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 fin d'études
En vue de l'obtention du diplôme de Master Professionnel en Informatique
Option : Administration et Sécurité des Réseaux

Thème

Administration et Supervision d'un Réseau LAN à l'aide des solutions open source

Cas : Entreprise SONATRACH Béjaia

Présenté par : Mlle BENBARA Naziha et Mlle BOUCHAMA Nesrine

Soutenu le 01 Juillet 2017 devant le jury composé de :

Président	**N.KHOULALENE**	**Maître Ass. A**	**U. A/Mira Béjaia.**
Rapporteurs	**M. MOKTEFI**	**Maître de conf. B**	**U. A/Mira Béjaia.**
	M. ATMANI	**Maître de conf. B**	**U. A/Mira Béjaia.**
Examinateurs	**K. BEDJOU**	**Maître Ass. A**	**U. A/Mira Béjaia.**
	K. OUAZINE	**Doctorante "LMD"**	**U. A/Mira Béjaia.**
Invité	**K. SOUADIH**	**Résponsable du Rés.**	**Sonatrach Béjaia.**

Béjaia, Juillet 2017.

⁕ *Remerciements* ⁕

Nous remercions en premier lieu le bon DIEU de nous avoir donnée les moyens, l'énergie mais surtout la volonté nécessaire pour la réalisation de ce modeste travail.

Et nous adressons nos vifs remerciements et notre gratitude

Â :
Nos chers parents pour tous les sacrifices consentis à notre égard et leur énorme soutien.
Nous tenons à adresser nos plus profonds et sincères remerciements à notre encadreur M^r MOKTEFI Mohand, et
notre Co-encadreur M^r ATMANI Mouloud, de nous avoir encadré et guidé tout au long de ce projet,
pour leurs conseils et leurs encouragements, pour leur disponibilité et leur compréhension.

Nos vifs et chaleureux remerciements s'adressent également à M^r SOUADIH Kamel, pour tous ses orientations, ses conseils, sa tolérance et sa disponibilité, Ainsi qu'à tout le personnel de l'entreprise SONATRACH particulièrement : M^r IDIRI Karim et M^r BOUOUNE Noureddine pour leurs orientations et accueil sympathique lors de la période du stage.

Nous tenons à remercier tous ceux qui nous ont
soutenu et aidé dans la réalisation
de ce mémoire de prés ou de loin.
Nous remercions, enfin, les membres de jury qui ont accepté d'évaluer ce mémoire.

⁂ *Dédicaces* ⁂

Au nom de Dieu,

C'est avec gratitude et développement total que nous tiendrons ce rapport :
A nos chers parents qui n'ont jamais cessé de nous faire des sacrifices de toutes nature pour nous permettre de suivre nos études dans de meilleures conditions.
A nos professeurs particulièrement notre encadreur et Co-encadreur qui ont déployés tous leurs efforts pour nous préparer à affronter la vie professionnelle.

Nos frères et soeurs.

Nos grands parents.

Nos tantes, nos oncles et leurs femmes.

Nos cousins et cousines.

Tous nos adorables amis.

Ainsi à tous ceux qui nous ont soutenus par leurs orientations, leurs conseils durant la réalisation de ce travail, qu'ils trouvent ici l'expression de notre grande reconnaissance et l'assurance de nos profonds respects.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

ANSI : American National Standards Institute.
ARP : Address Resolution Protocol.
BDD : Base De Données.
BPDU : Bridge Protocol Data Units.
CentOS : Community enterprise Operating System.
DARPA : Defense Advanced Research Project Agency.
DoD : Department of Defense.
DNS : Domain Name System.
DMZ : Demilitarized Zone.
DHCP : Dynamic Host Configuration Protocol.
EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité.
FDDI : Fiber Distributed Data Interface.
FTP : File Transfer Protocol.
GNS3 : Graphical Network Simulator.
HTTP : HyperText Transport Protocol.
IBM : International Business Machines Corporation.
IEEE : Institute of Electrical and Electronics Engineers.
ICMP : Internet Control and error Message Protocol.
IP : Internet Protocol.
IBM : International Business Machines Corporation.
LAN : Local Area Network.
MEHARIE : Méthode Harmonisée d'Analyse Risques.
MARION : Méthodologie d'Analyse des Risques Informatiques Orientée par Niveaux.
MAU : Medium Access Unit.
MAC : Media Access Control.
MAN : Metropolitan Area Network.
NOS : Network Operating System.
OSI : Open Systèmes Interconnexion.
OSPF : Open Shortest Path First.
PPP : Point to Point Protocol.
PAN : Personal Area Network.

POE : Power Over Ethernet.
QoS : Qualité de Service.
RIP : Routing Information Protocol.
RARP : Reverse Address Resolution Protocol.
RTC : Region de Transport Centre.
RNIS : Réseau Numérique à Intégration de Services.
SI : Système d'Information.
SOPEG : Société Pétrolière de Gérance.
STP : Spanning Tree.
SLIP : Serial Line Interface Protocol.
SNMP : Simple Network Management Protocol.
SMTP : Simple Mail Transfer Protocol.
TCP : Transmission Control Protocol.
TFTP : Trivial File Transfer Protocol.
USB : Universal Serial Bus.
VLAN : Virtual LAN.
VTP : VLAN Trunking Protocol.
WAN : Wide Area Network.
WLAN : Wireless Local Area Network.
yum : Yellow dog Updater

Introduction générale

Actuellement aucune entreprise ne peut se passer d'outils informatiques, et très souvent un réseau informatique de taille plus ou moins importante est mis en oeuvre. Le nombre de machines dans ces réseaux peut parfois devenir extrêmement élevé, la maintenance ainsi que la gestion de ces parcs informatiques deviennent alors des enjeux cruciaux, d'autant plus qu'une panne de réseau peut parfois avoir des conséquences catastrophiques.

C'est pourquoi les administrateurs réseaux font appel à des logiciels de surveillance et de supervision de réseaux. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir une vue d'ensemble en temps réel sur le parc informatique qui est sous sa responsabilité. Il peut être aussi informé (par email, par sms) en cas de problème. Grâce à un tel système, les délais d'interconnexions et de maintenance sont fortement réduits.

Plusieurs logiciels réalisent ces tâches, comme par exemple Websense, Tivoli, Observer, Hp, Openview, Zabbix, Nagios et d'autres, mais certains sont payants. Dans ce domaine, un logiciel fait office de référence : Nagios. En effet Nagios est très performant et possède une prise en main assez intuitive. Il s'installe sur une machine possédant un système d'exploitation Linux que Windows. Cet outil permet également une supervision des équipements réseau (routeur, switch) ce qui est primordial dans notre cas.

De plus, Nagios est un outil open source, chaque société peut l'adapter comme elle veut. Puis, la société ne payera pas de licence, elle ne payera que les frais de formation, d'installation et de maintenance.
Enfin un autre avantage : Nagios a une grosse communauté qui est réunie autour de ce logiciel, ce qui facilite la recherche de documentation et de réponses à nos questions.
Notre projet consiste en premier lieu à définir d'une manière générale les réseaux informatiques, puis dans le 2eme chapitre on s'intéressera à l'administration des réseaux afin de comprendre les concepts de base sur les réseaux commutés et les éléments indispensables qui contribuent à sa réalisation sans oublier le concept de virtualisation. Dans le troisième chapitre nous allons entamer la méthode audit en illustrant ces différentes types, sa nécessité et ses différentes méthodologies,

nous passons par la suite à la contribution de l'audit interne au niveau de réseau LAN de la RTC, nous finissons par la détection des anomalies.

Durant notre stage pratique nous avons pu constater au sein du service Système et Réseaux de nombreuses questions telles que :
- Est-il indispensable d'administrer un réseau informatique d'entreprise ?
- Ya-il un moyen de détection de panne ainsi que l'augmentation de performance de réseau ?
- Et malgré l'existence de logiciels gratuits, l'entreprise poursuit l'utilisation des logiciels payant qui augmente le coût de l'entreprise !

Afin de répondre à ces problèmes nous avons fixé quelques objectifs tels que l'utilisation d'outils open source afin d'administrer et superviser le réseau LAN de SONATRACH. Ainsi notre rapport contiendra un dernier chapitre qui sera consacré à la réalisation de notre projet qui montre l'implémentation de notre réseau ainsi que sa configuration sous GNS3 et toutes les installations qui ont été faites sous Vmware Workstation afin de mettre en place un système d'exploitation open source CentOS 6.9 et Nagios, sachant que ce dernier est un programme qui se fixe sous CentOS 6.9, et qui offre une nouvelle interface graphique.

Nous terminons notre mémoire par une conclusion générale et perspectives de notre travail.

Chapitre 1

Aperçu général sur les réseaux informatiques

1.1 Introduction

Un réseau informatique permet à plusieurs machines (ordinateurs au sens large) de communiquer entre elles afin d'assurer des échanges d'informations : transfert de fichiers, partage de ressources (imprimantes et données), utilisation de la messagerie ou l'exécution de programmes à distance.

Dans un premier temps, ces communications étaient uniquement destinées au transfert de données informatiques. Aujourd'hui avec l'intégration de la voix et de la vidéo, elle ne se limitent plus aux données mêmes si cela ne va pas sans difficulté.

Ce chapitre sera consacré à présenter les concepts de base liés aux réseaux informatiques.

1.2 Définition

Selon Tanenbaum Andrew, nous pouvons définir un réseau informatique comme étant un ensemble de deux ou plusieurs ordinateurs interconnectés entre eux au moyen des médias de communication avec pour objectif de réaliser le partage des différentes ressources matérielles et/ou logicielles existantes [23].

1.3 Types de réseaux filaires

Nous parlons de quatre types de réseaux en fonction de la localisation, de la distance et du débit [23].

- **Réseau PAN (Personnel Area Network) :** sont des réseaux personnels. Souvent de

faible portée, on l'utilise surtout pour les liaisons sans fil : souris, clavier, imprimante, etc. Il s'étend sur 1 mètre environ.

- **Réseau LAN (Local Area Network) :** c'est un ensemble d'ordinateurs et d'équipements informatiques reliés les uns aux autres dans un même bâtiment, site ou dans des sites différents ayant un air géographiquement proche ne dépassant pas 10 Km.

- **Réseau MAN (Métropolitain Area Network) :** c'est l'interconnexion des réseaux locaux se trouvant dans une même ville ou dans une même région. Ce réseau peut utiliser des lignes du réseau public (service de télécommunication, radiocommunication, câbles téléphoniques, ...) ou privées pour assurer la liaison entre deux ou plusieurs sites. Il permet à des utilisateurs qui se trouvant à plusieurs endroits géographiques de partager les ressources par le réseau comme s'ils étaient dans un LAN. Dans ce type de réseau, la distance entre les sites ne dépasse pas 200 Km.

- **Réseau WAN (Wide Area Network) :** réseau étendu à longue distance constitué par l'interconnexion de plusieurs réseaux et qui se distingue des réseaux locaux et métropolitains. Il relie plusieurs ordinateurs notamment à travers une ville, un pays, continent ou encore toute la planète ; la communication s'effectue grâce aux réseaux privées et/ou publiques.

1.4 Intérêt d'un réseau

Un ordinateur est une machine permettant de manipuler des données. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations.
Un réseau informatique peut servir plusieurs buts distincts : le partage de ressources (fichiers, applications ou matériels), la communication entre personnes (courrier électronique, discussion en direct, etc.), la communication entre processus (entre des machines industrielles par exemple), la garantie de l'unicité de l'information (bases de données), le jeu vidéo multi-joueurs. Aujourd'hui, la tendance est au développement vers des réseaux étendus (WAN) déployés à l'échelle du pays, voire à l'échelle mondiale. Ainsi, les intérêts sont multiples, que ce soit pour une entreprise ou pour un particulier [14].

1.5 Caractéristiques

Un réseau informatique est caractérisé par les topologies, l'architecture, le protocole, le poste de travail, le support de transmission et le serveur, etc. Le choix de certains matériaux physiques

à utiliser dans le réseau informatique dépend de certaines caractéristiques physiques ou standards [14].

1.6 Architectures réseaux

Il existe deux types d'architectures logiques qui peuvent cohabiter sur une même architecture physique [14] :

- **L'architecture d'égal à égal :** (peer to peer, parfois appelée poste à poste), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur joue un rôle similaire,

- **L'architecture de type client-serveur :** où un ordinateur (serveur) fournit des services réseau aux ordinateurs clients.

1.7 Topologies d'un réseau informatique

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, liaisons sans fil, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé topologie physique. On distingue généralement les topologies suivantes : (la topologie en bus, la topologie en étoile, la topologie en anneau)[5].

1.7.1 Topologies physiques

La topologie physique désigne la manière dont les équipements sont interconnectés en réseau. Dans cette topologie nous avons trois grandes topologies qui sont [5] :

- **Topologie en bus :** c'est une organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câbles, généralement de type coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau. Cette topologie a pour avantage d'être facile à mettre en oeuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

- **Topologie en étoile :** dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur. Le concentrateur a pour rôle d'assurer la communication entre les différentes jonctions. Contrairement aux réseaux construits

sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible. En revanche, un réseau à topologie en étoile est plus onéreux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire (le concentrateur).

- **Topologie en anneau :** dans un réseau possédant une topologie en anneau, les ordinateurs sont théoriquement situés sur une boucle et communiquent chacun à leur tour. Les deux principales topologies logiques utilisant cette topologie physique sont Token Ring (anneau à jeton) et FDDI (Fiber Distributed Data Interface).

1.8 Matériels Réseaux

Les différents matériels du réseau informatique sont [6] :

- **L'ordinateur :** c'est un appareil électronique capable de traiter des informations de façon automatique. Il fournit à l'utilisateur d'un réseau l'ensemble des possibilités presque illimitées (manipulation des logiciels, traitement des données, utilisation de l'Internet).

- **Le serveur :** c'est un logiciel ou ordinateur très puissant choisit pour coordonner, contrôler et gérer les ressources d'un réseau. Il met ses ressources à la disposition des autres ordinateurs sous la forme des services.

- **Imprimante :** c'est une unité d'impression, un périphérique capable de reproduire les caractères et ou des symboles et des graphiques prédéfinis sur un support comme papier, bande, tissus,... Il existe des imprimantes réseau et des imprimantes en réseau.
  Imprimante réseau : c'est une imprimante conçue avec un port réseau (RJ45 par exemple) lui permettant de fonctionner dans un réseau comme un poste de station, il fonctionne en collaboration avec le serveur d'impression.

1.9 Supports de communication

Un support de communication transporte des données sous forme des signaux, entre les interfaces réseaux [19].

1.9.1 Supports physiques

Le support physique est évidemment l'élément indispensable pour transmettre des signaux d'un émetteur vers un récepteur. Par support physique, il faut entendre tous les éléments permettant de transmettre les éléments binaires, suites de 0 et de 1, sur des supports câblés aussi bien que hertziens. Ces équipements sont les suivants :

- Les supports physiques d'interconnexion qui permettent l'acheminement des signaux transportant l'information ;
- Les prises qui assurent la connexion sur le support ;
- Les adaptateurs qui se chargent notamment du traitement des signaux à transmettre ;
- Les coupleurs, aussi appelés communicateurs ou cartes de transmission, qui prennent en charge les fonctions de communication [19].

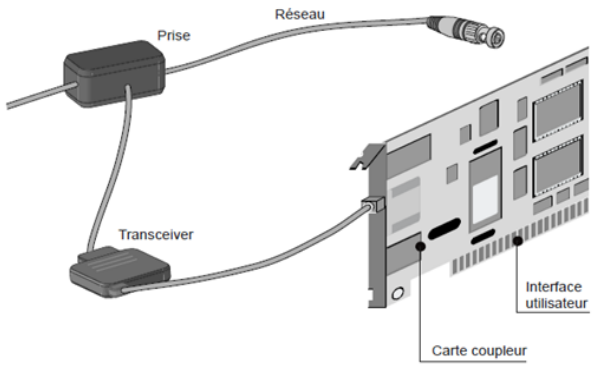

FIGURE 1.1 – Les équipements d'accès au support physique de transmission [19].

Les principaux supports utilisés dans les réseaux sont les fils métalliques, le câble coaxial, la fibre optique et les ondes hertziennes. Chacun de ces supports possède des caractéristiques très différentes en matière de bande passante, d'encombrement, d'affaiblissement ou de coût [19].

- **La paire de fils torsadés :** la paire de fils torsadés est le support de transmission le plus simple. Comme l'illustre la figure 1.2, elle est constituée d'une ou de plusieurs paires de fils électriques. Ce type de support convient à la transmission analogique comme numérique. Cependant, du fait que les câbles ne dépassent pas 0,2 à 1 mm de diamètre, l'affaiblissement des signaux véhiculés est très important, ce qui limite leur usage à des communications sur de courtes distances.

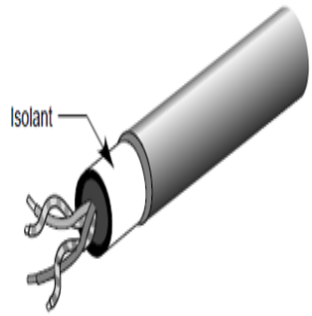

FIGURE 1.2 – La paire de fils torsadés [19].

Les paires torsadées peuvent être blindées, une gaine métallique enveloppant complètement les paires métalliques, ou non blindées [19].

- **Le câble coaxial :** un câble coaxial est constitué de deux conducteurs cylindriques de même axe, l'âme et la tresse, séparés par un isolant (voir figure 1.3). Ce dernier permet de limiter les perturbations dues au bruit externe. Si le bruit est important, un blindage peut être ajouté. Quoiqu'il perde du terrain, notamment par rapport à la fibre optique, ce support reste encore très utilisé [19].

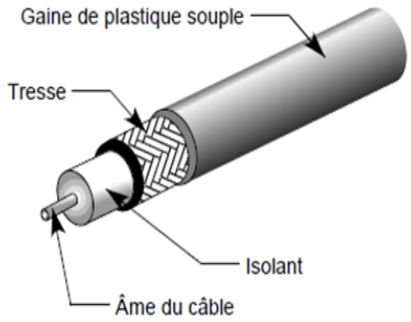

FIGURE 1.3 – La coupe d'un câble coaxial [19].

- **La fibre optique :** dans les fils métalliques, les informations sont transmises par le biais d'un courant électrique modulé. Avec la fibre optique, c'est un faisceau lumineux modulé qui est utilisé. Une connexion optique nécessite un émetteur et un récepteur. Pour la réaliser, différents types de composants sont envisageables.

  La figure 1.4 illustre la structure d'une liaison par fibre optique. Le faisceau lumineux est véhiculé à l'intérieur d'une fibre optique, qui n'est autre qu'un guide cylindrique d'un diamètre compris entre 100 et 300 microns et recouvert d'isolant [19].

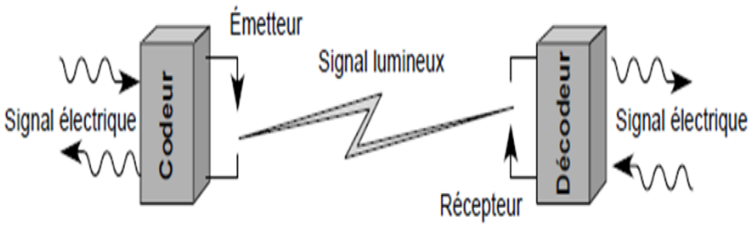

FIGURE 1.4 – Une liaison par fibre optique [19].

- **Les supports hertziens :** les communications par faisceaux hertziens se font en ligne directe de la tour d'émission à la tour de réception et ont un rayonnement très directif (line of sight). Ce type de transmission permet le multiplexage de nombreux canaux de communication autorisant ainsi un très grand débit de données [6].

1.10 Équipements intermédiaires d'un réseaux

Un système de télécommunications contient un support de transmission et des machines terminales. Pour les relier, il faut des équipements intermédiaires [19].

- **Le connecteur :** le connecteur réalise la connexion mécanique. Il permet le branchement sur le support. Le type de connecteur utilisé dépend évidemment du support physique [19].
  La figure 1.5 illustre un connecteur en T pour câble coaxial.

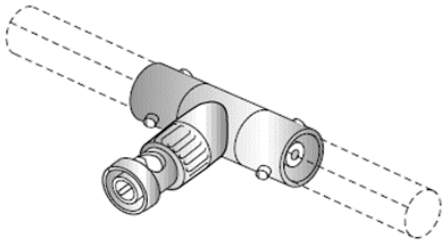

FIGURE 1.5 – Un connecteur en T pour câble coaxial [19].

- **L'adaptateur :** l'adaptateur (transceiver, ou transmetteur) est responsable de la connexion électrique. C'est un composant qui se trouve sur la carte qui gère l'interface entre l'équipement et le support physique. Il est chargé de la mise en série des octets, c'est-à-dire de la transmission des bits les uns après les autres. L'adaptateur effectue donc la sérialisation et la dé-sérialisation des paquets, ainsi que la transformation des signaux logiques en signaux transmissibles sur le support puis leur émission et leur réception [19].

- **Le coupleur :** l'organe appelé coupleur, ou carte réseau, ou encore carte d'accès (une carte Ethernet, par exemple), se charge de contrôler les transmissions sur le câble (voir la figure 1.6). Le coupleur assure le formatage et le déformatage des blocs de données à transmettre, la détection d'erreur, mais très rarement les reprises sur erreur lorsqu'une erreur est découverte. Il est aussi chargé de gérer les ressources telles que les zones mémoire ainsi que l'interface avec l'extérieur [19].

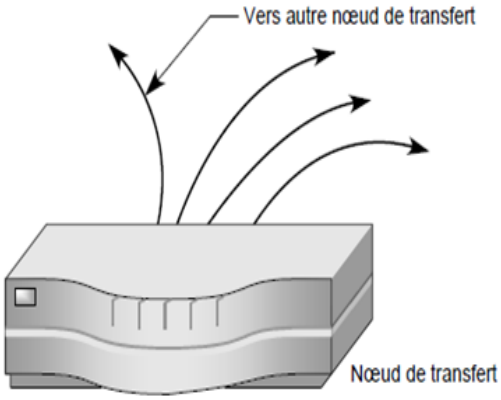

FIGURE 1.6 – Un noeud de transfert [19].

- **Le répéteur :** parmi les nombreux composants réseau qui font partie de la couche physique, le plus simple est le répéteur. C'est un organe non intelligent, qui répète automatiquement tous les signaux qui lui arrivent et transitent d'un support vers un autre support. Dans le même temps, le répéteur régénère les signaux, ce qui permet de prolonger le support physique vers un nouveau support physique. Le répéteur doit avoir des propriétés en accord avec le réseau [19].

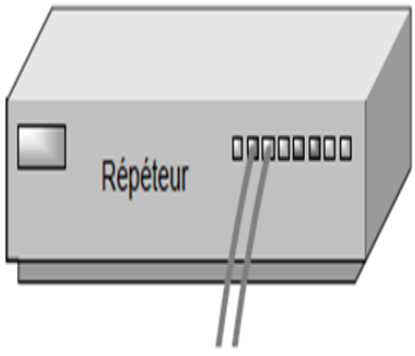

FIGURE 1.7 – Un répéteur [19].

- **Pont :** contrairement à un répéteur, un pont est un organe intelligent, capable de reconnaître les adresses des blocs d'information qui transitent sur le support physique. Un pont filtre les trames et laisse passer les blocs destinés au réseau raccordé. En d'autres

termes, un pont ne retransmet que les trames dont l'adresse correspond à une machine située sur le réseau raccordé. En général, un pont permet de passer d'un réseau vers un autre réseau de même type, mais il est possible d'avoir des ponts qui transforment la trame pour l'adapter au réseau raccordé. Par exemple, un réseau Ethernet peut être connecté à un réseau Token-Ring par un tel pont. Un pont est illustré à la figure 1.8 [19].

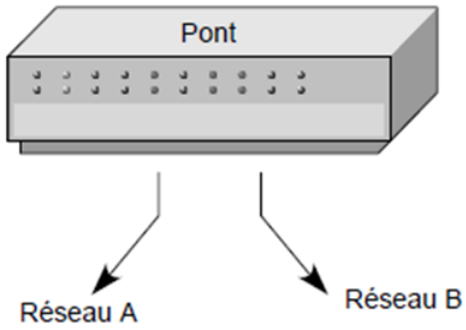

FIGURE 1.8 – Un pont [19].

- **Le hub :** un hub est un concentrateur capable de récupérer le signal arrivant par une entrée et de le dupliquer vers l'ensemble des portes de sortie. Le signal est en général ré-amplifié, car les données sont enregistrées dans des mémoires du type registre à décalage. Dans ce cas, les hubs sont dits actifs, c'est-à-dire qu'ils possèdent des éléments qui doivent être alimentés électriquement. Un hub Ethernet est illustré à la figure 1.9 [19].

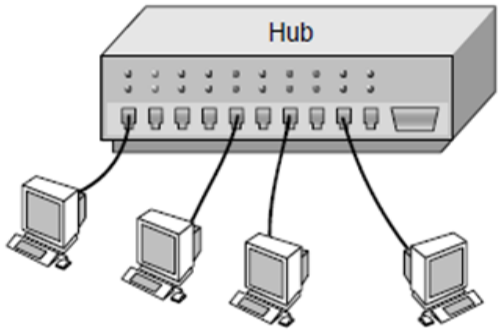

FIGURE 1.9 – Un hub Ethernet [19].

- **Switch (Commutateur) :** aussi appelé commutateur, en général, les stations d'un réseau Ethernet sont connectées directement à lui. Un commutateur relie les hôtes qui y sont connectés en lisant leur adresse MAC comprise dans les trames. Intervenant au niveau de la couche 2, il ouvre un circuit virtuel unique entre les noeuds d'origine et de destination, ce qui limite la commutation à ces deux ports sans affecter le trafic des autres ports [19].

- **Les routeurs :** un routeur est un élément d'interconnexion de niveau 3 qui achemine (route) les données vers un destinataire connu par son adresse de niveau 3. Agissant au niveau 3, les routeurs offrent plus de possibilités que les ponts puisqu'ils peuvent mettre en oeuvre les mécanismes du niveau 3 (segmentation, réassemblage, contrôle de congestion,etc.) [3].

- **Firewall :** très souvent, pour sa mise en place, le firewall nécessite deux composants essentiels : deux routeurs qui filtrent les paquets ou datagrammes et une passerelle d'application qui renforce la sécurité. En général le filtrage de paquets est géré dans des tables configurées par l'administrateur, ces tables contiennent des listes des sources/destinations qui sont verrouillées et les règles de gestion des paquets arrivant et allant vers d'autres machines. Très souvent des machines Unix jouent le rôle de routeur. La passerelle d'application quant à elle intervient pour surveiller chaque message entrant / sortant ; transmettre/rejeter suivant le contenu des champs de l'entête, de la taille du message ou de son contenu [8].

- **Modem (Modulateur-Demodulateur) :** est le périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via la ligne téléphoniques. Le modem module les informations numériques en ondes analogiques, en sens inverse il retranscrit les données sous forme analogique en données numériques [8].

- **Les passerelles (gateway) :** système logiciel et /ou matériel gérant le passage d'un environnement réseau à un autre, en assurant la conversion des données d'un format à un autre. La passerelle peut se présenter sous la forme d'un connecteur physique au réseau et être utilisée comme une interface pour transférer les informations entre les différents réseaux. Elle peut également se présenter sous forme d'un logiciel conçu pour permettre à deux protocoles différents d'échanger des informations [15].

1.11 Architectures protocolaires

En plus du matériel qui assure la connectivité et l'échange des signaux sur le support, physique ou non, il est nécessaire d'utiliser des règles de communication. Ces protocoles permettent de donner un sens au signal qui circule entre les postes et gérer l'accès au support partagé [19].

1.11.1 Définition de protocole

Un protocole est un ensemble de règles destiné à une tâche de communication particulière, deux ordinateurs doivent utiliser le même protocole pour pouvoir communiquer entre eux, en d'autres termes ils doivent parler le même langage pour se comprendre.

Un gestionnaire de protocole est un programme qui met en oeuvre un protocole particulier. Il existe plusieurs familles de protocoles ou modèles [19].

1.11.2 Modèle de référence OSI

Le modèle OSI (Open Systèmes Interconnexion, Interconnections de système ouvert en français) est un modèle de communications entre ordinateur proposé par l'ISO (organisation internationale de normalisation) en 1947, à laquelle adhérent plus de 100 pays. Son principe de base est la représentation des réseaux sous la forme de couche de fonctions superposées les unes aux autres. Chaque couche fournit des services pour la couche supérieure, communique avec son homologue via un protocole bien défini (règles de communication) et utilise les services fournis par la couche inferieure [19].

1.11.3 Architecture TCP/IP

1.11.3.1 Origine

L'architecture TCP/IP a été développée, dans le milieu des années 1970, par la DARPA (Defense Advanced Research Project Agency - USA -) pour les besoins d'interconnexion des systèmes informatiques de l'armée (DoD, Department of Defense). TCP/IP, du nom de ses deux protocoles principaux (TCP, Transmission Control Protocol et IP, Internet Protocol), est un ensemble de protocoles permettant de résoudre les problèmes d'interconnexion en milieu hétérogène [3].

1.11.4 Protocoles TCP/IP

Les principaux protocoles et applications de l'environnement TCP/IP sont [3] :

- **HTTP :** HyperText Transport Protocol, assure le transfert de fichiers hypertextes entre un serveur Web et un client Web ;
- **FTP :** File Transfer Protocol, est un système de manipulation de fichiers à distance (transfert, suppression, création, etc.) ;
- **TELNET :** TELetypewriter NETwork protocol (ARPA) ou TERminaL NETwork protocol, système de terminal virtuel, permet l'ouverture de sessions avec des applications distantes ;
- **SMTP :** Simple Mail Transfer Protocol, offre un service de courrier électronique ;

- **TFTP :** Trivial FTP, est une version allégée du protocole FTP ;
- **DNS :** Domain Name System, est un système de bases de données réparties assurant la correspondance d'un nom symbolique et d'une adresse Internet (adresse IP) ;
- **RIP :** Routing Information Protocol, est le premier protocole de routage (vecteur distance) utilisé dans Internet ;
- **SNMP :** Simple Network Management Protocol, est devenu le standard des protocoles d'administration de réseau ;
- **ICMP :** Internet Control and error Message Protocol, assure un dialogue IP/IP et permet notamment : la signalisation de la congestion, la synchronisation des horloges et l'estimation des temps de transit. Il est utilisé par l'utilitaire Ping qui permet de tester la présence d'une station sur le réseau.
- **ARP :** Address Resolution Protocol, est utilisé pour associer une adresse logique IP à une adresse physique MAC (Medium Access Control, adresse de l'interface dans les réseaux locaux) ;
- **RARP :** Reverse Address Resolution Protocol, permet l'attribution d'une adresse IP à une station ;
- **OSPF :** Open Shortest Path First, est un protocole de routage du type état des liens, il a succédé à RIP ;
- **SLIP :** Serial Line Interface Protocol, protocole d'encapsulation des paquets IP, il n'assure que la délimitation des trames ;
- **PPP :** Point to Point Protocol, protocole d'encapsulation des datagrammes IP, il assure la délimitation des trames, identifie le protocole transporté et la détection d'erreurs.

1.12 Conclusion

Ce chapitre a été axé sur la présentation de tout ce qui concerne les réseaux en général à savoir les différents types, les techniques de transfert, les équipements intermédiaires, les supports physiques, le modèle de référence OSI, et TCP/IP. Nous détaillerons l'administration des réseaux et la virtualisation dans le chapitre qui suit.

Chapitre 2

Administration des réseaux informatiques

2.1 Introduction

L'administration des réseaux informatiques évolue sans cesse et elle s'affirme aujourd'hui comme une activité clé de toute entreprise. En plus d'être constamment en fonction, ces outils d'échange de données et de partage d'information en temps réel doivent être en mesure d'offrir une confidentialité maximale et une sécurité à toute épreuve.

Dans ce chapitre, nous allons présenter une partie d'administration réseau qui se basera sur les réseaux commutés et les éléments indispensables qui contribuent à sa réalisation, nous effectuerons par la suite un tour d'horizon de la virtualisation.

2.2 Administration des réseaux informatiques

L'administration réseau est le processus permettant le contrôle d'un réseau de données pour en assurer l'efficacité et la productivité. Le but final de l'administration réseau est d'aider à maîtriser la complexité des réseaux de données et d'assurer que les données transitent sur le réseau avec le maximum d'efficacité et de transparence aux utilisateurs [13].

2.2.1 Rôle d'un administrateur réseau

Le rôle d'un administrateur réseau consiste à [13] :

- Mettre en place et maintenir l'infrastructure du réseau ;
- Installer et maintenir les services nécessaires au bon fonctionnement du réseau ;
- Assurer la sécurité des données internes au réseau ;
- Gérer les "logins" (i.e. noms d'utilisateurs, mot de passe, droits d'accès, permissions particulières, etc.) ;
- Le trafic des données qui circulent sur le réseau ;
- La sauvegarde des données ;

- La politique de sécurité régissant tous les types d'accès au réseau (accès interne, accès à distance et interconnexion avec des tierces parties) ;
- La surveillance et l'assurance de la fiabilité générale du réseau.

2.3 Réseaux de campus

2.3.1 Définition

Un réseau local ou commuté est un ensemble de moyens autonomes de calcul (micro-ordinateurs, stations de travail ou autres) reliés entre eux pour échanger des informations et partager des ressources matérielles (imprimantes, espace disque...) ou logicielles (programmes, bases de données...). Le terme de réseau local (LAN, Local Area Network) qui définit un LAN comme un système de communication entre unités centrales sur une étendue géographique limitée est restrictif [2].

2.3.2 Constituants d'un réseau local

Un réseau local est essentiellement constitué de [7] :

- Un câblage reliant les différents noeuds selon une certaine topologie ;
- Une méthode d'accès au support pour assurer son partage ;
- Une méthode d'adressage pour identifier chaque noeud ;
- Un ensemble cohérent de protocoles pour permettre la communication ;
- Un système d'exploitation spécifique (NOS, Network Operating System) capable de prendre en charge les périphériques distants partagés et d'en contrôler l'utilisation (administration et sécurité) ;
- Un ensemble de programmes utilisant les ressources mises en commun.

2.3.3 Architecture des réseaux locaux

Les réseaux locaux informatiques répondent aux besoins de communication entre ordinateurs au sein d'une même entreprise. Il s'agit de relier un ensemble de ressources devant communiquer : stations de travail, imprimantes, disques de stockage, ordinateurs, etc. Nés dans les années 1970, ils ont été proposés par les fournisseurs informatiques.

Un réseau local se caractérise par des équipements géographiquement proches les uns des autres et qui coopèrent en utilisant le support de transmission pour diffuser les données. L'ensemble des autres équipements du réseau reçoit tout bit émis par un équipement du réseau local. Cette

particularité est à la base des architectures spécifiques de réseaux locaux, standardisées dans les années 1980 [4].

2.3.3.1 Standards IEEE

Le comité 802 de l'IEEE, essentiellement constitué de représentants des constructeurs américains, s'est occupé de l'architecture des réseaux locaux. Plusieurs documents définissent les architectures proposées [4] :

- Le standard 802.1 définit le contexte général des réseaux locaux informatiques ;
- Le standard 802.2 définit la couche liaison de données ;
- Les standards 802.3, 802.4, 802.5 et 802.6 définissent différents protocoles d'accès au support, pour plusieurs types de supports physiques : paire métallique, câble coaxial ou fibre optique ;
- Le standard 802.11 définit un protocole d'accès pour les réseaux locaux sans fil (WLAN, Wireless LAN).

  D'autres standards ont vu le jour ultérieurement, au fur et à mesure de l'évolution technologique.

2.3.3.2 Adressage

Dans les réseaux locaux, l'adresse utilisée est une adresse physique (MAC) qui se gère au niveau du matériel. Elle possède un format défini par l'IEEE sur 16 ou sur 48 bits. Ce dernier format constitue l'adressage universel des équipements : il correspond à un numéro de série dont un premier champ de 24 bits qui donne le constructeur de la carte réseau (champ attribué par l'IEEE). Le second champ de 24 bits, librement choisi par le constructeur, est le numéro de la carte elle-même. De cette façon, toute carte réseau d'un ordinateur possède une adresse physique unique dans le monde. Le format universel sur 48 bits est le plus utilisé. Il est généralement baptisé adresse MAC, du nom de cette couche.

On peut également définir des adresses de groupe qui englobent plusieurs utilisateurs. Par exemple, dans le format universel, l'adresse de diffusion (ou broadcast) correspond à l'ensemble des équipements d'un réseau local. Dans cette adresse, tous les bits sont à 1. On l'écrit : FF :FF :FF :FF :FF :FF en hexadécimal [4].

2.3.4 Technologies d'un réseau local

Différentes technologies réseaux sont utilisées pour permettre aux ordinateurs de communiquer sur des réseaux locaux et étendus.

Chaque technologie respecte un ensemble de règles différentes pour placer les données sur le support de transmission réseau et les retirer. Cette méthode est appelée méthode d'accès. Lorsque les données sont transférées sur le réseau, ces différentes méthodes d'accès régulent le flux du trafic réseau.
Les principales technologies réseaux sont les suivantes [4] :

- Ethernet ;
- Token Bus ;
- Token Ring ;
- Réseau FDDI.

2.3.4.1 Réseaux Ethernet IEEE 802.3

La société Xerox a développé Ethernet en 1976. Ce fut le premier produit de réseau local utilisant le mécanisme CSMA/CD sur un bus physique. Vu son grand succès, les sociétés Xerox, DEC et Intel ont décidé d'en faire un standard qui a servi de base au comité IEEE pour sa norme 802.3. Même si Ethernet et le standard IEEE 802.3 diffèrent sur des points mineurs. La réussite d'Ethernet a été considérable : il est d'usage courant maintenant d'appeler Ethernet tout réseau local utilisant CSMA/CD, même s'il n'a plus grand-chose en commun avec le réseau initial [4].

Ethernet fonctionne selon deux modes très différents mais totalement compatibles, le mode partagé et le mode commuté, qui permettent tous deux de transporter des trames Ethernet [9] :

- **Le mode partagé** : indique que le support physique est partagé entre les terminaux munis de cartes Ethernet. Dans ce mode, deux stations qui émettraient en même temps verraient leurs signaux entrer en collision.

- **Le mode commuté :** les terminaux sont connectés à un commutateur, et il ne peut y avoir de collision puisque le terminal est seul sur la liaison connectée au commutateur. Le commutateur émet vers la station sur la même liaison mais en full-duplex, c'est-à-dire en parallèle mais dans l'autre sens.

2.3.4.2 Réseaux Token Bus IEEE 802.4

La société IBM a développé Token Bus, standardisé par l'IEEE sous le nom 802.4. Au niveau physique, les ordinateurs sont connectés via leur interface réseau à un bus physique. La gestion de bus est confiée à un élément actif particulier appelé superviseur. Ce dernier est en charge de la création de jeton à l'initialisation du réseau et de sa circulation entre les ordinateurs, le superviseur détermine aussi un ordre cyclique de passage du jeton entre tous les postes connectés, le bus physique support donc un anneau logique de circulation du jeton [20].

2.3.4.3 Réseaux Token Ring IEEE 802.5

La société IBM a développé l'anneau à jeton ou Token Ring, standardisé par l'IEEE sous le nom 802.5. Un réseau Token Ring est constitué d'un ensemble de MAU (Medium Access Unit) reliés entre eux pour constituer un anneau principal. Le MAU Token Ring est un élément similaire à un hub dans son fonctionnement. Il permet de connecter des stations à l'anneau et de répéter les informations reçues sur l'un de ses ports d'entrée/sortie sur les autres ports.

Chaque ordinateur doit être équipé d'une carte réseau Token Ring connectée au MAU par l'intermédiaire d'un câble à paires torsadées ou d'une fibre optique si la liaison est plus longue [20].

2.3.4.4 Réseaux FDDI (Fiber Distributed Data Interface)

FDDI est défini comme un réseau local ou métropolitain et semble aujourd'hui la principale solution adaptée à la demande d'interconnexion de réseaux locaux dans un contexte de réseau fédérateur. Les constructeurs offrent déjà des solutions d'interconnexion de type Ethernet et Token-Ring au travers de réseaux FDDI. En résumé, FDDI est une technologie de réseau local pouvant supporter la notion de réseau intégrateur de type métropolitain [20].

2.3.5 Gestion de la communication

Différentes directions du flot de données sont possibles, particulièrement dépendantes du support de transmission et des techniques utilisées [12] :

- **Mode simplex**
  Ce mode n'exploite qu'un seul sens de transfert de l'information. Il correspond généralement à l'usage d'un seul émetteur pour 'n' récepteurs. Ces derniers sont peu coûteux. Une fibre optique n'offre qu'un sens de connexion, ne permettant que le mode simplex. Ainsi, au moins deux fibres sont utilisées, en multimode, pour permettre une communication bidirectionnelle.

- **Mode half-duplex**
  Ici, les deux sens de communication sont alternés, chaque interface étant successivement émettrice et réceptrice. Le câble coaxial représente un bon exemple de support half-duplex.

- **Mode full-duplex**
  Dans ce mode, les deux extrémités peuvent transmettre simultanément. C'est la solution la plus coûteuse, mais également la plus efficace. Les communications téléphoniques sont de type full-duplex.

2.3.6 Conception du model réseau hiérarchique

2.3.6.1 Modèle de conception hiérarchique à trois couches

Un modèle de conception de réseau hiérarchique rend le problème complexe de la conception du réseau en petits problèmes plus faciles à gérer. Chaque niveau dans la hiérarchie répond à un ensemble de problèmes différents. Cela aide le concepteur à optimiser le matériel et le logiciel réseau. Cisco propose une hiérarchie à trois niveaux comme l'approche privilégiée pour la conception du réseau.
Dans ce modèle à trois couches, les dispositifs de réseau et de liaisons sont regroupés en fonction de trois couches [1] :

- Couche noyau ;
- Couche distribution ;
- Couche d'accès.

Le modèle à trois couches présenté dans la figure 2.1 est un cadre conceptuel. Il s'agit d'une image abstraite d'un réseau similaire au concept du modèle de référence Open System Interconnexion (OSI).

Les modèles en couches sont utiles car ils facilitent la modularité. Les dispositifs à chaque couche ont des fonctions similaires et bien définies, cela permet aux administrateurs d'ajouter facilement, remplacer et supprimer des composants individuels du réseau. Ce type de flexibilité et d'adaptabilité fait une conception de réseau hiérarchique hautement évolutive (voir la figure 2.1) [1].

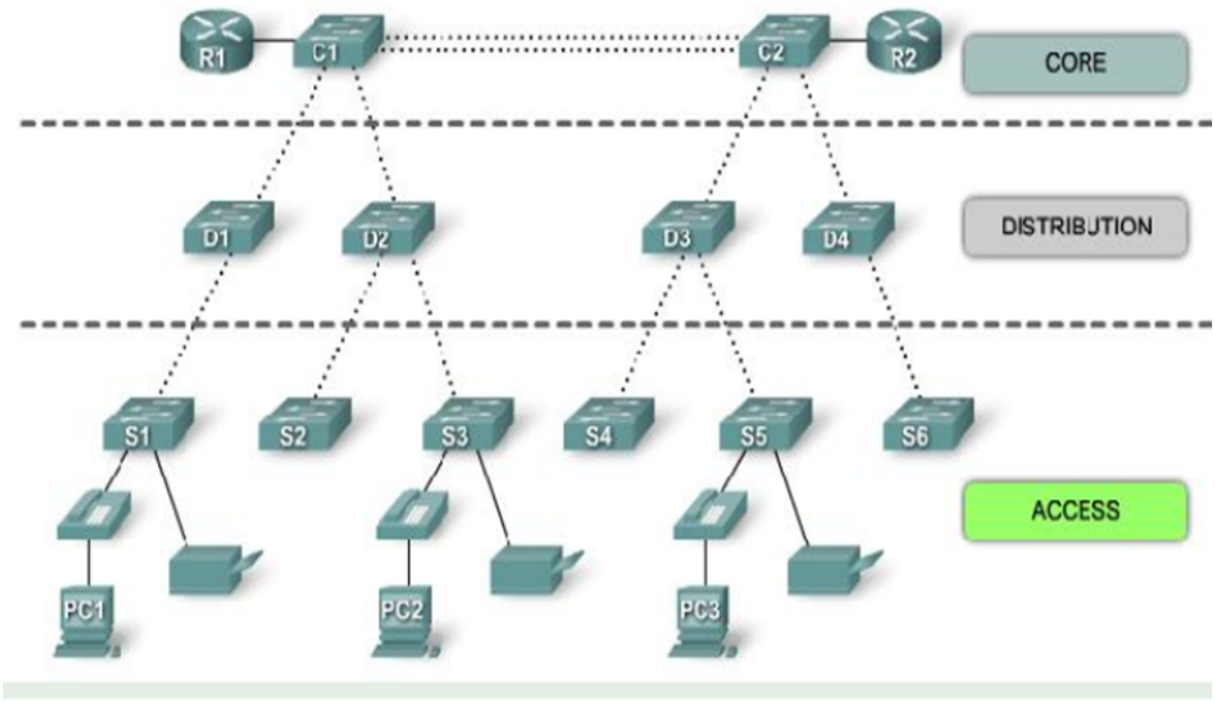

FIGURE 2.1 – Le modèle hiérarchique à trois couches.

- **La couche coeur (*Core layer*)**
  La couche de base fournit une structure de transport optimisée et fiable par le transfert du trafic à des vitesses très élevées. En d'autres termes, la couche centrale commute les paquets aussi vite que possible. Les dispositifs à la couche de base ne devraient pas être accablés par des processus qui se dressent sur la voie de la commutation de paquets à la vitesse supérieure, cela comprend les éléments suivants [1] :

  – Le cryptage des données ;
  – La traduction d'adresses.

- **La couche distribution**
  La couche distribution est située entre la couche d'accès et la couche de base et permet de différencier le noyau du reste du réseau. Le but de cette couche est de fournir la définition des limites en utilisant des listes d'accès et autres filtres pour limiter ce qui entre dans le noyau. Par conséquent, cette couche définit la politique du réseau. Une politique est une approche de traitement de certains types de trafics, y compris ce qui suit [1] :

  – Mise à jour de routage ;
  – Résumé de route ;

– Trafic VLAN.

- **La couche d'accès**
  La couche d'accès fournit le trafic sur le réseau et effectue une commande d'entrée du réseau. Les utilisateurs finaux accèdent aux ressources réseau par l'intermédiaire de la couche d'accès. Agissant comme la porte d'entrée à un réseau, la couche d'accès emploie des listes d'accès destinées à empêcher les utilisateurs non autorisés d'y parvenir et peut également donner des sites distants pour accéder au réseau par le biais d'une technologie à large zone, tels que Frame Relay, RNIS [1].

2.3.7 Différents types de commutateurs

Un commutateur est une unité réseau de couche 2 qui agit comme point de concentration pour le raccordement de stations de travail, de serveurs, de concentrateurs et d'autres commutateurs. Il fonctionne en mode full-duplex ce qui signifie qu'il peut envoyer et recevoir des données simultanément, pour cela nous allons voir les différents types de commutateurs qui existent [1] :

- **Commutateur à configuration modulaire**
  Offre une plateforme de haute performance destinée aux réseaux fédérateurs, environnements de campus. Le commutateur modulaire optimise le réseau grâce à des options permettant une croissance évolutive, 1 carte de ligne peut être ajoutée pour un total de 128 ports.

- **Commutateur à configuration empilable**
  C'est une nouvelle gamme de commutateurs administrables empilables Ethernet, qui offre toutes les capacités avancées pour assurer un environnement réseau plus exigeant à un tarif abordable, ces commutateurs fournissent une connectivité faste Ethernet 24 à 28 ports et gigabit Ethernet de 24 à 52 ports. En outre, ces commutateurs sont faciles à déployer et à gérer.

- **Commutateur à configuration fixe**
  Le commutateur à configuration fixe apporte aux postes de travail une connectivité faste Ethernet et gigabit Ethernet optimise les services LAN sur les réseaux d'entreprises. Ce commutateur offre une sécurité intégrée sur le réseau et une qualité de service évoluée pour distribuer des services intelligents à la périphérie du réseau.

La figure 2.2 montre ces trois types de commutateurs :

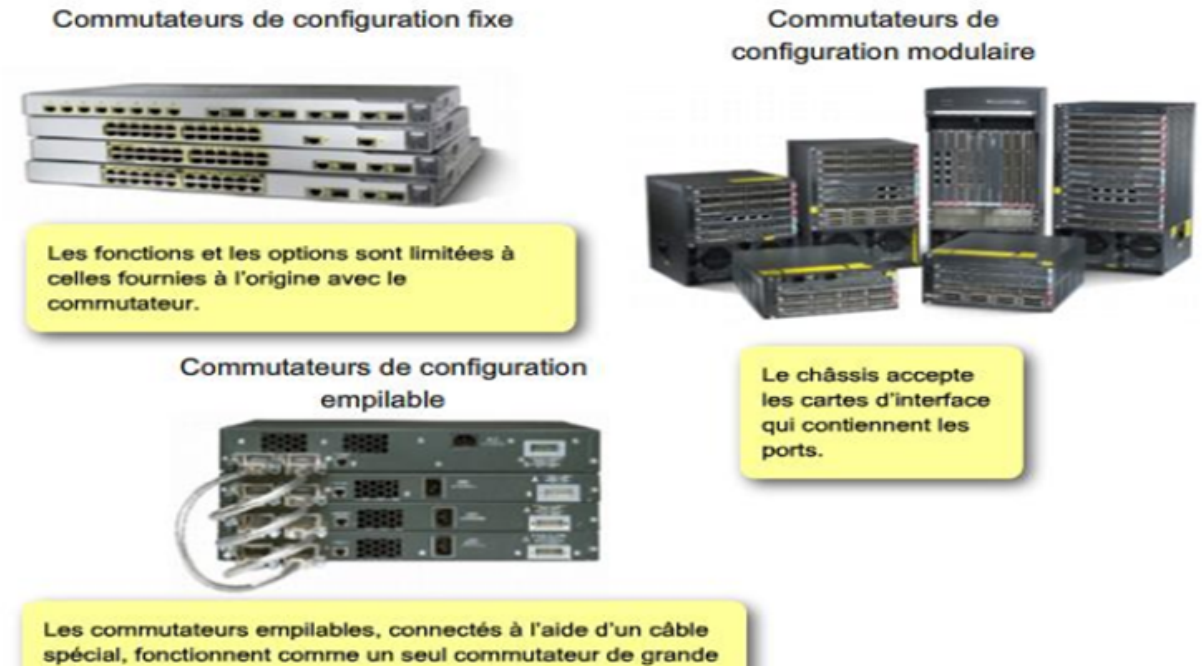

FIGURE 2.2 – Les différents types de commutateurs.

2.3.8 Réseaux locaux virtuels (VLAN)

Un VLAN (Virtual Local Area Network ou Virtual LAN, 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 (contraintes géographiques, contraintes d'adressage...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.) [14].

2.3.8.1 Typologie de VLAN

Plusieurs types de VLAN sont définis, selon le critère de commutation et le niveau auquel il s'effectue [14] :

- **Un VLAN de niveau 1** (aussi appelé VLAN par port ou Port-Based VLAN) 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

MAC Address-Based VLAN) définit 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 [14] :

  – **Le VLAN par sous-réseau (*Network Address-Based VLAN*)** associe 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.

  En contre partie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.

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

2.3.8.2 Les avantages du VLAN

Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants [1] :

– 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.

2.3.8.3 Les identifiants des VLAN

Les identifiants des VLAN font patient de 2 plages VLAN à plage normale et VLAN à plage étendue [1] :

- **VLAN à plage normale**

- Leurs identifiants commencent de 1 jusqu'à 1500 ;
- Utilisé dans les réseaux des petites et moyennes entreprises ;
- Les identifiants 1002 à 1005 sont réservés aux protocoles Token Ring et FDDI ;
- Les VLAN 1, 1002 et 1005 sont créés par défaut, ils ne peuvent être supprimés ;
- Les configurations des VLAN sont stockées dans un fichier, appelé vlan.dat en mémoire cash du switch.

- **VLAN à plage étendue**

  - Plage comprise entre 1006 et 4094 ;
  - Supporte moins de fonctionnalité que le normal range VLAN ;
  - Les switch Catalyst 2950 et 2960 supportent un maximum de 255 VLAN normal et étendu, simultané ;
  - Par contre, l'augmentation du nombre de VLAN sur un switch dégrade les performances de celui-ci.

2.3.8.4 Protocole VTP

Pour ajouter un VLAN sur un réseau, l'administrateur doit l'ajouter sur chaque commutateur, donc il exige beaucoup de manipulation surtout sur de grands réseaux. Pour éviter cela sur des commutateurs Cisco, la manipulation peut être faite sur un seul commutateur et la modification sera alors diffusée sur les autres via le protocole VTP (VLAN Trunking Protocol).

Nous distinguons dans ce cas des commutateurs VTP server, des VTP client et des VTP transparent [1].

2.3.8.5 Le fonctionnement d'un VTP

- **Le VTP domaine**

  Un domaine VTP est composé d'un ou de plusieurs équipements interconnectés qui partagent le même nom de domaine VTP. Un commutateur ne peut appartenir qu'à un seul domaine VTP.

  Le VTP varie en fonction du type de message VTP, mais quatre éléments sont généralement inclus dans tous les messages VTP [1] :

  - Version du protocole VTP : version 1 ,2 ,3 ;
  - Type de message VTP : indique l'un des quatre types ;

- Longueur du nom de domaine de gestion : indique la taille du nom qui suit ;
- Nom du domaine de gestion : nom configuré pour le domaine de gestion.

- **Les VTP mode**

Les dispositifs de VTP peuvent être configurés pour fonctionner selon les trois modes suivant [1] :

- **Un commutateur en mode serveur**

  Il diffuse ces informations sur les VLAN à tous les autres commutateurs appartenant au même VTP domaine, ces informations sont stockées en NVRAM et sur un tel commutateur, il est possible de créer, modifier ou supprimer un VLAN du VTP domaine.

- **Un commutateur en mode client**

  Dans ce mode, un commutateur ne peut créer, ni modifier ou supprimer des informations VLAN. Ce mode est utile pour les commutateurs qui manquent de mémoire pour stocker de grandes tables d'informations VLAN. Le seul rôle des clients VTP est de traiter les modifications VLAN et d'envoyer des messages VTP par tous les ports multi-VLAN.

- **Un commutateur en mode transparent**

  Il transmette des annonces VTP mais ignore les informations contenues dans le message. Un commutateur transparent ne modifie pas sa base de données et il n'envoie pas de mises à jour indiquant une modification apportée à l'état du VLAN excepté pour la transmission d'annonces VTP, le protocole VTP est désactivé sur un commutateur transparent.

2.3.8.6 Configuration de VTP

Grace à VTP chaque commutateur annonce sur les ports multi-VLAN son domaine de gestion, son numéro de révision de configuration, les VLANs qu'il connait et les paramètres correspondants. Ces trames d'annonce sont envoyées à une adresse multicast, de sorte que toutes les unités voisines puissent recevoir les trames. Toutefois, les trames ne sont pas transmises au moyen des procédures de pontage habituelles. Toutes les unités du même domaine de gestion acquièrent des informations sur les nouveaux VLAN configurés dans l'unité émettrice. Un nouveau VLAN doit être crée et

configuré sur une unité uniquement dans le domaine de gestion, toutes les autres unités du même domaine de gestion apprennent automatiquement les informations.

Les annonces sur les VLANs par défaut sont basées sur les types de média. Les ports utilisateur ne doivent pas être configurés en tant qu'agrégations VTP [1].

2.3.8.7 Protocole STP (*Spanning tree*)

Le protocole ***Spanning tree*** a été développé par le comité IEEE 802.1, dans le but d'interconnecter tout type de réseau, et ce quelle que soit la topologie utilisée. Le but de ce protocole est de construire un arbre qui recouvre tout le réseau, pour que tout point du réseau soit accessible à partir de toutes les feuilles de l'arbre.

Le but du spanning tree est de détecter les boucles et de les supprimer en désactivant certaines interfaces de certains pont afin d'obtenir une architecture arborescente du réseau local.

Ainsi, à un instant donné, il n'existe qu'un seul chemin entre segments distants. Les ports qui créent des boucles sont mis dans l'état " blocking " c'est à dire dans un état passif, à l'exception des paquets BPDU (Bridge Protocol Data Unit), paquets échangés par les ponts et contenant les informations nécessaires au bon déroulement de l'algorithme du spanning tree [26].

2.3.9 Principe de fonctionnement

Le protocole ***Spanning tree*** fonctionne selon ces quatres principes [26] :

- Election d'un pont racine sur tous les LAN, pour établir à partir de celui-ci un arbre recouvrant, sans boucles. A sa mise sous tension ou bien lorsqu'il est isolé, tout pont considère qu'il est lui-même le pont racine. Il émet donc périodiquement (toutes les 2s) des trames en diffusion sur les réseaux auxquels il est raccordé, indiquant qu'il est racine, et précisant son identificateur sur 8 octets. Cet identificateur est composé de 2 octets de priorité (fixé par l'administrateur) et des 6 octets de l'adresse MAC " la plus faible " Le pont élu est celui de plus haute priorité, c'est à dire ayant l'identificateur le plus faible. Chaque fois qu'un pont reçoit une BPDU d'un pont racine qui lui est supérieur, il cesse de s'annoncer en tant que pont racine et répercute les messages annonçant le nouveau pont racine ;

- Calcul de la distance entre le pont racine et les autres ponts ;

- Election d'un pont désigné sur chaque LAN (le plus proche de la racine en terme de coûts),

et désactivation de certains ports des autres ponts ;

– Choix d'un port racine sur chaque pont désigné.

2.4 Virtualisation informatique

2.4.1 Définition

En informatique, la virtualisation consiste à créer une version virtuelle d'un dispositif ou d'une ressource, comme un système d'exploitation, un serveur, un dispositif de stockage ou une ressource réseau. Nous pouvons donc considérer la virtualisation comme l'abstraction physique des ressources informatiques. En d'autres termes, les ressources physiques allouées à une machine virtuelle sont abstraites à partir de leurs équivalents physiques [16].

2.4.2 Présentation de la virtualisation

Le marché de la virtualisation des solutions d'infrastructure informatique est aujourd'hui en plein essor. Bien que cette notion ne soit pas nouvelle, les problématiques de rationalisation des ressources matérielles, de réduction des coûts et de comptabilité des systèmes hétérogènes offrent aujourd'hui un terrain fertile pour le développement rapide des solutions de virtualisation.

La virtualisation est l'ensemble des techniques matérielles et/ou logicielles qui permettent de faire fonctionner sur une seule machine physique plusieurs systèmes d'exploitation et/ou plusieurs applications, séparément les uns des autres. Comme s'ils fonctionnaient sur des machines physiques distinctes. La meilleure représentation qu'il puisse en être fait sur le principe est représentée par la figure 2.3 [22] :

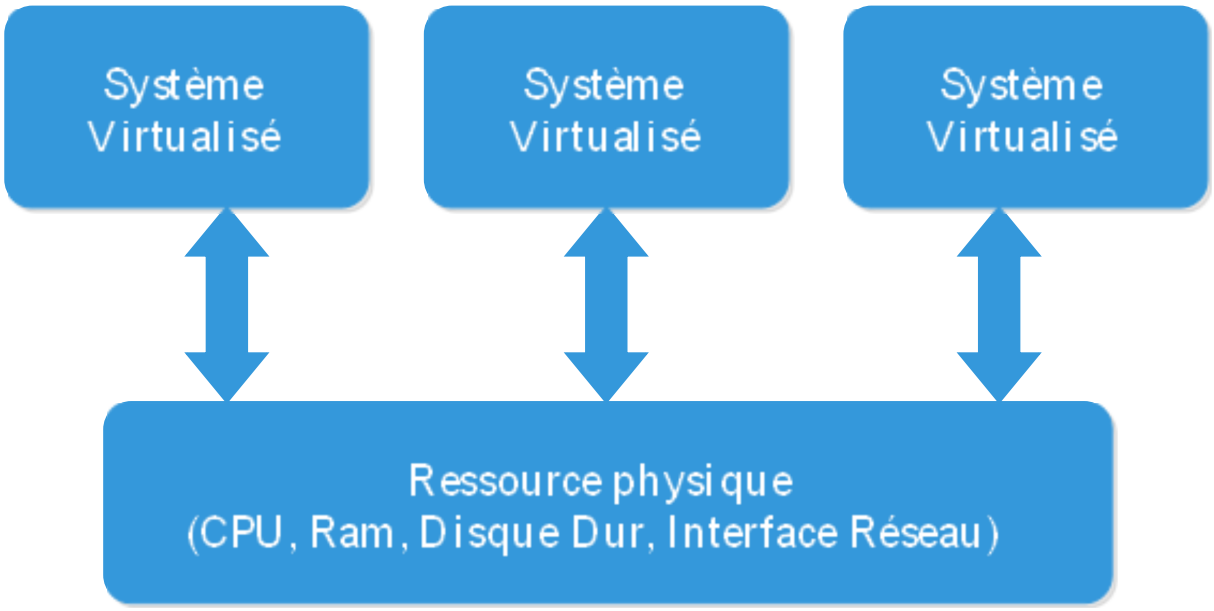

FIGURE 2.3 – Principe générale de la virtualisation.

- **Chaque outil de virtualisation met en oeuvre une ou plusieurs de ces notions** [22] :

  – Une couche d'abstraction matérielle et/ou logicielle ;
  – Un système d'exploitation hôte (installé directement sur le matériel) ;
  – Un systèmes d'exploitations (ou applications, ou encore ensemble d'applications) "virtualisé(s) " ou " invité(s) " ;
  – Un partitionnement, isolation et/ou partage des ressources physiques et/ou logicielles ;
  – Des images manipulables : démarrage, arrêt, sauvegarde et restauration, sauvegarde de contexte, migration d'une machine virtuelle à une autre ;
  – Un réseau virtuel : réseau purement logiciel, interne à la machine hôte, entre hôte et/ou invités.

- **Pour créer des machines virtuelles, différentes solutions existent**[22] :

  – **L'émulation**
  Consiste à utiliser un système d'exploitation (ou un programme) sur un système qui n'utilise pas la même architecture.

  – **La virtualisation**

  Consiste à simuler, au sein d'un serveur physique, l'existence de plusieurs systèmes d'exploitation cloisonnés et mutualisés. On distingue trois grandes catégories de solutions de virtualisation, dont les domaines d'applications sont différents.

2.4.3 Techniques de virtualisation

2.4.3.1 Virtualisation par container ou isolation

Un isolateur est un logiciel permettant d'isoler l'exécution des applications dans ce que l'on appelle des contextes ou bien zones d'exécution.
La virtualisation par container ou isolation est illustré dans la figure 2.4.

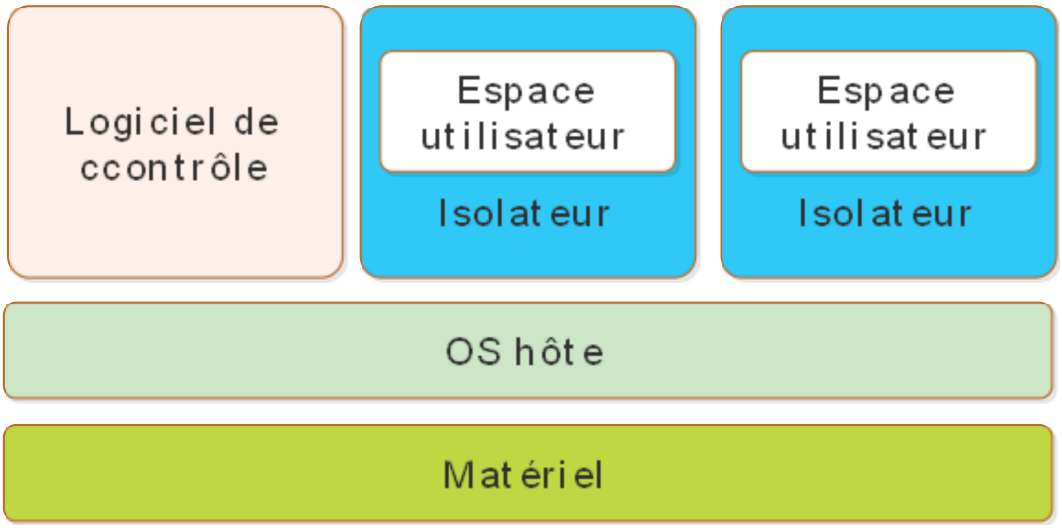

FIGURE 2.4 – Virtualisation par container ou Isolation.

La virtualisation par container ou isolation uniquement liés aux systèmes Linux. Les isolateurs sont en fait composés de plusieurs éléments et peuvent prendre plusieurs formes [22].
Voici un exemple de la virtualisation par isolation ci-dessous [22] :

– **Linux V Server** (isolation des processus en espace utilisateur) ;

2.4.3.2 Para-virtualisation (Hyperviseur type 1)

Un hyperviseur de type 1 est un hyperviseur s'exécutant directement sur une plateforme matérielle. Il implémente la plupart des services que fournissent les noyaux de systèmes d'exploitation courants, entre autres : la gestion mémoire complète des machines virtuelles ainsi que leur ordonnancement.

La para-virtualisation est illustré dans la figure 2.5 ci-dessous.

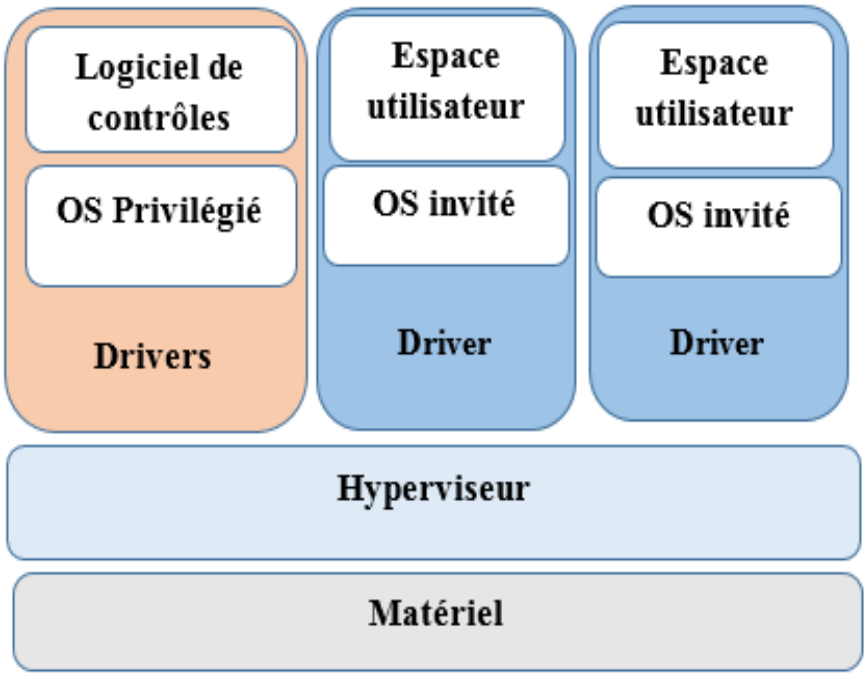

FIGURE 2.5 – Para-virtualisation (Hyperviseur type 1).

Les systèmes d'exploitation invités doivent généralement être adaptés à la couche de virtualisation, ils ont donc "conscience" d'être virtualisés [22].

Voici quelques exemples de la para-virtualisation ci-dessous [22] :

- **XEN :** c'est un logiciel libre, hyperviseur supportant des noyaux Linux ;
- **Oracle VM :** propriétaire, hyperviseur sur plateforme x86.

2.4.3.3 Virtualisation complète (Hyperviseur type 2)

Un hyperviseur de type 2 est un émulateur s'exécutant par-dessus un système d'exploitation classique (hôte) comme n'importe quel autre programme. Il utilise les services fournis par le système d'exploitation hôte pour gérer de la mémoire et l'ordonnancement des machines virtuelles. La virtualisation complète est illustré dans la figure 2.6.

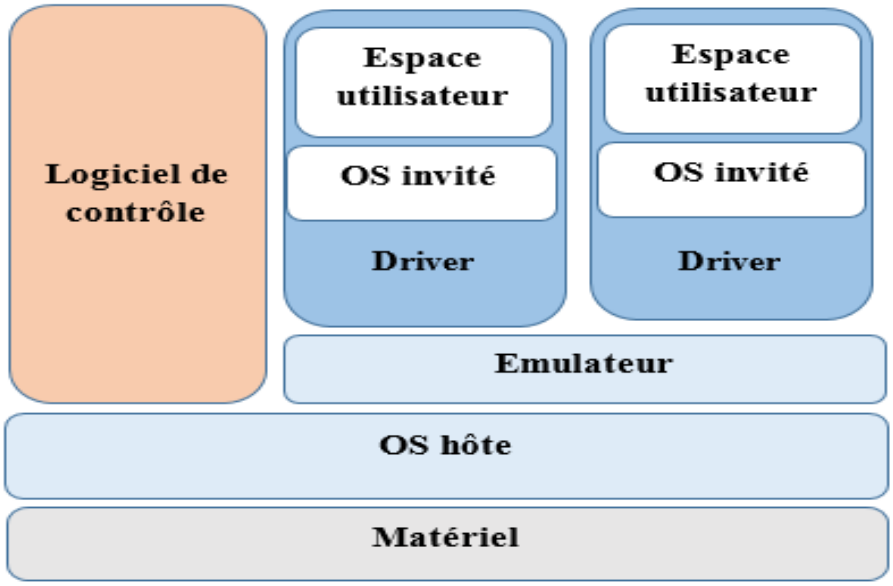

FIGURE 2.6 – Virtualisation complète (Hyperviseur type 2).

Cette solution est comparable à un émulateur, parfois même confondue. Le microprocesseur, la mémoire de travail (RAM) ainsi que la mémoire de stockage (via un fichier) sont directement accessibles aux machines virtuelles, alors que sur un émulateur l'unité centrale est simulée, les performances en sont donc considérablement réduites par rapport à la virtualisation.

Cette solution permet de faire cohabiter plusieurs systèmes hétérogènes sur une même machine grâce à une isolation complète. Les échanges entre les machines se font via les canaux standards de communication entre systèmes d'exploitation (TCP/IP et autres protocoles réseau), un tampon d'échange permet d'émuler des cartes réseaux virtuelles sur une seule carte réseau réelle [22].

Voici quelques exemples de la virtualisation complète [22] :

- **QEMU :** émulateur de plateformes x86,
- **Bochs :** émulateur de plateforme x86.

2.4.4 Avantages et inconvénients de la virtualisation

La virtualisation apporte de nombreux bénéfices mais aussi il faut tenir compte de ses limites pour cela nous allons présenter quelques avantages et inconvénients de la virtualisation [2] :

2.4.4.1 Avantages de la virtualisation

- Utiliser un autre système d'exploitation sans redémarrer son ordinateur ;
- Tester des systèmes d'exploitation sans compromettre un environnement stable ;
- Tester des logiciels dans des environnements isolés et sécurisés ;
- Meilleure utilisation des ressources machines ;
- Réduction du nombre de machines donc du coût du matériel et de sa maintenance ;
- Possibilité d'installer plusieurs systèmes (Windows, Linux) sur une même machine ;

2.4.4.2 Inconvénients de la virtualisation

- Pertes plus importantes en cas de chute d'une machine physique (plusieurs services indisponibles) ;
- Vulnérabilité généralisée : si l'hyperviseur est exposé à une faille de sécurité, les machines virtuelles peuvent l'être également et ne sont plus protégées. Cela a été pris en considération par les développeurs de solutions de virtualisation en adoptant des techniques d'isolation.

2.5 Conclusion

Ce chapitre nous a permis d'avoir une bonne compréhension sur l'administration des réseaux et d'éclaircir les différentes idées sur les réseaux de campus ainsi que les différentes techniques de virtualisation et de connaître les parties restraintes afin d'aborder notre thème.
Le chapitre suivant donnera une présentation sur l'audit de réseau de SONATRACH.

Chapitre 3

Audit du réseau informatique de SONATRACH de Béjaia

3.1 Introduction

L'audit a connu un développement important ces dernières années. Il est utilisé tant sur le plan interne qu'en externe. Il est donc essentiel de savoir pourquoi et comment travaille l'auditeur afin de comprendre l'importance de son rôle. La reconnaissance de l'audit interne en tant que fonction clef pour l'efficacité ou la performance du dispositif de contrôle interne, confère à l'entreprise la légitimité nécessaire pour jouer un rôle prépondérant au sein de l'organisation.

Dans ce présent chapitre, nous définissons l'audit toute en illustrant ces différents types, sa nécessité et ses différentes méthodologies. Ensuite, nous passons à la contribution de l'audit interne au niveau de réseau LAN de la RTC, nous finissons par la détection des anomalies.

3.2 Audit informatique pour les entreprises

3.2.1 Définition de l'audit

Le Petit Larousse [22], définit l'audit comme une procédure consistant à s'assurer du caractère complet, sincère et régulier des comptes d'une entreprise, ainsi à porter un jugement sur la qualité et la rigueur de sa gestion.

3.2.2 Types d'audit existants

Du point de vu général, il existe deux types d'audit [24] :

- **Interne**
  L'audit interne se base sur la tâche d'évaluation, de contrôle, de conformité et de vérification. Il est exercé d'une façon permanente par une entreprise. Cet audit à pour

mission de déceler les problèmes et de proposer des solutions.

- **Externe**
  L'audit externe est une opération volontaire décidée par la direction d'une entreprise pour faire apprécier la conformité de son système avec un référentiel, et ce par une firme d'audit tiers reconnue pour ses compétences et sa notoriété dans les secteurs d'activités concernés.

3.2.3 Intérêt et nécessité de l'audit

L'audit peut être envisagé à la suite de problèmes techniques, pour l'établissement d'une documentation dans le but d'évaluer les besoins en ressources en fonction de la tâche à effectuer. Mais il s'agit également souvent d'aider les entreprises à définir et à adopter un plan stratégique informatique. Ce plan identifiera les objectifs de l'entreprise à moyen terme et indiquera comment l'informatique peut aider à atteindre les objectifs posés [20].

3.2.4 Méthodologie d'audit

Une méthodologie est une démarche rigoureuse et standardisée s'appuyant sur des outils tels que des questionnaires, des logiciels spécialisés et permettant de faire l'analyse de sécurité du système d'information [7].

3.2.4.1 Phases d'audit

La démarche d'audit se décompose en trois phases [7] :

1. Phase préparatoire.
2. Audit de l'existant.
3. Evaluation de la qualité des services
   - **A. Phase préparatoire**
     1. La définition du domaine couvert qui consiste à délimiter le périmètre de l'étude et à préciser les cellules qui le composent [7].
   - **B. Audit de l'existant**
     1. L'audit de l'existant est déterminé en suivant la démarche d'un plan bien organisé et détaillé [7].
   - **C. Evaluation de la qualité des services**
     1. Le questionnaire d'audit : c'est un questionnaire prenant en compte les services à satisfaire.

2. La mesure globale de la qualité des services : une mesure globale de la qualité ou la performance d'ensemble d'un service est élaborée automatiquement par la méthode audit à partir des réponses au questionnaire d'audit correspondant [7].

3.3 Présentation de l'entreprise d'accueil

3.3.1 Présentation de la Direction Régionale de transport de Bejaia (RTC)

La direction régionale de transport de Bejaia (RTC) est l'une des cinq directions régionales de transport des hydrocarbures de la SONATRACH (RTC). Elle a pour mission de transporter, stocker et livrer les hydrocarbures liquides et gazeux. Elle est chargée de l'exploitation de deux oléoducs, d'un gazoduc et d'un port pétrolier.

1. Oléoduc Haoud-El-Hamra vers Bejaia : installé par la société SOPEG (Société Pétrolière de gérance), cet Oléoduc est premier pipe-line à être poser en Algérie. Il est d'une longueur de 660km et d'un diamètre de 24 pouces.
2. Oléoduc Beni-Mensour vers Alger : il est de longueur de 130 km et d'un diamètre de 16 pouces.
3. Gazoduc Hassi R'Mel vers Bordg-Menail : il est d'une longueur de 437 km et d'un diamètre de 42 pouces, il approvisionne en gaz naturel depuis 1981 toutes les villes et pôles industriels du centre du pays.
4. Le port pétrolier de Bejaia : il se compose de deux postes de chargement à partir d'un parc de pétrole brut composé de 16 bacs, de navires jaugeant jusqu'à 80.000 tonnes au moyen de pompières comportant 10 électropompes de 53.000 chevaux de puissance totale.
5. Le poste de chargement (SPM) : il peut accepter des navires jusqu'à 320.000 tonnes.

3.3.2 Structure de la RTC

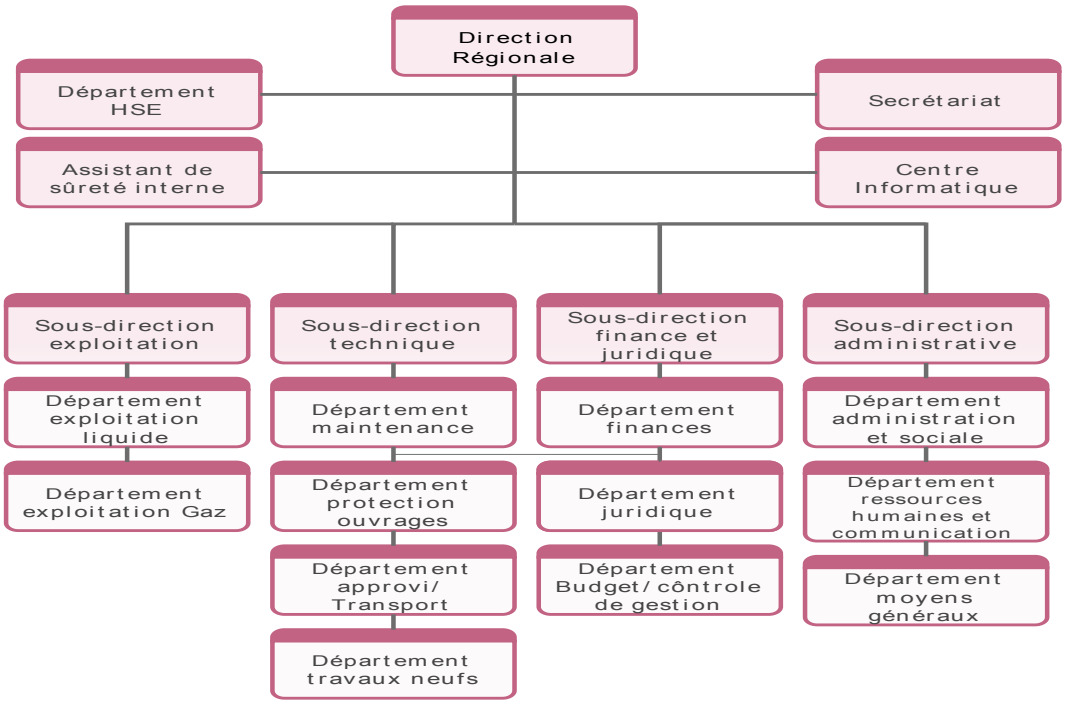

FIGURE 3.1 – Organigramme de SONATRACH

Comme on peut le voir sur la figure 3.1, la direction régionale de Bejaia est structurée comme suit :

- **Direction Régionale**
  Dirigée par un directeur régional aidé par des assistants et un secrétariat.

- **Assistant de sûreté interne**
  A pour mission de protéger et de sauvegarder le patrimoine humain et matériel.

- **Centre Informatique**
  Il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la RTC, ainsi que la gestion du réseau informatique interne.

- **Sous-direction Technique**
  Elle a pour mission d'assurer la maintenance et la protection des ouvrages. Elle est organisée en quatre départements :
  – Département maintenance.

- Département protection des ouvrages.
- Département approvisionnement et transport.
- Département des travaux neufs.

- **Sous-direction Exploitation**
  Elle est chargée de l'exploitation des installations, elle effectue des réparations en cas de fuite, de Sabotage ou de panne pour les stations de pompage. Elle est composée de deux départements :
  - Département exploitation liquide.
  - Département exploitation gaz.

- **Sous-direction Finance et Juridique**
  Elle a pour missions d'effectuer la gestion financière, le budget et le contrôle de gestion et de prendre en charge les affaires juridiques de la TRC. Elle est organisée en trois départements :
  - Département finance.
  - Département juridique.
  - Département budget et contrôle de gestion.

- **Sous-direction Administration**
  Elle a pour mission la gestion des ressources humaines et les moyens généraux. Elle est organisée en trois départements :
  - Département administration et social.
  - Département ressources humaines et communication.
  - Département moyens généraux.

3.4 Méthodologie d'audit de réseaux LAN de SONATRACH

3.4.1 Phase préparatoire

Dans cette phase nous allons délimiter le périmètre de l'étude en précisant tous les équipements informatiques utilisés au sein de l'entreprise.

3.4.1.1 Équipements utilisés

- **Plate forme matérielle**
  Un réseau Ethernet à 10/100/1000GB/s reliant huit serveurs (ES40 Compac, DS20 Compac, DELL POWERREDG 2800, HP Proliant DL380G5, HP Proliant DL580G5) et

203 micro-ordianteur (Dell, Wadoo, Fujistsu Siemens) et trente-cinq imprimantes (Laser HP, Laser Jet).

- **Types d'architecture :** client/serveur.
- **SGBD : Oracle.**
- **Matériel actif :** routeur, commutateurs et serveurs.
  - **Cinq commutateurs Cisco Catalyst 6509** de capacité d'acheminement moyenne de 40Gb/s =6.7872 paquets Ethernet/us.
  - **Quatorze commuateurs Cisco C3750** de capacité d'acheminement moyenne est de 32 Gb/s.
  - **Cinq commutateurs Cisco C2950G-24 ports** de capacité d'acheminement moyenne de 8.8Gb/s=1.4932 paquets Ethernet/us.
  - **Un commutateur Cisco C2950G -48 ports** de capacité d'acheminement moyenne de 13.6Gb/s=2.3077 paquets Ethernet/us.
- **Matériel passif**
  - Câblage entre bâtiment en fibre optique OM3.
  - Câblage en cuivre des postes de travail de type pair torsadé UTP catégorie 6.
- **Utilitaire**
  - Microsoft office (2007-2008).
  - WinRAR.
  - Firefox, Opera, IE.
  - Adobe Acrobat, Foxit Reader.
  - Norton Ghost 10.
  - VMware, Virtual pc.
  - etc.

3.5 Audit de l'existant

Dans l'audit de l'existant, nous allons suivre une démarche d'audit en commençant par le centre informatique de la RTC et nous finissons par l'audit de son réseau, ce qui nous permettra par la suite d'évaluer la qualité de leurs réseaux.

3.5.1 Présentation du centre informatique de la RTC

Le centre informatique de la RTC dispose de :

1. - 01 chef du centre informatique : ingénieur système.
2. - 01 chef de service système et réseau : ingénieur système qui chapote un 01 chef de service BDD et logiciel.
3. - 01 ingénieur SI qui chapote 04 ingénieurs systèmes d'information (SI).

3.5.2 Organisation du centre informatique

L'organisation du centre ne cesse de subir des changements et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois afin de subvenir aux nouveaux besoins de l'entreprise.
Pour mener à bien sa mission, le centre informatique est organisé en trois services tels qu'ils sont schématisés sur la figure 3.2 :

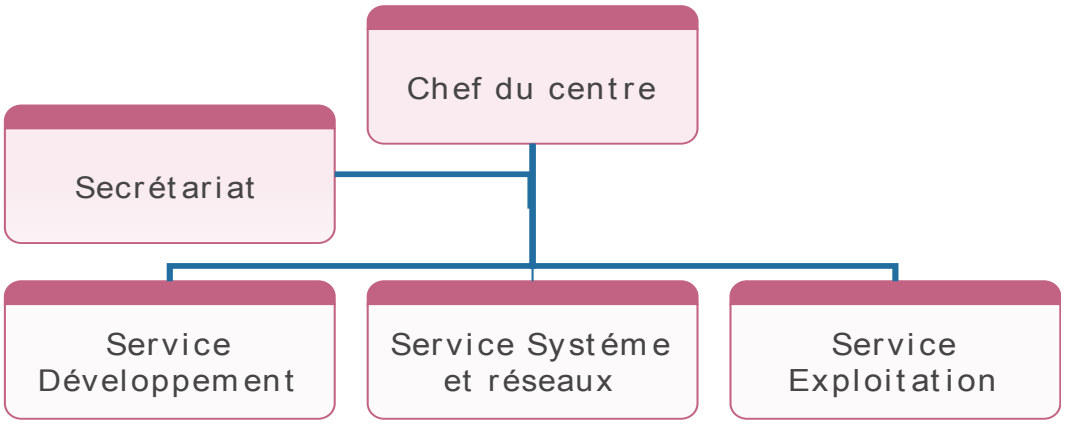

FIGURE 3.2 – Organisation du centre informatique.

3.5.3 Rôle de chaque service de l'entreprise

Chaque service à des rôles et des tâches spécifiques :

- **Service développement**
  Il est chargé de bénéficier des nouvelles technologies qu'il acquière tout en optimisant leurs utilisations, ainsi que la prise en charge des besoins des différentes structures de la direction en matière de développement de nouveaux systèmes d'informations :

  – Analyse et conception ;
  – Réalisation d'applications informatiques ;

– Administration des bases de données de l'entreprise.

- **Service système et réseaux**
  Il est chargé d'assurer les tâches suivantes :

  1. L'administration des serveurs ;
  2. Administration des bases de données de l'entreprise ;
  3. Installation des logiciels sur les serveurs ;
  4. Gestion des performances système et réseau ;
  5. Gestion de la sécurité et des utilisateurs connectés au réseau (droits d'accès) ;
  6. Gestion du parc informatique ;
  7. La prise en compte et résolution des pannes ;
  8. Planification et ordonnancement des travaux ;
  9. Sauvegarde et restauration des données ;
  10. Gestion des espaces disques ;
  11. Exploitation (saisie, validation, traitement) des anciennes applications batch pour la RTC et les autres directions régionales.

- **Service exploitation**
  Ce service à pour rôle la centralisation des bilans pour la branche transport et la gestion de la paie des temporaires.

3.5.4 Réseaux informatiques de l'entreprise SONATRACH

La mise en place d'un réseau au sein de l'entreprise SONATRACH de Bejaïa est une opération rigoureuse, qui mérite d'être perfectionnée et analysée soigneusement. Avant d'essayer de porter une amélioration au système déjà existant, une étude de l'existant sur le réseau est nécessaire.

3.5.4.1 Infrastructure réseau au niveau des blocs de la RTC

Le réseau de la RTC est constitué de deux parties connectées entre elles (réseau de l'ancien bâtiment et le réseau du nouveau bâtiment). En effet, ce dernier a subit une extension après la construction du nouveau bâtiment.

A. L'ancien bloc
C'est un ensemble de bâtiments, l'infrastructure informatique est répartie sur l'ensemble de

ces bâtiments.

L'ancien bloc est connecté avec le nouveau bloc via la fibre optique.

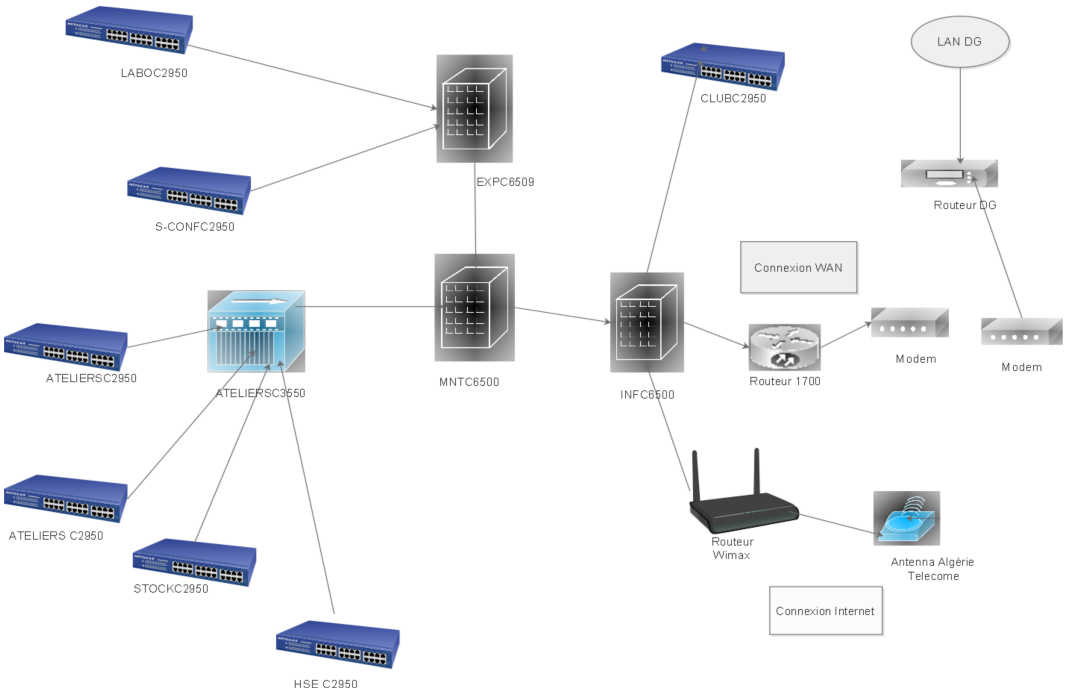

FIGURE 3.3 – Architecture d'ancien bloc

Le tableau suivant montre la liste des équipements et armoires de l'anciens bloc :

Bloc	Armoire	Equipement
Bloc principale	ARM 01 (salle informatique)	Cisco cat 6500 + un routeur d'accé à distance
Bloc principale	ARM 02 (salle n°)	Cisco cat 6500 et Cisco cat 2950
Bloc principale	ARM 03	Cisco cat 6509
Bloc atelier	ARM 04 (l'atelier)	Cisco cat 3550
Le club	ARM 05 (bloc de club)	Cisco cat 2950
La salle des conférences	ARM 06 (salle de conférence)	Cisco cat 2950
Laboratoire	ARM 07 (Laboratoire)	Cisco cat 2950
Le stock	ARM 08 (Le bloc de stock)	Cisco cat 2950
Le bloc PTO	ARM 09 (le bloc PTO)	Cisco cat 2950

TABLE 3.1 – La liste des équipements et armoires de l'anciens bloc

B. Le nouveau bloc

C'est un bâtiment constitue d'un Rez-de-chaussée et de 2 étages. L'infrastructure informatique est répartie sur l'ensemble d'étage de ce bâtiment. Ce dernier est connecté avec l'ancien bloc par une fibre optique.

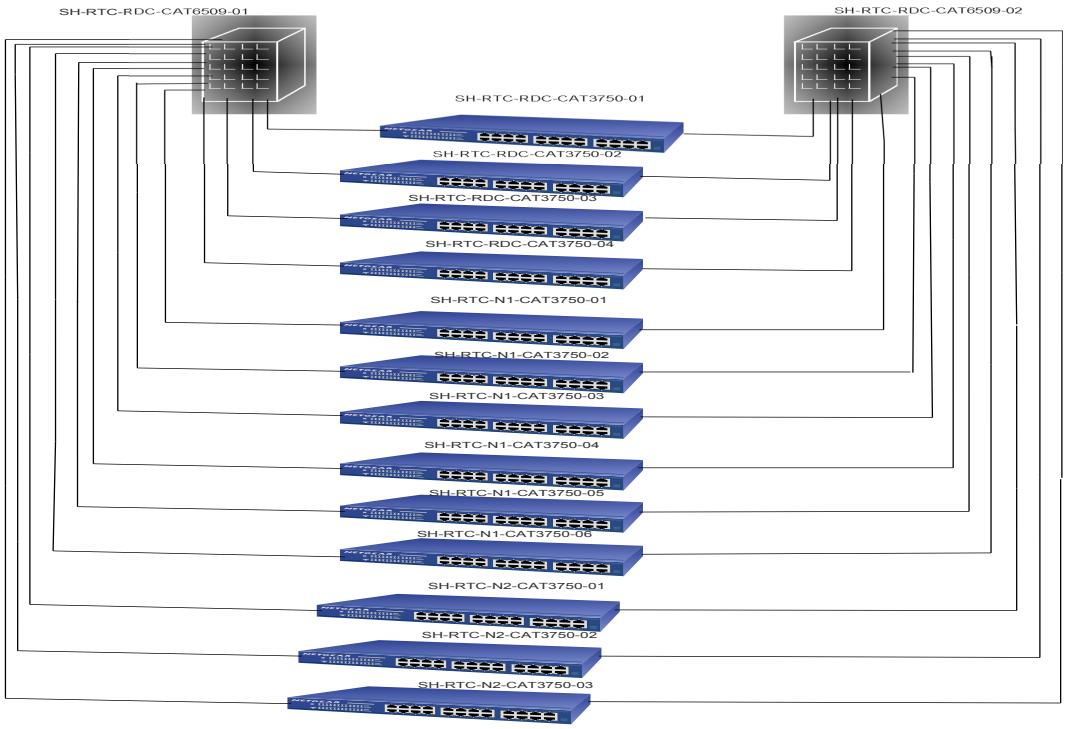

FIGURE 3.4 – Architecture de nouveau bâtiment

3.5.4.2 Équipements et matériels réseaux

Dans cette étape, nous allons présenter les équipements et le matériels réseaux de SONATRACH.

A.) Infrastructure réseau au niveau de la RTC

Tous les équipements actifs (catalyst 6509, catalyst 3750, routeur voix, routeur internet, serveur ACS, voie mail) sont physiquement installés à ce niveau.

- Les équipements réseaux sont hébergés dans une armoire de brassage équipée (câblage, ventilation, espacement,...)
- Un onduleur (USP) est installé dans chaque armoire afin de protéger les équipements réseaux installés (Switch, routeur, serveur)
- Chaque salle qui héberge les armoires de brassage est dotée d'une climatisation suffisante.

B.) Les commutateurs utilisés dans le réseau de la RTC

Le réseau de la RTC contient deux types de commutateurs :

- **Des commutateurs intelligents**
  En plus de leur fonction ils peuvent faire le routage. Dans le réseau de la RTC, on trouve trois exemples de ce type qui sont :

  Catalyst 6500
  C'est une gamme de commutateurs CISCO qui offre des performances et une densité de ports évolutives sur un large choix de configurations de châssis et d'interfaces LAN/WAN/MAN.

  Catalyst 3750
  C'est une gamme de commutateurs CISCO qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables.

  Catalyst 3550
  C'est une gamme de commutateurs CISCO empilables, il fournit une haute disponibilité et des fonctionnalités avancées de qualité de service et de la sécurité afin d'améliorer l'exploitation de réseau.

- **Des commutateurs non intelligents**
  Ce type de commutateurs ne permet pas de faire le routage. Le réseau de la RTC contient le type suivant :

  Catalyst 2950
  C'est une gamme de commutateurs CISCO destinée à la commutation d'étages dédiée Ethernet 10/100/1000 Mbits/s fixe, offrant des performances, une souplesse et une administration exceptionnelles.

C.) Les routeurs utilisés dans le réseau de la RTC

Le réseau de la RTC contient les deux types de routeurs suivants :

- **CISCO 1700**
  C'est une gamme de routeurs d'accès modulaires souples et sécurisés utilisée lorsqu'il s'agit de réseaux WAN.

- **CISCO 800**

C'est une gamme de routeurs à services intégré haut débit qui permet aux petits bureaux d'exploiter des services sécurisés simultanés comme le pare-feu, les VPN et les réseaux LAN sans fil.

3.5.5 Service de sécurité

Un service de sécurité est une réponse à un besoin de sécurité, exprimé en terme fonctionnel décrivant la finalité du service, généralement en référence à certains types de menaces.
Les domaines de responsabilité qui abordent dans la société, du point de vue de la sécurité sont :

- Sécurité des locaux ;
- Sécurité du réseau local ;
- Contrôle d'accès applicatif ;
- Contrôle de l'intégrité des données ;
- Confidentialité des données ;
- Disponibilité des données ;
- La sécurité logique des équipements ;
- Les plans de secours ;
- Les plans de sauvegarde ;
- Authentification ;
- Contrôle d'accès ;
- Configuration des logiciels ;
- La maintenance.

3.5.5.1 Serveur antivirus

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants.

3.5.5.2 Serveur filtrage web

Permet d'interdire l'accès à des sites au contenu répréhensible ou plus simplement de bloquer les bannières publicitaires.

3.5.5.3 Serveur reporting

C'est un outil complet et de rapport faciles à utiliser qui permet d'évaluer l'utilisation de l'Internet par des employés de l'entreprise.

3.5.5.4 Firwall juniper SSG 550

Représente une nouvelle classe de dispositif de sécurité construite à cet effet qui offre un parfait mélange de haute performance, de sécurité et de connectivité LAN/WAN pour les déploiements de bureau régional et de leurs branches.

- **La zone strust**
  C'est la zone la plus confiante, car elle autorise le trafic sortant et interdit le trafic entrant et c'est pour cela que la RTC lui à confier son réseau LAN.

- **La zone untrust**
  C'est une zone qui autorise le trafic entrant et interdit le trafic sortant.

- **La DMZ (Demilitarized Zone)**
  Est une zone tampon d'un réseau de l'entreprise, située entre le réseau local et Internet derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (DNS, HTTP, DHCP). Pour des besoins d'administration et d'organisation, la zone DMZ de la RTC est partitionnée en trois sous zones :

- **La DMZ administrateur (admin)**
  Contient une station admin.

- **La DMZ filtrage**
  Contient un proxy bluecoat qui est une fonction destinée essentiellement aux environnements LAN. Il stocke les pages les plus demandées et apporte les avantages suivants :

  - Authentification des utilisateurs et gestion des droits d'accès.
  - Optimisation de la bande passante entre le provider et votre réseau.
  - Amélioration des temps d'accès aux sites.

  - **La DMZ renverse proxy**
    Fonction destinée aux environnements d'hébergement. Le cache est déployé en amont des serveurs et permet d'adresser une requête directement sur le cache sans solliciter les serveurs (les rendant ainsi plus disponibles pour des tâches plus valorisantes telles l'accès aux bases de données, le backup et l'accès aux pages dynamiques,. . ...).

3.5.5.5 Evaluation de la qualité des services

Le réseau devient le principal outil du système d'information de l'entreprise, il facilite l'échange des ressources et des données.
Dans ce contexte et après avoir mis en place l'audit informatique de réseau de SONATRACH de Béjaia et le centre informatique lors de notre stage, nous avons détecté quelques problèmes au niveau du fonctionnement du réseau LAN de la RTC.

- **Problématique**

  Trois problématiques sont annoncées dans notre étude :
  - Est-il indispensable d'administrer un réseau informatique d'entreprise ? ;
  - Ya-t-il un moyen de détection de panne afin d'augmenter les performances ?.
  - Qu'est ce qui incite l'entreprise à utiliser des logiciels payants, malgré l'existence de logiciels open source gratuits, adaptable à leur structure ? ;

Pour répondre à ces problèmes, nous avons choisi un thème sur **l'Administration** et la **supervision** de réseau LAN de SONATRACH à l'aide des **outils open source**.
Ainsi, nous allons choisir le moniteur Nagios plus précisément Nagios XI, qui est considéré comme la solution la plus aboutie dans son genre et la plus utilisée dans le monde du logiciel libre de supervision afin de superviser le réseau LAN de l'entreprise SONATRACH.

Aussi il est le plus répandu, le plus suivi par la communauté de développeurs, et comme moyen de simulation, nous allons choisir GNS3 qui est une suite d'outils open source qui regroupe un émulateur cisco avec des plates formes de virtualisation.

Le pourcentage d'utilisation des logiciels open source de supervision dans le monde : cette comparaison se base sur l'utilitaire Google Trends. La figure 3.5 montre le pourcentage d'utilisation des outils open source dans le monde. On remarque que NAGIOS possède un plus grand pourcentage par rapport à d'autres logiciels de supervision.

FIGURE 3.5 – Le pourcentage d'utilisation des logiciels open source de supervision dans le monde

3.6 Conclusion

A l'issu de ce chapitre, nous avons présenté la démarche audit suivie pour l'expertise du réseaux de la RTC qui va nous guider dans la réalisation des prochaines étapes de notre projet.

Dans un autre temps, il nous a permet d'avoir une vue globale du système existant afin de détecter les problèmes que l'entreprise confronte en ce qui concerne l'administration des réseaux.

Dans le chapitre suivant, on entamera la partie implémentation du réseau LAN de l'entreprise SONATRACH sous GNS3 et sa supervision à l'aide de différentes solutions open source gratuits.

Chapitre 4

Implémentation et supervision de réseau LAN de l'entreprise SONATRACH

4.1 Introduction

Après avoir défini tous les concepts nécessaires vient l'étape d'implementation et de supervision de réseau LAN de l'entreprise SONATRACH qui sert à mettre en pratique tout ce que nous avons défini auparavant.

Pour ce faire, nous allons utiliser quelques outils pour la supervision (CentOS 6.9, Nagios XI) et GNS3 comme moyen de simulation.
Dans ce qui suit nous allons présenter et argumenter nos choix.

Démarche d'implémentation

Premier niveau

Utilisation d'un logiciel de simulation GNS3 qui permet de reproduire une architecture physique ou logique d'un réseau.

Deuxième niveau

Le deuxième niveau est l'utilisation d'un hyperviseur de type 2 (VMware Workstation 12).

Troisième niveau

Le troisième niveau est la supervision d'un réseau LAN à l'aide d'un outil open source appelé Nagios plus précisément Nagios XI qui présente une version récente de Nagios.

4.2 Supervision informatique

4.2.1 Définition

La supervision informatique est la surveillance permanente de l'état du Système d'Information (SI) dans l'objectif de détecter les anomalies et d'alerter en conséquence.

La mise en place d'une supervision réseau, a donc pour principale vocation de collecter à intervalle régulier les informations nécessaires sur l'état de l'infrastructure et des entités qui y sont utilisées, de les analyser et de les rapporter [21].

4.2.2 Objectifs

L'objectif d'une supervision de réseaux peut ainsi se résumer en trois points [21] :

- **Etre réactif** en alertant l'administrateur (e-mail ou sms) en cas de dysfonctionnement d'une partie du système 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.

4.3 Outils utilisés

La phase de réalisation et de mise en oeuvre a nécessité l'installation de plusieurs outils dont nous avons besoin :

4.3.1 GNS3

GNS3 (***Graphical Network Simulator***) est un logiciel libre et disponible pour Windows, Linux et MacOS X, il permet de reproduire une architecture physique ou logique grâce aux [27] :
-Dynamips qui est un émulateur IOS Cisco,
-Dynagen qui est une interface en mode texte pour Dynamips.

4.3.2 CentOS 6.9

CentOS (Community enterprise Operating System)
Est une distribution GNU/Linux principalement destinée aux serveurs. Tous ses paquets, à l'exception du logo, sont des paquets compilés à partir des sources de la distribution RHEL (Red Hat Enterprise Linux), éditée par la société Red Hat. Elle est donc quasiment identique à celle-ci et se voit compatible d'un point de vue binaire [25].

4.3.2.1 Paramétrage de CentOS 6.9

La distribution nécessite une mise à jour et quelques réglages pour la rendre fonctionnelle, pour cela nous allons aborder l'utilisation des utilitaires "***yum***".

- **Mise à jour du système avec "yum"(Yellow dog Updater)**
  La distribution dispose d'un outil pour la gestion des paquets. Il s'agit de "***yum update***" (Yellow dog Updater, Modified). Nous allons l'utiliser pour mettre à jour notre système. Nous nous sommes connectés au compte de l'administrateur "root", puis nous allons taper la commande suivante :

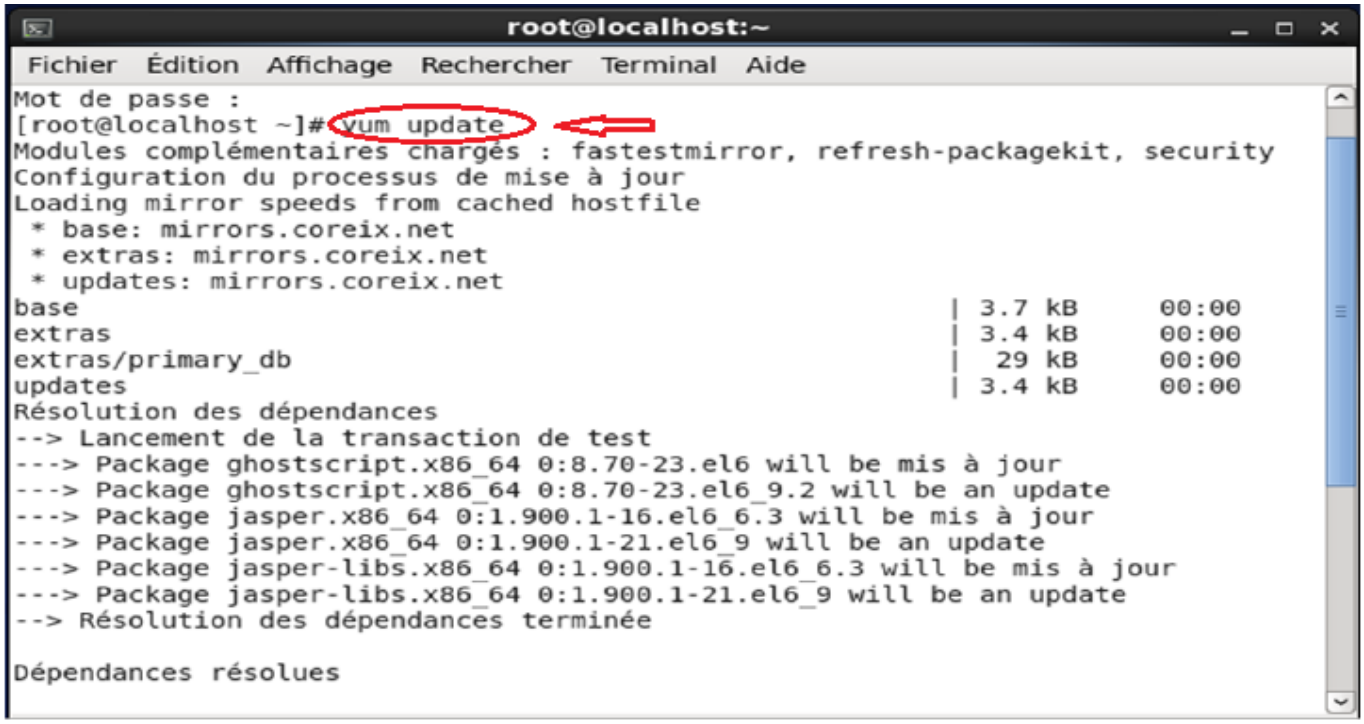

FIGURE 4.1 – Mise à jour avec yum update

Le reste de la procédure paramétrage de CentOS 6.9 est détaillé en annexe B à la fin de ce rapport.

4.3.2.2 Installation et configuration de DNS

Le Domain Name System (ou DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.
Les paquetages : la distribution CentOS dispose du paquet bind.

La figure 4.2 montre l'installation de bind-dns sous CentOS6.9 en utilisant la commande ***yum install bind bind-utils***

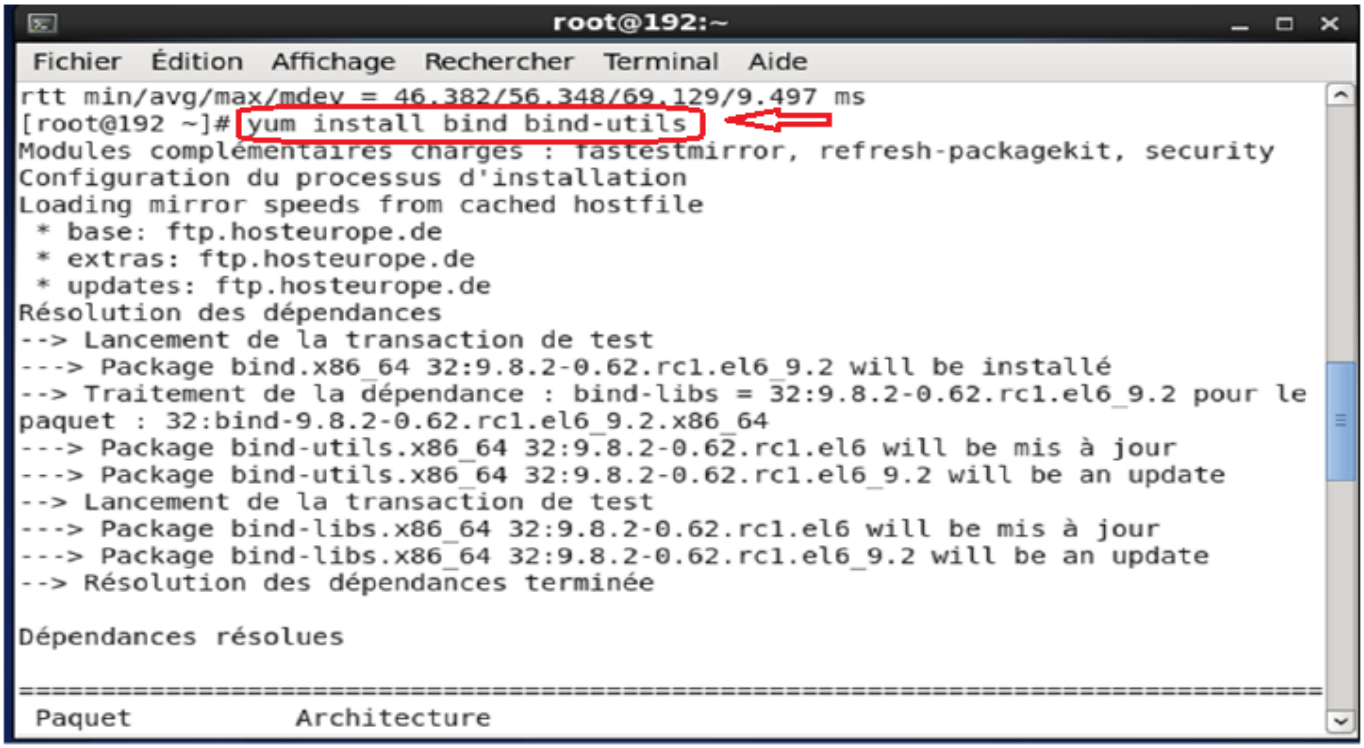

FIGURE 4.2 – Installation de bind

4.3.2.3 Installation et configuration d'un serveur DHCP

Dynamic Host Configuration Protocol (DHCP, protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau.

Avant d'installer le DHCP, nous devons s'assurer de l'établissement de la connexion pour cela nous devons acceder au fichier ***sysconfig/network-scripts*** en utilisant la commande ***cd /etc/sysconfig/network-scripts*** :

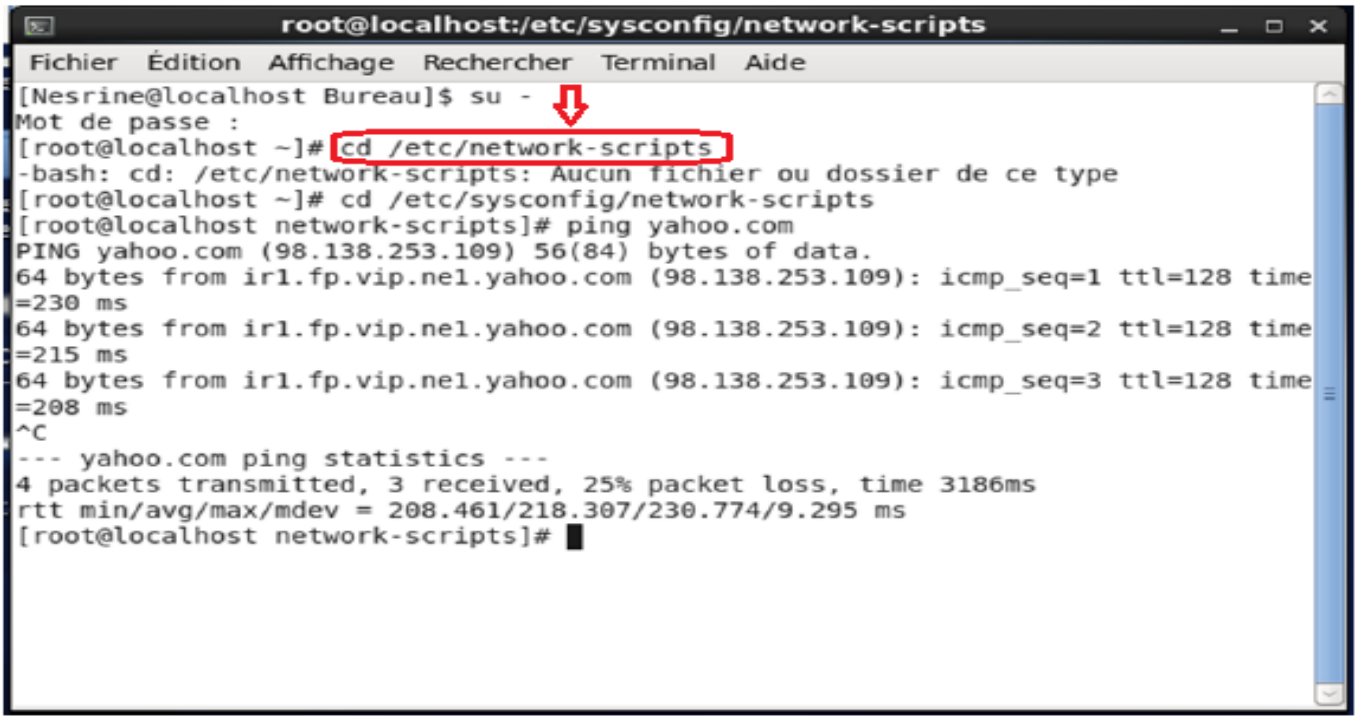

FIGURE 4.3 – Établissement de la connexion

4.3.3 Nagios XI

Est une application informatique gratuite et open source qui surveille les systèmes, les réseaux et l'infrastructure. Nagios offre des services de surveillance et d'alerte pour serveurs, commutateurs, applications et services. Il avertit les utilisateurs quand les problèmes surgissent et les avertit une seconde fois lorsque le problème est résolu [28].

4.3.3.1 Principales fonctionnalités de Nagios

Les principales fonctionnalités de Nagios sont [28] :

1. Surveillance des services réseaux (SMTP, POP3, HTTP, NNTP, PING, etc.) ;
2. Notifications des contacts quand un hôte ou un service a un problème et quand celui-ci est résolu (via email, sms, ou par tout autre méthode définie par l'utilisateur) ;
3. Surveillance des ressources des hôtes (charge processeur, utilisation des disques, etc.) ;
4. Parallélisation de la vérification des services.

4.3.3.2 Installation et configuration de Nagios XI sous CentOS 6.9

Après avoir fini l'installation de CentOS 6.9 nous allons poursuivre l'installation de Nagios XI sous l'interface de ce dernier mais avant d'entamer l'installation de Nagios XI nous devons

installer un support pour la sécurité, comme les pare-feu et la sécurisation du linux, pour cela on utilisera la commande "***yum install firewalld wget -y***" (voir la figure 4.4)

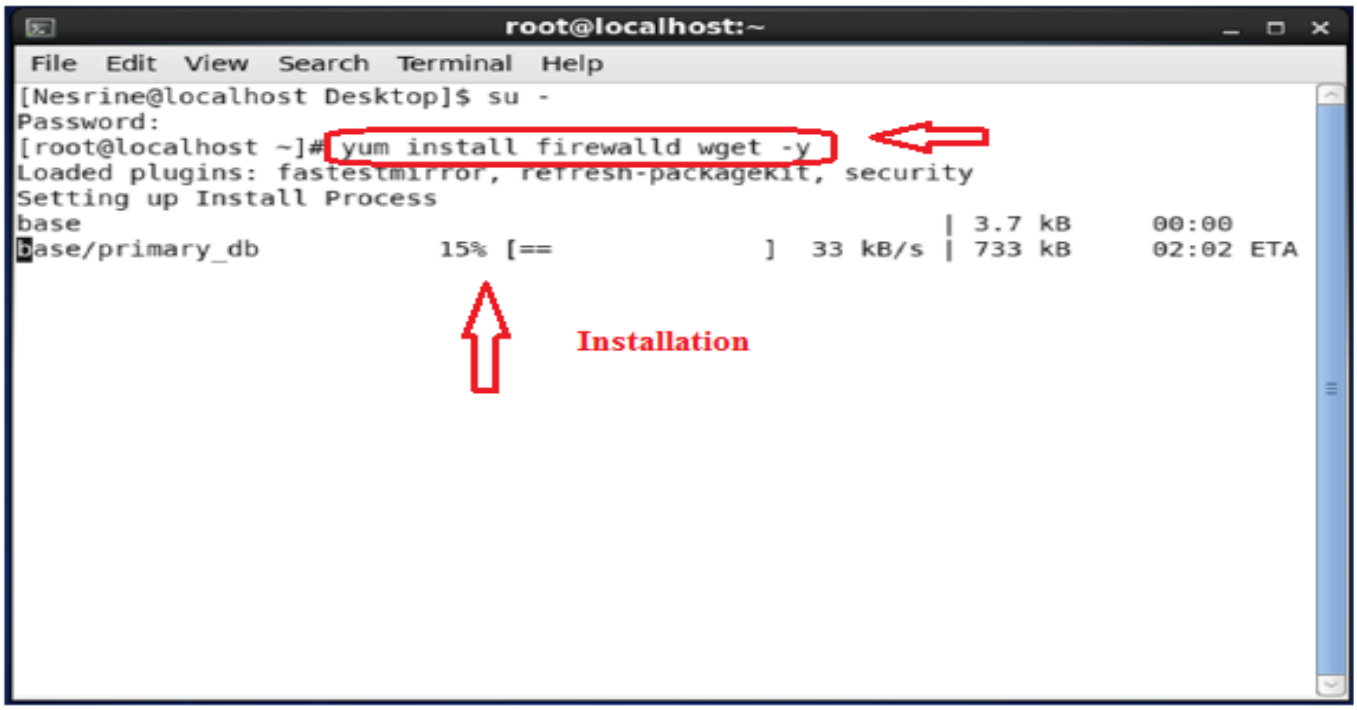

FIGURE 4.4 – Installation de support de sécurité

Maintenant nous allons exécuter l'installation complète de Nagios XI, pour cela nous devons accéder au répertoire Nagios XI et en utilisant la commande ***./fulinstall*** nous allons créer l'utilisateur Nagios, group nagcmd avec installation de toutes les dépendances et configurations de Nagios Core, Plugins, Bases de données pour Backend et NRPE.

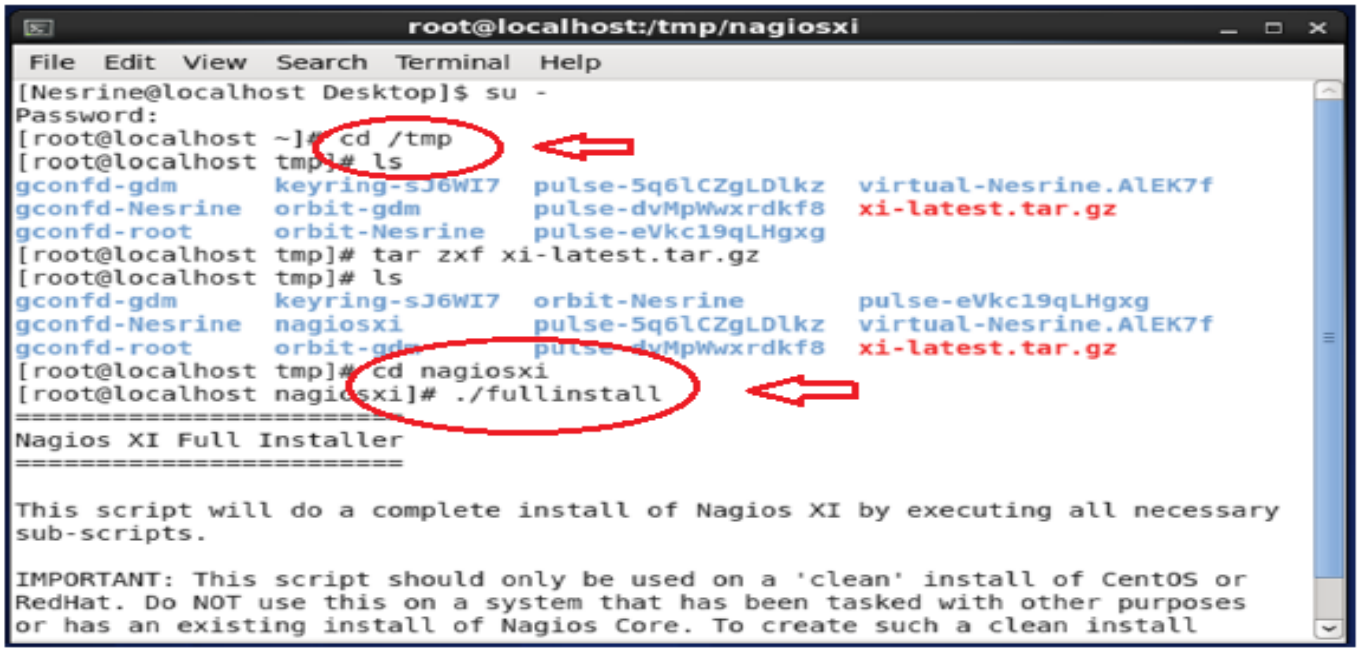

FIGURE 4.5 – la commande complète

Le reste de la procédure d'installation et configuration de Nagios XI sous CentOS 6.9 est détaillé en annexe C à la fin de ce rapport.

4.4 Reproduction du réseau LAN de SONATRACH

Afin de configurer et superviser notre réseau LAN de l'entreprise SONATRACH nous allons le reproduire sous le simulateur GNS3.

4.4.1 Partie théorique

4.4.1.1 Configuration des VLANs

Le tableau 4.1 suivant montre les noms des VLANs existant au niveau de l'entreprise ainsi que leur adresse de sous réseau.

Nom VlAN	ID VLAN	Adresse de sous réseau	Description
Mgmt	9	192.168.9.0/24	VLAN pour management des équipements
Finance	10	172.16.10.0/24	VLAN des postes de travail de la direction des Finances
Commercial	11	172.16.11.0/24	VLAN des postes de travail de la direction Commerciale
Juridique	20	172.16.20.0/24	VLAN des postes de travail de la direction Juridique
Technique	21	172.16.21.0/24	VLAN des postes de travail de la direction Technique

TABLE 4.1 – Nom des VLANs

4.4.1.2 Le VTP (Vlan Trunking Protocol)

Durant la phase de déploiement, nous allons configurer le switch Coeur (SW-Coeur1) en mode VTP Server alors que les autres switchs seront des VTP Client.

Le tableau ci-dessous montre comment le VTP sera configuré :

VTP	Nom	MODE
SW-Coeur	RTC	Server
Tous les autres switchs	RTC	Client

TABLE 4.2 – Configuration de VTP

4.4.1.3 Le STP (Spanning Tree Protocol)

Le protocole ***Spanning Tree*** (STP) est un protocole de la couche 2 (liaison de données) conçu pour les commutateurs. Il permet de créer un chemin sans boucle dans un environnement commuté et d'équipements redondant.

STP détecte et désactive ces boucles et fournit un mécanisme de liens de sauvegarde [26].

4.4.1.4 Classification des PC selon les VLANs

Les interfaces entre tous les switchs d'accés, distribution, coeur seront configurés en mode trunk pour qu'elles puissent transporter les informations des différents VLANs. Les interfaces qui seront connectées à des postes de travail seront configurées en mode accès.

La liste illustrée dans le tableau 4.3 ci-dessous présente les VLANs et les adresses IP employées :

Nom d'hôte N°	Port de switch	Vlan ID	Adresse IP	Passerelle
PC1	Port 1 SW-Acc01	10	172.16.10.1/24	172.16.10.254
PC2	Port 2 SW-Acc01	10	172.16.10.2/24	172.16.10.254
PC3	Port 3 SW-Acc02	11	172.16.11.1/24	172.16.11.254
PC4	Port 4 SW-Acc02	11	172.16.11.2/24	172.16.11.254
PC5	Port 5 SW-Acc03	20	172.16.20.1/24	172.16.20.254
PC6	Port 6 SW-Acc03	20	172.16.20.2/24	172.16.20.254
PC7	Port 7 SW-Acc04	21	172.16.21.1/24	172.16.20.254
PC8	Port 8 SW-Acc04	21	172.16.21.2/24	172.16.21.254

TABLE 4.3 – Classification des PC selon les VLANs

4.4.1.5 Administration des équipements

Le VLAN de management " vlan 9 " sera utilisé pour l'administration des équipements. Les adresses IP de management seront attribuées aux équipements.

4.4.2 Partie pratique

Afin de réaliser notre projet nous allons utiliser le simulateur GNS3 et l'outil de supervision NAGIOS XI qui vont être détaillé dans ce qui suit :

4.4.2.1 Le simulateur GNS3 (Graphical Network Simulator)

Il s'agit d'une interface graphique permettant de faciliter la conception de topologies réseaux complexes.

La figure 4.6 ci-dessous présente l'architecture réseau local de SONATRACH sous GNS3.

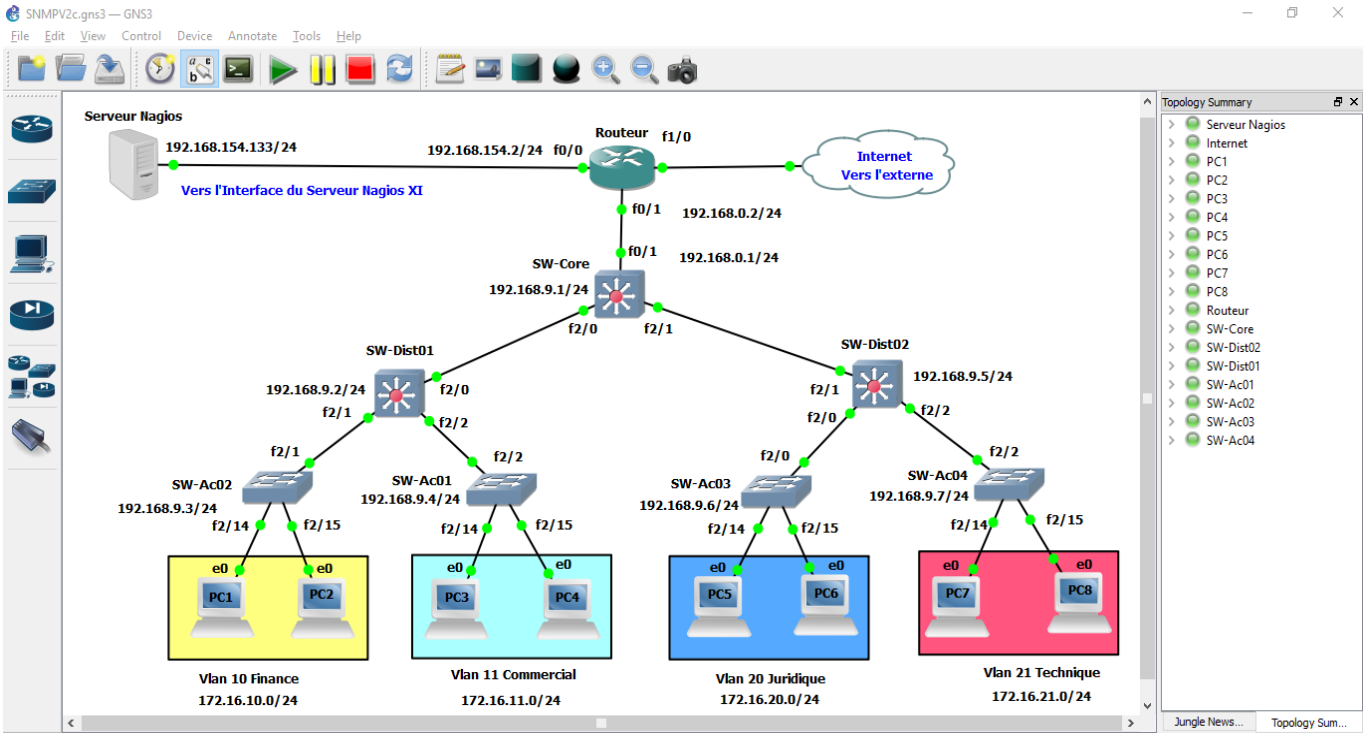

FIGURE 4.6 – Architecture du réseau LAN sous GNS3

4.4.2.2 Configuration des équipements

Pour configurer les équipements du modèle on utilise la console :
La figure suivante présente l'interface de la console (voir la figure 4.7).

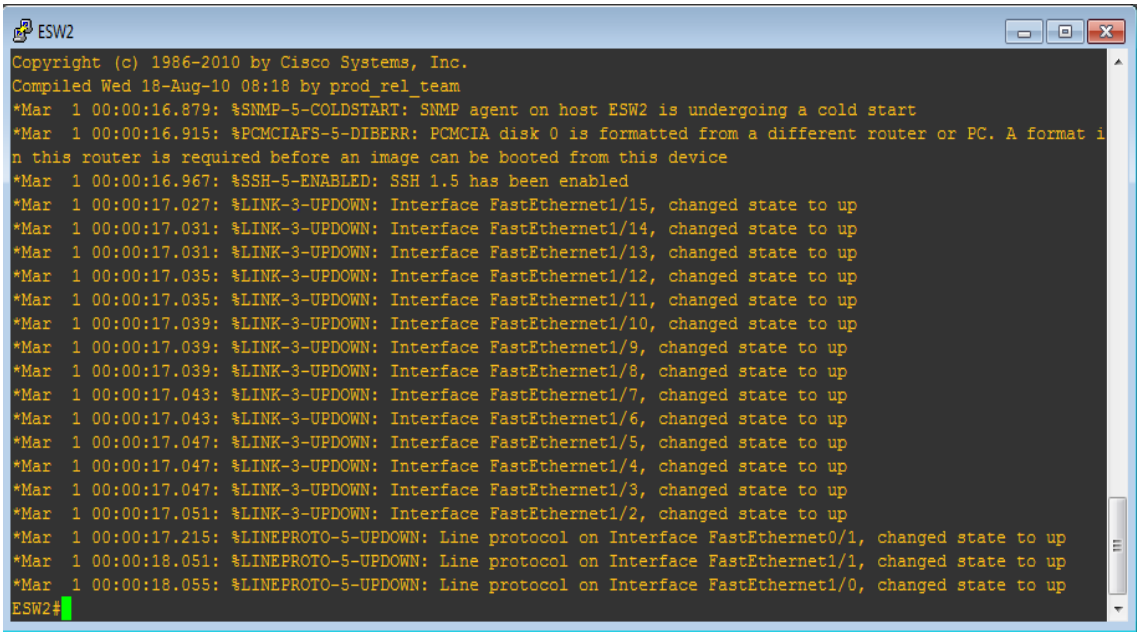

FIGURE 4.7 – Interface console

4.4.2.3 Configuration des équipements

Dans ce qui suit nous allons présenter la configuration en général de tous les équipements avec un exemple configuré.

Configuration des commutateurs

Nous allons lancer une série de configuration pour chaque switch.

- **Création des VLANs**

  La figure 4.8 indique la création des VLANs sur l'un des switchs d'accès (voir la figure 4.8).

```
SW-Coeur#vlan database
SW-Coeur(vlan)#vlan 9 name mgmt
VLAN 9 added:
    Name: mgmt
SW-Coeur(vlan)#vlan 10 name finance
VLAN 10 added:
    Name: finance
SW-Coeur(vlan)#vlan 11 name commercial
VLAN 11 added:
    Name: commercial
SW-Coeur(vlan)#vlan 20 name juridique
VLAN 20 added:
    Name: juridique
SW-Coeur(vlan)#vlan 21 name technique
VLAN 21 added:
    Name: technique
```

FIGURE 4.8 – Création des VLANs

- **Preuve de création de VLANs**
  Utilisation de la commande ***"show vlan-switch"*** dans l'un des switchs. Prenons comme cas l'un des switchs distribution (voir la figure 4.9) :

```
SW-Des1#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                Fa1/14, Fa1/15
9    mgmt                             active
10   finance                          active
11   commercial                       active
20   juridique                        active
21   technique                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-Des1#
```

FIGURE 4.9 – Preuve d'existence de VLAN (cas : switch coeur1)

Ensuite nous allons suivre les étapes de configuration illustrées ci-dessous :

1. Configuration de hostname (Nomination des équipements sur GNS3) ;
2. Configuration de mots de passe pour la ligne console et vertical ;
3. Configuration de VTP ;

4. Configuration des interfaces ;
5. Configuration de spanning-tree ;
6. Configuration de SSH ;
7. Configuration de DHCP et DNS ;
8. Configuration de routage inter-vlan.

Exemple de configuration : le switch coeur :

1. **Configuration de hostname** La figure 4.10 montre la configuration de hostname.

FIGURE 4.10 – Configuration de Hostname (cas : switch coeur)

2. **Configuration de mots de passe** La figure 4.11 montre la configuration de mot de passe pour la ligne console et vertical.

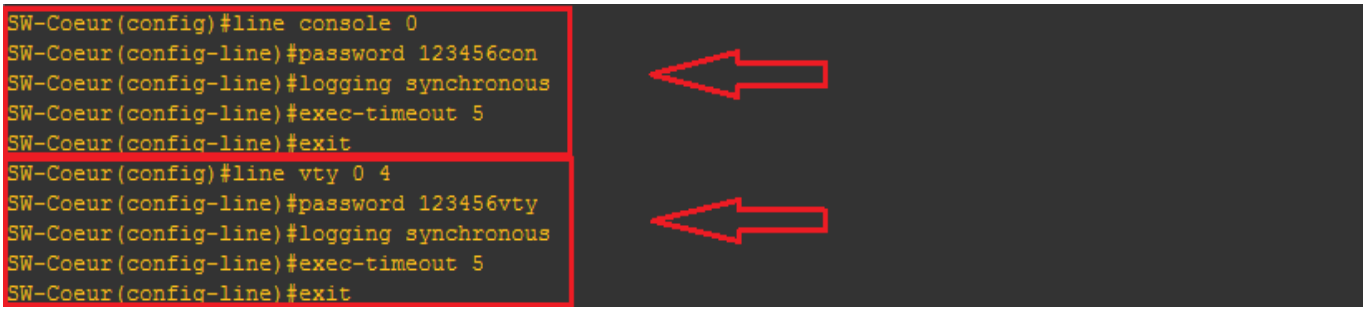

FIGURE 4.11 – Configuration de mots de passe (cas : switch coeur)

3. **Configuration de VTP** La figure 4.12 montre la configuration de vtp en mode server pour le switch coeur.

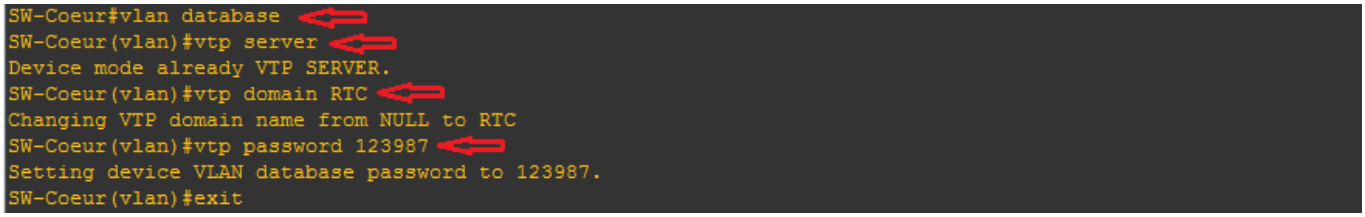

FIGURE 4.12 – Configuration de VTP (cas : switch coeur)

4. **Preuve d'existence de VTP** La figure 4.13 montre la preuve d'existence de vtp.

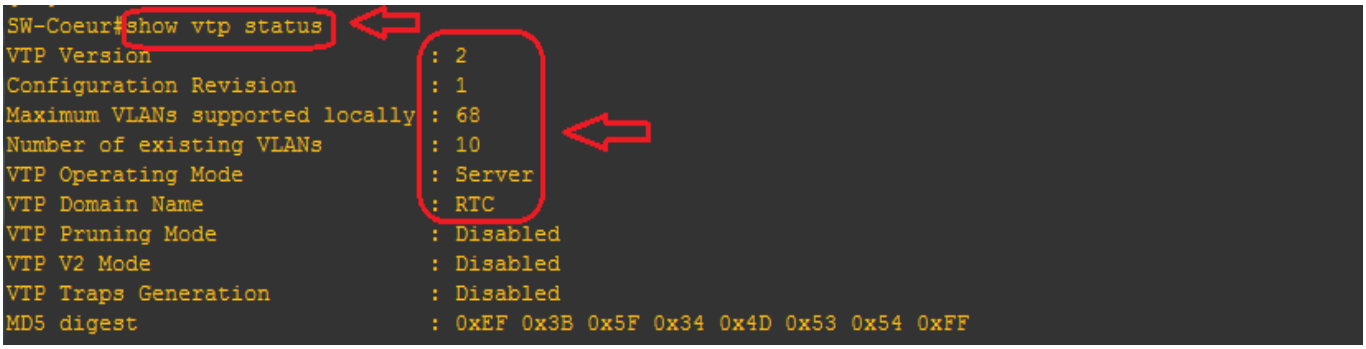

FIGURE 4.13 – Preuve d'existence de VTP (cas : switch coeur)

5. **Configuration des interfaces VLANs** La figure 4.14 montre la configuration des interfaces VLANs.

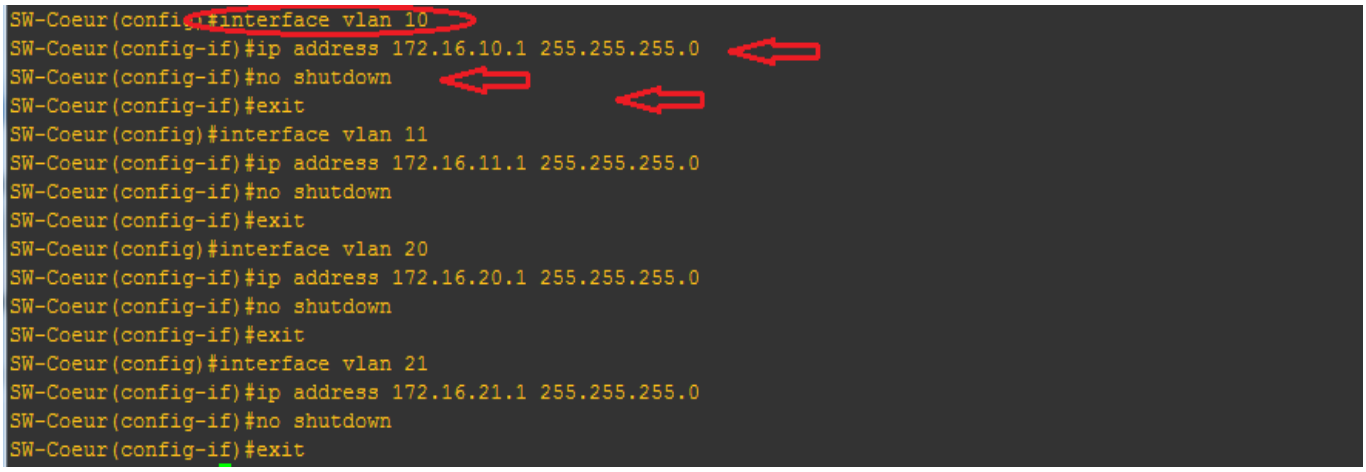

FIGURE 4.14 – Configuration des interfaces VLANs (cas : switch coeur)

5.1 Configuration des interfaces VLANs en mode access La figure 4.15 montre la configuration des interfaces VLANs en mode access.

FIGURE 4.15 – Configuration des interfaces VLANs en mode access (cas : switch Access)

5.2 Configuration des interfaces VLANs en mode trunk La figure 4.14 montre la configuration des interfaces VLANs en mode trunk.

```
SW-Coeur(config)#int range f1/0 - 3
SW-Coeur(config-if-range)#switchport trunk encapsulation dot1q
SW-Coeur(config-if-range)#switchport mode trunk
```

FIGURE 4.16 – Configuration des interfaces VLANs en mode trunk (Cas : switch Coeur)

6. **Configuration de spanning-tree**

Le "Spanning-Tree" est un protocole qui permet d'éviter les boucles en désactivant les liens redondants. Pour effectuer un diagnostic nous allons prendre le switch-coeur comme switch-serveur en lui introduisant la plus grande priorité (voir la figure 4.17).

```
SW-Coeur(config)#spanning-tree vlan 10 priority ?
  <0-65535>  bridge priority

SW-Coeur(config)#spanning-tree vlan 10 priority 65535
SW-Coeur(config)#spanning-tree vlan 11 priority 65535
SW-Coeur(config)#spanning-tree vlan 20 priority 65535
SW-Coeur(config)#spanning-tree vlan 21 priority 65535
SW-Coeur(config)#exit
```

FIGURE 4.17 – Configuration Spanning-Tree (cas : switch-coeur)

Pour les autres switch nous allons les configurés comme switch-client en lui introduisant la priorité 0 (voir la figure 4.18).

```
SW-Des1(config)#spanning-tree vlan 10 priority 0
SW-Des1(config)#spanning-tree vlan 11 priority 0
SW-Des1(config)#spanning-tree vlan 20 priority 0
SW-Des1(config)#spanning-tree vlan 21 priority 0
SW-Des1(config)#
```

FIGURE 4.18 – Configuration Spanning-Tree (cas : switch-distribution)

7. **Configuration de SSH (voir la figure 4.19)**

Configuration d'un compte utilisateur avec un mot de passe en utilisant la syntaxe ***username(nom-utilisateur) password(mot de passe)***, par la suite nous allons définir un nom de domaine pour que le routeur puisse générer les clés de chiffrement en utilisant la commande ***ip domain-name*** (voir la figure 4.19).

```
SERVEUR_SSH(config)#username admin password sonatrach
SERVEUR_SSH(config)#ip domain-name mondomaine.com
SERVEUR_SSH(config)#
```

FIGURE 4.19 – Configuration de SSH

Pour générer les clés nous allons utiliser la commande ***crypto key generate rsa*** (voir figure 4.20) :

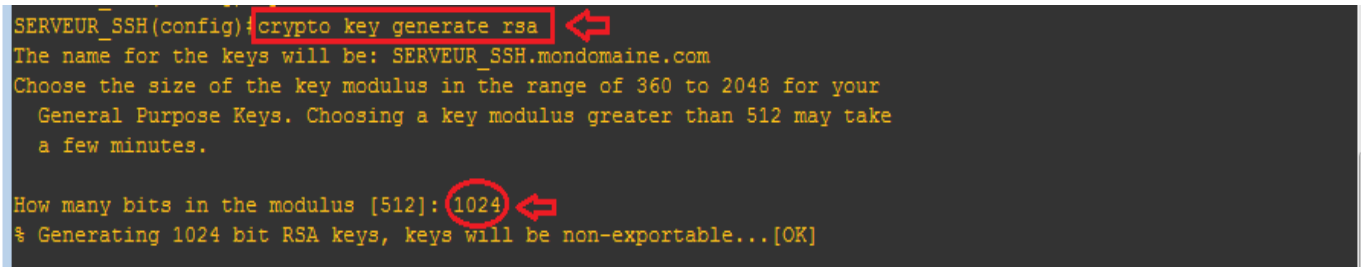

FIGURE 4.20 – Génération des clés

Configuration de la version de SSH à utiliser (voir la figure 4.21) :

FIGURE 4.21 – Configuration de la version de SSH

La commande ***ip ssh time-out 120*** consiste à déconnecter l'utilisateur en cas d'inactivité pour une durée déterminée (voir la figure 4.22) :

FIGURE 4.22 – détermination d'une durée de connectivité

Pour limiter le nombre de tentatives du mot de passe nous allons utiliser la commande ***ip ssh authentification-retries 3****(voir la figure 4.23)* :

FIGURE 4.23 – Limitation de nombres de tentatives

8. **Configuration de DHCP et DNS (voir la figure 4.24)**

Nous allons donc nous connecter au switch coeur afin de configurer le DHCP et le DNS, pour cela le serveur DHCP devra distribuer une adresse sur la plage IP 172.16.10.0/24 ainsi la passerelle qui est par défaut 172.16.10.1, le serveur DNS (8.8.8.8) :

```
SW-Coeur1(config)#ip dhcp pool finance
SW-Coeur1(dhcp-config)#network 172.16.10.0 255.255.255.0
SW-Coeur1(dhcp-config)#default-router 172.16.10.1
SW-Coeur1(dhcp-config)#dns-server 8.8.8.8
SW-Coeur1(dhcp-config)#exit
SW-Coeur1(config)#ip dhcp pool commercial
SW-Coeur1(dhcp-config)#network 172.16.11.0 255.255.255.0
SW-Coeur1(dhcp-config)#default-router 172.16.11.1
SW-Coeur1(dhcp-config)#dns-server 8.8.8.8
SW-Coeur1(dhcp-config)#exit
SW-Coeur1(config)#ip dhcp pool juridique
SW-Coeur1(dhcp-config)#network 172.16.20.0 255.255.255.0
SW-Coeur1(dhcp-config)#default-router 172.16.20.1
SW-Coeur1(dhcp-config)#dns-server 8.8.8.8
SW-Coeur1(dhcp-config)#exit
SW-Coeur1(config)#ip dhcp pool technique
SW-Coeur1(dhcp-config)#network 172.16.21.0 255.255.255.0
SW-Coeur1(dhcp-config)#default-router 172.16.21.1
SW-Coeur1(dhcp-config)#dns-server 8.8.8.8
SW-Coeur1(dhcp-config)#exit
```

FIGURE 4.24 – Configuration de DHCP et DNS (cas : switch-coeur)

Et avec une exclusion des adresses 172.16.10.1, 172.16.11.1, 172.16.20.1, 172.16.21.1, nous allons taper la commande suivante (voir la figure 4.25) :

```
SW-Coeur(config)#ip dhcp excluded-address 172.16.10.1
SW-Coeur(config)#ip dhcp excluded-address 172.16.11.1
SW-Coeur(config)#ip dhcp excluded-address 172.16.20.1
SW-Coeur(config)#ip dhcp excluded-address 172.16.21.1
SW-Coeur(config)#
```

FIGURE 4.25 – exclusion d'address ip (cas : switch-coeur)

Sauvegarde de configuration

Pour sauvegarder la configuration, nous allons taper la commande suivante (voir la figure 4.26) :

```
SW-Coeur#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

FIGURE 4.26 – Sauvegarde de configuration (cas : switch-coeur)

9. **Configuration de routage inter-vlan**

On détermine les adresses IP qu'on souhaite affecter à l'interface VLAN sur le switch. Pour que le switch puisse passer entre les VLAN, les interfaces VLAN doivent être configurées avec une adresse IP. Lorsque le switch reçoit un paquet destiné à un autre sous-réseau / VLAN, le switch examine la table de routage afin de déterminer l'emplacement de la transmission du paquet. Le paquet est ensuite transmis à l'interface VLAN de la destination. Nous allons configurer les interfaces VLAN avec une adresse IP (voir la figure 4.27).

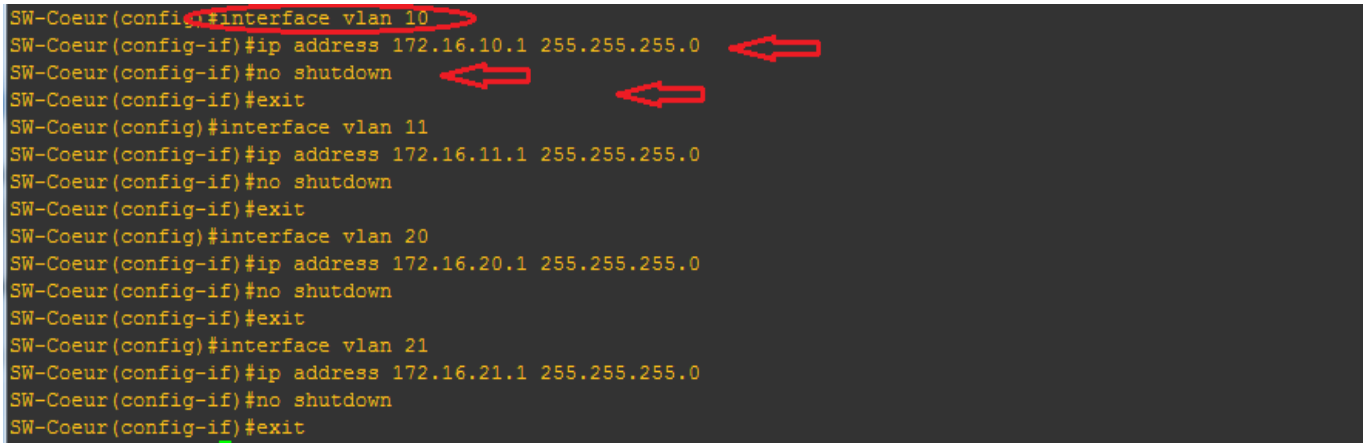

FIGURE 4.27 – Configuration de routage inter-vlan (cas : switch-coeur

Nous allons configurer l'interface par défaut pour le switch (voir la figure 4.28).

FIGURE 4.28 – Configuration de l'interface par défaut(cas : switch-coeur

4.4.3 Analyse Supervision - Conformité aux objectifs

Avant d'entamer la supervision des équipements (switch et routeur) nous devons d'abord configurer le snmp dans chaque équipement. Prenant comme exemple le SW-Coeur Figure (4.29) :

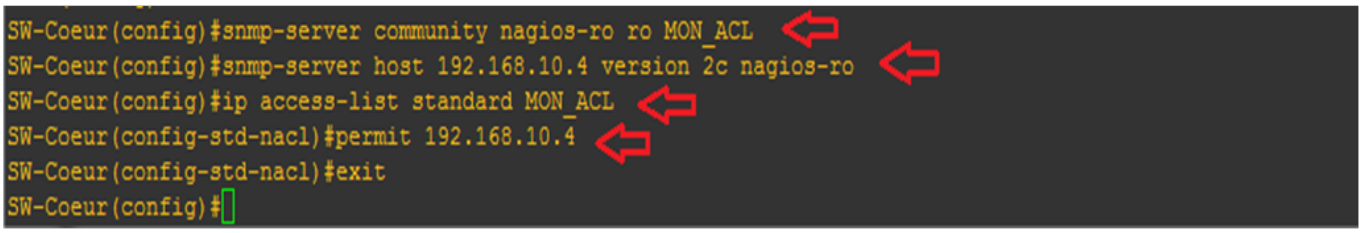

FIGURE 4.29 – configuration de snmp (cas : SW-Coeur)

4.4.3.1 Centralisation surveillance

La console permet le monitoring d'interface de switch et de routeur via SNMP.
Dans notre cas, nous allons superviser tous les équipements (routeur et switch) à travers la console de Nagios XI.
La figure 4.30 montre l'introduction d'une adresse IP ainsi que le nom de la commuté de Nagios XI afin de pouvoir mettre en place une supervision sur l'un des switchs.

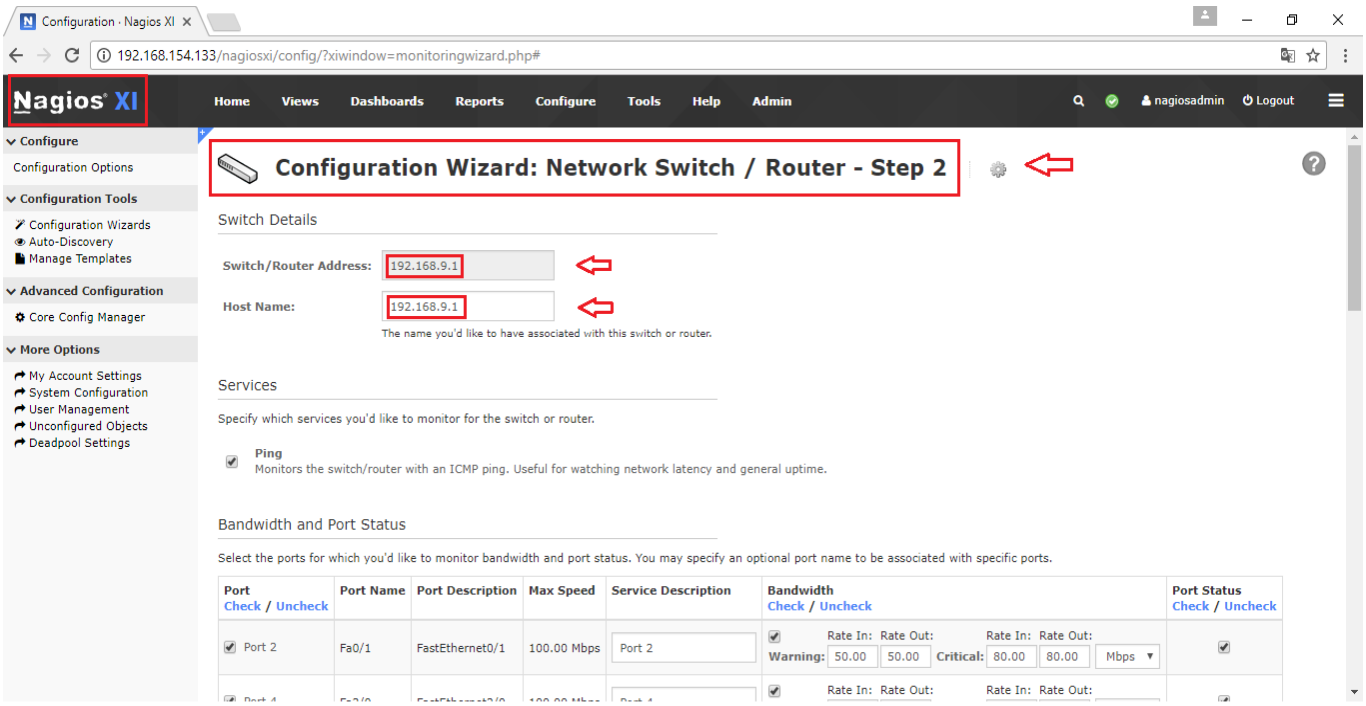

FIGURE 4.30 – Introduction d'une adresse IP

A partir de l'adresse IP introduite, Nagios XI lance ainsi une découverte des interfaces (figure 4.31)

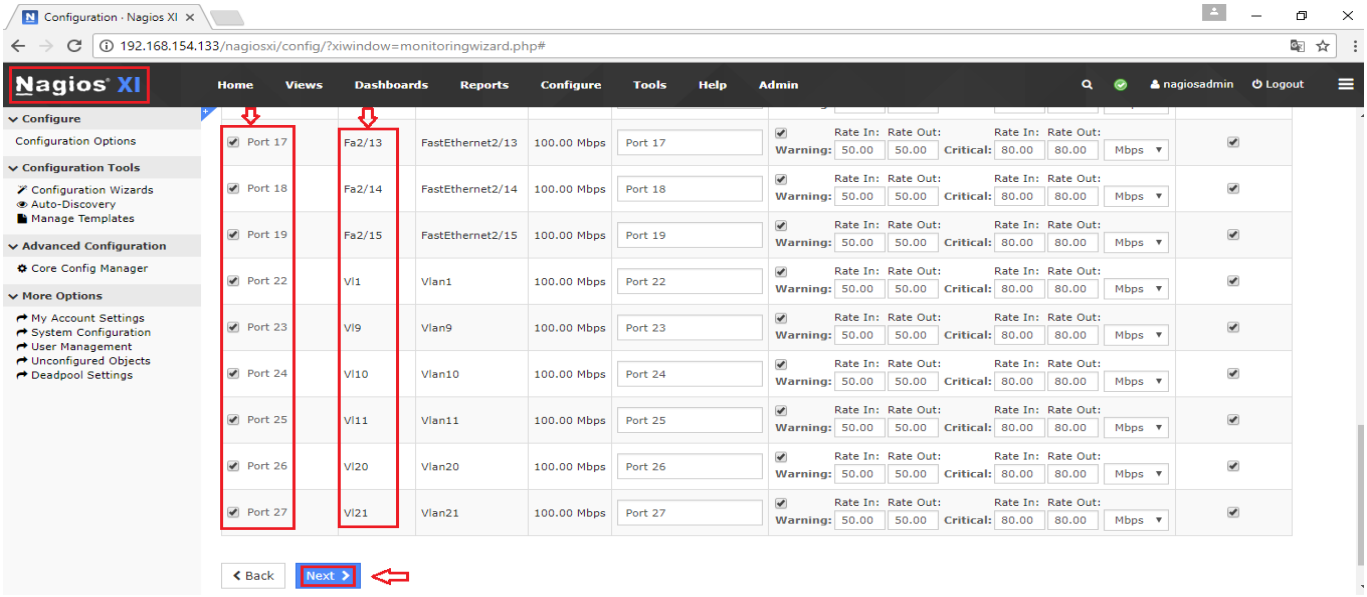

FIGURE 4.31 – Découverte des interfaces

En cliquant sur Next un message de succès apparait (figure 4.32).

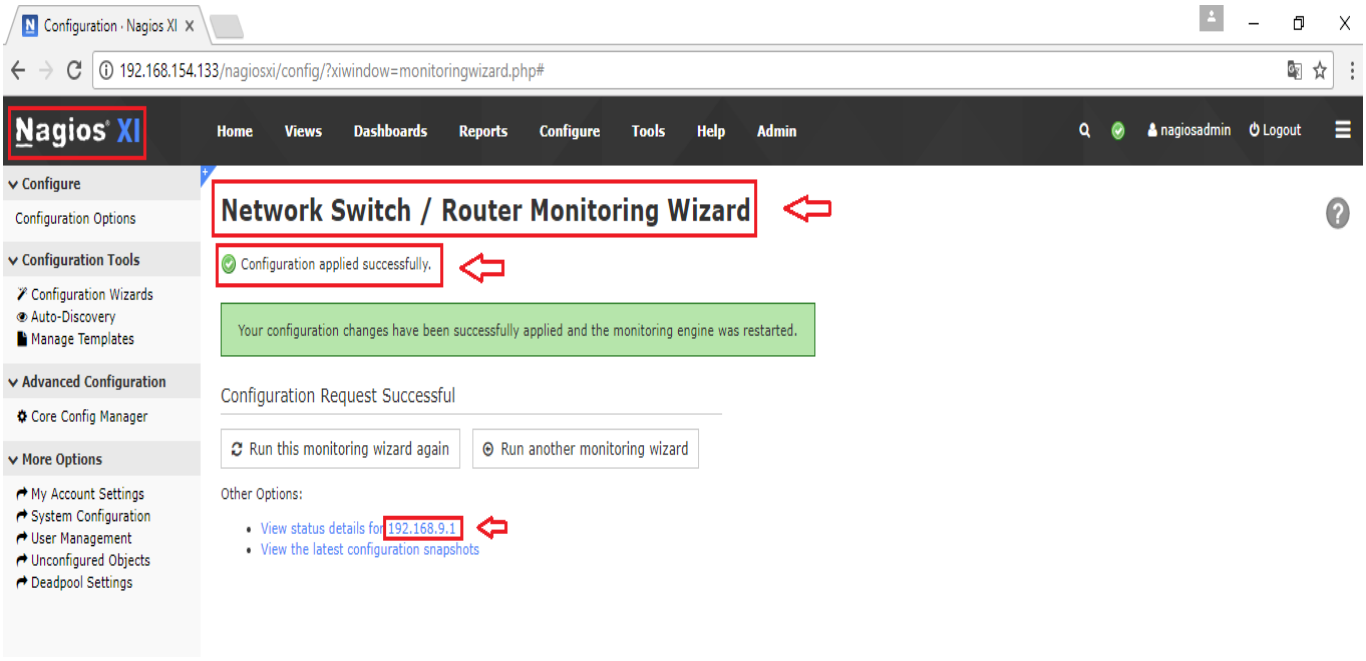

FIGURE 4.32 – Message de succès

En cliquant sur l'adresse IP Nagios XI met en place une visualisation de l'état des interfaces (figure 4.33 et 4.34).

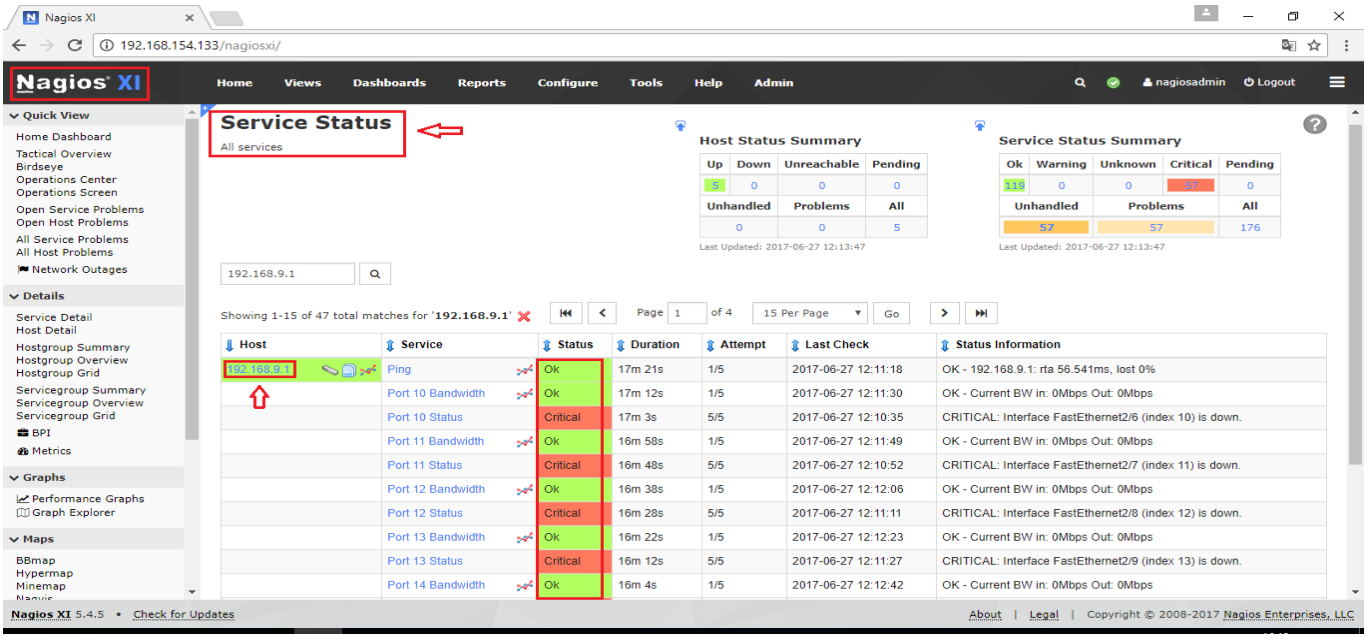

FIGURE 4.33 – visualisation de l'état des interfaces

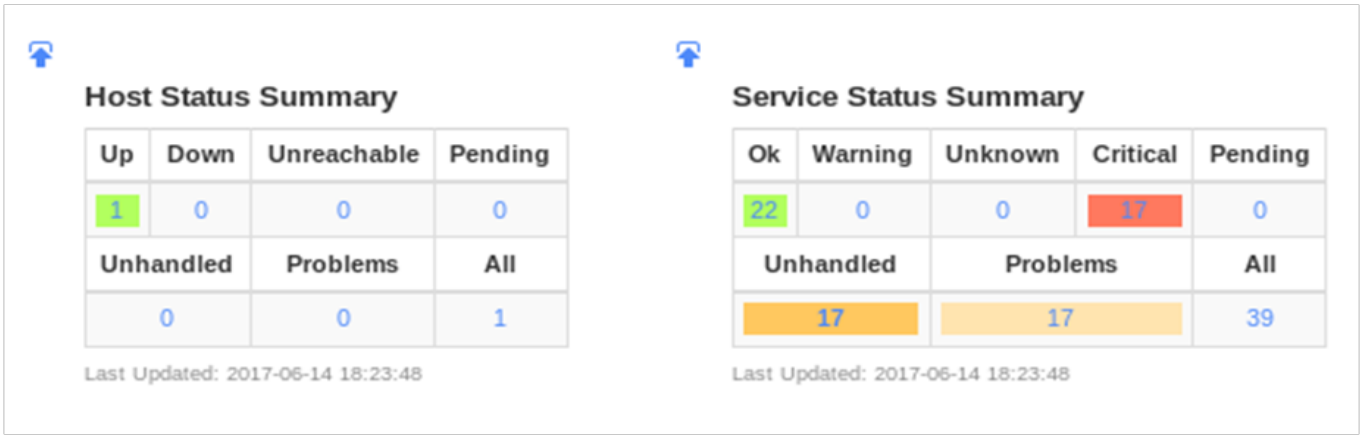

FIGURE 4.34 – visualisation de l'état des interfaces(suite)

Après avoir ajouter l'un des switch dans Nagios XI et à travers la console de ce dernier nous allons acceder au détail de ce switch auquel nous allons effectuer le ping vers son adresse IP qui a été configuré sous le simulateur GNS3 (figure 4.35).

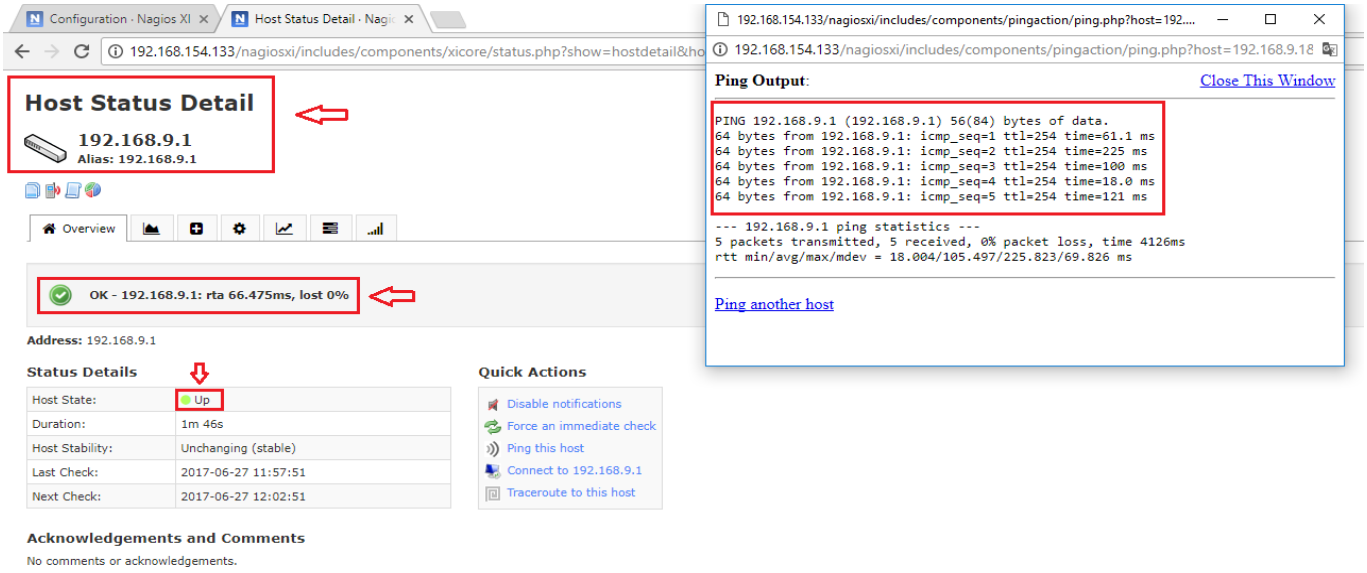

FIGURE 4.35 – Détaille de l'un des équipements (Cas : Switch coeur)

4.5 Configuration du courrier électronique et de la notification de texte dans Nagios XI

Il est extrêmement important de recevoir correctement les notifications par courrier électronique. La page Gérer les paramètres de messagerie a été créée pour nous permettre de gérer ces paramètres et de veiller à ce que les utilisateurs soient correctement notifiés par le serveur XI. Mais avant de configurer notre courrier électronique et les notifications de texte dans Nagios XI nous devons tout d'abord configurer le SMTP.

- **SNMP**
  Comme son nom voudrait le faire croire, Simple Network Management Protocol est un protocole "simple" destiné à gérer des équipements informatiques, à distance ou non [11].

  Il permet principalement de [11] :
  - visualiser une quantité pouvant être impressionnante d'informations concernant le matériel, les connexions réseaux, leur état de charge,
  - modifier le paramétrage de certains composants,
  - alerter l'administrateur en cas d'événements considérés comme grave,
  - et d'autres choses encore etc.

  La figure 4.36 nous montre une configuration de SNMP sous Nagios XI.

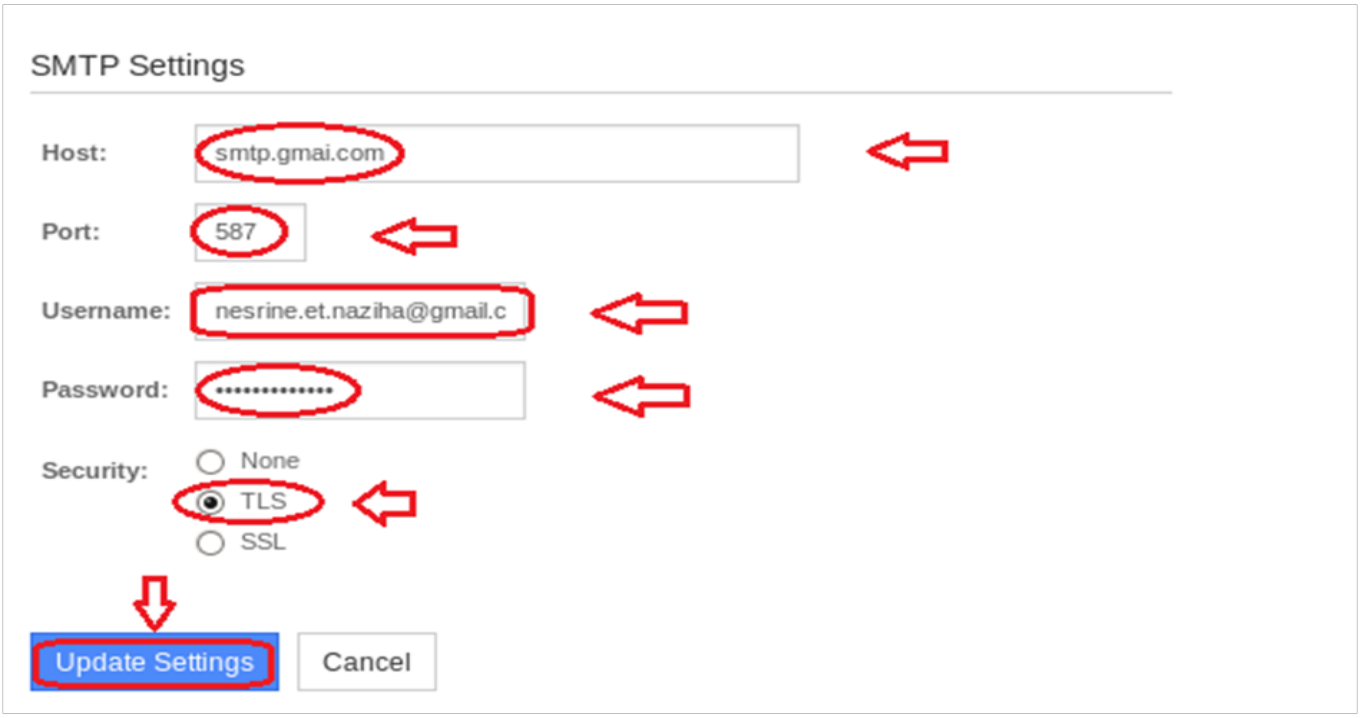

FIGURE 4.36 – configuration de SNMP sous Nagios XI

4.6 Test de paramètre de messagerie

Afin de vérifier la possibilité de recevoir des alertes de Nagios XI, nous avons envoyé un e-mail de test à notre adresse email auquel nous nous sommes connectés Un courrier sera envoyé à l'adresse email : nesrine.et.naziha@gmail.com (La figure 4.37)

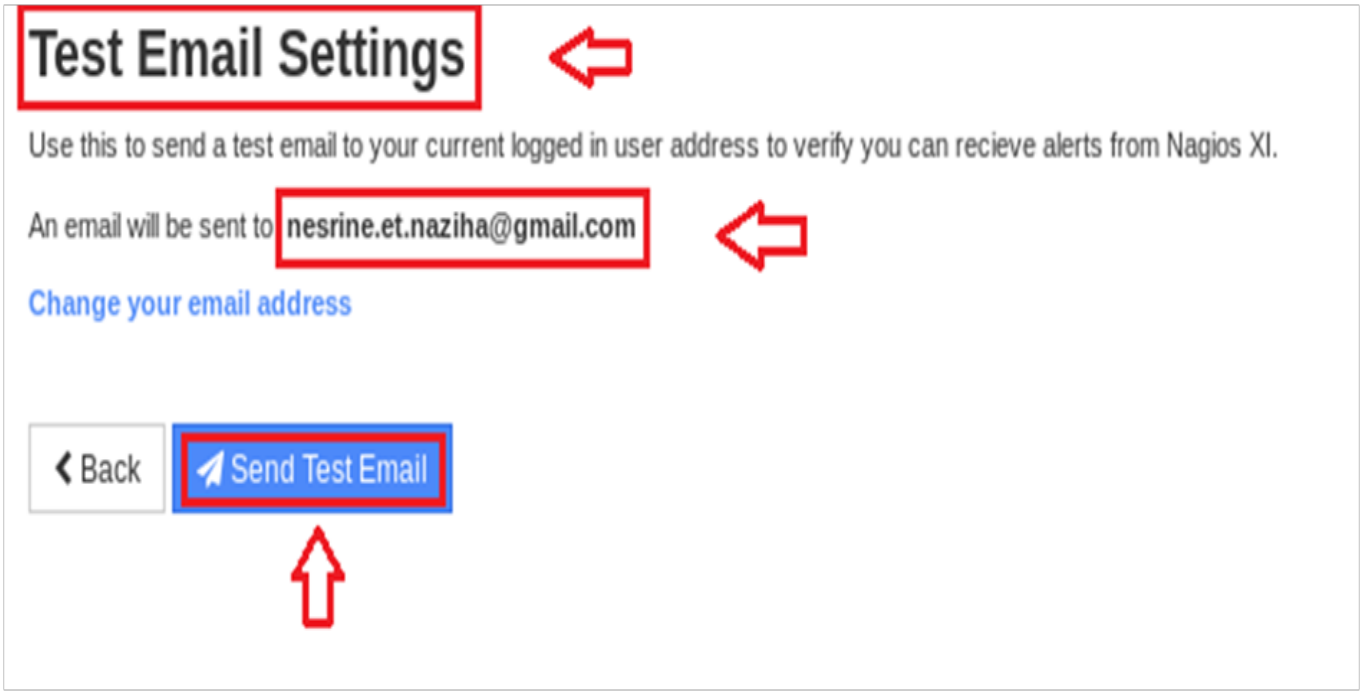

FIGURE 4.37 – Test de paramètre de messagerie

Cliquons sur " Send Test Email "

FIGURE 4.38 – Test de paramètre de messagerie (suite)

Un email de test de Nagios XI est bien reçu sur notre courrier électronique " nesrine.et.naziha@gmail.com " (figure 4.39)

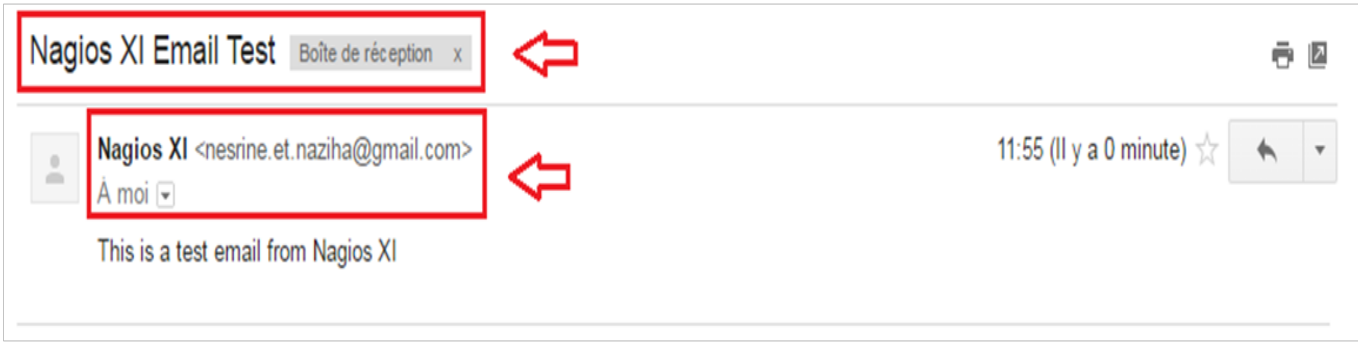

FIGURE 4.39 – recevoir un email par Nagios XI

4.7 Configuration des alertes par Email

Nous avons choisi de recevoir des messages d'alerte par email pour cela nous avons spécifié les types d'alertes à utiliser (Figure 4.40) Cliquons par la suite sur **update settings**

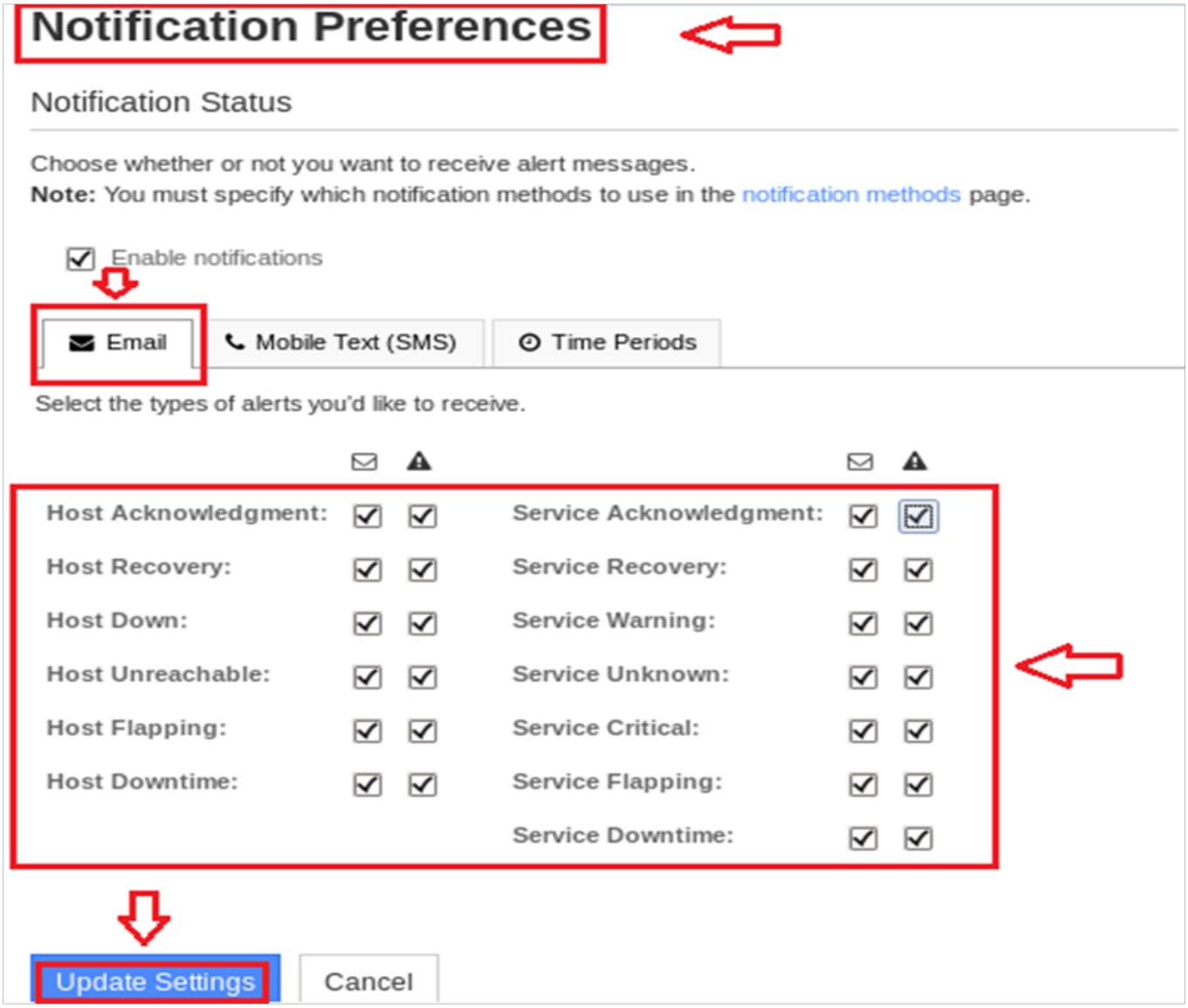

FIGURE 4.40 – Configuration des alertes par Email

4.7.1 Mise à jour de préférence de notification

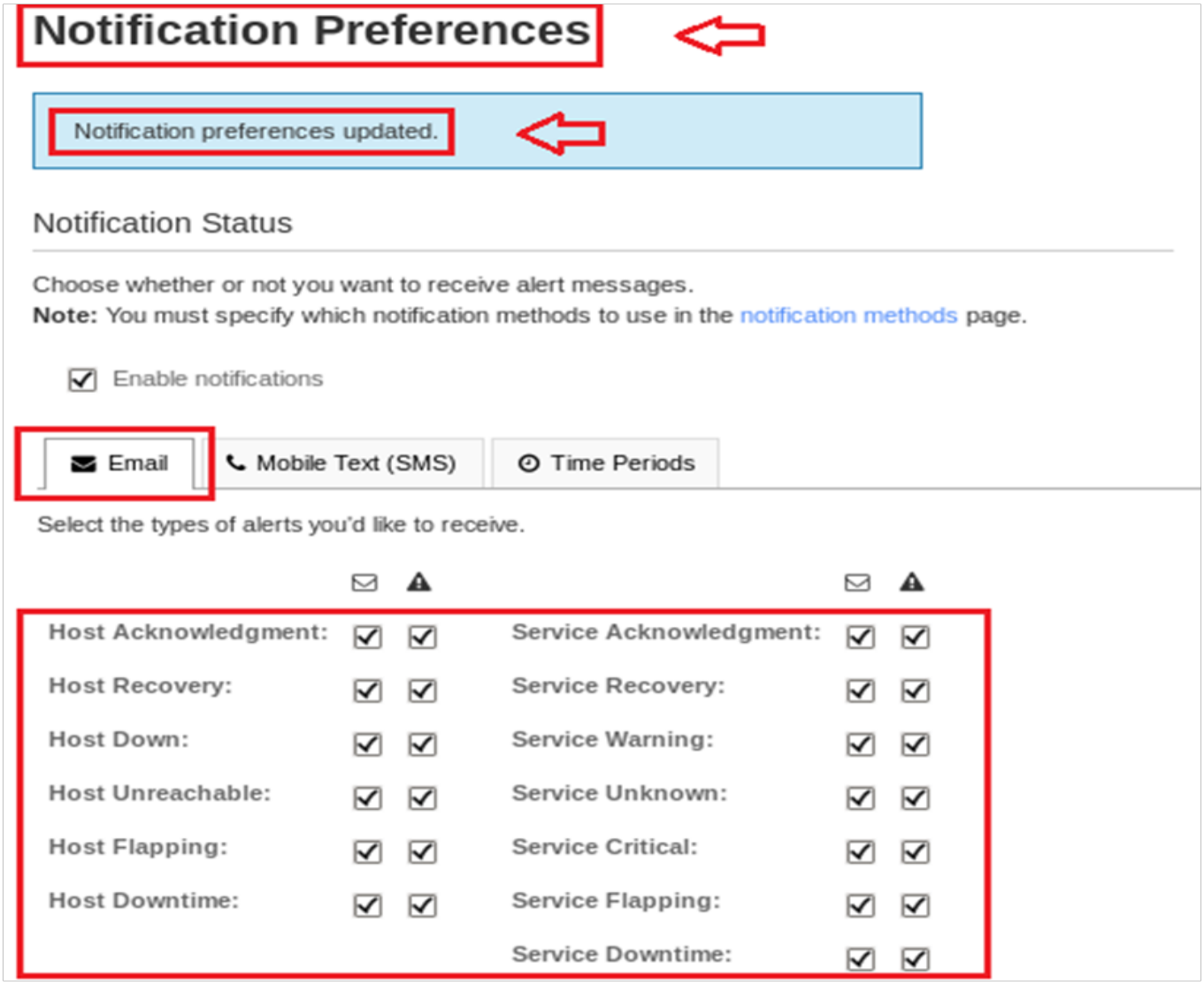

FIGURE 4.41 – Mise à jour de Préférence de notification

Nous avons par la suite configuré la méthode**" email "** afin de recevoir des alertes par message à notre courrier électronique (voir la figure 4.42).

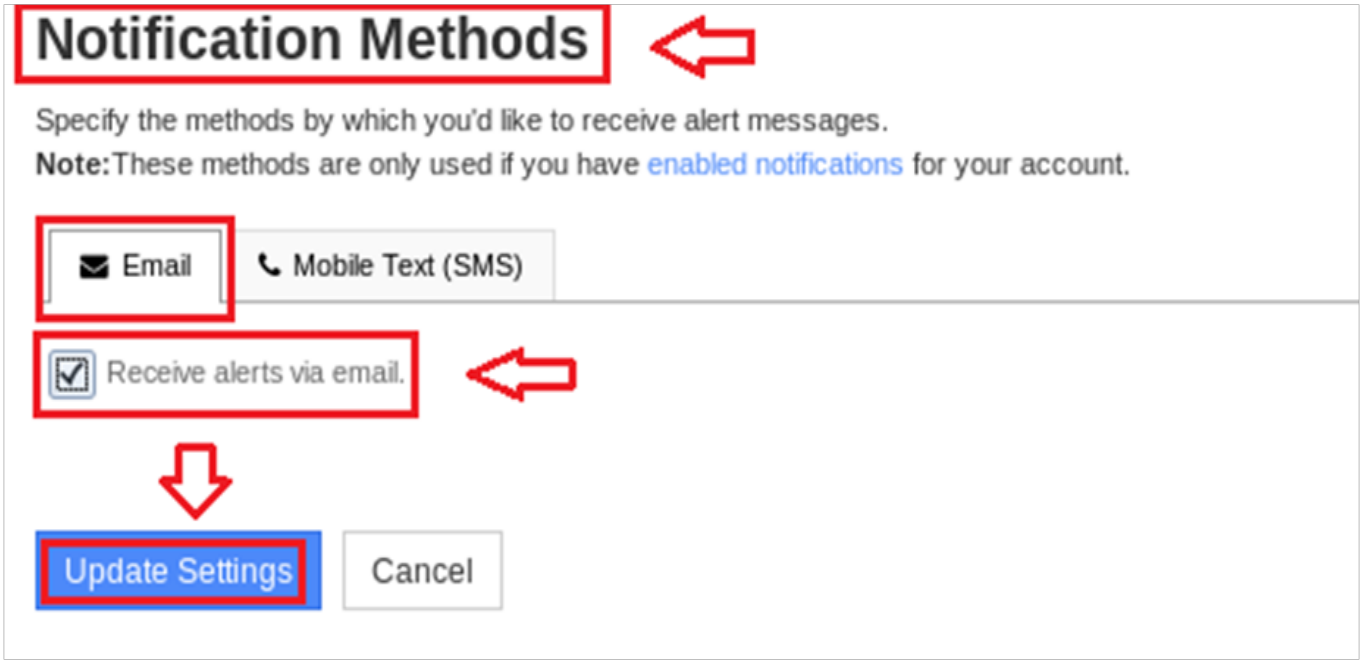

FIGURE 4.42 – Configuration de la méthode à utiliser

Cliquons par la suite sur **" Send Test Notifications "** afin d'envoyer toutes les notifications par email (voir la figure 4.43).

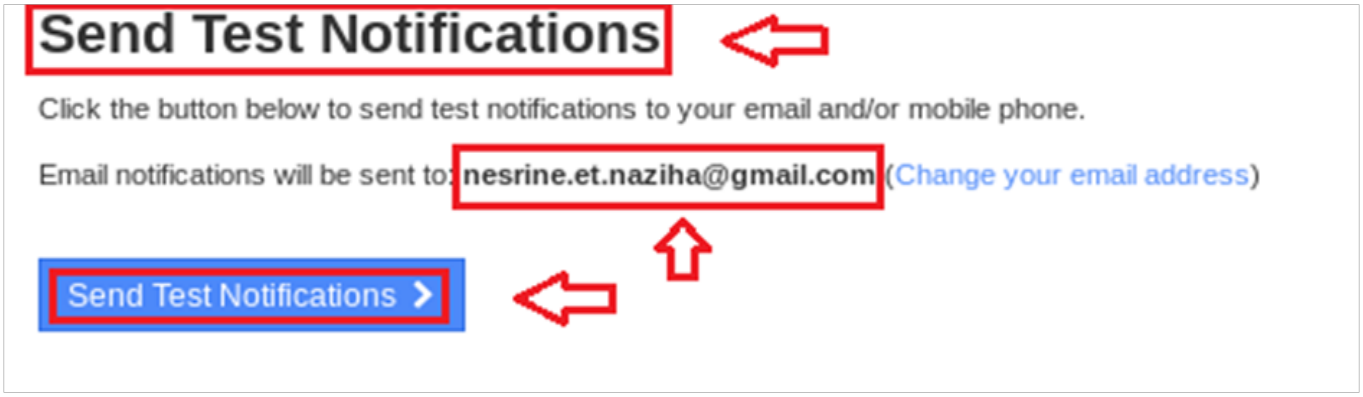

FIGURE 4.43 – Envoi des notifications

Le teste de notifications va être envoyé à l'email "nesrine.et.naziha@gmail.com" Cliquons sur **"Send Test Notification"** afin de l'envoyer (voir la figure 4.44)

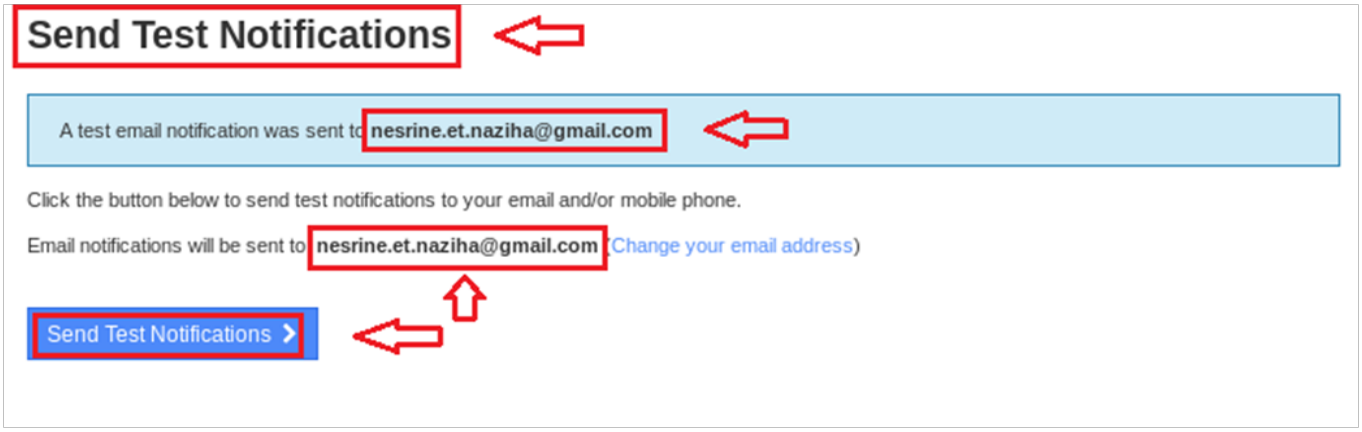

FIGURE 4.44 – Envoi des notifications

Les emails reçu de Nagios XI vers notre adresse électronique (figure 4.45) :

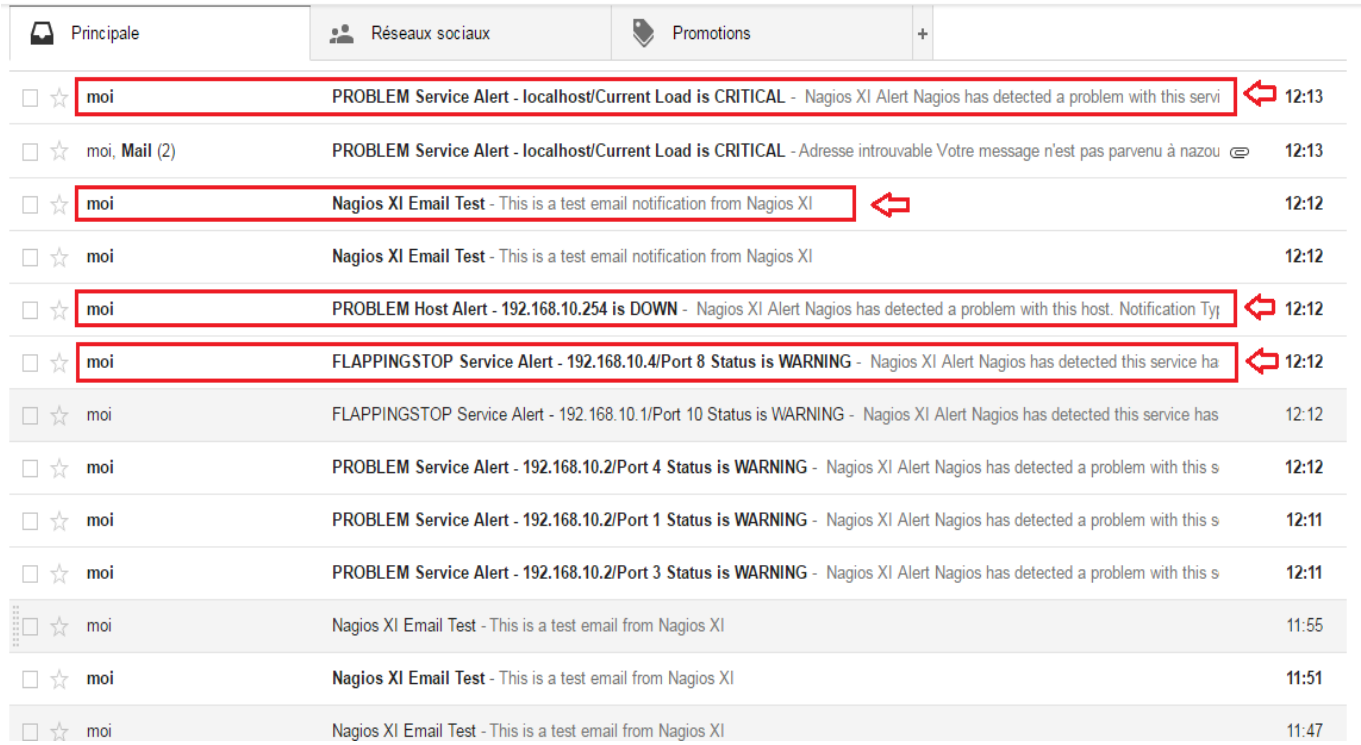

FIGURE 4.45 – Envoi des notifications

4.8 Conclusion

Dans ce chapitre nous nous sommes penchés sur l'aspect pratique de notre projet, en détaillant les étapes de la mise en place et l'utilisation de notre solution, et nous sommes ainsi pu prouver l'apport important de Nagios XI, qui est principalement, la facilité de la configuration,

mais aussi la compatibilité et la maturité étant très utilisés dans le monde professionnel.

Comme moyen de simulation nous avons utilisé le logiciel GNS3 qui regroupe un émulateur Cisco avec des plates-formes de virtualisation.

Conclusion générale et perspectives

Ce projet a été une occasion pour nous de révéler nos capacités. Au vue de l'ensemble du travail demandé, nous nous sommes impliquées de manière sérieuse et rigoureuse, afin que ce projet réussisse sur tous les aspects.

Notre stage pratique nous a permis de récupérer le plus d'informations possible sur l'état du réseau LAN de l'entreprise SONATRACH, de comprendre au mieux le fonctionnement de ce réseau et d'améliorer notre expérience sur le plan pratique.

Ce travail nous a également permis de comprendre les concepts de la supervision dans un système d'information et de mettre en évidence une architecture réseau local, dans le cadre de la supervision.

Le choix de NAGIOS et CentOS 6.9 comme logiciels compatibles et matures étant très utilisés dans le monde professionnel, nous a permis de se mettre en situation réelle en s'imaginant dans ce monde.

Bien que notre réseau local ainsi que sa supervision présente plusieurs fonctionnalités, il reste toujours sujet à des améliorations pour en tirer un maximum d'avantages, d'efficacité, de facilité d'emploi mais surtout l'informatisation de l'administration.

Bibliographie

[1] B.S.HAGGAR. *"Cours M2 Pro STIC-InfoI-NFO-Conception de réseaux de campus"*. 2010.

[2] C.SERVIN. *"Réseaux et Télécoms"*. Dunod, 2003.

[3] C.SERVIN. *"Réseaux et Télécoms"*. Dunod, 2013.

[4] D.SERET D.DROMARD. *"Architecture des Réseaux, Synthèse de cours et excercice corrigés"*. Edition collection Synthex Pearson Education, France, 2009.

[5] D.M.BANTIKO. "notes de cours de réseau informatique". *ISIPA*, (2013) , P.11.

[6] D.M.BANTIKO. *"Les Réseaux"*. Op.cit, 2013 , P.18.

[7] Président Veridion E.LACHAPELLE, CEO Veridion René St-Germain. *"Bonnes pratiques pour la gestion de la sécurité de l'information"*. Edition VERIDION, 2010.

[8] G.RUBINO et L.TOUTAIN. *"Réseaux locaux"*. Ecole Nationale Supérieure des Télécommunications de Bretagne, campus de rennes.

[9] G.PUJOLLE. *"Les Réseaux"*. Edition Eyrolles (6ème Edition), paris, 2008.

[10] G.PUJOLLE. *"Les Réseaux"*. Edition Eyrolles (3éme Edition mise à jour), Paris, 2016 , P.23.

[11] http ://cristian.caleca.free.fr/snmp/.

[12] J.DORDOIGNE. *"Réseaux Informatiques"*. Edition ENI (5ème Edition), janvier 2013.

[13] J.DORDOIGNE. *"Réseaux Informatiques", Notion fondamentales*. Edition Eni (6ème Edition), mars 2015.

[14] J.F.PILLOU. "tout sur les réseaux et internet". *Dunod*, (2015).

[15] M.HALIM KHALAFA. *"Introduction à la Sécurité Informatique"*. laboratoire des logiciels de base session, 2012.

[16] L.BERGER. *"La virtualisation des Systèmes d'Information"*. Mémoire de Bachelor, Haut Ecole de Gestion de Genève (HEG), 28 septembre 2012.

[17] L.BLAS. *"L'audit d'un système d'information au sien d'une petit structure"*. Université Charles de Gaule, lille 3, 2009.

[18] M.E.GANDE. *"Efficacité de l'audit interne dans une institution de sécurité sociale"*. Université polytechnique internationale du Bénin (UPIB), 2010.

[19] O.SALVATORI. *"Initiation aux Réseaux, Cours et Exercices"*. Edition AYROLLES, 2010.

[20] P.BERTRAND. *"Architecture des Réseaux"*. Edition Marketing S.A. (4ème Edition revue et augmentée), paris, 2013.

[21] R.BADDONNEL. "supervision des réseaux et services adhoc", option réseaux et télecommunication, université henri poicaré-nancy, (2006).

[22] S.GAUME. *"Citrix XenAPP 7.5-concepts et mise en oeuvre de la virtualisation d'application"*. Edition ENI, 2014.

[23] T.ANDREW. "les réseaux". *5ème Edition*, (2013), P.1.

[24] www.blog.wikimemoires.com/audit-définitions-types-de-audit controle/.

[25] www.centos.org.

[26] www.createurdeconvergence.com/glossaire-telecom-reseaux /spanning tree.

[27] www.GNS3.net.

[28] www.monitoring fr.org/solutions/nagios/.

[29] www.vmware.com/support/pubs.

Chapitre A

Installation et configuration de GNS3

A.1 Installation de GNS3

Etape 1 : Téléchargement du produit

1. Dans le site officiel de GNS3 : www.gns3.com, puis nous allons cliquer sur le bouton DOWNLOAD (Figure 4.1).

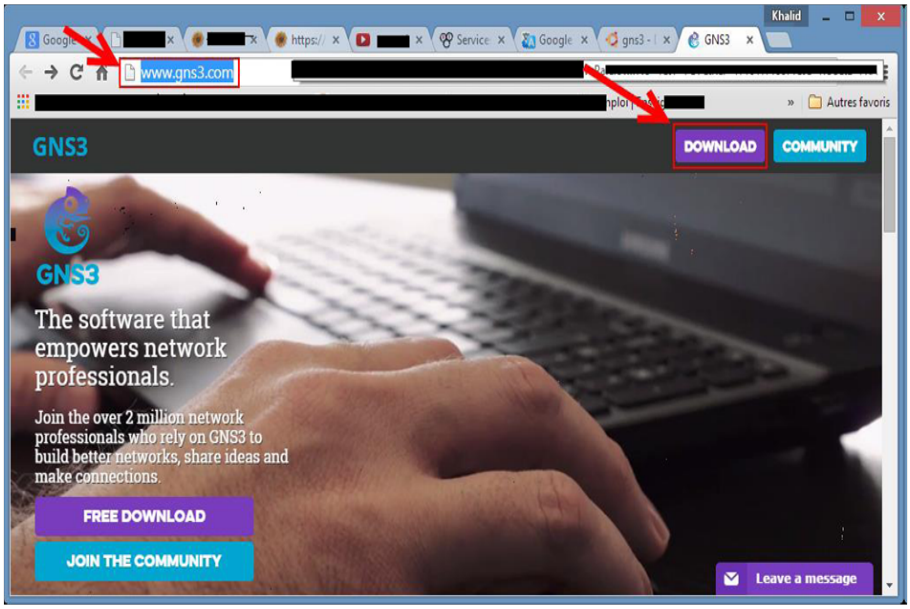

FIGURE A.1 – Le site officiel de GNS3

2. Nous allons créer un compte sur le site en fournissant les éléments d'identification.
3. Cliquons ensuite sur le lien approprié pour télécharger l'installable de GNS3.

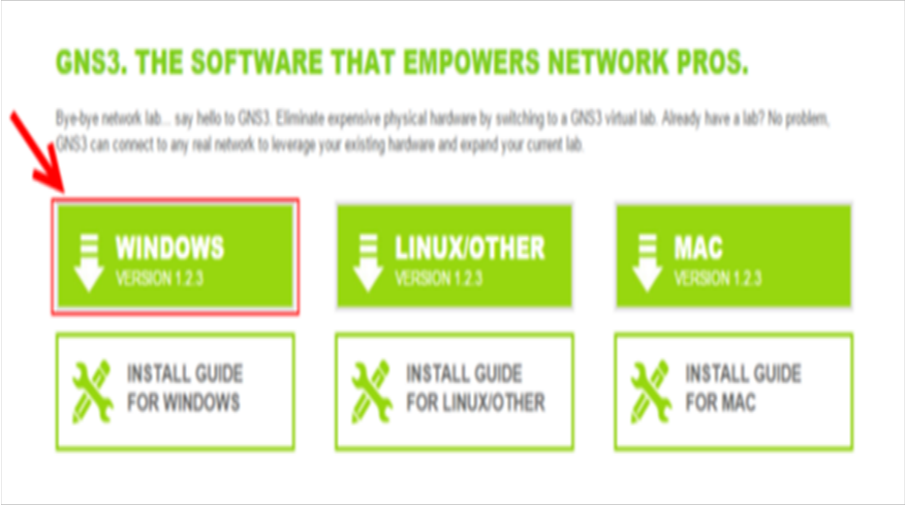

FIGURE A.2 – Choisir Windows comme système d'exploitation

Etape 2 : Installation de GNS3

En lançant le fichier d'installation, nous allons pouvoir suivre facilement les fenêtres ci-après :

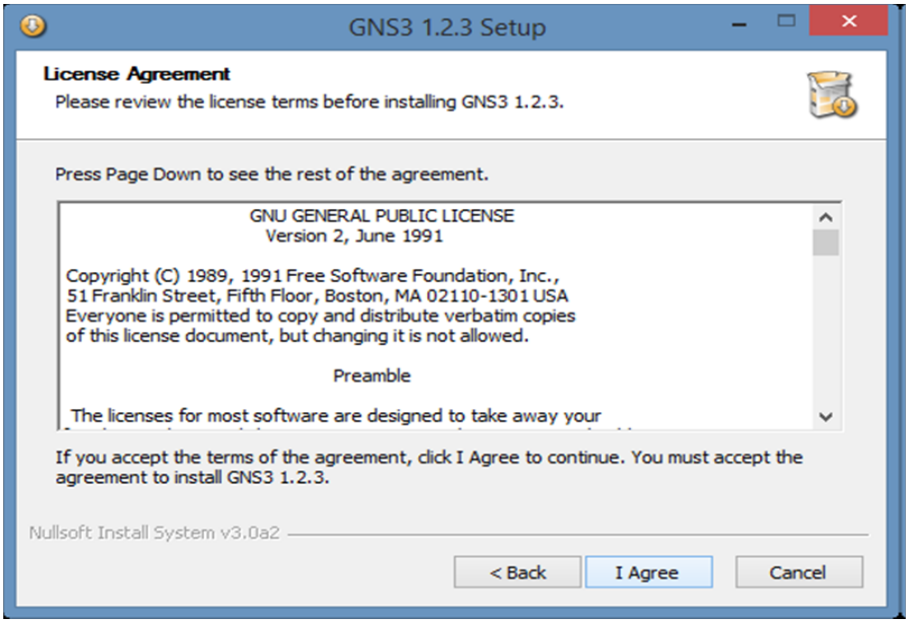

FIGURE A.3 – Acceptation de l'agrément pour l'installation de GNS3

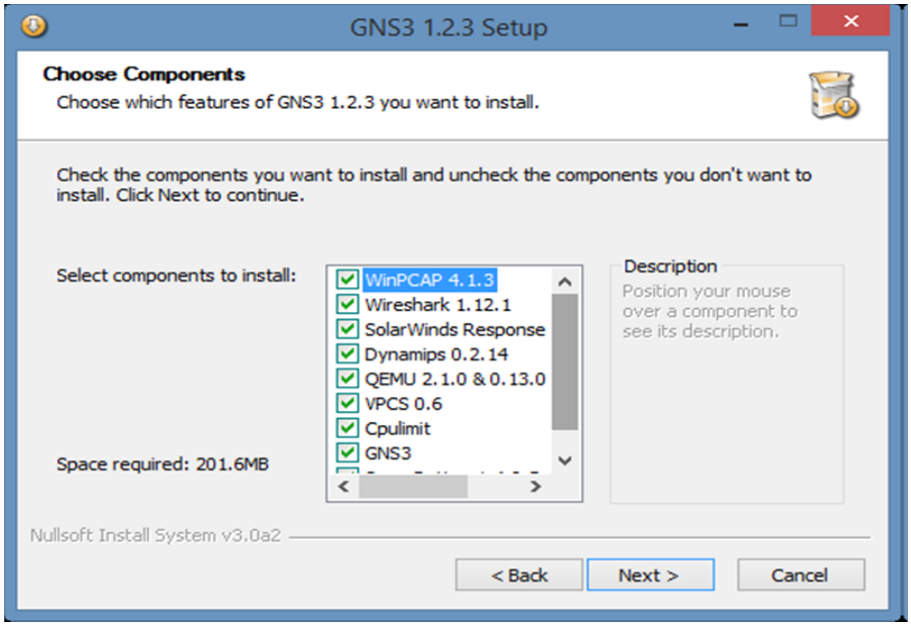

FIGURE A.4 – La liste des logiciels à coucher pour lancer leur téléchargement afin que GNS3 puisse s'installer

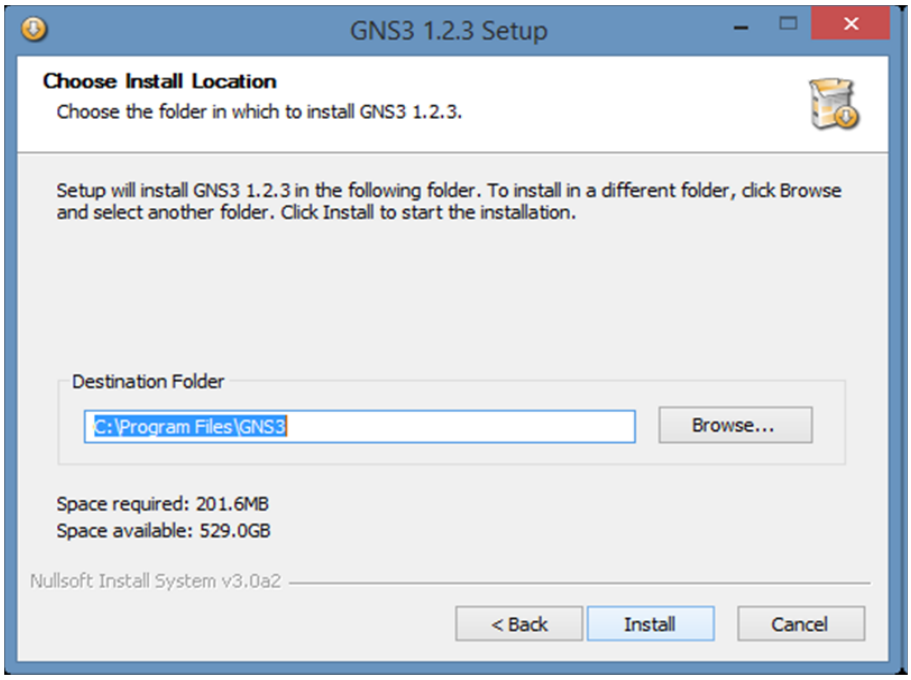

FIGURE A.5 – Indiquer l'emplacement de fichier GNS3

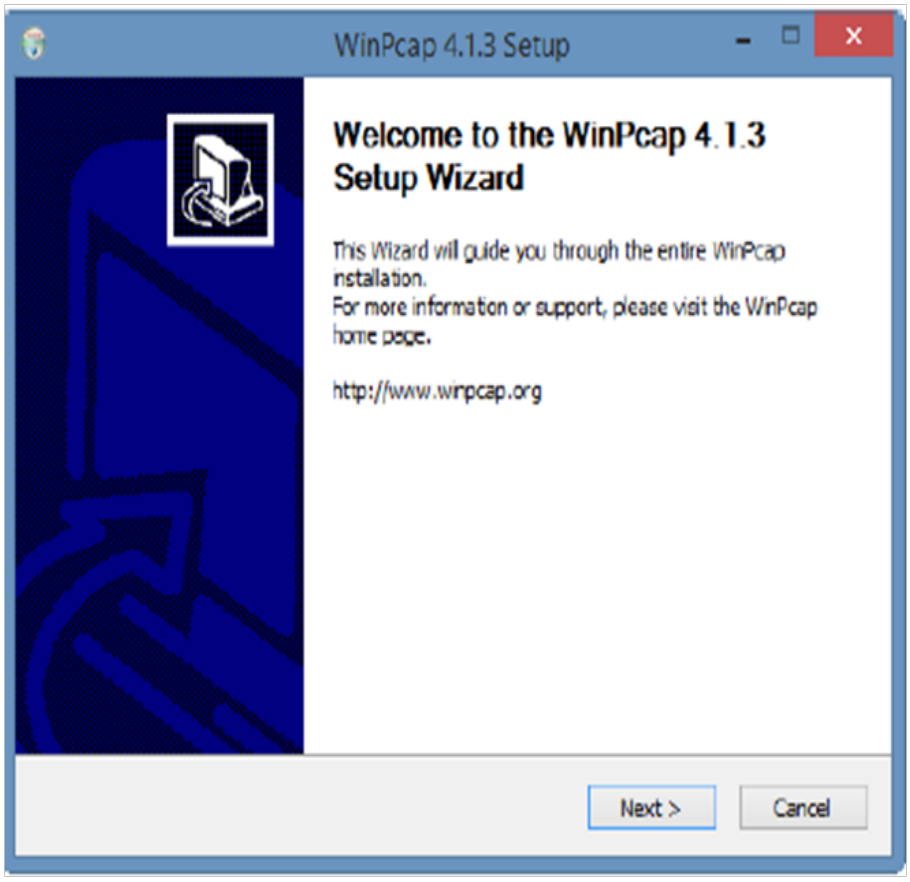

FIGURE A.6 – Lancement de fichier d'installation

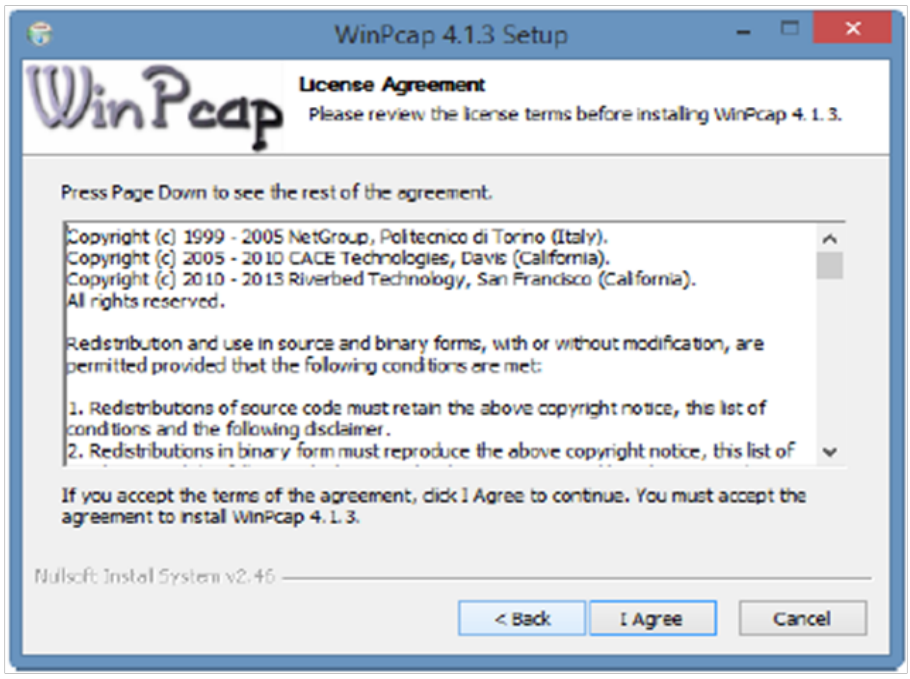

FIGURE A.7 – Lancement de WinPcap 4.1.3

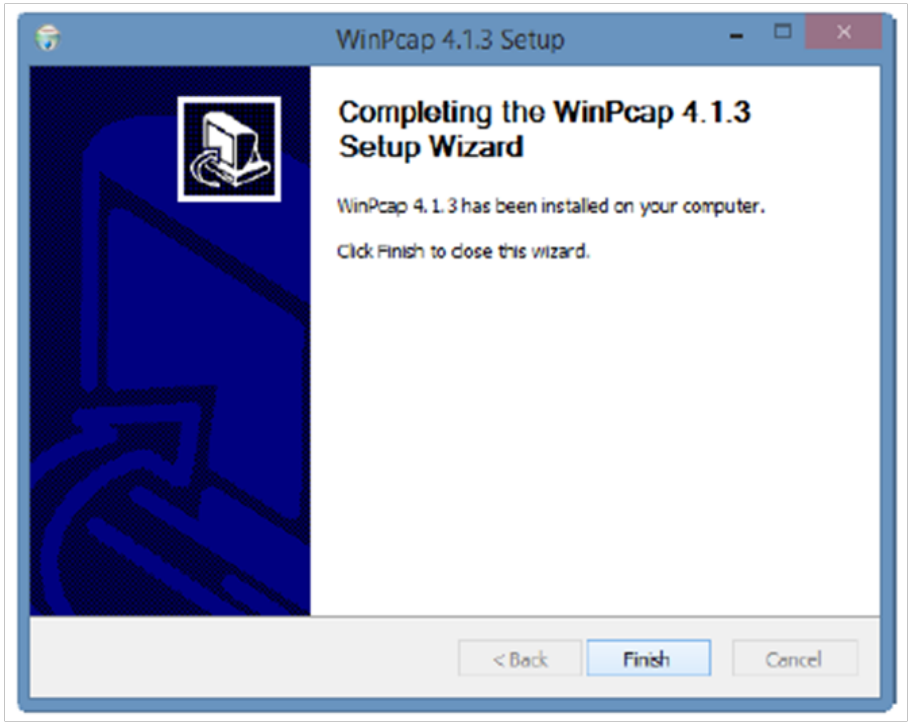

FIGURE A.8 – Finaliser l'installation de WinPcap 4.1.3

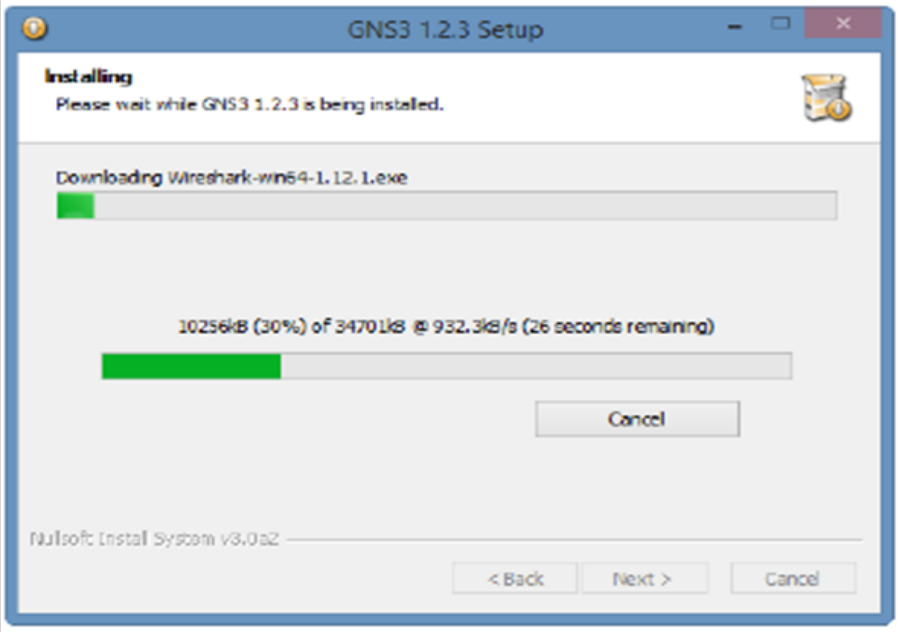

FIGURE A.9 – Téléchargement de Wireshark-win64 1.12.1

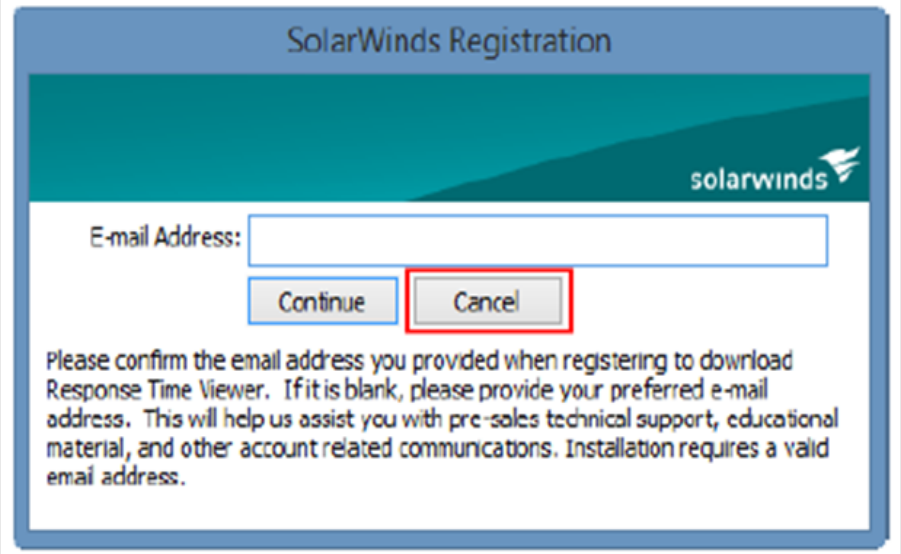

FIGURE A.10 – Confirmation de l'email

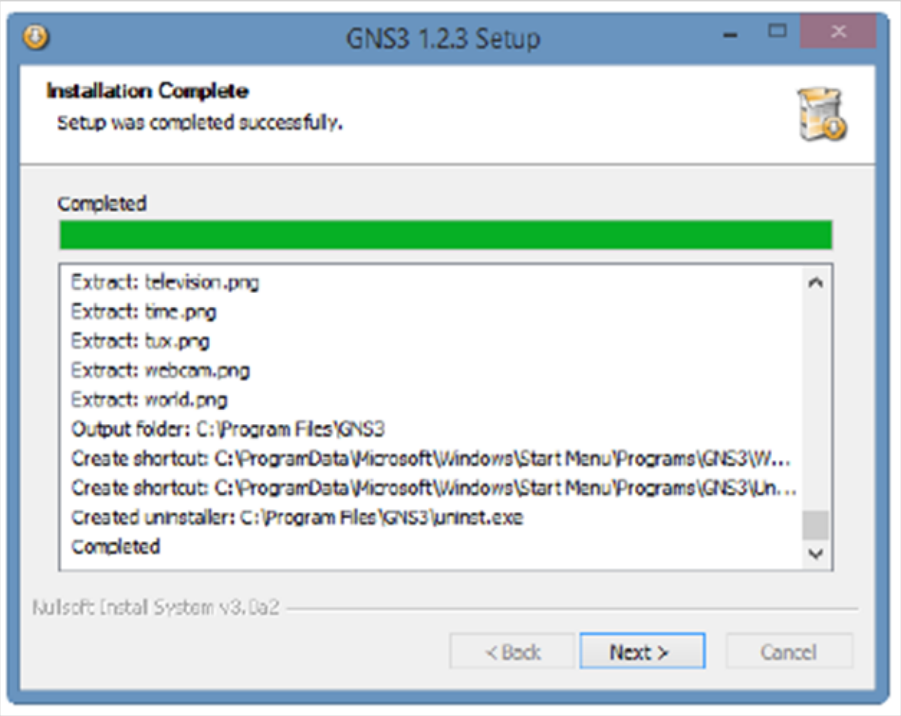

FIGURE A.11 – Installation complète de GNS3 1.2.3

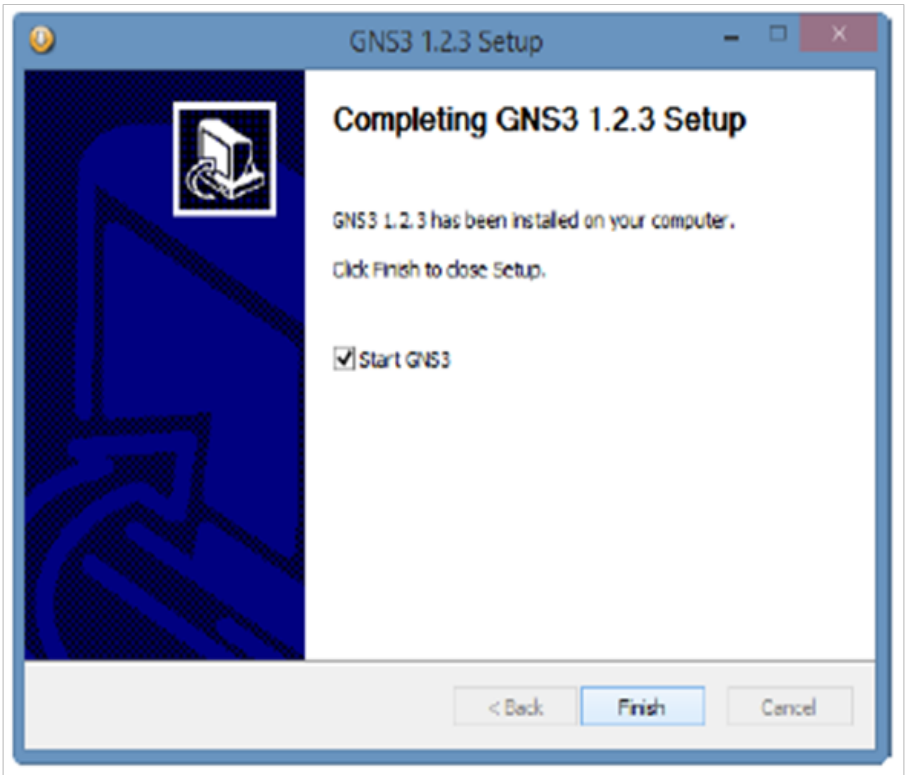

FIGURE A.12 – Finaliser l'installation de GNS3 1.2.3

Maintenant que notre installation est terminée, nous pouvons enfin exploiter l'interface Graphique GNS3 en créant un nouveau projet :

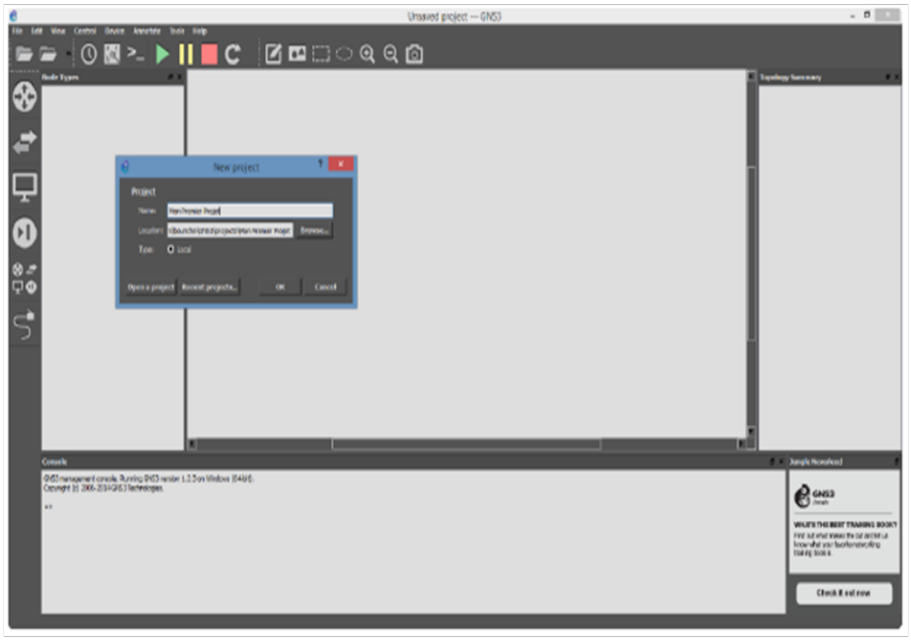

FIGURE A.13 – Création d'un nouveau projet sur l'interface graphique de GNS3

A.2 Déploiement d'un routeur CISCO dans GNS3

Lorsque GNS3 s'ouvre pour la première fois, il faut lui indiquer pour chaque équipement d'interconnexion, le fichier qu'il doit implémenter pour qu'il l'émule comme s'il s'agit d'un vrai équipement (Routeur, Switch, etc.). Par exemple si nous voulons déployer un routeur c7200 de CISCO, on doit donc télécharger le fichier correspondant en cherchant sur le Net : router 7200 ios image free download for gns3.

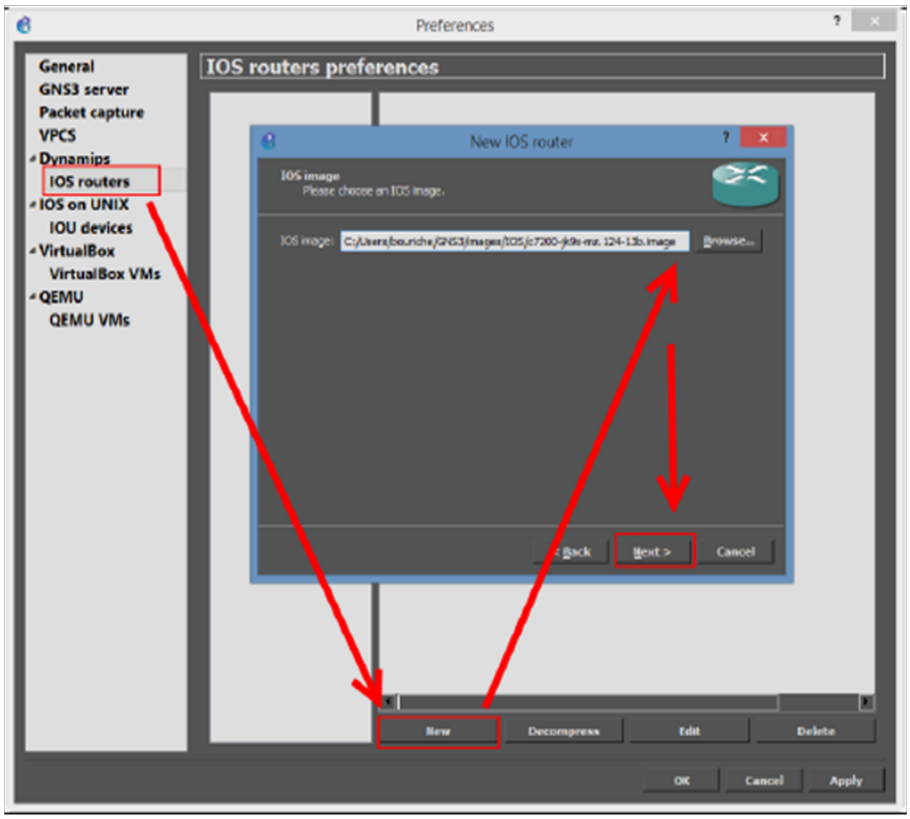

FIGURE A.14 – Déploiement d'un routeur c7200 de CISCO dans GNS3

Cliquons par la suite sur Next

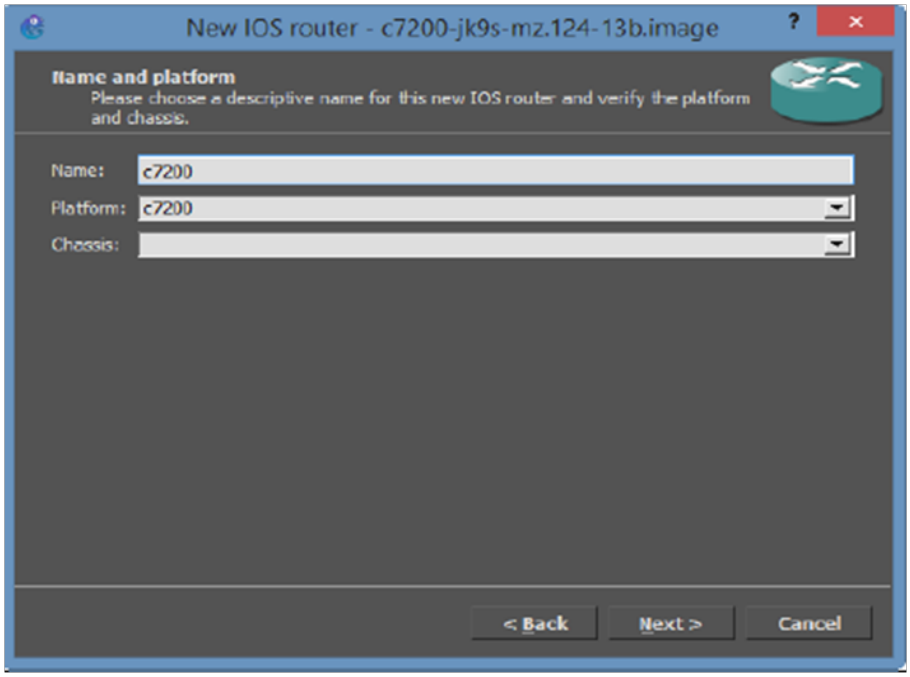

FIGURE A.15 – Attribution d'un nom ainsi qu'une plateforme au routeur c7200 de CISCO

Cliquons sur Next.

Fournissons la taille mémoire appropriée si notre routeur va être utilisé pour faire beaucoup de traitement, Sinon on laisse la valeur par défaut :

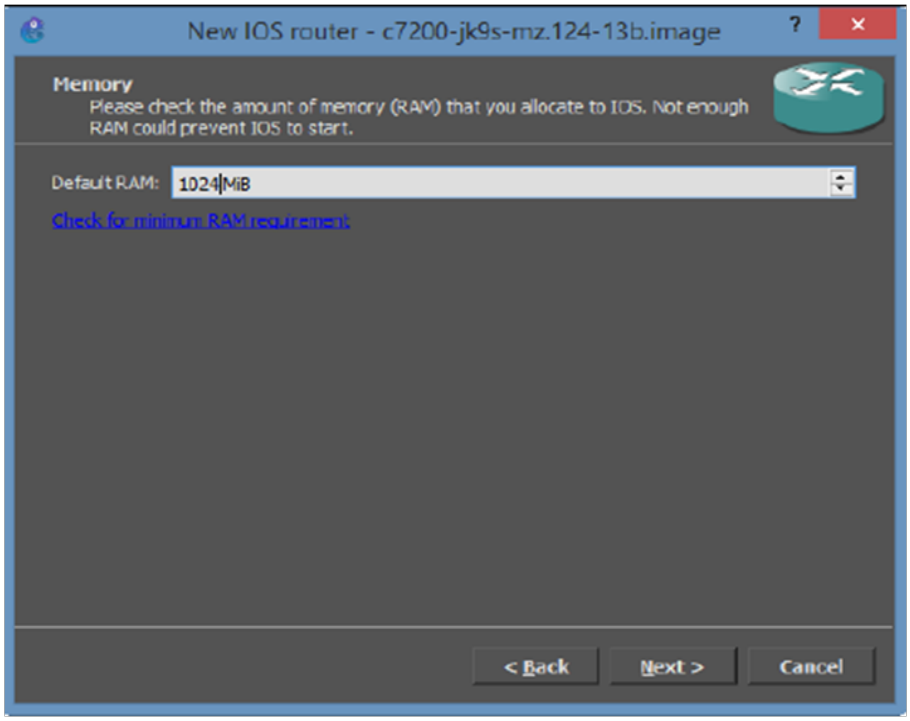

FIGURE A.16 – Attribution d'une taille mémoire appropriée au routeur 7200 de Cisco

Cliquons en suite sur Next.

Choisissons les cartes réseau qui vont être insérées par défaut pour chaque nouvelle instance de ce routeur :

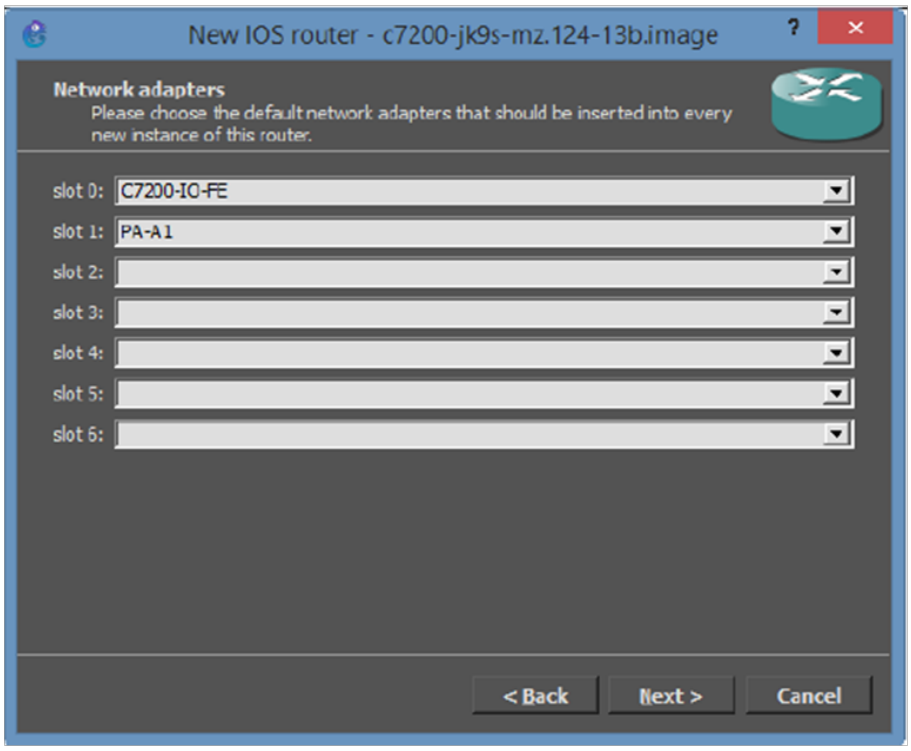

FIGURE A.17 – Choisir les cartes réseaux au routeur c7200 de CISCO dans GNS3

Cliquons en suite sur Next.

Si nous voulons que notre routeur travaille d'une puissance optimale pour le processeur ou l'un de ses coeurs, une valeur Idle-PC doit être ajoutée (cette étape n'est pas obligatoire pour le moment).

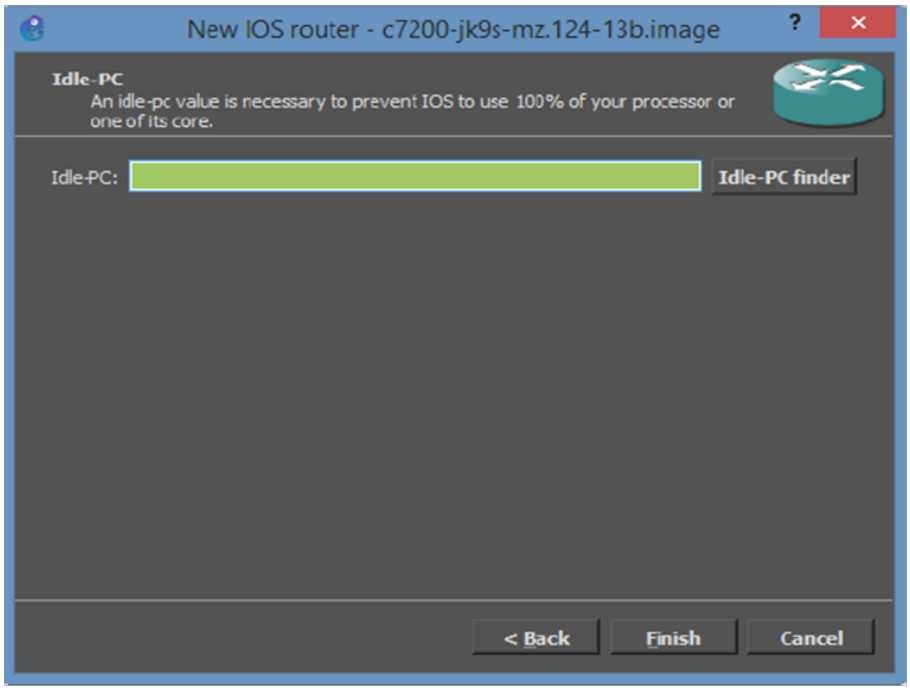

FIGURE A.18 – Ajout d'une valeur Idle-PC au routeur c7200 de CISCO si le routeur travaille d'une puissance optimale pour le processeur ou l'un de ses coeurs.

Notre routeur figure dans la liste des IOS disponibles.

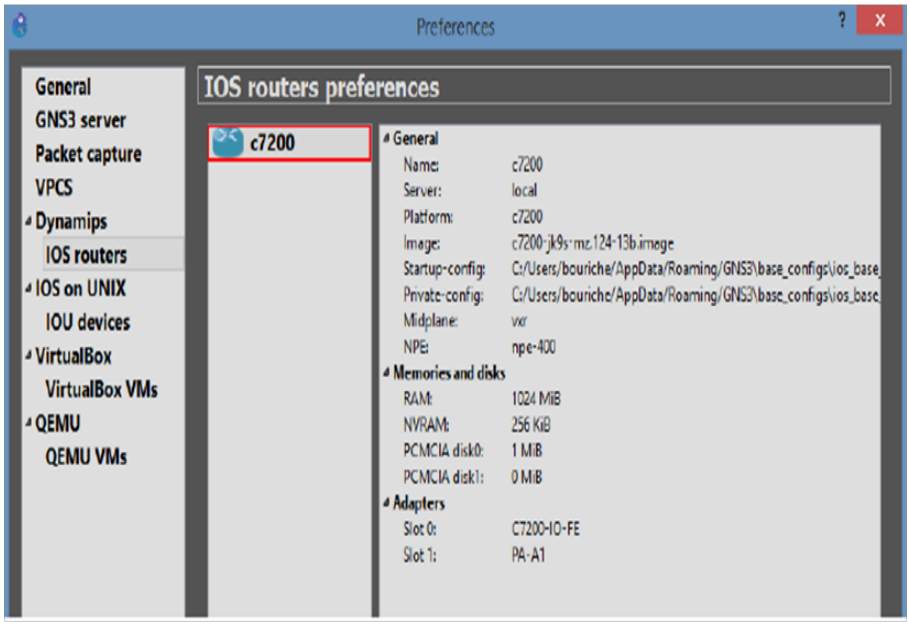

FIGURE A.19 – L'image de routeur est enfin mise en place dans l'interface de GNS3.

Chapitre B

Installation et configuration de CentOS 6.9

B.1 Installation de CentOS 6.9

Etape 1 : Téléchargement du produit

1. Téléchargement de l'image ISO de CentOS 6.9.
2. Une fois l'image ISO est téléchargé on lance l'installation de CentOS 6.9 sous notre machine virtuelle VMware.
3. **Les étapes d'installation de CentOS 6.9**
   Pour commencer l'installation de CentOS 6.9, il suffit de mettre en surbrillance "***Installer ou mettre à niveau un système existant***" et appuyer sur Entrée. L'installation commencera maintenant.

FIGURE B.1 – Installation de CentOS 6.9

Sur cet écran, nous devons sélectionner la langue qui doit être utilisée tout au long de l'installation.

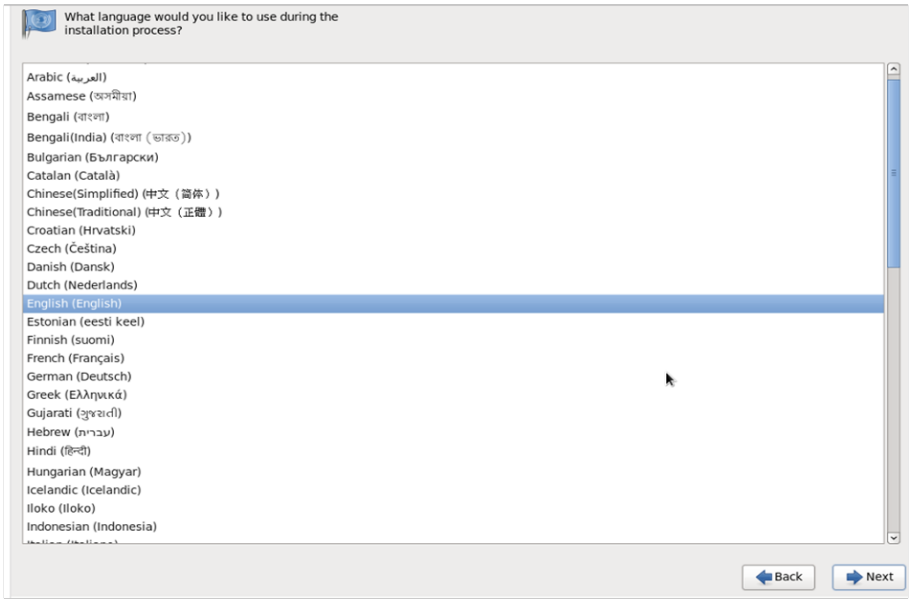

FIGURE B.2 – Le choix de la langue à utiliser

Sélection des périphériques de stockage, nous avons choisi "Dispositifs de stockage de base"

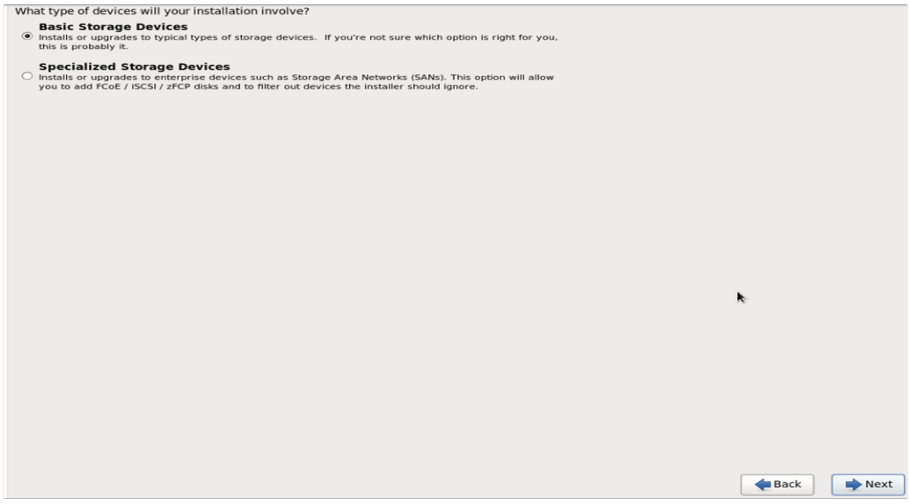

FIGURE B.3 – Le choix de l'espace à utiliser

Avertissement du périphérique de stockage, nous allons sélectionner oui.

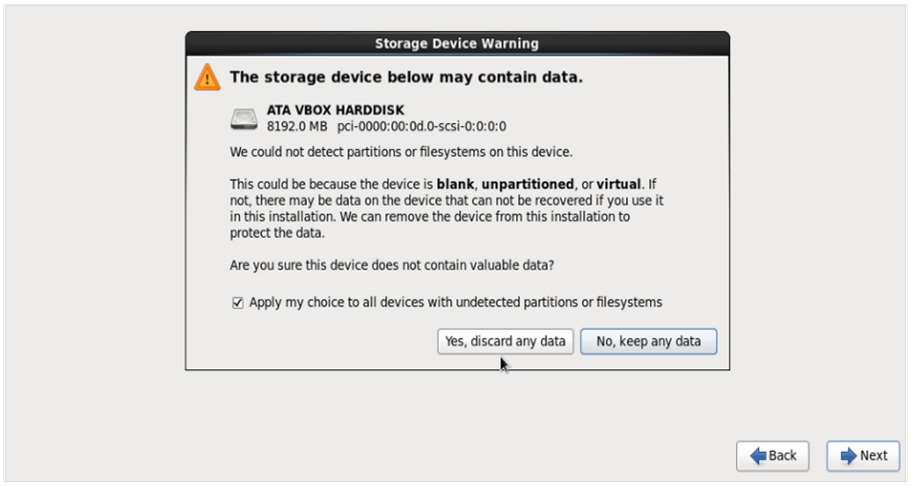

FIGURE B.4 – Avertissement du périphérique de stockage.

Sur cet écran, nous devons fournir un nom d'hôte de nom unique à utiliser par notre nouveau système.

FIGURE B.5 – Attribuer un nom pour notre système.

Sur cet écran, nous devons choisir notre emplacement géographique à partir du menu déroulant ou de la carte.

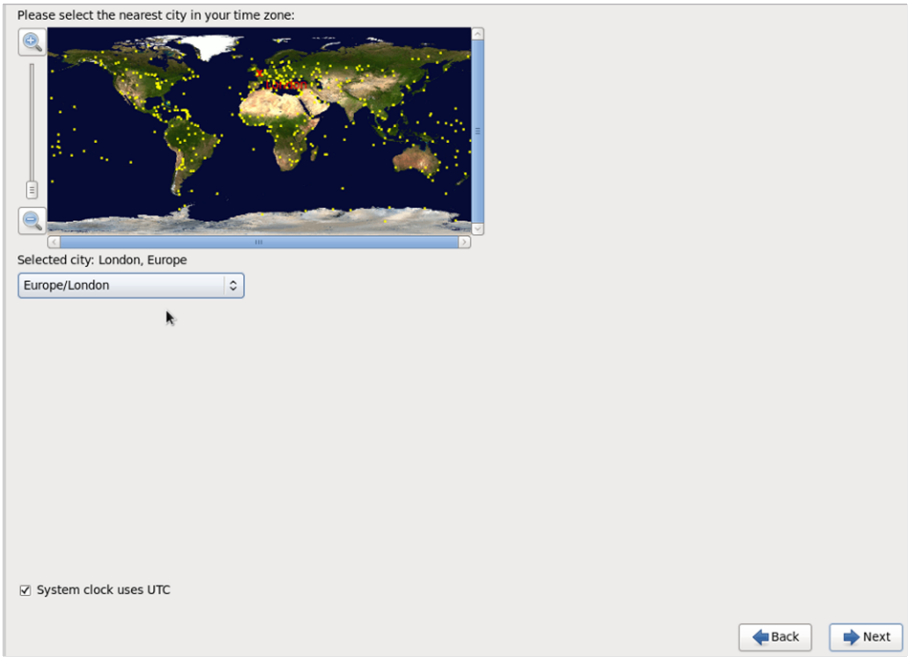

FIGURE B.6 – Choisir l'emplacement géographique

Sur cet écran, nous devons fournir un mot de passe "root" à utiliser sur notre système.

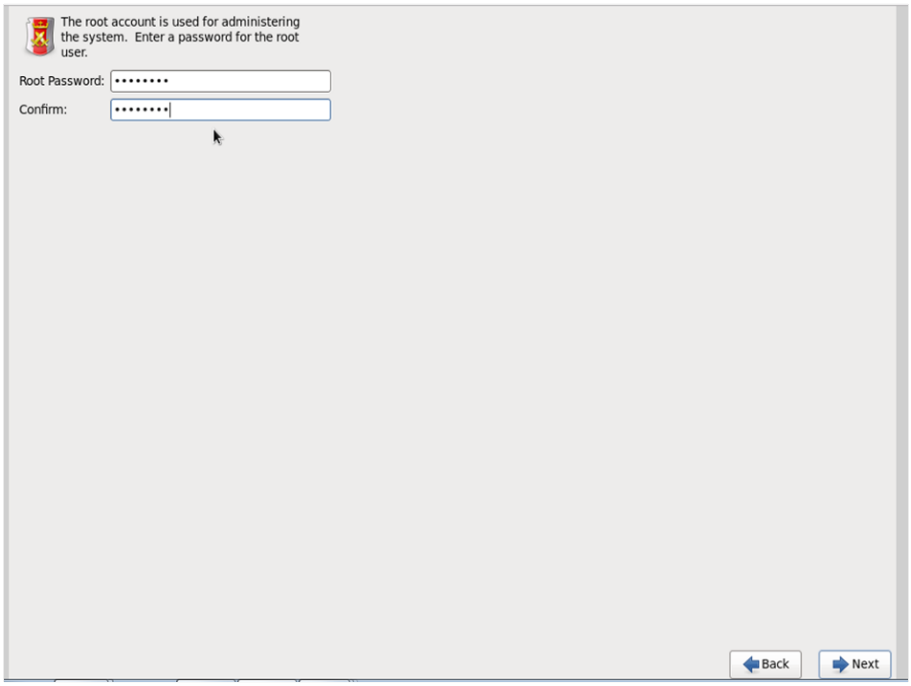

FIGURE B.7 – Saisir le mot de passe à utiliser

Sur cet écran, plusieurs options sont disponibles pour sélectionner. Dans l'exemple, nous avons choisi l'option "Utiliser tout l'espace". Nous avons également la possibilité de "chiffrer le système".

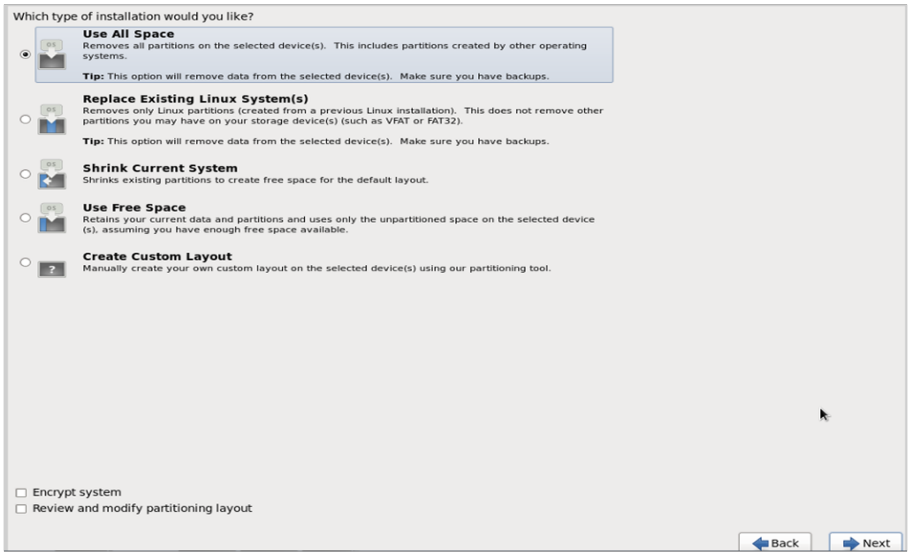

FIGURE B.8 – Choisir le type d'installation

Dans le menu pop, nous devons choisir "Enregistrer les modifications sur le disque" pour permettre à l'installation de continuer.

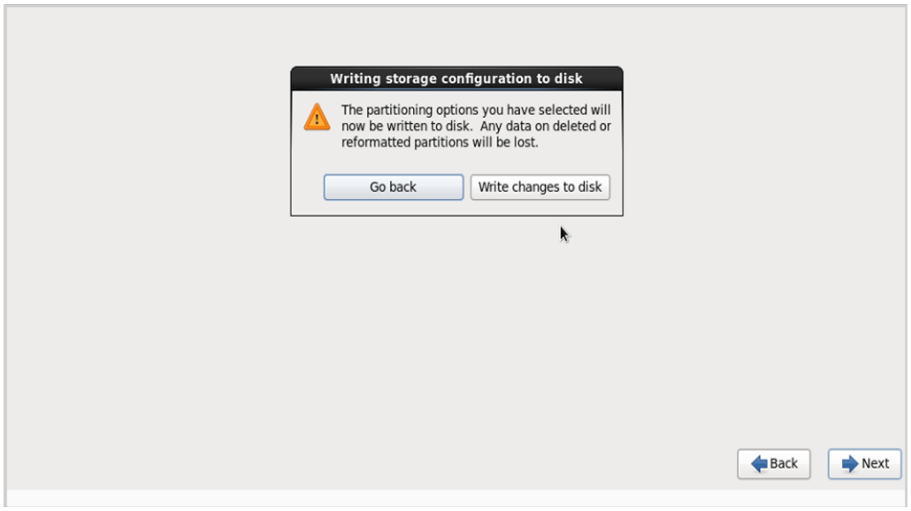

FIGURE B.9 – Enregistrement des modifications sur le disque

La progression de l'installation est affichée par une barre de progression.

FIGURE B.10 – Lancement d'installation de centOS 6.9

Notre installation de CentOS est maintenant terminée. Avant de pouvoir utiliser notre système, un nouveau démarrage est requis. Cliquez sur l'icône "Réinitialiser" dans le coin inférieur droit.

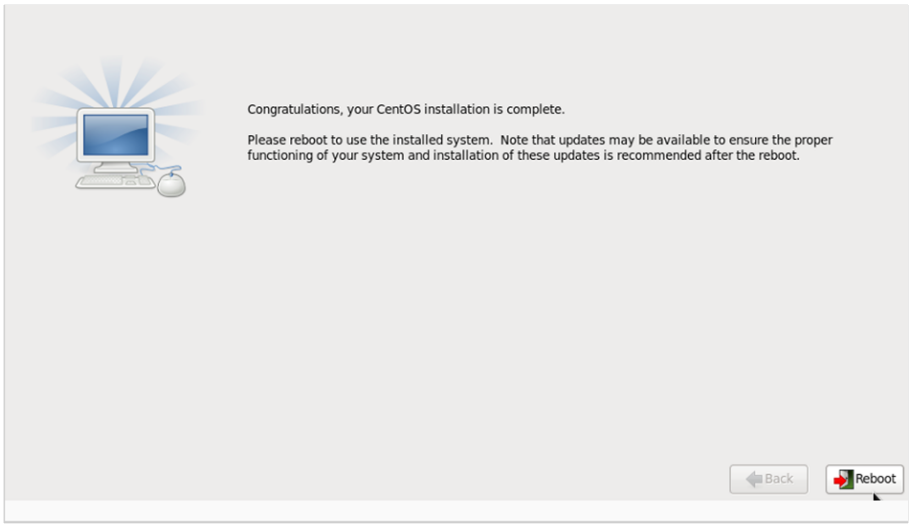

FIGURE B.11 – Réinitialiser le système

Maintenant que notre installation est terminée, nous pouvons enfin exploiter l'interface CentOS 6.9.

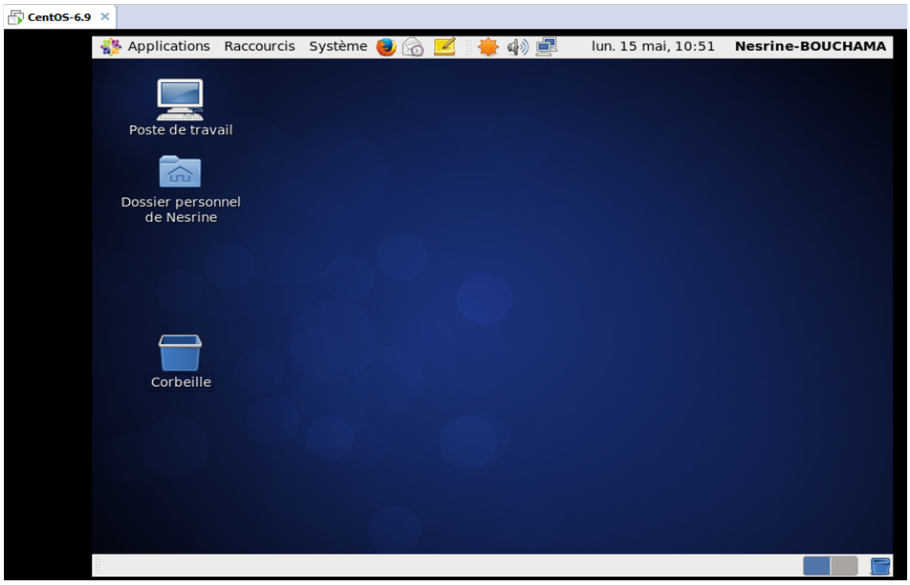

FIGURE B.12 – l'interface de CentOS 6.9.

Chapitre C

Suite d'installation et configuration de Nagios XI

Nous allons accéder à l'interface Web Nagios XI dans notre navigateur à l'aide de l'URL http : // **ip- address/nagiosxi**. Dans l'installateur Nagios XI, nous pouvons configurer notre nom, adresse e-mail, mot de passe. Une fois que toutes nos modifications ont été apportées, on clique sur "***Installer***".

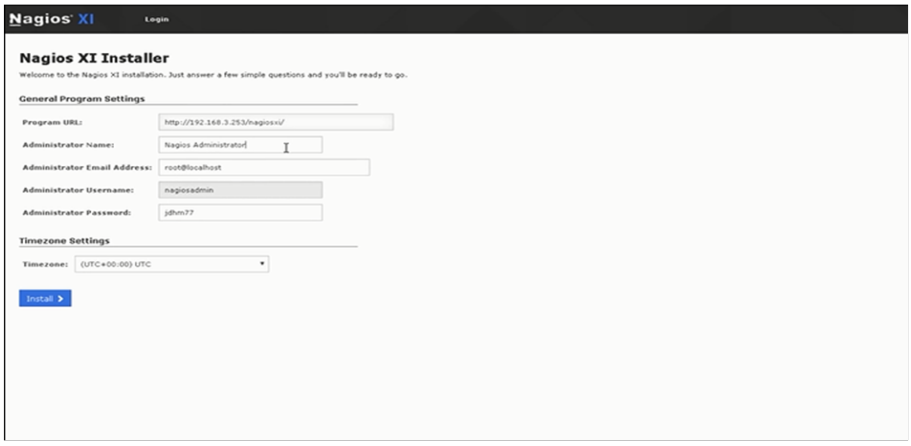

FIGURE C.1 – Configuration de nom, adresse e-mail

Nous avons installé Nagios XI avec succès, selon les configurations que nous avons faites sur l'écran précédent. Il est important qu'on connaisse notre nom d'utilisateur et notre mot de passe.

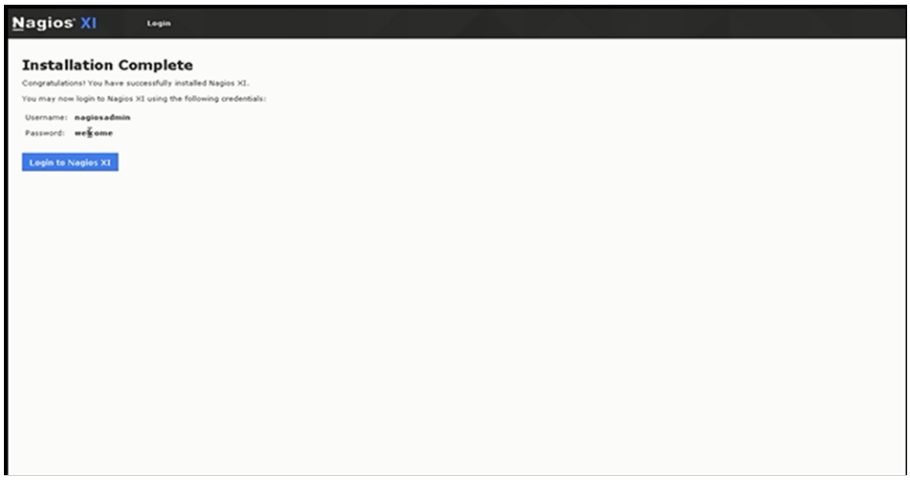

FIGURE C.2 – Installation complète de Nagios XI.

Nous allons insérer nos identifiants de connexion de la page précédente dans la boîte de connexion.

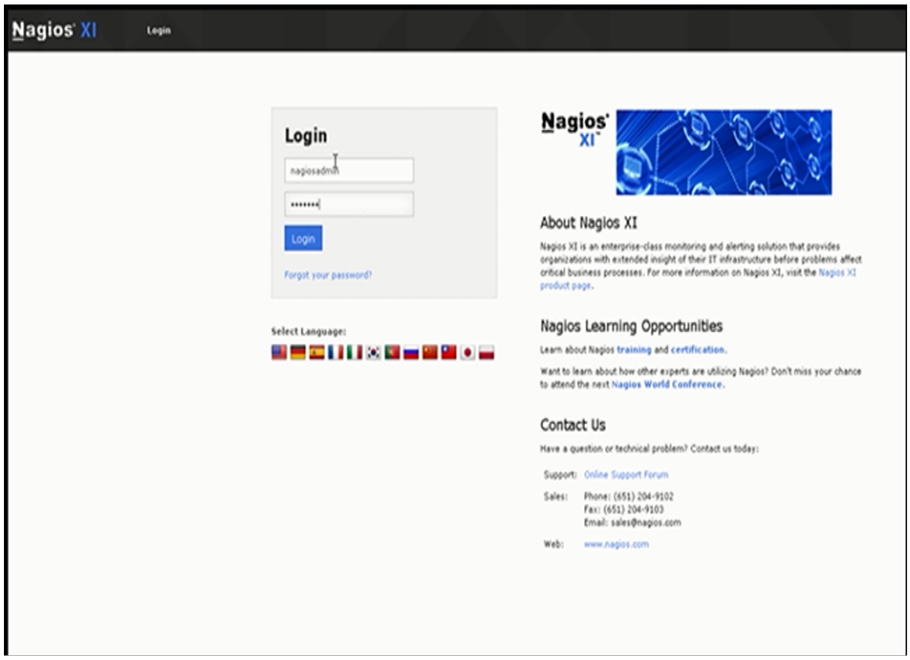

FIGURE C.3 – insérer les informations de connexion

Nous allons obtenir l'interface finale de Nagios XI :

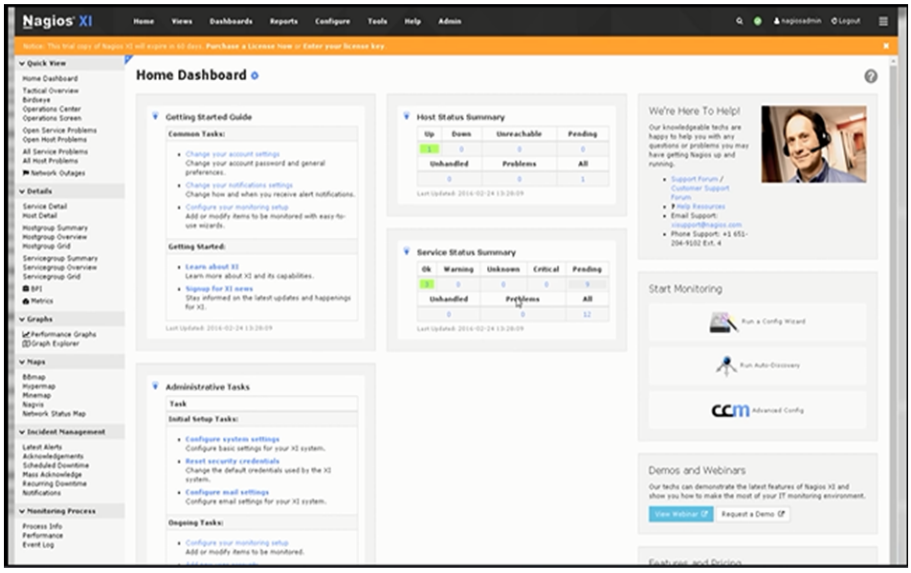

FIGURE C.4 – L'interface finale de Nagios XI.

RÉSUMÉ

Le but de ce projet a été de mettre en oeuvre une solution **open source** pour **superviser** des **switchs** et des **routeurs** et qui sont de la marque **CISCO** ainsi que l'utilisation de logiciel **GNS3** pour la simulation de notre **réseau LAN**. Notre choix a été fixé sur **Nagios** plus précisément **Nagios XI** qui est considéré comme la solution la plus aboutie dans le monde des développeurs.

Donc comme résumé du travail, pour la première phase nous avons installé le fameux logiciel **CentOS 6.9** sur une **machine virtuelle VMware Workstation 12** sur laquelle est installé **Nagios XI** vu que ce dernier fonctionne uniquement sur une machine possédant un système d'exploitation **Linux**.

Pour pouvoir superviser notre architecture **LAN** nous l'avons simulée sous **GNS3** par la suite intégrée sous **Nagios XI** et à travers l'interface de ce dernier nous avons configuré le **SMTP** afin de recevoir des emails à notre courrier électronique.

Mots clés : CentOS, Nagios XI, DHCP, DNS,LAN, GNS3, VMware Workstation 12.

ABSTRACT

The goal of this project was to implement a **open source supervise** solution of **switches** and **routers** and that are of the **CISCO** Than the use of software **GNS3** for the simulation of our **LAN** network. Our choice has been fixed on **Nagios** more precisely **Nagios XI** which is considered the most successful solution in the world of developers.

So as a summary of the work, for the first phase we installed the famous software **CentOS 6.9** on a **virtual machine VMware Workstation 12** on which is installed **Nagios XI** A machine with an operating system **Linux**.

In order to be able to supervise our architecture **LAN** which was simulated under **GNS3** we integrated it under **Nagios XI** and through the interface of it we configured the **SMTP** In order to receive emails to our e-mail.

keys words : CentOS, Nagios XI, DHCP, DNS, LAN, GNS3, VMware Workstation 12.