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

UNIVERSITE Dr. TAHAR MOULAY SAIDA
FACULTE DE TECHNOLOGIE
DEPARTEMENT D'INFORMATIQUE

MEMOIRE DE FIN D'ETUDES
EN VUE DE L'OBTENTION
DU DIPLOME DE MASTER
EN INFORMATIQUE.

OPTION : Réseaux Informatiques et systèmes réparties

Thème

Conception & réalisation d'un outil d'administration réseau

Présentée par :

HADROUG MOKHTARIA

BOUMEDIENNE CHAHRAZED

Sous la direction de :

Dr *A.* Khobzaoui

Promotion :juin 2017/2018

Remerciements

Nous remercions tout d'abord Dieu, le tous puissant de nous avoir accordé santé, courage et foie.

Ensuite, Nous tenons à exprimer, à notre encadreur Mr A. KHOBZAOUI, nos sincères remerciements pour son soutien moral, ses précieux conseils et ses encouragements.

Nous remercions vivement, également, tous nos enseignants qui nous on accompagnés tout au long de notre cursus.

Dédicaces

Je remercie Dieu tout puissant de m'avoir donnée la santé et le courage pour terminer ce modeste travail.
Je dédie mon travail :
A mon père pour son amour, sa patience, ses conseils et ses considérables sacrifices tout au long de ma vie. A ma mère pour son grand amour, ses sacrifices et toute l'affection qu'elle m'a toujours offerte.
A mon frère Imad Eddine et à mes soeurs.
A ma tante Meriem et à toute sa famille.
A mon binôme Mokhtaria et sa famille.
A tous mes amies sans exception surtout Samia et Fouzia
A tous les enseignants et les étudiants du département d'informatique

BOUMEDIENE Chahrazed

Dédicaces

Je dédie ce modeste travail qui n'aurait pas pu aboutir et voir la lumière sans l'aide de Dieu le tout puissant.
A ceux qui nous ont procuré soutien et courage,
A nos chers parents qui nous ont toujours honorés par leur fierté,
Á mes Chères sœurs et frères.
A nos chers enseignants, à qui nous devons respect et estime, pour n'avoir épargner aucun effort pour nous faciliter la tâche d'étudier
A tous les ami(e)s et à tous ceux qui nous avons eu la chance de croiser durant nos études universitaires

HADROUG mokhtaria

Table des matières

Table des figures **7**
Introduction générale 8

1 Généralités sur les réseaux **9**
1.1 Introduction 9
1.2 Qu'est-ce qu'un réseau ? 9
1.3 Intérêts d'un réseau 10
1.4 Classification des réseaux 10
1.4.1 L'étendue géographique 10
1.4.1.1 les PAN 10
1.4.1.2 les LAN 11
1.4.1.3 les MAN 11
1.4.1.4 les WAN 11
1.4.2 La nature de communication 12
1.4.2.1 Réseaux poste à poste (Peer to peer) 12
1.4.2.2 Réseaux avec serveur dédié (Server/Client) . . 12
1.5 Les Topologie des réseaux 13
1.5.1 Les topologies physiques de base 13
1.5.1.1 Topologie en bus 13
1.5.1.2 La topologie en étoile 14
1.5.1.3 La topologie en anneau 14
1.5.2 Les topologies logiques 14
1.6 Les éléments physiques du réseau 15
1.7 Les éléments logiciels du réseau 16
1.8 Concept d'architecture en couches 16
1.8.1 Pourquoi utiliser une architecteur en couche ? 17
1.9 Le modèle de référence OSI 18
1.9.1 Description du modèle 19
1.9.2 Les fonctionnalités des couches 19
1.9.2.1 La couche physique 19
1.9.2.2 La couche liaison 20

1.9.2.3 La couche réseau 20
1.9.2.4 La couche transport 21
1.9.2.5 La couche session 21
1.9.2.6 La couche présentation 22
1.9.2.7 La couche application 22
1.10 L'architecture TCP/IP 23
1.10.1 Origine 23
1.10.2 Principe architectural 23
1.11 Conclusion 25
Bibliographie 26

2 Administration réseau **27**
2.1 Introduction 27
2.2 Supervision 27
2.2.1 Supervision réseau 28
2.2.1.1 Principe 28
2.2.2 Fonctionnement d'une plateforme de supervision 28
2.2.3 Les méthodes de supervision 29
2.2.3.1 La supervision active 29
2.2.3.2 la supervision passive 29
2.3 Les modele de supervision réseau 29
2.3.1 Modèle organisationnel 29
2.3.2 Modèle fonctionnel (SMFA « SpecificManagement Functionnal Areas ») 29
2.3.2.1 Gestion des performances (Performance Management) 30
2.3.2.2 Gestion des configurations (Management Configuration) 30
2.3.2.3 Gestion de la comptabilité (Accounting Management) 30
2.3.2.4 Gestion des anomalies (Fault Management) . 31
2.3.2.5 Gestion de la sécurité (Security Management) 31
2.3.3 Modèle d'information (SMI « Structure of Management Information ») 31
2.3.3.1 Définitions formelles utilisant ASN.1 31
2.4 Administration réseau : 32
2.4.1 Principale tâche : 32
2.4.2 Principe de fonctionnement 32
2.4.3 Station d'administration (NMS Network Management System) 33
2.5 Les protocoles d'administration réseaux 34

2.5.1 Protocole pour la gestion des réseaux : SNMP 34
2.5.1.1 Historique 34
2.5.1.2 principe 35
2.5.1.3 Les messages du superviseur SNMP vers l'agent SNMP 38
2.5.1.4 Les messages de l'agent SNMP vers le superviseur SNMP 38
2.5.1.5 Les message entre les agents SNMP 39
2.5.2 Protocole pour la gestion des réseaux CMIP /CMIS . . 39
2.5.2.1 Les services CMISE 40
2.5.2.2 Les massages échangés 40
2.6 Les logiciels de supervision 41
2.6.1 Nagios 41
2.6.2 Centreon 42
2.6.3 Zabbix 43
2.6.4 Cacti 44
2.7 Conclusion 44
Bibliographie 45

3 Conception et réalisation **46**
3.1 Introduction 46
3.2 Présentation du l'UML 46
3.2.1 Définition 46
3.2.2 Diagramme des cas d'utilisation global 47
3.2.3 Diagramme de séquence 48
3.2.4 Diagramme d'activité 50
3.2.5 Le diagramme de classe 51
3.3 Réalisation 54
3.3.1 Choix du protocole SNMP 54
3.3.2 Choix du langage de programmation python 54
3.4 Description de l'application 55
3.4.1 Le formulaire d'authentification 55
3.4.2 Menu d'application 56
3.4.3 interface «scanne le réseau» 56
3.4.4 Conclusion 57
Bibliographie 59
Conclusion générale 60

Table des figures

1.1 Les différentes catégories de réseaux informatiques 11
1.2 Les topologies physiques de base 13
1.3 Le modèle de référence OSI 18
1.4 Le modèle OSI et l'architecture TCP/IP 24

2.1 architecteur d'administration réseau 33
2.2 Structure MIB 36

3.1 Diagramme de cas utilisation globale 47
3.2 Diagramme de séquence «authentification» 49
3.3 Diagramme de séquence « administration réseau » 50
3.4 Diagramme d'activité « authentification » 51
3.5 Diagramme d'activité « l'état des équipements » 52
3.6 Diagramme de classe 53
3.7 Login de l'application 56
3.8 Menu de l'application 56
3.9 scanne réseau 57
3.10 information machine 57

Introduction générale

Les réseaux informatiques sont devenus incontournables aujourd'hui. Au point que la plupart de nos activités ne pourraient plus être envisagées sans la mise en place de ces réseaux. On assiste à leur déploiement à tous les niveaux de la société, dans les entreprises, au niveau national et international, y compris dans les domiciles des usagers. Le nombre des machines dans ces réseaux peut parfois devenir extrêmement élevé, la maintenance ainsi que la gestion de ces parcs informatiques deviennent alors des enjeux importants, d'autant plus qu'une panne du réseau peut parfois avoir des conséquences catastrophiques.
le matériel d'infrastructure réseau est de plus en plus sophistiqué et permet d'être contrôlé à distance : c'est là un des points fondamentaux de la gestion réseau, il est aujourd'hui nécessaire, étant donné l'étendue et la complexité des réseaux, de pouvoir le gérer à distance depuis son poste de travail et n'avoir qu'à se déplacer qu'en derniers recours, lors qu'une opération physique est nécessaire.
C'est pourquoi les administrateurs réseau font appel à des logiciels de surveillance et de supervision réseau. Ces logiciels vérifient l'état du réseau ainsi que des machines connectées et permettent à l'administrateur d'avoir en temps réel une vue de l'ensemble du parc informatique.

Dans le cadre de notre projet de fin d'études, nous somme appelées à concevoir et à mettre en place un outil d'administration réseau permettant à la fois de collecter des données sur les équipements et notifier l'administrateur réseaux de toute éventuelle panne d'un équipement.
Le reste de ce manuscrit est structuré en trois chapitres comme suit :

- Le premier chapitre survol les concepts de base relatifs aux réseaux informatique.
- Le deuxième chapitre est présente la tâche de l'administration réseau. seront présentes ses objectifs, ses procédures et ses outils
- Le troisième chapitre quant est diviser en deux parties. La première est consacrée à l'étude conceptuelle du projet et la deuxième à l'implémentation de l'application

Chapitre 1

Généralités sur les réseaux

1.1 Introduction

Les réseaux informatiques sont nés du besoin de relier des terminaux distants à un site central puis des ordinateurs entre eux et en fin des machines terminales, telles que des stations de travail ou des serveurs. Dans un premier temps, ces communications étaient destinées au transport de données informatiques. Aujourd'hui, l'intégration de la parole téléphonique et de la vidéo sur ces réseaux informatiques devient naturelle, même si cela ne va pas sans difficulté.

1.2 Qu'est-ce qu'un réseau ?

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies (protocoles).
Dans le cas ou les objets sont des ordinateurs on parle d'un réseau informatique. Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à de gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types, d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche) et des particuliers (messagerie, loisirs, services d'informations par minitel et Internet)[1].

1.3 Intérêts d'un réseau

Un ordinateur est une machine permettant de manipuler des données. L'homme, un être de communication, a vite compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre eux afin de pouvoir échanger des informations. Voici un certain nombre de raisons pour lesquelles un réseau est utile, un réseau permet :

- Le partage de fichiers, d'applications et de ressources.
- La communication entre personnes (grâce au courrier électronique, la discussion en direct, ...).
- La communication entre processus (entre des machines industrielles).
- La garantie de l'unicité de l'information (bases de données).
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).
- Les réseaux permettent aussi de standardiser les applications, on parle généralement de groupware. Par exemple la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement[1].

1.4 Classification des réseaux

Il existe plusieurs critères pour classifier les réseaux informatiques, dont les suivants :

1.4.1 L'étendue géographique

Une classification (traditionnelle) est basée sur la notion d'étendue géographique (selon la distance), la figure1.1 illustre sommairement ces catégories :

1.4.1.1 les PAN

la plus petite taille de réseau définit les PAN (Personal Area Network) : Ces réseaux personnels interconnectent sur quelques mètres les équipements personnels tels que GSM, portables, d'un même utilisateur.

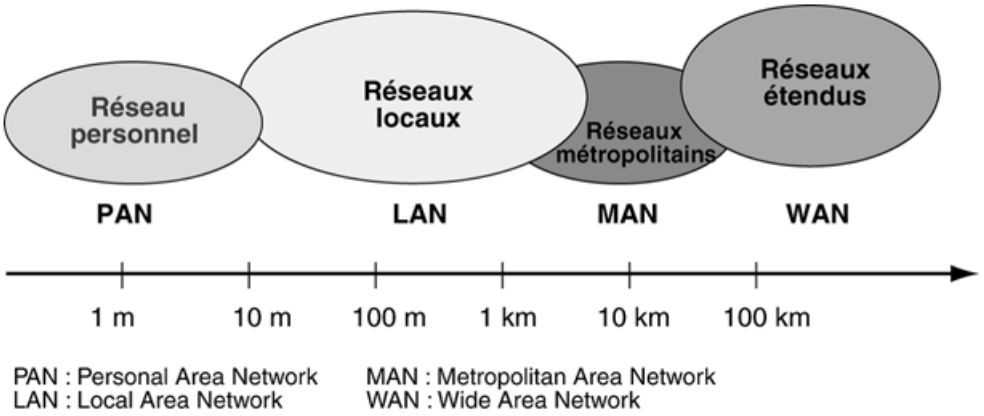

FIGURE 1.1 – Les différentes catégories de réseaux informatiques [2].

1.4.1.2 les LAN

les réseaux locaux, également appelés LAN (Local Area Network), correspondent par leur taille aux réseaux intra-entreprise. Ils servent au transport de toutes les informations numériques de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres.

1.4.1.3 les MAN

les réseaux métropolitains, ou MAN (Metropolitan Area Network), permettent l'interconnexion des entreprises ou éventuellement des particuliers sur un réseau spécialisé à haut débit qui est géré à l'échelle d'une métropole. Ils doivent être capables d'interconnecter les réseaux locaux des différentes entreprises pour leur donner la possibilité de dialoguer avec l'extérieur.

1.4.1.4 les WAN

les réseaux étendus, ou WAN (Wide Area Network), sont destinés, comme leur nom l'indique, à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents[1].

1.4.2 La nature de communication

On distingue deux catégories de réseaux selon la nature de communication entre les terminaux (Client/Client ou Client/Serveur) :

1.4.2.1 Réseaux poste à poste (Peer to peer)

Peer-to-peer signifie littéralement pair à pair (Client à Client). Ce concept introduit ainsi une relation d'égal à égal entre deux ordinateurs. Dans son essence, l'informatique paire à pair se définit comme le partage des ressources et des services par échange direct entre systèmes. Ces échanges peuvent porter sur les informations, les cycles de traitement, la mémoire cache ou encore le stockage sur disque des fichiers.

Principe :

- Les postes de travail sont simplement reliés entre eux par le réseau. Aucune machine ne joue un rôle particulier. Chaque poste peut partager ses ressources avec les autres postes.

C'est à l'utilisateur de chaque poste de définir l'accès à ses ressources. Il n'y a pas obligatoirement d'administrateur attitré[3].

1.4.2.2 Réseaux avec serveur dédié (Server/Client)

il ressemble un peu au réseau poste à poste mais cette fois-ci, on y rajoute un poste plus puissant, dédié à des tâches bien précises. Cette nouvelle station s'appelle serveur. Le serveur centralise les données relatives au bon fonctionnement du réseau.

Principe :

- Les ressources réseau sont centralisées.
- Un ou plusieurs serveurs sont dédiés au partage de ces ressources et en assurent la sécurité.
- Les postes clients ne sont en principe que des clients, ils ne partagent pas de ressources, ils utilisent celles qui sont offertes par les serveurs[3].

1.5 Les Topologie des réseaux

La topologie d'un réseau décrit la manière dont les nœuds sont connectés. Cependant, on distingue la topologie physique, qui décrit comment les machines sont raccordées au réseau, de la topologie logique qui renseigne sur le mode d'échange des messages dans le réseau (topologie d'échange).

1.5.1 Les topologies physiques de base

Les topologies physiques sont disposées selon trois principaux groupes de forme géométrique : le bus, l'anneau et l'étoile (La figure1.2) :

1.5.1.1 Topologie en bus

Dans ce mode de liaison, l'information émise par une station est diffusée sur tout le réseau. Le réseau en bus est aussi dit réseau à diffusion. Dans ce type de topologie, chaque station accède directement au réseau, d'où des problèmes de conflit d'accès (contentions ou collisions) qui nécessitent de définir une politique d'accès. Celle-ci peut être centralisée (relation dite maître/esclave) ou distribuée comme dans les réseaux locaux.

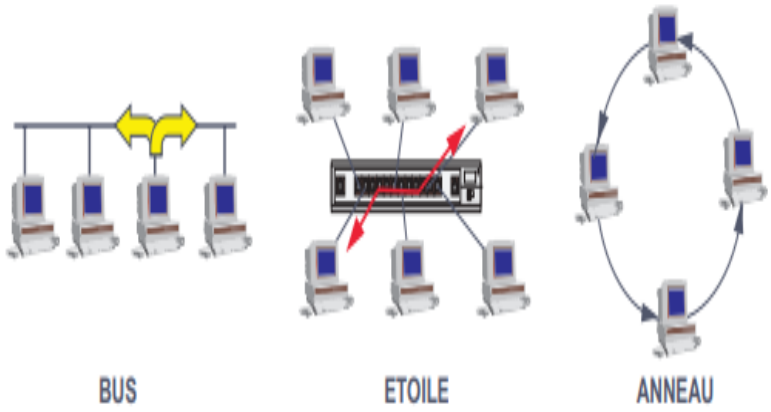

FIGURE 1.2 – Les topologies physiques de base [4].

1.5.1.2 La topologie en étoile

Tous les nœuds du réseau sont reliés à un nœud central commun : le concentrateur. Tous les messages transitent par ce point central. Le concentrateur est actif, il examine chaque message reçu et ne le retransmet qu'à son destinataire. Cette topologie correspond, par exemple, au réseau téléphonique privé d'une entreprise où le commutateur téléphonique met en relation les différents postes téléphoniques de l'installation. La topologie étoile autorise des dialogues intrenœud très performants. La défaillance d'un poste n'entraîne pas celle du réseau, cependant le réseau est très vulnérable à celle du nœud central.

1.5.1.3 La topologie en anneau

chaque poste est connecté au suivant en point à point. L'information circule dans un seul sens, chaque station reçoit le message et le régénère. Si le message lui est destiné, la station le recopie au passage (au vol). Ce type de connexion autorise des débits élevés et convient aux grandes distances (régénération du signal par chaque station). L'anneau est sensible à la rupture de la boucle. Les conséquences d'une rupture de l'anneau peuvent être prises en compte en réalisant un double anneau[4].

1.5.2 Les topologies logiques

Le terme topologie logique désigne la façon par laquelle les données transmises entre les nœuds, plutôt que la disposition des voies ou chemins qu'empruntent les données. Une topologie logique s'appelle aussi un système de transport réseau .la topologie logique d'un réseau décrit la manière par laquelle les données sont mises en trames et comment les impulsions électrique sont envoyées sur le support physique du réseau les éléments d'une topologie logique appartiennent a la fois aux couche liaison du modèle OSI (section 1.9).
Chaque topologie logique possède son propre ensemble de principe de signalisation de données, mais impose aussi des exigences particulières au niveau du média de transmission et de la topologie physique. Ethernet et Token Ring sont les deux systèmes de transport réseau (topologie logique) les plut courants[1].

1.6 Les éléments physiques du réseau

Un réseau est physiquement composé d'un ou plusieurs éléments actifs comme les hubs ou les switchs. En fonction du type d'interconnexion de réseaux locaux on utilise des répéteurs, des routeurs ou des passerelles. Pour la liaison longue distance de réseaux éloignés on utilise un modem. Il est à noter que les ordinateurs ne font pas partie intégrante d'un réseau. Pour la connexion des ordinateurs au réseau, on utilise des cartes réseau et des câbles.

- **La carte réseau :**est une carte additionnelle ou non qui adapte le format des signaux de l'ordinateur à ceux du réseau. Chaque carte réseau fabriquée dans le monde est unique par son adresse qui a été déterminée et inscrite en mémoire morte lors de sa fabrication. Une adresse de carte est définie sur 6 octets. Cette adresse est appelée adresse MAC (Media Access Control).
- **Le répéteur :**est un régénérateur de signal. Sur de grandes longueurs (plusieurs dizaines de mètres), les signaux parcourant un câble se « fatiguent » et se détériorent. Il faut donc leur redonner une nouvelle jeunesse en les régénérant et en filtrant leurs éventuels parasites.
- **Le concentrateur :** ou hub est un répéteur diffuseur sur lequel se branchent les câbles arrivant des ordinateurs. Son rôle consiste à maintenir la topologie en bus. Des ordinateurs reliés à un hub ne constituent donc pas physiquement un réseau en étoile. Le commutateur : ou switch est un hub « intelligent ». En effet, contrairement au concentrateur, le switch possède en mémoire l'adresse MAC de tous les ordinateurs qui lui sont connectés. Ainsi, les données ne vont plus d'ordinateur à ordinateur pour trouver leur destinataire. Le switch aiguille les informations vers le bon ordinateur. C'est un répéteur aiguilleur.
- **Le routeur :** permet de relier différents réseaux. Il oriente les données vers le meilleur itinéraire. Il peut même détecter automatiquement des itinéraires défectueux ou en ralentissement, et rediriger les informations vers un chemin plus approprié évitant les zones à problème. Le routeur est généralement utilisé pour connecter un réseau à Internet via un modem ou des réseaux de topologies différentes.
- **Les passerelles :** sont des appareils qui permettent la relation entre réseaux ne codifiant pas les informations de la même manière. Elles sont utilisées pour relier des mondes informatiques fondamentalement différents comme les micro-ordinateurs et des gros systèmes.
- **Le modem :** qui veut dire modulateur-démodulateur adapte les données numériques issues de l'ordinateur en données (analogiques ou numériques)

exploitables par le réseau téléphonique. C'est la modulation. La démodulation fait le contraire, elle adapte les données récupérées sur le réseau téléphonique en données compréhensibles par l'ordinateur. Le modem autorise la communication entre réseaux distants (LAN/LAN ou LAN/WAN) via des routeurs. Il existe des modems pour les lignes commutées du classique téléphone familial (RTC) ainsi que pour les lignes RNIS (Réseaux Numérique à Intégration de Service) ou ADSL[5].

1.7 Les éléments logiciels du réseau

les applications distribuées Les services offerts aux utilisateurs finaux sont de plus en plus sophistiqués. Ils ont largement évolué ces dernières années et vont certainement encore progresser dans le futur pour laisser apparaître des services bien plus interactifs et utilisant à la base les technologies multimédias. Parmi les services actuellement offerts, on retrouve :

- les services d'accès aux bases de données.
- les services de transferts de fichiers.
- les services de messagerie.
- les services de Workgroup.
- les services de téléphonie,ect.

Ces services sont mis à la disposition des usagers de manière sélective. En effet, en fonction de leur position et rôle dans l'entreprise, les utilisateurs peuvent accéder à des services différenciés, avec également différents droits d'accès aux serveurs, applications.
Un ensemble de règles d'utilisation est mis en place pour contrôler les accès au système d'information et aux ressources de l'entreprise et/ou rendre disponibles certains services à un groupe bien déterminé d'utilisateurs[6].

1.8 Concept d'architecture en couches

L'empilement des couches et les services qu'elles offrent constituent l'architecture de communication. Une architecture de communication est donc une représentation abstraite (Indépendante de toute référence à des logiciels ou des matériels particuliers) de la circulation des informations et des concepts utilisés au sein d'un réseau quelconque[7].

Historiquement, chaque grand constructeur avait défini la sienne : SNA (System Network Architecture) d'IBM, DSA (Distributed System Architecture) de BULL... Ces architectures propriétaires incompatibles entre elles ne permettent pas l'interopérabilité des systèmes. Aussi, convenait-il de définir des techniques de mises en relation en spécifiant une architecture normalisée. C'est ce qu'entreprit l'ISO (International Standardization Organization) en définissant une architecture de communication normalisée, couramment appelée modèle de référence ou modèle OSI (Open System Interconnection).
L'architecture réseau assure à l'utilisateur l'accès aux ressources informatiques et lui procure un service identique que les ressources soient locales ou distantes, pour cela elle doit être transparente à l'utilisateur[4].

1.8.1 Pourquoi utiliser une architecteur en couche ?

La structuration en couches considère un système comme logiquement composé d'un ensemble de n sous-systèmes ordonnés. Les sous-systèmes adjacents communiquent à travers leur interface commune. Un sous-système de rang i peut être constitué d'une ou plusieurs entités ; il communique avec les autres sous-systèmes de même rang : on parle alors de la couche de rang i ou, plus simplement, de la couche i. Les avantages d'une telle structure sont multiples :

- Une architecture de communication se définit entièrement en décrivant les services offerts par chaque couche, les interfaces entre les couches adjacentes et la manière dont ces couches coopèrent avec les entités du même niveau (les entités homologues) dans les autres systèmes.
- On peut développer séparément et simultanément toutes les couches d'une architecture de communication, une fois définies les interfaces entre les différents sous-systèmes.
- Le nombre d'interfaces à définir est minimal : il suffit de décrire, pour chaque niveau, les interfaces avec la couche supérieure (sauf pour la couche la plus élevée de l'architecture) et avec la couche inférieure (sauf pour la couche la plus basse). Les coopérations entre entités homologues sont régies par un ou plusieurs protocoles.

Ainsi, chaque couche fournit des services aux entités des couches supérieures et s'appuie sur les services offerts par les entités des couches inférieures. La couche la plus élevée offre à l'utilisateur tous les services utilisables dans l'architecture ; la couche la plus basse communique directement avec le support de transmission[7].

1.9 Le modèle de référence OSI

Cette norme établie par l'internationale standard organisation (ISO) en 1984 est la norme open system interconnexion (OSI, interconnexion de systèmes ouverts).

Un système ouvert est un ordinateur, un terminal, un réseau, n'importe quel équipement respectant cette norme et donc apte à échanger des l'information avec d'autres équipement hétérogènes et issus de constructeurs différents.

Le modèle OSI est composé de sept couches comme illustré dans la figure 1.3. Chacune remplissant une partie bien définie des fonctions permettant l'interconnexion. Ces couches sont classées en deux catégories comme suit :

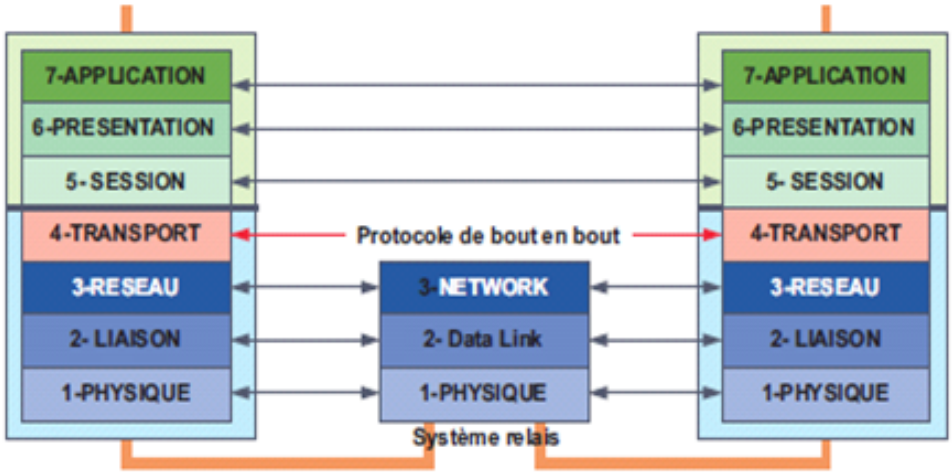

FIGURE 1.3 – Le modèle de référence OSI
[4]

- **Les couches hautes** essentiellement chargées d'assurer l'inter-fonctionnement des processus applicatifs distants, ces couches sont dites orientées application
- **Les couches basses** destinées à fournir aux couches hautes un service de transport fiable de données, déchargeant les couches hautes de la gestion de tous les mécanismes de localisation et de transfert d'information à travers un ou plusieurs systèmes relais, ces couches sont dites

orientées transport (ou transfert).

Les couches basses garantissent aux couches hautes que le transfert d'information se réalise correctement. Il est donc nécessaire que la dernière couche basse destination s'assure, avant de délivrer les données aux couches applicatives, que celles-ci sont correctes (contrôle de bout en bout). Les autres couches inférieures n'effectuent qu'un transfert de proche en proche entre systèmes. Les couches hautes n'assurent, globalement, que l'organisation des échanges et fournissent les mécanismes nécessaires à assurer l'inter-fonctionnement de une ou plusieurs applications distantes[4].

1.9.1 Description du modèle

Pour réaliser une communication à travers un ou plusieurs systèmes intermédiaires (relais) il faut :

- relier les systèmes par un lien physique (couche PHYSIQUE) .
- contrôler qu'une liaison peut être correctement établie sur ce lien (couche LIAISON).
- s'assurer qu'à travers le relais (réseau) les données sont correctement acheminées et délivrées au bon destinataire (couche RÉSEAU)
- contrôler, avant de délivrer les données à l'application que le transport s'est réalisé correctement de bout en bout (couche TRANSPORT).
- organiser le dialogue entre toutes les applications, en gérant des sessions d'échange (couche SESSION).
- traduire les données selon une syntaxe de présentation aux applications pour que celles-ci soient compréhensibles par les deux entités d'application (couche PRÉSENTATION) ;
- fournir à l'application utilisateur tous les mécanismes nécessaires à masquer à celle-ci les contraintes de transmission (couche APPLICATION)[4].

1.9.2 Les fonctionnalités des couches

1.9.2.1 La couche physique

La couche physique fournit l'interface avec le support physique sur lequel elle transmet un train de bits en assurant, éventuellement, la transparence de binaire. Elle est chargée de la synchronisation entre les horloges source

et destination. La couche physique ne distingue pas le mode connecté du mode sans connexion. Elle prend en charge les transmissions synchrones ou asynchrones en fonctionnement simplex, semi-duplex ou duplex que la liaison soit en mode point à point ou multipoint. Les services fournis, à la couche liaison, sont :

- l'établissement et la libération de la connexion physique .
- la transmission série et ou parallèle de **n** bits .
- l'identification des extrémités de la connexion physique, qui peut être unique (liaison point à point) ou multiple (liaison multipoints).
- l'identification du circuit de données, cette identification pouvant être utilisée par les entités réseaux pour identifier un circuit de données (voie logique) .
- le maintien en séquence des bits émis .
- l'horloge et la récupération d'horloge (synchronisation) .
- la notification de dérangement.

La qualité de service fournie dépend essentiellement des supports utilisés, elle est caractérisée par le débit offert, le débit effectif, le taux d'erreur et la disponibilité[4].

1.9.2.2 La couche liaison

C'est le niveau de cette couche que les données numériques sont traduites en signal. Les bits de données sont organisés en trames. Un en-tête est créé dans lequel on peut identifier l'émetteur et le destinataire par leur adresse physique. Au niveau de cette couche est ajouté un code de redondance cyclique (CRC) qui permet de détecter certains problèmes de transmission. Ainsi, le destinataire d'une trame calcule la somme et la compare avec celle qui a été transmis. S'il y a une différence la trame est rejetée[8].
La qualité de service fournie s'exprime principalement par le taux d'erreurs résiduelles, ces erreurs pouvant provenir de données altérées, perdues, dupliquées ou du non-respect de l'ordonnancement des trames[4].

1.9.2.3 La couche réseau

La couche réseau assure un transfert de données entre deux systèmes d'extrémité à travers un ou plusieurs sous-réseaux physiques (systèmes relais). Elle fournit les fonctions de routage et garantit aux entités de transport

un service réseau uniforme indépendamment des technologies utilisées dans les sous-réseaux physiques traversés. Deux fonctions essentielles en découlent :

- La localisation des systèmes : doit résoudre deux problèmes : l'adressage et l'acheminement (le routage).
- L'adaptation de la taille des unités de données aux capacités des différents sous-réseaux traversés[4].

1.9.2.4 La couche transport

Il s'agit du cœur du modèle OSI. Au niveau de cette couche, différents mécanismes sont mis en ouvre pour établir un mode connecté, c'est-à-dire un moyen de s'assurer que les informations ont toutes été transmises et sans problème. Un premier niveau de connexion consiste à accuser la réception systématiquement de tous les paquets reçus, et cela, dans un délai suffisant, faute de quoi le paquet et retransmis, car il est considéré comme égaré. De plus, le mode connecté permet de maitre à disposition une connexion pour la couche supérieure, comme il s'agissait d'un lien point à point[8]. Les mécanismes mis en œuvre par les protocoles de transport sont nombreux, quelques-uns sont :

- La segmentation,
- Le contrôle de flux,
- L'établissement de la connexion,
- La déconnexion.

Protocole de transport sans connexion : Le protocole de transport, en mode connecté, est lourd à mettre en œuvre, un additif à la norme (ISO 7498) spécifie un protocole en mode non connecté. Les fonctions assurées sont réduites :

- Aucune garantie de remise ni de séquencement n'est assurée à la couche session,
- Les unités de données ne sont pas acquittées, un total de contrôle optionnel peut être utilisé[4].

1.9.2.5 La couche session

Est la première couche orientée traitement. Elle permet l'ouverture et la fermeture d'une session de travail entre systèmes distants et assure la syn-

chronisation du dialogue. C'est à ce niveau que l'on décide également du mode de transmission (simplex, half-duplex, full-duplex). La synchronisation du dialogue se fait au moyen de "points de contrôle" ainsi, lorsqu'un problème de produit, seules les données émises après le dernier point de contrôle correctement reçu seront réexpédiées. Une connexion de session est découpée en activités :

- Une activité correspond à un transfert autonome de données (par exemple le transfert d'un fichier),
- Une session peut comporter une ou plusieurs activités, de même une activité peut être couverte par plusieurs sessions[8].

1.9.2.6 La couche présentation

La couche présentation est la première couche non impliquée dans les mécanismes de transfert d'information. Son rôle essentiel consiste à garantir la signification des données transférées, indépendamment de la représentation interne de celles-ci, du codage utilisé (ASCII, EBCDIC...), de la longueur des mots machines (32, 64 bits...), de la représentation des valeurs négatives (complément à 1 ou à 2) dans les hôtes communicants.
La couche présentation garantit à la couche application :

- l'accès aux services de la couche session, la plupart des primitives de service de présentation ne font que traverser la couche présentation, elles ont une correspondance directe avec les primitives de service de la couche session (services réfléchis).
- les services de cryptographie et de compression de données.
- la négociation d'une syntaxe de transfert (contexte de présentation) lors de l'établissement de la connexion de présentation[4].

1.9.2.7 La couche application

La couche application est la dernière couche et la plus abstraite du modèle OSI, cette couche assure l'interface de communication avec l'utilisateur, à travers des logiciels adéquats. Elles gèrent également la communication entre application, comme pour le courrier électronique, transferts de fichiers. [8].

1.10 L'architecture TCP/IP

1.10.1 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. À cet effet, TCP/IP décrit un réseau logique (réseau IP) au-dessus du ou des réseaux physiques réels auxquels sont effectivement connectés les ordinateurs.
Son intégration à UNIX BSD 4, par l'université de Berkeley, en fit le standard de la communauté UNIX (1980). TCP/IP a remplacé (1983) le protocole NCP (Network Control Program) dans ARPANET, ancêtre de l'Internet. Aujourd'hui, TCP/IP est le protocole standard de tous les réseaux, du LAN au WAN. De récentes adaptations autorisent les flux multimédia et, en particulier, la voix[4].

1.10.2 Principe architectural

Précédant le modèle OSI, TCP en diffère fortement, non seulement par le nombre de couches, mais aussi par l'approche. Le modèle OSI spécifie des services (approche formaliste), TCP/IP des protocoles (approche pragmatique). Développé au-dessus d'un environnement existant, TCP/IP ne décrit, à l'origine, ni de couche physique ni de couche liaison de données. Les applications s'appuient directement sur le service de transport, La figure1.4 compare les deux architectures :

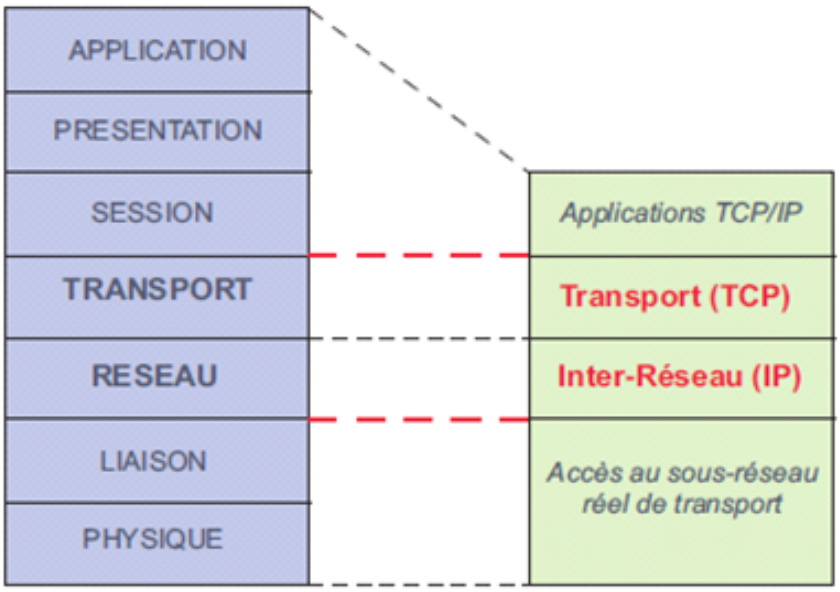

FIGURE 1.4 – Le modèle OSI et l'architecture TCP/IP [4].

- Il n'y a pas de couche application au sens OSI du terme, c'est-à-dire de couche qui présente des **API** (Application Programming Interface) aux applications, et qui rendent transparent à ces dernières le ou les sous-réseaux réels de transport utilisés. La couche application TCP/IP inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques à différentes applications d'utilisateur final
- La couche transport, sur laquelle s'appuient directement les applications, fournit deux types de service : un service en mode connecté (TCP : Transmission Control Protocol) comparable, en ce qui concerne d'ISO et un service de transport allégé UDP (User Datagram Protocol) qui n'offre qu'un service de type best effort (datagramme).
- La couche réseau (Internet Protocol, IP) assure la communication entre les réseaux grâce au protocole IP (Internet Protocol). On utilise la commutation de paquets de type datagramme pour acheminer des données entre les systèmes d'extrémité, quelle que soit la technologie réseau qu'ils emploient. Le protocole IP gère les datagrammes : il les achemine jusqu'à leur destinataire, se charge du routage et de l'adaptation de la taille des données au réseau sous-jacent. IP définit en fait un service minimal, l'acheminement des datagrammes à travers l'interconnexion de réseaux. Ce service est sans connexion et sans garantie. Il ne

fait aucune hypothèse quant à la fiabilité des réseaux traversés[7].

1.11 Conclusion

Dans ce chapitre nous avons cherché à survoler les concepts généraux des réseaux. Nous avons donné une définition des réseaux, présenter leur intérêt, leurs topologies et leurs types. Comme nous avons décrit leur modelé de référence ainsi que les différents modes de communication.

Bibliographie

[1] TAHRA Zahiaet. Etude et simulation d'un réseau de téléphonie sur ip toip. *Mémoire de fin d'étude pour l'optimisation de Diplôme d'ingénieur d'état en Informatique Université Kasdi Merbah Faculté des Sciences et Sciences de l'Ingénieur Département des Mathématiques et d'Informatique*, Décembre 2004.

[2] Guy Pujolle. « les réseaux ». *Eyrolles, édition*, 2003.

[3] k.SAYAH L.TEDJADJNA. « etude des solutions d'affichage dynamique multi-écrans sur ip – optimisation et intégration d'une solution open source ». *Mémoire master academique, Université Kasdi Merbah. Faculté des Nouvelles Technologies de l'Information et de la Communication Département d'Informatique et Technologie de l'Information –Ouargla*, 2014.

[4] Claude Servin. « rÉseaux et tÉlÉcoms ». *Dunod, Paris*, 2003.

[5] http ://indus.graph.free.fr/Cours ,, Consulter le 15/02/2018.

[6] Omar Cherkaoui Nazim Agoulmine. , « pratique de le gestion de reseau ». *Groupe Eyrolles*, 2003.

[7] Dominique Seret Danièle Dromard. « architecteur des réseaux ». *Pearson Education France*, 2009.

[8] S.RAHMANI H.BOUKALA. «administration des réseaux sous windows server ». *Mémoire de fin de Cycle Master 2 en Informatique, Université A/Mira de Béjaia, Faculté des Sciences Exactes Département d'Informatique*, 2016.

Chapitre 2

Administration réseau

2.1 Introduction

La taille des réseaux ne cessant de grandir de jour en jour et l'importance de ceux-ci dans le monde de l'entreprise prenant une place prépondérante, le besoin de contrôler en temps réel leur qualité et leur état est rapidement devenu une priorité. C'est dans ce but qu'est apparu, il y a maintenant une vingtaine d'années, le concept de supervision de réseaux. Nous présenterons dans ce document ce qu'est la supervision de réseaux ainsi que l'implémentation qui en a été faite. Pour ce faire nous définirons en premier lieu les concepts et les notions de la supervision de réseaux et nous présenterons ce que la normalisation a apporté en réponse a ces problématiques et plus particulièrement dans le monde IP. Nous étudierons ensuite l'exemple du plus en plus populaire Nagions, un logiciel libre dédié a la supervision de réseaux

2.2 Supervision

La supervision se définit comme une technique utilisant au mieux les ressources informatiques pour obtenir des informations sur l'état des réseaux et de leurs composants. Ces données seront ensuite traitées et affichées afin de mettre en lumière d éventuels problèmes. La supervision peut résoudre les problèmes automatiquement ou dans le cas contraire prévenir via un système d'alerte (email ou SMS par exemple) les administrateurs. Cette définition de la supervision est décrite plus en détail dans la norme ISO7498/4. Plusieurs actions sont ainsi réalisées : Acquisition de données, analyse, puis visualisation et réaction. Un tel processus est réalisé à plusieurs niveaux d'un parc de machines : Au niveau interconnexions (Réseau), au niveau de la machine elle-même (Systéme) et au niveau des services offerts par cette machine

(Applications)[1].

2.2.1 Supervision réseau

La supervision réseau est un ensemble de protocoles, matériels et logiciels informatiques assurant plusieurs les activités suivantes : surveiller, visualiser, analyser et agir. Cette opération est assuré par l'utilisation de ressources réseaux adaptées (matérielles ou logicielles) capable de fournir des informations sur l'état des réseaux et ses machines distantes. Il faut donc disposer d'une console de supervision qui regroupe et synthétise toutes les informations. On supervise pour avoir une visibilité sur le système d'information. Cela permet de disposer rapidement des informations, de connaître l'état de santé du réseau, des systèmes, ainsi que leurs performances. Ce qui donne rapidement une image du système étudié. Grace à Ces informations on peut gérer de manière automatique les pannes et les problèmes de surcharge survenant sur le réseau[1].

2.2.1.1 Principe

Le suivi régulier du bon fonctionnement de l'ensemble des équipements présents sur le réseau d'une entreprise et l'optimisation permanente de ses performances sont des fonctions incontournables. Mise en place d'un outil de supervision réseau , La mise en place d'une solution de supervision permet d'avoir une vue d'ensemble en temps-réel des équipements supervisés. Elle permet de visualiser à tout moment l'état des différents équipements configurés. Ainsi les objectifs sont multiples :

- Eviter les arrêts de service
- Remonter des alertes
- Détecter et prévenir les pannes

Un administrateur peut être informé, par le biais d'une alarme (SMS, mail..), à n'importe quel moment des problèmes qui peuvent survenir sur les équipements[1].

2.2.2 Fonctionnement d'une plateforme de supervision

Le fonctionnement d'une telle plateforme se fait à l'aide des tests qui sont envoyées vers les stations à surveiller dans un réseau, puis les réponses à ces tests sont analysées afin de voir leurs états. Le superviseur peut être alors informé d'une panne ou bien d'une défaillance qui survient sur le réseau à l'aide d'un message qui lui est transmis sur son mail ou bien par SMS[1].

2.2.3 Les méthodes de supervision

L'opération de supervision se fait selon 2 manières (figure 4), la supervision active et la supervision passive[1].

2.2.3.1 La supervision active

consiste sur le fait que l'outil de supervision décide quand il fait le test sur l'équipement à superviser .elle se base sur l'envoi des requêtes avec différents protocoles de communication vers une destination d'un équipement pour tester sa connectivité et son bon fonctionnement[1].

2.2.3.2 la supervision passive

c'est l'hôte qui décide quand elle renvoie son information vers la plateforme de supervision .Ses informations sont de types des traps SNMP, syslogs etc., puis déclenche une action en fonction de l'analyse des informations reçues[1].

2.3 Les modele de supervision réseau

La supervision peut être vue au travers de 3 modèles (selon l'ISO)

2.3.1 Modèle organisationnel

La gestion OSI (Open System Interconnection) fait reposer son modèle relationnel sur deux concepts importants qui sont le gestionnaire et l'agent, et précise aussi leur communication. Les correspondants administratifs (gestionnaire/agent) sont représentés par des processus qui échangent des informations à travers un protocole (agent/gestionnaire). L'échange entre agent (administré) et gestionnaire (administrateur) se fait :

- Soit par un mécanisme de demande du gestionnaire/réponse de l'agent
- soit par un compte rendu spontané de l'administré à l'administrateur à la suite d'un événement[2].

2.3.2 Modèle fonctionnel (SMFA « SpecificManagement Functionnal Areas »)

L'ISO s'intéresse de prés 'a la supervision. Et, d'es 1988, l'organisme publie la norme ISO7498/4 définissant les principales fonctions que doivent

implémenter les systèmes de supervision et d'administration. Ces fonctions sont les suivantes[3].

2.3.2.1 Gestion des performances (Performance Management)

La gestion des performances analyse de manière continue les performances du réseau afin de le maintenir dans un état de performance acceptable. Cette gestion s'opère en trois étapes. Tout d'abord, des variables contenant des informations significatives quant aux performances du réseau sont récupérées. Parmi celles-ci on peut citer le temps de réponse d'une station utilisateur ou encore le taux d'occupation d'un segment réseau. Une fois ces variables obtenues, elles sont analysées. Si elles dépassent un seuil de performance fixe préalablement, une alarme est tout de suite envoyée a l'administrateur du réseau, pour régler le problème au plus vite. Ces variables de gestion de performances sont réactualisées a court intervalle de temps dans le but d'être le plus réactif possible au moindre embryon de baisse de performance. La gestion des performances permet donc une évaluation du comportement des ressources et un contrôle de l'efficacité des activités de communication[3].

2.3.2.2 Gestion des configurations (Management Configuration)

La gestion des configurations effectue un suivi des différentes configurations des éléments présents sur le réseau. Elle stocke dans une base de données les versions des systèmes d'exploitation et des logiciels installés sur chaque machine du parc réseau. Par exemple pour un ordinateur du réseau, la base contiendra la version de son OS, du protocole TCP/IP, La gestion des configurations permet donc une identification et un contrôle des systèmes ouverts. Elle collecte et fournit des informations sur les différents systèmes du réseau[3].

2.3.2.3 Gestion de la comptabilité (Accounting Management)

La gestion de la comptabilité a pour but de mesurer l'utilisation des ressources afin de réguler les accès et d'instaurer une certaine équité entre les utilisateurs du réseau. Ainsi des quotas d'utilisation peuvent être fixés temporairement ou non sur chacune des ressources réseaux. De plus, la gestion de la comptabilité autorise la mise en place de systèmes de facturation en fonction de l'utilisation pour chaque utilisateur. La gestion de la comptabilité permet donc un établissement des couts d'utilisation ainsi qu'une facturation de l'utilisation des ressources[3].

2.3.2.4 Gestion des anomalies (Fault Management)

La gestion des anomalies détecte les problèmes réseaux (logiciels ou matériels). Elle essaie d'isoler le plus précisément le problème en effectuant divers tests. Quand cela est possible, elle règle elle-même automatiquement l'anomalie. Sinon, elle alerte les personnes concernées par le type du problème afin de solliciter leur intervention. La gestion des anomalies garde dans une base de données l'ensemble des problèmes survenus ainsi que leur solution, de manière 'a être encore plus efficace face 'a un incident récurrent. Cette fonction de la norme ISO7498/4 demeure de loin la fonction la plus implémentée a ce jour. La gestion des anomalies détecte donc et corrige les fonctionnements anormaux des éléments du réseau[3].

2.3.2.5 Gestion de la sécurité (Security Management)

La gestion de la sécurité contrôle l'accès aux ressources en fonction des politiques de droits d'utilisation établies. Elle veille a ce que les utilisateurs non autorisés ne puissent accéder a certaines ressources protégées. La gestion de la sécurité met donc en application les politiques de sécurité[3].

2.3.3 Modèle d'information (SMI « Structure of Management Information »)

En complément du standard MIB qui définit les informations spécifiques d'administration réseaux et leur signification, un standard séparé spécifie l'ensemble des règles utilisées pour définir et identifier les variables MIB. Ce sont les règles de gestion des informations d'administration, SMI (Structure of Management Information).Pour que le protocole d'administration de réseaux reste simple, SMI pose des restrictions sur les types de variables autorisées dans la MIB, spécifie les règles de nommage de ces variables et crée les règles de définition des types de variables[2].

2.3.3.1 Définitions formelles utilisant ASN.1

Le standard SMI indique que toutes les variables MIB doivent être définies et référencées à l'aide de la notation ISO de syntaxe abstraite ASN.1 (Abstract Syntax Notation 1). ASN.1 est un langage formel qui présente 2 caractéristiques principales : une notation utilisée dans les documents manipulés par les humains et une représentation codée et concise de la même information, utilisée dans les protocoles de communication. Dans les 2 cas, la notation formelle élimine toutes les ambiguïtés possibles, tant du point de vue de la représentation que de la signification. Au lieu de dire par exemple,

qu'une variable contient une valeur entière, un concepteur qui utilise ASN.1 doit définir la forme exacte et le domaine des valeurs prises par cet entier[4].

2.4 Administration réseau :

L'administrateur réseau définit les procédures de gestion et administre les infrastructures de communications (externe et interne) des systèmes d'information de la collectivité pour en assurer la cohérence, la qualité et la sécurité[1].

2.4.1 Principale tâche :

- Mise en œuvre, administration et maintenance des composants et de l'infrastructure réseau
- Supervision des réseaux en termes de charge et fluidité du trafic en termes de sécurité du réseau
- Définition et gestion des autorisations d'accès aux réseaux, aux machines et équipements du réseau
- Mise en œuvre, administration et maintenance des systèmes de protection (routeurs, firewall)
- Gestion des incidents, des problèmes et des configurations
- Documentation des processus de mise en œuvre, de mise à jour et d'exploitation des composants.
- Participation aux réunions techniques et force de propositions sur la définition et la mise en œuvre de nouveaux projets informatiques .[1].

2.4.2 Principe de fonctionnement

Sur le point de l'administration, un système de réseau informatique se compose d'un ensemble d'objets qu'un système d'administration surveille et contrôle. Chaque objet est géré localement par un processus appelé agent qui transmet régulièrement ou sur sollicitation les informations de gestion relatives à son état et aux événements qui le concernent au système d'administration. Le système d'administration comprend un processus (manager ou gérant) qui peut accéder aux informations de gestion de la MIB locale via un protocole d'administration comme SNMP ou CMIP de qui le met en relation avec les divers agents. Le principe se repose donc sur les échanges :

– D'une part, entre une base d'informations appelée MIB(Management Information Base) et l'ensemble des éléments administrés (objets) ;

– D'autre part, entre les éléments administrés et le système d'administration[4]. La figure 2.1 présente le principe générale d'administration réseau

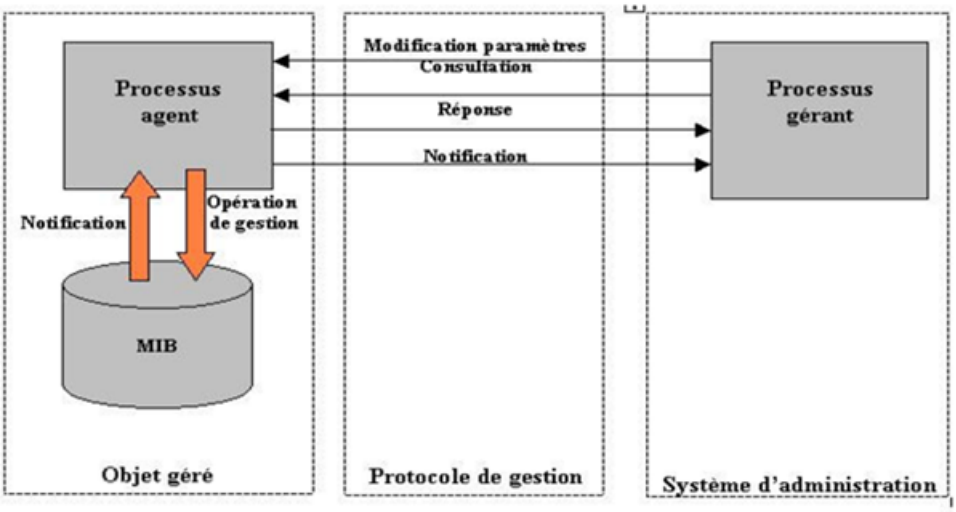

FIGURE 2.1 – architecteur d'administration réseau
[4]

2.4.3 Station d'administration (NMS Network Management System)

Ce terme désigne le périphérique utilisé par l'administrateur pour gérer son réseau. Celui-ci doit obligatoirement posséder :

- Des applications spécifiques à l'administration.
- Une interface avec l'administrateur.
- La capacité à pouvoir récupérer des informations des éléments administrés.
- Une base de données obtenue à partir des MIBs des éléments administrés.

La station NMS peut envoyer des requêtes à un périphérique afin d'obtenir des informations sur son paramètre. L'agent du périphérique reçoit la requête et renvoie les informations demandées. Lorsqu'elle reçoit cette réponse, la station NMS peut utiliser les informations de configuration du périphérique afin de déterminer les opérations à entreprendre en fonction de son état. [4].

2.5 Les protocoles d'administration réseaux

Un outil typique destiné à l'administration de réseaux consiste en un outil qui fonctionne en mode Client serveur, associant une station d'administration de réseau NMS (Network Management Station) et les équipements actifs du réseau. Pour fonctionner, ces outils utilisent soit le protocole SNMP dans le monde des réseaux IP ou le protocole CMIP dans le monde des télécommunications.

2.5.1 Protocole pour la gestion des réseaux : SNMP

SNMP Le protocole Simple Network Management Protocol(SNMP) est un protocole de famille TCP/IP (Internet Protocol), est peut donc être utilisé sur tous les réseaux de type internet, reposant sur UDP, permettant d'administrer à distance des équipements ou des logiciels. Deux entités composent un système SNMP : un superviseur et des agents, sont installés sur les équipements administrables, ils remontent leurs informations à un superviseur, gestionnaire centralisant les informations. Celui-ci peut également donner des consignes aux agents. Localement, les agents fonctionnent à certain niveaux du modèle OSI (sur des couches choisies) et stockent les informations dans des bases appelées Management Information Base(MIB). De nombreuses MIB existent offrant un panel de fonctionnalités assez importantes[5].

2.5.1.1 Historique

Le protocole SNMP a commencé à émerger dans les années 1980 et a évolué en plusieurs versions.

- SNMPv1 : c'est la première version du protocole. La sécurité de cette version est minimale, car elle est basée sur la connaissance entre les parties d'une chaîne de caractères appelée "communauté" ;
- SNMPsec : le but de cette version est de combler une lacune de la version précédente SNMPv1, la sécurité. Cette version, désormais largement oubliée, a été peu implémentée ;
- SNMPv2p : beaucoup de recherches ont été entreprises pour mettre à jour le protocole SNMPv1. Il en résulte l'apparition de nouvelles requêtes protocolaires ainsi que de nouveaux types de données. La sécurité reste basée sur les groupes d'utilisateurs de SNMPsec ;
- SNMPv2c : cette version du protocole est appelée "community string based SNMPv2". Elle améliore encore les requêtes protocolaires par

rapport à SNMPv2p et utilise la sécurité par chaîne de caractères "communauté" de SNMPv1 ;
- SNMPv2u : cette version du protocole utilise les requêtes et les types de données définis par la version SNMPv2c, mais la sécurité est basée sur les usagers ;
- SNMPv2* : cette version combine le meilleur de SNMPv2p et de SNMPv2u. Les documents de cette version n'ont jamais été officiellement publiés, il est toutefois possible de retrouver des copies de ces documents sur le site web de SNMP Research
- SNMPv3 : cette version, supportant les "proxies", est une combinaison de la sécurité basée sur les usagers, les types et les opérations définis dans SNMPv2p. La sécurité est basée sur les versions SNMPv2u et SNMPv2*[6].

2.5.1.2 principe

Les différents éléments que l'on peut identifier avec le protocole SNMP sont les suivants[2].

- **Les agents SNMP :** ce sont les équipements (réseau ou serveur) qu'il faut superviser.
- **Le superviseur SNMP :** c'est une machine centrale à partir de laquelle un opérateur humain peut superviser en temps réel toute son infrastructure, diagnostiquer les problèmes et finalement faire intervenir un technicien pour les résoudre.
- **La MIB :** Chaque agent SNMP maintient une base de données décrivant les paramètres de l'appareil géré. Le Manager SNMP utilise cette base de données pour demander à l'agent des renseignements spécifiques. Cette base de données commune partagée entre l'agent et le Manager est appelée Management Information Base (MIB). Généralement ces MIB contiennent l'ensemble des valeurs statistiques et de contrôle définis pour les éléments actif du réseau. SNMP permet également l'extension de ces valeurs standards avec des valeurs spécifiques à chaque agent, grâce à l'utilisation de MIB privées
  Un fichier MIB est écrit en utilisant une syntaxe particulière, cette syntaxe s'appelle SMI 3, basée sur ASN.1 tout comme SNMP lui-même. En résumé, les fichiers MIB sont l'ensemble des requêtes que le Manager peut effectuer vers l'agent. L'agent collecte ces données localement et les stocke, tel que défini dans la MIB. Ainsi le Manager doit être conscient de la structure (que celle -ci soit de type standard ou privée) de la MIB afin d'interroger l'agent au bon endroit.

La structure d'une MIB est une arborescence hiérarchique dont chaque noeud est défini par un nombre ou un Object IDentifier (OID). Chaque identifiant est unique et représente les caractéristiques spécifiques du périphérique géré. Lorsqu'un OID est interrogé, la valeur de retour n'est pas un type unique (texte,entier,compteur,tableau...) Un OID est donc une séquence de chiffres séparés par des points.
Une MIB est un arbre très dense, il peut y avoir des milliers d'OID dans la MIB(figure2.2)

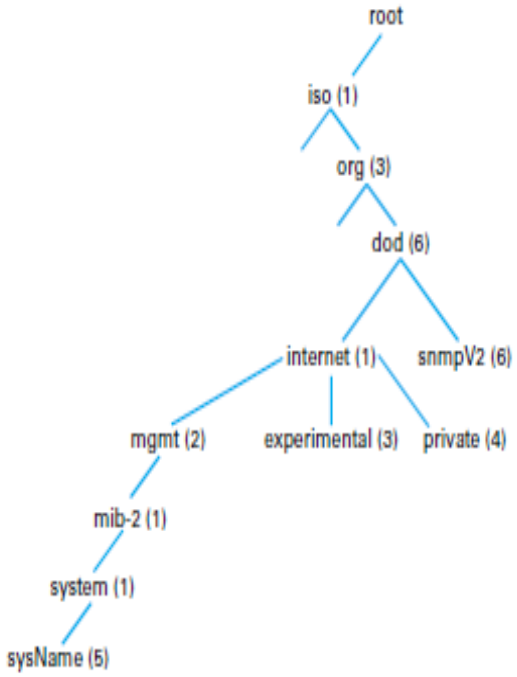

FIGURE 2.2 – Structure MIB

Le fichier MIB

le fichier MIB est représenté sous la forme suivante :

```
sysContact OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-write
STATUS mandatory
DESCRIPTION
"The textual identification of the contact
for this managed node, together with inf
on how to contact this person."
: :=  system 4
```

SYNTAX indique le type de l'objet selon la syntaxe ASN.1 (Abstract Syntax Notation One).
ACCESS indique le mode d'accès à l'objet. Les valeurs suivantes sont possibles :

- read-only
- read-write
- write-only
- not-accessible

STATUS indique si l'objet doit obligatoirement être présent dans toute implémentation de la MIB ou pas. Les valeurs suivantes sont possibles :

- mandatory
- optional
- obsolete

DESCRIPTION est un texte destiné à l'administrateur et qui décrit l'objet.
La dernière ligne de la définition attribue à l'objet sysContact le numéro 4 dans le groupe system. En effet, les MIB sont hiérarchisées à la manière des répertoires dans un système de fichiers. Le nom complet de cet objet au sein de la MIB-II est donc system.sysContact (le point est utilisé comme séparateur) ou bien system.4 ou bien 1.sysContact (system a pour numéro 1) ou, encore moins lisible, 1.4

```
iso.org.dod.internet.mgmt
.1.3.6.1.2
```

- La racine de la hiérarchie n'a pas de nom et est désignée simplement par un point.
- iso (1) désigne l'International Organization for Standardization.
- org (3) a été créé par l'ISO à l'intention de divers organismes.
- dod (6) a été attribué au ministère de la Défense des États-Unis (Department of Defense).
- internet (1) regroupe tout ce qui touche à l'Internet.
- mgmt (2), enfin, est utilisé pour les standards de l'IAB.

Sous .iso.org.dod.internet.mgmt, la MIB-II a pour nom mib-2 et pour numéro 1, de telle sorte que l'objet sysContact a pour nom absolu : .iso.org.dod.internet.mgmt.mib-2.syste .1.3.6.1.2.1.1.4

En pratique, cet objet est d'un type discret (ce n'est pas un tableau et il ne contient donc qu'une valeur) donc on lui ajoute un .0 final, ce qui donne comme nom absolu : .iso.org.dod.internet.mgmt.mib-2.system.sysContact.0 .1.3.6.1.2.1.1.4.0

Les objets pouvant contenir plusieurs valeurs se voient ajouter à leur nom un .1 pour la première valeur, .2 pour la deuxième et ainsi de suite. Somme toute, SNMP est simple

- **Les communautés :** Dans SNMPv2, le contrôle d'accès est fait en fournissant dans chaque message un mot de passe appelé communauté. Il existe généralement deux communautés, l'une utilisée pour les accès en lecture (c'est par défaut la chaîne de caractères public), l'autre utilisée pour les accès en écriture (c'est par défaut la chaîne de caractères private). Il est évidemment essentiel de modifier ces valeurs et de les tenir secrètes.

2.5.1.3 Les messages du superviseur SNMP vers l'agent SNMP

- Message "Get Request" : ce message permet au superviseur d'interroger un agent sur les valeurs d'un ou de plusieurs objets de la MIB.
- Message "Get Next Request" : ce message permet au superviseur d'interroger un agent pour obtenir la valeur de l'objet suivant dans l'arbre des objets de l'agent. Ce message permet de balayer des objets indexés de type tableau ;
- Message "Get Bulk Request" : introduite avec la version 2 du protocole SNMP, ce message permet de mixer les messages "Get Request" et "Get Next Request" pour obtenir des blocs entiers de réponses de la part de l'agent .
- Message "Set Request" : ce message permet au superviseur de positionner ou modifier la valeur d'un objet dans l'agent[6].

2.5.1.4 Les messages de l'agent SNMP vers le superviseur SNMP

- Message "Get Response" : ce message est utilisé par l'agent pour répondre aux messages "Get Request", "Get Next Request" et "Get Bulk Request" envoyés par le superviseur .

– Message "Trap" : ce message est envoyé par l'agent à son superviseur de manière asynchrone pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du superviseur.
– Message "Notification" : introduit avec la version 2 du protocole SNMP, ce message est similaire au message "Trap". Il est envoyé par l'agent à son superviseur de manière asynchrone pour signaler un événement, un changement d'état ou un défaut. L'agent n'attend pas d'acquittement de la part du manager.
– Message "Inform" : introduit avec la version 2 du protocole SNMP, ce message est envoyé par l'agent à son superviseur de manière asynchrone pour signaler un événement, un changement d'état ou un défaut. L'agent attend un acquittement de la part du superviseur et il y aura une retransmission en cas de non réponse. Ce message peut aussi être utilisé pour un dialogue superviseur - superviseur[6].

2.5.1.5 Les message entre les agents SNMP

Le seul message envoyé entre les agents SNMP est :
– Message "Report" : introduit avec la version 2 du protocole SNMP mais jamais implémenté, ce message permet aux différents agents de communiquer entre eux (principalement pour remonter des problèmes de traitement des messages SNMP)[6].

2.5.2 Protocole pour la gestion des réseaux CMIP /CMIS

L'ISO a proposé dans les années 80 la norme CMIS/CMIP (Common Management Information Service, Common Management Information Protocol) comme protocole d'administration de réseau supporte l'échange de l'information entre les applications de gestion de réseau et les agents de gestion. CMIS définit un système des services d'information de gestion de réseau. CMIP supporte une interface qui fournit les fonctions qui peut-être utilisé à supporter pour le modèle OSI. Les spécifications de CMIP pour des réseaux de TCP/IP s'appellent CMOT (CMIP au-dessus de TCP) CMIP n'indique pas la fonctionnalité de l'application de gestion de réseau, il définit seulement le mécanisme d'échange de l'information des objets contrôlés et n'indique pas comment l'information doit être employée ou interprétée. Le protocole CMIP pour le modèle OSI se base sur trois modèles suivants :
– Modèle d'architecture MSA (Managed System and Agents) qui définit l'architecture de la gestion du protocole CMIP et la notion de systèmes

gérés et gérants.
- Modèle d'information qui définit le modèle de représentation des l informations de gestion,
- Modèle fonctionnel SMFA (Specific Management Function Area) qui définit des domaines fonctionnels d'administration et leurs relations[2].

2.5.2.1 Les services CMISE

La gestion système est une application ; elle se localise donc en couche 7 du modèle de référence OSI. Les flux applicatifs générés par cette application s'appuieront comme tous les flux sur les services rendus par les couches inférieures et les autres services de la couche 7.
Parmi ces derniers, on recense :

- ACSE (Association Control Service Element) qui gère les associations d'application entre deux processus de gestion (établissement, contrôle, libération).
- ROSE (Remote Operation Service Element) qui permet l'invocation d'opérations distantes.
- CMISE (Common Management Information Service Element) qui fournit les services de gestion pour les applications de gestion
  - C'est le protocole CMIP (Common Management Information Protocol) qui fournit le support nécessaire à la communication entre entités d'applications utilisatrices du service CMIS.
  - La gestion système manipule des objets sur lesquels elle effectue des opérations et des notifications. Les opérations sont celles habituelles des bases de données, soit la création, la suppression, la mise à jour et la lecture d'une valeur auxquelles s'ajoute l'exécution d'action sur l'objet associé. La notification est de type rapport d'événements[2].

2.5.2.2 Les massages échangés

CMISE offre les moyens d'effectuer des échanges entre processus de gestion pour réaliser ces opérations et notifications. Les échanges sont de type demande et demande-réponse.
CMISE assure la mise en œuvre des services suivants :

- M-CREATE qui permet à un gestionnaire de créer un objet dans la MIB de l'agent,

- M-DELETE qui permet à un gestionnaire de supprimer un objet dans la MIB de l'agent,
- M-ACTION, confirmée ou non, qui permet à un gestionnaire de demander qu'une action soit effectuée par un objet géré.
- M-EVENT-REPORT, confirmée ou non, qui permet à un agent de transmettre la notification émise par un objet géré à un gestionnaire,
- M-GET qui permet à un gestionnaire de lire les valeurs d'attributs d'objets gérés,
- M-SET, confirmée ou non, qui permet à un gestionnaire de modifier les valeurs d'attributs,
- M-CANCEL-GET qui permet d'annuler un service M-GET invoqué. M-CREATE, M-DELETE, M-GET et M-CANCEL-GET sont des services opérant toujours en mode confirmé[2].

2.6 Les logiciels de supervision

Les logiciels de supervision sont des solutions applicatives répondant au concept de supervision tel qu'il a été défini précédemment. Ils s'appuient, pour la plupart, sur le protocole SNMP. Ces outils ont principalement pour objectif de connaître 'a tout instant l'état des nœuds critiques (serveurs, switchs, routeurs) et l'état des services tournant sur les différents serveurs. Ils doivent également être capables d'analyser le trafic réseau afin de permettre une meilleure répartition des ressources réseaux[7].

2.6.1 Nagios

Nagios est ce que l'on appelle un ordonnanceur , c'est-à-dire qu'il va lancer les différents tests de supervision, appelés contrôles, sur les hosts et services. Il reste l'outil de supervision le plus utilisé à l'heure actuelle, sa configuration sous forme de fichiers, peut s'avérer vite repoussante mais en fait cependant un candidat idéal pour l'automatisation.
L'inconvénient de Nagios reste son IHM (Interface Homme Machine) très basique. Il faut avouer que son interface ne donne pas spécialement envie d'être consultée, en effet au delà de la pertinence de l'information, il faut de la compréhension et de l'interprétation. C'est sur ce constat que vient se greffer la prochaine solution décrite : Centreon.
les plugins : sont des programmes externes permettent de controler une ressource ou un service locale ou distant en effectuant des tests de toutes

sorte(fonctionnement de services ,espace de disque, charge)sur la machine nagios, ainsi que des tests simple (par exemple) ping sur machine distance.

Avantages

- Reconnu auprès des entreprises, grande communauté.
- Très puissant et modulaire.
- Une solution complète permettant la gestion de panne et d'alarmes, gestion utilisateurs, ainsi que la cartographie du réseau.
- Beaucoup de documentations sur le web.
- Performances du moteur.

Inconvénients

- Interface non ergonomique et peu intuitive.
- Configuration fastidieuse via beaucoup de fichiers.
- Pour avoir toute les fonctionnalités il faut installer des plugins, de base c'est assez limité[7].

2.6.2 Centreon

Centreon, une interface à Nagios. Première précision à apporter, le cœur de Centreon est basé sur Nagios. Centreon propose une interface web différente de celle de Nagios et y ajoute des fonctionnalités (génération de la configuration de Nagios, stockage des données de performance, interface ergonomique...).
En résumé, Centreon est considéré comme un outil à part entière même si il est basé sur Nagios comme ordonnanceur. Il propose donc au sein d'une même interface tout ce qui est nécessaire à la surveillance de l'infrastructure et donc à faire de la supervision pure et dure. Malgré tout il ne propose que le minimum concernant la métrologie, on ne pourra pas par exemple remonter des informations orientées services comme celle d'une base de donnée, que l'on pourrait avoir sous Cacti ou Munin.(Anciennement Oréon), Créé en 2003 par des français souhaitant améliorer Nagios, il a été repris par une nouvelle entreprise nommée Merethis il se présente comme une évolution de celui-ci pour tout d'abord son interface mais aussi ses fonctionnalités. Il s'appuie également sur les technologies Apache et PHP pour l'interface web, MySQL pour le stockage des données de configuration et de supervision.

Avantages

- Une installation complète et automatique des packages nécessaires à l'utilisation de NAGIOS.
- Facilite la configuration de Nagios.
- Une Graphe le résultat des alertes, système de reporting.

Inconvénients

- Requiert plus de ressources matérielles que Nagios[2].

2.6.3 Zabbix

Zabbix est une application libre (open source) de supervision des systèmes et des réseaux.Par sa polyvalence, Zabbix peut superviser et vérifier les statuts d'une multitude de services réseaux, ou systèmes, ce qui fait de lui un outil complet proposant des fonctionnalités relatives à la supervision (alertes, mesures, actions sur conditions). Le principal reproche vient de l'aspect graphique où dans certains cas la lisibilité laisse à désirer. Certains lui reprochent également son interface web dite un peu (vieillotte) et la prise en main initiale n'est pas forcément intuitive.

Avantages

- Une solution très complète : cartographie de réseaux, gestion poussée d'alarmes via SMS, Jabber ou Email, gestion des utilisateurs, gestion de pannes, statistiques et reporting.

- Une entreprise qui pousse le développement, et une communauté croissante
- Une interface vaste mais claire.
- Des performances : l'application a été testée avec succès avec 10000 équipements supervisés.

Inconvénients

- Interface est un peu vaste, la mise en place des templates n'est pas évidente au début : petit temps de formation nécessaire.
- L'agent zabbix communique par défaut en clair les informations, nécessité de sécuriser ces données (via VPN par exemple). Peu d'interfaçage avec d'autres solutions commerciales[7].

2.6.4 Cacti

Cacti est un outil de monitoring qui a la particularité d'avoir une (Plugin architecture)qui va lui permettre l'ajout de fonctionnalités grâce à l'importation et à la configurations de plugins via l'interface web. L'aspect supervision proposé ici ne sera pas aussi développé que dans les autres logiciels (nagios par exemple) Donc Cacti reste un outil de métrologie intégrant de nombreuses possibilités grâce auxplugins, avec la possibilité d'une mise en place de supervision mais uniquement dans les cas les plus simples.

Avantages

- Installation et configuration facile
- Outil de métrologie complet.
- Multitude de fonctionnalités grâce aux plugins

Inconvénients

- Création complexe des templates
- Insuffisant pour une supervision d'un grand parc matériel[7].

2.7 Conclusion

Dans ce chapitre nous avons défini le principe de fonctionnement de l'administration réseau. Ainsi, nous avons introduit son principe, son intérêt,ses protocoles. Comme nous avons présenter certains outils logiciels d'administration réseaux.

Bibliographie

[1] *http://www-igm.univ-mlv.fr/~dr/XPOSE2007/dmichau_supervision/supervision.html , year = 2008,Consulter 07/3/2018.*

[2] EFORT. Cmis / cmip , architecture. *Protocole et Services*, 2004.

[3] Thierry Briche Matthieu Voland. Les outils d'administration et de supervision réseau l'exemple de nagios. *version 01*, Décembre 2004.

[4] Victor MORARU NGUYEN Manh Tuong. Les protocoles pour la gestion des réseaux informatiques. *Rapport Travail d'Intérêt Personnel Encadré Institut de la Francophonie pour l'Informatique Hanoi*, Juillet 2005.

[5] P.ATELIEN. Réseaux informatiques notions fondamentales. *3e édition, Eni édition,*, 2009.

[6] M.AURELIEN. Le protocole snmp. *La gestion réseau et le protocole SNMP, FIFO04*, 2006.

[7] Patrick IRSAPOULLE. Mise en place d'un outil de supervision et de contrôle distant. *Rapport de Stage de Master M2 INFORMATIQUE*, 7 Juillet 2014.

Chapitre 3

Conception et réalisation

3.1 Introduction

Dans ce chapitre, il est question de décrire l'aspect conception et implémentation. Nous commencerons alors par modéliser notre application en utilisant un langage de modélisation objet qui est UML. Puis, nous spécifierons l'environnement matériel et logiciel supportant notre application. Ensuite, nous allons décrire l'ossature globale et les principales fonctionnalités de notre application.

3.2 Présentation du l'UML

3.2.1 Définition

UML (Unified Modeling Langage) est un langage de modélisation orienté objet, destiné à modéliser les systèmes d'information. UML est formellement décrit et dispose d'une syntaxe et d'un métamodèle dans lequel il peut se décliner. Face à la complexité croissante des systèmes d'information, l'approche objet aide à appréhender la complexité des entreprises. Les principaux courants de conception orientés objet de systèmes informatiques ont été fusionnés pour donner naissance à l'UML. La notation UML est issue des notations des méthodes de Booch, d'OMT (Object Modeling Technique) et d'OOSE (Object Oriented Software Engineering). UML est né dans le cadre de l'OMG (Object Management Group) dont un des objectifs est de définir une notation standard utilisable dans le développement des systèmes informatiques basés sur l'objet[1]. Dans le cadre de ce mémoire, nous nous contenterons de présenter que les quatre principaux diagrammes : Le diagramme de cas d'utilisation, le diagramme d'activités, le diagramme de séquence et le

diagramme de classe. Ces derniers seront générés à l'aide d'ArgoUML [1] qui est un logiciel libre de création de diagramme UML.

3.2.2 Diagramme des cas d'utilisation global

Un cas d'utilisation est une manière spécifique d'utiliser un système. C'est l'image d'une fonctionnalité du système, déclenchée en réponse à la stimulation d'un acteur externe et le scénario entre les cas d'utilisations. Les cas d'utilisation apportent une solution au problème de la détermination et de la compréhension des besoins[2].
Dans notre cas un acteur externe désigne la personne responsable de la politique de sécurité et de son application par la surveillance et l'administration. Le scénario des cas utilisation représente dans notre application un ensemble des séquences d'actions qui sont réalisées par l'administrateur.

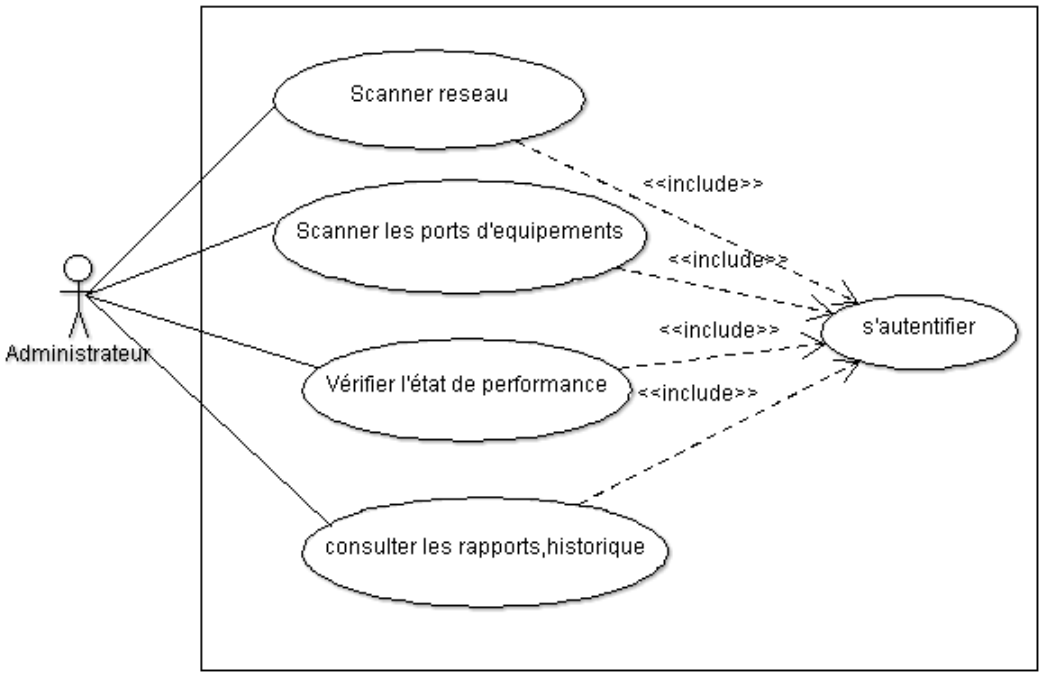

FIGURE 3.1 – Diagramme de cas utilisation globale

– La figure 3.1 : représente notre diagramme de cas d'utilisation globale qui donne à l'administrateur la possibilité de géré des équipements. En plus, il gère les comptes utilisateurs ainsi que la gestion des alertes et

1. http ://argouml.tigris.org/

configuration de SNMP. Enfin, il Consulte les rapports. Chaque administrateur doit s'authentifier avant d'accéder à l'application.

3.2.3 Diagramme de séquence

Définition

Un diagramme de séquence est une forme de diagramme comportemental qui nous permet de spécifier les interactions qui existent entre un groupe d'objets. Même si d'autres diagrammes comportement aux peuvent convenir, les diagrammes de séquence sont les plus utilisés, principalement parce qu'ils permettent de voir comment les objets s'utilisent mutuellement. Grâce à ces informations, vous pouvez déterminer plus précisément pourquoi deux objets sont liés. Comme les diagrammes de séquence sont toujours lus du haut vers le bas, ils illustrent l'ordre dans lequel les messages sont envoyés entre les objets. Il est tout à fait possible de supprimer certains messages qui participent au présent flux d'événements, si ces messages ne sont pas pertinents dans le contexte du diagramme de séquence. Bien que les diagrammes complexes puissent impressionner, ils apportent peu en matière de communication. Les diagrammes de séquence doivent rester aussi simples que possible et seuls les messages pertinents doivent être représentés[3].

Diagramme de séquence «authentification»

La figure3.2.3 : représente le diagramme de séquence « authentification »
1 L'utilisateur demande le formulaire d'authentification.
2 Le système affiche le formulaire d'authentification.
3 L'utilisateur saisit le mot de passe.
4 Le système vérifie la validité du mot de passe et affiche le résultat

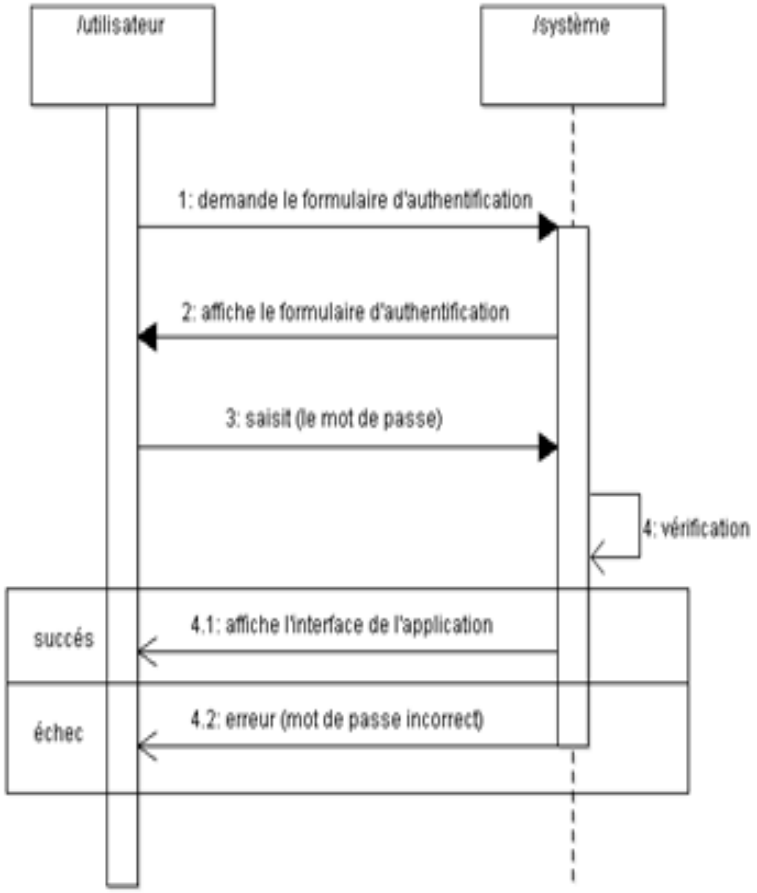

FIGURE 3.2 – Diagramme de séquence «authentification»

Diagramme de séquence «administration réseau»

La figure 3.3 : représente le diagramme de séquence d'administration réseau.

1 L'utilisateur demande au système l'état des équipements.
2 Le système scanne le réseau.
3 le système affiche l'état des équipements.
4 L'utilisateur demande au système l'état des ports.
5 Le système scanne le réseau.
6 L'utilisateur peut avoir l'état de chaque port.
7 L'utilisateur demande au système l'état de performance des équipements.
8 Le système scanne le réseau.
9 L'utilisateur peut avoir l'état de performance des équipements.

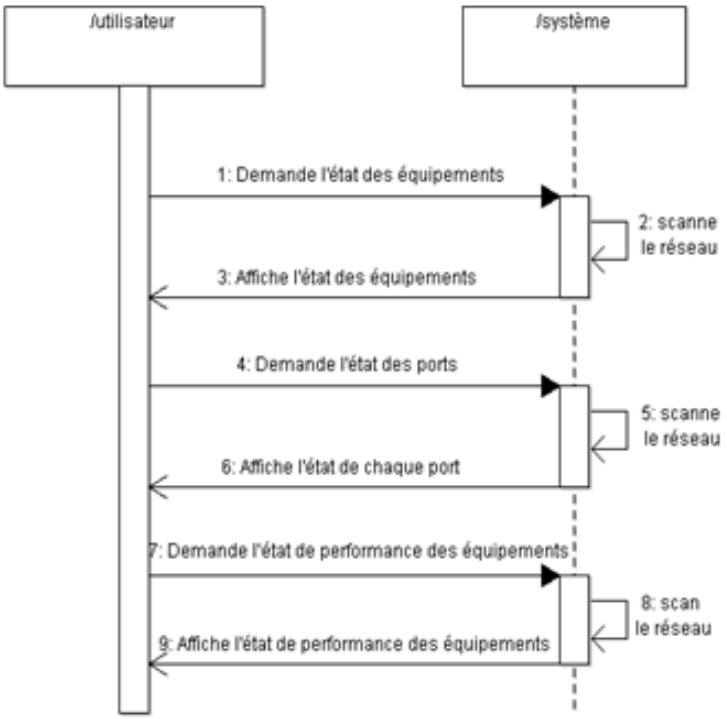

FIGURE 3.3 – Diagramme de séquence « administration réseau »

3.2.4 Diagramme d'activité

Définition Un diagramme d'activités représente l'état d'exécution d'un mécanisme, sous la forme d'un déroulement d'étapes regroupées séquentiellement dans des branches parallèles de flots de contrôle. Il ne représente ni la collaboration ni le comportement des objets. Il est utile pour la représentation des processus métiers et les cas d'utilisation

Diagramme d'activité «authentification»

Le diagramme d'activité d'authentification nous permet de voir les comportements internes du système, lors du démarrage de l'application par l'utilisateur, le système lui affiche le formulaire d'authentification, après que le mot de passe soit saisit le système vérifie sa validité et affiche la page d'accueil sinon il affiche un message d'erreur. La figure 3.4 représente le diagramme d'activité d'authentification

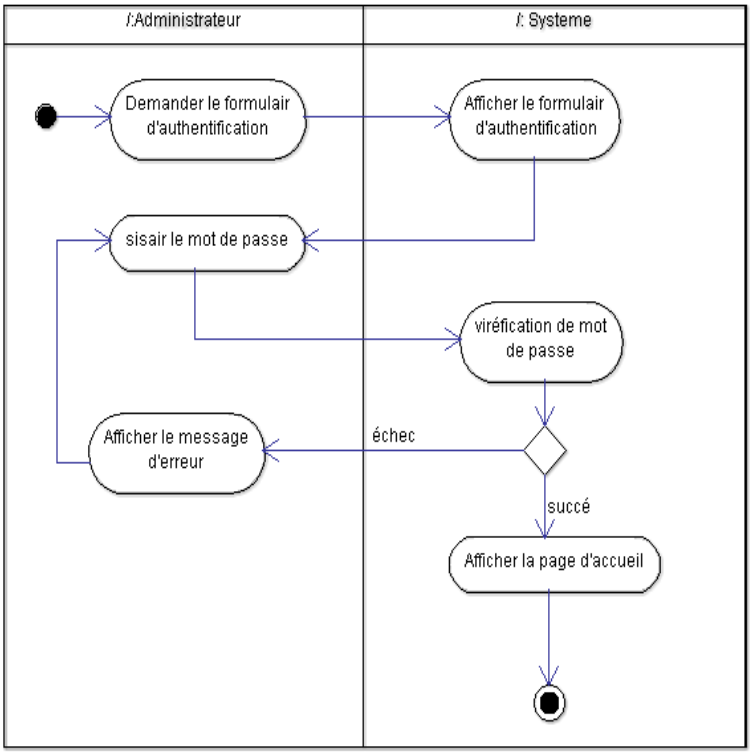

FIGURE 3.4 – Diagramme d'activité « authentification »

Diagramme d'activité «l'état des équipements»

Après une demande d'état des équipments par l'administrateur le système lui scanne le réseau et afficher l'état des équipement sinon (en cas d'erreur), il affiche un message d'erreur. La figure3.5 représente le diagramme d'activité de l'état des équipements

3.2.5 Le diagramme de classe

Définition

Un diagramme de classes est une vue graphique de la structure statique d'un système (car on ne tient pas compte du facteur temporel dans le comportement du système), exprimée en termes de classes et de relations entre ces classes. Une classe décrit un ensemble d'objets et une association décrit un ensemble de liens ; les objets sont instances des classes et les liens sont instances des associations. Le diagramme de classes est considéré comme le plus important de la modélisation orientée objet, il est le seul obligatoire

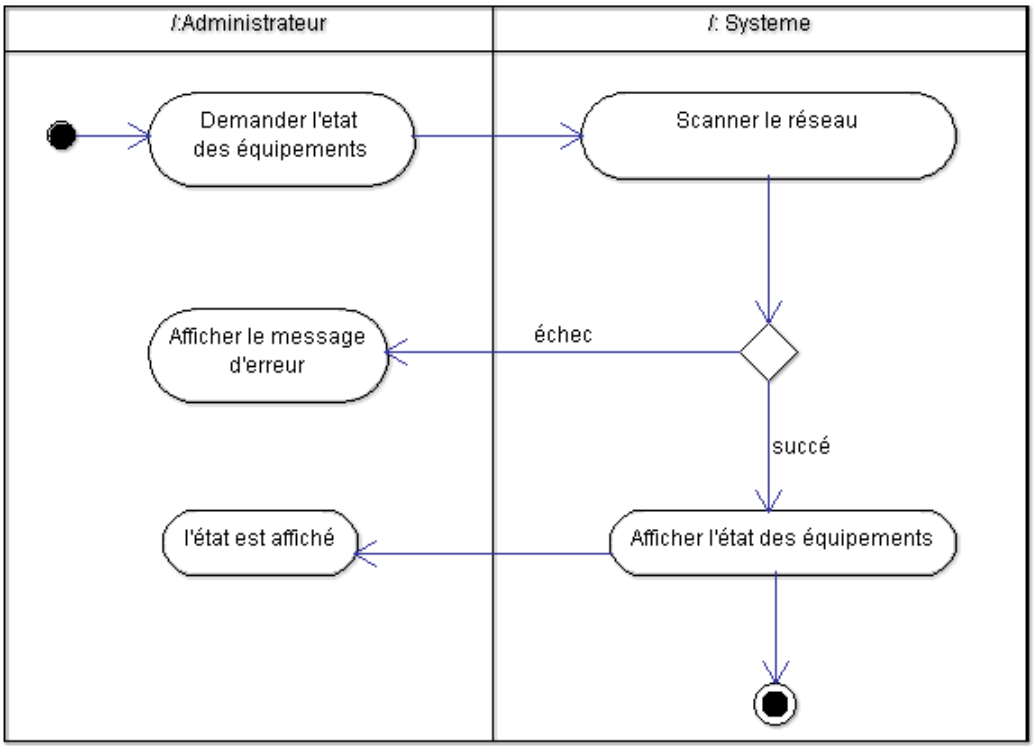

FIGURE 3.5 – Diagramme d'activité « l'état des équipements »

lors d'une telle modélisation. Il permet de définir quelles seront les composantes du système final : il ne permet en revanche pas de définir le nombre et l'état des instances individuelles. Néanmoins, on constate souvent qu'un diagramme de classes proprement réalisé permet de structurer le travail de développement de manière très efficace ; il permet aussi, dans le cas de travaux réalisés en groupe (ce qui est pratiquement toujours le cas dans les milieux industriels), de séparer les composantes de manière à pouvoir répartir le travail de développement entre les membres du groupe. Enfin, il permet de construire le système de manière correcte[4].
La figure3.6 représente le diagramme de classe de notre application

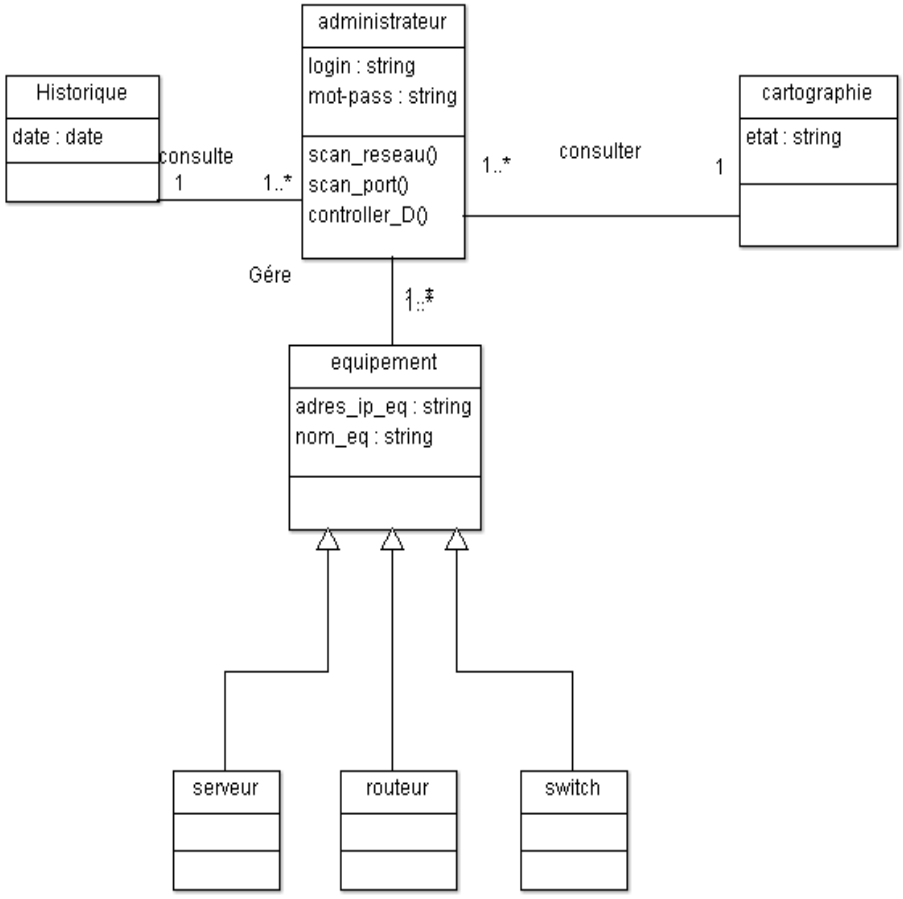

FIGURE 3.6 – Diagramme de classe

Le passage du diagramme de classe à la base de données nécessite le suivi de ces règles : 1. Transformation des classes : chaque classe du diagramme UML devient une relation, il faut choisir un attribut de la classe pouvant jouer le rôle de clé.
Transformation des associations : Nous distinguons trois familles d'associations 2. Association 1..* : il faut ajouter un attribut de type clé étrangère dans la relation fils de l'association. L'attribut porte le nom de la clé primaire de la relation père de l'association.
3. Association *..* et n-aire et classes-association : la classe-association devient une relation. La clé primaire de cette relation est la concaténation des identifiants des classes connectées à l'association.
4. Association 1..1 : il faut ajouter un attribut de type clé étrangère dans la relation dérivée de la classe ayant la multiplicité minimale égale à un. L'attribut porte le nom de la clé primaire de la relation dérivée de la classe

connectée à l'association. Si les deux multiplicités minimales sont à un, il est préférable de fusionner les deux classes en une seule.

3.3 Réalisation

Comme mentionné ci-haut, notre projet de fin d'études consiste à concevoir et à réaliser, sous le système d'exploitation Linux, une application d'administration réseau permettant de collecter et stocker dans une base de données

Dans ce qui suit, nous présenterons l'environnement, le langage et le protocole utilisées. Comme nous présenterons des exemples de fenêtres d'interaction de l'utilisateur avec l'application.

3.3.1 Choix du protocole SNMP

Le protocole SNMP (Simple Network Mangement Protocol) est un protocole, comme son nom l'indique, qui permet d'assurer la gestion du réseau. Il permet également de contrôler un réseau à distance en interrogeant les stations qui en font partie sur leur état et configurer leur configuration, de faire des tests de sécurité et observer les différentes informations liées a l'émissions de données. Il peut même être utilise pour gérer les logiciels et bases de données liées a distance. Le protocole SNMP est le protocole le plus adéquat a notre application, et le plus simple utiliser.

3.3.2 Choix du langage de programmation python

On fouillons dans Internet une définition et/ou présentation concise du langage de programmation, nous somme tomber sur celle donnée dans le cite : **"http ://www.formation-django.fr/python/presentation-ensemble-langage-python.html"**. Et vue sa clarté et sa consistance nous avons choisi de la porter dans sons intégralité toute en reconnaissant les droit d'auteur de son propriétaire que tenons à remercier.

Python est un langage de programmation portable, dynamique, extensible, gratuit, qui est développé depuis 1989 par Guido van Rossum et de nombreux contributeurs bénévoles.
L'une des principales caractéristiques de Python est qu'il est orienté objet (il permet donc la POO : programmation orientée objet), mais pas seulement. En effet, la programmation objet n'est pas strictement obligatoire en Python. Si vous avez besoin de coder un petit script dont le but est de réaliser une

maintenance système rapide, pas besoin d'envisager la création de classes et de méthodes, voire même de fonctions : quelques lignes de code suffiront !
Python est un langage interprété : à l'image du PHP, un programme Python ne nécessite pas d'étape de compilation en langage machine pour fonctionner. Le code est interprété à l'exécution. Python présente néanmoins une caractéristique intéressante : comme en Java, le code Python est compilé en bytecode (format intermédiaire) avant lancement, ce qui optimise ses performances.
Python est doté d'un typage dynamique fort : cela signifie que le typage, bien que non vérifié lors de la compilation, Python effectue des vérifications de cohérence sur les types manipulés, et permet de transformer explicitement une variable d'un type à l'autre.

Python a cette force que de réussir à fédérer des profils d'informaticiens assez différents. Parlez par exemple à un administrateur système, il y a fort à parier qu'il connaisse Python et le pratique régulièrement. Parlez à un développeur généraliste qui utilise Sublime Text comme éditeur tout terrain : Python lui est familier en tant que langage d'automatisation, de script et de macros au sein de cet éditeur. Parlez à un développeur d'application web : il ne sera pas sans connaître, au moins de nom et de réputation, des frameworks de développement web comme Django, Flask, Pyramid (Pylons), TurboGears...

Bref, on utilise Python partout, dans une grande variété de contextes et d'application. En découle une communauté très large, une grande diversité de librairies disponibles et une excellente maturité du langage.

3.4 Description de l'application

Nous allons présenter dans cette partie les principales interfaces de l'application

3.4.1 Le formulaire d'authentification

Au lancement de notre application, un formulaire s'affiche à l'écran, il permet aux utilisateurs de s'authentifier pour pouvoir accéder au menu d'application :

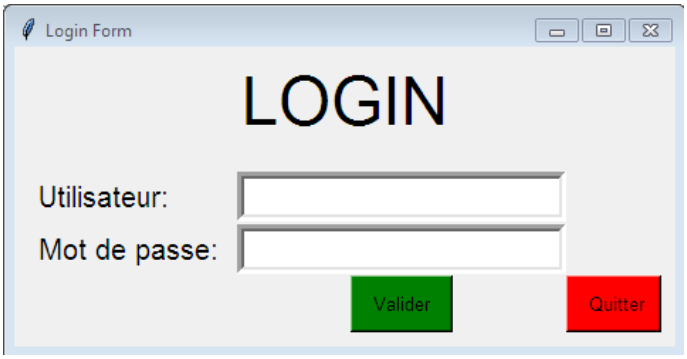

FIGURE 3.7 – Login de l'application

3.4.2 Menu d'application

Après avoir saisi un mot de passe valide par l'administrateur, la fenêtre ci-après s'affiche, elle comporte le menu d'application où pourra sélectionner la tâche à effectuer :

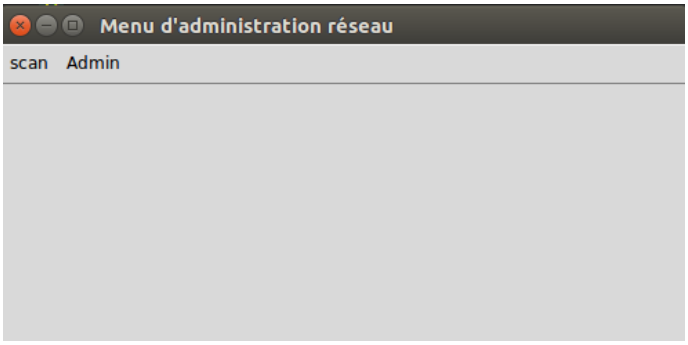

FIGURE 3.8 – Menu de l'application

3.4.3 interface «scanne le réseau»

cette interface permet de contrôler les équipements et collecter les infomations de chaque équipement. Un double-clique sur l'item fait apparaître la fenêtre d'information machine.

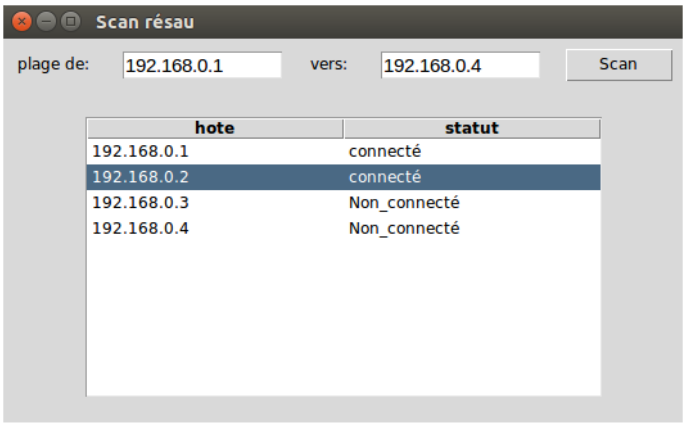

FIGURE 3.9 – scanne réseau

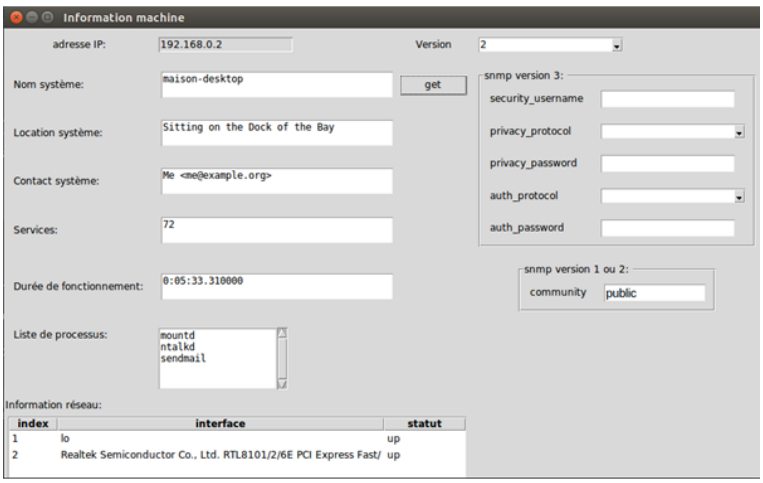

FIGURE 3.10 – information machine

3.4.4 Conclusion

Dans ce dernier chapitre, nous avons présenté, en premier lieu, l'étude conceptuelle de notre projet que nous l'avons élaborer avec UML qui est langage de modélisation très connue et utilisé. Ainsi, nous avons présenté les principaux diagrammes relatifs à notre application comme les diagrammes de cas d'utilisation, de séquence , d'activité et celui des classes. Cette études nous a permit de construire un schéma conceptuelle décrivant l'ossature globale de notre application ainsi que les différentes interactions et relation entre ses différentes entités. Le schéma obtenu ainsi que les règles de passage définies par UML ont été utilisés pour en fin implémenter l'application. Ensuite nous avons décrit les différents outil logiciels utilisés dans le cadre

de l'implémentation de la dite application. Comme nous avons présenté les principales images écrans de notre application. Ces images contiennent des testes réels effectues lors des essais de notre applications. Nous avons essayé de rendre nos programmes les plus claire possibles, pour permettre aux autre étudiant la mise à jour de cette application.

Bibliographie

[1] Camille Rosenthal-Sabroux Alexandre Besse, Jean-Louis Ermine. « modéliser l'organisation». *les pratiques et les procédures pour la réalisation des livres de connaissances*, 2014.

[2] Daly Seif Allah. « etude, conception et réalisation d'un tableau de bord pour la supervision réseau à l'aide d'un outil open source « nagios »». *Mémoire de fin d'étude pour l'optimisation de MASTERE PROFESSIONNEL « Nouvelles Technologies des Télécommunications et Réseaux », Université virtuelle de Tunis*, 2014.

[3] Y. Hammami M.mannai, B. Khabouchi. « développement d'un outil de supervision d'un système d'exploitation». *(Tunisie Télécom) RAPPORT DE PROJET DU FIN D'ETUDES, Université virtuelle de Tunis.*

[4] les diagrammes uml pdf pdf — coderprof.com.

Conclusion générale

L'administration réseau est devenue l'un des profils les plus demandés dans le monde du travail, car toute société, organisme, banque, université, usine, ou autre ne peut plus se passer d'un réseau informatique reliant tous ses postes de travail, en vue de partager ou échanger des données et des informations entre collaborateurs .

Un réseau informatique englobe tous les services qu'il offre comme le mail, le web, le transfert de fichiers, la prise de commande à distance, la ToIP, la vente en ligne, et tous les nouveaux services qui sont en train de voir le jour ou qui verront le jour dans un futur proche. Et donc pour gérer un réseau, il faut avoir certaines compétences, en l'occurrence dans la sécurité, la gestion et la maintenance des différents serveurs, pour que le réseau soit toujours disponible, performant et agréable à utiliser. Notre projet de fin d'étude s'inscrit dans le cadre de l'administration réseau et consiste à concevoir et réaliser une application permettant d'administrer (superviser) le réseau

Pour concrétiser cet objectif nous avons adopte une démarche simple et claire. Dans un premier lieu nous avons identifier les besoins à satisfaire. Après quoi, nous avons procédé à l'étude conceptuelle de notre projet en se servant du langage de modélisation UML. Ainsi nous avons construit les principaux diagrammes à savoir :les diagrammes de cas d'utilisation, de séquence , d'activité et celui des classes. Une fois l'ossature de notre application devenue claire, nous avons entamé l'étape d'implémentation pour laquelle nous avons choisie le langage Python pour ses caractéristiques citées ci-haut.

Ce projet a été pour nous une réelle opportunité pour mettre en œuvre et d'approfondir les connaissances acquises lors de notre cursus universitaire notamment en matière de conception, de programmation réseaux et surtout dans le domaine de l'administration réseau.

Résumé

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 sécurité optimale à toute épreuve. Sachant que plus le nombre des équipements et des services informatiques augmente plus la tâche de les superviser devient trop compliquées ce qui engendre une perte du temps et d'efforts. De ce fait, un outil d'administration réseaux semble être très nécessaire. Dans ce contexte et dans le cadre de notre projet de fin d'études, il nous a été demander de concevoir et réaliser un outil logiciel d'administration réseau permettant à l'administrateur réseau de mieux superviser ses équipements et services avec des efforts et des délais minimes