République du Sénégal

Un peuple – Un but – Une Foi

UNIVERSITE CHEIKH ANTA DIOP DE DAKAR

Faculté des Sciences et Techniques
Département de Mathématiques et Informatique
Section Informatique

MEMOIRE DE MASTER D'INFORMATIQUE

Option : Réseaux et Services de Télécommunications

Présenté par : ***Medoune DIAGNE***

Sujet :

Optimisation des Services de Transfert d'Argent (WU), de l'Interconnexion des Sites distants et du Système de Supervision des équipements monétiques de la CBAO Groupe AttijariWafa bank

LIEU DE STAGE : **Département Ingénierie Technique /DSI/CBAO Groupe AttijariWafa bank**

Membres du Jury :

Pr. Bamba GUEYE
Dr. Abdourahmane RAIMY
Dr. Moussa Diallo

Sous la direction de :

Dr. Cherif DIALLO
PhD, CISSP

Maitre de Stage

M. Etienne DIAFATTE
Responsable Département IT/DOSI
CBAO Groupe AttijariWafa bank

Année Universitaire : 2013 – 2014

Soutenu en : 7 Mars 2015

DEDICACES

Ce mémoire est dédié :

A ma très chère Maman, *qui a été toujours à mes côtés dans les moments les plus sombres et n'a ménagé aucuns efforts pour mon épanouissement, que ce travail soit le témoignage de mon amour pour toi.*

A mon regretté Père*, tu aurais voulu être là, mais les valeurs de travail et d'Intégrité que tu m'as inculpé m'ont été toujours d'un grand secours pour l'accomplissement de mes projets.*

A mon beau-père Ibrahima Idrissa NDIAYE*, encore et toujours, vous avez été un modèle de persévérance et d'humilité, je ne saurai vous remercier assez.*

A mon très cher Oncle Babacar THIAW*, il a toujours cru en moi et a consenti des sacrifices inestimables pour ma réussite et mon éducation religieuse, je ne saurai trouver les mots pour cela, mais j'espère que vous verrez en ces lignes toute l'expression de ma gratitude ;*

A ma tante Rokhaya S. Gueye*, qui de par son soutien indéfectible et ses conseils des plus sages, a grandement participé à ce qui je suis devenu. Jazakillahou hayrane*

A mon grand frère ***Issa NGOM****, qui ne cesse de me donner des conseils et se soucier de mon aura. Par la grâce de dieu, je ne te décevrai pas incha allah.*

A mon oncle et ami ***Pape Médoune DIAGNE****, dont ses conseils et encouragements m'ont été d'une grande utilité.*

A mes sœurs Sooba et Codou*, qui m'ont toujours comblé de leurs présences et leurs soutiens et à leurs époux Habib et Ousseynou.*

A mon regretté ami et professeur*, Monsieur Habib Thiam, tu as été à la base de tous .Vos conseils et les valeurs morales et civiques qu'il me prodiguait, constituent mes compagnons de toujours. Que dieu vous accueille dans son paradis éternel.*

Aux familles DIAGNE, THIAW, MBENGUE, NDIAYE et DIEYE ;

A Madame Dienne*, Enseignant Chercheur au Département Informatique de l'ESP, je voue un grand respect pour vous.*

A toute la famille RETEL *qui ont toujours fait preuve de bon camaraderie et d'entre-aide*

A tous mes amis *;*

A tout ceux qui m'ont aidé à réaliser ce travail de prêt ou de loin.

REMERCIEMENTS

Tout d'abord je remercie et rends grâce à Dieu pour m'avoir donné la foi de persévérer, la force d'exceller et la santé pour mener à bien mes projets.

A mon grand frère ***Issa NGOM,*** *tu as toujours été un modèle pour moi .Votre parcours m'a beaucoup inspiré.*

Monsieur Etienne DIAFATTE*, Responsable Département Ingénierie Technique /CBAO qui a accepté de m'accueillir et de m'encadrer pour ce travail.*

Je te remercie d'avoir cru en moi et de m'avoir confié ce travail qui tout au début paraissait presque irréalisable dans les délais.

Docteur Cherif DIALLO*, pour avoir accepté de diriger ces travaux et pour qui ses enseignements de qualité m'ont poussé à opter pour ce sujet.*

A tous les agents du Département IT/CBAO *qui, de par leur ouverture d'esprit et leur sens du travail en équipe m'ont permis d'évoluer dans un environnement favorable pour mener à bien ce travail .*

A Monsieur Djibril Niang et Monsieur Pape Ly*, SI Monétique qui de par leurs appuis et nos échanges fructueuses, m'ont permis de mieux appréhender les problématiques de Supervision de la banque.*

A tous les membres du Corps Professoral *de la Section Informatique, leurs enseignements de qualité m'ont été d'une grande utilité.*

A mon très cher Oncle Babacar THIAW*, il a toujours cru en moi et a consenti des sacrifices inestimables pour ma réussite et mon éducation religieuse, je ne saurai trouver les mots pour cela, mais j'espère que vous verrez en ces lignes toute l'expression de ma gratitude ;*

A ma tante Rokhaya S. Gueye*, qui de par son soutien indéfectible et ses conseils des plus sages, a grandement participé à ce qui je suis devenu. Jazakillahou hayrane*

A tous le personnel Administratif de la Section Informatique particulièrement au Secrétariat.

Table des Matières

DEDICACES I
REMERCIEMENTS II
Table des Matières III
Table des Figures VI
Liste des Tableaux VII
Avant-propos VIII
RESUME X
Introduction Générale 1
Partie 1 : Présentation Générale 2
I. Présentation du Sujet 3
1) Problématique 3
2) Objectifs 3
3) Méthodologie 4
II. Présentation du lieu de Stage 5
1) Présentation 5
2) Historique 6
3) Constitution du Capital 7
4) Organisation 7
Partie 2 : Etude Technique 9
I. Problématique 1 : Disponibilité des équipements Monétiques 10
1) Présentation 10
2) Mission 10
3) Equipements et outils utilisés 10
a) Les GAB ou DAB 10
b) Les Terminaux de Paiement Electroniques (TPE) 12
4) Gestion des flux 13
a) Les flux domestiques 13
b) Les flux internationaux 14
c) Diagramme des flux 14
5) Dysfonctionnements 15
a) Approche technique 15

b) Approche Organisationnelle 15
6) Solution SightGAB : Approche Technique 16
a) Objectifs 16
b) Architecture SightGAB 17
c) Comment superviser 18
d) Etude pour la mise en place 19
7) Mise en place de la Solution 35
a) Installation du protocole Snmp 35
b) Configuration EON 39
8) BILAN 50
II. Problématique 2: Sécurisation et Augmentation de la Qos du service de transfert d'Argent 51
1) Présentation de l'Infrastructure 51
a) Introduction 51
a) Architecture 52
2) Les VPN 53
a) Principe de fonctionnement 53
b) Fonctionnalités des Vpn 53
c) - Bilan des caractéristiques fondamentales d'un Vpn 54
d) Le protocole Ipsec 55
3) Configuration des liaisons VPN 57
a) Politique de Sécurité 57
b) Explication détaillée 58
c) Protocoles Utilisés 61
4) Dysfonctionnements Constatés 61
5) Solution proposée 62
a) Les ACL 62
b) Mise en œuvre de la solution 68
c) Test et évaluation des configurations 69
6) Conclusion 70
III. Problématique 3 : Augmentation du débit et rationalisation des Coûts 71
1) Synoptique de l'Architecture LAN-MAN de la CBAO 71
2) Manquements et Points à améliorer 74
1) Proposition de Solution 76
a) Mise en place d'une BLR (Boucle Locale Radio) 76

2) Mise en place de la solution 102
a) Choix du type de liaison 102
b) Cahier de Charges 104
c) Schéma R-Planner 106
d) Bilan : 107
Conclusions et Perspectives 108
Références 109
..... 109
Liste des Acronymes 110
Annexe 1 112
Installation de EyesOfNetwork 112

Table des Figures

Figure 1:Diagramme des flux bancaires 14
Figure 2: Schéma illustratif des composants supervisés/GAB 16
Figure 3:Architecture SightGAB 17
Figure 4:Schéma explicatif du fonctionnement des requêtes SNMP 18
Figure 5:Exemple de table MIB 22
Figure 6:Chiffrement DES/SNMPv3 26
Figure 7:Bundle EyesOfNetwork 32
Figure 8:Archtecture EyesOfNetwork 33
Figure 9:Exemple de frise chronologie/Alerte Nagios 45
Figure 10:Exemple d'Escalade 47
Figure 11:Architecture liaisons VPN 52
Figure 12:Schéma synoptique du fonctionnement des VPN 56
Figure 13:Parcours des instructions ACL [4] 63
Figure 14:Architecture Réseau CBAO 73
Figure 15:Performance en débit de RADWIN 2000 C @40 MHz 78
Figure 16: RADWIN 2000 C-Series Performance Range TDM (E1s) 78
Figure 17:Performance Ethernet de RADWIN 2000 B /20 MHz 79
Figure 18 : Performance RADWIN 2000 A avec un débit de 25 Mbps 80
Figure 19;Configuration Radio Multiband 83
Figure 20:Mécanisme d'acheminement des paquets/Qos 86
Figure 21: Schéma explicatif VLAN 87
Figure 22:Architecture utilisant Queue in Queue 88
Figure 23:Caractéristiques des HBS 89
Figure 24:Approche TDMA 92
Figure 25:Evolution de l'atténuation du signa l en fonction de la fréquence 93
Figure 26:Symboles de données occupent 15KHz pour une période de symbole OFDM 95
Figure 27:Occupation spectrale/OFDM 96
Figure 28:Diversité d'Antenne gain: améliore jusqu'à 15db la performance nLOS 98
Figure 29:Comparaison entre MIMO et Diversité 98
Figure 30:Graphe de comparaison entre les performances de Diversity et OFDM 99
Figure 31:Mecanisme de retransmission des bits (ARQ) 100
Figure 32:Adaptation Automatique du Niveau de Codage 100
Figure 33:Evolution du débit en fonction de la modulation 101
Figure 34:Configuration du Jitter Buffer 102
Figure 35:Architecture Point-to-Multipoint 103
Figure 36: Architecture Point-to-Point 103
Figure 37:Synoptique Installation BLR 106

Liste des Tableaux

Tableau 1:Tableau comparatif des logiciels de supervision..... 34
Tableau 2:Coùt de location des LS 75
Tableau 3: Produit RADWIN PtP 77
Tableau 4: Priorité de Classification 87

Avant-propos

Créée en **1990** du besoin de diversifier les filières au sein du département de Mathématiques-Informatique, la Section Informatique délivrait jusqu'en 2003 trois diplômes: Licence, Maîtrise et DEA. Suite à la demande grandissante et plus exigeante du marché, d'autres filières ont été créés et par la même occasion le diplôme de Master et de Licence Professionnelle.

Ainsi, la section commençait à délivrer le diplôme de Master Informatique, de même la formation Création MultiMedia voyait le jour. Ce n'est qu'en 2009, que les filières réseaux & Télécoms et Bio-informatique ont été créées et voient leurs premières promotions de Master 2 successivement en 2010 et 2011.

L'excellence dans la discipline et la réussite des étudiants à ces différentes formations place la section dans une dynamique d'ouverture de nouvelles filières pour élargir les bases de la connaissance et promouvoir l'expertise des étudiants au vu des exigences de plus en plus évolutives des entreprises .

A ce effet , le Master 2 Business Intelligence s'est tout récemment ajouté au catalogue de formations sous forme de spécialisations afin de permettre aux étudiants de s'orienter résolument dans les métiers de l'Analyse et l'Exploitation des données et de répondre à une nouvelle dynamique du marché du travail.

La richesse des formations offertes et la qualité de son corps professoral ont permis à la section, depuis sa création, de s'illustrer comme étant une valeur sure dans la formation en tic au Sénégal et dans la sous-région notamment par les nombreux cadres d'entreprises et enseignants qui y sont issus.

En effet, son effectif très riche en diversité est composé de 11 nationalités (Sénégal, Mauritanie, Congo, Gabon, Benin, Tchad, Niger, Togo, Burkina, Guinée Conakry, Comores)

Le corps professoral est composé de :

- 6 Maitres de conférences en Informatique
- 2 Maitres assistants
- 6 Assistants
- des Professeurs coopérants étrangers d'universités partenaires (France, Tunisie, Etats-Unis)
- des Professionnels de l'entreprise

La section coordonne aussi des formations doctorales en bases de données, en performance et en réseaux dans l'Ecole Doctorale de Mathématiques et Informatique.

Le nombre d'étudiants est passé entre 1990 et 2014, de 30 à 308 (formation continue et formation classique). A ce jour elle propose en effet, une large gamme de formations allant de l'Informatique, Bio-informatique, Création MultiMedia, Business Intelligence et Réseaux & Télécoms.

Ces formations sont dispensées en trois niveaux excepté celle de la Création MultiMedia qui, n'est disponible que pour la licence.

1) **LICENCES**

- Licence Classique d'Informatique
- Licence Professionnelle d'Informatique
- Licence Professionnelle de Création Multimédia
- Licence Professionnelle Bio-Informatique

2) **MASTERS**

- Systèmes d'Informations Répartis (SIR)
- Réseaux et Télécommunications (RETEL)
- Bio-informatique
- Business Intelligence

Se voulant être une institution sérieuse et performante, l'admission à la section informatique est soumise à plusieurs conditions comme les Tests d'entrée suivi d'entretien et/ou la sélection sur dossier .De ce fait, elle se permet de disposer des meilleurs profils pour l'acquisition et la pratique du métier d'Informaticien qui demande de grandes exigences tant intellectuelles que psychologiques.

- Licence (Titulaires d'un DUES scientifique et tout diplôme équivalent)
  Test d'entrée + entretien

- Master I: (titulaire d'une Licence d'Informatique)
  Sélection sur dossier + entretien

- Master II: (titulaire d'une maîtrise d'informatique ou ingénieur et tout diplôme équivalent) **Sélection sur dossier + entretien**

Dans l'optique de valider notre formation suivie pendant ces 5 dernières années, il nous incombe de rédiger un mémoire de fin d'études portant sur un thème afférent à la spécialité des réseaux et télécommunications. De ce fait, l'étudiant en collaboration avec les autorités pédagogiques, choisit un thème de mémoire que ce soit un mémoire de recherche ou d'entreprise : ceci est entièrement du ressort de l'étudiant et/ou de son maitre de stage s'il a pu bénéficier d'un stage.

Ainsi , mon stage au Département Ingénierie Technique de CBAO Groupe AttijariWafa BANK , m'a permis de mieux appréhender les réalités ainsi que les besoins pressants dans le domaine bancaire. A cet effet , le choix de mon thème de mémoire n'est guère fortuit car ayant rapport direct avec beaucoup de modules d'enseignement vus pendant ma formation à savoir la Performance des Réseaux , l'Audit des SI et la gestion des projets .

Ce thème, portant sur l'Optimisation des Services Réseaux de la CBAO, sera l'occasion pour moi de mettre en pratique les connaissances théoriques et ainsi consolider les acquis.

RESUME

Dans la dynamique d'amélioration des performances et l'augmentation de la Qualité de service offerts par les entreprises, l'optimisation constitue une étape importante voire indispensable afin de répondre aux nouveaux défis technologiques.

La course effrénée vers le contrôle du marché bancaire Sénégalais pousse les établissements financiers à créer de nouveaux services .Or ces services basés sur les systèmes d'Information ne sont pas toujours exploitée au mieux de leurs potentiels.

En effet , depuis quelques années , les équipements monétiques sont victimes de plusieurs pannes qui influent considérablement sur le chiffre d'affaire de la banque et même sur sa réputation .De même , dans le souci de rationaliser les coûts télécoms qui constituent le plus grand aspirateur de dépenses des DSI , il est devenu indispensable voire inéluctable d'utiliser des technologies d'interconnexion alternatives avec un meilleur rapport coût/débit .

Fort de ces constats, l'objectif de notre étude est de faire une étude approfondie des services phares de la banque à savoir le transfert d'Argent, l'Interconnexion des Sites distants (agences) et le système de supervision des équipements monétiques et d'apporter des solutions techniques, et/ou organisationnelles.

Introduction Générale

Dans le contexte actuel de forte concurrence où la productivité et la disponibilité des services offerts aux clients sont plus que capitales, les systèmes d'information des entreprises constituent une partie prenante indispensable dans cette course effrénée vers la compétitivité et la conquête de nouveaux marchés.

En effet, dans le cadre général et en particulier dans le domaine bancaire, tous les services offerts se reposent inéluctablement dans un système d'information du fait de l'orientation de plus en plus accentuée vers l'automatisation des taches et l'accroissement exponentiel des transactions électroniques. De ce fait, l'amélioration de l'expérience client et de la qualité de service, passent inexorablement par l'optimisation des Services réseaux.

L'optimisation est un concept d'amélioration des performances ou de corrections des erreurs ou manquements dans un système bien défini. De ce fait, elle consiste à tirer la meilleure partie possible de quelque chose.

Le périmètre de notre étude se limite aux services de transfert d'argent, de supervision des équipements monétiques ainsi que le réseau d'interconnexion des agences. C'est ainsi que notre travail, consistant à mettre en œuvre des mécanismes d'organisation et d'optimisation des services réseaux, va s'articuler autour de 4 grandes axes citées ci-après :

Dans un premier temps, nous allons faire une brève présentation de notre sujet ainsi que du cadre de stage.

Ensuite, nous allons à l'étude technique pour déceler les manquements et dysfonctionnements de tous les services de notre périmètre d'étude afin de proposer des solutions d'optimisations

Nous allons finir par la conclusion et les perspectives

Partie 1 : Présentation Générale

I. Présentation du Sujet

1) Problématique

La CBAO, leader dans le domaine bancaire en Afrique de l'Ouest et au Sénégal, depuis quelques années, se veut comme tradition une banque innovante et attractive à travers la création de valeurs ajoutées et de services ainsi qu'une qualité de service et une expérience client exceptionnelles ; ce qui a fait les beaux jours de cette structure depuis sa création aux débuts du 20éme siècle. Mais dans le contexte actuel , avec l'émergence de nouvelles banques plutôt compétitives et l'accroissement de la clientèle donc du réseau , il est nécessaire de procéder à un audit complet du réseau en procédant à l'évaluation des besoins actuels et futurs afin de s'aligner sur les nouvelles exigences du marché et l'évolution technologique.

Ceci étant dit, passe immanquablement par une politique de planification et d'optimisation des services afférents aux métiers des banques. Dans la même logique, avec le programme Excellence 2017 visant à doubler la taille de la clientèle et le déploiement de nouveaux services dans les points dédiés, un nouveau dimensionnement du réseau s'impose car ce surplus de clients va probablement entrainer la création de nouvelles agences et de filiales dans la sous-région et l'augmentation du trafic.

Pour prévenir l'attrition des clients, la CBAO doit tenir compte de toutes ces contraintes tout en prenant en compte l'aspect financier .Ainsi, la politique actuelle et révolutionnaire des entreprises consiste maintenant à faire des directions Informatique, non pas des aspirateurs de dépenses mais plutôt par des créatrices de valeurs ajoutées donc des centres de profits.

2) Objectifs

Le périmètre d'étude défini est le service de transfert d'argent, le système de télésurveillance des GAB ainsi que les réseaux d'interconnexion avec les sites distants. Il sera question d'étudier scrupuleusement le fonctionnement de chaque service pour déterminer les manquements et/ou les points à améliorer.

Notre objectif principal pour cet étude est de proposer au finish des solutions d'optimisation, en fonction des besoins de la structure et des contraintes techniques et/ou financières, pour chacun des services concernés afin d'améliorer leurs efficacités.

3) Méthodologie

Dans la dynamique nouvelle de gestion des systèmes d'information où le rapport coût et efficacité est plus que décisif, il est très important de procéder à un audit plus poussé de l'aspect organisationnel ainsi que de son efficacité par rapport aux missions allouées et les ressources humaines disponibles.

De ce fait, notre travail plutôt technique, à première vue, va de même s'orienter sur l'aspect « Process » de l'Informatique avant de passer à l'estimation des besoins (bandes passantes, délai, disponibilité…) des services, l'ébauche de solutions d'optimisation, l'implémentation de ces solutions à travers des labos et enfin l'évaluation des solutions et amélioration.

- Aspect Process et Organisationnel

Cette partie du travail, consiste dans une moindre mesure à l'analyse de l'organisation des services de la direction des systèmes d'information et à la mesure de son impact direct sur l'efficacité du système d'informations.

- Audit et Estimation des besoins

Cette partie plus que capitale dans l'élaboration de ce travail, va s'articuler autour de l'évaluation de l'efficacité des services, la détection des failles et dysfonctionnements.

- Ebauche de solutions

Par rapport aux résultats de la section précédente, nous allons tenter d'apporter des solutions aux éventuels problèmes, ou des améliorations de la qualité de service afin de booster la productivité de l'entreprise de même que l'expérience client.

Ceci ne se fera sans la prise en compte de l'aspect financier et organisationnel desdites solutions.

- Implémentation et évaluations des solutions

Cette partie sera l'occasion de mettre en pratique les solutions proposées plutôt, à travers des labos en se référant surtout sur une architecture le plus fidèle possible à la réalité de l'entreprise. A partir des résultats obtenus lors des simulations des solutions, nous allons procéder à une analyse critique afin d'apporter d'éventuelles améliorations pour enfin les valider.

II. Présentation du lieu de Stage

1) Présentation

Filiale d'AttijariWafa bank, premier groupe bancaire et financier du Maghreb et huitième au niveau Africain, la CBAO Groupe AttijariWafa bank, résultat de la fusion entre la CBAO et Attijari bank Sénégal se veut une banque au service de tous les sénégalais et leader sur le marché. Le nouvel ensemble s'engage à l'édification d'une grande institution sénégalaise, porteuse de progrès et de développement pour tous nos partenaires.

A travers l'acquisition de CBAO et la fusion par voie d'absorption d'Attijari bank Sénégal, le Groupe AttijariWafa bank accompagné de ses actionnaires de référence ONA et SNI, confirme son ambition de poursuivre son développement en Afrique de l'Ouest et sa volonté de faire de son implantation au Sénégal une tête de pont pour la réalisation de ses ambitions dans la région.

Notre ambition est de proposer des services bancaires et financiers, modernes et adaptés, afin de favoriser l'accès de tous les sénégalais à des réseaux d'échanges économiques élargis. La CBAO Groupe AttijariWafa bank souhaite également mettre en œuvre une approche spécifique pour les sénégalais résidents à l'étranger : un réseau de proximité en Europe, et des produits de transferts efficaces à des coûts compétitifs avec des mécanismes performants de réinvestissement dans le pays d'origine. Enfin, le nouvel ensemble se veut un vecteur de la coopération Maroco-Sénégalaise en termes d'échanges commerciaux et d'investissements, le Sénégal devenant à terme, le « hub » du groupe pour son développement sur l'Afrique Occidentale et servir de modèle référence.

Plusieurs facteurs clés constituent notre force, à savoir :

L'appartenance à un grand groupe

La nouvelle banque va bénéficier des avantages liés à l'appartenance à un groupe présent dans plusieurs pays d'Europe, d'Asie, d'Afrique, du Maghreb, etc.
Aussi elle pourra bénéficier de toute l'expertise d'AttijariWafa bank qui est leader dans le domaine bancaire au Maghreb.

Le premier réseau bancaire

CBAO est le premier réseau bancaire du Sénégal avec la coexistence des deux réseaux de transfert d'argent (WU et Money Gram).

La complémentarité sectorielle

Le nouvel ensemble, CBAO Groupe AttijariWafa bank est positionné sur des marchés complémentaires : le segment des « Petites et Moyennes Entreprises » et des « Très Petites Entreprises » d'une part et le segment « Grandes Entreprises », Entreprises publiques et Entreprises d'Etat d'autre part. Avec des atouts intéressants par rapport au marché des « Sénégalais Résidants à l'Etranger ».

Les ressources humaines

Plus de 1 000 personnes au service de la clientèle. Une force de vente de qualité, des hommes et des femmes d'expérience.

Une gamme de produits et services plus large
Désormais, nos clients bénéficient d'une offre commerciale enrichie des produits des deux banques.

2) Historique

La CBAO Groupe AttijariWafa est née de la fusion entre la Compagnie Bancaire de l'Afrique Occidentale et Attijari bank Sénégal.
Créée il y a un siècle et demi, en 1853, la Compagnie Bancaire de l'Afrique Occidentale (CBAO) dénommée à cette époque Banque du Sénégal, est la banque la plus ancienne de l'Afrique de l'Ouest.

Elle a tout au long de son histoire eu à changer de nom à plusieurs reprises : d'abord Banque du Sénégal à sa création, elle est devenue la Banque de l'Afrique Occidentale (BAO) en 1901.En 1960, année de l'indépendance de nombreux pays africains, la BAO a 38 sièges en Afrique. Le changement de l'environnement politico-juridique pousse alors les banques à réfléchir à leur structure.

Dans ce cadre, la BAO crée en 1965, avec la First National City Bank of New York, un nouvel établissement bancaire : la Banque Internationale de l'Afrique Occidentale (BIAO), dont le siège est à Paris et dont elle détient 51% du capital. Ainsi, elle cesse toute activité bancaire en propre et devient la Compagnie Financière France-Afrique « COFIFA ».

La BIAO s'est développée de façon globalement positive, malgré les problèmes rencontrés dans certains pays du fait de soubresauts politiques ou de campagnes agricoles déprimées jusqu'en 1975.

En 1980, la BIAO Sénégal est créée au capital initial de 2 milliards porté immédiatement à 3 077 M. F. CFA, l'Etat du Sénégal détenant alors 35% du capital.
En 1988, faisant suite au second choc pétrolier, à une sécheresse importante et aux carences du management du groupe BIAO, une restructuration du capital a été menée permettant au Groupe MIMRAN de devenir actionnaire à hauteur de 10%.
En 1993, à l'occasion des 140 ans de la banque, la dénomination a changé pour devenir la Compagnie Bancaire de l'Afrique Occidentale (CBAO).

Enfin, en novembre 2007, le groupe AttijariWafa bank, accompagné par ses actionnaires de référence (ONA, SNI) a amorcé l'acquisition de 79.15% du capital de la Compagnie Bancaire de l'Afrique Occidentale (CBAO) auprès du groupe Mimran. Cette opération a été conclue en avril 2008 suite au Conseil d'administration de la CBAO qui a constaté sa recomposition du capital.

Le groupe AttijariWafa bank, par cette acquisition, réitère ainsi sa volonté de disposer des atouts nécessaires au déploiement de son projet de développement au Sénégal et dans l'ensemble des pays de la région de l'Afrique de l'Ouest.
Ce développement avait d'ailleurs commencé par la création d'AttijariWafa bank Sénégal en juillet 2006, première filiale du Groupe en Afrique Occidentale, suivi par l'acquisition de la Banque Sénégalo-Tunisienne (BST) en 2006 et enfin la fusion entre AttijariWafa bank Sénégal et la BST un an plus tard, donnant naissance à Attijari bank Sénégal.

Fiche d'identité du Groupe AttijariWafa bank :

Le Groupe AttijariWafa bank, premier groupe bancaire et financier du Maghreb, avec plus de 4,2 millions de clients et 12 400 collaborateurs, est une multinationale panafricaine.
Présent dans 21 pays, le Groupe se donne pour priorité la proximité avec ses clients et les met au cœur de sa stratégie via son ambitieux programme de bancarisation et ses efforts d'innovation continus.

3) Constitution du Capital

Le capital social de la CBAO Groupe AttijariWafa bank s'élève aujourd'hui à 11 milliards 450 millions de francs CFA et est détenu à hauteur :

- de 79,15% par le Groupe AttijariWafa bank (Maroc),
- 9% par l'Etat du Sénégal
- 12% par des privés.

4) Organisation

La CBAO Groupe AttijariWafa bank est dirigée depuis la mi-juillet 2008 par M. Abdelkrim RAGHNI.
Elle dispose d'une Conseil d'Administration de 11 membres dont :

- Le Président du Conseil d'Administration
- L'Administrateur Directeur Général
- 8 administrateurs
- 1 Représentant de l'Etat du Sénégal [1]

La banque est composée de 18 directions dont la DOSI (Direction de l'organisation des Systèmes d' Information.

Cette dernière est constituée de 3 départements

- Département Etudes et Développements

Il est chargé du développement des applications utilitaires ainsi que du support des applications bancaires.

- Département SI Monétiques

Créée depuis peu, il est chargé de gérer la productivité des logiciels bancaires, le bon fonctionnement des équipements monétiques et de toutes les transactions.

- Département Traitement Monétiques

Il est chargé de traiter les requêtes monétiques comme la création de cartes, la résiliation, les déclarations de perte la distribution et les contentieux.

- Département Sécurité des Systèmes d'Information

Son rôle est de veiller à l'intégrité des systèmes d'Information. Il est garant de la bonne marche. De ce fait, il dispose de politiques et outils sophistiqués pour se prémunir des éventuelles attaques extérieures.

- Département Ingénierie Technique

Il est constitué de deux services :

- Le service Support et Systèmes : Son rôle est d'assurer le bon fonctionnement des systèmes d'exploitation clients et hébergeant les applications de la banque et d'apporter un support technique aux usagers.
- Le service Réseaux : Son rôle est d'assurer le bon fonctionnement des installations Réseau de la banque afin de garantir la continuité des services de la banque.

Partie 2 : Etude Technique

I. Problématique 1 : Disponibilité des équipements Monétiques

1) Présentation

La monétique désigne l'ensemble des traitements électroniques, informatiques et télématiques nécessaires à la gestion de cartes bancaires ainsi que des transactions associées. Elle constitue de ce fait une partie essentielle quant à la survie d'une banque du fait de l'évolution grandissante des technologies ainsi que la modernisation des transactions bancaires.

Conscient de cela, la CBAO dispose d'un réseau fort impressionnant de 100 GAB et de plus de 800 TPE à travers le territoire national. Tous ces équipements sont interconnectés au réseau du siège via des lignes spécialisées, ADSL ou GPRS.

2) Mission

La mission du Département SI Monétique, crée il y'a un an, est de veiller à la bonne marche de tous les services monétiques proposés aux clients à savoir les GAB, TPE…..

Pour ce faire, il dispose d'outils de supervision et monitoring afin de savoir en temps réel l'état de chaque équipement et des interfaces de connexions aux dédits équipements.

3) Equipements et outils utilisés

a) Les GAB ou DAB

1. Utilisation

Dans la plupart des GAB modernes, le client insère une carte en plastique munie d'une bande magnétique ou d'une puce contenant les données nécessaires à l'identification du client. Pour demander l'accès à ses comptes, le client saisit un code de quatre à quinze chiffres. Si le code est saisi de façon incorrecte plusieurs fois de suite, la plupart des GAB retiennent la carte dans le but d'éviter des fraudes. Dans le cas contraire, il serait possible de découvrir le code par force brute. Ces cartes sont parfois détruites pour éviter que des employés de banque n'en profitent.

2. Réseau

Tous les GAB sont connectés à un GDG (Gestionnaire de DAB/GAB). Ce GDG est lui-même connecté au réseau interbancaire, ce qui facilite le retrait et autres opérations n'appartenant pas à la banque où le client possède un compte. Cette structure est particulièrement utile aux personnes qui voyagent. Par exemple, un client de la banque en voyage dans un autre pays, peut grâce à sa carte Visa, GIM ou MasterCard effectué des transactions bancaires dans les banques locales.

De ce fait, ces transactions seront gérées par ces groupements interbancaires partenaires. Parmi ces réseaux bancaires, on peut citer le Groupement Interbancaire Monétique (GIM) de l'Union Economique et Monétaire Ouest Africaine (UEMOA).

Les GAB n'effectuent de transactions que si l'institution bancaire les autorise, celles-ci passent nécessairement par le réseau interbancaire concerné.

3. Matériel et logiciel

Les GAB font appel à des processeurs avec chiffrement, habituellement installés à l'intérieur de PC enchâssés dans une enceinte sécurisée. Les logiciels tournent dans un système d'exploitation courant. La sécurité de l'appareil s'appuie pour beaucoup sur le processeur sécurisé.

Les GAB se connectent au système d'information de la banque via un modem raccordé à une ligne téléphonique, commutée ou dédiée. Le deuxième type de connexion est préférable, puisque le temps de connexion est plus court. Cependant, elle est plus coûteuse, les GAB moins utilisés seront plutôt connectés de la première façon (ligne commutée). Le coût d'un lien externe étant souvent moins coûteux que celui d'une ligne dédiée, l'utilisation d'une ligne partagée tend à disparaître. De plus, les GAB installés contiennent de moins en moins de circuits intégrés spécialisés (pour la plupart autour du processeur Intel 8086) et font de plus en plus appel à un PC venant avec un système d'exploitation courant tels que Windows. Par exemple, CBAO quant à elle utilise des systèmes Windows 7 ou XP.

4. Fiabilité

Les GAB sont en général fiables, mais dès qu'ils ont une panne quelconque, le client doit attendre l'ouverture d'une succursale pour obtenir réparation. Bien que la plupart du temps, les erreurs soient en défaveur des clients, il y a parfois des cas où elles sont en sa faveur.

Les causes d'erreur sont multiples :

- mécanique : lecteur de cartes défectueux, clavier brisé et disque dur corrompu
- logiciel : système d'exploitation en faute et pilote de périphérique dépassé
- communication : réseau en panne de façon intermittente
- humaine : mauvaise saisie

Plusieurs GAB impriment les transactions sur un papier, lequel provient d'un rouleau de papier situé à l'intérieur de l'appareil. L'impression est faite en double, ce qui permet aux institutions bancaires de faire valoir leur point de vue si un client conteste une transaction financière. Dans certains cas, les transactions sont notées électroniquement dans le but de réduire la consommation de papier. Pour le cas de la Cbao, les pannes sont généralement mécaniques ou dues à une défection du lecteur ou à un bourrage de papiers au sein de l'imprimante.

5. Sécurité

La sécurité des guichets automatiques de banque repose sur la cryptographie et constitue une importance capitale pour l'intégrité des systèmes bancaires or certaines banques ne font pas suffisamment d'efforts pour sécuriser les GAB.

Il existe des cas documentés de fraudeurs qui ont construit de faux GAB dans le but de soutirer différentes informations des clients. Il y en a qui ont aussi attaché de faux claviers ou de faux lecteurs de cartes à de vrais GAB ou qui ont développé la technique du collet marseillais, ce qui n'a jusque-là jamais été signalé au Sénégal.

De ce fait, il est indispensable d'assurer les principes de non-répudiation, l'authentification, la confidentialité et l'intégrité .Ainsi des algorithmes de cryptographie très sophistiqués qui sont restés jusque-là inconnus du public sont utilisés pour les besoins.

b) Les Terminaux de Paiement Electroniques (TPE)

Ce sont les terminaux permettant des transactions (paiement ou retrait) par carte bancaire. Au Sénégal, elle est utilisée en majeure partie par les commerçants, les hôtels et restaurants .La partie permettant de saisir le code confidentiel parfois autonome du reste du TPE s'appelle le PinPad.

Le TPE, dans le modèle français adopté au Sénégal, va gérer deux types de transactions :

- d'une part les transactions de demande d'autorisation.
- d'autre part les transactions de télécollecte.

L'ensemble des transactions sont stockées dans le TPE et sont envoyées durant la nuit à un serveur monétique pour les besoins de traitement de fin de journée. Ce système français est moins coûteux en communication (volume de trafic) mais moins fiable du fait des risques encourus comme la perte des données au niveau du TPE. En effet, les porte-monnaies électroniques doivent pouvoir fonctionner hors connexion, ensuite des télécollectes permettent aux commerçants d'être crédités.

En outre, il existe un autre modèle belge, qui consiste à faire des transactions full on-line c'est-à-dire, toutes les opérations passent inéluctablement par le serveur monétique.

Cependant, ce modèle est très couteux en termes de trafic mais confère plus de sécurité que le précédent.

Traditionnellement, il existe deux types de TPE :

- Les TPE RTC-ADSL

Qui utilisent une connexion ADSL pour communiquer avec le serveur distant

- Les TPE GPRS

- Les TPE 3G : Tout récemment, certains constructeurs tels que INGENICO ont sorti de nouveaux modèles de TPE capables de communiquer avec des puces 3G « mono operateur » ou « multi operateur » ce qui facilitera et augmentera la qualité de transmission des informations transactionnelles.

1. Principe de fonctionnement

Pour la connexion aux serveurs d'application monétique(Zone CHD) , les TPE sont obligés de passer par des Gateway des constructeurs localisés dans la DMZ publique pour les besoins de cryptage , d'authentification et de conversion IP-X25.

En effet, chaque constructeur dispose de ces propres Gateway, de même l'interface entre ces passerelles et le serveur d'application s'établit avec le protocole X.25. Ces deux zones sont séparées par des équipements de sécurité très sophistiqués comme IPS, Firewall ASA …..

4) Gestion des flux

La gestion des flux dans le domaine de la monétique n'est possible qu'à la condition que les différents acteurs (émetteur, porteur, accepteur, acquéreur) adhérent sans réserve aux multiples contraintes imposées par les systèmes de transfert des informations proposés par les établissements financiers. De ce fait, il existe plusieurs organismes internationaux et sous régionaux chargés de veiller sur ces règles et d'interconnecter les différents établissements bancaires. Le typage des informations obéit à des règles très strictes et normalisées au niveau domestique et international.

a) Les flux domestiques

Il s'agit d'opérations faites dans un pays (niveau local) par des porteurs de cartes émises par les établissements financiers dudit pays. Ces opérations sont échangées entre émetteur et acquéreur via un système de compensation (Zone Uemoa : GIM (Groupement Interbancaire Monétique)). Ces échanges sont réalisées tous les jours ouvrables (du lundi au vendredi) entre banques membres et sont supervisées par la BCEAO. GIM a pour rôle de router les transactions en fonction du BIN (Bank Identification Number) et de régulariser des opérations bancaires. En effet, si un client d'une banque A insère sa carte dans un GAB ou TPE d'une banque B, alors celle-ci envoie le numéro de ladite carte à GIM pour qu'il identifie la banque émettrice .Ainsi, une fois la banque connue, la communication sera établie pour vérifier les identifiants du client et son solde. [2]

b) Les flux internationaux

Il s'agit d'opérations faites soit :

- dans le pays même par des porteurs de cartes émises par des établissements étrangers avec un acquéreur et accepteur du pays ;
- à l'étranger par des porteurs de cartes émises par les établissements du pays d'origine.

Ces flux, appelés outgoing et incoming sont échangés entre banques via la passerelle des réseaux internationaux Visa et EuroCard-MasterCard.

Si une carte émise par une banque étrangère est insérée dans un terminal de paiement, le logiciel monétique PowerCard contacte le réseau de Visa Ou MasterCard pour identifier la banque émettrice.

Les flux passent dans le réseau de la banque, pour transiter vers Visa ou MasterCard enfin d'être router à la banque d'origine .A cet effet, les transactions consomment une très grosse part de la bande passante du système ce qui nécessite un bon dimensionnement du réseau pour assurer la disponibilité du service.

c) Diagramme des flux

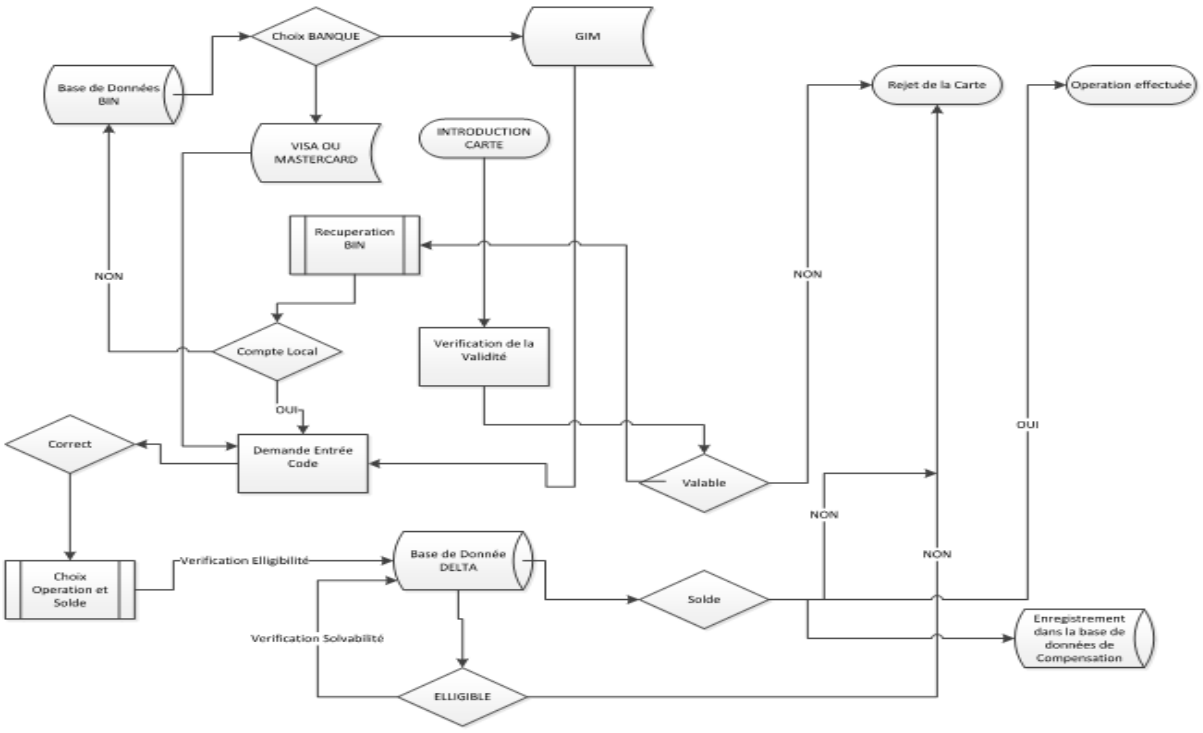


Figure 1:Diagramme des flux bancaires

5) Dysfonctionnements

a) Approche technique

Le service dispose d'un système d'alerte pour les pannes survenues dans les terminaux de paiement comme les GAB ou TPE. Le logiciel de traitement des transactions électroniques POWERCARD dispose d'un système de télésurveillance, qui permet à la personne en charge de savoir en « temps réel » les problèmes survenus au niveau des équipements interconnectés au réseau .Mais ceci ne pourrais être efficace qu'avec une surveillance 24h/24, ce qui est loin d'être évident.

La supervision de l'état des interfaces monétiques qui sont les garants des transactions monétiques locales (GIM etc.) et internationales (Visa, MasterCard) est le souci majeur car ne disposant pas d'un système des plus fiables.

De ce fait, une interface peut tomber en panne pendant plusieurs minutes sans pour autant que le système le signale, ainsi plusieurs transactions seront perdues ce qui constitue un gros manque à gagner.

L'une des principales causes de l'inefficacité des interventions est **l'avalanche d'alertes** qui consiste à envoyer plusieurs alertes pour un même incident ou pour un incident mineur. Ainsi une alerte importante peut être noyée dans une grande masse d'alerte et sera ignorée.

b) Approche Organisationnelle

Avec l'outil de supervision actuel les agents ne disposent pas de statistiques sur la fréquence des pannes et la gestion des alertes bien qu'étant opérationnelles n'est pas optimisée.

En effet, le logiciel renseigne tous les changements d'états des différents périphériques supervisés sur les tables temporaires à partir desquelles il procède à des sondes régulières ce qui ne facilite pas la génération de rapports d'incidents. Ainsi, l'équipe chargée de la gestion de l'exploitation des Gabs ne dispose d'aucune donnée pour la mesure de rendements (dépenses, total commissions) et de l'efficacité d'intervention de prestataires afin d'évaluer leurs travails.

De même, la majeure partie des incidents signalés par les alertes mails aux gestionnaires de Gabs ne sont pas prises en charge .De ce fait, le client peut rester des heures à vouloir effectuer une transaction sans pour autant y parvenir.

Fort de tous ces constats et dans le souci d'améliorer la prise en charge des incidents, nous proposerons dans ce qui suit un système de notification d'alerte unifié avec la possibilité d'alerter les concernés (télé surveillant et gestionnaires de GAB ou commerçants) de l'état des équipements.

6) Solution SightGAB : Approche Technique

La supervision des GAB est un point important dans la gestion des incidents et de ce fait constitue un moyen très efficace dans l'amélioration de l'efficacité et la productivité des services monétiques.

En effet, la CBAO dispose actuellement d'un système de télésurveillance couplé avec le logiciel POWERCARD, mais celui-ci ne permet pas de connaitre à coup sûr la nature du problème survenu donc n'aide pas à la pratique de trouble-shooting. Les gestionnaires Gabs et les responsables des agences ne disposent d'aucun outil leur permettant d'analyser l'activité des Gabs dont ils ont la charge et ne disposent d'aucune statistique sur le bon fonctionnement.

Or ces statistiques pourraient leur permettre de mieux gérer l'approvisionnement en consommables et billets par exemple.

a) Objectifs

Ce système permet la supervision en temps réel des guichets automatiques bancaires en se basant sur les journaux électroniques et les agents SNMP actifs sur les Gabs et fournit ainsi les fonctionnalités suivantes :

- Suivi de l'état global du GAB et de ses périphériques et des TPE
- Suivi particulier des états des imprimantes (journal et reçu) et de leurs consommables.
- Suivi du contenu des cassettes.
- Détection des coupures de la ligne entre le GAB et le serveur monétique.

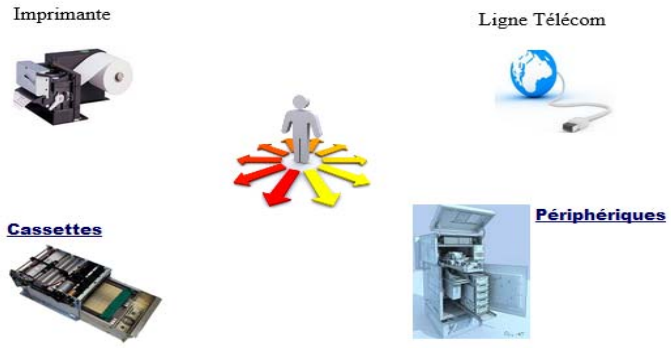


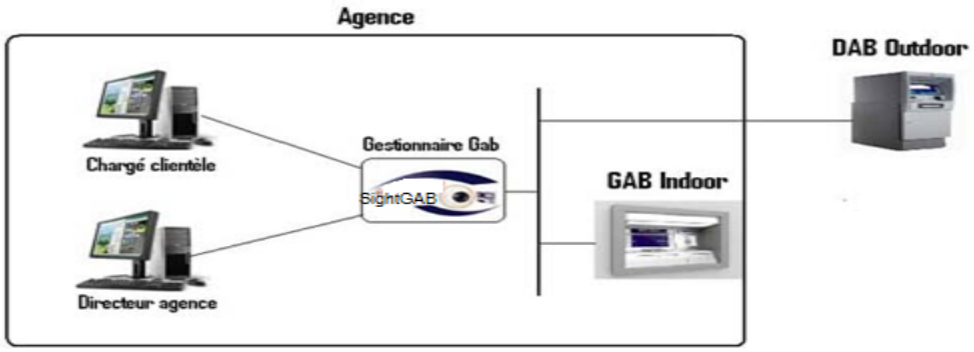
Figure 2: Schéma illustratif des composants supervisés/GAB

b) Architecture SightGAB

1. Principe

SightGAB est en architecture Client/serveur et peut être déployé sur deux types de postes :

- Principal : Un seul poste principal est nécessaire et suffisant pour gérer les terminaux GAB et héberge : la base de données, le composant serveur et l'application client
- Secondaire : Aucun déploiement n'est nécessaire sur le poste, car le client peut accéder à la plateforme via un navigateur selon ses habilitations.



SightGAB est accessible sur un ou plusieurs PC en agence via le navigateur et se présente sous forme d'un tableau de bord simple et intuitif qui se met à jour en temps réel selon les évènements qui se produisent sur le GAB.

Composantes

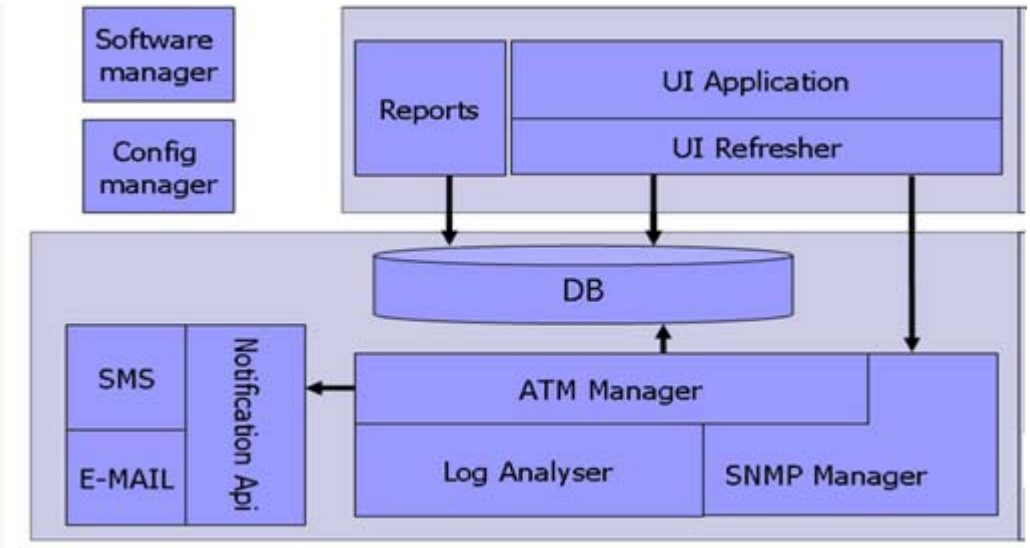


Figure 3:Architecture SightGAB

c) Comment superviser

De nombreuses solutions sont disponibles. Certaines sont spécialisées dans la supervision de système d'information, d'autres sont plus globales. La différenciation s'effectue généralement sur le nombre de paramètres exploitables et leur finesse d'analyse. Cette précision ne doit pas pour autant rendre les tableaux de bord et les synthèses illisibles pour les administrateurs. Cependant elle doit alerter d'un fonctionnement normal ou anormal.
Le fonctionnement est simple, il se compose d'un superviseur qui va effectuer l'acquisition de données de manière active ou passive.

Cette acquisition va se faire de façon automatique avec le protocole SNMP, qui est présent sur la majorité des équipements informatiques.

1. Fonctionnement

L'agent SNMP installé gére les informations relatives à l'equipement qui sont stockées dans une base de données propre : la MIB (Managment Information Base).
Pour faire simple, chaque equipement contient des OID, les OID sont une liste de numeros servant à identifier des ressources.Une MIB sert à faire la translation d'un OID en un nom comprehensible.

Le serveur de supervision va interroger l'agent SNMP d'un equipement ,cet equipement va chercher dans sa MIB pour lui envoyer une valeur précise.Cette interrogation est réalisée avec le protocole UDP sur les ports 161 et 162.
Pour communiquer ensemble , le serveur et l'equipement doivent etre dans la meme communauté SNMP. [3]
Ci-dessous , un schema explicatif :

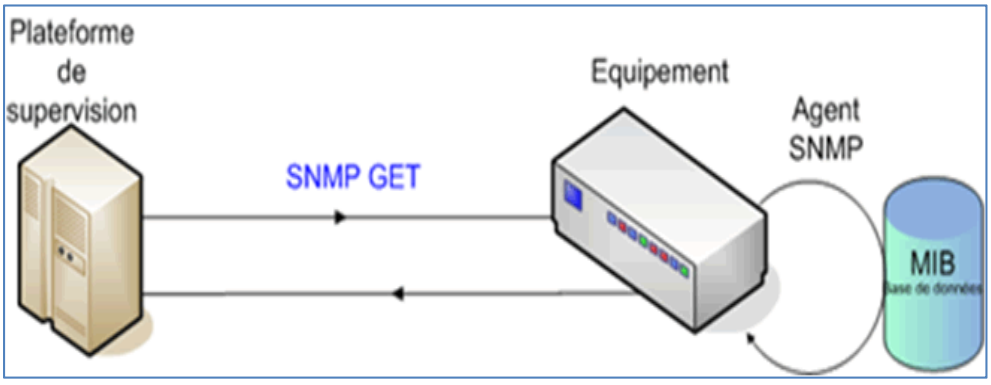
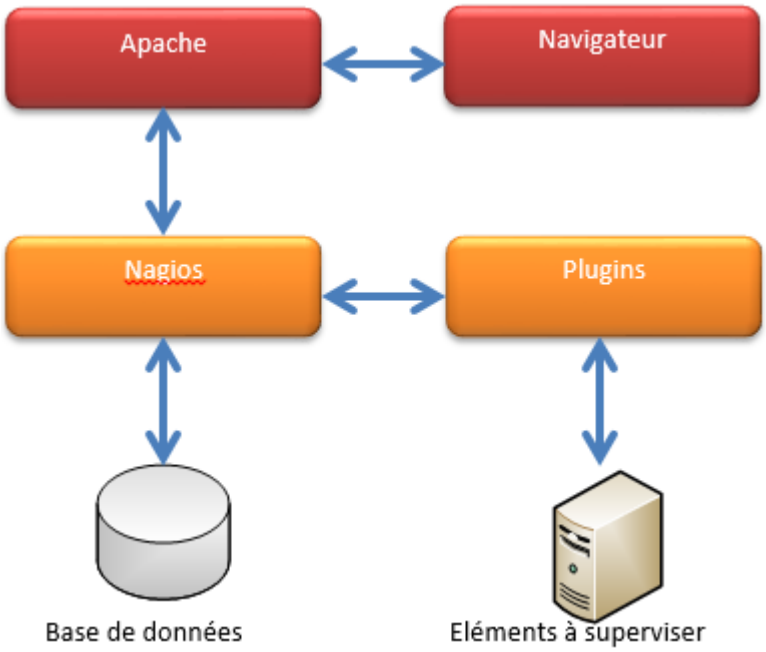


Figure 4:Schéma explicatif du fonctionnement des requêtes SNMP

L'architecture du système se compose de 5 éléments :

1- Le serveur Nagios qui récupère les informations des plugins et qui opère en conséquence
2- Une base de données qui stocke ces informations
3- Des plugins que l'on va choisir en fonction de nos besoins et qui permettent d'obtenir des valeurs sur les éléments supervisés.
4- Les éléments supervisés qui fournissent les informations
5- Une interface web qui permet de gérer le tout.

Schéma



d) Etude pour la mise en place

1. Concept de la supervision SNMP

L'informatique est de plus en plus présente dans notre vie de tous les jours. On compte désormais sur les services offerts par les réseaux pour le fonctionnement de l'outil informatique, que ce soit en entreprise, lors des transactions bancaires, lors de téléconférences etc. Les services offerts sont devenus quasi-indispensables. Pour assurer que ces services soient efficaces, il est nécessaire de surveiller le réseau et d'agir quand une erreur se produit.

Sur les réseaux physiques de nombreuses composantes sont donc à surveiller : l'utilisation de la largeur de bande, l'état de fonctionnement des liens, les éventuels goulets d'étranglement, les problèmes de câblage, le bon cheminement de l'information entre les machines, etc.

Pour ce faire, différents points stratégiques sont à observer comme les routeurs, les concentrateurs, les liens, les postes, les imprimantes.

Ainsi, en cas de panne ou de mauvais fonctionnement sur le réseau, l'administrateur doit pouvoir interpréter l'information reçue pour identifier la source du problème. A cet effet, un protocole de gestion est nécessaire pour exercer les fonctions de gestion sur un réseau. Il doit être capable de dialoguer avec tous les éléments de celui-ci.

2. SNMP (Simple Network Management Protocol)

a. *Présentation Générale*

SNMP (Simple Network Management Protocol) est le protocole de gestion de réseaux proposé par l'IETF. Il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux.
SNMP est un protocole relativement simple. Pourtant l'ensemble de ses fonctionnalités est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications: les bases de données, les serveurs, les logiciels, etc.

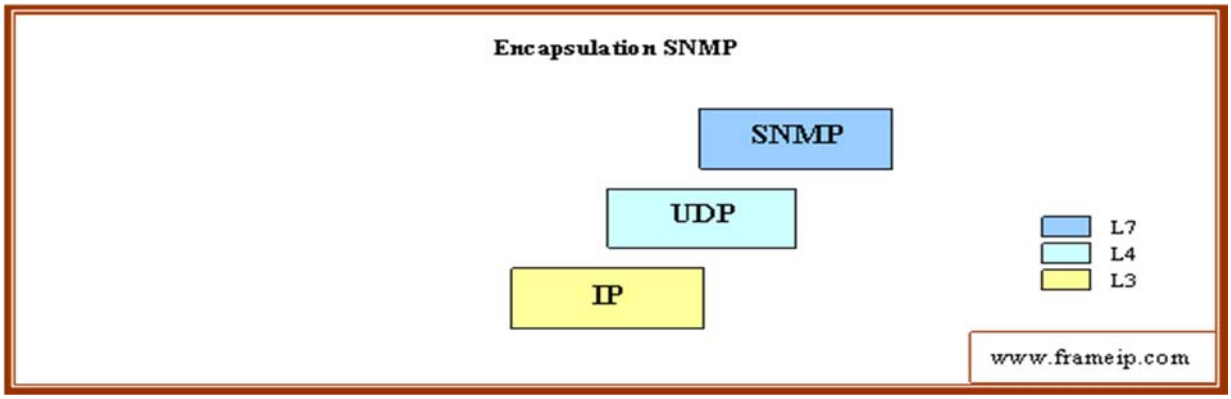
L'environnement de gestion SNMP est constitué de plusieurs composantes : la station de supervision, les éléments actifs du réseau, les variables MIB et un protocole. Les différentes composantes du protocole SNMP sont les suivantes:

- Les éléments actifs du réseau sont les équipements ou les logiciels que l'on cherche à gérer. Cela va d'une station de travail à un concentrateur, un routeur, un pont, etc. Chaque élément du réseau dispose d'une entité dite agent qui répond aux requêtes de la station de supervision. Les agents sont des modules qui résident dans les éléments réseau. Ils vont chercher l'information de gestion comme par exemple le nombre de paquets reçus ou transmis.

- La station de supervision (appelée aussi manager) exécute les applications de gestion qui contrôlent les éléments réseaux. Physiquement, la station est un poste de travail.
- La MIB (Management Information Base) est une collection d'objets résidant dans une base d'information virtuelle. Ces collections d'objets sont définies dans des modules MIB spécifiques.
- Le protocole, qui permet à la station de supervision d'aller chercher les informations sur les éléments de réseaux et de recevoir des alertes provenant de ces mêmes éléments.

Le protocole SNMP est basé sur un fonctionnement asymétrique. Il est constitué d'un ensemble de requêtes, de réponses et d'un nombre limité d'alertes. Le manager envoie des requêtes à l'agent, lequel retourne des réponses. Lorsqu'un événement anormal surgit sur l'élément réseau, l'agent envoie une alerte (trap) au manager.

SNMP utilise le protocole UDP [RFC 768]. Le port 161 est utilisé par l'agent pour recevoir les requêtes de la station de gestion (SNMP Get). Le port 162 est réservé pour la station de gestion pour recevoir les alertes des agents (SNMP Trap). [3]



Les requêtes SNMP
Il existe quatre types de requêtes: GetRequest, GetNextRequest, GetBulk, SetRequest.

- La requête GetRequest permet la recherche d'une variable sur un agent.
- La requête GetNextRequest permet la recherche de la variable suivante.
- La requête GetBulk permet la recherche d'un ensemble de variables regroupées.
- La requête SetRequest permet de changer la valeur d'une variable sur un agent.

Les réponses de SNMP
À la suite de requêtes, l'agent répond toujours par GetResponse. Toutefois si le variable demandé n'est pas disponible, le GetResponse sera accompagné d'une erreur noSuchObject.

Les alertes (Traps, Notifications)
Les alertes sont envoyées quand un événement non attendu se produit sur l'agent. Celui-ci en informe la station de supervision via une trap. Les alertes possibles sont: ColdStart, WarmStart, LinkDown, LinkUp, AuthentificationFailure. [3]

b. MIB (Management Information Base)

La MIB (Management Information base) est la base de données des informations de gestion maintenue par l'agent, auprès de laquelle le manager va venir pour s'informer.

Deux MIB publics ont été normalisées: MIB I et MIB II (dite 1 et 2)

Un fichier MIB est un document texte écrit en langage ASN.1 (Abstract Syntax Notation 1) qui décrit les variables, les tables et les alarmes gérées au sein d'une MIB. La MIB est une structure arborescente dont chaque nœud est défini par un nombre ou OID (Object Identifier).
Elle contient une partie commune à tous les agents SNMP en général, une partie commune à tous les agents SNMP d'un même type de matériel et une partie spécifique à chaque constructeur. Chaque équipement à superviser possède sa propre MIB. Non seulement la structure est normalisée, mais également les appellations des diverses rubriques.

Ces appellations ne sont présentes que dans un souci de lisibilité. En réalité, chaque niveau de la hiérarchie est repéré par un index numérique et SNMP n'utilise que celui-ci pour y accéder. [3]

Voici un exemple de structure de table MIB :

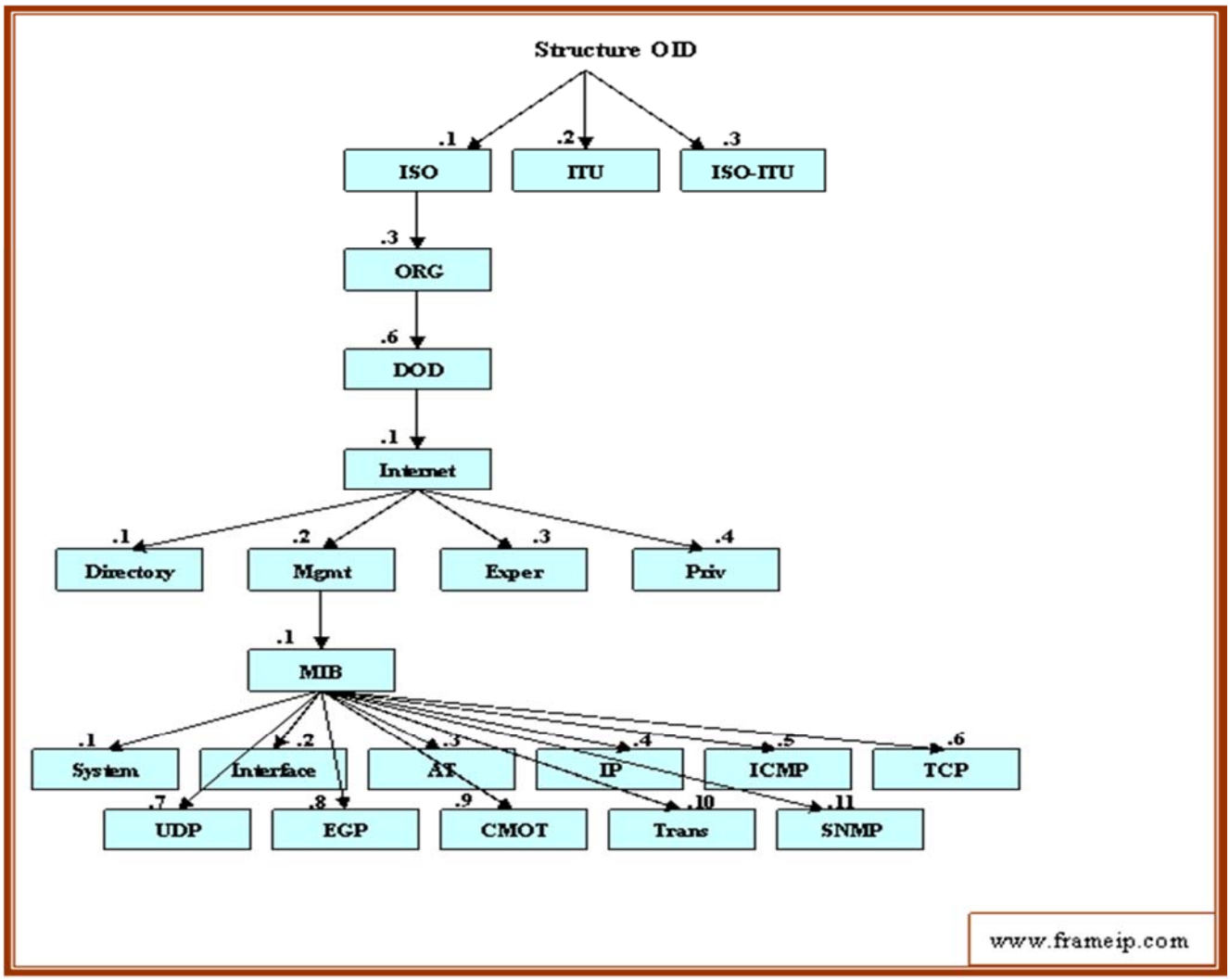


Figure 5:Exemple de table MIB

Ainsi, pour interroger les différentes variables d'activité sur un appareil, il faudra explorer son arborescence MIB. Celle-ci est généralement fournie par le constructeur mais il est aussi possible d'utiliser un explorateur de MIB tel que « Getif MIB Browser ».
Ensuite, pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne l'emplacement de la variable à consulter dans la MIB. On aura par exemple sur un commutateur Nortel Passport l'OID .1.3.6.1.4.1.2272.1.1.20 désignant le taux de charge du CPU.
Lorsqu'une entreprise veut définir son propre ensemble de variables de gestion, elle va enregistrer son numéro d'objet sous le nœud iso.org.dod.internet.private.entreprise.Ces MIB seront dites privées. Elles correspondent à la racine 1.3.6.1.4.1. Voici la liste de toutes les affectations officielles :

entreprise.0-4998
entreprise.5000-9999
entreprise.10000-14999
entreprise.14999-19999
entreprise.20000-24999
entreprise.25000-27274

c. Présentation, évolution des versions de SNMP

Voici les différentes versions de SNMP:

- SNMPv1 (ancien standard): Celui-ci est la première version du protocole, tel que définie dans le RFC 1157. On dit que la sécurité de cette version est triviale, car la seule vérification qui est faite est basée sur la chaîne de caractères "community ". SNMPsec (historique): Cette version ajoute de la sécurité au protocole SNMPv1. La sécurité est basée sur des groupes. Très peu ou aucun manufacturier n'a utilisé cette version qui est maintenant largement oubliée.
  RFC 1155

- SNMPv2p (historique): Beaucoup de travaux ont été exécutés pour faire une mise à jour de SNMPv1. Ces travaux ne portaient pas seulement sur la sécurité. Le résultat est une mise à jour des opérations du protocole, des nouvelles opérations, des nouveaux types de données. La sécurité est basée sur les groupes de SNMPsec.

- SNMPv2c (expérimental): Cette version du protocole est appelée "community stringbased SNMPv2 ". Ceci est une amélioration des opérations de protocole et des types d'opérations de SNMPv2p et utilise la sécurité par chaîne de caractères "community " de SNMPv1.
  RFC-1441

- SNMPv2u (expérimental): Cette version du protocole utilise les opérations, les types de données de SNMPv2c et la sécurité basée sur les usagers.

- SNMPv2* (expérimental): Cette version combine les meilleures parties de SNMPv2p et SNMPv2u. Les documents qui décrivent cette version n'ont jamais été publiés dans les RFC. Des copies de ces documents peuvent être trouvées sur le site web et SNMP Research (un des premiers à défendre cette version).
  RFC - 1901

- SNMPv3 (standard actuel): Cette version comprend une combinaison de la sécurité basée sur les usagers et les types et les opérations de SNMPv2p, avec en plus la capacité pour les "proxies ". La sécurité est basée sur ce qui se trouve dans SNMPv2u et SNMPv2*.
  RFC - 3411 [3]

i. Les faiblesses de SNMPv1

Une des plus grandes faiblesses du protocole SNMPv1 est l'absence d'un mécanisme adéquat pour assurer la confidentialité et la sécurité des fonctions de gestion. Les faiblesses comprennent aussi l'authentification et le chiffrement, en plus de l'absence d'un cadre administratif pour l'autorisation et le contrôle d'accès.

Ce problème rend la sécurité sur SNMPv1 du type : "SHOW-AND-TELNET", c'est à dire qu'on utilise SNMP pour l'acquisition des données de gestion, mais pas pour effectuer le contrôle on utilise le protocole Telnet.

Tous les consensus du groupe de travail ont été rassemblés (seulement les améliorations ne portaient pas sur la sécurité), et le groupe de travail SNMPv2 de l'IETF a terminé ses travaux en publiant une version de SNMPv2 (on l'appelle SNMPv2c, RFC 1901, RFC 1905 et RFC 1906) sans sécurité.

ii. Les améliorations de SNMPv2c

SNMPv2c a introduit quelques nouveaux types, mais sa nouveauté majeure est l'opération GETBULK, qui permet à une plateforme de gestion, de demander en bloc de plusieurs variables consécutives dans la MIB de l'agent. Généralement, on demande autant de variables que l'on peut mettre dans un paquet SNMP. Ceci règle un problème majeur de performance dans SNMPv1. Avec la version 1, la plateforme est obligée de faire un GETNEXT et d'attendre la réponse pour chaque variable de gestion.

iii. Les améliorations de SNMPv3

Cette nouvelle version du protocole SNMP vise essentiellement à inclure la sécurité des transactions. La sécurité comprend l'identification des parties qui communiquent et l'assurance que la conversation soit privée, même si elle passe par un réseau public.

Cette sécurité est basée sur 2 concepts :

- ***USM (User-based Security Model)***

Trois mécanismes sont utilisés. Chacun de ces mécanismes a pour but d'empêcher un type d'attaque.

- L'authentification : empêche quelqu'un de changer le paquet SNMPv3 en cours de route et de valider le mot de passe de la personne qui transmet la requête.
- Le chiffrement : empêche quiconque de lire les informations de gestions contenues dans un paquet SNMPv3.
- L'estampillage du temps : empêche la réutilisation d'un paquet SNMPv3 valide a déjà transmis par quelqu'un.

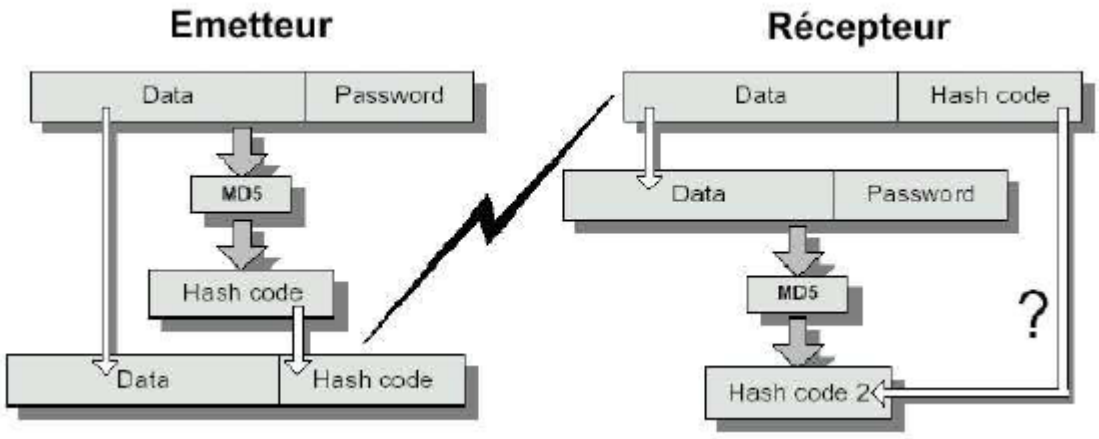
- L'authentification

L'authentification a pour rôle d'assurer que le paquet reste inchangé pendant la transmission, et que le mot de passe est valide pour l'usager qui fait la requête.

Pour construire ce mécanisme, on doit avoir connaissance des fonctions de hachage à une seule direction. Des exemples de ces fonctions sont : MD5 et SHA-1. Ces fonctions prennent en entrée une chaîne de caractères de longueur indéfinie, et génèrent en sortie une chaîne d'octets de longueur finie (16 octets pour MD5, 20 octets pour SHA-1).

Pour authentifier l'information qui va être transmise, on doit aussi avoir un mot de passe qui est « partagé ». Le mot de passe ne doit donc être connu que par les deux entités qui s'envoient les messages, et préférablement par personne d'autre. [3]

La figure ci-dessous montre le mécanisme d'authentification :



Les étapes d'authentification sont les suivantes :

- Le transmetteur groupe des informations à transmettre avec le mot de passe.
- On passe ensuite ce groupe dans la fonction de hachage à une direction.
- Les données et le code de hachage sont ensuite transmis sur le réseau.
- Le receveur prend le bloc des données, et y ajoute le mot de passe.
- On passe ce groupe dans la fonction de hachage à une direction.
- Si le code de hachage est identique à celui transmis, le transmetteur est authentifié.

Avec cette technique, le mot de passe est validé sans qu'il ait été transmis sur le réseau. Quelqu'un qui saisit les paquets SNMPv3 passants sur le réseau ne peut pas facilement trouver le mot de passe.

Pour ce qui est de SNMPv3, l'authentification se fait à l'aide de HMAC-MD5-96 ou de HMAC-SHA- 96, qui est un peu plus compliqué que ce qui a été décrit ici. Le résultat de la fonction de hachage est placé dans le bloc paramètres de sécurité du paquet SNMPv3.

L'authentification se fait sur tout le paquet.

L'étape d'authentification ne vise pas à cacher l'existence du paquet ou à le chiffrement. Si l'on utilise uniquement l'authentification, les personnes qui saisissent les paquets passants sur le réseau peuvent encore en voir le contenu. Toutefois, elles ne peuvent pas changer le contenu sans connaître le mot de passe.

- Le chiffrement

Le chiffrement a pour but d'empêcher que quelqu'un n'obtienne les informations de gestion en écoutant sur le réseau les requêtes et les réponses de quelqu'un d'autre. Avec SNMPv3, le chiffrement de base se fait sur un mot de passe « partagé » entre le manager et l'agent.

Ce mot de passe ne doit être connu par personne d'autre. Pour des raisons de sécurité, SNMPv3 utilise deux mots de passe : un pour l'authentification et un pour le chiffrement. Ceci permet au système d'authentification et au système de chiffrement d'être indépendants. Un de ces systèmes ne peut pas compromettre l'autre.

SNMPv3 se base sur DES (Data Encryption Standard) pour effectuer le chiffrement.

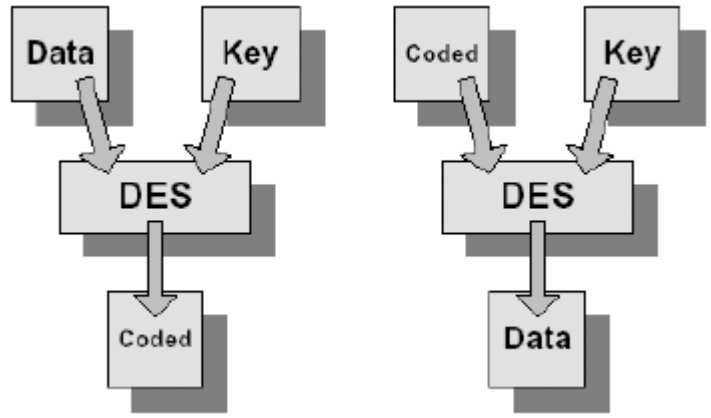


Figure 6:Chiffrement DES/SNMPv3

On utilise une clé de 64 bits (8 des 64 bits sont des parités, la clé réelle est donc longue de 56 bits) et DES chiffrement 64 bits à la fois. Comme les informations que l'on doit chiffrer sont plus longues que 8 octets, on utilise du chaînage de blocs DES de 64 bits.

Une combinaison du mot de passe, d'une chaîne aléatoire et d'autres informations forme le « Vecteur d'initialisation ». Chacun des blocs de 64 bits est passé par DES et est chaîné avec le bloc précédent avec un XOR. Le premier bloc est chaîné par un XOR au vecteur d'initialisation. Le vecteur d'initialisation est transmis avec chaque paquet dans les « Paramètres de sécurité », un champ qui fait partie du paquet SNMPv3.

Contrairement à l'authentification qui est appliquée à tout le paquet, le chiffrement est seulement appliqué sur le PDU.

La RFC 3826 "The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model" relate l'intégration d'AES dans SNMP. Celui renforce le chiffrement en remplacement du DES. Cependant, pour le moment, cette RFC est en cours de validation et donc pas encore officialisée.

- L'estampillage de temps

Si une requête est transmise, les mécanismes d'authentification et de chiffrement n'empêchent pas quelqu'un de saisir un paquet SNMPv3 valide du réseau et de tenter de le réutiliser plus tard, sans modification.

Par exemple, si l'administrateur effectue l'opération de remise à jours d'un équipement, quelqu'un peut saisir ce paquet et tenter de le retransmettre à l'équipement à chaque fois que cette personne désire faire une mise à jour illicite de l'équipement.

Même si la personne n'a pas l'autorisation nécessaire, elle envoie un paquet, authentifié et chiffré correctement pour l'administration de l'équipement.

On appelle ce type d'attaques le « Replay Attack ». Pour éviter ceci, le temps est estampillé sur chaque paquet. Quand on reçoit un paquet SNMPv3, on compare le temps actuel avec le temps dans le paquet. Si la différence est plus que supérieur à 150 secondes, le paquet est ignoré.

SNMPv3 n'utilise pas l'heure normale. On utilise plutôt une horloge différente dans chaque agent. Ceux-ci gardent en mémoire le nombre de secondes écoulées depuis que l'agent a été mis en circuit. Ils gardent également un compteur pour connaître le nombre de fois où l'équipement a été mis en fonctionnement. On appelle ces compteurs BOOTS (Nombre de fois ou l'équipement a été allumé) et TIME (Nombre de secondes depuis la dernière fois que l'équipement a été mis en fonctionnement).

La combinaison du BOOTS et du TIME donne une valeur qui augmente toujours, et qui peut être utilisée pour l'estampillage. Comme chaque agent a sa propre valeur du BOOTS/TIME, la plate-forme de gestion doit garder une horloge qui doit être synchronisée pour chaque agent qu'elle contacte. Au moment du contact initial, la plateforme obtient la valeur du BOOTS/TIME de l'agent et synchronise une horloge distincte.

- ***VACM (View- based Access Control Model)***

Permet le contrôle d'accès au MIB. Ainsi on a la possibilité de restreindre l'accès en lecture et/ou écriture pour un groupe ou par utilisateur.

Le format de la trame SNMPv3 est très différent du format de SNMPv1. Ils sont toutefois codés tous deux dans le format ASN.1 [ISO 87]. Ceci assure la compatibilité des types de données entres les ordinateurs d'architectures différentes.

Pour rendre plus facile la distinction entre les versions, le numéro de la version SNMP est placé tout au début du paquet. Toutefois, le contenu de chaque champ varie selon la situation. Selon que l'on envoie une requête, une réponse, ou un message d'erreur, les informations placées dans le paquet respectent des règles bien définies dans le standard.

Voici comment les champs d'un paquet SNMPv3 sont remplis :

Version SNMP
Pour SNMPv3, on place la valeur 3 dans ce champ. On place 0 pour un paquet SNMPv1.

Identificateur de message
Ce champ est laissé à la discrétion du moteur SNMP. On retrouve souvent des algorithmes, où le premier message de requête est envoyé avec un nombre aléatoire et les suivants avec les incréments de 1. Les paquets qui sont émis en réponse à une requête portent la même identification que le paquet de la requête.

Taille maximale
Le moteur choisit la taille maximale d'une réponse à une requête selon ses capacités en mémoire tampon et ses limites à décoder de longs paquets. Quand on envoie une réponse à une requête, on doit veiller à ne pas dépasser la taille maximale.

Drapeaux
Trois bits sont utilisés pour indiquer :
- Si une réponse est attendue à la réception de ce paquet. (Reportable Flag)
- Si un modèle de chiffrement a été utilisé (Privacy Flag)
- Si un modèle d'authentification a été utilisé (Authentification Flag)

Le modèle de sécurité
Ce module identifie le type de sécurité qui est utilisé pour chiffrer le reste du paquet. Cet identificateur doit identifier de façon unique chaque module de sécurité. Actuellement, l'algorithme de chiffrement DES (Data Encryption Standard) et l'algorithme d'authentification HMAC-MD5-96 ont été choisis comme algorithmes utilisés dans SNMPv3. HMAC-SHA-96 est optionnel.

Les informations de sécurité
Ces informations ne sont pas décrites dans le standard SNMPv3, ce bloc est laissé au soin des

modules de sécurité. D'un module de sécurité à un autre, ces informations seront différentes. Le module de sécurité DES a standardisé le contenu de ce bloc.

Les identificateurs de contextes

Avec SNMPv1, il était possible d'avoir une seule base d'informations (MIB) par agent. Ceci n'est pas suffisant pour certains équipements qui peuvent contenir plusieurs fois les mêmes variables. Par exemple, un commutateur ATM contient plusieurs cartes qui ont chacune leurs propres bases d'informations. Le contexte permet de distinguer entre plusieurs bases d'informations et même plusieurs agents. On distingue entre des agents, par exemple, quand on a un moteur qui agit comme passerelle entre SNMPv3 et du SNMPv1. On envoie donc un paquet SNMPv3 en identifiant à quel agent SNMPv1 on désire que le paquet soit retransmis.

3. Etude des solutions logicielles de supervision

L'étude des solutions va suivre un certain cheminement logique .Tout d'abord nous allons définir les critères de sélection pour s'assurer que le produit remplit bien des fonctions attendues importantes pour mener à bien ce projet .

Ensuite nous allons définir une liste de solution les plus utilisées par la communauté et qui ont fait leurs preuves.

Puis, à partir des critères préalablement définis, nous utiliserons un tableau des icônes colorées allant du rouge au vert.

Enfin, nous choisirons à l'aide du tableau la solution qui sera retenue pour le déploiement du système.

Critères de Sélection

Pour permettre de mieux calibrer la solution, les logiciels retenus seront jugés selon les critères suivants

- Langue
- Ajout de Plugins
- Plateforme d'installation
- Simplicité d'installation et d'utilisation
- Modularité du produit
- Génération de rapport
- Sauvegarde du produit
- Finesse et Pertinence des alertes

a. FAN

FAN pour Fully Automated Nagios est une distribution qui permet d'installer Nagios très rapidement avec les outils utilisés couramment pour Nagios.
Les avantages sont que l'installation est rapide et simple, il y a peu de configuration pour commencer et cette dernière est simple.
C'est une distribution parfaite pour ceux qui débute avec Nagios, mais elle présente aussi des inconvénients tels que la vieillesse des applications par rapports aux versions d'aujourd'hui, l'emplacement des fichiers de configurations est différent et peut donc compliquer la vie lors de la recherche de solution sur des problèmes de configuration.
Le plus gros inconvénient et pas des moindres est que la version de Nagios est « patchée », sans une nouvelle version de FAN, il est impossible d'upgrader Nagios.
De plus le fait que tout soit préconfiguré ne nous permet pas de bien connaitre le fonctionnement de notre serveur.

b. Nagios

Nagios est un programme libre sous licence GPL qui fonctionne sur linux et qui permet de surveiller le système et le réseau.

Il peut surveiller des hôtes, des services et des actifs réseaux.

Son rôle est d'alerter quand un élément supervisé a un problème.

C'est un programme modulaire qui se décompose en trois parties :

- Le moteur de l'application qui vient ordonnancer les tâches de supervision.
- L'interface web, qui permet d'avoir une vue d'ensemble du système d'information et des possibles anomalies.
- Les plugins, mini programmes que l'on peut compléter en fonction des besoins pour superviser chaque service ou ressource disponible sur l'ensemble des ordinateurs ou éléments réseaux du SI.

c. Shinken

Shinken est une version modifiée de Nagios par le célèbre (dans la communauté de la supervision) Jean GABES.
En effet il a réécrit totalement Nagios et a rajouté d'autres fonctionnalités, mais suite au refus des développeurs de Nagios d'en faire la branche principale du futur développement, le projet Shinken est devenu indépendant.
C'est un outil très puissant et qui évolue très rapidement (en date de la rédaction de ce document).

d. Spiceworks

Il propose un outil destiné à simplifier le travail des administrateurs réseaux. L'application combine inventaire réseau, help desk, cartographie et surveillance. Spiceworks peut également vous mettre en relation avec des professionnels de l'Informatique pour échanger des idées, résoudre des problèmes et décider de quelle nouvelle fonctionnalité vous pourriez avoir besoin.
Enfin, le logiciel revêt une interface utilisateur avec une ergonomie à toute épreuve.
L'avantage principal est la simplicité et la rapidité d'installation mais aussi la possibilité d'intégrer l'application dans un Smartphone.
L'inconvénient majeur est le fait que la solution soit uniquement disponible pour Windows et que nous ne sommes pas maitre des échanges entre le logiciel et la société qui le développe.

e. EyesOfNetwork

EyesOfNetwork (« EON ») est la solution Open Source réunissant de manière pragmatique les processus ITIL et l'interface technologique permettant leur application. EyesOfNetwork Supervision est la première brique d'une gamme de produits bâtie autour de la gestion des évènements, de la disponibilité, des problèmes et de la capacité.
La version 4 renforce ce positionnement en offrant :
Une interface graphique de définition des processus métiers
Des profils de rapports PDF (supervision + graphiques de performances)
Un nouveau design de l'interface web
La génération automatique des graphiques à partir des données de performance de Nagios (Pnp4nagios)
Un calcul du temps de prise en compte des événements
La génération de pop-ups à l'arrivée d'événements (RSS Feed)
La simplification de la création des équipements et des services
Des nouveaux plugins : Oracle, Network…

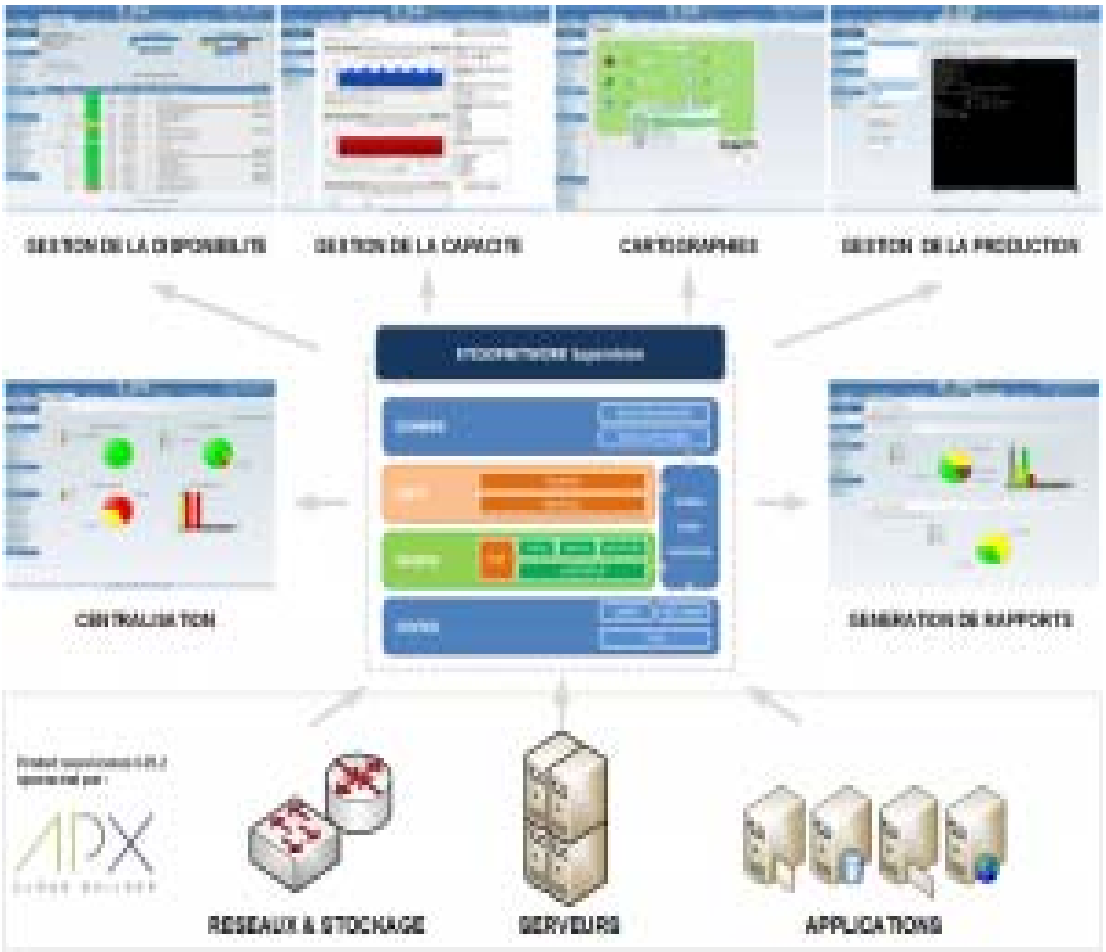


Figure 7:Bundle EyesOfNetwork

Le « bundle » EyesOfNetwork est composé d'un système d'exploitation minimaliste incluant un ensemble intégré d'applications répondant aux différents besoins de supervision :
GED (Generic Event Dispatcher) : gestion multi sites et sécurisée des évènements,
NAGIOS : gestion des incidents et des problèmes,
THRUK : interface de supervision multibackend,
NAGVIS : cartographie personnalisée de la disponibilité,
NAGIOSBP : gestion de la criticité des applications,
CACTI et PNP4NAGIOS : gestion des performances,
WEATHERMAP : cartographie de la bande passante,
BACKUP MANAGER : Outil de sauvegarde de la solution,
EONWEB : Interface Web unifiée de la solution,
EZGRAPH : Librairie d'affichage des graphiques,
SNMPTT : Traduction des traps snmp,
GLPI / OCS / FUSION : Gestion de parc et inventaire.

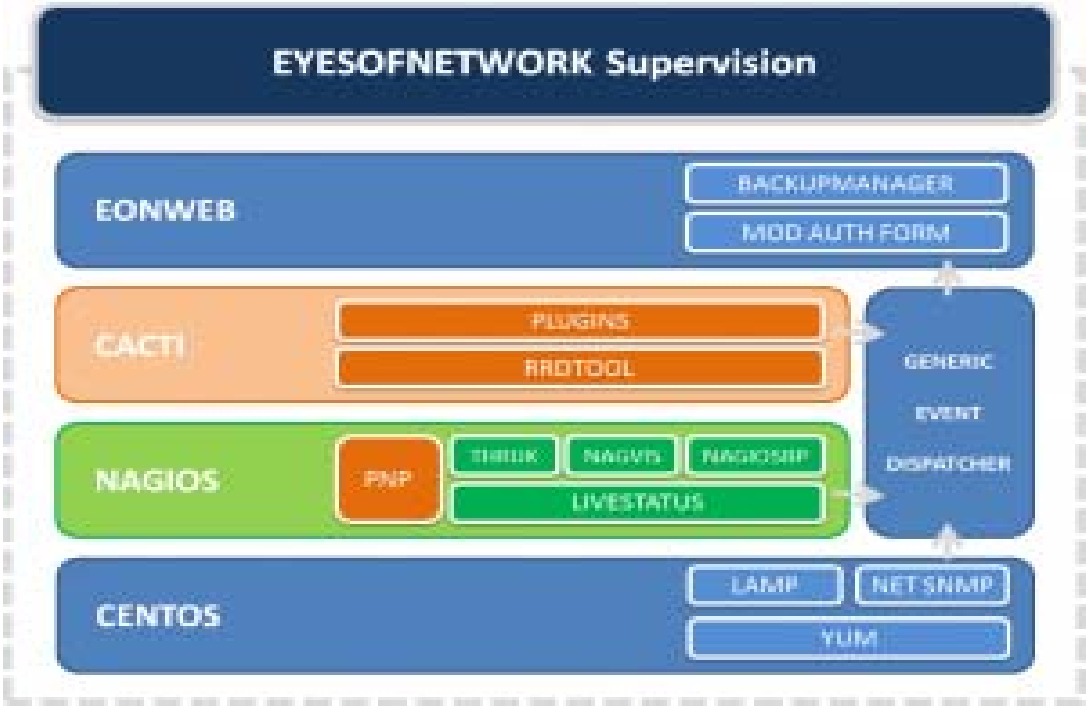


Figure 8:Archtecture EyesOfNetwork

EyesOfNetwork est accessible via une interface Web unique dont l'objectif est de réunir les différents acteurs d'un système d'informations (DSI, Administrateurs, Techniciens, Opérateurs, …). Chacun de ces acteurs dispose d'une vue correspondant à son métier. Toutes les informations sont consolidées en Base de Données MYSQL ou BERKELEY.
EyesOfNetwork est un produit sous licence GPL2 sponsorisé et proposé par APX Cloud Builder dans le cadre de prestations de services (Intégration, Télé-service, Support téléphonique et Tierce Maintenance Applicative).

f. Solution retenue

Les produits seront jugés et classés en fonction des critères de sélection.
Le choix s'est arrêté sur la solution EyesOfNetwork car elle est mieux adaptée à notre demande.

Légende :



Tableau 1:Tableau comparatif des logiciels de supervision

OUTILS	FAN	NAGIOS	SHINKEN	SPICEWORK	Eyes Of NetWORK
Plateforme d'Installation	★	★	★	★	★
Facilité d'Installation	☆	☆	★	★	☆
Modularité du produit	☆	★	★	★	☆
Sauvegarde	★	★	★	★	★
Ajout de Plugins	☆	★	★	★	★
Génération de rapports	☆	☆	☆	★	★
Finesse	☆	☆	☆	☆	★
Langue	★	★	★	★	★

7) Mise en place de la Solution

a) Installation du protocole Snmp

1. Installation et paramétrage SNMP sous Linux

Pour installer un manager SNMP, nous pouvons utiliser Net-SNMP. L'application Net-SNMP est un ensemble de programmes console permettant de tout faire avec le protocole SNMP. L'avantage d'utiliser des programmes console est que vous pouvez facilement écrire des petits scripts de vérification que vous pourrez intégrer dans Nagios

Nous allons donc installer les paquets SNMP : Snmp et snmpd

Sous un système Debian: ouvrir une console et taper la commande :

```
sudo apt-get install snmp snmpd
```

Ensuite nous allons éditer le fichier snmpd.conf avec la commande :

```
Sudo nano /etc/snmp/snmpd.conf
```

Et rentrer les paramètres suivant :

```
#com2sec paranoid  default        public
#com2sec readonly  default        public
com2sec readwrite default        cbao
```

Ici on autorise en lecture et écriture la communauté EyesOfNetwork

Valider les changements (ctrl+x, o, entrer).

Nous allons aussi éditer le fichier /etc/default/snmpd

```
Sudo nano /etc/default/snmpd
```

Chercher la ligne, et remplacez 127.0.0.1 par l'adresse IP de l'interface réseau utilisée pour communiquer avec le serveur de supervision (généralement l'IP de notre machine).

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1'
```

Redémarrer le serveur

```
sudo /etc/init.d/snmpd restart
```

Pour tester SNMP sur le serveur linux, on rentre la commande :

```
snmpwalk -v 2c –c cbao localhost
```

Pour tester que cela fonctionne du serveur de supervision, on rentre la commande :

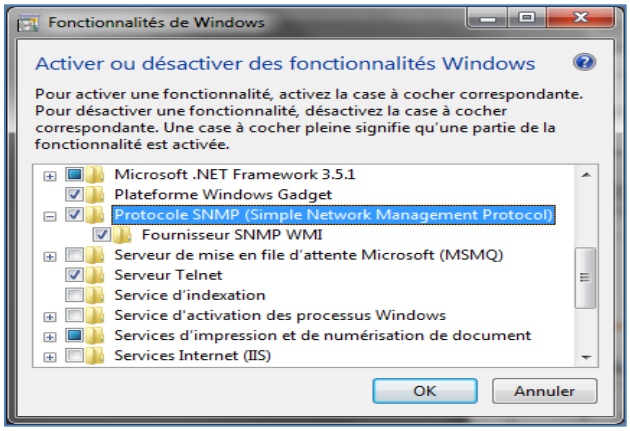
```
snmpwalk -v 2c -c cbao localhost ip-serveur-supervisé
```

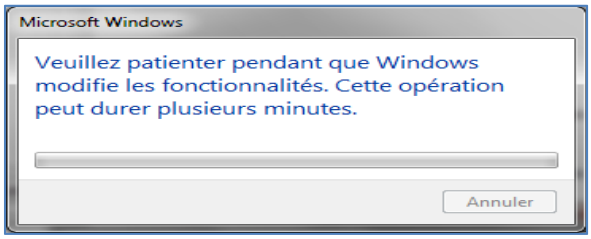
2. *Installation et paramétrage SNMP sous Windows*

a. Windows 7

Aller dans le **panneau de configuration>programmes>Activer ou désactiver des fonctionnalités Windows**

Cocher ensuite la case correspondant au Protocole SNMP, puis cliquer sur ok.



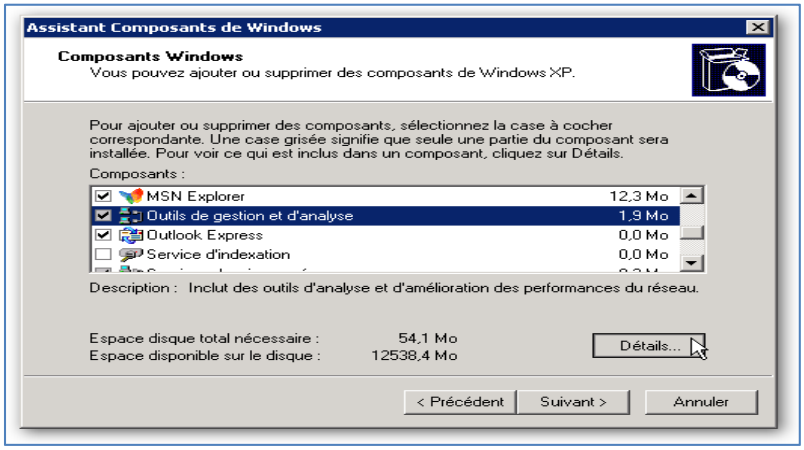


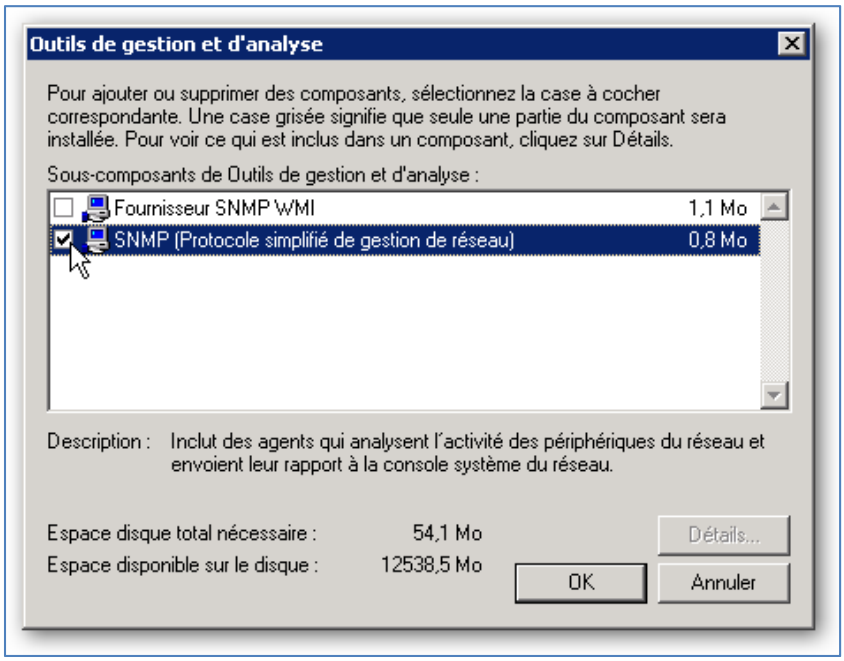
b. Windows XP et Windows server

Aller dans

Panneau de configuration>ajout/suppression de programmes>Ajouter/Supprimer des composants Windows

L'Assistant Composants de Windows s'ouvre alors. Cliquer sur Outils de gestion et d'analyse, puis cliquer sur le bouton Détails. Sélectionner ensuite le fournisseur SNMP WMI et le protocole SNMP.



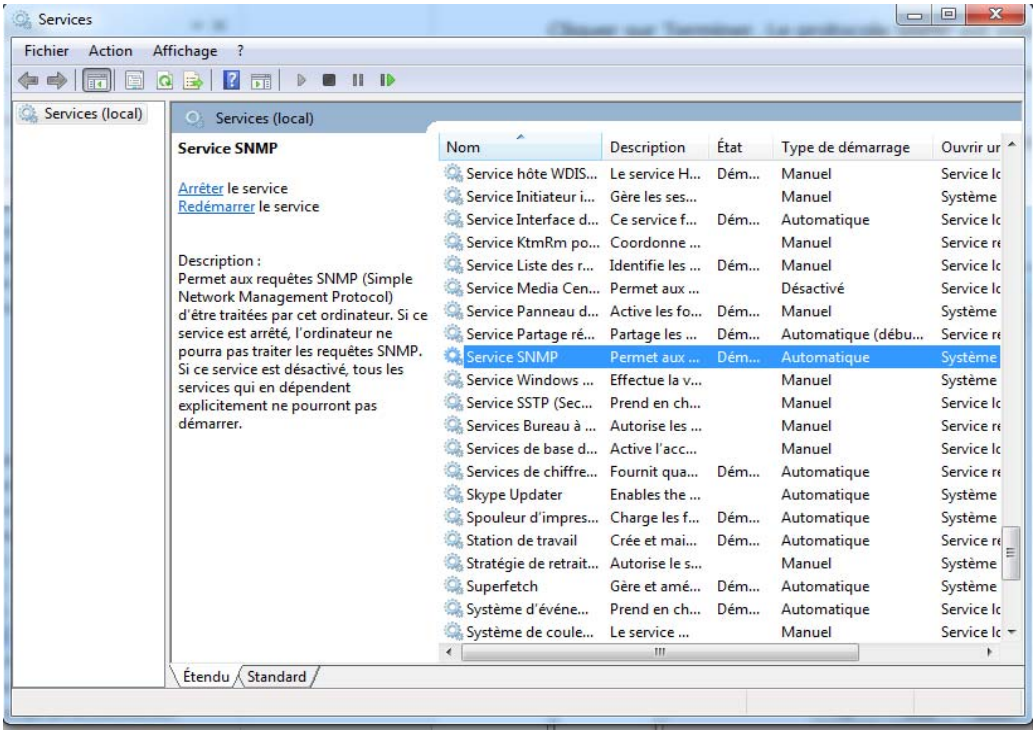


Cliquer sur OK puis Suivant : Windows enregistre les nouveaux composants (le CD-Rom d'installation vous sera éventuellement demandé).

Cliquer sur Terminer. Le protocole SNMP est maintenant installé.

Ensuite le paramétrage reste le même sur toutes les plateformes Windows comme décrit ci-dessous.

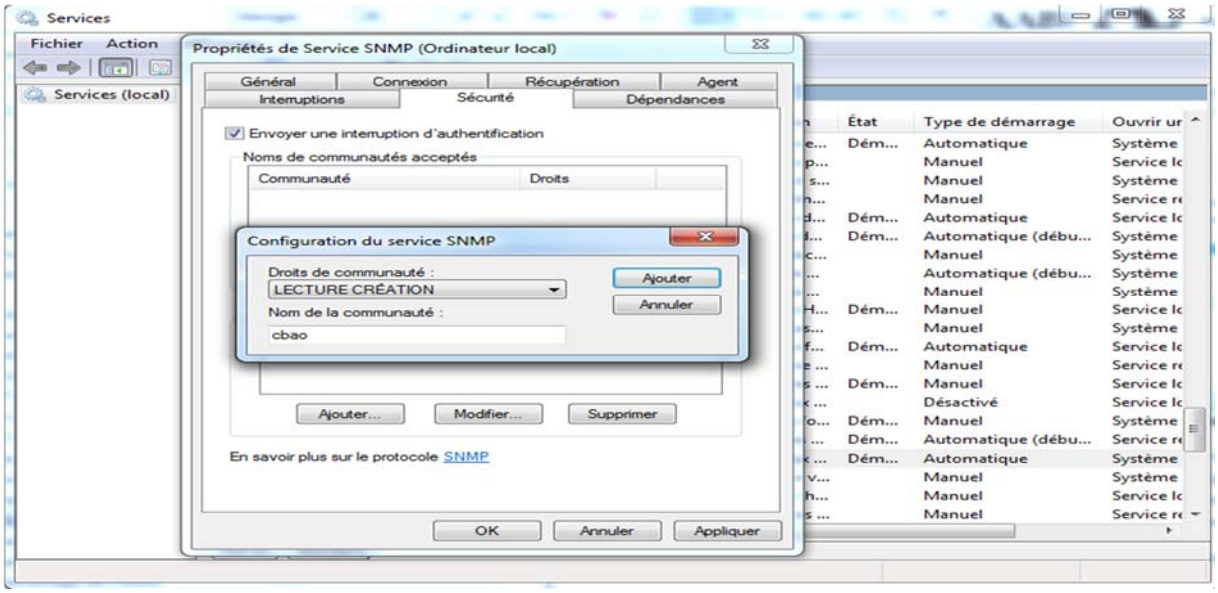
Dans Windows, ouvrir le panneau des services en lançant la commande services.msc



Cette fenêtre ouverte, chercher le service SNMP et faire un clic droit/propriété pour accéder à la configuration.

Aller dans l'onglet sécurité, ici l'on va renseigner la communauté que possède notre serveur de supervision et lui accorder les droits en lecture et écriture.

Nous allons aussi renseigner l'IP de notre serveur de supervision, ou autoriser toutes les adresses ce qui est notre cas du fait qu'on travaille dans des environnements différents.



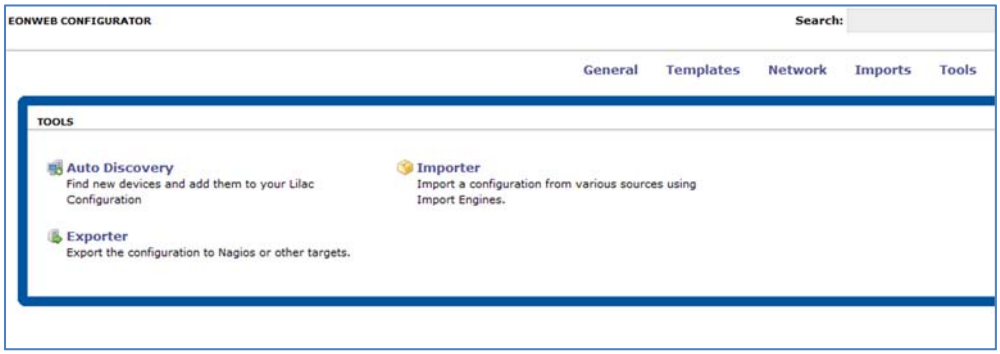
b) Configuration EON

1. SUPERVISER SERVEUR

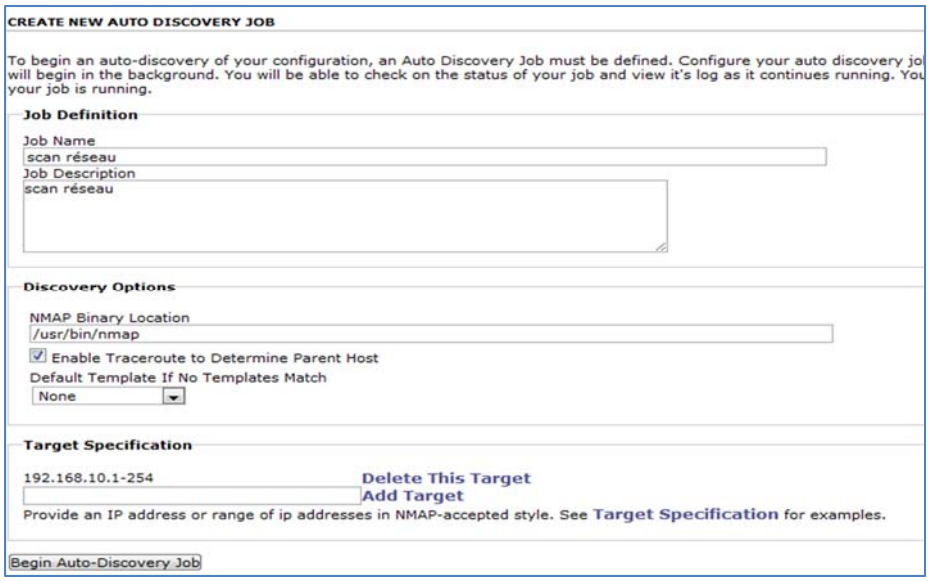
Pour pouvoir scanner le réseau, il faut se connecter sur l'interface web d'EON.

Lilac va nous permettre de découvrir automatiquement le réseau car il s'appuie sur le logiciel Nmap qui est un scanner de port.

Dans Lilac, cliquez sur « Tools » puis « Auto Discovery ».



Ensuite dans la fenêtre suivante nous allons remplir les champs suivant :



Job Name :nom du travail

Job description : description du travail

Nmap binary location :emplacement de l'executable Nmap(laisser par défaut)

Target Specification : adresse que l'on souhaite superviser,

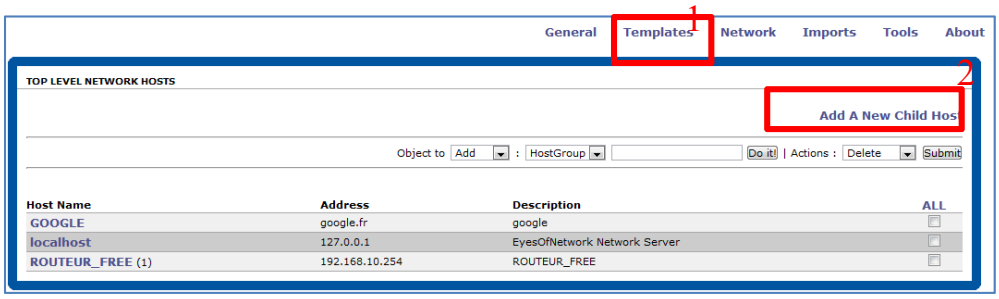
Exemple :192.168.10.x/2 ou 192.168.10.x-x

Cliquez ensuite sur « add target » puis sur « Begin auto-discovery job »

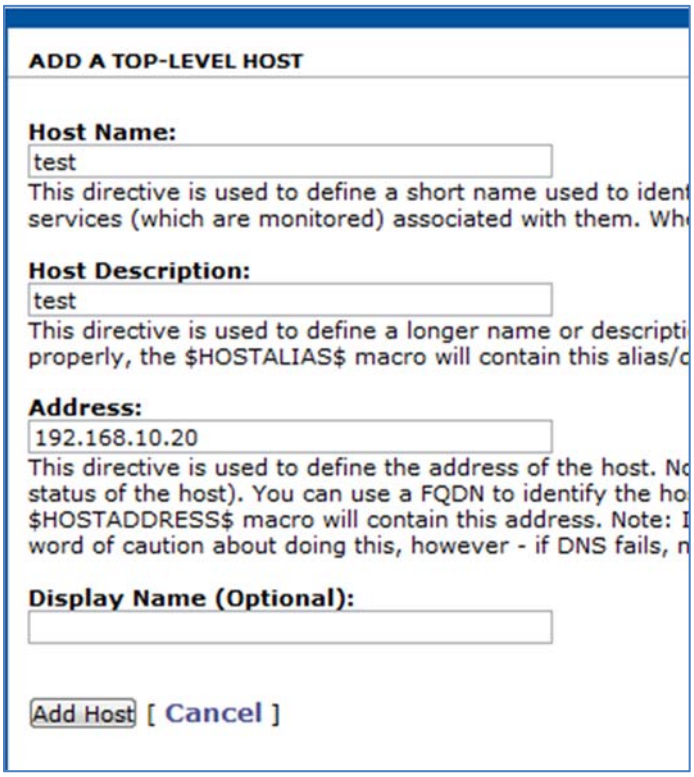
Le processus démarre ,il faut maintenant attendre la fin du processus pour pouvoir exporter les hotes dans Nagios.

2. *Superviser un hote*

Dans Lilac, cliquez sur « Network » puis « add a new child host »



Remplissez ensuite les champs suivants :



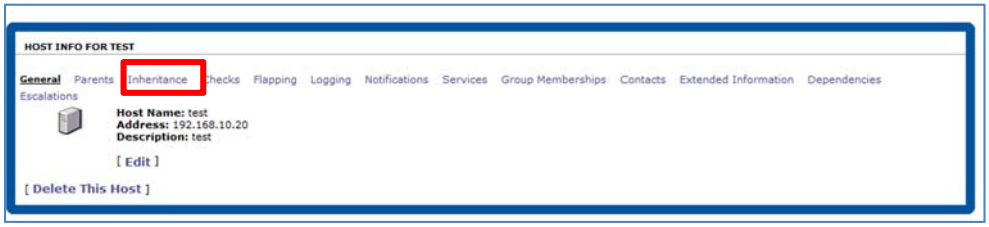
Host Name :Nom de l'hote (ne doit pas contenir d'espace)

Host Description : Description de l'hote

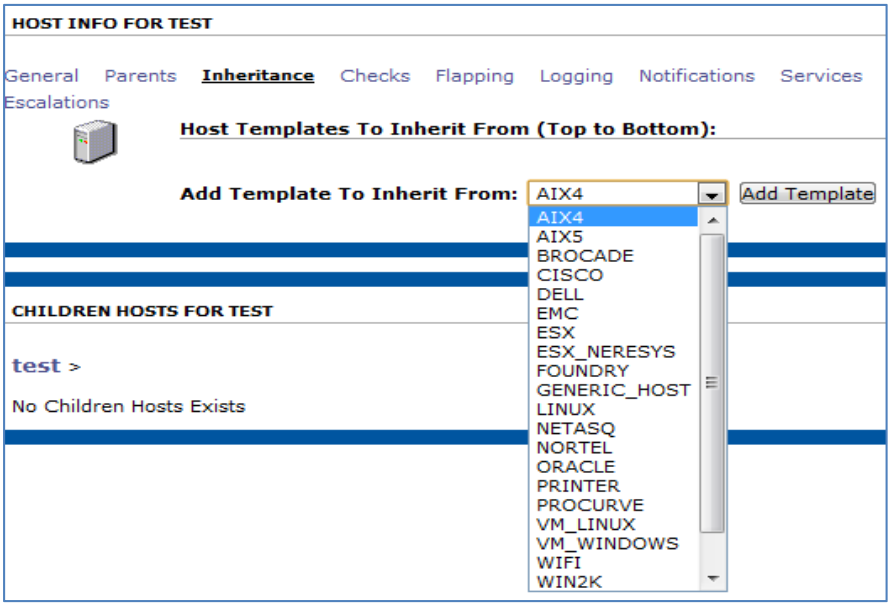
Address : adresse ip,nom d'hote ou adresse internet

Cliquez sur « Add host » pour l'ajouter dans Lilac

La fenétre suivante apparait :



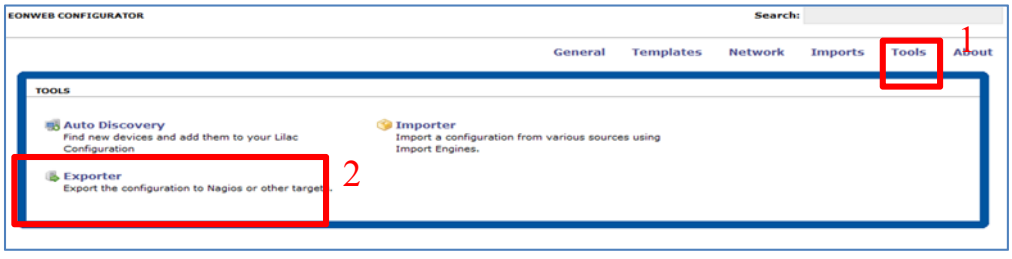
Dans cette fenétre,cliquez sur « Inheritance » pour choisir un template à associer à l'hote : exemple Windows, linux.



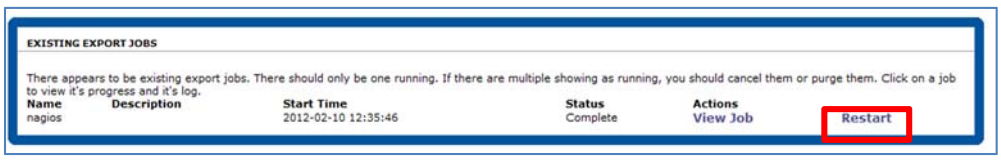
Une fois le Template sélectionné,cliquez sur « Add Template »

Nagios recherchera alors les checks qui sont personnalisés pour le template en question.

Dans Lilac,cliquez ensuite sur « Tools » puis sur « Exporter »



Et enfin sur « Restart » pour pouvoir charger la configuration de Lilac dans Nagios

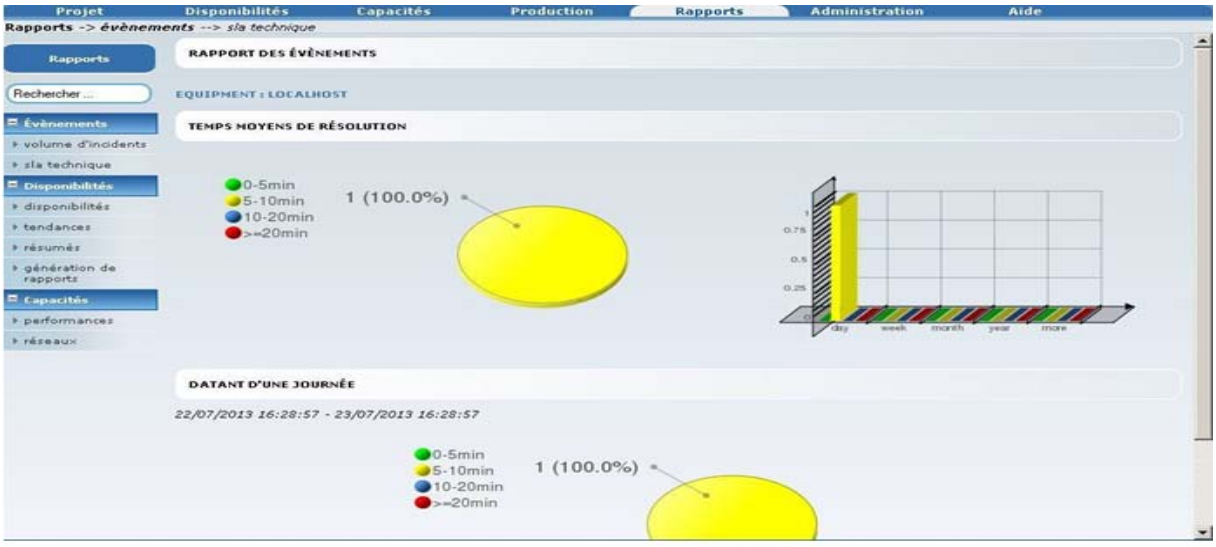


3. Génération de rapports statistiques



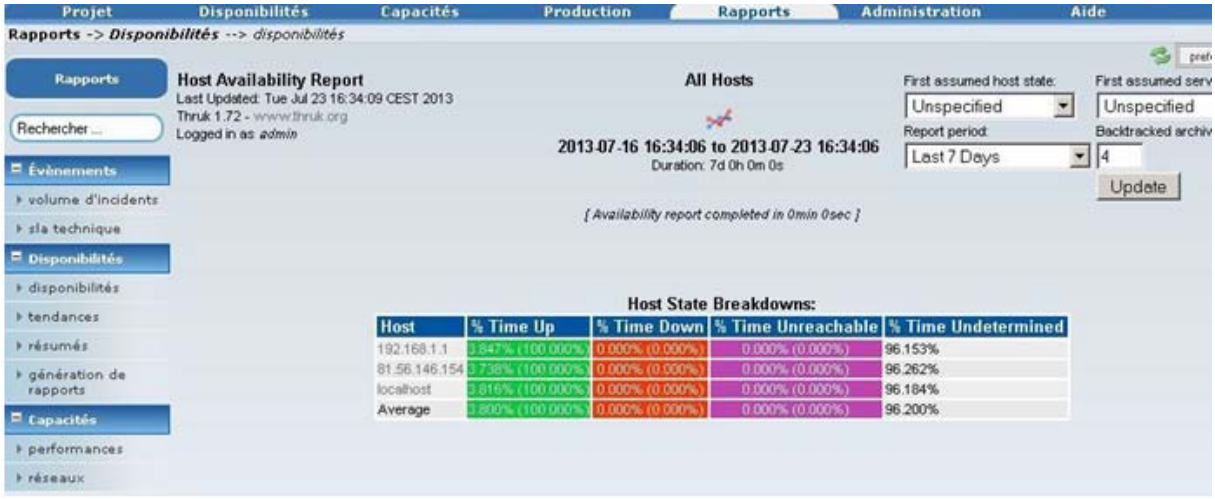
Permet de synthétiser le nombre de « panne » rencontrées sur une période donnée (hôte ou service en panne). Dans cet exemple c'est la vue « équipement » / « localhost » / « datant d'une journée » qui a été choisie.

Efficacité de la gestion des Incidents



Permet de synthétiser le temps moyen de résolution de panne pour une période donnée.

Disponibilité



Permet d'avoir la disponibilité hôte/service ou groupe d'hôtes/services sur une période donnée.

4. Stratégie d'alerte

Lorsque le deploiement des elements supervisés est en statut de bon fonctionnement , Nagios n'enverra pas d'alerte.
Nagios sera paramétré par contre en respectant trois catégories :
D'abord , les alertes devront étre limitées et claires.
Ensuite, nous mettrons en place une procédure d'escalade , pour pallier au manque de temps, de competence ou d'une absence d'un collaborateur.
Enfin ,lorsqu'un element comme un commutateur réseau ne fonctionne plus,uniquement une alerte le concernant devra etre renvoyée.Les elements qui sont connectés sur le commutateur ne devront pas générer d'alerte.



c. Alerter de façon intelligente

i. Diminuer le nombre de notifications

L'un des principaux problèmes posés par le monitoring est l'avalanche d'alertes que celui-ci peut générer. Hors une alerte importante, si elle est noyée dans une grande masse d'alerte sera ignorée :

- soit parce que les utilisateurs auront pris l'habitude de ne pas lire les mails d'alerte, voire de les archiver automatiquement en dehors de leur INBOX ;
- Soit parce que parmi 200 alertes ils ne pourront pas repérer l'alerte important, celle qui est prioritaire.

Quand nous avons étudié la topologie, nous avons vu que la relation parent, permettant de détecter les network outages était déjà pensée dans le but de réduire le nombre d'alertes et de générer un alerte unique et ciblée sur l'équipement réseau fautif.

D'autres éléments vont pouvoir entrer en jeu dans le paramétrage du système de notification afin de réduire les alertes.

Il est possible de suspendre les alertes au niveau global. Il n'y a alors plus aucune alerte générée. A un niveau inférieur, on va pouvoir pour chaque hôte et chaque service décider s'il peut générer des alertes et, le cas échéant quels types d'alertes il génère.

On peut par exemple dire qu'un service donné ne génère des alertes que pour CRITICAL et RECOVERY, jamais pour UNKNOWN et WARNING. Mais on aura tout intérêt à définir ces paramètres non pas au niveau d'un service ou d'un hôte en particulier mais plutôt dans un modèle d'hôte ou de service afin que toute la famille profite des mêmes paramétrages.

S'il est très important d'alerter sur les services critiques, il existe certainement certains services non critiques qui ne nécessitent pas de génération d'alertes (comme le manque de papier d'impression des reçus), il va falloir donc suspendre les alertes pour cette famille de services.

De même, il peut être nécessaire de changer la planification des vérifications sur ces services, une vérification horaire ou quotidienne ne serait-elle pas plus adaptée qu'une vérification toutes les 5 minutes ? Pour nous simplifier la vie, nous allons utiliser les modèles et définir ces paramètres importants dans les modèles.

Après l'activation des alertes, il faut aussi définir, soit dans les modèles, soit dans des services ou hôtes, les utilisateurs ou groupes d'utilisateurs destinataires de ces alertes. On peut envoyer les alertes d'un même service à plusieurs destinataires (gestionnaire de Gabs, chef de service télésurveillance monétique). On préférera cependant toujours une gestion basée sur des groupes afin de gérer facilement le management des équipes.

ii. Répéter les alertes

Le graphique « Statut et type de statut: analyse des états de service » présenté plus haut montrait plusieurs flèches d'alertes suite au passage en HARD du statut CRITICAL d'un service. A chaque nouvelle alerte théorique, le sous-système de notification se déclenche et va décider de lancer ou non une alerte.

Un nouveau paramètre de configuration important de l'hôte ou du service entre alors en jeu:

« notification_interval ». Celui-ci permet d'indiquer un temps minimum entre deux notifications. Une valeur à 0 de ce paramètre signifie qu'on ne veut recevoir l'alerte que la première fois. C'est le choix le plus courant. On ne reçoit l'info du service en état critique qu'au moment où Nagios le détecte en HARD.

La prochaine alerte sur ce service sera pour un changement d'état (WARNING ou RECOVERY). Mais si nous indiquons 14 minutes alors il est possible qu'une fois le délai de 14 minutes dépassé Nagios décide de ré-envoyer l'alerte.

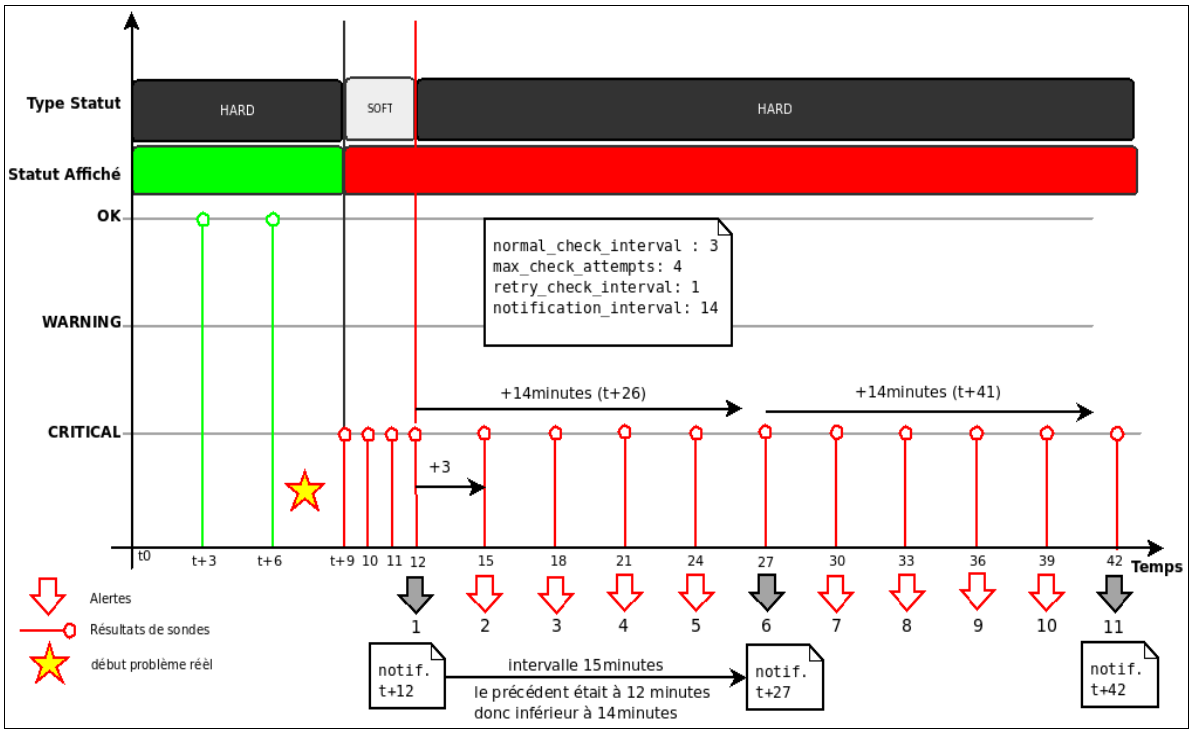


Figure 9:Exemple de frise chronologie/Alerte Nagios

L'examen de la frise ci-dessus montre qu'une fois le statut passé en HARD au temps t+12 une première alerte est émise. Toutes les 3 minutes (normal_check_interval), E O N (Nagios) va relancer sa sonde qui va lui renvoyer un état Critique.

Au bout de 15 minutes, Nagios vérifiera que l'intervalle de 14 minutes de silence est passé et renverra l'alerte. Un nouvel intervalle de silence est alors démarré.

> On remarquera qu'on obtient des notifications toutes les 15 minutes et non toutes les 14 minutes, choisir un intervalle de notification multiple du normal_check_interval peut simplifier la lisibilité (ici 15 minutes au lieu de 14 minutes).

Certaines versions récentes de Nagios3 supportent le paramètre first_notification_delay qui est u n délai supplémentaire associé à l'envoi de la première notification et qui pourrait alors intervenir dans cette frise en décalant l'envoi de la première notification.

iii. Dépendances, Arrêts programmés et Escalades

Toujours dans l'optique de diminuer les notifications, Nagios propose un **système de dépendances entre services** ce qui ne sera pas détailler dans ce document. Il suffira pour le moment de savoir que leur but est de cibler la notification à envoyer en indiquant à Nagios que certains services dépendent d'un autre, et que si tous sont en état critique il convient d'envoyer la notification d'erreur du service Maître plutôt que sur ses dépendants.

Nous pouvons aussi indiquer à Nagios des phases d'arrêt prévues (Scheduled Downtime). Si par exemple il est prévu que chaque jour à une heure précise des opérations sont faites sur les équipements et que ces dernières pourront affecter le bon fonctionnement des services alors nous allons créer une phase d'arrêt programmé pour tous ces services et la stocker dans Nagios.

Au moment où les services passeront en état critique Nagios, n'enverra pas de notifications tant que cette plage de temps ne sera pas dépassée.

Enfin Nagios propose une notion d'escalade. L'escalade consiste à prévenir des groupes d'utilisateurs différents au fur et à mesure de l'évolution d'un même incident.

Le cas d'utilisation le plus courant est la gestion d'équipes de support en premier puis en second niveau. On peut aussi imaginer prévenir un groupe de gestionnaires de Gabs puis prévenir le Responsable des Operations au bout d'une heure de panne, puis prévenir le chef d'agence au bout de deux heures, etc.

On peut associer un grand nombre d'escalades à un même service. Afin de bien les utiliser, il faut noter quelques particularités dans la façon de définir ces escalades :

- les escalades ne travaillent pas sur le nombre de remontées d'alerte mais sur le nombre d'alertes ayant généré réellement des notifications ;
- une escalade s'exprime ainsi : « A partir de la nième notification, jusqu'à la nième notification sur ce service merci de notifier les groupes de cette escalade » ;
- dès qu'au moins une escalade entre en jeu, les contacts classiques du service ou de l'hôte ne sont plus notifiés, si on veut qu'ils continuent à être notifiés il faut les intégrer dans les contacts de l'escalade ;
- Si une escalade utilise un notification_interval à 0 (une seule alerte) les escalades s'arrêteront après lui, car il n'y aura plus de notifications ;

- les escalades possèdent un intervalle de notification qui peut être différent de celui du service. L'intervalle de notification le plus court est choisi (parmi le service et les n escalades actives à un instant t).

Le schéma suivant peut nous permettre de comprendre ce qui se passe réellement en cas d'escalade:

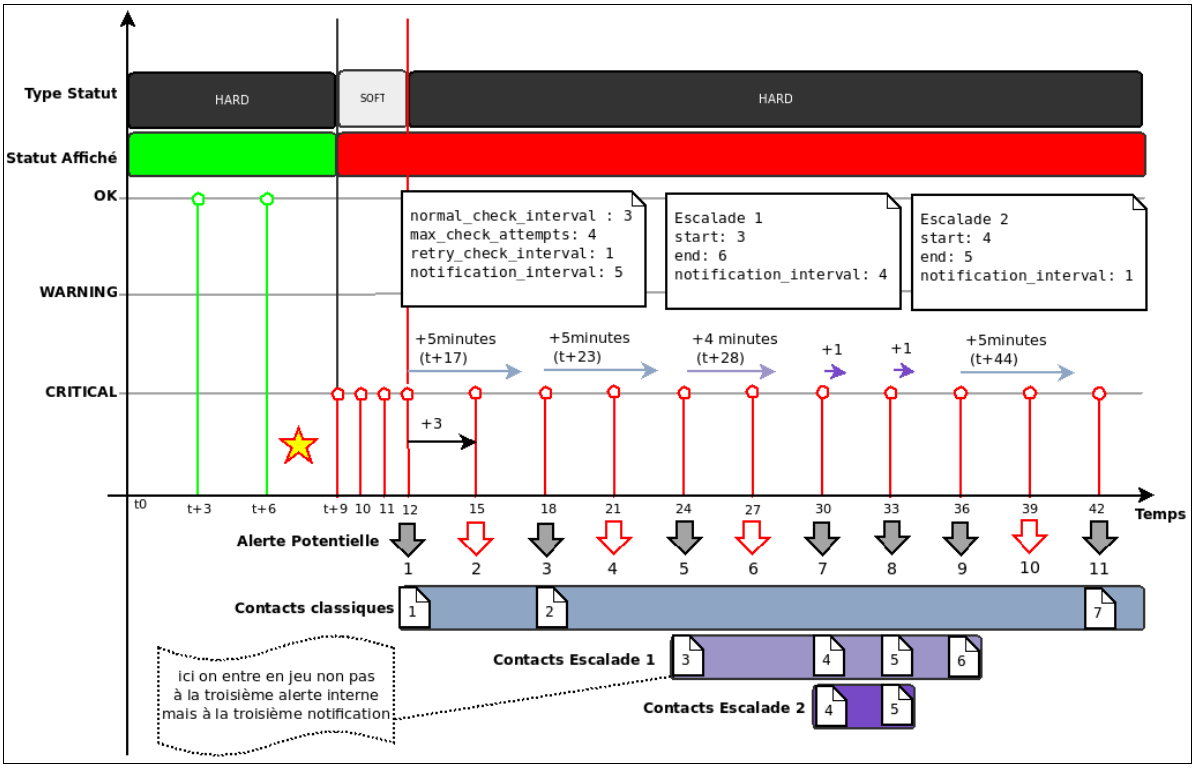


Figure 10:Exemple d'Escalade

Sur cette frise on observe que la deuxième escalade, possédant un intervalle de notification très court a provoqué l'émission d'alertes très rapprochées, y compris pour les contacts de la première escalade qui avaient été définis avec un intervalle de notification assez long. On voit aussi que si les notifications ne sont plus envoyées aux contacts classiques elles sont par contre envoyées à toutes les escalades actives.

Enfin on peut constater un comportement qu'on pourrait presque qualifier de bug. Lorsque la deuxième escalade s'arrête à la 5ème notification, l'intervalle de temps choisi avant la 6ème notification est calculé en prenant l'intervalle de temps le plus court parmi celui du service, de la première escalade, mais aussi de la deuxième escalade alors qu'elle n'est plus active. [4]

> Là encore choisir des intervalles de temps de notification notification_interval multiples du normal_check_interval permet d'améliorer la lisibilité des différentes escalades. Jouer sur les paramètres start et stop est aussi plus clair que jouer sur des intervalles de notifications différents entre les différents niveaux d'escalade.

iv. Intégrer la gestion des périodes de temps

Pour les services, les hôtes et les individus, Nagios permet d'indiquer des périodes de temps. Ces périodes vont définir des plages horaires et journalières dans lesquelles les notifications sont autorisées.

Il est alors possible de se servir de ce système pour :

- décider qu'un service n'est critique qu'à certaines plages horaires ;
- piloter des équipes travaillant à des horaires différents ;
- gérer les week-ends en n'envoyant l'alerte qu'à certains contacts dans cette plage de temps (par exemple, un contact possédant un téléphone d'équipe).

Dans la définition des plages temps, nous indiquons les plages de validité horaire pour chaque jour de la semaine (du lundi au dimanche). Il n'est pas possible de définir des choses comme « uniquement le premier lundi du mois ». On peut, par contre, indiquer plusieurs plages horaires par jour, ce qui permet de gérer les nuits en indiquant une plage horaire de minuit à 8:00, puis de 18:00 à 23:59.

Que se passe-t-il si un service à un notification_interval à 0 et que la première alerte se situe dans une plage de temps ou les notifications sont inactives ?

En théorie le notification_interval à zéro signifie que vous ne voulez recevoir qu'une seule alerte. Et c'est bien ce qui se passera, la première alerte que vous recevrez sera celle qui sera générée lorsque la sonde remontera un état d'alerte dans la plage de temps autorisée.

Toutes les remontées précédentes auront été ignorées en termes d'alerte.

notification_interval 0 ne signifie pas que seule la première alerte sera envoyée, cela signifie qu'une seule notification sera envoyée, cette première notification pouvant intervenir assez tard dans la vie de l'alerte. [4]

5. Medium de l'alerte

Une fois que Nagios a décidé de vous envoyer une alerte, il faut qu'il choisisse sous quelle forme cette alerte sera envoyée.

Ceci est défini par une commande externe, associée à une commande interne d'envoi d'alerte qui elle-même est associée à l'utilisateur.

Par exemple, la plupart des utilisateurs auront par défaut une commande associée d'envoi d'alerte par mail pour les problèmes de services appelée « notify-by-email » de messagerie instantanées (Postfix), ou pour envoyer des SMS.

a. Envoi de Mails

Vous avez noté qu'EON permet d'envoyer des notifications nagios via mail.

En effet un serveur Postfix est intégré dans ce but mais aucun agent de distribution de courrier aux clients n'est en place. Vous pouvez donc vous servir de ce postfix pour le configurer comme relay-smtp vers le domaine de messagerie principal de a CBAO.



Le fichier principal de configuration de postfix se trouve en /etc/postfix/main.cf

Exemple de quelques variables importantes du main.cf pour « pousser » les mails :

myhostname =nagios.localdomain (hostname fqdn de EON)

mydomain = localdomain (fqdn de EON moins le nom de l'hôte)

myorigin = $myhostname (indiquera de quel « serveur » viendra le futur mail)

relay_domains = cbao.lan

default_transport = smtp

relayhost = IP du serveur de messagerie de l'entreprise

A l'issue de chaque modification :

```
/etc/init.d/postfix restart
```

b. Notification SMS

L'envoi de SMS se gère de deux façons :

- soit vous utilisez une passerelle de type service web ou mail-to-sms. En prenant en compte le risque que la communication vers cette plate-forme externe soit indisponible au moment de l'alerte ;
- soit vous installez un téléphone GSM avec un accès GSM (carte SIM) à côté de votre serveur, et vous reliez les deux par un protocole de communication (série, USB, etc.).

Il est possible d'ajouter des macros personnalisées dans Nagios (variables/attributs personnalisés), pour les associer aux utilisateurs, aux services ou aux hôtes et y stocker ces informations supplémentaires

8) BILAN

Approche technique

La fiabilité du système proposé permettra d'avoir des données claires et concises sur les états de chaque équipement monétique .Ainsi des interventions rapides pourront être peaufinées pour parer à ces situations et assurer des services de qualités aux clients de la banque.

Approche Organisationnelle

La possibilité de donner l'accès aux chefs d'agences sur l'interface de gestion des équipements monétiques sous leurs responsabilités, amènera de la souplesse sur les procédures de gestion des incidents et à cet effet va améliorer les temps d'intervention.

De même, les rapports générés sur les disponibilités et les fréquences des pannes permettront une étude plus fine de l'activité des équipements afin de pourvoir mieux gérer le parc.

II. Problématique 2: Sécurisation et Augmentation de la Qos du service de transfert d'Argent

Western Union est un service de transfert d'argent international .Il est établi dans plusieurs pays du monde avec une quasi couverture mondiale. Pour les besoins d'expansion de son réseau et la démocratisation de l'accès à son service, il s'est lié en partenaire la CBAO Groupe AttijariWafa Bank, qui a la charge de lui dédié des points d'échange à travers le territoire national.

De ce fait, 69 points dédiés ont été implantés au niveau national, en plus des 98 agences déjà existantes qui viennent en appoint. Ces points dédiés sont situés dans des zones stratégiques où la mise en place d'une agence n'est pas toujours évidente .De même, le service unique rendu dans ces guichets participera sans doute à l'amélioration de l'efficacité du service afin de satisfaire davantage le client.

Ceci ne pourra être effectif qu'avec l'interconnexion de ces différents sites au réseau principal de la banque où se trouve le serveur .Ainsi, des liaisons VPN ont été établies entre ces points et l'agence de Point E qui constitue à cet effet le Hub central.

1) Présentation de l'Infrastructure

a) Introduction

Les applications et les systèmes distribués font de plus en plus partie intégrante du paysage d'un grand nombre d'entreprises. Ces technologies ont pu se développer grâce aux performances toujours plus importantes des réseaux locaux. Mais le succès de ces applications a fait aussi apparaître un de leur écueil. En effet si les applications distribuées deviennent le principal outil du système d'information de l'entreprise, comment assurer leur accès sécurisé au sein de structures parfois réparties sur de grandes distances géographiques ? Concrètement comment une succursale d'une entreprise peut-elle accéder aux données situées sur un serveur de la maison mère distant de plusieurs milliers de kilomètres ? Les Vpn ont commencé à être mis en place pour répondre à ce type de problématique.

La mise en place d'une infrastructure VPN a été encouragée par les nombreuses attaques subies par les machines des points dédiés dans les dernières années .Ainsi, deux solutions s'imposaient :

- La location des liaisons spécialisées auprès des opérateurs de télécommunications

Cette solution s'avère très onéreuse et les débits offerts ne répondent pas toujours aux besoins croissants en ressources.

- La mise en place d'un VPN

Cette solution s'annonce meilleure que la précédente car en plus d'apporter plus de sécurité, elle permet aussi d'avoir des performances acceptables pour un coût moindre .Ce qui est en grande partie, les raisons qui sous-tendent son implémentation.

a) Architecture

Ce réseau VPN est constitué de 3 parties :

- **L'infrastructure Client** est composée de 69 sites avec chacun à la disposition d'un routeur Cisco 500 compatible avec ATM et d'un Switch
- **L'infrastructure d'interconnexion** : Elle est constituée d'un routeur CISCO 500 avec une liaison LS et une liaison ADSL coté Client et un port Gigabit Ethernet, un firewall BlueCoat pour le filtrage des connexions entrantes
- **L'infrastructure Datacenter :** Elle est composée de serveurs d'applications, Proxy, routeurs avec des IP publiques et des Serveurs de fichiers.

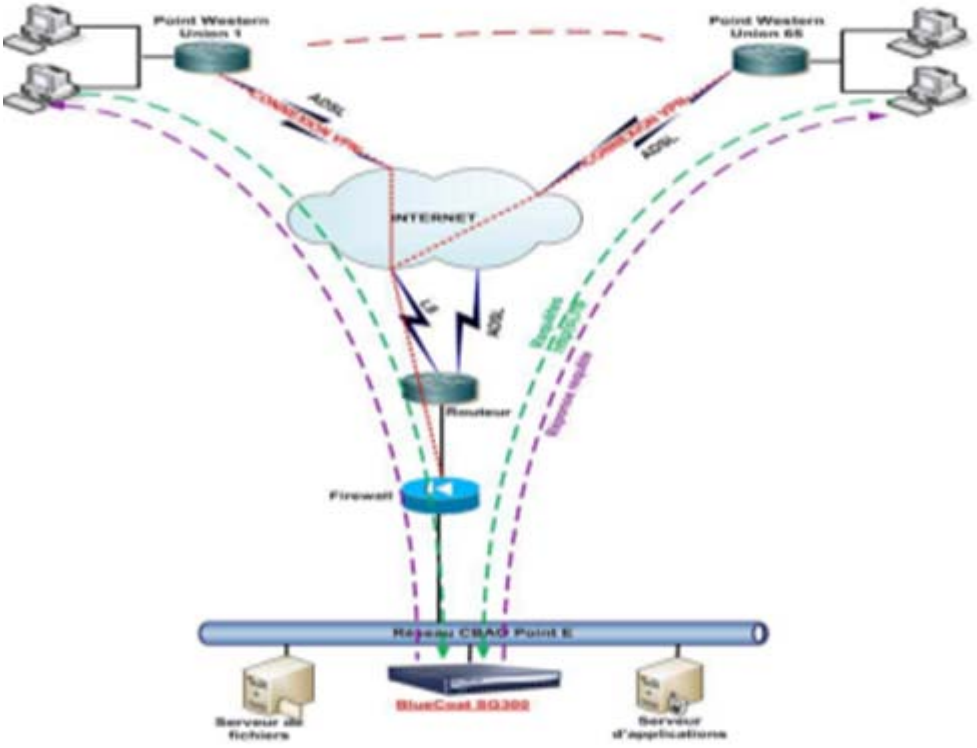


Figure 11:Architecture liaisons VPN

2) Les VPN

a) Principe de fonctionnement

1. Principe général

Un réseau Vpn repose sur un protocole appelé "protocole de tunneling". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

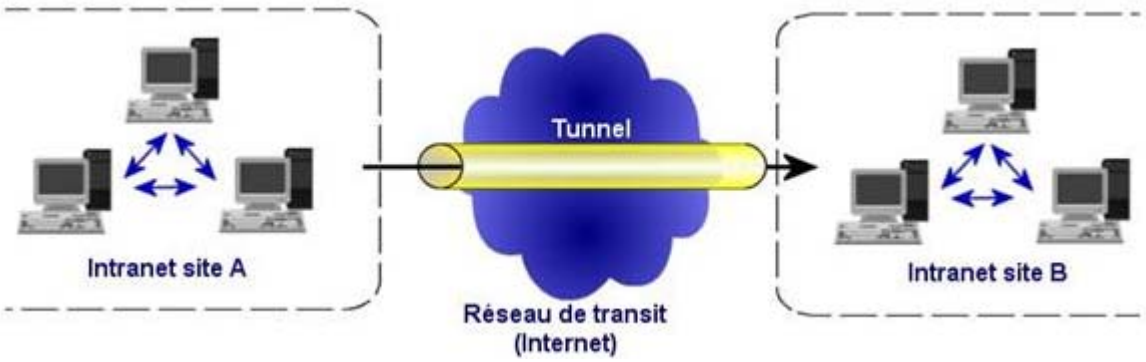
Les données à transmettre peuvent être prises en charge par un protocole différent d'IP.

Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés-encapsulation.

b) Fonctionnalités des Vpn

Il existe 3 types standards d'utilisation des Vpn qui sont le VPN d'accès, l'Intranet VPN et l'Extranet VPN. Mais dans ce document, seule la méthode Intranet VPN y sera traitée. En étudiant ce schéma d'utilisation, il est possible d'isoler les fonctionnalités indispensables des Vpn.

1. L'Intranet Vpn



L'intranet Vpn est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données.

Certaines données très sensibles peuvent être amenées à transiter sur le Vpn (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation.

La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie.

La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Le coût matériel des équipements de cryptage et décryptage ainsi que les limites légales interdisent l'utilisation d'un codage " infaillible ". Généralement pour la confidentialité, le codage en lui-même pourra être moyen une faiblesse, mais sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

c) - Bilan des caractéristiques fondamentales d'un Vpn

Un système de Vpn doit pouvoir mettre en œuvre les fonctionnalités suivantes :

Authentification d'utilisateur. Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.

Gestion d'adresses. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.

Cryptage des données. Lors de leurs transports sur le réseau public, les données doivent être protégées par un cryptage efficace.

Gestion de clés. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

Prise en charge multi protocole. La solution Vpn doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

Le Vpn est un principe : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs produits différents sur le marché dont certains sont devenus standard, et même considérés comme des normes.

d) Le protocole Ipsec

Ipsec, définit par la Rfc 2401, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau Ipv4 étant largement déployé et la migration vers Ipv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à Ipv4 et Ipv6. Ces mécanismes sont couramment désignés par le terme Ipsec pour IP Security Protocols. Ipsec est basé sur deux mécanismes. Le premier, AH, pour Authentification Header vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par ce "protocole" ne sont pas encodées.

Le second, Esp, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations.

Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement. Enfin, le protocole Ike permet de gérer les échanges ou les associations entre protocoles de sécurité. Avant de décrire ces différents protocoles, nous allons exposer les différents éléments utilisés dans Ipsec.

Vue d'ensemble

Les mécanismes mentionnés ci-dessus font bien sûr appel à la cryptographie et utilisent donc un certain nombre de paramètres (algorithmes de chiffrement utilisés, clefs, mécanismes sélectionnés...) sur lesquels les tiers communicants doivent se mettre d'accord. Afin de gérer ces paramètres, Ipsec a recours à la notion d'association de sécurité (Security Association, SA).

Une association de sécurité Ipsec est une "connexion" simplexe qui fournit des services de sécurité au trafic qu'elle transporte. On peut aussi la considérer comme une structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée.

Une SA est unidirectionnelle ; en conséquence, protéger les deux sens d'une communication classique requiert deux associations, une dans chaque sens. Les services de sécurité sont fournis par l'utilisation soit de AH soit de Esp. Si AH et Esp sont tous deux appliqués au trafic en question, deux SA (voire plus) sont créées ; on parle alors de paquet (bundle) de SA.

Chaque association est identifiée de manière unique à l'aide d'un triplé composé de:

L'adresse de destination des paquets,

L'identifiant du protocole de sécurité utilisé (AH ou Esp),
Un index des paramètres de sécurité (Security Parameter Index, SPI). Un SPI est un bloc de 32 bits inscrit en clair dans l'en-tête de chaque paquet échangé ; il est choisi par le récepteur.

Pour gérer les associations de sécurités actives, on utilise une "base de données des associations de sécurité" (Security Association Database, SAD). Elle contient tous les paramètres relatifs à chaque SA et sera consultée pour savoir comment traiter chaque paquet reçu ou à émettre.

Les protections offertes par Ipsec sont basées sur des choix définis dans une "base de données de politique de sécurité" (Security Policy Database, SPD). Cette base de données est établie et maintenue par un utilisateur, un administrateur système ou une application mise en place par ceux-ci. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer ou rejeté.

2. *Principe de fonctionnement*

Le schéma ci-dessous représente tous les éléments présentés ci-dessus (en bleu), leurs positions et leurs interactions.

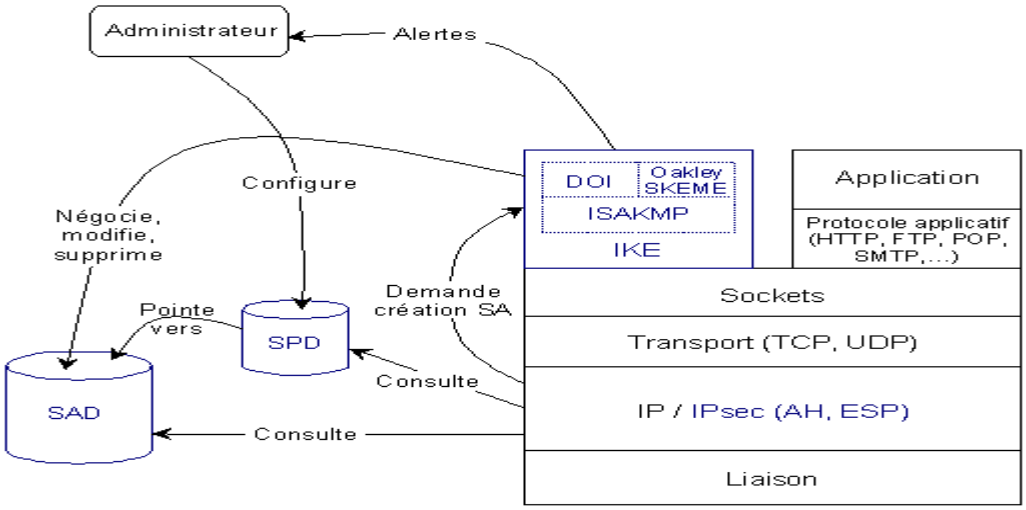


Figure 12:Schéma synoptique du fonctionnement des VPN

On distingue deux situations :

Trafic sortant

Lorsque la "couche" Ipsec reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD). Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, Ipsec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.

Trafic entrant
Lorsque la couche Ipsec reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si ce paquet s'est vu appliquer un ou plusieurs services Ipsec et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la Spd est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité.

Dans le cas où le paquet reçu est un paquet IP classique, la Spd permet de savoir s'il a néanmoins le droit de passer. Par exemple, les paquets IKE sont une exception. Ils sont traités par Ike, qui peut envoyer des alertes administratives. [3]

3) Configuration des liaisons VPN

a) Politique de Sécurité

Les tunnels IPSEC établis entre les routeurs des Points dédiés et celui de Point E utilise la politique de sécurité suivante :

encryption 3DES

Hash md5 : pour l'authentification

Authentification pre-share : authentification à clé partagée

Group 2

Les trafics de l'ACL 101 sont matchés sur le tunnel IPSEC vers_POINT_E :

```
crypto map vers_POINT_E 10 ipsec-isakmp
set peer 213.154.79.xxx
set transform-set vpncbao
match address 101
```

De ce fait, tous les paquets respectant les conditions de l'ACL 101 seront obligés de transiter par le tunnel IPSEC.

b) Explication détaillée

```
service password-encryption
!
hostname RTR_WU_Kao_Bo
enable secret passer1360
username admin password passer1360
//Définition des Access List pour les politiques de filtrages des connexions
access-list 101 permit ip 192.168.228.108 0.0.0.7 172.20.7.0 0.0.0.255
access-list 101 permit ip 192.168.228.108 0.0.0.7 172.20.0.0 0.0.15.255
access-list 101 permit ip 192.168.228.108 0.0.0.7 host 172.20.17.38
//Refus des connexions venant de 192.168.228.108/29 vers 172.10.7.0/24
   *** toutes les connexions vers ces réseaux doivent passer par le vpn
access-list 102 deny ip 192.168.228.108 0.0.0.7 172.20.7.0 0.0.0.255
access-list 102 deny ip 192.168.228.108 0.0.0.7 172.20.0.0 0.0.15.255
access-list 102 deny ip 192.168.228.108 0.0.0.7 host 172.20.17.38
//autorisation des connexions vers les adresses 206.211.128.186 et 206.211.127.186
access-list 102 permit ip 192.168.228.108 0.0.0.7 host 206.211.128.186
access-list 102 permit ip 192.168.228.108 0.0.0.7 host 206.211.127.186
ip dhcp excluded-address 192.168.228.109 192.168.228.111
ip dhcp pool USERS
   network 192.168.128.108 255.255.255.148
   default-router 192.168.128.109
   dns-server  172.20.0.20 172.20.0.90
ip name-server 223.254.95.126
ip name-server 223.254.64.13
//définition de la politique à utiliser
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
```

```
 group
//
crypto isakmp key passer@1360!1674! address 223.254.79.98
crypto ipsec transform-set vpnCbao esp-3des esp-md5-hmac
crypto map vers_POINT_E 10 ipsec-isakmp
 set peer 223.254.79.98
 set transform-set vpnCbao
 match address 101
 // Seule les connexions de l'ACl 101 seront cryptées ce qui fait que les connexions de l'ACL 102 ne passeront pas par le vpn
!
archive
 log config
  hidekeys
!
interface ATM0
 description Modem Adsl
 no shut
 no ip address
 no atm ilmi-keepalive
pvc 0/35
  pppoe-client dial-pool-number 1
interface FastEthernet0
interface FastEthernet1
interface FastEthernet2
interface FastEthernet3
interface vlan 1
 ip address 192.168.228.109 255.255.255.248
 ip nat inside
 ip virtual-reassembly
 no shut
```

```
exit
interface Dialer1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp authentication chap pap callin
 ppp chap hostname cbaowu-adsl
 ppp chap password westunion
 ppp pap sent-username cbaowu-adsl password supervision
 crypto map vers_POINT_E
 no shut
exit
ip nat inside source list 102 interface Dialer 1 overload
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer1
!
no ip http server
no ip http secure-server
!
banner exec ^
ip domain-name cbao.sn
crypto key generate rsa general-keys modulus 1024
ip ssh version 2
line vty 0 4
login local
transport input ssh
```

exit

!

c) Protocoles Utilisés

ISAKMP - (Internet Association and Key Management Protocol) - Un protocole cadre qui définit le format des charges utiles, les mécanismes d'implémentation d'un protocole d'échange de clés et la négociation d'une SA.

IPSEC : Protocole de tunnélisation qui utilise en général IKE

IKE : Internet Key Exchange Permet de gérer la négociation de protocoles et d'algorithmes basée sur une politique locale et de générer les clés d'authentification et de cryptage devant être utilisées par IPSec.

Md5 : méthode de hashage des messages pour la gestion de l'intégrité des données

Algorithme Diffie-Hellman : Protocole de cryptage à clé publique qui permet à deux parties d'établir un secret partagé sur un canal de communication non-sécurisé utilisé dans IKE pour établir les sessions de clés

3DES : Algorithme de cryptage de données utilisant une clé d'une longueur de 168 bits et exécute trois opérations DES en séquence

4) Dysfonctionnements Constatés

1. Diagnostic

Pour situer l'origine du problème, nous avons procéder à un troubleshooting de toutes de quelques liaisons VPN pour ainsi déterminer tous les flux .De ce fait, nous allons suivre les étapes suivantes :

- dans un premier temps, nous allons prendre en main la configuration des liaisons VPN pour ainsi comprendre ce qui a été fait.
- En second lieu, nous allons procéder au « trace route » des paquets pour déterminer les flux
- En dernier lieu, des simulations seront effectuées pour vérifier les hypothèses émises auparavant.

2. Résultats

Le trouble shooting des liaisons ont permet de constater que les points dédiés, pour se connecter sur Internet doivent tous transiter au niveau du proxy Bluecoat pour remonter sur le routeur de Point E .Or ce routeur ne dispose que d'une liaison ADSL de 2 Mbits, ce qui apparait très insuffisante pour une bonne performance.

De ce fait, cela engendre une dégradation importante de la qualité de la connexion aux serveurs de western union donc une diminution des performances des points dédiés de la banque, ce qui a largement contribué à des latences dans le traitement des requêtes utilisateurs.

De même, les traitements effectués sur les paquets par le proxy apportent à leurs tours une certaine latence ce qui participe grandement à la dégradation des performances.

Conséquences :

- Augmentation des files d'attentes au niveau de l'Interface du routeur

En effet, 65 LAN se partagent une connexion ADSL d'environ de 2 Mbits/s sur le routeur du Point E.

- De même, la perte de la liaison ADSL du routeur de POINT E entraine inexorablement l'impossibilité aux points dédiés de se connecter à western union

Pour parer à cette situation, nous allons proposer une solution d'optimisation permettant de répondant à la problématique d'une infrastructure sécurisée alliant une bonne gestion des ressources et des besoins en termes de Qos.

5) Solution proposée

La solution proposée consiste à faire des réajustements dans les configurations des routeurs des points dédiés en redirigeant le trafic western union directement sur l'ADSL local (du routeur). Puisque les trafics de messagerie et ceux afférents aux services monétiques (Powercard etc.) doivent toujours passer par le VPN alors il sera nécessaire d'ajouter les noms de domaines concernés comme exceptions sur le paramétrage du proxy au niveau du navigateur.

Pour ce faire nous allons devoir utiliser des listes d'accès (ACL) pour faire de la discrimination de trafic.

a) Les ACL

Les listes de contrôle d'accès (ACL) servent principalement au filtrage des paquets sur les interfaces physiques. Cependant on les utilise le plus souvent pour le cloisonnement des réseaux mais surtout dans le routage et la QoS. Il y'a deux types principal d'ACL les listes d'accès standard et étendue. Une **liste d'accès standard** filtre sur l'adresse source. Par contre une **liste d'accès étendue** permet un contrôle beaucoup plus fin du trafic en offrant le moyen de tester un ensemble de conditions dont les adresses source et destination, les protocoles utilisés en couche transport (TCP, UDP…) et en couche application (les numéros de ports) et certains champs de l'entête transport (TOS, DSCP). Les ACLs peuvent être nommés c'est-à-dire au lieu d'utiliser des numéros pour identifier l'ACL on utilise un nom tout simplement et ce type ACL est appelé une liste d'accès nommée.

Au fur du temps d'autres fonctions ont été ajoutées aux ACLs à savoir, une liste d'accès datée fonde le filtrage sur des critères de temps, une liste d'accès dynamique le

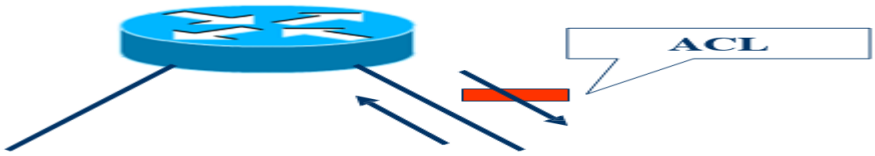
filtrage réalisé dépend du degré d'habilitation de l'utilisateur et une liste d'accès réflexive le trafic entrant n'est autorisé qu'en réponse à un trafic sortant.

1. Principes fondamentaux

C'est l'outil de base pour le filtrage des paquets IP (niveau 3)

Une ACL est une collection séquentielle d'instructions d'acceptation ou d'interdiction qui s'applique aux adresses IP aux protocoles de couche supérieure. De ce fait, elle permet de contrôler le trafic (interdire certaines actions à certains utilisateurs etc.) et de mieux gérer les performances du réseau en limitant le trafic.

Une ACL s'applique à une interface orientée d'un routeur



Traitement des instructions

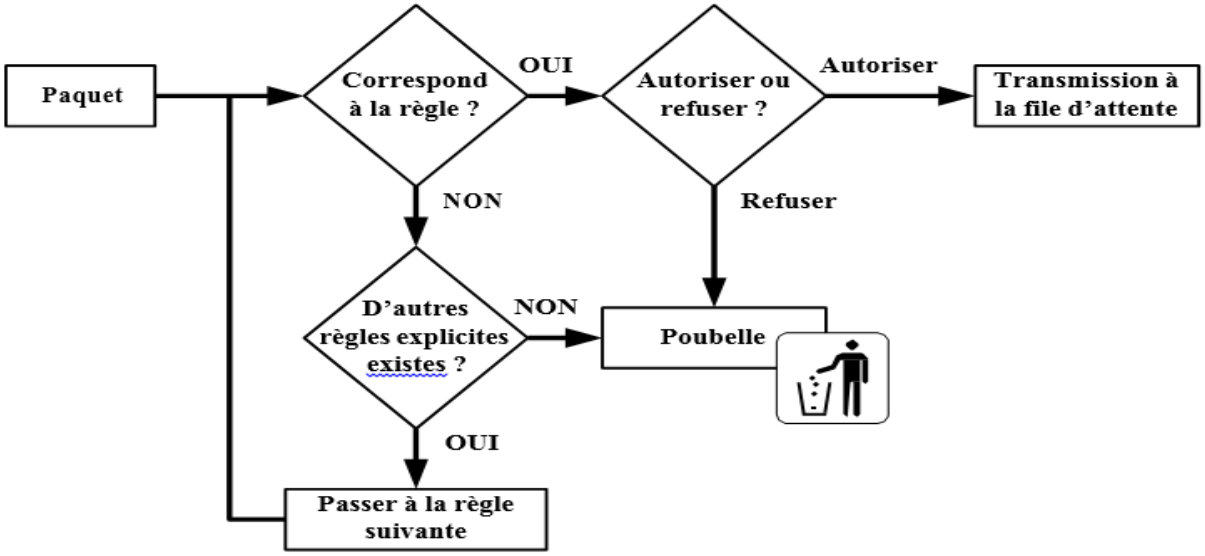


Figure 13:Parcours des instructions ACL [4]

L'acceptation ou le refus peuvent être fondés sur :

- L'adresse IP d'origine
- L'adresse IP de destination

Tous les paquets qui arrivent sur l'interface d'un routeur où une ACL a été activée sont confrontés à cette ACL.

Un paquet refusé est tout simplement abandonné.

Critères spécifiables dans une ACL

- Adresses sources
- Adresses de destination
- Protocoles utilisés (toute couche)
- Numéros de ports (couche 4)

2. *Avantage et inconvénients des ACLs*

* Avantage
  - Fournir une base de sécurité réseau
* Inconvénients
  - Traitement CPU supplémentaire
  - Latence réseau augmentée

3. *Notion de Masque Générique*

Les instructions qui composent les ACL utilisent une syntaxe de désignation générique de groupes d'accès. C'est l'utilisation du masque générique qui permet de le faire.

En effet, un masque générique est une suite de 32 bits :

- Un bit 0 de masque générique signifie « vérifier la valeur du bit correspondant »
- Un bit 1 signifie « ne pas vérifier (ignorer) la valeur du bit correspondant »

Par exemple, si on veut refuser tous les paquets qui viennent des réseaux compris entre 172.30.16.0/24 et 172.30.31.0/24, l'instruction correspondante dans l'ACL contiendra entre autres, les termes suivants : 172.30.31.0 0.0.16.255

		Décimal	binaire	Décimal
Adresse IP		172. 30.	0 0 0 1 1 1 1 1.	0
Masque générique		0. 0.	0 0 0 0 1 1 1 1.	255
			Vérifiés / non vérifiés	
Ainsi, les adresses concernées par cette instruction sont :	de	172. 30.	0 0 0 1 0 0 0 0.	0
	à	172. 30.	0 0 0 1 1 1 1 1.	255

Autrement dit : de 172.30.16.0 à 172.30.31.255
soit de 172.30.16.0/24 à 172.30.31.0/24

Par rapport à un masque de sous-réseau

- Inversion binaire
- En notation décimale pointée

Masque de sous-réseau	1111 1111.1111 1111.1110 000.0000 0000
Masque générique	0000 0000.0000 0000.0001 111.1111 1111

255 . 255 . 255 . 255
\- 255 . 255 . 224 . 0 (Masque de sous-réseau)

= 0 . 0 . 31 . 255 (Masque générique)

0.0.0.0 255.255.255.255 est équivalent à any



[4]

172.16.1.132 0.0.0.0 désigne seulement cette adresse et est équivalent à l'hôte 172.16.1.132

0.0.0.0 = 1 seule adresse 255.255.255.255 = Toutes les adresses

{IP} {0.0.0.0} = host {IP} {IP} {255.255.255.255} = any

L'association d'une adresse IP et d'un masque générique permet de définir une plage d'adresses réseau.

La plage d'adresses définie par l'association @IP/masque générique est une plage continue et correspond à un réseau quand le masque générique est continu, c'est-à-dire composé d'une suite ininterrompue de « 0 » suivie d'une suite ininterrompue de « 1 ». Dans ce cas, le masque générique résulte de la simple inversion du masque réseau.

Avec beaucoup de précautions, il est possible d'exprimer l'agglomération de plusieurs réseaux non contigus dans une seule association @IP/masque générique. Dans ce cas, le masque est discontinu, la seule règle étant que les bits à « 1 » du masque correspondent aux positions qui seront ignorées dans l'adresse.

4. Types d'ACLs

Il existe deux grandes familles d'ACLs : Les ACLs Standards et les ACLs étendues. Par contre, depuis la version 11.2 de l'IOS Cisco, d'autres sont apparues comme les ACLs nommées.

a. Les ACLs Standards

Les ACLs Standard sont la forme la plus simple mise en œuvre sur les routeurs et le contrôle porte uniquement sur l'adresse source ou le réseau source. Le champ d'application des listes d'accès standards convient quand il s'agit de, filtrer un trafic, limiter l'accès à des sessions Telnet, limiter l'accès à des sessions http, filtrer des mises à jour de routage, limiter la portée de la commande debug ip packet.

Voici la syntaxe globale de la commande permettant de créer un élément de la liste d'accès standard :

Router(config)#access-list ACL {permit | deny} {@IP_source [masq_générique] | any} [log[cookie_utilisateur]]

Les arguments de cette commande sont :

* **ACL** : Un nombre (1-99 ou 1300-1999) qui identifie l'ensemble des éléments de la liste d'accès standard.
* **Permit | Deny** : choix de l'action, le paquet doit il vivre ou mourir.
* **@IP_source [masq_générique] | any** : certains hôtes ou Tous les hôtes.
* **Masq_générique** : utile quand la source n'est pas limitée à un seul hôte.
* **Log** : Active la journalisation d'évènements liés à cet élément de la liste d'accès.
* **Cookie_utilisateur** : Chaîne de caractères optionnelle, ajoutée à l'événement journalisé l'option log afin d'aider l'administrateur à identifier l'élément de la liste d'accès qui a provoqué l'événement. Des restrictions existent, la chaîne ne doit pas utiliser de mots clés des listes d'accès et ne doit pas démarrer par une notion hexadécimale 0x. [5]

b. Les ACLs étendues

Une **liste d'accès étendue** permet un contrôle beaucoup plus fin du trafic en offrant le moyen de tester un ensemble de conditions dont les adresses source et destination, les protocoles utilisés en couche transport et en couche application et certains champs de l'entête transport. On peut placer la liste au plus près de la source du trafic à filtrer et ainsi éviter de gaspiller de la bande passante alors que la liste standard est placée au plus près de la destination et laisse cheminer un trafic qui sera finalement filtré en fin de parcours.

- ✓ Une liste d'accès standard est économe en ressources machine mais entraîne un gaspillage de bande passante.
- ✓ Une liste d'accès étendue est optimale quant à l'utilisation de la bande passante du réseau mais consomme d'avantage de ressources mémoire et CPU.

Voici la syntaxe globale de la commande permettant de créer un élément de la liste d'accès étendue.

Router(config)# access-list ACL [dynamic dynamic_name [timeout minutes]] {permit | deny} protocol {@IP_source [masq_générique] | any} {@IP_destin [masq_générique] | any} [precedence precedence] [tos tos] [dscp dscp] [time-range plage_de_temps] [fragments] [log [cookie_utilisateur] | log-input [cookie_utilisateur]]

Les arguments de cette commande sont :

* **ACL** un nombre (100-199 ou 2000-2699) qui identifie l'ensemble des éléments de la liste.
* **Dynamic** dynamic_name [timeout minutes] Identifie une liste d'accès dynamique, également appelée « Lock-and-key » dans les documents CISCO.
* **Permit | Deny** choix de l'action, le paquet doit-il vivre ou mourir ?
* **Protocol** test du champ Protocol de l'entête IP. Dans l'entête IP, ce champ occupe 8 bits. Le protocole encapsulé est donc identifié par une valeur comprise entre 0 et 255.
*

  Pour quelques protocoles importants, il existe un mot-clé que l'administrateur peut substituer à la valeur décimale dans le but de rendre plus lisible le fichier de configuration. [5] [6]

b) Mise en œuvre de la solution

1. Ajout de ACLs

Il a été convenu de faire le listing des adresses IP répondant aux domaines westernunion.com, wupos.westernunion.com, agentportal.westernunion.com et de les autoriser dans les ACL des routeurs des points dédiés.

- Ajout de quelques ACL

Ces autorisations sont matchées sur l'ACL étendue 102

permit ip 192.168.129.200 0.0.0.7 host 206.201.227.186

permit ip 192.168.129.200 0.0.0.7 host 206.201.229.252

permit ip 192.168.129.200 0.0.0.7 host 206.201.226.252

permit ip 192.168.129.200 0.0.0.7 host 206.201.227.93

permit ip 192.168.129.200 0.0.0.7 host 206.201.227.36

permit ip 192.168.129.200 0.0.0.7 host 173.194.40.220

permit ip 192.168.129.200 0.0.0.7 host 173.194.40.219

permit ip 192.168.129.200 0.0.0.7 host 54.236.198.163

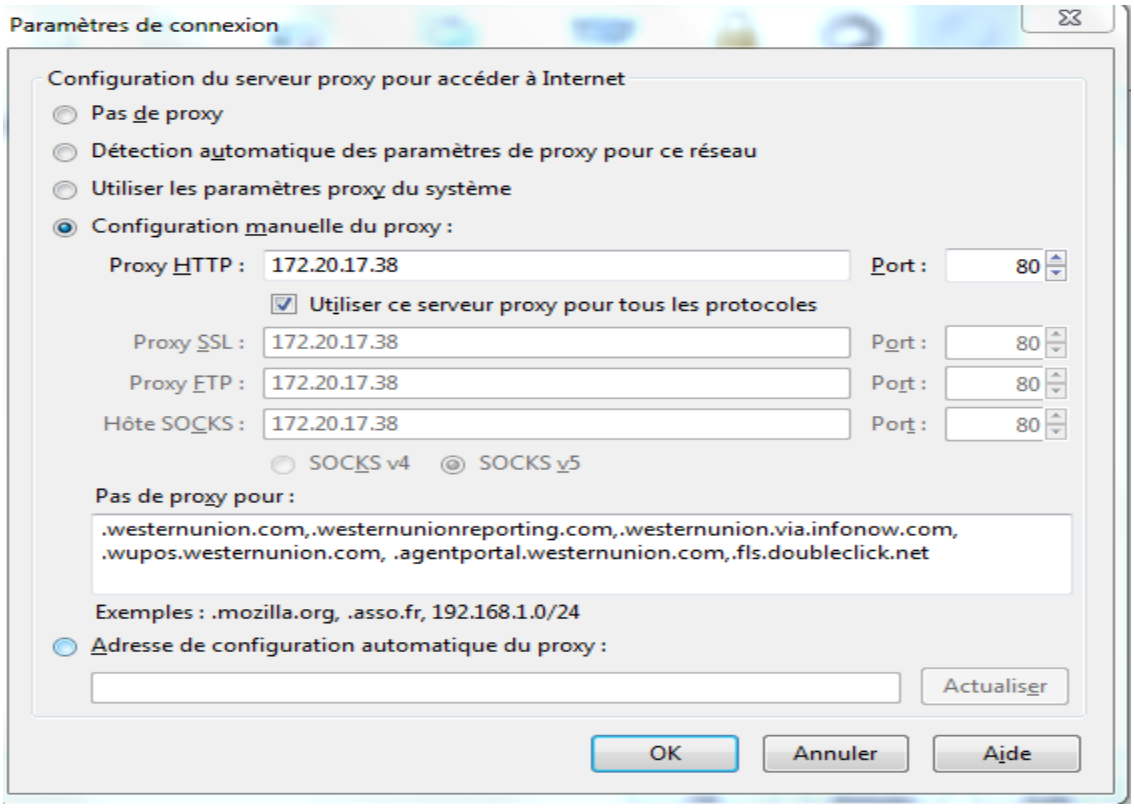
permit ip 192.168.129.200 0.0.0.7 host 54.209.12.180

Ces ACL permettons d'accéder aux différentes adresses de Western Union sans pour autant passer par le proxy .D'autres l'accès aux services de messagerie interne et les autres services monétiques de la banque passera inéluctablement par le proxy.

Ceci à première vue, peut sembler constituer une faille dans la sécurité des transactions. Mais puisque toutes les connexions sont certifiées (https) et que les machines hôtes disposent assez d'outils de préventions, les risques quant aux sniffing et à 'usurpation peuvent être moindre.

2. *Paramétrage du Proxy*

Puisque l'accès à certains sites ne nécessite pas la transition à travers le proxy Bluecoat de Point E, les noms de domaine de ces derniers ont été ajoutés comme exceptions au niveau de la configuration des navigateurs des PC.



c) Test et évaluation des configurations

Afin de nous assurer que le trafic actuel de western passe par la liaison ADSL de Point E, nous avons procédé par étape à la mise hors tension de l'interface dialer1 (interconnexion de connexion ADSL) du routeur de Point E , et observé par la suite le comportement des points dédiés.

Apres 24H d'observation, aucune incidence majeure n'a été signalée sur la connectivité réseau des points dédiés .Ce que nous a menés à la conclusion comme quoi, le trafic western est indépendant de la connectivité ADSL de Point E.

6) Conclusion

Apres plusieurs tests, nous nous sommes rendu compte que la perte de la connexion ADSL au niveau du routeur du Point n'a aucune incidence sur le trafic western. De ce fait, la configuration test préalablement implémentée dans le routeur de Thiaroye Sur Mer sera prise comme modèle pour le paramétrage des autres points dédiés.

Par contre, si à l'avenir les Points dédiés devront accéder à des applications hébergées en Interne (LAN de Point E), alors un redimensionnement des liens du tunnel devra être effectué afin d'avoir une bonne qualité de service. Pour cela, l'implémentation de VPN/MPLS et de l'agrégation de plusieurs LS (routeurs Point E) sont entre autres des solutions pour palier à ce problème. Cependant, des aspects importants comme le cout et les contraintes techniques devront être pris en compte.

III. Problématique 3 : Augmentation du débit et rationalisation des Coûts

1) Synoptique de l'Architecture LAN-MAN de la CBAO

La CBAO dispose d'un réseau de plusieurs niveaux. A des fins de souplesse de management et de sécurité, le réseau local est organisé en plusieurs VLAN en fonction du service ou départements.

Etant un établissement bancaire, elle dispose de plusieurs connexions avec d'autres établissements bancaires à travers Swift et partenaires (Visa, Mastercard)

Le réseau local siège est composé essentiellement de cinq sous-ensembles :

- DMZ public

C'est le sous-réseau qui héberge toutes les passerelles TPE, le serveur d'authentification, le serveur de supervision ainsi que les passerelles de messagerie.

- DMZ partenaires

C'est le sous réseau qui regroupe les équipements appartenant aux partenaires VISA et MASTERCARD pour les transactions bancaires par carte.

Il est relié aux réseaux des partenaires à travers des liaisons hertziennes.

- DMZ filiale

Du fait de sa vocation sous régionale, la CBAO dispose des filiales dans d'autres pays comme le Burkina, Niger, la Guinée Bissau et le Bénin.

Leurs différents réseaux sont reliés au siège à travers des liaisons satellitaires .De ce fait, une zone spéciale leur est dédiée afin de leurs faciliter l'accès partagé aux ressources de la banque

- Zone CHD

C'est la zone la plus sensible de tout le réseau car hébergeant toutes les applications du cœur de métier .Elle bénéficie d'une politique de sécurité renforcée avec un Firewall et un IPS. Du fait, des exigences en termes de sécurité, la banque s'est donné les moyens de disposer d'un réseau respectant les normes internationaux comme PCI/DSS

- LAN

C'est le réseau des hôtes .Il héberge les machines clientes du Siege et Pompidou, de même certains serveurs comme la BAL, partage de fichiers etc.…y sont implantés pour un accès facile et à moindre coût (bande passante) aux ressources.

Le réseau dispose de cinq connexions vers l'extérieur

- BCEAO-GIM

Membre intégrant de la BCEAO et du GIM, la CBAO a le devoir de rendre compte de ses opérations bancaires afin de faciliter le contrôle de la conformité avec les règles en vigueur dans l'Union Monétaire.

De ce fait, une liaison partant de l'UAP, qui est la plateforme de compensation, a été établie avec ces institutions à travers une liaison double (LS et RNIS).

- Liaisons Inter-agences

L'interconnexion des agences avec le siège s'établit à travers 3 liaisons suivantes :

  - SENTRANET AGENCES

Puisque toutes les applications bancaires sont centralisées au siège, alors les agences éparpillées partout dans le pays doivent accéder à ces ressources à travers un réseau fiable et sécurisé .De ce fait, une liaison de 4 LS agrégée de 2 Mbits (niveau Siege) et une liaison de 2 Mbits (niveau Point E) ont été louée à l'operateur pour faire face à ce défi majeur .Du côté des agences, il existe 2 liaisons : 1 LS (128 et 256 Ko) et 1 lien BRI /RNIS de 64 Kbits.

  - Des liaisons LASER
  - Boucle Local Radio

L'augmentation croissante des besoins en ressources de bande passante et les besoins d'économie de coût d'interconnexion, il est apparu nécessaire de trouver une solution

De ce fait, ils ont opté la solution de BLR pour relier certaines agences de Dakar avec la technologie Radwin.

  - VSAT

A cause des contraintes géographiques, il est apparu presque impossible d'installer des liaisons filaires(LS) dans certaines zones du pays .De ce fait, pour pallier à cela la solution VSAT a été choisie pour l'interconnexion de l'agence de Sabadola.

- INTERNET

Pour l'accès à Internet, une liaison spécialisée a été louée de même une ADSL.

Le trafic critique comme la messagerie, Western Union …sont redirigés vers la liaison Ls qui est beaucoup plus fiable.

- LIAISON INTER-FILIALE / VSAT

C'est la liaison par satellite qui permet de relier les agences aux différentes filiales dans la sous-région et le site de Casablanca.

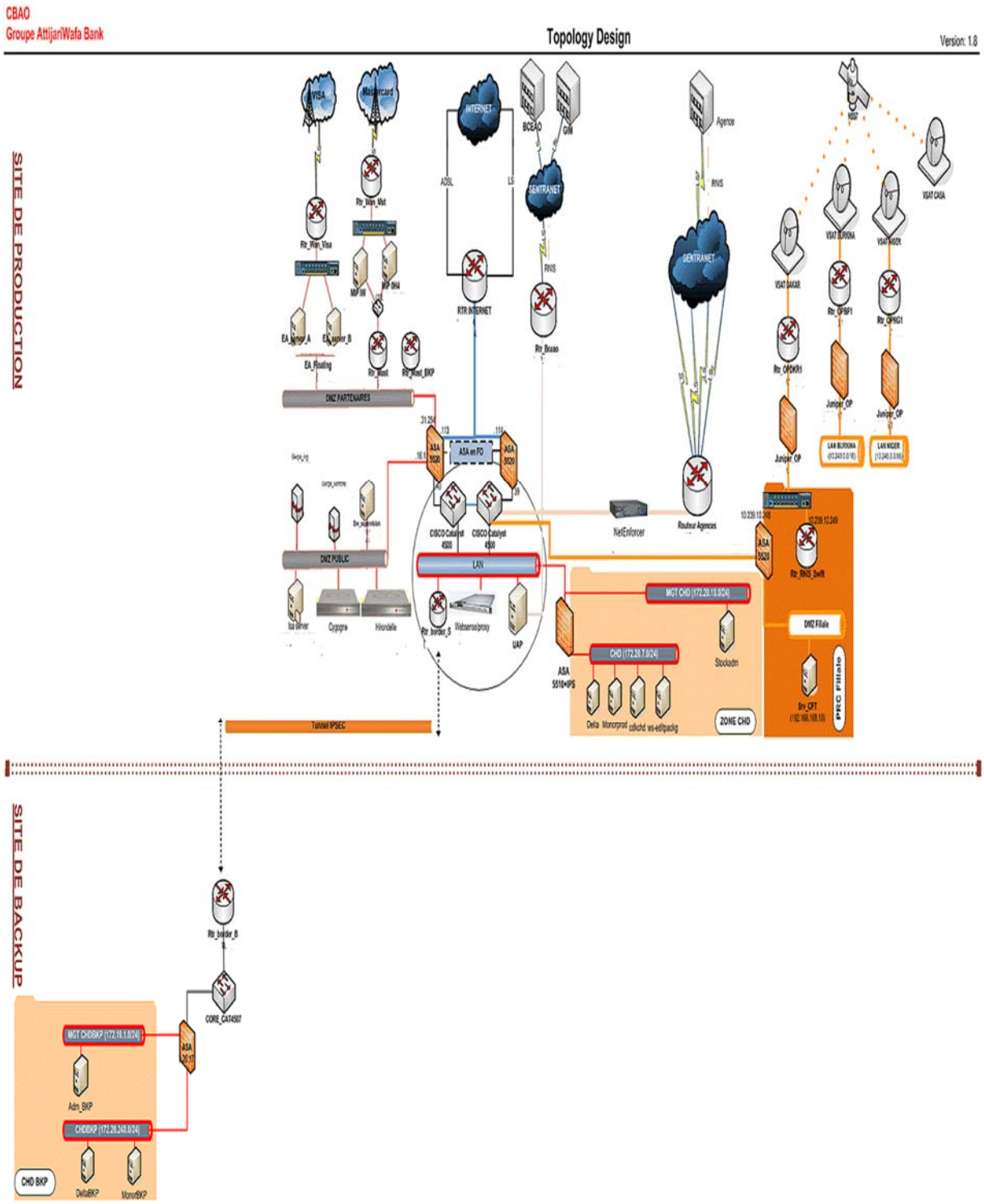


Figure 14:Architecture Réseau CBAO

2) Manquements et Points à améliorer

La CBAO de par sa place d'établissement financier historique et leader dans le marché sous régionale dispose d'un parc d'agences éparpillés dans le territoire national et les pays frontaliers. Les réseaux d'entreprise actuels doivent répondre à diverses problématiques, parfois contradictoires.

Un des enjeux majeurs consiste à améliorer le niveau de performances et d'efficacité élevée, dans un contexte de réduction des budgets et des ressources associés au SI.

Les architectures modernes doivent garantir la sécurité et la disponibilité des services et applications critiques, pour une satisfaction accrue des utilisateurs, tant en local qu'en situation de mobilité. Il est ainsi essentiel d'intégrer des technologies innovantes dans la conception des réseaux de nouvelle génération.

En effet, rien qu'au Sénégal, le réseau est composé de 98 agences reliées entre elles par des liaisons louées aux opérateurs.

De ce fait, l'interconnexion de ces différents sites nécessite l'établissement de réseau de grande envergure et d'un parc informatique important .C'est ainsi que grâce à l'offre de supports infrastructurels des opérateurs de télécoms comme Orange, ce réseau a pu être constitué sur plusieurs niveaux avec des liaisons louées avec l'extérieur.

Cependant, la location de ces liens coûtent excessivement chère à la structure et pèse énormément sur le budget de la DSI alors cette dernière conformément à la nouvelle politique de gestion des actifs informationnels, devait non pas être un absorbeur de ressources mais plutôt un créateur de valeurs ajoutées donc de revenus.

Le tableau ci-dessous donne les coûts de location des liaisons louées pour les agences qui seront par le déploiement dans un premier temps de la boucle locale radio.

Tableau 2:Coût de location des LS

CHARGE AGENCES

	AGENCE	Débit lien	cout mensuel	cout annuel	Backup ADSL
1	ZI 1	256 ko	287 400	3 448 800	321 600
2	ZI 2	256 ko	306 800	3 681 600	321 600
3	LSS	128 ko	191 500	2 298 000	321 600
4	Blaise Diagne	256 ko	287 400	3 448 800	321 600
5	Castors 1	256 ko	287 400	3 448 800	321 600
6	Castors 2	256 ko	306 700	3 680 400	321 600
7	Colobane	256 ko	287 400	3 448 800	321 600
8	Liberté 3	256 ko	287 400	3 448 800	321 600
9	Soumbédioune	256 ko	287 400	3 448 800	321 600
10	Claire de Lune	256 ko	287 400	3 448 800	321 600
11	Sipres	256 ko	256400	3 076 800	321 600
12	Sahm	256 ko	256400	3 076 800	321 600
TOTAL				39 955 200	3 859 200

De même, avec l'avènement de nouveaux services offerts aux usagers et l'accroissement des besoins en ressources (bande passante) des applications bancaires et utilitaires, les débits offerts par les opérateurs ne suffisent plus pour garantir une bonne qualité de service.

En effet, les débits disponibles de l'ordre de 256Ko dans la plupart des agences ne permettent pas dés fois d'utiliser tous les équipements réseau (ex : la téléphonie) en même temps et ceci peut constituer un facteur de baisse de la productivité donc du chiffre d'affaires de la banque.

Ainsi, les réseaux sont souvent pointés du doigt pour des problèmes de performance :

- conférences vidéo interrompues
- piètre qualité des communications audio ou encore temps de réponse applicatif dégradé.

De ce fait, il incombe de prime abord de trouver des solutions efficaces afin de répondre aux nombreux défis d'augmentation de ressources (bande passante, débits), diminution de couts et de fiabilité du réseau.

1) Proposition de Solution

La mise en place d'une solution répondant à la problématique de rationalisation des coûts télécoms et l'augmentation.

a) Mise en place d'une BLR (Boucle Locale Radio)

Face au challenge de réduction des coûts et amélioration des performances des liaisons inter-sites, une solution plus ou moins révolutionnaire s'impose car proposant une indépendance quasi-définitive vis-à-vis des opérateurs de télécoms.

En effet, la mise en place d'un réseau BLR bien que demandant plus de capitaux travail et de responsabilité constitue une solution viable et répondant parfaitement à la nouvelle donne .De ce fait, conformément à la politique interne de l'entreprise , les produits de l'operateur RADWIN qui constitue le leader mondial dans la fourniture de produits Point to Point et Point to Multipoint , ont été sélectionnés à cet effet .

Cependant, une liaison hertzienne n'est pas pour autant exempte d'inconvénients et de contraintes du fait du support de transmission qu'est l'air et dont l'homme n'a aucune maitrise parfaite de son environnement .Ainsi dans ce qui suit nous ferons une brève présentation des produits de RADWIN et du principe de transmission hertzienne avec les nombreux obstacles susceptibles de perturber la propagation des ondes.

1. Solution Point to Point

RADWIN a une gamme de produits diversifiés adaptés aux besoins des clients. La gamme correspondante aux liaisons PtP est dénommée RADWIN 2000 et est composé de plusieurs séries A, B et C.

Voici un tableau représentatif de toutes les séries de produits PtP.

Tableau 3: Produit RADWIN PtP

Product Series	Max. Throughput*	Target Applications	Band (GHz)
C-Series	200 Mbps, jusqu'à 16E1s/T1s	IP backhaul	2.3-2.7 3.3-3.8** 4.5-5.0, 4.8-6.0, 5.9-6.4
B-Series	50 Mbps, jusqu'à 8E1s/T1s	IP + TDM	2.3-2.7,4.9-6.0
A-Series	25Mbps, jusqu'à 4E1s /T1s	IP+TMD	2.3, 2.4, 4.9-5.9
A-Series	10Mbps	IP	2.3, 2.4, 4.9-5.9
X-series	20Mbps, jusqu'à 3E1s /4T1s	IP +TDM Access	3.3-3.8

Série RADWIN 2000 C

Elle est conçue pour les réseaux à grande capacité et exposé dans un environnement à forte interférence. Son débit total en agrégation peut atteindre 200 Mbps avec Ip et TDM sur la même liaison que ce soit en symétrique ou asymétrique. Les produits de la série C s'appuient sur IP avec une qualité de service de bout-en-bout avec la possibilité d'utiliser une large bande de fréquences.

En effet, selon les conditions climatiques et le niveau d'interférence, le système peux indépendamment d'une intervention extérieure basculer sur une autre fréquence afin de parer à la situation. De même, ils fonctionnent en mode symétrique et asymétrique adaptatif, où la capacité des canaux est allouée de manière dynamique entre ligne ascendante et ligne descendante selon la charge de trafic et les conditions de l'interface radio.

Les améliorations apportées à cette dernière permettent de fonctionner de manière parfaite dans les environnements les plus difficiles, y compris en scenarios NLOS (Non Line-of-Sight), à hautes interférences et lors de températures extrêmes

> Pour les opérateurs souhaitant briser la barrière des capacités et satisfaire à la demande croissante en haut débit, la série C de RADWIN 2000 constitue le bon choix. [4]

Points Saillants

- Capacité et Fiabilité
  - » Jusqu'à 200 Mbps net débit total (Asymétrique & Symétrique)
  - » 5/10/20/40 MHz bande passante du canal
  - » Optimisé pour les applications à haute capacité de backhaul IP
  - » Réseau avancé & QoS
- Support Services et Interface Radio
  - » Native TDM (Jusqu'à 16 E1s/T1s) + Ethernet
  - » 10/100/1000 Ethernet interface
  - » Bandes de fréquences 2.5, 4.8, 3.3-3.8, 4.4 – 5.0, 4.9– 5.x, 5.9 - 6.4 GHz
- Technologies : OFDM, MIMO et DIVERSITY
- Flexibilité : Migration transparente de TDM vers des réseaux tout-IP [4]

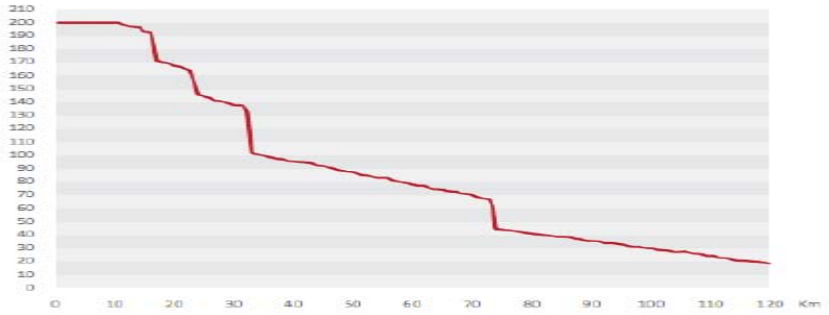


Figure 15:Performance en débit de RADWIN 2000 C @40 MHz

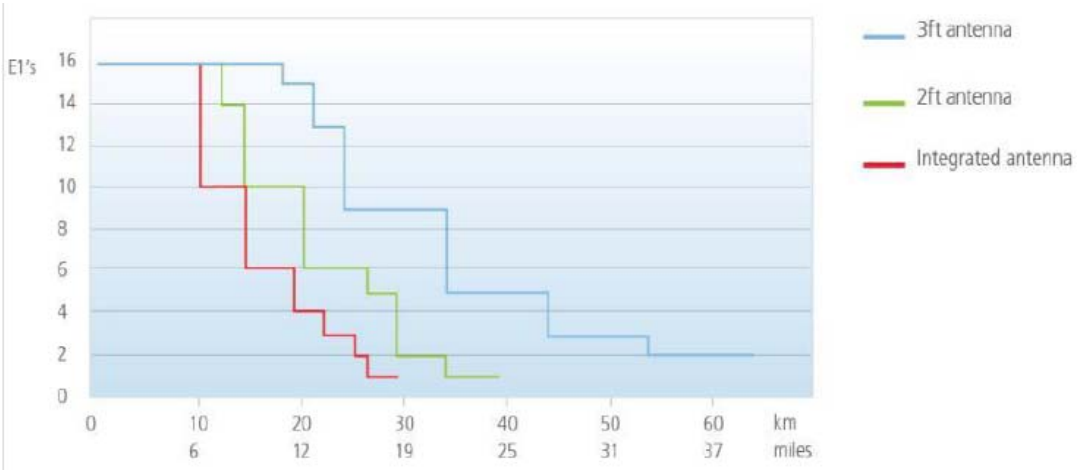


Figure 16: RADWIN 2000 C-Series Performance Range TDM (E1s)

Série RADWIN 2000 B

Comme la série C, elle est bâtie pour les applications Backhaul IP et dispose ainsi de fonctionnalités de réseau avancé avec Qos mais à la différence de cette dernière elle est peut être utilisée dans des réseaux d'accès avec une capacité de 50 Mbps .Sa Capacité de combiner TDM et Ethernet lui permet d'utiliser jusqu'à 8 E1s/T1s.Son débit plus acceptable et son cout moindre font qu'elle soit la série avec le meilleur rapport débit/coût dans la gamme 2000.

Points Saillants

- Capacité et Fiabilité
  - » Jusqu'à 50 Mbps débit total (Trafic Asymétrique et Symétrique)
  - » 5/10/20/40* MHz bande passante du canal
  - » Réseau avancé & QoS
- Flexibilité
  - » Combinaison flexible de native TDM + Ethernet Jusqu'à 8 E1s/T1s
  - » Supporte IP convergents + TDM Access & application backhaul
  - » Disponible en format Embedded avec antenne intégrée compacte et 2x connecteurs de type N - pour antenne externe

* - Disponible avec HW Révision 9 et version 2.8 [4]

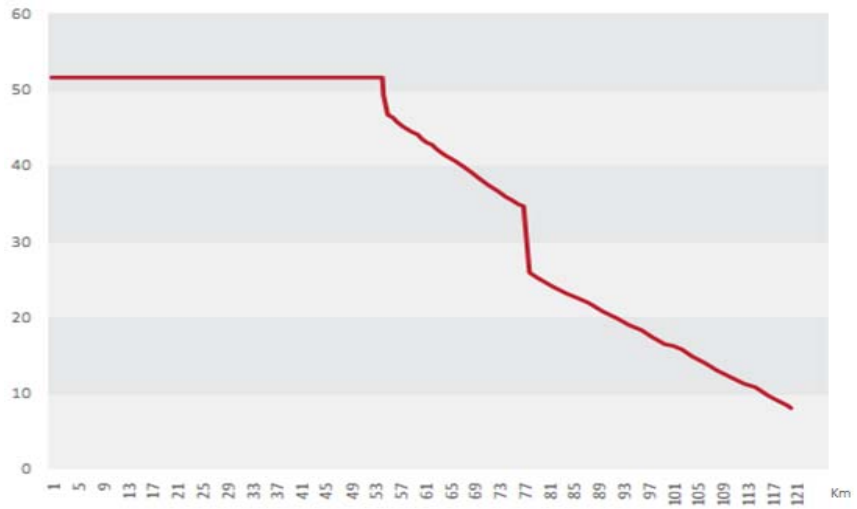


Figure 17:Performance Ethernet de RADWIN 2000 B /20 MHz

Série RADWIN 2000 A

Bâtie pour les applications de 'last miles', RADWIN 2000 A est la solution idéale pour les réseaux de faible capacité comme les réseaux d'accès ou la surveillance vidéo.

En effet, elle offre une capacité de 10 et 25 Mbps (asymétrique et symétrique) sur une liaison et sa portée peut dépasser les 120 Km selon les conditions radio .Comme toutes les autres séries de RADWIN 2000, la série A est disponible en plusieurs bandes de fréquence (2.3, 2.4, 4.9-5.9) avec des bandes passantes de l'ordre de 5, 10 ou 20Mbps par canal.

Points Saillants

- La meilleure solution compétitive pour l'Accès et la surveillance Vidéo
- Disponible en 2 modèles (à la fois avec antenne intégrée ou d'une unité connectée)
  - » Jusqu'à 25MBps et 4E1
  - » Jusqu'à 10Mbps
- MiMO /OFDM avec des fonctionnalités complètes de la famille RADWIN 2000
- 5, 10, 20Mbps bande passante du canal
- Évolutif grâce à clé de licence à partir de 10Mbps à 25Mbps [4]

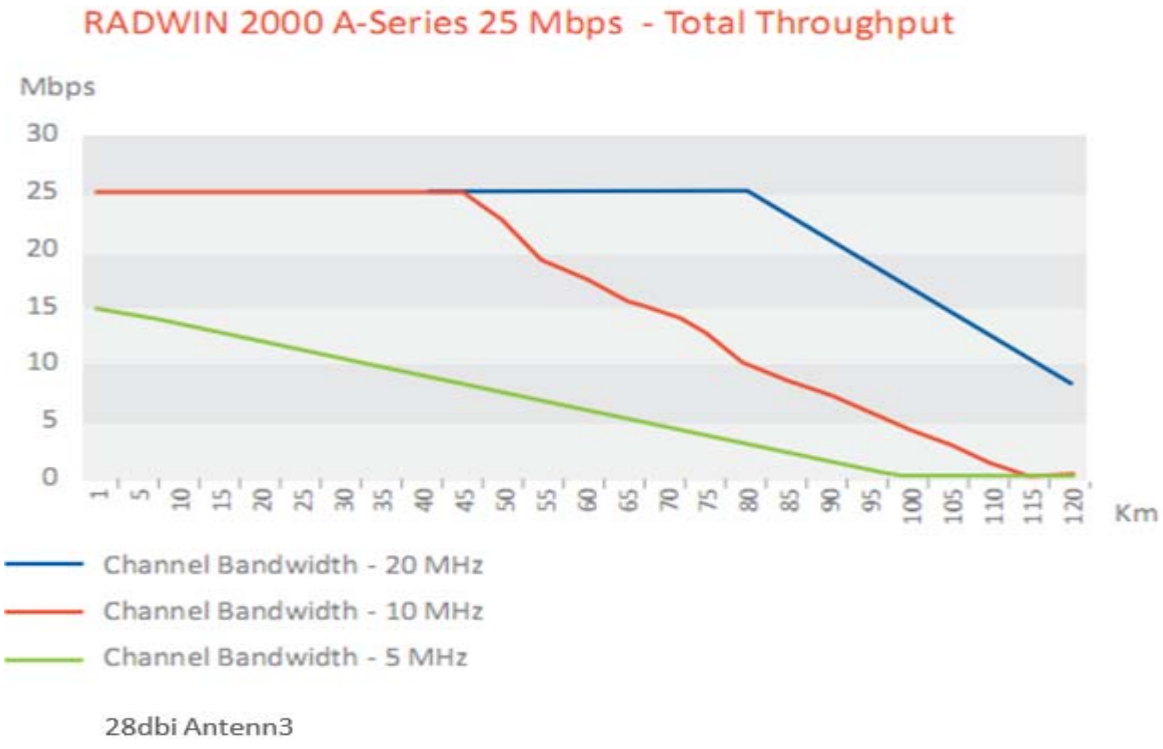


Figure 18 : Performance RADWIN 2000 A avec un débit de 25 Mbps

Série RADWIN 2000 X

A la différence de la série A, X-série offre un débit de 20 MHz symétrique mais seulement sur la bande de fréquences des 3.X GHz, avec la capacité de supporter aussi bien TDM et Ethernet avec 3 E1s/4 T1s

Points Saillants

- Jusqu'à 20 Mbps débit symétrique
- 5/10/20 MHz bande passante du canal
- Combinaison flexible de native TDM (jusqu'à 3 E1s/4 T1s) + Ethernet
- Supporte IP convergents + Réseau TDM [4]

2. RADWIN PtP Performance

a. Performance Radio

Performance: qualité du service, disponibilité, fiabilité, efficacité, maintenabilité

- OFDM BASE AIR-INTERFACE, permettant nLOS / NLOS déploiements
- RATE ADAPTIVE AUTOMATIQUE, maximisation de la capacité par distance donnée
- MIMO / DIVERSITY *, double la capacité & l'efficacité du spectre et de la performance nLOS
- AUTOMATIC REPEAT REQUEST, assure une transmission sans erreur même sous un environnement spectral congestionné
- AUTOMATIC CHANNEL SELECTION (ACS), sécurisation de connectivité dans un spectre congestionné
- CONFIGURABLE JITTER BUFFER, permet une transmission TDM sans d'erreur avec une latence minimale
- MULTI-BAND RADIO, assure une flexibilité maximale de la planification radio
- INTRA SITE TDD SYNC permet la coexistence de multiples Point-to-Point radios tout en utilisant l'espace minimum de mât et de spectre.
- INTER SITE TDD SYNC, réduit les soi-interférences et maximise la capacité du réseau
- SPECTRUM VIEWER *, facilite installation de radio dans le spectre congestionné

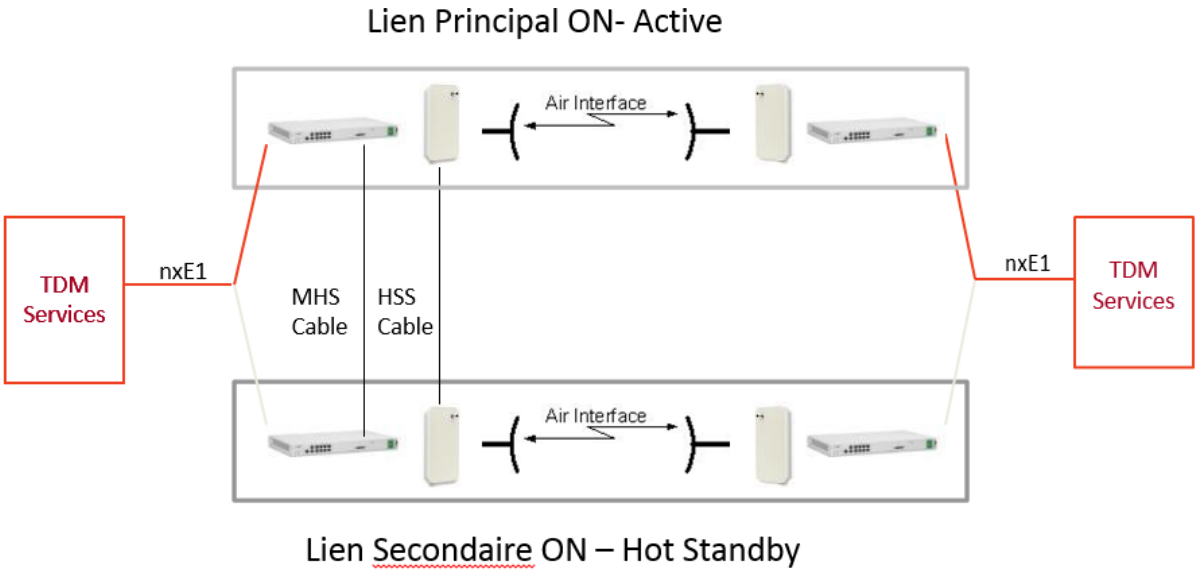
* RADWIN 2000 famille seulement

- Distance beaucoup plus grande
  - » Perte de diffraction réduite par suite d'obstruction
  - » Susceptibilité réduite aux effets environnementaux
- Opération en nLOS
  - » Capacité à utiliser le régime d'accès OFDM [5]

3. Gestion de la Haute disponibilité

a. Topologie de Redondance

TDM Redondance 1 +1 Topologie de Réseau



Protection Ethernet 1+1 Topologie du Réseau





b. Radio Multi Band

Radio Multi Band supporte des bandes multiples (2.4 GHz, 3.3-3.8 GHz & 4.8-6.0 GHz) sur la même plateforme Ainsi il permet d'installer plusieurs radios dans la même zone et d'éliminer les interférences mais ils ne peuvent pour autant pas opérer sur la même bande .De ce fait, il assure une transmission optimale et une meilleure utilisation des ressources de fréquences.

Si des interférences seront connues il suffit de sélectionner un autre canal

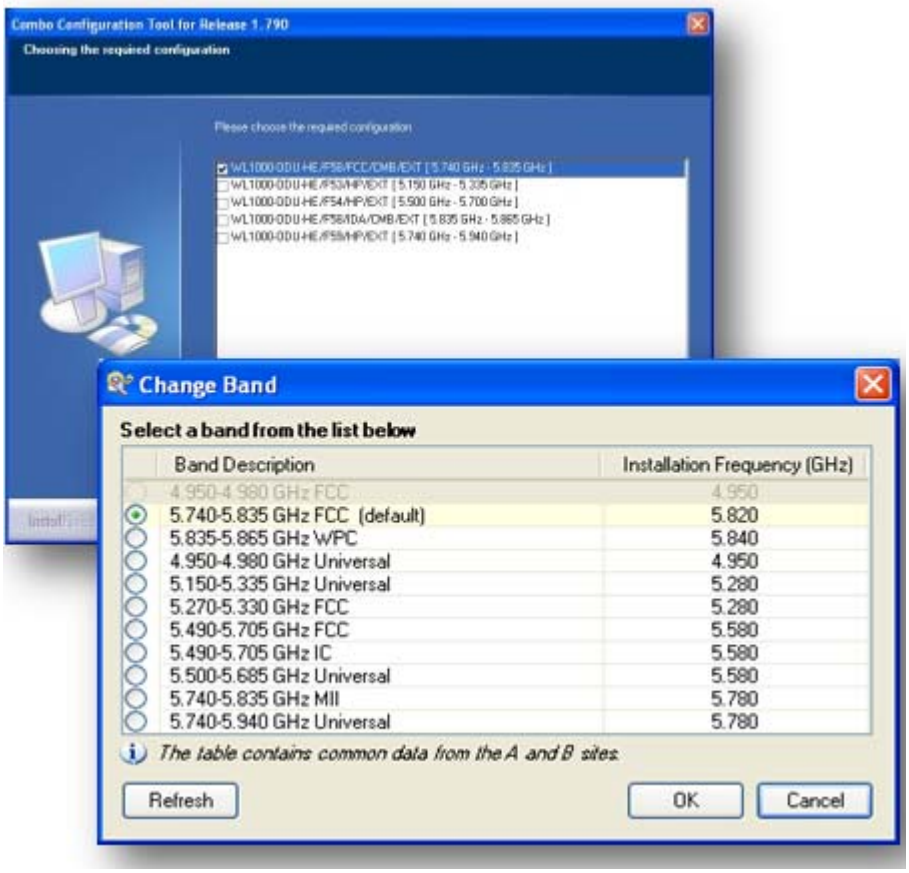


Figure 19;Configuration Radio Multiband

Dans un réseau de grande envergure, il existe plusieurs applications avec des exigences différentes en termes de temps de latence, débit etc. De ce fait, il doit exister un système efficace permettant de différencier tous ces trafics afin de mieux gérer les ressources partagées.

4. Gestion des ressources et de la qualité de service

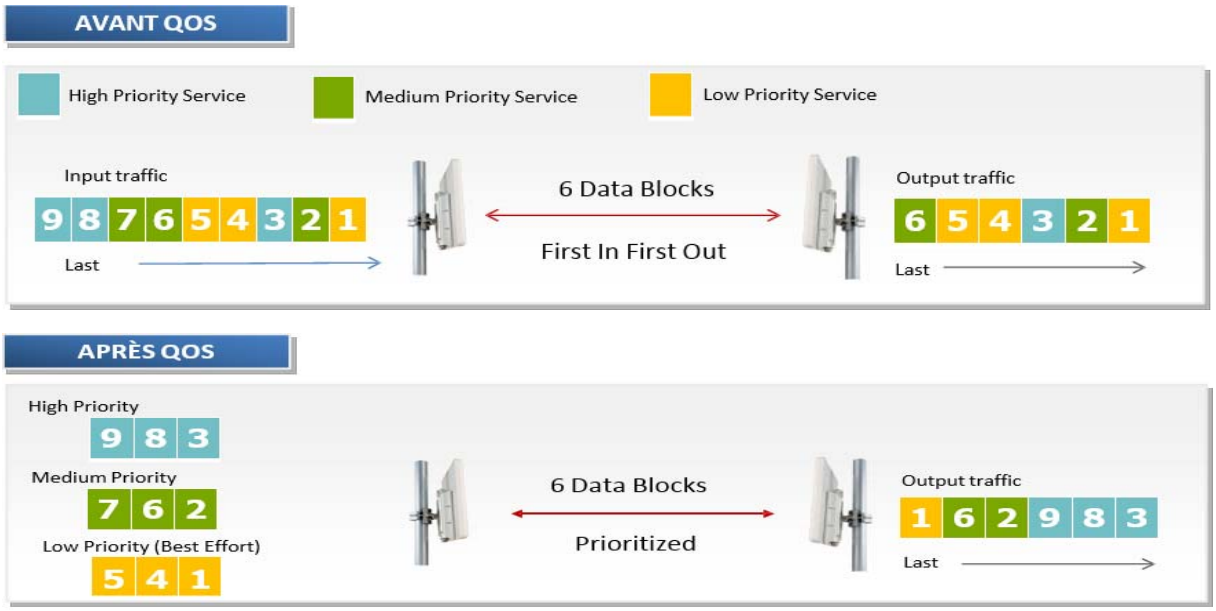
a. Qos : Qualité de Service Layer 2 Ethernet

La qualité de service (QDS) ou quality of service (QoS) est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets…

C'est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau (en management du système d'information) et de garantir de bonnes performances aux applications critiques pour l'organisation. La qualité de service permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par applications (ou activités) suivant les protocoles mis en œuvre au niveau de la structure. Ainsi, elle permet aux fournisseurs de services (départements réseaux des entreprises, opérateurs…) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport des données applicatives sur leurs infrastructures IP.

Cependant, la Qos est une notion subjective. Selon le type de service envisagé, la qualité pourra résider dans le débit (téléchargement ou diffusion vidéo), le délai (pour les applications interactives ou la téléphonie), la disponibilité (accès à un service partagé) ou encore le taux de pertes de paquets (pertes sans influence pour de la voix ou de la vidéo, mais critiques pour le téléchargement).

b. Principe



c. Qos dans RADWIN

RADWIN supporte deux critères de classification :

i. Diffserv

Le modèle Diffserv est une méthode de classification des paquets sous forme de classes.

Chaque classe est identifiée par une valeur codée dans l'en-tête IP. Cette classification doit se faire sur les routeurs de bordures (edge router) à l'entrée du réseau.

L'architecture des services différenciés contient 2 types d'éléments fonctionnels :

» Les éléments de bordures (edge functions) : ils sont responsables de la classification des paquets et du conditionnement du trafic. En bordure du réseau, c'est à dire à l'arrivée du premier élément actif capable de traiter le champ DS (DS-capable), les paquets arrivant ont dans leur champ TOS (pour IPv4) ou Traffic Class Octet (pour IPv6), une certaine valeur DS. La marque qu'un paquet reçoit identifie la classe de trafic auquel il appartient. Après son marquage, le paquet est envoyé dans le réseau ou jeté.

» Les éléments du cœur du réseau (core functions) : ils sont responsables de l'envoi uniquement. Quand un paquet, marqué de son champ DS, arrive sur un routeur DS-capable, celui-ci est envoyé au prochain nœud selon ce que l'on appelle son Per Hop Behaviour (PHB) associé à la classe du paquet. Le PHB influence la façon dont les buffers du routeur et le lien sont partagés parmi les différentes classes de trafic. Une chose importante dans l'architecture DS est que les PHB routeurs se basent uniquement sur le marquage de paquet, c'est à dire la classe de trafic auquel le paquet appartient ; en aucun cas ils ne traiteront différemment des paquets de sources différentes.

ii. 802.1p

IEEE 802.1p définit les 3 bits d'un champ contenu dans l'en-tête d'une trame Ethernet, utilisé pour marquer les trames d'un réseau IEEE 802.1. Il détermine la priorité, valeur entre 0 et 7 inclus, qui peut être utilisée par un mécanisme de Qualité de service (Quality of Service ou QoS) pour différencier les flux.

Elle définit 8 classes de service différentes qui sont disponibles et habituellement exprimée dans les 3 bits du champ priorité utilisateur (user_priority) dans l'en-tête IEEE 802.1Q ajouté à la trame. La manière dont le trafic sera ensuite géré en fonction de la classe à laquelle il sera affecté, n'est pas définie et reste du ressort des choix d'implémentation.

❖ ***Mécanismes d'acheminement***

Les trames vers l'interface radio sont mappées dans une des 4 Queues (real time, near real time, controlled load, best effort) en fonction des critères de classification.

Les trames sont tirées des queues vers l'interface air en fonction des priorités et un mécanisme d'importance.

Chaque queue a une proportion configurable en pourcentage de capacité totale de la liaison. L'utilisateur peut limiter le Maximum Information Rate (MIR) sur chaque file de priorité

Le MIR de la file de queue ne peut excéder le MIR de la liaison.

Avec QoS désactivé, tout le trafic est traité avec la même priorité.

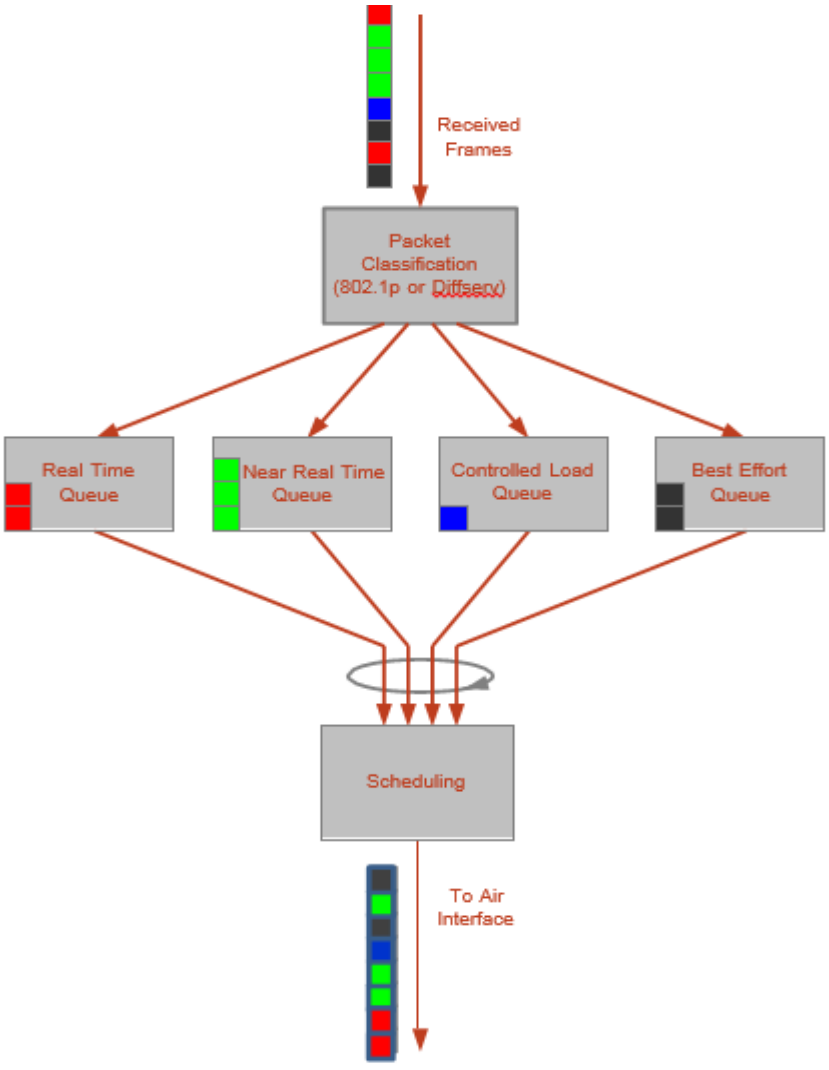


Figure 20:Mécanisme d'acheminement des paquets/Qos

❖ ***Classification***

Les frames sont classés vers les queues en fonction de leur 802.1p ou Diffserv domaines prioritaires.

Tableau 4: Priorité de Classification

Queue	VLAN priority	Diffserv DSCP value
Real time	6-7	48-63
Near real time	4-5	32-47
Controlled load	2-3	16-31
Best-effort	0-1	0-15

Pour des soucis de souplesse dans la gestion des réseaux de sécurité ou de fonctionnalités, les réseaux d'entreprises actuels sont organisés en réseau virtuels en fonction de plusieurs critères d'ordre fonctionnels, géographiques ou du type de trafic véhiculés. Ainsi, on trouve généralement les VLAN standards suivants dans presque tous les réseaux (Vlan Voix, Vlan Donnée, Vlan Management et Vlan Vidéo).

De ce fait, la fonctionnalité de configuration des Vlan a été intégrée aux équipements RADWIN.

d. VLAN (Virtual Local Area Network)

Chaque IDU sur le lien a une configuration individuelle indépendamment de l'autre côté de la liaison. Chaque port LAN (1,2 ou SFP) a une configuration individuelle

Ingress : Le trafic du réseau filaire vers les ports LAN DE IDU

Egress : Le trafic du port d'IDU LAN vers le réseau filaire

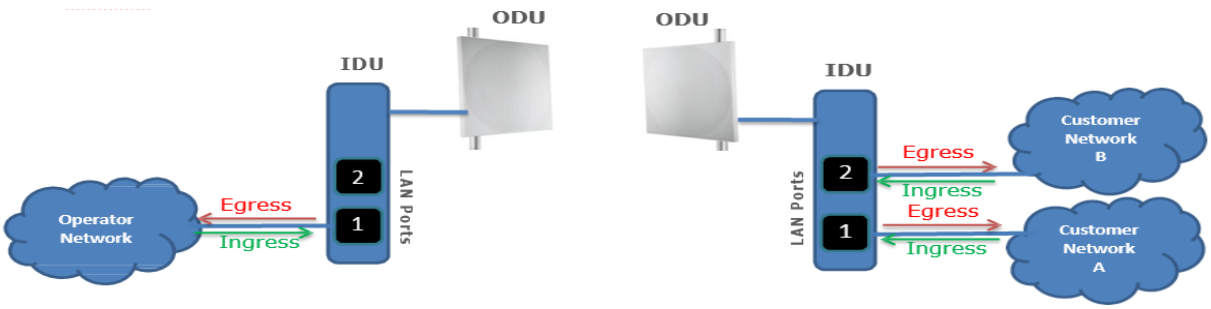


Figure 21: Schéma explicatif VLAN

e. Queue in Queue

Il permet aux clients d'utiliser les mêmes VLAN intérieurement dans leur «réseau de transport», tout en mélangeant le trafic des clients qui sont déjà VLAN-tagged.

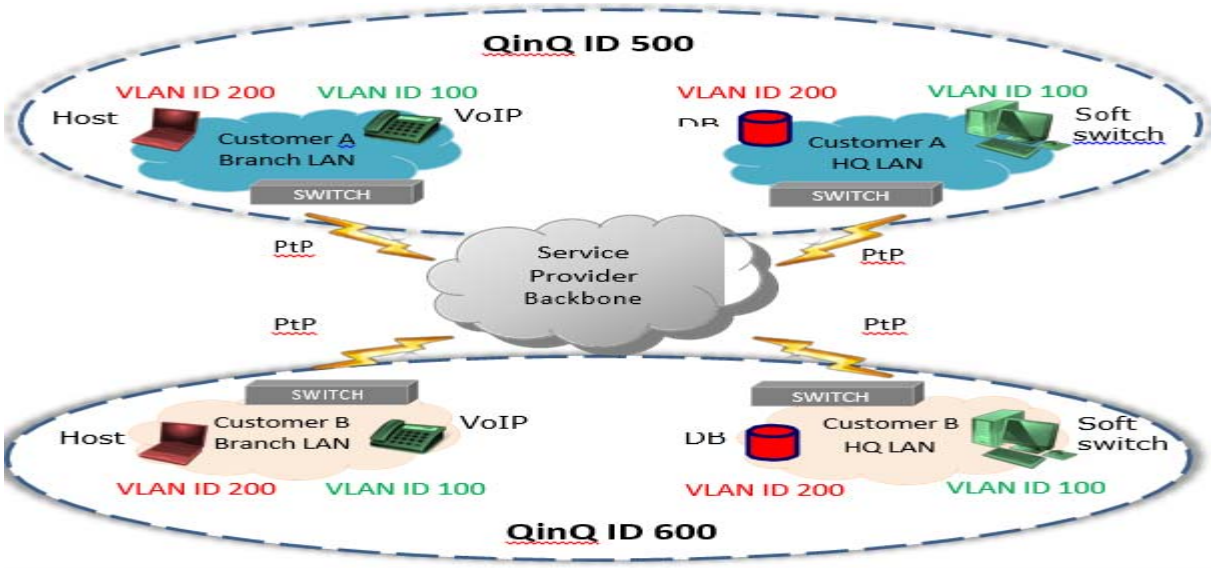


Figure 22:Architecture utilisant Queue in Queue

5. Point to Multipoint

C'est une technologie à haute capacité par secteur offrant un débit total qui peut aller jusqu'à 250 Mbps .Chaque secteur peut gérer jusqu'à 32 SU (Subscriber Unit) avec des débits de l'ordre de 5, 10,25 et 50 Mbps. La haute performance de son interface Air permet de garantir une latence mineure et constante à 10 ms typique en charge complète du secteur .De même, elle offre une large gamme de bandes de fréquences - 4,9 à 6 GHz, 3,3-3.8GHz, 2.5-2.7GHz. [5]

a. Composants

RADWIN 5000 est composé de deux unités principales : HBS (High Capacity Base Station) et HSU (High Capacity Subscriber Unit)

RADWIN HBS 5x00 High Capacity Base Station

Ce sont des antennes à basse consommation d'énergie (-25 W) avec une haute puissance de transmission permettant ainsi de desservir de longues distances .Afin de se prémunir des effets environnementaux et de visibilité, elle a la capacité d'intégrer MIMO et Diversity par SU.

HBS	Max Capacity
HBS 5200 – 2.5-2.7GHz, 3.3-3.8GHz, 4.9-6GHz	250Mbps
HBS 5100/5200 - 6.4 , 2.5GHz	100Mbps
HBS 5050 - 4.9-6GHz	50Mbps
HBS 5025 – 4.9-6GHz	25Mbps

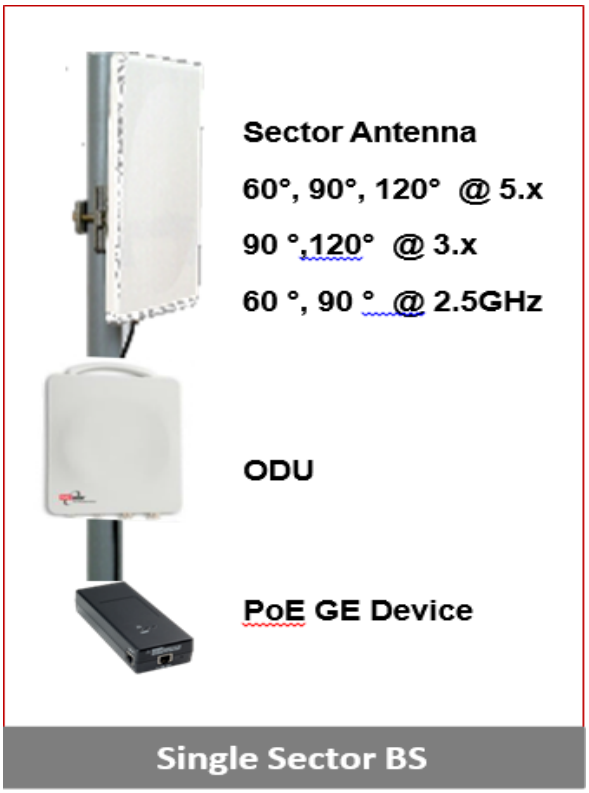


Figure 23:Caractéristiques des HBS

RADWIN HSU5xx - High Capacity Subscriber Unit

Ce sont les unités de transmission/réception situées au niveau de l'abonné ou du client .Elles sont disponibles dans plusieurs versions avec des capacités en débits différentes selon la fréquence.



b. Fonction RADWIN 5000

Smart Bandwidth Management - permet à l'efficacité des ressources supérieure

- Envergure complète de trafic asymétrique - jusqu'à 92% par DL ou UL
- QoS Améliorée - 4 niveaux de queue par HSU
- Maximum Information Rate (MIR) Configurable par HSU / queue / Direction
- Caractéristiques du réseau – VLAN, QinQ par HSU
- Longue Distance – 40km/25miles @ 20Mbps [5]

c. Performance Radio

- OFDM & MiMO 2x2 avancés / Diversity pour performance nLOS
- Enhanced interférence mitigation capability
- Inter & intra site sync. pour réduire les interférences de soi
- allocation de trafic de bande passante dédiée assurant le SLA et la Latence
- Latence basse, min <3msec, typique de 4 à 10 msec
- BW du Canal – 5, 10, 20GHz, 40* MHz est supporté (*seulement dans 5.x)
- Régulation- FCC/ETSI/WPC/UNI /MII [5]

d. Opérationnelle

- Multi bande - Stations de Base et Sus
- Totalement intégré avec les solutions RADWIN héritage:

  Coexiste avec RADWIN 2000 / WinLink 1000

  RADWIN Manager Commun

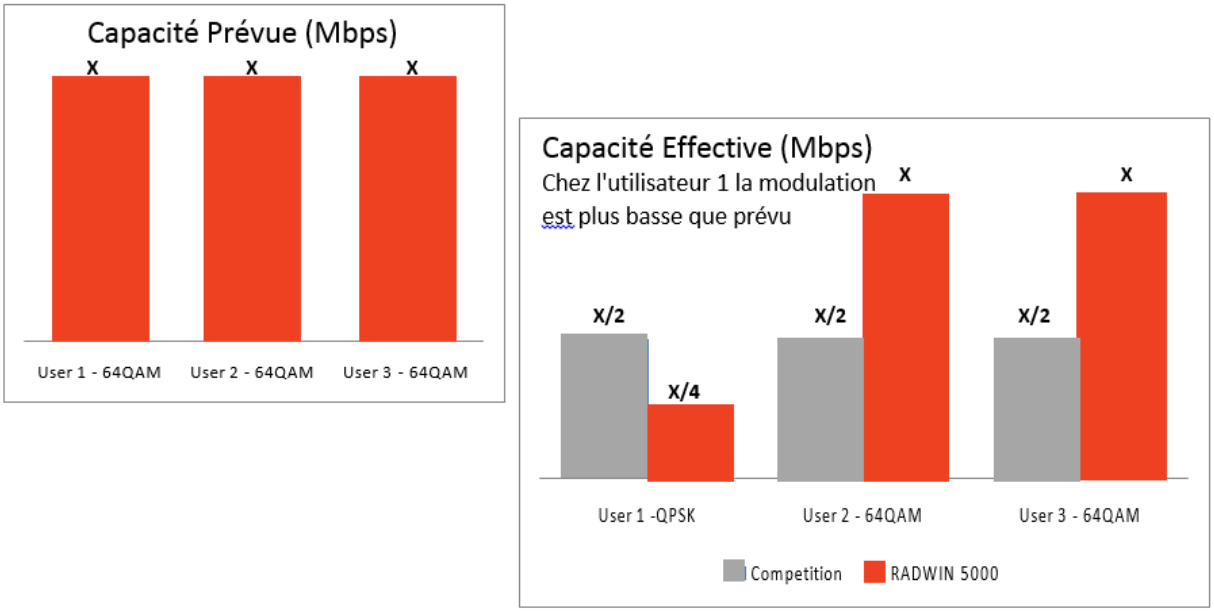
  RNMS Commun

  Management de Web

- Simple à déployer
- Visualiseur de spectre intégré, sélection de fréquence simple (disponible dans toutes les bandes de fréquences)
- Management basé sur le Web pour une installation de SU facile [5]

L'un des critères essentiels dans les liens d'accès est la capacité à garantir un SLA aux clients ou sites .De même , dans un secteur bancaire où les applications monétiques sont gourmandes en ressources et que le Système d'information constitue la charnière de toutes les activités , garantir un SLA est capital .Or dans un secteur où différents SU coexistent , la dégradation d'une liaison peut affecter celles des autres .

Service Layer Agreement (SLA) Scenario



La réduction de performance inattendue de la liaison de l'utilisateur-1 (par exemple niveau de modulation inférieur) n'affecte pas d'autres utilisateurs de RADWIN dans le secteur sauf l'utilisateur 1. Ainsi, le SLA des autres SU est garanti.

e. Gestion de la bande passante

i. Approche de TDMA

Le Time Division Multiple Access (TDMA) ou Accès multiple à répartition dans le temps en français, est un mode de multiplexage permettant de transmettre plusieurs signaux sur un seul canal.

Il s'agit de multiplexage temporel dont le principe est de découper le temps disponible entre les différentes connexions (utilisateurs). Par ce moyen, une fréquence (porteuse) peut être utilisée par plusieurs abonnés simultanément.

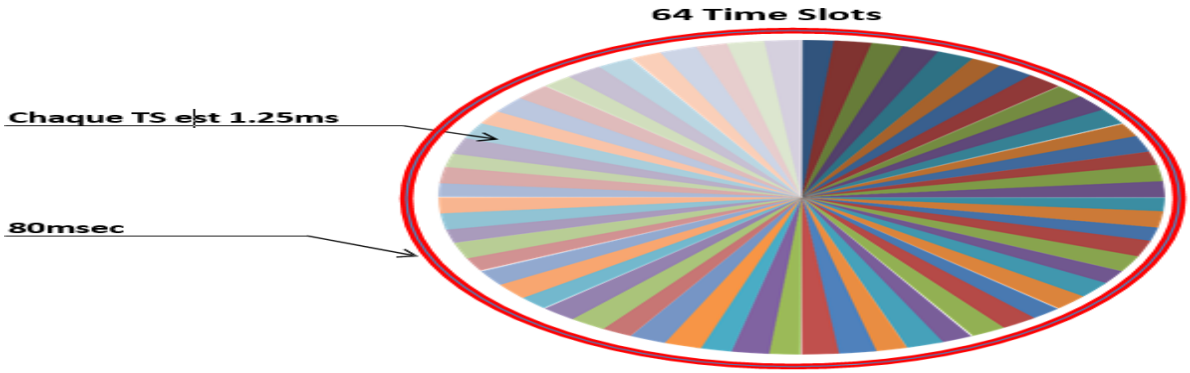


Figure 24:Approche TDMA

64 TS dont 1 dédié à la signalisation, de ce fait 63 sont disponibles pour le transport du trafic.

ii. Smart Bandwidth Management (SBM)

C'est une nouvelle fonctionnalité offerte dans les équipements RADWIN et permet une gestion plus flexible des ressources de bandes passantes pour chaque secteur.

❖ *Caractéristiques Principales*

Time Slots-allocations

Les allocations de Time Slots pour le Uplink ou le Downlink pour leurs applications dans le même secteur en fonction du service (service orienté DL ou UL)

Secured SLA : Quand il y'a interférence dans une des HSU ou diminution des performances, cela permet de sécuriser le SLA des autres HSU du même secteur.

Peak Rate : Dans les scénarios où le secteur n'est pas surchargé, les HSUs peuvent atteindre un débit maximal élevé (jusqu'à 90% du trafic du secteur dans le sens Downlink).

Sector Utilisation – Meilleure utilisation des ressources de bande passante inutilisée

Délai - scénarios dans lesquels le secteur n'est pas surchargé, certains HSUs peuvent atteindre un délai plus bas.

Récupération rapide des interférences: Dans les scénarios où le secteur n'est pas surchargé, certains HSUs peuvent atteindre un délai plus bas sous les interférences [5]

6. *Effets Environnementaux*

La perte de trajet est beaucoup moins affectée par les effets de l'environnement, ainsi le déclin du signal est proportionnelle à la fréquence.

- Pluie
- Tempêtes de Poussière
  - » La poussière absorbe et disperse le signal RF
  - » Peut changer la polarisation du signal
  - » Affecte les ondes au-dessus de 10 GHz
  - » Peut causer une atténuation de plus de 1 Db/Km [5]

Rain Loss @ 40Km	2.5GHz	5Ghz	7GHz	10GHz
10mm/h	<1db	<1db	2db	8db
50mm/h	<1db	4db	20db	48db

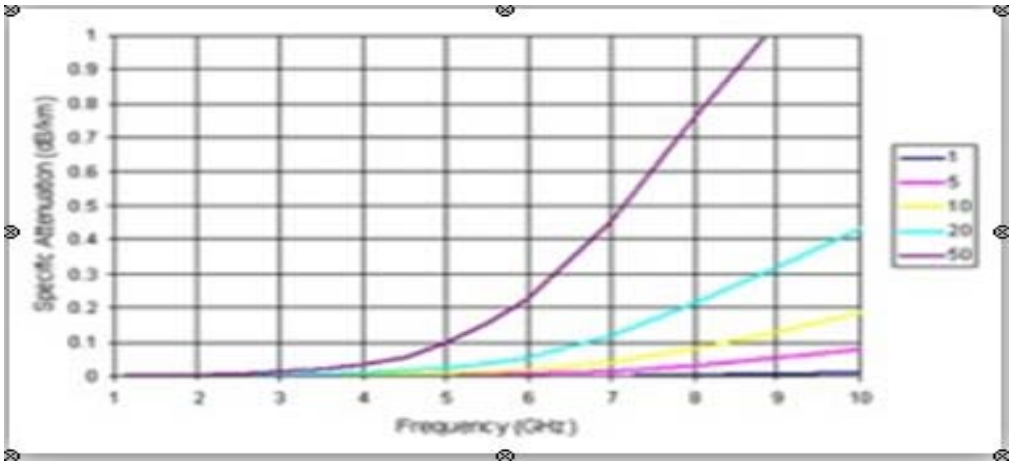


Figure 25:Evolution de l'atténuation du signa l en fonction de la fréquence

7. *Multipath et Obstructions*

Le déploiement d'une liaison BLR dans un milieu urbain n'est pas exempt d'inconvénients dû à l'environnement et les nombreux obstacles (immeubles, arbre etc.) .Ces obstacles font que pour la majeure partie de ces liaisons , il est presque impossible d'avoir un lien LOS(Line-of-Sight) .

Pour parer à cette situation il est possible d'utiliser de nombreuses technologies comme la diversité (spatiale ou de polarisation), OFDM (Orthogonal Frequency Division Multiplexing) et MIMO (Multiple Input Multiple Output).Le phénomène de Multipath peut entrainer des évanouissements profonds à la réception de plusieurs signaux ayant suivi des chemins multiples au cours de la propagation .

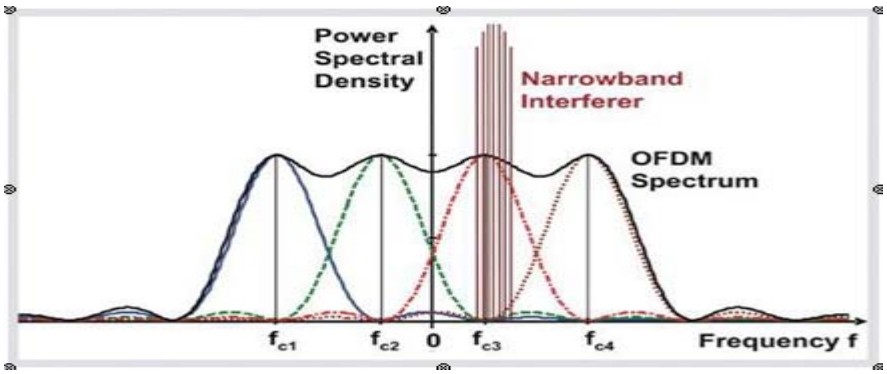
a. OFDM (Orthogonal Frequency Division Multiplexing)

i. Principe

Il consiste à diviser le signal en plusieurs sous porteuses codées orthogonalement, ainsi si deux signaux de chemins différents se rencontrent, leur addition donnera une valeur nulle ce qui atténuera les interférences. L'utilisation de l'OFDM réduit les effets de trajets multiples et la propagation de retard, ce qui est particulièrement important pour les basses fréquences et de transmission nLOS. Elle peut fonctionner jusqu'à 40 % d'obstruction de la zone de Fresnel.

ii. Codage

Les sous-porteuses sont de petites portions du spectre de fréquences. Par conséquent, ils sont individuellement pas lésés par l'interférence entre symboles (ISI - les distorsions de symboles adjacents). Si les données sont codées dans toutes les sous-porteuses, les interférences à bande étroite peuvent facilement être manipulées en éteignant les sous-porteuses où l' « interfereur » à bande étroite respectif est persistant.



Les données sont codées sur plusieurs canaux

Le graphique ci-dessous montre comment une séquence de symboles 8 QPSK est représentée dans les domaines fréquence et temps(OFDM):

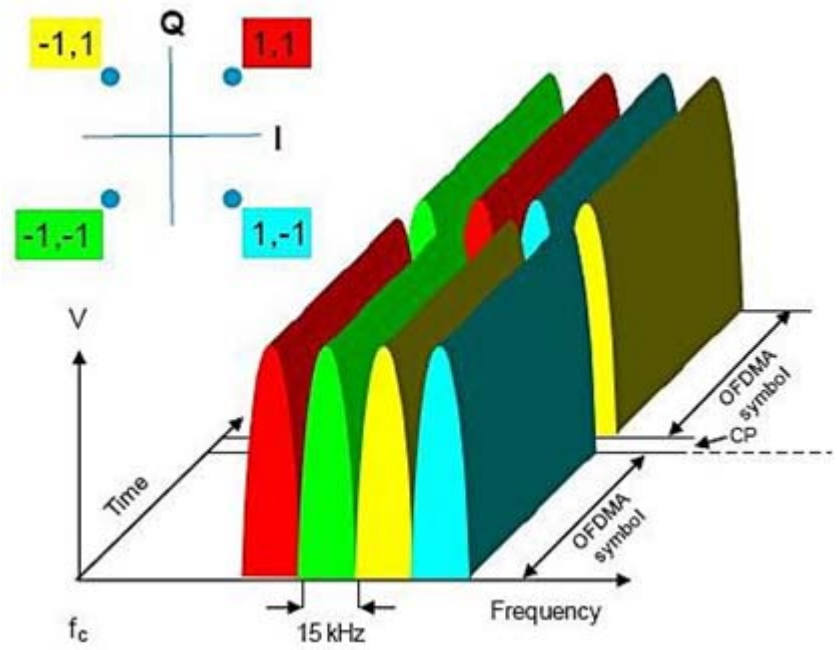


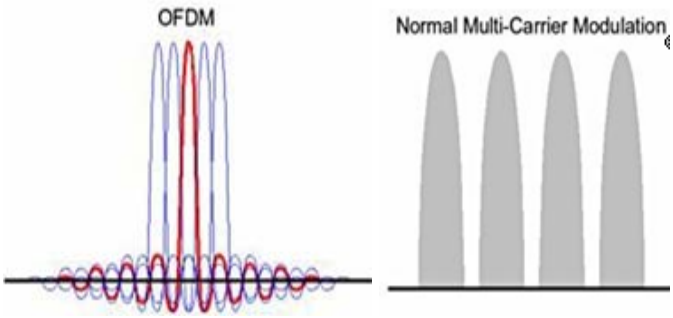
Figure 26:Symboles de données occupent 15KHz pour une période de symbole OFDM

iii. Haute Efficacité Spectrale

Dans le domaine de fréquence, le spectre de chaque sous-porteuse est une fonction de synchronisation avec croisement zéro chaque passage f0.

Puisque l'espacement de sous-porteuse f0 est identique alors il n'y a pas d'interférence inter-sous-porteuse. Les spectres OFDM se chevauchent, un grand nombre de sous-porteuses peut être placé dans chaque intervalle de fréquence f0. Alors la forme du spectre de puissance totale se trouve à proximité d'un carré.

Cela signifie qu'OFDM a une très haute efficacité d'utilisation de fréquence.



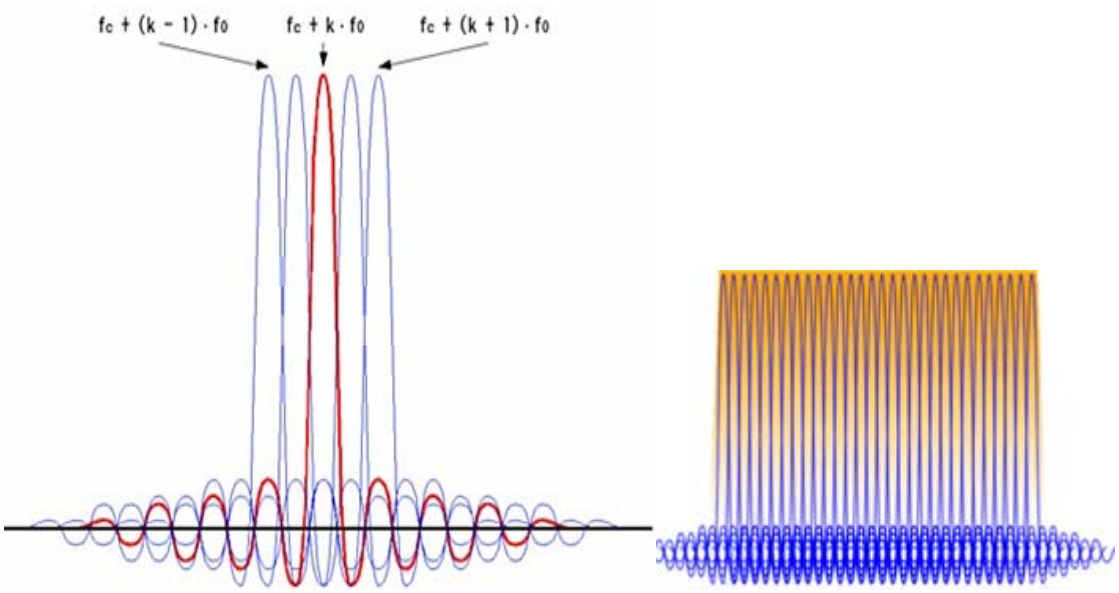


Figure 27:Occupation spectrale/OFDM

b. MIMO Multiple Input Multiple Output

Avec MIMO, le système double la capacité de liaison. Simultanément, il maintient le même débit et la modulation par radio comme on l'a utilisée avec une seule antenne, augmentant ainsi la capacité, la distance et la disponibilité. Par exemple, avec une double antenne RADWIN 2000 peut transmettre à modulation de 64QAM et FEC 5/6 et obtenir un débit d'air de 130 Mbps contre 65 Mbps avec une antenne seule.

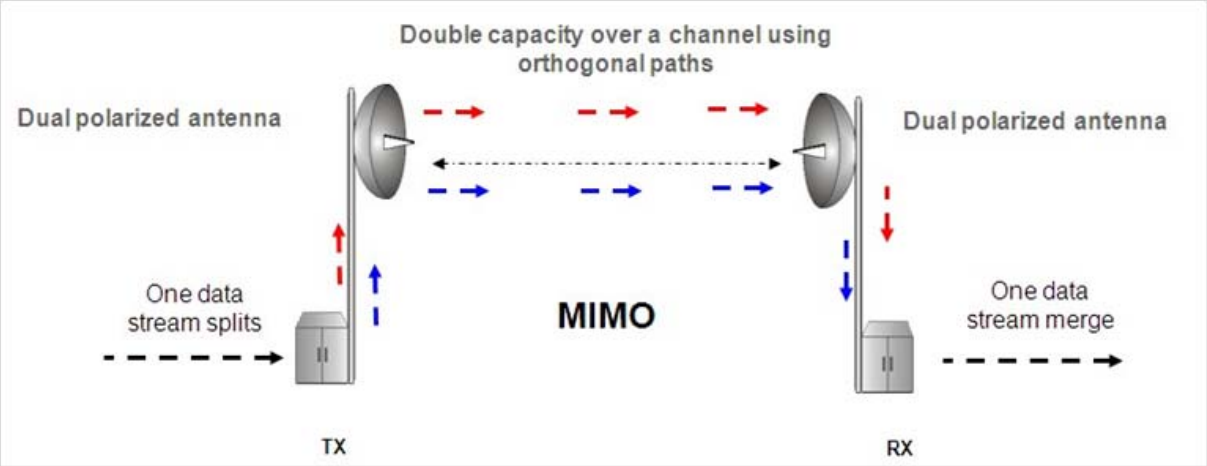
Pour travailler dans ce mode, chaque port d'antenne doit être connecté à une antenne, le niveau de RSS dans les deux récepteurs doit être équilibré et une séparation minimale entre les antennes doit être maintenue. (Par exemple, en utilisant des antennes à polarisation double une séparation de polarisation croisée est obtenue).

Tant que le mode de polarisation double d'antenne est sélectionné, RADWIN 2000 sélectionne automatiquement le mode MIMO et double le débit d'air.

RADWIN Manager indique en cas de déséquilibre entre les RSS de deux antennes.

Points saillants

- Capacité double est effectuée sur un canal de fréquence donnée en utilisant 2 flux en cours sur des chemins orthogonaux à travers l'antenne polarisée double
- MiMO permet beaucoup plus de fade marge pour une capacité donnée, puisque la modulation inférieure peut être utilisée (grâce à des flux doublés)



c. Diversité

Le Mode de diversité utilise deux antennes pour ameliorer la qualité et la fiabilité de la liaison.

Souvent ,la ligne de vue n'est pas claire (LOS) entre le transmetteur et le recepteur ainsi le signal est réfléchi le long de plusieurs chemins avant que le recepteur ne le reçoive .

Chaque rebond peut introduire des déphasages,des retards, des atténuations et méme des distorsions qui peuvent interferer de facon destructive avec l'autre à l'ouverture de l'antenne de reception.La Diversité d'antenne est particuliérerment éfficace pour reduire ces situations de multi-trajets du fait que plusieurs antennes permettent de recevoir plusieurs enregistrements du méme signal.Chaque antenne sera exposé à une interference differente très rémanente.

Ainsi ,si une antenne est en cours d'évanouissement profond , il est probable que l'autre ait un signal suffisamment fort. Le systéme choisit le meilleur signal reçu fournissant une robustesse améliorée .Collectivement,un tel systéme permet d'avoir une liaison de meilleure qualité.

Elle necessite cependant une séparation d'antenne qui est possible grace à deux methodes :

- Diversité de Polarisation - combine une paire d'antennes avec des polarisations orthogonales
- Diversité spatiale utilise des antennes qui sont physiquement séparés les uns des autres

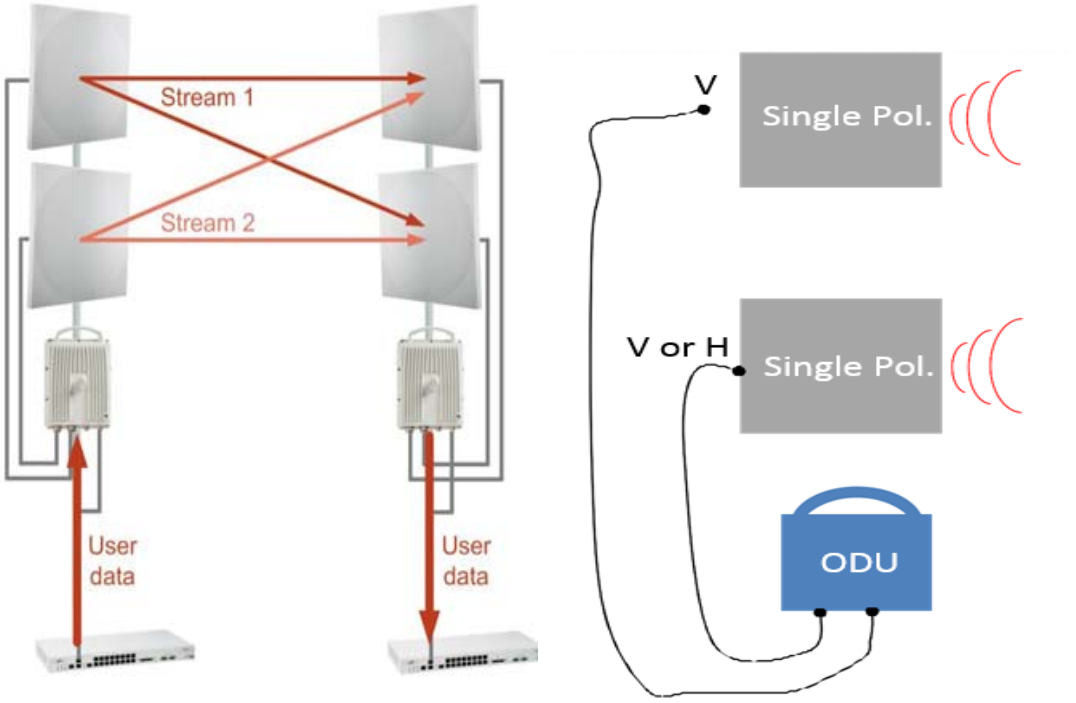


Figure 28:Diversité d'Antenne gain: améliore jusqu'à 15db la performance nLOS

d. Diversité vs MIMO

Ces deux modes sont faits pour parer aux conditions meteologiques précaires afin de garantir une bonne fiabilité aux liaisons BLR .Toutefois , il existe des conditions bien specifiques pour le choix de l'un ou de l'autre .Ainsi , tout dependra des enjeux (SLA ….) et de l'environnement de propagation des ondes hertziennes.

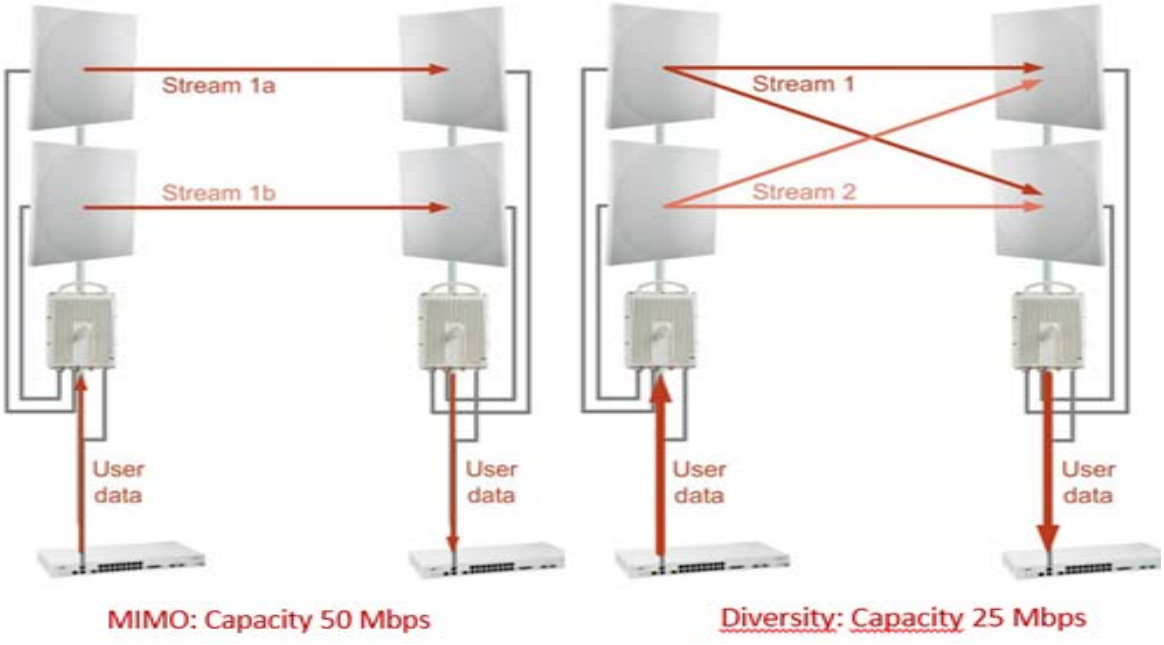


Figure 29:Comparaison entre MIMO et Diversité

Utilisez MIMO

» Quand la plus grande capacité est nécessaire jusqu'à 50 Mbps Full Duplex

» Quand les conditions aériennes sont similaires entre les antennes

Utiliser Diversity

» Quand le système ne peut pas fonctionner en mode MIMO à cause des conditions de la liaison

» Quand vous obtenez une capacité supérieure en mode Diversity que dans le mode MIMO

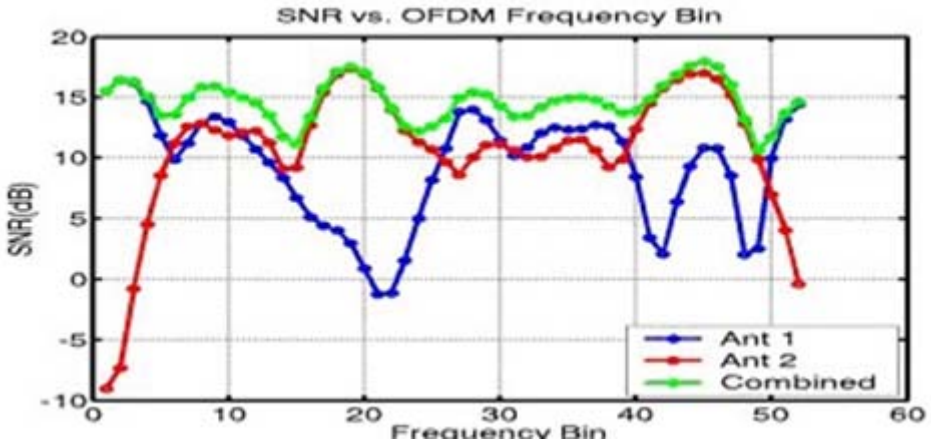


Figure 30:Graphe de comparaison entre les performances de Diversity et OFDM

L'environnement bien qu'étant souvent responsable des problèmes de transmissions pour les supports hertziens n'est pas pour autant le seul car d'autres facteurs peuvent aussi influer.

8. Gestion des erreurs

Tout système de transmission est enclin à être victime d'erreurs de transmissions des informations .Celles-ci peuvent être d'origine diverses comme des conditions climatiques pas très reluisantes, un buffer plein etc. Ainsi, dans le monde moderne de la transmission l'intégrité des données est capitale de ce fait les systèmes fiables sont souvent jugés entre autres sur leurs taux d'erreur binaires ou leurs méthodes de gestion de tels cas.

a. Automatic Repeat Request (ARQ) Rapide

C'est un mécanisme breveté par la société qui assure la retransmission ultra-rapide des données erronées. En effet la répétition de la transmission est initiée sans avoir à attendre une demande de l'unité distante (récepteur) ce qui minimise la proportion des erreurs tout en gardant le temps de latence au minimum pour mieux soutenir les services pressés par le temps (par exemple TDM) [5]

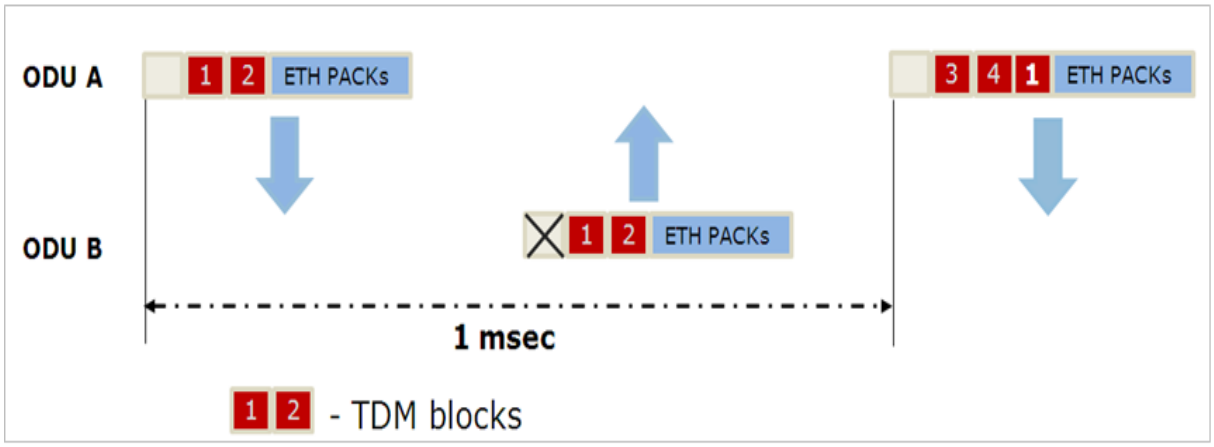


Figure 31:Mecanisme de retransmission des bits (ARQ)

b. Rate Adaptive Automatique

Cette fonctionnalité permet à RADWIN 2000 de changer le niveau de modulation rate de l'interface aérienne dynamiquement, en fonction des conditions de liaison radio

Avantage:

Maximisation du débit Ethernet, tout en assurant la proportion d'erreurs minimale

Robustesse accrue et performance meilleure en interférence

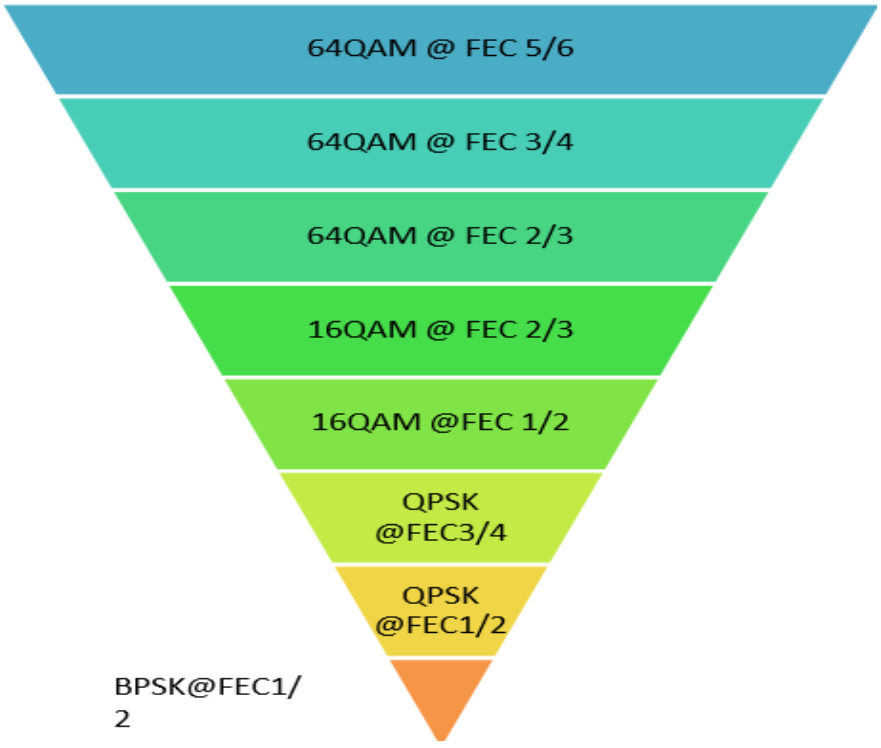


Figure 32:Adaptation Automatique du Niveau de Codage

Cette adaptation de la modulation en fonction des conditions climatiques n'enlèvent en rien la qualité de la transmission .Ainsi, les performances de débit sont proportionnelles au niveau de codage utilisé pour la modulation de l'interface air.

La figure ci-après montre l'évolution gracieuse du débit en fonction de la modulation dans un scenario où la fréquence utilisée est 40 MHz.

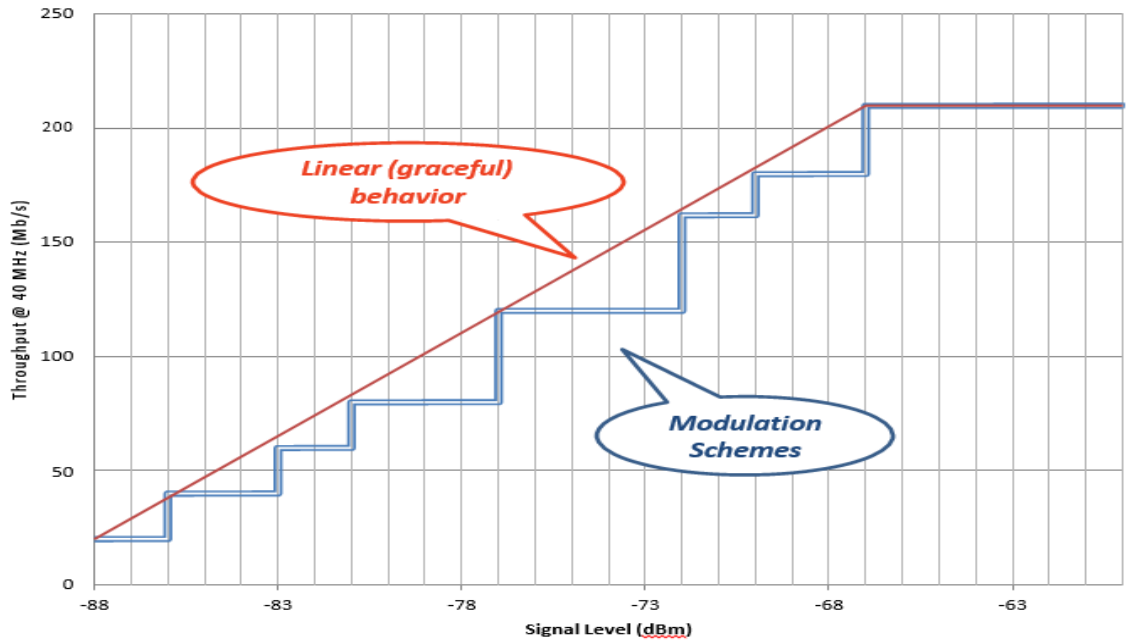


Figure 33:Evolution du débit en fonction de la modulation

c. Jitter Buffer

En configurant le Jitter Buffer, le jitter buffer récepteur pour chaque site peut être agrandi ce qui augmente la résistance aux interférences.

La diminution de Jitter Buffer diminue le retard du système. Jitter Buffer peut être configuré entre 2.1 et 16.0 millisecondes.

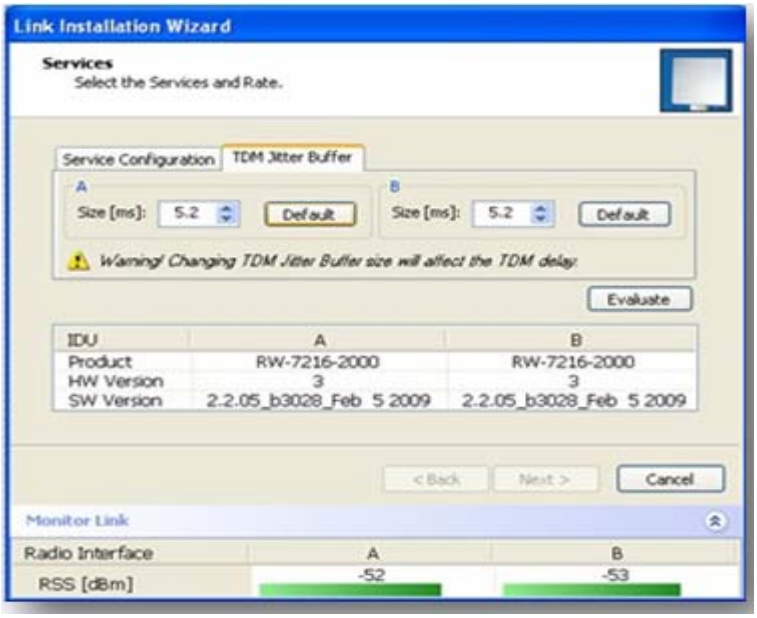


Figure 34:Configuration du Jitter Buffer

La mesure d'un système fiable repose en grande partie sur sa capacité de disponibilité des services offerts, de ce fait afin de se prémunir de certaines failles ou pannes, il est nécessaire de trouver des solutions pour la continuité d'activité.

2) Mise en place de la solution

L'implémentation d'une solution BLR dans un environnement urbain n'est pas aisée à cause des interférences et les nombreux obstacles dus à la taille des bâtiments et les nombreuses installations BLR existantes.

Dans un premier temps, la solution sera déployée sur quelques agences de Dakar à savoir Bourguiba, LSS, Zone Industrielle 1, Zone Industrielle 2 et Castor.

Afin de se prémunir, des éventuels dysfonctionnements nous allons mettre en place un système de redondance pour assurer la qualité des services.

a) Choix du type de liaison

La technologie RADWIN offre deux types de liaisons Point-to-Point et Point-to-Multipoint.

Le choix entre les deux dépend étroitement de l'environnement et des besoins en termes de débit. Ainsi, pour parer à toutes éventualités, la solution Point-to-Point bien qu'étant plus onéreuse à déployer a été choisie.

1. *Justification*

Scénario 1 :

- Point-to-Multipoint

Le secteur est composé d'un HBS et de plusieurs HSU, de ce fait si le HBS tombe alors tous les sites appartenant au dit secteur cessent de fonctionner et le PRA est activé.

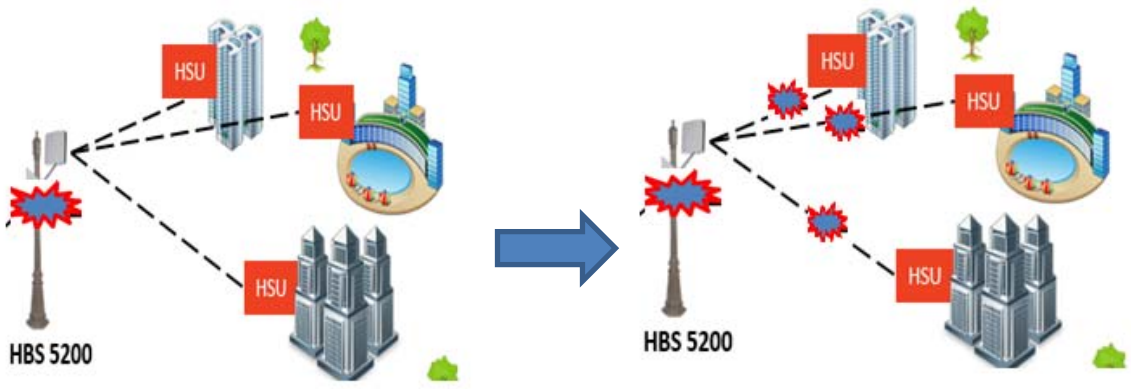


Figure 35:Architecture Point-to-Multipoint

Cette solution constitue cependant un choix très risqué du fait de la sensibilité des informations qui y seront envoyées.

- Point-to-Point

Les liaisons Point-to-Point sont toutes indépendantes les unes des autres .De ce fait, les perturbations survenues dans une des liaisons n'affectent en aucun cas les autres ce qui assure un SLA pour chaque liaison.

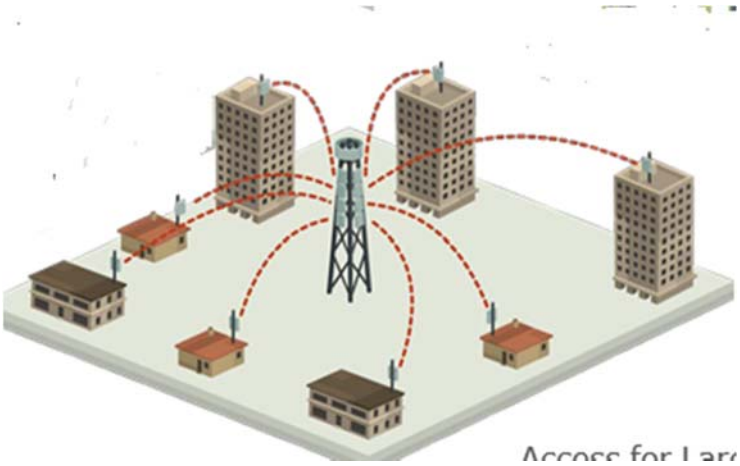


Figure 36: Architecture Point-to-Point

b) Cahier de Charges

Les différentes études qui ont été menées sur le terrain et grâce à l'outil de simulation Radio Planner ont permis de définir la hauteur de chaque antenne et de mesurer les interférences pour ainsi avoir les débits théoriques. A cet effet, les équipements qui seront utilisés ont été choisis selon les besoins et sur la base des résultats des simulations.

Le tableau ci-dessous renseigne la liste des équipements utilisés.

INTERCONNEXION : LIAISONS POINT A POINT

N°	Désignation	Quantité	N° Série
	Siège		
1	**ODU** RADWIN 5.8 GHz 2000 C série, 200Mbps, antenne incorporée	03	
2	Alimentation POE: 100-240VAC nominal range. 90-264VAC max range	03	
3	**IDU** (IP, E1 ou IP+E1) RADWIN 5.8 GHz 2000 C série ; 200Mbps	03	L2110109429
4	Hub Site Synchronization (HSS)	01	
5	**Pylône** ST30, 18m haubané	01	
	Kermel		
6	**ODU** RADWIN 5.8 GHz 2000 C série, 200Mbps, antenne incorporée	01	
7	**IDU** (IP, E1 ou IP+E1) RADWIN 5.8 GHz 2000 C série ; 200Mbps	01	
8	Alimentation POE: 100-240VAC nominal range. 90-264VAC max range	01	
9	**Pylône** ST15 24m; Paratonnerre; parafoudres	01	
	Agence Zone Industrielle 1		
10	**ODU** RADWIN 5.8 GHz, 2000 A10-Série ; 10 Mbps	01	
11	**IDU** RADWIN 2000 Série A10 ; 5.8 GHz, 10 Mbps	01	

12	Antenne Directionnelle à Polarisation Double 5.8 GHz: Antenne RADWIN de 23 dBi	01	
13	Alimentation POE: 100-240VAC nominal range. 90-264VAC max range	01	
13	Hub Site Synchronization (HSS)	01	
14	**Pylône** ST15 24m; Paratonnerre; parafoudres ; balise nocturne	01	
	Agence Zone Industrielle 2		
15	**ODU** antenne intégrée RADWIN 5.8 GHz, 2000 A10-Série ; 10 Mbps	01	
16	**IDU** RADWIN 2000 Série A10 ; 5.8 GHz, 10 Mbps	01	
17	Alimentation POE: 100-240VAC nominal range. 90-264VAC max range	01	
18	Hub Site Synchronization (HSS)	01	
19	**Pylône** ST15 24m; Paratonnerre; parafoudres ; balise nocturne	01	
	Agence L S Senghor		
20	**ODU** antenne intégrée RADWIN WINLINK 1000 (Radwin Séries: A, B ou C)	01	
21	**IDU** RADWIN WINLINK 1000 (IP, E1 ou IP+E1)	01	L2110109424
22	Alimentation 100 – 240VAC	01	
23	**Pylône** ST15 12m	01	
	Agence Bourguiba		
24	**ODU** antenne intégrée **RADWIN 5000** (Radwin Séries: A, B ou C)	01	01
25	**IDU** RADWIN 5000 (IP, E1 ou IP+E1)	01	L2110109433
26	Alimentation 100 – 240VAC	01	
27	**Pylône** 12m,	01	
	Agence Point E		
28	**ODU** antenne intégrée RADWIN 5.8 GHz, 2000 A10-Série ; 10 Mbps	01	

29	**IDU** (IP, E1 ou IP+E1) RADWIN 5.8 GHz 2000 C série ; 200Mbps	01	
30	**Pylône** ST15 30m	01	
31	Alimentation 100 – 240VAC	01	

c) Schéma R-Planner

Suite à l'étude théorique sur les aspects techniques des produits RADWIN, nous avons modélisé sur R-Planner le synoptique radio afin de pouvoir estimer les débits théoriques attendus.

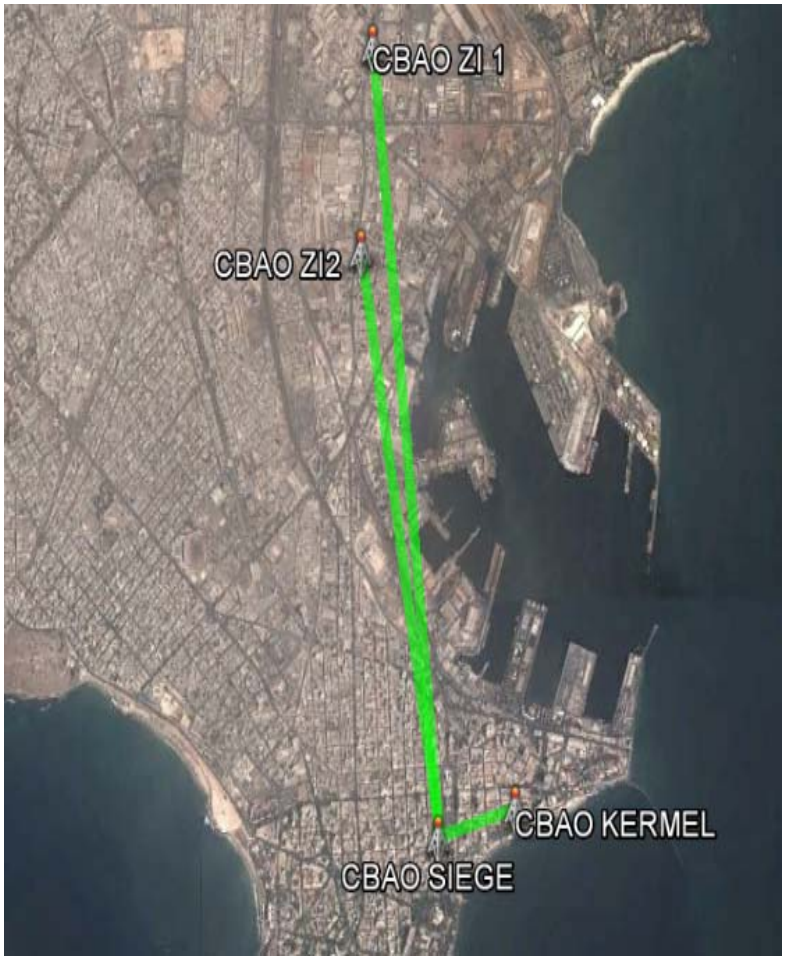


Figure 37:Synoptique Installation BLR

d) Bilan :

La rationalisation des couts télécoms est une étape importante dans l'optimisation des charges des DSI.

L'installation des BLR a été pensée avec un modèle de financement très souple dont les couts seront amortis sur une période de 5 ans. Comparés aux liaisons louées qui non seulement offrent des débits faibles mais aussi coutent chères, l'investissement sur la BLR constitue une solution rentable.

Conclusions et Perspectives

Au cours de ce travail, nous avons eu à étudier le mode de fonctionnement de plusieurs services notamment la monétique afin de déceler des dysfonctionnements pour ainsi apporter des solutions d'optimisation En effet, dans un premier temps, nous avons eu à étudier les manquements du système de supervision des équipements monétiques existant suivant deux approches ; approche technique et approche organisationnelle. A partir des résultats, nous avons à la modélisation et à l'implémentation d'une solution proposée afin de répondre convenable aux besoins de la banque à savoir une supervision efficace pour ainsi mieux gerer leur parc.

En second , il a été question de procéder à un trouble-shooting des liaisons VPN des points dédiés Western Union pour pouvoir situer l'origine des lenteurs constatés sur le traitement des requêtes afin de pouvoir solutionner le problème à travers des configurations qui ont été effectuées .A cet effet , une politique de discrimination de trafic & été adopté pour augmenter la qualité de service tout en assurant la sécurité des données .

Dans une dynamique de création de nouveaux services d'accroissement exponentiel des besoins et des exigences en termes de ressources et la rationalisation des couts, il est devenu nécessaire voire inéluctable de trouver une solution alternative d'interconnexion.

Pour ce faire, dans la dernière partie de notre travail, nous avons eu à procéder à l'étude de la mise en place d'une infrastructure BLR (Boucle Locale Radio) pour l'interconnexion des sites de Zone Industrielle 1 et 2,Bouguiba,Castor,Kermel, Léopold Sédar Senghor et Siege .Ainsi, à la suite de cet étude, notre choix s'est porté sur les produits RADWIN qui non seulement offre des débits élevés mais sont à coût moindre. Et en dernier lieu, nous avons eu à faire des simulations sur l'outil R-Planner pour les sites de Zone Industrielle 1,2, Kermel et Siege.

Les résultats de cette simulation nous ont permis d'avoir un meilleur aperçu des caractéristiques des équipements pour ainsi dresser un cahier de charges pour tous les sites concernés.

Perspectives

Les conditions de rédaction de ce mémoire ne nous a pas permis d'avoir une approche plus fine des systèmes d'exploitation utilisées par le SI Monétique .De ce fait, toutes les possibilités qu'offre notre système de supervision n'ont pas été exploités à fond .Ainsi, dans un avenir proche, nous envisageons d'affiner certaines parties de ce mémoire et mettre en place des mécanismes pour une meilleure gestion des équipements :

- Système de prise en main des équipements supervisés qui sera intégré dans EON
- Système de déploiement d'applications
- Gestion de parc
- Création de deux serveurs « satellite » ou secondaires qui seront chargés uniquement de gérer les TPE et les équipements réseaux.

Références

[1] [En ligne]. Available: http://www.cbao.sn.

[2] [En ligne]. Available: http://wikipedia.org.

[3] [En ligne]. Available: http://www.frameip.com.

[4] M. Corpus, «Introduction_a_la_supervision_dans_l_univers_Nagios_v1-0,» 2011.

[5] P. NIANG, «Mécanismes de Classification et de Marquage de trafic (Classification and Marking)».

[6] F. X. DIOP, «Solution Globale sur la Congiruation des ACLs».

[7] A. Leduc, «EON - Configuration et administration d'un logiciel de supervision reseau».

[8] RADWIN, RW2000 Francais V1.0.

[9] RADWIN, RADWIN Product Portfolio Francais v1.32.

Liste des Acronymes

ACL : Access Control List	**MIR** : Maximum Information Rat
ADSL: Asymetrical Digital Subscriber Line	**ODU** : Output Data Unit
ARQ : Automatic Repeat Request	**OID** : Object Identifier
ATM: Asynchronous Transfer Mode	**OFDM**: Orthogonal Frequency Division Multiplexing
BLR : Boucle Locale Radio	**PC** : Pentium Compact
CPU; Core Processor Unit	**PHB** : Per Hop Behaviour
DAB: Distributeur Automatique de Billets	**POE** : Power Over Ethernet
DEA : Diplôme d'Etude Appliquée	**PRA** : Plan de Reprise d'Activité
DES : Data Encryption System	**QOS** : Quality Of Service
DMZ : Dimilitarized Zone	**QIQ** : Queue in Queue
DSI : Direction des Systèmes d'Information	**QPSK** : Quadrature Phase Shift Keying
DUES : Diplôme Universitaire d'Enseignement Supérieur	**RETEL** : Réseaux et Télécoms
EON : Eyes Of Network	**RFC** : Requests For Comment
GAB: Guichet Automatique de Banque	**RNIS** : Réseau Numérique à Intégration de Services
GDG: Gestionnaire de GAB	**RTC** : Réseau Téléphonique Commuté
GIM: Groupe Interbancaire de l'UEMOA	**SHA** : Secure Hash Algorithm
GPRS: General Packet for Radio Service	**SI** : Système d'Information
HBS : Hub Base Station	**SIM** : Subscriber Information
HSS : Hub Synchronization System	**SIR** : Systéme d'Information Réparti
IDU : Input Data Unit	**SLA** : Service Level Agreement
IETF :Internet Ingeneering Task Force	**SMPT** : Simple Mail Transfer Protocol
IP : Internet Protocol	**SMS** : Short Messages Services
IPS : Intrusion Preventive System	**SNMP** : Simple Network Management Protocol
LAN : Local Area Network	**SU** : Station Unit
LOS : Line Of Sight	**TDD** : Time Division Duplex
	TDM : Time Division Multiplexing
	TDMA : Time Division Multiple Access

NLOS : Non Line Of Sight **LS** : Liaison Spécialisée **MPLS** : Multi-Protocol Label Switching **MAN** : Metropolitan Area Network **MD5** : Message Digest 5 **MIB**:Management Information Base **MIMO**: Multiple Input Multiple Output	**TPE** : Terminal de Paiement Electronique **UDP** : User Datagram Protocol **USB** : Universal Serial Bus **VLAN** : Virtual Local Area Network **VPN** : Virtual Private **VSAT** : Very Small Aperture Terminal

Annexe 1

Installation de EyesOfNetwork

L'installation de EyesOf Network n'est pas très difficile en soit mais assez longue, qui est basée sur le système de CentOS.
Pour télécharger l'ISO, il faut se rendre à cette adresse:
http://www.eyesofnetwork.com/?page_id=48&lang=fr.

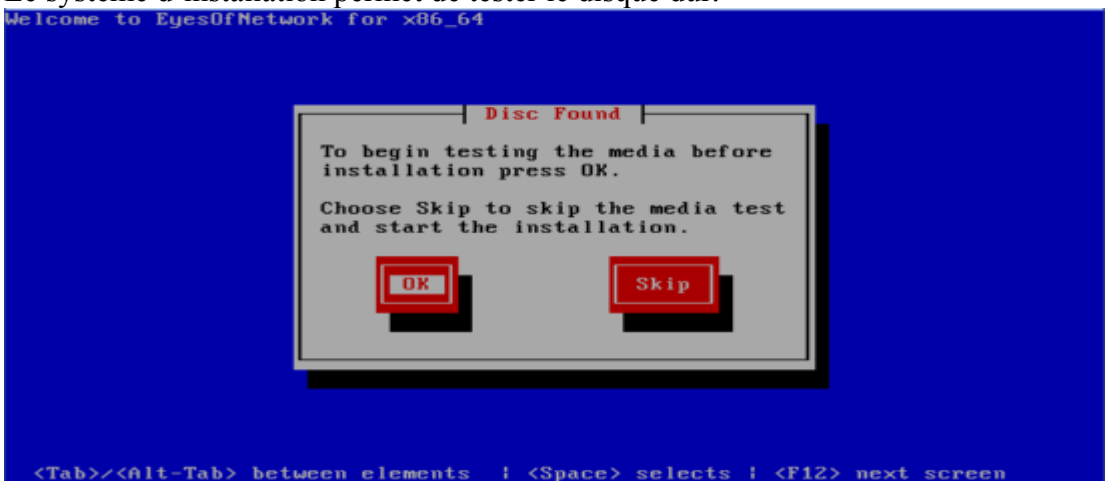
Une fois booté sur le CD d'installation d'EON, on arrive sur un menu, qui permet:

- Installer ou mettre à jour EON
- Installer le système avec un pilote vidéo basic
- Réparer le système installé
- Démarrer sur le disque dur local
- Tester la mémoire

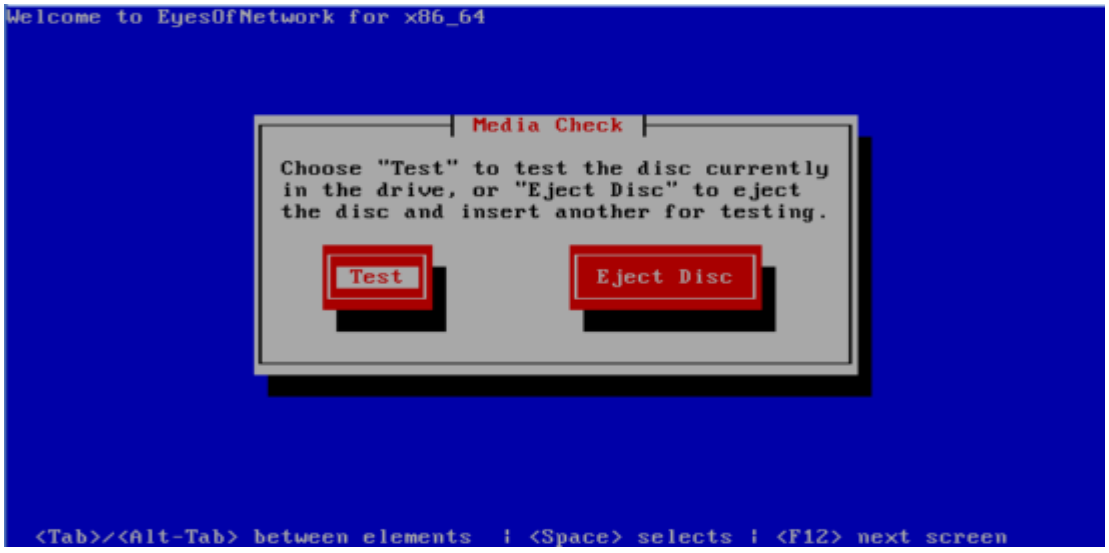
Dans notre cas, on va installer EON.



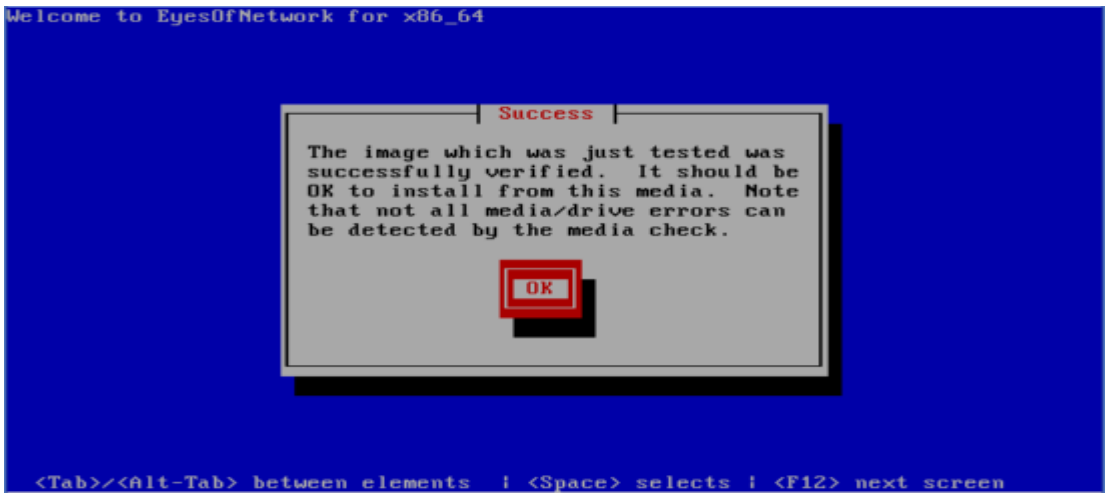
Le système d'installation permet de tester le disque dur.

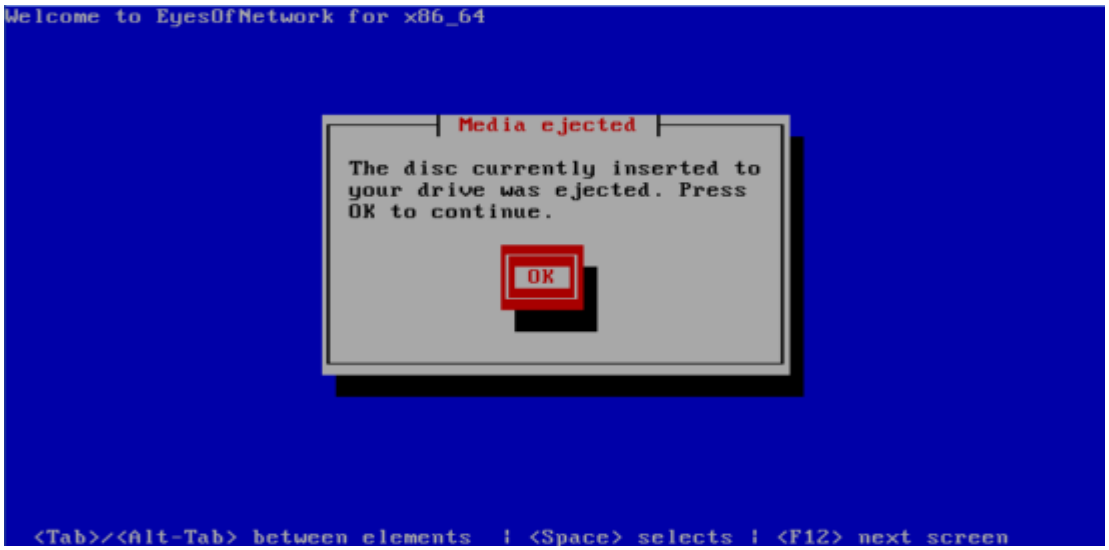


De tester aussi le CD.



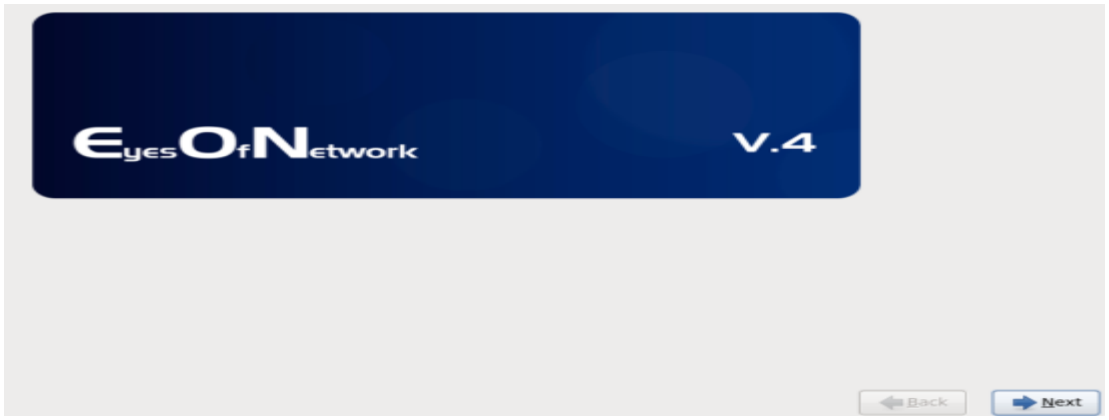
Une fois les différents tests passés et validés, on peut passer à l'installation.







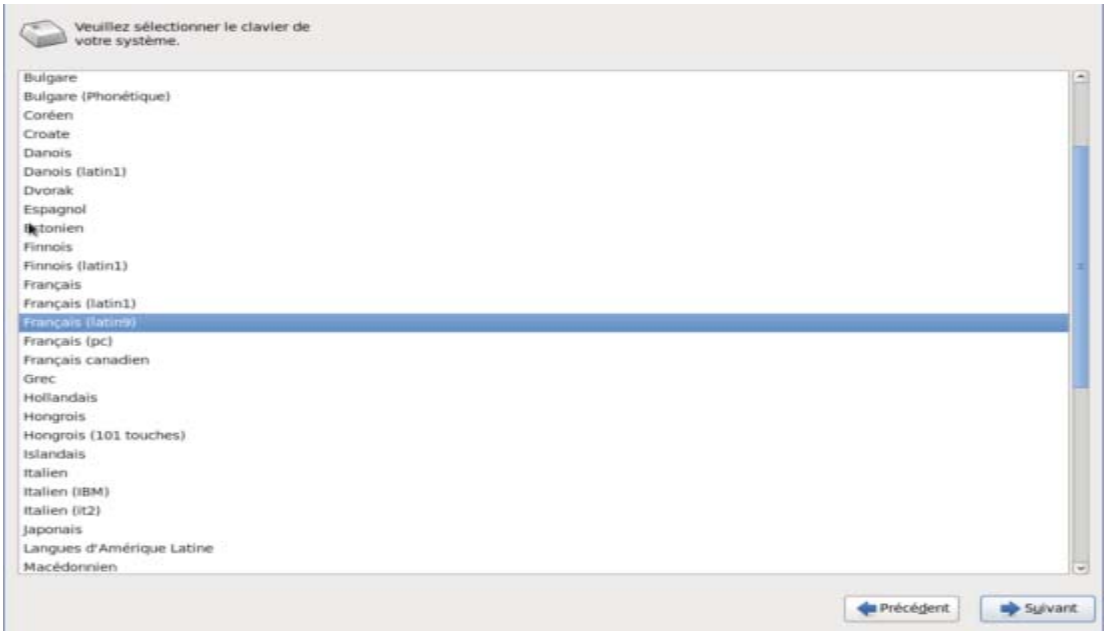
Pour passer à l'installation, on clique sur « Next ».



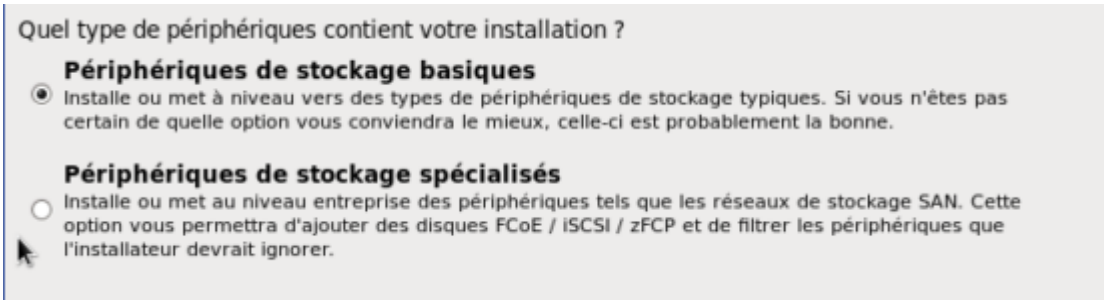
Le classique choix de la langue.



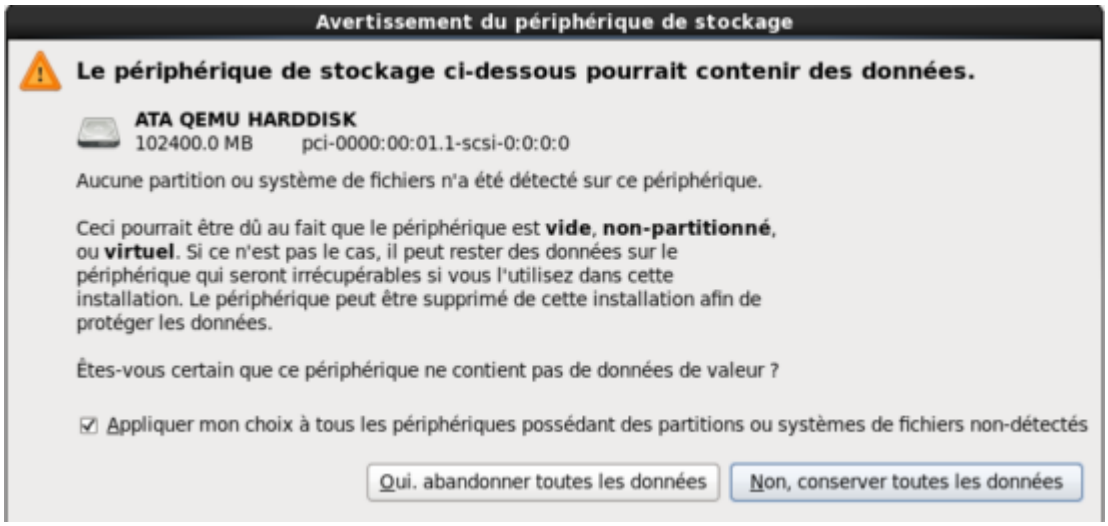
Le choix du type de clavier



Le choix du stockage.



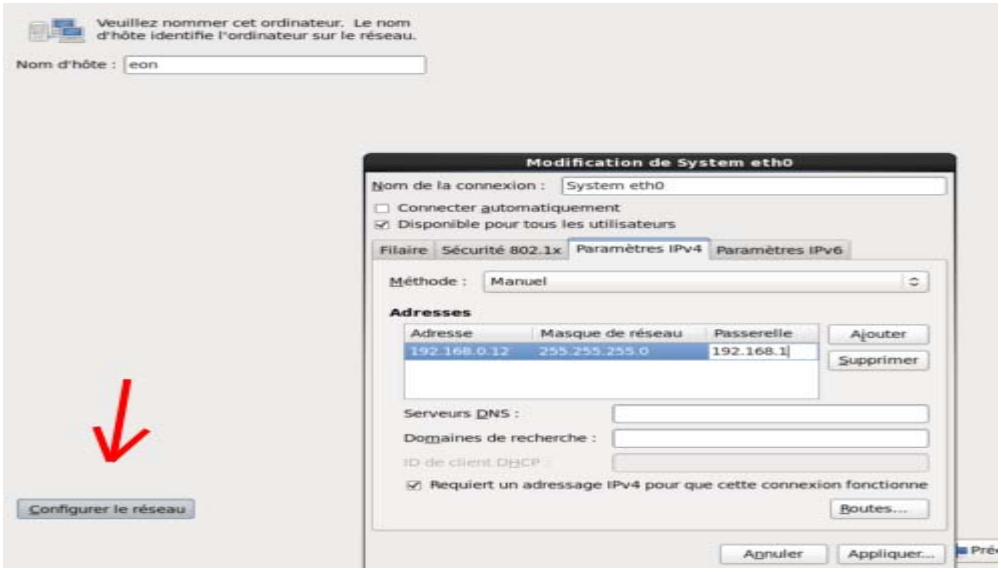
Après avoir choisi le stockage, un petit message d'alerte pour bien être sûr du choix.



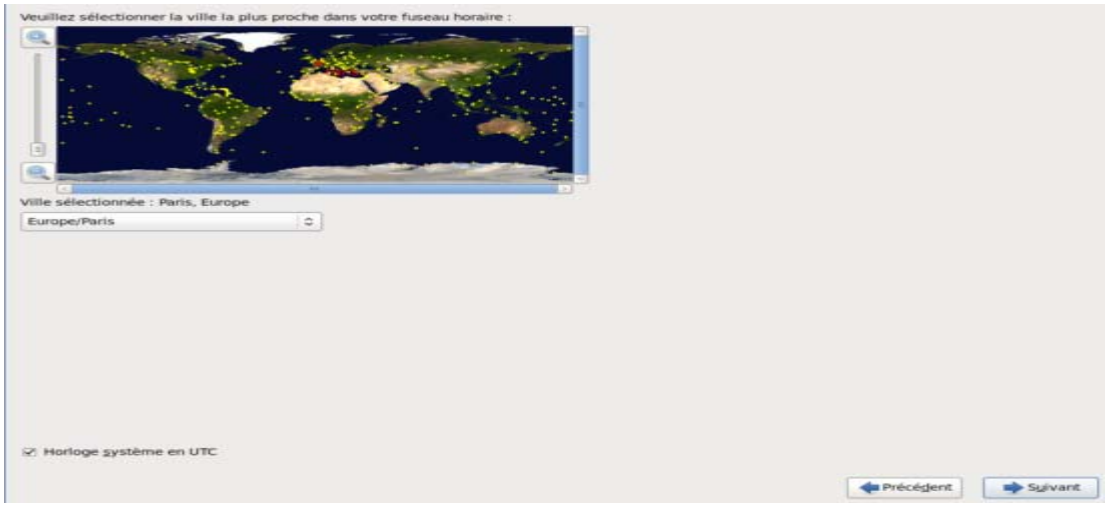
Le choix du nom d'hôte.



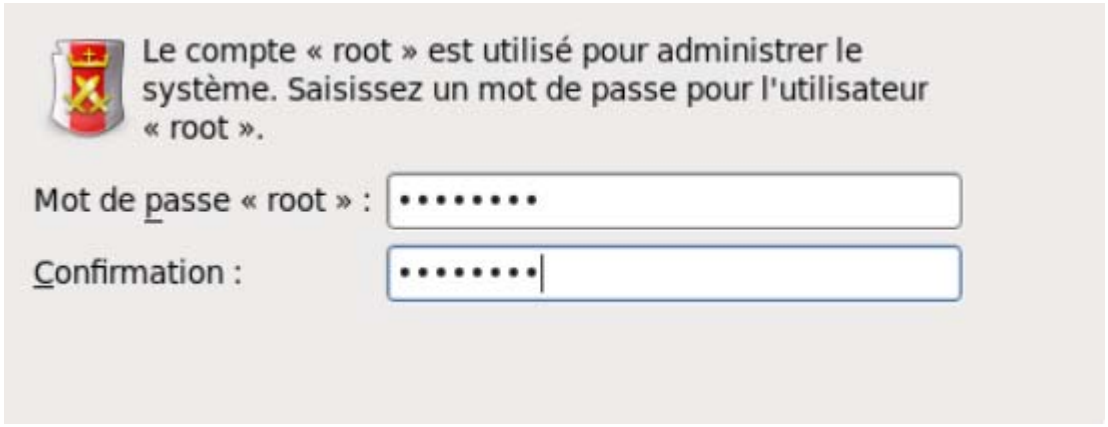
A cette étape, il est possible de paramétrer le réseau.



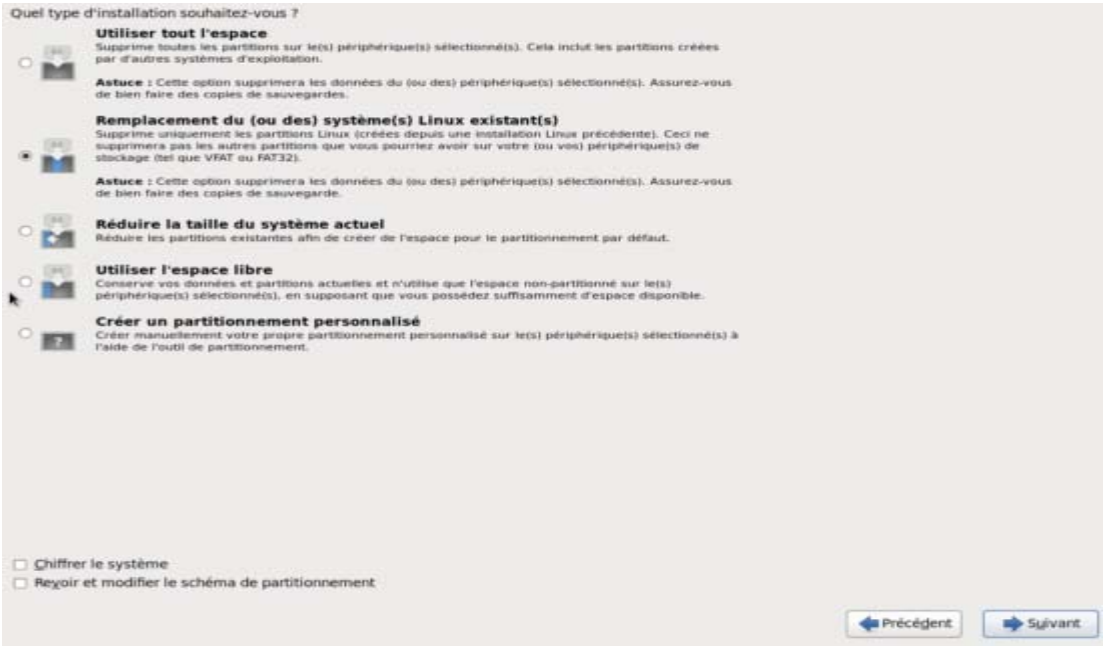
Le fuseau horaire.



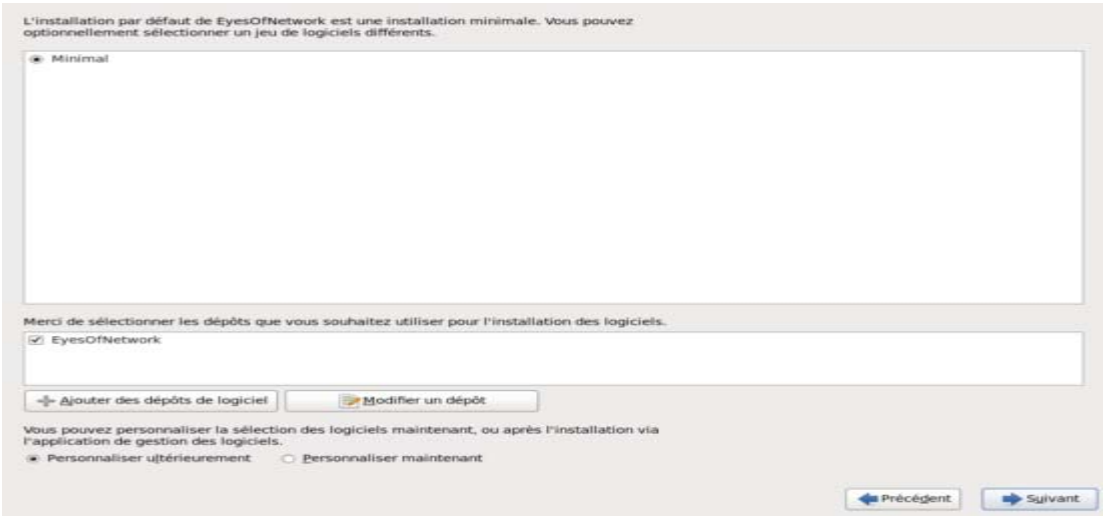
Saisir le mot de passe du compte root.



Le type d'installation.



Ajout ou pas de dépôts logiciels en plus.



Installation en cours.



Fin d'installation et reboot du système.



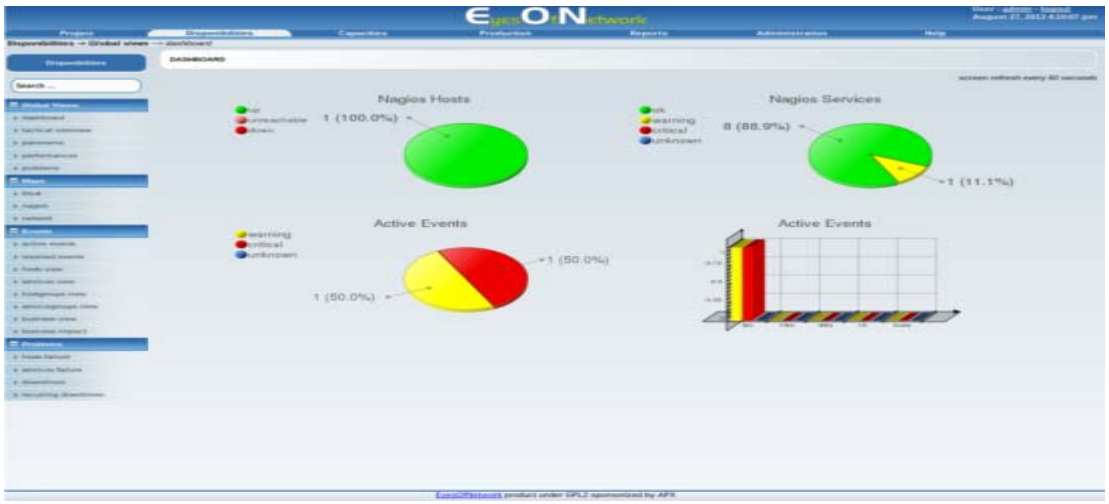
Lors du redémarrage, dans mon cas j'ai dû activer l'interface réseau avec un « ifup eth0″



Saisir l'adresse IP dans un navigateur pour se rendre sur EON.
Se connecter avec l'identifiant par défaut:
login: admin:
password: admin



Nous voilà arrivé sur le tableau de bord.



A ce stade, il faut paramétrer l'ensemble des outils par rapport à son réseau. [6] [9]