République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER PROFESSIONNEL

En
Informatique

Option
Administration et Sécurité des Réseaux

Thème

Mise en place d'une solution de monitoring et d'optimisation d'un réseau local cas : NAFTAL District Carburant de Béjaïa

Réalisé par :

Mlle. BENNAI Nawel

Mlle. ZIDELKHIL Nawal

Soutenu devant le jury composé de :

Encadreur	**M SIDER Abderrahmane**	**Maître de conférence B**	**U. A/Mira Bejaia.**
Présidente	**M AZNI Mohammed**	**Maître de conférence A**	**U. A/Mira Bejaia.**
Examinatrice	**Mme GASMI Badrina**	**Maître de conférence A**	**U. A/Mira Bejaia.**

Promotion 2015-2016

⁕ Remerciements ⁕

Ce travail n'aurait pas pu être accompli sans l'aide précieuse et les conseils encourageants de nombreuses personnes.

Nous rendons grâce au Seigneur tout puissant, à qui revient le mérite de toute reconnaissance.

Nos plus profonds remerciements vont à nos parents. Tout au long de notre cursus, ils nous ont toujours soutenus, encouragés et aidés. Ils ont su nous donner toutes les chances pour réussir. Qu'ils trouvent, dans la réalisation de ce travail, l'aboutissement de leurs efforts ainsi que l'expression de notre plus affectueuse gratitude.

Nous adressons nos remerciements à Monsieur TALALBIRE Fatsah , notre encadreur et chef de département Informatique du District Carburant Naftal de Béjaïa pour nous avoir permis d'effectuer notre stage au sein de son département.

Nous adressons également nos remerciements les plus chaleureux à notre Co-encadreur Mr SEKHRIOU Noureddine, pour sa disponibilité et pour tous les conseils qu'il nous a prodigué tout au long de notre période de stage.

Nous exprimons nos reconnaissances à notre encadreur académique Mr Sider.A , pour sa disponibilité, et son envie de toujours vouloir transmettre son savoir à ses étudiants. Qu'il trouve ici l'expression de notre profonde gratitude.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche, en acceptant d'examiner notre travail et de l'enrichir par leurs connaissances.

Nos remerciements à toute notre famille et à nos amies et camarades de promotion pour les bons et les mauvais moments passés ensemble.

Un grand Merci à tous ceux que nous avons omis de citer ici, et qui ont contribué d'une façon ou d'une autre, dans ce travail.

⁂ *Dédicaces* ⁂

Toutes les lettres ne sauraient trouver les mots qu'il faut, Tous les mots ne sauraient exprimer la gratitude, l'amour, Le respect, la reconnaissance, Aussi, c'est tout simplement que je dédie ce travail :

Au meilleur des papas, autant de phrases et d'expressions aussi éloquentes soit-elles ne sauraient exprimer ma gratitude et ma reconnaissance. Tu as su m'inculquer le sens de la responsabilité, de l'optimisme et de la confiance en soi face aux difficultés de la vie.

À Ma tendre Mère Ghania : Tu représentes pour moi la source de tendresse et l'exemple de dévouement qui n'a pas cessé de m'encourager. Tu as fait plus qu'une mère puisse faire pour que ses enfants suivent le bon chemin dans leur vie et leurs études.

Je Vous dois ce que je suis aujourd'hui et ce que je serai demain et je ferai toujours de mon mieux pour rester Votre fierté et ne jamais Vous décevoir. Que Dieu le tout puissant Vous préserve, vous accorde santé, bonheur, quiétude de l'esprit et Vous protège de tout mal.

À mes adorables sœurs pour leurs tendresses, leurs complicités et leurs présences.

À mes chers frères pour leur soutien et leurs conseil, en particulier mon petit frère yugou.

À mes beaux-frères et belles sœurs.

Que Dieu leur apporte le bonheur, les aide à réaliser tous leurs vœux et leur offre un avenir plein de succès.

À Aimen qui n'a pas cessée de me conseiller, encourager et soutenir tout au long de mes études. Que Dieu le protège et lui offre la chance et le bonheur.

À mes neveux : Ilyane , adem et yani à qui je souhaite un avenir radieux pleins de réussite.

À toute ma grande famille qui m'a permis de vivre dans un environnement serein et paisible.

À mes Chères amie : Hadjer, Kenza, mounia, sabah, feriel et aldjia en témoignage de l'amitié qui nous uni et des souvenirs de tous les moments passée ensemble , je vous dédie ce travail et je vous souhaite une vie plein de santé et de réussite.

À ma chère et douce binôme Nawal, qui a eu la patience de me supporter durant ce mémoire, et qui m'a soutenu et encouragé pendant tous les moments difficiles vécus.

À toute personne ayant contribué de près ou de loin à la réalisation de ce travail.

Mlle. BENNAI Nawel

⁂ *Dédicaces* ⁂

Je commence par rendre grâce à DIEU et à sa bonté, pour la patience, la compétence et le courage qu'il m'a donné pour arriver à ce stade.

Avec tout mon amour éternel et avec l'intensité de mes émotions. Je dédie ce mémoire :

À mon cher père, l'amour qui m'a donner,sans oublier ses sacrifices ; Pour son encouragement : je te souhaite la joie et de bonne santé.

À celle qui m'a transmis la vie, l'amour, le courage, à toi chère maman toutes mes joies, mon amour et ma reconnaissance.

À mon frère FAYÇAL et sa femme FOUZIA : en témoignage de mon amour éternel que Dieu vous garde, vous protège et vous offre une vie pleine de joie et de réussite.

À ma sœur SONIA, son mari DJAMAL je vous souhaite une vie pleine de plaisir et de réussite et une bonne santé.

À mon neveu Aymen, ma plus grande source de bonheur, j'espère que la vie lui réserve le meilleur.

Vous avez toujours été là pour moi, m'entourant de votre bienveillance usant de tous les sacrifices possibles. Ce travail n'est que le fruit de vos soutiens, de vos prières, de votre amour profond. Je souhaite que ce mémoire vous apporte la joie.

À la mémoire de mon grand-père et grand-mère, qui ont été toujours dans mon esprit et dans mon cœur, je vous dédie aujourd'hui ma réussite. Que Dieu, le miséricordieux, vous accueille dans son éternel paradis.

À tous mes oncles et tantes, cousins et cousines sans exception ; pour votre sympathie, douceur et gentillesse. Je vous souhaite beaucoup de succès, de courage et de bonheur tant professionnel que familial.

À ma belle famille, beaux frères SOFIANE et AHMED , belles sœurs KENZA ET FAIZA et sans oublier mon fiancé ,je vous dédie ce travail en témoignage de mon affection et de mon amour incessant.

À mes adorables amies, Aldjia, Feriel, pour leur fidélité.

À ma chère binome Nawel ; avec lesquels j'ai partagé mes moments de joie et de bonheur Que toute personne m'ayant aidé de près ou de loin, trouve ici l'expression de ma reconnaissance.

Tous les mots que je pourrais utiliser seraient insuffisants pour vous témoigner l'amour que je vous porter. J'espère être à la hauteur de votre attente. Que dieu vous préserve et vous prête longue vie de joie.

Mlle. ZIDELKHIL Nawal

Table des matières

Table des matières i

Table des figures iv

Liste des tableaux vi

LISTE DES ABREVIATIONS vii

Introduction générale 1

1 État de l'art sur le monitoring réseau 2

1.1 Introduction . . . 2
1.2 Monitoring réseau . . . 2
1.2.1 Définition . . . 2
1.2.2 Types de surveillance et actions liées . . . 2
1.2.3 Objectifs . . . 3
1.3 Protocole SNMP . . . 3
1.3.1 Définition . . . 3
1.3.2 Principe du SNMP . . . 3
1.3.3 Fonctionnement de SNMP . . . 4
1.4 Quelques solutions de monitoring . . . 4
1.4.1 Présentations des logiciels de monitoring . . . 4
1.4.2 Étude comparative . . . 5
1.4.3 Choix de la solution . . . 6
1.5 Réseaux locaux virtuels (VLANs) . . . 7
1.5.1 Définitions . . . 7
1.5.2 Avantages offerts par les vlans . . . 7
1.5.3 Types de vlans . . . 7
1.6 Conclusion . . . 8

2 Présentation de l'organisme d'accueil 9
2.1 Introduction . . . 9
2.2 Présentation de l'entreprise de NAFTAL . . . 9
2.2.1 Historique . . . 9
2.2.2 Activités principales de l'entreprise . . . 10
2.2.3 Organisation de la branche CBR . . . 11
2.2.4 Description et rôle de chaque département au sein du district CBR Béjaïa 11
2.3 Présentation du département informatique . . . 14
2.3.1 Organigramme du département informatique . . . 14
2.3.2 Description et rôle de chaque service du département informatique . . . 14
2.4 Architecture réseau du district CBR . . . 16
2.4.1 Parc informatique . . . 17
2.4.2 Applications de l'entreprise . . . 17
2.5 Contexte du projet à réaliser . . . 18
2.5.1 Présentation du projet . . . 18
2.5.2 Objectif du projet à réaliser . . . 18
2.5.3 Problématique . . . 18
2.5.4 Solution proposée . . . 21
2.6 Conclusion . . . 22

3 Présentation des outils mis en œuvre 23
3.1 Introduction . . . 23
3.2 VMWare . . . 23
3.3 PRTG . . . 25
3.3.1 Service SNMP . . . 25
3.3.2 Installation du PRTG . . . 27
3.4 Protocole DHCP . . . 29
3.4.1 Définition . . . 30
3.4.2 Rôle du DHCP . . . 30
3.4.3 Avantages du protocole DHCP . . . 30
3.5 Listes de contrôle d'accès (ACL) . . . 31
3.5.1 Définition . . . 31
3.5.2 Rôle d'une ACL . . . 31
3.5.3 Caractéristiques d'une ACL . . . 31
3.5.4 Types de listes d'une ACL . . . 32
3.6 GNS3 . . . 33
3.6.1 Définition . . . 33
3.6.2 Installation de GNS3 . . . 33

3.6.3 Configuration de GNS3 35
3.7 Conclusion 37

4 Réalisation 38
4.1 Introduction 38
4.2 Topologie sous GNS3 sans VLAN 38
4.3 Configuration du routeur sans VLANS 42
4.3.1 Affectation de l'addresse IP et activation du SNMP 42
4.3.2 Configuration du dhcp 43
4.4 Vérification et test de connectivité sans VLAN 43
4.4.1 Vérification de la configuration 43
4.4.2 Test de connectivité 45
4.5 Topologie sous GNS3 avec VLAN 47
4.6 Configuration des commutateurs 49
4.7 Configuration du routeur avec VLAN 49
4.7.1 Configuration du protocole DHCP 49
4.7.2 Ajout d'une ACL 51
4.8 Vérification et test de connectivité avec VLAN 52
4.8.1 Vérification de la configuration 52
4.8.2 Test de connectivité 53
4.9 Configuration du PRTG 55
4.9.1 Page d'accueil 55
4.9.2 Ajout d'un groupe 55
4.9.3 Ajout des équipements 56
4.9.4 Ajout des capteurs 58
4.10 Surveillance du réseau avant et après les vlans 61
4.10.1 Avant les vlans 61
4.10.2 Après les vlans 63
4.11 Conclusion 66

Conclusion et perspectives 67

Bibliographie 67

Table des figures

1.1 Fonctionnement du SNMP 4

2.1 Organigramme du District CBR de Béjaïa 11
2.2 Organigramme du département informatique 14
2.3 Organigramme du service Système & Réseau 15
2.4 Organigramme du Service Information de Gestion 16
2.5 Réseau de Naftal détaillé 16
2.6 États des switch 19
2.7 Surveillance des switchs en 2jours 20
2.8 Surveillance des switchs en 30jours 20
2.9 Surveillance du réseau en 2 heures 21
2.10 Surveillance du réseau d'une semaine 21

3.1 Interface de notre machine virtuelle 24
3.2 Icône de windows server 2012 25
3.3 Activation du SNMP au niveau des switchs 25
3.4 Gestionnaire de serveur 26
3.5 Installation de SNMP 26
3.6 Connexion au PRTG 27
3.7 Page d'accueil 28
3.8 Menu du PRTG 28
3.9 Alertes du PRTG 29
3.10 Interface de gns3 34
3.11 Préférences dans GNS3 35
3.12 La virtualbox de GNS3 36
3.13 GNS3 - IOS Image 37

4.1 Topologie sous GNS3 sans VLAN 38
4.2 Configuration de la vmnet 39
4.3 Configuration de la carte réseau vmnet1 40
4.4 Configuration du serveur 40

4.5 Affectation d'un IP et activation de SNMP 42
4.6 Configuration du dhcp 43
4.7 Vérification résussite 44
4.8 Affectation de l'adresse ip à la Vmnet1 45
4.9 Ping entre le PC9 et le PC2 46
4.10 Topologie de notre réseau avec VLAN 47
4.11 Configuration du DHCP 50
4.12 DHCP pools 50
4.13 Sous interfaces du routeur 51
4.14 Ajout d'une ACL 51
4.15 Affectation d'une adresse IP par le DHCP au PCs 52
4.16 Affectation d'une adresse IP par le DHCP au serveur 53
4.17 Routage inter-vlan avant et après 54
4.18 Ping du PC1 vers le serveur 54
4.19 Ping du serveur vers le PC1 54
4.20 Page d'accueil du PRTG 55
4.21 Ajout du groupe surveillance 56
4.22 Ajout de l'équipement routeur 57
4.23 Vue l'ensemble de l'équipement routeur 58
4.24 Bibliothèque de PRTG 59
4.25 Ajout d'un capteur PING 59
4.26 Détails du PING 60
4.27 Ajout d'un capteur bande passante 61
4.28 Surveillance du PING en temps réel 62
4.29 Surveillance du switch pendant 2 jours 62
4.30 Surveillance de la bande passante 63
4.31 Capteur de PING avec les vlans 63
4.32 Surveillance du switch en 2 jours 64
4.33 Surveillance de la bande passante en temps réel 64
4.34 Détail du trafic 65
4.35 Surveillance de la bande passante 65
4.36 Rapport du PING 66

Liste des tableaux

1.1 Tableau comparatif entre les outils de monitoring réseau 6

2.1 Environnement client 17

4.1 Liens manuels sans les vlans 41
4.2 Lien manuel du serveur sans VLAN 42
4.3 Liens manuels avec les VLAN 48
4.4 Lien manuel du serveur avec VLAN 49

LISTE DES ABREVIATIONS

A	
ACL	**Acces Control List**
B	
BOOTP	**BOOTstrap Protocol**
C	
CBR	**CarBuRant**
CLP	**Carburant Lubrifiant Pneumatique**
D	
DHCP	**Dynamic Host Configuration Protocol**
E	
ERDP	**Entreprise de Raffinage et de Distribution de produits Pétroliers**
F	
FTP	**File Transfer Protocol**
G	
GNS	**Graphical Network Simulation**
GPL	**Gaz Pétrole Liquifié**
I	
ICMP	**Internet Control Message Protocol**
IEEE	**Institute of Electrical and Electronics Engineers**
INF	**INFormatique**
IOS	**Internetworking Operating System**
IP	**Internet Protocol**

IPX	**Internetwork Packet eXchange**
ISO	**Internationnal Standardization for Organization**
L	
LAN	**Local Area Network**
M	
MAC	**Media Access Control**
MIB	**Management Information Base**
O	
OSC	**Oeuvre Sociales et Culturelles**
P	
PC	**Personal Computer**
PRC	**Prime de Rendement du Collectif**
PRTG	**Paessler Router Traffic Network**
S	
SNMP	**Simple Network Management Protocol**
T	
TCP/IP	**Transmission Control Protocol / Internet Protocol**
U	
UND	**Unité NAFTAL de Distribution**
V	
VLAN	**Virtual Local Area Network**
VMnet	**Virtual Machine network**
VM	**Virtual Machine**

Introduction générale

Aujourd'hui l'outil informatique constitue le nerf de la guerre économique, tenant compte de toutes les taches qui gèrent avec rapidité, efficacité. Il permet aux administrateurs d'entreprises de gérer à distance toutes leurs activités, ce qui a introduit de nouveaux besoins en ce qui concerne la supervision et l'administration des systèmes.

Le logiciel de supervision exploité dans notre travail est PRTG, un logiciel qui est basé sur le protocole SNMP, qui vérifie l'état du réseau ainsi que les machines connectées et permet à l'administrateur d'avoir une vue globale en temps réel de l'ensemble du parc informatique sous sa responsabilité. Il peut être même informé par email en cas de problèmes. Grâce à ce système, il peut donc intervenir et régler les différentes anomalies signalées en des délais fortement réduits.

Notre projet de fin d'étude consiste à exploiter le logiciel PRTG, le configurer, surveiller le réseau local du District Carburant NAFTAL de Béjaïa ,tirer les problèmes rencontrés et proposer une ou plusieurs solutions de résolution pour ces derniers.

Le présent travail est subdivisé en quatres grands axes :

- Le premier chapitre porte sur l'étude de l'organisme d'accueil,en faisant une étude sur son réseau, tirer la problématique et suggérer une solution.
- Le second chapitre concerne des généralités sur le monitoring réseau ainsi que sur les réseaux locaux.
- Le troisième chapitre consiste à définir et installer les différents outils et logiciels mis en place.
- Enfin nous terminerons notre travail avec le dernier chapitre qui est la mis en œuvre de notre solution.

Chapitre 1

État de l'art sur le monitoring réseau

1.1 Introduction

L'objectif de ce chapitre est d'étudier les concepts de base du monitoring réseau. Pour cela, nous commencerons par une définition du monitoring,ses types et actions liées, nous parlerons en outre sur le protocole SNMP, son principe et fonctionnement, ensuite nous allons faire une étude comparative des différentes solutions de monitoring. Enfin, nous cloturons ce chapitre par une généralité sur les réseaux locaux.

1.2 Monitoring réseau

1.2.1 Définition

La supervision réseau (ou monitoring) comprend un ensemble de protocoles, matériels et logiciels informatiques permettant de suivre à distance l'activité d'un réseau informatique. Ces solutions permettent également de cartographier le réseau.La supervision est particulièrement adaptée pour des réseaux de plus de 50 machines et pour les prestataires de services.[7] Le principe général est le suivant :

- Des agents sont placés sur les équipements à surveiller.
- Un ou plusieurs serveurs centralisent les informations pour les afficher de manière cohérente aux techniciens ou aux administrateurs.

1.2.2 Types de surveillance et actions liées

Globalement, les outils de supervision sont utilisés pour la surveillance [24] :

- Matérielle (activité d'un équipement, charge, ...).

- Réseau (débit, latence, taux d'erreur, protocoles, sécurité ...).
- Système (performances, intégrité).
- Applicative (performances, modifications de configuration, analyse).

Les actions liées aux événements peuvent être :

- Un enregistrement dans un journal.
- Un tracé graphique.
- Une alerte.
- Une exécution de script pour automatiser les tâches à faire.

1.2.3 Objectifs

L'objectif d'une supervision de réseaux peut ainsi se resumer en trois points :

- Etre réactif en alertant l'administrateur (e-mail ou sms) en cas de dysfonctionnement d'une partie du systeme d'information.
- Etre pro-actif en anticipant les pannes possibles.
- Cibler le problème dès son apparition afin d'agir rapidement de la façon la plus pertinente possible.

1.3 Protocole SNMP

1.3.1 Définition

SNMP signifie Simple Network Management Protocol, il s'agit d'un protocole qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau à travers des paquets transmis de l'équipement au serveur SNMP.[26]

1.3.2 Principe du SNMP

Le SNMP est un protocole qui fonctionne dans un ensemble appelé " communauté " qui n'inclue une sécurité qu'à partir de la version 3. Dans cette " communauté " il y a les " agents " (Switchs, imprimantes : les éléments à surveiller) et l'élément charger de récupérer les informations envoyé par les " agents " : le " manager " (l'outil de supervision : PRTG, Nagios...).

1.3.3 Fonctionnement de SNMP

La communication entre les différents éléments de la " communauté " SNMP se fait avec un langage particulier, par le bais des fichiers MIB(Management Information Base) qui sont des fichiers d'interprétation, ils permettent au " manager " de comprendre les informations envoyé par les "agents".[26]
La figure suivante représente le fonctionnement du SNMP :

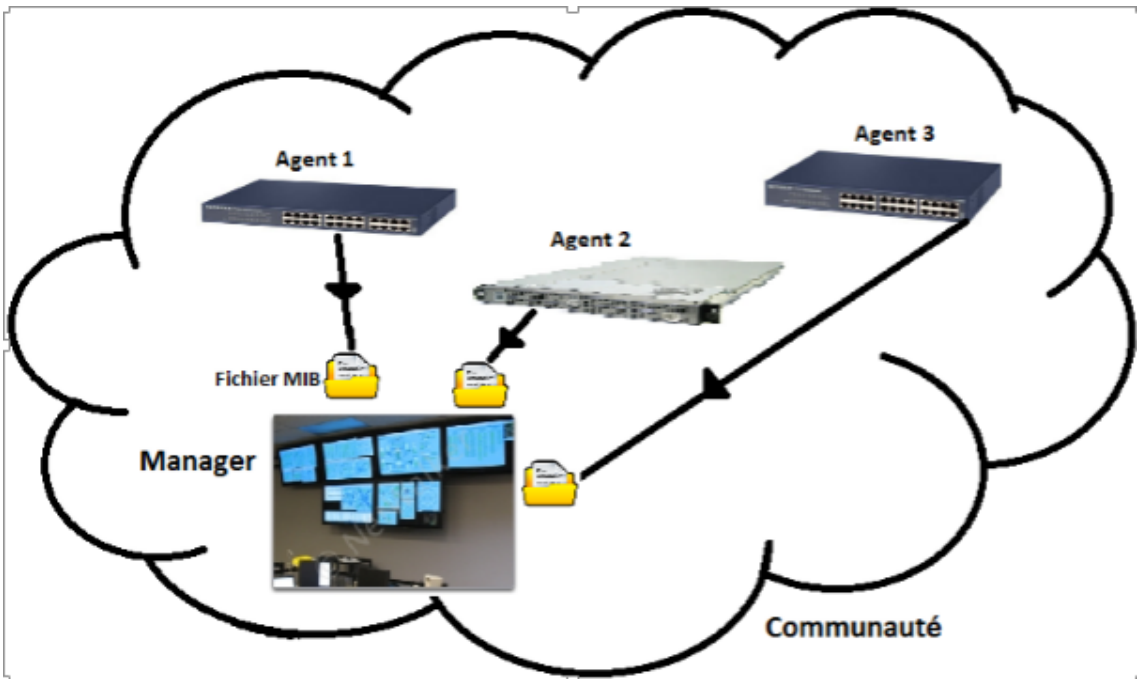


FIGURE 1.1 – Fonctionnement du SNMP

1.4 Quelques solutions de monitoring

Nous allons explorer quatres solutions de supervision qui se veulent assez complètes. Cette étude ressemble à un banc d'essai puisque pour chacun des logiciels nous allons faire une courte présentation et une étude comparative.

1.4.1 Présentations des logiciels de monitoring

Voici les quatres logiciels de monitoring[16] :

Zabbix : Zabbix est une solution de supervision open-source de plus en plus prisée. L'entreprise vise à faire de Zabbix un logiciel reconnu dans le milieu de la supervision et

créer une communauté autour de lui pour permettre une évolution plus rapide. A côté de cela, cette societé propose un service de maintenance commercial.

Nagios : Nagios est certainement le logiciel libre le plus connu dans le milieu de la supervision réseau. Appréciée des entreprises ainsi que des particuliers, cette application possède une très grande communauté qui participent activement au développement.

PRTG : PRTG est une solution de supervision de réseau en temps réel basé sur le protocole SNMP. Il permet au service informatique d'avoir une remonté d'information quasi instantané lors d'un problème. Malgré un système basé sur le SNMP, PRTG utilise d'autres protocoles ou ressources systèmes pour obtenir un maximum d'information sur les différents éléments du réseau.

Cisco Network Assistant : Cisco Network Assistant est une application de gestion de réseau, disponible pour OS X et Windows, optimisé pour les réseaux locaux filaires et sans fil pour les entreprises qui ont de plus en plus.
Cisco Network Assistant est gratuit et optimisé pour appliquer les services communs à tous les commutateurs Cisco, les routeurs, les contrôleurs sans fil et les points d'accès.

1.4.2 Étude comparative

Les solutions suivantes sont toutes basées sur le protocole Service Network Management Protocole(SNMP). Le tableau suivant représente une étude comparative que nous avons fait pour les quatres logiciels PRTG, Cisco Network Assistant, Nagios, Zabbix :

Outils	Avantages	Inconvénients
Nagios	Beaucoup de documentations sur le web[16] Plétore de plugins qui permettent d'étendre les possibilités (agents comme zabbix, reporting amélioré, etc...) [16]	La solution offre des fonctionnalités limitées[16] Interface non ergonomique et peu intuitive[16] Configuration fastidieuse via beaucoup de fichiers [16]
Cisco Network Assistant	Surveillance clair d'utilisation de bande passante	Aucune alerte sur la défaillance du matériel Fonctionnalités limités Logiciel basique peu utilisé et en voix de disparition.

Zabbix	Une interface vaste mais claire ; Compatible avec MySQL, PostgreSQL, Oracle, SQLite[16]	Interface est un peu vaste, la mise en place des templates n'est pas évidente au début : petit temps de formation nécessaire ; L'agent zabbix communique par défaut en clair les informations, nécessité de sécuriser ces données ; Commence à être connu, mais pas encore auprès des entreprises : Peu d'interfaçage avec d'autres solutions commerciales.[16]
PRTG	Une solution pour tous Surveillance réseau – Rapide, facile, évident PRTG Network Monitor fournit exactement les données que vous avez besoin clair, individuel et attractif Fournit toutes les informations importantes en un clin d'oeil Liste d'aperçu de toutes les sondes bande passante d'un LAN Sondes et protocoles Mises en alerte selon des critères individuellement définis	Coût de la licence PRTG Network Monitor dépend du nombre de capteurs désirés

TABLE 1.1 – Tableau comparatif entre les outils de monitoring réseau

1.4.3 Choix de la solution

Après avoir fait une étude comparative entre les logiciels de supervision des réseaux, le choix a été porté sur PRTG, car cette solution ayant le gros avantage de la simplicité d'utilisation et de configuration, tout en répondant aux demandes de l'entreprise.
De plus l'enreprise nous a convaincu d'utiliser ce logiciel de monitoring.

1.5 Réseaux locaux virtuels (VLANs)

1.5.1 Définitions

Un réseau local représente un système de communication locale reliant plusieurs ordinateurs.(serveurs, stations de travail et périphériques) permettant de transférer des données à des vitesses élevées, sur des courtes distances et dans les limites d'une enceinte privée.[15]

Un VLAN (Virtual Local Area Network, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLAN) il est possible de s'affranchir des limitations de l'architecture physique en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères.[21]

1.5.2 Avantages offerts par les vlans

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants [21] :

- Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs.
- Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées.
- Réduction de la diffusion du trafic sur le réseau.

1.5.3 Types de vlans

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue[21] :

Un VLAN de niveau 1 : aussi appelés VLAN par port, définit un réseau virtuel en fonction des ports de raccordement sur le commutateur.

Un VLAN de niveau 2 : également appelé VLAN MAC, VLAN par adresse IEEE ou en anglais MAC, consiste à définir un réseau virtuel en fonction des adresses MAC des stations.Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

Un VLAN de niveau 3 : on distingue plusieurs types de VLAN de niveau 3 : Le VLAN par sous-réseau : des sous-réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station.

Le VLAN par protocole : permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

1.6 Conclusion

Ce deuxième chapitre nous a permet d'avoir une idée bien claire sur le monitoring réseaux et comprendre mieux les raisons pour lesquelles les spécialistes en réseau ont élaboré les outils de supervision et surtout l'apport de ce dernier pour la supervision des réseaux locaux.

Dans le chapitre suivant, nous allons présenter les différents outils exploités dans notre projet.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

Pour mieux comprendre le problème détourné, nous avons pris un cas concret concernant l'unité Naftal District Carburants de Béjaïa , cette enquête nous permettra de vivre plus clairement la réalité des choses.Tout d'abord nous allons présenter l'entreprise NAFTAL en générale, son historique ensuite nous allons illustrer les départements existant au sein du district CBR de Béjaïa ; enfin nous allons présenter notre cas d'étude, poser la problématique et les solutions proposées.

2.2 Présentation de l'entreprise de NAFTAL

Voici une présentation générale sur l'entreprise NAFTAL de Béjaïa [19] :

2.2.1 Historique

Issue de SONATRACH, (société nationale pour la recherche, transport, production, transformation, la commercialisation des hydrocarbures), l'entreprise nationale de raffinage et de distribution de produits pétroliers (ERDP) a été crée par le décret N°80-101 du 06 avril 1980.

Entrée en activité le 01 janvier 1982, elle est chargée de l'industrie de raffinage et de la distribution de produits pétroliers.

Le 04 mars 1985, les anciens districts (carburants, lubrifiants, pneumatique et bitume) ont été regroupés sous le nom UND (Unité NAFTAL de Distribution).

En 1987, l'activité raffinage est séparée de la distribution, conformément au décret n° 87- 189 du 25 Août 1987 modifiant le décret n°80-101 du 6 Avril 1980, modifié, portant création de l'entreprise nationale de raffinage et de distribution de produits pétroliers, il a

crée une entreprise nationale dénommée : " Entreprise nationale de commercialisation et de distribution de produits pétroliers ", sous le sigle de " NAFTAL ".

A partir de 1998, elle change de statue et devient société par action filiale à 100% de SONATRACH, en intervenant dans les domaines suivants :

- De l'enfûtage GPL.
- De la formulation des bitumes.
- De la distribution, stockage et commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatique, GPL /produits spéciaux.
- Du transport des produits pétroliers.

2.2.2 Activités principales de l'entreprise

Elle est chargée, dans le cadre du plan national de développement économique et social, de la commercialisation et de la distribution des produits pétroliers et dérivé.

Le 01 janvier 2000, l'activité GPL enfûtage est séparée de l'activité CLP.

Par décision n° S 554 du 29 Mars 2000, il a été procédé à l'organisation générale de la division CLP et l'identification des zones de distribution " CLP " (carburants, lubrifiants et pneumatiques).

Par décision n° S 555 du 29 Mars 2000, il a été procédé à la création des zones de distribution CLP.

Par décision n° S 606 du 10 Février 2001, il a été procédé à l'organisation et la classification des centres Bitumes de la division Bitume.

Par décision n° S 705 du 17 Juin 2002, il a été procédé à la dénomination des zones de distribution CLP et GPL en District.

Par décision n° S 766 du 22 Décembre 2003, il a été procédé à la dissolution de la Branche CLPB.

Par décision n° S 770 du 03 Janvier 2004, il a été procédé à la dissolution des Districts CLP et création des Districts Commercialisation.

A partir du 01.12.2006 l'activité Carburants est séparée de l'activité commercialisation.

2.2.3 Organisation de la branche CBR

La Branche carburants est l'une des trois branches de NAFTAL. Elle est chargée des activités d'approvisionnement, de stockage et de livraison des carburants Aviation (Jet-A1 et Methmix), Marine (Gas-oil et fuel-oils) et Terre (Essences Super, normal et sans plomb, Gas-oil, A72, white spirit) ainsi que les lubrifiants et graisses aviation et marine.

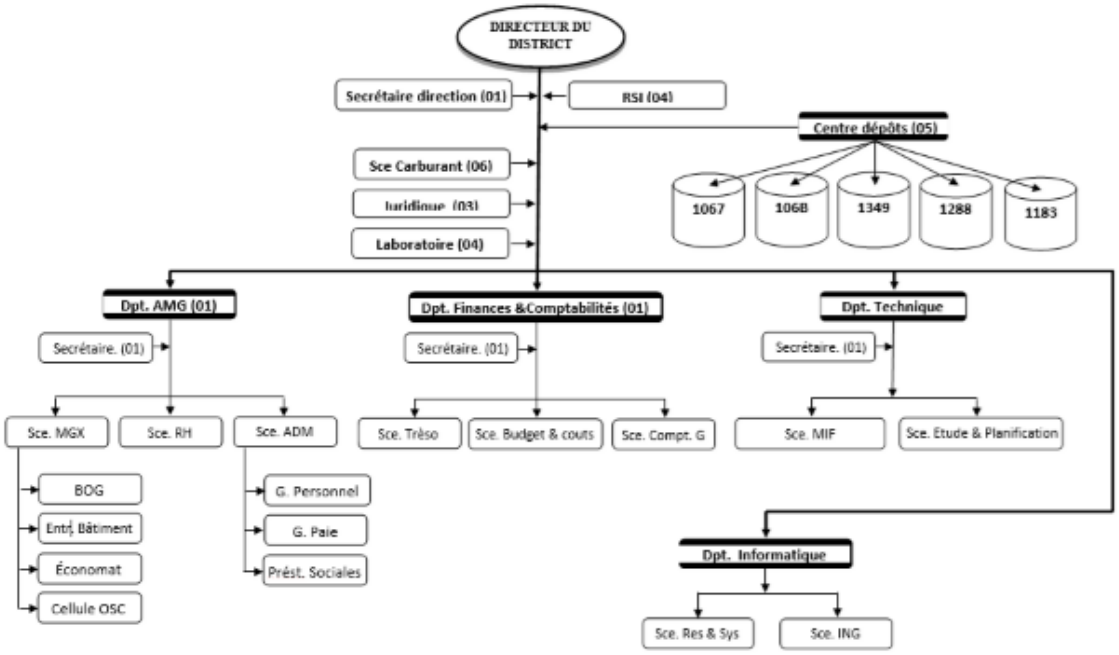


FIGURE 2.1 – Organigramme du District CBR de Béjaïa

2.2.4 Description et rôle de chaque département au sein du district CBR Béjaïa

Le district CBR Béjaïa est organisé comme suit :

2.2.4.1 Direction

Une secrétaire, le responsable de la sécurité industrielle, le laboratoire, le juridique les différents départements et dépôts carburants sont rattachés à la direction.

Ses principales tâches et responsabilités sont :

- Identifier et recenser les infrastructures, équipements et autres moyens matériels (ca-

mions, canalisations) relevant de l'activité carburants du district ainsi que les structures d'organisation et les moyens humains œuvrant pour l'activité carburante.

- Exécuter les programmes de distribution établis par les districts de commercialisation pour la livraison de la clientèle.
- Gérer les stocks en carburants au niveau des dépôts et communiquer régulièrement des points de situation aux structures concernées de la branche.
- Gérer les relations avec les partenaires locaux (fournisseurs et clients) et les autorités et administrations locales.

2.2.4.2 Département Informatique

Le département informatique est assuré par un chef de département, sont rôle principal est de garantir la continuité de service des systèmes informatiques déployés au niveau du district et centres opérationnels et veiller à la mise à disposition des informations de gestion aux structures du district, les branches et les structures centrales.

Nous allons détailler ce département prochainement.

2.2.4.3 Département Administration et Moyens Généraux

Les missions du département AMG sont :

- Assurer la gestion des moyens généraux du district.
- Assurer la gestion des ressources humaines.
- Assurer la gestion de l'administration.
- Assurer la gestion des œuvres sociales et culturelles.

Le département AMG est composé de 4 services :

1. Service administration
    a) Section gestion du personnel.
    b) Section gestion de paie.
    c) Section prestation sociale.
2. Service ressources humaines

3. Services du moyen généraux : Ses activités sont assurées par les trois sections suivantes :
    a) Section BOG (bureau d'ordre).
    b) Section entretien bâtiment.
    c) Section économat.
4. Cellule OSC (Œuvres Sociales et Culturelles).

2.2.4.4 Département Finance et Comptabilité

Le département finances et comptabilité a pour mission de :

- Coordonner et suivre toutes les activités de comptabilité de trésorier, budget et patrimoine.
- Consolider, analyser les états comptables et veiller à la sincérité des comptes du district.
- Veiller à la concordance des écritures comptables avec les flux physiques et financiers.

Il comprend trois services à savoir :

1. Service trésorerie.
2. Service comptabilité générale : Il est composé de deux sections, la section SVCD et la section comptabilité.
3. Service budgets et coûts.

2.2.4.5 Département Maintenance Technique

Il a pour mission :

- Élaborer les plans de maintenance préventive et curative des équipements, dépôts, et canalisation et suivre l'exécution.
- Suivi de la réalisation des travaux.
- Élabore les plans annuels et pluriannuels de transport, en prenant en charge les besoins de distribution net ravitaillement des produits commercialisés.
- Etablir un rapport d'activité périodique.

Ce département comporte les services suivants :

1. Service exploitation et maintenance.

2. Service études et réalisation.

Le district dispose de deux (02) dépôts carburants à Béjaïa, un (01) à TAHER /W.JIJEL, un (01) à Bordj Bou Arreridj et un (01) à M'SILA.

2.3 Présentation du département informatique

Dans cette partie nous allons présenter le département où nous avons effectués notre stage[19] :

2.3.1 Organigramme du département informatique

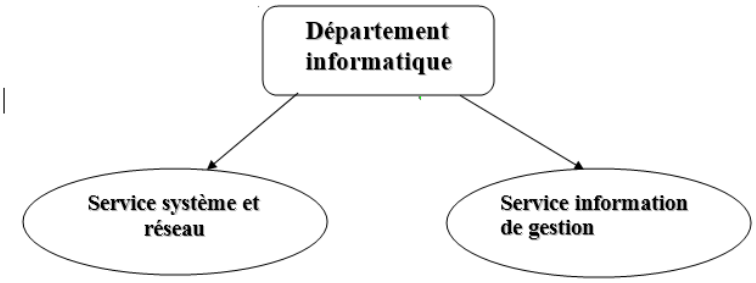


FIGURE 2.2 – Organigramme du département informatique

Le département est divisé en deux services :

- Service Système et Réseau
- Service Information de Gestion

2.3.2 Description et rôle de chaque service du département informatique

1. Service système et réseau : Ce service est composé d'un(1) chef de service SYS & RES, d'un(1) ingénieur informatique et de deux (2) analyste.

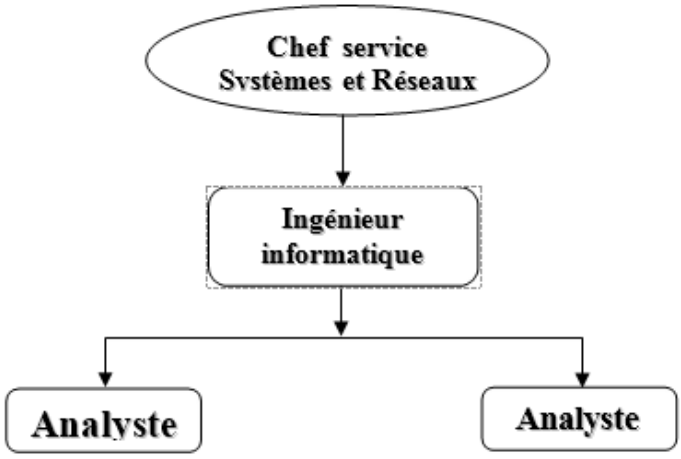


FIGURE 2.3 – Organigramme du service Système & Réseau

Le rôle de ce service est de prendre en charge les infrastructures réseaux filaires et Wifi, et des services généralistes (sécurité, distribution logicielle, gestion des postes de travail...), assure aussi la maintenance des équipements informatique et établissement des formations sur le fonctionnement de certains logiciels ou applications.

Ce service assure deux rôles :

a) La maintenance informatique : Assure la maintenance corrective de tous types de matériels informatiques. Il analyse les causes des pannes et y apporte la solution adéquate dans les meilleurs délais. Il peut être amené à intervenir sur des logiciels et à effectuer tout ou partie de l'installation et de la mise en route des matériels informatiques. Prendre en chargé aussi l'installation de matériels neufs, de modification et d'adaptation des matériels.

b) L'infrastructure réseau : Mise en place et configuration du réseau informatique de l'entreprise, il intervient à chaque étape de la mise en place d'un réseau local, où s'en occuper intégralement de fournir le matériel nécessaire et faire :

- La pose du câblage informatique.
- La configuration des postes utilisateurs, système d'exploitation, messagerie, internet, intranet, FTP.
- Assure aussi la gestion des domaines, groupe et ressource du réseau.
- Administrer les serveurs de réseaux (serveur FTP, messagerie, web,...).

2. Service Information de Gestion (ING)

Ce service est composé d'un(1) chef de service ING et d'un (1) Cadre d'étude.

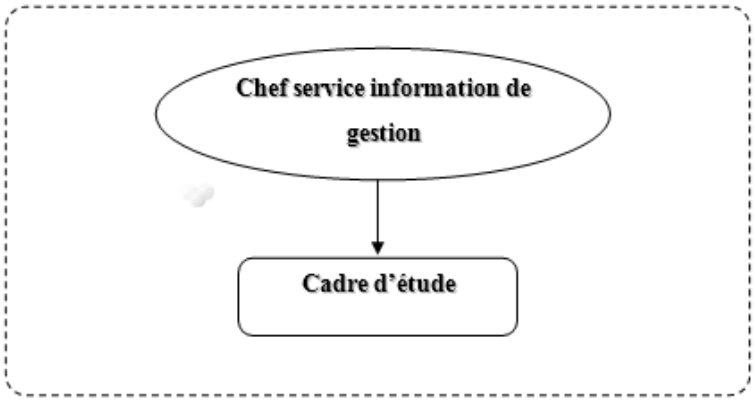


FIGURE 2.4 – Organigramme du Service Information de Gestion

Rôles du Service Information de Gestion est :

- Gérer et mettre à jour une banque de données de toutes les activités du District.
- Procéder au calcul de la PRC (Prime de Rendement du Collectif) des différents collectifs du District.
- Consolider les différents plans et budgets des structures du District.
- Préparer les différentes présentations.
- Collecter, contrôler et analyser les informations concernant les activités du district.
- Participer à l'élaboration des rapports d'activité périodiques et les tableaux de bord.
- Assurer la diffusion des PV des conseils de direction du district aux membres présents et aux structures centrales de la branche carburants.

2.4 Architecture réseau du district CBR

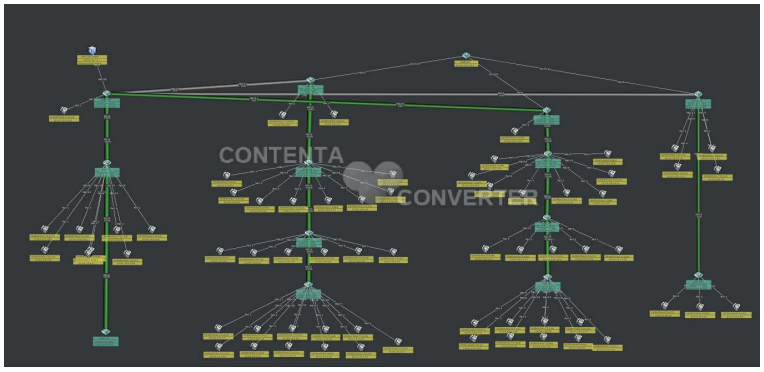


FIGURE 2.5 – Réseau de Naftal détaillé

Le réseau local du district CBR de Béjaïa interconnecte tous les ordinateurs du parc informatique en étoile étendu et leur permet d'accéder aux ressources du réseau et à internet. Pour adresser facilement les hôtes du réseau, un service DHCP est fonctionnel dans le LAN. Les machines du parc ont deux systèmes d'exploitation, Windows 7, et Windows server 2008 pour leur serveur. Des imprimantes sont mises en réseau pour être partagées entre les employés afin que ceux-ci puissent y accéder sans avoir à transporter les documents d'un poste à un autre. Il est également à noter que, ce réseau LAN se compose d'un réseau filaire et d'un réseau wifi pour permettre l'accès à internet aux visiteurs. Des onduleurs sont également mis à contribution en cas de coupures brusques du courant électrique. On dénombre un dans chacun des deux services informatique et d'autre dans les services cités plus haut.

2.4.1 Parc informatique

1. Environnement client : Le district dispose d'un parc informatique composé :

Equipement	Nombre	Caractéristique
PC bureau	89	HP Compac 8300
PC portable	04	HP Compac 600pro
Imprimentes	15	EPSON Aculaser M2000

TABLE 2.1 – Environnement client

2. Environnement serveur : Le district dispose d'un serveur 2008 qui permet de gérer et configurer les différents équipements de leur réseaux.

3. Matériels d'interconnexion : Les équipements d'interconnexion représentent le coeur du réseau dans une architecture.S'ils sont mal dimensionnés, ils pourront avoir des effets négatifs sur le trafic du réseau, pouvant entrainer la détérioration de celui-ci. Dans notre cas d'étude, l'infrastructure du réseau de district comporte 13 commutateurs CISCO CATALYSTE 2960 de 24 ports et un commutateur fibre optique CISCO 2911 pour l'interconnexion des différents clients et d'un routeur CISCO 2911.

2.4.2 Applications de l'entreprise

Le système d'exploitation utilisé par les machines au sein du district est Windows 7 pour les ordinateurs de bureau et portable.Un certain nombre d'applications sont utilisées, il s'agit :

NAFTCOM : Système informatique pour la gestion de l'activité distribution et commercialisation au sein des CDS.

NAFT-GD : Contrôlée des stations-service en gérance direct.

WINCANAL : Système de comptabilité analytique.

IMMOSYS GESTION : Logiciel de gestion des biens mobile et immobile (véhicule, Bureau, table, pc. . ..).

POSTPAIE : Gestion Paie des employés.

NOVACH RH : Application Web pour la gestion du personnels.

GIF : Application Web pour la gestion des installations fixe (pompe, vane,. . .etc)

V15 : Application Web pour établissement des bons de chargement volume a 15.

REF TRANSPORT : Application web pour le suivie des transporteurs.

SGC : Logiciel de gestion des créances.

BASSMA : Application pour la gestion Pointage des employés.

2.5 Contexte du projet à réaliser

2.5.1 Présentation du projet

Notre projet intitulé " Mise en place d'une solution de monitoring et d'optimisation d'un réseau local au sein du district CBR de Béjaïa " ,ce dernier consiste à mettre en place un logiciel de supervision réseau tout en améliorant le réseau local de l'entreprise.

2.5.2 Objectif du projet à réaliser

Notre objectif principal est de remédier au problèmes rencontrés durant notre période de stage et d'essayer de trouver une solution optimale pour la gestion du réseau local du district et la surveillance des différents équipements de ce dernier.

2.5.3 Problématique

Durant notre période de stage au sein du district CBR de Béjaïa, nous avons remarqués qu'il dispose d'un réseau local de taille importante composée d'une plateforme de services reliant les différents départements et composants de ce district, nous avons pu mettre le point sur divers manquement du réseau à savoir :

- Le district ne dispose d'aucun logiciel interne adéquat de monitoring réseau.
- Le réseau constitue une seule entitée peuplée par les différents services de chaque département ce qui provoque une charge énorme sur ce dernier.

Pour mieux spécifier les problèmes rencontrés au sein du district nous avons installés et configurés deux logiciels de surveillances réseau qui sont : PRTG, Cisco Network Assistant. Nous illustrons par les figures suivantes les résultats de la surveillance faite durant un mois au sein du district CBR de Béjaïa.

2.5.3.1 Surveillance avec PRTG

La figure suivante représente l'état des switchs de l'entreprise après les avoir ajouter, comme nous remarquons tous les switchs de l'entreprise sont en vert donc fonctionnent bien.

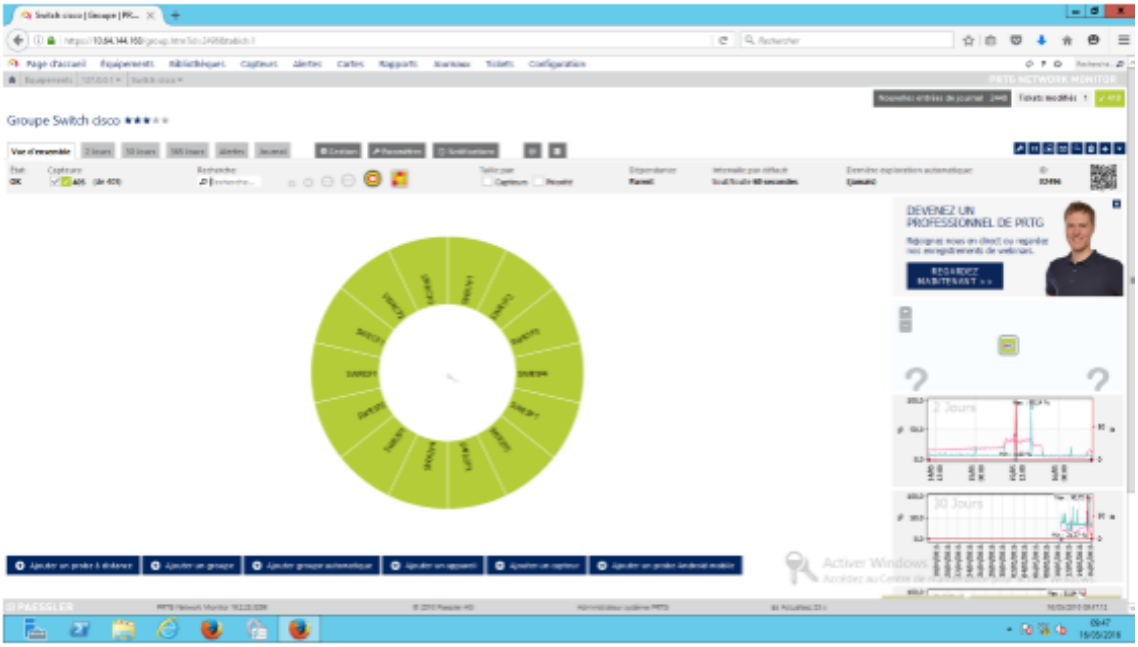


FIGURE 2.6 – États des switch

La figure suivante représente la surveillance des switchs en deux jours, qui a atteint les 90% ce qui provoque une charge sur le réseau.

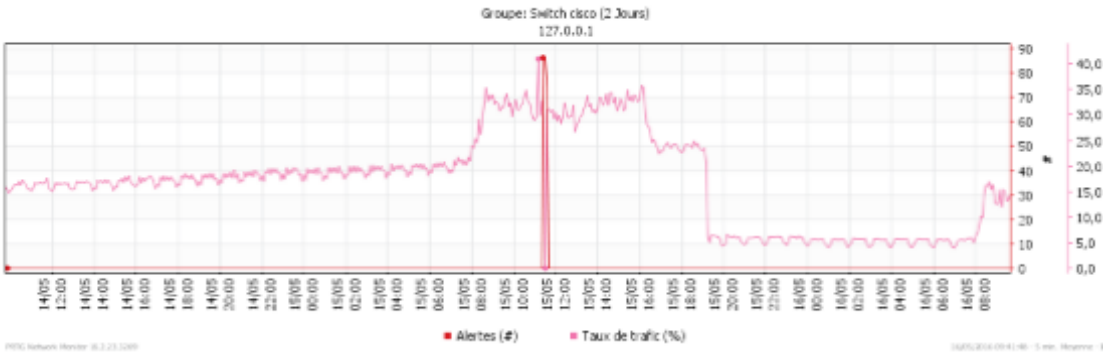


FIGURE 2.7 – Surveillance des switchs en 2jours

Et dans la figure suivante, nous avons présentés la surveillance des switchs en 30 jours

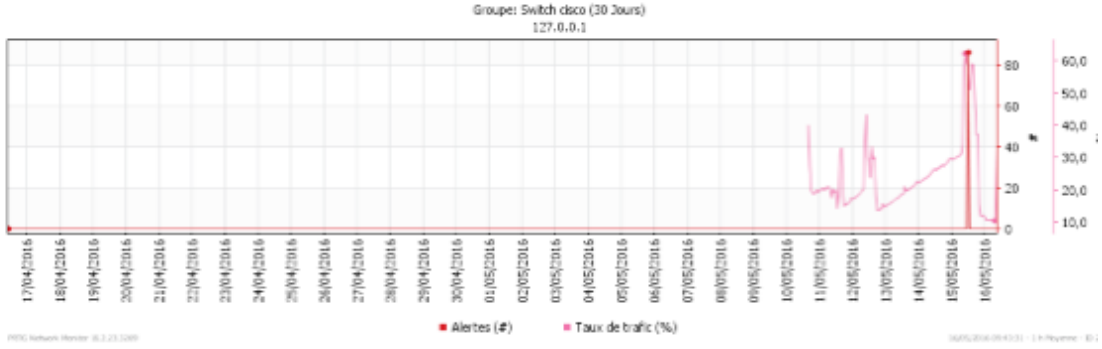


FIGURE 2.8 – Surveillance des switchs en 30jours

2.5.3.2 Surveillance avec Cisco Network Assistant

Après avoir configuré cisco network assistant en ajoutant une communauté qui a comme addresse ip l'addresse réseau de l'entreprise "10.64.144.0", nous avons surveillés le réseau du district dans deux périodes différentes :

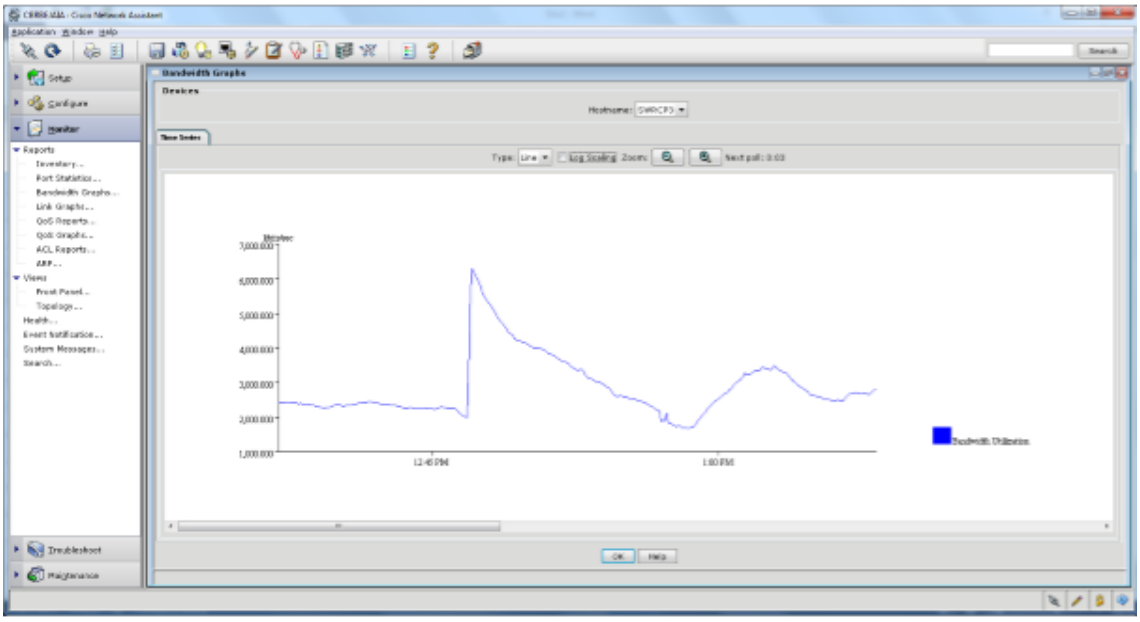


FIGURE 2.9 – Surveillance du réseau en 2 heures

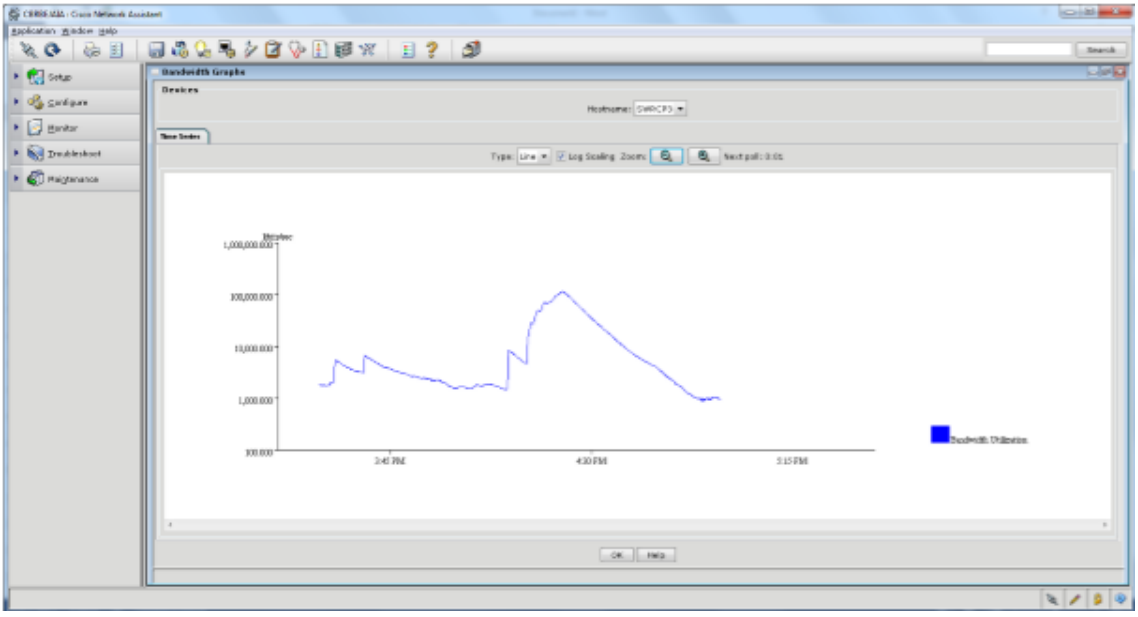


FIGURE 2.10 – Surveillance du réseau d'une semaine

2.5.4 Solution proposée

Nous avons remarqués par les figures ci-dessus qu'il y a une forte utilisation de bande passante d'où nous sommes parties sur la segmentation du réseau du district en un ensemble de VLANs, chaque département et direction représente donc un VLAN ; de plus installer et configurer un logiciel performant de monitoring réseau.

2.6 Conclusion

L'étude de l'existant nous a permis de nous familiariser avec le district CBR de Béjaïa ainsi que de son réseau.

Les problèmes que rencontre le district se sont imposés suite à une étude profonde de leur réseau et à sa critique, ce qui nous a permis de cerner la problematique de notre projet et de proposer des solutions.

Chapitre 3

Présentation des outils mis en œuvre

3.1 Introduction

La solution que nous avons proposés est née dans le contexte d'offrir aux entreprises un plus pour la supervision des réseaux, afin de détecter les anomalies du réseau et remédier à ces dernières.

Dans ce chapitre, nous allons présenter les détails des différents mécanismes mis en œuvre dans notre travail et découvrir quelques services peuvent être pris en charge par ces derniers.

3.2 VMWare

La virtualisation consiste à intercaler une couche d'abstraction entre un client et un fournisseur au sens large du terme. Dans le monde du système d'information, cela consiste à utiliser des moyens techniques (matériels et/ou logiciels) afin de faire fonctionner sur une seule machine plusieurs systèmes d'exploitation ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes[27]. De nombreux logiciels permettent de faire de la virtualisation, parmi lesquels :

- VirtualPC.
- VirtualBOX.
- VMware Workstation.
- VMware vSphere.

Pour notre mémoire nous avons choisis de travailler avec VMware Workstation la version 10. Elle permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local

avec une adresse IP différente, tout en étant sur la même machine physique (machine existante réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. La figure suivant représente l'interface de la VMWare workstation 10 :

FIGURE 3.1 – Interface de notre machine virtuelle

Pour créer une nouvelle machine virtuelle (à partir d'un ISO), il suffit de cliquer sur "Create a New Virtual Machine", mais avant nous devons télécharger d'abord l'image ISO que nous voudrions installer pour notre cas nous allons utiliser l'ISO de Windows Server 2012.

Windows server 2012 : Microsoft Windows Server 2012, anciennement connu sous le nom de code Windows Server 8, est la seconde avant dernière version du système d'exploitation réseau Windows Server. La version suivante est Windows Server 2012 R2.Puis Windows Server 2016 est sorti en phase de développement.

Microsoft a renforcé son portefeuille de technologies réseaux ainsi que les fonctions stockage dans Windows Server 2012, avec pour objectif affiché de simplifier les déploiements d'Hyper-V et d'en améliorer les performances. Windows Server 2012 est utile si l'on souhaite créer un domaine pour mettre en réseau des postes de travail. Ce serveur deviendra donc contrôleur de domaine, un rôle minimum qu'il convient de bien configurer. [3] Voici l'icône de ce dernier aprés le téléchargement [3] :

FIGURE 3.2 – Icône de windows server 2012

3.3 PRTG

PRTG (Paessler Router Traffic Grapher) est un logiciel qui permet grâce à l'analyse de trames SNMP de créer des graphiques sur le trafic réseau. Fondée en 1997 à Nuremberg, la société Paessler a développé une solution dédiée à la surveillance de la bande passante et à la gestion de la performance des équipements réseau pour les entreprises de taille intermédiaire.[11] Des tableaux de bord en temps réel permettent de suivre les performances du réseau.

3.3.1 Service SNMP

Avant d'entamer l'installation de PRTG, nous devons d'abord activer le service SNMP.

- Au niveau des switchs et du routeur : Dans la figure suivante nous avons activés SNMP au niveau du SW7 , de la même manière nous l'avons activés sur les autres switchs et aussi sur le routeur.

```
SW7#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW7(config)#snmp-server community cbrbejaia ro
SW7(config)#
```

FIGURE 3.3 – Activation du SNMP au niveau des switchs

- Au niveau de windows server 2012 : Les figures suivantes vous montre l'activation de SNMP :

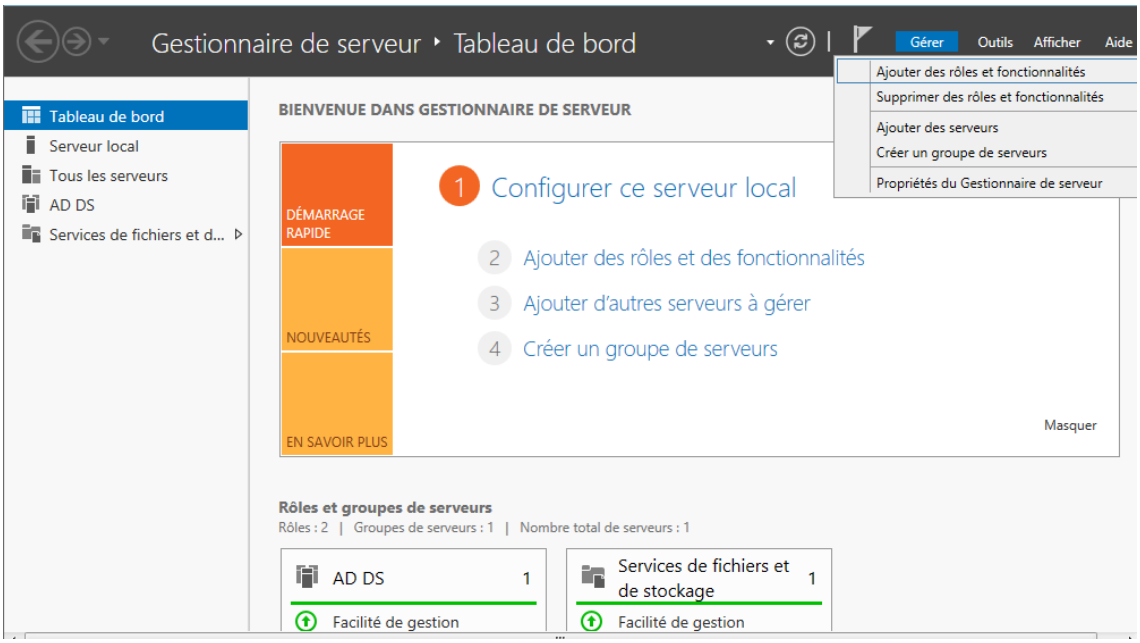


FIGURE 3.4 – Gestionnaire de serveur

En cliquant sur ’Ajouter des rôles et fonctionnalités” nous aurons la figure suivante :

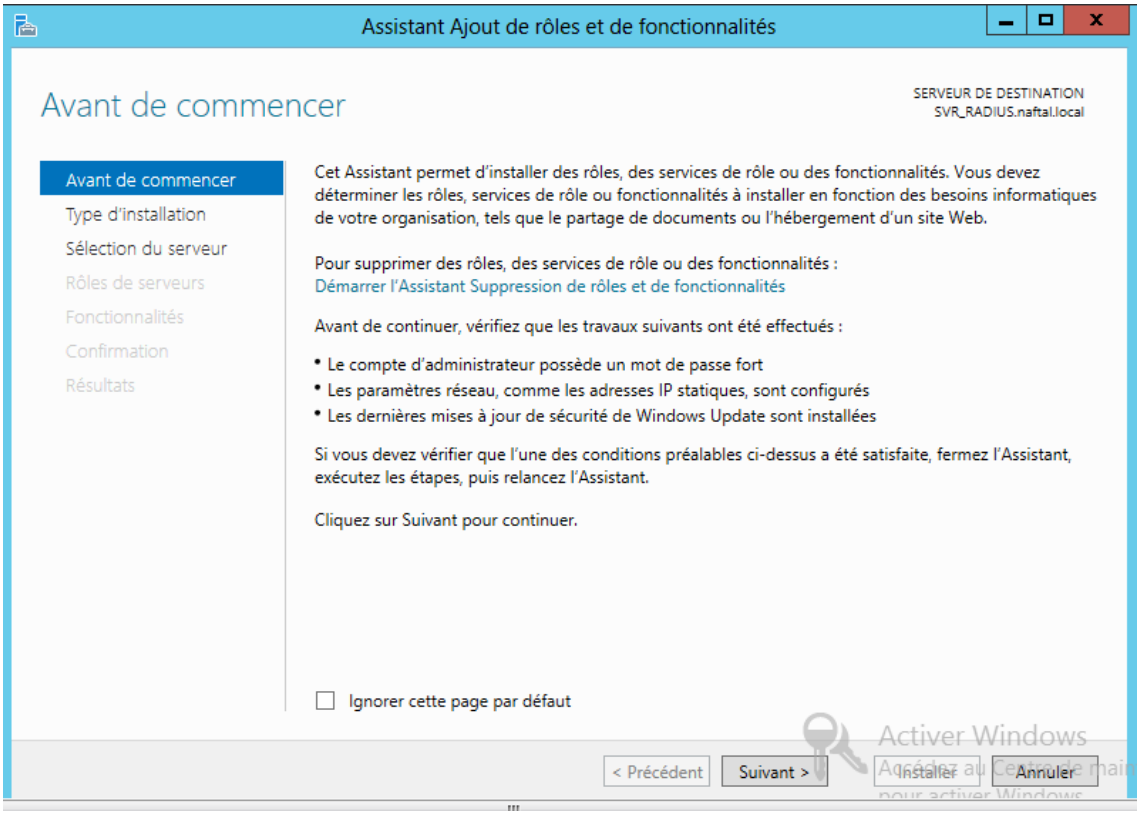


FIGURE 3.5 – Installation de SNMP

Dans cette étape nous cliquons sur "suivant" jusqu'à ce que nous arrivons à la partie où nous devons choisir la fonctionnalité que nous désirons ajouter. Séléctionnez le service SNMP ensuite suivant , confirmer les séléctions d'installation et enfin fermer la fenêtre lorsque la progression d'installation est réussite.

3.3.2 Installation du PRTG

Nous nous sommes appuyés sur l'ouvrage de passsler afin de pouvoir installer PRTG ; les étapes d'installation sont décrites par cet ouvrage[20] :

Avant de lancer l'executable nous allons d'abord le télécharger à partir de ce site : "https ://www.fr.paessler.com" , ensuite cliquez sur ce fichier et suivez les étapes, durant l'installation une fenêtre vous demandera d'accepter le contrat de la licence,donc cliquez sur "Je comprends et j'accepte les termes du contrat de la licence".
Ensuite, vous allez introduire votre email, après cliquez sur suivant, suivant. Une fenêtre qui apparait vous demandera d'introduire la clé de la licence que vous l'aurez lors du téléchargement du fichier par le site du passlear.

Enfin cochez oui pour redémarrer l'ordinateur, enfin cliquez sur terminer.

Maintenant PRTG est installé il suffit d'aller au bureau et cliquer sur PRTG network monitor.

Par défaut le nom utilisateur et le mot de passe sont définit mais vous pouvez le changer par la suite, dans notre cas nous l'avons changé.

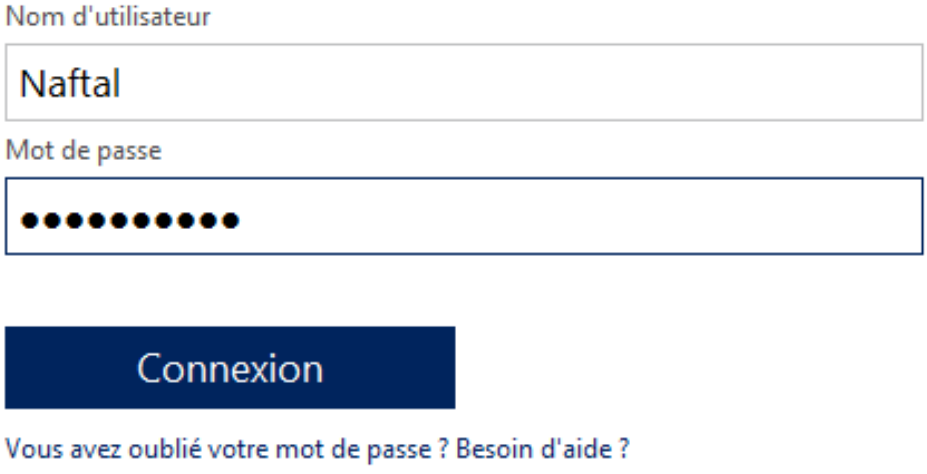


FIGURE 3.6 – Connexion au PRTG

Après lorsque l'authentification est effetuée, cette page d'accueil vous apparaîtra :

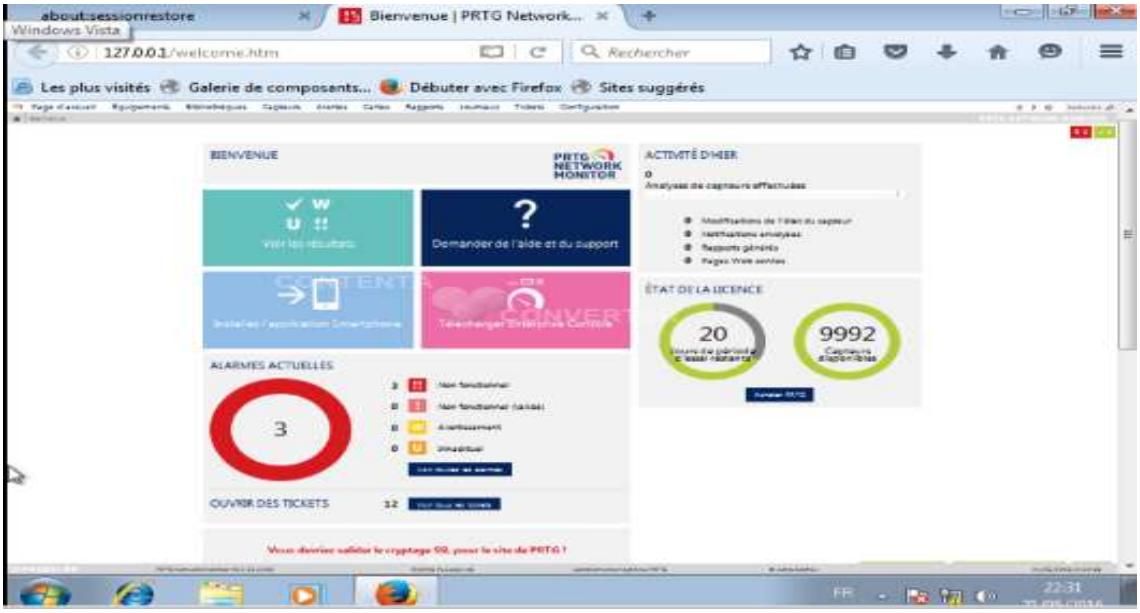


FIGURE 3.7 – Page d'accueil

Différents menus sont présents en haut de la page d'administration :

FIGURE 3.8 – Menu du PRTG

Page d'accueil : Permet de revenir à la page principale de monitoring ainsi que de choisir différentes formes de tableau de bord.

Equipements : Permet de voir tous les périphériques qui ont été ajoutés avec plusieurs règles de filtrage pour les visualiser, comme par groupe ou par dépendance.

Bibliothèques : Permet de créer des vues personnalisées de nos objets de surveillance.

Capteurs : Permet de visualiser l'ensemble de nos capteurs avec des filtrages et d'en associés à nos appareils enregistré dans PRTG.

Alertes : Permet de voir les alertes qui ont été émises par les capteurs.

Ces capteurs sont liés à nos équipements qui nous permettent à nous avertir si les informations qu'ils surveillent sont OK, anormales ou complétements erronées.
Pour voir les alertes, il suffit d'aller dans le menu " Alertes " et de cliquer sur " Tout

" pour pourvoir ainsi les visualiser.
Il y a un code couleur associée aux messages des capteurs qui s'affichent en haut à droit d'un "Tableau de bord" :

FIGURE 3.9 – Alertes du PRTG

La couleur gris veut dire qu'un évènement s'est produit et a été enregistré dans le journal.
La couleur rouge signale l'erreur ou l'échec de la prise d'information d'un capteur.
La couleur verte signifie que les capteurs nous signalent que tout va bien.
La couleur bleue indique les capteurs qui ont été mis en pause.

Cartes : Permet de créer notre propre vu d'ensemble de notre réseau surveillé.

Rapports : Les rapports sont utilisés pour analyser les données de surveillance, nous pouvons définir le nombre de rapport que nous le souhaitons.

Journaux : Le journal présente toute l'activité historique surveillée par PRTG. Nous pouvons aussi filtrer le journal à notre convenance.

Ticket : Les tickets permettent de gérer et de traiter divers problèmes qui peuvent survenir au cours de la surveillance.

Configuration : Permet de configurer l'interface et notre compte PRTG.

Dans le chapitre suivant nous allons voir en détail comment associer PRTG à notre réseau.

3.4 Protocole DHCP

Tout ordinateur d'un réseau TCP/IP nécessite une adresse IP pour pouvoir communiquer avec les autres ordinateurs du réseau. Ces adresses IP sont attribuées :

- Statiquement, en configurant le réseau directement sur l'ordinateur.
- Dynamiquement, avec un serveur DHCP qui attribue les adresses en fonction de son fichier de configuration.

3.4.1 Définition

DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP comme distribuant des adresses IP, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau. Cette dernière possibilité est très intéressante pour la maintenance de gros parcs machines. Les versions actuelles des serveurs DHCP fonctionne pour IPv4.[4]

3.4.2 Rôle du DHCP

Un serveur DHCP a pour rôle de distribuer des adresses IP à des clients pour une durée déterminée.Au lieu d'affecter manuellement à chaque hôte une adresse statique, ainsi que tous les paramètres tels que (serveur de noms, passerelle par défaut, nom du réseau), un serveur DHCP alloue à un client, un bail d'accès au réseau, pour une durée déterminée (durée du bail). Le serveur passe en paramètres au client toutes les informations dont il a besoin.[4]

3.4.3 Avantages du protocole DHCP

Les avantages du protocole du DHCP sont [5] :

- Le protocole DHCP offre une configuration de réseau TCP/IP fiable et simple, empêche les conflits d'adresses et permet de contrôler l'utilisation des adresses IP de façon centralisée. Ainsi, si un paramètre change au niveau du réseau, comme, par exemple l'adresse de la passerelle par défaut, il suffit de changer la valeur du paramètre au niveau du serveur DHCP, pour que toutes les stations aient une prise en compte du nouveau paramètre dès que le bail sera renouvelé. Dans le cas de l'adressage statique, il faudrait manuellement reconfigurer toutes les machines.
- Economie d'adresse : ce protocole est presque toujours utilisé par les fournisseurs d'accès Internet qui disposent d'un nombre d'adresses limité. Ainsi grâce à DHCP, seules les machines connectées en ligne ont une adresse IP.
- Les postes itinérants sont plus faciles à gérer.
- Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution.

Avec DHCP, il suffit d'attribuer une adresse au serveur. Lorsqu'un ordinateur client DHCP demande l'accès au réseau en TCP/IP son adresse est allouée dynamiquement à l'intérieur d'une plage d'adresses définie sur le serveur .

L'administrateur de réseau contrôle le mode d'attribution des adresses IP en spécifiant une durée de bail qui indique combien de temps l'hôte peut utiliser une configuration IP attribuée, avant de devoir solliciter le renouvellement du bail auprès du serveur DHCP.

3.5 Listes de contrôle d'accès (ACL)

3.5.1 Définition

Les listes d'accès (access list) sont des instructions qui expriment une liste de règle, imposées par l'opérateur, donnant un contrôle supplémentaire sur les paquets reçue et transmis par le routeur mais ne concernant pas ceux générés par le routeur. Les listes d'accès sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie vers une destination. Elles opèrent selon un ordre séquentiel et logique, en évaluant les paquets à partir du début de la liste d'instruction. Il ne peut pas avoir qu'une seule liste d'accès par protocole et par interface.[6]

3.5.2 Rôle d'une ACL

Une liste d'accès va servir de[6] :

- Supprimer des paquets pour des raisons de sécurité.
- Filtrer des mises à jour de routage.
- Filtrer des paquets en fonction de leur priorité
- Définir du trafic intéressant pour des configurations spécifiques

3.5.3 Caractéristiques d'une ACL

- Les paquets peuvent être filtrés en entrée (quand ils entrent sur une interface) avant la décision de routage.
- Les paquets peuvent être filtrés en sortie (avant de quitter une interface) après la décision de routage.

- Le mot clef IOS est "deny" pour signifier que les paquets doivent être filtrés ; précisément les paquets seront refusés selon les critères définis.
- Le mot clef IOS est "permit" pour signifier que les paquets ne doivent pas être filtrés ; précisément les paquets seront permis selon les critères définis.
- La logique de filtrage est configurée dans les listes d'accès.
- Une instruction implicite rejette tout le trafic à la fin de chaque liste d'accès.

3.5.4 Types de listes d'une ACL

La mise en œuvre d'une ACL se déroule en deux étapes :

- Création de la liste, en plaçant les instructions les unes après les autres suivies d'un retour chariot.
- Application sur une interface en entrée ou en sortie.

Les types de liste de controle sont les suivantes [6] :

a) Liste d'accès standard : Permet d'analyser du trafic en fonction de l'adresse IP source.

b) Liste d'accès étendu : Permet d'analyser du trafic en fonction de :

- Adresse IP source
- Adresse IP destination
- Protocole (tcp, udp, icmp, ...)
- Port source
- Port destination
- Etc.

c) Liste d'accès IP nommée : ACL identifiées par un nom sous la forme d'une chaîne de caractères alphanumériques.

d) Activation d'une liste d'accès sur une interface.

3.6 GNS3

3.6.1 Définition

GNS3 (Graphical Network Simulation) est une solution libre disponible sous Windows, GNU/Linux et MacOS permettant l'émulation ou la simulation de réseaux informatiques via une interface graphique ; il permet de reproduire une architecture physique ou logique grâce à[13] :

Dynamips qui est un émulateur IOS Cisco.

Dynagen qui est une interface en mode text pour Dynamips. Cet outil va permettre l'interconnexion de plusieurs machines émulées.

Qemu qui est un émulateur de système. Cet outil va permettre à GNS3 d'exécuter Cisco ASA, PIX et IDS .

Virtualbox qui va nous permettre de créer et lancer ces machines virtuelles.

Contrairement à « Cisco Packet Tracer », qui est un simulateur de matériel réseau Cisco, GNS3 va émuler de véritable IOS Cisco. De ce fait, nous pouvons user de toutes les fonctionnalités de l'IOS Cisco chargé.

3.6.2 Installation de GNS3

Pour installer l'émulateur GNS3 vous devez télécharger le fichier exécutable, ensuite le lancer et suivre les étapes de d'installation[13].

La figure suivante représente l'interface de GNS3 :

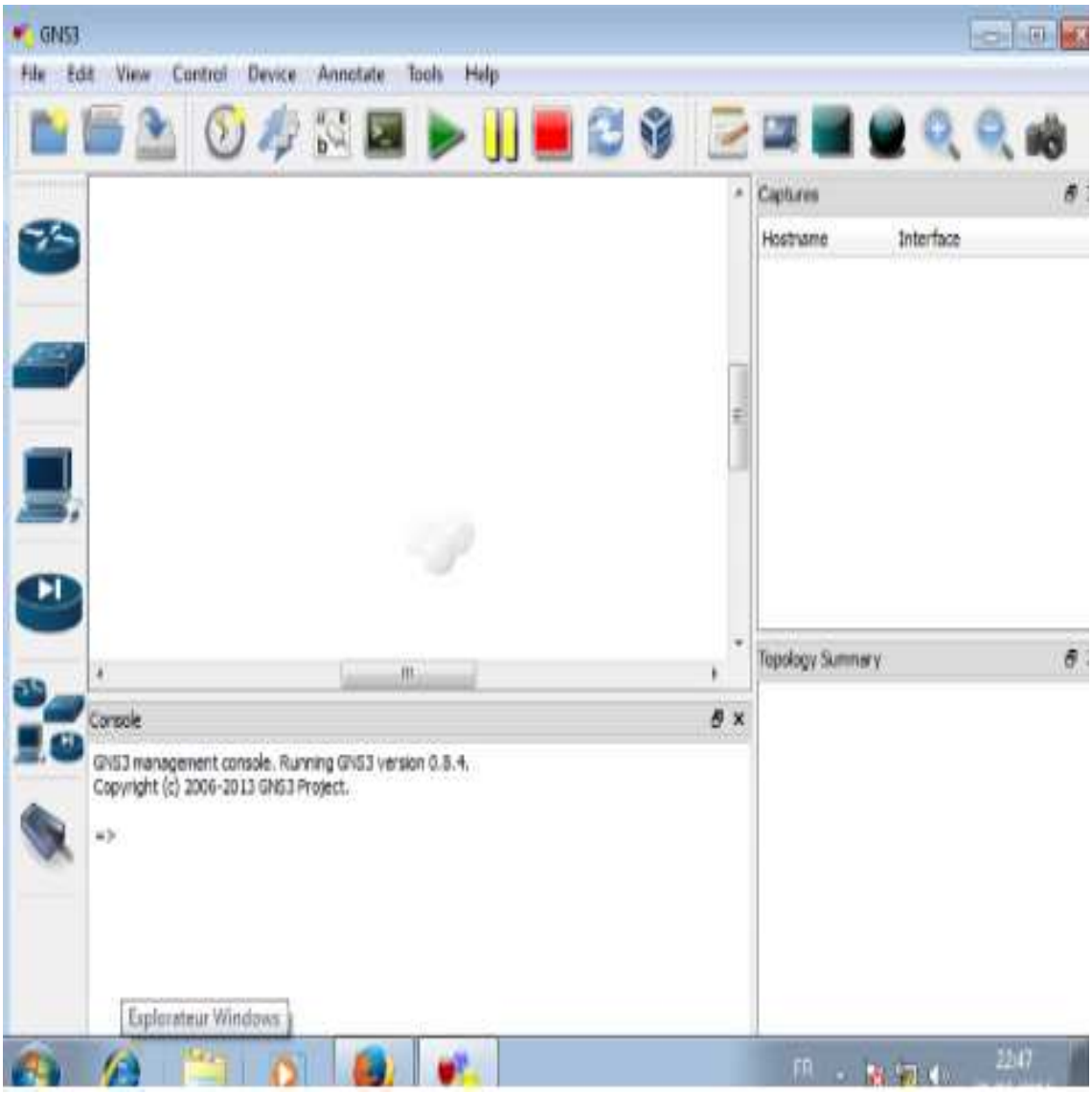


FIGURE 3.10 – Interface de gns3

Sur la gauche de l'interface, nous pouvons voir la liste des éléments actifs et materiels disponible que nous pouvons ajouter à notre topologie.
Sur la droite de l'interface, il y a une partie en haut appelée "Topologie" qui contient les éléments ajoutés dans l'architecture réalisée en GNS3.Si l'élément est en vert donc il est en marche, si c'est en rouge donc il est en arrêt.Juste en bas nous trouvons les captures qui permet de visualiser les captures réalisées.

3.6.3 Configuration de GNS3

3.6.3.1 Modifier la langue d'utilisation de GNS3

Sélectionnez l'option "General". Cliquez sur l'onglet "General Settings". Sélectonnez "Français (fr)". Cliquez sur le bouton "OK", Relancez GNS3.[12]

3.6.3.2 Les préférences dans GNS3

Créez, dans le répertoire C :Simulateur, les répertoires "Projets" et "Images".

Indiquez, dans les "Préférences" de GNS3, ces deux répertoires.

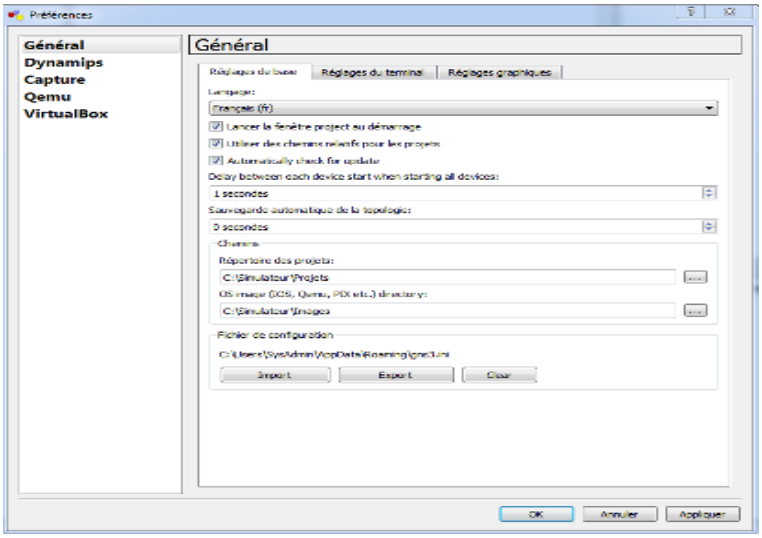


FIGURE 3.11 – Préférences dans GNS3

Sélectionnez l'option "VirtualBox". Ne modifiez pas les paramètres définis par défauts. Cliquez sur le bouton "Test Settings".

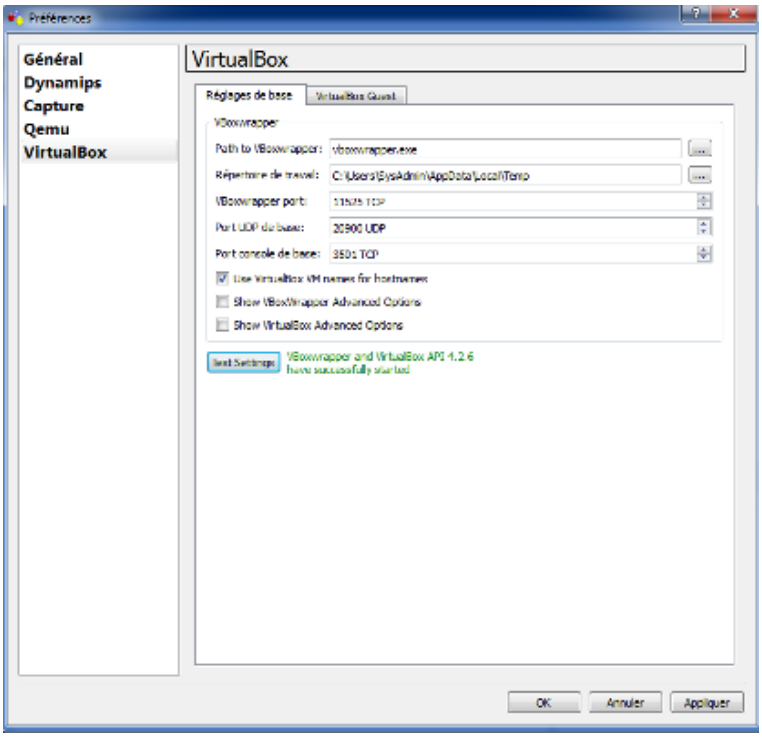


FIGURE 3.12 – La virtualbox de GNS3

3.6.3.3 Associer un fichier "IOS" à un routeur

Pour utiliser GNS3 avec les routeurs proposés dans son interface, il est nécessaire de les associer à un fichier "IOS".Les fichiers images "IOS" ne sont pas fournis par GNS3. Donc les avons télécharger par : www.4shared.com

À partir de l'onglet "Images IOS", sélectionnez l'image binaire de votre routeur. GNS3 vous informe que l'image "IOS" est compressée.

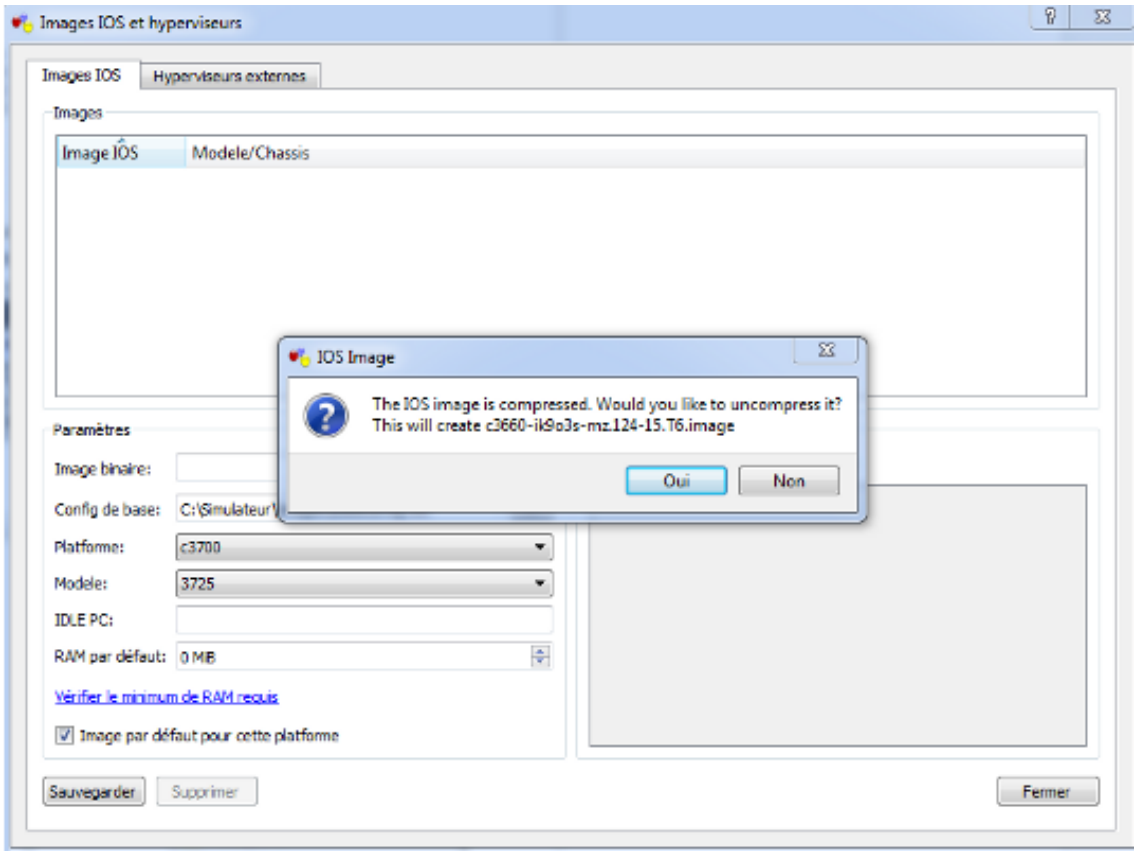


FIGURE 3.13 – GNS3 - IOS Image

Sélectinnez "Oui" pour décompresser l'image binaire.Ensuite cliquez sur sauvegarder et voilà le GNS3 est bien configuré et prêt à être utiliser.

3.7 Conclusion

Dans ce chapitre, nous avons présentés VMWare workstation 10 comme machine virtuelle et PRTG logiciel de surveillance réseau ainsi GNS3 comme émulateur.
Dans le chapitre suivant nous allons implémenter les solutions proposées en utilisant les différents outils.

Chapitre 4

Réalisation

4.1 Introduction

Dans ce chapitre nous allons présenter la partie réalisation, qui est subdivisé en deux grandes parties essentiels, la première partie est la simulation, configuration et la surveillance de notre réseau sans VLAN , la seconde partie quant à elle est avec vlans .

4.2 Topologie sous GNS3 sans VLAN

Nous avons choisis de calquer l'architecture du réseau de CBR Naftal de Béjaïa mais en l'émulant avec moins de PCs, voici la topologie réalisée :

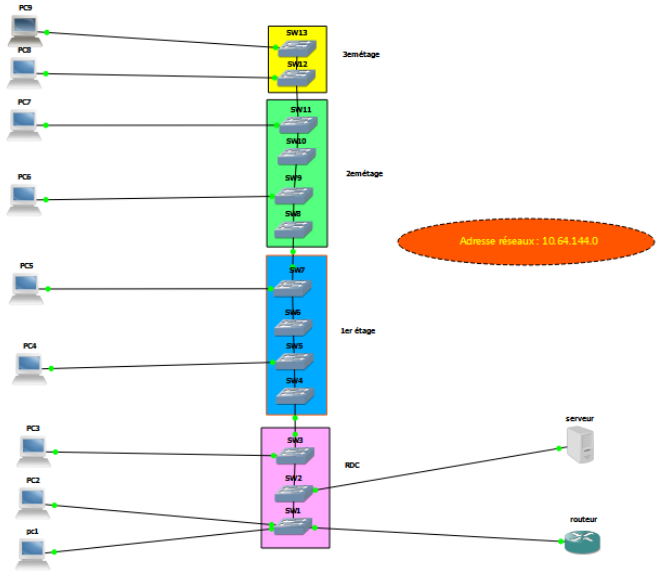


FIGURE 4.1 – Topologie sous GNS3 sans VLAN

Cette topologie comporte : 9 ordinateurs,un serveur, 13switchs qui sont répartis selon les quatres étages du CBR, et d'un routeur.

Notre serveur permet d'interconnecter notre réseau sous GNS3 dans la machine réelle à notre machine virtuelle. Il servira de passerelle entre nos schémas réseau GNS3 et notre machine virtuelle Workstation.
Mais avant de faire cela nous devons d'abord préparer notre carte réseau au niveau de la machine virtuelle afin de la relier au serveur sur GNS3. Pour cela nous allons dans la machine virtuelle ensuite sur edit, Virtual Machine Setting, nous aurons la fenêtre suivante :

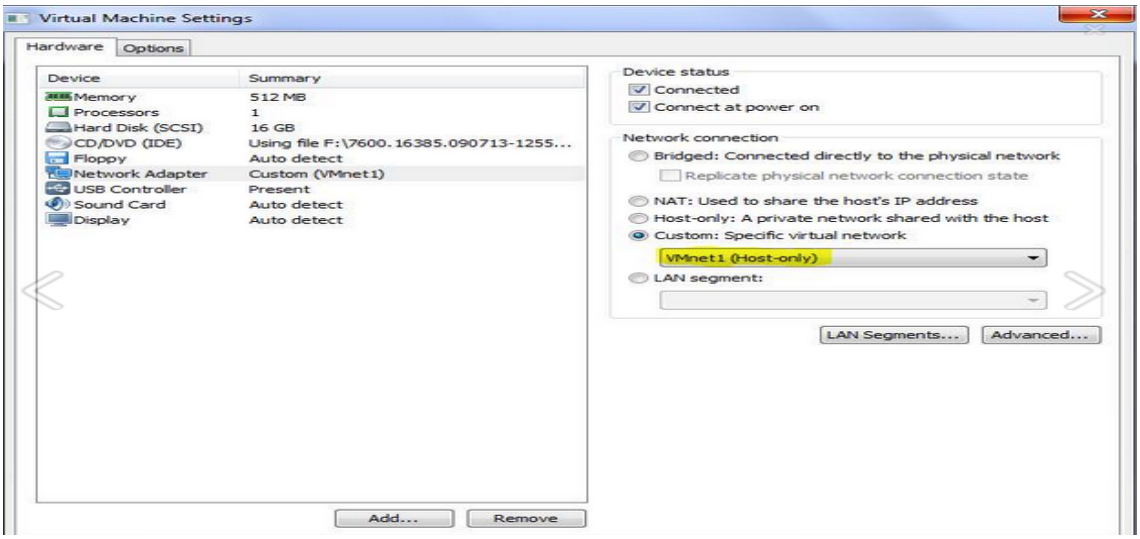


FIGURE 4.2 – Configuration de la vmnet

Ici dans cette figure nous allons cocher la case Custum pour spécifier la carte réseau virtuelle utilisée. Maintenant dans Virtual Network Editor de la VMworkstation la carte réseau VMnet1 est connecté et que la case " Use Local DHCP service to distribute IP address to VMs " est décoché :

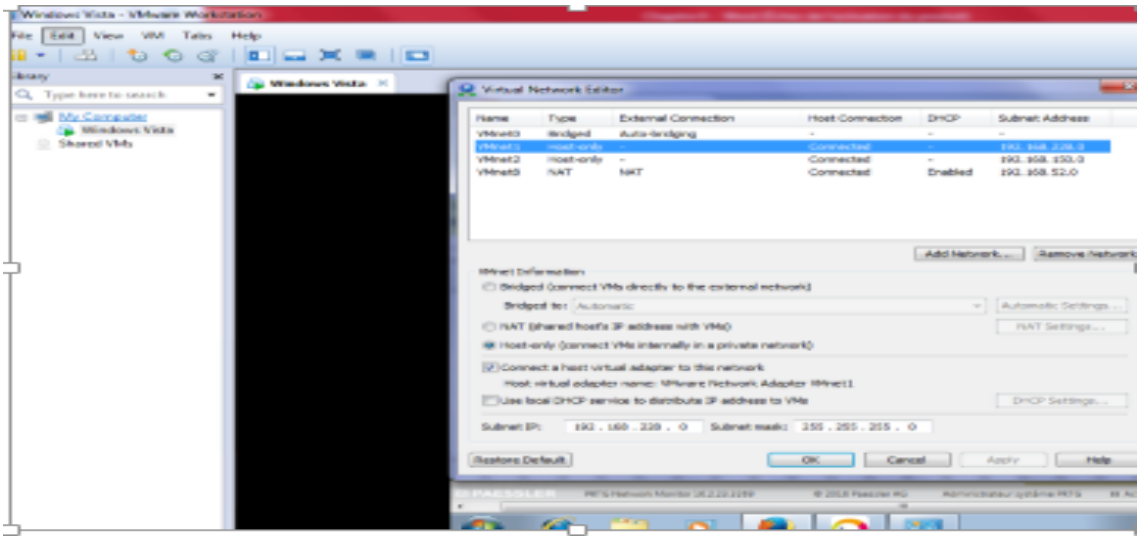


FIGURE 4.3 – Configuration de la carte réseau vmnet1

Voilà maintenant notre carte réseau est prête à être utliser.
Une fois le serveur ajouté dans GNS3 on fait un clic droit sur ce dernier " Configurer ", ensuite choisir la VMnet1.

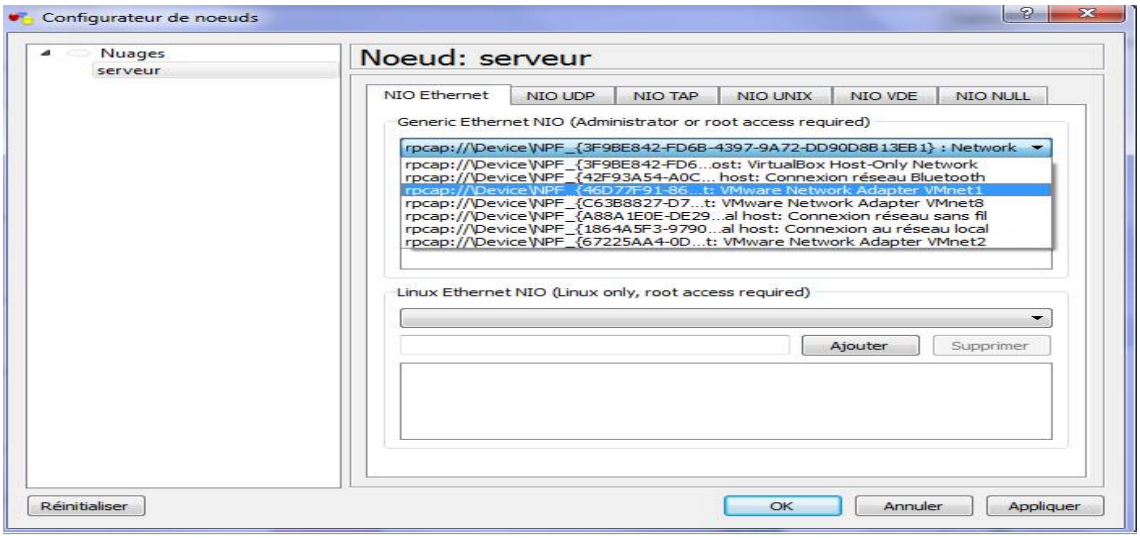


FIGURE 4.4 – Configuration du serveur

Voilà donc notre serveur est prêt à être utilisé ; maintemant nous allons montrer les différentes liaisons que nous avons fait lors de la création de notre topologie :

- Liens manuels : routeur, switch

Routeur/switch	Liens
Router	L'interface fa0/0 est connectée au SW1 via l'interface 1
SW1	L'interface 1 est connectée au routeur via l'interface fa0/0 L'interface 2 est connectée au PC2 via l'interface 20000 L'interface 3 est connectée au PC1 via l'interface 20001 L'interface 4 est connectée au SW2 via l'interface 2
SW2	L'interface 1 est connecter au SW3 via l'interface 1 L'interface 2 est connecter au SW1 via l'interface 4 L'interface 3 est connecter au Serveur via l'interface Vmnet1
SW3	L'interface 1 est connecter au SW2 via l'interface 1 L'interface 2 est connecter au PC3 via l'interface 20002 L'interface 5 est connecter au SW4 via l'interface 1
SW4	L'interface 1 est connecter au SW3 via l'interface 5 L'interface 2 est connecter au SW5 via l'interface 1
SW5	L'interface 1 est connecter au SW4 via l'interface 2 L'interface 2 est connecter au SW6 via l'interface 1 L'interface 3 est connecter au PC4 via l'interface 20003
SW6	L'interface 1 est connecter au SW5 via l'interface 2 L'interface 2 est connecter au SW7 via l'interface 1
SW7	L'interface 1 est connecter au SW6 via l'interface 2 L'interface 2 est connecter au SW8 via l'interface 2 L'interface 1 est connecter au PC5 via l'interface 20004
SW8	L'interface 2 est connecter au SW7 via l'interface 2 L'interface 3 est connecter au SW9 via l'interface 1
SW9	L'interface 1 est connecter au SW8 via l'interface 3 L'interface 1 est connecter au SW10 via l'interface 1 L'interface 1 est connecter au PC6 via l'interface 20005
SW10	L'interface 1 est connecter au SW9 via l'interface 2 L'interface 2 est connecter au SW11 via l'interface 1
SW11	L'interface 1 est connecter au SW10 via l'interface 2 L'interface 2 est connecter au SW12 via l'interface 1 L'interface 3 est connecter au PC7 via l'interface 20006
SW12	L'interface 1 est connecter au SW11 via l'interface 2 L'interface 2 est connecter au SW13 via l'interface 1 L'interface 3 est connecter au PC8 via l'interface 20007
SW13	L'interface 1 est connecter au SW12 via l'interface 2 L'interface 2 est connecter au PC9 via l'interface 20008

TABLE 4.1 – Liens manuels sans les vlans

Concernant les switchs nous avons utilisé " Commutateur Ethernet" qui a au minimum

3 ports mais que nous pouvons en rajouter selon nos besoins, et pour le routeur nous avons utilisé le " c2691 ".

- Serveur

Serveur/ Liens	
serveur	L'interface Vmnet1 est connectée au SW2 via l'interface 3

TABLE 4.2 – Lien manuel du serveur sans VLAN

4.3 Configuration du routeur sans VLANS

4.3.1 Affectation de l'addresse IP et activation du SNMP

Afin de pouvoir affecter une adresse ip au routeur nous devons être en mode configuration. Le shell est le suivant :

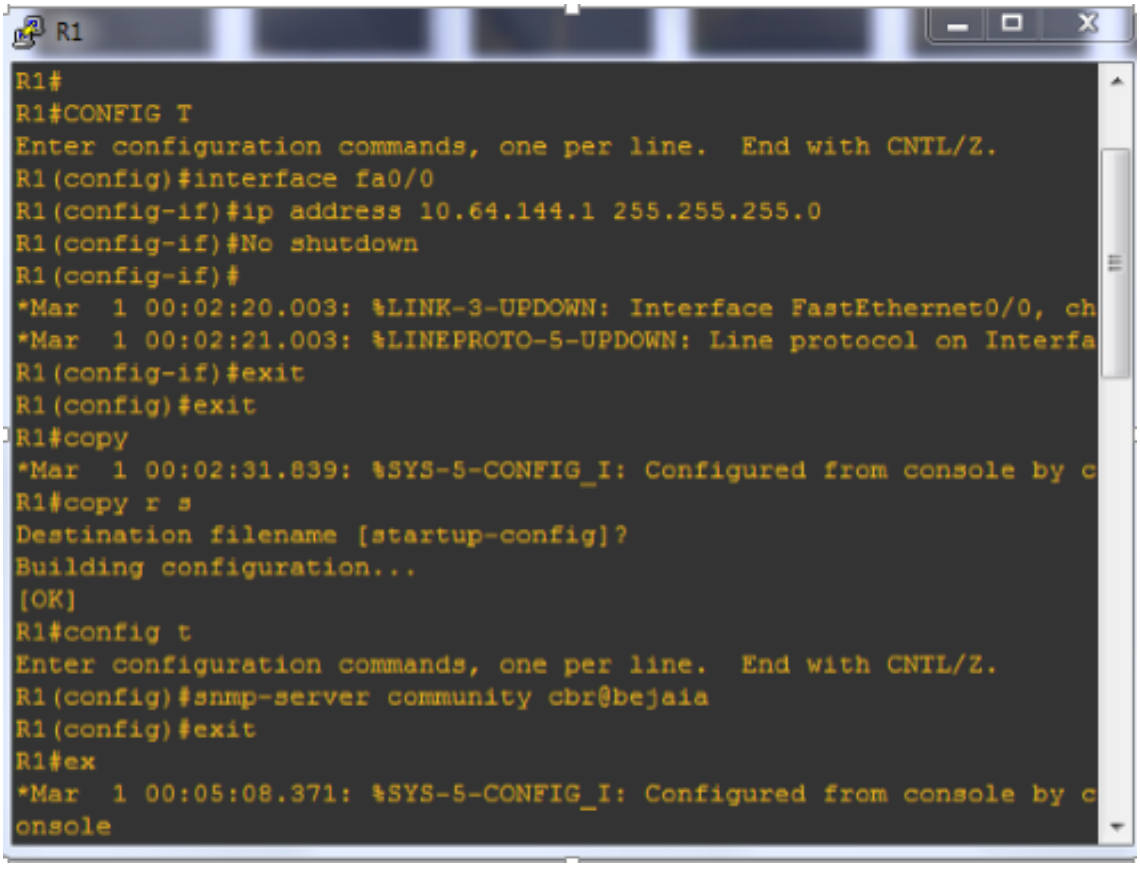


FIGURE 4.5 – Affectation d'un IP et activation de SNMP

Cette figure représente l'affectation de l'adresse 10.64.144.1 à l'interface fa0/0 avec un

masque sous réseau 255.255.255.0. Et la commande snmp-server community cbr@bejaia ro permet d'activer le serveur SNMP. Lorsqu'on termine la configuration nous devons enregistrer notre configuration en saisissant la commande copy r s ou bien wr.

4.3.2 Configuration du dhcp

Afin d'éviter la fastidieuse tâche de configurer manuellement les machines une à une ,le serveur DHCP a le pouvoir d'effectuer cette tâche. Dans la figure suivante, nous allons présenter toutes étapes suivies pour pouvoir activer le serveur DHCP :

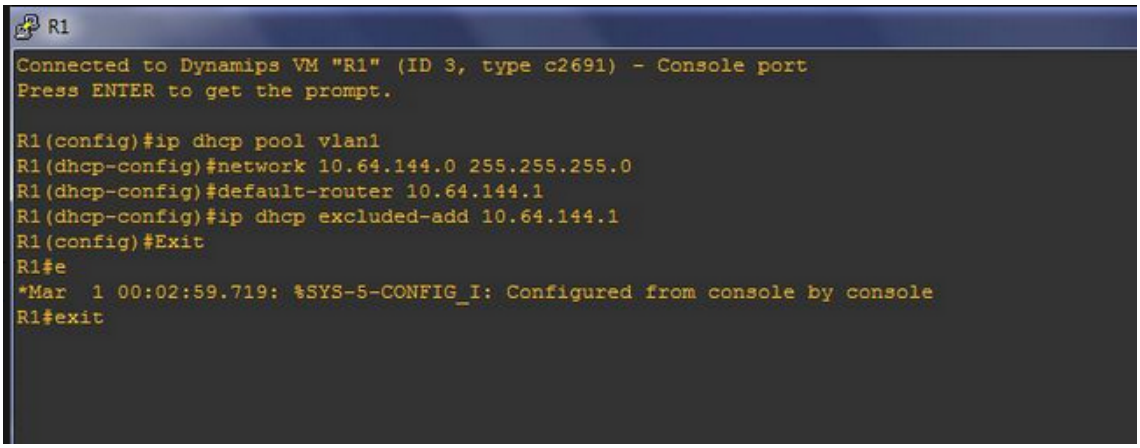


FIGURE 4.6 – Configuration du dhcp

4.4 Vérification et test de connectivité sans VLAN

4.4.1 Vérification de la configuration

Pour pouvoir vérifier la validité de notre configuration, nous allons dans l'icône Tools - VPCs et nous allons avoir la figure suivante :

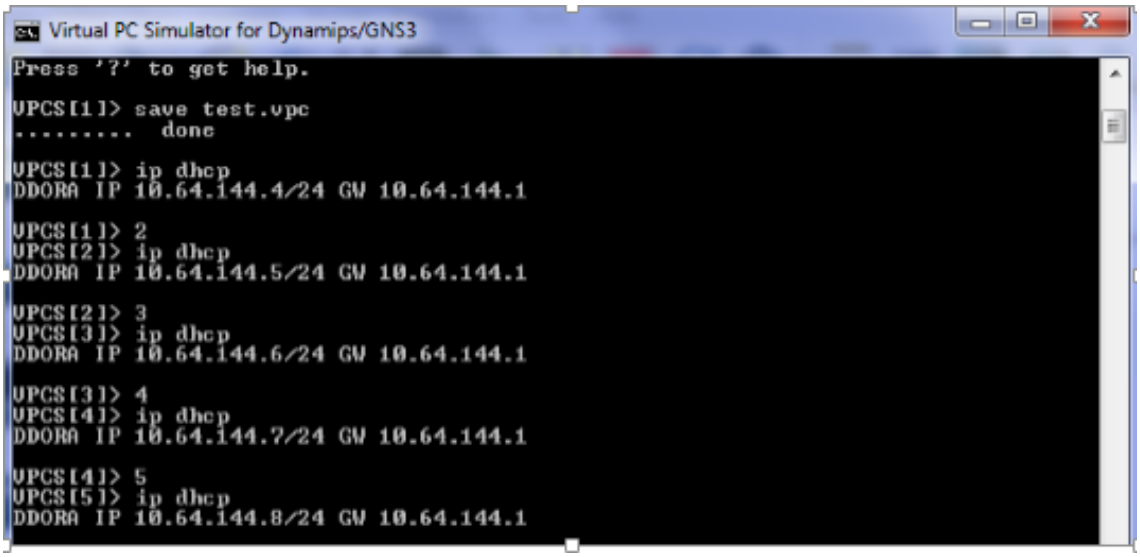


FIGURE 4.7 – Vérification résussite

À cette étape là nous allons en premier lieu sauvegarder la configuration des PCs en utilisant la commande : "save test.vpc" , ensuite activer le DHCP avec la commande : "ip dhcp" si tout marche bien la réponse sera comme nous la voyons dans la figure sinon un message de type DDD sera affiché.

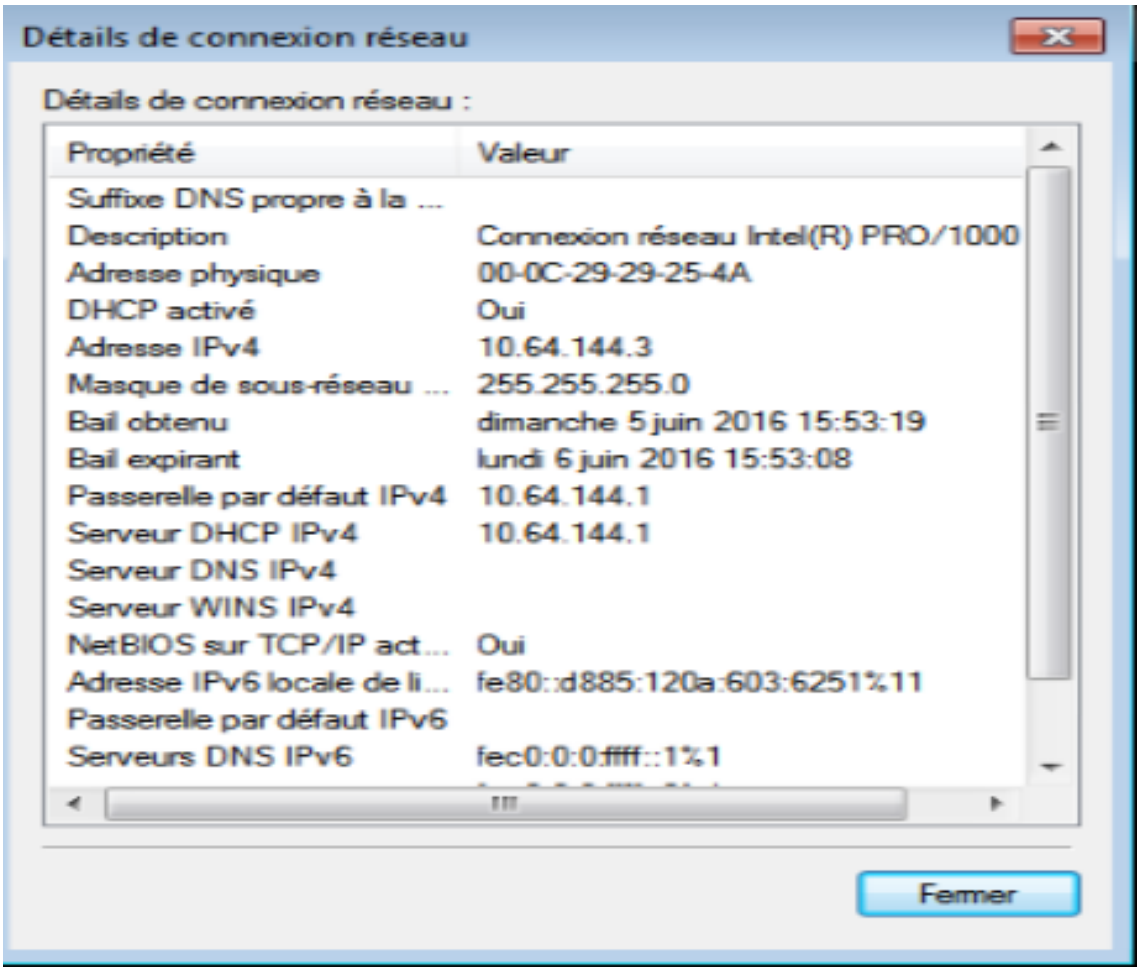


FIGURE 4.8 – Affectation de l'adresse ip à la Vmnet1

Dans cette figure nous remarquons que le DHCP configuré dans notre routeur a évidemment donné une adresse IP à notre machine virtuelle. Donc nous pouvons le relier au PRTG pour pouvoir commencer notre surveillance.

4.4.2 Test de connectivité

Dans les figures ci-dessous, nous remarquons que la communication passe entre tous les PCs c'est-à-dire tous les départements du District peuvent communiquer et cela peut causer un problème au niveau de la sécurité.

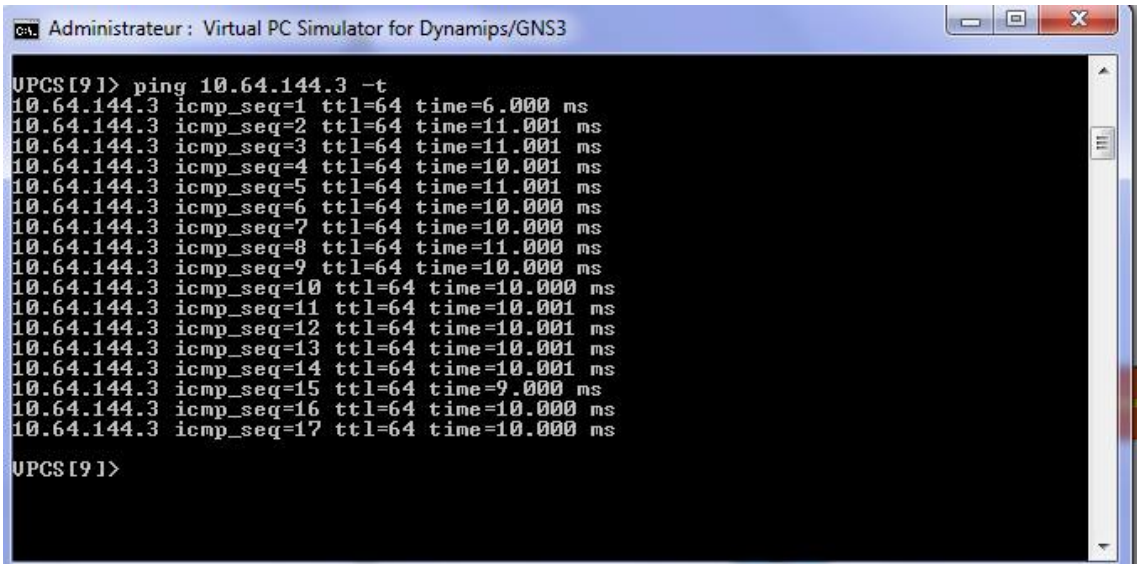


FIGURE 4.9 – Ping entre le PC9 et le PC2

4.5 Topologie sous GNS3 avec VLAN

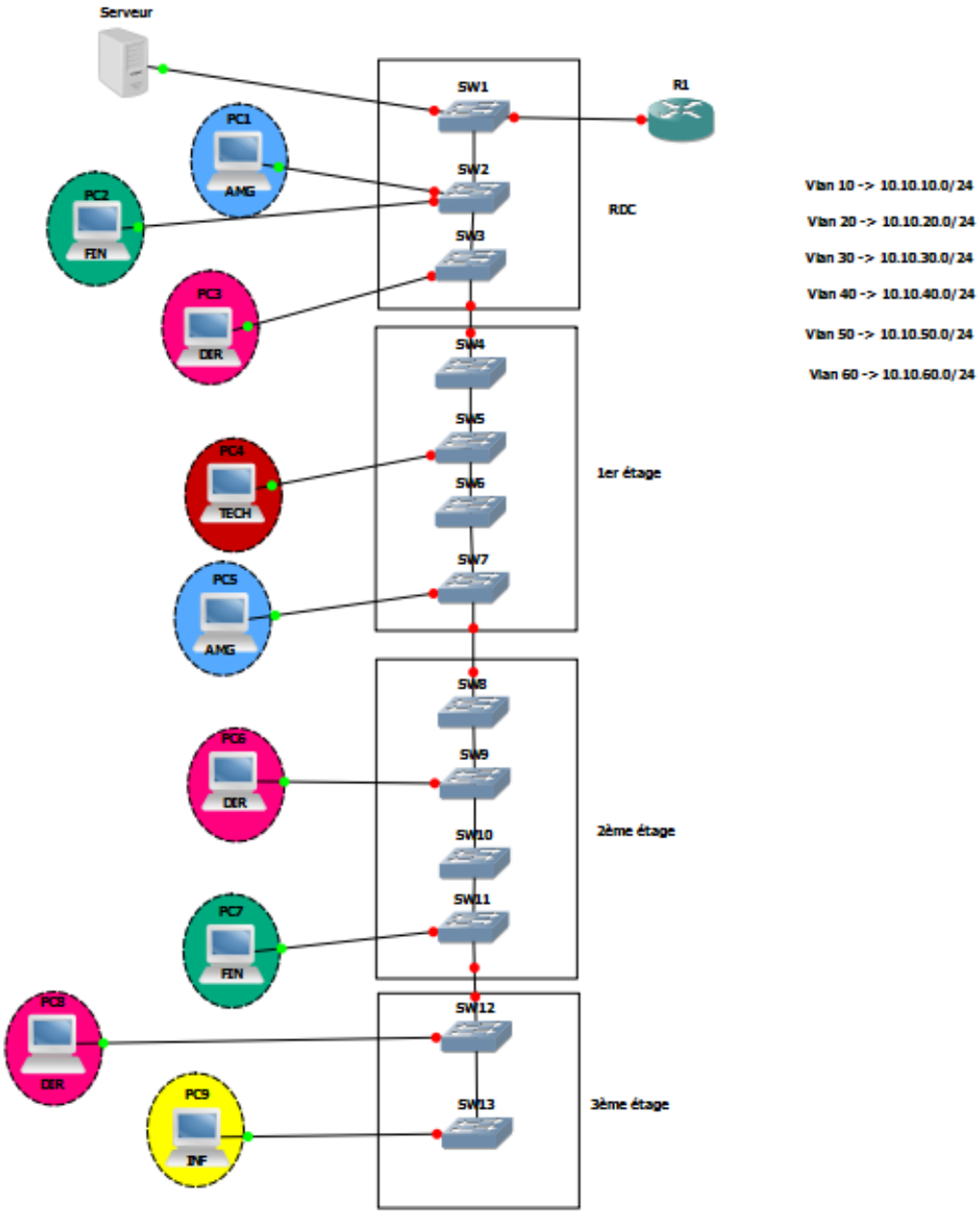


FIGURE 4.10 – Topologie de notre réseau avec VLAN

À la différence de la topologie sans VLAN, ici nous avons utilisé des switch-routeur car en GNS3 il n'existe pas des switchs de niveau 3 donc nous avons émulé notre réseau en utilisant des routeurs " 3700 " que nous avons juste changé de symbole en faisant un clic droit-¿ changer de symbole. De la même manière nous avons renommé les routeurs en SW1

jusqu'à SW13. Nous avons aussi ajouté une carte nommée " NM-16ESW". Concernant le serveur, c'est la même configuration faite dans la 1ere partie.

Le tableau suivant représente les liens manuels que nous avons faits :

Routeur/switch	Liens
Router	f0/0 est connectée au SW1 via f1/0
SW1	f1/0 est connectée au Router via f1/0 f1/1 est connectée au SW2 via f1/0 f1/2 est connectée au Serveur via Vmnet1
SW2	f1/0 est connectée au SW1 via f1/1 f1/1 est connectée au SW3 via f1/0 f1/2 est connectée au PC1 via 20000 f1/3 est connectée au PC2 via 20001
SW3	f1/0 est connectée au SW2 via f1/2 f1/1 est connectée au PC3 via 20002 f1/2 est connectée au SW4 via f1/0
SW4	f1/0 est connectée au SW3 via f1/2 f1/1 est connectée au SW5 via f1/0
SW5	f1/0 est connectée au SW4 via f1/1 f1/1 est connectée au PC4 via 20003 f1/2 est connectée au SW6 via f1/0
SW6	f1/0 est connectée au SW5 via f1/2 f1/1 est connectée au SW7 via f1/0
SW7	f1/0 est connectée au SW6 via f1/1 f1/1 est connectée au PC5 via 20004 f1/2 est connectée au SW8 via f1/0
SW8	f1/0 est connectée au SW7 via f1/2 f1/1 est connectée au SW9 via f1/0
SW9	f1/0 est connectée au SW8 via f1/1 f1/1 est connectée au PC6 via 20005 f1/2 est connectée au SW10 via f1/0
SW10	f1/0 est connectée au SW9 via f1/2 f1/1 est connectée au SW11 via f1/0
SW11	f1/0 est connectée au SW10 via f1/1 f1/1 est connectée au PC7 via 20006 f1/2 est connectée au SW12 via f1/0
SW12	f1/0 est connectée au SW11 via f1/2 f1/1 est connectée au PC8 via 20007 f1/2 est connectée au SW13 via f1/0
SW13	f1/0 est connectée au SW12 via f1/2 f1/1 est connectée au PC9 via 20008

TABLE 4.3 – Liens manuels avec les VLAN

Serveur	Liens
serveur	Vmnet1 est connectée au SW1 via f1/2

Table 4.4 – Lien manuel du serveur avec VLAN

4.6 Configuration des commutateurs

Pour commencer nous allons créer 6 vlans :

Vlan 10 nommé INF : regroupe tous les ordinateurs appartenant au département informatique.

Vlan 20 nommé AMG : regroupe tous les ordinateurs appartenant au département administration et moyens généraux.

Vlan 30 nommé FIN : regroupe tous les ordinateurs appartenant au département finance et comptabilité.

Vlan 40 nommé TECH : regroupe tous les ordinateurs appartenant au département technique.

Vlan 50 nommé DIR : regroupe tous les ordinateurs appartenant à la direction.

Vlan 60 nommé ADMIN : est l'administrateur de l'entreprise.

Ensuite affecter les ports aux PCs,

4.7 Configuration du routeur avec VLAN

4.7.1 Configuration du protocole DHCP

Dans cette topologie avec VLAN nous aurons besoin de créer 6 pool c'est-à-dire pour chaque VLAN nous devons lui créer son pool d'adresse, la figure suivante représente la configuration du DHCP.

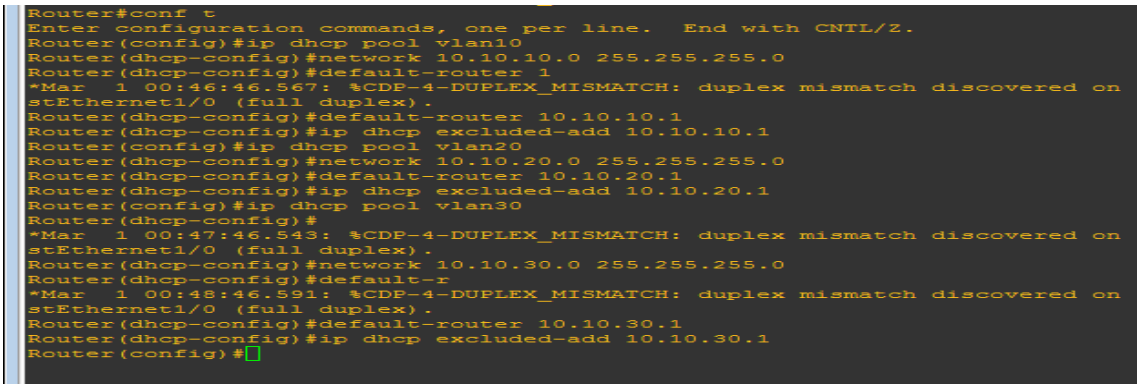


FIGURE 4.11 – Configuration du DHCP

De la même manière nous avons créé les autres pools voici le résultat obtenu :

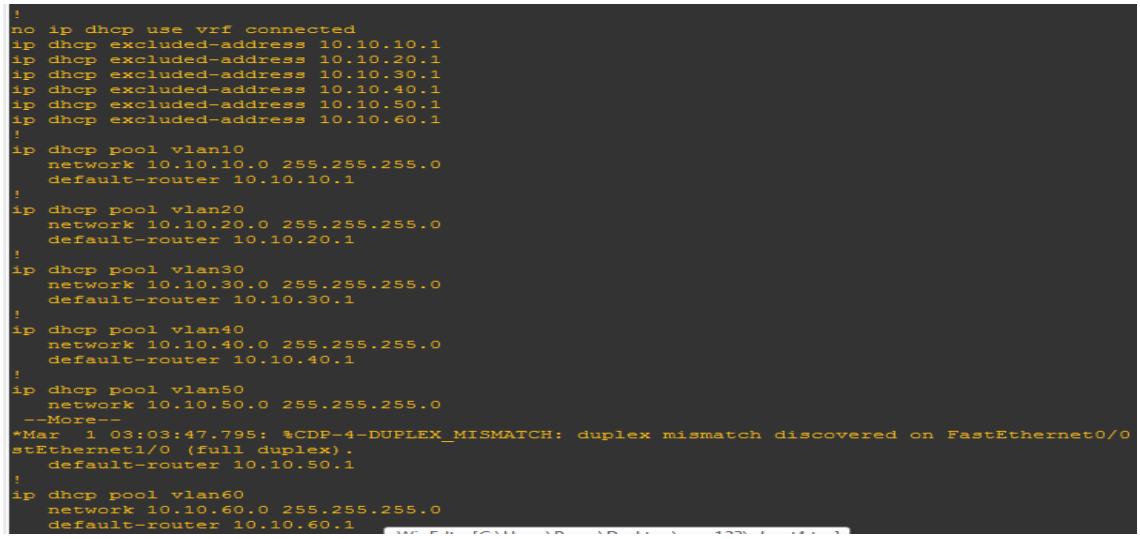


FIGURE 4.12 – DHCP pools

```
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 10
 ip address 10.10.10.1 255.255.255.0
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
 ip address 10.10.20.1 255.255.255.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 30
 ip address 10.10.30.1 255.255.255.0
!
interface FastEthernet0/0.4
 encapsulation dot1Q 40
 ip address 10.10.40.1 255.255.255.0
!
interface FastEthernet0/0.5
 encapsulation dot1Q 50
 ip address 10.10.50.1 255.255.255.0
!
interface FastEthernet0/0.6
 encapsulation dot1Q 60
 ip address 10.10.60.1 255.255.255.0
!
```

FIGURE 4.13 – Sous interfaces du routeur

4.7.2 Ajout d'une ACL

```
R1#
*Mar  1 02:11:18.819: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
stEthernet1/0 (full duplex).
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access
R1(config)#access-list 100 permit icmp 10.10.20.0
*Mar  1 02:12:18.827: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
stEthernet1/0 (full duplex).
R1(config)#$t icmp 10.10.20.0 0.0.0.255 10.10.60.0 0.0.0.255 echo-reply
R1(config)#int f
*Mar  1 02:13:18.871: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
stEthernet1/0 (full duplex).
R1(config)#int f0/0.6
R1(config-subif)#ip access
R1(config-subif)#ip access-group 100 out
R1(config-subif)#
```

FIGURE 4.14 – Ajout d'une ACL

Cette configuration autorise le trafic ICMP de passer par le réseau du VLAN 10 mais pas le contraire , de la même manière nous avons crées les autres listes d'accé avec le même numéro pour le reste des VLANs.

4.8 Vérification et test de connectivité avec VLAN

4.8.1 Vérification de la configuration

Pour vérifier que DHCP marche, nous allons dans l'icône "Tools" ensuite cliquez sur VPCs et nous allons faire les mêmes étapes vues dans la première partie.

```
VPCS[1]> ip dhcp
DDORA IP 10.10.20.2/24 GW 10.10.20.1

VPCS[1]> 2
VPCS[2]> ip dhcp
DDORA IP 10.10.30.2/24 GW 10.10.30.1

VPCS[2]> 3
VPCS[3]> ip dhcp
DDORA IP 10.10.50.2/24 GW 10.10.50.1

VPCS[3]> 4
VPCS[4]> ip dhcp
DDORA IP 10.10.40.2/24 GW 10.10.40.1

VPCS[4]> 5
VPCS[5]> ip dhcp
DDORA IP 10.10.20.3/24 GW 10.10.20.1

VPCS[5]> 6
VPCS[6]> ip dhcp
DDORA IP 10.10.50.3/24 GW 10.10.50.1

VPCS[6]> 7
VPCS[7]> ip dhcp
DDORA IP 10.10.30.3/24 GW 10.10.30.1

VPCS[7]> 8
VPCS[8]> ip dhcp
DDORA IP 10.10.50.4/24 GW 10.10.50.1

VPCS[8]> 9
VPCS[9]> ip dhcp
DDORRA IP 10.10.10.2/24 GW 10.10.10.1
```

FIGURE 4.15 – Affectation d'une adresse IP par le DHCP au PCs

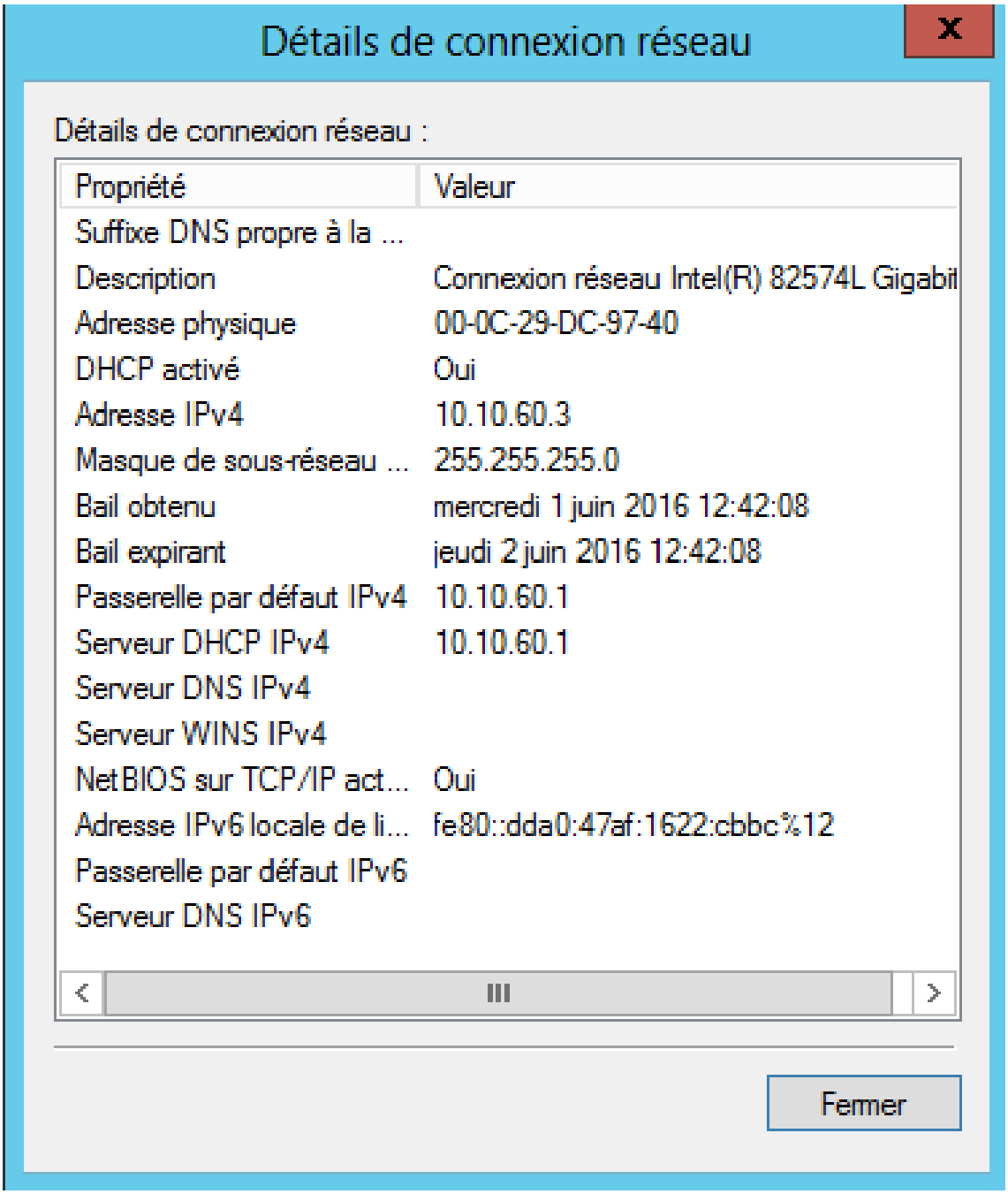


FIGURE 4.16 – Affectation d'une adresse IP par le DHCP au serveur

4.8.2 Test de connectivité

Afin de remédier au problème posé dans la première partie nous avons créé des VLANs pour une meilleure gestion du réseau de l'entreprise et nous avons fait un routage inter-vlan pour que les VLANs peuvent communiquer entre eux en faisant appel à cette commande " ip routing ". Voici une figure qui représente avant et après le routage inter-vlan :

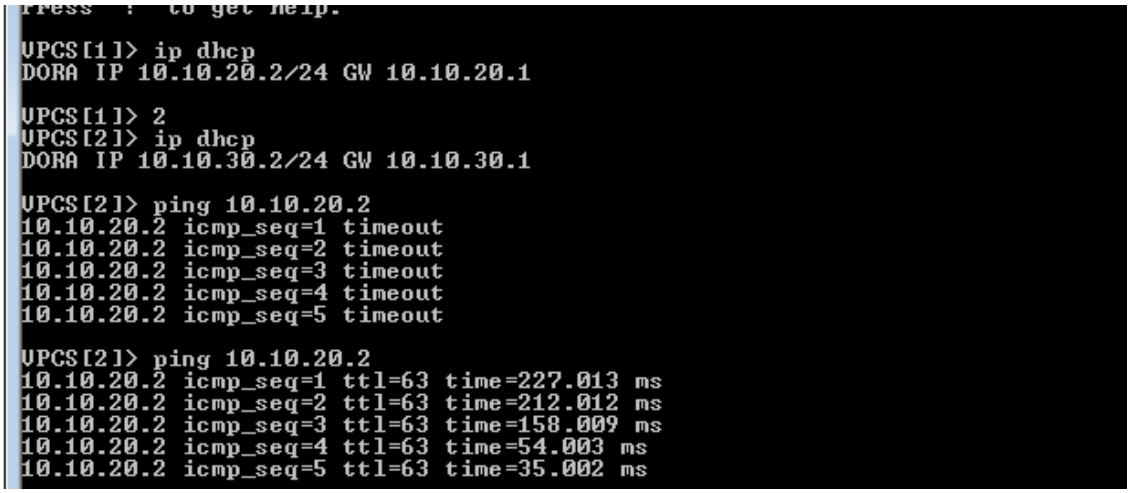


FIGURE 4.17 – Routage inter-vlan avant et après

Après la création des ACLs :

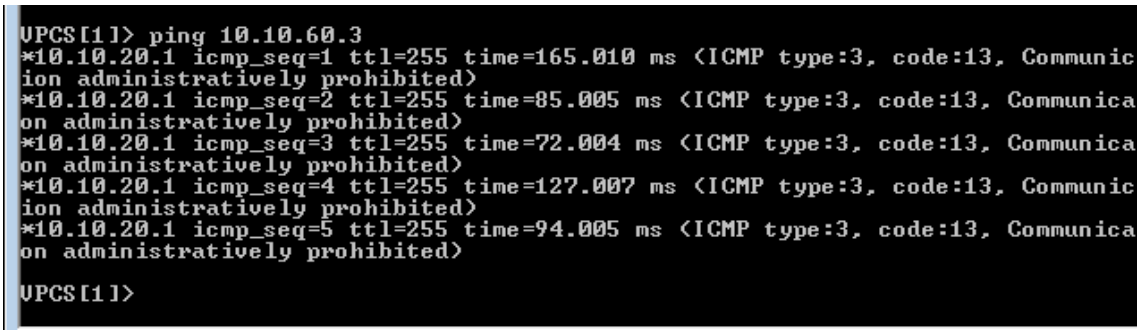


FIGURE 4.18 – Ping du PC1 vers le serveur

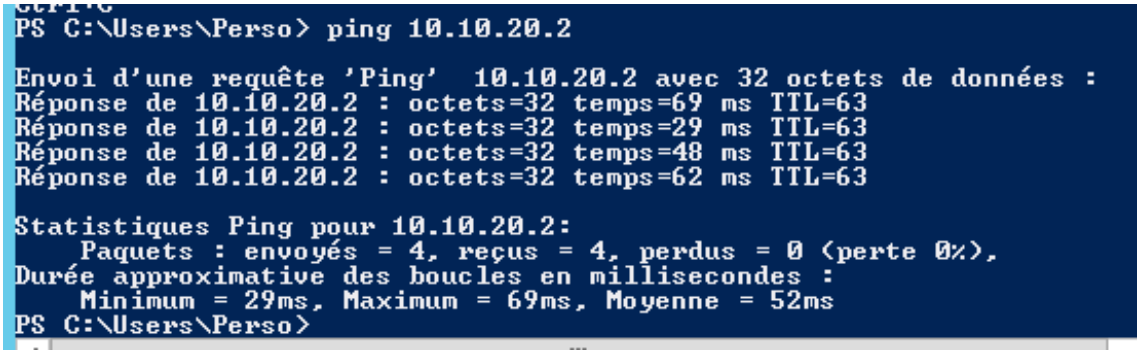


FIGURE 4.19 – Ping du serveur vers le PC1

4.9 Configuration du PRTG

4.9.1 Page d'accueil

Après avoir être authentifié, nous accedons à la page d'accueil PRTG :

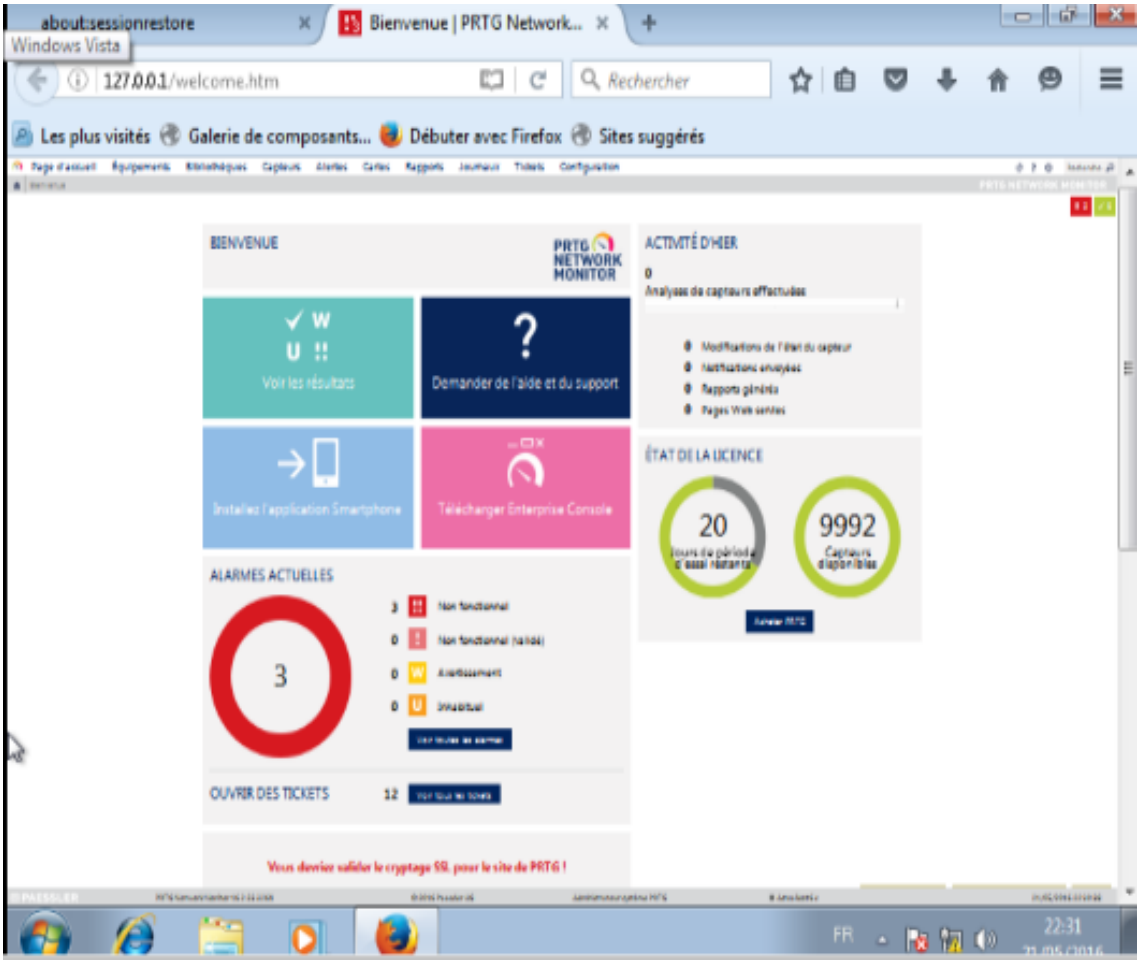


FIGURE 4.20 – Page d'accueil du PRTG

4.9.2 Ajout d'un groupe

Pour pouvoir surveiller notre réseau nous devons l'ajouter , pour cela nous allons ajouté un groupe nommé surveillance :

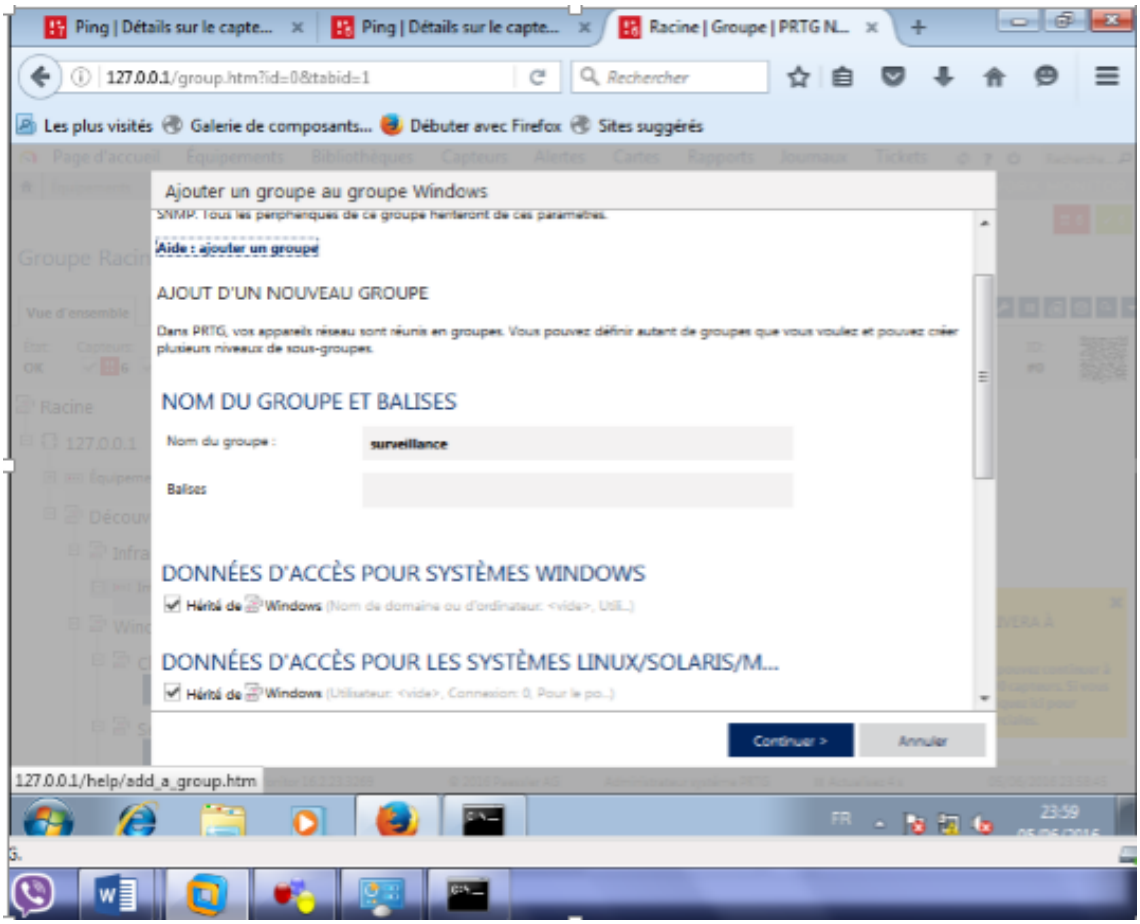


FIGURE 4.21 – Ajout du groupe surveillance

Après cette étape vient l'étape d'ajout des équipement que possède notre réseau.

4.9.3 Ajout des équipements

Nous allons ajouté notre routeur , nos 13 switchs et nos PCs. Avant d'ajouter n'importe quel équipement nous devons séléctionner le groupe où nous voudrions mettre nos équipements, pour notre cas nous allons ajouté tout nos équipements au groupe surveillance.

FIGURE 4.22 – Ajout de l'équipement routeur

La figure ci-dessus représente l'ajout d'un équipement en PRTG, en saisissant le nom de l'équipement et l'addresse de l'équipement.

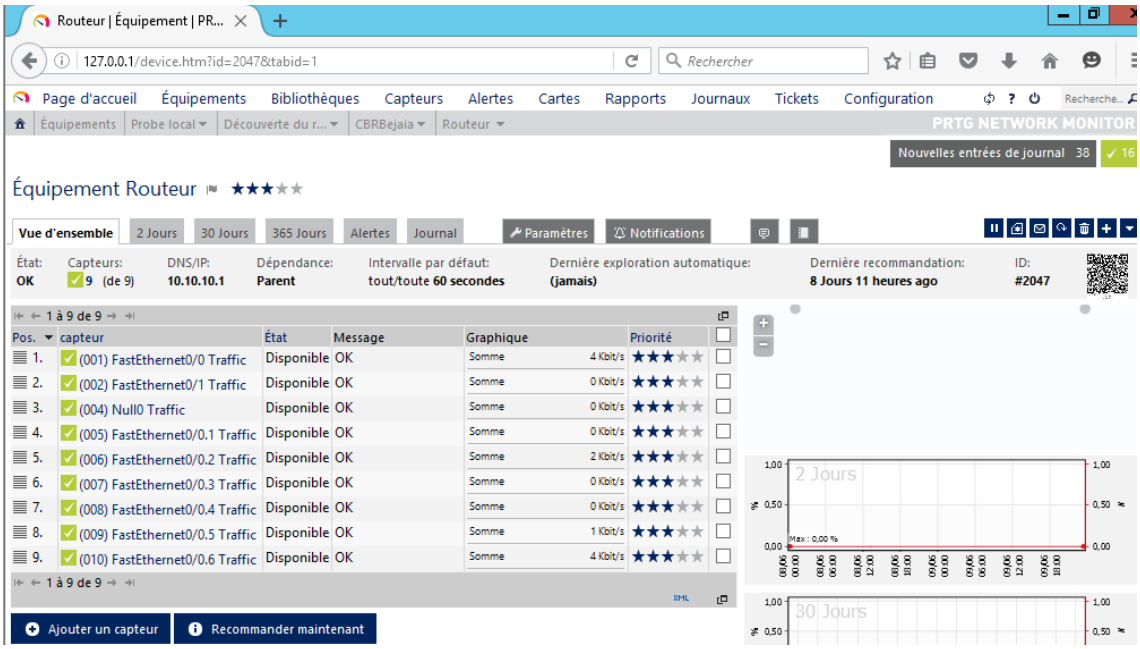


FIGURE 4.23 – Vue l'ensemble de l'équipement routeur

Comme nous remarquons, PRTG a automatiquement détecté les autres sous interfaces donc maintenant notre réseau émulé avec GNS3 dans une machine physique (Windows 7) est relié au PRTG installé dans la machine virtuelle VM Workstation.
De la même manière, nous avons procédés l'ajout des autres équipements(switch et pcs).

4.9.4 Ajout des capteurs

En PRTG, il existe plusieurs type de capteurs : PING, bande passande , utilisation UC, utilisation de la mémoire, HTTP , ...etc , mais dans notre cas , nous nous interéssons à la bande passante et au PING afin de surveiller notre réseau.

Ces capteurs sont classé selon la bibliothèque suivante :

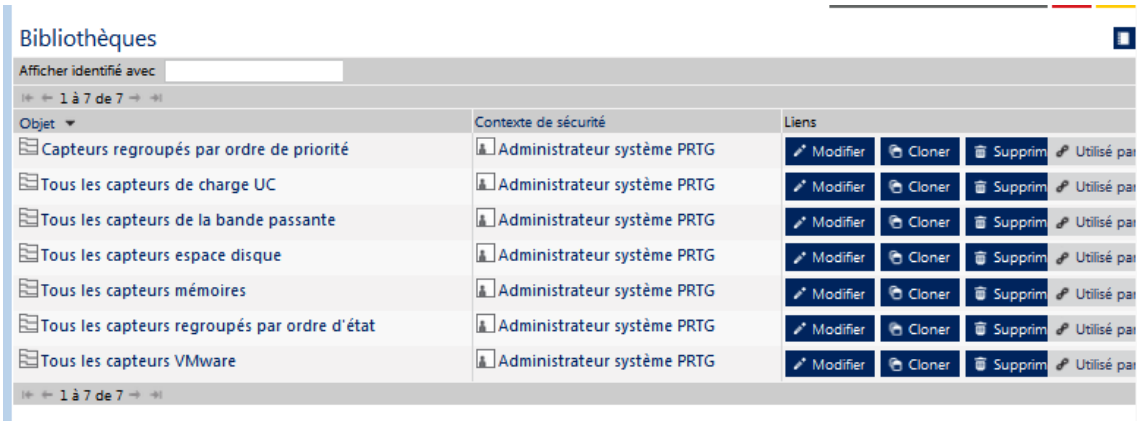


FIGURE 4.24 – Bibliothèque de PRTG

4.9.4.1 Ajout de capteur PING

la figure suivante représente l'ajoute d'un capteur PING qui permet de surveiller la connectivité.

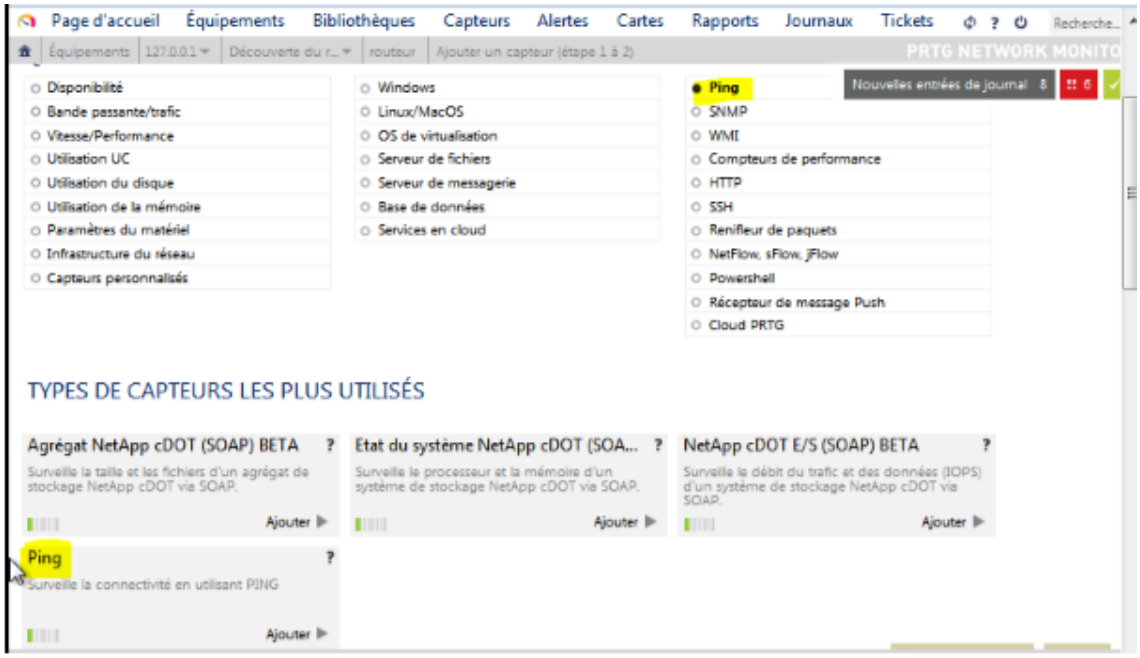


FIGURE 4.25 – Ajout d'un capteur PING

Pour consulter les détails du capteur ajouté il suffit de cliquer dessus, la figure suivante nous montre celà.

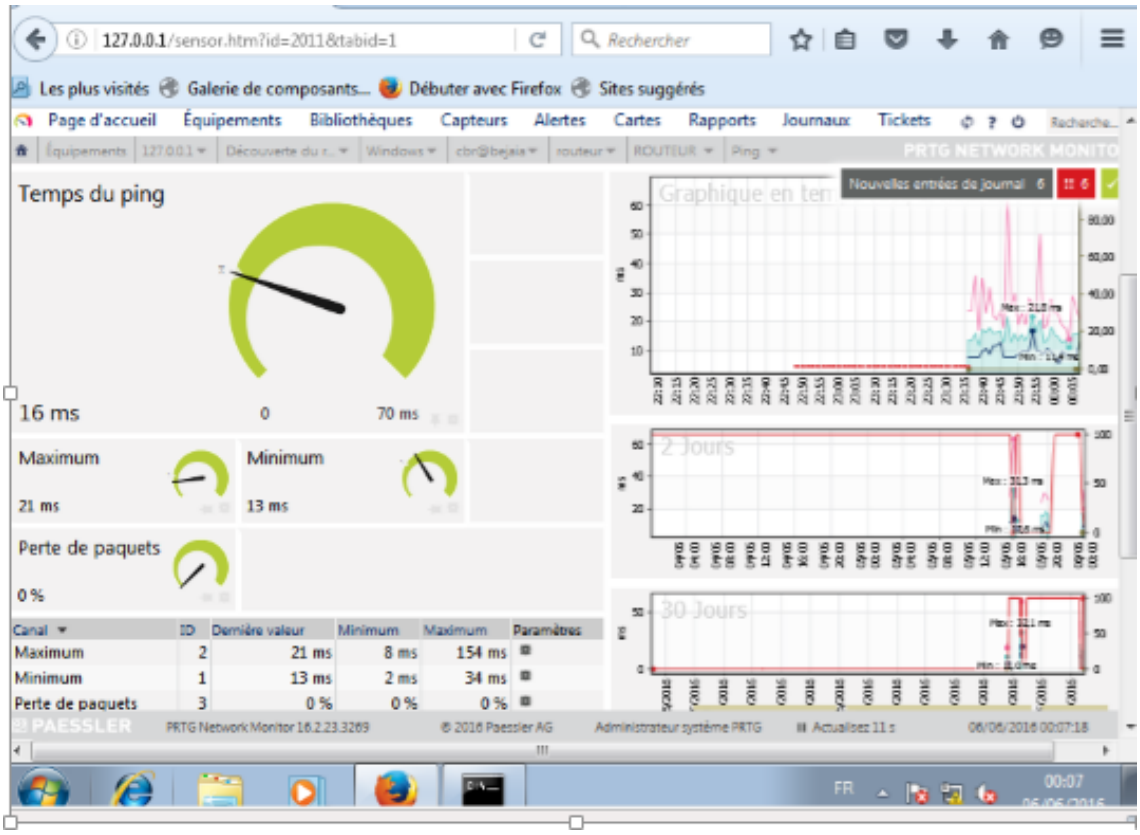


FIGURE 4.26 – Détails du PING

4.9.4.2 Ajout de capteur Bande Passante

La figure suivante représente l'ajout d'un capteur bande passante qui permet la surveillance de bande passante et le trafic des équipements en utilisant SNMP.

FIGURE 4.27 – Ajout d'un capteur bande passante

4.10 Surveillance du réseau avant et après les vlans

4.10.1 Avant les vlans

4.10.1.1 PING

Les figuress suivante représente la connectivité entre les ordinateurs. Le minimum du temps du ping est à 44ms et le maximum est plus de 468ms :

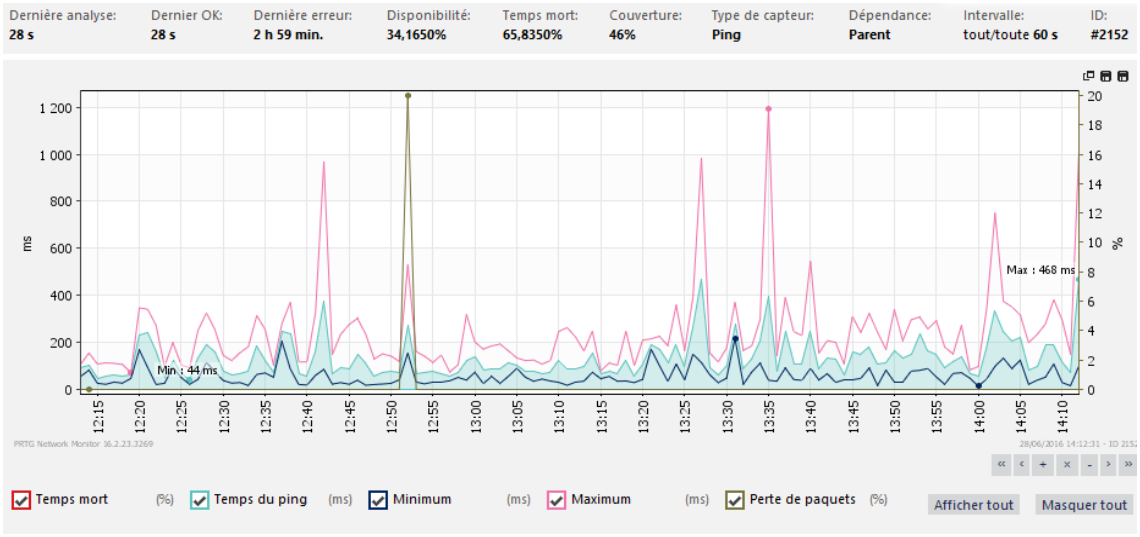


FIGURE 4.28 – Surveillance du PING en temps réel

Et pour cette surveillance le maximum est à environ 20 ms mais plusieurs temps mort se sont produit ce qui a provoqué des pertes de paquets

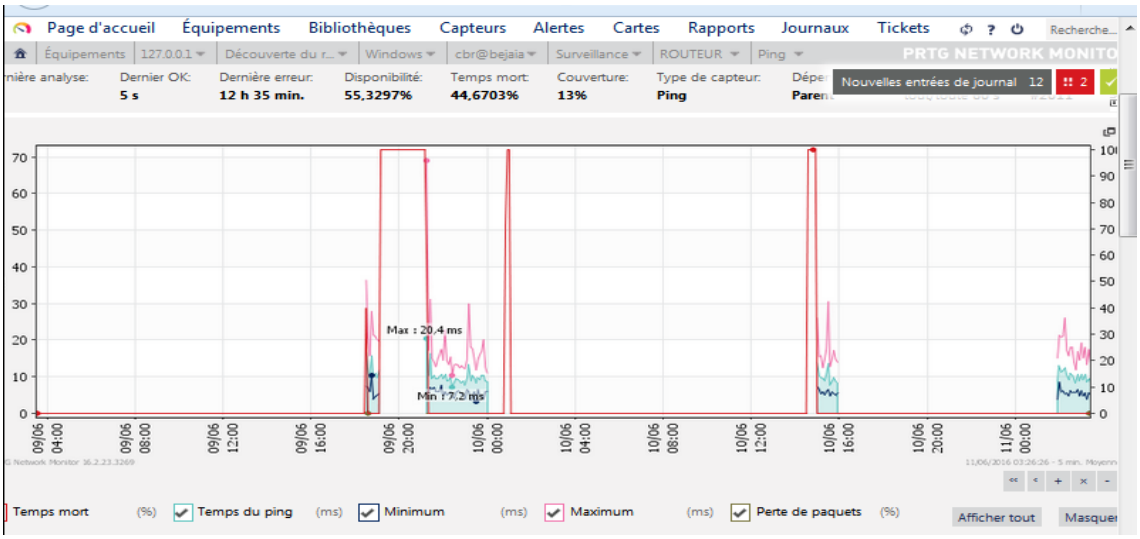


FIGURE 4.29 – Surveillance du switch pendant 2 jours

4.10.1.2 Bande Passante

La figure suivante représente la surveillance de la bande passante qui a comme valeur maximale = 3.75 kbit/s et 0.22kbit/s comme valeur minimale :

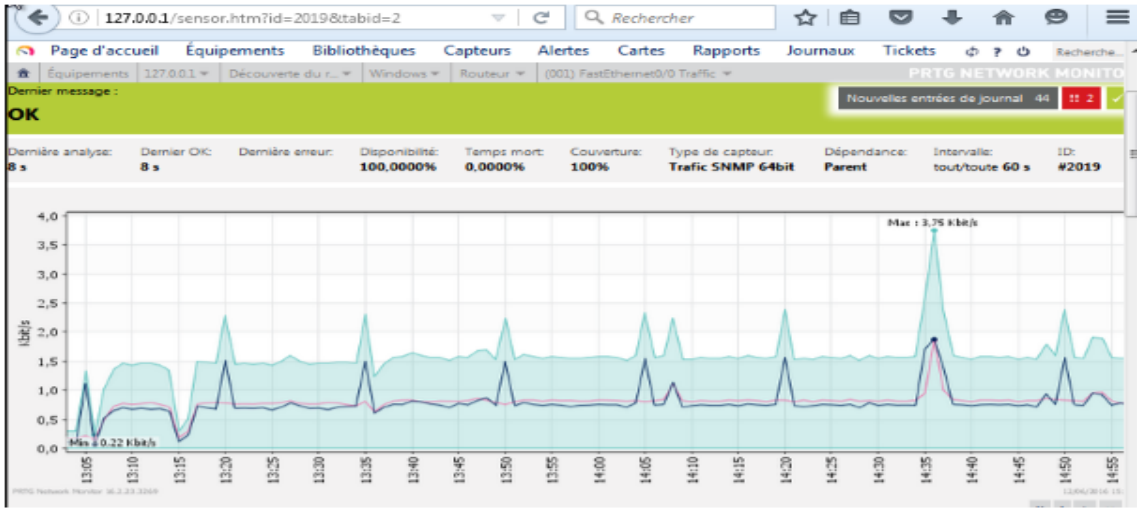


FIGURE 4.30 – Surveillance de la bande passante

4.10.2 Après les vlans

4.10.2.1 PING

Pour le PING après la mise en place des vlans nous voyons directement la différence le maximum est à 65ms et le minimum est à 6ms :

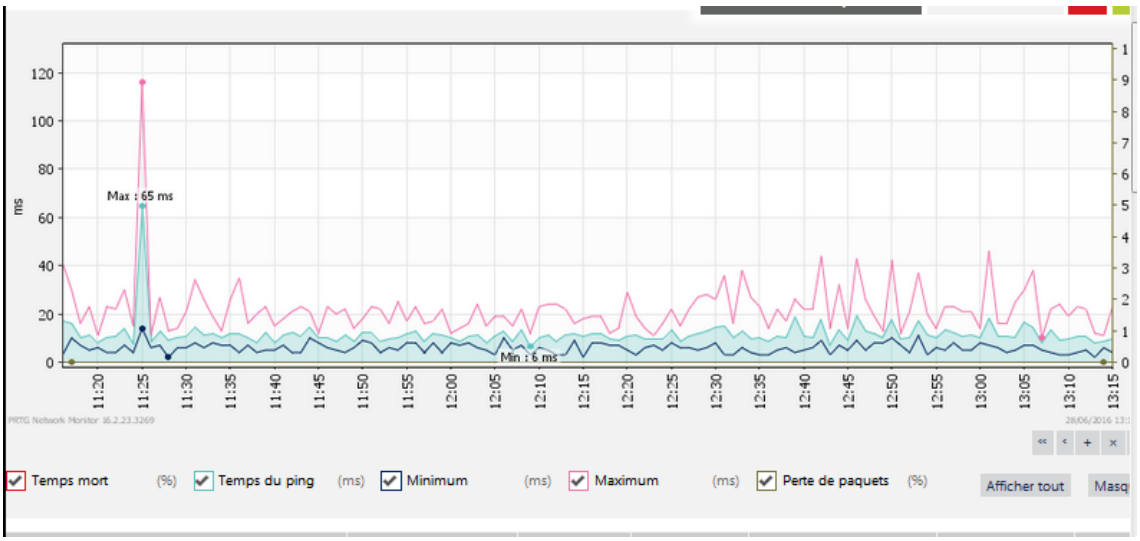


FIGURE 4.31 – Capteur de PING avec les vlans

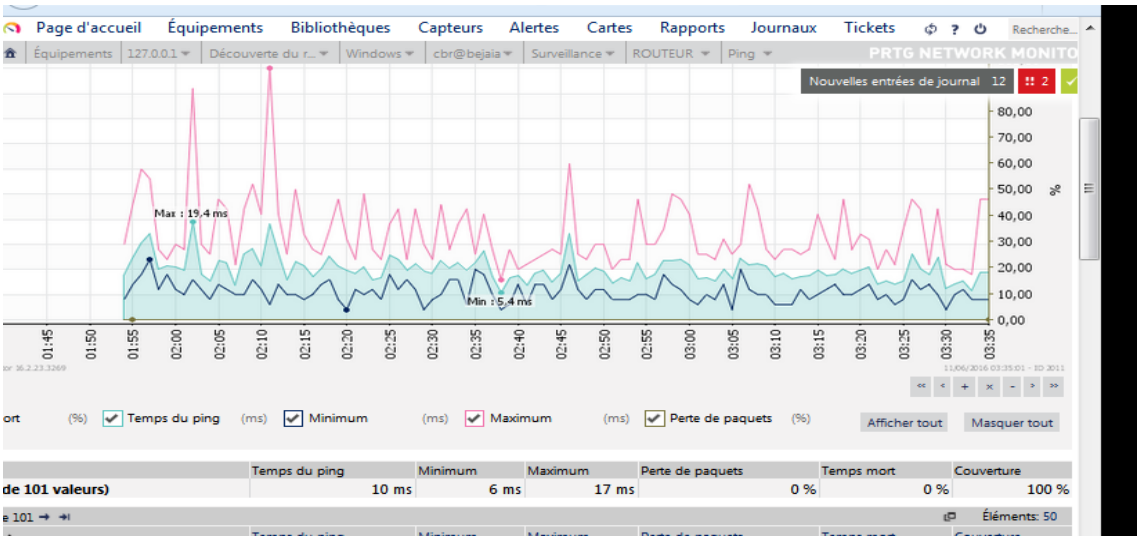


FIGURE 4.32 – Surveillance du switch en 2 jours

Nous remarquons qu'après la mise en place des VLANs le maximum a baissé et nous n'avons enregistré aucune perte de paquets.

4.10.2.2 Bande Passante

La figure suivante représente la surveillance du trafic de la bande passante en temps réel qui atteint 2.37kbit/s comme valeur maximale et 0.37kbit/s comme valeur minimale :

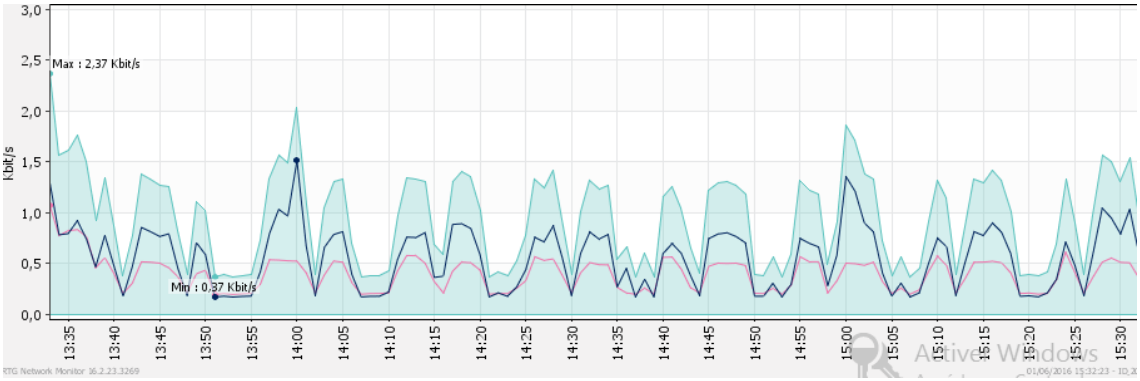
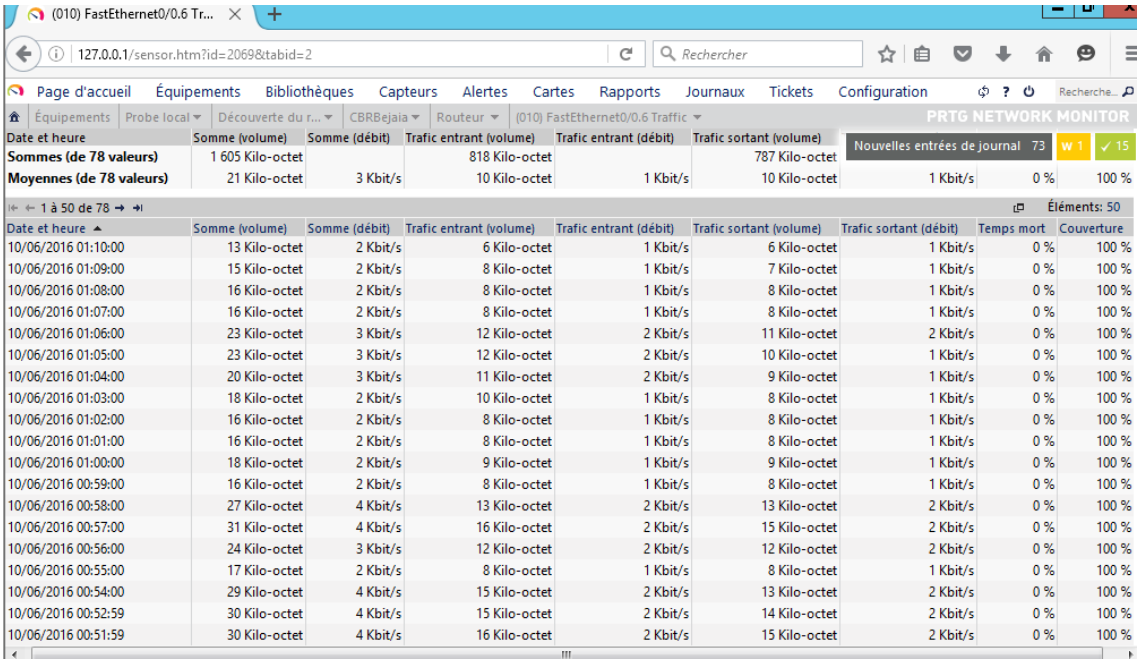


FIGURE 4.33 – Surveillance de la bande passante en temps réel

Pour consulter le détail du trafic il suffit de voir en dessous du graphe et vous allez avoir la figure suivante :



Date et heure	Somme (volume)	Somme (débit)	Trafic entrant (volume)	Trafic entrant (débit)	Trafic sortant (volume)	Trafic sortant (débit)	Temps mort	Couverture
Sommes (de 78 valeurs)	1 605 Kilo-octet		818 Kilo-octet		787 Kilo-octet			
Moyennes (de 78 valeurs)	21 Kilo-octet	3 Kbit/s	10 Kilo-octet	1 Kbit/s	10 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:10:00	13 Kilo-octet	2 Kbit/s	6 Kilo-octet	1 Kbit/s	6 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:09:00	15 Kilo-octet	2 Kbit/s	8 Kilo-octet	1 Kbit/s	7 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:08:00	16 Kilo-octet	2 Kbit/s	8 Kilo-octet	1 Kbit/s	8 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:07:00	16 Kilo-octet	2 Kbit/s	8 Kilo-octet	1 Kbit/s	8 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:06:00	23 Kilo-octet	3 Kbit/s	12 Kilo-octet	2 Kbit/s	11 Kilo-octet	2 Kbit/s	0 %	100 %
10/06/2016 01:05:00	23 Kilo-octet	3 Kbit/s	12 Kilo-octet	2 Kbit/s	10 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:04:00	20 Kilo-octet	3 Kbit/s	11 Kilo-octet	2 Kbit/s	9 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:03:00	18 Kilo-octet	2 Kbit/s	10 Kilo-octet	1 Kbit/s	8 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:02:00	16 Kilo-octet	2 Kbit/s	8 Kilo-octet	1 Kbit/s	8 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:01:00	16 Kilo-octet	2 Kbit/s	8 Kilo-octet	1 Kbit/s	8 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 01:00:00	18 Kilo-octet	2 Kbit/s	9 Kilo-octet	1 Kbit/s	9 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 00:59:00	16 Kilo-octet	2 Kbit/s	8 Kilo-octet	1 Kbit/s	8 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 00:58:00	27 Kilo-octet	4 Kbit/s	13 Kilo-octet	2 Kbit/s	13 Kilo-octet	2 Kbit/s	0 %	100 %
10/06/2016 00:57:00	31 Kilo-octet	4 Kbit/s	16 Kilo-octet	2 Kbit/s	15 Kilo-octet	2 Kbit/s	0 %	100 %
10/06/2016 00:56:00	24 Kilo-octet	3 Kbit/s	12 Kilo-octet	2 Kbit/s	12 Kilo-octet	2 Kbit/s	0 %	100 %
10/06/2016 00:55:00	17 Kilo-octet	2 Kbit/s	8 Kilo-octet	1 Kbit/s	8 Kilo-octet	1 Kbit/s	0 %	100 %
10/06/2016 00:54:00	29 Kilo-octet	4 Kbit/s	15 Kilo-octet	2 Kbit/s	13 Kilo-octet	2 Kbit/s	0 %	100 %
10/06/2016 00:52:59	30 Kilo-octet	4 Kbit/s	15 Kilo-octet	2 Kbit/s	14 Kilo-octet	2 Kbit/s	0 %	100 %
10/06/2016 00:51:59	30 Kilo-octet	4 Kbit/s	16 Kilo-octet	2 Kbit/s	15 Kilo-octet	2 Kbit/s	0 %	100 %

FIGURE 4.34 – Détail du trafic

Dans la figure suivante, nous avons effectués une autre capture sur une autre periode.

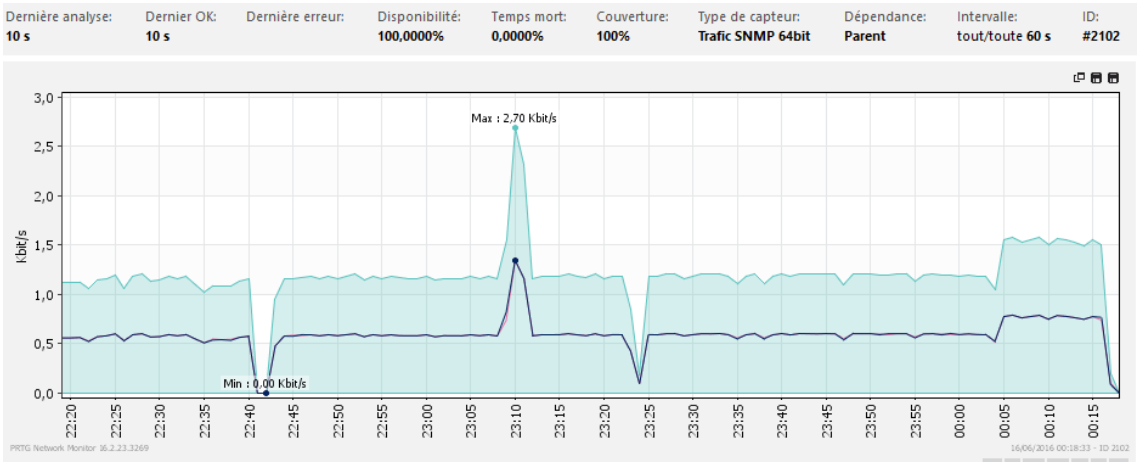
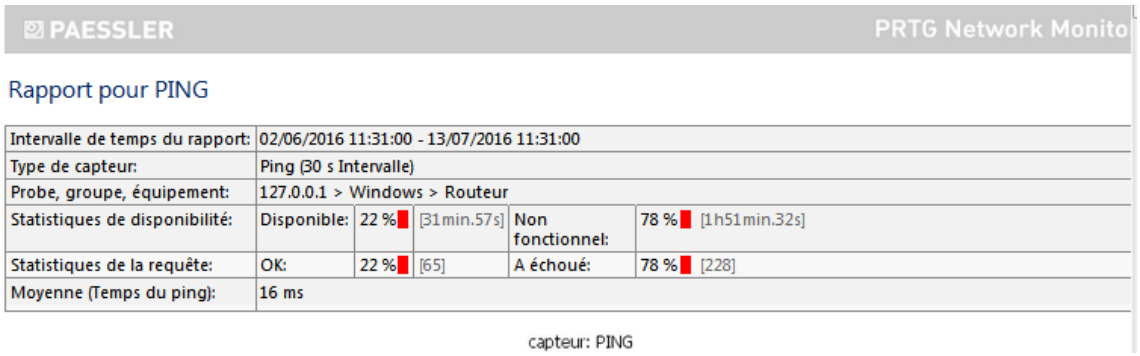


FIGURE 4.35 – Surveillance de la bande passante

Après la mise en place des VLANs le temps du ping idem pour l'utilisation bande passante ont diminués d'une façon remarquable notre solution est donc optimale.

Avec PRTG nous pouvons consulter le rapport du PING comme suit :


PAESSLER PRTG Network Monito

Rapport pour PING

Intervalle de temps du rapport:	02/06/2016 11:31:00 - 13/07/2016 11:31:00				
Type de capteur:	Ping (30 s Intervalle)				
Probe, groupe, équipement:	127.0.0.1 > Windows > Routeur				
Statistiques de disponibilité:	Disponible:	22 %	[31min.57s]	Non fonctionnel:	78 % [1h51min.32s]
Statistiques de la requête:	OK:	22 %	[65]	A échoué:	78 % [228]
Moyenne (Temps du ping):	16 ms				

capteur: PING

FIGURE 4.36 – Rapport du PING

4.11 Conclusion

Nous avons pu aboutir aux objectifs visés pour l'accomplissement de ce mémoire, après l'étude de chaque partie et une comparaison de graphes nous avons conclus que notre solution de départ est efficace car elle nous a permis un gain remarquable d'utilisation de bande passante et donc nous avons pu régler un problème majeur au niveau de l'entreprise .

Conclusion et perspectives

Au terme de ce projet, nous pouvons dire qu'avoir un réseau c'est bien mais, se munir de puissants outils d'administration et de supervision c'est encore mieux. Bien que notre travail ne soit pas parti d'un besoin exprimé, nous avons pu prouver son importance. Notre encadreur au sein de l'entreprise a rapidement compris sa nécessité et accepter de nous guider et de nous appuyer ce qui nous as permis de nous donner à fonds et mener à bout notre travail.

Nous avons été étonnés des possibilités qui s'offraient à nous après la mise sur pied de notre travail. PRTG bien qu'assez complexe à configurer, nous permet ainsi de surveiller, maîtriser et réagir au comportement de chaque équipement de notre réseau.

Il ne nous reste plus qu'à assurer l'inévitable souci, le plus gênant dans les réseaux informatique qui est les pannes des équipements, sans logiciel de surveillance aucun ne peut identifier le problème et le régler en un petit laps de temps, donc il y aura une perte de données. Ce qui va causer des perturbations dans le système. Nous avons donc pu atteindre notre objectifs et avoir enfin un réseau répondant toujours à nos attentes, ce qui est obligatoire surtout dans un domaine tel que l'informatique, réputé pour ses constantes évolutions.

Notre travail peut être amélioré en développant les points suivant :

- Simuler le réseau réel avec le même nombre d'ordinateurs.
- Intégration de notre solution par les autres districts de NAFTAL.
- Utiliseation d'autres logiciels de monitoring réseau open source.

Bibliographie

[1] Bertrand Alain. Cours reseaux informatique. http ://www.formationgratuit.com/fr/reseau-informatique/cours-reseaux-informatique/orderby5, Mis en ligne le 20 avril 2005.

[2] Olivier Dalle. Introduction aux réseaux. Mars 2014.

[3] Ndimurundo Dieudonné. *Windows Server 2012*. PhD thesis, Epreuve intégrée de la promotion sociale de Saint-Gilles, Année académique 2012-2013.

[4] Sylvain et Christian. Dhcp. `http://www.frameip.com/dhcp`, En juin 2003, par Christian et En septembre 2000, par Sylvain, création du document.

[5] L'équipe Freeduc-Sup. Tutoriel sur les serveurs. `http://www.linux-france.org/prj/edu/archinet/systeme/ch27s02.html`, 2004.

[6] L'équipe Freeduc-Sup. Les listes d'accès. `http://www.technologuepro.com/reseaux/Configuration-des-ACLs/les-ACLs.html`, Révisé le :24-09-2010.

[7] ADJIDO Idjiwa. *Rapport sur la mise en place d'une solution de supervision avec Nagios*. PhD thesis, Université de NANTES, Promotion 2004-2005.

[8] YBET informatique. Introduction aux réseaux informatiques. `http://www.ybet.be/hardware2_ch2/hard2_ch2.php`, 2015.

[9] B. Jaumard. Les équipements d'interconnexion. Jan 2003.

[10] Philippe Latu. Adressage ipv4. `http://www.inetdoc.net`, 2000-2016.

[11] Serge Leblal. Avec prtg, paessler propose d'anticiper la croissance du réseau. `http://www.lemondeinformatique.fr/actualites/lire-avec-prtg-paessler-propose-d-anticiper-la-croissance-du-reseau-58188.html`, Le 28 Juillet 2014.

[12] Stéphane Maas. Ii. configurer gns3. http://www.smnet.fr/gns3/gns3-conf.html, 2013-2016.

[13] Stéphane Maas. Partie i. installer gns3 sur windows et debian. http://www.smnet.fr/gns3/gns3-install-intro.html, 2013-2016.

[14] Stéphane Maas. V. gns3 rÉseau n° 3. http://www.smnet.fr/gns3/gns3-res3.html, 2013-2016.

[15] Patrick Siarry Malek Rahoual. *Réseaux inormatiques : conception et optimisation*. Editions TECHNIP 27 rue Ginoux, 75737 PARIS Cedex 15, FRANCE, 2006.

[16] Hadrien MARQUET. Etude des outils de surveillance (monitoring) réseau. http://www.o00o.org/monitoring/solutions.html#footer, 2008-2009.

[17] Ahmed Mehaoua. - partie 4 -interconnexion de réseaux. page pp.28, Mar 2005.

[18] Rziza Mohammed. Cours des réseaux informatiques.

[19] NAFTAL. *Présentation du District CBR de Béjaïa*.

[20] PAESSLER. *PRTG Network Monitor V8 Mise en route*. PhD thesis.

[21] Fondateur de CommentCaMarche.net. Réalisé sous la direction de Jean-François PILLOU. *VLAN - Réseaux virtuels*. PhD thesis.

[22] Groupe randstad. *Supervision réseau utilisant le protocole SNMP*. PhD thesis.

[23] Quentin SCHUELLER. Modèle osi et modèle tcp/ip. Sep 2015.

[24] Patrick Siarry. *Supervision des réseaux*. PhD thesis, Université de NANTES, Dernières modifications le 30/05/13.

[25] Julien Soulas. Les reseaux d'ordinateurs. http://jetel.free.fr/inf_rsx.htm, Mise à jour du 18/6/2001.

[26] Réalisé sous la direction de Jean-François PILLOU. Le protocole snmp. http://www.commentcamarche.net/contents/537-le-protocole-snmp, 2016.

[27] Fabien Troussel. Vmware workstation. http://www.tuto-it.fr/vmware.php, 2010.

[28] Fabien Troussel. Les différents types de réseaux informatiques. May 2015.

RÉSUMÉ

Notre projet concerne la supervision d'un réseau d'entreprise et la proposition de solutions permettant l'optimisation de ce dernier. Nous avons pu mettre en place et configurer une station de surveillance PRTG chargée d'informer l'administrateur de l'état global du réseau et l'alerter en cas de pannes ou de dysfonctionnement de ces différents composants.

Nous avons installés et configurés ce logiciel au sein du District Carburants NAFTAL de Béjaïa, après une surveillance d'un mois de leur réseau local, nous avons remarqués une forte utilisation de bande passante, ce qui nous a poussé à proposer la segmentation du réseau en un ensemble de vlans.

Nous avons donc émulés notre solution avec le logiciel GNS3, avant et après la mise en place des vlans et relier ces réseaux via une VMware avec PRTG. Après avoir comparer les graphes d'utilisation de bande passante avant et après les vlans nous avons pu constater le changement. Nous avons donc réglés le problème rencontré lors de notre surveillance du réseau local réel de l'entreprise.

Mots clés : PRTG, bande passante, vlans, GNS3 , VMware

ABSTRACT

Our project concerns supervision of an corporate network and the proposition of solutions for the optimization to the latter, in this study we have installed and configured PRTG monitoring station responsible to inform the administrator of overall state of the network and alert it in case of breakdowns or malfunction of different components.

We have installed and configured this software within the District CBR NAFTAL of Béjaïa , after monitoring a month of their local network, we have noticed a high bandwidth utilization, which led us to offer network segmentation a set of vlans.

We have emulated our solution with GNS3 software after and befor the establishment of VLANs , and connected via a VMware these simulated network with PRTG. After having compared the graphs of bandwidth usage we notice that there are changes, so we had really solved the problem encountered during monitoring of the actual local network of the company.

Keywords : PRTG , bandwidth , Vlan , GNS3 , Vmware