso.

Tableau 1 : Tableau récapitulatif des équipements actifs du réseau

Local	Localisation précise	Equipements actifs	Nombres de prises utilisables	Distance maximale (m)
Direction générale	R+0	01 Switch CISCO 2950	15	15
	R+1	02 Switch CISCO 2950 01 Switch CISCO 2960 01 Switch CISCO 3500 01 Routeur CISCO 2900	32	1
	R+2	03 Switch CISCO 2950	25	15
	R+3	01 Switch CISCO 2950	15	30
	Total	10	87	
Immeuble KAMBOU		01 Switch CISCO 2950	07	115
	Total	01	07	
DEEP		02 Switch CISCO 2950 01 Switch CISCO 2960 01 point d'accès linksys	09	905
	Total	04	09	
Bobo I		01 Switch CISCO 2960 02 Switch CISCO 2950	30	2 200
	Total	03	30	
Bobo II		04 Switch CISCO 2950 03 BLR CISCO Aironet 1300	19	2 300
	Total	07	19	
Bobo III		06 Switch CISCO 2950 02 BLR CISCO Aironet 1300	38	4 100
	Total	08	38	
Garage Lourd		05 Switch CISCO 2950	53	2 500
	Total	05	53	
Sapagri		01 Switch CISCO 2950		2 700
	Total	01		
DI		02 Switch CISCO 2950	27	2 100

Local	Localisation précise	Equipements actifs	Nombres de prises utilisables	Distance maximale (m)
		02	27	
DTL		01 Switch CISCO 2950	14	2 000
		01	14	
DICA		01 Switch CISCO 2950	05	1 500
		01	05	
CMGS		03 Switch CISCO 2950	37	1 900
		03	37	
Total général		**46**	**326**	

NB : la distance maximale consignée dans le Tableau 1 représente la distance entre le switch 3500 au niveau du local R+1 de direction générale à un switch dans chaque local technique.

Bâti sur une topologie en étoile, l'architecture de l'ensemble du réseau actuel de Bobo-Dioulasso est présentée sur le schéma de la Figure 6 ci-après.

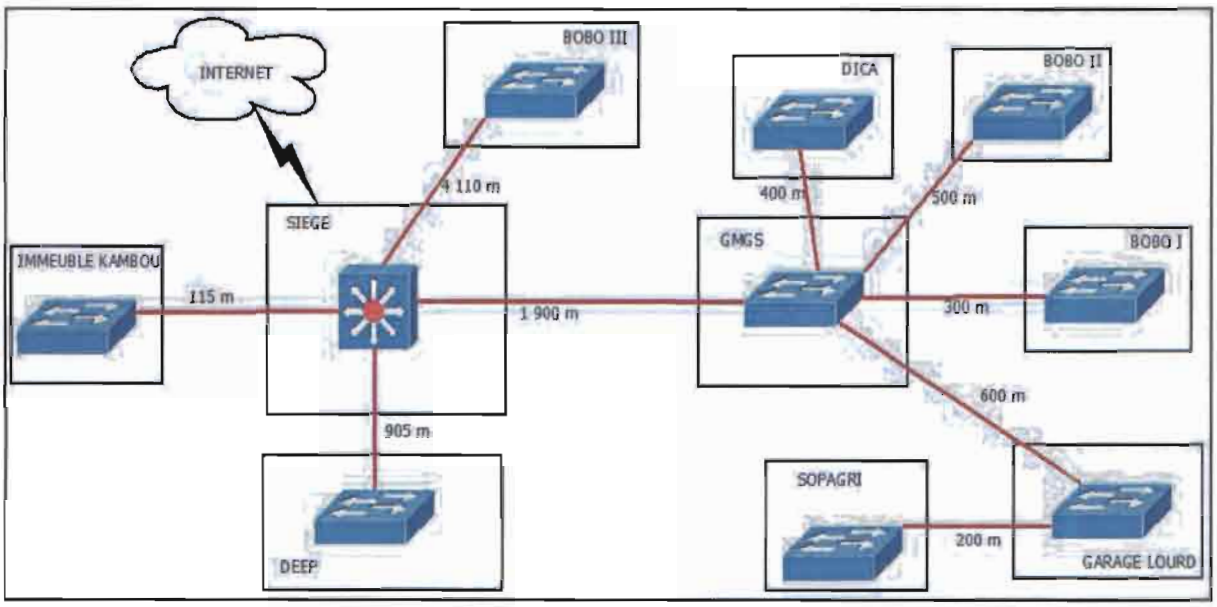

Figure 5 : Architecture simplifiée du réseau de Bobo-Dioulasso

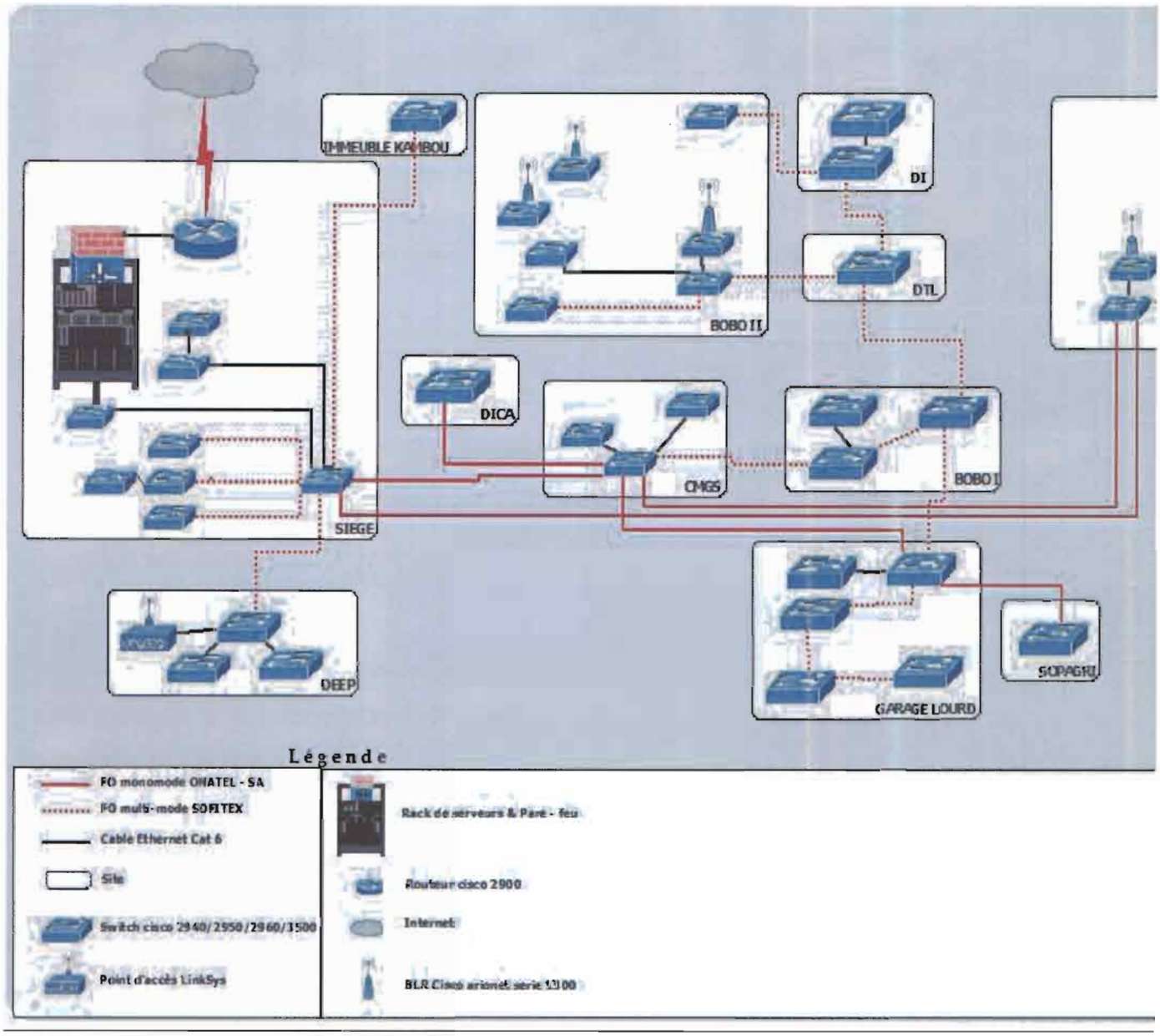

Figure 6 : Architecture du réseau existant de Bobo-Dioulasso

2. Topologie logique

Après avoir defini la topologie physique qui nous a permis de montrer l'agencement des équipements réseau, nous allons dans cette partie, montrer comment circulent les informations sur ce réseau physique.

La topologie logique définit la façon avec laquelle les postes accèdent et émettent sur le support. Mise en œuvre sur le réseau de la SOFITEX, Ethernet qui est la technologie LAN la plus répandue, utilise le mécanisme de gestion partagée de l'accès physique au réseau. La communication sur un réseau Ethernet se fait à l'aide du protocole Carrier Sense Multiple Acces with Collision Detection (CSMA/CD) qui permet de réduire le nombre de conflits d'accès au media. Le réseau de Bobo-Dioulasso utilise le Fast Ethernet (100 Mbit/s) en local et en backbone.

Le principe d'adressage du réseau local de Bobo-Dioulasso est basé sur le protocole d'internet IPv4 et les différentes adresses des postes de travail sont définies dans la classe B. De manière pratique, cette classe B est découpée en fonction des entités et de la categorie des adresses.

Les principales entités sont :

- les serveurs physiques,
- les serveurs virtuels,
- les utilisateurs,
- les imprimantes réseaux,
- les switchs,
- les points d'accès.

Dans les catégories d'adresses on distingue :

- les adresses allouées manuellement,
- les adresses allouées automatiquement,
- les adresses allouées temporairement pour des tests.

3. Présentation du système

La SOFITEX a fait le choix d'un environnement Microsoft et cela se traduit par la mise en place d'un domaine Active Directory et d'un contrôleur Windows 2003 server. Une étude est en cours pour la migration de Windows 2003 server vers Windows 2008 server. La

messagerie qui est Exchange 2003 est en cours de migration également vers Exchange 2010. Le système est composé de dix (10) machines physiques dont chacune peut supporter jusqu'à quatre (04) machines virtuelles de type HP Proliant. Dix-huit (18) machines virtuelles sont actuellement utilisées à la SOFITEX. L'évolution des machines virtuelles est fonction des besoins exprimés. La protection du réseau vis-à-vis de l'extérieur est assurée par un pare feu de type TMG 2010. Le domaine Active Directory est reparti sur l'ensemble de la SOFITEX avec une décentralisation de la messagerie. La SOFITEX héberge son propre domaine internet (sofitex.bf) au niveau de la DMZ. Une solution de sauvegarde automatique est en cours de déploiement et est délocalisée au niveau de la salle technique de l'immeuble KAMBOU qui sert de salle secours pour la redondance de certains serveurs.

Tableau 2 : Présentation des différents serveurs physiques et virtuels

caractéristiques / **Serveurs**	**Marque**	**Système d'exploitation**	**Utilisation**	**localisation**
Serveurs physiques	HP DL 380 G5	Windows server 2003	TMG 2010	Siège
	HP DL 380 G5	Windows server 2003	- DMS - Web	
	HP DL 380 G5	Windows server 2003	- Resume7 - Oracle 10	
	HP DL 380 G5	Windows server 2003	- SQL Server,SQL Base - Proginov - Lync 2010	
	HP DL 380 G5	Windows server 2003	- Exchange frontal 2003 - Impression - DHCP	
	HP DL 380 G5	Windows server 2003	- Web - Ciscoworks - TSE 2003	
	HP DL 380 G5	Windows server 2003	- Symantec - Sharepoint	
	HP ML 370 G5	Windows server 2003	Contrôleur domaine 3	
	HP ML 350 G6	Windows server 2003	Serveur AIC	
	HP ML 350 G6	Windows server 2003	SCE 2010	Immeuble KAMBOU
Serveurs virtuels		Windows server 2003	VM (1-18)	Siège

4. Présentation des applications

Toutes les applications métiers tel que la facturation, la gestion des stocks ou les applications de gestions telles que Proginov ou Reshum7 sont installés sur des machines virtuelles au niveau de la direction générale.

Durant la période charnière qui équivaut à la campagne d'égrenage (novembre à mars), le réseau est très sollicité avec au moins 200 à 300 machines à temps pleins. Les serveurs utilisés sont de la marque HP et de la gamme Proliant.

Tableau 3 : Les applications métiers utilisées à la SOFITEX

Nom Application	Type d'application	Description	Période charnière d'utilisation
PROGINOV	lourd	Application de comptabilité	Toute l'année
G STOCK	lourd	Application de gestion des stocks	Toute l'année
OR BLANC	lourd	Application d'achat et de paie du coton	Toute l'année
GAFIA	lourd	Application de facturation des intrants	Toute l'année
GESPONT	lourd	Application de pesée des remorques	novembre à mars
CLASS FDL	lourd	Application d'égrainage, de gestion des stocks et de classement	novembre à mars
GESCOTON	lourd	Application d'évacuation des bals	novembre à mars
AIC	lourd	Application de suivi de la chaine cotonnière	Toute l'année

5. Présentation des postes de travail

Les postes clients de la SOFITEX sont sous le système Windows XP où une migration est en cours vers Windows 7. Ce sont essentiellement des micro-ordinateurs dont 261 ordinateurs de bureau et 77 portables. D'autres terminaux font leur entrée sur le réseau de Bobo-Dioulasso via les points d'accès, ce sont les smartphones et les tablettes dont l'utilisation connait une évolution rapide. Les utilisateurs disent ne plus pouvoir se passer de leurs appareils mobiles et souhaitent, de plus en plus, pouvoir les utiliser sur les lieux de travail.

Les imprimantes sont très largement utilisées par la SOFITEX. Nous dénombrons sur le réseau de Bobo-Dioulasso 17 imprimantes réseaux et 145 imprimantes individuelles. Ces imprimantes, vues du réseau, sont accessibles à tous les utilisateurs du réseau LAN de Bobo.

La politique actuelle du service est de remplacer tous les imprimantes individuelles par des imprimantes réseaux afin de mutualiser les impressions.

II. Critiques de l'existant

Conçu depuis 2004, le réseau informatique de la SOFITEX est un réseau local unique où l'ensemble des bureaux sont connectés malgré l'étendue de la société. Dix (10) ans après sa conception, ce réseau permet une circulation de l'information tout en assurant un gain en temps non négligeable. La capacité de ce réseau à répondre aux différentes demandes d'acheminement des paquets est obtenue par l'utilisation :

- d'équipements actifs adéquats et homogènes de la gamme CISCO, un constructeur mondialement reconnu ;
- d'un réseau fédérateur sur de la fibre optique ;
- d'un câblage horizontal UTP catégorie 6 qui en 2004 était novateur.

Outre ces atouts, après étude, contrôle et vérification du réseau, nous avons détecté ce qui suit :

- Une inadaptation de l'architecture relativement aux besoins.

  Nous constatons que tous les switchs du réseau de Bobo-Dioulasso sont connectés en cascade. Cet agencement des équipements actifs conduit à avoir un réseau à plat.
- Une absence de redondance des équipements.

  Le réseau informatique représente de nos jours le point central pour les échanges d'informations dans une entreprise moderne et joue un rôle primordial pour le fonctionnement des services. De ce fait une redondance des équipements doit être effective pour assurer la continuité du service en cas de panne de ces équipements actifs. Nous remarquons une absence de redondance d'équipements à certains endroits très critiques du réseau de la SOFITEX, comme c'est le cas à la Direction Générale qui est le point le plus important de ce réseau. Sur ce site, les différents serveurs y sont centralisés avec l'absence de redondance pour le switch 3500 qui est le point de rencontre des différents liens.
- Une absence de redondance des liens.

  Tous les serveurs sont localisés sur le site de la Direction Générale. En cas de rupture ou de dysfonctionnement de du lien venant à la Direction Générale, nous assisterons à un isolement de ces locaux causant du même coup l'arrêt ou la suspension des activités. En pleine campagne, correspondant à la période charnière des activités de la

société, les usines et laboratoires tournent en plein régime et ne doivent pas être arrêtées : ce sont celles de Bobo III, Bobo II, Bobo I. A ces locaux abritant les usines et les laboratoires il faut ajouter le local du CMGS par lequel toute la zone industrielle passe pour rejoindre les serveurs à la Direction Générale. Pour pallier ce problème, une solution de lien secours doit être mise en place pour éviter l'isolement de ces différents locaux.

- Une absence de segmentation du réseau.

  La communication sur le réseau de la SOFITEX s'effectue sans contrôle c'est-à-dire que chaque poste peut communiquer avec n'importe quel autre. Par exemple, n'importe quel utilisateur à Bobo 3 peut faire une impression sur l'imprimante réseau se trouvant à la Direction Générale. Ceci montre que le réseau n'est pas découpé en portions ou segments logiques. Avec un aussi grand domaine de collision, ce réseau est vulnérable et il y est difficile de détecter et de résoudre des pannes.

- Une absence d'outil de supervision.

  Le réseau de la SOFITEX étant vaste, le besoin de contrôler en temps réel sa qualité, d'analyser les hôtes et les services afin de prévenir les pannes ou de les gérer dans les plus brefs délais devient une nécessité. Paradoxalement, aucun outil de supervision et d'administration n'y est présent.

- Une documentation du réseau non mise à jour.

  Nous avons constaté une absence de documentation à jour du réseau de la SOFITEX. Une documentation à jour permet d'élaborer l'architecture du réseau avec les détails nécessaires sur les équipements actifs et passifs du réseau, les équipements terminaux, les différents services réseau et les applications clientes, ce qui facilite la planification d'extension future, les besoins d'audit et d'intégration de nouveaux services.

- Une absence de Sécurisation des données.

  Tous les switchs sont paramétrés avec leur configuration par défaut. Cette configuration montre que les Switchs ne sont pas sécurisés et que toute personne ayant accès à une prise sur un des sites de la région de Bobo pourra se connecter sans difficulté. Nous remarquons également que l'interconnexion des différents sites est réalisée à certains niveau avec l'appui de l'opérateur ONATEL-SA. Cette coopération peut porter atteinte à la sécurité des données. Les données sont envoyées sur la fibre sans chiffrement) et l'interception des données peut être effectuée par la connexion d'un pirate sur la ligne.

DEUXIEME PARTIE : ETUDE TECHNIQUE

Chapitre 1 : Etude préalable et choix techniques

I. Architecture physique du réseau

L'architecture physique du réseau définit les connexions entre les postes avec éventuellement une hiérarchie entre eux. Cette topologie physique peut avoir des implications sur la disposition géographique des différents équipements réseaux. Les architectures en bus et anneaux n'étant plus adaptées aux besoins réseau des entreprises, nous allons focaliser notre étude sur les topologies en étoile et hiérarchisée en couches.

1. Présentation des topologies existantes

- Le réseau en étoile

C'est la topologie la plus courante actuellement. Omniprésente, elle est aussi très souple en matière de gestion et dépannage de réseau étant donné que la panne d'un nœud ne perturbe pas le fonctionnement global du réseau. En revanche, l'équipement central qui relie tous les nœuds constitue un point héraldique dont la panne paralyse l'ensemble du réseau. Il a donc besoin d'être renforcé.

- Le réseau hiérarchique

Aussi connu sous le nom de réseau en arbre, le réseau hiérarchique est divisé en niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence. Le point faible de ce type de topologie réside dans le commutateur "père" de la hiérarchie qui, s'il tombe en panne, paralyse alors la moitié du réseau.

2. Comparaison des topologies physiques du réseau

Les réseaux ont été construits à travers l'utilisation des topologies bus, anneau, étoile et hiérarchisé. Le choix de l'une ou l'autre de ces topologies est essentiel pour non seulement la performance, la facilité de maintenance, la sécurité que pour l'évolutivité du réseau. Nous allons dans le Tableau 4 ci-dessous, récapituler les avantages et les inconvénients des différentes topologies physiques existantes pour un réseau informatique.

Tableau 4 : Comparaison des topologies physiques

Topologie	Avantages	Inconvénients
Etoile	- Ajout facile de nouveaux ordinateurs - Modification facile du réseau. - Contrôle et administration centralisés. - Panne d'un seul ordinateur sans incidence sur le reste du réseau.	- Reconfiguration du réseau interrompant sur son fonctionnement. - Panne du point central mettant tout le réseau hors service.
Hiérarchique	- Réseaux aisément extensibles. - Redondance permettant d'augmenter la disponibilité du réseau. - Plus haut niveau de sécurité possible sur les ports d'accès et des stratégies au niveau distribution. - Modularité rendant plus facile la maintenance. - Administration plus aisée. - Satisfaction des besoins des petits et moyens réseaux.	- Mise en œuvre coûteuse

3. Choix de la topologie

Nous avons fait le choix de la topologie hiérarchisée. Ce modèle de conception hiérarchisé répond aux besoins de performance, d'évolutivité, de maintenabilité et d'administration qui permettra l'utilisation efficace de la bande passante du réseau de la SOFITEX par les applications. Il répond ainsi à tous les besoins actuels et futures de la société au niveau topologie physique.

II. Gestion de la redondance physique

La redondance est un facteur essentiel pour atteindre une bonne disponibilité du réseau. Une telle redondance devrait assurer la tolérance aux pannes et assurer une continuité de service au cas où des équipements actifs du réseau seraient détériorés et/ou des liens entre équipements se casseraient.

1. Redondance des équipements actifs du réseau

Il s'agit de doubler les équipements actifs au niveau des nœuds critiques du réseau. Les points jugés critiques du réseau sont :

- le siège car il héberge l'ensemble des serveurs,
- le CMGS parce qu'il permet de relier toute la zone industrielle à la direction générale,

- le site de BOBO III car il abrite la plus grande usine d'égrainage et le laboratoire de qualité de la SOFITEX.

2. Redondance des liens d'interconnexion

La redondance des liens utilise quant à elle les différents supports de transmission des données sur le réseau. Dans notre contexte, nous avons essentiellement la fibre optique et la BLR.

2.1. Comparaison des supports de transmission

Tableau 5 : Comparaison des supports de transmission utilisés pour l'interconnexion

Caractéristiques / Solutions	Débit maximum	Portée maximale (Km)	Coût de mise en œuvre (en f cfa)
Fibre optique	10 Gbit/s	100	Supérieur à 30 000 000
BLR	54 Mbit/s	45	Environ 4 500 000

La fibre optique possède une large bande passante comparée à la BLR (Tableau 5) et présente une immunité au bruit même si elle a un coût relativement élevé pour sa mise en place. La fibre optique se présente comme une solution envisageable mais nous jugeons mieux de nous tourner vers les solutions passant par les airs pour la transmission des données pour également mener une étude.

La BLR contrairement à la solution guidée, n'utilise pas de supports physiques pour la transmission de données. Elle est un moyen d'interconnexion des sites en haut débit qui a une zone de couverture de l'ordre de dizaine de kilomètre et à un coût de déploiement moins élevé (Tableau 5).

2.2. Choix de la solution pour la redondance des liens

Après l'analyse des solutions possibles d'interconnexion et vu ces avantages qui sont entre autre le faible coût et la facilité de déploiement, la solution de la BLR est appropriée du fait qu'elle ne sera utilisée que comme un chemin alternatif en cas de défaillance de la liaison fibre optique.

III. Gestion de la redondance

Les réseaux Ethernet comportent des mécanismes de tolérance de pannes vis à vis de leur architecture plus ou moins complexe. Ces mécanismes sont en fait de vrais protocoles de communication destinés à la création automatique de chemin de communication de secours. Ainsi, une topologie physique redondante fournira des chemins multiples visant à améliorer la fiabilité d'un réseau. Toutefois, elle présente le désavantage d'introduire la circulation en boucle des paquets de données qui conduirait à une augmentation importante des collisions et à la détérioration de la bande passante.

Pour résoudre ce problème, le protocole Spanning Tree Protocol (STP) a été créé. Il a connu différentes évolutions et extensions que nous avons choisi de présenter en plus de STP lui-même.

1. Le protocole Spanning Tree Protocol (STP)

Le protocole STP également connu sous le standard IEEE 802.1d, est inclu dans certains commutateurs ou switchs Ethernet, a pour fonction, s'il est activé, de gérer la redondance des chemins de communication entre les différents nœuds d'un réseau, en ne validant à un moment précis qu'un seul et unique chemin de communication entre deux nœuds du réseau. Cette procédure de rétablissement avec un nouveau chemin de communication implique des échanges entre les différents commutateurs ou Switch Ethernet avec un délai moyen de convergence d'environ 30 secondes, selon la complexité du réseau [6].

2. Le protocole Rapid Spanning Tree Protocol (RSTP)

Le protocole RSTP connu sous le standard IEEE 802.1w, est une évolution du protocole STP avec un nouveau mécanisme d'échanges d'information entre commutateurs, ce mécanisme permet de réduire le temps de rétablissement du réseau en cas de défaillance du chemin de communication principal, autour de trois fois la valeur du délai Hello (deux secondes par défaut pour un Hello) c'est-à-dire 6 secondes de temps de convergence. Le fonctionnement général de RSTP est semblable à celui du STP classique [7].

3. Le protocole Per-VLAN Spanning Tree (PVST)

Quand plusieurs VLAN existent dans un réseau Ethernet commuté, STP peut fonctionner de façon indépendante sur chacun des VLAN séparément. Ce mode de fonctionnement a été baptisé PVST(+) [8] par Cisco et est du standard 802.1d. C'est le mode par défaut sur les commutateurs de la marque. Il s'agit d'un développement propriétaire qui est également pris

en charge par certains fournisseurs concurrents. PVST fonctionne uniquement avec Cisco Inter-Switch Link (ISL). PVST+ est utilisé avec dot1q.

4. Le protocole RPVST+

Ce protocole correspond à la variante STP rapide à utiliser dans les réseaux Cisco. C'est une implémentation Cisco du protocole RSTP [9] de IEEE et prend en charge un arbre recouvrant pour chaque VLAN. RPVST+ entraine un changement rapide de la topologie en cas de problème sur le commutateur, sur le port ou sur le lien. Il fournit une convergence rapide (moins d'une (01) seconde) pour les ports d'extrémités, les nouveaux ports racine et ports connectés à travers les liens point à point.

5. Le protocole MSTP

Le Multiple Spanning Tree Protocol (MSTP) [10], défini dans la norme IEEE 802.1s puis inclus dans IEEE 802.1Q-2003, est une extension de RSTP dans laquelle une instance de RSTP existe par groupe de VLAN.

Disposer de plusieurs instances de STP permet de mieux utiliser les liaisons dans le réseau si la topologie STP est différente pour certains groupes de VLAN. Contrairement à PVST, ce protocole n'exige pas de disposer d'une instance par VLAN. Puisque les VLAN pouvent être très nombreux, ils sont groupés. Le MSTP est compatible avec les commutateurs RSTP, le format de BPDU étant le même.

6. Le protocole SPB.

Le protocole Shortest Path Bridging (SPB) [11] connu sous le standard IEEE 802.1aq est une technologie qui simplifie la création et la configuration des réseaux d'entreprise, des réseaux de télécommunication et du réseau en nuage qui élimine pratiquement les erreurs humaines tout en activant le routage à trajets multiples.

SPB) est le remplaçant des protocoles de Spanning Tree (IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP), qui bloquaient le trafic sur les chemins redondants. Il permet d'avoir tous les chemins actifs avec plusieurs chemins à coût égaux, supporte de plus grande topologie de niveau 2, accélère le temps de convergence, et améliore l'utilisation des topologies maillés par l'augmentation de la bande passante et de la redondance entre tous les

équipements en permettant le partage de charge du trafic sur tous les chemins d'un réseau maillé.

7. Comparaison des solutions pour la redondance logique

Pour la gestion de la redondance logique, nous avons deux blocs à savoir le bloc des solutions propriétaires et le bloc des solutions standards. La référence au niveau du bloc propriétaire est implémentée par Cisco et celle au niveau standard par l'IEEE. Chez Cisco, nous avons le PVST, le PVST+ et le Rapid PVST+. Chez l'organisme de standardisation IEEE, nous avons le STP, le RSTP, le MSTP et le SBP (successeur du MSTP non répandu).

Au sein du monde propriétaire, le PVST est le premier, ensuite c'est PVST+ qui améliore le PVST et enfin le Rapid PVST+ est une évolution du PVST+ avec un temps de convergence amélioré. Ce dernier implémente le RSTP de l'IEEE. Avec ce protocole, on a une instance de PVST+ par VLAN et les switch gèrent les trames BPDU chaque 2 secondes. Nous constatons qu'il est plus adapté pour des réseaux n'implémentant pas beaucoup de VLAN. Avec le RPVST+, nous avons une facilité d'ajout ou de suppression de topologie de réseau avec un temps de convergence de moins d'une seconde.

Au niveau des protocoles standard, nous avons le STP qui n'est plus implémenté sur les réseaux. Cela est principalement dû à son temps de convergence (environs 30 à 50 secondes selon la complexité du réseau).

Le RSTP permet de corriger cette lacune du STP en offrant un temps de convergence de l'ordre de 6 secondes. Le protocole RSTP est plus adapté aux réseaux n'ayant qu'une seule instance de VLAN à implémenter.

Afin de pallier cette insuffisance, le protocole MSTP a été développé. En effet, il permet d'avoir un groupe de VLAN par instance de STP. En d'autres termes, nous avons du RSTP pour chaque groupe de VLAN sur le réseau. Ce protocole allie ainsi un meilleur temps de convergence ou de changement de topologie de l'ordre de 3 secondes et permet également d'avoir l'implémentation de plusieurs instances de VLAN sur le réseau.

Notons que le MSTP est complexe à mettre en œuvre au niveau conceptuel mais est néanmoins supporté par pratiquement tous les commutateurs des différents constructeurs.

8. Choix de la solution de gestion de redondance logique

Au regard de cette analyse des protocoles de STP, nous pouvons retenir Rapide PVST+ du constructeur CISCO et le MSTP de IEEE. Ces deux protocoles ont des similitudes à divers

points de leur fonctionnement. Le RPVST+ est propriétaire CISCO et sied bien à notre infrastructure réseau vu que tous nos équipements actifs sont CISCO. Egalement, le RPVST+ est facile à déployer, évolutif, très utilisé et permet :

- d'avoir du spanning tree par VLAN ;
- d'avoir une convergence en moins d'une seconde;
- d'avoir une compatibilité avec 802.1D STP, 802.1w RSTP et MSTP;
- de faire du spanning tree à travers les trunks en regroupant des VLAN ensemble et en les associant dans des instances ;
- d'améliorer la tolérance aux pannes car si une instance est touchée, les autres ne le sont pas ;
- d'avoir une évolutivité vers de grandes topologies (environ10 000 ports logiques).

Ainsi, pour l'implémentation du STP sur le réseau de la SOFITEX, nous avons opté pour le RPVST+ au vu des caractéristiques citées plus haut.

IV. Segmentation du réseau

1. Présentation des solutions de segmentation

Parallèlement à la hiérarchie physique, la hiérarchie logique pose les fondations d'un réseau stable. Ainsi un réseau peut être divisé en unités plus petites appelées segments. Chaque segment utilise le mode d'accès CSMA/CD et assure le trafic entre les utilisateurs sur le segment. Cette caractéristique permet d'avoir un domaine de collision par segment. La segmentation permet alors de réduire significativement la congestion liée aux paquets de diffusion, de réduire les distances entre les ressources, d'équilibrer le trafic du réseau mais aussi permet d'avoir une organisation administrative de l'entreprise. Dans le monde des réseaux TCP/IP, cette segmentation est réalisée soit à l'aide de sous-réseaux, soit à l'aide des Virtual Local Area Network (VLAN), soit en combinant les deux.

1.1. Sous réseautage

Un sous-réseau est une subdivision logique d'un réseau de taille plus importante. Le masque de sous-réseau permet de distinguer la partie de l'adresse utilisée pour le réseau et celle utilisable pour numéroter des interfaces. Un sous-réseau correspond typiquement à un réseau local sous-jacent.

La subdivision d'un réseau en sous-réseaux permet de limiter la propagation des paquets de diffusion. Cette propagation restant limitée au réseau local est coûteuse en bande passante et en ressource au niveau des commutateurs réseau. Les routeurs sont utilisés pour la communication entre les machines appartenant à des sous-réseaux différents.

1.2. VLAN

Par définition, un VLAN [2] est un réseau local virtuel utilisant la technologie Ethernet pour regrouper les éléments du réseau (utilisateurs, périphériques, ...) selon des critères logiques (fonction, partage de ressources, appartenance à un département,...) sans se heurter à des contraintes physiques (dispersion des ordinateurs, câblage informatique inapproprié, ...).

2. Comparaison des solutions de segmentation

Il existe des différences entre les deux solutions. Le tableau 3 ci-dessous récapitule les avantages et inconvénients de ces deux solutions.

Tableau 6 : Avantages et inconvénients entre sous réseautage et VLAN

Solution de segmentation	Avantages	Inconvénients
Sous réseaux	- Flexibilité de segmentation du réseau. - Augmentation considérable des performances du réseau. - Régulation de la bande passante. - Division de groupes de travail en domaines de diffusion gérables.	- Impossibilité d'appliquer des stratégies de sécurité par groupes de travail - Impossibilité de gérer dynamiquement de la mobilité des utilisateurs. - Administration et configuration manuelles.

Solution de segmentation	Avantages	Inconvénients
VLANs	- Applications des stratégies de sécurité selon les groupes de travail. - Gestion dynamique de la mobilité des utilisateurs. - Administration automatique et aisée. - Flexibilité de la segmentation du réseau. - Augmentation considérable des performances du réseau. - Régulation de la bande passante. - Division de groupes de travail en domaines de diffusion gérables.	- Plus de temps pour la configuration des VLANs. - Mauvaise configuration entrainant indisponibilité du réseau.

3. Choix de la solution de segmentation

Au vu de nos objectifs, de la comparaison entre les deux solutions et étant donné que le réseau de la SOFITEX est un réseau commuté Ethernet à 100 Mbit/s, nous avons choisi la solution de la segmentation LAN à base de commutateurs, en implémentant le VLAN (segmentation logique du réseau). En effet cette solution réduira considérablement la taille du domaine de diffusion. Cette solution est attrayante du point de vue de la gestion du parc informatique et de la bande passante. Elle pourra répondre au besoin d'optimisation du réseau de la SOFITEX et surtout dans l'utilisation de ses services (voix/données), surtout celle de la VoIp qui est imminente.

V. La supervision du réseau

Le réseau de la SOFITEX étant vaste et les équipements dispersés, le besoin de contrôler en temps réel sa qualité et son état est rapidement devenu une priorité.

La supervision peut se définir comme étant l'utilisation de ressources réseaux adaptées (matérielles ou logicielles) afin d'obtenir des informations sur l'utilisation et sur l'état du réseau et de ses composants (logiciels, matériels).

Ces informations peuvent alors servir d'outils pour gérer de manière optimale (automatique si possible) le traitement des pannes, la qualité des réseaux (problèmes de surcharge) et aussi

d'anticiper les incidents. Elles permettent également de prévoir toute future évolution nécessaire.

1. Les solutions de supervision

L'un des besoins les plus exprimés en matière de gestion de réseau est la surveillance des services. C'est donc dans une démarche de qualité de service, et de manière à pouvoir réagir dans les plus brefs délais, que de nombreuses solutions de supervision, aussi bien dans le monde libre que propriétaire ont vu le jour. Au nombre de ces outils nous pouvons citer Nagios, Cisco Works, HP Open View NNM, Trivoli, NetFiger…. Dans la suite, nous présenterons uniquement dans le monde libre que Nagios et dans le monde propriétaire nous présenterons que HP Open View NNM et Cisco Works.

1.1. Nagios

Nagios [17] est un logiciel libre de surveillance (Monitoring) des réseaux et systèmes, très connu dans le monde de l'entreprise et des professionnels réseaux. Il permet de surveiller les hôtes et les services spécifiés dans son fichier de configuration, et d'alerter les administrateurs systèmes et réseaux en cas d'évènement (mauvais ou bon).

- Nagios récupère les informations fournis par les services de surveillance et les analyse. Si le résultat de cette analyse fait remonter un problème, les services de surveillance peuvent envoyer des avertissements à l'administrateur du réseau de différentes manières : courriers électroniques, messages instantanés, SMS.

1.2. Cisco Works

Cisco Works LAN Management Solution (LMS) est une suite d'outils de gestion qui simplifient la configuration, l'administration, la surveillance et le dépannage des réseaux Cisco. Il intègre ces fonctionnalités dans une solution best-in-class pour:

- l'amélioration de la précision et l'efficacité du personnel d'exploitation du réseau ;
- l'augmentation de la disponibilité globale du réseau en simplifiant la configuration et rapidement identifier et résoudre les problèmes de réseau ;
- maximiser la sécurité du réseau grâce à l'intégration avec les services de contrôle d'accès et l'audit des changements au niveau du réseau.

1.3.HP Open View Network Node Manager (NNM)

HP Open View (HPOV) est une plate-forme proposant un ensemble d'outils d'administration développé par la compagnie HP, cette application client-serveur conçue pour aider les administrateurs systèmes à détecter, prévenir ou résoudre les problèmes qui peuvent survenir sur des équipements réseau, sur des systèmes ou des applications. Elle utilise pour ce faire des agents que l'on installe sur les machines à superviser et qui communiquent avec le gestionnaire par l'intermédiaire de procédures d'appels à distance. Elle récupère et interprète aussi les messages SNMP émis par diverses entités. Elle permet l'exécution automatique d'actions sur événements ou bien à intervalle régulier. Elle ajoute à la vue classique de la liste d'alarmes une vue graphique du service supervisé, qui permet après configuration d'avoir une vision précise d'une application distribuée et de son comportement, accélérant ainsi le processus de traitement des problèmes.

Pour gérer l'ensemble des éléments actifs de notre réseau, nous utilisons une station de gestion NMS (Network Management Station) qui contient le protocole de gestion de réseaux et les applications de gestion. Elle permet de récolter et d'analyser les données relatives aux équipements physiques connectés au réseau (ponts, routeurs, hubs) et de les gérer. La station de gestion interroge les agents pour observer leur fonctionnement et leur envoie des commandes pour leur faire exécuter certaines tâches. Les agents renvoient les informations requises aux stations de gestion. La NMS est composée d'une console centrale, de différents programmes, et bases de données qui interagissent entre eux.

2. Comparaison des outils de supervision

Pour garantir une bonne qualité de service et une facilité de maintenabilité du réseau de la SOFITEX, un choix adéquat de l'outil doit être effectué.

Le tableau 4 suivant fera un récapitulatif des avantages et inconvénients de quelques outils de supervision.

Tableau 7 : comparaison des outils de supervision

Outils de supervision	Avantages	Inconvénients
Nagios	- Grosse communauté et bonne réputation. - Libre et gratuit. - Très puissant et modulaire. - Peut disposer d'une surcouche graphique. - Peut disposer de nombreux plugins qui permettent d'étendre les possibilités. - Présente un moyen efficace de supervision des ressources du réseau. - Son code est ouvert. - Aucune limitation à son niveau. - Beaucoup de documentation sur le web.	- Fastidieuse via beaucoup de fichiers. - Nagios n'affiche pas de graphiques en natif. - Interface non ergonomique et peu intuitive. - Pour avoir toute les fonctionnalités il faut installer des plugins car de base, c'est assez limité.
Cisco Works	- Réduction des tâches manuelles lourdes. - Augmentation de la disponibilité du réseau en réduisant les temps d'arrêt ou la dégradation de performances - Les équipements sont en Cisco. - Acquis par la SOFITEX en 2005	- Le coût est élevé. - La plateforme ne peut être utilisée qu'avec les équipements Cisco.
HP Open View	- un moyen de supervision des ressources du réseau efficace qui offre un pilotage intuitif ; - une référence de la supervision de réseaux et représente une solution professionnelle de qualité. - Une prise en compte des services du réseau offrirait une réponse globale aux besoins de la supervision d'un réseau IP, fonctionnalité dont la mise en place reste essentielle.	- L'automatisation des réponses ne peut être effectuée que manuellement par un administrateur ; - Le prix est très élevé ; - ne propose pas non plus d'interfaçage de base avec un serveur mail. C'est un point qui limite les temps de réaction d'un processus d'escalade dans la résolution des pannes ; - ne propose pas automatiquement de mesures de réponses aux événements

3. Choix de l'outil de supervision

Notre choix s'est porté sur Nagios pour entre autre sa puissance, sa modularité et le fait qu'il répond, aux attentes de la SOFITEX en terme de supervision. Afin d'avoir une interface ergonomique et intuitive, Nagios sera couplé à Centreon [18], un outil libre qui lui fournira cette puissance graphique.

Chapitre 2 : Etude détaillée de la solution retenue

Le chapitre précédent nous a permis de faire l'état de l'art des différentes solutions et de faire un choix judicieux permettant d'assurer l'optimisation du réseau de la SOFITEX. Au cours de ce chapitre, il a été question de définir l'architecture hiérarchisée en 3 couches, de choisir la BLR pour la liaison redondante, le RPVST+ pour l'élimination des boucles dans le réseau, les VLAN pour limiter les domaines de broadcast et enfin Nagios pour la supervision de ce vaste réseau.

A l'issu du choix des différentes briques constituant notre solution pour l'optimisation, nous allons dans ce présent chapitre étudier en détail l'ensemble des éléments de la solution.

I. L'architecture hiérarchisée en trois couches

Ce modèle inventé et diffusé par CISCO, permet de créer un design réseau structuré en trois couches, chacune ayant un rôle précis impliquant des matériels et outils différents. La couche cœur « Core layer », la couche distribution « Distribution layer », et la couche accès « Access layer » constituent les trois couches du modèle. Un exemple d'agencement de ces couches est représenté par le schéma de la figure 7 ci-dessous.

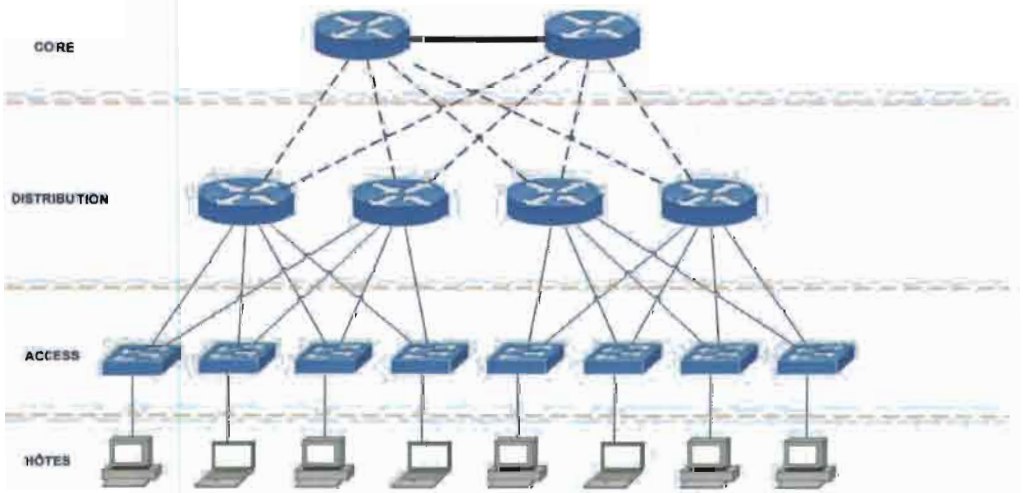

Figure 7 : Architecture hiérarchisée en trois couches [13]

1. La couche cœur

La couche cœur ou Backbone représente la couche supérieure de ce modèle. Cette couche permet de relier les différents segments du réseau, par exemple les sites distants, les LANs ou les étages d'une société. L'ensemble du trafic passe par le cœur d'où l'utilisation des équipements performants.

2. La couche distribution

Cette couche se trouve entre le cœur et la couche d'accès du réseau. Elle permet d'interconnecter les switchs de la couche d'accès à la couche cœur du réseau et est architecturée avec de la commutation rapide de niveau 3. Elle doit gérer les fonctionnalités de niveau 3 et mettre en place la politique de sécurité. Elle permet la gestion des VLANs, le routage entre les VLANs, l'agrégation des routes, de relier les différents types de média utilisés comme FDDI, Ethernet ou Token Ring.

3. La couche d'accès

C'est la dernière couche du modèle qui a pour rôle de connecter les périphériques « end-users » au réseau. Elle permet de définir les VLANs afin d'interdire la propagation des broadcasts et des multicasts, de filtrer le trafic en fonction des adresses MAC, de dédier la bande passante à destination des serveurs et d'authentifier les accès des utilisateurs au réseau.

II. Gestion de la redondance des liens : La Boucle Locale Radio (BLR)

1. Définition

La boucle locale radio (BLR) est une technologie fondée sur la transmission hertzienne. Elle utilise des signaux radio large bande, pour la transmission des données point à point ou point à multipoint. Avec la BLR, les usagers peuvent aussi avoir accès à des services comme l'Internet et la téléphonie.

2. Les technologies BLR

Dans cette partie nous détaillerons plus la technologie WiMax puisque c'est elle qui sera utilisée. Nous présenterons brièvement les autres technologies BLR existantes.

1.1. Le Local Multipoint Distribution Service (LMDS)

Le LMDS est une technologie cellulaire "Point à multipoint". Un émetteur central dessert un nombre élevé d'abonnés (4000 en théorie). Ce réseau permet de distribuer les services à très haut débit par voie hertzienne haute fréquence sur une zone géographique limitée à 8 km. Elle utilise des fréquences situées entre 26 et 29 GHz. Selon les constructeurs, la technologie fournit un débit maximal de 8 à 10 Mbit/s en voie montante et descendante.

1.2. Le Microwave Multichannel Distribution System (MMDS)

La technologie MMDS (Microwave Multichannel Distribution System) ou réseau de distribution à large bande hyperfréquence est un système de diffusion terrestre, en espace libre et à l'horizontale. Elle utilise des fréquences micro-ondes porteuses de signaux analogiques et numériques dans des bandes de fréquence 11,7 à 12,5 GHz et avec des débits variant entre 2 et 15 Mbit/s. Une antenne d'émission multidirectionnelle envoie les signaux à l'horizontale depuis un point élevé du relief ou depuis le sommet d'un pylône.

1.3. Le WiMax

1.3.1. Définition

Le WiMax (World Interoperability for Microwave Access) est un standard de communication sans fil. Il est constitué d'un ensemble de normes techniques (la norme 802.16) permettant la transmission de données IP haut débit par voie hertzienne. Son débit théorique maximum est de 70 Mbit/s sur une distance théorique de 50 Km. Les débits réels devraient davantage se rapprocher des 15 à 25 Mbit/s. Le WiMax est une solution alternative pour le déploiement des réseaux haut débit sur les territoires, qu'ils soient couverts ou non par d'autres technologies comme l'ADSL ou le câble.

1.3.2. Principe de fonctionnement

Le cœur de la technologie WiMAX est la station de base, c'est-à-dire l'antenne centrale chargée de communiquer avec les autres antennes. On parle ainsi de liaison *point-multipoints* pour désigner le mode de communication du WiMAX. Par ailleurs, il existe deux modes de fonctionnement à savoir le WiMax fixe et le WiMax mobile.

Le WiMAX fixe est prévu pour un usage fixe avec une antenne montée sur un toit, à la manière d'une antenne TV. Le WiMAX fixe opère dans les bandes de fréquences 2.5 GHz et 3.5 GHz, pour lesquelles une licence d'exploitation est nécessaire, ainsi que la bande libre des 5.8 GHz.

Le WiMAX mobile prévoit la possibilité de connecter des clients mobiles au réseau internet. Le WiMAX mobile ouvre ainsi la voie à la téléphonie mobile sur IP ou plus largement à des services mobiles à haut débit.

Le tableau 5 suivant synthétise les caractéristiques des deux modes de fonctionnement du WiMAX.

Tableau 8 : Caractéristiques du WiMax

Standard	Bande de fréquence	Débit	Portée
WiMAX fixe (802.16-2004)	2-11 GHz	75 Mbit/s	10 Km
WiMAX mobile (802.16e)	2-6 GHz	30 Mbit/s	3.5 Km

Notre choix se portera sur le WiMax fixe car, servant de chemin alternatif, ce standard pourra en cas de défaillance du lien principal servir de lien redondant avec son débit acceptable. En plus sa portée de 10 Km répond parfaitement à nos besoins sachant que la plus grande distance entre deux points du réseau de la SOFITEX à savoir la direction générale et BOBO III est de 5 Km au plus.

3. Sécurité des systèmes BLR

La sécurité est un point important dans les systèmes BLR [3]. La particularité diffusive de la radio laisse un doute quant à la possibilité d'une écoute clandestine. Le chiffrement de l'information sur la voie radio est indispensable afin d'éviter toute réception malveillante.

La sécurité s'articule autour des points suivants :

- la sécurité contre l'écoute malveillante qui nécessite le chiffrement de l'information véhiculée sur la voie radio. La plupart des systèmes radio utilisent des techniques de chiffrement plus sophistiquées ;
- la force du chiffrement radio se situe dans la fréquence de changement de la clé de chiffrement. Les derniers développements permettent actuellement d'avoir une clé de chiffrement pour chaque transmise ;
- la sécurité grâce aux adresses MAC pour assurer la communication entre les antennes BLR seulement. Aucun poste ne pourra donc se connecter à une antenne BLR.

III. La gestion de la redondance logique

1. L'algorithme Spanning Tree

Le protocole STP utilise l'algorithme Spanning-Tree (STA) pour déterminer quels ports de commutateurs doivent être configurés en état de blocage afin d'empêcher la formation de boucles sur un réseau. L'algorithme STA désigne un commutateur unique comme pont racine et il l'utilise comme point de référence pour le calcul de tous les chemins. Le pont racine est choisi par le biais d'un processus de sélection. Tous les commutateurs associés au protocole STP échangent des trames BPDU pour identifier le commutateur doté de l'identificateur de pont (BID) le plus faible sur le réseau. Le commutateur doté de l'identificateur (ID) le plus faible devient automatiquement le pont racine pour les calculs de l'algorithme STA.

L'unité BPDU est la trame de message échangée par les commutateurs pour le protocole STP. Chaque trame BPDU contient un identificateur de pont qui identifie le commutateur ayant envoyé la trame BPDU. L'identificateur de pont contient une valeur de priorité, l'adresse MAC du commutateur émetteur et un ID système étendu facultatif. La valeur d'identificateur de pont la plus faible est déterminée par la combinaison de ces trois champs (valeur de priorité, l'adresse MAC et l'id système). Une fois que le pont racine a été déterminé, l'algorithme STA calcule le chemin le plus court vers le pont racine. Chaque commutateur utilise l'algorithme STA pour identifier les ports devant être bloqués. Pendant que l'algorithme STA détermine les meilleurs chemins vers le pont racine pour toutes les destinations du domaine de diffusion, aucune donnée ne peut être transmise sur le réseau.

L'algorithme STA prend en compte les coûts de chemin et de port lors de la sélection du chemin qui ne doit pas être bloqué. Le coût de la route est calculé à l'aide des valeurs de coût de port associées à la vitesse de port de chacun des ports des commutateurs sur un chemin donné. La somme des valeurs des coûts de ports détermine le coût du chemin global vers le pont racine. Si plusieurs chemins sont disponibles, l'algorithme STA choisit le chemin doté du coût de chemin le plus faible.

Lorsque l'algorithme STA a déterminé les chemins qui doivent rester disponibles, il configure les ports des commutateurs dans des rôles de ports indépendants. Les rôles des ports décrivent le lien entre les ports et le pont racine du réseau et spécifient s'ils sont autorisés à acheminer le trafic.

2. Vu d'ensemble du RPVST+

Le protocole RPVST+ prenant en charge un arbre recouvrant pour chaque VLAN permet d'obtenir une convergence rapide pour les ports d'extrémités (edge ports), les nouveaux ports racines et ports connectés à travers les liens point-to-point comme suit :

- *Edge ports*—Ou encore port d'extrémité en français, est un port de commutateur qui ne doit jamais être connecté à un autre commutateur. Il passe immédiatement à l'état d'acheminement lorsqu'il est activé. Le concept de edge port est déjà bien connu des utilisateurs du protocole Spanning Tree de Cisco, car il correspond à la fonctionnalité « PortFast » dans laquelle tous les ports directement connectés aux stations d'extrémité anticipent qu'ils ne sont connectés à aucun commutateur. Les ports PortFast basculent immédiatement vers l'état d'acheminement STP sans passer par les longues étapes d'écoute et d'identification. Ni les ports d'extrémité ni les ports PortFast ne produisent de changement de topologie lorsque le port passe à un état désactivé ou activé.
- *Root ports* -- Si le RPVST+ sélectionne un nouveau port racine, il block l'ancien root port et bascule immédiatement le nouveau root port à l'état d'acheminement (forwarding).
- *Point-to-point links* — Si nous connectons un port à un autre port à travers une liaison point-to-point et le port du switch devient un port désigné alors il négocie une transition rapide avec les autres ports en utilisant le proposal-agreement Handshake (décrit plus bas) afin d'assurer une topologie sans boucle.

Le type de liaison permet de classer dans différentes catégories chacun des ports d'une configuration RPVST+. Le type de liaison peut prédéterminer le rôle actif que joue le port lorsqu'il est en attente d'une transition immédiate vers l'état d'acheminement si certaines conditions sont réunies. Ces conditions ne sont pas les mêmes pour les ports d'extrémité et les autres types de ports. Les ports qui ne sont pas des ports d'extrémité appartiennent à deux catégories de type de liaison : point à point et partagée. Le type de liaison est automatiquement déterminé, mais il peut être remplacé par une configuration de port explicite. Les ports d'extrémité (l'équivalent des ports PortFast) et les liaisons point-à-point sont d'excellents choix pour une transition rapide vers l'état d'acheminement. Cependant,

avant que le paramètre de type de liaison soit pris en compte, le protocole RPVST+ doit déterminer le rôle du port.

Seuls les ports désignés et les ports racines peuvent générer un changement de topologie et cela à travers des BPDU de Notification de Changement de Topologie (NCT). La NCT est une trame BPDU très simple qui ne contient aucune information et qui est envoyée selon l'intervalle Hello Time. Le commutateur récepteur est appelé pont désigné et il accuse réception de la NCT en renvoyant immédiatement une trame BPDU normale avec le bit TCA (Topology Change Acknowledgement) à l'état 1. Cet échange se poursuit jusqu'à ce que le pont racine réponde.

Une fois que le pont racine a été informé d'une modification de la topologie du réseau, il commence à envoyer ses BPDU de configuration avec le bit TC (Topology Change). Ces BPDU sont ensuite relayées par chaque commutateur du réseau avec ce bit défini. Par conséquent, tous les commutateurs sont informés de la modification de topologie et peuvent réduire leur paramètre

« aging time » pour le délai de passage à l'état d'acheminement. Les commutateurs reçoivent les BPDU de changement de topologie sur les ports en état d'acheminement et les ports en état de blocage. Le bit TC est défini par la racine pour une durée équivalente à un message Hello plus une (01) seconde.

Lorsque le RPVST+ détecte un changement de topologie, il suit les étapes suivantes :

- il démarre un TC pendant un temps égal à deux fois la valeur d'un «hello-time» pour tous les ports n'étant pas ports d'extrémité, et le pont racine si nécessaire
- vide les adresses MAC associées à tous ces ports. A la réception d'un BPDU avec le flag TC à 1, toutes les adresses MAC associées aux non edge ports sont vidées afin de refaire un apprentissage

3. Les rôles et les états des ports

3.1. Les rôles des ports

Le rôle d'un port définit la fonction finale d'un port de commutateur et la manière dont il gère les trames de données. Les rôles des ports et les états des ports peuvent changer indépendamment les uns des autres. La création de rôles de ports supplémentaires permet au protocole RPVST+ de définir un port de commutateur de secours avant une panne ou une modification de topologie. Le port alternatif passe à l'état d'acheminement en cas de panne sur le port désigné pour le segment.

Le RPVST+ construit sur le 802.1D STP sélectionne le switch ayant la priorité la plus faible en valeur numérique comme le pont racine. A la suite, RPVST+ assigne l'un des rôles suivants à chaque port :

- *Root port* qui fournit le meilleur chemin (plus faible cout) lorsque le switch désire envoyer des paquets en direction du pont racine;
- *Designated port* s'il est capable d'envoyer la meilleure BPDU sur le segment réseau qu'il est connecté. Tous les ponts connectés à un segment donné, reçoivent les BPDU émis sur ce segment et s'accordent sur le pont envoyant la meilleure BPDU pour être le pont désigné sur ce segment. Le port correspondant à ce pont, est dit port désigné.
- *Alternate port* qui offre un chemin alternatif vers le pont racine au chemin fourni par le root port courant. Un *alternate port* fournit un chemin à un autre switch dans le réseau.
- Backup port qui est un port de secours ne pouvant exister que lorsque deux (02) ports sont connectés au même segment par une liaison point à point ou quand un switch possède au moins deux (2) liaisons sur un même segment du réseau. Le port backup fournit un autre chemin au switch.
- *Disabled port* qui est ce port qui n'a aucun rôle dans l'opération du Spanning-tree.

Dans une topologie stable ayant des rôles de ports bien définis, le RPVST+ s'assure que chaque port racine et port désigné passe en état d'acheminement tandis que les ports *alternate* et *backup* restent à l'état bloqué. (cf figure 10).

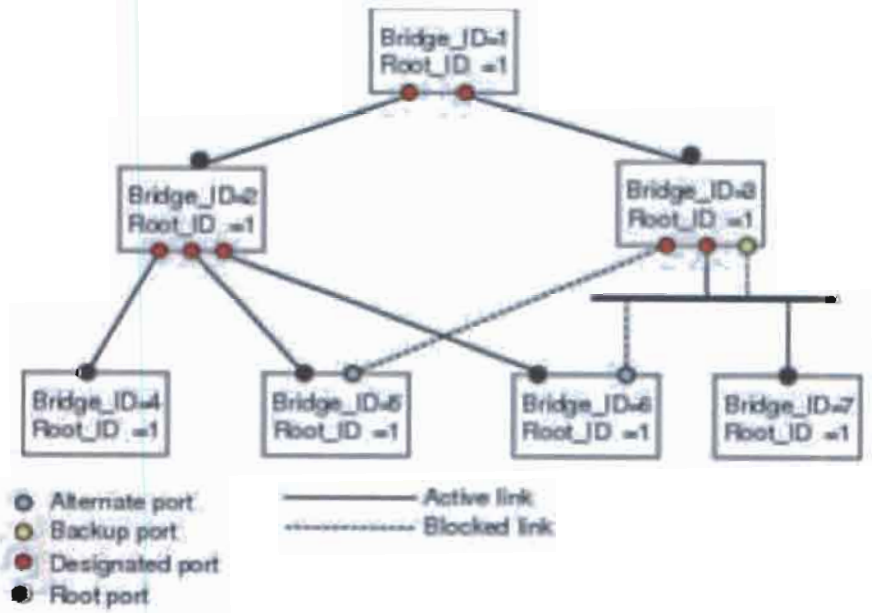

Figure 8 : Exemple de rôles des ports dans une topologie [13]

3.2. Les états des ports

L'arbre recouvrant toute la topologie est défini dès la fin de l'initialisation de l'ensemble des commutateurs. Si le port d'un commutateur passait directement de l'état de blocage à l'état d'acheminement, le port pourrait créer temporairement une boucle de données si le commutateur n'avait pas connaissance de toutes les informations de topologie à ce moment-là. Pour cette raison, le protocole RPVST+ introduit quatre (04) états de port. Les informations complémentaires présentées apès expliquent comment les états des ports garantissent qu'aucune boucle ne se forme durant la création de l'arbre recouvrant logique. Ainsi dans une configuration RPVST+, les ports du commutateur ne peuvent prendre que l'un des états suivant:

- *Blocking* où le port ne participe pas à l'acheminement des trames ;
- *Learning* où le port se prépare à participer à l'acheminement des trames et commence à enrichir la table d'adresses MAC ;
- *Forwarding* où le port est considéré comme intégré à la topologie active ; il achemine les trames, et il envoie et reçoit également des trames BPDU ;
- *Disabled* où le port ne participe pas à l'arbre recouvrant et n'achemine aucune trame est défini lorsque le port du commutateur est désactivé sur le plan administratif.

Lorsque le protocole STP est activé, tous les ports des commutateurs du réseau passent par l'état de blocage puis par les états intermédiaires d'écoute et d'identification à la mise sous tension. Les ports se stabilisent ensuite à l'état d'acheminement ou de blocage. Lors d'une modification de la topologie, un port passe temporairement par l'état d'écoute, puis d'identification pendant une période donnée appelée « temporisation de mise à jour ».

Lorsque l'algorithme STA met un port en état d'acheminement, les processus suivants se produisent :

- le port est mis en état bloqué en attendant l'instruction de passer à l'état d'apprentissage ;
- le port attend la fin du temps *delay timer,* bascule encore en état d'apprentissage et redémarre le *delay timer ;*
- dans l'état d'apprentissage, le port continue à bloquer la transmission de paquet et recueille des informations de localisation des postes de travail pour une future transmission des paquets ;
- le port attend la fin du *delay timer et* passe ensuite à l'état d'acheminement.

3.3. Le coût des ports

Le coût du chemin est déterminé en fonction du débit de l'interface et de la méthode de calcul utilisée. Lorsqu'une boucle se crée sur un segment, le protocole Spanning-tree considère le coût du port lorsqu'il sélectionne le port à mettre en état d'acheminement. La valeur des différents coûts des ports est donnée selon le débit et la méthode de calcul utilisée sur le tableau 6.

Nous pouvons donner un coût réduit au port pour que le RPVST+ le sélectionne en premier et une valeur plus élevée pour qu'il soit choisi en dernier. Si tous les ports ont le même coût alors le port ayant le plus petit numéro d'interface est mis en état d'acheminement et tous les autres ports sont bloqués. Sur les ports *access* le coût est donné par port. Sur les ports *trunk* le coût des ports est donné par VLAN. Le même coût de port peut être donné à tous les VLAN sur un port *trunk*.

Notons que le RPVST+ utilise par défaut la méthode courte pour le calcul du coût du chemin vers le pont racine codé sur 16 bits. Avec cette méthode, on peut donner n'importe quelles valeurs comprises entre 1 et 65 535. Egalement, nous pouvons configurer le switch pour qu'il utilise la méthode longue code sur 32 bits. Cette seconde méthode permet de choisir des valeurs entre 1 et 2 000 000. La méthode de calcul du coût des différents chemin est configurée de façon globale.

Tableau 9 : Valeur par défaut du cout des ports

Debit	Méthode courte
10 Mbit/s	100
100Mbit/s	19
1Gbit/s	4
10Gbit/s	2

3.4. La priorité des ports

Lorsque nous avons la formation d'une boucle et que plusieurs ports ont le même coût de chemin, le PVST+ considère la priorité des ports pour la sélection du port à mettre en état d'acheminement. La valeur de cette priorité est une donnée paramétrable. Ainsi, nous pouvons donner une valeur plus petite à la priorité du port si nous souhaitons que ce port soit choisi en premier par le RPVST+ ou une valeur plus grande sinon.

Si tous les ports ont la même priorité, alors le RPVST+ met le port ayant le plus petit numéro de port en état d'acheminement et bloque tous les autres ports. Les valeurs possibles de cette priorité varient de 0 à 224 et 128 est la valeur par défaut. Notons que si le port est configuré en mode *access* c'est la valeur du port qui est choisie comme priorité et la valeur du port VLAN comme priorité si le port est configuré en mode *trunk*.

IV. Les VLAN

1. Présentation

Les VLAN (Virtual Local Area Network), situés au niveau 2 du modèle OSI permettent de segmenter un support physique en plusieurs segments logiques. Il est ainsi possible de se passer de l'emplacement physique des équipements dans le réseau afin de réaliser la segmentation de celui-ci. Un VLAN Ethernet spécifique a le comportement d'un LAN Ethernet aux vues des couches supérieures. La norme 802.1Q qui a permis l'amélioration des VLAN sera utilisée dans le cadre de la mise en œuvre de la segmentation du réseau de la SOFITEX. Cette norme ajoute la fonctionnalité d'enregistrement dynamique des VLAN grâce au protocole GVRP. Par ailleurs elle introduit la possibilité de transmettre sur plusieurs instances de Spanning-Tree, ce qui permet de supprimer les problèmes liés à la mise en œuvre du Spanning-Tree sur un réseau utilisant les VLAN. Elle est la plus communément utilisée.

2. Les types de VLAN

Dans les équipements réseaux, l'association d'un VLAN à un port se fait par une table d'association. Ainsi les VLAN doivent être déclarés sur l'équipement. L'association à un VLAN peut se faire en fonction du port, d'une adresse MAC, d'un protocole, ou d'un sous réseau IP. Un port trunk sera associé aux VLAN qu'il autorise.

3. Fonctionnement

- **L'agrégation de VLAN**

La trame 802.1Q permet de distinguer l'appartenance d'une trame à un VLAN. De ce fait, il est possible sur un même lien de véhiculer des trames étiquetées avec des VID (Vlan Identifier) différents. On dit alors que le lien permet l'agrégation de VLAN, ce lien est dit " Trunk " ou " Tagged ". Pour cela les équipements reliant le lien trunk doivent nécessairement supporter l'encapsulation 802.1Q.

- **Mode d'association par port**

Nous aborderons uniquement le mode d'association par port puisque c'est ce mode qui sera utilisé dans notre solution VLAN.

Une trame non tagguée arrivant sur un port d'access ou un port ayant un PVID sera associé au VLAN correspondant. Elle ne peut être alors commutée que vers les ports access ayant le PVID identique, ou vers les ports trunks ayant au moins le VLAN autorisé.

Si une trame tagguée arrive sur un port access, elle sera systématiquement rejetée. Si une trame étiquétée avec un n° de VLAN arrive sur un port trunk, elle pourra être commutée que sur les ports d'access ayant le même PVID ou alors sur les ports trunk en conservant la même encapsulation.

Un lien trunk peut véhiculer des trames appartenant à plusieurs VLAN grâce à l'encapsulation 802.1Q.

4. Routage inter-VLAN

Les VLAN étant au niveau 2 du modèle OSI, l'interconnexion entre deux VLAN ne peut s'effectuer que par l'intermédiaire d'une passerelle de niveau 3. Il est donc nécessaire de réaliser du routage entre deux VLAN au même titre qu'entre deux réseaux Ethernet. Ce routage est réalisé entre des interfaces virtuelles (une par VLAN) de la même manière qu'il serait réalisé entre des interfaces physiques.

Pour router les trames entre deux VLANs, les switch de niveau 3 doivent pouvoir les détagguer puis les tagguer à nouveau avec le bon VID.

Les commutateurs aujourd'hui permettent d'associer un même VLAN à plusieurs interfaces physiques. Les routeurs réalisent alors une commutation entre leurs interfaces appartenant au même réseau virtuel (dans le cadre d'un même VLAN il n'y a à priori pas de routage).

5. La gestion centralisée des VLAN

La configuration statique nécessite, à chaque déclaration d'un nouveau VLAN, la déclaration de ce VLAN sur l'ensemble des Switch par lequel il transitera. Nous désirons donc que ce VLAN puisse se propager sur l'ensemble des ports trunk du réseau connectant des switch sur lesquels est relié ce VLAN. Pour cela, nous avons principalement deux protocoles à savoir le GVRP et le VTP.

Le protocole GVRP est directement proposé dans la norme 802.1P. Il permet de diffuser des informations sur les VLAN qui sont déclarés sur les ports d'un switch. Il permet de plus de configurer dynamiquement les VLAN déclarés sur les switch et de mettre à jour la table d'association des VLAN.

Quant au VTP, il permet de diffuser la déclaration des VLAN pour les ports trunk sur l'ensemble du réseau en réalisant une administration centralisée de ceux-ci. Il fonctionne avec une architecture client-serveur et est propriétaire CISCO.

Les switch peuvent être en mode :

- Serveur quand il est associé à un domaine VTP et que la déclaration des VLAN s'effectue en son sein avec la tenue à jour la liste des VLAN déclarés qui est diffusée à l'ensemble des clients.
- Client quand il est associé à un domaine VTP. Il reçoit la liste des VLAN, qu'il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.
- Transparent quand il n'est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mise à jour lorsqu'il reçoit une trame VTP. Cependant il propage les listes de VLAN qu'il reçoit.

Pour la gestion de nos VLAN, nous allons utiliser le protocole VTP car il est propriétaire CISCO et convient mieux avec nos équipements qui sont de cette marque. De plus, son administration est centralisée et aisée.

V. L'outil de supervision : NAGIOS

1. Présentation

Dans le monde professionnel, Nagios est connu comme un logiciel de supervision permettant la surveillance des composants d'infrastructures critiques y compris les applications, les services, les systèmes d'exploitation, les protocoles réseau, les paramètres du système et l'infrastructure de réseau. Nagios possède des moyens d'alerter les administrateurs en cas d'événements. Il est fiable même pour de très grands réseaux d'entreprise avec plusieurs milliers de machines (jusqu'à environ 3000 serveurs).

Anciennement appelé NetSaint, Nagios est actuellement un ensemble de produits classés dans deux catégories : payant et open source.

- Du côté payant, on trouve Nagios XI, le système de supervision dédié entreprise basé sur Nagios Core, ainsi que plusieurs autres produits ou services comme Nagios Fusion, Nagios Network Analyzer.
- Du côté open source, on trouve Nagios Core (le noyau), Nagios Plugins (des plugins), Nagios Frontends (l'interface web, Windows, Linux, des applications pour mobiles) et Nagios Configuration Tools (Outils et interfaces graphiques pour simplifier la configuration de Nagios Core).

Nagios est écrit en C et utilise un serveur Web Apache. Il fonctionne sous Linux et Unix, mais il y a également une version Windows nommé Nagwin.

Sur le marché des logiciels de supervision, il existe plusieurs logiciels basés sur Nagios comme par exemple : Icinga, Centreon, Overmon, Shinken, Vigilo, Eyesofnetwork, etc.

2. Fonctionnalités

Nagios récupère les informations fournies par les services de surveillance et les analysent. Si le résultat de cette analyse fait remonter un problème, les services de surveillance peuvent envoyer des avertissements à l'administrateur du réseau de différentes manières : courriers électroniques, messages instantanés, SMS. Il permet aussi :

- la surveillance des services réseaux tels que SMTP, HTTP, FTP, SSH ;
- la définition de la hiérarchie du réseau en utilisant des hôtes « parents », ce qui permet la détection des hôtes qui sont à l'arrêt ou injoignables;

- la définition des gestionnaires d'événements pour une résolution proactive des problèmes ;
- les notifications des contacts quand un hôte ou un service a un problème ;
- la définition des gestionnaires d'évènements qui s'exécutent pour des évènements sur des hôtes ou des services, pour une résolution proactive des problèmes ;
- la supervision à distance en utilisant SSH ou un tunnel SSL ;
- l'acquittement des alertes par les administrateurs. ;
- la gestion des escalades pour les alertes (une alerte non acquittée est envoyée à un groupe différent).

3. Fonctionnement

Nagios est un programme modulaire qui s'adapte facilement aux besoins grâce à l'utilisation de plugins. Nagios contient les parties principales suivantes :

- le noyau – Nagios Core correspondant un moteur léger qui offre les fonctionnalités essentielles de supervision, avec une portée limitée mais possédant plusieurs API pour les étendre. Ces fonctionnalités sont l'ordonnancement des contrôles, la vérification de l'exécution, la vérification des traitements, la gestion des événements et des alertes. Effectuer les vérifications, envoyer les notifications, traiter les données de performance et de nombreuses autres tâches sont généralement hors de portée pour Nagios Core et sont manipulés essentiellement par des Plugins.
- l'interface d'utilisateur – Nagios Frontends : à la base Nagios Core propose une interface par défaut de CGI (Common Gateway Interface). D'ailleurs, son interface d'utilisateur a été enrichie par l'interface web, des thèmes, l'interface Windows et Linux et des applications mobiles. Elle donne une vue d'ensemble du système d'information et des possibles anomalies.
- les plugins – Nagios Plugins: ce sont des extensions autonomes qui fournissent énormément de fonctionnalités au noyau. Ils sont sous forme de scripts ou de programmes exécutables que l'on peut compléter en fonction des besoins de chacun. On connaît environ 3000 plugins de Nagios dont environ 50 sont officiels. Ces plugins fonctionnent soit en local sur la

machine supervisée, soit s'exécutent à distance en utilisant des protocoles réseaux tels que HTTP, SMTP, SSH ou autres.

L'architecture de Nagios est représentée comme suit :

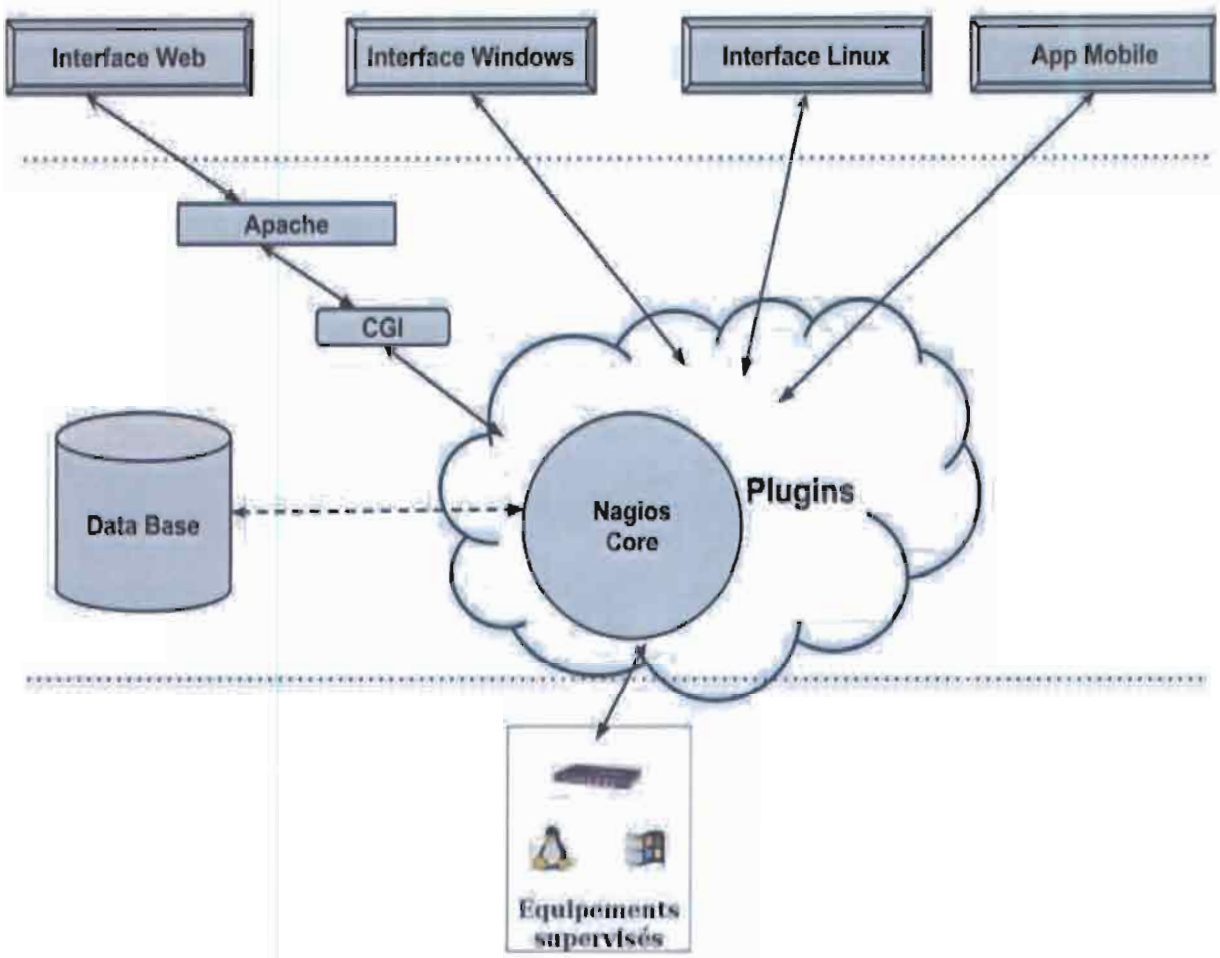

Figure 9 : L'architecture de Nagios [18]

Nagios propose deux manières de supervision des hôtes et des services à savoir la supervision active et la supervision passive.

- **Supervision active**

Généralement, Nagios utilise la supervision active. Ces principales caractéristiques sont les contrôles actifs initiés par le processus Nagios et les contrôles actifs gérés sur une base régulière. Le processus est illustré par la figure 13 suivante :

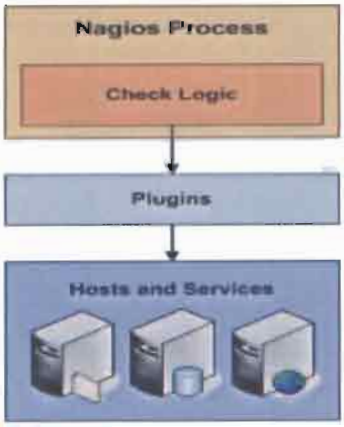

Figure 10 : Supervision active [18]

Les contrôles actifs sont initiés par le démon Nagios. Quand Nagios a besoin de vérifier le statut d'un hôte ou un service, il exécute un plugin et transmet des informations sur ce qui doit être vérifié. Le plugin va alors vérifier l'état de fonctionnement de l'hôte ou du service et renvoie ses résultats au démon Nagios. Nagios traite les résultats de vérification de l'hôte ou du service et prend les mesures appropriées si nécessaire.

- **Supervision passive**

Les principales caractéristiques de la supervision passive sont les contrôles passifs initiées et réalisées par les applications / processus externes et les résultats des contrôles passifs soumis à Nagios pour le traitement.

Les contrôles passifs sont utiles pour superviser des services qui sont soit asynchrones et ne peuvent pas être monitorés efficacement par des activités planifiés régulièrement, soit situés derrière un pare-feu et ne peuvent pas être contrôlés depuis l'hôte de surveillance. Le processus est illustré par la Figure 14 suivante.

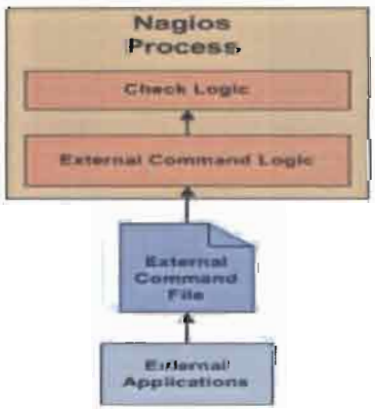

Figure 11 : Supervision passive [18]

- une application externe vérifie l'état d'un hôte ou d'un service.
- l'application externe écrit les résultats de la vérification au fichier de commandes externe.

- Nagios lit le fichier de commande externe, il mettra les résultats de tous les contrôles passifs dans une file d'attente pour un traitement ultérieur. La même file d'attente est utilisée pour stocker les résultats de contrôles actifs.
- Nagios vérifie régulièrement les événements et la file d'attente des résultats de la vérification. Chaque résultat de service qui se trouve dans la file d'attente est traité de la même manière.

4. Les sondes ou plugins

La force principale de Nagios est sa grande modularité qui lui permet de s'adapter facilement aux besoins des utilisateurs. Ils fonctionnent comme des applications autonomes, mais sont généralement conçus pour être exécutés par Nagios base.

Les plugins sont des codes binaires (écrits et compilés en C, C++, etc.) ou des scripts shell exécutables (shell, Php, Perl, etc.). En personnalisant des plugins, il faut respecter les codes retour qui sont :

- 0 OK (tout va bien) ;
- 1 WARNING (Alerte) ;
- 2 CRITICAL (Alerte critique) ;
- 3 UNKNOWN (impossible de connaître l'état du service).

L'avantage des plugins est que l'utilisateur peut les créer lui-même en fonction de ses besoins pour étendre les fonctionnalités du noyau.

Pour pouvoir administrer plus simplement Nagios et lui donner des fonctions de graphes évolués, nous lui ajouterons Centreon.

Chapitre 3 : IMPLEMENTATION DE LA SOLUTION

I. Mise en œuvre de la solution

1. Chronogramme du déploiement

La planification indique le calendrier général d'exécution des grandes étapes du projet. Ainsi, avec l'outil de gestion des projets, GANTT PROJET, nous allons proposer un chronogramme du déploiement de la solution. Le déploiement de la solution complète proposée tient en trois semaines.

Les différentes phases de ce déploiement sont :

- la définition des caractéristiques techniques et acquisition des matériels : commande 1e semaine, définition des caractéristiques techniques 1esemaine, 2eme semaine consultation des fournitures (SOFITEX), 1 mois pour livraison et exécution de la commande (fournisseur).
- le déploiement de l'architecture : cette partie qui comporte la mise en place des équipements actifs de la solution et la configuration de ces derniers s'étendra sur une (01) semaine.
- la mise en œuvre des VLAN : dans cette partie, il s'agira de mettre en place les différents VLANs, les configurer et faire éventuellement des tests. Cette phase durera deux (02) semaines.
- la mise en œuvre du RPVST+ : dans cette partie, nous allons mettre en place ce protocole sur les différents équipements de notre réseau afin de gérer la redondance. Cette phase durera deux (02) semaines.
- la mise en œuvre de l'outil de supervision : dans cette partie, il s'agira d'installer Nagios et Centrion, les configurer pour pouvoir permettre la supervision de l'ensemble du réseau. Elle durera deux semaines (02) et se fera en parallèle avec la mise en œuvre du VLAN.

Une marge d'une semaine sera envisagée afin de pouvoir finir l'ensemble du déploiement, comme le montre le chronogramme du déploiement présenté à la Figure 12.

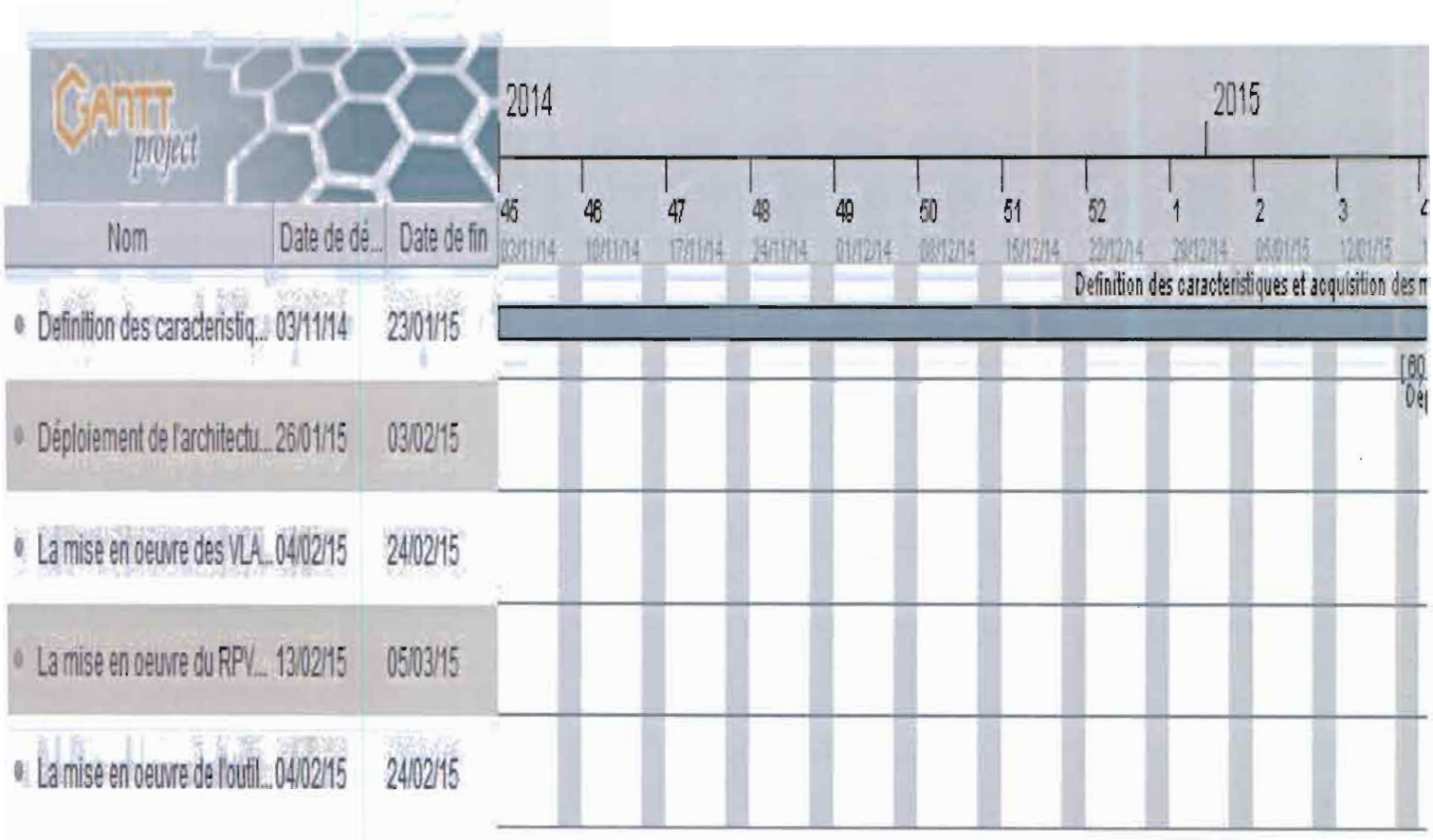

Figure 12 : Chronogramme de déploiement prévisionnel.

2. Mise en œuvre

2.1. Architecture

L'implémentation de l'architecture hiérarchisée en trois couches dans le réseau de la SOFITEX donne le résultat illustré sur la Figure 13. Nous aurons donc deux (02) cœurs, chacun étant redondant et localisés au niveau de la Direction générale et du CMGS. Le cœur situé à la Direction Générale sera relié aux distributions de celle-ci dénommé distribution centre-ville. Le second cœur sera quant à lui relié aux distributions CMGS (distribution ZI I) et Bobo III (distribution ZI II). Enfin, les distributions sont reliées aux différents accès.

La Figure 13 présente la structure finale du réseau de la SOFITEX avec ses différents composants.

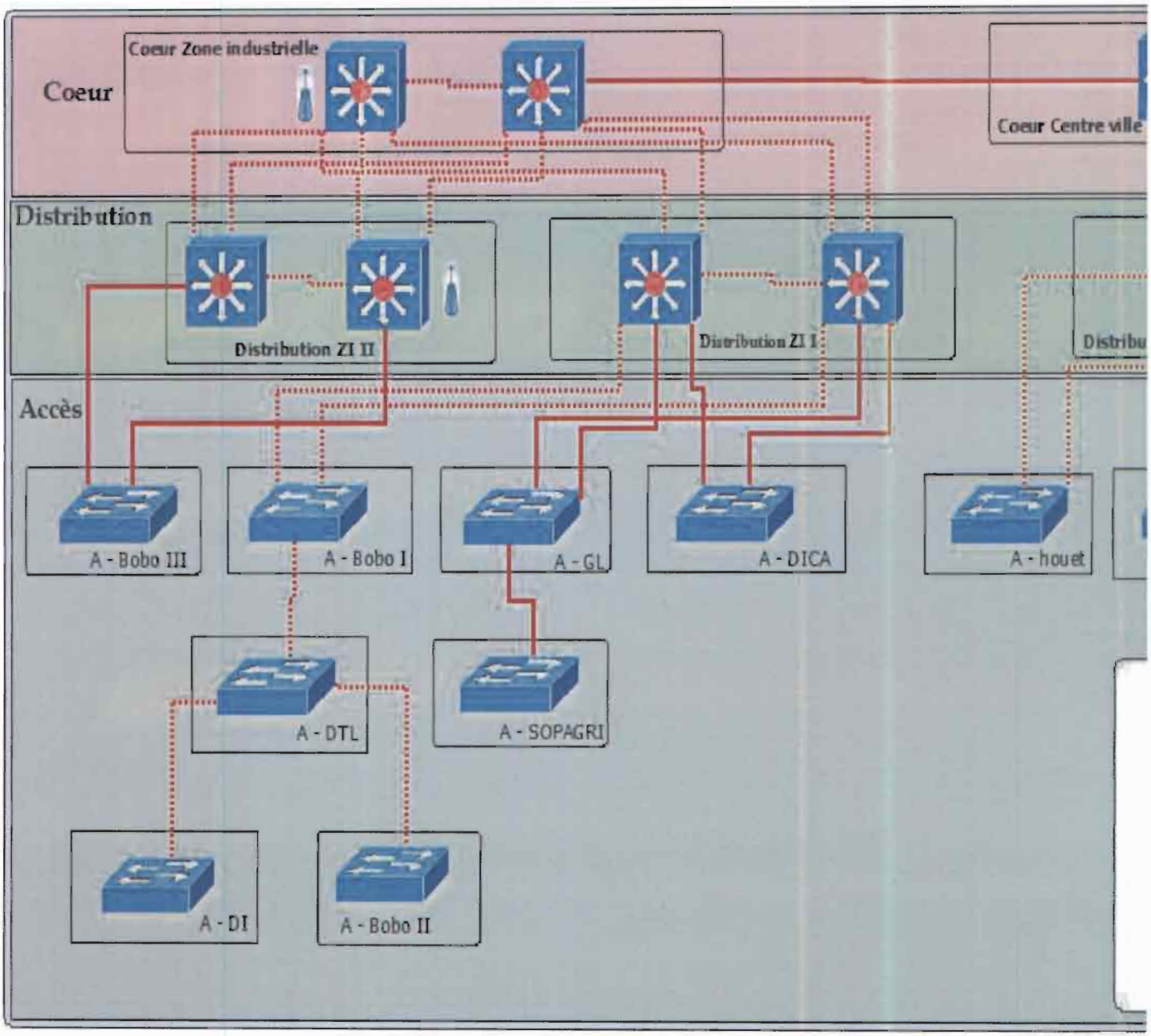

Figure 13 : Architecture hiérarchisée en trois couches

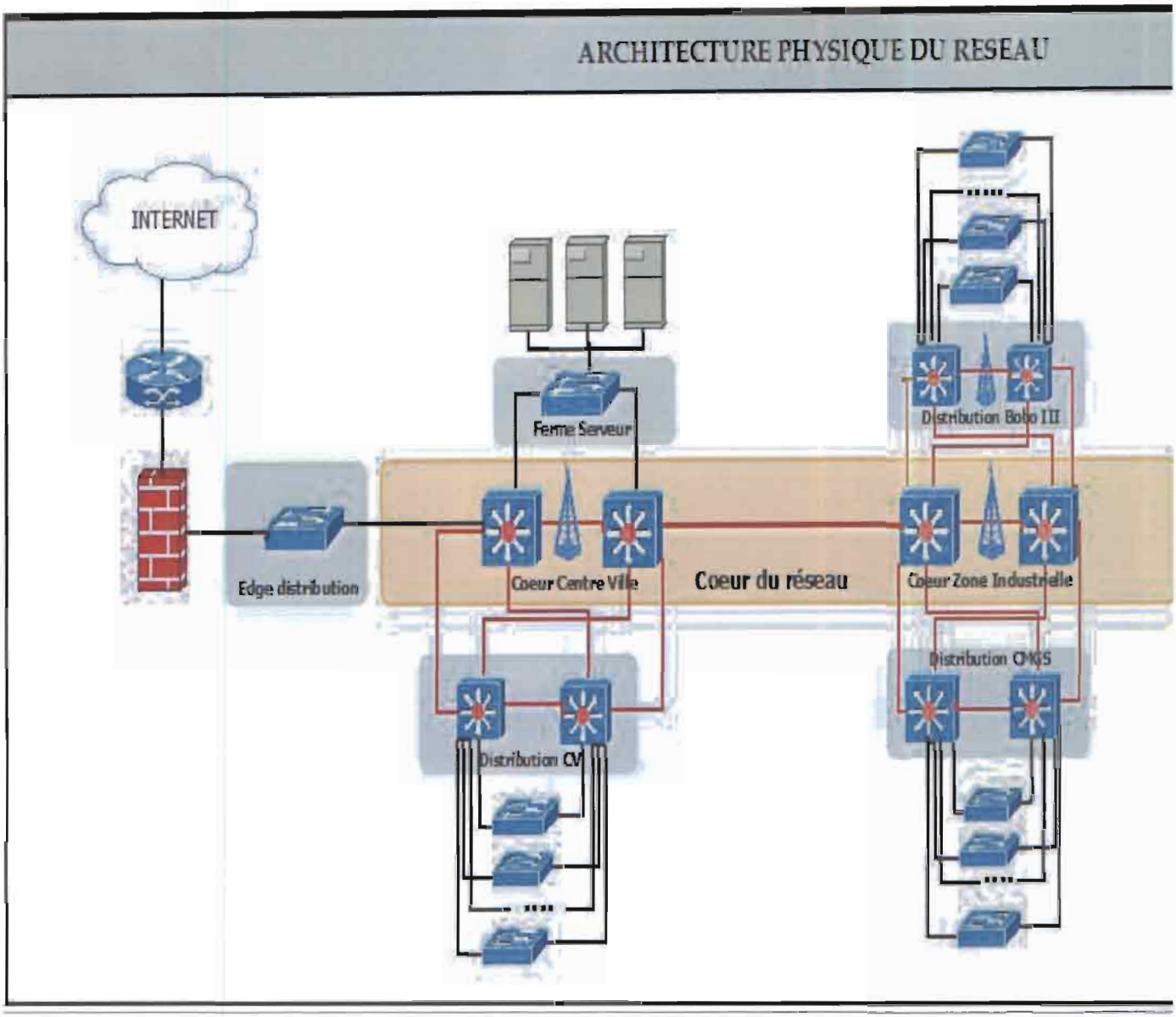

Figure 14 : Architecture physique du réseau

2.2. Les VLAN

2.2.1. Les différents VlAN à implémenter

Après analyse, nous avons défini dix (10) VLAN répartis comme suit :

- VLAN administration (VLAN 10) ;
- VLAN Serveur (VLAN 20) ;
- VLAN Siège (VLAN 30) ;
- VLAN Houet (VLAN 40) ;
- VLAN DEP (VLAN 50) ;
- VLAN GL comportant les locaux Garage Lourds et SOPAGRI (VLAN 60) ;
- VLAN ZI1 composé des locaux Bobo I, DTL, Bobo II et DI (VLAN 70) ;
- VLAN CMGS (VLAN 80) ;
- VLAN Bobo III (VLAN 90) ;
- VLAN DICA (VLAN 100).

Notons que nous avons fait le choix de numéroter les VLAN par 10 qui sera respecté chaque fois qu'un VLAN sera ajouté.

2.2.2. Configurations générales

- **Définition des VLAN** : Création du vlan 10 puis des vlans 20,30 et 40

```
SA0/1-siège-24 (config)#vlan 20
SA0/1-siège-24 (config-vlan)#name serveur
SA0/1-siège-24 (config-vlan)#ex
SA0/1-siège-24 (config)#vlan 30
SA0/1-siège-24 (config-vlan)#ex
SA0/1-siège-24 (config)#
```

- **Création des liens Trunk 802.1q**

```
SA0/1-siège-24(config)# interface fastethernet 0/1
SA0/1-siège-24(config-if)# shutdown
SA0/1-siège-24(config-if)# switchport trunk encapsulation dot1q
SA0/1-siège-24(config-if)# switchport mode trunk
SA0/1-siège-24(config-if)# no shutdown
```

- **Configuration des ports attribués aux VLAN**

```
SA0/1-siège-24#conf t
SA0/1-siège-24(config)#int fastEthernet 0/1
SA0/1-siège-24(config-if)# switchport mode access
SA0/1-siège-24(config-if)# switchport access vlan 10
```

- **Suppression de la configuration d'un port**

Pour cela, il suffit de mettre la commande no devant les commandes entrées précédemment.

```
SA0/1-siège-24(config)#int fastEthernet 0/1
SA0/1-siège-24(config-if)#no switchport access vlan
SA0/1-siège-24(config-if)#end
```

2.2.3. Gestion des VLAN (VTP)

Le protocole de jonction VLAN (VTP) réduit la gestion dans un réseau commuté. Quand on configure un nouveau VLAN sur un serveur VTP, le VLAN est distribué par tous les commutateurs dans le domaine. Ceci réduit la nécessité de configurer le même VLAN partout. VTP est un protocole propriétaire de Cisco qui est disponible sur la plupart des produits de la gamme Cisco Catalyst.

```
SA0/1-siège-24>enable
SA0/1-siège-24#configure terminal
SA0/1-siège-24 (config)#interface {type d'interface} [numéro d'interface]
SA0/1-siège-24 (config-if)# switchport mode trunk
```

- **Configurer les interconnexions en tant que liens Trunk**

Cette manipulation est à répéter sur chaque interface servant d'interconnexion. Pour vérifier la bonne configuration on peut lancer la commande suivante :

```
SA0/1-siège-24#show interfaces trunk
```

- **Configurer les serveurs VTP**

Cette manipulation est à répéter sur chaque switch servant de serveur VTP. Pour ce faire on utilise la commande suivante :

```
Switch>enable
Switch#configure terminal
Switch(config)#vtp domain CentreVille
Switch(config)#vtp password Sofitex
Switch(config)#vtp version 2
Switch(config)#vtp mode server
```

Pour vérifier la configuration on tape la commande suivante

```
Switch#show vtp status
```

- **Configurer les clients VTP**

Cette manipulation est à répéter sur chaque switch servant de client VTP. La commande suivante utilisée est:

```
Switch>enable
Switch#configure terminal
Switch(config)#vtp mode client
Switch(config)#vtp password Sofitex
```

Pour vérifier la configuration on tape la commande suivante:

```
Switch#show vtp status
```

- **Ajouter les VLAN au serveur VTP principal**

```
Switch>enable
Switch#configure terminal
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name DG
```

2.3. Rapid – PVST+

Dans cette partie, nous nous appuierons sur la partie centre-ville du réseau. Les commandes utilisées sont valables pour le reste du réseau. Pour la mise en œuvre du Rapid-PVST+, nous allons activer ce protocole sur tous les commutateurs du réseau. Ensuite, les différents switch racines pour un ensemble de Vlan seront définis au niveau des switch de distribution. Par exemple, le Switch SW-D1-CV sera racine pour l'arbre de recouvrement des VLAN (20, 30, 40, 10) et secondaire pour le VLAN (50) tandis que le SW-D2-CV sera racine pour le VLAN

(50) et racine secondaire pour les VLAN (20, 30, 40, 10). Avec cette séparation des VLAN sur les équipements, on a une partage de charge donc un gain de performance.

- Activation du RPVST+ sur l'ensemble des switch du réseau :

```
SW-D1-CV>enable
SW-D1-CV#configure terminal
SW-D1-CV(config)#spanning-tree mode rapid-pvst
```

- Définition des commutateurs racines :

```
SW-D1-CV >enable
SW-D1-CV#configure terminal
SW-D1-CV(config)#spanning-tree vlan 20,30,40,10 root primary
SW-D1-CV(config)#spanning-tree vlan 50 root Secondary
```

L'utilisation de cette commande définira la priorité du switch a 24576 pour les VLAN 20, 30, 40 et à 28676 pour le VLAN 50. Si un autre switch avait une priorité plus faible que les 24576 du switch racine celui-ci changera sa priorité à une valeur plus faible et restera ainsi la racine.

- Définition d'une priorité de port

```
SW-D1-CV >enable
SW-D1-CV #configure terminal
SW-D1-CV(config)#int fa0/2
SW-D1-CV(config-if)#spanning-tree vlan 30,40 port-priority 64
SW-D1-CV(config-if)#ex
```

Cette commande rendra l'interface fa0/2 du switch prioritaire pour le transit des trames des VLAN 30 et 40.

- Activation du portfast sur tous les ports non trunk au niveau des switch d'accès.

```
Sw-A1R-DG>enable
Sw-A1R-DG #configure terminal
Sw-A1R-DG (config)#spanning-tree portfast
```

L'utilisation de cette commande permet d'utiliser un spanning-tree plus rapide qui économise les 2 états consommateurs de temps : listening et learning, pour ne garder que blocking et forwarding, le switch supposant alors qu'il est connecté à un équipement terminal.

- Activation du bpduguard

```
Sw-A1R-DG >enable
Sw-A1R-DG #configure terminal
Sw-A1R-DG (config-vlan)#spanning-tree bpduguard enable
```

Cette commande est liée au passage en portfast : un port configuré en portfast ne doit pas normalement recevoir de Brigde Protocil Data Unit (BPDU) vu qu'il n'est pas connecté à un autre switch et donc s'il en reçoit, c'est une erreur de connexion. *Spanning-tree bpduguard enable* permet de désactiver un port configuré en portfast dès qu'il reçoit une BPDU. Cela permet donc de bloquer la connexion de switch « fantôme » sur le réseau.

2.4. Nagios

Pour mettre en œuvre Nagios et Centreon, nous avons installé VMware sur notre ordinateur afin de virtualiser un réseau LAN contenant :

- un serveur Linux nommé « ubuntu » sur lequel sera installé Nagios pour superviser notre réseau. Il aura pour IP 172.16.2.177. Il est sous Ubuntu 10.04.
- un serveur Windows « winprod » qui sera supervisé. Il aura pour IP 172.16.2.128.
- un switch nommé « switch » que l'on supervisera également. Il aura pour IP 172.16.2.1.

2.4.1. Installation de Nagios

Les étapes pour installer Nagios se présentent comme suit :

- Mettre à niveau l'existant

```
# apt-get update
# apt-get upgrade
```

- Installer les librairies de développement de bases, du serveur web et de Nagios

```
# apt-get install apache2 libapache2-mod-php5 php5-gd php5 make gcc build-essential wget libgd-gd2-perl libgd2-xpm libgd2-xpm-dev libnet-snmp-perl libssl-dev snmp daemon
```

- Créer un groupe

```
# groupadd nagios
```

- Créer un compte utilisateur « nagios » que nous allons mettre dans le groupe

```
# useradd -m -g nagios nagios
```

- Attribution d'un mot de passe à l'utilisateur « nagios ». Ce mot de passe est « nagios ».

```
# passwd nagios
```

- Créer un groupe « nagcmd » permettant l'exécution des commandes externes à travers l'interface Web. Ajouter les utilisateurs Nagios et Apache à l'intérieur du groupe « nagcmd »

```
# groupadd nagcmd
# usermod -g nagcmd nagios
# usermod -g nagcmd www-data
```

- Télécharger Nagios et ses plugins

Créer un répertoire /nagios/download dans lequel nous déposerons les archives à installer.

```
# mkdir -p /nagios/download
# cd /nagios/download
# wget http://prdownloads.sourceforge.net/sourceforge/nagios/ nagios-4.0.1.tar.gz
# wget http://www.nagios-plugins.org/download/nagiosplugins- 1.5.tar.gz
# ls –alh
```

- Compiler et installer Nagios

Extraire le code source de l'archive de Nagios

```
# cd /nagios/download/
# tar -xzf nagios-4.0.1.tar.gz
```

Exécuter le script de configuration en lui précisant le nom du groupe créé précédemment.

```
# cd nagios-4.0.1/
# ./configure --with-command-group=nagcmd
```

- Compiler le code source de Nagios

```
# make all
```

- Installer les binaires.

```
# make install
```

- Installer les scripts de démarrage.

```
# make install-init
```

- Installer les fichiers de configuration. Les fichiers seront automatiquement installés dans le répertoire /usr/local/nagios/etc.

```
# make install-config
```

- Installer et configurer les permissions.

```
# make install-commandmode
```

- Personnaliser la configuration de Nagios

Éditons le fichier contacts.cfg pour y mettre les informations de l'administrateur de Nagios, notamment l'adresse électronique où les alertes seront envoyées.

```
# gedit /usr/local/nagios/etc/objects/contacts.cfg
```

Le renseignement de l'adresse mail ne suffit pas pour que les envois de mails se fassent par Nagios. Il faut que le serveur ait un serveur de messagerie activé (sendmail, postfix…).

- Configurer l'interface web

Installer le fichier de configuration de Nagios dans le répertoire conf.d d'Apache.

```
# make install-webconf
```

Créer un compte « nagiosadmin » pour se connecter à la page web Nagios.

```
# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Le mot de passe choisi est « nagios»

- Redémarrer le service apache2

```
#service apache2 reload
```

- Décompresser, compiler et installer les sources

```
# cd /nagios/download/
# tar -xzf nagios-plugins-1.5.tar.gz
# cd nagios-plugins-1.5/
# ./configure --with-nagios-user=nagios --with-nagios-group=nagios
# make
# make install
```

- Lancer Nagios et Apache2 au démarrage du serveur

```
# update-rc.d nagios defaults
```

- Démarrer Nagios

```
# /etc/init.d/nagios start
```

- Changer la permission de ce répertoire /usr/local/nagios/var/rw afin de pouvoir effectuer certaines actions depuis l'interface Nagios.

```
# chown nagios.nagcmd /usr/local/nagios/var/rw
```

Maintenant nous pouvons nous connecter à Nagios via le lien suivant : http://localhost/nagios.

2.4.2. Configuration de Nagios

- Surveiller en local

Certains services sont par défaut surveillés, notamment le swap, l'espace disque de la partition root /, le ping, etc. Par exemple, pour vérifier l'espace disque on fait :

```
# /usr/local/nagios/libexec/check_disk -w 20% -c 10% -p / -u GB
```

Pour les autres services, le principe est le même.

- Surveiller une machine qui se trouve sous Windows

Le greffon check_nt qui communique avec NSClient++ et étant déjà installé sur Nagios, nous allons installer maintenant l'addon NSClient++ sur la machine Windows. Nous allons éditer le fichier « /usr/local/nagios/etc/objects/commands.cfg » afin de changer le mot de passe qui sera utilisé pour surveiller la machine Windows.

 # /usr/local/nagios/etc/objects/commands.cfg (le mot de passe choisi pour notre cas est pwdwin).

On télécharge sur le site http://nsclient.org et on récupère NSClient++-0.3.9-Win32.msi.Rappellons que notre machine Windows s'appelle « winprod ».

- Installation de l'agent

Une fois le fichier MSI téléchargé, on l'installe sur la machine winprod. On met l'adresse IP de notre serveur Nagios (172.16.2.177), on peut aussi mettre le nom DNS si notre réseau en dispose d'un. On précise un mot de passe, ensuite on active les champs plugins, check_nt et check_nrpe. On ouvre maintenant le gestionnaire de service afin de s'assurer que le service

NSClient est autorisé à interagir avec le bureau. Maintenant, il faut ouvrir le fichier « NSC.ini» qui se trouve à cet emplacement : C:\Program Files\NSClient++\.

Dans la section [modules], on décommente tous les modules listés exceptés CheckWMI.dll et RemoteConfiguration.dll.

Dans la section [Settings], nous devons avoir ces deux lignes :

```
password=pwdwin
allowed_hosts=172.16.2.177
```

- Configuration de Nagios

Sur le serveur Nagios, on édite le fichier de configuration de Nagios.

```
# gedit /usr/local/nagios/etc/nagios.cfg
```

Si nous décommentons la ligne avec windows.cfg, nous disons à Nagios de regarder le fichier windows.cfg pour y trouver les définitions des hôtes Windows. Cette méthode nous permet de définir toutes nos machines Windows dans le même fichier.

Modifions le fichier en remplaçant winserver par winprod (nom de notre serveur Windows). Puis changeons l'adresse IP par la nôtre. Pour vérifier si tout est correct, on applique la commande suivante :

```
#/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

On peut redémarrer Nagios (sous root) et vérifier sur notre site Nagios http://localhost/nagios

- Surveiller un switch

Il existe un fichier d'exemple de configuration pour les switch (/usr/local/nagios/etc/objects/switch.cfg), on crée un répertoire /usr/local/nagios/etc/switches et on rajoute ce fichier à l'intérieur.

```
# cp /usr/local/nagios/etc/objects/switch.cfg /usr/local/nagios/etc/switches/switch3com
```

Dans nagios.cfg, par défaut la ligne définissant le chemin où trouver les fichiers de configuration des switch existe déjà mais elle est commentée, il suffit donc de la décommenter. Ensuite, on modifie notre fichier /usr/local/nagios/etc/switches/switch3com.cfg en précisant l'adresse IP du switch. On enlève la section hostgroup pour le mettre dans un fichier à part. Il ne reste plus qu'à redémarrer Nagios.

```
# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
# /etc/init.d/nagios stop; pkill nagios; /etc/init.d/nagios start
```

Le service de switch lance une commande SNMP avec pour arguments –C public -o ifOperStatus.1 -r 1 -m RFC1213-MIB [-o ifOperStatus. 1 fait référence à OID pour l'état opérationnel du port 1 sur le switch.

L'option -r 1 indique au plugin check_snmp de retourner un état OK si 1 est trouvé dans la réponse SNMP (1 indique que le port est up) et CRITICAL sinon. L'option -m RFC1213-MIB est facultative et indique la MIB à utiliser parmi celles installées sur notre système et peut aider à accélérer les choses :

```
# Monitor Port 1 status via SNMP
```

Pour trouver les OID qui peuvent être supervisés sur un switch, on exécute la commande suivante :

```
#snmpwalk -v1 -c public IP_DE_VOTRE_SWITCH (172.16.2.1 dans notre cas) -m ALL
```

Nous pouvons ainsi surveiller notre switch sur le site.

Les étapes de l'installation de Centreon seront présentées en annexe 1.

3. Simulation du réseau de la SOFITEX

Cette simulation est réalisée via l'outil didactique de simulation réseau Packet tracer dans sa version 6. Pour l'implémentation du réseau, nous avons choisi des switch multi niveau pour la couche cœur et distribution, les autres switch sont de la gamme 2960. Egalement pour des soucis de présentation, nous n'avons pas représenté tous les switch présents dans l'architecture finale du réseau.

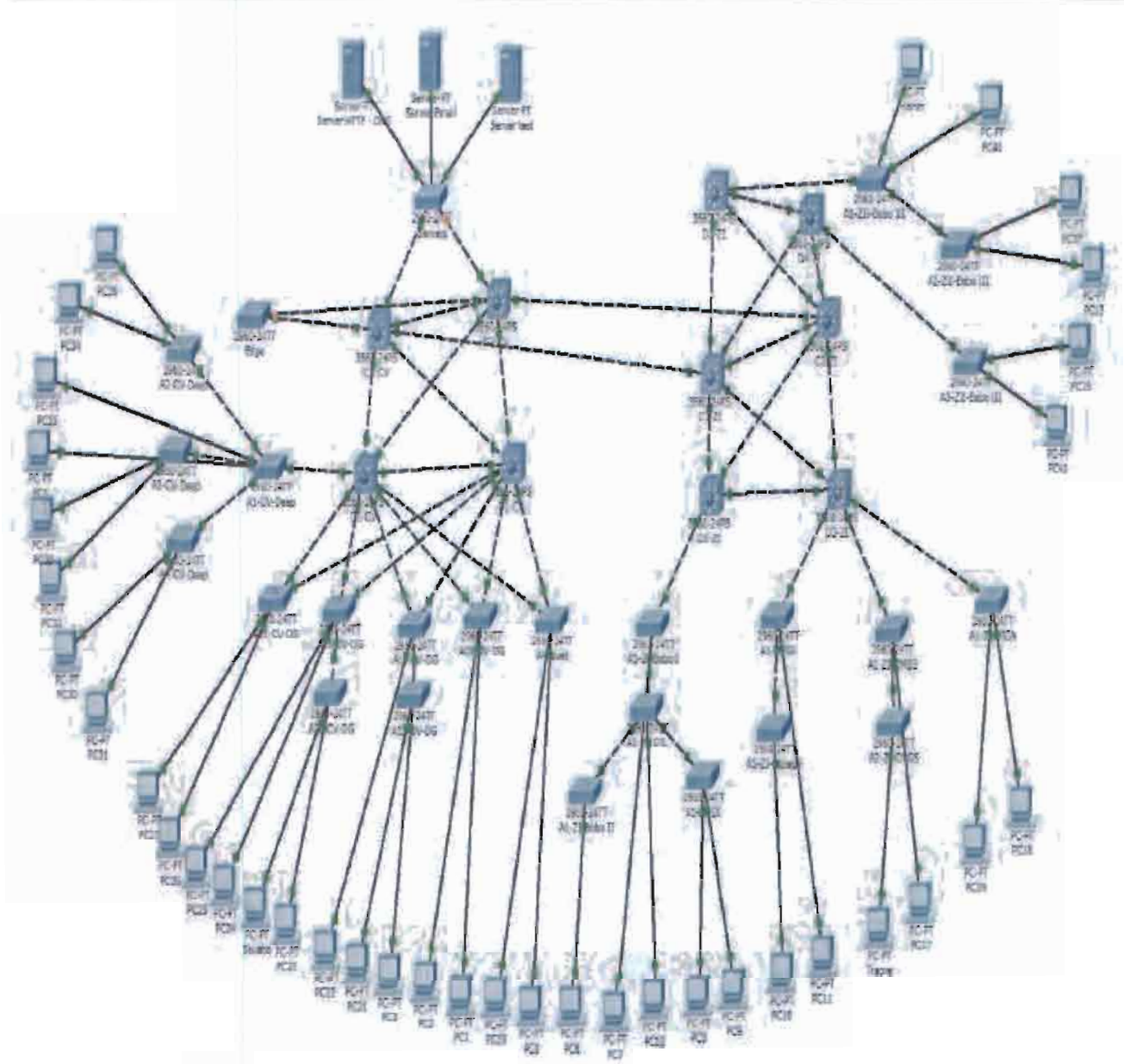

Figure 15 : réseau de simulation

Une fois les différents switch inter connectés, nous passons à la phase de configuration. Pour ce faire nous allons suivre les étapes suivantes.

3.1. Identification et configuration des ports trunk

Sur chaque switch du cœur et distribution, les ports Fa0/1-4 et Gi0/1-2 sont configurés en ports trunk. Egalement deux (02) ports sont identifiés et configurés en trunk sur les autres switchs.

- **Commande pour switch multi niveau**

```
en
!
conf t
!
int range fastethernet 0/1-4
!
switchport trunk encapsulation dot1q
!
switchport mode trunk
!
no shut
!
end
!
```

- **Commande pour les switch 2960**

```
en
!
conf t
!
int range fastethernet 0/4 -24
!
switchport mode trunk
!
no shut
!
end
!
```

3.2. Mise en œuvre du VTP et définition des VLAN

Le serveur STP sera défini sur le switch D1-CV. Les autres switchs du réseau seront configurés en client VTP. La définition des VLAN est effectuée sur le serveur et sera propagée par les switch via les ports trunk aux différents switch du réseau.

- **Configuration du serveur VTP**

```
vtp domain CentreVille
!
vtp password sofitex
!
vtp version 2
!
vtp mode server
```

- **Configuration des clients vtp**

```
en
!
conf t
!
vtp mode client
!
vtp password sofitex
!
end
!
```

- **Définition des différents VLAN**

```
en
!
conf t
!
vlan 10
!
name Administrateur
!
ex
!
vlan 20
!
name Serveur
!
ex
!
vlan 30
!
name DG
!
ex
!
```

3.3. Affectation des VLAN aux différents ports des switch Access

En fonction des différents locaux, nous avons le vlan qui y sied. En guise d'exemple le VLAN 30 est pour le DG et 40 pour le DEEP.

Nous aurons donc par défaut sur les interfaces fastEthernet Fa0/4-24 l'affectation des différents VLAN.

- **Commande pour les VLAN admin, serveur, DG et DEEP**

```
#VLAN administrateur
en
!
conf t
!
int range fa 0/12-14
!
switchport mode access
!
switchport access vlan 10
!
end
!

# VLAN serveur
en
!
conf t
!
int range fa 0/4-24
!
switchport mode access
!
switchport access vlan 20
!
end
!

#Vlan DG
en
!
conf t
!
int range fa 0/4-24
!
switchport mode access
!
switchport access vlan 30
!
end
!

#Vlan Deep
en
!
conf t
!
int range fa 0/4-24
!
switchport mode access
!
switchport access vlan 40
!
```

3.4. Adressage IP

Pour réaliser l'adressage IP de notre réseau de simulation, nous avons fait le choix de la réaliser via le DHCP qui sera défini sur le switch D1-CV.

Pour ce faire nous allons définir une plage d'adressage pour chaque VLAN. Nous aurons donc à titre indicatif :

- **Commande pour le DHCP de la DG**

```
en
!
conf t
!
ip dhcp pool DG
!
network 192.168.30.0 255.255.255.0
!
default-router 192.168.30.1
!
dns-server 192.168.20.100
!
ex
!
```

- **Application des adresses IP aux différentes interfaces VLAN**

```
#vlan DG
en
!
conf t
!
interface vlan 30
!
ip address 192.168.30.1 255.255.255.0
!
ex
```

3.5. Routage Inter VLAN

A l'étape 4, les différents Vlan sont disponibles et accessibles depuis les postes utilisateur via les adressages IP définies à cet effet mais ne peuvent pas communiquer entre eux. Vu que nous sommes sur un switch L3, il faut activer la fonction de routage. Cela se fait via la commande ***ip routing***. A travers l'activation de cette commande nos Vlans peuvent communiquer ensemble.

```
En
!
Conf t
!
Ip routing
!
End
!
```

Notons que notre objectif n'est pas de permettre la communication inter VLAN complète. Les VLAN ne doivent pas communiquer directement entre eux. Seul le VLAN serveur est autorisé à échanger avec l'ensemble des VLAN. Pour réaliser ce filtrage, nous avons défini des ACL, des ACL étendus pour être plus précis. Les ACL suivants sont définis sur le D1-CV.

- **Commande des ACL**

```
#on defini l'ACL et on applique cela sur une interface
en
!
conf t
!
access-list 101 permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
!
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
!
access-list 101 permit ip 192.168.30.0 0.0.0.255 192.168.30.0 0.0.0.255
!
access-list 101 deny ip 192.168.30.0 0.0.0.255 any
!
int vlan 30
!
ip access-group 101 out
!
##
ex
!
access-list 102 permit ip 192.168.40.0 0.0.0.255 192.168.20.0 0.0.0.255
!
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
!
access-list 102 permit ip 192.168.40.0 0.0.0.255 192.168.40.0 0.0.0.255
!
access-list 102 deny ip 192.168.40.0 0.0.0.255 any
!
int vlan 40
!
ip access-group 102 out
!
ex
!
```

3.6. Activation du STP (Rapid-pvst) sur l'ensemble des switch du réseau

Le STP dans sa variante PVST est déjà activé par défaut sur les switch CISCO, nous aurons donc à activer le rapid-pvst sur l'ensemble des switch.

- **Commande STP**

```
#D1-CV
en
!
conf t
!
spanning-tree mode rapid-pvst
!
spanning-tree vlan 10,20,30,40 root primary
!
spanning-tree vlan 50 root secondary
!
end
!
```

Une fois l'activation faite, nous devons définir les ports d'extrémités comme étant des portfast et activer en même temps le bpduguard.

- **Commandes portfast et bpduguard**

```
en
!
conf t
!
spanning-tree mode rapid-pvst
!
int range fa 0/4-24
!
spanning-tree portfast
!
spanning-tree bpduguard enable
!
end
!
```

3.7. Test de vérification

Afin de vérifier la bonne marche de nos configurations, nous allons effectuer des tests à travers l'implémentation d'un server DNS, HTTP, E-mail. Les serveurs DNS et Email seront configurés sur le même serveur physique et l'E-mail sur un serveur indépendant. Les captures d'écran des figures 16 à 19 montrent aussi bien un exemple de configuration de serveur mail que de test d'envoi et de réception de mail dans l'outil Packet Tracer.

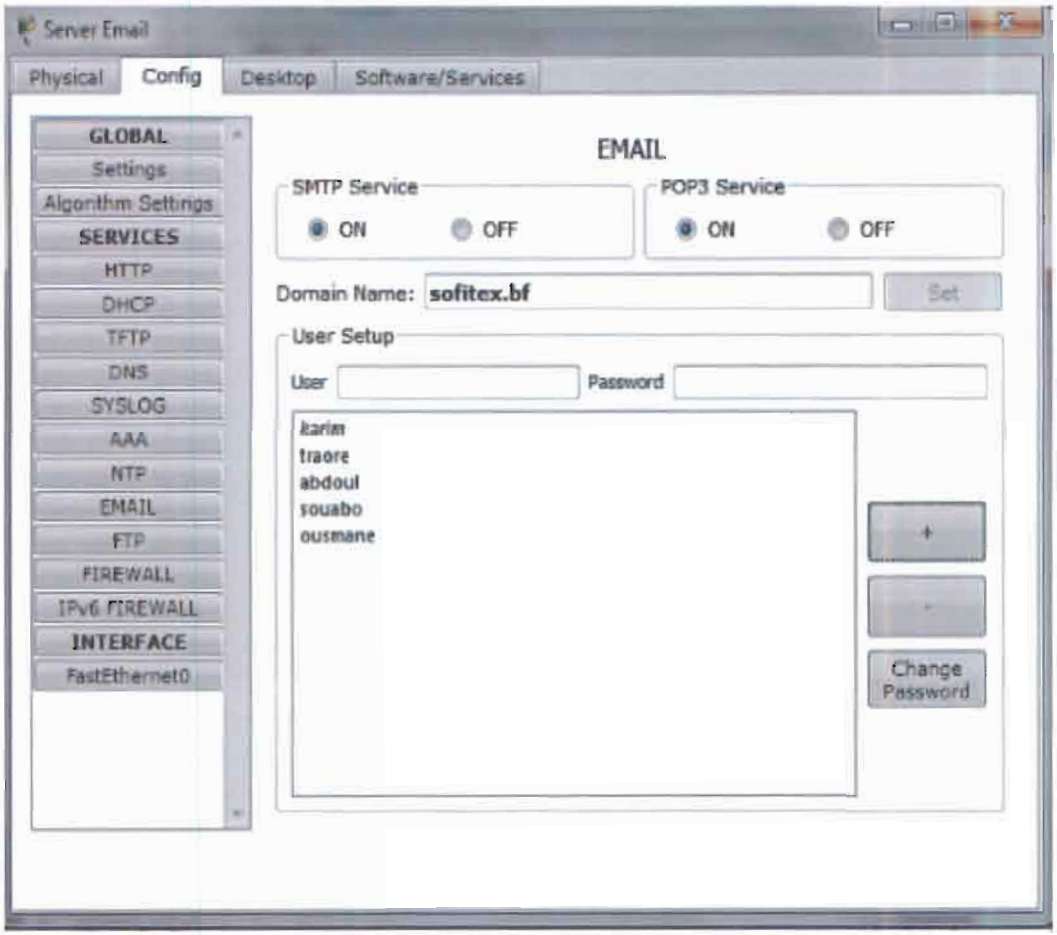

Figure 16 : configuration du serveur mail

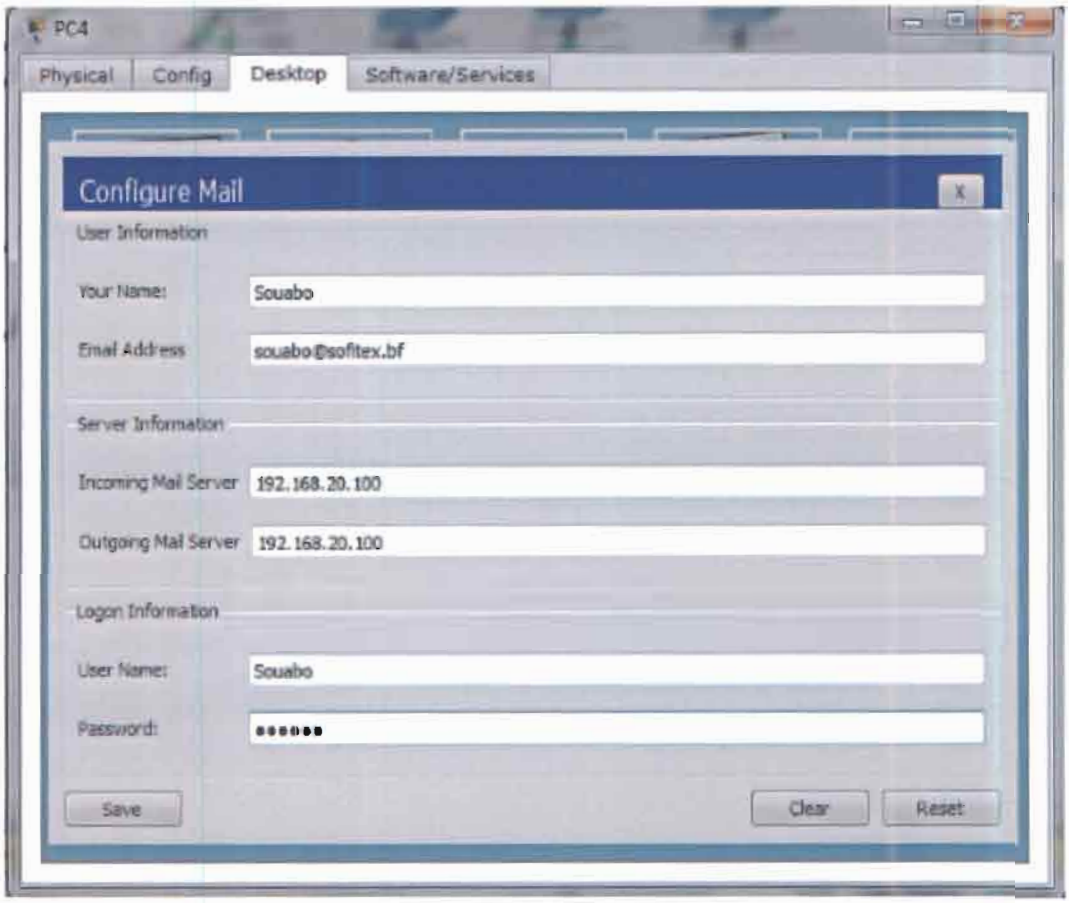

Figure 17 : Configuration du mail sur un PC client

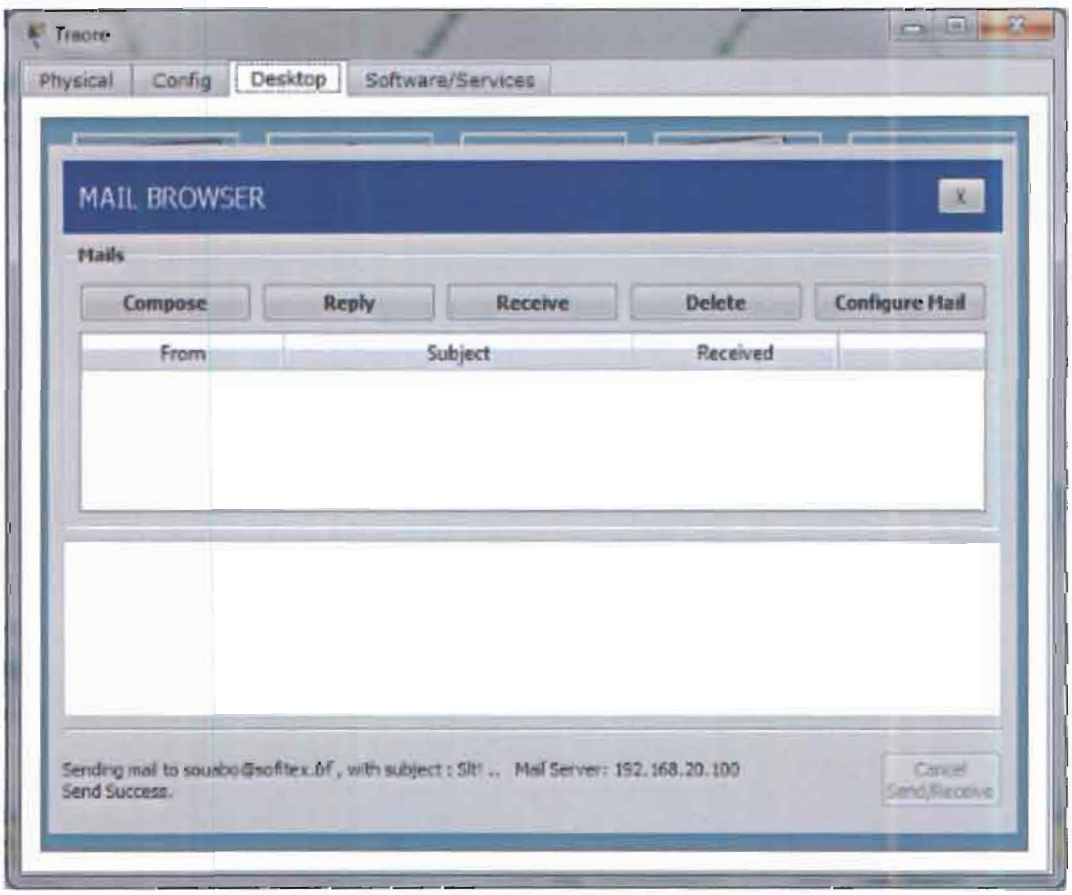

Figure 18 : Envoi d'un mail

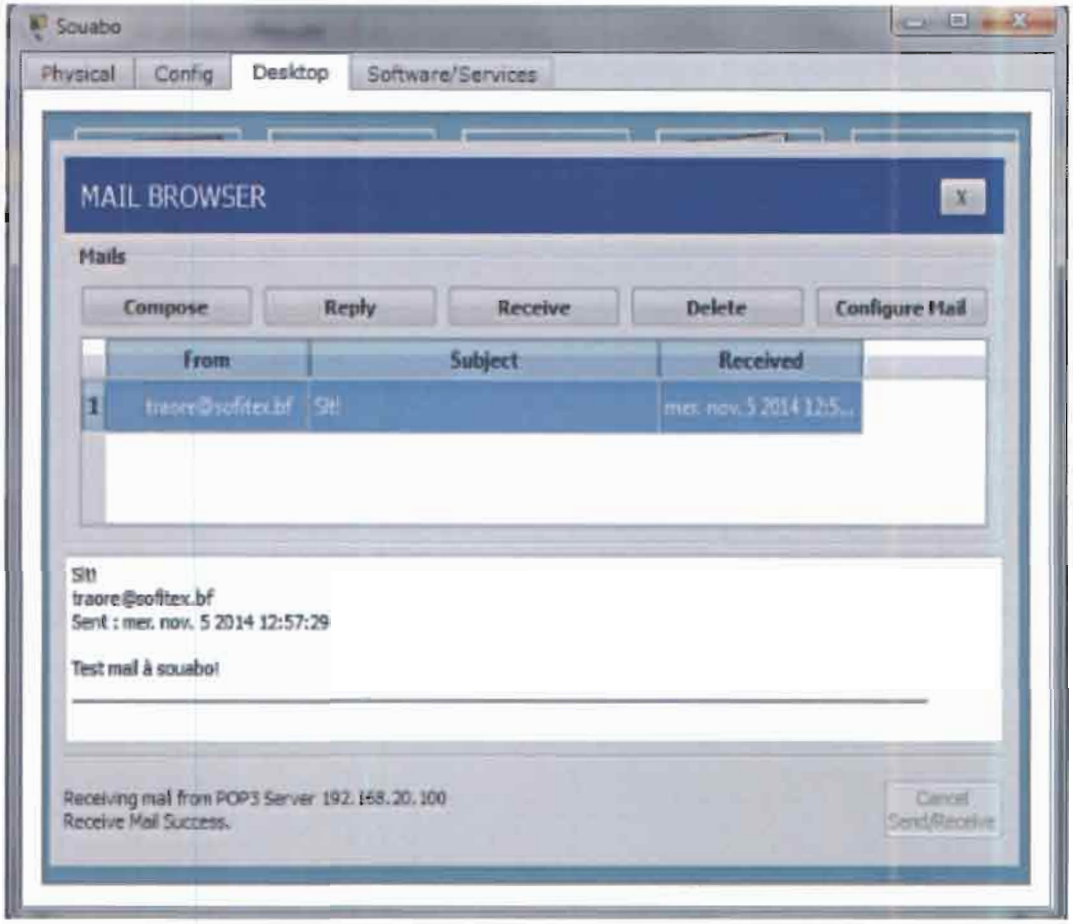

Figure 19 : Réception d'un mail

II. Evaluation financière de la solution

1. Coût de la mise en œuvre

Pour pouvoir mettre en œuvre la solution retenue, nous avons effectué une évaluation financière prenant en compte le prix des équipements à ajouter au niveau de l'infrastructure et celui des ingénieurs et techniciens qui vont la déployer. Notons que nous avons fait un prix forfaitaire par jour pour leurs prestations.

Tableau 10 : Coût financier de la mise en œuvre

Désignations	Caractéristiques	Quantité ou Durée en jours	Prix unitaire HT (F. C.F.A.)	Prix total H.T. (F. C.F.A.)
Switch distribution	CISCO Catalyst C3560X-24P-S	06	1.960.000	11.760.000
Switch Coeur	CISCO Catalyst 3750G-24TS-E1U	04	2.400.000	9.600.000

Désignations	Caractéristiques	Quantité ou Durée en jours	Prix unitaire HT (F. C.F.A.)	Prix total H.T. (F. C.F.A.)
Antennes BLR	CISCO Aironet 1300	03	178.535	535.605
Mise en œuvre de l'architecture	----	07	100.000	700.000
Mise en œuvre des VLANs	----	15	100.000	1.500.000
Mise en œuvre du RPVST+	----	15	100.000	1.500.000
Mise en œuvre de Nagios	----	15	100.000	1.500.000
TOTAL			**4.838.535**	**27.095.605**

2. Etude de l'amortissement

L'amortissement est une étude qui mesure la perte annuelle de valeur d'une immobilisation. Elle permet à l'entreprise de dégager les ressources internes suffisantes pour substituer à l'immobilisation amortie un nouvel actif.

L'amortissement est reparti sur un temps donné. Le modèle associé aux équipements actifs a un cycle de vie beaucoup plus court (2 à 5 ans selon les standards du secteur) et sont déterminant dans le caractère innovant, la qualité et les caractéristiques des services.

Dans le cas de la SOFITEX, nous considèrerons pour les nouveaux équipements actifs une durée d'amortissement de 5 ans avec donc un taux de 20% qui sera consigné dans le tableau Tableau 11.

Tableau 11 : coût d'amortissement annuel des équipements actifs de la mise en œuvre

Désignation	Quantités	Prix Unitaire en F CFA	Prix Total en F CFA	Prix du cout d'amortissement annuel (20%) en F CFA
Switchs distribution	6	1.960.000	11.760.000	2.352.000
Switchs cœur	4	2.400.000	9.600.000	1.920.000
Antennes BLR	3	178.535	535.605	107.121
Total		**4.538.535**	**21.895.605**	**4.379.121**

CONCLUSION

Les six mois passés au sein de la société des fibres textiles ont été pour nous des mois très bénéfiques. Cela nous a permis de connaitre la SOFITEX à travers son historique, son organisation, ses objectifs et de tisser des liens avec son personnel.

Outre ces acquis, l'**amélioration de l'architecture réseau du siège** nous a permis de mettre en pratique nos connaissances théoriques acquises tout au long de notre formation et de nous plonger dans l'univers de la conception et l'administration des réseaux informatiques. L'étude du thème nous a permis d'appréhender les besoins dans le but de proposer une solution adéquate pouvant satisfaire au mieux les objectifs de la structure. Ainsi, après avoir mis en relief les solutions existant pour l'optimisation d'une architecture réseau, nous avons choisi l'architecture hiérarchisée en trois couches afin d'avoir une architecture physique performante, évolutive et offrant une facilité de maintenance et d'administration. A l'issu de la définition de l'ossature du réseau, nous y avons introduit de la redondance pour assurer la disponibilité du réseau même en cas de panne d'équipement actif ou de lien critique. La redondance des liens critiques a été assurée par la BLR, la gestion des boucles dues à cette redondance fut gérer par le RPVST+ et la fluidité par la segmentation par VLAN. Enfin, pour avoir une vue du réseau en temps réel, Nagios une solution de supervision a été choisie.

Pour l'implémentation de la solution faute d'avoir tout le matériel nécessaire sur place, nous nous sommes limités à la simulation de la solution sur l'outil Packet Tracer. Notre souhait serait de participer à la mise en production de cette solution qui permettra d'optimiser le réseau de la SOFITEX.

REFERENCES BIBLIOGRAPHIQUES

[1] François Pignet, Réseaux informatiques : *Supervision et administration,* Edition ENI, 274 pages

[2] Daniel Dromard et Dominique Seret, *Architecture des réseaux* : 2e édition, Edition Pearson, 250 pages

[3] Cédric Llorens, Laurent Levier, Denis Valois, Tableau de bord de la sécurité réseau : 2e édition, Edition EYROLLES, 583 pages

[4] Informations sur la SOFITEX, www.sofitex.bf , 02/10/2013

[5] les Vlan http://1999.jres.org/articles/wolfhugel-te-05-final.pdf , 02/112013

[6] Présenatation du STP (Spanning Tree Protocol https://fr.wikipedia.org/wiki/Spanning_Tree_Protocol consulté le 12/12/2013)

[7] Presentation du RSTP (Spanning Tree Protocol https://fr.wikipedia.org/wiki/Spanning_Tree_Protocol consulté le 12/12/2013)

[8] Presentation du PVTP (Spanning Tree Protocol https://fr.wikipedia.org/wiki/Spanning_Tree_Protocol consulté le 12/12/2013)

[9] Presentation du RPVST+ (Spanning Tree Protocol https://fr.wikipedia.org/wiki/Spanning_Tree_Protocol consulté le 12/12/2013)

[10] Presentation du MSTP (Spanning Tree Protocol https://fr.wikipedia.org/wiki/Spanning_Tree_Protocol consulté le 12/12/2013)

[11] Presentation du SPB (Spanning Tree Protocol (https://fr.wikipedia.org/wiki/Spanning_Tree_Protocol consulté le 12/12/2013)

[12] Documentation sur le MSTP, http://books.google.bf/books?id=r9kWSQYBN6QC&pg=PA51&lpg=PA51&dq=M%C3%A9canismes+apr%C3%A8s+un+Topologie+Change+Notification&source=bl&ots=PW7hCFn6KV&sig=pkgcYEuR7pXalRX1bHzm5j_qaJw&hl=fr&sa=X&ei=qt4eU6P6A8Gs7QaYg4GIAg#v=onepage&q=M%C3%A9canismes%20apr%C3%A8s%20un%20Topologie%20Change%20Notification&f=false , 11/02/2014

[13] Configuration du RPVST+, http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/RPVSpanningTree.html , 14/01/2014

[14] STP – fonctionnement portfast - bpduguard, http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html , 12/12/2013

[15] Architecture Hiéarchisée en trois couches, http://bibabox.fr/topologie-reseau-le-modele-hierarchique-en-3-couches/ consulté le 14/01/2014)

[16] Cisco Works, www.cisco.com/web/FR/.../pdfs/.../ciscoworks_lanmanagement_21.pdf consulté le 22/02/2014

[17] Nagios, https://www.nagios.org/ , 11/03/2014

[18] Nagios et centreon, http://blog.nicolargo.com/nagios-tutoriels-et-documentations, 11/03/2014

ANNEXES

Annexe 1: Installation et configuration de Centreon 84

Annexe 1: Installation et configuration de Centreon

Les étapes pour installer Centreon se déroulent de la manière suivante :

Installation de MySQL

```
#apt-get install mysql-server php-db php-date php5-gd php5-mysql php5-snmp php5-ldap php5-xmlrpc
```

Installation de librairie de perl

```
#cpan
#install Config::IniFiles
```

Installation de la base de données NDO

```
#mysqladmin -u root -p create ndo
#mysql -u root -p mysql
        GRANT ALL ON ndo.* TO "nagios"@"localhost" IDENTIFIED BY "pwdndo";
        FLUSH PRIVILEGES;
        exit
```

Installation de NDO

```
# cd /usr/local/src
# wget http://sourceforge.net/projects/nagios/files/ndoutils-2.x/ndoutils-2.0.0/ndoutils-2.0.0.tar.gz
# tar -xzf ndoutils-2.0.0.tar.gz
# cd ndoutils-2.0.0
# ./configure --disable-pgsql --with-mysql-lib=/usr/lib/mysql --with-ndo2db-user=nagios --with-ndo2db-group=nagios
# make
#cp/usr/local/src/ndoutils-2.0.0/src/ndomod-*.o /usr/local/nagios/bin/
# cp /usr/local/src/ndoutils-2.0.0/src/ndo2db* /usr/local/nagios/bin/
```

Installation de Centreon

```
# cd /usr/local/src/
# wget http://download.centreon.com/centreon/centreon2.5.0.tar.gz
# tar -xzf centreon-2.5.0.tar.gz
# cd centreon-2.5.0
# ./install.sh -i
```

On répond aux différentes questions demandées par le script d'installation (généralement on peut laisser par défaut et appuyer sur la touche entrée).

On recharge Apache (serveur web) puis on lance centstorage

```
# /etc/init.d/apache2 reload
# /etc/init.d/centstorage start
```

On modifie SNMP

Pour que les check_snmp fonctionnent, il faut modifier le fichier **/etc/snmp/snmpd.conf** pour avoir :

```
#sec.name sourcecommunity
#com2sec paranoid default      public
com2sec readonly default       public
#com2sec readwrite default     private
```

Installation Web de Centreon

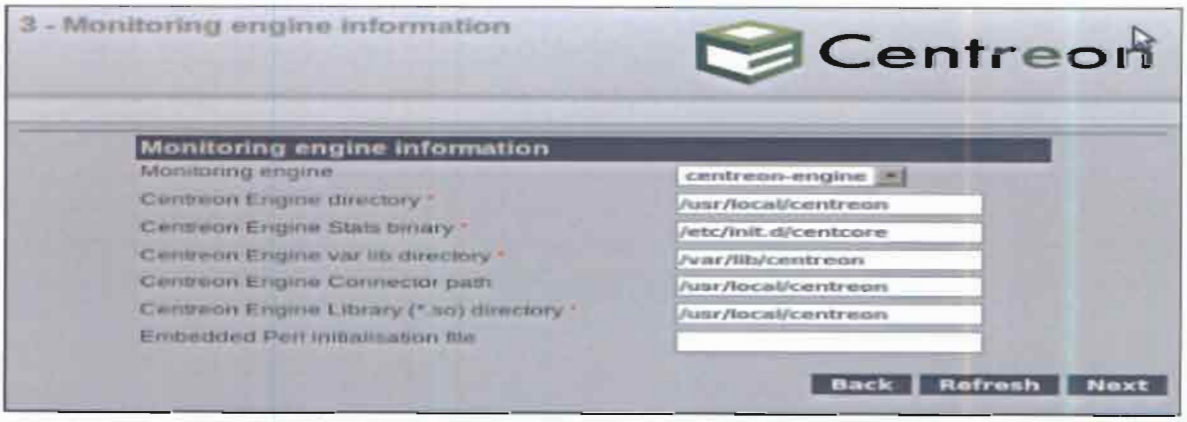

Figure 20 : Monitoring Engine information

Aller sur l'url suivante : http://localhost/centreon. On intègre les utilisateurs spécifiques à Nagios créé auparavant :

La validation des composants faite, on configure maintenant notre base de données en lui indiquant le mot de passe à utiliser. On passe ensuite à la mise en place du nom d'utilisateur et du mot de passe nécessaire pour se connecter à l'interface web Centreon. On définit également notre nom et notre adresse email.

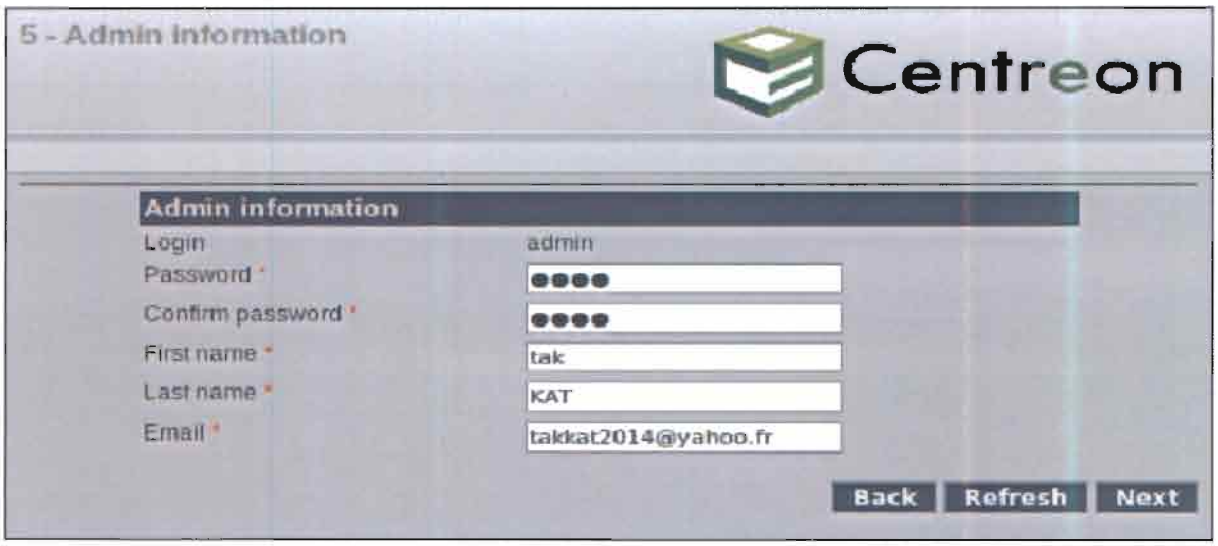

Figure 21 : Admin information

Dans l'onglet suivant, on remplit les autres champs en laissant par défaut le database port, le nom de la configuration de base de données, le Storage *database name*, l'utils database name et le database user name.

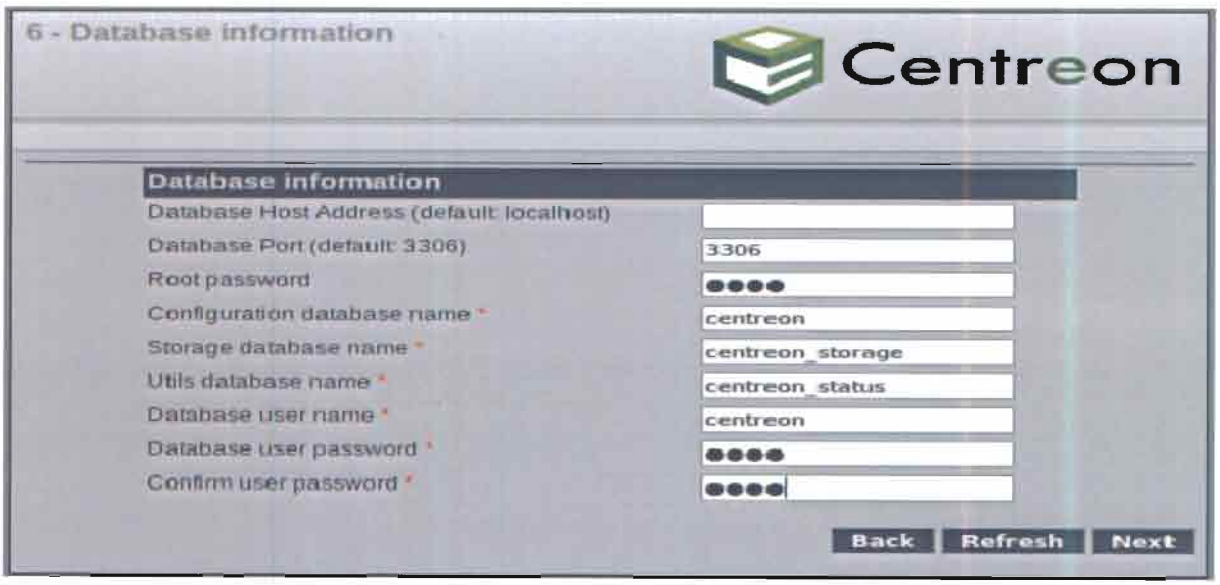

Figure 22 : Informations de la base de données

L'onglet suivant montre que toutes les configurations ont été établies.

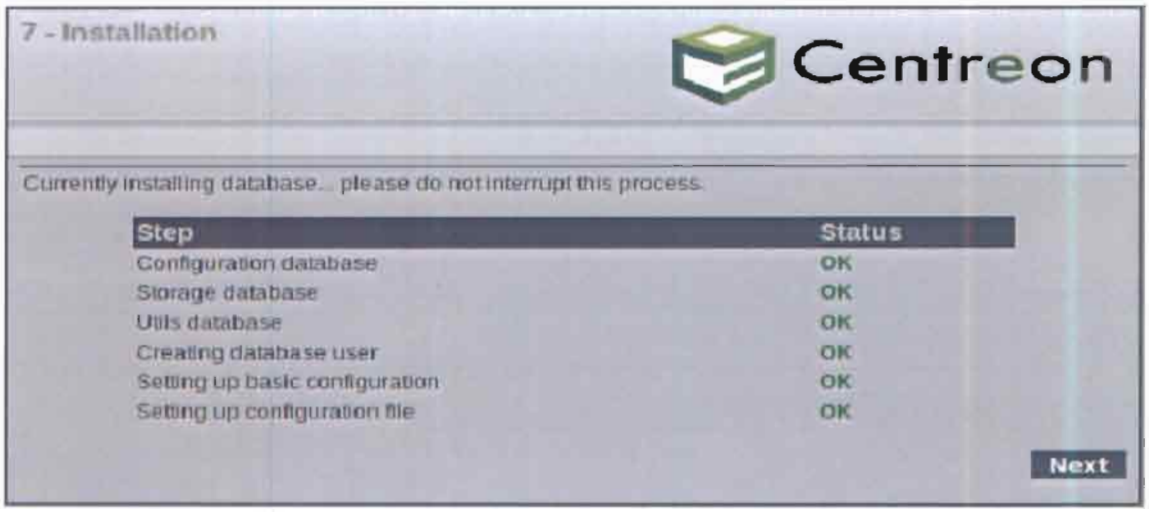

Figure 23 : Création des bases de données

On modifie le fichier de configuration MySql/etc/mysql/my.cnf en ajoutant la ligne : innodb_file_per_table=1 et on redemarre MySql avec la commande :

```
#service mysql restart
```

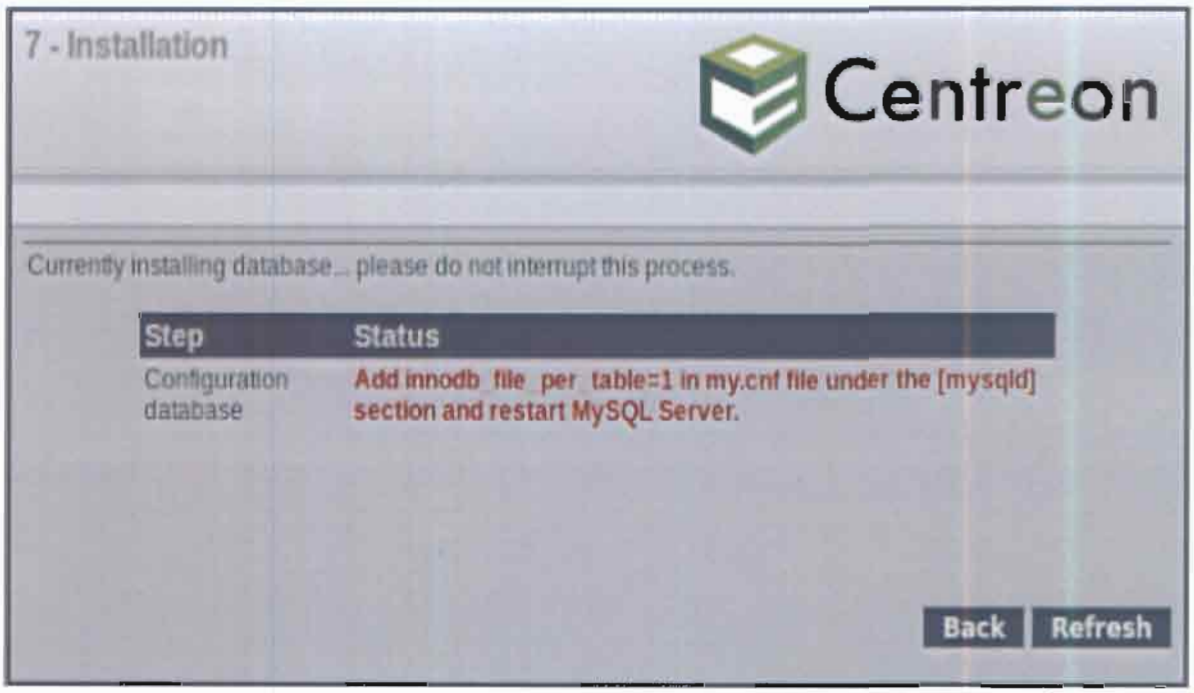

Figure 24 : Suite de la création de la base de données

L'onglet suivant nous montre que l'installation a été bien effectuée.

Figure 25 : Fin de l'installation

On lance les services suivants :

```
#service centcore start
#service centreontrapd start
```

On se connecte sur l'interface de Centreon en mettant le nom et le mot de passe valide puis on effectue des modifications en faisant : « -> Configuration -> Nagios -> Nagios.cfg -> Onglet Data -> Broker Module » et on change comme ceci : /usr/local/nagios/bin/ndomod-3x.o config_file=/usr/local/nagios/etc/ndomod.cfg. On exporte les fichiers et on redémarre Nagios. On modifie également le fichier **/etc/init.d/nagios** pour inclure le lancement de ndo2db au démarrage de nagios et nous pouvons enfin commencer notre surveillance.

TABLE DES MATIERES

REMERCIEMENTS II

SIGLES ET ABREVIATIONS IV

LISTE DES TABLEAUX VII

LISTE DES FIGURES VIII

AVANT-PROPOS IX

INTRODUCTION 1

PREMIERE PARTIE : CONTEXTE ET ENVIRONNEMENT D'ETUDE 2

CHAPITRE 1 : PRESENTATION DE LA STRUCTURE D'ACCUEIL 3

I. Organisation et fonctionnement du SIRT 3

II. Missions et activités 4

1. Les missions du SIRT 4
2. Les activités du SIRT 5

CHAPITRE 2 : PROBLEMATIQUE ET CAHIER DE CHARGES 7

I. Problématique 7

II. Cahier de charges 7

III. Démarche à suivre 8

CHAPITRE 3 : ETUDE DU RESEAU LOCAL DE BOBO-DIOULASSO 10

I. Présentation de l'existant 11

1. Topologie physique 11
2. Topologie logique 17
3. Présentation du système 17
4. Présentation des applications 19
5. Présentation des postes de travail 19

II. Critiques de l'existant 20

DEUXIEME PARTIE : ETUDE TECHNIQUE 22

CHAPITRE 1 : ETUDE PREALABLE ET CHOIX TECHNIQUES 23

I. Architecture physique du réseau 23
1. Présentation des topologies existantes 23
2. Comparaison des topologies physiques du réseau 23
3. Choix de la topologie 24

II. Gestion de la redondance physique 24
1. Redondance des équipements actifs du réseau 24
2. Redondance des liens d'interconnexion 25

III. Gestion de la redondance 26
1. Le protocole Spanning Tree Protocol (STP) 26
2. Le protocole Rapid Spanning Tree Protocol (RSTP) 26
3. Le protocole Per-VLAN Spanning Tree (PVST) 26
4. Le protocole RPVST+ 27
5. Le protocole MSTP 27
6. Le protocole SPB. 27
7. Comparaison des solutions pour la redondance logique 28
8. Choix de la solution de gestion de redondance logique 28

IV. Segmentation du réseau 29
1. Présentation des solutions de segmentation 29
2. Comparaison des solutions de segmentation 30
3. Choix de la solution de segmentation 31

V. La supervision du réseau 31
1. Les solutions de supervision 32
2. Comparaison des outils de supervision 33
3. Choix de l'outil de supervision 35

CHAPITRE 2 : ETUDE DETAILLEE DE LA SOLUTION RETENUE 35

I. L'architecture hiérarchisée en trois couches 35
1. La couche cœur 36
2. La couche distribution 36
3. La couche d'accès 36

II. Gestion de la redondance des liens : La Boucle Locale Radio (BLR) 36
1. Définition 36
2. Les technologies BLR 36
3. Sécurité des systèmes BLR 38

III. La gestion de la redondance logique 39
1. L'algorithme Spanning Tree 39
2. Vu d'ensemble du RPVST+ 40
3. Les rôles et les états des ports 41

IV. Les VLAN 45
1. Présentation 45
2. Les types de VLAN 45

3. Fonctionnement 46
4. Routage inter-VLAN 46
5. La gestion centralisée des VLAN 47

V. L'outil de supervision : NAGIOS 48
1. Présentation 48
2. Fonctionnalités 48
3. Fonctionnement 49
4. Les sondes ou plugins 52

CHAPITRE 3 : IMPLEMENTATION DE LA SOLUTION 53

I. Mise en œuvre de la solution 53
1. Chronogramme du déploiement 53
2. Mise en œuvre 55
3. Simulation du réseau de la SOFITEX 67

II. Evaluation financière de la solution 77
1. Coût de la mise en œuvre 77
2. Etude de l'amortissement 78

CONCLUSION 80

REFERENCES BIBLIOGRAPHIQUES 81

ANNEXES 83